Jakarta Platform Capabilities

Last updated: November 15, 2019
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 Capabilities................................................................. 8
  Connect................................................................................................. 8
    Supported browsers for Connect......................................................... 8
    Activate Connect................................................................................. 9
    Activate Connect Support................................................................. 13
    Connect interface............................................................................... 17
  Enable or disable Connect notifications globally............................... 26
  Edit which notifications you receive for a conversation....................... 27
  Upload a profile picture....................................................................... 29
  Drag a file into a Connect conversation............................................. 30
  Share a Visual Task Board in a Connect conversation......................... 30
  Mention a user in a Connect conversation......................................... 30
  Connect administration......................................................................... 31
  Connect Chat....................................................................................... 38
  Connect Support................................................................................. 43
Notifications.......................................................................................... 61
  Email and SMS notifications.............................................................. 61
  Push notifications............................................................................... 230
  Subscription-based notifications......................................................... 260
Notify....................................................................................................... 292
  Notify with the Twilio service............................................................ 292
  Outbound communication requirements............................................. 296
  Notify calls......................................................................................... 297
  Using SMS with Notify....................................................................... 298
  Properties for Notify........................................................................... 299
  Notify tables....................................................................................... 299
  Business rules installed with Notify..................................................... 300
  Notify workflow activities................................................................... 301
  Notify languages............................................................................... 311
  Notify on task.................................................................................... 312
  Notify with incident alert.................................................................... 312
  Notify with on-call scheduling............................................................ 317
  Scripting Notify................................................................................. 319
  Activate Notify................................................................................... 346
Legacy Notify....................................................................................... 348
  Working with Legacy Notify............................................................... 348
  Administering Legacy Notify.............................................................. 354
  Installed with Legacy Notify............................................................... 362
  Legacy Notify API.............................................................................. 365
Legacy: Chat......................................................................................... 382
  Legacy: Get started with Chat............................................................ 383
  Legacy: Installed with Chat................................................................. 384
  Legacy: Chat use............................................................................... 387
  Legacy chat administration................................................................. 405
  Legacy: Help desk chat..................................................................... 411
Live Feed............................................................................................... 418
  Live Feed browser support................................................................. 420
  Activate Live Feed.............................................................................. 420
  Administer live feed........................................................................... 420
  Use Live Feed..................................................................................... 441
Configuration Management Database (CMDB)................................................................. 501
Configuration Management and the CMDB................................................................. 502
ITIL Configuration Management integration.............................................................. 503
ITIL.................................................................................................................................. 503
Options to populate the CMDB.................................................................................. 506
Baseline CMDB............................................................................................................ 509
Proposed changes........................................................................................................ 510
CI relationships in the CMDB..................................................................................... 515
CMDB classifications..................................................................................................... 531
Querying the CMDB..................................................................................................... 539
CMDB CI Lifecycle Management.................................................................................. 550
CMDB groups................................................................................................................ 559
CMDB Identification and Reconciliation..................................................................... 561
CMDB Health................................................................................................................ 603
View CMDB benchmarks............................................................................................ 628
Useful related lists in CI forms..................................................................................... 629
Activate the Extended CMDB plugins........................................................................ 629
Help the Help Desk....................................................................................................... 630
Enterprise CMDB......................................................................................................... 641
Table form views.......................................................................................................... 645
Content packs for Configuration Management (CMDB)............................................. 645
Dependency Views....................................................................................................... 646
Components installed with Dependency Views.......................................................... 646
Dependency Views map............................................................................................... 650
Dependency Views map menus and controls.............................................................. 651
Supported browsers for Dependency Views.............................................................. 655
Cluster nodes in a Dependency Views map................................................................. 655
Virtual grouping of nodes in a Dependency Views map............................................... 658
Use Dependency Views............................................................................................... 660
Administer Dependency Views.................................................................................... 665
Compliance................................................................................................................... 675
Compliance Activation................................................................................................. 675
Installed with Compliance............................................................................................ 676
Compliance Templates and Audits............................................................................. 681
Compliance Overview module.................................................................................... 681
Architecture Compliance............................................................................................. 683
Desired State................................................................................................................ 687
Certification audits....................................................................................................... 693
Certification filters........................................................................................................ 710
Certification follow-on tasks...................................................................................... 718
Certification templates............................................................................................... 723
Controls and tests management.................................................................................. 738
Scripted audits.............................................................................................................. 747
Data Certification......................................................................................................... 757
Activate Data Certification......................................................................................... 757
Certification schedules............................................................................................... 764
Certification tasks........................................................................................................ 766
Certification elements................................................................................................. 768
Certification instances............................................................................................... 769
Certification audit instances...................................................................................... 769
Certification audit definition....................................................................................... 770
Data Certification Overview module.......................................................................... 772
Data Certification planning......................................................................................... 775
Data certification performance................................................................................... 786
Reassign a certification task....................................................................................... 793
Send certification task reminders............................................................................... 793
Mark a certification task as closed incomplete.......................................................... 794
Certification tasks cancellation.................................................................................. 795

Content Management System................................................................................. 795
Content Management design.................................................................................. 796
Activate the Content Management System............................................................. 803
Configure Content Management sites.................................................................. 806
Content Management integration points................................................................. 857
Content Management testing.................................................................................. 865
Global search in Content Management................................................................... 865
CMS translation........................................................................................................ 866

Credentials and connection information................................................................. 866
Introduction to credentials..................................................................................... 867
Create credentials................................................................................................... 869
Test your credentials............................................................................................... 899
Credential affinity for Discovery and Orchestration.................................................. 902
Credential tagging for Orchestration activities....................................................... 903
Check IP service affinity for Discovery and Orchestration....................................... 904
External credential storage..................................................................................... 907
Credentials troubleshooting..................................................................................... 925

Edge Encryption...................................................................................................... 927
Understanding Edge Encryption.............................................................................. 927
Planning for Edge Encryption................................................................................ 935
Edge Encryption installation................................................................................... 941
Edge Encryption upgrades..................................................................................... 977
Edge Encryption configuration............................................................................... 982
Edge Encryption ODBC driver integration.............................................................. 1021
Edge Encryption MID Server integration............................................................... 1025

Knowledge Management......................................................................................... 1025
Knowledge Management setup guide for admins.................................................... 1026
Knowledge base setup guide for knowledge admins and managers......................... 1028
Knowledge Management guide for users............................................................... 1029
Knowledge Management roles............................................................................. 1030
Knowledge homepage............................................................................................. 1030
Social Q&A............................................................................................................. 1034
Knowledge feedback............................................................................................... 1039
Request a knowledge base..................................................................................... 1040
Create a knowledge article..................................................................................... 1040
Knowledge manager.............................................................................................. 1048
Knowledge administration...................................................................................... 1061
Use knowledge on mobile devices......................................................................... 1080
Knowledge Management v3 migration.................................................................. 1083
Content packs for Knowledge Management......................................................... 1089
Article versioning.................................................................................................... 1090
Knowledge Management Service Portal............................................................... 1100
Integrating new knowledge portal pages with the service portal.......................... 1123
Knowledge subscriptions......................................................................................... 1133

Managed Documents.............................................................................................. 1137
Managed Document features.................................................................................. 1137
Create a new managed document record............................................................... 1141
Check in a document after making changes........................................................... 1142
Check out a document to make changes................................................................ 1142
Publish a document in Managed Documents....................................................... 1143
Send a document out for review and approval....................................................... 1144
Upload a document as an attachment................................................................... 1144
Defining Document Parameters............................................................................ 1145
Defining Document Workflow............................................................................... 1149

© 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>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge document</td>
<td>1151</td>
</tr>
<tr>
<td>Create a document</td>
<td>1153</td>
</tr>
<tr>
<td><strong>MetricBase</strong></td>
<td>1166</td>
</tr>
<tr>
<td>Request the MetricBase product</td>
<td>1166</td>
</tr>
<tr>
<td>View time series retention policies</td>
<td>1166</td>
</tr>
<tr>
<td>Create a time series metric</td>
<td>1167</td>
</tr>
<tr>
<td>Store time series data</td>
<td>1167</td>
</tr>
<tr>
<td>Analyze time series data</td>
<td>1168</td>
</tr>
<tr>
<td>View time series data</td>
<td>1169</td>
</tr>
<tr>
<td>View MetricBase status</td>
<td>1169</td>
</tr>
<tr>
<td>Debug MetricBase</td>
<td>1169</td>
</tr>
<tr>
<td><strong>MID Server</strong></td>
<td>1169</td>
</tr>
<tr>
<td>Introducing the MID Server</td>
<td>1170</td>
</tr>
<tr>
<td>MID Server heartbeat</td>
<td>1173</td>
</tr>
<tr>
<td>MID Server system requirements</td>
<td>1174</td>
</tr>
<tr>
<td>MID Server version compatibility</td>
<td>1177</td>
</tr>
<tr>
<td>MID Server connection prerequisites</td>
<td>1178</td>
</tr>
<tr>
<td>MID Server installation</td>
<td>1180</td>
</tr>
<tr>
<td>Post installation MID Server administration</td>
<td>1211</td>
</tr>
<tr>
<td>MID Server upgrade</td>
<td>1213</td>
</tr>
<tr>
<td>MID Server configuration</td>
<td>1218</td>
</tr>
<tr>
<td>Advanced MID Server configuration</td>
<td>1281</td>
</tr>
<tr>
<td>The MID Server ECC queue</td>
<td>1291</td>
</tr>
<tr>
<td>MID Server cluster configuration</td>
<td>1295</td>
</tr>
<tr>
<td>MID Server capabilities</td>
<td>1297</td>
</tr>
<tr>
<td>MID Server troubleshooting</td>
<td>1299</td>
</tr>
<tr>
<td><strong>Orchestration</strong></td>
<td>1323</td>
</tr>
<tr>
<td>Introduction to Orchestration</td>
<td>1323</td>
</tr>
<tr>
<td>Activate Orchestration</td>
<td>1326</td>
</tr>
<tr>
<td>Orchestration applications</td>
<td>1346</td>
</tr>
<tr>
<td>Orchestration examples</td>
<td>1478</td>
</tr>
<tr>
<td>Orchestration activity packs</td>
<td>1485</td>
</tr>
<tr>
<td>Orchestration activity designer</td>
<td>1620</td>
</tr>
<tr>
<td>Orchestration databus</td>
<td>1724</td>
</tr>
<tr>
<td>MID Servers for Orchestration</td>
<td>1726</td>
</tr>
<tr>
<td>Use the Orchestration Usage dashboard</td>
<td>1729</td>
</tr>
<tr>
<td><strong>Password Reset and Password Change applications</strong></td>
<td>1730</td>
</tr>
<tr>
<td>Password Reset setup guide</td>
<td>1731</td>
</tr>
<tr>
<td>Password Reset admin guide</td>
<td>1744</td>
</tr>
<tr>
<td>Users: Reset your password on Windows systems</td>
<td>1809</td>
</tr>
<tr>
<td>Users: Enroll in the Password Reset program</td>
<td>1811</td>
</tr>
<tr>
<td><strong>Self-service</strong></td>
<td>1812</td>
</tr>
<tr>
<td>Service catalog requests</td>
<td>1812</td>
</tr>
<tr>
<td>Service Delegation</td>
<td>1822</td>
</tr>
<tr>
<td><strong>Service administration</strong></td>
<td>1825</td>
</tr>
<tr>
<td>Assessments</td>
<td>1825</td>
</tr>
<tr>
<td>Approvals</td>
<td>1973</td>
</tr>
<tr>
<td>Geolocation</td>
<td>1993</td>
</tr>
<tr>
<td>State flows</td>
<td>1998</td>
</tr>
<tr>
<td>Survey Management</td>
<td>2006</td>
</tr>
<tr>
<td>Quizzes</td>
<td>2091</td>
</tr>
<tr>
<td>Wizards</td>
<td>2121</td>
</tr>
<tr>
<td><strong>Service Portal</strong></td>
<td>2131</td>
</tr>
<tr>
<td>Understanding Service Portal</td>
<td>2132</td>
</tr>
<tr>
<td>Understanding Widgets</td>
<td>2200</td>
</tr>
<tr>
<td>Search sources</td>
<td>2345</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>---------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Service Portal security</td>
<td>2360</td>
</tr>
<tr>
<td>Service Portal components</td>
<td>2373</td>
</tr>
<tr>
<td>Service Portal SCSS Primer</td>
<td>2373</td>
</tr>
<tr>
<td>Advanced resources for Service Portal</td>
<td>2379</td>
</tr>
<tr>
<td>Subscription Management</td>
<td>2388</td>
</tr>
<tr>
<td>Subscription Management setup guide</td>
<td>2389</td>
</tr>
<tr>
<td>Subscription Management admin guide</td>
<td>2390</td>
</tr>
<tr>
<td>Survey Management</td>
<td>2409</td>
</tr>
<tr>
<td>Get started with Survey Management</td>
<td>2409</td>
</tr>
<tr>
<td>Survey responses and results</td>
<td>2414</td>
</tr>
<tr>
<td>Survey administration</td>
<td>2432</td>
</tr>
<tr>
<td>Timeline Visualizations</td>
<td>2495</td>
</tr>
<tr>
<td>Activate Timeline Visualization</td>
<td>2497</td>
</tr>
<tr>
<td>Create a Timeline Visualization</td>
<td>2498</td>
</tr>
<tr>
<td>Create a Timeline Visualization view</td>
<td>2502</td>
</tr>
<tr>
<td>Planning Your Timeline Visualization</td>
<td>2502</td>
</tr>
<tr>
<td>Use Timeline Visualization</td>
<td>2503</td>
</tr>
<tr>
<td>Installed with Timeline Visualizations</td>
<td>2510</td>
</tr>
<tr>
<td>Visual Task Boards</td>
<td>2512</td>
</tr>
<tr>
<td>Activate Visual Task Boards</td>
<td>2512</td>
</tr>
<tr>
<td>Installed with Visual Task Boards</td>
<td>2513</td>
</tr>
<tr>
<td>Supported browsers for Visual Task Boards</td>
<td>2516</td>
</tr>
<tr>
<td>Board structure</td>
<td>2516</td>
</tr>
<tr>
<td>Visual Task Board use</td>
<td>2520</td>
</tr>
<tr>
<td>Configure the task board</td>
<td>2545</td>
</tr>
<tr>
<td>Configure Visual Task Board labels</td>
<td>2547</td>
</tr>
<tr>
<td>Modify the query or lane field for an existing board</td>
<td>2547</td>
</tr>
<tr>
<td>Configure the card limit for freeform boards</td>
<td>2548</td>
</tr>
<tr>
<td>Configure the card limit for flexible and guided boards</td>
<td>2548</td>
</tr>
<tr>
<td>Configure the task board card view</td>
<td>2549</td>
</tr>
<tr>
<td>Workflow</td>
<td>2549</td>
</tr>
<tr>
<td>Getting started with workflows</td>
<td>2549</td>
</tr>
<tr>
<td>Workflow editor</td>
<td>2552</td>
</tr>
<tr>
<td>Managing workflows</td>
<td>2561</td>
</tr>
<tr>
<td>Workflow concepts</td>
<td>2651</td>
</tr>
<tr>
<td>Workflow administration</td>
<td>2661</td>
</tr>
<tr>
<td>Troubleshoot workflows</td>
<td>2688</td>
</tr>
<tr>
<td>Use the Workflow Operations Dashboard</td>
<td>2691</td>
</tr>
<tr>
<td>Workflow performance timing</td>
<td>2693</td>
</tr>
<tr>
<td>Workflow activities</td>
<td>2693</td>
</tr>
<tr>
<td>Index</td>
<td>2792</td>
</tr>
</tbody>
</table>
Now Platform Capabilities

The Now Platform® technology delivers a system of action for the enterprise. Using a single data model, it makes it easy to create contextual workflows and automate business processes.

Connect

ServiceNow® Connect is a real-time messaging platform that connects you to your coworkers, bypassing email and static documents.

Connect integrates with other features within the system, such as Visual Task Boards, Human Resources Management, and Customer Service Management. The Connect interface overlays the standard interface, which allows users to participate in conversations while they work.

Connect contains the following features:

- **Connect Chat**: Enables users to chat with individuals and groups, quickly share files, and collaborate on any record by connecting with the right people instantly.
- **Connect Support**: Enables support agents to provide real-time assistance to end users, using queues. Requires the Connect Support plugin.

UI16 or UI15 is required to use Connect.

**Note:**
- Connect does not replace legacy chat but offers some of the same functionality. Do not use these features concurrently.

Supported browsers for Connect

The system supports Connect Chat and Connect Support on most modern browsers.

- The latest public release of Firefox or Firefox ESR
- The latest public release of Chrome
- Safari version 9.1 and later
- Internet Explorer version 11

© 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.
- 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 11 is susceptible to memory leaks, which may impact performance, especially in Windows 7.

**Activate Connect**

Connect is active by default on new instances. For upgraded instances, you can activate the Connect plugin (com.glide.connect) if you have the admin role.

Role required: admin

If you used Collaboration in the Fuji release, the Connect plugin is activated automatically.

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 Connect**

Several types of components are installed with Connect.

**Notifications installed with Connect**

Connect adds the following notifications.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collaboration Offline Group Message(s)</td>
<td>Sends an email notification to offline users when there are new messages in group chats they are members of. Contains a link to open the conversation and a summary of the messages.</td>
</tr>
<tr>
<td>Collaboration Offline Message Bundle</td>
<td>Sends an email notification to offline users when there are new messages in direct chats. Contains a link to open the conversation and a summary of the messages.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ConnectMessagePushNotification</td>
<td>Sends push notifications to users according to their notification preferences. This notification also impacts Connect Support.</td>
</tr>
</tbody>
</table>

### Tables installed with Connect

Connect adds the following tables.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Collaborator (collaborator) | Stores a record for each conversation, for each conversation member.   
Note: The Collaborator table is left over from the Collaborator plugin in Fuji. It is not used in Connect or Live Feed. |
| Connect Action (connect_action) | Stores a record for each Connect action. This table is also used in Connect Support.                                                   |

### Properties installed with Connect

Connect adds the following system properties.

**Note:** To open the System Property (sys_properties) table, enter `sys_properties.list` in the navigation filter.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| collaboration.email_interval | Sets the number of minutes the system waits before sending a Connect notification email to an inactive user.     
- **Type:** integer   
- **Default value:** 3  
- **Location:** Collaborate > Administration > Properties   
- **Learn more:** Configure the email notification interval |
| collaboration.frameset  | Determines whether the Connect overlay is visible (enabled). This property also impacts Connect Support.  
- **Type:** true | false   
- **Default value:** true  
- **Location:** Collaborate > Administration > Properties   
- **Learn more:** Disable the Connect overlay |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>collaboration.polling_interval</td>
<td>Sets the number of seconds the system waits between polling for new Connect messages. This property also impacts Connect Support.</td>
</tr>
</tbody>
</table>
|                                          | - **Type**: integer  
|                                          | - **Default value**: 10  
|                                          | - **Location**: System Property (sys_properties) table                                                                                                                                                                                                                                                                                                                                                                           |
| connect.notification.audio_alert         | Specifies the audio file to play to notify users of new messages, support conversation transfers, and @mentions in Connect. This property's value must point to the **Name** field of a record in the Audio File (db_audio) table. This property also impacts Connect Support.                                                                                                                                                                                                                           |
|                                          | - **Type**: string  
|                                          | - **Default value**: connect_alert.mp3  
|                                          | - **Location**: Collaborate > Administration > Properties  
|                                          | - **Learn more**: Customize the Connect audio notification sound                                                                                                                                                                                                                                                                                                                                                         |
| connect.retrieve_external_link_content   | Enables Connect to render URLs for external sites as links. When this property is disabled, URLs that point anywhere outside the instance appear as plain text. This property also impacts Connect Support.                                                                                                                                                                                                                                                                               |
|                                          | - **Type**: true | false  
|                                          | - **Default value**: true  
|                                          | - **Location**: Collaborate > Administration > Properties                                                                                                                                                                                                                                                                                                                                                                           |
| connect.roles                            | Determines which user roles are required to access Connect. When the value is blank, no role is required. This property also impacts Connect Support.                                                                                                                                                                                                                                                                                                                                                   |
|                                          | - **Note**: If you choose to restrict Connect access to specific roles, consider updating the role requirements for Connect modules and other access points.                                                                                                                                                                                                                                                                                                                                 |
|                                          | - **Type**: string  
|                                          | - **Default value**: <empty>  
|                                          | - **Location**: Collaborate > Administration > Properties                                                                                                                                                                                                                                                                                                                                                                           |
### Name | Description
--- | ---
glide.connect.enabled | Hides the Create or Join Chat Room related link, which appears on the Incident form when legacy chat is enabled. Legacy chat and Connect Chat should not be used concurrently and this property should not be modified.  
| **Type:** true | false  
| **Default value:** true  
| **Location:** Collaborate > Administration > Properties

glide.connect.chat.disabled | Disables and hides all UI elements related to Connect.  
| **Type:** true | false  
| **Default value:** false  
| **Location:** System Property (sys_properties) table

glide.live_feed.task_header_button | Determines whether the show live feed icon ( ) and Follow button are available in the form header of tables that have the live_feed=true dictionary attribute.  
| **Type:** choice list  
| **Default value:** collaboration  
| **Other possible values:**  
| both: enables both the show live feed icon and the Follow button.  
| live_feed: enables the show live feed icon.  
| none: disables both the show live feed icon and the Follow button.  
| **Location:** Collaborate > Administration > Properties  
| **Learn more:** Configure record conversations

### Business rules installed with Connect

Connect adds the following business rules.

<table>
<thead>
<tr>
<th>Business rule</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add message to conversations</td>
<td>Visual Task Board Card (vtb_card)</td>
<td>Generates system messages for conversations created from Visual Task Boards. The messages provide updates when cards are added to the board or moved between lanes.</td>
</tr>
<tr>
<td>Broadcast Chat APNS</td>
<td>Live Feed Message (live_message)</td>
<td>Generates push notifications when new messages are received in a conversation.</td>
</tr>
</tbody>
</table>
### Activate Connect Support

You can activate the Connect Support plugin (com.glide.connect.support) if you have the admin role. This plugin includes demo data.

**Role required:** Admin

If you are currently using the legacy chat feature to provide help desk support, close any open help desk chats before activating Connect Support. Legacy chat and Connect Support should not be used concurrently. When you activate Connect Support, the system automatically sets the state of all Chat Queue Entry (chat_queue_entry) records to **Closed Complete**. This ends any open help desk chats. For more information, see [Migrate from legacy chat to Connect Support](#).

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 Connect Support

Several types of components are installed with Connect Support.
Note: Connect Support also utilizes many of the components installed with Connect Chat.

### Tables installed with Connect Support

Connect Support adds the following tables for system use.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chat Queue Entry Transfer</td>
<td>Stores a record each time an agent transfers a support conversation to another agent.</td>
</tr>
<tr>
<td>(chat_queue_entry_transfer)</td>
<td></td>
</tr>
</tbody>
</table>

### Properties installed with Connect Support

Connect Support adds the following system properties.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>connect.support.conversation_limit</td>
<td>Determines how many support conversations an individual agent can have at one time. When the value is set to -1, an agent can participate in an unlimited number of conversations.</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: -1</td>
</tr>
<tr>
<td></td>
<td>• Location: Collaborate &gt; Support Administration &gt; Properties</td>
</tr>
<tr>
<td>connect.support.idle.delay</td>
<td>Determines how many seconds a user must be inactive in a support conversation before an idle countdown timer appears.</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 120</td>
</tr>
<tr>
<td></td>
<td>• Location: Collaborate &gt; Support Administration &gt; Properties</td>
</tr>
<tr>
<td>connect.support.idle.count_down</td>
<td>Determines how many seconds the idle countdown timer remains open after it appears. If the idle user does not dismiss the timer before the countdown completes, the system closes the support session.</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 60</td>
</tr>
<tr>
<td></td>
<td>• Location: Collaborate &gt; Support Administration &gt; Properties</td>
</tr>
<tr>
<td>connect.support.show_agent_avatar</td>
<td>Determines whether an agent's avatar is shown in a support conversation (enabled). When the property is disabled, users see the agent's name only.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: true</td>
</tr>
<tr>
<td></td>
<td>• Location: Collaborate &gt; Support Administration &gt; Properties</td>
</tr>
</tbody>
</table>
### ServiceNow Jakarta Now Platform Capabilities

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>connect.support.user.closed.conversation_limit</td>
<td>Determines how many closed conversations appear in a user’s support conversation history. When the value is set to 0, all previous conversations appear in the history.</td>
</tr>
<tr>
<td></td>
<td>- Type: integer</td>
</tr>
<tr>
<td></td>
<td>- Default value: 0</td>
</tr>
<tr>
<td></td>
<td>- Location: Collaborate &gt; Support Administration &gt; Properties</td>
</tr>
<tr>
<td>glide.connect.support.enabled</td>
<td>Disables or enables Connect Support. When the property is enabled, the Service Desk Chat button in the Employee Self-Service portal opens the conversation in Connect Support, rather than legacy chat. Additionally, the Support tab appears in the Connect sidebar.</td>
</tr>
<tr>
<td></td>
<td>- Type: true</td>
</tr>
<tr>
<td></td>
<td>- Default value: true</td>
</tr>
<tr>
<td></td>
<td>- Location: Collaborate &gt; Support Administration &gt; Properties</td>
</tr>
<tr>
<td>glide.connect.support.reflect_system_messages</td>
<td>Controls whether Connect Support reflects system messages in records created from a support chat, for example, transfer notices, automated queue messages, etc.</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>
</tbody>
</table>

### Business rules installed with Connect Support

Business rules installed with Connect Support adds the following business rules.

<table>
<thead>
<tr>
<th>Business rule</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNC - Chat Queue Average Wait Time</td>
<td>Chat Queue Entry</td>
<td>Populates the Average wait time field on the Chat Queue table with a calculated value when a support conversation is accepted. The calculation is based on the last 20 support conversations for the queue.</td>
</tr>
<tr>
<td></td>
<td>(chat_queue_entry)</td>
<td></td>
</tr>
<tr>
<td>SNC - Chat Queue Entry Duration</td>
<td>Chat Queue Entry</td>
<td>Populates the Duration field on the Chat Queue Entry table with a calculated value, based on the amount of time the support conversation was open.</td>
</tr>
<tr>
<td></td>
<td>(chat_queue_entry)</td>
<td></td>
</tr>
<tr>
<td>SNC - Reflect Support Record in Q.Entry</td>
<td>Live Group Profile</td>
<td>Populates the Document table and Document ID fields on the Chat Queue Entry table when an agent creates an incident from a support conversation.</td>
</tr>
<tr>
<td></td>
<td>(live_group_profile)</td>
<td></td>
</tr>
</tbody>
</table>
## Additional plugins for Connect Support

Additional plugins are available for Connect Support. These plugins integrate Connect Support with other features and provide capabilities to track performance metrics.

You must have the admin role to activate these additional plugins. For details, see [Activate a plugin](#).

### Additional plugins for Connect Support

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect Support Manager’s Dashboard (com.glide.connect.managers_dashboard)</td>
<td>Provides a homepage for Connect Support, and all required configuration records. Though the plugin name contains the term dashboard, the plugin does not provide functionality related to Performance Analytics dashboards. Homepages are similar to dashboards, but do not require Performance Analytics roles to view. &lt;br&gt;&lt;br&gt;<strong>Note:</strong> The Connect Support Manager’s Dashboard plugin does not activate Connect Support automatically. You must activate Connect Support to collect data for the homepage.</td>
</tr>
</tbody>
</table>
| Human Resources Application: HR Connect (com.snc.hr.hr_connect) | Sets up a human resources (HR) chat queue and makes it available on the HR Service Portal. The Human Resources Application: HR Connect plugin activates these related plugins if they are not already active:  
  - **Human Resources Application: Core** (com.snc.hr.core): Provides basic HR features. |
| Performance Analytics - Content Pack - Service Desk Chat (com.snc.pa.chat) | Provides the Service Desk Chat Monitor dashboard, which analyzes key Connect Support metrics and indicators. The Performance Analytics - Content Pack - Service Desk Chat plugin activates these related plugins if they are not already active:  
  - **Connect Support Manager’s Dashboard** (com.glide.connect.managers_dashboard): See description in this table. |
### Connect interface

Users can work in a compact view of Connect, which overlays the standard user interface, or in a full-screen workspace.

Connect Chat and Connect Support share the same interface, so support agents can keep track of all their conversations in one place.

### Connect overlay

The Connect overlay appears over the standard user interface. It consists of the Connect sidebar and any Connect mini windows that are open.

---

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Description</th>
</tr>
</thead>
</table>
| Performance Analytics - Context Sensitive Analytics for Chat (com.snc.pa.chat.context_sensitive_analytics) | Provides in-form analytics for Connect Support. These analytics are available as a related link on the Chat Queue Entry (chat_queue_entry) form, and also as the **Context Sensitive Analytics - Chat** dashboard. The Performance Analytics - Context Sensitive Analytics for Chat plugin activates these related plugins if they are not already active:  
**Note:** An administrator can **disable** the Connect overlay so users can only use the Connect workspace, a full-screen interface with additional Connect tools.

**Connect sidebar**

The Connect sidebar is the primary interface for Connect Chat and Connect Support. It lists your conversations and provides access to create new conversations.

The sidebar is collapsed by default. Click the toggle Connect sidebar icon (.twig) in the banner frame to expand or collapse the sidebar, which appears on the right edge of the interface.

**Connect Chat**

The chat view of the sidebar is available to all users. If Connect Support is enabled, users must click the chat tab of the sidebar, which is represented by a speech bubble icon. If Connect Support is not enabled, there are no tabs in the sidebar and the chat view displays by default.

The chat view of the sidebar lists all your current Connect Chat conversations. It also contains a filter tool and a button to create new conversations.
If you have unread messages in a conversation, a number appears by the conversation in the sidebar. Point to a conversation and click the x icon to remove the conversation from the sidebar.

**Connect Support**

The support view of the sidebar is available when Connect Support is activated. The support view is visible only to users who are agents for at least one support queue. Users must click the support tab of the sidebar, which is represented by a headset icon.

The support view displays Queues to which you belong. It also displays your open support conversations under Cases.
If you have unread messages in a conversation, a number appears by the conversation in the sidebar.

Support view of the Connect sidebar

Connect mini windows

When you open a Connect Chat or Connect Support conversation in the Connect overlay, it opens in a Connect mini window. Each mini window contains a header, a conversation area, and a message field.

Several icons appear in the mini window header and by the message field.

**Note:** The icons you see for each conversation depend on the conversation type and other conditions.
### Chat mini window icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Add user" /></td>
<td>Add user</td>
<td>Add a user to the conversation. This icon is visible for group and record conversations only. Administrators can enable this icon for Connect Support conversations.</td>
</tr>
<tr>
<td><img src="image" alt="View document" /></td>
<td>View document</td>
<td>View the record associated with the conversation. This icon is visible for record and support conversations only.</td>
</tr>
<tr>
<td><img src="image" alt="New window" /></td>
<td>New window</td>
<td>Open the conversation in the Connect workspace, a full-screen window with additional Connect tools.</td>
</tr>
<tr>
<td><img src="image" alt="Collapse/Expand conversation" /></td>
<td>Collapse/Expand conversation</td>
<td>Hide or show the conversation. Alternatively, click anywhere in the mini window header to the left of the icons.</td>
</tr>
<tr>
<td><img src="image" alt="Close window" /></td>
<td>Close window</td>
<td>Close the mini window. The conversation remains in the Connect sidebar and the history is preserved when you reopen the conversation. You can also close a mini window by pressing the Escape key.</td>
</tr>
<tr>
<td><img src="image" alt="Connect actions" /></td>
<td>Connect actions</td>
<td>Open the Connect actions menu, which contains options like Transfer and Create Incident. This icon is visible only when Connect actions are available for the conversation. By default, this icon is visible for support conversations only. Administrators can add options to this menu by creating new Connect actions.</td>
</tr>
<tr>
<td><img src="image" alt="Message type" /></td>
<td>Message type</td>
<td>Choose whether messages are added to the associated record as comments or work notes. This icon is visible only for record and support conversations.</td>
</tr>
<tr>
<td><img src="image" alt="Attach file" /></td>
<td>Attach file</td>
<td>Attach and send a file. Select one or more files and click Open. You can also add an attachment by dragging and dropping it directly in the conversation.</td>
</tr>
</tbody>
</table>
Connect workspace

The Connect workspace is a full-screen view of all your Connect Chat and Connect Support conversations in one place. It provides additional tools to help keep track of important information in conversations.

To open the Connect workspace, navigate to Collaborate > Connect Chat or click the new window icon (확장) in a Connect mini window. If you do not have any recent conversations, a screen appears with helpful information about Connect.

The Connect workspace is composed of the following elements.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sidebar</td>
<td>Provides access to conversations. The Connect sidebar behaves the same way in the workspace as it does in the Connect overlay. The only difference is that the sidebar appears on the left edge of the Connect workspace. For more information about using the sidebar, see Connect sidebar.</td>
</tr>
<tr>
<td>Conversation pane</td>
<td>Displays the currently selected conversation.</td>
</tr>
<tr>
<td>Conversation tools</td>
<td>Provides quick access to key information, conversation members, attachments, and notification preferences for the currently selected conversation. Some of the conversation tools vary depending on the type of conversation.</td>
</tr>
</tbody>
</table>
Connect workspace
Conversation pane

The conversation pane of the Connect workspace displays the conversation header and an expanded version of the mini window.

The header displays basic conversation details like the avatar and name. You can edit these details for group or record conversations.

Below the header, messages appear in chronological order. You can enter messages in the text entry field at the bottom of the window.

Connect conversation tools

The conversation tools area in the Connect workspace contains several tabs, each represented by an icon.

Click an icon to open the tab. Click the same icon again to hide the tab. The tabs you see for each conversation depend on the conversation type and other conditions.

### Conversation tool tabs

<table>
<thead>
<tr>
<th>Tab icon</th>
<th>Tab name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="#" alt="Info" /></td>
<td>Info</td>
<td>Contains the following sections, each of which appears only if it contains information.</td>
</tr>
<tr>
<td></td>
<td>Record</td>
<td>Contains sections, each of which appears only if it contains information.</td>
</tr>
<tr>
<td></td>
<td>Related Records</td>
<td>Lists Visual Task Boards and task records that have been referenced in the conversation, such as incidents, problems, or changes. When you send a record number as a message or drag a record in a conversation, it appears as a link. The list displays the short description for each task. Click a task to open the record in a new browser tab. Only conversation members who have rights to view the tasks can access them.</td>
</tr>
<tr>
<td></td>
<td>Links</td>
<td>Lists URLs that have been referenced in the conversation. Click a link to open the destination page in a new browser tab. This tab is not available for support conversations.</td>
</tr>
<tr>
<td><img src="#" alt="Record" /></td>
<td>Record</td>
<td>Displays a compact form view of a record created from the current conversation, such as an incident. If more than one record has been created from the conversation, there is a separate record tab for each one. These tabs are available only for support conversations.</td>
</tr>
<tr>
<td><img src="#" alt="Knowledge Base" /></td>
<td>Knowledge Base</td>
<td>Displays a compact view of the knowledge homepage. For more information, see Share knowledge in a Connect Support conversation.</td>
</tr>
<tr>
<td><img src="#" alt="Members" /></td>
<td>Members</td>
<td>Lists all members of the current conversation. You can add or remove conversation members for group and record conversations.</td>
</tr>
<tr>
<td><img src="#" alt="Attachments" /></td>
<td>Attachments</td>
<td>Lists all attachments in the conversation. Click an attachment to open it. Click Add Attachment to upload an attachment.</td>
</tr>
<tr>
<td><img src="#" alt="Notification preferences" /></td>
<td>Notification preferences</td>
<td>Contains settings to control which notifications you receive for the current conversation. For more information, see Edit which notifications you receive for a conversation.</td>
</tr>
</tbody>
</table>
Enable or disable Connect notifications globally

You can edit your Connect notification settings globally to enable or disable mobile, desktop, email, or audio notifications for all your Connect Chat and Connect Support conversations.

Role required: none

By default, Connect mobile, email, and audio notifications are enabled globally. You must enable desktop notifications.

An administrator can customize the sound used for audio notifications.

**Note:** You receive mobile notifications only if you have installed the ServiceNow mobile app.

1. In the banner frame, click the gear icon (⚙️) to open the system settings.
2. In the system settings window, click the **Notifications** tab.
3. In Notifications by Category, navigate to **Connect**.
4. Enable or disable Connect mobile, desktop, email, or audio notifications.
5. Optional: Configure the following system notifications. For more information on how to configure system notifications, see [Apply notification conditions](#).

<table>
<thead>
<tr>
<th>Notification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity Stream @Mention Email</td>
<td>Sends an email alert to a user anytime they get @mentioned in an activity stream</td>
</tr>
<tr>
<td>Collaboration Offline Group Message(s)</td>
<td>Sends email to offline users who are members of a group conversation after a certain number of minutes determined by the <code>collaboration.email_interval</code> property to limit spam. <strong>Note:</strong> It takes 90 seconds after a user logs out for the system to register that the user is offline. If a message is sent to the user within 90 seconds of them logging out, then the user does not receive the notification.</td>
</tr>
<tr>
<td>Collaboration Offline Message Bundle</td>
<td>Sends email to offline users after a certain number of minutes determined by the <code>collaboration.email_interval</code> property to limit spam. <strong>Note:</strong> It takes 90 seconds after a user logs out for the system to register that the user is offline. If a message is sent to the user within 90 seconds of them logging out, then the user does not receive the notification.</td>
</tr>
<tr>
<td>ConnectMessagePushNotification</td>
<td>Uses a push notification to inform users when there are new messages in a conversation</td>
</tr>
<tr>
<td>Notification</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ConnectNotificationPushNotification</td>
<td>Uses a push notification to inform a user when they have been @Mentioned in a record</td>
</tr>
</tbody>
</table>

Edit which notifications you receive for a specific conversation.

**Connect notification browser support**

The following browsers support Connect chat notifications.

**Connect chat browser support**

<table>
<thead>
<tr>
<th>Browser</th>
<th>Enable notification steps</th>
</tr>
</thead>
</table>
| Chrome                                                          | 1. From a Chrome window, click the Chrome menu in the upper right corner.  
2. Go to Settings > Show advanced settings... > Privacy > Content settings.  
3. In the Content settings window, from the notifications section, select your notification settings. |
| Mozilla Firefox (starting with version 44)                      | Manage browser notification settings using the information icon next to the URL.          |
| Safari (starting with OS X Mavericks)                           | 1. From a Safari window, open Preferences.  
2. Select the notifications tab.  
3. Select Allow or Deny to control which websites have access to notifications. |
| Microsoft Edge                                                  | Notifications are enabled by default on Windows 10 PCs and tablets starting with EdgeHTML 14. For more information, see [https://blogs.windows.com/msedgedev/2016/05/16/web-notifications-microsoft-edge/#pVkwubg7uvROayy1.97](https://blogs.windows.com/msedgedev/2016/05/16/web-notifications-microsoft-edge/#pVkwubg7uvROayy1.97). |

**Note:** Internet Explorer does not support Connect notifications out of box.

**Edit which notifications you receive for a conversation**

You can control which types of Connect notifications you receive for each conversation and when you receive them.

**Role required:** none

Connect can send mobile, desktop, email, and audio notifications to inform you of messages and other activity, when you are not actively viewing Connect. You can edit your notification preferences in each conversation to control which notifications you receive for the conversation and under what circumstances. For example, if you are a member of a large group conversation, you might want to receive mobile, desktop, and email notifications for all activity, and audio
notifications only when someone mentions you. You might also want to disable a certain type of notification entirely for a conversation.

By default, you receive mobile, email, and audio notifications for all activity in every conversation you belong to. You must enable desktop notifications manually. Not all browsers allow desktop notifications. For more information, see Enable or disable Connect notifications globally.

An administrator can customize the sound used for audio notifications.

**Note:** You receive mobile notifications only if you have installed the ServiceNow mobile app.

1. Open a conversation in the Connect workspace.
2. In the conversation tools to the right of the conversation, click the notification settings tab (奂).
3. Edit the following settings according to your preferences.

**Note:** If a notification type is disabled globally, a link to enable that type appears. You must click the link before you can edit conversation-specific notification settings.

<table>
<thead>
<tr>
<th>Mobile Notification Settings</th>
<th>Choose to receive push notifications:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• For all activity</td>
</tr>
<tr>
<td></td>
<td>• Only when @ mentioned (this option is not available for direct conversations)</td>
</tr>
<tr>
<td></td>
<td>• Never</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Desktop Notification Settings</th>
<th>Choose to receive desktop notifications:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• For all activity</td>
</tr>
<tr>
<td></td>
<td>• Only when @ mentioned (this option is not available for direct conversations)</td>
</tr>
<tr>
<td></td>
<td>• Never</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Email Settings</th>
<th>Choose to receive email notifications:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• For all activity</td>
</tr>
<tr>
<td></td>
<td>• Only when @ mentioned (this option is not available for direct conversations)</td>
</tr>
<tr>
<td></td>
<td>• Never</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Audio Notification Settings</th>
<th>Choose to receive audio notifications:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>ServiceNow</td>
<td>Jakarta</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>
</tbody>
</table>

**Upload a profile picture**

You can upload a profile picture in your Live Feed profile to use as an avatar in Connect Chat and Connect Support conversations.

Role required: none

Users who do not have profile pictures are represented by an avatar with their initials.

Administrators can upload a profile picture in a user record which displays if there is no Live Feed photo.

1. Navigate to Collaborate > Live Feed.
2. Click the tile with your picture or initials and title.

3. Use one of the following actions to add your photo.
   - Locate the photo file you want to use and drag it over the existing photo.
   - Point to the existing picture (or tap the photo in the smartphone or tablet interface) to display the Upload a picture link. Click the link, navigate to the location of the photo you want to use, and click Open.
**Drag a file into a Connect conversation**

Drag and drop functionality in Connect Chat and Connect Support provides an easy way to share external attachments and links or items from within your instance.

Role required: none

You can drag several things from within an instance, including items from the application navigator, records or breadcrumbs from lists, and Visual Task Boards from the My Task Boards page.

- Drag an item in a Connect mini window.
- To drag a record from a list, drag the reference icon, the record number, or a reference column value.
- Connect accepts the same file extensions as the platform. For more information, see [Add and manage attachments](#).

**Share a Visual Task Board in a Connect conversation**

You can share a Visual Task Board in a Connect Chat or Connect Support conversation.

Role required: none

1. Navigate to **Self-Service > Visual Task Boards**.
2. Drag a task board to a Connect mini window.
   - A link to the task board appears in the conversation. The task board is also listed in the conversation tools, which are visible in the Connect workspace. Only conversation members who are members of the board can access it. If you share a task board in a [record conversation](#), it appears as a URL in the record activity stream.

**Mention a user in a Connect conversation**

You can get someone's attention in a group conversation by mentioning them.

Role required: none
Users can set their notification preferences so they receive notifications only when they are mentioned. Mentioning a user creates a shortcut to view their basic information and send them a direct message.

1. Open a Connect group conversation.
2. In the message field, type the @ character. A suggestion menu appears with the names of the conversation members.
3. Select the person you want to mention and send the message.

Connect administration

Administrators can configure various performance settings and features that impact both Connect Chat and Connect Support.

Note: There are also administrative options specifically for Connect Chat or Connect Support. For more information, see Connect Chat administration and Connect Support administration.

Properties for Connect

The Connect Properties page provides several configuration options for Connect.
These properties are available for Connect. Users with the admin role can access these properties by navigating to **Collaborate > Administration > Properties**.

**Note:** Many of the properties also impact Connect Support.

### Properties for Connect

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Type</th>
<th>Default value</th>
<th>Location</th>
<th>Learn more</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable Presence glide.ui.presence.disabled</td>
<td>Turns off user presence globally when enabled. Enabling this property turns off user presence throughout the platform, not just in Connect.</td>
<td>true</td>
<td>false</td>
<td>Collaborate &gt; Administration &gt; Properties</td>
<td>User presence</td>
</tr>
<tr>
<td>Enable Connect in the frameset collaboration.frameset</td>
<td>Determines whether the Connect overlay is visible (enabled). This property also impacts Connect Support.</td>
<td>true</td>
<td>false</td>
<td>Collaborate &gt; Administration &gt; Properties</td>
<td>Disable the Connect overlay</td>
</tr>
<tr>
<td>Enable Connect to retrieve external link metadata in order to render richer content in messages with links to YouTube, news articles, images, etc. connect.retrieve_external_link_content</td>
<td>Enables Connect to render URLs for external sites as links. When this property is disabled, URLs that point anywhere outside the instance appear as plain text. This property also impacts Connect Support.</td>
<td>true</td>
<td>true</td>
<td>Collaborate &gt; Administration &gt; Properties</td>
<td>Disable the Connect overlay</td>
</tr>
<tr>
<td>Number of minutes to wait before collecting unread messages and sending an email to offline users. collaboration.email_interval</td>
<td>Sets the number of minutes the system waits before sending a Connect notification email to an inactive user.</td>
<td>integer</td>
<td>3</td>
<td>Collaborate &gt; Administration &gt; Properties</td>
<td>Configure the email notification interval</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audio file to play to notify users of new messages, support conversation transfers and @mentions in Connect. This property’s value should point to the ‘name’ field of an audio file in the db_audio table. connect.notification.audio_alert</td>
<td>Specifies the audio file to play to notify users of new messages, support conversation transfers, and @mentions in Connect. This property’s value must point to the Name field of a record in the Audio File (db_audio) table. This property also impacts Connect Support.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Default value: connect_alert.mp3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Location: Collaborate &gt; Administration &gt; Properties</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Learn more: Customize the Connect audio notification sound</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comma separated whitelist of roles able access Connect. Empty allows all roles. connect.roles</td>
<td>Determines which user roles are required to access Connect. When the value is blank, no role is required. This property also impacts Connect Support.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: If you choose to restrict Connect access to specific roles, consider updating the role requirements for Connect modules and other access points.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Default value: &lt;empty&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Location: Collaborate &gt; Administration &gt; Properties</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Determine whether or not a button is shown in task forms to view the Collaboration document conversation or Live Feed Record Feed related to the task. Note: The Collaboration button will only be enabled if the frameset view is also enabled with collaboration.frameset = true glide.live_feed.task_header_button</td>
<td>Determines whether the show live feed icon ( ) and Follow button are available in the form header of tables that have the live_feed=true dictionary attribute.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Type: choice list</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Default value: collaboration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Other possible values:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• both: enables both the show live feed icon and the Follow button.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• live_feed: enables the show live feed icon.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• none: disables both the show live feed icon and the Follow button.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Location: Collaborate &gt; Administration &gt; Properties</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Learn more: Configure record conversations</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configure the polling interval

The polling interval determines how frequently the system polls for new Connect messages.

Role required: admin

The default interval is 10 seconds. You can change this value. The shorter the polling interval, the more frequently the system checks for new messages and the greater the impact on performance.

**Note:** This setting impacts Connect Chat and Connect Support.

1. Navigate to `sys_properties.list`.
2. Locate the `collaboration.polling_interval` property.
3. Set the **Value** to a different number of seconds.

   Setting the polling interval to a value smaller than 2 is likely to tax the system too heavily, while a value greater than 10 is likely to result in a poor user experience.

### Disable the Connect overlay

The Connect overlay is enabled by default and is integrated with the standard user interface. You can disable the Connect overlay.

Role required: admin

To disable the Connect overlay and remove the toggle Connect sidebar icon from the banner frame, set the `collaboration.frameset` property to `false`.

1. Navigate to **Collaborate > Administration > Properties**.
2. Locate the property called `Enable Connect in the frameset (collaboration.frameset)` and clear the check box.
3. Click **Save**.

When the frameset is disabled, any Connect chats open in the Connect workspace. For more information on completely disabling Connect Chat, see [Disable Connect Chat](#).

### Customize the Connect audio notification sound

You can replace the default Connect audio notification sound with an audio file of your choice. *Upload the audio file* you want to use as the notification sound.

Role required: admin
The audio notification sound is used for all Connect conversation types, including Connect Support conversations.

1. Navigate to **System UI > Audio Files**.
2. Locate the audio file you want to use as the notification sound and copy the **Name** value.
3. Navigate to **Collaborate > Administration > Properties**.
4. Locate the property called **Audio file to play to notify users of new messages, support conversation transfers and @mentions in Connect** (`connect.notification.audio_alert`) and replace the default value with the name of the audio file.
5. Click **Save**.

End users receive audio notifications when sending and receiving support chats. Support agents only receive audio notifications for inbound chats when the chat window is not in focus.

**Administer Connect actions**

You can create or modify Connect actions to provide custom functionality in Connect Chat or Connect Support conversations.

If you want to customize the icon for a Connect action, navigate to **Collaborate > Administration > Action Icons** to view the available icons and their class names. Note the class name of the icon you want to use.

**Role required:** admin

The Connect action menu appears by the message entry field when one or more Connect actions are available for a conversation, based on defined conditions. When a user selects a Connect action, the system runs the script defined for that action.

1. Navigate to **Collaborate > Administration > Actions**.
2. Click **New** or open an existing Connect action.
3. Complete the Connect Action form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition</td>
<td>JavaScript condition statement that must return true for the action to be available in a conversation. For example, to show the action in Connect Support conversations only, enter `conversation.type === &quot;support&quot;</td>
</tr>
<tr>
<td>Hint</td>
<td>This field is not used.</td>
</tr>
<tr>
<td>Icon Class Name</td>
<td>Class name of icon to use. To view all available icons and their class names, navigate to <strong>Collaborate &gt; Administration &gt; Action Icons</strong>.</td>
</tr>
<tr>
<td>Order</td>
<td>Order of the action relative to other items in the Connect action menu.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Script</td>
<td>Script to execute when the action is run. For example, to create a new incident based on the conversation, enter the following code:</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>response.newRecord(&quot;incident&quot;, {</td>
</tr>
<tr>
<td></td>
<td>short_description:</td>
</tr>
<tr>
<td></td>
<td>conversation.document.short_description</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>caller_id:</td>
</tr>
<tr>
<td></td>
<td>conversation.document.opened_by</td>
</tr>
<tr>
<td></td>
<td>});</td>
</tr>
<tr>
<td></td>
<td>For information about the response object, see the API reference documentation.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You can only create a Connect action based on a task table.</td>
</tr>
<tr>
<td>Shortcut</td>
<td>Text that triggers the action when entered after the &quot;/&quot; character in a conversation.</td>
</tr>
<tr>
<td>Title</td>
<td>Text that appears in the Connect action menu. The title for each Connect action should be unique.</td>
</tr>
</tbody>
</table>
Configure the fields on a record card in Connect

When a record is either linked to or create from a Connect conversation, the details of the record display as a card in the chat window.

The card view only applies to the full Connect page and the end user view of Connect Support conversations.

Role required: admin

1. Navigate to the form you want to configure fields for.
2. Right-click the header and select Configure > Form Layout.
3. Under the Form View section, select the Connect view.
You may need to create a Connect view for the form. For more information on creating a form view, see Create and delete views.

4. Select the fields to appear on the card by adding or removing the fields from the Selected column. You can also adjust the order they appear on the form by moving the fields up or down.

You cannot remove the Author or the Updated fields from the card regardless of whether they are on the view or not. The card always shows the Short Description field in the top even if it is in a different order in the list.

Connect Chat

Connect Chat is a real-time messaging tool that enables users to chat with individuals and groups, quickly share files, and collaborate on any record by connecting with the right people instantly.

Connect Chat animates communication around records, Visual Task Boards, topics of interest, or groups of people.

Features include:

- Direct conversations between two users.
- Group conversations between three or more users.
- Conversations linked to records. Comments and work notes appear in conversations in real time and users can update the record directly from the conversation.
- Drag-and-drop sharing of links, files, and records.

UI16 or UI15 is required to use Connect Chat.

This video demonstrates how to use Connect Chat.

This video demonstrates how to use Connect Support.

Note:

- Connect Chat does not replace legacy chat but offers some of the same functionality. The features should not be used concurrently.

Connect Chat use

All users have access to Connect Chat, a convenient way to stay updated on all the people and documents you work with in a familiar chat interface.

You can start using Connect Chat right away with virtually no setup. Connect Chat supports a few different types of conversations so you can use it as a social tool or a quick way to follow specific records.

Start a direct or group conversation

You can start a conversation with one or more users in Connect Chat.

Role required: none

A conversation between two users is called a direct conversation. A conversation between three or more users is called a group conversation.

1. In the chat view of the Connect sidebar, click the plus icon (⁺) by the filter.
   A Connect mini window appears.
2. In the To field, enter the name of the user you want to chat with. Suggestions appear as you type.
3. Optional: Enter additional names to create a group conversation. You can add or remove group conversation members later. You cannot add members to a direct conversation after you create it.
4. Press the Enter key to shift focus to the message field.
5. Send a message to create the conversation. The conversation is added to the Connect sidebar for quick access.

**Follow a record in Connect**

You can follow a record in Connect Chat to track activity as it happens, in a familiar chat interface. When you follow a record, you become a member of a record conversation.

Role required: whichever role is required to access the record you want to follow in Connect

You must first activate the Connect (com.glide.connect) plugin to complete this task.

Any record conversation you create in Connect becomes a record feed in live feed, and vice versa. Unlike direct or group conversations, all messages in record conversations are comments or work notes.

**Note:** By default, record conversations are enabled for all tables that extend Task (task). Administrators can enable record conversations for additional tables or disable them if desired.

1. Navigate to a task record.
2. Do one of the following actions.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Follow the record</td>
<td>1. In the form header, click <strong>Follow</strong>. The system adds you as a member of the record conversation, but does not open the conversation. You can open the conversation from the Connect sidebar.</td>
</tr>
<tr>
<td>Follow the record and open a chat mini window</td>
<td>1. In the form header, click the down arrow in the <strong>Follow</strong> button. 2. Select <strong>Open Connect Mini</strong>. The system adds you as a member of the record conversation and opens it in a Connect mini window.</td>
</tr>
<tr>
<td>Follow the record and open the Connect workspace</td>
<td>1. In the form header, click the down arrow in the <strong>Follow</strong> button. 2. Select <strong>Open Connect Full</strong>. The system adds you as a member of the record conversation and opens it in the Connect workspace, the full-screen view.</td>
</tr>
</tbody>
</table>

The **Follow** button is relabeled **Following**.

3. Add comments or work notes to the record directly from Connect.
Any comments or work notes added to the record appear in the record conversation. Likewise, comments and work notes you add to the conversation appear on the record.

a) In the record conversation, by the text entry field, click the message type icon.

b) Select Comment or Work Note.

c) Enter a message.

By default, record conversation messages are added as comments.

**Note:** If you add an attachment to a record conversation, it is attached to the underlying record as well.

*Edit your notification settings* for the record conversation.

**Edit basic conversation details**

In Connect Chat, you can customize the avatar, name, and description for a group or record conversation.

Role required: none

These details are not editable for direct conversations.

**Note:** The name and description for a record conversation default to the record name and short description. However, editing the name or description for a record conversation does not change anything on the underlying record.

1. Open the a group or record conversation in the Connect workspace.
2. Click anywhere in the conversation header to the left of the icons. A pop-up appears to edit conversation details.
3. Edit the conversation image, name, and description as needed.
4. Click Save.

**Add or remove conversation members**

In Connect Chat, any member of a group or record conversation can add or remove other conversation members. In a direct conversation with only two people, you cannot add members to the conversation after you create it.

Role required: none

1. Open a group or record conversation in the Connect workspace.
2. In the conversation tools to the right of the conversation pane, click the member list tab.
3. Do one of the following actions.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a member</td>
<td>1. Click Add Member to Group.</td>
</tr>
<tr>
<td></td>
<td>2. Use the search field to find and select a user.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Remove a member</td>
<td>1. Point to a member name.</td>
</tr>
<tr>
<td></td>
<td>2. Click the minus icon (-).</td>
</tr>
</tbody>
</table>

**Create a Connect conversation from a Visual Task Board**

Create a Connect Chat conversation from a Visual Task Board to collaborate with board members and keep track of activity as it happens.

Role required: none

When you create a conversation from a task board, all the board members become members of the conversation. The members are synchronized between the task board and the conversation. For example, if you remove a user from the conversation, the system automatically removes the user from the board as well.

1. Navigate to **Self-Service > Visual Task Boards**.
2. Open a task board.
3. In the board header, click the connect with board members icon ( ).

The system automatically opens a record conversation for the board. Each board member becomes a member of the conversation.

**Connect Chat administration**

Administrators can configure various performance settings and features of Connect Chat.

**Note:** There are also settings that apply to both Connect Chat and Connect Support. For more information, see [Connect administration](#).

**Configure the email notification interval**

The email notification interval determines how long the system waits before sending a Connect Chat email notification to an inactive user.

Role required: admin

The default interval is 3 minutes. You can change this value.

1. Navigate to **Collaborate > Administration > Properties**.
2. Locate the property called **Number of minutes to wait before collecting unread messages and sending an email to offline users. (collaboration.email_interval)** and set the value to a different number of minutes.
3. Click **Save**.

When an offline user is sent a Connect message, the collaboration.new_offline_message event fires. The system waits the amount of time provided in the collaboration.email_interval property, then triggers the collaboration.notify_offline_user and collaboration.notify_offline_user.group events (depending on if the conversation was peer to peer or a group conversation). The sysevent_email_action record listens for collaboration.notify_offline_user(.group) then builds an email notification containing all the messages from the last collaboration.email_interval minutes that the user has received in that conversation.
Enable record conversations for a table

Record conversations are enabled for all tables that extend Task (task) by default. You can configure record conversations for additional tables that extend Task.

Role required: admin

To create record conversations, users must have access to the **Follow** button in the form header. To show the button and thus enable record conversations for a table, the following conditions must be true.

- The `live_feed` dictionary attribute must be set to **true** for the table.
  - By default, `live_feed=true` for all tables that extend Task (task).
- The `glide.live_feed.task_header_button` property must be set to **both** or **collaboration**.
  - By default, `glide.live_feed.task_header_button` is set to **collaboration**.

1. Navigate to the list view of a table for which you want to enable record conversations.
2. Perform the appropriate action for the list version.

<table>
<thead>
<tr>
<th>Version</th>
<th>Action</th>
</tr>
</thead>
</table>
| List v3   | 1. Click the list title menu and select **Configure**.  
2. In the Configure window, click **Dictionary**. |
| List v2   | Right-click any column header and select **Configure > Dictionary**. |

The list of dictionary entries for the table appears.

3. Open the dictionary entry that has **Type** set to **Collection**.
   The Dictionary Entry form appears.
4. In the **Attributes** related list, click **New**.
   The Dictionary Attribute form appears.
5. In the **Attribute** field, enter **Live feed**.
6. In the **Value** field, enter **true**.
7. Click **Submit**.
8. Navigate to **Collaborate > Administration > Properties**.
9. Locate the property called **Determine whether or not a button is shown in task forms to view the Collaboration document conversation or Live Feed Record Feed related to the task** (`glide.live_feed.task_header_button`).
10. Ensure the property is set to **both** or **collaboration**.

   The `glide.live_feed.task_header_button` property also controls whether the show live feed icon appears. If the property is set to **collaboration**, the show live feed icon does not appear on form headers.

Prevent users from following records in Connect for all tables

Users can follow records in Connect for any table that extends Task (task) by default. You can disable this functionality for all tables.

Role required: admin
To disable record conversations for all tables, prevent the **Follow** button from appearing in all form headers by editing the `glide.live_feed.task_header_button` property.

1. Navigate to `sys_properties.list`.
2. Locate the `glide.live_feed.task_header_button` property.
3. Set the **Value** to `live_feed`.

### Prevent users from following records in Connect for a specific table

Users can follow records in Connect for any table that extends Task (task) by default. You can disable this functionality for a specific table.

**Role required:** admin

To disable record conversations for a specific table, prevent the **Follow** button from appearing in form headers for the table. To do so, set the `live_feed` dictionary attribute to `false` for the table.

1. Navigate to the list view of a table for which you want to disable record conversations.
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 any column header and select Configure &gt; Dictionary.</td>
</tr>
<tr>
<td>List v3</td>
<td>Open the list title menu and select Configure, and then select Dictionary.</td>
</tr>
</tbody>
</table>

The list of dictionary entries for the table appears.

3. **Open the dictionary entry that has Type set to Collection.**
   The Dictionary Entry form appears.
4. **In the Attributes related list, locate the Live feed dictionary attribute.**
5. **Set the Value to false.**

Setting the dictionary attribute to `false` also removes the show live feed icon ( ) for the table.

### Disable Connect Chat

You can disable Connect Chat to prevent users from being able to chat within the platform.

**Role required:** admin

Disabling Connect Chat hides the Connect Chat sidebar icon. Users who try to access Connect Chat from the navigation pane receive a message that says Connect has been disabled.

1. In the navigation filter, type `sys_properties.list` and press Enter.
2. Search for the `glide.connect.chat.disabled` property.
3. Set the property value to `true`.

### Connect Support

Connect Support is a real-time messaging tool that enables support agents to easily keep track of their support cases, quickly find solutions, and resolve problems quickly.

Connect Support builds on the messaging platform provided with Connect. For general information about the Connect interface, setup, and administration, see [Connect](#). When Connect Support is enabled, users designated as support agents have access to the support tab of the Connect sidebar.
Features include:

- Administrators can create chat queues and enable users to access live support.
- Support agents can monitor the queues to provide instant support.
- Drag-and-drop sharing of links, files, and records.

UI16 or UI15 is required to use Connect Support.

**Note:**
- Connect Support does not replace legacy chat but offers some of the same functionality. The features should not be used concurrently.

**Monitor incoming Connect Support conversations**

In the support tab of the Connect sidebar, you can monitor the queues for which you are an agent and accept incoming conversations.

Role required: none

**Note:** The support tab is visible only if you are an agent for one or more queues.

1. Navigate to **Collaborate > Connect Support**. The Connect workspace opens in a new tab.
2. Click the support tab of the Connect sidebar, indicated by a headset icon (📞). The support tab displays **Queues** to which you belong. It also displays your open support conversations under **Cases**. When a user starts a support conversation or an agent transfers a conversation to a queue, any agent who belongs to the associated queue can accept the conversation. An agent can also request to **transfer a conversation** directly to you.
3. Accept a conversation in one of the following ways.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept a conversation from a queue</td>
<td>Under Queues, click Accept by the queue. The conversation opens in the conversation pane and an entry appears in the Cases section of the sidebar.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Accept a transfer request</td>
<td>Under Cases, click Accept by a transfer request.</td>
</tr>
</tbody>
</table>

![Transfer request](image)

The conversation opens in the conversation pane. The agent who transferred the conversation can stay in the conversation.

4. Respond to the user and help resolve the issue.
   By default, your messages are added to the conversation record as comments and are visible to the user.

**Share knowledge in a Connect Support conversation**

The support view of the Connect workspace has a built-in knowledge tool that makes it easy to search for knowledge articles and share them in a conversation.

Role required: none

Use the knowledge tool to research user questions and provide solutions quickly and easily.

1. Open a support conversation in the Connect workspace.
   The knowledge tool is not available in Connect mini windows.

2. In the conversation tools area to the right of the conversation pane, click the knowledge base tab, which is represented by an open book icon.

![Knowledge tool](image)

The knowledge homepage appears in the conversation tools pane.
3. Search for articles related to the user’s issue.
   For more information about finding knowledge, see Knowledge search.
4. To share an article in the conversation, drag a knowledge article link to the conversation
   pane and drop it anywhere in the drop zone that appears.

**Transfer a Connect Support conversation to a different agent or queue**

You can transfer a Connect Support conversation to a different agent in the queue or to a
   different queue.

Role required: none

1. Open a Connect Support conversation.
2. At the bottom of the conversation, click the menu icon (≡) to open the Connect actions menu.
3. In the Connect actions menu, select **Transfer**. A transfer dialog box opens.

4. Do one of the following actions.
### Option | Description
---|---
**Transfer the conversation to an agent** | 1. To start the transfer request, click **Transfer** by an agent’s name.

   Be sure to choose an agent who is online, which is indicated by a green dot on their avatar.

   You can cancel the transfer any time before it is accepted.

2. When the transfer is accepted, select one of the following options in the dialog box that appears.

   - **Stay**: Remain in the conversation. This is also known as a warm transfer. This option is ideal if you want to provide the new agent with background information or introduce the user to the new agent.
   - **Leave**: Exit the conversation. This is also known as a cold transfer.

**Transfer the conversation to a queue** | Click **Transfer** by a queue.

   The system automatically removes you from the conversation and the conversation enters the queue you selected.

---

### Add a user to a Connect Support conversation

You can add additional users to a Connect Support conversation.

An administrator must enable the `glide.connect.support.add_members` property before users can be added to conversations.

Role required: none

1. Open a group or record conversation in the Connect workspace.
2. In the conversation tools to the right of the conversation pane, click the member list tab.
3. Do one of the following actions.
### Add a member

1. Click Add Member to Group.
2. Use the search field to find and select a user.

### Remove a member

1. Point to a member name.
2. Click the minus icon (-).

The assigned support agent cannot be removed from a Connect Support conversation.

**Note:** Only the assigned support agent can create an incident from the Connect Support conversation.

---

### Escalate a Connect Support conversation

If an escalation path is defined for a Connect Support conversation, you can use a shortcut to escalate a Connect Support conversation to a different queue.

1. Open a Connect Support conversation.
2. At the bottom of the conversation, click the menu icon (≡) to open the Connect actions menu.
3. In the Connect actions menu, select Escalate.
4. A confirmation dialog box appears.
5. In the dialog box, click Escalate.

The system automatically removes you from the conversation and the conversation enters the escalated queue.

### Create an incident from a Connect Support conversation

You can use a shortcut to create an incident on behalf of a user, directly from a Connect Support conversation.

**Role required:** none

You might want to create an incident if you cannot resolve the user’s issue over chat or if you want to create a record of the conversation to share with the user. When you create an incident from a support conversation, the system copies the conversation history to the incident activity stream as comments and work notes. Future messages are tracked in the incident as well.

**Note:** Administrators can customize the behavior of the Create Incident Connect action. For more information, see Administrate Connect actions.

1. Open a Connect Support conversation.
2. At the bottom of the conversation, click the menu icon (≡) to open the Connect actions menu.
3. In the Connect actions menu, select Create Incident.
In the conversation tools area to the right of the conversation, a new incident form opens in a record tab. The system automatically sets the **Caller** field to the user who opened the support conversation.

4. Complete the form as necessary and click **Submit**.

Any comments or work notes in the record conversation appear as comments on the incident form. Work notes do not appear in the chat for the ESS user. The chat agent can select whether a message is a Comment or Work Note in the conversation.

a) In the record conversation, by the text entry field, click the message type icon ![Message Type Icon](image)

b) Select **Comment** or **Work Note**.

c) Enter a message.

By default, record conversation messages are added as comments.

---

**Note:** If you add an attachment to a record conversation, it is attached to the underlying record as well.

---

The system automatically shares the record in the conversation, copies the conversation to the record activity stream, and references the record on the Chat Queue Entry (chat_queue_entry) table. Any new journal fields added to the record do not appear in the chat. The system also changes the document ID for the conversation to reference the incident number instead of the entry in the Chat Queue Entry table.

---

**Connect Support chat states**

Connect Support chats move through specific states.
Connect Support states diagram
Connect Support chat states

<table>
<thead>
<tr>
<th>State</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Waiting             | • Requestor/end user entered a queue by sending a message; agent did not accept it yet  
• End user re-joins a session before agent closes it                                                                                      |
| Work in Progress    | • Agent accepts a chat from a queue. Both requester and agent  
• Requestor/client leaves an ongoing conversation (session times out, loss of connectivity); agent does not end a session; requester re-joins                                    |
| Closed Abandoned    | Requestor/client leaves a conversation before agents accepts it                                                                                                                                          |
| Closed Escalated    | Agents escalated an ongoing conversation by performing Escalate action from a hamburger menu.                                                                                                              |
| Closed Complete     | • Agent leaves/closes an ongoing conversation with a requestor/client  
• End user times out  
• End user ends their session                                                                                                                                 |

Connect Support administration

Administrators can configure various performance settings and features of Connect Support.

Note: There are also settings that apply to both Connect Chat and Connect Support. For more information, see Connect administration.

Migrate from legacy chat to Connect Support

Connect Support is an extension of Connect. Users designated as support agents have access to the support tab of the connect sidebar. Connect Support should not be used concurrently with legacy chat.

Before you activate Connect Support, inform your support agents to close out any existing chats.

Legacy chat uses a different field to determine which state a help desk chat is in. A fix script is included in the Connect Support plugin that circumvents this issue by closing out any existing help desk chat sessions. Manually closing out any existing chats before allowing this script to run helps prevent any loss of chat information.

If you do not close out existing help desk chats, your metrics and chat queue will not work accurately.

1. Activate the Connect Support plugin.

   When you activate the Connect Support plugin, the glide.connect.support.enabled property redirects the legacy chat URL to Connect Support.

   For more information, see Activate Connect Support.

2. Hide the Social IT application.

   Activating Connect Support does not completely eliminate the legacy chat module. To prevent users from using the legacy chat, hide the Social IT application menu. For more information, see Enable or disable an application menu or module.
Properties for Connect Support

The Connect Support Properties page provides several configuration options specifically for Connect Support.

These properties are available for Connect Support.

**Properties for Connect Support**

Users with the admin role can access these properties by navigating to Collaborate > Support Administration > Properties.

**Note:** The [Connect Properties page](#) contains many general Connect properties that impact Connect Support.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Should Connect be used for handling chat queue entries</td>
<td>Disables or enables Connect Support. When the property is enabled, the Service Desk Chat button in the Employee Self-Service portal opens the conversation in Connect Support, rather than legacy chat. Additionally, the Support tab appears in the Connect sidebar.</td>
</tr>
<tr>
<td>glide.connect.support.enabled</td>
<td>Type: true</td>
</tr>
<tr>
<td></td>
<td>Default value: true</td>
</tr>
<tr>
<td></td>
<td>Location: Collaborate &gt; Support Administration &gt; Properties</td>
</tr>
<tr>
<td>Number of support conversations an individual agent can have at one time (-1 is unlimited)</td>
<td>Determines how many support conversations an individual agent can have at one time. When the value is set to -1, an agent can participate in an unlimited number of conversations.</td>
</tr>
<tr>
<td>connect.support.conversation_limit</td>
<td>Type: integer</td>
</tr>
<tr>
<td></td>
<td>Default value: -1</td>
</tr>
<tr>
<td></td>
<td>Location: Collaborate &gt; Support Administration &gt; Properties</td>
</tr>
<tr>
<td>Show agent avatar in Connect Support conversations.</td>
<td>Determines whether an agent's avatar is shown in a support conversation (enabled). When the property is disabled, users see the agent's name only.</td>
</tr>
<tr>
<td>connect.support.show_agent_avatar</td>
<td>Type: true</td>
</tr>
<tr>
<td></td>
<td>Default value: true</td>
</tr>
<tr>
<td></td>
<td>Location: Collaborate &gt; Support Administration &gt; Properties</td>
</tr>
<tr>
<td>Number of seconds to wait (without user interaction), before presenting end-users with an idle countdown timer</td>
<td>Determines how many seconds a user must be inactive in a support conversation before an idle countdown timer appears.</td>
</tr>
<tr>
<td>connect.support.idle.delay</td>
<td>Type: integer</td>
</tr>
<tr>
<td></td>
<td>Default value: 120</td>
</tr>
<tr>
<td></td>
<td>Location: Collaborate &gt; Support Administration &gt; Properties</td>
</tr>
</tbody>
</table>
### ServiceNow Jakarta Now Platform Capabilities

#### Property

| Number of seconds to count down from before marking end-user as having left their support session |
| connect.support.idle.count_down |

**Description**

Determines how many seconds the idle countdown timer remains open after it appears. If the idle user does not dismiss the timer before the countdown completes, the system closes the support session.

- **Type**: integer
- **Default value**: 60
- **Location**: Collaborate > Support Administration > Properties

---

| Limits the number of closed conversations that the support user can see. (0 = unlimited) |
| connect.support.user.closed.conversation_limit |

**Description**

Determines how many closed conversations appear in a user’s support conversation history. When the value is set to 0, all previous conversations appear in the history.

- **Type**: integer
- **Default value**: 0
- **Location**: Collaborate > Support Administration > Properties

---

### Administer Connect Support queues

You can define the support agents, default messages, schedule, and escalation path for each Connect Support queue.

**Role required**: admin

**Note**: Both Connect Support queues and legacy chat queues are stored on the Chat Queue (chat_queue) table. Connect and legacy chat should not be used concurrently.

1. Navigate to **Collaborate > Queues**.
2. Click **New** or open an existing queue from the list.
3. Complete the Chat Queue form, as appropriate.

---

#### Chat Queue form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the queue.</td>
</tr>
<tr>
<td>Active</td>
<td>Not used in Connect.</td>
</tr>
<tr>
<td>Assignment group</td>
<td>User group that contains the support staff for the queue. Any user in the group can view the queue in the Connect sidebar and accept chats. No other users can access the queue. This field must be populated.</td>
</tr>
<tr>
<td>Average wait time</td>
<td>Average time it takes for an agent to accept a chat in the queue. This value is automatically calculated. Do not manually edit.</td>
</tr>
<tr>
<td>Confirm problem</td>
<td>Not used in Connect.</td>
</tr>
</tbody>
</table>
### Field Description

- **Escalate to**
  Different queue to which an agent can escalate a chat. For example, there is a queue for high priority support chats. When a queue is defined in this field, agents can access the Escalate option in conversations.

- **Initial agent response**
  Message that users see when an agent accepts their chat. For example, Thank you for contacting support. We are looking into your question now and will be with you shortly.

- **Not available**
  Message that users see when they attempt to start a chat outside the defined queue Schedule. You can use HTML to format the message and include links or media.

- **Question**
  Initial phrase that users see when they start a new chat in the queue. For example, How can I help you?

- **Schedule**
  Schedule that defines when the queue is available. Leave the field blank to make the queue available all the time. Users cannot start a new conversation in the queue outside the schedule hours.

4. To review conversations associated with the queue, add the Chat Queue Entries related list and review the records for the following information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>How long the user waited and the result</td>
<td>Review information in the State and Wait time columns.</td>
</tr>
<tr>
<td>Who is actively helping employees in the queue</td>
<td>Review the names of agents in the Assigned to column.</td>
</tr>
</tbody>
</table>

### Make a Connect Support queue accessible to end users

To make a Connect Support queue accessible to end users, use the accepted URL format.

Create a queue. Create agents for the queue by assigning users to the assignment group associated with the queue.

Role required: admin

For example you might create a module or add a link to a portal. The accepted URL format is https://<instancename>.service-now.com/$chat_support.do?queueID=<sys_id>.

1. Navigate to Collaborate > Administration > Queues.
2. Right-click the name of the queue to which you want to link.
3. In the context menu, select Copy sys_id. Follow browser instructions to copy the sys_id if browser security measures restrict this function.
4. Preview the support queue by navigating to https://<instancename>.service-now.com/$chat_support.do?queueID=<sys_id>.
5. Create a module or other link to the queue using the URL.
Configure the add support users property

To enable support agents to add users to a Connect Support conversation, add the `glide.connect.support.add_members` property.

Role required: admin

When the `glide.connect.support.add_members` property is added and enabled, support agents can add users to a support conversation. Any added user can also add other users. Only the assigned agent can create an incident from the chat. When non-support agents are added to a chat, the chat appears in their chat tab.

**Note:** Make sure you are in the Global scope when adding this property.

1. Enter `sys_properties.list` in the navigation filter.
   The entire list of properties in the System Properties (sys_properties) table appears.
2. Verify the property does not already exist by searching for the property name. If it does exist, update the property with the information in the following table.
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.connect.support.add_members</code></td>
</tr>
<tr>
<td>Type</td>
<td>true</td>
</tr>
<tr>
<td>Value</td>
<td>true</td>
</tr>
</tbody>
</table>

Support agents can add users to a support conversation. Any added user can also add other users. Only the assigned agent can create an incident from the chat. When non-support agents are added to a chat, the chat appears in their chat tab.

Connect Support metrics

Optional plugins provide a homepage and Performance Analytics dashboards, which contain helpful Connect Support metrics.

The reporting homepage is ideal for support managers who want a simple solution to track the support organization's recent performance. The Performance Analytics dashboards provide a more full-featured solution for support managers who want to analyze trends over time.

Users with the admin role can activate the following plugins to use these features.

**Connect Support homepage and dashboard plugins**

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect Support Manager's Dashboard (com.glide.connect.managers_dashboard)</td>
<td>Provides a homepage for Connect Support, and all required configuration records. Though the plugin name contains the term dashboard, the plugin does not provide functionality related to Performance Analytics dashboards. Homepages are similar to dashboards, but do not require Performance Analytics roles to view.</td>
</tr>
<tr>
<td>Performance Analytics - Content Pack - Service Desk Chat (com.snc.pa.chat)</td>
<td>Provides the <strong>Service Desk Chat Monitor</strong> dashboard, which analyzes key Connect Support metrics and indicators.</td>
</tr>
</tbody>
</table>
### Performance Analytics - Context Sensitive Analytics for Chat

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Analytics - Context Sensitive Analytics for Chat (com.snc.pa.chat.context_sensitive_analytics)</td>
<td>Provides in-form analytics for Connect Support. These analytics are available as a related link on the Chat Queue Entry (chat_queue_entry) form, and also as the <strong>Context Sensitive Analytics - Chat</strong> dashboard.</td>
</tr>
</tbody>
</table>

**Note:** For more information about these plugins, including which other plugins they activate, see [Additional plugins for Connect Support](#).

---

**Use the Connect Support homepage**

Use the Connect Support homepage to view key indicators and metrics related to support conversations, queues, and agents.

Activate the Connect Support Manager’s Dashboard plugin (com.glide.connect.managers_dashboard) to view this homepage.

Role required: chat_admin

The homepage is called **Service Desk - Chat**.

1. Navigate to **Collaborate > Support Administration > Reporting Dashboard**.

   **Note:** Though the module name contains the term dashboard, the module does not provide functionality related to Performance Analytics dashboards. Homepages are similar to dashboards, but do not require Performance Analytics roles to view.

   The Connect Support homepage, which is called **Service Desk - Chat**, opens.

2. Click a widget to drill down into its data.

**Use the Connect Support dashboards**

Use the Connect Support dashboards in Performance Analytics to understand trends in your support organization’s performance over time.

Activate one or both of the following plugins, according to your analytics needs:

- **Performance Analytics - Content Pack - Service Desk Chat** (com.snc.pa.chat)
- **Performance Analytics - Context Sensitive Analytics for Chat** (com.snc.pa.chat.context_sensitive_analytics)

Role required: both chat_admin and pa_viewer

The Performance Analytics - Content Pack - Service Desk Chat plugin (com.snc.pa.chat) includes the **Service Desk Chat Monitor** dashboard, which contains the following tabs:

- **Chat Monitor By State**: Contains metrics related to closed support conversations.
- **Overview**: Contains several metrics related to support conversations, queues, and agents.
- **KPI Process**: Contains metrics that are key performance indicators (KPIs) of the Connect Support process, including the average queue response time, the average duration of support conversations, and the number of new support conversations per day.

The Performance Analytics - Context Sensitive Analytics for Chat plugin (com.snc.pa.chat.context_sensitive_analytics) includes the **Context Sensitive Analytics - Chat** dashboard. The dashboard contains additional metrics related to support queues, including the number of support conversations closed.
Note: You must license Performance Analytics to collect scores for the indicators on the dashboards. Without Performance Analytics premium, the dashboards display the indicators with no data.

1. Navigate to **Performance Analytics > Dashboards**. The last dashboard you viewed opens.
2. In the dashboard picker, under the **Connect Chat** group, select the dashboard you want to view.
3. View the indicators.

### Content packs and in-form analytics for Service Desk Chat

Content packs contain preconfigured best practice dashboards. These dashboards contain actionable data visualizations that help you improve your business processes and practices.

Note: To evaluate the functionality, you can activate Performance Analytics solutions and in-form analytics on instances that have not licensed Performance Analytics Premium. However, you have the following limitations:
- You cannot create new indicators.
- You cannot collect data older than 180 days.

For full functionality, license Performance Analytics Premium. For more information, see [Get started with Performance Analytics Premium](#).

### Content packs

The Performance Analytics widgets on the dashboard visualize data over time, which allows you to analyze your business processes and identify areas of improvement. With content packs, you can get value from Performance Analytics for your application with minimal setup.

Note: Content packs include some dashboards that are inactive by default. You can activate these dashboards to make them visible to end users according to your business needs.

To enable the content pack for Service Desk Chat, an admin can navigate to **Performance Analytics > Guided Setup**. Click **Get Started** then scroll to the section for Service Desk Chat. The guided setup takes you through the entire setup and configuration process.

### Connect Support and Service Portal

Use Connect Support in your portal to allow your users to ask questions or submit requests to support agents.

The Connect Support and Service Portal integration creates a Connect Support widget that you can add to a page in the Service Portal.

### Activate Connect Support for Service Portal

Activate the Connect Support and Service Portal integration plugin so you can add the Connect Support widget to a portal page.

Role required: admin
Activating the Connect Support and Service Portal integration plugin automatically activates the Connect Support plugin.

1. Navigate to **System Definition > Plugins**.
2. Search for and activate the Connect Support and Service Portal integration plugin (com.glide.connect.support.service-portal).

After activating the plugin, the Connect Support widget appears in the list of widgets under **Service Portal > Widgets**. Use Connect Support in a portal by adding the widget to any page within the portal. For more information on adding a widget to a page, see *Create and edit a service portal page*.

### Configure Connect Support widget instance options

You can control the appearance of your widget and how it functions by configuring the instance options.

**Role required:** admin

1. Navigate to **Service Portal > Service Portal Configuration** and open the Service Portal Designer.
2. From the Service Portal Designer, select the page you added the Connect Support widget to. If you have not yet added the widget to a page, see *Create and edit a service portal page* for more information.
3. Click the edit icon in the corner of the widget to open the instance options menu.
4. Complete the fields using the table below. Depending on the functionality you want to add, you may not need to add all of these fields. For example, if you include the Queue ID, you don't also need to include the Queue Name or the Queue URL.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bootstrap color</td>
<td>Select a color for your widget from a list of common bootstrap colors. Themes control the overall color of a widget, but if you want your widget to be a specific color, you can select it from the list.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Queue URL</td>
<td>The URL for the Connect Support chat queue that you want questions to be directed to. For example, https://&lt;instancename.service-now.com/chat_support.do?queueID=&lt;sys_id&gt;</td>
</tr>
<tr>
<td>Queue Name</td>
<td>The name of the queue you want the questions to be directed to. You can find a list of queue names in Collaborate &gt; Connect Support &gt; Queues.</td>
</tr>
<tr>
<td>Queue ID</td>
<td>The sys_id of the queue you want questions to be directed to. You can find this by going to the support queue and either copying the queue ID from the support link, or by selecting Copy sys_id from the context menu.</td>
</tr>
<tr>
<td>Message</td>
<td>The text for the button in the Connect Support widget</td>
</tr>
<tr>
<td>Window</td>
<td>Use this option to open the chat in another tab rather than in a new window.</td>
</tr>
<tr>
<td>Title</td>
<td>The name in the widget header</td>
</tr>
</tbody>
</table>

**Notifications**

Notifications keep users informed of events that concern them. The system can notify users by email, SMS text message, or push notification.

**Explore**
- Notifications release notes
- Upgrade to Jakarta

**Email**
- Basic email setup
- Advanced email setup
- Create an email notification
- The email client
- System mailboxes
- Inbound email actions

**Push Notifications**
- Push notifications
- Push notification setup with the ServiceNow mobile application
- Push notification setup with a custom push application

**Subscription-based notifications**
- Create notification channels
- Modify notification channels
- Create personal notifications

**Troubleshoot and get help**
- Ask or answer questions in the Platform forum
- Search the HI knowledge base for known error articles
- Contact ServiceNow Technical Support

**Email and SMS notifications**

Use email notifications to send selected users email or SMS notifications about specific activities in the system, such as updates to incidents or change requests.

Email notifications allow administrators to specify:
- When to send the notification
- Who receives the notification
- What content is in the notification

Additional email notification options are available. Users can subscribe to notifications, and administrators can make some notifications mandatory.

Administrators also have the option of converting existing email notifications to a rich HTML format. This format provides several advantages, including:

- Raw HTML content is converted into a WYSIWYG format.
- The content can be edited in a feature-rich HTML editor.
- Mail scripts are condensed into a single, easy-to-read line that can be reused in multiple email notifications.
- To prevent broken links, items like images and incidents, that are linked with URLs relative to an instance are converted to absolute links. For example, if an incident is linked using a relative URL, the link is converted to an absolute link.

**Note:** The rich HTML format is the default for all new email notifications.

**Note:** Instances cannot send or receive encrypted email messages. The system strips out the body of the encrypted email because it cannot process the encrypted content in plain text or HTML.

An email notification can also send as an SMS notification if the recipient has subscribed to the notification on an SMS channel. The system uses the subject line of the email notification and converts it to an SMS message. If the administrator doesn’t want to use the email notification subject for the SMS notification, they can define an alternate SMS message in the email template form or email notification form. For more information, see [Create an email notification](#).

For more information on creating an SMS channel, see [Create notification channels](#).

If you want to change how the instance processes incoming email, see [Inbound email actions](#).

See [Email logs](#) for examples of messages the system displays when notifications or inbound email actions are not processed.

**Email setup**

All email notifications use the email properties that you define and the email accounts that you set up. Your email service can also affect the successful transmission of incoming and outgoing email.

**Email accounts**

Email administrators set up [email accounts](#) to allow the system to connect to external mail services such as POP3, SMTP, or IMAP servers. You can use the ServiceNow-provided email accounts or create your own accounts for your own email services.

**Email properties**

Use [Email Properties](#) to configure settings for inbound and outbound email. Email properties apply to all email accounts.
Email service size restrictions

Your email service, whether you are using a standard ServiceNow email configuration or an alternate email configuration, determines the successful transmission of incoming or outgoing emails based on a maximum email size. An email configuration consists of your instance, email server, and email client.

- **Standard email configurations** – For instances that use the standard email configuration, the ServiceNow mail servers cannot send or receive emails larger than approximately 50 MB (before encoding), including the email header, body text, and attachments. Email messages are encoded by an email client, which increases total email message size. The maximum ServiceNow mail server size restriction is 75 MB (after encoding). The maximum email size limit is enforced regardless of any configured attachment size limits.

- **Alternate email configurations** – If your email service uses a company-owned or third-party server, the approximate size restriction of 50 MB (including the email header, body text, and attachments) may still apply. However, your service might support different maximum total file sizes for inbound and outbound emails. Check with the email administrator of your email service to verify email size limits.

For details on how encoding can affect email message size and email transmission, see [KB0521772](#).

Email service availability

Email service is intentionally shut down on instance clones to prevent resending already delivered email. Upgrades no longer require an extended interruption of email service. Instances continue to process email during an upgrade. For a possible explanation for undelivered emails, see the blog post *[Whitelisting emails sent from the ServiceNow infrastructure](#)* by a ServiceNow Technical Support Engineer in the Now Community.

For instructions on creating and sending custom emails when events on the instance occur, see the tasks in *[Email and SMS notifications](#)*.

Instance-to-instance communication via email

Use *[Web services](#)* to communicate between two instances.

Basic email setup

All production instances can send and receive email using ServiceNow-provided resources. The instance has an email address of instance@service-now.com.
Network layout for standard email configuration
Basic email services and features

- Mail servers maintained by ServiceNow.
  - Encrypt mail with opportunistic TLS (Transport Layer Security) if supported by your mail servers.
    - If your internal mail servers send and receive messages via a TLS-encrypted channel, ServiceNow mail servers support that communication.
  - Provide a dedicated mailbox for your instance.
- Pre-configured email accounts to connect to ServiceNow mail servers.
  - An SMTP account sends email to your primary Mail Exchange (MX) server from your instance email address of instance@service-now.com.
  - A POP3 account receives email sent to your instance email address of instance@service-now.com.
- High availability features from ServiceNow datacenters.
- Spam detection for incoming email.

Administrators who want to use basic email services can do so by enabling the email properties for sending and receiving email.

Enable basic email
Enable basic email to use ServiceNow-provided email servers and accounts.

Role required: admin

1. Navigate to System Properties > Email.
2. Configure these email properties and click Save.

<table>
<thead>
<tr>
<th>Property section</th>
<th>Label</th>
<th>System property</th>
<th>Setting required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound Email Configuration</td>
<td>Email sending enabled</td>
<td>glide.email.smtp.active</td>
<td>Yes</td>
</tr>
<tr>
<td>Inbound Email Configuration</td>
<td>Email receiving enabled</td>
<td>glide.email.read.active</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Advanced email setup

With an advanced email setup, you can use your own SMTP server, POP3 server, or both.

Setting up your own email environment can be useful if you want to use existing filtering, retention, or compliance aspects of your internal email architecture. You can set up email in several ways:

- Use your own SMTP server to forward email to ServiceNow servers.
- Use your own SMTP server to send email.
- Use your own POP3 server to receive email.
- Use your own SMTP and POP3 servers to send and receive email.
- Use an OAuth 2.0-enabled SMTP server to send email from a third-party service.
- Use an OAuth 2.0-enabled IMAP server to receive email from a third-party service.

The following procedures assume that you enabled basic email properties.
Enable using your own SMTP server
Enable using your own SMTP server so that you can leverage the existing filtering, retention, or compliance aspects of your own SMTP server while also using the ServiceNow POP3 server.

- Role required: admin
- Email server required: SMTP
- Basic email properties: enabled

You can combine your own internal email architecture with the ServiceNow email architecture to handle email. The following diagram demonstrates how you would use your own SMTP server alongside the ServiceNow POP3 server.
Sending email using your own SMTP server

1. Navigate to System Mailboxes > Administration > Email Accounts.
The system displays the list of available email accounts.

2. Locate the record for **ServiceNow SMTP** and change **Active** to **false**.

   ![Email Accounts Table]

3. Click **New**.
4. Create an email account record for your SMTP server where the **Type** is **SMTP**.
5. From **Related Links**, click **Test Connection**.
   If the email account is valid, the system returns a success message.

![Connection Test]

Configure the SMTP server in your internal email architecture to forward email from the custom email address to the instance email address. Implement a spam filter on the custom email address.

*Enable using your own POP3 server*
You can use your own POP3 server to store and receive email for the instance.
- Role required: admin
- Email server required: POP3
- **Basic email properties:** enabled

1. On your POP3 server, create a mailbox for your instance that has a custom email address. For example, create a mailbox for service-desk@company.com.

2. Navigate to **System Mailboxes > Administration > Email Accounts.** The system displays the list of available email accounts.

3. Optional: If you do not want to receive email sent to the instance@service-now.com mailbox, locate the record for **ServiceNow POP3** and change **Active** to **false.** An instance can receive email from multiple POP3 accounts at the same time. Leaving the **ServiceNow POP3** account active allows the instance to receive email sent to the instance default email address.

4. Click **New.** The system displays a blank Email Account form.

5. Create an email account record for your POP3 server where the **Type** is **POP3.**

6. From **Related Links,** click **Test Connection.** If the email account is valid, the system returns a success message.
Connection Test

Connection Successful
Enable using your own SMTP and POP3 servers
You can use your own SMTP and POP3 servers to send email from the instance and to store and receive email for the instance.

- Role required: admin
- Email servers required:
  - SMTP
  - POP3

- **Basic email properties**: enabled

1. On your POP3 server, create a mailbox for your instance. For example, create a mailbox for service-desk@company.com.
2. Navigate to **System Mailboxes > Administration > Email Accounts**. The system displays the list of available email accounts.
3. Locate the record for **ServiceNow SMTP** and change **Active** to false.

   ![Email Accounts Table]

4. Optional: If you do not want to receive email sent to the instance@service-now.com mailbox, locate the record for **ServiceNow POP3** and change **Active** to false.

   An instance can receive email from multiple POP3 accounts at the same time. Leaving the **ServiceNow POP3** account active means that the instance receives email sent to its default email address.
5. Click **New**.
The system displays a blank Email Account form.

6. Create an email account record for your SMTP server where the **Type** is **SMTP**.

7. From **Related Links**, click **Test Connection**.
If the email account is valid, the system returns a success message.

8. Click **New**.
The system displays a blank Email Account form.

9. Create an email account record for your POP3 server where the **Type** is **POP3**.

10. From **Related Links**, click **Test Connection**.
If the email account is valid, the system returns a success message.
Connection Test

Connection Successful
ServiceNow Instance

Outbox with Email To:
user@yourdomain.com

Send

Domain Name System (DNS)

Lookup Mail Server For:
yourdomain.com
mx.yourdomain.com

Receive

Your Outbound Mail Server
smtp.yourdomain.com
Send Email To:
user@yourdomain.com

Your Incoming Mail Server
pop.yourdomain.com
Route To Mailbox For:
user@yourdomain.com

Your Incoming Mail Server
pop.yourdomain.com
Route To Mailbox For:
helpdesk@yourdomain.com

Your Outbound Mail Server
smtp.yourdomain.com
Send Email To:
helpdesk@yourdomain.com

Email Passed Your Spam Filter?

Yes

No

Stop

Receive

Inbox For:
user@yourdomain.com

User Email Account

Outbox with Email To:
helpdesk@yourdomain.com

Send
OAuth email authentication

OAuth enables your instance to receive and send email through a third-party email account.

Open Authentication (OAuth) is an open standard for authorization that provides administrators with an authorization method when connecting to incoming IMAP and outgoing SMTP servers. OAuth enables an instance to receive and send email from a third-party account, such as Gmail, without having to enter the credentials for that account.

The OAuth 2.0 implementation requires you to obtain an access and refresh token from your third-party email provider for each third-party email account. The tokens are automatically saved to the instance database. They provide authorization for all email communication between the instance and the authorized third-party account. A scheduled job regularly checks to see if email access tokens are valid. If the access token is not valid, but the refresh token is, the instance automatically regenerates a new access token.

OAuth 2.0 support is available starting with the Geneva release. The OAuth implementation supports IMAP and SMTP accounts only. POP3 is not supported. OAuth 1.0 is no longer supported.

Note: Customer email accounts configured to use OAuth 1.0 authentication with Gmail cease to function as of April 20, 2015. See KB0546976 for more information.

Activating the Email - OAuth support for IMAP and SMTP plugin allows you to use OAuth with email. If you upgrade to Geneva or later instances and are already using OAuth 1.0, activate the plugin again.

See Outbound REST with OAuth 2.0 profile tutorial - integrating with Google Contacts API for an example of using an OAuth 2.0 profile to authenticate an outbound REST message with Google to retrieve contact information. Also see OAuth 2.0 for more information on OAuth 2.0 support in the instance.

Activate the OAuth email authentication plugin

OAuth email authentication requires the Email - OAuth support for IMAP and SMTP 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.

Enable OAuth 2.0 for email

Setting up OAuth 2.0 for email requires you to obtain access and refresh tokens from your email provider.
• Role required: admin
• Plugin required: Email - OAUTH support for IMAP and SMTP

1. Log in to your third-party email account, such as Gmail, and enable OAuth 2.0.
2. Obtain the following from your third-party email account:
   • client ID
   • client secret
   • authorization URL
   • token URL
   • redirect URL
   • token revocation URL

3. Navigate to System OAuth > Application Registry.
4. Click New.
5. Click Connect to a third party OAuth Provider to create an application registry record that email uses.
6. Use the information you obtained from your third-party email account to fill in the fields on the form. See Use a third-party OAuth provider for instructions. Create the OAuth application registry record and its associated OAuth Entity Profile and OAuth Entity Scope records.
7. Click Submit.
8. Navigate to System Mailboxes > Administration > Email Accounts.
The system displays the list of available email accounts.
9. Optional: If you do not want to receive email sent to the default instance email address, locate the record for ServiceNow POP3 and change Active to false.
The system can receive email from multiple POP3 email accounts.
10. Locate the records for ServiceNow SMTP and change Active to false.

11. Click New.
The system displays a blank Email Account form.
12. Create an email account record for your OAuth 2.0 SMTP server where the Type is SMTP.
13. For Authentication, select OAuth 2.0.
14. For OAuth Profile, select the application registry record you created.
15. Click Authorize Email Account Access to obtain the access and refresh tokens.
   
   Another browser window opens asking you to authorize the account access on the third-party email account.
16. Authorize the access.
   
   After the authorization is successful and the tokens are saved to the instance, the Authorize Email Account Access button no longer appears on the Email Account form.
17. Click New.
   
   The system displays a blank Email Account form.
18. Create an email account record for your OAuth 2.0 IMAP server where the Type is IMAP.
   
   Use the same Authentication and OAuth profile settings as the OAuth SMTP email account.

Email accounts

Email accounts store the connection details and credentials the system uses to access external email servers and services.

By default, instances come with email accounts for ServiceNow-managed SMTP and POP3 servers to send and receive email. These accounts cannot be modified, but can be deactivated if you do not want to use them. To connect to other email servers and services you must create email accounts for them. You can create email accounts for servers and services that use these protocols:

- SMTP
- POP3
- IMAP

**Note:** The system only allows one SMTP email account to be active at a time and sends all email through this account. You can however receive email from multiple POP3 or IMAP accounts.

The system stores individual email accounts in the sys_email_account table. Create separate email accounts to send and receive email. Use email properties to define how the system processes email for all email accounts.

By default, the ServiceNow POP3 server provides each instance with its own mailbox at the address instance@service-now.com. Likewise, the ServiceNow SMTP server sends email from the address instance@service-now.com. To create another mailbox, provision your own POP3 or IMAP server and create an email account to the server on the instance. To change the sent from email address, update the address in the email account you use for sending email.
Configure an email account
You can create email accounts in addition to the accounts provisioned for you.

- Role required: admin
- Email server: a compatible email server
  - SMTP
  - POP3
  - IMAP

1. Navigate to System Mailboxes > Administration > Email Accounts.
2. Click New.
3. Fill in the fields on the form (see table).

### Email Account fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name to identify this Email Account.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Mail server type. The choices are:</td>
</tr>
<tr>
<td></td>
<td>· Email Reader</td>
</tr>
<tr>
<td></td>
<td>· POP3</td>
</tr>
<tr>
<td></td>
<td>· IMAP</td>
</tr>
<tr>
<td></td>
<td>· Email Sender</td>
</tr>
<tr>
<td></td>
<td>· SMTP (only one active account permitted)</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>The type of authentication used for the email account to connect to the email server. The choices are <strong>Password</strong>, <strong>OAUTH</strong>, and <strong>OAUTH 2.0</strong>. The Email - OAUTH support for IMAP and SMTP plugin must be active for the OAUTH options to be visible.</td>
</tr>
<tr>
<td><strong>OAuth Provider</strong></td>
<td>Select the OAUTH application registry record for this account. This field appears if you selected <strong>OAUTH 2.0</strong></td>
</tr>
<tr>
<td><strong>Server</strong></td>
<td>Remote Server to which this account connects.</td>
</tr>
<tr>
<td><strong>Active</strong></td>
<td>Determines if this Email Account is active.</td>
</tr>
<tr>
<td><strong>ServiceNow Configured</strong></td>
<td>Indicates if this account is provisioned by ServiceNow. This field is read-only. If you create an account, this option is not selected.</td>
</tr>
<tr>
<td><strong>Email user label</strong></td>
<td>A display value used for outgoing messages. This field is for SMTP type accounts only.</td>
</tr>
<tr>
<td><strong>User name</strong></td>
<td>The user name or ID to authenticate an email address. The value in this field is also the From address when the instance sends email. If you are using SMTP, this must be a full email address. The value in the From field can override this (for SMTP accounts).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The address in the From field on the Notification form takes precedence over this field.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Password when <strong>Authentication</strong> type is <strong>Password</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You may need to increase the size of this field to accommodate longer passwords. By default, this field has a size of 40.</td>
</tr>
<tr>
<td><strong>From</strong></td>
<td>(SMTP only) The from address used for notifications sent with this account. This address takes precedence over the User name field. If nothing is present in this field, the User name is used as the return address for notifications sent from the instance.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable SSL</td>
<td>Option to upgrade an insecure connection to a secure connection using SSL encryption.</td>
</tr>
<tr>
<td>Enable TLS</td>
<td>Option to upgrade an insecure connection to a secure connection using the TLS encryption protocol, if your email server supports TLS.</td>
</tr>
<tr>
<td>Port</td>
<td>Connection TCP port.</td>
</tr>
</tbody>
</table>

4. **Click Submit.**

5. **Click the test connection link at the bottom to test the SMTP, POP3, or IMAP account.**

   The system displays a pop-up window with the results of the connection test.
If the test succeeds, click **Close** to return to the email account record. If the test fails, click **View Logs** to display more information about the test results.

The system uses the email account to send or receive email.

Enable the system to send or receive email.

**Email properties**

The Email Properties page is where you can configure settings for inbound and outbound email.

Email properties are available from either of these modules:

- **System Mailboxes > Email Properties**
- **System Properties > Email Properties**
### Outbound Email Configuration

- **Email sending enabled**: Yes | No

- **Send all email to this test email address (non-production testing)**: 

- **Append timezone to dates and times in sent email**: Yes | No

- **Create visible watermark in sent email. If false, create invisible watermark via hidden div tag**: Yes | No

- **Resend email if server returns these SMTP error codes**: 421, 450, 451, 452

- **Do not resend email if server returns these SMTP error codes**: 500, 501, 502, 503, 504, 505, 506, 510, 520, 550, 554

- **Resend email when server returns unknown SMTP error codes**: Yes | No

- **Notes that can view email in the Activity formatter when including “Sent/Received Emails”**: 

- **Number of journal entries (Additional comments, Work notes, etc) included in email notifications (-1 means all)**: 3

### Inbound Email Configuration

- **Email receiving enabled**: Yes | No

- **Identify email as a reply to these subject prefixes**: rc.*, r.*

- **Identify email as a forward from these subject prefixes**: Fw, Fwd:

- **Discard everything below this text if found in a reply body (comma separated, case sensitive)**: 

- **Ignore email with these headers (comma separated, case sensitive)**: X-Originated-By, X-Originated-From, X-Received, X-Header, X-Origin, X-Mailer, X-Mail-From

- **Ignore email when subject starts with the following words (case insensitive)**: out of office, autoresponse, welcome, unsubscribe, delivery failure, returned mail

- **Ignore email from these senders. Use the name before the @ sign. (comma-separated)**: mailer-daemon, postmaster

- **Automatically create users for incoming emails from trusted domains**: Yes | No

- **Default password for users created from email sent from trusted domains. (must reset upon login)**: 

- **Trusted domains when creating new users from incoming email (ignore email from untrusted domains unless from an existing user, use * for all domains)**: *
Email accounts are configured in the **System Mailboxes > Administration > Email Accounts** module, starting with the Geneva release. See [Configure an email account](#) for instructions.

Email diagnostics are available from the **System Mailboxes > Email Diagnostics** module, starting with the Geneva release.

**Outbound mail configuration**

The **Outbound Mail Configuration** section of the Email Properties page contains properties for sending email.
### Outbound Email Configuration

<table>
<thead>
<tr>
<th>Email sending enabled</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send all email to this test email address (non-production testing)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Append timezone to dates and times in sent email</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Create visible watermark in sent email. If false, create invisible watermark via hidden div tag.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Resend email if server returns these SMTP error codes</td>
<td>421,450,451,452</td>
<td></td>
</tr>
<tr>
<td>Do not resend email if server returns these SMTP error codes</td>
<td>500,501,502,503,504,550,551,552,553,554</td>
<td></td>
</tr>
<tr>
<td>Resend email when server returns unknown SMTP error codes.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Roles that can view email in the Activity formatter when including &quot;Sent/Received Emails&quot;</td>
<td>itil</td>
<td></td>
</tr>
<tr>
<td>Number of journal entries (Additional comments, Work notes, etc.) included in email notifications (-1 means all).</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>
### Outbound email properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.email.smtp.active</td>
<td>Email sending enabled</td>
<td>Specifies whether to enable or disable the outgoing mail server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: true</td>
</tr>
<tr>
<td>glide.email.test.user</td>
<td>Send all email to this test email address (non-production testing)</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: none</td>
</tr>
<tr>
<td>glide.email.append.timezone</td>
<td>Append time zone to dates and times in sent mail</td>
<td>Specifies whether to append the system time zone to date and date/time values in outbound emails. For example, 2010-07-02 04:01:14 PST.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: true</td>
</tr>
<tr>
<td>glide.email.watermark.visible</td>
<td>Create visible watermark in sent mail</td>
<td>Indicates whether the watermark in email notifications is visible (true) or wrapped in a hidden div tag (false).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td>glide.smtp.defer_retry_ids</td>
<td>Resend email if server returns these SMTP error codes</td>
<td>Specifies the comma-separated list of SMTP error codes that force the instance to resend email.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: 421,450,451,452</td>
</tr>
<tr>
<td>glide.smtp.fail_message_ids</td>
<td>Do not resend email if server returns these SMTP error codes</td>
<td>Specifies the comma-separated list of SMTP error codes that prevent the instance from resending email.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: 500,501,502,503,504,550,551,552,553,554</td>
</tr>
<tr>
<td>Property</td>
<td>Label</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>glide.smtp.default_retry</td>
<td>Resend email when server returns unknown SMTP error codes.</td>
<td>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.defe_retr_y_ids property.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Default value: true</td>
</tr>
<tr>
<td>glide.ui.activity.email_roles</td>
<td>Roles that can view email in the Activity formatter when including “Sent/Received Emails”</td>
<td>Specifies the comma-separated list of roles that can view email in the activity formatter.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: string</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Default value: itil</td>
</tr>
<tr>
<td>glide.email.journal.lines</td>
<td>Number of journal entries (Additional comments, Work notes, etc.) included in email notifications (-1 means all).</td>
<td>Specifies the number of entries from a journal field, such as Additional comments or Work notes, included in email notifications. A value of -1 includes all journal entries.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Default value: 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Learn More: Restrict the Number of Entries Sent in a Notification</td>
</tr>
</tbody>
</table>

**Inbound mail configuration**

The **Inbound Mail Configuration** section of the Email Properties page contains properties to control inbound email.
Inbound Email Configuration

Email receiving enabled

☑ Yes | No

Identify email as a reply by these subject prefixes

re:, aw:, r:, Accepted:, Tentative:, Declined:

Identify email as a forward by these subject prefixes

fw:, fwd:

Discard everything below this text if found in a reply body (comma separated, case sensitive)

\n\n-----Original Message-----\n\n\n_____ \n\nFrom:

Ignore mail with these headers (comma separated name:value pairs)

X-ServiceNow-Spam-Flag:YES,X-ServiceNow-Virus:INFECTED,Auto-Subn

Ignore email when subject starts with text (comma separated, case insensitive)

out of office autoreply, undeliverable:, delivery failure:, returned mail:, at

Ignore email from these senders. Use the name before the @ sign. (comma-separated)

mailer-daemon, postmaster

Automatically create users for incoming emails from trusted domains

☑ Yes | No

Default password for users created from email sent from trusted domains. (must reset upon login)

MyComp@ny123!

Trusted domains when creating new users from incoming email (Ignore email from untrusted domains unless from an existing user; use * for all domains)

*
<table>
<thead>
<tr>
<th>Property</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.email.read.active</td>
<td>Email receiving enabled</td>
<td>Specifies whether to enable or disable the inbound mail server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Default value: true</td>
</tr>
<tr>
<td>glide.email.reply_subject_prefix</td>
<td>Identify email as a reply by these subject prefixes</td>
<td>Specifies the comma-separated list of prefixes in the subject line that identify an email reply.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: string</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Default value: re:, aw:, r:, Accepted:, Tentative:, Declined:</td>
</tr>
</tbody>
</table>

**Note:** The case of the reply prefix in the email, for example RE:, must exactly match the case of the prefixes defined in this property. If, for example, an email contains the Re: prefix and only RE: is defined in the property, the email will not be recognized as a reply. Therefore, it is a best practice to define multiple versions of the prefix, including mixed-case versions, such as RE:, Re:, and so on.
<table>
<thead>
<tr>
<th>Property</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.email.forward_subject_prefix</td>
<td>Identify email as a forward by these subject prefixes</td>
<td>Specifies the comma-separated list of prefixes in the subject line that identify a forwarded email.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: string</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Default value: fw:,fwd:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The case of the forward prefix in the email, for example fw:, must exactly match the case of the prefixes defined in this property. If, for example, an email contains the Fwd: prefix and only fwd: is defined in the property, the email will not be recognized as a forward. Therefore, it is a best practice to define multiple versions of the prefix, including mixed-case versions, such as FWD:, Fwd:, and so on.</td>
</tr>
<tr>
<td>glide.pop3.reply_separators</td>
<td>Discard everything below this text if found in a reply body (comma separated, case sensitive)</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></td>
<td>- Type: string</td>
</tr>
</tbody>
</table>
|                               |                                                                      | - Default value: 

```                                                                                                                                                                                                 |
|                               |                                                                      | Original Message-----,\n
From:                                                                                                                                                                                                 |
<p>|                               |                                                                      | <strong>Note:</strong> Some email service providers don’t support this default format. If your reply emails aren’t formatting as expected, edit this property manually.                                             |</p>
<table>
<thead>
<tr>
<th>Property</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.pop3.ignore_headers</td>
<td>Ignore email with these headers (comma separated name:value pairs)</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>) in the Content-Type header for the subtype. For example, Content-Type:multipart/</em>; report-type=delivery-status; ignores emails containing a type of multipart and a value 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></td>
<td>• Type: string</td>
</tr>
</tbody>
</table>

**Note:** If the Email Filters plugin is activated, the Ignore header email filter overrides this property. The property does not appear on the Mail Properties page when email filters are enabled.
<table>
<thead>
<tr>
<th>Property</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
</table>
| glide.pop3.ignore_subjects | Ignore email when subject starts with text (comma separated, case insensitive) | Specifies the comma-separated list of strings that cause the instance to ignore an email message if the string is present at the start of a subject line. These values are case-insensitive.  
· Type: string  
· Default value: out of office autoreply, undeliverable:, delivery failure:, returned mail:, autoreply  

**Note:** If the Email Filters plugin is activated, the **ignore subject** email filter overrides this property. The property does not appear on the Mail Properties page when email filters are enabled.

| glide.pop3.ignore_senders | Ignore email from these senders. Use the name before the @ sign. (comma-separated) | Specifies the comma-separated list of senders that cause the instance to ignore an email message. Enter only the name before the at sign (@).  
· Type: string  
· Default value: mailer-daemon, postmaster  

**Note:** If the Email Filters plugin is activated, the **ignore sender** email filter overrides this property. The property does not appear on the Mail Properties page when email filters are enabled.
<table>
<thead>
<tr>
<th>Property</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.pop3readerjob.createCaller</td>
<td>Automatically create users for incoming emails from trusted domains</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, the instance creates a new user record for the email address and places that new user in the Caller field of any tickets created. If the property is set to false, the instance places Guest in the Caller field of any tickets created.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Default value: false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Learn More: Enabling Automatic User Creation</td>
</tr>
<tr>
<td>glide.user.default_password</td>
<td>Default password for users created from email sent from trusted domains. (must reset upon login)</td>
<td>Specifies the password for new users created from incoming email. Users must reset the password at first login.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: string</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Default value: password</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Learn More: Enabling Automatic User Creation</td>
</tr>
<tr>
<td>glide.user.trusted_domain</td>
<td>Trusted domains when creating users from incoming email (Ignore mail from untrusted domains unless from an existing user; use * for all domains)</td>
<td>Comma-separated list of trusted domains for which the instance automatically creates a user based on incoming emails. Use an asterisk (*) to trust all domains. If an email is not from a trusted domain, the instance processes the inbound email as a 'guest user' but it does not create a guest user in the instance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: string</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Default value: asterisk (*)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Learn More: Enabling Automatic User Creation</td>
</tr>
</tbody>
</table>

**Email image filtering properties**

Use email image filtering properties to control how inbound email images attach to a target record.

When a user sends an email to the system, email images (such as logos or email signatures) attach to the target record by default. These images are also visible in the activity stream of the target record. The system then replicates these images, which can cause duplicate image attachments to the target record and also duplicate images in the activity stream.

To filter images from emails and reduce duplicate image attachments to target records, configure the following properties in the System Properties (sys_properties) table. Use these properties to:
- Specify the email image sizes eligible for filtering.
- Choose an action that controls image attachment behavior and image visibility in the activity stream.

**Note:** These properties do not delete attachments. You can verify attachment records in the Attachments (sys_attachment) table.

### Email image filtering properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.email.inbound.image_sys_attachment.filter.minimum_bytes</td>
<td>Sets the minimum image size in bytes of inbound email images that can be filtered. Any image that is below this size limit does not attach to the target record.</td>
</tr>
<tr>
<td>glide.email.inbound.image_sys_attachment.filter.action</td>
<td>Specifies the image filtering behavior.</td>
</tr>
</tbody>
</table>

**Name:** glide.email.inbound.image_sys_attachment.filter.minimum_bytes

**Type:** Integer

**Default value:** 0 (no filtering)

**Name:** glide.email.inbound.image_sys_attachment.filter.action

**Type:** Choice list

- AttachTarget - Associate the image to the target record. The image is visible in the activity formatter and in the attachment to the target record.
- AttachEmail - Attach the image to the email record. The image is not visible in the activity formatter of the target record nor in the attachment to the target record.
- AttachNone - Do not attach the image to a record. You can select this option to attach the image manually at a later time.

**Default value:** AttachTarget

### Additional email properties

There are several advanced email properties that you can use to fine tune the way your instance sends or receives email.

You must add these properties to the System Property (sys_properties) table before they can be used to overwrite the defaults.

#### Additional properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.glide.email.max_body_bytes</td>
<td>Sets the maximum body size in bytes allowed per inbound email.</td>
</tr>
<tr>
<td></td>
<td><strong>Type:</strong> integer</td>
</tr>
<tr>
<td></td>
<td><strong>Default value:</strong> 1048576</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| com.glide.email.max_read | Specifies the maximum number of emails a POP3 reader should process concurrently.  
   - Type: integer  
   - Default value: 20 |
| com.snc.on_call_rotation.reminders.showtz | Specifies whether to show a user's timezone.  
   - Type: true | false  
   - Default value: false |
| glide.email.allow_duplicate_message_ids | Allows storing of emails with duplicate message IDs and adds error message "Duplicate message-id encountered, prevented loop."  
   - Type: true | false  
   - Default value: false |
| glide.email.inbound.calendar_behavior | Specifies how the system stores calendar data, such as an invitation or an invitation response. Enter one of these options (not case sensitive):  
   - Attach: Store the calendar data as an attachment on the associated record, such as the incident or change that triggers an invitation.  
   - Ignore: Discard the calendar data.  
   - Inline: Store the calendar data as text in the email Body field.  
   - Type: string  
   - Default value: Attach |
| glide.email.inbound.convert_html_inline_attachment_references | Specifies whether to convert inbound email HTML so email images appear in the email HTML body preview. The system displays broken cid (content ID) links in place of images received when this property is disabled. The format in which the system displays an email image depends on the property setting at the time the email is received, not the current property setting.  
   - Type: true | false  
   - Default value: true |
| glide.email.inbound.generate.missing.html.part | Enables the system to generate HTML text for inbound emails that contain only a plain text message.  
   - Type: true | false  
   - Default value: true |
| glide.email.inbound.generate.missing.text.part | Enables the system to generate plain text for inbound emails that contain only an HTML message.  
   - Type: true | false  
   - Default value: true |
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| glide.email.inbound.max_attachment_count | Sets the maximum number of attachments allowed per inbound email. This property is available starting with the Eureka Patch 4 release.  
  - Type: integer  
  - Default value: 30  
  - Location: System Property (sys_properties) table |
| glide.email.inbound.max_total_attachment_size_bytes | Sets the maximum total attachment size in bytes allowed per inbound email. This property is available starting with the Eureka Patch 4 release.  
  - Type: integer  
  - Default value: 18874368  
  - Location: System Property (sys_properties) table |
| glide.email.mail_to | Specifies the email address for sending notifications that use the ${mailto:} variable.  
  - Type: string  
  - Default value: SMTP email address that is active by default |
| glide.email.name_split | Specifies the delimiter used between first and last names in an email address. For example, a delimiter of "." (period) in the email address john.smith@company.com tells the system to look for a user record for John Smith.  
  - Type: string  
  - Default value: period (.) |
| glide.email.notification.save_when_no_recipients | 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.  
  - Type: true | false  
  - Default value: true |
| glide.email.outbound.header.auto_submitted | Stores the value used in the "Auto-submitted" outbound email header. Clear the property value to remove the "Auto-submitted" header from all outbound emails. Some spam filters flag auto-generated email as spam.  
  - Type: string  
  - Default value: auto-generated |
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| glide.email.outbound.max_attachment_count    | Sets the maximum number of attachments allowed per outbound email. This property is available starting with the Eureka Patch 4 release.  
  - Type: integer  
  - Default value: 30  
  - Location: System Property (sys_properties) table |
| glide.email.outbound.max_body_bytes          | Sets the maximum body size in bytes allowed per outbound email.  
  - Type: integer  
  - Default value: 1048576 |
| glide.email.outbound.max_total_attachment_size_bytes | Sets the maximum total attachment size in bytes allowed per outbound email. This property is available starting with the Eureka Patch 4 release.  
  - Type: integer  
  - Default value: 18874368  
  - Location: System Property (sys_properties) table |
| glide.email.override.url                     | Sets the URL to use in emailed links in place of the instance URL. The URL should end with nav_to.do. An example value is: https://servicenow.customerdomain.com/production/nav_to.do. This property is suitable for customers who use custom redirect URLs for their instances.  
  - Type: string  
  - Default value: instance URL |
| glide.cms.use_email_override_url             | Forces the system to use the glide.email.override.url property, rather than the glide.servlet.uri property, when a notification has a link to a CMS page in an instance.  
  - Type: true | false  
  - Default value: false  
  - Location: System Property (sys_properties) 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 |
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.email.smtp.max_send</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- Type: integer</td>
</tr>
<tr>
<td></td>
<td>- Default value: 100</td>
</tr>
<tr>
<td>glide.email.text_plain.strip_xhtml</td>
<td>Indicates whether both outbound and inbound emails that are shown in comments convert the XML to plain text (true) or preserve the XML (false).</td>
</tr>
<tr>
<td></td>
<td>- Type: true</td>
</tr>
<tr>
<td></td>
<td>- Default value: true</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>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>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>glide.notification.recipient.exclude_logging</td>
<td>Master switch to enable or disable logging all reasons a recipient was excluded. If set to true, the subsequent properties dealing with the exclusion of logging are enabled. If it is set to false, none of the subsequent properties relating to the exclusion of logging are enabled. This property cannot suppress log messages generated by the glide.email.test.user property.</td>
</tr>
<tr>
<td></td>
<td>- Type: true</td>
</tr>
<tr>
<td></td>
<td>- Default value: true</td>
</tr>
<tr>
<td>glide.notification.recipient.exclude_logging.device_inactive</td>
<td>Logs recipients who are excluded because their chosen notification device record is marked as inactive.</td>
</tr>
<tr>
<td></td>
<td>- Type: true</td>
</tr>
<tr>
<td></td>
<td>- Default value: true</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| glide.notification.recipient.exclude_logging.device_schedule | Logs recipients who are excluded based on the Schedule field on the New Device for System Administrator form for their chosen notification device.  
- Type: true | false  
- Default value: true |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| glide.notification.recipient.include_logging | Master switch to enable or disable logging all reasons a recipient was included. If 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 |
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.notification.recipient.include_logging.delegate</td>
<td>Logs recipients who are included because they are delegates of another user.</td>
</tr>
</tbody>
</table>
|                                                                 | • Type: true | false  
|                                                                 | • Default value: true                                                                                                                                                                                     |
| glide.notification.recipient.include_logging.event_parm         | Logs recipients who are included because they are in the parm1 or parm2 fields of the event record.                                                                                                        |
|                                                                 | • Type: true | false  
|                                                                 | • Default value: true                                                                                                                                                                                     |
| glide.notification.recipient.include_logging.recipient_fields   | Logs recipients who are included via a notification target record, such as an incident record, specified in the Users/Groups in Field field for the notification record. The recipient_fields are fields in the target record that contain a recipient to add. For example, if the record that triggered the notification is an incident, and the assigned_to field for the incident is listed in recipient_fields, that user is included as a recipient. |
|                                                                 | • Type: true | false  
|                                                                 | • Default value: true                                                                                                                                                                                     |
| glide.notification.recipient.include_logging.recipient_groups.group_email | Logs recipients who are included in a group email for any group provided in the notification record’s recipient_groups or the event parm1 or parm2 field.                                                |
|                                                                 | • Type: true | false  
|                                                                 | • Default value: true                                                                                                                                                                                     |
| glide.notification.recipient.include_logging.recipient_groups.manager | Logs recipients who are included because they manage any group provided in the notification record’s recipient_groups or the event parm1 or parm2 field.                                           |
|                                                                 | • Type: true | false  
|                                                                 | • Default value: true                                                                                                                                                                                     |
| glide.notification.recipient.include_logging.recipient_groups.membership | Logs recipients who are included via membership in any group provided in the notification record recipient_groups or the event parm1 or parm2 field.                                                                |
|                                                                 | • Type: true | false  
|                                                                 | • Default value: true                                                                                                                                                                                     |
| glide.notification.recipient.include_logging.recipient_users     | Logs recipients who are included via notification record’s Users field (recipient_users).                                                                                                                    |
|                                                                 | • Type: true | false  
<p>|                                                                 | • Default value: true                                                                                                                                                                                     |</p>
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| **glide.notification.recipient.include_logging.subscription** | Logs recipients because they are subscribed via User Notification Preferences.  
- Type: true | false  
- Default value: true |
| **glide.pop3.parse_start** | Specifies the text that indicates the beginning of the email body section. The instance parses name:value pairs within this section to set or update field values when processing inbound email actions.  
- Type: string  
- Default value: none |
| **glide.pop3.parse_end** | Text indicating the end of the email body section where the instance should parse name:value pairs to update field values when processing inbound email actions.  
- Type: string  
- Default value: none |
| **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] |
| **glide.smtp.precedence_bulk** | Specifies whether outbound email includes the header "Precedence: bulk". Some spam filters flag bulk email as spam. Set the value to false to remove this header from outbound email.  
- Type: true | false  
- Default value: true |
| **glide.smtp.timeformat** | Specify the time format to use for outgoing email notifications.  
- Type: string  
- Default value: time format listed in email sender’s user record  
  [sys_user.time_format] |
| **glide.ui.activity.email.use_display** | Specifies whether to display email addresses or user IDs (display value from 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 |
### Property Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.ui.email_client.email_address.disambiguator</td>
<td>Sets the columns from the User [sys_user] table that the autocomplete list displays. Separate each column name with a semicolon character (;).</td>
</tr>
<tr>
<td></td>
<td>- Type: string</td>
</tr>
<tr>
<td></td>
<td>- Default value: name</td>
</tr>
<tr>
<td></td>
<td>- Learn more: Displaying Additional Information in the Email Client Autocomplete</td>
</tr>
<tr>
<td>glide.ui.incident_activity.max_addresses</td>
<td>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 (...).</td>
</tr>
<tr>
<td></td>
<td>- Type: string</td>
</tr>
<tr>
<td></td>
<td>- Default value: 5</td>
</tr>
<tr>
<td>NotifyAffectedCI.max_rel_level</td>
<td>Sets a value used by the Affected ci notifications business rule, which notifies subscribers when configuration items (CIs) are affected by tasks. The business rule generates notifications for parent CIs up to the level defined by this property. You might need to adjust the property value according to the complexity and depth of your CI relationships.</td>
</tr>
<tr>
<td></td>
<td>- Type: integer</td>
</tr>
<tr>
<td></td>
<td>- Default value: 5</td>
</tr>
</tbody>
</table>

### Email logs

The email log records all email notifications sent from the instance.

This is a verbose and unfiltered view of email. For a more detailed view, see the System Mailbox application.

This log provides the following information for all notifications.

#### Email log

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mailbox</td>
<td>The system mailbox to use for filtering the email notifications displayed.</td>
</tr>
<tr>
<td>State</td>
<td>The current state of the notification (Error, Ignored, Processed, or Ready).</td>
</tr>
<tr>
<td>Receive type</td>
<td>The type of inbound email notification (None, Forward, New, or Reply).</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Type</td>
<td>The status of the email notification. Choices are:</td>
</tr>
<tr>
<td></td>
<td>- received: The server received this email.</td>
</tr>
<tr>
<td></td>
<td>- received - ignored: The server received this email, but it was ignored by the instance for inbound email action purposes. Typically,</td>
</tr>
<tr>
<td></td>
<td>these emails are either spam or auto-replies. See the Error String field for details.</td>
</tr>
<tr>
<td></td>
<td>- send - failed: The server has attempted to send the email and failed. See the Error String field for details.</td>
</tr>
<tr>
<td></td>
<td>- send - ignored: The server skipped sending this email. Typically, this is for an email which was generated but lacked a recipient email</td>
</tr>
<tr>
<td></td>
<td>address or is a duplicate email. See the Error String field for details.</td>
</tr>
<tr>
<td></td>
<td>- send - ready: The email is ready to be sent, but has not been sent out by the mail server. Typically, an email remains in this state for</td>
</tr>
<tr>
<td></td>
<td>only a short time.</td>
</tr>
<tr>
<td></td>
<td>- sent: The email was sent by the instance without any errors or issues.</td>
</tr>
<tr>
<td>Target</td>
<td>A Document ID reference to the record if the email is generated by an insert, update, or delete of a particular record.</td>
</tr>
<tr>
<td>User</td>
<td>The name of the user, from the user record, of the instance from which the email notification was sent.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a string field.</td>
</tr>
<tr>
<td>Notification Type</td>
<td>The type of notification. Choices are:</td>
</tr>
<tr>
<td></td>
<td>- None</td>
</tr>
<tr>
<td></td>
<td>- SMS</td>
</tr>
<tr>
<td></td>
<td>- SMTP</td>
</tr>
<tr>
<td>UID</td>
<td>The unique ID for the server.</td>
</tr>
<tr>
<td>Created</td>
<td>The date and time of the email activity for the locale of the machine running the instance.</td>
</tr>
<tr>
<td>Deleted</td>
<td>An indication of whether the email was deleted from an instance mailbox.</td>
</tr>
<tr>
<td>Weight</td>
<td>The weight of the email, which determines the sending priority relative to other notifications on the same table.</td>
</tr>
<tr>
<td>Importance</td>
<td>An indication that the email was sent with a changed level of importance, such as Urgent.</td>
</tr>
<tr>
<td>Originating Event and Notification</td>
<td>An embedded list that stores the event and notification that initiated the email notification.</td>
</tr>
<tr>
<td>Subject</td>
<td>A configured description of the action that generated the email notification. You create the subject text for notifications in System Notification &gt; Email &gt; Notifications.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Error String</td>
<td>The error string captured from the email server to determine why the email was not sent. This is logged only if the email is send-failed.</td>
</tr>
<tr>
<td>Recipients</td>
<td>The email address of the recipient of each notification.</td>
</tr>
<tr>
<td>Body</td>
<td>The body of the email, displayed in raw HTML markup. Use the related link Preview HTML Body to see the body text as rendered HTML.</td>
</tr>
<tr>
<td>Content type</td>
<td>The email content type.</td>
</tr>
<tr>
<td>Headers</td>
<td>Any headers embedded in the email.</td>
</tr>
</tbody>
</table>

Invalid email addresses that the instance strips out of outbound email messages are logged, starting with the Geneva release.

**Outbound email notification recipients**

For outbound notifications, the email system log provides reasons that recipients were included or excluded.

Each log entry corresponds to a reason for inclusion or exclusion. For example, all users who were excluded because they are inactive appear in a single log entry.

A series of system properties can be used to fine-tune the information to be logged. Two master switch properties, glide.notification.recipient.include_logging and glide.notification.recipient.exclude_logging, control all recipient inclusion and exclusion logging. Several other properties allow you to tailor the information reported in the logs to meet your needs. All of the properties are enabled by default.

**Outbound system logs**

**Email size limits**

To prevent issues with large email messages, the system enforces configured limits on the maximum allowed email body size, total attachment file size, and number of attachments per email.
An email or attachment that exceeds the system capacity may not be processed as expected. To ensure that your emails and attachments are processed as expected, you can configure properties that limit the size of emails and attachments.

**Message body size limit properties**
Several properties enforce the maximum email body size allowed for inbound and outbound email messages.

**Properties**

By default, the system processes up to 1MB worth of information in the email `body` and `body_text` fields (524KB each).

You can add and configure system properties `com.glide.email.max_body_bytes` and `glide.email.outbound.max_body_bytes` to increase or decrease the email body size limits, but note that the system truncates the body text for emails that exceed the configured limit. For example, if you configure the body size limit of `com.glide.email.max_body_bytes` to 2MB but receive an inbound email that is 3MB, then the system cuts 1MB worth of information from the email body.

Also note that the system cannot process emails larger than 16MB. Even if you configure the email body size limits to a value larger than 16MB, emails larger than 16MB are truncated.

**Message body size limit properties**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>com.glide.email.max_body_bytes</code></td>
<td>Sets the maximum body size in bytes allowed per inbound email. Ensure that the sum of this property and the <code>glide.email.inbound.max_total_attachment_size_bytes</code> property is well below the maximum total email size (16MB).</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 1048576</td>
</tr>
<tr>
<td><code>glide.email.outbound.max_body_bytes</code></td>
<td>Sets the maximum body size in bytes allowed per outbound email. Ensure that the sum of this property and the <code>glide.email.outbound.max_total_attachment_size_bytes</code> property is well below the maximum total email size (16MB).</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 1048576</td>
</tr>
</tbody>
</table>

**Note:** A different property, `com.glide.attachment.max_size`, sets the maximum file size allowed for any attachment in the system and overrides any larger values of `glide.email.inbound.max_total_attachment_size_bytes` and `glide.email.outbound.max_total_attachment_size_bytes`.

**Inbound email body processing**

For inbound emails, the system enforces the maximum body size as set by the `com.glide.email.max_body_bytes` property. When the body size exceeds the configured value:
• The system does not run inbound email actions that would otherwise be triggered by the email.
• The system truncates the Body text on the Email form.
• The system logs a warning and sets the Error string field on the Email form. The log message for such an email might look like this:

```
Email set to receive-ignored because its size exceeds the value set in com.glide.email.max_body_bytes. 1995 character(s) were truncated from the body field.
```

Outbound email body processing

For outbound emails, the system enforces the maximum body size as set by the `glide.email.outbound.max_body_bytes` property. When the body size exceeds the configured value:

• The system does not send the email.
• The system truncates the Body text on the Email form.
• The system logs a warning and sets the Error string field on the Email form. The log message for such an email might look like this:

```
Email set to send-ignored because its size exceeds the value set in glide.email.outbound.max_body_bytes. 1337 character(s) were truncated from the body field.
```

Attachment limit properties

Several properties control email attachment limits.

Properties

All the properties are located in the System Property (sys_properties) table. Setting any of the following properties to an excessively large value may cause performance issues.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>glide.email.inbound.max_attachment_count</code></td>
<td>Sets the maximum number of attachments allowed per inbound email.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Type</strong>: integer</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default value</strong>: 30</td>
</tr>
<tr>
<td></td>
<td>• <strong>Learn more</strong>: Inbound Email Attachment Processing</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><code>glide.email.inbound.max_total_attachment_size_bytes</code></th>
<th>The maximum total attachment size in bytes allowed per inbound email.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>Type</strong>: integer</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default value</strong>: 18874368</td>
</tr>
<tr>
<td></td>
<td>• <strong>Learn more</strong>: Inbound Email Attachment Processing</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>glide.email.outbound.max_attachment_count</code></td>
<td>Sets the maximum number of attachments allowed per outbound email.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Type</strong>: integer</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default value</strong>: 30</td>
</tr>
<tr>
<td></td>
<td>• <strong>Learn more</strong>: Outbound Email Attachment Processing</td>
</tr>
<tr>
<td><code>glide.email.outbound.max_total_attachment_size_bytes</code></td>
<td>Sets the maximum total attachment size in bytes allowed per outbound email.</td>
</tr>
<tr>
<td></td>
<td>To send an email, the system must encode the contents of the email. This process may significantly increase the size of the email, including any attachments. It is best to set this property to a value well below the maximum email size.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Type</strong>: integer</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default value</strong>: 18874368</td>
</tr>
<tr>
<td></td>
<td>• <strong>Learn more</strong>: Outbound Email Attachment Processing</td>
</tr>
</tbody>
</table>

**Note:** A different property, `com.glide.attachment.max_size`, sets the maximum file size allowed for any attachment in the system and overrides any larger values of `glide.email.inbound.max_total_attachment_size_bytes` and `glide.email.outbound.max_total_attachment_size_bytes`.

**Inbound email attachment processing**

For inbound emails, the system enforces the maximum number and size of attachments as set by the `glide.email.inbound.max_attachment_count` and `glide.email.inbound.max_total_attachment_size_bytes` properties. When the attachments for an inbound email exceed either value, the system logs a warning and discards the excess attachments. The order in which the system processes the attachments determines which attachments are discarded. This order may not be consistent from email to email.

**Outbound email attachment processing**

For outbound emails, the system enforces the maximum number and size of attachments as set by the `glide.email.outbound.max_attachment_count` and `glide.email.outbound.max_total_attachment_size_bytes` properties. Email records are created from various sources and may exceed the configured attachment limits.

Emails that are ready to be sent from the Email (sys_email) table are subject to the outbound attachment limits. Emails that exceed either limit trigger a warning in the email system log and are sent with attachments up to the maximum number or total file size.

The log message for such an email might look like this:

Maximum combined attachment size exceeded. (max:15728640 bytes). One or more attachment records ignored.
Emails for notifications, scheduled reports, and exported tables

Notifications can be set to include all the attachments from the record that triggers the notification. If the attachments exceed either of the outbound email attachment limits, the system excludes the excess attachments from the email and logs a warning message.

Reports can be scheduled for email distribution as attachments. Large reports may exceed the outbound attachment size limit. In this case, the system sends the scheduled report email without the report attached and logs a warning message. To avoid the issue, send links to large reports instead of sending the reports as attachments.

If a user attempts to export numerous records from a list that exceeds a configured warning threshold, a dialog box offers the option to email the exported records as an attachment. If the attachment exceeds the outbound attachment size limit, the system sends the email without the exported record list attached and logs a warning message.

Email diagnostics and troubleshooting inbound and outbound email

The Diagnostics and Connection page displays information about the current state of your email configuration. This page includes status on email properties, scheduled jobs, and email account connections that affect how your instance receives and sends email.

Email diagnostics

Email diagnostic information can help you identify problems with inbound or outbound email. The following video shows different steps to determine why your instance is not receiving inbound emails. One of the steps uses email diagnostics to check the email connection status and email reader scheduled job.

Navigate to the Diagnostics and Connection page from either of these modules:

- System Mailboxes > Email Diagnostics
- System Diagnostics > Email Diagnostics
## Email Diagnostics and Connection page

### Mail diagnostics

<table>
<thead>
<tr>
<th>Diagnostic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Sending is (Status)</td>
<td>Status of outbound email as either <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
</tr>
<tr>
<td>Diagnostic</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Email in Queue</td>
<td>Number of email messages that are ready to be sent.</td>
</tr>
<tr>
<td>Last Sent Mail</td>
<td>Date and time the last email message was sent.</td>
</tr>
<tr>
<td>SMTP Sender State</td>
<td>Current state of the SMTP Sender job, which sends email on a recurring schedule. By default, this job runs every minute.</td>
</tr>
<tr>
<td></td>
<td>To update the SMTP Sender state, click the <strong>SMTP Sender Job</strong> related link, and in the Schedule table, open the SMTP Sender record to be changed.</td>
</tr>
<tr>
<td>SMTP Sender Processing Time</td>
<td>Duration of the last SMTP Sender job run. This value should be shorter than the SMTP Sender interval.</td>
</tr>
<tr>
<td>SMTP Sender Job Last Run</td>
<td>Date and time when the SMTP Sender job last ran.</td>
</tr>
<tr>
<td>Default SMTP Status</td>
<td>Indication of whether the SMTP connection was successful, shown only if the email accounts feature is active. Click <strong>Default SMTP</strong> to change your SMTP account settings.</td>
</tr>
<tr>
<td>SMS Sender State</td>
<td>Current state of the <strong>SMS Sender</strong> job, which sends SMS notifications on a recurring schedule. By default, this job runs every minute.</td>
</tr>
<tr>
<td></td>
<td>To update the SMS Sender job, click the <strong>SMS Sender Job</strong> related link, and in the Schedule table, open the SMS sender record to be changed.</td>
</tr>
<tr>
<td>SMS Sender Processing Time</td>
<td>Duration of the last <strong>SMS Sender</strong> job run. This value should be shorter than the <strong>SMS Sender</strong> interval.</td>
</tr>
<tr>
<td>SMS Sender Job Last Run</td>
<td>Date and time when the <strong>SMS Sender</strong> job last ran.</td>
</tr>
<tr>
<td><strong>Email Receiving is (Status)</strong></td>
<td></td>
</tr>
<tr>
<td>Email Receiving</td>
<td>Status of inbound email as either <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
</tr>
<tr>
<td>Last Received Email</td>
<td>Date and time the last email message was received.</td>
</tr>
<tr>
<td>Email Reader Status</td>
<td>Current state of the email reader job, which downloads any email waiting on the mail server and creates email.read events.</td>
</tr>
<tr>
<td></td>
<td>To update the Email Reader Status job, click the <strong>Email Reader Job</strong> related link, and in the Schedule table, open the email reader record to be changed.</td>
</tr>
<tr>
<td>Email Reader Processing Time</td>
<td>Duration of the last reader job run. This value should be shorter than the reader interval.</td>
</tr>
<tr>
<td>Job Last Run</td>
<td>Date and time when the reader job last ran.</td>
</tr>
<tr>
<td><strong>Connection Status</strong></td>
<td></td>
</tr>
<tr>
<td>{Accounts}</td>
<td>The result of the test connection to the accounts. The connection is tested every time you load the page.</td>
</tr>
</tbody>
</table>
Troubleshooting email problems

See the following resources on troubleshooting inbound and outbound email problems.

<table>
<thead>
<tr>
<th>Error or symptom</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance not receiving inbound email</td>
<td>See Inbound Email Troubleshooting, ServiceNow KB0524472. This KB article also provides links to a video series on troubleshooting inbound emails.</td>
</tr>
<tr>
<td>Instance not sending outbound email</td>
<td>See Troubleshooting Outbound Email, ServiceNow KB0521382. This KB article also provides links to a video series on troubleshooting outbound emails.</td>
</tr>
<tr>
<td>Email from Outlook produces an empty Incident record containing an attachment named winmail.dat.</td>
<td>Configure the local Outlook client or Exchange server to not send Rich Text formatted (RTF) data to the instance.</td>
</tr>
</tbody>
</table>

Next steps after enabling email

After enabling email on your instance, consider performing several of these important tasks.

- Test the email configuration by routing all email to a single user (set the glide.email.test.user property).
- Review the baseline notification categories, email notifications, and templates to determine if they meet your business needs.
- Review the baseline inbound email actions to determine if they meet your business needs.
- Determine if you want to use email layouts to add consistent content elements.
- Determine if you want to use email filters to restrict the email the instance receives.
- Determine if you want to implement a retention policy to archive and destroy email at certain intervals.
- Determine what kind of watermarks outbound email uses to associate records with email messages.
- Determine if you want to create users when the instance receives an email from an unrecognized user.
- Set the precedence of outgoing mail. By default, the instance sends email with a precedence of bulk (set the glide.smtp.precedence_bulk property).
- Consider preventing untrusted users from triggering inbound actions to prevent unwanted email from affecting your instance.
- Implement a spam filter to restrict unwanted messages sent to your custom email addresses.

Create notification categories

You can create notification categories to identify and group related notifications that are listed in the notification settings for your users.

Role required: admin

Before adding new categories, review the base system notification categories in the Notification Categories (sys_notification_category) table to determine if you need a new category.

1. Navigate to System Notification > Email > Notification Categories.
2. Click New.
3. Enter the Name of the category to identify the family of notifications. Provide a category name that is meaningful to your users, so that they can easily find their notifications under the appropriate category in their notification settings.
4. Enter a Short description to identify the category.

© 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.
5. Click Submit.

The system adds the new category to the Notification Categories (sys_notification_category) table. After you create at least one, active notification that uses the new category, the category and notification are listed in the notification settings for users (Notifications tab in the System Settings window).

Create an email notification

Creating an email notification involves specifying when to send it, who receives it, and what it contains.

Your notification recipients must be active users and have a valid email address defined.

To have your email notification also send as an SMS notification, recipients must subscribe to the notification on an SMS channel. For more information on creating an SMS channel, see Create notification channels.

Role required: admin

Note: If you do not see all the fields on the form, switch to the Advanced view.

1. Configure email properties to enable your instance to send and receive email.
2. Navigate to System Notification > Email > Notifications.
3. Click New.
4. Fill in the fields at the top of the Notification form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique name for the email notification. Descriptive names help identify the purpose of the email notification. For example, Incident Opened &amp; Unassigned.</td>
</tr>
<tr>
<td>Table</td>
<td>Select the database table to link the notification to, for example Incident (incident). <strong>Attention:</strong> Do not select the Task (task) table. This table is for extending other tables. Notifications that run on the Task table directly are not supported. <strong>Note:</strong> Only tables and database views that are in the same application scope appear in the list.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Type</td>
<td>Select the type of notification you are creating: EMAIL or Meeting Invitation.</td>
</tr>
<tr>
<td>Active</td>
<td>Select the check box to enable the email notification.</td>
</tr>
<tr>
<td>Category</td>
<td>Select the category to which this notification belongs. A category identifies and groups related notifications. This notification, if active and subscribable, is listed in the selected Category in the notification preferences for each user (Notifications tab in the System Settings window).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Do not leave the category as Uncategorized, as users may not be able to find the notification in their list of notifications.</td>
</tr>
<tr>
<td></td>
<td>If you need a new category, see Create notification categories.</td>
</tr>
<tr>
<td>Description</td>
<td>Type a description for this notification.</td>
</tr>
</tbody>
</table>

5. Fill in the fields on the When to send tab.
Note: If the same trigger generates multiple notifications, the system only sends one notification. The system considers all other notifications, even if they have a different subject and body, as duplicates. The Ignore Duplicates business rule controls this functionality.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send when</td>
<td>Select under what condition the notification is sent: when a record is inserted or updated or when a particular event is triggered.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Weight</td>
<td>(Required) Set a numerical value for the notification priority relative to duplicate notifications. Notifications that have the same target table and recipients, or the same subject and body, are considered duplicates. When there are duplicate notifications, the system only sends the notification with the highest weight. All other notifications are moved from the Outbox to the Skipped mailbox. The default value 0 causes the system to always send the notification (assuming the conditions are met). For example, suppose that a service desk agent adds a comment to an incident and shortly thereafter closes it. By default, these actions trigger both the Incident commented and Incident Closed notifications. However, both notifications are from the Incident table and also notify the incident caller. The system only sends the notification with the highest weight, which in this case is the Incident Closed notification.</td>
</tr>
<tr>
<td>Conditions</td>
<td>Use the condition builder to select the conditions under which this notification is sent. For example, select Priority &gt; greater than &gt; 3 - Moderate to send the notification only for High and Critical priority incidents.</td>
</tr>
<tr>
<td>Inserted</td>
<td>Select the check box to enable email notification when a record is inserted. This field is visible only when the Send when field has been set to Record inserted or updated.</td>
</tr>
<tr>
<td>Updated</td>
<td>Select the check box to enable email notification when a record is updated. This field is visible only when the Send when field has been set to Record inserted or updated.</td>
</tr>
<tr>
<td>Event name</td>
<td>Select the event that triggers this notification. This field is visible only when the Send when field has been set to Event is fired.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Advanced condition</td>
<td>Create a script to perform certain actions, like sending a notification based on the current email record, changing field values, or changing system properties. <strong>The advanced condition</strong> script must return <strong>true</strong> or set a global answer variable to <strong>true</strong> to send the notification. The advanced condition script uses the following global variables: • current: contains the current record from the table to which the notification is linked. • event: contains the event that triggered the notification. <strong>Note:</strong> The Advanced condition field is evaluated in addition to other conditions you set on the notification. Both the condition and advanced condition must evaluate to true to send the notification.</td>
</tr>
</tbody>
</table>

6. Fill in the fields on the **Who will receive** tab.

**Tip:** Consider limiting the recipient list of any notification to 1000 users. By default, if a notification has more than 100 intended recipients, the system creates multiple notification messages with up to 100 recipients each. If you want to change the recipient limit, set the system property **glide.email.smtp.max_recipients**.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>Select the users you want to receive the email notification. You can search for users with the reference lookup icon or manually add their email addresses. This list of users is static.</td>
</tr>
<tr>
<td>Users/groups in fields</td>
<td>Select users or groups from reference fields. For example, if a notification uses the Incident (incident) table, then you can select users or groups from incident fields like Opened by and Assignment group. This list of users or groups is variable and depends upon the values of the associated task record.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You can dot-walk to values in reference fields by clicking the plus sign in the field selector and then selecting the related field.</td>
</tr>
<tr>
<td></td>
<td>If you address the notification to a user with an inactive record in the User (sys_user) table, the system does not send the notification to that user.</td>
</tr>
<tr>
<td>Groups</td>
<td>Select the groups you want to receive the email notification. You can search for groups with the reference lookup icon or by manually entering the group name. This list of groups is static.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Group members receive individual notifications only if Include members is selected in the group record.</td>
</tr>
<tr>
<td>Exclude delegates</td>
<td>Select this option to prevent the instance from sending email notifications to delegates of the users you selected.</td>
</tr>
<tr>
<td>Send to event creator</td>
<td>Select this check box to send the notification to the person who performed the action that started the notification process if the person is also a recipient. If the event creator is not specified in one of the recipient fields, the event creator does not receive a notification regardless of the setting in this field. For new notifications, this option is selected by default. If you want to know why you may not be receiving certain email notifications, see the blog post Troubleshooting email notifications - Send to the Event Creator by a ServiceNow Technical Support Engineer in the ServiceNow Now Community.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Event parm 1 contains recipient</td>
<td>Select this check box if the event parameter 1 contains one or more email recipients (in a comma separated-list). This field is visible only when the <strong>Send when</strong> field is set to <strong>Event is fired</strong>.</td>
</tr>
<tr>
<td>Event parm 2 contains recipient</td>
<td>Select this check box if the event parameter 2 contains one or more email recipients (in a comma-separated list). This field is visible only when the <strong>Send when</strong> field is set to <strong>Event is fired</strong>.</td>
</tr>
<tr>
<td>Subscribable</td>
<td>Select this check box to allow all users to subscribe to this notification. See <strong>Subscription-based notifications</strong> for more information.</td>
</tr>
</tbody>
</table>

**Note:** Do not enable this option for notifications that contain sensitive or protected data or where you want to restrict who can see it.

The system does not exclude recipients based on access controls. Recipients can receive email about records that they cannot normally access from the user interface. For example, requesters can receive email about incidents and catalog requests opened on their behalf even though they normally do not have access to these records. If a notification includes record details, verify that all recipients need these details.

**Note:** By default, the system does not send email notifications to itself. For example, an email notification from instanceABC@service-now.com does not send to instanceABC@service-now.com. The system prevents this behavior to avoid looping.

7. Fill in the fields on the **What it will contain** tab.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Email template| If you want to reuse existing content, select an email template to add content to the email notification. You can only select an email template that meets one of the following conditions:  
• shares the same scope and table as the notification  
• shares the same scope but has no specified table  
• shares the same table and is in the global scope                                                                                                                                                                                                                                                                                            |
| Subject       | Enter the subject line for the email message. The subject can include variables from the Select variables column.  
If empty, the system uses the Subject value from the Email template. If you enter a value in this field, it overrides the template value.  
If your recipients subscribe to the email notification on an SMS channel, then the system sends the email notification subject as an SMS message. To send a different SMS message, fill in the SMS alternate field on the email template form or the email notification form.                                                                                           |
| Message HTML  | Enter the content of the email notification message. The message can include variables from the Select variables column.  
Variables map to column names available from the notification table, its parent tables, and reference tables. Use variables to include values from a record in the table such as an incident short description or comments and work notes.  
The Message HTML field is visible only if you set the content type to HTML and plain text or HTML only.  
If empty, the system uses the Message HTML value from the Email template. If you enter a value in this field, it overrides the template value.  
To prevent adding extra <p> and <div> elements to your email notifications, see the blog post Extra line spacing with paragraph tags in email client by a ServiceNow employee in the ServiceNow Now Community.                                                                                     |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS alternate</td>
<td>Enter the notification message to send to an SMS device. The SMS alternate message is limited to 140 characters. If empty, the system uses the SMS alternate value from the Email template. If you enter a value in this field, it overrides the template value. If you don’t fill in the SMS alternate field on this form or the email template, then the system uses the email notification subject as the SMS message.</td>
</tr>
<tr>
<td>Importance</td>
<td>Set the importance of the email message to low or high.</td>
</tr>
<tr>
<td>Content type</td>
<td>Select the content type for the email notification:</td>
</tr>
<tr>
<td></td>
<td>· HTML and plain text</td>
</tr>
<tr>
<td></td>
<td>· HTML only                                                                                                           By default, HTML only is enabled.</td>
</tr>
<tr>
<td></td>
<td>· Plain text only</td>
</tr>
<tr>
<td>Include attachments</td>
<td>Select this check box to send all attachments from the triggering record as email attachments.</td>
</tr>
<tr>
<td>Omit watermark</td>
<td>Use this check box to apply or remove the watermark attached to each email. Do not remove the watermark as a reply to an email without a watermark creates an incident rather than updating the incident the original email referred to. For more information, and an alternative way to hide watermarks, see Watermarks on notification emails.</td>
</tr>
<tr>
<td>Message Text</td>
<td>Enter the notification message to send in plain text. This field is visible only if you set the content type to HTML and plain text or Plain text only. If empty, the system uses the Message Text value from the Email template. If you enter a value in this field it overrides the template value.</td>
</tr>
<tr>
<td>From</td>
<td>Enter the email address that you want the email notification to use in the From field. For example, <a href="mailto:helpdesk@yourcompany.com">helpdesk@yourcompany.com</a>. The email must be in a valid format, otherwise a notification message appears near the field. Changing this address requires an advanced email setup such as enabling email forwarding.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Reply to</td>
<td>Enter the email address you want people to use when replying to the email notification. For example, <a href="mailto:helpdesk@yourcompany.com">helpdesk@yourcompany.com</a>. The email must be in a valid format, otherwise a notification message appears near the field. You can add no more than one email address in this field. Changing this address requires an advanced email setup such as enabling email forwarding.</td>
</tr>
<tr>
<td>Push message only</td>
<td>Select this option to send this notification only as a push notification to a mobile device. The Push Notification feature must be active.</td>
</tr>
<tr>
<td>Push messages</td>
<td>Associate one or more push messages with this notification. The Push Notification feature must be active.</td>
</tr>
</tbody>
</table>

**Note:** The push message and notification must be for the same table.

8. Click **Submit**.

Images can be inserted into email notifications that were created in the Eureka release or that were converted to rich format using the HTML editor. The images can be stored in the image library in your instance, or they can be inserted as attachments.

*Convert legacy email notifications to rich HTML*

By default, new email notifications are created in the rich HTML format. But you can also convert legacy notifications to rich HTML.

Role required: admin

1. Navigate to **System Notification > Email > Notifications**.
2. On the **Email Notifications** list screen, click the name of the email notification you want to convert.
3. Click the **What it will contain** tab.
### Notification - Notify test case user

<table>
<thead>
<tr>
<th>When to send</th>
<th>Who will receive</th>
<th>What it will contain</th>
</tr>
</thead>
</table>

If using an Email Template, then Subject and Message will be used from the template unless overridden with a Subject and Message on this form.

**Content type**: HTML and plain text

**Include attachments**: 

**Omit watermark**: 

**Push Message Only**: 

**Email template**: 

**Subject**: Test notification: New test assigned to you (metric_type) - due by (due_date)

**Message**:

You have been assigned to complete tests on (metric_type). Please follow the link below and complete the tests by (due_date). You can save your results until you are ready to submit them. When you have completed the test, and filled in all final results, submit the test.

Click here to begin the test:

```xml
<mail_script>
var title = getAssessmentTitle();
var assessmentInstanceURL = (current.sys_id);
var url = "a href=" + link + "">" + link + ""></a>

<mailto>
</mail_script>
```

To view your test queue at any time, sign in and navigate to Self-Service > My Tests.

**SMS alternate**: 

Select variables:
4. Click **Switch to Rich HTML Editor**.

The system copies any raw HTML from the **Message** field and converts it to rich HTML in the **Message HTML** field. Additionally, any mail scripts in the body are automatically saved to the **Email Script [sys_script_email]** table and are replaced in the notification body with an embedded script tag. This makes the notification body easier to read.
If using an Email Template then Subject and Message will be used from the template unless overridden with a Subject and Message on this form.

Content type: HTML and/or text

Include attachments

Omit watermark

Push Message Only

Email template:

Subject: Test notification: New test assigned to you on "$(metric_type)" - due by $(due_date)

Message HTML:

You have been assigned to complete tests on "$(metric_type)". Please follow the link below and complete the tests by $(due_date). You can save your results until you are ready to submit them.

When you have completed the test and filled in all final results, submit the test.

Click here to begin the test:

$(mail_script:Notify test case script_1)

To view your test queue at any time, sign in and navigate to Self-Service > My Tests.
When you convert an email notification that was created in a version prior to Eureka to rich HTML, mail scripts are automatically moved to the Email Script (sys_script_email) table and an embedded script tag with the name of the script is automatically inserted into the body of the notification.

When creating new email notifications, write mail scripts using System Notification > Email > Notification Email Scripts. When the scripts are completed, add a ${mail_script:script name} embedded script tag to the email notification body. This makes it easy to use the same scripts in multiple email notifications. All you need to copy and paste from one notification to the next is the embedded script tag.

If you manually enter a mail script, any text bounded by <mail_script> </mail_script> in the body of a new or converted email notification or template which is saved to the record, a message asks whether the mail script should be converted.

In many cases, an unconverted mail script fails to run from inside the HTML editor. If you select Yes, the script is added to the Email Script (sys_script_email) table and is automatically replaced in the body with an embedded script tag. You can view the mail scripts in their original form by opening the email notification and clicking the Show Notification Scripts related link.

Advanced conditions for email notifications
Use an advanced condition to send a notification based on the current email record, changing field values, or system properties.

To send a notification using an advanced condition, you can:

- Call a function that returns a value, or
- Set the global variable answer using a script

For example, in the following code, you call a function to prevent the system from sending an email notification if the sender of a self-service request is a member of the XYZ group:

```javascript
(function() {
    var groupMember = gs.getUser();
    return !groupMember.isMemberOf('XYZ');
})();
```
Alternatively, you can script the same advanced condition by using the `answer` variable:

```javascript
var groupMember = gs.getUser();
if(groupMember.isMemberOf('XYZ')){
    answer = false;
} else {
    answer = true;
};
```

Note that the script must set the `answer` variable to `true` to send the notification. If you script no conditionals, the value of `answer` is equal to the last value that you set for the variable.

You can add a script-based condition in the **Advanced condition** field by configuring the Email Notification form and adding the field. You can access the field in the **Advanced** view without configuring the form.

The advanced condition script uses the following business rule global variables:

- `current`: contains the current record from the table to which the notification is linked.
- `event`: contains the event that triggered the notification.

---

**Note:** The **Advanced condition** field is evaluated in addition to other conditions you set on the notification. Both the **Condition** and **Advanced condition** must evaluate to true in order to send the notification.

---

**Edit HTML content in an email notification**

For added control over the content of an email notification, you can edit the underlying HTML.

Role required: admin

1. Navigate to **System Notification** > **Email** > **Notifications**.
2. Open an email notification record.
3. On the form, open the **What it will contain** tab.
4. In the **Message HTML** field, click the source code icon (余额) to open the HTML source code editor.
5. Make the needed changes to the HTML.
6. On the window, click **Ok**.
7. On the form, click **Update**.

**Document attachments on an email notification**

You can attach documents and reports to email notifications by scripting or linking to the sys ID of the record.

You can include all attachments from the source record with the notification. For example, if an incident update generates a notification, you can include all attachments from the incident record with the notification. To include all attachments from the source record, select the check box for the **Include attachments** field. Note that email messages, including attachments, cannot exceed the maximum email size. This size includes MIME encoding, which increases total attachment size by approximately 37%.
Attaching documents with scripting

Using scripting, you can attach documents by linking to them, or you can attach various types of reports by specifying their IDs in the system.

Linking to an attachment

You can add attachments to a notification by linking to the attachment record in the message of the notification. Linking to attachment records in this fashion requires using email notification scripting. For example:

```java
template.print ( 'Attachment: <a href="/sys_attachment.do?sys_id=' + gr.sys_id + '">' + gr.file_name + '</a>');
```

Attaching reports using the Sys ID

You can also attach various types of reports, including gauges, dashboards, and charts, to a notification. The scripts to attach these reports take the following syntax:

```java
${report:X:Y}
```

where:

- X is the type of report you want to attach (reportID, gaugeID, dashboardID, or chartID).
- Y is the sys ID of the report, gauge, dashboard, or chart to be attached.

For example:

- ${report:reportID:<abc123>}
- ${report:gaugeID:<abc123>}
- ${report:dashboardID:<abc123>}
- ${report:chartID:<abc123>}

Line breaks in email notifications and rich HTML

Rich HTML provides additional control over line breaks in your email notifications and templates. To provide control over line breaks, a Newlines to HTML check box is available in the Email Script form.
Newlines to HTML option

Selecting the **Newlines to HTML** check box indicates that the method for handling line breaks in earlier versions carries forward for email notifications and templates. When an email notification or template is converted to rich HTML, the **Newlines to HTML** check box is automatically selected.

For new mail scripts, add correct HTML line breaks to `template.print()` statements.

If an email notification or template is not converted to rich HTML, newlines are automatically wrapped with `<div>` tags, the same as previous versions. The old mail scripts still work. However, the administrator does not enjoy the benefits of working in the rich HTML format, and does not have as much control over exact HTML formatting.
HTML line breaks in new scripts

When writing new scripts, insert explicit HTML line breaks and clear the Newlines to HTML check box so that no HTML tags are injected when email notifications are generated. For existing notifications and templates, replace template.print("\n") JavaScript function calls with template.print("<br />"). This replacement gives you better control over the HTML formatting of your email notifications.

Preview email notifications

You can preview what notifications look like before you actually enable the instance to send them.

Role required: admin

You can preview both types of notifications as specified by the Send when field on the Notification form:

- **Record inserted or updated**: A change to a record in the instance triggers the notification.
- **Event is fired**: An event, such as expiration of a certificate or an inbound email action, triggers the notification.

1. Navigate to System Notification > Email > Notifications.
2. Open the notification or create one.
   - You must save the record before you can view the preview accurately.
3. Click Preview Notification on the form header.
4. On the Notification Preview window, verify that the notification works as expected.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preview records for this breakdown source</td>
<td>The type of event that triggers the notification. This choice list appears if you preview an event-triggered notification. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Generated Event</strong>: Preview the notification with a generic event that the previewer creates. This does not actually generate an event record.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Existing Event</strong>: Preview with an existing event record in the instance. If you select this option, select the event in the Event Record field.</td>
</tr>
<tr>
<td>Event Record</td>
<td>An existing event to preview an event-created notification. This option appears if you select Existing Event as the event type (for event-triggered notifications only).</td>
</tr>
<tr>
<td>Event Creator</td>
<td>The user triggering the notification for the purpose of the preview. The event creator defaults to the user who clicked Preview Notification.</td>
</tr>
<tr>
<td></td>
<td>You can change the creator as needed. You can change the preview record as needed to see the changes in the notification content.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Preview Record</td>
<td>The record triggering the notification for the purpose of the preview. The preview record defaults to one of the records in the table specified in the Table field on the Email Notification form. You can change the preview record as needed to see the changes in the notification content.</td>
</tr>
<tr>
<td>Users</td>
<td>The users who will receive the notification, as specified in the Who will receive section of the Email Notification form:</td>
</tr>
<tr>
<td></td>
<td>· All users that you specify on the form appear, but only the users that will actually receive the notification with the current preview settings appear in black text.</td>
</tr>
<tr>
<td></td>
<td>· Users that are specified but for whatever reason will not receive the notification appear in red, strikethrough text. Place the cursor over any of these names to see the reason the user will not receive the notification. For example, one reason could be that the user’s notification settings are disabled.</td>
</tr>
<tr>
<td>Subject and Body</td>
<td>The content of the notification as defined by the template. The Subject and Body sections on the preview display the content in the corresponding Subject and Message fields on the template.</td>
</tr>
<tr>
<td></td>
<td>If the template includes a link to the record that triggered the notification, the Preview Record link is used. Click the link to go to that record.</td>
</tr>
</tbody>
</table>

5. After you have reviewed the notification, exit the preview window.
6. Make the necessary changes to the notification or template, if necessary.

**Time zone for email notifications**
A system property controls the time zone that the instance uses for the date and time stamp of a message.

The date and time stamp of a notification uses the system time zone, not the time zone of any recipient. The email property `glide.email.append.timezone` controls whether to append the time zone. If true, the system time zone of the instance is appended to any Date/Time fields in outbound email messages (for example, 2018-07-02 04:01:14 PST).

**Specify alternative outbound email addresses for notifications**
By default, the system sends all outbound email notifications from the default email address of the instance, but you can specify an alternative address.

Role required: admin
For organizations that need to send email messages from specific email addresses, such as from multiple service desks, or they want to send notifications in different languages, the platform supports configuring multiple outbound addresses.

1. Navigate to **System Notification > Email > Notifications**.
2. Select an existing notification record for the desired event, such as **Incident Closed**.
3. Create a copy of this notification for each outbound email address.
4. Open one of the notification copies, and click the **Advanced view** related link.
5. In the **What it will contain** section, add an email address to the From field that is different from the default instance address.
   
   For more information on how to construct the From address, refer to section 3.6.2 of **RFC 2822**.
6. Add a different email address than the From address to the **Reply to** field if you want replies to this notification to go to a different address.

   The system checks the From field for an address. If this field is empty, then the system uses the default address for the instance. If the Reply to field is empty, then all replies are sent to the address from which the notification was sent. If the Reply to field contains an email address, then the system sends all replies to the notification to this address.
7. Create mutually-exclusive conditions for notifications of the same type, so only the desired notification is sent when the event is fired.

   For example, if the **Company** is a certain value, then the notification comes from a unique email address entered in the From field.
8. Click **Update**.

**Specify an outbound email address for a particular language**

You can specify a different email address for each language your instance supports.

Role required: admin

1. Create or copy a notification record for the desired event.
2. In the **What will it contain** section, enter a new email address in the From field.
3. Create the **Subject** and **Message** content in the desired language.
4. In the **When to send** section, create a condition as follows:
   1. In the list of **Condition** fields, select **Show Related Fields** from the bottom of the choice list.
   2. From the choice list of **Related Fields**, select the field that identifies the recipient.

      For example, select **Caller > User** fields to send the notification to the user who called in an incident, or **Assigned to > User** fields to send the notification to the user to whom an incident is assigned.
   3. From the choice list of user fields, select **Language**.
   4. Select the **is** operator.
   5. Complete the condition by selecting the language of the desired user.

5. Click **Update**.

   All notifications for that event originate from the specified email address and go out in the language of the recipient.

**Notification variables**

Use notification variables to display dynamic information in the body of a notification such as a field value, a link to a record, or a link to system preferences.
Syntax

Specify a notification variable using this syntax:

`${variable-name+variable-parameters}`

The `variable-name` portion is always required. Not all notification variables support the `variable-parameters` portion. When available, most variable parameters are optional. See the list of available notification variables for variable names and available parameters.

Available variables

The system provides these notification variables.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Available parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>${field-name}</code></td>
<td>Display the value of the specified field.</td>
<td>None</td>
</tr>
<tr>
<td><code>${image-field-</code></td>
<td>Display an image associated with a record. This variable is typically used</td>
<td>None</td>
</tr>
<tr>
<td>name}`</td>
<td>with HTML to specify the source of an image element.</td>
<td></td>
</tr>
<tr>
<td>· <code>${URI}</code></td>
<td>Display a link to the current record.</td>
<td>Any valid <code>sysparm</code></td>
</tr>
<tr>
<td>· <code>${URL_REF}</code></td>
<td><code>URI</code>: The link text is the word <code>LINK</code>.</td>
<td><code>sysparm_scriptlet</code></td>
</tr>
<tr>
<td></td>
<td><code>URI_REF</code>: The link text is the display value of the record.</td>
<td><code>sysparm_view</code></td>
</tr>
<tr>
<td>· <code>${reference-</code></td>
<td>Display a link to the record listed in a reference field.</td>
<td>Any valid <code>sysparm</code></td>
</tr>
<tr>
<td>field.URI}`</td>
<td><code>URI</code>: The link text is the word <code>LINK</code>.</td>
<td><code>sysparm_scriptlet</code></td>
</tr>
<tr>
<td></td>
<td><code>URI_REF</code>: The link text is the display value of the record.</td>
<td><code>sysparm_view</code></td>
</tr>
<tr>
<td><code>${CMS_URI}</code></td>
<td>Display a link to the specified record within a CMS page.</td>
<td><code>&lt;CMS-site&gt;/CMS-</code></td>
</tr>
<tr>
<td></td>
<td>page&gt;`: The required relative path to the CMS page.</td>
<td></td>
</tr>
<tr>
<td><code>${notification:body}</code></td>
<td>Display the body contents of an email template or email notification. Use this notification variable to specify where to display body content in an email layout.</td>
<td>None</td>
</tr>
<tr>
<td><code>${mail_script:script-name}</code></td>
<td>Run the specified mail script.</td>
<td>None</td>
</tr>
<tr>
<td><code>${NOTIF_UNSUB}</code></td>
<td>Display a link unsubscribe from this notification.</td>
<td><code>link_text</code>: specify the text to display as a link within quotation marks.</td>
</tr>
<tr>
<td><code>${NOTIF_PREFS}</code></td>
<td>Display a link to set notification preferences.</td>
<td><code>link_text</code>: specify the text to display as a link within quotation marks.</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
<td>Available parameters</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td><code>${comments:n}</code></td>
<td>Display the most recent comments that were made on the target record. The number of comments to display is n. For example, <code>${comments:3}</code> displays the last three comments that were made to the record. To display all comments, use the variable <code>${comments}</code>.</td>
<td>Any number greater than 0.</td>
</tr>
<tr>
<td><code>${comments_and_work_notes:n}</code></td>
<td>Display the most recent comments and work notes that were made on the target record. The number of comments and work notes to display is n. For example, <code>${comments_and_work_notes:3}</code> displays the last three comments and work notes that were made to the record. To display all comments and work notes, use the variable <code>${comments_and_work_notes}</code>.</td>
<td>Any number greater than 0.</td>
</tr>
</tbody>
</table>

**Examples**

Refer to the following examples to see how each notification variable is rendered in the output:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Example</th>
</tr>
</thead>
</table>
| `${field-name}` | Source: Incident ${number} - comments added  
Output: Incident INC1000001 - comments added |
<table>
<thead>
<tr>
<th><strong>Variable</strong></th>
<th><strong>Example</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>${image-field-name}</td>
<td>Source: <code>&lt;img src='${picture}?t=medium'/&gt;</code></td>
</tr>
<tr>
<td></td>
<td>Output:</td>
</tr>
<tr>
<td></td>
<td><img src="image-field-name" alt="Image Field Example" /></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Variable</strong>: <code>$(URI)</code> and <code>$(URI_REF)</code></td>
</tr>
<tr>
<td></td>
<td>Source: Click here to view incident: <code>$(URI)</code></td>
</tr>
<tr>
<td></td>
<td><code>$(URI)</code> Output:</td>
</tr>
<tr>
<td></td>
<td><img src="URI" alt="URI Example" /></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Variable</strong>: <code>$(reference-field.URI)</code> and <code>$(reference-field.URI_REF)</code></td>
</tr>
<tr>
<td></td>
<td>Source: Click here to view Incident: <code>$(URI_REF)</code></td>
</tr>
<tr>
<td></td>
<td>Click here to view Related Problem: <code>$(problem_id.URI_REF)</code></td>
</tr>
<tr>
<td></td>
<td>Output:</td>
</tr>
<tr>
<td></td>
<td><img src="reference-field.URI" alt="Reference Field Example" /></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>Variable</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>${CMS_URI}</td>
<td>Source: <code>${CMS_URI+ess/incident_detail}</code></td>
</tr>
<tr>
<td></td>
<td>Output: a link to a target CMS page such as</td>
</tr>
<tr>
<td></td>
<td>https://&lt;instance name&gt;.service-now.com/ess/incident_detail.do?</td>
</tr>
<tr>
<td></td>
<td>sysparm_document_key=incident,46e18c0fa9fe19810066a0083f76bd56</td>
</tr>
<tr>
<td>Variable</td>
<td>Example</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>${notification:body}</td>
<td></td>
</tr>
<tr>
<td>${mail_script:script-name}</td>
<td></td>
</tr>
<tr>
<td>${NOTIF_UNSUB}</td>
<td></td>
</tr>
<tr>
<td>${NOTIF_PREFS}</td>
<td></td>
</tr>
</tbody>
</table>
Links to records in email notifications

Adding the \${URI} parameter to an outbound email body or template creates a link to a specific record.

When a user clicks the word LINK, the instance prompts the user to log in if not already logged in, and then redirects the user to the record specified in the URI.

![Short description: SAP Sales app is not accessible](image)

Click here to view incident: LINK

Comments:

**Link displayed by \${URI} parameter**

The \${URI} parameter has an extension called the \${URI+} format to specify additional arguments in the email link, such as sysparm terms, in addition to the automatically created URI. For example (whitespace added for improved readability):

```
\${URI+&sysparm_scriptlet=current.assigned_to=gs.getUserID()
&sysparm_scriptlet_condition=current.assigned_to.nil()
&sysparm_view=incident_active}
```

This example executes the JavaScript:

```
current.assigned_to=gs.getUserID()
```

when the condition of

```
current.assigned_to.nil()
```

is satisfied. Additionally, the script sets the view to incident_active.

Enable links to records

Adding the special \${URI} parameter to an outbound email body or template creates a link to a specific record.

When a user clicks the word LINK, the instance prompts the user to log in if not already logged in, and then redirects the user to the record specified in the URI.

![Short description: SAP Sales app is not accessible](image)

Click here to view incident: LINK

Comments:

**URI email notification**

The \${URI} parameter has an extension called the \${URI+} format to specify additional arguments in the email link, such as sysparm terms, in addition to the automatically created URI. For example (whitespace added for improved readability):

```
\${URI+&sysparm_scriptlet=current.assigned_to=gs.getUserID()
&sysparm_scriptlet_condition=current.assigned_to.nil()}
```
This example executes the JavaScript:

```javascript
current.assigned_to=gs.getUserID()
```

when the condition of

```javascript
current.assigned_to.nil()
```

is satisfied. Additionally, the script sets the view to `incident_active`.

Change the link text

To show the display value of the record as the link text instead of the word LINK, use the `${URI_REF}` parameter instead of the `${URI}` parameter.

---

**Short description: SAP Sales app is not accessible**

**Click here to view incident: INC0000055**

**Comments:**

---

**URI_REF email notification**

For example, if the URL displays an incident record, the link text is the incident number, which is the display value for incidents. If the URL displays a user record, then the link text is the user name.

**Link to related records**

A notification can link to a related record by specifying a reference field in front of the `${URI}` or `${URI_REF}` parameters.

Format the related record link as follows:

- `${<reference field that contains the related record you want to display>}.URI`
- `${<reference field that contains the related record you want to display>}.URI_REF`

For example:

<table>
<thead>
<tr>
<th>Related record to provide link to</th>
<th>Notification record table</th>
<th>Reference field</th>
<th>Samples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Related task record to be approved from an approval notification</td>
<td>Approval (sysapproval_approver)</td>
<td>Approval for (sysapproval)</td>
<td>${sysapproval.URI} ${sysapproval.URI_REF}</td>
</tr>
<tr>
<td>Related problem record in an incident notification</td>
<td>Incident</td>
<td>Problem (problem_id)</td>
<td>${problem_id.URI} ${problem_id.URI_REF}</td>
</tr>
</tbody>
</table>

For example, the following notification template produces the email links in the picture below:

```java
Click here to view Incident: ${URI_REF}
```
Content page links in email notifications

Links to CMS pages can be put in notifications to make it easy for the reader to access the pages. The link takes the following format: \( \text{
CMS\_URI+<site>/<page>} \).

For example, to link the email recipient to a page called \text{Incident} in the content site \text{ESS}, with the current incident as the target document, use the following format: \( \text{
CMS\_URI+ess/incident\_detail} \).

The resulting email URL has this format: \( https://<\text{instance}\_name>.service-now.com/ess/incident\_detail.do?sysparm\_document\_key=incident,46e18c0fa9fe19810066a0083f76bd56 \).

Email unsubscribe

Administrators can add unsubscribe links to notifications so that users can stop receiving particular email messages.

The system offers two types of macros to create unsubscribe links.

- An unsubscribe link that creates an email message to the instance.
- An unsubscribe link that opens the notification preferences for the user on the instance.

### Available unsubscribe macros

<table>
<thead>
<tr>
<th>Unsubscribe type</th>
<th>Macro used</th>
<th>Description</th>
<th>Available parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unsubscribe by email (Unauthenticated)</td>
<td>( \text{NOTIF_UNSUB} )</td>
<td>The system generates an HTML \text{mailto} hyperlink. When users click the link, their browser or email client creates a pre-formatted unsubscribe email message to the instance.</td>
<td>\text{link_text}: specify the text to display as a link within quotation marks.</td>
</tr>
<tr>
<td>Unsubscribe by notification preferences (Authenticated)</td>
<td>( \text{NOTIF_PREFS} )</td>
<td>The system generates an instance link directly to the notification preferences for this notification type.</td>
<td>\text{link_text}: specify the text to display as a link within quotation marks.</td>
</tr>
</tbody>
</table>

Administrators can add unsubscribe macros to any notification record type such as:

- Email layouts
- Email templates
- Email notifications

### Unsubscribe by email

Unsubscribe by email requires the user email client or browser to create a pre-formatted email message containing these elements:

- The \text{To} field has the email address of the instance.
- The \text{Subject} starts with the string \text{Unsubscribe from}. 
ServiceNow    Jakarta    Now Platform Capabilities

- The **Body** has a JSON string with a name-value pair of **Unsubscribe** and an array value that contains two more name-value pairs.
- The **notification_id** parameter specifies the Sys ID of the notification the user wants to unsubscribe from.
- The **unsub_token** parameter specifies an instance ID the system uses to verify that the email came from a ServiceNow instance.

---

**Note:** Some email clients and web browsers, such as GMail on Chrome, require extra client configuration to support mailto hyperlinks. Administrators can provide an alternative unsubscribe method for users whose email client or browser does not support mailto links. See [RFC6068](#) for information about the mailto URI scheme.

The **Unsubscribe from Notification** inbound action processes the email and unsubscribes the sender from the listed notification.

---

**Note:** Unsubscribing by email message does not require users to authenticate with the instance first.

### Unsubscribe by notification preferences

Unsubscribe by notification preferences requires the user’s browser to navigate to the notification preferences page on the instance. After logging in, the system displays the notification preferences for this particular notification.

Users can set preferences for this notification such as disabling notifications for a particular device. Users must save their notification preferences for changes to take effect.

### Unsubscribe links

This email layout adds several unsubscribe links to the bottom of each email notification.

```html
${NOTIF_UNSUB} from this notification by email or ${NOTIF_UNSUB+link_text="click here"}.
Manage your ${NOTIF_PREFS} or ${NOTIF_PREFS+link_text="click here"}.
```

When rendered in an email notification, the unsubscribe links only display the link text.
Sample email with unsubscribe links

If a user clicks the **Unsubscribe** link, the email client creates a message such as this:
Scripting for email notifications
Email scripts allow for business rule-like scripting within an outbound email message.

With mail scripts, you can dynamically change the email output of your system based on different criteria. Mail scripts allow you to perform simple tasks, such as displaying incident data, and complex ones, such as making advanced database queries.

You can add a `${mail_script:script name}` embedded script tag to the body of the email notification or template, replacing `script name` with the name of the script you created. This makes it easy to use the same scripts in multiple email notifications or templates.

If you manually enter a mail script bounded by `<mail_script>` and `</mail_script>` in the body of a new or converted email notification or template, and then attempt to save the record, a message asks whether the mail script should be converted. In many cases, an unconverted mail script fails to run from inside the HTML editor. If you select Yes, the script is added to the Email Script (sys_script_email) table and is automatically replaced in the body with an embedded script tag `${mail_script:script_name}`).

JavaScript in emails
Create mail scripts in System Notifications > Email > Notification Email Script, and refer to them by using `${mail_script:script name}` in the script field.

To print text into the body of the message, use the `template.print("a string")` function.
JavaScript in templates

The `event.parm1` and `event.parm2` parameters that come from the originating event can also be used.

**Mail script API**

Certain variables are available when processing mail_script scripts.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Object Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>template</code></td>
<td>Handles printing from the mail script to the email message.</td>
</tr>
<tr>
<td></td>
<td><code>template.print(&quot;message&quot;);</code> // outputs message to the email body.</td>
</tr>
<tr>
<td></td>
<td><code>template.space(&quot;number of spaces&quot;);</code> // outputs spaces to the email body.</td>
</tr>
<tr>
<td><code>email_action</code></td>
<td>GlideRecord object for the email notification (sysevent_email_action).</td>
</tr>
<tr>
<td><code>event</code></td>
<td>GlideRecord object for the event that fired the notification (sysevent).</td>
</tr>
</tbody>
</table>
### Variable | Object Description
---|---
email | EmailOutbound object

**Available methods:**
- `addAddress(String type, String address, String displayname)`
  - Type can be cc or bcc.
- `setFrom(String address)`
  - Override the sender address.
- `setReplyTo(String address)`
  - Override the reply to address.
- `setSubject(String subject)`
  - Override the subject of the message.
- `setBody(String message)`
  - Override the body of the message.

The email address that is passed by `setFrom` and `setReplyTo` needs to be in a valid form such as helpdesk@sn.com or Display Name <helpdesk@sn.com>. If the email address includes a 'Display Name', then that value overrides the instance's display name.

Example scripting for email notifications

Examples of scripting for email notifications.

#### Scripting examples for email notifications

A simple text string is the most basic example of the way a mail script works. This script prints out "Incident number - INC00001".

```java
template.print("Incident number - " + current.number);
```

More advanced scripts, like this one, can be found by browsing through the base system email templates.

```java
template.print("Summary of Requested items:<br />");
var gr = new GlideRecord("sc_req_item");
gr.addQuery("request", current.sysapproval);
gr.query();
while(gr.next()) {
    template.print(gr.number + ": " + gr.quantity + " X " +
gr.cat_item.getDisplayValue()
    + " at " + gr.cat_item.price.getDisplayValue() + " each
    <br />");
}
```

To dynamically change field values within an email, use the following functions within `<mail_script>` syntax:

```java
...email.setFrom(current.caller_id.email);
email.setReplyTo("joe.employee@yourcompany.com");
email.setSubject("This is the new subject line");
email.setBody("This is the new body");
```
Using the `instance_name` property ensures that the notification still works when migrated between instances.

```javascript
function dothis(){
  var gr =new GlideRecord('sys_attachment');
  gr.addQuery('table_sys_id',current.sys_id);
  gr.query();while(gr.next()){/
    template.print('Attachment: <a href=https://' +
    gs.getProperty('instance_name')+'.service-now.com/sys_attachment.do?sys_id=' + gr.sys_id+'">'+
    gr.file_name+'</a>');}
}
```

You can specify copied and blind copied recipients by using the email object within a mail script.

```javascript
//email.addAddress(type, address, displayname);
email.addAddress("cc","john.copy@example.com","John Roberts");
email.addAddress("bcc","john.secret@example.com","John Roberts");
```

The following is an example script to add users from `watch_list` as copied recipients.

```javascript
if(!current.watch_list.nil()){/
  //get watch list addresses and add to cc
  var watcherIds = current.watch_list.split(",");

  //get user records
  var user =new GlideRecord("sys_user");
  user.addQuery("sys_id", watcherIds);
  user.addQuery("notification",2);
  //email
  user.addQuery("email","!=","”);
  user.query();

  while(user.next()){/
    //add to cc list
    email.addAddress("cc", user.email, user.getDisplayValue());}
}
```

Useful attachment scripts

This is a searchable version of the Useful Attachment Scripts.

**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](https://community.servicenow.com).

**Copy attachments from record to record**

Use the following script to copy an attachment from one record to another record:

```javascript
GlideSysAttachment.copy('sourcetable','sys_id','destinationtable','sys_id');
```

**Note:** GlideSysAttachment.copy copies all attachments; it cannot select specific attachments.
Delete duplicate attachments

Use the following script in a business rule, scheduled job, or background script to delete duplicate attachments located in the Attachments (sys_attachment) table:

```javascript
function fixDuplicateImages(){
var gr = new GlideRecord('sys_attachment');
gr.addQuery('table_name','LIKE','ZZ_YY%');
gr.orderBy('table_sys_id');
gr.orderByDesc('sys_created_on');
gr.query();
while(gr.next()){
var isDuplicate = (gr.table_sys_id == lastID &&
gr.file_name == lastFile);
lastID = gr.table_sys_id;
lastFile = gr.file_name;
gs.print(gr.table_sys_id + ' ' + gr.table_name + ' ' + gr.file_name + ' ' +
gr.sys_created_on + ' ' + isDuplicate);
if(isDuplicate) gr.deleteRecord();
}
}
```

Display whether tasks have attachments in list view

Use the following script in a business rule to display whether tasks have attachments when viewed in the record list view. Note that the script needs a custom field on the Has Attachments (u_has_attachments) table.

```javascript
function checkAttachment(){
if(current.operation()=='insert'){
hasAttachment('true');
}
if(current.operation()=='delete'){
var attachCount = new GlideAggregate('sys_attachment');
attachCount.addQuery('table_sys_id',current.sys_id);
attachCount.addAggregate('COUNT');
attachCount.query();
var numAttachments = '0';
if(attachCount.next()){
numAttachments = attachCount.getAggregate("COUNT");
}
if(numAttachments >0){
hasAttachment = 'true';
} else{
hasAttachment = 'false';
}
var timeNow4 = new GlideDateTime();
gs.log('has_attachment br: gliderecord query start date time is: ' +
timeNow4.getNumericValue(),'jwtest');
}
function hasAttachment(answer){
var task = new GlideRecord('task');
task.addQuery('sys_id',current.table_sys_id);
task.query();
if(task.next()){
task.u_has_attachment = answer;
task.autoSysFields(false); //Don't set the lastUpdatedTime or the
Simultaneous Update Alert will likely get triggered
}
task.setWorkflow(false); //Don't allow other business rules to run,
otherwise multiple notifications will likely be sent
```
Link to attachments in an email notification

Use the following script in an email notification or template to include links to attachments:

```javascript
printattachments();

function printattachments(){var gr =new GlideRecord('sys_attachment');
    gr.addQuery('table_sys_id',current.sys_id);
    gr.query();while(gr.next()){ template.print('Attachment: <a href="http://'+gs.getProperty("instance_name")+'.service-now.com/
    sys_attachment.do?sys_id='+ gr.sys_id+'">'+ gr.file_name+'</a>');}}
```

Note: Replace “instance_name” with your instance name.

Attachment Logging

Whenever a user downloads an attachment, the action writes an attachment.read event record to the event log. If desired, you can process these events with a Script Action or an Email Notification. This can be useful if you want to do something when an attachment is read. For example, you can record when and by whom certain attachments are downloaded. For this functionality, the current variable must point to a sys_attachment record, and the event record must use the following parameters:

- parm1: File name
- parm2: Table name

Baseline email notifications

The baseline system provides several email notifications.

Some events listed in this table do not appear in a business rule and are fired by other conditions in the platform. Some events are hardcoded and are not user configurable.

Baseline email notification descriptions

<table>
<thead>
<tr>
<th>Email notification</th>
<th>Description</th>
<th>Triggering event</th>
<th>Business Rule Controlling Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appointment Invite</td>
<td>Type: Meeting Invitation Adds a meeting invitation to the recipient’s calendar by sending an iCalendar formatted email</td>
<td>itil_appointment.inserted</td>
<td>Global business rule</td>
</tr>
</tbody>
</table>

Note: Schedule the business rule to run after insert/delete.
<table>
<thead>
<tr>
<th>Email notification</th>
<th>Description</th>
<th>Triggering event</th>
<th>Business Rule Controlling Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appointment Update</td>
<td>Type: Meeting Invitation&lt;br&gt;Updates an existing meeting in the recipient’s calendar by sending an iCalendar formatted email</td>
<td>itil_appointment.updated</td>
<td>Global business rule</td>
</tr>
<tr>
<td>Approval Rejected</td>
<td>Type: EMAIL&lt;br&gt;A task-based approval has been rejected – includes the approver’s name.</td>
<td>approval.rejected</td>
<td>approver events</td>
</tr>
<tr>
<td>Approval Rejected by Other</td>
<td>Type: EMAIL&lt;br&gt;A task-based approval has been rejected – includes the approver’s name.</td>
<td>approval.rejected.by.other</td>
<td>approval events</td>
</tr>
<tr>
<td>Approval Request</td>
<td>Type: EMAIL&lt;br&gt;Sends an email for the recipient to reply with an approval decision. In the approval email, the recipient selects a link that builds the appropriate reply email. These emails come only from task-based approvals.</td>
<td>approval.inserted</td>
<td>approver changes</td>
</tr>
<tr>
<td>Catalog Approval Rejected</td>
<td>Type: EMAIL&lt;br&gt;A catalog request has been rejected – includes the approver’s name.</td>
<td>request.approval.rejected</td>
<td>approval events</td>
</tr>
<tr>
<td>Catalog Approval Request</td>
<td>Type: EMAIL&lt;br&gt;A catalog request for which you were an approver has been cancelled.</td>
<td>request.approval.cancelled</td>
<td>approver changes</td>
</tr>
<tr>
<td>Catalog Approval Request</td>
<td>Type: EMAIL&lt;br&gt;A catalog request for which you are an approver has been made.</td>
<td>request.approval.inserted</td>
<td>approval events</td>
</tr>
<tr>
<td>Certificate Expired</td>
<td>Type: EMAIL&lt;br&gt;Notification that the X.509 certificate has expired.</td>
<td>certificate.expired</td>
<td>certificate events</td>
</tr>
<tr>
<td>Email notification</td>
<td>Description</td>
<td>Triggering event</td>
<td>Business Rule Controlling Event</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------</td>
<td>----------------------------------</td>
</tr>
</tbody>
</table>
| Certificate Expiring                      | Type: EMAIL  
Notification that the X.509 certificate is expiring in N days.       | certificate.expiring | certificate events               |
| Change approved                            | Type: EMAIL  
A change request has been approved.                                     | change.approved   | Change events and task events    |
| Change assigned to me                      | Type: EMAIL  
A change request has been assigned to you.                                 | change.assigned   | Change events                    |
| Change assigned to my group                | Type: EMAIL  
A change request has been assigned to your group.                           | change.assigned.to.group | Change events                   |
| Change commented (to assignee)            | Type: EMAIL  
A comment has been added to a change request. The person assigned to the change request receives an email notification. | change.commented  | Change events                    |
| Change commented (unassigned)             | Type: EMAIL  
A comment has been added to a change request. The assignment group assigned to the change request receives an email notification. | change.commented  | Change events                    |
| Change Notification                        | Type: EMAIL  
Notification of a change in the fields label in a form.                   | label.notify      |                                  |
| Change rejected                            | Type: EMAIL  
A change request has been rejected.                                        | change.rejected   | Change events and task events    |
| Change Task worknoted (unassigned)        | Type: EMAIL  
A work note has been added to a change task. The assignment group assigned to the change task receives an email notification. | change_task.worknoted | Change task events               |
<table>
<thead>
<tr>
<th>Email notification</th>
<th>Description</th>
<th>Triggering event</th>
<th>Business Rule Controlling Event</th>
</tr>
</thead>
</table>
| Change Task worknoted (to assignee)| Type: EMAIL  
A work note has been added to a change task. The person assigned to the change task receives an email notification. | change_task.worknoted | Change task events               |
| Change Task assigned to my group    | Type: EMAIL  
A change task has been assigned to your group. | change_task.assigned.to.mygroup | Change task events               |
| Change Task assigned to me          | Type: EMAIL  
A change task has been assigned to you. | change_task.assigned | Change task events               |
| Change worknoted (to assignee)     | Type: EMAIL  
A work note has been added to a change request. The person assigned to the change request receives an email notification. | change.worknoted | Change events                    |
| Change worknoted (unassigned)      | Type: EMAIL  
A work note has been added to a change request. The assignment group assigned to the change request receives an email notification. | change.worknoted | Change events                    |
| Email assigned to                   | Type: EMAIL  
An incident has been assigned to you (the recipient of the email). | incident.assigned | incident.events                  |
<table>
<thead>
<tr>
<th>Email notification</th>
<th>Description</th>
<th>Triggering event</th>
<th>Business Rule Controlling Event</th>
</tr>
</thead>
</table>
| Email assigned to (sc_task)       | Type: EMAIL  
A task has been assigned to you (the recipient of the email). | sc_task.assigned.to.user    | sc_task_events                  |
| Email assigned To Group           | Type: EMAIL  
An incident has been assigned to an assignment group of which you are a member (the recipient of the email). | incident.assigned.to.group  | incident_events                 |
| Email assigned to group (sc_task) | Type: EMAIL  
A Service Catalog task has been assigned to an assignment group of which you are a member (the recipient of the email). | sc_task.assigned.to.group    | sc_task_events                  |
| Incident Closed                   | Type: EMAIL  
An incident opened by you (the recipient of the email), has been closed. | incident.updated            | incident_events                 |
| Incident Commented                | Type: EMAIL  
An incident opened by you (the recipient of the email) has had comments added.  
This notification uses a template for an employee self-service (ESS) user. | incident-commented          | incident_events                 |
<table>
<thead>
<tr>
<th>Email notification</th>
<th>Description</th>
<th>Triggering event</th>
<th>Business Rule Controlling Event</th>
</tr>
</thead>
</table>
| Incident Commented                       | Type: EMAIL  
An incident assigned to you (the recipient of the email) has had comments added. This notification uses a template for an ITIL user. | incident.commented | incident events                 |
| Incident Opened                          | Type: EMAIL  
An incident has been opened for you (the recipient of the email) by someone else. This notification uses a template for an employee self-service (ESS) user. | incident.inserted | incident events                 |
| Incident Opened & Unassigned             | Type: EMAIL  
An incident has been opened and is unassigned. This notification uses a template for an ITIL user.                                      | incident.inserted | incident events                 |
| Incident Resolved                        | Type: EMAIL  
An incident opened by you has been resolved, and feedback is required to determine if the incident should be closed.          | incident.updated  | incident events                 |
| Knowledge Closed Created                 | Type: EMAIL  
A contributor’s submission to the Knowledge Base was accepted and an article was created.                                           | kb.submission.closed_created |                             |
| Knowledge Closed Duplicate               | Type: EMAIL  
A contributor’s submission to the Knowledge Base was determined to be a duplicate, and no article was created.            | kb.submission.closed_duplicate |                             |
| Knowledge Closed Invalid                 | Type: EMAIL  
A contributor’s submission to the Knowledge Base was determined to be invalid ( unusable).                                        | kb.submission.closed_invalid |                             |
<table>
<thead>
<tr>
<th>Email notification</th>
<th>Description</th>
<th>Triggering event</th>
<th>Business Rule Controlling Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify Change Calendar</td>
<td>Type: Meeting Invitation</td>
<td>change.calendar.notify</td>
<td>change events</td>
</tr>
<tr>
<td></td>
<td>Notifies the recipients of the schedule for a change request and exports the schedule to the Microsoft Outlook calendar. The email is in the format of iCalendar formatted email.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notify Change Calendar Remove</td>
<td>Type: Meeting Invitation</td>
<td>change.calendar.notify.re</td>
<td>change events</td>
</tr>
<tr>
<td></td>
<td>Notifies the recipients that a scheduled change has been closed or assigned to someone else and removes the entry from the Microsoft Outlook calendar. The email is in the format of iCalendar formatted email.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Problem Task assigned to me</td>
<td>Type: EMAIL</td>
<td>problem_task.assigned</td>
<td>Problem task events</td>
</tr>
<tr>
<td></td>
<td>A problem task has been assigned to you.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Problem Task assigned to my group</td>
<td>Type: EMAIL</td>
<td>problem_task.assigned.to</td>
<td>Problem task events</td>
</tr>
<tr>
<td></td>
<td>A problem task has been assigned to your group.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Problem Task worknoted (to assignee)</td>
<td>Type: EMAIL</td>
<td>problem_task.worknoted</td>
<td>Problem task events</td>
</tr>
<tr>
<td></td>
<td>A work note has been added to a problem task. The person assigned to the problem task receives an email notification.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Problem Task worknoted (unassigned)</td>
<td>Type: EMAIL</td>
<td>problem_task.worknoted</td>
<td>Problem task events</td>
</tr>
<tr>
<td></td>
<td>A work note has been added to a problem task. The assignment group assigned to the problem task receives an email notification.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Problem worknoted (to assignee)</td>
<td>Type: EMAIL</td>
<td>problem.worknoted</td>
<td>Problem events</td>
</tr>
<tr>
<td></td>
<td>A work note has been added to a problem. The person assigned to the problem receives an email notification.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email notification (unassigned)</td>
<td>Description</td>
<td>Triggering event</td>
<td>Business Rule Controlling Event</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------</td>
<td>------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Problem worknoted</td>
<td>Type: EMAIL</td>
<td>problem.worknoted</td>
<td>Problem events</td>
</tr>
<tr>
<td></td>
<td>A work note has been added to a problem. The assignment group assigned to the problem receives an email notification.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reminder Insert</td>
<td>Type: Meeting Invitation</td>
<td>reminder.notify</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Creates a calendar reminder regarding an open task. The email is in the format of iCalendar formatted email.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reminder Insert</td>
<td>Type: Meeting Invitation</td>
<td>reminder.notify.delete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A task has been closed or deleted. This notification removes the task reminder from Outlook. The email is in the format of iCalendar formatted email.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reminder Insert Email</td>
<td>Type: EMAIL</td>
<td>reminder.notify.email</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sends the recipient a reminder email about a specific task.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Request Approved</td>
<td>Type: EMAIL</td>
<td>sc_request.approved</td>
<td>sc_request events</td>
</tr>
<tr>
<td></td>
<td>A Service Catalog request, opened by the recipient, has been approved.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Request Assigned</td>
<td>Type: EMAIL</td>
<td>sc_request.assigned</td>
<td>sc_request events</td>
</tr>
<tr>
<td></td>
<td>A Service Catalog request has been assigned to the recipient.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Request Completed</td>
<td>Type: EMAIL</td>
<td>sc_request.updated</td>
<td>sc_request events</td>
</tr>
<tr>
<td></td>
<td>A Service Catalog request, opened by the recipient, has been completed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Request Item Assigned</td>
<td>Type: EMAIL</td>
<td>sc_req_item.assigned</td>
<td>sc_request events</td>
</tr>
<tr>
<td></td>
<td>An item requested from the Service Catalog has been assigned to you.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email notification</td>
<td>Description</td>
<td>Triggering event</td>
<td>Business Rule Controlling Event</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Request Item Delivery</td>
<td>Type: EMAIL</td>
<td>sc_req_item.delivery</td>
<td>sc_request events</td>
</tr>
<tr>
<td></td>
<td>An item requested from the Service Catalog by the recipient is being delivered.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Request Opened on Behalf</td>
<td>Type: EMAIL</td>
<td>sc_request.requested_for</td>
<td>sc_request events</td>
</tr>
<tr>
<td></td>
<td>A Service Catalog request has been opened on behalf of the recipient.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reset Password</td>
<td>Type: EMAIL</td>
<td>reset.password</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The recipient’s password has been reset as requested.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scheduled Import Completed</td>
<td>Type: EMAIL</td>
<td>scheduled_import_set.completed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A scheduled import set has completed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Upgraded</td>
<td>Type: EMAIL</td>
<td>system.upgraded</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The recipient’s system has been upgraded.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task approved</td>
<td>Type: EMAIL</td>
<td>task.approved</td>
<td>Change events and task events</td>
</tr>
<tr>
<td></td>
<td>An ITIL task has been approved.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Text Index Completed</td>
<td>Type: EMAIL</td>
<td>text_index.complete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A scheduled system index has completed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unscheduled Change</td>
<td>Type: EMAIL</td>
<td>cmdb.unscheduled.change</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A named configuration item has changed, and no active change request exists.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Notification example:** notify task assignees
Notify users who are assigned a Task (task) record.

Role required: admin

Set up your email as a test email address. Navigate to **System Properties > Email Properties**, and then enter your email address under **Send all email to this test email address**.

1. Navigate to **System Notification > Email > Notifications**, and then click **New**.
2. On the form, enter the following values:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Task Assigned</td>
</tr>
</tbody>
</table>
### ServiceNow Jakarta Now Platform Capabilities

#### Field | Value
---|---
Table | Task (task)
Active | Selected
Category | Uncategorized
Send when | Record inserted or updated
Inserted | Selected
Updated | Selected
Conditions | (Assigned to)(changes)
Users/Groups in fields | Assigned to
Subject | Task Assigned

3. In the **Message HTML** field, add a message to send to whomever the task is assigned to.
4. From the form context menu, click **Save**.
5. To see a mock version of the system email that you created, click **Preview Notification** on the notification form.
6. Test the notification sends to a task assignee.
   a) Assign some task records.
   b) Check your email for assignment notifications.

**Notification example:** notify an assignment group of updates to Priority 1 Incidents

Notify users by email when there are updates to high priority incidents.

Role required: admin

Send emails to an assignment group whenever there are updates to an incident in which the **Priority** is **1 - Critical**. Include information that is of interest to the recipients, such as the incident number, category, assignees, and any comments that were added to the incident.

1. Navigate to **System Notification > Email > Notifications**, and then click **New**.
2. On the email notification form, enter the following values:

#### Field | Value
---|---
Name | Priority 1 Incident Updated
Table | Incident (incident)
Active | Selected
Category | Incident Alert
Send when | Record inserted or updated
Inserted | Selected
Updated | Selected
Conditions | (Priority) (is) (1 - Critical) AND (Updated) (changes)
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users/Groups in fields</td>
<td>Assignment group</td>
</tr>
<tr>
<td>Subject</td>
<td>Priority ${priority} Incident updated</td>
</tr>
</tbody>
</table>

**Note:** In this notification, the variable ${priority} returns the value 1 - Critical.

3. In the **Message HTML** field, enter the following message and script:

```html
Short Description: ${short_description}  
Click here to view incident: ${URI}  
Incident number: ${number}  
Category: ${category}  
Assigned to: ${assigned_to}  
Assignment group: ${assignment_group}  
<br/>
Comments:  
${comments}
```

4. From the form context menu, click **Save**.

5. Preview the email notification to ensure it includes all the needed information.
   a) On the notifications form, click **Preview Notification**.
   b) Note that the email includes the following information:
      - Short description
      - A link to the incident record
      - Incident number
      - Category
      - The name of the user to whom the incident is assigned
      - The group assigned to the incident
      - Comments from the incident record

6. Test that the email notification sends to an assignment group when its Priority 1 Incident is updated.
   a) **Create a user** who has an email address that you can monitor, and then **create a group** that includes the user that you created.
   b) Navigate to **Incident > Open**, and then open an incident in which the Priority is 1 - Critical.
   c) In the **Assignment group** field, enter the group that you created.
   d) From the form context menu, click **Save**.
   e) Add comments to the form to update the incident, and then click **Update**.
   f) Check the email account of the user member in the assignment group.

**Email templates**

Email templates enable administrators to create reusable content for the subject line and message body of email notifications.
Templates deliver consistent information on specific system activities and improve the efficiency of creating multiple email notifications for similar actions. If necessary, you can make minor changes on the fly to an email that uses a template by overriding the subject line and message body content in the notification form. A common practice is to define the message body in a template and create new subject lines for different types of recipients. There is no limit to the number of templates that you can create.

Email templates are created in rich HTML format, and administrators have the option of converting existing email templates to rich HTML (starting with the Eureka release). This format provides several advantages, including:

- Raw HTML content is converted into a WYSIWYG format.
- The content can be edited in a feature-rich HTML editor.
- Mail scripts are condensed into a single, easy-to-read line that can be reused in multiple email notifications.
- To prevent broken links, images linked using URLs relative to a particular instance are converted to absolute links.

Create an email template
You can create an email template with rich HTML formatting, rather than plain text.

Role required: admin

1. Navigate to **System Policy > Email > Templates**.
2. Click **New**.
3. Fill in the form fields (see table).
Email Template form with the HTML editor

Subject: \$\{sys_class_name\} \$\{number\} has been \$\{approval\}

Message HTML:

Short Description: \$\{short_description\}
Click here to view \$\{(sys_class_name): \$\{URI: REF\}

Priority: \$\{priority\}
Category: \$\{approval.category\}
Description: \$\{description\}

div

Message text:

SMS alternate:

Select variables:

Fields

Submit
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique name for the template. For example, change.update.risk.</td>
</tr>
<tr>
<td>Application</td>
<td>The type of scoped application.</td>
</tr>
<tr>
<td>Email layout</td>
<td>If the message body for the template is to be formatted using a predefined email layout, select the layout.</td>
</tr>
<tr>
<td>Table</td>
<td>Select the name of the table involved. For example, Change Request [change_request].</td>
</tr>
</tbody>
</table>
| Subject             | Enter a subject line that explains the purpose of the email. Select the appropriate variables for the subject line from the fields available on the selected table. Place the cursor where you want the variable to appear, and click the field name in the Select variables column. For example:  

```plaintext
${sys_class_name} ${number} with ${risk} risk has been assigned to you.
```

| Message HTML        | Enter the content of the email template message. You can use the HTML editor toolbar to format the HTML, and you can include variables from the Select variables column. Variables map to column names available from the notification table, its parent tables, and reference tables. Use variables to include values from a record in the table such as an incident short description or comments and work notes.  

**Notes:**  
- When a template is applied to a notification, the contents of this field are used when you select HTML and plain text or HTML in the Content Type field in the Email Notification form.  
- You cannot use HTML code to control the appearance of the contents in the $(comments) variable.  
- If you want to include a link to the record that triggered the notification, see Enable links to records.  

| Message Text        | Enter the notification message to send in plain text.  

**Note:** When a template is applied to a notification, the contents of this field are used when you select HTML and plain text or Text in the Content Type field in the Email Notification form.  

© 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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS alternate</td>
<td>Create a different message to be delivered to an SMS device. Enter a brief message, showing the most important information only. If this message field is blank, the contents of the Message Text field are used for the SMS message. <strong>Note:</strong> The message in this field is used when the message is sent to a device configured as SMS.</td>
</tr>
</tbody>
</table>

**Apply a template to an email notification**
After you create an email template, you can apply it to a notification.

Role required: admin
1. Navigate to System Notification > Email > Notifications.
2. Open the email notification record that should use the template.
3. Navigate to the What it will contain section.
4. From the Email template field, select the appropriate template.
5. Click Update.

**Convert an email template to rich HTML**
If you have an email template created prior to the Eureka release, you can convert it to rich HTML.

Role required: admin
1. Navigate to System Policy > Email > Templates.
2. Open the email template you want to convert.
Email Template
notify.change

Name
notify.change

Email layout
Unsubscribe and Preferences

Subject
${TABLE_NAME} ${DISPLAY_VALUE}

Message
Click here to view ${TABLE_NAME}:

SMS alternate
3. Click **Switch to Rich HTML Editor**.

When content is converted, these changes are made to the content:

- **HTML Editor**: Any raw HTML in the **Message** field is rendered as WYSIWYG text in the **Message HTML** field. The content can be edited in a feature-rich HTML editor.

- **Simplified Mail Scripts**: Any mail scripts in the body are automatically saved to the **Email Script (sys_script_email)** table and are replaced in the notification body with an embedded script tag. This makes the template body easier to read and makes it easier to reuse scripts in multiple email templates.
<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>notify.change</th>
<th><strong>Table</strong></th>
<th>Incident [incident]</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Email layout</strong></td>
<td>Unsubscribe and Preferences</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Subject</strong></td>
<td>${TABLE_NAME} ${DISPLAY_VALUE} Change Notification</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Message HTML**

```
Click here to view ${TABLE_NAME}: ${URL}
```
4. Modify the message text, as needed, using the WYSIWYG editor or by editing the underlying HTML.

**Note:** The letter "P" at the bottom of the screen shows the location of your cursor within the Message field. In this case, the cursor is in a line containing an <HTML> tag.

**Note:** Email templates that are already formatted with rich HTML do not show the Switch to Rich HTML Editor button.

Whether you are working with templates converted from earlier versions or creating new templates in the rich HTML format, it is a good practice to write mail scripts in System Notification > Email > Notification Email Scripts. When the scripts are completed, a $(mail_script:script name) embedded script tag should be added to the email template body. This makes it easy to use the same scripts in multiple email templates. All that needs to be copied and pasted from one template to the next is the embedded script tag.

If you manually enter a mail script in the body of a new or converted email notification or template, and then attempt to save the record, a message asks whether the mail script should be converted. Unconverted mail scripts often fail to run from inside the HTML editor. If you select Yes, the script is added to the Email Script (sys_script_email) table and is automatically replaced in the body with an embedded script tag.

You can view the mail scripts in their original form by opening the email template and clicking the Show Notification Scripts related link.

**Construct an email message with a template**

Email templates provide a list of the fields from database tables that are available for constructing an email message.

An email template can include a mailto automatic response link, which enables the email recipient to simply choose a link that sends a preformatted response back to the instance. An example is the email template used for notification that an approval is required. The following example shows the base email:
The selection list on the right shows the available fields from the `sysapproval_approver` table. All email templates used are based on an event that was created. Generally events are created based on business rules that execute when a database record is modified in some way. The database record being modified when the event is created is the record that is available for generating an email request.

In this case, a change request approval was requested, which results in an update to the `sysapproval_approval` table. The "approval events" business rule was executed, which created the "approval.inserted" event. The "Approval Request" email event is defined to process the approval.inserted event, and this email event is defined to use the following `change.itil.approve.role` email template. Notice that this template has two mailto: items specified. One for "mailto.approval" and one for "mailto.rejection." This email template builds an automatic response that lets the email receiver simply click a link in the email to either approve or reject the change request.

Here is what the `change.itil.approve.role` template looks like using the rich HTML editor:
Email Template
change.itil.approve.role

Name: change.itil.approve.role
Application: Global

Email layout: Unsubscribe and Preferences
Table: Approval [sysapproval.approver]

Subject: ${sysapproval.sys_class_name} ${sysapproval} Approval Request

Message HTML:

Short Description: ${sysapproval.short_description}
Priority: ${sysapproval.priority}
Category: ${sysapproval.category}

${mail_script:change_request_summary}
Comments:
${sysapproval.description}

${mailto:mailto.approval}

${mailto:mailto.rejection}

Click here to view Approval Request: ${URI}
Click here to view ${sysapproval.sys_class_name}: ${sysapproval.URI}

div
Notice the `change.itil.approve.role` template also uses a predefined email layout (Unsubscribe and Preferences), which provides links for the recipient to unsubscribe from approval notifications and set notification preferences.

And here is the `mailto.approval` template:

```
Click here to approve ${sysapproval}:
```

**Note:** If you put text on the lines following the **Click here to approve ${sysapproval}** line, this text forms the actual body of the email.

The combination of templates used would generate an email similar to the following example:
Template generated email message

Notice that the email recipient can use the following links in the mail:
- A link to view all the details of the change request
- A link to view the approval record
- A link that generates an automatic email response to approve the change
- A link that generates an automatic email response to reject the change
- A link to unsubscribe from approval notifications and another link to set notification preferences

Add blank lines in an email template
You can easily add blank lines in an email template using HTML tags.
Judicious use of these HTML tags can make your email easier to read.
- You can use `<br/>` to insert a line break
- You can wrap paragraphs in `<p>` . . . `</p>` tags to format your email nicely.

Calendar integration
With email notifications, you can use import export maps to leverage information about records and integrate with Outlook or another calendar.

For example, an email notification can create a calendar event based on the planned start and end dates of a change request. To enable integration with a calendar, the following iCalendar variables are available to be added to an email template message and reference the email template from the notification. The variables must be added to the Message Text field.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(dtstart)</td>
<td>Start Date</td>
</tr>
<tr>
<td>$(dtend)</td>
<td>End Date</td>
</tr>
<tr>
<td>$(location)</td>
<td>Location</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>${alarm_time}</td>
<td>Alert or reminder time</td>
</tr>
</tbody>
</table>

The instance computes the value of iCalendar variables using import and export maps for the following tables:

- change_request
- reminder
- itil_appointment
- incident

Import export maps

Each import export map can specify a different set of iCalendar fields. For example, the icalendar.change_request import export map only maps two iCalendar fields.
iCalendar change request mappings

The instance uses the External Name value as the variable name in the email template. For example, the icalendar.change_request import export map defines the dtstart and dtend variables.

<table>
<thead>
<tr>
<th>External name</th>
<th>Associated variable name</th>
<th>Table</th>
<th>Field mapped</th>
<th>Field label</th>
</tr>
</thead>
<tbody>
<tr>
<td>dtstart</td>
<td>${dtstart}</td>
<td>change_request</td>
<td>start_date</td>
<td>Planned start date</td>
</tr>
<tr>
<td>dtend</td>
<td>${dtend}</td>
<td>change_request</td>
<td>end_date</td>
<td>Planned end date</td>
</tr>
</tbody>
</table>

Map date fields to iCalendar variables

You can specify what fields provide the date information in calendar invitation notifications by changing the field mappings of the dtstart and dtend variables in the import export map for the iCalendar invitation.

Role required: admin

1. In the navigation filter, enter sys_impex_map.list.
2. Open the icalendar.change_request map or the map you want to edit.
3. In the Field Maps related list, click either the end_date or start_date mapped field to change the mapping for dtstart or dtend, as needed.
4. Change the Database field to the field you want to use to set the start date or end date.
5. Click Update.

Create iCalendar invitations for custom tables
To generate iCalendar invitations that use field values from custom tables, create an import export map that computes the values of the iCalendar fields.

Role required: admin

1. Create the custom table and fields using the **Date/Time** field type for the fields that map to the `${dtstart}` and `${dtend}` variables.
2. In the navigation filter, enter `sys_impex_map.list`.
3. Click **New**.
4. Set the following fields:
   - **Name**: Use the following naming convention: `icalendar.<table name>`. For example, `icalendar.u_my_custom_table`.
   - **Table**: Select the custom table you created.
   - **Type**: Select `icalendar`.
5. Right-click the form header and select **Save**.
6. In the Field Maps related list, click **New**.
7. In the Mapping Entry Wizard, select **Mapping to a Database Field**.
8. Create field mappings for `dtstart` and `dtend`. These variables are required.
   
   For example, map the **External Name** `dtstart` to the `u_meeting_start_time` field in `u_my_custom_table`.
9. Click **Submit**.
10. Create field mappings for any other iCalendar fields as necessary.
11. Click **Update**.

   Here are sample field mappings between iCalendar variables and custom fields in a custom table, `u_my_custom_table`:

<table>
<thead>
<tr>
<th>External name</th>
<th>Database field</th>
<th>Type</th>
<th>Map</th>
</tr>
</thead>
<tbody>
<tr>
<td>dtstart</td>
<td>u_meeting_start_time</td>
<td>field</td>
<td>icalendar.u_my_custom_table</td>
</tr>
<tr>
<td>dtend</td>
<td>u_meeting_end_time</td>
<td>field</td>
<td>icalendar.u_my_custom_table</td>
</tr>
<tr>
<td>description</td>
<td>u_meeting_description</td>
<td>field</td>
<td>icalendar.u_my_custom_table</td>
</tr>
</tbody>
</table>

12. Create an email template that defines what to include in the iCalendar invitation.
   a) Set the **Table** field to the custom table you created.
   b) In the **Message** text field, use the following format to define the iCalendar invitation.

   ```
   BEGIN:VCALENDAR
   PRODID:--//Service-now.com//Outlook 11.0 MIMEDIR//EN
   VERSION:2.0
   METHOD:REQUEST
   BEGIN:VEVENT
   ATTENDEE;ROLE=REQ-PARTICIPANT;RSVP=TRUE;MAILTO:${to}
   DTSTART:${dtstart}
   DTEND:${dtend}
   UID:${sys_id}
   DTSTAMP:${dtstamp}
   DESCRIPTION:${description}
   SUMMARY:${u_meeting_summary}
   END:VEVENT
   END:VCALENDAR
   ```
Note: Mail script is not allowed or processed in meeting invitation email templates.

iCalendar invitation template details

<table>
<thead>
<tr>
<th>iCalendar template line</th>
<th>Required?</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>BEGIN:VCALENDAR</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>PRODID:-//Service-now.com//Outlook 11.0 MIMEDIR//EN</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>VERSION:2.0</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>METHOD:REQUEST</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>BEGIN:VEVENT</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>ATTENDEE;ROLE=REQ-PARTICIPANT;RSVP=TRUE:MAILTO: ${to}</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>DTSTART:${dtstart}</td>
<td>Yes</td>
<td>You must use the import export map to map dtstart to a start time field on the custom table.</td>
</tr>
<tr>
<td>DTEND:${dtend}</td>
<td>Yes</td>
<td>You must use the import export map to map dtend to an end time field on the custom table.</td>
</tr>
<tr>
<td>UID:${sys_id}</td>
<td>Yes</td>
<td>You must provide the name of a field that uniquely identifies the record, such as the sys_id or the record number field.</td>
</tr>
<tr>
<td>DTSTAMP:${dtstamp}</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>DESCRIPTION:${description}</td>
<td>No</td>
<td>To include a multiple line description, you must use the import export map to map description to a text field on the custom table. The field mapping ensures that the system encodes line breaks correctly for the iCalendar file format.</td>
</tr>
<tr>
<td>SUMMARY: ${u_meeting_summary}</td>
<td>No</td>
<td>To include a summary from a text field on the custom table, provide the name of the field, such as u_meeting_summary. The summary field value must not contain line breaks. You do not need to create a field mapping.</td>
</tr>
<tr>
<td>END:VEVENT</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>END:VCALENDAR</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

13. Create an email notification to trigger the iCalendar invitation and ensure the following fields are set accordingly:
   - **Table**: Select the custom table.
   - **Type**: Select **Meeting Invitation**.
• **Content type**: Select *Plain text* only.
• **Email template**: Select the template you created.

**Email layouts**

Create reusable content for the message body of email templates.
Administrators can use email layouts to:

- Ensure all email notifications have a consistent layout such as always displaying a header, body, and footer.
- Display static content on all email notifications such as a company logo or a background.
- Declare inline styles available for use in the message body of an email template such as setting a text font, size, and color.
- Provide users with links to common response actions such as unsubscribe from a notification or manage notification preferences.

**Note:** To display dynamic content such as mail scripts, use email templates. For more information, see Create an email template.

Email layouts insert HTML elements into the message body of email templates. Any style elements you define in the email layout are available to the email template. Email layouts support style sheets in these formats.

- Internal style sheets defined within a `<style>` element.
- Inline styles within a `style` attribute.

By default, the system includes several sample layouts administrators can use to create their own layouts. Administrators can create email layouts using an inline HTML editor or manually entering HTML code. The system stores email layout records in the Email Layout (sys_email_layout) table.

*Create an email layout*

Create an email layout to specify the HTML content you want to appear in the body of one or more email templates.

- Role required: admin
- Record required: email template record

1. Navigate to **System Policy > Email > Layouts**. The system displays the list of existing email layouts.
2. Click **New**. The system displays a blank email layout form.
3. Fill in the form.

**Email layout fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify a unique name for the record.</td>
</tr>
<tr>
<td>Application</td>
<td>Lists the parent application to which this record belongs.</td>
</tr>
<tr>
<td>Description</td>
<td>Specify an optional description of the layout.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Select whether to display the Advanced Layout field.</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 Layout

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the inline editor to add HTML elements. The system displays HTML from this field in the body of any email template that uses the layout. Include notification variables to show content from the related record. For more information notification variables see Notification variables.</td>
</tr>
</tbody>
</table>

**Note:** The editor automatically formats any HTML code you enter from the Source code view.

### Advanced Layout

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use this field to manually enter HTML code. The system displays HTML from this field in the body of any email template that uses the layout.</td>
</tr>
</tbody>
</table>

**Note:** To enter text in this field, select Click here to disable syntax highlighting and script formatting.

4. Click **Submit**. The system creates the email layout record.

5. Navigate to **System Policy > Email > Templates**. The system displays the list of existing email templates.

6. Select the email template which you want to use an email layout. The system displays the email template record.

7. In **Email layout**, select the email layout you want to use to format the body of email messages.

8. Click **Update**. The email template uses the selected email layout to format the body of email messages.

### Inbound email actions

Inbound email actions enable you to define the actions an instance takes when receiving email.

Inbound email actions are similar to business rules; both use conditions and scripts that take action on a target table. An inbound email action checks the email for a watermark that associates it with a task and checks for other conditions. If the conditions are met, the inbound email action takes the action that you configure. The system can take two types of actions:

- Record action: setting a value for a field in the target table.
- Email reply: sending an email back to the source that triggered the action.

By default, if an email has no identifiable watermark, an inbound email action attempts to create an incident from the message. If the email has a watermark of an existing incident, an inbound email action updates the existing incident according to the action's script.

The following video explains the actions that the instance can take in response to messages from users and shows how to create or modify inbound email actions.
Inbound email action types

The system categorizes all incoming email into one of three types: forward, reply, or new. The system uses these criteria to determine the inbound action type of incoming email.

Determining the inbound action type of incoming email
# Inbound action type criteria

<table>
<thead>
<tr>
<th>Order</th>
<th>Type</th>
<th>Criteria</th>
</tr>
</thead>
</table>
| 1     | Forward | The system classifies an email as a forward only when it meets all of these criteria:  
|       |        | · The *subject line* contains a recognized forward prefix such as **FW**:.
|       |        | · The *email body* contains a recognized forward string such as **From**:.
|       |        | The system classifies any email that meets these criteria as a forward even if the message also contains a watermark or record number that would otherwise classify it as a reply. |
| 2     | Reply  | The system classifies an email as a reply if it fails to match it to the forward inbound action type and it meets any one of these criteria:  
|       |        | · The subject line or email body contains a recognized watermark such as **Ref:MSG0000008**.  
|       |        | · There is no watermark and the **Reply-To header** contains a recognized message ID.
|       |        | · There is no watermark and the subject line contains a recognized reply prefix such as **RE:** and a recognized record number such as **INC0005574** |
| 3     | New    | The system classifies an email as new if it fails to match it to the forward and reply inbound action types. |

## Attachments

If an inbound email contains one or more email attachments, the inbound email action adds the attachments to the first record the action produces.

## Character encoding

- If the email encoding is ASCII-7 or UTF-8, inbound email actions preserve the character encoding in any associated task records they produce.
- If the email encoding is ISO-8859-1, the inbound email action attempts to convert the email to Windows 1252.
- Inbound email actions convert any other encodings (for example, Mac OS Roman) to plain text, which may or may not be readable.

See the *Email logs* for examples of what you might see if a notification or inbound email action is not processed.

**Note:** The state of all incoming emails that have been run against inbound email actions, even if there is no matching action, is changed to **Processed**.
Domain separation

The system ignores the domain that the inbound email action record is in when it creates a record based on the inbound email action. Keep inbound actions in the global domain. For example, if your inbound email action creates an incident, the system creates the incident in the same domain as the user in the **Caller** field. If that user is not in the User (sys_user) table, the incident is in the global domain.

**Inbound email processing**

The system determines which inbound actions to run by comparing the inbound email type and inbound action conditions to the incoming email message. Certain properties are available to set the reply and forwarding prefixes in the email subject lines that your instance recognizes when processing inbound emails.

The system follows this processing flow to determine whether to run an inbound action.
The system only runs an inbound action when:

- The incoming email type matches the inbound action **Type**.
- If present, the watermark or record number refers to a record in the **Target table**.
• The inbound action **Conditions** evaluates to true.

If any of these criteria are not met, the system skips the current inbound action and evaluates the next active inbound action. The system processes inbound actions from the lowest to highest **Order** value. If the inbound action has **Stop processing** enabled, then the system updates the **State** of the email record to **Processed** after running the inbound action **Script**.

The following video shows how an inbound action condition prevents an incident from being created.

**Prefixes recognized in email subject lines**

**Email reply prefixes**

When no watermark is present or the In-Reply-To email header is present, the instance recognizes email containing a prefix from the *glide.email.reply_subject_prefix* property as reply email. You can use this property to set non-standard reply prefixes in your email system.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>glide.email.reply_subject_prefix</strong></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 Properties (sys_properties) table</td>
</tr>
</tbody>
</table>

**Email forward prefixes**

Emails with certain prefixes trigger the forward type of inbound email action. The instance recognizes any email whose subject line contains a prefix from the *glide.email.forward_subject_prefix* property as forwarded email. Emails with these prefixes trigger inbound email actions of the type forward. Use this property to set non-standard forward prefixes in your email system or you want email forwards to behave like replies. If the value of the system property is empty, then the system reverts to using the values **fw:** and **fwd:**.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>glide.email.forward_subject_prefix</strong></td>
<td>Specifies the list of prefixes (comma-separated) in the subject line that identify a 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 Properties (sys_properties) table</td>
</tr>
</tbody>
</table>

**Email forwards as replies**
Properties are available to force inbound actions to process forwarded mail as replied mail. These properties control the subject prefix that the inbound actions use.

<table>
<thead>
<tr>
<th>Property</th>
<th>Value needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.email.reply_subject_prefix</td>
<td>re:, Re:, aw:, r:, fw:, Fwd:, FWD:</td>
</tr>
<tr>
<td>glide.email.forward_subject_prefix</td>
<td>(any text that is not a forward prefix)</td>
</tr>
</tbody>
</table>

These properties cause the Update Incident inbound action to process all forwarded and replied-to mail.

**Note:** The `glide.email.forward_subject_prefix` property must contain some text so that the forwarded email can be processed as a Reply. It can be any text except a forward prefix (that is, fw:, Fwd:, FWD:).

### Matching a sender email address to a user

The instance matches a sender's email address to an active user in the User (sys_user) table using inbound actions.

**Note:** The Email Automatic User Creation plugin must be active.

When processing an email, the instance sets the current user to the user whose email address matches `email.from`. Inbound actions can then reference that current user. For example, the base system inbound action Create Incident sets the `caller_id` of the incident to the value returned by `gs.getUserID()`.

If multiple users have the same email address, the instance first searches for an active user with the email address. The instance does not match inactive users.

**Note:** Each user record must have a unique email address so that the instance can reliably match the email to the correct user.

If a unique email address for each user is not possible, assign a shared email address to only one active user so that the instance always matches incoming email from that address to the active user.

### Matching watermarks in the Subject line or Body

The following examples illustrate how the instance matches randomized watermarks in an email subject line or body.

**Note:** For instances upgraded from a release before Jakarta, the system can recognize both randomized and non-randomized watermarks during a watermark transition period. For details, see the [Notifications upgrade information](#).
Matching record numbers in the Subject line or Body

The following examples illustrate how the instance matches record numbers in the subject line of an email to an existing record when no watermark is present.

Examples of matching record numbers in the Subject line

<table>
<thead>
<tr>
<th>Subject line contents</th>
<th>Matching results</th>
</tr>
</thead>
<tbody>
<tr>
<td>RE: Example INC0005574</td>
<td>The instance recognizes this subject line as a reply and recognizes the INC prefix as belonging to the Incident table. The instance searches the Incident table for an existing record INC0005574. If this incident exists, the email is associated with this incident. If this incident record does not exist, the instance uses the inbound action for new emails to create an incident and associates the new incident with the email.</td>
</tr>
<tr>
<td>RE: Example &quot;INC0005574&quot;</td>
<td>The instance recognizes this subject line as a reply but does not recognize the &quot;INC prefix as belonging to the Incident table because of the quotation mark. The same error occurs for any character other than a space before the record number. The instance instead uses the inbound action for new emails to create an incident and associates the new incident with the email.</td>
</tr>
<tr>
<td>Subject line contents</td>
<td>Matching results</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RE: &quot;Example INC0005574&quot;</td>
<td>The instance recognizes this subject line as a reply and recognizes the INC prefix as belonging to the Incident table. The instance searches the Incident table for an existing record INC0005574&quot;, which it cannot find because of the quotation mark. The same error occurs for any character other than a space at the end of the record number. The instance instead uses the inbound action for new emails to create an incident and associates the new incident with the email.</td>
</tr>
<tr>
<td>RE: Example INC0005574*</td>
<td></td>
</tr>
<tr>
<td>RE: CHG0008593 and INC000576</td>
<td>The instance recognizes this subject line as a reply and recognizes one, but not both, of the number prefixes. There is no way to predict which prefix the instance matches first. Whichever prefix it matches, it searches the corresponding table for a matching record. If the record exists, the email is associated with the table. If the record does not exist, the instance uses the inbound action for new emails to create an incident and associates the new incident with the email.</td>
</tr>
<tr>
<td>Note:</td>
<td>The instance does not support processing email with multiple numbers in the subject line because there is no way to predict which record the instance matches first. For this reason, do not include more than one $number variable in your notifications.</td>
</tr>
<tr>
<td>FW: Example INC0005574</td>
<td>The instance recognizes this subject line as a forward because of the FW: prefix. It uses the inbound action for forwarded emails to create an incident and associates the new incident with the email.</td>
</tr>
<tr>
<td>Example INC0005574</td>
<td>The instance recognizes this subject as a new email because it does not contain a matching reply or forward prefix. It uses the inbound action for new emails to create an incident and associates the new incident with the email.</td>
</tr>
</tbody>
</table>

Criteria for matching email to inbound actions

The system matches incoming email to the conditions of the active inbound actions.

The default inbound actions create or update task record under these conditions.
Default matching criteria

If you customize or deactivate the default inbound actions, the system checks the conditions of the active inbound actions. If the system cannot find an inbound action with matching conditions, it sets the state to **Processed**.
Custom matching criteria
### Inbound action type criteria

<table>
<thead>
<tr>
<th>Inbound email action type</th>
<th>Required matching criteria</th>
<th>Name of default action (Incident table)</th>
<th>Result of default action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forward</td>
<td>The email contains the following conditions:</td>
<td>Create Incident (Forwarded)</td>
<td>Create new record</td>
</tr>
<tr>
<td></td>
<td>1. A subject starting with a recognized forward prefix (even if a watermark or an In-Reply-To header is present).</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. From &lt;user email&gt; appears anywhere in the email body.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reply</td>
<td>The email contains one of the following conditions and the table specified in the email matches the table of the inbound action:</td>
<td>Update Incident (BP)</td>
<td>Update existing record</td>
</tr>
<tr>
<td></td>
<td>1. A valid watermark that matches an existing record.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. An In-Reply-To email header (when no watermark is present) that matches an existing record.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. A subject line starting with a recognized reply prefix (when neither a watermark nor an In-Reply-To header is present) and a valid record number that matches an existing record.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New</td>
<td>The email does not meet the conditions for either a reply or forward type inbound email action</td>
<td>Create Incident</td>
<td>Create new record</td>
</tr>
</tbody>
</table>

If more than one inbound action is available for a particular type, the instance uses the Table field to match the email to a particular table. If there is also more than one action for the inbound action's table, the instance uses the Order field to determine the order in which the actions run.
Create an inbound email action

You can create inbound email actions to define the actions that the system takes when an email is received.

Role required: admin

1. Navigate to System Policy > Email > Inbound Actions.
2. Click New.
3. Fill in the fields as described in the table.
Inbound Email Actions - Create Incident

Inbound email actions specify how ServiceNow creates or updates task records in a table when the instance receives an email. The inbound email action looks for a watermark in the email to associate it with a specific task. If the conditions specified in the inbound action are met, the script is run.

| Name          | Create Incident | Application | Global | | |
|---------------|-----------------|-------------|--------| | |
| Target table  | Incident [incident] | Active      |        | | |
| Action type   | Record Action   | Stop processing |      | | |

When to run Actions Description

- **Only emails of the selected Type will trigger this inbound action.**
- **Order determines when to run relative to other inbound actions. The inbound action with the lowest order runs first.**

| Type | Now | Required roles | | |
|------|-----|----------------| | |

- **Only emails from senders with the Required roles will trigger this inbound action.**
- **Only emails from this sender will trigger this inbound action.**

Order 100

All of the following conditions must be true, to trigger this inbound action.

| Conditions | Add Filter Condition | Add "OR" Clause | | |
|------------|----------------------|-----------------| | |
| -- choose field -- | -- oper -- | -- value -- | | |
**Note:** You might need to configure the form to see all fields.

## Inbound Email Actions form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>When to run</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Enter a descriptive name for this email action.</td>
</tr>
<tr>
<td><strong>Target table</strong></td>
<td>Select the table where the action will add or update records.</td>
</tr>
<tr>
<td><strong>Action type</strong></td>
<td>Select the type of action the instance takes.</td>
</tr>
<tr>
<td></td>
<td>Select Record Action to modify a record in the instance or select Reply Email to have the instance send an email back to the source of the inbound email.</td>
</tr>
<tr>
<td><strong>Active</strong></td>
<td>Select the check box to activate the inbound email action. Clear the check box to disable the action.</td>
</tr>
<tr>
<td><strong>Stop processing</strong></td>
<td>Select this check box to prevent the system from running additional inbound email actions after this action runs.</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Select the message type required to run the action. The action runs only if the inbound email is of the selected type. Available types are:</td>
</tr>
<tr>
<td></td>
<td>- New: An email that is not recognized as a reply or forward.</td>
</tr>
<tr>
<td></td>
<td>- Reply: An email with a watermark with an In-Reply-To email header, or whose subject line begins with a recognized reply prefix.</td>
</tr>
<tr>
<td></td>
<td>- Forward: An email whose subject line begins with a recognized forward prefix, even if the email also contains a watermark or In-Reply-To header.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>By default, inbound emails of the Forward type always generate new incidents regardless of the presence of a watermark. If this behavior does not match your business logic, you can change the recognized reply and forward prefixes to treat forwards like replies.</td>
</tr>
<tr>
<td><strong>Required roles</strong></td>
<td>Specify required roles the sender must have to trigger the inbound action.</td>
</tr>
<tr>
<td><strong>Order</strong></td>
<td>Enter a number that specifies when this inbound action runs relative to other inbound actions that use the same target table. The instance processes the action with the lowest order number first.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>From</td>
<td>Select the user required to run the action. If a user is selected, the action runs only when the email sender matches the user name. Leave this field blank to perform the action for all users.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If the selected user is later archived or deleted, the restriction is removed and anyone can trigger the inbound email action.</td>
</tr>
<tr>
<td>Condition</td>
<td>Specify the condition that must evaluate to true to trigger the inbound action. Build a condition with the choice lists or enter a statement that determines when the inbound email action runs. For example:</td>
</tr>
</tbody>
</table>
|             | ```                                             
|             |     email.subject. startsWith ( "chg:" )       
<p>|             | ```                                             |
| Actions     | Specify how information in the email is inserted into the record. For example, select <strong>(Created by)</strong> <em>(From email)</em>* <em>(Sender)</em>, so that when the request is inserted, you can see who it is for. This field appears if the action type is <strong>Record Action</strong>. |
| Reply email | Compose the email message to send to the source that triggered the inbound email action.                                                                                                                   |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Script</td>
<td>Enter the script the action runs. Typically, this script uses the validators script include and email variables. A template is provided:</td>
</tr>
<tr>
<td></td>
<td>(function runAction(/ <em>GlideRecord</em>/ current, / <em>GlideRecord</em>/ event, / <em>EmailWrapper</em>/ email, / <em>ScopedEmailLogger</em>/ logger) { // Implement email action here }) (current, event, email, logger);</td>
</tr>
<tr>
<td></td>
<td>These are the objects available:</td>
</tr>
<tr>
<td></td>
<td>• <strong>current</strong>: access the record referred to by the inbound email. For example, current.assigned_to accesses the person assigned to the task.</td>
</tr>
<tr>
<td></td>
<td>• <strong>event</strong>: access one of the parameters of the originating event. For example, event.parm1 accesses the first parameter of the event or event.parm2 for the second parameter. See Events for more information.</td>
</tr>
<tr>
<td></td>
<td>• <strong>email</strong>: access the inbound current email record. For example, email.subject accesses the content in the subject line of the email. See Accessing email object variables for more information.</td>
</tr>
<tr>
<td></td>
<td>• <strong>logger</strong>: add a message to the log file with the source set to email.&lt;Sys ID of incoming email&gt;. For example: logger.log (&quot;Some information&quot;)</td>
</tr>
</tbody>
</table>

| Description | Enter a detailed explanation of what this inbound email action does.                                                                          |

<table>
<thead>
<tr>
<th>Other fields</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Order</td>
<td>Enter a number to define the order in which this email action should be processed. Actions with lower numbers are processed first. For more information. This field is not installed by the Ordered Email Processing plugin.</td>
</tr>
</tbody>
</table>

**Accessing email object variables**

An inbound email action script contains the email object to access various pieces of an inbound email through variables. You can use the global variable sys_email with inbound email actions.
### Accessing email objects with variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>email.to</code></td>
<td>Contains a comma-separated list of email addresses in the To: and Cc: boxes.</td>
</tr>
<tr>
<td><code>email.direct</code></td>
<td>Contains a comma-separated list of email addresses in the To: box.</td>
</tr>
<tr>
<td><code>email.copied</code></td>
<td>Contains a comma-separated list of email addresses in the Cc: box.</td>
</tr>
<tr>
<td><code>email.body_text</code></td>
<td>Contains the body of the email as a plain text string.</td>
</tr>
<tr>
<td><code>email_body_html</code></td>
<td>Contains the body of the email as an HTML string.</td>
</tr>
<tr>
<td><code>email.from</code></td>
<td>Contains an email address that depends on the following conditions:</td>
</tr>
<tr>
<td></td>
<td>• If the address listed in the email Headers field matches an existing user's Email address, this variable contains the user's email address.</td>
</tr>
<tr>
<td></td>
<td>• If the address listed in the email Headers field does not match an existing user's Email address, this variable contains the address listed in the email Headers field.</td>
</tr>
<tr>
<td><code>email.from_sys_id</code></td>
<td>Contains the Sys ID of the user who sent the email to the instance.</td>
</tr>
<tr>
<td><code>email.origemail</code></td>
<td>Contains the address of the email sender as listed in the email Headers field.</td>
</tr>
<tr>
<td><code>email.subject</code></td>
<td>Contains the subject of the email as a plain text string.</td>
</tr>
<tr>
<td><code>email.recipients</code></td>
<td>Contains a comma-separated list of recipient addresses.</td>
</tr>
<tr>
<td><code>email.recipients_array</code></td>
<td>Contains the recipient addresses as an array.</td>
</tr>
<tr>
<td><code>email.content_type</code></td>
<td>Contains the MIME content type of the email (for example, text/plain; charset=&quot;us-ascii&quot; or text/html; charset=&quot;us-ascii&quot;).</td>
</tr>
<tr>
<td><code>email.headers</code></td>
<td>Contains details about the sender, route, and receiver as a plain text string in the format of the sending email client.</td>
</tr>
<tr>
<td><code>email.importance</code></td>
<td>Contains an indication from the sender about how important a message is. The value can be High, Low, or empty.</td>
</tr>
</tbody>
</table>

**Note:** The instance follows RFC 2822 (Internet Message Format), which requires multiple email addresses in a group to be separated by commas, not semicolons. The instance can set the values of the `email.to`, `email.direct`, and `email.copied` variables only if emails addressed to groups follow the expected RFC format.
**Inbound email.recipient variables**

The recipients variables (email.recipients, email.recipients-array) allow processing of inbound email based on the email recipients. For example, you can create a script to process email based on the array values:

```javascript
var rarray  = email.recipients_array ; for ( var i  = 0 ; i  < rarray.length ; i ++ ) { var recipient  = rarray [i ] ; // do something with it }
```

**The sys_email variable**

This variable lets you access the received sys_email record that triggered the inbound email action. It can be used to reference fields on the email record, such as uid, sys_id, content_type, and so on.

**Email user matching**

When the instance receives an email message, the system searches for an existing user record with the same email address as the sender.

<table>
<thead>
<tr>
<th>Value of email.from Variable</th>
<th>Matching User ID</th>
<th>Email Address</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:michael.tossi@company.com">michael.tossi@company.com</a></td>
<td><a href="mailto:michael.tossi@company.com">michael.tossi@company.com</a></td>
<td><a href="mailto:michael.tossi@company.com">michael.tossi@company.com</a></td>
<td>Michael Tossi</td>
</tr>
<tr>
<td>&quot;Michael Tossi&quot; <a href="mailto:michael.tossi@company.com">michael.tossi@company.com</a></td>
<td><a href="mailto:michael.tossi@company.com">michael.tossi@company.com</a></td>
<td><a href="mailto:michael.tossi@company.com">michael.tossi@company.com</a></td>
<td>Michael Tossi</td>
</tr>
<tr>
<td>&quot;Tossi, Michael&quot; <a href="mailto:michael.tossi@company.com">michael.tossi@company.com</a></td>
<td><a href="mailto:michael.tossi@company.com">michael.tossi@company.com</a></td>
<td><a href="mailto:michael.tossi@company.com">michael.tossi@company.com</a></td>
<td>Michael Tossi</td>
</tr>
<tr>
<td>&quot;Tossi&quot;<a href="mailto:mtossi@company.com">mtossi@company.com</a></td>
<td><a href="mailto:mtossi@company.com">mtossi@company.com</a></td>
<td><a href="mailto:mtossi@company.com">mtossi@company.com</a></td>
<td>Tossi</td>
</tr>
</tbody>
</table>

**Note:** This functionality requires that you activate the Email Automatic User Creation plugin.

Inbound Email Action scripts no longer support the gs.createUser() method. Use either the automatically-generated email variables or the gs.GetUserID() method instead.

**User impersonations and inbound actions**

When the instance receives an email, it can take a variety of actions by impersonating the sender.

If the sender of an incoming email matches an existing user, the instance impersonates the matching user to complete any inbound email actions. If the sender does not match an existing user, the instance impersonates the Guest user to complete any inbound email actions. If the impersonated user is locked out, the inbound email action fails.

**Note:** If inbound email comes from an untrusted domain, the instance impersonates the Guest user unless you explicitly prevent users from untrusted domains from triggering inbound actions. For more information, see the glide.user.trusted_domain system property in Inbound mail configuration.

Enable automatic user creation
An administrator can set an email property to automatically create users from incoming email. The administrator provides a list of trusted domains to prevent untrusted users from being automatically created.

Role required: admin

For example, you can prevent email from users outside your company domain from creating incidents. When an instance receives a message and there is no matching email address from the sender, the instance can create a user with the User ID (sys_user.user_name) set to the sender’s full email address.

Users in your instance must still have write and update access to the records that they create or update through inbound email actions.

Creating users from incoming email

<table>
<thead>
<tr>
<th>Value of email from Variable</th>
<th>User ID Created</th>
<th>Email Address</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:new.user@company.com">new.user@company.com</a></td>
<td><a href="mailto:new.user@company.com">new.user@company.com</a></td>
<td><a href="mailto:new.user@company.com">new.user@company.com</a></td>
<td>New User</td>
</tr>
<tr>
<td><em>New User</em><a href="mailto:new.user@company.com">new.user@company.com</a></td>
<td><a href="mailto:new.user@company.com">new.user@company.com</a></td>
<td><a href="mailto:new.user@company.com">new.user@company.com</a></td>
<td>New User</td>
</tr>
<tr>
<td><em>User, New</em><a href="mailto:new.user@company.com">new.user@company.com</a></td>
<td><a href="mailto:new.user@company.com">new.user@company.com</a></td>
<td><a href="mailto:new.user@company.com">new.user@company.com</a></td>
<td>New User</td>
</tr>
<tr>
<td><em>User</em><a href="mailto:nuser@company.com">nuser@company.com</a></td>
<td><a href="mailto:nuser@company.com">nuser@company.com</a></td>
<td><a href="mailto:nuser@company.com">nuser@company.com</a></td>
<td>User</td>
</tr>
</tbody>
</table>

1. Navigate to **System Properties > Email Properties**.
2. Select the check box for **Automatically create users for incoming email from trusted domains (glide.pop3readerjob.create_caller)**.

![Automatically create users for incoming emails from trusted domains](image)

3. Enter the list of trusted domains in **Trusted domains for creating users from incoming emails (glide.user.trusted_domain)**.

![Trusted domains for creating users from incoming emails](image)

**Note:** The glide.user.trusted_domain property only prevents user creation if the sender is not from a trusted domain. The system processes the inbound actions of the email as a guest user. If you want the system to ignore these email messages, use the email filters plugin, specifically the “ignore sender” setting. You can also prevent untrusted users from triggering inbound actions by locking out the guest user.

4. Click **Save**.
5. Optional: Complete the following steps to lock out the guest user.
a) Navigate to User Administration > Users and select the user guest.
b) Select the Locked out field to disable the guest account.

When the property glide.pop3readerjob.create_caller is set to false, the instance runs inbound actions from users who do not match an existing user by impersonating the guest user.

If the property glide.pop3readerjob.create_caller is set to true, but a user has a valid email address associated with a non-primary device, the instance creates a new user record for that email address if there is no matching email address in the Users (sys_user) table. The instance does not validate non-primary email addresses against the Notification Devices (cmn_notif_device) table.

The method the instance uses to create users can be upgraded to use the full email address by activating the Email Automatic User Creation plugin.

The plugin makes the following changes:

- Sets the property glide.email.create_userid_from_email to true.
- Increases the width of the User ID (sys_user.user_name) column to accommodate email addresses.

After activating the plugin, enable automatic user creation from email.

**Warning:** Review your existing user records to reconcile any that contain identical email addresses. If you activate the plugin prior to reconciling email addresses, your instance cannot distinguish between users with identical email addresses and randomly selects one of the users with the matching email address.

Allowing locked out users to process inbound email actions

A property is available to allow locked out users to trigger inbound actions. For example, enabling the property can allow locked out users to reset their password and send email to the instance asking for assistance.

**Property allowing locked out users to trigger inbound email actions**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>• System Properties (sys_properties) table</td>
</tr>
</tbody>
</table>

**Warning:** Enabling this property (glide.pop3.process_locked_out) also enables users from untrusted domains to trigger inbound actions.

Redirecting email to the instance POP3 account

You can have other mailboxes forward email to the instance's POP3 account.

By default, the POP Reader scheduled job checks for new email every two minutes. It connects to the mail server and account specified in email properties. The POP Reader downloads any email waiting on the mail server and creates email.read events. After the instance processes the events, the inbound email actions run.
The **POP Reader** shows the number of emails processed during the reader’s last run. The message shows the number of emails the reader processed or 0 processed if no emails were available. The reader resets the status each time it runs.

While it is not possible to specify more than one POP3 account for the instance, you can forward other mailboxes to the designated POP3 account. This script can be added to the Create Incident inbound email action to differentiate the content based on the original recipient, and then set an `assignment_group` value.

```java
if(email.direct.indexOf('facilities@anycorp.com')>-1)
current.assignment_group.setDisplayValue('Facilities Management');
```

**Setting field values from the email body**

Values in an inbound email can set field values in a task record.

Any name:value pair in an inbound email body gets parsed into a variable/value pair in the inbound email script. The name:value pair must be on its own line. Note that most email clients limit the number of characters allowed per line and may truncate excessively long name:value pairs.

Tip: To prevent unexpected parsing, ensure that all the names in the name:value pairs are unique.

To populate a reference field, use `setDisplayValue()` instead. See Redirecting Emails for an example of using `setDisplayValue()` in an inbound email action.

**Note:** The action always generates a lowercase variable name. Also, this functionality does not work on reference fields.

For example, if an email body contains this line:

```
Foo:bar
```

The inbound email script creates the variable `email.body.foo` with the value of `bar`. You can use these variables to create conditions such as:

```java
if(email.body.foo!=undefined){
current.[field]=email.body.foo;
}
```

In this example, the script sets the value of `field` to the value `bar`.

**Note:** Spaces are rendered as underscores when a name:value pair gets parsed into a variable/value pair. For example, if an email body contains a line with spaces like `my variable:data`, then the inbound email script creates the variable `email.body.my_variable`. The value of the variable is `data`.

Integrate inbound events

This example illustrates how to create a notification from an inbound JSON request.

Role required: admin

When complete, you will be able to:

- Send a JSON request to the `imp_notification` web service import set with the JSON processor
- Create a new import set in the `imp_notification` table in the instance using data from the JSON request
The following example steps assume you have your own demonstration instance.

1. Activate the JSON Web Service plugin.
2. Install the RESTClient Firefox plugin.
3. Open the RESTClient.
4. Create the following JSON request.
   - **Method**: POST
   - **URL**: `http://<instance name>.service-now.com/imp_notification.do?JSON`
   - **Headers**: Authorization: Basic
   - **Body**: 
     ```json
     {"sysparm_action":"insert","message":"this is an event","uuid":"abc"}
     ```

5. Click *Send*.
7. Verify that the instance sends back a response with a sys_id.
8. Login to your development instance.
10. Verify that the import set table has an event matching your JSON request.

Inbound email action examples
Several examples of inbound email actions are available to help you build your own inbound email actions.

Inbound email action example: handling email replies
This example shows you how to set up inbound email actions to handle replies that users send back to the instance.

Role required: admin

The inbound email action parses the email and responds using a script. By default, an email received by the instance creates a new incident, and the body of the email is added to the Additional Comments text box. More refined Inbound Email Actions can create incident tickets with more data, thus saving the incident management team valuable time.

Normally, when a user responds to an email sent by the instance, the inbound email action matches the watermark to an existing incident, and updates the incident rather than creating a new record. However, if the watermark is missing, this inbound email action attempts to match a reply to the original incident.

1. Navigate to System Policy > Inbound Actions and click New.
2. Populate the form as follows:
Inbound action field values

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Update Incident</td>
</tr>
<tr>
<td>Type</td>
<td>Reply</td>
</tr>
<tr>
<td>Target table</td>
<td>Incident (incident)</td>
</tr>
</tbody>
</table>
### Inbound email action example: requesting a change

This example shows you how to set up inbound email actions to create a change request record.

**Role required:** admin

Inbound Email Actions allow users to log or update incidents on an instance via email. The inbound email action parses the email and responds using a script.

1. Navigate to **System Policy > Inbound Actions** and click **New**.
2. Populate the form as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Request Change</td>
</tr>
<tr>
<td>Type</td>
<td>New</td>
</tr>
<tr>
<td>Active</td>
<td>True</td>
</tr>
<tr>
<td>Target Table</td>
<td>Change Request (change_request)</td>
</tr>
<tr>
<td>Condition</td>
<td>email.subject.indexOf(&quot;Change Request: &quot;) == 0</td>
</tr>
<tr>
<td>Script</td>
<td>current.comments = email.body_text;</td>
</tr>
<tr>
<td></td>
<td>current.short_description = email.subject;</td>
</tr>
<tr>
<td></td>
<td>current.notify = 2;</td>
</tr>
<tr>
<td></td>
<td>if (email.body_text.assign != undefined)</td>
</tr>
<tr>
<td></td>
<td>current.assigned_to = email.body_text.assign;</td>
</tr>
</tbody>
</table>
Values automatically set from incoming email

The default inbound action for the incident table automatically sets the following field values when it receives an incoming email.

<table>
<thead>
<tr>
<th>Field</th>
<th>Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>if (email.body_text.priority != undefined)</td>
<td>current.priority = email.body_text.priority; if (email.body_text.category != undefined) current.category = email.body_text.category; current.insert();</td>
</tr>
</tbody>
</table>

If multiple users have the same email address, the instance first searches for an active user with the email address. Use unique email addresses for each user record whenever possible. If not, having only one active user with the shared email address guarantees that the instance always matches incoming email from this address to the active user.

**Specifying the inbound email processing order**

The Ordered Email Processing plugin enables you to configure a processing order for inbound email actions.

In addition to forcing email actions to run in a prescribed order, the administrator can add a command to the script for an action that halts processing after the script runs. The plugin simply adds the **Order** column to the Rules (sysrule) table, which the instance uses to determine when to process emails.

Configure the processing order

Configure the processing order for inbound email actions to force them to run in a prescribed order.

**Role required**: admin

1. Navigate to System Policy > Email > Inbound Actions.
2. Open an existing inbound action or create one.
3. Complete the form and assign an order number to the Order field to establish when this inbound rule should run in relation to other rules. If you upgraded and activated the plugin, the **Order** field might be named Execution Order.

**Note**: Ensure each inbound action has a unique Order value to ensure the system stops processing as expected. If multiple inbound actions have the same Order value, the system might evaluate all of the inbound actions, even if one of them contains the event.state="stop_processing"; script or has the Stop processing option selected.
4. To stop rule processing when an inbound email action runs successfully: add the following line to the bottom of the script:

- Select the **Stop processing** check box.
- Add the following line to the bottom of the **Actions** script:

```
   event.state="stop_processing";
```
Inbound email actions specify how ServiceNow creates or updates task records in response to an incoming email. Each email action looks for a watermark in the email to associate it with a specific task. When the script is run, More Info

- **Name**: Unsubscribe from Notification
- **Target table**: Notification Messages
- **Action type**: Record Action

### When to run

**Only emails of the selected Type will trigger this inbound action.**

- **Type**: New

**Order determines when to run relative to other inbound actions. The inbound action with the lowest order runs first.**

- **Execution Order**: 35

### Conditions

All of the following conditions must be true, to trigger this inbound action.
Manage multiple filters in an inbound email action

Use process ordering and the `stop_processing` command to manage multiple filters in inbound email actions.

Role required: admin

In this example, you can create new problem records when `prb:` appears in the subject line and new change requests when `chg:` appears in the subject line. All other emails are used to create an incident. The actions are set up as follows:

1. Create an action with a condition of `Subject > starts with > chg:` and the `event.state="stop_processing";` command appended to the script.
2. Assign this action an Order value of 100.
3. Create an action with a condition of `Subject > starts with > prb:` and the `event.state="stop_processing";` command appended to the script.
4. Assign this action an Order value of 200.
5. Create an action for incident with no conditions and an Order value of 300.

   It is not necessary to add the `stop_processing` command to the script for the incident action unless you want processing to stop at this rule to avoid continuing to another action.

If either a change request or a problem is created, the `stop_processing` command stops processing, and no incident record is created. If neither a change request nor a problem is created, the inbound email action for incident creates a record.

Email filters

Email filters enable administrators to specify when to move email to particular mailboxes or to ignore it using a condition builder or a condition script. Email filters are inactive by default.

When an email is ignored, the email is saved to your instance but is not processed. You can access an ignored email by viewing its Email (sys_email) record.

Default email filters

After activation, these filters are available from the System Mailboxes > Filters module:

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore VCAL</td>
<td>Ignores all email containing vCalendar requests. This filter prevents inbound email actions from creating unnecessary incident records when</td>
</tr>
<tr>
<td></td>
<td>the instance receives a response to sent email. vCalendar requests in email responses are identified by the EmailUtils script include.</td>
</tr>
<tr>
<td>Ignore header</td>
<td>Ignores email that contains specific headers. This filter overrides the <code>glide.pop3.ignore_headers</code> property.</td>
</tr>
<tr>
<td>Ignore sender</td>
<td>Ignores email from specific senders. This filter overrides the <code>glide.pop3.ignore_senders</code> property.</td>
</tr>
<tr>
<td>Ignore subject</td>
<td>Ignores email with specific terms or phrases in the subject line. This filter overrides the <code>glide.pop3.ignore_subjects</code> property. This filter might not apply to emails arriving from unknown users. Unknown users can be locked out.</td>
</tr>
<tr>
<td>Filter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Move spam to junk folder</td>
<td>Moves email identified as spam to the Junk folder. This filter checks for</td>
</tr>
<tr>
<td></td>
<td>the value of the ServiceNow spam header. If the header is</td>
</tr>
<tr>
<td></td>
<td>X-ServiceNow-Spam-Status:Yes, the filter moves the email to the Junk folder</td>
</tr>
</tbody>
</table>

**Email filter script include**

Email filters use a script include called `EmailUtils` that contains a simple utility function to determine if `vCalendar` is in the body of the response email. The results of this query are used in a condition script in the Ignore VCAL email filter.

**Spam scoring and filtering**

Every message sent through email servers is assessed for the likelihood of being spam. Based on this assessment, the instance adds headers to each message that can be used for filtering within the customer instance using the Email Filters plugin. This is only available for instances that use the ServiceNow email infrastructure. See [KB0549426](#) for an explanation of email scoring and filtering.

**Activate email filters**

Administrators can activate the Email Filters plugin (`com.glide.email_filter`).

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 an email filter**

You can create email filters to apply a custom action script or filter actions when email matches your filter’s conditions.

Role required: admin

1. Navigate to System Mailboxes > Administration > Filters.
2. Click New.
3. Complete the fields (see the table).
4. Right-click in the header bar and select **Save** from the context menu. The Filter Actions related list appears.

5. Click **New** in the related list.

6. Select how the system should react when the conditions of this filter evaluate to true.

The two choices in the base system are: Mark as Ignored and Move to Junk. You can use the Action script to perform additional email tasks.

**New filter table**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Brief, descriptive name for this filter.</td>
</tr>
<tr>
<td>Order</td>
<td>Define an order for this filter to determine when it is evaluated. By default, the Ignore VCAL filter has the lowest order number and is evaluated first.</td>
</tr>
<tr>
<td>Active</td>
<td>Select the check box (true) to enable this filter.</td>
</tr>
<tr>
<td>Short description</td>
<td>Concise description of the function of this filter.</td>
</tr>
<tr>
<td>Conditions</td>
<td>Add conditions for this filter with the condition builder or with a condition script. Note that conditions are case sensitive.</td>
</tr>
<tr>
<td>Condition script</td>
<td>Create a script that defines the conditions for this filter. Use this script to access other tables, variables, or methods. For example, the condition script for the Ignore VCAL filter looks for the results of the EmailUtils script include, which detects vCalendar attachments.</td>
</tr>
<tr>
<td>Action script</td>
<td>Use the action script to define additional behavior to be performed when the filter condition evaluates to true. This might include an email action not included in the default filter actions. In the base system, the action script is used to produce the error string that is published to the email log (System Logs &gt; Email).</td>
</tr>
</tbody>
</table>

**Note:** Before creating additional email actions with a script, see *Inbound Email Actions*. Like business rules, inbound email actions use both conditions and scripts and can provide a number of useful actions on emails the instance receives.

**Email retention**

You can archive and eventually destroy email messages that you no longer need or if your Email table is excessively large.

Email retention is available starting with the Helsinki release.
Email archive and destruction plugins

The email archiving and destruction feature uses the Data Archiving and Email Retention plugins. The Data Archiving plugin must be active to archive and destroy email records. The Email Retention plugin provides a set of rules that specify when the system archives and destroys email records.

**Note:** The Email Retention plugin also prevents the system from deleting watermarks, which are required for inbound email actions to continue to function.

The Email Retention plugin and associated archive and destroy rules are active by default on new instances. On upgraded instances, you must manually activate both the plugin and the archive and destroy rules. ServiceNow recommends that you review and approve these rules before activating them.

If your instance already has a process to manage email records, you do not need to activate the Email Retention plugin. If you want to replace your current process with Email Retention, be sure to deactivate the current process before activating the archive and destroy rules.

Archiving and destroying email records

Archiving means moving records from the Email (sys_email) table to the Archive Email (ar_sys_email) table when they exceed the archive rule time limit. Destroying means deleting records in the Archive Email table when they exceed the destroy rule time limit.

**Note:** When a destroy rule deletes email records, associated watermarks are not deleted. They are preserved to ensure that your inbound email actions continue to function.

Default archive and destroy rules

Email Retention provides these email archive rules:

- **Emails - Ignored and over 90 days old:** archives email message records that were created more than 90 days prior to the current date and are of type received-ignored or sent-ignored.
- **Emails - Over a year old:** archives email message records that were created more than 365 days prior to the current date.

Email Retention also provides this email destroy rule:

- **Email Archive - Over a year old:** destroys email records that have been archived for more than 365 days prior to the current date.

With these default settings, your email messages are kept on the instance for a total of two years: one year in the Email table, and one year in the Email archive table. At the end of this period, the system deletes the expired email records from the Email archive table.

**Note:** By default these rules are active on new instances and inactive on upgrades. The system runs archive and destroy rules when you activate them.
Compatibility with other record management implementations

If you are already using another method to manage email records, such as table cleaners, you do not have to use the Email Retention feature. To prevent unexpected record deletion, ServiceNow recommends that you avoid using multiple email management processes on the same instance at the same time.

Note: For assistance replacing your existing record management implementation with Email Retention, contact your professional services or sales representative.

Effects of archiving and deleting email records

Inbound email actions copy the body of an email to the work notes of the related record. If the inbound email record is later deleted, the work notes still contain a text copy of the email.

When the system sends an email message about a record, the activity formatter displays a Sent Email section with a link to the email message. If the system archives the email message, the activity formatter removes Sent Email section. When the system deletes the email message, it is no longer visible in the activity formatter nor the work notes.

Note: Set the archive time length long enough so your users can access sent emails though the activity formatter.

Archiving email records changes the methods available to the system to identify inbound email as a reply. After archiving an email record, the system can no longer use the In-Reply-To field to match an incoming email to an email record. However, the system can still match incoming email to an existing record from a record number or watermark.

Activate the Email Retention plugin

The Email Retention plugin provides archive and destruction rules for email messages. It is active by default for new instances, but must be activated for upgrades.

Required role: admin

The Email Retention plugin requires these plugins:

- Data Archiving
- System Mailboxes

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**.

**Archive email manually**

You can archive email messages manually on demand instead of waiting for the instance to archive them based on a scheduled job.

Role required: admin

Email Retention provides these email archive rules:

- **Emails - Ignored and over 90 days old**: archives email message records that were created more than 90 days prior to the current date and are of type `received-ignored` or `sent-ignored`.
- **Emails - Over a year old**: archives email message records that were created more than 365 days prior to the current date.

You can manually archive email messages that meet these archive rules or any additional archive rules that you create.

---

**Note:** An archive record must be active for the instance to be able to process records with it.

1. Navigate to **System Archiving > Archive Rules**.
2. Open the email archiving rule that you want to modify.
3. Click **Recalculate Estimate** to see how many records in the Email (`sys_email`) table are going to be archived. The estimate appears in the **Record estimate** field.
4. Click **Run Archive Now**.

**Note:** You can also archive related records.

---

**Watermarks on notification emails**

By default, the system generates a watermark label at the bottom of each notification email to allow matching incoming email to existing records. Each watermark includes a random 20-character string that makes it unique.

Starting with the Jakarta release, the system automatically generates randomized watermarks for notification emails in base systems. The random 20-character string reduces the possibility of a watermark being guessed or coincidentally matching the watermark of an email from another instance.

**Note:** If you are upgrading to Jakarta, random watermark support is optional and requires the Random Watermark Support plugin to be activated. For details on the plugin and related upgrade considerations, see **Notifications upgrade information**.

---

**Watermark format**

The email watermark always begins with "**Ref:**" to identify the label as a watermark. After this identifier, the default label is 31 characters in length and consists of:

- **Customizable prefix** - The default prefix is `MSG`.
- **Auto-numbered identifier** - The numeric string identifying the source record, such as incident, problem, or change request.
An underscore character followed by a random 20-character string

Watermark configuration

Watermarks are always generated, but you can configure them to:
- Create a custom watermark prefix for each instance to prevent accidentally triggering events in the wrong instance.
- Have custom prefix characters after MSG
- Be hidden globally
- Be omitted from individual email messages

If watermarks are omitted from email notifications, inbound email actions might not work properly. Without a watermark, the system processes inbound email messages as described in Criteria for matching email to inbound actions.

**Note:** Email clients that use the plain text version of the email still show the watermark.

Create a custom watermark prefix for email notifications

By default, email notifications use the watermark prefix MSG, but you can create a custom watermark prefix.

Role required: admin

Any email notifications that are forwarded from one instance to another might be more easily distinguished with different prefixes for each instance. To avoid unintentionally triggering events in the wrong instance, create a unique watermark prefix for each instance.
Note: Do not use colons (:) in custom watermark prefixes. Colons are a reserved character and may cause the watermark to be ignored.

1. Navigate to System Definition > Number Maintenance.
2. Open the MSG record in the Email Watermark (sys_watermark) table.
3. Enter the unique Prefix for this instance.

   ![Number Maintenance Table]

4. Click Update.

Your custom watermark applies to all new email notifications. Email notifications that existed before you created a custom watermark keep the same watermarks as before.

**Omit an email notification watermark**

You can omit watermarks on email notifications if you do not want the instance to match the notification to an existing record.

Role required: admin

1. Navigate to System Notification > Email > Notifications.
2. Select the email notification to update.
3. Click the Advanced View related link.
4. In the What it will contain section, select the Omit watermark check box.

When incoming email does not contain a watermark, the system searches the subject line and message body for a record number. The system attempts to match any record number that it finds to an existing record. If there is a matching record number, the system updates the record with the values in the incoming email. To ensure that response email messages don’t update records, remove the record number variable $\{\text{number}\}$ from the Subject and Message HTML fields.
**Hide email watermarks globally**

Rather than omitting watermarks, it is possible to hide watermarks on a global basis using HTML markup.

Role required: admin

Watermarks can only be hidden in the HTML message. The text version of the message, because it does not have markup allowing show/hide semantics, will always have the watermark.

1. Navigate to `sys_properties.list` in the Application Navigator.
2. Create a new property named `glide.email.watermark.visible` and set it to `false`.

This ensures that all watermarks are hidden on all email messages. This cannot be done on a per-email basis.

**System mailboxes**

Email messages can be seen in the System Mailboxes menu, which gives you access to the system Inbox, Outbox, and Sent mail box.

Each provides a filtered view of emails to let you see only what you need to at any given time, including list fields applicable to each. The system mailboxes menu shows your current POP and SMTP status.

The System Mailbox is hosted by ServiceNow, who have sole access to the mailboxes. By default, once the instance pulls an email message, it is deleted from the mail server and stored in the application on the Email (sys_email) table.

**System Mailboxes**

- **Inbound emails**: All inbound mail is placed into the Inbox until it is processed. After it is cleared, the email moves to the Received state. If the email message matches the criteria in an inbound email action, the email is changed to Processed. If not, it is changed to Ready. If the system is restarted for any reason (such as during a system upgrade), all inbound mail waits on the external mail server until the system can request delivery.
- **Outbound emails**: All outbound mail is placed into the Outbox until it is processed. Once cleared, it is moved to Sent (if sent) or Skipped (not sent, as in the case of no valid recipients). If the system is restarted for any reason (such as during a system upgrade), all outbound mail waits in the instance database until the system comes online, and the scheduler looks for mail to deliver.

**The email client**

The email client enables you to send email directly from any record, such as an incident, change request, problem, or user record.

The email client is available by default, and enabled by default on the incident table.

The email client can be useful in cases where you want to send an email:

- To engage more people in a piece of work
- That includes Cc and Bcc recipients
- That includes personalized comments
- To a third party who doesn’t have an account in your instance
- To someone about an incident where you don’t have an email notification set up to do exactly what you want

The email client always uses the **multipart/mixed** content type and supports HTML markup in the message body.
Enable the email client for a table
Enable the email client for a table so that users can send emails directly from the table record.

Role required: admin

The email client is enabled by default on the Incident (incident) table. You can enable the email client for another table by adding the `email_client` dictionary attribute to the table.

Note: This capability is not inherited by tables that extend the current table. For example, enabling the email client on the Task table does not enable it for the Incident or Problem tables.

1. Open a record in the table that you want to enable the email client for.
   For example, to enable the email client for the Problem (problem) table, navigate to `Problem > Open`, and then open any problem record.

2. On the form, click the menu icon (☰) and then click `Configure > Dictionary`.

3. On the Dictionary Entries list, open the first record.
   The first record has the record type `Collection` and does not have any entry for `Column name`.

4. On the form, in the Related Links section, click `Advanced view`.

5. In the `Attributes` field, enter `email_client=true`.
   If there are other values in the field, separate the attribute with a comma.

6. Click `Update`.

Email client interface
The instance’s email client interface looks like a standard email interface, which contains a toolbar for text formatting and adding attachments.

Users see an email icon based on the UI version.

- **UI16**: The email icon (✉️) appears in the more options menu.
- **UI15**: The email icon (✉️) appears in the form header.

Users click the email icon to launch the email client as a pop-up window.
The email client interface

**Note:** The **Subject** field on the email client allows a larger character count than the default setting for the **Subject** field on the Email table. If the subject text from the client is being truncated, increase the **Max length** value for the **Subject** field on the Email table.

**Customize the email client**

The email client has default properties and values that you can customize to suit your needs.
## Email client default properties and values

<table>
<thead>
<tr>
<th>Property</th>
<th>Default Value</th>
<th>How to Customize</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL access</td>
<td>Defaults to allowing only users with the itil role to access the email client. Change the ACL rule to control access to the email client.</td>
<td>To control who can see the email client, see <a href="#">Control access to the email client</a>.</td>
</tr>
<tr>
<td>Email icon</td>
<td>Allows only users with write access to the current table to see the email icon.</td>
<td>To remove the email icon, see <a href="#">Email icon display</a>.</td>
</tr>
<tr>
<td>Autocomplete</td>
<td>Defaults to only displaying a user's first and last name. A system property controls what columns the email client auto-complete displays. If your organization has several users with the same name, consider adding company or email address columns to help distinguish between users.</td>
<td>• To change search behavior, see <a href="#">Configure email client auto-complete search results</a>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To display additional information, see <a href="#">Additional information in the email client auto-complete</a>.</td>
</tr>
<tr>
<td>To</td>
<td>Defaults to the email address of the caller.</td>
<td>To edit the default value, create an email client template.</td>
</tr>
<tr>
<td>Cc</td>
<td>Defaults to the email addresses of the user who opened the incident and all users in the watch_list.</td>
<td>To edit the default value, create an email client template.</td>
</tr>
<tr>
<td>Subject</td>
<td>Defaults to the incident number and short description.</td>
<td>To edit the default value, create an email client template.</td>
</tr>
</tbody>
</table>

**Configure email client auto-complete search results**

You can control the email client's auto-complete search results with an email client property.

The following properties on **System Properties > UI Properties** control the auto-complete functionality for the email client.

**Maximum number of autocomplete matches to return to the email client. Applies separately to users and groups.**

| 10 |

Include groups in email client autocomplete results.

**Yes | No**

### Email client autocomplete properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.ui.email_client.autocomplete.count</td>
<td>Set the maximum number of auto-complete matches.</td>
</tr>
</tbody>
</table>
Additional information in the email client auto-complete

A system property allows the email client to display additional columns from the User table in the auto-complete list.

Administrators can add this system property to help distinguish between individuals who have the same first and last names, and to ensure that users select the proper recipient for an email.

**Email client properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.ui.email_client.autocomplete.group</td>
<td>Specify whether groups are included in auto-complete results.</td>
</tr>
</tbody>
</table>

**glide.ui.email_client.autocomplete.group**

Sets the columns from the User (sys_user) table that the autocomplete list displays. Separate each column name with a semicolon character (;). See the system dictionary for a list of available column names. For example, to add the sys_user.email and sys_user.company columns, enter email;company in the Value field.

- Type: string
- Default value: name
- Location: Add to the System Property (sys_properties) table

**Auto-complete in the email client**

**Control access to the email client**

You can control access to the email client by changing an ACL rule.

Only users with the itil role can access the email client. The following ACL rule controls this access:
ACL rule

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>EmailClientProcessor</td>
<td>processor</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Note:** Because the visibility of the email icon is determined by whether the current user has write access to the table, it is possible that a user may be able to see the email icon and still not open the email client.

---

Create an email client template

You can create a different template for each table that uses the email client.

Role required: admin

The email client uses its own email templates to define default values for fields. You can use HTML formatting to enter the content of the message body, rather than plain text. You can also use mail scripts to dynamically generate content for the email body. For more information, see [JavaScript in emails](#).

You can create one email client template per table. When users open the email client from the table record, the template content is applied automatically to the email client message.

1. Navigate to **System Policy > Email > Client Templates**.
2. Click **New**.
3. Fill in the fields on the Email Client Template form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique template name.</td>
</tr>
<tr>
<td>Content type</td>
<td>Select HTML or plain text to create the body of the template.</td>
</tr>
<tr>
<td>Table</td>
<td>Select the table that the template applies to. Enable the email client for the same table.</td>
</tr>
<tr>
<td>To</td>
<td>Enter a comma-separated list of either field names that contain user email addresses or specific email addresses. To reference an email address using a script, create a script include and then call the script include in the <strong>To</strong> field. Your script must start with the <code>javascript:</code> prefix. The script must return email addresses in a comma-separated string.</td>
</tr>
<tr>
<td>Cc</td>
<td>Enter a comma-separated list of either field names that contain user email addresses or specific email addresses. To reference an email address using a script, create a script include and then call the script include in the <strong>Cc</strong> field. Your script must start with the <code>javascript:</code> prefix. The script must return email addresses in a comma-separated string. This field cannot have the same values as the <strong>To</strong> field.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Bcc</td>
<td>Enter a comma-separated list of either field names that contain user email addresses or specific email addresses. To reference an email address using a script, create a script include and then call the script include in the Bcc field. Your script must start with the javascript: prefix. The script must return email addresses in a comma-separated string. This field cannot have the same values as the To or Cc fields.</td>
</tr>
<tr>
<td>Subject</td>
<td>Enter a description of the email. The description can contain a comma-separated list of field names or specific values.</td>
</tr>
<tr>
<td>Body HTML</td>
<td>If you selected HTML for the Content type, enter the content of the message body using the HTML editor toolbar to format the HTML. You can include variables from the Select variables column. Variables map to column names available from the notification table, its parent tables, and reference tables. Use variables to include values from a record in the table, such as an incident short description or comments and work notes. You can call a mail script by using ${mail_script:script name} in the Body HTML field.</td>
</tr>
<tr>
<td>Body text</td>
<td>If you selected plain text for the Content type, enter any text or mail script that you want to appear in the message body. You can insert a mail script in the Body text field using the following syntax: &lt;mail_script&gt; [code] &lt;/mail_script&gt;</td>
</tr>
</tbody>
</table>

4. Click Submit.

Set the from address with an email client template
Use an email client template to set a default value for the From field if it should be different from the system default.

Role required: admin

For example, you can dynamically set the From field to the email address of the current user.

1. Navigate to System Policy > Email > Client Templates.
2. Select an existing template or create one. For example, select the Incident Template record.
3. Configure the form to add the From field.
4. Enter a script to add a default value to the From field.
For example, the following script displays the current user name and the current user email address.

```javascript
gs.getUser().getDisplayName() + " <" + gs.getUser().getEmail() + ">
```

**Display an editable From field**

By default, the email client does not display a From field on email messages, but you can add one and have it be editable.

Role required: admin

By default, the email client uses an email address taken from the email account. To display an editable From field in the email client:

1. Navigate to System Properties > UI Properties.
2. Select the Yes check box for Override the email 'From:' address in the email client (glide.ui.email_client.from).

**Display the Reply To field**

By default, the email client does not display the Reply to field because users cannot change this address. But you can display this field using a UI property.

Role required: admin

The email client always uses the same Reply to address as that defined for email notifications. This ensures that the email has a valid watermark and can generate inbound email actions as normal. If you want to change the global reply-to address you must configure your instance to use your own SMTP server.

1. Navigate to System Properties > UI Properties.
2. In the Override the email 'Reply to:' address in the email client (glide.ui.email_client.reply_to) field, select the Yes check box.

**SMS delivery with the email client**

A property is available that lets the user select an option to send a notification via SMS.

The Subscription Based Notifications plugin activates the following system property:

**Email client system property**

<table>
<thead>
<tr>
<th>Property</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>
</tbody>
</table>
Configuring the email client

Quick messages
Quick messages allow you to insert predefined text into the message body of the email client.
Role required: admin

Selecting a quick message fills the Message Text field with the body specified in the quick message. After you define one or more quick messages, the Quick Message selector appears in the email client. Use the following syntax: ${variable_name}.

**Note:** If you add attachments to the Quick Message templates, the attachments are not sent as part of the email distribution.

1. Navigate to **System Policy** > **Email** > **Quick Messages**.
2. Click **New**.
3. Fill in the Email Client Canned Messages form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Enter a name to appear in the Quick Message selector.</td>
</tr>
<tr>
<td>Active</td>
<td>Select this check box to make the quick message available for selection. Clear this check box to remove the message from the Quick Message selector.</td>
</tr>
<tr>
<td>User</td>
<td>Select the user who has access to this quick message. Selecting a user restricts access to that user only. Leave the field blank to have no user-based restrictions.</td>
</tr>
<tr>
<td>Group</td>
<td>Select the group whose members have access to this quick message. Selecting a group restricts access to members of that group only. Leave the field blank to have no group-based restrictions.</td>
</tr>
<tr>
<td>Body</td>
<td>Enter the text you want to insert into the Message Text field. By default, the field supports HTML format.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.
**Email icon display**

You can use access control rules to hide or display the email icon on forms.

Users with write access to the current table can see the email icon. To remove the icon, remove the user's write access to the table. Typically you do this in one of two ways:

- Make the user an Employee Self-Service (ESS) user. ESS users do not have a user role, and without a role they do not have write access to the Incident table. Making a user an ESS users, therefore, hides the email icon on the Incident form.

<table>
<thead>
<tr>
<th>Title</th>
<th>Work in progress</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>✔</td>
</tr>
</tbody>
</table>

**Body**

The incident is now in the **Work in Progress** state.

```
<p>Work in progress</p>
```
Create a custom ACL rule and user role that does not have write access to the table. The default ACL rule for the email client checks to see if the user has the itil role. If you grant users a custom role other than itil, then any such users will not see the email icon.

Remove or display the email icon for a table by setting the email_client dictionary attribute to true or false on the table’s collection record. This will not display the email icon for users without write access to the table. For more detail see Dictionary attributes.

Email Service

Email Service installs the Email API on the instance. By default, Email Service only allows admin users to access the Email API. Administrators can grant access to the Email API by:

1. Adding an access control for creating records in the Email (sys_email) table linked to the email_api_send role.
2. Assigning the email_api_send role to the non-admin user.
3. Verifying the non-admin user has read access to the notification target table. For example, an email notification for an incident, requires read access to the Incident table.

Non-admin users with the email_api_send role can access the Email API from the REST API Explorer.

Activate Email Service

Users with the admin role can activate the Email Service plugin (com.glide.email.service) to enable the Email API.

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.

Grant access to the Email API

To grant non-admin users access to the Email API, administrators must create an access control and assign a special role.

Role required: admin
For additional details, see Email API.

1. Elevate privileges to security_admin.
3. Click New.
4. Create an access control for the Email (sys_email) table.

### Access control values

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>record</td>
</tr>
<tr>
<td>Operation</td>
<td>create</td>
</tr>
<tr>
<td>Admin overrides</td>
<td>Selected</td>
</tr>
<tr>
<td>Name</td>
<td>sys_email</td>
</tr>
<tr>
<td>Requires role</td>
<td>email_api_send</td>
</tr>
</tbody>
</table>

5. Assign the email_api_send role to the non-admin user.
6. Verify the non-admin user either has read access to all records in the notification target table or has read access to a specific record in the table.

For example, to work with incident notifications the non-admin user needs access to the Incident table. You can provide record access by:

- Granting the user an appropriate role, such as the itil role.
- Selecting a specific incident that was opened on behalf of the user.

## Push notifications

In addition to sending email and SMS notifications, an instance can send push notifications to mobile devices.

A push notification is a text message that appears on a user’s mobile device to alert them about something important or to ask them to perform an action. Starting with the Geneva release, your instance supports push notifications.
An example push notification

Use push notifications to send messages to users when certain conditions are triggered on your instance, such as the assignment of an incident to the user. A push notification can even ask for a reply, and the instance can process the reply by acting on the related records. For example, you can have the instance send an approval request for a Change to a user. You can let the user approve or deny the Change by clicking a response button on push notification. The user’s response can then update the status of the Change record.

You can set up push notifications in a similar manner to email and SMS notifications. Determine:

- who to send the notification to
- when it should be sent
- what it should contain

By default, the ServiceNow mobile application supports push notifications. But you can also develop your own push application and configure your instance to send push notifications to it.
Push notification setup

Push notification setup differs depending on the mobile or push application that you want your users to use. For an overview, see:

- **Push notification setup with the ServiceNow mobile application**

  Note: Push notifications for on-premise instances are not supported.

- **Push notification setup with a custom push application.** If you create your own application, you must understand how push notifications and the Apple Push Notification Service system work. For more information, see the APNs Overview in the [Local and Remote Notification Programming Guide](#) for Apple developers.

  Attention: Apple does not guarantee delivery of all push notifications. Review the Quality of Service (QoS) information in the [Local and Remote Notification Programming Guide](#) for Apple developers.

Push notification system

The push notification system involves several key elements that manage the delivery of push messages, push notification responses, and push feedback.

- **Customer instance:** Your instance.
- **Push proxy:** An instance that collects all push notifications that go to the ServiceNow mobile application and forwards them to the ServiceNow iOS or Android applications. If you create a custom push application, you do not use the push proxy.
- **Push provider:** The provider of push messages, which is the Apple Push Notification service (APNs) or Google Cloud Messaging (GCM) service, for the ServiceNow mobile app or custom mobile apps.
- **Feedback provider:** The provider of feedback messages, which tell the instance what devices are no longer valid. The Apple feedback or GCM server handles feedback messages for the ServiceNow mobile application on iOS and Android devices respectively.
- **Feedback proxy:** The ServiceNow instance that handles feedback messages from the Apple feedback server.
- **Push application on a mobile device:** The application, such as the ServiceNow mobile application. You can also build and customize your own push application.

Push notification process

The push notification process is as follows:

1. Activity on the instance triggers a push notification.
2. The instance looks for who to send the notification to and checks the user notification preferences to find their push device settings.
3. The instance sends the push notification to the push notification service, either the Apple Push Notification service (APNs) or Google Cloud Messaging (GCM) service. If you are using the ServiceNow mobile app, the instance sends the notification through a push proxy instance, which then forwards the notification to the APNs or GCM service.
4. The push notification service sends the notification to the user’s push application. When the instance sends the notification to the push notification service, it includes message content along with the instance name and ID. This information ensures that a response to the
notification is sent back to the correct instance. If the user can reply to the notification, such as sending an approval to a change request, the response is sent via REST message back to the instance.

5. The instance identifies a script to run to handle the response.

6. The script performs an action on the instance, such as marking a change request approved. If there is invalid JSON or if the script fails, an error response is sent back to the device.

The following diagram shows the elements of the push notification system with the ServiceNow mobile application. Within the ServiceNow infrastructure is your instance, the optional push proxy instance, and the ServiceNow feedback proxy. External to ServiceNow are the messaging services (APNs or GCM) and user mobile devices, which include the application that is registered to receive push notifications. See Push feedback for an explanation of the feedback service.

Push notification system with the ServiceNow mobile app
Push notification responses

With custom push applications, you can have your users act on records in the instance by responding to a push notification.

The actions that they can take are defined in a script that you associate with the notification message. The response is sent to the instance in this format:

```plaintext
https://{instance_name}/api/now/v1/push/{application Name}/action/{action}
```
The application name is the push application the user is using. The application name must match the application name in the Push Application (sys_push_application) table. The action is the Sys ID of the action in the Push Notifications Actions (sys_push_notif_act_script) table.

**Push feedback**

Feedback refers to the information about failed iOS message delivery and the iOS push applications that can no longer receive push notifications.

The instance uses a scheduled job to pull feedback data every hour from the APNs. When the APNs determines that a device can no longer receive push messages, the corresponding device is set to inactive, making it unable to receive push notification messages. The Push Feedback (sys_push_feedback) table shows the token for the device that failed. If the same device is again able to receive push notifications, the device might receive the same token from the APNs. A new record is inserted into the Push Notification Installation (sys_push_notif_app_install) table.

**Activate push notifications**

Several plugins must be activated to use push notifications. If you have the Mobile UI (com.glide.ui.m) plugin active, push notification plugins are automatically activated.

Role required: admin

You must have the following plugins active on your instance:

- **Push Notification**: Provides the necessary components and REST APIs to send push notifications to mobile devices.
- **Notification System Push Addon**: Adds support for push notifications to the existing notification system.

This plugin is installed in the push notification infrastructure:

- **Push Feedback**: Handles feedback from Apple on which devices are no longer valid so they do not keep receiving push notifications.

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 timezone, 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 | Any information that would be helpful for the ServiceNow personnel activating the plugin such as if you need the plugin activated at a specific time instead of during one of the default activation windows. |
3. Click Submit.

Installed with push notifications
Several types of components are installed with the push notifications plugins.

Tables installed with push notifications
These tables are installed with push notifications.

<table>
<thead>
<tr>
<th>Table name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Push Applications (sys_push_application)</td>
<td>Push applications registered to the instance to receive push messages.</td>
</tr>
<tr>
<td>Push Default Registrations (sys_pushnotif_default_reg)</td>
<td>Contains all the notifications users are automatically subscribed to for a given push application. You can add notifications to this table on the Push Default Registrations related list on the Push Application form.</td>
</tr>
<tr>
<td>Push Feedbacks (sys_push_feedback)</td>
<td>Feedback from the APNs that tells the instance which push devices can no longer receive push messages. The feedback is handled on the same instance where your notifications are triggered, or on a central instance that uses a REST call to tell your instance which push applications to deactivate.</td>
</tr>
<tr>
<td>Push Message Attribute Definitions (sys_pushnotif_msg_attr_def)</td>
<td>The attribute definitions used for push message content specification.</td>
</tr>
<tr>
<td>Push Message Attribute Values (sys_pushnotif_msg_attr_val)</td>
<td>The values associated with push messages.</td>
</tr>
<tr>
<td>Push Notifications (sys_push_notification)</td>
<td>The push notifications that the instance attempted to send to users.</td>
</tr>
<tr>
<td>Push Notification Actions (sys_pushnotif_act_script)</td>
<td>The action scripts that the instance uses in response to an actionable push message.</td>
</tr>
<tr>
<td>Push Notification Installations (sys_pushnotif_app_install)</td>
<td>The devices with push apps where users agreed to receive push notifications. This table lists the records by the token for the push app. The instance uses this information to know which push device and app to send notifications to. Records are created in this table when a user logs on an instance with the push app. The Mobile Devices (sys_mobile_devices) table, which is installed with the Mobile UI plugin, contains all the user devices that logged in to the instance with the ServiceNow mobile application.</td>
</tr>
<tr>
<td>Push Notification Messages (sys_pushnotif_msg)</td>
<td>Messages customized for push notifications. These messages can be associated with a notification.</td>
</tr>
<tr>
<td>Push Notification Message Contents (sys_pushnotif_msg_content)</td>
<td>The entire content, including JSON, for push messages.</td>
</tr>
<tr>
<td>Push Platforms (sys_push_platform)</td>
<td>The platforms that are supported for push notifications, and the maximum payload size.</td>
</tr>
</tbody>
</table>
**Business rules installed with push notifications**

These business rules are installed with push notifications.

<table>
<thead>
<tr>
<th>Business rule</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build Device and Subscriptions</td>
<td>Push Installation</td>
<td>Automatically creates a notification device on a user’s notification preferences when the user registers a mobile application with the instance.</td>
</tr>
</tbody>
</table>

**Outbound REST messages installed with push notifications**

These outbound REST messages are installed with push notifications.

<table>
<thead>
<tr>
<th>REST message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServiceNowMobileApp Push</td>
<td>The REST message that you can use with your custom iOS mobile app.</td>
</tr>
</tbody>
</table>

**Roles installed with push notifications**

These roles are installed with push notifications.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>push_admin</td>
<td>Can create and modify push notifications.</td>
</tr>
</tbody>
</table>

**Push components installed with push notifications**

These components are installed with push notifications.

**Push applications installed with push notifications**

<table>
<thead>
<tr>
<th>Push application</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServiceNowPushApp</td>
<td>The push application record for the ServiceNow mobile application.</td>
</tr>
</tbody>
</table>

**Note:** The ServiceNow mobile application automatically subscribes users to several push notifications. You can see the list of these notifications in the Push Default Registrations related list on the ServiceNowPushApp application record.

**Message content installed with push notifications**

<table>
<thead>
<tr>
<th>Message content</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConnectMessageContent</td>
<td>The payload for ServiceNow connect messages.</td>
</tr>
<tr>
<td>Generic Approval (Background)</td>
<td>The payload that provides an approval and rejection option to the user receiving the push message.</td>
</tr>
</tbody>
</table>
### Message content

| Generic Approval (Foreground) | The payload that provides an approval and rejection option to the user receiving the push message. |
| Generic Record Payload       | A generic payload that you can use to send push messages to users. |

### Push notification actions installed with push notifications

<table>
<thead>
<tr>
<th>Push notification action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approval - Approve</td>
<td>Allows an administrator to approve a request.</td>
</tr>
<tr>
<td>Approval - Reject</td>
<td>Allows an administrator to reject a request.</td>
</tr>
</tbody>
</table>

### Push notifications installed with push notifications

<table>
<thead>
<tr>
<th>Push notifications</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConnectMessagePushNotification</td>
<td>Live Feed Message (live_message)</td>
<td>Sends a push notification when a new live feed message</td>
</tr>
</tbody>
</table>

### Push notification properties

Push notifications provides several properties to customize the setup. Add these properties to the System Properties (sys_properties) table.

- **glide.push.debug**
  - Creates entries in the system log for push notification errors.
  - Type: true | false
  - Default value: false

- **glide.push.feedback.debug**
  - Creates entries in the system log for feedback sent by the APNs for custom iOS push applications.
  - Type: true | false
  - Default value: false

- **glide.push.notification.ttl_seconds**
  - Specifies the number of seconds after which a queued push notification expires. After a push notification is triggered, it is queued and finally processed by a scheduled job. If the time the notification sits in the queue exceeds this value, the notification is not sent. Check the Push Notifications log for more information.
  - Type: integer
  - Default value: 21600

- **glide.push.enabled**
  - Enables or disables push notifications.
Push notification setup with the ServiceNow mobile application

The default ServiceNow mobile application automatically enables push notifications and configures mobile devices for push notifications when users initially log in to the instance with the mobile app.

**Note:** Push notifications with the ServiceNow mobile application are not supported in on-premise instances.

Setting up push notifications involves both the system administrator and users:

- Admin creates or updates push notifications for the ServiceNow mobile app. The admin does not need to set up the mobile devices for users nor update their user preferences for receiving push notifications.
- Users install the ServiceNow mobile app on their iOS or Android mobile devices and set their preferences for receiving notifications on the ServiceNow mobile app.
What to do - admins

Admins create push notifications, similar to setting up email notifications. A push notification has two main parts: the push message and the notification, which includes the push message.

Note: The push message and notification must be for the same table.

Create the push message

Before creating a push notification, create the push message with the actual message content (JSON payload) to be included in the push notification.

Create the push notification that includes the push message

Create the push notification that includes the push message and message content. A push notification specifically sends the push message. You can update a standard platform notification and use it as a push notification that includes the push message.

Add the new push notification to the Push Default Registration table
To ensure that a new push notification is included and enabled in the notification preferences of your users, register a new push notification in the Push Default Registration table. The notification is listed in the notification preferences of your users the next time that they log in to the ServiceNow mobile app.

What to do - users

Download the ServiceNow mobile app
Install the ServiceNow mobile app on an iOS or Android mobile device.

Agree to accept push notifications
After installing the ServiceNow mobile app, users are asked to accept push notifications. When the instance receives the push notification acceptance message from a user, it creates a record in the Push Notification Installations (sys_push_notif_app_install) table. This record is what the instance uses to identify the device + mobile application combination necessary to identify a push notification recipient.

The device then:
- Obtains a token that identifies the device.
- Triggers the creation of the device in the user notification preferences.

Log in to the company instance from the ServiceNow mobile app
Logging in automatically subscribes users to the push-specific notifications registered in the Push Default Registration table.

Update preferences for receiving notifications on the ServiceNow mobile app
Users can enable or disable notifications through Notification Settings in the ServiceNow mobile app. They can set additional notification preferences, such as conditions or filters that affect notification delivery, by using the System Settings window on a desktop or mobile browser. For details, see User notification preferences in UI16.

Next steps

If you are an admin, review the base system notifications and determine if new push message content and push notifications are needed.

Create a push message
Before you create a push notification, create the push message with the actual message content for the notification.

The Push notification plugin must be active. The plugin is active by default, starting with the Geneva release.

Role required: admin

The push message and notification must be for the same table.

2. Fill out the fields on the form (see table).
3. Click Submit.
Push Notification Message form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name for the message.</td>
</tr>
<tr>
<td>Push App</td>
<td>Select the ServiceNow Mobile Application.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Push Message Content</td>
<td>Select the JSON content to be included in the push notification payload.</td>
</tr>
<tr>
<td>Note:</td>
<td>For details on defining payloads that control push notification behavior, see <a href="#">KB0622333</a>. For example, you can specify predefined button pairs (Yes/No, Approve/Reject, Accept/Decline) as part of the push message content.</td>
</tr>
<tr>
<td>Message</td>
<td>Enter the message. You can add variables just as you would for other notifications. Any message you enter here overrides the message in the notification.</td>
</tr>
<tr>
<td>Related list</td>
<td></td>
</tr>
<tr>
<td>Push Message Attribute Values</td>
<td>Optional. Select the attributes that apply to this notification. For details, see <a href="#">Create an attribute value or action for a push message</a>.</td>
</tr>
</tbody>
</table>

**Set up the push notification** that contains the message created or update an existing push notification to use the push message.

**Create a notification using a push message**

Email administrators can create a notification that specifically sends a push notification.

Configure the *push message* before performing these steps.

Role required: admin

You can associate a push message with a standard notification. A push message specifies the text the system sends as part of the push notification to the mobile device.

1. Navigate to **System Notification > Create Push Notification**.
2. Fill out the notification form as necessary (see [Create an email notification](#) for descriptions of the form fields).
3. Click the **What it will contain** tab.
4. Next to **Push Messages**, click the lock icon and select a push message.

**Note:** The push message and notification must be for the same table.

5. If you want this notification to be sent only as a push notification and not as any other type of notification, select **Push Message Only**.
6. Click **Submit**.

   If the notification fails, the user is not notified. If the message fails to send because it exceeds the maximum payload, the instance logs the failure in the System Log.

**Add the push notification to the Push Defaults Registrations table** so that the push notification is listed in the notification preferences for users. Users can then select which notifications they want to receive for the ServiceNow mobile app.
Add a push notification to the Push Default Registrations table

After you create a new push notification, add it to the Push Default Registration table. Push notifications registered in this table are listed and automatically enabled in the notification settings of your ServiceNow Mobile Application users.

Role required: admin

2. Select the ServiceNow Mobile Application.
3. In the Push Application form for the ServiceNow Mobile Application, select the Push Default Registrations tab and click New.
A push application is a mobile app that can receive push notifications from a ServiceNow instance. Create a mobile application record for your customized mobile app and specify how to handle push messages and feedback.

**More info**

- **Display Name**: ServiceNow Mobile Application
- **Name**: ServiceNowPushApp
- **Push**: REST API

**Push Notification Message Center...**

- **Push Default Registrations (170)**
  - **Push Application** = ServiceNow Mobile Application
  - **Notification**
    - Notify quiz manager overdue
    - Approval Error Message response
    - Change commented (unassigned)
4. In the Push Default Registration New record, select the notification to be registered.
5. Click **Submit**.
   The next time that users log in to their instance, the new push notification is included in their list of notifications.

**Push notification setup with a custom push application**

If you are using your own custom mobile or push application, you must configure your app for use and set up the push contents.

Setting up a push notification infrastructure that uses a custom push app involves a push admin (also called push app developer or mobile app developer) and system administrator. When push admins create a customized push app, they also configure the app, its push message content (payload generators), and optional attributes, such as push action scripts. The admin creates and updates the push notifications for the custom push app. After users install the custom push app and initially log in to their instance from their mobile device, the system automatically creates a device (channel) for the custom app.

**Note:** These instructions are intended for users who develop their own customized push application. You do not need to configure the ServiceNow mobile application.
What to do - push admin

Create the PKCS file that contains the certificate for publishing your custom push app

The PKCS (.p12) file contains the iPhone developer certificate and the private key used to sign the certificate. The instance uses the information in the PKCS file to communicate with the APNs. Attach the .p12 file to the X.509 Certificates (sys_certificate) record (System Definition > Certificates) and change the Type to PKCS12 Key Store.

**Note:** For details on generating the .p12 file with the required certificate and private key, see Configure push notifications in Xcode Help for Apple developers.

Configure the custom push application

1. Create a push application record in the Push Application (sys_push_application) table for the custom push app.
The instance uses this push application record to identify the device + push application combination necessary to determine a push notification recipient.

2. Create **push message content**.

   Create a JSON content payload for different types of push notifications. The content determines how a push notification appears on the push application, and whether the user can send a message in response to the push notification. The push admin can create attribute definitions that specify a default push action script or string, for use in the push message content (next step).

3. Create an **attribute value or action for a push message**.

   You can create attribute values that override the default attribute definitions used in the push message content.

4. (Optional) Create a **push action**, a server-side script that tells the instance how to handle responses to push notifications.

What to do - admin

Create the push messages and push notifications

The administrator creates the push messages, sets up push notifications for the custom push app, and if desired, the content.

Next steps

If you are a push admin, begin the configuration process by creating the push application record for your custom push app.

If you are an admin, create the push messages and push notifications for the custom push app.

Create a push application record for your custom app

Register your customized mobile application with your instance to receive push notifications for the application.

The Push notification plugin must be active. The plugin is active by default, starting with the Geneva release.

Role required: admin or push_admin

Push notifications are application-specific: They are sent to one type of mobile application, regardless of how many users have this application installed. If you develop your own mobile application, you must configure it for use by creating a record for it in the Push Application (sys_push_application) table. By default, the ServiceNow mobile application is automatically set up and ready to use.

1. Navigate to System Notification > Email > Push Application.
2. Fill out the fields on the form (see table).
3. Click Submit.
A push application is a mobile app that can receive push notifications from a ServiceNow instance and specify how to handle push messages and feedback.

More info

Display Name: ServiceNow Mobile Application

Name: ServiceNowPushApp

Push: Direct

Certificate

Sandbox Certificate

Update Delete

Push Notification Message Contents

Push Default Registrations (170)

Push app = ServiceNow Mobile Application
### Push Application form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>Enter a descriptive name for the application.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter a descriptive name, without spaces, for the application.</td>
</tr>
<tr>
<td>Push</td>
<td>Select an option:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Direct</strong>: Send push notifications directly to the push service without going through an intermediary. If you select this option, you must specify an X.509 Certificate or a GCM API key.</td>
</tr>
<tr>
<td></td>
<td>- <strong>REST API</strong>: Not applicable to custom push apps.</td>
</tr>
<tr>
<td></td>
<td>- <strong>None</strong>: Do not enable push notifications for this application.</td>
</tr>
<tr>
<td>Feedback</td>
<td>Select an option:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Apple</strong>: Send push notifications directly to the APNs without going through an intermediary.</td>
</tr>
<tr>
<td></td>
<td>- <strong>REST API</strong>: Not applicable to custom push apps.</td>
</tr>
<tr>
<td></td>
<td>- <strong>None</strong>: Do not handle feedback for this push application.</td>
</tr>
<tr>
<td>Apple</td>
<td>The X.509 Certificate and Sandbox Certificate you created on the Apple notifications portal. The certificate enables a device to talk to the APNs. This option appears only if you select Direct for the Push field.</td>
</tr>
<tr>
<td>Google</td>
<td>Select the GCM API key you obtained from Google for the Android push notification.</td>
</tr>
</tbody>
</table>

### Create push message content

Create push message content that contains the JSON content in the push notification payload.

**Create push message content**

Push message content specifies additional JSON content in the push notification payload that is sent to the push provider.

You must know how to use JSON with push messages.

Role required: admin or push_admin
Push message content defines the style of push notification that can be sent out for your custom app. You can add custom content, such as a picture, icons, or action buttons for the user to respond to the notification. Use the following variables in the script:

- **current**: properties of the current record.
- **message**: push message sent as the body of the entire push content.
- **attributes**: object of the push message *attributes that you define*.

1. Navigate to **System Notification > Push > Push Message Content**.
2. In the Push Notification Message Contents table, click **New**.
3. Fill out the fields on the Push Notifications Message Content form (see table).
4. Click **Submit**.
Push notification message content specifies additional JSON content in the push notification payload that is sent to the push provider. Use this record to create the JSON content and specify the provider-specific values, such as a sound or badge.

The following variables are available for use in the script:
- `current`: access properties of the record that triggered this push notification, such as the fields on an incident record.
- `message`: access contents of the message that will be sent as the body of the push notification.
- `attributes`: access attributes defined for this push notification.

```javascript
var JSON = {
    "app": "{app}",
    "sound": "default",
    "record": {
        "table": current.getTableName(),
        "sys_id": current.sys_id
    }
};
```
### Notification Message form 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 the message content.</td>
</tr>
<tr>
<td><strong>Push app</strong></td>
<td>The push application the content can be used with.</td>
</tr>
<tr>
<td><strong>Push Message Generation</strong></td>
<td>Enter a script that determines the message content. See the example scripts.</td>
</tr>
<tr>
<td><strong>Related list</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Push Message Attribute Definitions</strong></td>
<td>Select the attributes that apply to this notification. Attributes can be a value or an action. These attributes are used as default values for the content items you create in the content script. However, any attributes you create with the push message can override these attributes. See <a href="#">Create a push message attribute definition</a> for information on creating attributes.</td>
</tr>
</tbody>
</table>

The following is an example of a content record that creates a two-button layout, one to approve something, such as a change request, and one to decline it.

```javascript
var json = {
    "table" : current.getTableName(),
    "sys_id" : current.sys_id,
    "template" : {
        "type": "2 button",
        "button1" : {
            "title" : "Approve",
            "action" : attributes.button_action,
            "parameters" : {
                "response" : "approve"
            }
        },
        "button2" : {
            "title" : "Decline",
            "action" : attributes.button_action,
            "parameters" : { "response" : "decline" }
        }
    }
};
```

**Define a push message attribute** to specify a default push action script or string that you can use in the push message content.

**Create a push message attribute definition**

Push message attribute definitions allow you to create reusable properties for push message content specification.

Role required: admin or push_admin
Use an attribute definition to specify a default push action script or string that you can then use in the push message content.

You can override these attributes by creating any *push message attribute values*.

1. Navigate to **System Notification > Push > Push Message Content**.
2. Select a content record or script record.
3. In the Push Message Attribute Definitions related list, click **New**.
4. Fill out the fields on the form (see table).
5. Click **Submit**.

### Push Message Attribute Definition form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute Name</td>
<td>Enter a descriptive name for the layout.</td>
</tr>
<tr>
<td>Attribute Type</td>
<td>Select the type of attribute:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Action</strong>: An action to take on the instance, as defined by a script.</td>
</tr>
<tr>
<td></td>
<td>- <strong>String</strong>: An arbitrary string to send as part of the message content.</td>
</tr>
<tr>
<td></td>
<td>The string can specify items like a button label in the 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.
Create an attribute value or action for a push message

Attribute values are associated with push messages to provide a way for the message to include certain types of information in the push notification.

Create default definitions on the Push Message Attribute Definitions related list of the Push Message Content form.

Role required: admin or push_admin

These push message attribute values override values that you set in an attribute definition on the Push Content form.

2. Select a message.
3. In the Push Message Attribute Values related list, click New.
4. Fill out the fields on the form (see table).
5. Click Submit.
Push Message Attribute Values form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute</td>
<td>Select a push message attribute definition.</td>
</tr>
<tr>
<td>Value/Action</td>
<td>Enter the value for the attribute or select the push action. This field changes to Value or Action depending on the type of attribute you select in the Attribute field.</td>
</tr>
</tbody>
</table>

(Optional) Create a push action to perform an action on the instance.

Create a push action

A push action is a server-side script that runs when the instance receives a response to an actionable push message.

Create a push action to perform an action on the instance. For example, you might have an actionable push message that lets the user approve a change request. The action that handles the response should update the Approval field on the relevant Change Request record.

You can use global variables or, optionally, current variables and parameters passed through the JSON content.

Role required: admin or push_admin

2. Fill in the form fields (see table).
3. Click Submit.
Push Notification Action form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name for the action.</td>
</tr>
<tr>
<td>Script</td>
<td>Enter the script.</td>
</tr>
</tbody>
</table>

Failed push notification messages

Push notification delivery might fail for various reasons. You can view which messages failed and requeue them to be sent out if necessary.

Role required: admin

**Note:** There is no way for the instance to guarantee or confirm push message delivery. For more information on how Apple handles push notifications, see the [Local and Remote Notification Programming Guide](https://developer.apple.com/documentation/user annotator) for Apple developers.

Messages can also fail to send for several reasons, such as a large message queue or other issue with the instance. You can use a system property to control how long the instance queues a push notification after it is triggered.

Push notification message payload size is limited by provider:

- Apple iOS: **2,048 bytes**
- Google: **4,096 bytes**

Your instance does not send push messages that exceed this limitation. System logs save any failed messages. For details on Apple payload limitations, see the [Local and Remote Notification Programming Guide](https://developer.apple.com/documentation/user annotator) for Apple developers.

1. Navigate to System Logs > Push Notifications.
   By default, the messages that were created today appear. You can change the filter if necessary. The Type column can have these values:
   - **failure**: The message could not be sent.
   - **pending**: The message is queued for processing.
   - **success**: The message was successfully sent, although not necessarily received by the mobile device.

2. Put any failed messages back into the queue to be resent by selecting the check boxes next to the failed messages, and then selecting Re-queue failed push notifications from the choice list.

3. If some push notifications continue to fail, consider increasing the value in the glide.push.notification.ttl_seconds property. See Push notification properties for more information.

Push notification retention

You can archive and eventually destroy push notifications that you no longer need or if your Push Notification table is excessively large.

Push notification retention is available starting with the Jakarta release.
Push notification archive and destruction plugins

The push notification archiving and destruction feature uses the Data Archiving and Push Retention plugins. The Data Archiving plugin must be active to archive and destroy push notification records. The Push Retention plugin provides a set of rules that specify when the system archives and destroys push notification records.

In new instances, the Push Retention plugin and associated archive and destroy rules are active by default. On upgraded instances, you must manually activate both the plugin and the archive and destroy rules. Be sure to review and approve the archive and destroy rules before activating them.

If your instance already has a process for managing push notification records, you do not need to activate the Push Retention plugin. If you want to replace your current process with Push Retention, be sure to deactivate the current process before activating the archive and destroy rules.

Archiving and destroying push notification records

Archiving means moving records from the Push Notification (sys_push_notification) table to the Push Notification Archive (ar_sys_push_notification) table when they exceed the archive rule time limit. Destroying means deleting records in the Push Notification Archive table when they exceed the destroy rule time limit.

Default archive and destroy rules

Push retention provides the following push archive rules:

- **Push Notification - Over a year old**: archives push notification records that were created more than 365 days prior to the current date.
- **Push Notification Archive - Over a year old**: destroys push notification records that have been archived for more than 365 days prior to the current date.

With these default settings, your messages are kept on the instance for a total of two years: one year in the Push Notification table, and one year in the Push Notification Archive table. At the end of the period, the system deletes the expired notification records from the Push Notification Archive table.

**Note:** By default these rules are active on new instances and inactive on upgrades. The system runs archive and destroy rules when you activate them.

Compatibility with other record management implementations

If you are already using another method for managing push notification records, such as table cleaners, you do not have to use the Push Retention feature. To prevent unexpected record deletion, avoid using multiple push notification management processes on the same instance at the same time.

**Note:** For assistance replacing your existing record management implementation with push notification retention, contact your professional services or sales representative.
Activate the Push Retention plugin

The Push Retention plugin (com.glide.push_retention) provides the retention policy for push notifications, so that you can specify when the system archives and destroys push notification records.

Role required: admin

The Push Retention plugin requires the Data Archiving 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 Only related link on the System Plugin form.

5. Click Activate.

Archive push notifications manually

You can manually archive push notifications on demand instead of waiting for the instance to archive them based on a scheduled job.

Role required: admin

Push retention provides these push notification archive rules:

- **Push Notification - Over a year old**: archives push notification records that were created more than 365 days prior to the current date.
- **Push Notification Archive - Over a year old**: destroys push notification records that have been archived for more than 365 days prior to the current date.

You can manually archive push notification messages that meet the default archive and destroy rules or any additional archive rules that you create.

1. Navigate to System Archiving > Archive Rules.
2. Open the push notification archiving rule, for example Push Notification - Over a year old
3. Click Recalculate Estimate to see how many records in the Push Notification (sys_push_notification) table are going to be archived. The estimate appears in the Record estimate field.
4. Click Run Archive Now.
Subscription-based notifications

Subscription-based notifications enable users to proactively subscribe to items that interest them and unsubscribe from messages that are not mandatory.

Users can also specify additional notification channels that each of their notifications can be configured to use.

Before users can manage the notifications that are sent to them, administrators must create email notifications to which users can subscribe. Administrators can also make subscription-based notifications mandatory so users cannot unsubscribe to them. Then users can subscribe or unsubscribe to the notifications, and add schedules and filters to the subscription to limit the notifications that can be received.

Starting with the Helsinki release, notifications that administrators mark as subscribable are automatically available in user notification settings.

Administrators should create subscription-based notifications when they do not want to specify users for a notification and want to let users proactively subscribe to the notification.

Note: Subscription-based notifications are not domain aware and cannot support domain-specific settings.

Subscriptions 2.0 plugin

The Subscription Based Notifications 2.0 plugin must be active to use subscribable notifications. This plugin is active by default on all new and upgraded instances.

The plugin installs the Notification Subscription (sys_notif_subscription) table, which holds user subscriptions to all notifications.

Subscriptions and notification preferences

Users can subscribe to notifications available to them through their notification preferences. In the UI16 interface, all users can set and modify their notification preferences through the Notifications tab of the System Settings window. In the UI15 interface and earlier, admins and users set their notification preferences through the Notification Preferences link in the User form.

User notification preferences in UI16

You can set your own notification preferences, including personal subscriptions and channels (devices) for receiving them. All users can set these preferences through the Notifications tab of the System Settings window.

With the Notifications tab, you can:

- Use a global switch to enable or disable all your notifications.
- Enable or disable a particular channel for receiving notifications, as well as create, edit, or delete channels.
- Control the notifications that you receive and apply conditions to restrict notification delivery.
- Create personal notifications, which are subscriptions to notifications that are important to you.
Comparison between notification preferences in UI16 and earlier interfaces

In new and upgraded instances that use the UI16 interface, the System Settings window is the central location for managing your notification preferences. The Notification Preference User Interface plugin (com.glide.notification.preference.ui) is activated by default.
Notification preferences in UI16 interface

In UI15 and earlier interfaces:

- Users set notification preferences through the **Notification Preferences** link in the User form (Self service > My Notification Preferences).
Admins created user devices and set notification preferences for users through the Notification Preferences link in the User form, accessed through the User Administration module (User Administration > Users).

**Note:** Admins can revert to the UI15 notification preferences interface by setting the glide.notification.preference.UI.enabled property to false.

### Manage your notification preferences in UI16

To access your notification preferences, click the gear icon (⚙️) in the banner frame, and in the System Settings window, click the **Notifications** tab. You can also access the System Settings by navigating to Self Service > My Notification Preferences.

![Notifications tab in System Settings window](image-url)
In the **Notifications** tab, use the following settings to manage your notifications:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow notifications</td>
<td>Global switch for enabling or disabling all notifications.</td>
</tr>
<tr>
<td>Notification channels</td>
<td>List of your channels for receiving notifications. Use this section to:</td>
</tr>
<tr>
<td></td>
<td>• Enable or disable a channel by using its toggle switch. If you disable a channel, notifications are not delivered through that channel.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Add channels</strong> using the <strong>Create Channel</strong> option.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Modify channel information</strong>. Click the channel row or the right arrow (&gt;) next to the appropriate channel to edit or delete it.</td>
</tr>
<tr>
<td>Notifications by category</td>
<td>List of notification categories that identify and group related notifications. Each category contains the notifications that you can subscribe to.</td>
</tr>
<tr>
<td></td>
<td>To view the notifications in a given category, click the category row or the right arrow (&gt;) next to the appropriate category. You can:</td>
</tr>
<tr>
<td></td>
<td>• Edit a notification.</td>
</tr>
<tr>
<td></td>
<td>• Enable or disable channels for the selected notification.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Apply notification conditions</strong>, such as schedules and filters, that affect the delivery of the notification.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Create personal notifications</strong>, which are subscriptions to specific notifications that matter to you.</td>
</tr>
</tbody>
</table>

**Create notification channels**

You can add channels to receive your notifications. A notification channel is an email account or voice message system that you have access to.

Role required: user

Notification channels include email addresses, service providers for SMS messages, and mobile applications. You can create voice notification channels to support applications like Notify.

**Note:** If you are using the ServiceNow mobile application or a custom push application, you do not need to create a push channel for your mobile device. The system automatically creates a channel for the mobile app after you initially log in to your instance from your mobile device.

1. Click the gear icon (⚙️) in the banner frame to open the System Settings window, and click the **Notifications** tab.
2. Click **Create Channel**.
3. Complete the fields on the New Channel form.
## ServiceNow Jakarta Now Platform Capabilities

### System Settings
- General
- Theme
- Lists
- Forms
- Notifications
- Developer

### Notifications

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A descriptive name for the channel, such as the device or email account.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Type</td>
<td>The type of channel:</td>
</tr>
<tr>
<td></td>
<td>• Email: for email messages.</td>
</tr>
<tr>
<td></td>
<td>• SMS: for SMS messages.</td>
</tr>
<tr>
<td></td>
<td>• Voice: for phone messages.</td>
</tr>
<tr>
<td></td>
<td>Note: All users with an email address have a primary email channel, which</td>
</tr>
<tr>
<td></td>
<td>is created automatically after a notification is sent to them.</td>
</tr>
<tr>
<td></td>
<td>If you are using the ServiceNow mobile application or a custom push</td>
</tr>
<tr>
<td></td>
<td>application, the system automatically creates a channel for the mobile app</td>
</tr>
<tr>
<td></td>
<td>after you initially log in to your instance from your mobile device.</td>
</tr>
<tr>
<td>Email address</td>
<td>The email address of the channel.</td>
</tr>
<tr>
<td>Phone number</td>
<td>The phone number for SMS messages or for voice messages.</td>
</tr>
<tr>
<td>Service provider</td>
<td>The service provider for SMS messages.</td>
</tr>
</tbody>
</table>

4. Click **Save**. The system creates and enables the channel, and adds it to the list of notification channels.

To receive notifications on your new notification channel, you must enable the channel for individual notifications. After you enable the channel for a notification, you can set conditions to further control the notifications that you receive on the channel. For more information, see **Apply notification conditions**.

**Modify notification channels**

You can update channel information for your notifications.

Role required: none

1. Click the gear icon (⚙️) in the banner frame to open the System Settings window, and click the **Notifications** tab.
2. In the Notification Channels section, click the channel row or the right arrow (►) next to the channel name.
3. In the Edit Channel form, update the fields (see **Create notification channels** for descriptions of the form fields).
4. Click **Save**.

The system updates and saves the channel information that you modified.

**Delete a notification channel**

Delete a notification channel so that you no longer receive notifications through the channel.

Role required: admin

1. Click the gear icon (⚙️) in the banner frame to open the System Settings window, and click the **Notifications** tab.
2. In the Notification Channels section, click the channel row or the right arrow (>) next to the channel name.

3. On the Edit Channel form, click Delete.

The system deletes the channel from the list of notification channels and no longer delivers notifications to that channel.

**Apply notification conditions**

You can enable or disable the delivery of individual notifications by channel, as well as apply different conditions that control the notifications you receive.

Role required: user
You can choose preconfigured schedules and filters that determine when you receive your notifications. You can also set more advanced filter conditions to limit the notifications you receive.

1. Click the gear icon (⚙️) in the banner frame to open the System Settings window, and click the Notifications tab.

2. Select the notification:
   a) In the Notifications By Category section, click the row or right arrow (►) of the category that you want to view.
   b) In the list of notifications for the category, click the row or right arrow (►) next to the notification that you want to edit.

3. To enable or disable the channel on which the notification is received, click the switch for the channel.
   The notification is enabled when the switch is green and disabled when the switch is grey. If you previously disabled an entire channel, you cannot enable that channel for the notification.

4. To set more criteria for notification delivery, click the row or the right arrow (►) next to the channel for the notification.

5. Complete the Apply Conditions form (see table).
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule</td>
<td>Select a schedule that determines when the notification can and cannot be received.</td>
</tr>
<tr>
<td>Filter</td>
<td>Select a pre-configured filter with the criteria that determines when the notification can be sent. For example, you might select a filter whose conditions send notifications when an incident with a priority of <strong>1 - Critical</strong> is opened for a network issue.</td>
</tr>
<tr>
<td>Advanced filter</td>
<td>Select this check box to use the condition builder to create additional criteria. When you select the check box, the <strong>Table</strong> and <strong>Conditions</strong> fields are displayed.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Table</td>
<td>Select the table for the notification. For example, if you selected an incident-related notification, you might select the Incident (incident) table.</td>
</tr>
<tr>
<td>Conditions</td>
<td>Define as many conditions as needed to limit the notifications you receive. For example, you can choose to be notified only when an incident alert is created for a specific configuration item.</td>
</tr>
</tbody>
</table>

6. Click **Save**.
   To navigate back, click the left arrow (⟨) at the top of the Notification form.

**Create personal notifications**

You can create personal notifications, which are subscriptions to notifications that are important to you. You can apply conditions that control specific content included in your personal notification and also enable or disable the channels for delivery.

Role required: user

A personal notification is a subscribable notification that you can customize. You can assign the notification a name that is meaningful to you and filter the information received in that notification.

1. Click the gear icon (🛠) in the banner frame to open the System Settings window, and click the Notifications tab.
2. Click **Create Personal Notification**.
3. Complete the New Personal Notification form (see table).
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A descriptive name for your personal notification. Use a meaningful name to</td>
</tr>
<tr>
<td></td>
<td>distinguish it from system notifications.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Notification</td>
<td>The notification to subscribe to. You can subscribe only to notifications that are configured to allow subscriptions. Depending on the notification you select, the Table, Affected record, and Send when fields are displayed.</td>
</tr>
<tr>
<td>Table</td>
<td>The database table that the notification is linked to.</td>
</tr>
<tr>
<td>Affected record</td>
<td>The specific record that the notification is based on. This field appears when you select a notification that has an affected record (for example, a notification for a problem record that has multiple affected CIs). Click the lookup icon, select the table and specific document (record) in that table, and click OK.</td>
</tr>
<tr>
<td>Send when</td>
<td>Another condition that must be met to send the notification. For example, you might create a filter whose conditions send notifications when an incident with a priority of 1 - Critical is opened for a network issue.</td>
</tr>
</tbody>
</table>

4. Click Save. The system creates the personal notification and adds it to the appropriate notification category.

In the following example, notice the category in which the system placed the personal notification.
5. Enable or disable the channels for your personal notification.
6. Navigate back to the list of notifications for the category by clicking the left back arrow («) at the top of the form.
   Notice that your Personal Notifications are listed above the System Notifications in the given category.
7. Navigate back by clicking the left back arrow («) at the top of the form or by clicking the Notifications tab.

User notification preferences in UI15 and earlier

In UI15 and earlier interfaces, use the Notification Preferences link in the User form to manage the notifications that you can subscribe to.

The following instructions explain how to use Notification Preferences to manage notifications.

Set up a notification device in UI15 and earlier

You can add devices for a user to receive notifications. A device is a mobile device, email account, or voice message system that the user has access to.
Role required: admin

Notification devices include email addresses, service providers for SMS messages, and mobile applications.

1. Navigate to User Administration > Users.
2. Select a user.
3. Click Notification Preferences.
4. Click Create New Device.
5. Fill in the fields on the form (see table).
6. Click Submit.

### New Device form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A descriptive name of the device or account.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of device:</td>
</tr>
<tr>
<td></td>
<td>- Email: for email messages.</td>
</tr>
<tr>
<td></td>
<td>- SMS: for SMS messages.</td>
</tr>
<tr>
<td></td>
<td>- Mobile: for push notifications.</td>
</tr>
<tr>
<td>Email address</td>
<td>The user’s email address.</td>
</tr>
<tr>
<td>Mobile application</td>
<td>The mobile application for push notifications.</td>
</tr>
<tr>
<td>Phone number</td>
<td>The user’s phone number for SMS messages.</td>
</tr>
<tr>
<td>Service provider</td>
<td>The service provider for SMS messages.</td>
</tr>
<tr>
<td>User</td>
<td>The user’s record in the system.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Order</td>
<td>A number that determines which device receives the notification when multiple devices are configured. The device with the lowest number receives the notification.</td>
</tr>
<tr>
<td>Active</td>
<td>A flag that indicates if the device is active.</td>
</tr>
<tr>
<td>Related list</td>
<td></td>
</tr>
<tr>
<td>Notification Device Variables</td>
<td>Additional, optional attributes of an SMS device used inside an advanced script from the SMS service provider. These attributes are generally used to deliver SMS notifications to an internal SMS distribution technology. This advanced scripting procedure is not necessary for configuring external SMS providers.</td>
</tr>
</tbody>
</table>

**Note:** If you inactivate a device, it still appears in the user preferences, but the switches that allow users to select the notifications are grayed out for that device column.

**Edit a notification device in UI15 and earlier**

All users can edit their notification preferences, including notification devices.

Role required: any user

1. Navigate to **Self-Service > My Profile**.
2. Click **Notification Preferences**.
3. Click the name of the existing device.

The device form opens allowing you to make certain modifications, depending on your user role. See [Set up a notification device in UI15 and earlier](#) for a description of all fields.

**Add personal subscriptions in UI15 and earlier**

After setting up your devices, you can subscribe to notifications that are configured as subscribable.

The Subscription Based Notifications 2.0 plugin must be active.

If you have subscribed to messages, your list of notification messages can build over time. You can create preferences for how and when these messages are delivered, or unsubscribe to messages that are not configured as mandatory.

**Note:** Conditions that you apply to personal subscriptions do not override the filters that the administrator creates for the subscribable notifications. Your conditions are evaluated.
after the conditions on the subscribable notification are met. If the notification filter set by
the administrator fails, the filter conditions on your personal subscription are not evaluated.

1. Navigate to Self-Service > My Profile to open your user profile.
2. Click the Notification Preferences related link.
The Notification Preferences page opens. You can see your personal subscriptions and the
general notifications that you are subscribed to.
3. Click Subscriptions.
4. Click Add Personal Subscriptions.
5. Fill in the fields as described in the table.

Add Personal Subscriptions

Add personal subscriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A descriptive name for the subscription.</td>
</tr>
<tr>
<td>Notification</td>
<td>The notification to subscribe to. You can only subscribe to notifications that are configured to allow subscriptions.</td>
</tr>
<tr>
<td>Table</td>
<td>The table that the incident is configured to run on. You cannot modify the table from this form. To select another table, configure the notification. See <a href="#">Create an email notification</a>.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box indicating whether the subscription is active. Users can receive notifications for subscriptions only if the subscription is active. If it is not active, the on-off switch for the subscription is set to off and is read-only.</td>
</tr>
<tr>
<td>Send to</td>
<td>The devices that this subscription is sent to. Selecting the devices in this field is the same as turning on the switch for the subscription on the Subscriptions page.</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
Affected record | The specific record that the subscription is based on. Click the lookup icon, and then select the table and the specific record in that table.
Send when | Another condition that must be met to send the notification. For example, you might select a filter whose conditions send notifications when an incident with a priority of 1 - Critical is opened for a network issue. The system evaluates the conditions in this filter after the conditions set in the notification filter by the administrator.

6. Click Submit.
7. You can turn the subscription for active subscribable notifications on or off using the switch on the Subscriptions management section of the Notification Preferences page.

![Subscription and Primary Email](image)

**Personal subscriptions**

Personal subscriptions are saved in the Notification Subscriptions (sys_notif_subscription) table. The records in this table are made active or inactive when you click the switch to subscribe or unsubscribe from the notification.

8. You can edit the subscription at any time by clicking Edit next to it.

**Select notifications in UI15 and earlier**

Administrators can configure notification preferences for each user and users can also select which notifications they want to receive for various devices.

1. Navigate to **Self-Service > My Profile** to select your own notifications, or if you have admin access, navigate to **User Administration > Users** to select notifications for another user.
2. Click a user record to open it.
3. On the User form, click **Notification Preferences** under Related Links.

The notification preferences page appears. The preferences pages show all the notifications available to the user and the devices that the user has configured, such as email or mobile phone. If a user does not have read access to the table on which the notification is based, the notification does not appear.

Every user has the **Primary email** device, where subscriptions to email notifications can be enabled.
Modify notifications for a user device in UI15 and earlier

After you set up the devices through which users receive notifications, you can assign the notifications to each device and add advanced conditions to limit what notifications are received.

Role required: admin

1. On the Notification Preferences page for a user, find the notification from the list of notifications.
2. Click Edit next to the notification. The preferences for that notification appear.
3. Fill in the fields on the form (see table).
4. Click Submit.
Notification preferences for a user’s device

Form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notification Message</td>
<td>Select the notification. Related fields appear for certain notifications. For example, if you select <strong>CI affected</strong> or <strong>Location affected</strong>, a field appears for selecting the CI or the location. Duplicate messages are not permitted on a device.</td>
</tr>
<tr>
<td>Device</td>
<td>Modify the device if necessary.</td>
</tr>
<tr>
<td>Schedule</td>
<td>Select a schedule that determines when the notification can and cannot be received.</td>
</tr>
</tbody>
</table>
### ServiceNow Jakarta

#### Now Platform Capabilities

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>Select a pre-configured filter with the criteria that determines when the notification can be sent. For example, you might select a filter whose conditions send notifications when an incident with a priority of 1 - Critical is opened for a network issue. The system evaluates the conditions in this filter after the conditions in the notification filter set by the administrator. This field is not available when an advanced filter is configured.</td>
</tr>
<tr>
<td>Advanced filter</td>
<td>Select this option if you want to use the condition builder to create additional criteria. When you select the check box, the Table and Conditions fields replace the Filter field.</td>
</tr>
<tr>
<td>Table</td>
<td>Select the table for the notification. For example, if you select the CI affected notification message, you might select the Incident (incident) or Change Request (change_request) table. This field appears when you check the Advanced filter check box.</td>
</tr>
<tr>
<td>Conditions</td>
<td>Define as many conditions as needed to limit the notifications you receive.</td>
</tr>
</tbody>
</table>

#### Create a service provider

Administrators can configure service providers for devices that use SMS.

**Role required:** admin

Administrators also have the option of configuring how a device’s service provider affects the construction of the device’s email address.

1. Navigate to the Notification Service Provider (cmn_notif_service_provider) table by typing `cmn_notif_service_provider.list` in the application navigator filter.
2. Fill out or change the fields on the form (see table).
3. Click Update.
4. Click Save on the Notification Preferences page.
## The Notification Service Provider form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Configured name of the service provider.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of device, in this case SMS.</td>
</tr>
<tr>
<td>Active</td>
<td>Enables or disables this notification device.</td>
</tr>
<tr>
<td>Advanced notification</td>
<td>Removes all the previous options and displays the Advanced script field.</td>
</tr>
<tr>
<td>Advanced script</td>
<td>Used for custom notifications that run a script rather than construct a traditional SMS/email. This is generally used when all outbound SMS messages must run through a central SMS hub, as opposed to being sent directly from the instance to the SMS provider. Advanced users can construct a script in this field that will send a notification to an old style numeric pager that cannot receive SMS communications. This field is rarely used and employs advanced scripts. Contact your representative to assist you with any advanced SMS scripting.</td>
</tr>
<tr>
<td>Construct address manually</td>
<td>Removes the prefix and suffix options and displays the Construction script field.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Construction script</td>
<td>Allows you to script the email address construction as you would in a business rule. For example, abc + current.phone_number + <a href="mailto:def@text.att.net">def@text.att.net</a> would construct an email address of <a href="mailto:abc222334444def@text.att.net">abc222334444def@text.att.net</a>. NOTE: Current is a reference to the device, not the service provider, hence the current.phone_number variable that uses the device's phone_number value.</td>
</tr>
<tr>
<td>SMS Provider Email Prefix</td>
<td>Places the provided text before the device's specified phone number; for example: <a href="mailto:PREFIX222334444@text.att.net">PREFIX222334444@text.att.net</a></td>
</tr>
<tr>
<td>SMS Provider Email Suffix</td>
<td>Places the provided text after '@' sign; for example: 222334444@SUFFIX</td>
</tr>
<tr>
<td>Notification Device Variables</td>
<td>Additional, optional attributes of an SMS device used inside an SMS service provider's Advanced script. This is generally used to deliver SMS notifications to an internal SMS distribution technology. This is an advanced scripting procedure and is not necessary for configuring external SMS providers.</td>
</tr>
</tbody>
</table>

### Select a service provider

You can configure how a device's service provider affects the construction of the device's email address.

Role required: admin

1. Navigate to User Administration > Users and open any user's record.
2. Under Related Links, click Notification Preferences, and then click an SMS notification device.
3. If no SMS device is present, click New Device and configure one.
4. Select the appropriate service provider, and then click the reference icon for the Service provider field. The service providers are saved in the Notification Service Provider (cmn_notif_service_provider) table. Only active providers are visible.

### SMS notification advanced scripting

You can use these objects and their attributes in your advanced notification scripts on the SMS Notification Service Provider form.

**Objects and attributes**

<table>
<thead>
<tr>
<th>Object</th>
<th>Example attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>current</td>
<td>• current.number</td>
</tr>
<tr>
<td></td>
<td>• current.assigned_to</td>
</tr>
<tr>
<td></td>
<td>• current.company</td>
</tr>
<tr>
<td></td>
<td>• current.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>Object</th>
<th>Example attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>email</td>
<td>• email.notify</td>
</tr>
<tr>
<td></td>
<td>• email.sourceTable</td>
</tr>
<tr>
<td></td>
<td>• email.contentType</td>
</tr>
<tr>
<td></td>
<td>• email.attachments</td>
</tr>
<tr>
<td></td>
<td>• email.HTML</td>
</tr>
<tr>
<td></td>
<td>• email.dataVersionHeader</td>
</tr>
<tr>
<td></td>
<td>• email.UID</td>
</tr>
<tr>
<td></td>
<td>• email.allowSavingNoRecipientEmail</td>
</tr>
<tr>
<td></td>
<td>• email.recipients</td>
</tr>
<tr>
<td></td>
<td>• email.ignore</td>
</tr>
<tr>
<td></td>
<td>• email.save</td>
</tr>
<tr>
<td></td>
<td>• email.headers</td>
</tr>
<tr>
<td></td>
<td>• email.sysID</td>
</tr>
<tr>
<td></td>
<td>• email.attachmentLimits</td>
</tr>
<tr>
<td></td>
<td>• email.class</td>
</tr>
<tr>
<td></td>
<td>• email.sysId</td>
</tr>
<tr>
<td></td>
<td>• email.textBody</td>
</tr>
<tr>
<td></td>
<td>• email.hashCode</td>
</tr>
<tr>
<td></td>
<td>• email.weight</td>
</tr>
<tr>
<td></td>
<td>• email.equals</td>
</tr>
<tr>
<td></td>
<td>• email.logEmail</td>
</tr>
<tr>
<td></td>
<td>• email.reset</td>
</tr>
<tr>
<td></td>
<td>• email.wait</td>
</tr>
<tr>
<td></td>
<td>• email.body</td>
</tr>
<tr>
<td></td>
<td>• email.SMSText</td>
</tr>
<tr>
<td></td>
<td>• email.watermark</td>
</tr>
<tr>
<td></td>
<td>• email.textBodyLegacy</td>
</tr>
<tr>
<td></td>
<td>• email.sourceHeader</td>
</tr>
<tr>
<td></td>
<td>• email.instance</td>
</tr>
<tr>
<td></td>
<td>• email.instance</td>
</tr>
<tr>
<td></td>
<td>• email.importance</td>
</tr>
<tr>
<td>device</td>
<td>• device.service_provider</td>
</tr>
<tr>
<td></td>
<td>• device.group</td>
</tr>
<tr>
<td></td>
<td>• device.order</td>
</tr>
<tr>
<td></td>
<td>• device.sys_id</td>
</tr>
<tr>
<td></td>
<td>• device.sys_updated_by</td>
</tr>
<tr>
<td></td>
<td>• device.sys_created_by</td>
</tr>
<tr>
<td></td>
<td>• device.primary_email</td>
</tr>
<tr>
<td></td>
<td>• device.schedule</td>
</tr>
<tr>
<td></td>
<td>• device.name</td>
</tr>
<tr>
<td></td>
<td>• device.sys_created_on</td>
</tr>
<tr>
<td></td>
<td>• device.email_address</td>
</tr>
<tr>
<td></td>
<td>• device.active</td>
</tr>
<tr>
<td></td>
<td>• device.phone_number</td>
</tr>
<tr>
<td></td>
<td>• device.sys_mod_count</td>
</tr>
<tr>
<td></td>
<td>• device.sys_updated_on</td>
</tr>
<tr>
<td></td>
<td>• device.user</td>
</tr>
<tr>
<td></td>
<td>• device.sys_meta</td>
</tr>
<tr>
<td></td>
<td>• device.type</td>
</tr>
</tbody>
</table>
Make a notification mandatory

To prevent users from turning off or deleting a subscription to a notification, make the notification mandatory.

Role required: admin

When you make a notification mandatory, the notification is locked in user notification preferences, preventing the user from removing or unsubscribing to the notification, filtering it, or changing the schedule.

Users receive mandatory notifications even if they disable notifications.

Note: Mandatory notifications apply to only the primary device of the user. You cannot make a notification mandatory for secondary devices.

1. Navigate to System Notification > Email > Notifications.
2. Open the appropriate notification.
3. Configure the form and add the Mandatory field. This field does not display by default.
   a) Click the context menu icon ( ) and select Configure > Form Layout.
   b) Using the slushbucket, select the Mandatory field and the order in which you want the field to appear.
   c) Click Save.
4. Select the Mandatory check box.

When a user checks their notification preferences, the control button for the mandatory notification is on and is read only.
**Force a notification to be sent**

To force a notification to be sent to the specified users, enable forced delivery.

Role required: admin

Forcing a notification means that the relevant users receive the notification, even if they have not subscribed to the notification or have turned off the subscription. In addition, the users receive the notification even if the Notification field is set to Disable.

| Note: Forced delivery applies to only the primary device of the user. You cannot force a notification to be sent to secondary devices. |

1. Navigate to System Notification > Email > Notifications.
2. Open the appropriate notification.
3. Configure the form and add the Force delivery field.
4. Select the Force delivery check box.
5. Click Update.

Unlike using the Mandatory option, forcing the delivery does not lock the user’s preference or prevent the user from unsubscribing from the notification.

**Create a notification filter**

Notification filters enable a user to control the delivery of messages by creating special conditions on multiple tables in a single, reusable filter.

Role required: admin

For example, you can create a filter that controls message delivery when active incidents, problems, and change requests for network issues reach a critical state. For UI15 and earlier interfaces, notification filters are available for selection in the Filter field of a user’s Notification Preferences form. For UI16, filters for notifications or channels are set through the Notifications tab of the System Settings window. For details, see Apply notification conditions.

| Note: The system applies the user’s filter conditions after the administrator’s conditions have been evaluated. If the administrator’s conditions fail, the system ignores notification filters. |

1. Navigate to System Notification > Email > Notification Filters and create a record.
2. In the Notification conditions related list of the new record, create and submit filter conditions on one or more tables.
3. Repeat the procedure to create additional conditions on other tables for this filter.
Filter device notifications using a schedule

You can associate devices, such as Email, SMS, and Voice, to schedules that define when the devices can and cannot receive notifications.

Role required: admin

Notifications that are triggered outside of the scheduled days and times for the device are not queued up for delivery at a later time. For example, if an administrator selects the Weekdays schedule for an email device, the device receives email notifications triggered between Monday and Friday. If notifications are triggered on Saturday, they are not delivered to the device.

1. Define schedules as needed using System Scheduler > Schedules > Schedules.
2. Add or edit a device.
3. Configure the New Device for System Administrator form and add the Schedule field.
4. In the Schedule field, select the schedule for the device.
5. Click Submit.

Edit the schedule or filter of an existing notification message

You can update a schedule or filter that was previously created for an email notification.

Role required: admin

To edit the schedule or filter of an existing notification message:
1. In the Notification Preferences screen, click the message to edit.
   You cannot edit any attributes of a mandatory message.
2. Make the appropriate changes in the form.
3. Click Update.
Email unsubscribe

Administrators can add unsubscribe links to notifications so that users can stop receiving particular email messages.

The system offers two types of macros to create unsubscribe links.

- An unsubscribe link that creates an email message to the instance.
- An unsubscribe link that opens the notification preferences for the user on the instance.

Available unsubscribe macros

<table>
<thead>
<tr>
<th>Unsubscribe type</th>
<th>Macro used</th>
<th>Description</th>
<th>Available parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unsubscribe by email (Unauthenticated)</td>
<td>${NOTIF_UNSUB}</td>
<td>The system generates an HTML mailto hyperlink. When users click the link, their browser or email client creates a pre-formatted unsubscribe email message to the instance.</td>
<td>link_text: specify the text to display as a link within quotation marks.</td>
</tr>
<tr>
<td>Unsubscribe by notification preferences (Authenticated)</td>
<td>${NOTIF_PREFS}</td>
<td>The system generates an instance link directly to the notification preferences for this notification type.</td>
<td>link_text: specify the text to display as a link within quotation marks.</td>
</tr>
</tbody>
</table>

Administrators can add unsubscribe macros to any notification record type such as:

- Email layouts
- Email templates
- Email notifications

Unsubscribe by email

Unsubscribe by email requires the user email client or browser to create a pre-formatted email message containing these elements:

- The To field has the email address of the instance.
- The Subject starts with the string Unsubscribe from.
- The Body has a JSON string with a name-value pair of Unsubscribe and an array value that contains two more name-value pairs.
  - The notification_id parameter specifies the Sys ID of the notification the user wants to unsubscribe from.
  - The unsub_token parameter specifies an instance ID the system uses to verify that the email came from a ServiceNow instance.

Note: Some email clients and web browsers, such as GMail on Chrome, require extra client configuration to support mailto hyperlinks. Administrators can provide an alternative unsubscribe method for users whose email client or browser does not support mailto links. See RFC6068 for information about the mailto URI scheme.

The Unsubscribe from Notification inbound action processes the email and unsubscribes the sender from the listed notification.
**Note:** Unsubscribing by email message does not require users to authenticate with the instance first.

**Unsubscribe by notification preferences**

Unsubscribe by notification preferences requires the user's browser to navigate to the notification preferences page on the instance. After logging in, the system displays the notification preferences for this particular notification.

Users can set preferences for this notification such as disabling notifications for a particular device. Users must save their notification preferences for changes to take effect.

**Unsubscribe links**

This email layout adds several unsubscribe links to the bottom of each email notification.

```javascript
${NOTIF_UNSUB} from this notification by email or ${NOTIF_UNSUB+link_text="click here"}.
Manage your ${NOTIF_PREFS} or ${NOTIF_PREFS+link_text="click here"}.
```

When rendered in an email notification, the unsubscribe links only display the link text.
Sample email with unsubscribe links

If a user clicks the **Unsubscribe** link, the email client creates a message such as this:
Notify allows you to integrate with telephony providers such as the Twilio service to manage phone calls and SMS messages from within your instance.

**Notify with the Twilio service**

Notify allows you to send and receive phone calls and SMS messages from your instance using the Twilio telephony service.

Notify automatically creates a TwiML application in the Twilio service and configures the application to use the instance as an endpoint. Phone numbers associated with the Twilio subaccount are imported to Notify.

To manage phone numbers per instance, set up one Twilio subaccount for each instance and configure all relevant phone numbers for the instance under that subaccount.

The Notify plugin must be active to access the Notify product.

---

**Note:** Only one Twilio account (or subaccount) can be configured on Notify at a time.
Configure Notify with the Twilio service

You can configure Notify to use the Twilio telephony service.

You must have an SID and authentication token for an active Twilio account (https://www.twilio.com/).

**Important:** Ensure that each instance on which you configure Notify uses a different Twilio account. Each account specifies a unique SID, authentication token, telephone numbers, and endpoint. Using the same account across multiple instances may cause your Twilio service configuration to be overwritten.

**Note:** Account and subaccount are Twilio categorizations and both act the same for a ServiceNow instance.

Role required: notify_admin

1. Navigate to Notify > Twilio Configuration.
2. On the Twilio Account Properties page, enter your **Account SID**.

   **Note:** This value is only visible to users with the admin role.

3. Enter your **Auth Token**.

   **Note:** This value is only visible to users with the admin role.

4. Click **Connect**.

   If the account is not associated with an instance and the connection is successful, a read-only list of E.164 and short code phone numbers associated with this Twilio account appears. This list displays the phone number, supported capabilities such as voice or SMS, the country for each Twilio number, and the Notify number group to which the number belongs.

   If the account is already associated with an instance, the system displays an error message. To connect to this account, you must do one of the following:

   - *Disconnect the account from the instance*
   - Clear the request URLs on Twilio’s TwiML app

   **Note:** If you buy or release numbers on the Twilio account, open the configuration page again to refresh the list of numbers. Numbers removed from the Twilio service remain as Notify Number records, but with the **Active** field set to false. Use only active phone numbers for inbound or outbound communication.
Phone numbers and short codes are provided by Twilio once the account is successfully connect and are stored on the Notify Phone Numbers (notify_number) table. Assign each number to a number group. Number groups allow you to control which workflows run when using the phone numbers in each number group.

**Disconnect from a Twilio account**

If a Twilio account is already associated with a different system, disconnect the account from the other system before connecting to the current instance.

Role required: notify_admin

1. Navigate to **Notify > Twilio Configuration**.
2. On the Twilio Account Properties page, click **Disconnect**.
3. In the Disconnecting Twilio account pop-up window, click **OK**.

The account is disconnected from the instance. The system clears the **Account SID** and **Auth Token** fields and deactivates the list of associated phone numbers.

**Create a number group**

Number groups allow you to group Notify phone numbers and share workflows across grouped numbers.

Role required: notify_admin

Each phone number within Notify has an associated number group. Numbers within a group use the same workflows for handling incoming and outgoing calls and SMS messages.

Numbers associated with a group appear on the **Notify Phone Numbers** related list on the Notify Phone Number Group form.

1. Navigate to **Notify > Number Groups**.

2. Click **New**.
3. Enter a **Name**, and select **Notify: (Re)join Conference Call** for the **Incoming call workflow** field.
Incoming call workflows must run on the Notify Call (notify_call) table. Incoming and outgoing SMS workflows must run on the Notify Message (notify_message) or Global (global) tables.

Short codes can only be associated with SMS workflow groups. You cannot add an incoming or outgoing call to a short code group.

4. Click Submit.

**Associate a number to a number group**

After creating a number group, associate numbers with that group to use the selected workflows.

**Note:** Each phone number can only be associated with one number group.
Associate a number to a number group

Associate a Notify number to a number group to use inbound and outbound workflows.

Role required: notify_admin

1. Navigate to Notify > Numbers.

2. Click the listed phone number and assign it to a Number Group, as appropriate.

   Note: Each phone number can only be associated with one number group.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Number for the entry.</td>
</tr>
<tr>
<td>Phone number</td>
<td>E.164 phone number, if applicable.</td>
</tr>
<tr>
<td>Notify group</td>
<td>(Optional) Group to which this number is assigned.</td>
</tr>
<tr>
<td>Number owner</td>
<td>Service provider of the number.</td>
</tr>
<tr>
<td>Short Code</td>
<td>Short code number, if applicable.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box that indicates whether the number is active or not.</td>
</tr>
</tbody>
</table>

3. Click Update.

Outbound communication requirements

Outbound communications initiated through Notify, such as phone calls and SMS messages, must satisfy certain requirements.

These requirements apply to all outbound communications initiated through Notify, such as by using Notify workflow activities or the Notify JavaScript API.

Invalid numbers prevent Notify workflows from running and cause an error to be logged. Set the glide.notify.debug property to true to create detailed error logs.

Recipient number requirements

These requirements apply to any number that receives a Notify phone call or message.

- Calling country must be authorized from Twilio
- The number must be E.164 compliant
• The number must be different than the phone number used to initiate the call or message

Notify calls

As a Notify administrator, you can view a list of calls made to or from Notify.
To view a list of calls, navigate to Notify > Calls.

Call records are generated automatically when a user calls a Notify number, or when a user makes an outbound call through Notify. You cannot create call records manually. You can delete call records.

Note: Deleting a call record may result in cascade deletion of related records.

<table>
<thead>
<tr>
<th>Call status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No answer</td>
<td>The call is not answered, or if the number is configured for voicemail, a message is left on the voice mailbox.</td>
</tr>
<tr>
<td>In-progress</td>
<td>The call is answered and is active.</td>
</tr>
<tr>
<td>Completed</td>
<td>The conference call is completed.</td>
</tr>
<tr>
<td>Failed</td>
<td>The provided phone number is invalid.</td>
</tr>
</tbody>
</table>

How incoming Notify calls are processed

Notify processes incoming calls using workflow activities.

Any Notify activity that manages incoming phone calls creates a record on the Notify Workflow Activity (notify_wf_activity) table. Each notify_wf_activity record is associated with a single call. These records store JSON data detailing the actions to send to the telephony provider.

Notify processes incoming calls in the following way:

1. A person calls a Notify phone number.
2. Notify launches the incoming call workflow associated with that Notify phone number.
3. The workflow reaches a Notify activity and invokes the activity onExecute() function.
4. The activity creates a new notify_wf_activity record detailing any actions to take, with a State value of execute.
5. Notify sends the specified actions to the telephony provider.
6. The notify_wf_activity record State changes to processed.
7. The telephony provider sends a response.
8. Response arguments, such as user input or recording info, are stored as JSON data in the notify_wf_activity response_args field.
9. The notify_wf_activity State changes to complete.
10. The JSON data from the notify_wf_activity record is copied to the Last action field in the Notify call record that triggered the workflow.
11. The workflow invokes the onUpdate() function in executing activities.
12. The activity confirms that the associated notify_wf_activity record has completed, and changes the activity state to finished.
13. The workflow transitions to the next activity.

**Notify conference calls**

Notify allows you to connect multiple callers to a single conference call.

Conference call records are stored on the Notify Conference Call (notify_conference_call) table. Conference call participant records are stored on the Notify Participant (notify_participant) table. Conference call and participant records are created automatically when starting and connecting to a conference call. Most fields, such as the **Duration** of a call are set automatically using business rules.

**Note:** If a participant attempts to join a conference call using an invalid phone number, the caller is added to the participant list and the phone number is marked with a status of **Invalid**.

Notify administrators can manage conference call participants, such as by muting or kicking them.

Several conference call workflows are available by default. These workflows can be used for incoming and outgoing calls and incoming SMS messages. Conference call workflows are:

- Notify: (Re)join Conference Call
- Notify: Join Conference Call Via SMS

The number groups Conference Call Group and Notify On Task Group use these conference call workflows by default.

**Mute or kick a conference call participant**

You can mute or kick conference call participants.

Role required: notify_admin

Before starting this procedure, ensure there is an active conference call with one or more participants.

1. Navigate to **Notify > Conference Calls**.
2. Select a conference call.
3. In the **Notify Conference Call Participants** related list, select a participant.
4. Click **Mute** or **Kick**.

You can unmute a muted participant but cannot add a kicked participant back to the conference call. A kicked participant may rejoin the conference call, such as by calling in again.

**Using SMS with Notify**

You can send and receive SMS messages using Notify.

Use the Notify API sendSMS method, or using the send SMS workflow activity. Inbound and outbound SMS messages are stored on the Notify Messages (notify_message) table. Notify supports sending concatenated SMS messages. Messages that exceed 160 characters, or 70 unicode characters, are split into multiple messages. This may affect your total telephony cost as each message can incur a cost. Some mobile carries, such as Sprint, do not support concatenated SMS messages.
Properties for Notify

These are the properties related to Notify.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>sn_twilio_driver.max_conference_participants</code></td>
<td>Twilio max limit for number of participants in the conference call.</td>
</tr>
<tr>
<td><code>com.snc.iam.notify_number</code></td>
<td>The Notify number to use for conference calls.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This number needs to have a group configured with conference call workflows.</td>
</tr>
<tr>
<td><code>glide.notify.task.phone_number</code></td>
<td>Notify phone number used for sending SMS-s and starting conference calls from any record that belongs to the task table (or table that extends task table). The number must be entered in E.164-compliant format.</td>
</tr>
<tr>
<td><code>glide.notify.sms.max_concatenation</code></td>
<td>Maximum number of concatenated messages to receiver mobile phone.</td>
</tr>
</tbody>
</table>

Notify tables

Notify tables store information related to Notify.

<table>
<thead>
<tr>
<th>Tables</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Notify</strong></td>
<td><strong>Legacy Notify</strong></td>
</tr>
<tr>
<td>notify_conference_call</td>
<td>notifynow_conference_call</td>
</tr>
<tr>
<td>notify_call</td>
<td>notifynow_participant</td>
</tr>
<tr>
<td>notify_call_status</td>
<td>notifynow_participant</td>
</tr>
<tr>
<td>notify_participant</td>
<td>notifynow_participant</td>
</tr>
<tr>
<td>notify_participant_session</td>
<td>notifynow_participant_session</td>
</tr>
<tr>
<td>notify_message</td>
<td>notifynow_message</td>
</tr>
</tbody>
</table>
Notify call sequence

Business rules installed with Notify

Notify adds the following business rules.

<table>
<thead>
<tr>
<th>Business rule</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Call Workflows for Shortcodes</td>
<td>(notify_group)</td>
<td>Checks and displays an error if the call is being triggered by a short code.</td>
</tr>
<tr>
<td>Update Call Active State</td>
<td>(notify_call_status)</td>
<td>Updates the status of the call in notify_call_status with the status received from Twilio.</td>
</tr>
<tr>
<td>Business rule</td>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Update Conference Call Active State</td>
<td>(notify_participant)</td>
<td>Updates the active flag in notify_participant table. Also calculates the duration when the call is ended by a participant.</td>
</tr>
<tr>
<td>Update Participant Active State</td>
<td>(notify_participant_session)</td>
<td>Updates the active flag for the participant (notify_participant), and calculates the total time on the call upon disconnecting from the call.</td>
</tr>
<tr>
<td>Update Participant Session Active State</td>
<td>(notify_call)</td>
<td>Synchronizes the state of the call between notify_call and notify_participant_session. Upon disconnecting from the call, updates notify_participant_session with the duration of the call.</td>
</tr>
</tbody>
</table>

**Notify workflow activities**

Notify activities manage calls and SMS messages in Notify.

All Notify workflows that manage a phone call must run on the notify_call table. Call-related Notify activities can be added only to workflows where the **Table** field value is **Notify Call (notify_call)**.

You can identify if an outbound call was answered by a human or by an answering machine from within a Notify workflow by evaluating the **current.is_human** variable, such as with an **If** workflow activity. This variable is set by the telephony provider when an outbound call is answered. This variable is always true for inbound calls.

**Note:** Do not add a **Timer** activity between multiple Notify activities that interact with active phone calls.

**Important:** When creating a Notify workflow, set the workflow **If condition matches** field to **-- None --**. Notify controls which workflow to run based on the configured number groups.

**Join conference call workflow activity**

The **Join Conference Call** connects an incoming or outgoing call to a Notify conference call.

Notify includes the workflows Notify: (Re)join Conference Call and Notify: Join Conference Call Via SMS to demonstrate how to use the **join conference call** activity to connect inbound and outbound calls, and inbound SMS messages to a conference call.

**Input variables**

Input variables determine the initial behavior of the activity.
Input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced</td>
<td>Select this check box to display advanced configuration options.</td>
</tr>
<tr>
<td>Script</td>
<td>Specify advanced configuration options using JavaScript, such as if the new participant should be muted upon joining the conference call. You can access values from the workflow scratchpad.</td>
</tr>
</tbody>
</table>

Conditions

The conditions determine which transition comes after this activity. The `join conference call` activity does not specify any conditions by default.

You can add an error condition to this activity. The activity transitions through the error condition if the `conference_call` scratchpad variable is not set.

Scratchpad entries

The activity uses the workflow scratchpad to read persistent values.

Values read from scratchpad

<table>
<thead>
<tr>
<th>Scratchpad variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>workflow.scratchpad.conference_call</td>
<td>A GlideRecord for a single conference call record. A call processed by this activity is added to this conference call. If this value is not specified, the <code>join conference call</code> activity will log an error. When initiating an outgoing call workflow using the Notify API <code>call(String notifyPhoneNumber, String toPhoneNumber, GlideRecord conferenceCall)</code> method, this scratchpad value is set automatically to the conference call GlideRecord. For incoming call workflows, or workflows initiated using a different mechanism, you must explicitly set this scratchpad value.</td>
</tr>
</tbody>
</table>

Call workflow activity

The `Call` activity makes outbound phone calls using a Notify workflow.

Input variables

Input variables determine the initial behavior of the activity.
### Input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify Number</td>
<td>The Notify phone number to make the call from. When you initiate a call, the outgoing call workflow for the number group associated with this number runs.</td>
</tr>
<tr>
<td>Phone number to call</td>
<td>The E.164-compliant phone number to call.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Select this check box to use a script to determine number to call, and the Notify number to call from instead of using the Phone number to call and Notify Number variables.</td>
</tr>
<tr>
<td>Script</td>
<td>Define a script that controls which number to call. This script should return a string listing the Notify number sys_id, as well as the phone number to call, such as <code>{notify_number: 'sys_id', phone_number: '+316...'} </code></td>
</tr>
</tbody>
</table>

### Conditions

The conditions determine which transition comes after this activity. The call activity does not specify any conditions by default.

You can add an error condition to this activity. The activity transitions through the error condition if the call could not be set up due to invalid data returned by the advanced script.

### Send SMS workflow activity

The send SMS workflow activity to send short text messages using Notify to users' phones.

### Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From</td>
<td>Select the Notify phone number to use to send the SMS message.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Select this check box to use JavaScript to determine which numbers to send the message to, and the Notify number to use to send the message.</td>
</tr>
<tr>
<td>To</td>
<td>Select any number of users to send the message to. The user record must have a E.164-compliant phone number or notification device configured for SMS messages.</td>
</tr>
<tr>
<td>To (groups)</td>
<td>Select any number of groups to send the message to. All members of that group with an E.164-compliant phone number or SMS notification device receive the message.</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Message</td>
<td>Enter the message to send. You can add field values from the current record by using the <strong>Select variables</strong> box. You can also add values from the workflow scratchpad. If a field and a scratchpad variable have the same name, the field value is used. Because you can use variables in this message, it is not possible to determine the length of the message at design time. If the activity sends a message that is longer than supported by the telephony provider, the message is truncated and the instance logs a warning.</td>
</tr>
<tr>
<td>To (script)</td>
<td>Enter a script to determine which numbers to send the message to, and the Notify number to use to send the message. The script should return a JavaScript object with the format <code>{notify_number: &quot;...sys_id...&quot;, users: [...], groups: [...], numbers: [...]}</code>. Specify the users or groups to send the message to as an array of sys_id values. Specify other numbers as an array of E.164-compliant phone numbers. This field appears only if <strong>Advanced</strong> is selected.</td>
</tr>
</tbody>
</table>

### Conditions

The conditions determine which transition comes after this activity. This activity does not specify any conditions by default.

You can add an error condition to this activity. The activity transitions through the error condition if the Notify number used to make the call is not configured correctly or unable to send SMS messages, or if an error occurs while sending the SMS.

### Forward call workflow activity

The **Forward Call** activity forwards a Notify call to an E.164-compliant phone number. If the person receiving a forwarded call hangs up, the **forward call** activity completes and transitions to the next activity. Any further Notify activities in the workflow run for the caller only.

### Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone number to call</td>
<td>Enter the phone number to forward the call to.</td>
</tr>
<tr>
<td>Timeout (in seconds)</td>
<td>Enter the amount of time to wait for the call to be answered before hanging up.</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Record</td>
<td>Select this check box to record the conversation.</td>
</tr>
</tbody>
</table>

**Conditions**

The conditions determine which transition comes after this activity. The **forward call** activity does not specify any conditions by default.

You can add an error condition to this activity. The activity transitions through the error condition if the phone number to call is invalid.

**Input workflow activity**

The **Input** activity creates a phone menu by presenting a list of options on a Notify call.

**Input Variables**

Input variables determine the initial behavior of the activity.

**Input Variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of digits</td>
<td>Specify the maximum number of digits the caller can enter. A caller can enter fewer digits than the maximum and press the <strong>Finish key</strong> to complete the entry.</td>
</tr>
<tr>
<td>Finish key</td>
<td>Specify the key a caller can press on their phone when finished selecting a menu option.</td>
</tr>
<tr>
<td>Timeout (in seconds)</td>
<td>Specify the amount of time to wait before closing the menu automatically when the caller does not select a menu option.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Select this check box to use a script to build the phone menu, instead of using the activity conditions.</td>
</tr>
</tbody>
</table>
**Variable** | **Description**
--- | ---
**Script** | Define the script to build the phone menu. The script must specify an answer variable as a JavaScript object with the following format:

```javascript
answer = {
  1: {
    "say": "https://some_url.com/options/one.mp3",
    "myCustomData": "some data here"
  },
  2: {
    "say": "type 2 to speak to a representative",
    "language": "en-US",
    "myCustomData": "some more data here"
  }
};
```

The script may specify either a text-to-speech string and language code or the URL of a prerecorded message for each entry. You can also add optional attributes to store related information, such as myCustomData in the example above.

**Conditions**

The conditions determine the transition that comes after this activity.

The input activity does not specify any conditions by default. You must define conditions to build the phone menu. Each condition is one option on the phone menu. Notify reads the text from each condition Name to the caller, up to 100 characters per condition.

You can specify a language for each condition by prefixing the message with the language code, in the format xx-XX:<Message>. For example, add fr-CA: for Canadian French. Available languages are stored on the Notify Language [notify_language] table.

The condition that the activity transitions through depends on the digits entered by the caller. Set the condition Condition value to `parseInt(workflow.scratchpad.digits) == <expected digits>`. For example, to transition through a condition when the caller presses the number 3, set the Condition to `parseInt(workflow.scratchpad.digits) == 3`.

You can add an error condition to this activity. The activity transitions through the error condition if the advanced script returns an invalid value, or if the text to say for a condition is empty.

**Scratchpad Entries**

The activity uses the workflow scratchpad to write persistent values.

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>workflow.scratchpad.digits</td>
<td>The digits entered by the caller, as a string.</td>
</tr>
</tbody>
</table>
## workflow.scratchpad.menu<activity name>

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
</tr>
</thead>
</table>
| workflow.scratchpad.menu<activity name> | The entire `answer` variable, if using the advanced script option. You can access this menu from other activities after this activity successfully executes.  
For example, if the activity name is `choices`, you can access values from the menu using  

```javascript
var previousActivity = "choices";
var choicesMenu = workflow.scratchpad.menu[previousActivity];
var menuItem = choicesMenu[workflow.scratchpad.digits];  
// Selects the menu item based on the caller's input.
var selectedValue = menuItem.myCustomData;  
// get the custom data for the selected menu item.
```

## Hangup workflow activity

The **Hangup** activity disconnects an active Notify phone call.

You can use the **hangup** activity to disconnect only calls that have been answered. Use the **reject** activity to disconnect calls that have not been answered.

## Play workflow activity

The **Play** activity plays a sound file on a Notify call.

### Input Variables

Input variables determine the initial behavior of the activity.

#### Input Variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>Enter the URL of a sound file to play. If the URL is inaccessible, or if the audio file mime type is not supported by the telephony provider, the <strong>play</strong> activity is skipped.</td>
</tr>
<tr>
<td>Loop</td>
<td>Enter the number of times the sound file should play.</td>
</tr>
</tbody>
</table>

### Conditions

The conditions determine which transition comes after this activity. The **play** activity does not specify any conditions by default.
You can create an error condition to handle errors with the sound file. The activity transitions through the error condition if the specified sound file is not available, or has an unsupported mime type. Supported mime types are listed on the Notify Audio MIME Types (notify_mime_type) table.

**Record workflow activity**

The Record workflow activity records audio from a user on a Notify call.

**Input Variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max duration (in seconds)</td>
<td>Enter the maximum duration, in seconds, allowed for a recording.</td>
</tr>
<tr>
<td>Timeout (in seconds)</td>
<td>Enter the amount of time to wait before ending a recording automatically when the caller is silent.</td>
</tr>
<tr>
<td>Finish Key</td>
<td>Specify the key a caller can press on their phone to end the recording.</td>
</tr>
</tbody>
</table>

**Scratchpad Entries**

The activity uses the workflow scratchpad to store persistent values.

The record activity adds the recording variable to the workflow scratchpad. This variable stores metadata about the recording, such as URI, ID, and duration. You can access the following values from this variable.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>recording.recordingDuration</td>
<td>The duration of the recording, in seconds.</td>
</tr>
<tr>
<td>recording.from_number</td>
<td>The caller's phone number, including country code.</td>
</tr>
<tr>
<td>recording.notify_number</td>
<td>The Notify phone number used to respond to the call, including country code.</td>
</tr>
<tr>
<td>recording.recordingID</td>
<td>The ID used by the telephony provider to identify the recording.</td>
</tr>
<tr>
<td>recording.recordingURL</td>
<td>The URL from the telephony provider to access the recording.</td>
</tr>
</tbody>
</table>

**Reject workflow**

The Reject workflow activity rejects an incoming Notify call.

You can use the reject activity to disconnect only calls that have not yet been answered. Use the hang up activity to disconnect calls that have been answered.
Input variables

Input variables determine the initial behavior of the activity.

### Input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reason</td>
<td>Select a reason for rejecting the call, such as busy.</td>
</tr>
</tbody>
</table>

Say workflow activity

The **say** workflow activity allows you to play a message, using text to speech, on a Notify call.

**Input variables**

Input variables determine the initial behavior of the activity.

### Input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text to say</td>
<td>Specify the text to read.</td>
</tr>
<tr>
<td>Language</td>
<td>Select the language and locale to use when reading text.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Select this check box to use a script to define the language and message, instead of using the Text to say and Language values.</td>
</tr>
<tr>
<td>Script</td>
<td>Define a script to set what text is read on the call. The script must return a string that defines the language and the text to read. For example, to play an English-language message, return {language: 'en-US', text: 'Text to read'}.</td>
</tr>
</tbody>
</table>

Forward to notify client workflow activity

The **forward to notify client** workflow activity connects a phone call to a Notify WebRTC client.

**Input variables**

Input variables determine the initial behavior of the activity.

### Input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Select the user to connect the call to.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Select this check box to use a script to determine which client to connect to, instead of using the User variable.</td>
</tr>
</tbody>
</table>
### Conditions

The conditions determine which transition comes after this activity. The **Forward to Notify Client** activity does not specify any conditions by default.

You can add an error condition to this activity. The activity transitions through the error condition if there is an issue with the Notify client.

### Queue workflow activity

The **Queue** activity places an active Notify call in a queue.

Add the **Queue** activity to a workflow on the Notify Call (notify_call) table to put the current call on hold. This activity does not specify any input variables.

The queue that the call is added to is given a random ID.

### Notify activity event handlers

Notify workflow activities provide JavaScript functions that are invoked automatically when your telephony provider broadcasts certain events.

When a telephony provider such as the Twilio service broadcasts an event related to a Notify call, such as the caller hanging up, the event is processed by the workflow associated with that Notify call. All currently-executing Notify activities in that workflow invoke a JavaScript function associated with that event.

Not all activities that support an event provide a default event handler implementation. You can provide an implementation for those event handlers when creating custom Notify activities.

### Creating Notify activities

Default Notify workflow generally perform a single action, such as initiating a phone call. You can create custom Notify workflow activities to implement more complex functionality.

Use event handler functions in each Notify activity definition to design your own activity behavior. For example, you can set the activity result if the caller hangs up by using the `onCompleted` function.

```javascript
onCompleted: function() {
    activity.result = 'call_ended';
},
```

When creating a new Notify workflow activity, follow these design principles.

- Within `onExecute` event handler function, create a new NotifyAction object. Use this object to create a simple or complex action, then serialize the object to the `notify_wf_activity` table.
Within the `onUpdate` event handler function, deserialize the NotifyAction object from the `notify_wf_activity` table and use this object to perform any other operations.

Use the other event handler functions and the Notify as needed to implement the desired activity behavior.

**Available Notify activity event handlers**

When creating Notify workflow activities, you can use event-handler functions to respond to events from a telephony provider.

Not all activities or telephony providers support all events. For example, the `Reject` activity ends the call before the caller connects so the `onNoAnswer` function is never invoked from this activity.

**Note:** When configuring an activity to respond to an event, ensure that your telephony provider supports that event.

The following table describes available event handlers and lists the Notify workflow activities that can invoke each handler.

**Event handlers**

<table>
<thead>
<tr>
<th>Handler</th>
<th>Description</th>
<th>Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>onExecute</td>
<td>Runs when the activity first runs.</td>
<td>All call-related activities</td>
</tr>
<tr>
<td>onUpdate</td>
<td>Runs when the call record associated with the workflow is updated.</td>
<td>All call-related activities</td>
</tr>
<tr>
<td>onCompleted</td>
<td>Runs when a call ends.</td>
<td>All call-related activities</td>
</tr>
<tr>
<td>onRinging</td>
<td>Runs when a call starts ringing.</td>
<td>Forward call, call, join conference call, forward to notify client</td>
</tr>
<tr>
<td>onInProgress</td>
<td>Runs when both parties are connected on a call.</td>
<td>Forward call, call, join conference call, forward to notify client</td>
</tr>
<tr>
<td>onNoAnswer</td>
<td>Runs when a call is not answered.</td>
<td>Forward call, call, join conference call, forward to notify client</td>
</tr>
<tr>
<td>onBusy</td>
<td>Runs when a called number is busy.</td>
<td>Forward call, call, join conference call, forward to notify client</td>
</tr>
<tr>
<td>onFailed</td>
<td>Runs when an error occurs.</td>
<td>All call-related activities</td>
</tr>
</tbody>
</table>

**Notify languages**

Notify supports multiple languages when using text-to-speech.

For example, when using the `input` or `say` workflow activities, you can specify which language to use when reading the text.

The list of available languages is stored on the Notify Language (`notify_language`) table. By default, languages supported by all Notify telephony providers are available. You can add additional languages if they are supported by your specific telephony provider.
Notify on task

Notify allows you to send SMS alerts and initiate conference calls from any task record.

This functionality is available for all tables that extend the Task table, such as Incident, Problem, or Change. All calls and messages made from tasks are initiated using a single Notify phone number (E.164 or short code). You can configure which phone number is used by setting the property `glide.notify.task.phone_number`.

Send an SMS message from a task

You can use Notify to send SMS alerts from a task record.

Role required: itil

Notify must be set up before you can use Notify on task. Ensure there are Notify phone numbers (E.164 or short code) in number groups with SMS workflows. Also ensure the property `glide.notify.task.phone_number` is set to one of these Notify phone numbers.

1. Navigate to any task record, such as an incident or change.
2. Click the Send SMS related link.
3. Select one or more Recipients to send the SMS to.
4. Enter the Message to send.
   The task record number is added to the message automatically.
5. Click Send.

   Any SMS records created from a task are associated with that task. You can view associated SMS messages from the task record in the SMS Messages related list. You may need to configure the form to add the related list.

Start a conference call from a task

You can use Notify to start conference calls from a task record.

Role required: itil

Notify must be set up before you can use Notify on task. Ensure there are Notify phone numbers (E.164 or short code) in number groups with phone call workflows. Also ensure the property `glide.notify.task.phone_number` is set to one of these Notify phone numbers.

1. Navigate to any task record, such as an incident or change.
2. Click the Start conference call related link.
3. Select one or more Recipients to send the SMS to.
4. Click Start.

   Any conference call records created from a task are associated with that task. You can view associated conference calls from the task record in the Conference calls related list. You may need to configure the form to add the related list.

Notify with incident alert

You can use Notify with Incident Alert to send SMS messages or start conference calls based on incident alerts.

Notify with incident alert requirements

Certain configuration steps are required to use Notify with Incident Alert.
To use Notify with incident alert:

- Both Notify and Incident Alert must be active.
- Notify must be configured and able to initiate and receive phone calls and SMS messages.
- The property `com.snc.iam.notify_number` must be set to an active Notify number.
- This Notify number must belong to a number group configured with inbound and outbound conference call workflows.

**Note:** The Conference Call Group number group is configured with conference call workflows by default.

### Numbers and number groups

Number groups allow you to group Notify phone numbers and share workflows across grouped numbers.

Each phone number within Notify has an associated number group. Numbers within a group use the same workflows for handling incoming and outgoing calls and SMS messages.

Numbers associated with a group appear on the Notify Phone Numbers related list on the Notify Phone Number Group form.

### Launch a conference call from an incident alert

As part of processing an incident alert, a conference call can be created between involved users.

Call participants can include:

- Those users who have been assigned specific responsibilities.
- Any required ad-hoc user contacts.
- Other involved parties who are not recorded as users, such as third-party contacts.

**Note:** Only one conference call at a time can be active for each incident.

1. Navigate to Incident Management > Open.
2. Open the relevant incident alert.
3. Click the Initiate Conference Call related link.
4. Within the dialog box that appears, select the participants for the conference.
### Select participants

The dialog box displays the recommended and selected participants for the conference. All users from the **User Contacts** list in the incident alert are selected by default. If a rotation schedule exists for the group contacts, the primary and secondary on-call resources are shown in the **Recommended** list. This way, the current on-call persons can quickly be invited to join the conference call. Calls are placed to the number in the **Mobile** phone field on the user record. If that information is blank, the user cannot be contacted through Notify. The mobile phone number has to be an [E.164](https://en.wikipedia.org/wiki/E.164) compliant phone number. If the phone number is a local number, without the + prefix, the number will be retrieved based on the user's location and, if possible, converted into a valid E.164 number.

5. **To select ad-hoc participants, do one of the following:**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click the reference lookup icon, and select the relevant user.</td>
<td>Click <strong>Add to selected</strong>.</td>
</tr>
<tr>
<td>Enter the participant’s phone number in the field beside the telephone icon.</td>
<td>Click <strong>Add to selected</strong>.</td>
</tr>
</tbody>
</table>

6. **After the participant list is finalized, click OK.**

The conference call starts and a **Conference call initiated** message is displayed at the top of the incident Alert form. Each user is called and can accept the call to join the conference.
Several response types are possible from users invited to join the conference call, apart from Accepted.

7. Click the **Conference call initiated** message to see details of that conference call. When the final participant leaves the conference, the conference call closes.

---

**Note:** VoIP phone systems, which do not use touch tone phones, may encounter issues with recognizing key presses. To avoid problems, ensure that conference call users use touch tone phones, or configure your VoIP system settings to recognize key presses, as described in your VoIP system documentation.

---

**Viewing conference call information**

Conference calls are listed as system activities in the **Activity** section of the Incident Alert form and also are listed in the **Conference Calls** related list.
Conference bridge history
Send an SMS notification for an incident alert

Notify sends an SMS to the users defined as default contacts for the alert.

When you create a new incident alert, Notify sends an SMS notification to the users defined as default contact responsibilities for the alert.

This text message is sent to the user’s mobile phone number: IA<number>: a <Severity> severity <Event Type> incident alert for <CI Name> has been opened.

Administrators can modify the content of this message by editing the SMS on new Incident Alert business rule.

Notify with on-call scheduling

When using both Notify and On-call scheduling you can send scheduling notifications as SMS messages, in addition to emails.

Notify with on-call scheduling requirements

Certain configuration steps are required to use Notify with On-call scheduling.

- You must add at least one Notify phone number to the On-Call Group number group. This group is configured by default to handle inbound SMS responses that accept or reject an on-call assignment.
- You must configure any outbound SMS workflows, such as the On-Call: Assign by Acknowledgement workflow to use this Notify phone number to send SMS messages. Edit all Send SMS activities in these workflows to use this number as the From value.

Set up Notify with on-call scheduling

You can configure on-call scheduling to use Notify functionality to send SMS alerts and assign users to tasks based on the SMS responses.

Ensure that the Notify and On-Call Scheduling plugins on your instance are activated.

Role required: admin

Set up Notify with On-call scheduling for the first time or migrate from On-call scheduling with NotifyNow.

1. Navigate to Notify > Numbers.
2. Select the phone number you want to use to send and receive on-call scheduling messages.
3. In the Notify group field, select the On-Call Group.
   The On-Call Group is configured with the on-call workflow by default.
4. Navigate to Workflow > Workflow Editor.
5. Select the On-Call: Assign by Acknowledgement workflow.
   If migrating from NotifyNow, and you have previously customized this workflow, you must import the new version of the workflow manually. See KB0551603 for more information.
6. Click the workflow menu icon in the title bar and select Copy to copy the On-Call: Assign by Acknowledgement workflow. Save the copied workflow under a different name than what it is named by default.

Note: You must avoid modifying default workflows and instead choose to copy and then modify the required workflow.
7. Select a **Send SMS** activity.
8. In the **To (script)** field, modify the `getRecipientsAndNumberToSendFrom()` function and uncomment the line `//notify_number : getNotifyNumber()`,.
9. Perform one of the following actions.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify a static number</td>
<td>Within the <code>getRecipientsAndNumberToSendFromChange()</code> function, change <code>getNotifyNumber()</code> to the <code>sys_id</code> of the Notify phone number you selected in step 2.</td>
</tr>
<tr>
<td>Specify a number procedurally</td>
<td>Update the <code>getNotifyNumber()</code> function to return the <code>sys_id</code> of the Notify phone number you selected in step 2.</td>
</tr>
</tbody>
</table>

10. Repeat the previous 2 steps for each **Send SMS** activity on the workflow.
11. Click the workflow actions icon and select **Publish**.
12. Close the workflow editor interface.
13. Navigate to **On-Call Scheduling > Trigger Rules**.
14. Select a trigger rule that launches an assignment workflow.
15. In the **Trigger action** field, select **Workflow**.
16. In the **Trigger workflow** field, select the `On-call: Assign by Acknowledgement` workflow.
17. Click **Update**.
18. Repeat the previous 3 steps for each assignment trigger rule. Each time the conditions for one of these trigger rules is met, the `On-call: Assign by Acknowledgement` workflow runs.

**Using the on-call: assign by acknowledgement workflow**

The `On-call: Assign by Acknowledgement` workflow is provided with Notify.

The workflow uses data from the escalation settings of rotas and rosters. Depending on these settings, the workflow iterates through the defined escalation chain and sends notifications by SMS or email to users asking them for incident assignment. The workflow respects time-off as specified in the rosters. People who have time-off are not included in the escalation chain and no notifications are sent to them.

When you install both On-call scheduling and Notify, the `message_number` column is added to the Notify Messages (`notify_messages`) table to track responses to on-call assignment requests. This column indicates if the contacted user accepted or rejected the assignment. Before you can send notifications, you must define trigger rules. Trigger rules determine the conditions that must be met before a notification is sent and what action must be taken.

**Controlling the on-call communication channel with Notify**

You can configure On-call scheduling with Notify to always use a user’s preferred communication channel.

If **Force communication channel** is specified in the **Escalation settings** for rosters, the preferred user device is used, either SMS or email.

If the preferred device is SMS, and the on-call member does not have an SMS device defined, the user is not contacted even if the user has an email address. When forcing a communication channel on an escalation level does not succeed, no further communication attempts are made. The fact that the user could not be reached is logged.

The setting **Force communication channel** is only available if Notify is installed.
Key differences between on-call scheduling with NotifyNow and with Notify

There are key differences between on-call scheduling with NotifyNow and on-call scheduling with Notify.

Tracking responses to questions

The On call:Assign by Acknowledgement workflow no longer uses the Notify Question tables to track assignment responses. When you install On-call scheduling with Notify, the message_number column is added to the Notify Messages (notify_messages) table to track responses to on-call assignment requests. This column indicates if the contacted user accepted or rejected the assignment.

Scripting Notify

You can use scripts with Notify to interact with calls and SMS messages, or to provide a custom client interface.

Notify

The Notify API allows you to interact with Notify calls and SMS messages using scripts.

Notify - getPhoneNumbers()

Returns all phone numbers and short codes available to Notify, as an array.

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>Array</td>
<td>An array of NotifyPhoneNumber objects, each object representing one phone number available to Notify.</td>
</tr>
</tbody>
</table>

```
// instantiate notify
var notify = new SNC.Notify();

// get all available phone numbers
var phoneNumbers = notify.getPhoneNumbers();

// iterate over phone numbers
for (var i = 0; i < phoneNumbers.size(); i++) {
  var number = phoneNumbers.get(i);
  //perform any actions using each phone number
```
Notify - getShortCodes()

Returns all short codes available to Notify, as an array.

**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>Array</td>
<td>An array of NotifyPhoneNumber objects, each object representing one short code available to Notify.</td>
</tr>
</tbody>
</table>

```javascript
// instantiate notify
var notify = new SNC.Notify();

// get all available shortcodes
var shortCodes = notify.getShortCodes();

// iterate over phone numbers
for (var i = 0; i < shortCodes.size(); i++) {
    var shortCode = shortCodes.get(i);
    gs.log(shortCode.getNumber());
    //perform any actions using each shortcode
}
```

Notify - call(String notifyPhoneNumber, String toPhoneNumber)

Makes a call to an E.164-compliant phone number.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>notifyPhoneNumber</td>
<td>String</td>
<td>The phone number to make the call from. This number appears as the caller ID.</td>
</tr>
<tr>
<td>toPhoneNumber</td>
<td>String</td>
<td>The phone number to call.</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>
var from = '+14048007337';
var to = '+31646810495';

// set up call
new SNC.Notify().call(from, to);

**Notify - call(String notifyPhoneNumber, String toPhoneNumber, GlideRecord conferenceCall)**

Call a number to add that number to an active conference call.

This method is intended specifically for conference calls. To initiate calls between only two participants, use the `call(String notifyPhoneNumber, String toPhoneNumber)` method instead.

### Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>notifyPhoneNumber</td>
<td>String</td>
<td>The Notify phone number to make the call from. When you initiate a call, the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>outgoing call workflow for the number group associated with this number runs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ensure this workflow includes a <em>join conference call</em> activity to connect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the user to the conference call.</td>
</tr>
<tr>
<td>toPhoneNumber</td>
<td>String</td>
<td>The phone number to call. Called numbers are added to the conference call.</td>
</tr>
<tr>
<td>conferenceCall</td>
<td>GlideRecord</td>
<td>A GlideRecord for the Notify Call (notify_call) table identifying the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>conference call record. This record is automatically added to the outgoing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>call workflow scratchpad as the workflow.scratchpad.conference_call variable.</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>

```javascript
var notify = new SNC.Notify();
var from = '+14041234567';
var participants = ['+31612345678', '+31623456789', '+31687654321'];

// set up a conference call
var conferenceCall = notify.conferenceCall();
```
// set up the outbound calls for all conference call participants
for (var i in participants) {
    var to = participants[i];
    notify.call(from, to, conferenceCall);
}

// feedback
gs.log(gs.getMessage('set up a conference call with number {0} and (re)join code: {1}',
                        [ conferenceCall.getValue('number'),
                          conferenceCall.getValue('code') ]));

**Notify - sendSMS(NotifyPhoneNumber notifyPhoneNumber, String toPhoneNumber, String messageBody)**

Sends an SMS text message to an E.164-compliant phone number.

This function creates a new record on the Notify Message (notify_message) table.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>notifyPhoneNumber</td>
<td>NotifyPhoneNumber</td>
<td>The Notify phone number or short code to send this SMS from.</td>
</tr>
<tr>
<td>toPhoneNumber</td>
<td>String</td>
<td>An E.164-compliant phone number to send the SMS to.</td>
</tr>
<tr>
<td>messageBody</td>
<td>String</td>
<td>The SMS text.</td>
</tr>
</tbody>
</table>

**Returns**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>The sys_id of the Notify Message (notify_message) record created by this function.</td>
</tr>
</tbody>
</table>

**Notify - sendSMS(NotifyPhoneNumber notifyPhoneNumber, String toPhoneNumber, String messageBody, GlideRecord source)**

Sends an SMS text message to an E.164-compliant phone number.

This function creates a new record on the Notify Message (notify_message) table and associates it with the source record.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>notifyPhoneNumber</td>
<td>NotifyPhoneNumber</td>
<td>The Notify phone number or short code to send this SMS from.</td>
</tr>
<tr>
<td>toPhoneNumber</td>
<td>String</td>
<td>An E.164-compliant phone number to send the SMS to.</td>
</tr>
<tr>
<td>messageBody</td>
<td>String</td>
<td>The SMS text.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>source</td>
<td>GlideRecord</td>
<td>The source record that prompted this SMS message, such as an incident.</td>
</tr>
</tbody>
</table>

**Returns**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>The sys_id of the Notify Message (notify_message) record created by this function.</td>
</tr>
</tbody>
</table>

**Notify - getChildCallIDs(GlideRecord callRecord)**

Returns the sys_id values of calls that are children of a specified call.

Any call started by forwarding another call, such as with the Forward workflow activity, is considered a child of the original call. The original call is the parent call.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>callRecord</td>
<td>GlideRecord</td>
<td>A record on the Notify Call (notify_call) table.</td>
</tr>
</tbody>
</table>

**Returns**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Array</td>
<td>The sys_id values of all calls that are children of the specified call.</td>
</tr>
</tbody>
</table>

```javascript
var callRecord = new GlideRecord('notify_call');
callRecord.get("0f4f5863ff13310014ecffffffff28");
var notify = new SNC.Notify();
var childCallIDs = notify.getChildCallIDs(callRecord);
for(var callID in childCallIDs)
  //perform any operations with the child callID values
```

**Notify - getParentCallID(GlideRecord callRecord)**

Returns the sys_id of a specified call's parent call.

Any call started by forwarding another call, such as with the Forward workflow activity, is considered a child of the original call. The original call is the parent call.
Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>callRecord</td>
<td>GlideRecord</td>
<td>A record on the Notify Call (notify_call) table.</td>
</tr>
</tbody>
</table>

Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>The sys_id of the parent call record.</td>
</tr>
</tbody>
</table>

```javascript
var callRecord = new GlideRecord('notify_call');
callRecord.get("0f4f5863ff13310014ecfffffffff28");

var notify = new SNC.Notify();
var parentCallID = notify.getParentCallID(callRecord);
```

**Notify - getTokens()**

Returns client tokens for any installed telephony drivers for use in WebRTC or mobile clients. This function uses the currently logged-in user record as the client.

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 client tokens, as a JSON string.</td>
</tr>
</tbody>
</table>

```javascript
// get Notify Client Tokens per active Notify Driver for the currently logged in user
var json = new SNC.Notify().getTokens();

// parse the json that was return into a tokens object
var tokens = JSON.parse(json);

// log line
gs.log('Notify Client Tokens for the currently logged in user');

// iterate over the driver tokens
for (var driver in tokens) {
    gs.log(driver + ' Driver token: ' + tokens[driver]);
}
```
### Notify - getTokens(GlideRecord record)

Get client tokens for any installed telephony drivers for use in WebRTC or mobile clients.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>record</td>
<td>GlideRecord</td>
<td>A record used to generate the client tokens.</td>
</tr>
</tbody>
</table>

**Returns**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>The client tokens. The value of the string depends on the GlideRecord parameter.</td>
</tr>
</tbody>
</table>

This example demonstrates getting Notify client tokens for every Notify group.

```javascript
// instantiate Notify
var notify = new SNC.Notify();

// get all Notify Groups
var notifyGroup = new GlideRecord("notify_group");
notifyGroup.query();

// iterate over all notify groups
while (notifyGroup.next()) {
    // generate Notify Client tokens per active Notify Driver for this group
    var json = notify.getTokens(notifyGroup);
    var tokens = JSON.parse(json);
    for (var driver in tokens) {
        gs.log(gs.getMessage("Notify Client token for {0} driver and Notify Group '{1}': {2}", [driver, notifyGroup.getValue('name'), tokens[driver]]));
    }
}
```

### Notify - getAvailableClients(String notifyNumber)

Returns a list of client sessions that are available to receive calls.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>notifyNumber</td>
<td>String</td>
<td>Any valid Notify phone number.</td>
</tr>
</tbody>
</table>
### Notify - conferenceCall()

Create a new conference call GlideRecord.

#### Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

#### Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GlideRecord</td>
<td>A new Notify Call (notify_call) record for a conference call.</td>
</tr>
</tbody>
</table>

```javascript
var notify = new SNC.Notify();
var from = '+14041234567';
var participants = ['+31612345678', '+31623456789', '+31687654321'];

// set up a conference call
var conferenceCall = notify.conferenceCall();

// set up the outbound calls for all conference call participants
for (var i in participants) {
    var to = participants[i];
    notify.call(from, to, conferenceCall);
}

// feedback
gs.log(gs.getMessage('set up a conference call with number {0} and (re)join code: {1}',
    [ conferenceCall.getValue('number'),
    conferenceCall.getValue('code') ]));
```

### Notify - queueCall(GlideRecord callRecord)

Put a call into a queue.

Resume a queued call using the dequeueCall method.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GlideRecord</td>
<td>A new Notify Call (notify_call) record for a conference call.</td>
</tr>
</tbody>
</table>
### Notify - dequeueCall(GlideRecord callRecord)

Resume a call after it was put in a queue.

Use this method to resume calls that were put in a queue with the `queueCall` method.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>callRecord</td>
<td>GlideRecord</td>
<td>A GlideRecord object on the Notify Call (notify_call) table with the held call you want to resume.</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>

```java
var call = new GlideRecord('notify_call');
call.get('<call record sys_id>');
if (call.isValid()) {
    new SNC.Notify().dequeueCall(call);
}
```

### Notify - kick(GlideRecord participant)

Kicks a specified user from a Notify conference call.

```java
var call = new GlideRecord('notify_call');
call.get('some sys_id');
if (call.isValid()) {
    new SNC.Notify().kick(call);
}
```
Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>participant</td>
<td>GlideRecord</td>
<td>A GlideRecord object containing the Notify Participant (notify_participant) to kick from the conference call.</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>

```javascript
var participant = new GlideRecord('notify_participant');
participant.get('<sys_id>');
if (participant.isValid()) {
    new SNC.Notify().kick(participant);
}
```

**Notify - forwardCall(GlideRecord call, String destination, String dtmf)**

Forwards a call to connect that call with a different recipient.

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>call</td>
<td>GlideRecord or String</td>
<td>A Notify call record, or the telephony provider call ID.</td>
</tr>
<tr>
<td>destination</td>
<td>GlideRecord or String</td>
<td>A Notify phone number record, or an E.164-compliant phone number.</td>
</tr>
<tr>
<td>dtmf</td>
<td>String</td>
<td>A DTMF code to play upon connection.</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>

**NotifyAction**

The NotifyAction API allows you to define actions to send to a telephony provider.

You add actions to a NotifyAction object by calling the respective `add` function for each type of action.

Each `add` function returns an Action object, such as a SayAction object for the `addSay()` function. Refer to each method example for information about returned objects.
NotifyAction - addDial()

Makes an outbound call.

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>DialAction</td>
<td>The action added to the NotifyAction object. Use the DialAction object to define.</td>
</tr>
</tbody>
</table>

```javascript
var action = new SNC.NotifyAction();
var dial = action.addDial();
dial.setRecord(activity.vars.record);
dial.setClientRecord(activity.vars.user, "sys_user");
```

NotifyAction - addGather()

Presents an interactive phone menu to the user.

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>GatherAction</td>
<td>The action added to the NotifyAction object. Use the GatherAction object to define the menu settings and options to present to the user.</td>
</tr>
</tbody>
</table>

```javascript
// instantiate NotifyAction
var notifyAction = new SNC.NotifyAction();

// present the user with a menu
var gather = notifyAction.addGather();
gather.setNumberOfDigits(1);   // the user can type 1 digit
gather.setFinishKey('#');     // # or *, usefull for > 1 digits
gather.setTimeout(10);        // time to enter answer, in seconds

// add first menu item
var usSay = gather.addSay();
```
usSay.setText('Press 1 for english');
usSay.setLanguage('en-US');

// add second menu item
var nlSay = gather.addSay();
nlSay.setText('Kies 2 voor Nederlands');
nlSay.setLanguage('nl-NL');

// add third menu item
var frSay = gather.addSay();
frSay.setText('Choisissez 3 pour le français.');
frSay.setLanguage('fr-FR');

// and finish off with an applause
var play = gather.addPlay();
play.setURL('http://www.wavsource.com/
snds_2015-04-12_5971820382841326/sfx/applause_y.wav');

**NotifyAction - addHangUp()**

Ends an active phone call.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

**Returns**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HangUpAction</td>
<td>The action added to the NotifyAction object.</td>
</tr>
</tbody>
</table>

// instantiate NotifyAction
var notifyAction = new SNC.NotifyAction();

// hang up
notifyAction.addHangUp();

**NotifyAction - addQueue()**

Queue the call, putting it on hold.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>
Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QueueAction</td>
<td>The action added to the NotifyAction object. Use the QueueAction object to define the queue name, and queueing or dequeueing behavior.</td>
</tr>
</tbody>
</table>

```javascript
// instantiate NotifyAction
var notifyAction = new SNC.NotifyAction();

// queue the call
var queue = notifyAction.addQueue();
queue.setName('my queue');
```

```javascript
// instantiate NotifyAction
var notifyAction = new SNC.NotifyAction();

// dequeue the call
var queue = notifyAction.addQueue();
queue.setDequeue(true);
```

**NotifyAction - addPlay()**
Plays an audio file on the call.

**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>PlayAction</td>
<td>The action added to the NotifyAction object. Use the PlayAction object to define the audio file URL and number of times to loop the audio.</td>
</tr>
</tbody>
</table>

```javascript
// instantiate NotifyAction
var notifyAction = new SNC.NotifyAction();

// add a play action
var play = notifyAction.addPlay();
play.setURL('http://www.moviesounds.com/2001/imsorry.wav');
play.setLoop(1);
```

**NotifyAction - addReject()**
Rejects an incoming call.
### 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>RejectAction</td>
<td>The action added to the NotifyAction object. Use the RejectAction object to define the reason for rejecting the call.</td>
</tr>
</tbody>
</table>

```javascript
// instantiate NotifyAction
var notifyAction = new SNC.NotifyAction();

// reject the call
var rejectAction = notifyAction.addReject();
rejectAction.setReason('busy'); // 'busy' or 'rejected'
```

### NotifyAction - addSay()

Use text-to-speech to read text on the call.

Multiple languages are supported with text-to-speech. Available languages depend on the telephony provider.

#### 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>SayAction</td>
<td>The action added to the NotifyAction object. Use the SayAction object to define the text and language to read.</td>
</tr>
</tbody>
</table>

This example demonstrates reading text in several languages.

```javascript
// instantiate NotifyAction
var notifyAction = new SNC.NotifyAction();

// add a say action to say something in US English
var usSay = notifyAction.addSay();
usSay.setText('Welcome. I can speak english');
usSay.setLanguage('en-US');

// add a say action to say something in Dutch
var nlSay = notifyAction.addSay();
nlSay.setText('Ik spreek ook vloeiend nederlands');
```
nlSay.setLanguage('nl-NL');

// and german
var deSay = notifyAction.addSay();
deSay.setText('Und ich kann auch deutsch sprechen');
deSay.setLanguage('de-DE');

**NotifyAction - addSMS()**

Sends an SMS message.

When using this function with an active call, you do not need to call the `setTo` function on the returned SMSAction object. The SMS is automatically sent to the caller.

**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>SMSAction</td>
<td>The action added to the NotifyAction object. Use the SMSAction object to define the message text and the phone number to send the message to.</td>
</tr>
</tbody>
</table>

// instantiate NotifyAction
var notifyAction = new SNC.NotifyAction();

// define where to send the sms to
var number = new GlideElementPhoneNumber();
number.setPhoneNumber('+31612345678', true);

// add a SMS action
var sms = notifyAction.addSMS();
sms.setMessage('Lorem ipsum dolor sit amet, consectetur adipiscing elit.');
sms.setTo(number);

**NotifyAction - fromJson(String json)**

Deserialize a NotifyAction object from a JSON string.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>json</td>
<td>String</td>
<td>A JSON string representation of a NotifyAction object.</td>
</tr>
</tbody>
</table>
This example demonstrates deserializing a NotifyAction object.

```javascript
var json = ".... some json obtained from toJson ....";

// instantiate notify action
var notifyAction = new SNC.NotifyAction();

// deserialize and reconstruct the notify action instance
notifyAction.fromJson(json);
```

This example demonstrates both serializing and deserializing a NotifyAction object.

```javascript
// instantiate notify action
var notifyAction = new SNC.NotifyAction();

// add a queue
var queue = notifyAction.addQueue();
queue.setName('myQueueName');
queue.setDequeue(false);

// serialize to json
var json = notifyAction.toJson();
gs.log('serialization result: ' + json);

// instantiate a new notify action
var newAction = new SNC.NotifyAction();

// deserialize the json generated above
newAction.fromJson(json);

// serialize the new object and log the result
newJson = newAction.toJson();
gs.log('new serialization result: ' + newJson);
gs.log('the same: ' + (json == newJson));
```

Output: *** Script: serialization result: {'fClassName':"NotifyAction","fActions":[{"fClassName":"QueueAction","fDequeue":true,"fQueueName":"myQueueName"}]}
*** Script: new serialization result: {'fClassName':"NotifyAction","fActions":[{"fClassName":"QueueAction","fDequeue":true,"fQueueName":"myQueueName"}]}
*** Script: the same: true

**NotifyAction - toJson()**

Serialize the NotifyAction object to a JSON 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>
This example demonstrates serializing a NotifyAction object.

```javascript
// instantiate notify action
var notifyAction = new SNC.NotifyAction();

// add one or more notify actions
// ...

// and serialize to json
var json = notifyAction.toJson();
```

This example demonstrates both serializing and deserializing a NotifyAction object.

```javascript
// instantiate notify action
var notifyAction = new SNC.NotifyAction();

// add a queue
var queue = notifyAction.addQueue();
queue.setName('myQueueName');
queue.setDequeue(false);

// serialize to json
var json = notifyAction.toJson();
gs.log('serialization result: ' + json);

// instantiate a new notify action
var newAction = new SNC.NotifyAction();

// deserialize the json generated above
newAction.fromJson(json);

// serialize the new object and log the result
newJson = newAction.toJson();
gs.log('new serialization result: ' + newJson);
gs.log('the same: ' + (json == newJson));
```

**Output:**

```javascript
*** Script: serialization result: 
{ fClassName: "NotifyAction", fActions: [{ fClassName: "QueueAction", fDequeue: true, fQueueName: "myQueueName" }] }
*** Script: new serialization result: 
{ fClassName: "NotifyAction", fActions: [{ fClassName: "QueueAction", fDequeue: true, fQueueName: "myQueueName" }] }
*** Script: the same: true
```

**NotifyAction - addConference()**

Add a call to a Notify conference call.
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>ConferenceAction</td>
<td>The action added to the NotifyAction object. Use the ConferenceAction object to define the conference call name, and the behavior of the conference call when a participant joins or leaves.</td>
</tr>
</tbody>
</table>

**NotifyPhoneNumber**

The NotifyPhoneNumber API allows you to query information about a Notify phone number.

**NotifyPhoneNumber - getDialCode()**

Returns the international dialing code for a Notify phone number.

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>International phone code for a country.</td>
</tr>
</tbody>
</table>

**NotifyPhoneNumber - getID()**

Returns the ID of this phone number as defined by the telephony provider.

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 ID of the number within the telephony provider.</td>
</tr>
</tbody>
</table>

**NotifyPhoneNumber - getNumber()**

Returns the numerical phone number for a NotifyPhoneNumber.
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>An E.164-compliant phone number.</td>
</tr>
</tbody>
</table>

**NotifyPhoneNumber - getOwner()**

Returns the telephony provider associated with this phone number.

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>void</td>
<td>The telephony provider associated with the number, such as the Twilio service.</td>
</tr>
</tbody>
</table>

**NotifyPhoneNumber - getTerritory()**

Returns the country associated with the phone number.

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 name of the country the phone number belongs to.</td>
</tr>
</tbody>
</table>

**NotifyPhoneNumber - supportsConferenceCall()**

Determines if the Notify phone number supports conference calling.

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>Returns true if the Notify phone number supports conference calling.</td>
</tr>
</tbody>
</table>

**NotifyPhoneNumber - supportsIncomingPhoneCall()**

Determines if the Notify phone number supports receiving phone calls.

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>Returns true if the Notify phone number supports receiving incoming phone calls.</td>
</tr>
</tbody>
</table>

**NotifyPhoneNumber - supportsIncomingSMS()**

Determines if the Notify phone number supports receiving SMS messages.

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>Returns true if the Notify phone number supports receiving incoming MMS messages.</td>
</tr>
</tbody>
</table>

**NotifyPhoneNumber - supportsOutgoingPhoneCall()**

Determines if the Notify phone number supports initiating phone calls.

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>Returns true if the Notify phone number supports initiating outgoing phone calls.</td>
</tr>
</tbody>
</table>
NotifyPhoneNumber - supportsOutgoingSMS()

Determines if the Notify phone number supports sending SMS messages.

<table>
<thead>
<tr>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Returns</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
</tr>
<tr>
<td>boolean</td>
</tr>
</tbody>
</table>

NotifyPhoneNumber - supportsRecording()

Determines if the Notify phone number supports recording phone calls.

<table>
<thead>
<tr>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Returns</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
</tr>
<tr>
<td>boolean</td>
</tr>
</tbody>
</table>

NotifyPhoneNumber - supportsWebRTC()

Determines if the Notify phone number supports calls to a browser, such as in a WebRTC implementation.

<table>
<thead>
<tr>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Returns</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
</tr>
<tr>
<td>boolean</td>
</tr>
</tbody>
</table>

Notify Client

The Notify Client API allows you use Notify telephony functionality, such as making and receiving calls, from a web browser.
Several Notify Client methods take a callback function as a parameter. Because Notify Client calls are made asynchronously, these methods cannot return a value directly. Use the callback function to parse the returned data, such as by assigning variables or making other API calls.

**Notify Client - Client(Object notifyConfig)**

Instantiates a new Notify WebRTC Client object.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>notifyConfig</td>
<td>Object</td>
<td>The configuration settings for the Notify WebRTC Client, as a JSON object.</td>
</tr>
</tbody>
</table>

```javascript
var notifyConfig = {
    vendor: SNC.Notify.Vendor.TWILIO,
    callerId: 'xyz',
    autoReconnect: true,
    onReady: function() {},
    onOffline: function() {},
    onError: function( message ) {},
    onConnect: function( status ) {},
    onDisconnect: function() {},
    onIncoming: function( {from, to, callSid} ) {},
    onOutgoing: function( callSid ) {},
    onAccept: function() {},
    onMute: function() {},
    onUnmute: function() {},
    onCancel: function() {}
};

$j(function() {
    notifyClient = new SNC.Notify.Client(notifyConfig);
    notifyClient.init();
});
```

**Notify Client - call(Object identifier)**

Call a specified phone number or the phone number associated with a specified user.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>identifier</td>
<td>Object</td>
<td>Enter a JSON object that provides either the phone number to call or the sys_id of a user record to get the phone number from.</td>
</tr>
</tbody>
</table>

**Note:** If you provide both a phone number and user sys_id, only the phone number is used.
This example demonstrates passing a phone number as the function parameter.

```javascript
notifyClient.call({
    phoneNumber: "+18001112223"
});
```

This example demonstrates passing a user record sys_id as the function parameter.

```javascript
notifyClient.call({
    userId: "6816f79cc0a8016401c5a33be04be441"
});
```

**Notify Client - hangupCall()**

End the current call.

**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>void</td>
<td></td>
</tr>
</tbody>
</table>

This example demonstrates mapping a client function to an interface button using jQuery.

```javascript
$j("#pickupCallBtn").on("click", function() {
    notifyClient.hangupCall();
});
```

**Notify Client - pickupCall()**

Answers and connects to an incoming call from a Twilio WebRTC client. Call this method when there is a notification of an incoming call.
### Notify Client - mute(Boolean muted)

Mutes or unmutes the current client.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>muted</td>
<td>Boolean</td>
<td>Set this value to true to mute the current client, false to unmute.</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>

### NotifyClient - forwardCall(Object argument)

Forward the current call to a different phone number or Notify client session.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>argument</td>
<td>Object</td>
<td>A JavaScript object detailing the number or Notify client to forward the call to.</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>

This example demonstrates forwarding a call to a different phone number. The `dtmf` attribute allows you to send DTMF dial tones to the receiving number.

```javascript
var arg = {
    type: "number",
    id: "+17012345678",
    dtmf: "1234"
}
```
This example demonstrates forwarding a call to a different Notify client.

```javascript
var arg = {
  type: "userId",
  id: "6816f79cc0a8016401c5a33be0be441"
}
client.forwardCall(arg);
```

### NotifyClient - sendDtmf(String digits)

Send one or more DTMF-valid digits over the current call.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>digits</td>
<td>String</td>
<td>One or more DTMF-valid digits.</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>

### Notify client event handlers

Notify Client event handlers allow you to define scripted behavior for responding to events from a telephony provider such as the Twilio service.

#### Event handlers

A communication between the Notify WebRTC Client and a telephony provider is asynchronous. The client function calls, such as `notifyClient.call()` do not wait for a response from the telephony provider. Instead, event handler methods define how to respond to certain events from the telephony provider.

You can create event handler implementations when creating the Notify Client configuration object. Fully define the handlers in the configuration object before instantiating a Notify Client object.

**onReady**

The `onReady` function runs after you call the `init` function on the client object. The `onReady` function indicates that the WebRTC session is ready.

**onOffline**

The `onOffline` function runs if the WebRTC session is not active.
onError

The `onError` function runs if the client encounters an error.

This function exposes one parameter. Use this parameter when implementing the event handler function.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>message</td>
<td>String</td>
<td>The error message text.</td>
</tr>
</tbody>
</table>

onConnect

The `onConnect` function runs when the client receives a call connection event for an incoming or outgoing call.

This function exposes one parameter. Use this parameter when implementing the event handler function.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>String</td>
<td>The call status, as a string constant. Note: When evaluating call status, use the constants provided by <code>SNC.Notify.Status</code>.</td>
</tr>
</tbody>
</table>

```javascript
onConnect: function(status) { // webRTC receives a call connection event (incoming or outgoing).
  if (status == SNC.Notify.Status.OPEN) {
    setStatus(getTimeStamp() + " -- Successfully established call");
    showHangupButton(); //update the UI
  }
},
```

onDisconnect

The `onDisconnect` function runs when a call disconnects.

onIncoming

The `onIncoming` function runs when a call is made to the client and the telephony provider returns the parent call ID.

This function exposes these parameters as a single JSON object. Use these parameters when implementing the event handler function.
Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>callInfo.from</td>
<td>String</td>
<td>The caller's phone number.</td>
</tr>
<tr>
<td>callInfo.to</td>
<td>String</td>
<td>The called phone number.</td>
</tr>
<tr>
<td>callInfo.callSid</td>
<td>String</td>
<td>The SID of the call from the telephony provider.</td>
</tr>
</tbody>
</table>

onIncoming: function(callInfo) {
  gs.log('incoming call from : ' + callInfo.from);
  var gru = new GlideRecord('sys_user');
  gru.addQuery('phone', callInfo.from);
  gru.query(function() {
    while (gru.next()) { // there may be more than one person with same number?
      // fetch caller's info
      gs.log('caller : ' + gru.name);
    }
  });
},

onOutgoing

The onOutgoing function runs when an outgoing call is made from the client.
This function exposes one parameter. Use this parameter when implementing the event handler function.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>callSid</td>
<td>String</td>
<td>The SID of the call from the telephony provider.</td>
</tr>
</tbody>
</table>

onAccept

The onAccept function when the client accepts an incoming call.

onMute

The onMute function runs when the client is muted.

onUnmute

The onUnmute function runs when the client is unmuted.
**onCancel**

The `onCancel` function runs if the caller cancels the call.

**Notify client building a configuration object example**

This example demonstrates how to construct the configuration object needed to instantiate a Notify WebRTC Client object.

The configuration object is a JSON object that specifies properties such as the telephony service provider and caller information, and event handler functions.

This sample code demonstrates how to create a simple configuration object.

```javascript
var notifyConfig = {
    vendor: SNC.Notify.Vendor.TWILIO, //Pass one of the supported vendor constants. Supported value is SNC.Notify.Vendor.TWILIO. Do not pass raw string values.
    callerId: '19991231234', //Pass a valid phone number to use as the caller ID. This number is usually provided by your telephony vendor.
    autoReconnect: true, //Pass true to automatically create a new WebRTC vendor session when the current session expires.
    onReady: function() {},
    onOffline: function() {},
    onError: function( message ) {},
    onConnect: function( status ) {},
    onDisconnect: function() {},
    onIncoming: function( {from, to, callSid} ) {},
    onOutgoing: function( callSid ) {},
    onAccept: function() {},
    onMute: function() {},
    onUnmute: function() {},
    onCancel: function() {}
};
```

**Activate Notify**

The Notify plugin (com.snc.notify) requires a separate subscription. This plugin includes demo data and activates related plugins if they are not already active.

Role required: admin

Notify activates these related plugins if they are not already active.

**Plugins for Notify**

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E164 Compliant Phone Number</td>
<td>Provides E-164 compliant phone number support.</td>
</tr>
<tr>
<td>(com.glide.phone_number)</td>
<td></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>
</tr>
<tr>
<td>(com.snc.notify.twilio)</td>
<td></td>
</tr>
</tbody>
</table>

To purchase a subscription, contact your ServiceNow account manager. After purchasing the subscription, activate the plugin within the production instance.

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**.

### Migrating from Legacy Notify

When migrating to Notify from the Legacy Notify functionality, several changes are made to the instance.

### Automatic changes

Several automatic changes occur when you activate Notify if the Legacy Notify functionality is already enabled.

- The Legacy Notify application menu is removed.
- Two separators are added to the new Notify application menu, Legacy Notify and Legacy Notify Admin. New modules that replace the legacy Notify modules are added to these sections.

  **Note:** The added modules are not the same modules that were in the legacy Notify application menu. Any customizations made to the legacy Notify modules are not preserved.

- The notify_admin role allows access to Notify modules.
- The notifynow_admin role allows access to legacy Notify modules.
- All workflow activities from the legacy Notify application are moved to the Legacy Notify group.

### Differences between Notify and Legacy Notify

Describes the differences between the Notify and Legacy Notify applications, including architecture, workflows, Twilio support, and task-initiated conference calls.

<table>
<thead>
<tr>
<th>Legacy Notify (com.snc.notifynow)</th>
<th>Notify (com.snc.notify)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage a single number from a Twilio account per instance.</td>
<td>Provides support for multiple numbers per Twilio account, especially gross-geographical scenarios.</td>
</tr>
<tr>
<td>Does not include support for customizable workflows for Voice and SMS incoming or outgoing scenarios.</td>
<td>Workflow-driven approach for handling incoming and outgoing Voice and SMS events, making the integration easy to customize.</td>
</tr>
</tbody>
</table>
### Legacy Notify

Notify enables organizations with a Twilio account to send notifications using text and voice messages.

**Note:** This content applies only to the Legacy Notify application, available prior to the Geneva release. For information about the Notify application available starting with Geneva, see Notify.

It also allows conference calls between ServiceNow users to enable quick communications.

When Notify is active, you can configure ServiceNow to automatically generate and send notifications to selected contacts, for instance when a new incident alert is raised in the incident alert management process.

Users with the notifynow_admin role can set properties and monitor message and conference call activities.

Notify has been implemented for use within incident alert management. Refer to the Notify API documentation for details on how to implement Notify for use within other ServiceNow applications.

### Working with Legacy Notify

Follow this process to enable and use Notify.

**Note:** This content applies only to the Legacy Notify application, available prior to the Geneva release. For information about the Notify application available starting with Geneva, see Notify.

1. Set up a Twilio account to provide phone connectivity for Notify.
2. Activate Notify.
3. Configure Notify to use Twilio.
4. Begin using Notify immediately within incident alert management.
5. Use the Notify API with other ServiceNow applications to provide SMS, voicemail, email, and conference calls for those applications.

### View a Legacy Notify question

Questions contain a response action and a set of response choices. Use these questions to simplify communications. Then, you can monitor the resulting communication thread.

Role required: notifynow_admin

**Note:** This content applies only to the Legacy Notify application, available prior to the Geneva release. For information about the Notify application available starting with Geneva, see Notify.

© 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.
For example, the process can be used to ask members of a specific on-call group to acknowledge or reject an incident. Depending on the answer from the first team member, the incident is assigned to that person or an SMS question is sent to the next on-call member. In this example, the questions are used as part of a workflow.

To see a list of predefined questions both Notify and On-Call Scheduling need to be active.

1. Navigate to **Notify > Questions**.
2. Click the question **On-Call responsibility Accept/Reject** to see the question details.

3. Click the **Notify Response Choices** related list to view or edit the choices. The person who receives the SMS question can either choose to accept or reject the assignment. If the assignment is accepted, the **Response action** can be that the incident is actually assigned to that person. The response action is a script that you can modify or replace. If the assignment is rejected, an SMS question may be sent to the next person in the escalation chain, and so on. You can combine questions with a workflow to automate a process like on-call scheduling escalation.

**Create a question in Legacy Notify**

Define a question that can be sent to users.
Role required: notifynow_admin

Note: This content applies only to the Legacy Notify application, available prior to the Geneva release. For information about the Notify application available starting with Geneva, see Notify.

1. Navigate to Notify > Questions.
2. Click New.
3. Fill in the fields, as appropriate.

Notify New Question form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a description of the question.</td>
</tr>
<tr>
<td>Question</td>
<td>Enter the question you want to send. You can enter variables in the question with the { } tags, for example, {0}. When using more than one variable, use consecutive numbering. When using multiple variables, reference them by specifying their position in the parameter list, starting from {0}. The variable is picked up by the script and translated into, for example, an incident or a problem number.</td>
</tr>
<tr>
<td>Params</td>
<td>Enter parameters which map to the fields on the record that the workflow was triggered for. This enables the message to show dynamic data. Multiple parameters should be separated by a comma. For example, number, shows the incident number in case the workflow was triggered from an incident. A second parameter could be, for example short_description.</td>
</tr>
<tr>
<td>Response Action</td>
<td>Select the action that must be taken. This is a script that can be modified, or you can create a new script by clicking the search button and selecting New. Several examples of scripts are shown. Write your own script and click Submit.</td>
</tr>
</tbody>
</table>

4. Click Submit.

Create a new response choice in Legacy Notify

Create a new response choice to allow users to select that response for a Notify question.

Role required: notifynow_admin

Note: This content applies only to the Legacy Notify application, available prior to the Geneva release. For information about the Notify application available starting with Geneva, see Notify.

1. Navigate to Notify > Questions.
2. Open the notify question you have just created.
3. Click New to create a new notify response choice.
4. Fill in the fields, as appropriate.
### Notify New Response Choice form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code</td>
<td>The abbreviation for the response choice in the text message. For example, ACC for accept or REJ for reject.</td>
</tr>
<tr>
<td>Text</td>
<td>The text displayed for this response choice.</td>
</tr>
<tr>
<td>Order</td>
<td>A number indicating the order in the list of response choices. Choices with lower order numbers are listed before choices with higher order numbers.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.

### View Legacy Notify messages

Applications implementing Notify, such as incident alert management, can send Short Message Service (SMS) text messages to relevant contacts under predefined conditions, such as when a new incident alert has been created.

Role required: notifynow_admin

**Note:** This content applies only to the Legacy Notify application, available prior to the Geneva release. For information about the Notify application available starting with Geneva, see [Notify](https://knowledge.cissta.com).

1. Navigate to **Notify > Messages**.
2. Click a message to see the message details.

### View Legacy Notify conversations

The Notify Conversation (notifynow_conversation) table tracks bi-directional communications and adds the ability to have more than one active conversation with the same phone number at the same time.
Role required: notifynow_admin

**Note:** This content applies only to the Legacy Notify application, available prior to the Geneva release. For information about the Notify application available starting with Geneva, see Notify.

The thread number is combined with the phone number to link the SMS or email response to the correct conversation. Conversations remain active until a response is received or until they are automatically deactivated after the thread release time runs out. The default thread release time is 10 days. To change this value, add the `nn.thread.release.age` property.

1. Navigate to Notify > Conversations.
2. Click a conversation record to see the conversation details.

Notify Conversation Details

The State of the conversation can have one of the following values:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ended</td>
<td>The conversation has been completed.</td>
</tr>
<tr>
<td>Failed</td>
<td>The conversation has failed.</td>
</tr>
<tr>
<td>Pending</td>
<td>The SMS or email is waiting to be sent.</td>
</tr>
<tr>
<td>Sent</td>
<td>The SMS or email has been sent.</td>
</tr>
<tr>
<td>Unanswered</td>
<td>The SMS or email has not been answered.</td>
</tr>
</tbody>
</table>

**Note:** The mode of conversation cannot be changed during one conversation thread. For example, you cannot switch between SMS and email during one conversation.

**View Legacy Notify conference calls**

Applications that use Notify, such as incident alert management, can launch and maintain conference calls between involved parties.

Role required: notifynow_admin
1. Navigate to **Notify > Conference Calls**.
   You can also access conference call information from the relevant record, such as the **Conference Calls** related list in an incident alert record.

2. Click a conference call in the list to view details.

3. Click the arrow beside the check box to expand a **Participant** entry.
   This shows participant session information, including details of the conference calls that the participant has been involved in.

4. Click a **Participant** name to see more detailed information about that participant.
Legacy public conference calls

A Notify conference call can be public.

Note: This content applies only to the Legacy Notify application, available prior to the Geneva release. For information about the Notify application available starting with Geneva, see Notify.

The Private field on the conference call record indicates if a call is private (selected) or public (not selected). By default, all calls created automatically, such as those created through Incident Alert Management, are public. You can create private calls using the Notify API initiateConferenceCall method.

When created, public conference calls generate an associated Code which is sent via SMS to all invited participants. These participants can distribute the code to allow other users to join the public call. An administrator can control the format of the code using the property glide.notifynow.conference_call.code.pattern. Anyone with the code can connect to a public conference call using one of these methods:

- By calling the Twilio phone number and entering the code for that conference call.
- By sending the code in an SMS message to the Twilio phone number. Participants that join a public call this way are considered ad-hoc participants, indicated on the participant record.

Administering Legacy Notify

An administrator can set up Notify, manage Notify properties and conference call participants.
Configuring legacy Notify to use the Twilio service

Each ServiceNow instance using Notify requires a valid Twilio account and telephone number. Refer to the Twilio documentation for detailed instructions.

After the Twilio account is set up, perform the following to use that account with Notify:

- Associate the account with Notify
- Configure Twilio with ServiceNow endpoints

Associate a Twilio account with Legacy Notify

Associate a Twilio account with your instance to use that account for legacy Notify.

Role required: notifynow_admin

1. Navigate to Notify > Administration > Properties.
2. **Enter the AccountSID, AuthToken and phone number values.**
   These values can be obtained from the Twilio dashboard:
When the Twilio account details are entered in the **Notify Properties** page, the account status is updated.

3. (Optional) To use Notify on multiple ServiceNow instances, activate Notify on each instance and create a separate Twilio account and telephone number for each instance.

**Note:** Some telephone numbers are voice capable, but not SMS capable. This is shown in the Notify properties with relevant messages. Two methods are available to check this: `isSMSCapable` and `isVoiceCapable`.

### Configuring the Twilio service with endpoints in legacy Notify

In order for the Twilio service to receive Notify commands, the **Request URL** field value for every Twilio telephone number must point to the ServiceNow instance that uses Notify with that Twilio telephone number.

**Note:** This content applies only to the Legacy Notify application, available prior to the Geneva release. For information about the Notify application available starting with Geneva, see [Notify](#).

To set these values, do one of the following:

- Define them manually in the Twilio service dashboard.
- Ensure the fields are blank in the Twilio service dashboard, then open the **Notify Properties** page. Notify automatically configures the correct endpoints if the **Request URL** fields are blank.

Set these values from within the Twilio service dashboard.
Twilio Numbers Dashboard

The notifyusa values underlined in the image should be replaced with your ServiceNow instance name, for:

- **Voice Request URL**: https://notifyusa.service-now.com/NotifyNowCallProcessor.do
- Status Callback URL: https://notifyusa.service-now.com/NotifyNowCallStatusProcessor.do
- Messaging Request URL: https://notifyusa.service-now.com/NotifyNowSmsProcessor.do

**View and edit legacy Notify properties**

You can view and edit Notify properties.

Role required: notifynow_admin

**Note:** This content applies only to the Legacy Notify application, available prior to the Geneva release. For information about the Notify application available starting with Geneva, see [Notify](#).

1. Navigate to Notify > Administration > Properties.
## Notify Properties form

2. Fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Status</td>
<td>Information showing the status of the associated Twilio account.</td>
</tr>
<tr>
<td>Twilio AccountSID</td>
<td>The Twilio account AccountSID, acting as the user name for that account.</td>
</tr>
<tr>
<td>Twilio AuthToken</td>
<td>The Twilio account AuthToken, acting as the password for that account. See Associating a Twilio Account.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Twilio SMS and voice enabled phone number</td>
<td>The Twilio number that Notify will use. Telephone numbers must be entered in the E.164 format and need to exist under the Twilio account. See Associating a Twilio Account.</td>
</tr>
<tr>
<td>Number of frequent conference call participants to be displayed</td>
<td>The number of people to display in the frequently called list.</td>
</tr>
<tr>
<td>Voice</td>
<td>The voice used for Notify communications. Select <strong>woman</strong> or <strong>man</strong> to provide female or male voice support for English, Spanish, French, German, and Italian. Select <strong>alice</strong> to provide female voice support for a wider range of languages.</td>
</tr>
</tbody>
</table>

3. Click **Submit**.

### Legacy Notify account status messages

Account status messages are visible on the Notify Properties page.

**Account Status Message Descriptions**

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your account is ready for use</td>
<td>Notify is correctly configured and ready for use.</td>
</tr>
<tr>
<td>Your Twilio AccountSID or AuthToken are not valid</td>
<td>An incorrect value has been entered in the AccountSID or AuthToken fields in the Notify properties.</td>
</tr>
<tr>
<td>Your Twilio phone number is not valid</td>
<td>Incorrect telephone number information is defined in the Notify properties.</td>
</tr>
<tr>
<td>Your Twilio phone number does not have properly configured endpoints</td>
<td>The Request URL endpoint settings have not been properly configured.</td>
</tr>
<tr>
<td>Your Twilio account is not configured properly</td>
<td>One or more of your Twilio account settings is incorrect. Open the Twilio dashboard and check the settings.</td>
</tr>
</tbody>
</table>

### Manage Legacy Notify conference call participants

As a Notify administrator, you can mute, unmute, and kick participants on a conference call.

Role required: notifynow_admin

Note: This content applies only to the Legacy Notify application, available prior to the Geneva release. For information about the Notify application available starting with Geneva, see Notify.

Muting a participant prevents that person from speaking on the conference call but does not notify any participants, including the muted participant. Kicking a participant removes that person from the conference call and sets the Response field for the participant session to kicked.

1. Navigate to Notify > Conference Calls.
2. Select an active conference call.
3. In the Notify Conference Call Participants related list, select a participant.
4. Click the button for the action you want to perform, such as **Mute** to mute the participant.
   
   You can perform these actions for multiple participants as a single operation using the **Actions on selected rows** choice list on the **Notify Conference Call Participants** related list.

### Installed with Legacy Notify

Activating the Notify plugin adds or modifies tables, user roles, script includes, and other components.

**Note:** This content applies only to the Legacy Notify application, available prior to the Geneva release. For information about the Notify application available starting with Geneva, see [Notify](#).

### Tables

Notify adds or modifies the following tables.

#### Display Name (Table Name) | Description
--- | ---
Answer [notifynow_answer] | Information for possible answers to the SMS question sent.
Conversation [notifynow_conversation] | Information for the conversation thread.
NotifyNow Conference Call [notifynow_conference_call] | Information for conference call records.
NotifyNow Participant Session [notifynow_participant_session] | Information regarding conference call sessions for individual conference call participants.
Participant [notifynow_participant] | Information regarding individual conference call participants.
Question [notifynow_question] | Information for the possible questions in the SMS.
Response_action [notifynow_response_action] | Information for the notify response action associated with the question.
Response_choice [notifynow_response_choice] | Information for the notify response choice associated with the question.
SMS Messages [notifynow_message] | Information for the actual SMS messages sent.

### Properties

Notify adds the following system properties.

#### Property | Description
--- | ---
**glide.notifynow.frequent_participant_count** | The number of frequent conference call participants to be displayed.
**glide.notifynow.voice** | The voice used for Notify communications.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.notifynow.twilio.accountsid</td>
<td>The Twilio account AccountSID.</td>
</tr>
<tr>
<td>glide.notifynow.twilio.token</td>
<td>The Twilio account AuthToken.</td>
</tr>
<tr>
<td>glide.notifynow.twilio.phonenumber</td>
<td>The Twilio number that Notify will use.</td>
</tr>
<tr>
<td>glide.notifynow.twilio.answering_machine_detection</td>
<td>A boolean flag to enable or disable answering machine detection. Set to true to use answering machine detection. Set to false to continue the call.</td>
</tr>
<tr>
<td>nn.thread.release.age</td>
<td>The number of days after which the conversation thread release time runs out. Defaults to 10 days.</td>
</tr>
<tr>
<td>glide.notifynow.conference_call.code.pattern</td>
<td>The pattern used to generate a conference call code for public conference calls. Number signs (#) in the pattern are replaced with random numbers when a code is generated.</td>
</tr>
<tr>
<td>glide.notifynow.fix_invalid_phone_number</td>
<td>A boolean flag to enable or disable automatic correction of invalid phone numbers. Twilio might incorrectly prefix non-US phone numbers with 1. When this property is true, the instance automatically removes the 1 for non-US calls. When this property is false, you might be incorrectly identified when reconnecting to a call using SMS.</td>
</tr>
</tbody>
</table>

**User Roles**

Notify adds the following user roles.

**User Roles**

<table>
<thead>
<tr>
<th>Role</th>
<th>Contains Roles</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>notifynow_admin</td>
<td>None</td>
<td>Administrator with privileges for Notify functionality.</td>
</tr>
</tbody>
</table>

**UI Actions**

Notify adds the following UI actions.

**UI Actions**

<table>
<thead>
<tr>
<th>UI Action</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiate Conference Call</td>
<td>Incident Alert [incident_alert]</td>
<td>Adds a link to the Incident Alert form, if that plugin is activated, which displays a dialog box for starting a conference call with selected participants.</td>
</tr>
<tr>
<td>UI Action</td>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Invite to Conference Call</td>
<td>NotifyNow Conference Call [notifynow_conference_call]</td>
<td>Adds a link to the Notify Conference Call form which displays a dialog box for adding more users to an active conference call.</td>
</tr>
</tbody>
</table>

**Script Includes**

Notify adds the following script includes.

**Script Includes**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IncidentAlertConferenceCall</td>
<td>A utility JavaScript Prototype class allowing users to initiate the conference call and add other users to the conference call. Should be used in conjunction with the slushbucket UI page (notifynow_participant).</td>
</tr>
</tbody>
</table>

**Business Rules**

Notify adds the following business rules.

**Business Rules**

<table>
<thead>
<tr>
<th>Business Rule Name</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS on new Incident Alert</td>
<td>Incident Alert [incident_alert]</td>
<td>Sends an SMS to any default contacts added when an incident alert record is created.</td>
</tr>
<tr>
<td>Conference Call Allowed</td>
<td>Incident Alert [incident_alert]</td>
<td>Displays or hides the initiate conference call UI action by storing true or false in g_scratchpad.conferenceCallAllowed.</td>
</tr>
<tr>
<td>Update Conference Call Started IA Activity</td>
<td>NotifyNow Conference Call [notifynow_conference_call]</td>
<td>Logs when a conference call started by writing to an incident alert’s comment field if the source record is from the incident_alert table.</td>
</tr>
<tr>
<td>Update Conference Call Finished IA Activity</td>
<td>NotifyNow Conference Call [notifynow_conference_call]</td>
<td>Logs when a conference call ended and what actions the conference call participants took by writing to an incident alert’s comment field if the source record is from the incident_alert table.</td>
</tr>
</tbody>
</table>
**Workflow Activities**

Notify adds the following workflow activities.

### Workflow Activities

<table>
<thead>
<tr>
<th>Activity Name</th>
<th>Activity Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Notify SMS</td>
<td>Notify</td>
<td>Sends an SMS message (maximum 1600 Characters) to an E.164 compliant mobile phone number of the selected recipients and/or groups.</td>
</tr>
<tr>
<td>Send Notify SMS Question</td>
<td>Notify</td>
<td>Sends predefined SMS Question message (maximum 1600 Characters) to an E.164 compliant mobile phone number of the selected recipients and/or groups. This is one of two main activities for workflow On-Call Assign by Acknowledgement. In a predefined message, the recipient is asked to assign himself to a newly created incident. The same message also contains predefined answers.</td>
</tr>
<tr>
<td>Send Email Question</td>
<td>Notify</td>
<td>Sends email generated from email template containing notification that recipient is the current On-call resource for a newly created task. This is one of two main activities for the workflow On-Call Assign by Acknowledgement. In a predefined message, the recipient is asked to assign himself to a newly created incident. The email contains two links that enable the user to accept or reject assignment.</td>
</tr>
</tbody>
</table>

### Legacy Notify API

The legacy Notify API provides functionality for sending emails, sending SMS messages, and setting up conference calls.

Use this when you want to use Notify functionality with applications on your system.

**Note:** This API is included with the legacy Notify functionality. For APIs included in the current Notify feature, see the Notify, NotifyAction, NotifyPhoneNumber, and NotifyClient APIs.
**NotifyNow - getReadyState()**

Indicates whether Notify is set up correctly or not.

This method can only be accessed by administrators or users with the notifynow_admin role. Users with all other roles get the message False when trying to run the function in a script.

**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 Notify is set up correctly, otherwise false.</td>
</tr>
</tbody>
</table>

```
var nn = new SNC.NotifyNow();
gs.log((nn.getReadyState()) ? "OK" : "NOT OK");
```

**NotifyNow - getStatus()**

Returns the current status of Notify configuration.

This method can only be accessed by administrators or users with the notifynow_admin role. Users with all other roles get the message Unauthorized when trying to run the function in a script.

**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>One of the possible status messages.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO_NUMBER_MESSAGE</td>
<td>The account does not have a telephone number set up. Ensure that you set up the telephone number for the account.</td>
</tr>
<tr>
<td>NO_ENDPOINTS_MESSAGE</td>
<td>The account does not have its endpoints set up correctly. Ensure that you set up the endpoints for the account.</td>
</tr>
<tr>
<td>ACCOUNT_OK_MESSAGE</td>
<td>The account is active and ready for use.</td>
</tr>
<tr>
<td>ACCOUNT_NO_AUTH</td>
<td>The Twilio AuthToken is not valid.</td>
</tr>
<tr>
<td>ACCOUNT_NOT_CONFIGURED</td>
<td>Twilio AccountSID or AuthToken is not valid.</td>
</tr>
</tbody>
</table>

```
var nn = new SNC.NotifyNow();
gs.log(nn.getStatus());
```

**NotifyNow - initiateConferenceCall(String[] conferenceCallParticipants, String conferenceCallTitle)**

Initiate a new conference call.

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>conferenceCallParticipants</td>
<td>String</td>
<td>One or more users, conference call participants, identified by the sys_ids from the sys_user table or E.164-compliant phone numbers.</td>
</tr>
<tr>
<td>conferenceCallTitle</td>
<td>String</td>
<td>Title of the conference call. This parameter has a maximum length of 40 characters.</td>
</tr>
</tbody>
</table>
This initiates a conference call with E.164-compliant phone numbers for participants, without the optional source record parameter and and does not send any conference call details via SMS or email.

```
var participants = ['+31205655548', '+31205655552',
' +31652825393'];
// set up conference call
var nn = new SNC.NotifyNow();
var conferenceCall = nn.initiateConferenceCall(participants,
"testing12");
gs.log('started conference call: ' +
conferenceCall.getUniqueValue());
```

**NotifyNow - initiateConferenceCall(String[] conferenceCallParticipants, String conferenceCallTitle, GlideRecord sourceRecord, Boolean private)**

Initiate a new conference call.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>conferenceCallParticipants</td>
<td>String</td>
<td>One or more users, conference call participants, identified by the sys_ids from the sys_user table or E.164-compliant phone numbers.</td>
</tr>
<tr>
<td>conferenceCallTitle</td>
<td>String</td>
<td>Title of the conference call. This parameter has a maximum length of 40 characters.</td>
</tr>
<tr>
<td>sourceRecord</td>
<td>GlideRecord</td>
<td>Source record to associate to the conference call such as an incident or problem number.</td>
</tr>
<tr>
<td>private</td>
<td>Boolean</td>
<td>Value to control if a conference call is private. This value defaults to false.</td>
</tr>
</tbody>
</table>

**Returns**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GlideRecord</td>
<td>The conference call record, or null if there was an error.</td>
</tr>
</tbody>
</table>
This initiates a conference call with participants that have a E.164-compliant phone number and participants from the sys_user table and sends conference call details via SMS and email to all participants.

```javascript
// define phone number participants
var participants = ['+31205655548', '+31205655552', '+31652825393'];

// we also want to add two Dutch sys_user participants
var user = new GlideRecord('sys_user');
user.addNotNullQuery('mobile_phone');
user.addQuery('mobile_phone', 'STARTSWITH', '+316');
user.setLimit(2);
user.query();

// add users to the participant array
while (user.hasNext() && user.next()) {
    gs.log('adding user ' + user.getValue('name') + ' with phone number ' + user.getValue('mobile_phone') + ' to the participant array');
    participants.push(user.getUniqueValue());
}

// define a source record to associate with the conference call
var source = new GlideRecord("cmdb_ci");
source.query("asset_tag", "P1000167");
if (source.hasNext() && source.next()) {
    // set up conference call
    var nn = new SNC.NotifyNow();
    var conferenceCall = nn.initiateConferenceCall(participants, 'testing 1 2', source);
    // check if the conference call was successfully created
    if (conferenceCall != null) {
        gs.log('started conference call: ' + conferenceCall.getUniqueValue());
    } else {
        gs.log('could not start the conference call :(');
    }
}
```

### NotifyNow - isCallable(String participant)

Determines whether a user is callable or not.

A user must have a valid phone number to be callable. A user who is already in an active session is not callable.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>participant</td>
<td>String or GlideRecord</td>
<td>A sys_user or notifynow_participant record, or an E.164-compliant phone number.</td>
</tr>
<tr>
<td>Returns</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td><strong>Description</strong></td>
<td></td>
</tr>
<tr>
<td>boolean</td>
<td>Whether this participant can be called or not.</td>
<td></td>
</tr>
</tbody>
</table>

```
var nn = new SNC.NotifyNow();
gs.log('by number: ' + nn.isCallable('+31612345678'));

var user = GlideRecord('sys_user');
user.query('sys_id', '13d39544eb5201003cf587b9d106fea9');
if (user.hasNext() && user.next())
gs.log('by user: ' + nn.isCallable(user));

var participant = GlideRecord('notifynow_participant');
participant.query('sys_id', '33b11430eb1201003cf587b9d106feb9');
if (participant.hasNext() && participant.next())
gs.log('by participant: ' + nn.isCallable(participant));
```

**NotifyNow - isSMSCapable()**

Checks if the telephone number associated with the Twilio account is capable of sending SMS messages.

**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>Whether the telephone number associated with the Twilio account is capable of sending SMS messages.</td>
</tr>
</tbody>
</table>

```
gs.log('The twilio number is SMS capable: ' + ((new SNC.NotifyNow().isSMSCapable()) ? 'yes' : 'no'));
```

**NotifyNow - isSMSCapable(String userID)**

Checks if a user is able to send SMS messages.
Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>userID</td>
<td>String</td>
<td>The sys_id of the user you want to check for an SMS-capable phone number.</td>
</tr>
</tbody>
</table>

Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boolean</td>
<td>If the user can send SMS messages.</td>
</tr>
</tbody>
</table>

```
gs.log('the user is able to send SMS messages (e.g. has a SMS device): ' + ((new SNC.NotifyNow().isSMSCapable('<user sys_id>')) ? 'yes' : 'no'));
```

NotifyNow - isVoiceCapable()

Checks if the telephone number associated with the Twilio account is capable of setting up phone calls.

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>Whether the telephone number associated with the Twilio account is capable of setting up phone calls.</td>
</tr>
</tbody>
</table>

```
gs.log('the Twilio number is Voice capable: ' + ((new SNC.NotifyNow().isVoiceCapable()) ? 'yes' : 'no'));
```

NotifyNow - isVoiceCapable(String userID)

Checks if a user is able to make voice calls.
## NotifyNow - kick(GlideRecord participant)

Removes a participant from a conference call.

### Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>participant</td>
<td>GlideRecord</td>
<td>The conference call participant to remove from the call.</td>
</tr>
</tbody>
</table>

### Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boolean</td>
<td>True if the participant was removed, otherwise false.</td>
</tr>
</tbody>
</table>

```javascript
var participantId = "<participant sys_id>";
var participant = new GlideRecord('notifynow_participant');
participant.get(participantId);
if (participant.isValid()) {
  // kick participant
  result = new SNC.NotifyNow().kick(participant);
  gs.log('participant kicked: ' + result);
}
```

## NotifyNow - mute(GlideRecord participant)

Mutes a participant on a conference call.

### Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>participant</td>
<td>GlideRecord</td>
<td>The conference call participant to mute.</td>
</tr>
</tbody>
</table>

### Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boolean</td>
<td>True if the participant was muted, otherwise false.</td>
</tr>
</tbody>
</table>

```javascript
var participantId = "<participant sys_id>";
var participant = new GlideRecord('notifynow_participant');
participant.get(participantId);
if (participant.isValid()) {
  // mute participant
  result = new SNC.NotifyNow().mute(participant);
  gs.log('participant muted: ' + result);
}
```
Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>participant</td>
<td>GlideRecord</td>
<td>The conference call participant to mute.</td>
</tr>
</tbody>
</table>

Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boolean</td>
<td>True if the participant was muted, otherwise false.</td>
</tr>
</tbody>
</table>

```javascript
var participantId = "<participant sys_id>";
var participant = new GlideRecord('notifynow_participant');
participant.get(participantId);
if (participant.isValid()) {
    // mute participant
    result = new SNC.NotifyNow().mute(participant);
    gs.log('participant muted: ' + result);
}
```

**NotifyNow - umute(GlideRecord participant)**

Unmutes a participant on a conference call.

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>participant</td>
<td>GlideRecord</td>
<td>The muted conference call participant to unmute.</td>
</tr>
</tbody>
</table>

Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boolean</td>
<td>True if the participant was unmuted, otherwise false.</td>
</tr>
</tbody>
</table>

```javascript
var participantId = "<participant sys_id>";
var participant = new GlideRecord('notifynow_participant');
participant.get(participantId);
if (participant.isValid()) {
    // unmute participant
    result = new SNC.NotifyNow().unmute(participant);
    gs.log('participant unmuted: ' + result);
}
```
**NotifyNow - sendEmailQuestion(String emailAddress, String question, GlideRecord sourceRecord, String emailSubject)**

Send an email question to an email address.

The sendEmailQuestion method produces a question body and requires users to click a link to indicate their choice.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>emailAddress</td>
<td>String</td>
<td>Email address to send the question to.</td>
</tr>
<tr>
<td>question</td>
<td>String or GlideRecord</td>
<td>The question record to send or the sys_id of a question record.</td>
</tr>
<tr>
<td>sourceRecord</td>
<td>GlideRecord</td>
<td>An optional source record to associate to the SMS question, such as an incident.</td>
</tr>
<tr>
<td>emailSubject</td>
<td>String</td>
<td>Optional text to override the default email subject.</td>
</tr>
</tbody>
</table>

**Returns**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>The conversation sys_id.</td>
</tr>
</tbody>
</table>

This example demonstrates using the default email subject.

```java
var user = GlideRecord("sys_user");
user.get("email", "someone@somedomain.com");

ew SNC.NotifyNow().sendEmailQuestion(user.getValue('email'), "b6b34500bf3111003cf585ce2c0739ce", user);
```

This example uses dot-walking and specifies a source record and email subject.

```java
new SNC.NotifyNow().sendEmailQuestion("someone@somedomain.com", "b6071733bf1111003cf585ce2c07390f", current, "Please answer this question");
```

This example uses dot-walking and specifies an email subject but no source record.

```java
new SNC.NotifyNow().sendEmailQuestion("someone@somedomain.com", "b6071733bf1111003cf585ce2c07390f", "Please answer this question");
```
**NotifyNow - sendSMS(String phoneNumber, String smsBody)**

Sends an SMS message to an E.164-compliant mobile phone number.

Notify supports international numbers. Using this method with a number that does not support sending SMS messages results in an error being logged.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>phoneNumber</td>
<td>String</td>
<td>The E.164-compliant phone number to send the message to.</td>
</tr>
<tr>
<td>smsBody</td>
<td>String</td>
<td>The message to send, maximum 1600 characters.</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>

```java
new SNC.NotifyNow().sendSMS("+31612345678", "This is a message without source record");
```

**NotifyNow - sendSMS(String phoneNumber, String smsBody, GlideRecord source)**

Sends an SMS message to an E.164-compliant mobile phone number.

Notify supports international numbers. Using this method with a number that does not support sending SMS messages results in an error being logged.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>phoneNumber</td>
<td>String</td>
<td>The E.164-compliant phone number to send the message to.</td>
</tr>
<tr>
<td>smsBody</td>
<td>String</td>
<td>The message to send, maximum 1600 characters.</td>
</tr>
<tr>
<td>source</td>
<td>GlideRecord</td>
<td>The source record to associate with this SMS message.</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>

```java
var source = new GlideRecord("my_table");
```
source.query("my_field", "my_value");

if (source.hasNext() && source.next()) {
    // send a text message
    var nn = new SNC.NotifyNow();
    var message = "this is just a test";
    var number = "+31612345678";
    nn.sendSMS(number, message, source);
}

This example uses dot-walking and the current record as the source record.

new SNC.NotifyNow().sendSMS("+31612345678", "this is a test", current);

**NotifyNow - sendSMSQuestion(String phoneNumber, String question, GlideRecord sourceRecord)**

Sends an SMS question.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>phoneNumber</td>
<td>An E.164-compliant phone number</td>
<td>to send the message to.</td>
</tr>
<tr>
<td>question</td>
<td>String or GlideRecord</td>
<td>The question record to send or the sys_id of a question record.</td>
</tr>
<tr>
<td>sourceRecord</td>
<td>An optional source record to</td>
<td>associate to the SMS question, such as an incident.</td>
</tr>
</tbody>
</table>

**Returns**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>The conversation sys_id, or null if the SMS was not sent successfully.</td>
</tr>
</tbody>
</table>

var question = new GlideRecord("notifynow_question");
question.query();

// get the first question
if (question.hasNext() && question.next()) {
    // send the sms question
    var number = "+31612345678";
    var nn = new SNC.NotifyNow();
    nn.sendSMSQuestion(number, question.getUniqueValue(), current);
}
**NotifyNow - addConferenceCallParticipant(String conferenceCall, String participant)**

Adds ad-hoc users to an ongoing conference call.

When the method is called with a phone number for the participant parameter and there is exactly one sys_user record that matches the phone number, that sys_user record will be related to the participant. The participant's phone number field will be left blank because the phone number is in the sys_user record. If there are several sys_user records that match the phone number, or if there are no results, the participant's phone number field will be filled in, and there will be no stored reference to sys_user because the user is not known.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>conferenceCall</td>
<td>String or GlideRecord</td>
<td>The sys_id or GlideRecord of an active conference call.</td>
</tr>
<tr>
<td>participant</td>
<td>String or GlideRecord</td>
<td>The sys_id or GlideRecord of a user with an E.164-compliant phone number, or an E.164-compliant phone number.</td>
</tr>
</tbody>
</table>

**Returns**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GlideRecord</td>
<td>The participant record of the new participant that was added to the conference call.</td>
</tr>
</tbody>
</table>

```javascript
// add a new participant by conference call sys_id (string) and phone number (string)
var nn = new SNC.NotifyNow();
gs.log(nn.addConferenceCallParticipant('d193b242eb020100a04d4910f206fe39', '+31612345678'));

// add a new participant by conference call sys_id (string) and user record (GlideRecord)
var user = new GlideRecord('sys_user');
user.query('user_name', 'myUserName');
if (user.hasNext() && user.next()) {
    var nn = new SNC.NotifyNow();
    gs.log(nn.addConferenceCallParticipant('d193b242eb020100a04d4910f206fe39', user));
    // you could have added the user by sys_id as well:
    //
    nn.addConferenceCallParticipant('d193b242eb020100a04d4910f206fe39', user.getValue('sys_id'));
} else {
    gs.log('no such user');
```
// add a new participant by conference call record (GlideRecord) and phone number (string)
var conferenceCall = new GlideRecord('notifynow_conference_call');
conferenceCall.query('title', 'IA0001001');
if (conferenceCall.hasNext() && conferenceCall.next()) {
    var nn = new SNC.NotifyNow();
    gs.log(nn.addConferenceCallParticipant(conferenceCall, '+31612345678'));
} else {
    gs.log('no such conference call');
}

NotifyNow - convertLocalPhoneNumberToE164(String userID, String phoneNumber)

Converts a local phone number to an E.164-compliant phone number based on a user's location.

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>userID</td>
<td>String</td>
<td>The sys_id of a sys_user record to get location information from.</td>
</tr>
<tr>
<td>phoneNumber</td>
<td>String</td>
<td>The phone number.</td>
</tr>
</tbody>
</table>

Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>The E.164-compliant phone number.</td>
</tr>
</tbody>
</table>

var localPhoneNumber = '01784 221600';
var userName = 'Heath Vanalphen';

var user = new GlideRecord('sys_user');
user.get('name', userName);
var E164Number = new SNC.NotifyNow().convertLocalPhoneNumberToE164(user.getUniqueValue(), localPhoneNumber);
gs.log('converted: ' + localPhoneNumber + ' to ' + E164Number + ' based on ' + user.getValue('name') + '
's location (' + user.getValue('location') + ')');
NotifyNow - getConferenceCallParticipants(String conferenceCallId, Boolean isCallable)

Returns all participants for a conference call.

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>conferenceCallId</td>
<td>String</td>
<td>The ID of the conference call.</td>
</tr>
<tr>
<td>isCallable</td>
<td>Boolean</td>
<td>An optional flag to return either only the users you can call (true) or those you cannot call (false).</td>
</tr>
</tbody>
</table>

Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GlideRecord</td>
<td>The participants</td>
</tr>
</tbody>
</table>

```javascript
var nn = new SNC.NotifyNow();
var user =
nn.getConferenceCallParticipants('c2e91710eb120100f34087b9d106fe37');

while (user.hasNext() && user.next()) {
  if (user.getValue('participant')) {
    gs.log('user: ' + user.getValue('sys_id'));
  } else {
    gs.log('phone number: ' +
           user.getValue('phone_number'));
  }
}
```

```javascript
var nn = new SNC.NotifyNow();
var user =
nn.getConferenceCallParticipants('c2e91710eb120100f34087b9d106fe37',
                                 true);

while (user.hasNext() && user.next()) {
  if (user.getValue('participant')) {
    gs.log('user: ' + user.getValue('sys_id'));
  } else {
    gs.log('phone number: ' +
           user.getValue('phone_number'));
  }
}
```

```javascript
var conferenceCallId = '32b11430eb1201003cf587b9d106feb8';
// get all participants
```
gs.log('all conference call participants:');
var nn = new SNC.NotifyNow();
var user = nn.getConferenceCallParticipants(conferenceCallId);
gs.log(user);

// get all callable participants
gs.log('all conference call participants we can call:');
user = nn.getConferenceCallParticipants(conferenceCallId, true);
gs.log(user);

// get all un callable participants
gs.log('all conference call participants that are already in an active session and whom we cannot call:');
user = nn.getConferenceCallParticipants(conferenceCallId, false);
gs.log(user);

NotifyNow - getFrequentlyCalledUsers(Number limit)

Returns a number of frequently-called users, up to the limit parameter, in alphabetical order.

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>limit</td>
<td>Number</td>
<td>The maximum number of results.</td>
</tr>
</tbody>
</table>

Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GlideRecord</td>
<td>The frequently called users in alphabetical order.</td>
</tr>
</tbody>
</table>

var nn = new SNC.NotifyNow();
var fc = nn.getFrequentlyCalledUsers(10);

while (fc.hasNext() && fc.next()) {
gs.log("got user " + fc.getValue('name') + ' - ' + fc.getValue('sys_id'));
}

NotifyNow - getPreferredE164VoiceNumber(GlideRecord user)

Returns a user's preferred E.164-compliant phone number for voice calls.

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>GlideRecord or String</td>
<td>The user record or the sys_id of a user to get the E.164-compliant phone number from.</td>
</tr>
</tbody>
</table>
returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>The E.164-compliant phone number or null.</td>
</tr>
</tbody>
</table>

```
var userID = "<user sys_id>";
var E164Number = new SNC.NotifyNow().getPreferredE164VoiceNumber(userID);
gs.log('the preferred phone number for setting up voice calls is ' + E164Number + ' for user with id: ' + userID);
```

**NotifyNow - getPreferredE164SMSNumber(GlideRecord user)**

Returns a user's preferred E.164-compliant phone number for SMS messages.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>GlideRecord or String</td>
<td>The user record or the sys_id of a user to get the E.164-compliant phone number from.</td>
</tr>
</tbody>
</table>

returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>The E.164-compliant phone number or null.</td>
</tr>
</tbody>
</table>

```
var userID = "<user sys_id>";
var E164Number = new SNC.NotifyNow().getPreferredE164SMSNumber(userID);
gs.log('the preferred phone number for sending SMS notifications is ' + E164Number + ' for user with id: ' + userID);
```

**NotifyNow - getPreferredEmailAddress(GlideRecord user)**

Returns a user's preferred email address

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>GlideRecord or String</td>
<td>The user record or the sys_id of a user to get the email address from.</td>
</tr>
</tbody>
</table>
### Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>The email address or null.</td>
</tr>
</tbody>
</table>

```
var userID = "some user sys id";
var email = new SNC.NotifyNow().getPreferredEmailAddress(userID);
gs.log('the preferred email address for sending email notifications is ' + email + ' for user with id: ' + userID);
```

#### Legacy: Chat

Legacy chat provides real-time communication via instant messaging between users in a ServiceNow instance.

**Note:** The Connect feature provides an updated instant messaging platform, which is activated by default for new instances. The legacy chat and Connect features should not be used concurrently. There is no migration path from legacy chat to Connect.

Chat provides real-time communication via instant messaging between users in a ServiceNow instance. Features include:

- One-to-one chats (instant messaging) between users.
- Chat rooms for conversations with multiple users. Chat rooms may be public (any user can join) or private (only invited users can join).
- Chat rooms linked to task records. Users can work together to solve issues, and conversation history can be shared by everyone who needs to reference it.
- Help desk chat. End users can access live support via instant messaging. Service desk staff can resolve basic issues in real-time or create incidents directly from chat requests for more extensive issues.
Legacy: Get started with Chat

Get started with legacy chat.

Role required: admin

1. Establish use guidelines. Social media can improve communication and aid productivity. To get the most out of these tools, establish clear and simple social media guidelines that foster information sharing and a comfortable work environment.

2. Activate the Chat plugin to enable the legacy chat and legacy Help Desk Chat features.

3. Configure security settings. Users must log in to use the legacy chat features in the base system. The standard system security settings and Social IT-specific security settings are available. To learn more about setting up these features, refer to the plugin activation pages.

   - Chat rooms may be Public (any user can join) or Private (only invited users can join).
- Administrators can limit who can read chat messages on tasks and who can create chat rooms.

**Legacy: Installed with Chat**

What components are installed with legacy chat.

Demo data is available for legacy chat. The demo data creates a chat queue called Help Desk Chat that is supported by the assignment group Chat Support. Additionally, the Help Desk Chat link is added to the header of the Employee Self-Service portal. To learn more, see [Set Up Chat Queues for Help Desk Chat](#).

Other:
- Event: A new event called `chat.invite` is registered to trigger an email notification when users are invited into a chat room.
- Email Notification: An email notification called Chat Room Invite is added to send when users are invited to a chat room.

**Legacy: Fields installed with legacy chat**

Legacy chat adds the following fields.

<table>
<thead>
<tr>
<th>Display name (Table name)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Header</td>
<td>Adds the Help Desk Chat link to the ESS portal page.</td>
</tr>
<tr>
<td>(content_block_header)</td>
<td></td>
</tr>
</tbody>
</table>

**Legacy: Properties installed with legacy chat**

Legacy chat adds the following properties.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.chat.invite_fields</td>
<td>Comma-separated list of fields used to generate the invites when creating a chat room from a task. The user is presented with check boxes for each of the specified fields to select the invites for the chat room. The fields should be references or glide_lists of sys_user or sys_user_group.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Type</strong>: string</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default value</strong>: assignment_group.watch_list</td>
</tr>
<tr>
<td></td>
<td>• <strong>Location</strong>: Social IT &gt; Chat Administration &gt; Properties</td>
</tr>
<tr>
<td>glide.chat.show_emoticons</td>
<td>Setting that determines whether to display emoticons in conversations.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Type</strong>: true</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default value</strong>: true</td>
</tr>
<tr>
<td></td>
<td>• <strong>Location</strong>: Social IT &gt; Chat Administration &gt; Properties</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| glide.chat.sound.message_received.mp3 | Sound played when a message is received in chat (mp3).  
  - **Type**: string  
  - **Default value**: media/rcvmsg.mp3  
  - **Location**: Social IT > Chat Administration > Properties |
| glide.chat.sound.message_received.ogg | Sound played when a message is received in chat (ogg).  
  - **Type**: string  
  - **Default value**: media/rcvmsg.oggx  
  - **Location**: Social IT > Chat Administration > Properties |
| glide.chat.sound.queue_beep.mp3 | Sound played when a new user enters the chat queue (mp3). Both this property and `glide.chat.sound.queue_beep.ogg` must be defined for either property to work.  
  - **Type**: string  
  - **Default value**: media/button_toggle_on.mp3x  
  - **Location**: Social IT > Chat Administration > Properties |
| glide.chat.sound.queue_beep.ogg | Sound played when a new user enters the chat queue (ogg).  
  - **Type**: string  
  - **Default value**: media/button_toggle_on.oggx  
  - **Location**: Social IT > Chat Administration > Properties |
| glide.chat_room.create_roles | Comma-separated list of roles that are allowed to create chat rooms.  
  - **Type**: string  
  - **Default value**: itil  
  - **Location**: Social IT > Chat Administration > Properties |
| glide.short_poll_delay | Short polling delay for XMPP requests. Enter a value in milliseconds. The minimum value is 250. With short polling, the browser sends a request to the server in fixed intervals defined by the property. To minimize performance impact, it is recommended that this value is set greater than or equal to the default value.  
  - **Type**: integer  
  - **Default value**: 1000 (one second)  
  - **Location**: Social IT > Chat Administration > Properties |
### Legacy: Script includes installed with legacy chat

Legacy chat adds the following script includes.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ChatUtils</td>
<td>Provides utilities for chat conversations.</td>
</tr>
</tbody>
</table>

### Legacy: Tables installed with legacy chat

Legacy chat adds the following tables.

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chat Actions (chat_actions)</td>
<td>Defines additional chat window menu items. Access at Social IT &gt; Chat Administration &gt; Actions (administrator and chat_admin).</td>
</tr>
<tr>
<td>Chat Channel (chat_channel)</td>
<td>Stores chat channels, which are chats between members. This table is extended by Chat thread (chat_thread) (a one-to-one chat) and chat_room (a multi-user chat). Extending or modifying data in this table is not recommended.</td>
</tr>
<tr>
<td>Chat Channel Member (chat_channel_member)</td>
<td>Relationship table that associates channels and members. Extending or modifying data in this table is not recommended.</td>
</tr>
<tr>
<td>Chat Message (chat_message)</td>
<td>Stores instant messages sent from any chat window. Extending or modifying data in this table is not recommended.</td>
</tr>
<tr>
<td>Chat Presence (chat_presence)</td>
<td>Stores presence (status) information for a user. Extending or modifying data in this table is not recommended.</td>
</tr>
<tr>
<td>Chat Queue (chat_queue)</td>
<td>Stores the groups and schedules for providing support via instant message. Defined at Social IT &gt; Chat Administration &gt; Queues (administrator and chat_admin).</td>
</tr>
<tr>
<td>Chat Queue Entry (chat_queue_entry)</td>
<td>Stores user requests for live support. Extends Task (task). On a chat queue record, the Chat queue entries related list displays the entries that are associated with that chat queue. Extending or modifying data in this table is not recommended.</td>
</tr>
<tr>
<td>Chat Room (chat_room)</td>
<td>Stores chat rooms (multi-user chat). Extends Chat channel (chat_channel). Can be modified if necessary (such as to change a chat room from public to private), but should almost always be managed by system functionality.</td>
</tr>
<tr>
<td>Chat Roster (chat_roster)</td>
<td>Maintains users that are associated with a user's My Friends list. Extending or modifying data in this table is not recommended.</td>
</tr>
<tr>
<td>Chat Roster Member (chat_roster_member)</td>
<td>Tracks users that are members of a chat room. Extending or modifying data in this table is not recommended.</td>
</tr>
</tbody>
</table>
### Table

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chat Thread (chat_thread)</td>
<td>Stores one-to-one chats. Extends Chat channel (chat_channel). Extending or modifying data in this table is not recommended.</td>
</tr>
<tr>
<td>Live Headline (live_headline)</td>
<td>Sends system messages. For example, the system may send a message when a user enters or leaves a chat room. Extending or modifying data in this table is not recommended.</td>
</tr>
<tr>
<td>Live Poll Message (sys_live_message)</td>
<td>System table that stores and manages chat messages. Extending or modifying data in this table is not recommended.</td>
</tr>
<tr>
<td>Live User (sys_live_user)</td>
<td>System table that stores and maintains chat users. Extending or modifying data in this table is not recommended.</td>
</tr>
<tr>
<td>Stores the last live sequence number (sys_live_last_sequence)</td>
<td>Stores the last sequence ID. Extending or modifying data in this table is not recommended.</td>
</tr>
</tbody>
</table>

### Legacy: Business rules installed with legacy chat

Legacy chat adds the following business rules.

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chat Queue (Task.active) Updater</td>
<td>Chat Queue Entry (chat_queue_entry)</td>
<td>Sets the chat queue entry Action field to Waiting when the action changes.</td>
</tr>
<tr>
<td>SNC - Chat Queue Average Wait Time</td>
<td>Chat Queue Entry (chat_queue_entry)</td>
<td>When a chat queue entry is accepted, calculates the average wait time for the queue by averaging the last 20 chat queue entries.</td>
</tr>
</tbody>
</table>

### Legacy: Chat use

Legacy chat allows you to interact and collaborate through real-time instant messages with other users in an instance.

Use legacy chat to:

- Initiate or participate in chat conversations with one or multiple users.
- Initiate or participate in chat conversations that are attached to task records (such as an incident).
- See when other users are available to chat.

To open the chat desktop, navigate to **Social IT > Chat**.

**Note:** Service desk staff may also provide live support to other users via help desk chat.
Legacy: Update your profile

Your profile identifies your contributions to legacy chat conversations. It is created automatically the first time you use chat and consists of:

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>From your user account in ServiceNow. Your name appears on your messages and in the member list of any chat room you join.</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Picture</td>
<td>Select any picture. Your picture appears beside your name in other users' favorites list and at the top of your favorites list.</td>
</tr>
</tbody>
</table>

To update your profile picture:

1. Click your picture in the top of the favorites list.
2. Browse to the desired picture file and click **Open**.

**Note:** Changes to your profile picture affect legacy chat and live feed if the Live Feed plugin is activated.

![Chat profile picture](image.png)

**Legacy: Update your status**

In legacy chat, your status lets other users know whether you are available to chat. Your status lets other users know whether you are available to chat. Your current status is indicated by the color of the icon in the upper right of your favorites list, beside your name. View the status of other users in your favorites list.

To change your status:

1. Click the status icon beside your name.
2. Select a status (see table).
### Change status

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
<th>Appears to others</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Online</strong></td>
<td>Indicates that you are available to chat.</td>
<td>Green icon:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Beth Anglin</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Chat available</td>
</tr>
<tr>
<td><strong>Away</strong></td>
<td>Indicates that you are not available because you are away.</td>
<td>Red icon:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Beth Anglin</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Away</td>
</tr>
<tr>
<td><strong>Away with a message</strong></td>
<td>Indicates that you are not available and gives a reason:</td>
<td>Red icon and message:</td>
</tr>
</tbody>
</table>
|                   |     • In a meeting
|                   |     • On the phone
<p>|                   |     • Out to lunch                                                         | <strong>Beth Anglin</strong>                                                                   |
|                   |                                                                             | In a meeting                                                                      |
|                   |                                                                             | Chat away msg                                                                     |
| <strong>Invisible</strong>     | Indicates that you are not available. You can send and receive messages when your status is Invisible. You appear as Offline to other users. | Black icon:                                                                       |
|                   |                                                                             | <strong>Beth Anglin</strong>                                                                   |
|                   |                                                                             | Chat offline                                                                      |</p>
<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
<th>Appears to others</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offline</td>
<td>Indicates that you are not available. You cannot send or receive messages when your status is Offline. Users that are not logged in appear as Offline.</td>
<td>Black icon: Beth Anglin Chat offline</td>
</tr>
</tbody>
</table>

**Legacy: Use your favorites list**

In legacy chat, your favorites list appears on your chat desktop and provides certain functions.
Favorites list

- Users:
  - **Add another user** in the system to your favorites list.
  - See if your favorite users are available to chat. Users are organized alphabetically and in sections by status.
  - Start a conversation by double-clicking a name.
  - Expand or collapse a section by clicking **Online** or **Offline**.

- Rooms:
  - See the list of your favorite chat rooms.
  - Join a chat room by double-clicking its name.

- Favorites list toolbar:
  - Options ()
    - **Chat window menu**: access a menu with options to **add a favorite user**, **view online users**, **create a chat room**, and **view chat rooms**.
  - **Add User** ()
    - **Add friend**: **add a favorite user**.
  - **Create Room** ()
    - **Add room**: **create a chat room**.
  - **Invitations** ()
    - **Chat invitation**: respond to invitations to **join chat rooms**.

To expand or collapse a section in the favorites list, click the section header or click the arrows () on the section header.
Legacy: Add a favorite user
How to add a user to your favorite users list in legacy chat.

1. Click the Add User button.

    ![Add friend]

2. Begin typing a user name and select a user from the list, or click the reference lookup and select a user from the table.

    ![Search icon]

3. Click OK.

Legacy: Remove a favorite user
How to remove a favorite user in legacy chat.

To remove a user from your favorite users list, right-click the user’s name and select Remove From List.

Legacy: View an online user
How to view a list of all users who are available to chat (status of Online) in legacy chat.

1. Right-click the Users section header or click Options on the toolbar.

    ![Chat window menu]

2. Select Show Online Users.
   - Start a one-to-one chat with a user on the list by double-clicking a name.
   - Send Message or Add To Friend List by right-clicking a name.
Legacy: View a room

How to view a list of all public chat rooms in legacy chat.

1. Right-click the Rooms section header or click Options on the toolbar.

2. Select Public Rooms.
   - To join a room, double-click a name or right-click and select Join Room. See Joining Chat Rooms.
Legacy: Start a one-to-one chat

How to start a one-to-one chat in legacy chat:

- To start a chat with one user in your favorites list, double-click the user's name or right-click and select Send Message.
- To start a chat with one available user, double-click the user's name on the online users list. See Viewing Online Users.
  Send a message to start a conversation.

Legacy: Create a chat room

How to start a chat with multiple users from the legacy chat desktop.

To start a chat with multiple users from the chat desktop (requires access rights):

1. Click Create Room on the favorites list toolbar.

2. Enter the room details (see table).
3. Click Create Room. An invitation appears in the favorites list of all invited users and a new chat window opens on your chat desktop.
Create Room

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Room name</td>
<td>Chat Room for ENC0000003</td>
</tr>
<tr>
<td>Description</td>
<td>Wireless access not available on floor 3</td>
</tr>
<tr>
<td>Password</td>
<td>****</td>
</tr>
<tr>
<td>Room availability</td>
<td></td>
</tr>
<tr>
<td>Public</td>
<td></td>
</tr>
<tr>
<td>Members Only</td>
<td>A room that a user cannot enter without being on the member list or invited.</td>
</tr>
<tr>
<td>Temporary</td>
<td>A room that is destroyed if the last occupant exits.</td>
</tr>
</tbody>
</table>

Invite:
- Fred Luddy
- Beth Anglin
- ITIL User

Options:
- Assignment group
- Watch list

Create Room | Cancel
## Chat task create

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Room name</td>
<td>Enter a name to appear on the chat window header or click the <strong>Generate a unique room name</strong> button (Room name generator) to use a system-generated name. The default name for a room created from a task is Chat Room for &lt;Task Number&gt;.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a room description that appears under the name in the rooms list. The default description for a room created from a task is &lt;Short Description&gt;.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter a password, if desired. If a password is specified, only users with the password can join the chat room.</td>
</tr>
<tr>
<td>Room avatar</td>
<td>Upload an image that appears beside the room name in the list of rooms. Click the picture and browse to the desired image file.</td>
</tr>
<tr>
<td>Features</td>
<td>Select all applicable check boxes:</td>
</tr>
<tr>
<td></td>
<td>• Public if all users can see the room in the rooms lists.</td>
</tr>
<tr>
<td></td>
<td>• Members Only if only invited users can join the room.</td>
</tr>
<tr>
<td></td>
<td>• Temporary if the room is not saved once all participants have left. This feature is not available for rooms created from tasks; task chat rooms are always available on the task record.</td>
</tr>
<tr>
<td>Invite</td>
<td>Add invited users by using the <strong>glide list</strong>. For a room created from a task, you can also select all applicable check boxes:</td>
</tr>
<tr>
<td></td>
<td>• Assignment group: invite all users in the assignment group for the task.</td>
</tr>
<tr>
<td></td>
<td>• Watch list: invite all users on the watch list for the task.</td>
</tr>
</tbody>
</table>

### Legacy: Create a chat room for a task

How to start a legacy chat with multiple users from a task record.

**Note:** This procedure is not possible if the **Connect** feature is enabled.

1. Open the record (example, an incident on which you are working).
Chat task link

2. Click the Create or Join Chat Room related link.
3. If a chat room already exists, click a name to join the existing chat room. If no chat room exists, continue to the next step to create a new room.

Chat task open

4. Click the create link at the bottom of the window.
5. Enter the room details as you would for a chat room.
6. Click Create Room. An email notification is sent and appears in the favorites list for all invited users (the assignment group and the watch list, if selected, and additional invited users).
7. In the New Room Created message, click Join Room.
   - A new chat window opens on your chat desktop.
- All invited users are listed in the chat member list. Invited users that are not currently participating in the chat are listed in gray.

**Legacy: Join one-to-one chats**

In legacy chat, when another user starts a chat by sending a message to you, a chat window opens on your chat desktop. To join the chat, click the window.

**Legacy: Join a chat room**

How to join a chat room in legacy chat.

1. If another user invites you to join a chat room, an invitation appears in your favorites list.

   ![Chat invitation](image)

   Chat invitation

2. To respond, click the invitation.

   A window opens that displays the room name, room description, and the name of the user who invited you.

   - To join the chat, click **Join**. When the chat window opens on your chat desktop, click the window.
   - To ignore the invitation, click **Decline**.

   ![Chat Room for INC0000003 - Wireless access not available on floor 3](image)

   Chat Room for INC0000003 - Wireless access not available on floor 3
   
   Invited By: System Administrator
   
   Emergency CAB meeting
   
   Review change that fixes voicemail error
   
   Invited By: System Administrator

   ![Chat Room for INC0000003 - Wireless access not available on floor 3](image)

   Chat Room for INC0000003 - Wireless access not available on floor 3
   
   Invited By: System Administrator
   
   Emergency CAB meeting
   
   Review change that fixes voicemail error
   
   Invited By: System Administrator

   View invitations

   To rejoin a favorite chat room that you have left, click the chat room name in the Rooms section of the favorites list.

   To join a public chat room without an invitation, right-click the Rooms section header and select **Public Rooms**. Double-click a room name on the list.

**Legacy: Join a chat room for a task**

In legacy chat, if another user invites you to join a chat room from a task record, you receive an email notification.

1. Click the link in the email notification.
2. If a prompt for a password appears, enter the password listed in the email notification.
3. When the chat window opens on your chat desktop, click the window.

**Legacy: Join a chat room from a task record without an invitation**

How to join a chat room in legacy chat without an invitation.

**Note:** This procedure is not possible if the Connect feature is enabled.

1. Open the task record.
2. Click the Create or Join Chat Room related link.
3. Click a chat room name.
4. If a prompt for a password appears, contact the person who created the chat room for the password.
   - If a chat room has a password, only users with the password can join the chat.
5. When the chat window opens on your chat desktop, click the window.

**Legacy: Chat windows**

In legacy chat, a chat window appears on your chat desktop for each chat conversation that you start or join.
Legacy: Send messages in legacy chat

How to send messages in legacy chat.

To chat with other users that have joined the conversation, enter your message in the text field at the bottom of the window and press Enter. The message appears in the other users’ chat windows.

To send a link, type the full URL (example, http://www.service-now.com). When the message is sent, the text appears blue and any user in the conversation can click it to follow the link.

To send a smiley face, type a colon followed by a close parentheses (:)). When the message is sent, a smiley face 😊 appears in place of the text. For more emoticons, see Sending Emoticons in Messages (Smileys).

Chat activity is indicated with the following alerts:

- When a new message is posted to an inactive browser tab, the tab name blinks.
- When a new message is posted to an inactive chat window, the window header appears in yellow and blinks.
• When a user joins or leaves a room, a message appears in the other room members' chat windows.

Legacy: Send emoticons in legacy chat messages (smiley)

How to send emoticons (smiley) in legacy chat.

To send an emoticon (smiley), type text from the following table. When your message is sent, the emoticon appears in place of the text. For example, enter colon followed by a close parentheses (:) and a smiley face (😊) appears in your message.

<table>
<thead>
<tr>
<th>Emoticons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text</td>
</tr>
<tr>
<td>:)</td>
</tr>
<tr>
<td>:-)</td>
</tr>
<tr>
<td>B-)</td>
</tr>
<tr>
<td>B-) BD</td>
</tr>
<tr>
<td>:D</td>
</tr>
<tr>
<td>:-D</td>
</tr>
<tr>
<td>:*</td>
</tr>
<tr>
<td>:*(</td>
</tr>
<tr>
<td>:{</td>
</tr>
<tr>
<td>:{(</td>
</tr>
<tr>
<td>&lt;3</td>
</tr>
<tr>
<td>;)</td>
</tr>
<tr>
<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>Text</th>
<th>Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>:P :P</td>
<td>😞</td>
</tr>
<tr>
<td></td>
<td>Playful</td>
</tr>
<tr>
<td>:O :O</td>
<td>😞</td>
</tr>
<tr>
<td></td>
<td>Surprise</td>
</tr>
<tr>
<td>X( X(</td>
<td>😜</td>
</tr>
<tr>
<td></td>
<td>Angry</td>
</tr>
<tr>
<td>:) :)</td>
<td>😄</td>
</tr>
<tr>
<td></td>
<td>Blush</td>
</tr>
<tr>
<td>:(( :((</td>
<td>😞</td>
</tr>
<tr>
<td></td>
<td>Crying</td>
</tr>
<tr>
<td>(A)</td>
<td>😢</td>
</tr>
<tr>
<td></td>
<td>Halo</td>
</tr>
<tr>
<td>:? :?</td>
<td>😡</td>
</tr>
<tr>
<td></td>
<td>Undecided</td>
</tr>
</tbody>
</table>

**Legacy: Change the display**

How to change the display of legacy chat.

To view the chat window menu, click the gear button ()

Chat window menu

) in the bottom left.

- To show or hide timestamps, select **Show Timestamps** from the chat window menu or press **F2**.
- To show or hide the chat member list, select **Show Members** from the chat window menu or press **F4**.
To resize the window, point to the lower corner (left or right). When the pointer changes shape, drag the window to the desired size.

To move the window, point to the header. When the pointer changes shape, drag the window anywhere on your chat desktop.

To close a chat window, click the X in the upper right corner.

**Legacy: Invite a user into a chat**

How to invite another user into a chat in legacy chat.

1. Select **Invite User** from the chat window menu.

2. Begin typing a user name and select a user from the list, or click the reference lookup and select a user from the table.

3. Click **OK**.

   An invitation is sent to the selected user. One-to-one chats are automatically converted into temporary chat rooms.

**Legacy: Add a favorite room**

How to add a favorite room in legacy chat.

To add a room to your favorites, click the chat window and select **Add To Favorites** from the chat window menu.

**Legacy: Remove a favorite room**

How to remove a favorite room in legacy chat.

To remove a room from your favorites, right-click the room name and select **Remove From List**.

**Legacy: Set your chat preferences**

Use the Chat Window Preferences to set audio notifications and default chat window display options in legacy chat.

Use the Chat Window Preferences to set audio notifications and default chat window display options. The default display options control how a chat window looks when you first open it. You can still control the display options for an individual window as described in *Changing the Display*.

To view your chat preferences, click your name in the upper left corner of the chat desktop and select **Chat Preferences**.

© 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.
Chat preferences

To set your preferences, select or clear the check boxes next to the options, then click **Update**.

<table>
<thead>
<tr>
<th>Preferences</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio</td>
<td>Turn audio notifications on or off.</td>
</tr>
<tr>
<td>Conversation Windows</td>
<td>Set default options for showing timestamps and members in one-to-one chats.</td>
</tr>
<tr>
<td>Group Chat Windows</td>
<td>Set default options for showing timestamps members in chat rooms.</td>
</tr>
</tbody>
</table>

**Legacy: Delete a chat room**

You can delete chat rooms in legacy chat.

Role required: chat_admin

Note that when you delete a chat room, the system also deletes the records for any chat members and messages.

1. In the application navigator filter, enter `chat_room.list`
2. Delete multiple chat rooms from the list or open a chat room record and click **Delete**.

**Legacy chat administration**

Users with the chat_admin role can administer various aspects of legacy chat.

**Define chat room access rights**

Control the access rights for creating a chat room so that not all users can create a chat room.

Role required: chat_admin
To define the access rights for creating chat rooms:

1. Navigate to Social IT > Chat Administration > Properties.
2. Locate the property Comma-separated list of roles that are allowed to create chat rooms.
3. Enter user roles. A user must have one of the specified roles to create a chat room.

**Change chat room message read access**

In legacy chat, you can associate a chat room with a record, such as an incident, and add the chat messages to a Chat Activity journal field on the form.

Role required: admin

By default, a user can read the chat messages for a room if either of the following is true:

- The room is public
- The user is a member of the room

To change chat room message read access:

- Modify the Chat message access control rule or create a new rule.

  Read access to the messages displayed is handled by the access control list security operation chat_messages_read on the Chat room (chat_room) table.

**View a legacy chat message as a journal field**

You can view all chat messages in one place by viewing them as a journal field.

Chat rooms can be linked to any task record in the following ways:

- Create a room from the record.
- Create a record from a chat room, such as creating an incident from a Help Desk Chat.

To view the chat messages as a journal field:

- Configure the task record form to select the Chat Activity field.
  The maximum number of chat messages that are displayed by this field is 1000.
Chat Activity

2011-01-21 13:48:35: Chat Room for INC0010010 - I can't access the shared server

2011-01-12 15:11:43: Help Desk Chat - rachel user

[2011-01-12 23:12:05] rachel user: I can't access the shared server

[2011-01-12 23:12:05] Help Desk Chat: Thank you for contacting support. Your principal agent will be with you shortly.


[2011-01-12 23:12:49] Fred Luddy: Where are you?
[2011-01-12 23:12:56] rachel user: I'm at home on the VPN


[2011-01-12 23:13:38] Fred Luddy: I'll open an incident for you to get the update

[2011-01-12 23:14:03] rachel user: Great, thanks!

Chat actions

Chat actions are additional items that appear in the chat window menu (requires the Chat plugin). Administrators and users with the chat_admin role can define chat actions.
Add actions to the legacy chat window menu

You can create new actions and add them to the chat window menu.

1. Navigate to Social IT > Chat Administration > Actions.
2. Select an action to edit or click New.
3. Enter the chat action details and click Update or Submit.

The following example demonstrates how to add a chat action that appears only on windows where the user is a Help Desk Agent. The action appears on the menu as Show User Type and opens a popup window that indicates a current user of queue_agent.

- **Action Name:** Show User Type
- **Active:** Select the check box.
- **Order:** 100
- **Client Show Condition:**
  ```javascript
  answer = g_chat.getChatType() == 'queue_agent';
  ```
- **OnClick Action Script:**
  ```javascript
  alert('The current user is: ' + g_chat.getChatType());
  ```
Chat action details
You can define a chat action name and the script that runs when the action is selected.

Chat action details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action Name</td>
<td>Enter a label for the action as it appears in the menu.</td>
</tr>
<tr>
<td>Active</td>
<td>Select the check box to activate or clear the check box to deactivate the action. Only active actions may appear in the menu.</td>
</tr>
<tr>
<td>Order</td>
<td>Enter the order in which the action appears in the menu. Standard menu items (such as Show Timestamps) always appear at the top of the chat menu, followed by chat actions in order.</td>
</tr>
<tr>
<td>Client Show Condition</td>
<td>Define the conditions under which this menu option appears. The show condition must set the pre-defined answer variable to a boolean value.</td>
</tr>
<tr>
<td>OnClick Action Script</td>
<td>Enter the JavaScript code that runs when the menu item is selected.</td>
</tr>
</tbody>
</table>

Available methods associated with the g_chat variable

The g_chat variable is a legacy chat window object that is available in the Client Show Condition and OnClick Action Script of a chat action definition.

The following table defines the available methods associated with this object.

Method Summary

<table>
<thead>
<tr>
<th>Return Object</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Array</td>
<td><strong>getActiveUsers()</strong>&lt;br&gt;Returns the active users.&lt;br&gt;Returns: Array - Returns the active users.</td>
</tr>
<tr>
<td>String</td>
<td><strong>getChannelJID()</strong>&lt;br&gt;Returns the channel JID, which is a <em>sys_id</em> for a record chat_channel table.&lt;br&gt;Returns: String - Returns the channel JID.</td>
</tr>
<tr>
<td>String</td>
<td><strong>getChatType()</strong>&lt;br&gt;Determines the chat window type.</td>
</tr>
</tbody>
</table>
### Return Object

**Details**

Returns:

String - Returns one of the following values that specifies the type of user:

- queue_agent: Help Desk Chat support agent
- queue_user: Help Desk Chat end user
- group_chat: The individual is a member of a chat room (multiple users)
- conversation: The individual is a member in a private chat with another user

---

**String**

**getChatQueueAgent()**

Returns the `sys_id` for agent that is administering this thread.

Returns:

String - Returns the `sys_id` of the chat queue agent.

**String**

**getChatQueueUser()**

Returns the `sys_id` for end user of the chat queue.

Returns:

String - Returns the `sys_id` of the chat queue user.

**String**

**getThreadID()**

Returns the thread ID. This returns the same value as `g_chat.getChannelJID().getID()`.

Returns:

String - Returns the thread ID.

---

### Legacy: Help desk chat

Communicate with service desk staff using instant messaging.

**Note:** The **Connect Support** feature provides an updated messaging platform similar to help desk chat. The help desk chat and Connect Support features should not be used concurrently. There is no migration path from help desk chat to Connect Support.

Users can communicate directly with service desk staff using instant messaging in a ServiceNow instance (requires the Chat plugin.)

- Users access live support from the Employee Self-Service portal.
- Service desk staff provide support from the chat desktop.
Legacy: Use help desk chat to get support

You can contact service desk staff.

2. Log in to your ServiceNow account. Only logged in users can use chat.
3. In the upper right, click the Service Desk Chat button. A chat window opens.
4. Enter your question in the text field at the bottom of the window and press Enter.
   1. A message confirms that you have entered the chat queue and indicates your position and estimated wait time.
   2. When a service desk staff member accepts your chat and begins working on your question, another message appears.
5. Chat with your service desk agent via instant messaging.
   Service desk staff may lead you through troubleshooting, ask clarifying questions, or create an incident record to address your question.

   **Note:** Administrators can configure Service Desk Chat to be accessible on content management (CMS) pages.

Legacy: Use help desk chat to provide support

Staff who are assigned to chat support can provide live support via instant messaging. Administrators and users with the chat_admin role can assign chat support staff (see Set Up Chat Queues for Help Desk Chat).
To provide users with live support using chat:

1. Navigate to Social IT > Chat to open your chat desktop.
   - A chat queue agent window appears on your chat desktop for each chat queue you are assigned to. If no agent windows appear, ask an administrator to add you as a member of the assignment group for a chat queue.
   - The chat queue agent window displays the number of users in the queue and how long they have been waiting.
   - Every member of the assignment group sees the associated chat queue agent window.

2. Click Answer Next User to answer the next user or click Answer beside a specific user in the queue. A chat window opens.
   - Only the agent and the user can see the chat window.

Provide support via instant messaging. Chat queue agents can access additional support functions in the chat window menu:

- **Invite User**: invite another expert to assist with a support chat. An invitation appears in the favorites list of an invited user.
- **Create Incident from Chat**: create a new incident record with the initial question as the short description and the support chat as a linked chat room (accessible from the Create or Join Chat Room related link on the Incident form).

**Note**: Administrators can edit this action or add additional actions to the chat window menu.
Legacy: Set up chat queues for help desk chat

Help desk chat allows users to communicate directly with Service Desk staff via instant messaging in an instance.

Chat queues define the schedules, staff, and system messages for help desk chat. Administrators and users with the chat_admin role can set up chat queues.

Define a chat queue for legacy chat

How to define a chat queue for legacy chat.

Note: The Chat Queue (chat_queue) table is also used by Connect Support. Legacy chat and Connect Support should not be used concurrently.

1. Navigate to Social IT > Chat Administration > Queues.
2. Select a chat queue to edit or click New.
3. Enter the chat queue details and click Update or Submit.

Chat queue details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name that end users see as a title for the queue.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Active</td>
<td>Select the check box to activate or clear the check box to deactivate the chat queue.</td>
</tr>
<tr>
<td>Assignment group</td>
<td>Select the group that contains the support staff for the chat queue. Every agent sees the chat queue on their chat desktop and can answer any user that is waiting in the queue. To assign staff members to the group, see <a href="#">Assign Service Desk Staff to a Chat Queue</a>.</td>
</tr>
<tr>
<td>Schedule</td>
<td>Select a schedule that defines when a queue is available (see <a href="#">Use Schedules</a>). If the queue is always available, clear the field.</td>
</tr>
<tr>
<td>Question</td>
<td>Enter the initial question that end users see when they open a new Help Desk Chat. For example, How can I help you?</td>
</tr>
<tr>
<td>Confirm problem</td>
<td>(Optional) Enter the confirmation message that end users see when they enter an initial question. For example, Thank you for contacting support. Your problem has been submitted and an agent will be with you shortly.</td>
</tr>
<tr>
<td>Initial agent response</td>
<td>(Optional) Enter the message that end users see when an agent accepts their chat. For example, Thank you for waiting. I am looking into your question now and will be with you shortly.</td>
</tr>
<tr>
<td>Not available</td>
<td>Enter the message that end users see when a Help Desk Chat request is not accepted because the queue is outside its scheduled availability (defined by the Schedule field).</td>
</tr>
</tbody>
</table>

**Assign service desk staff to a chat queue**
Chat queue agents are Service Desk staff that are members of a chat queue's assignment group.

To assign agents to a chat queue:

1. Navigate to [User Administration > Groups](#).
2. Select an existing assignment group or click [New](#).
3. Enter or modify the group details (see [Create a Group](#)).
4. Right-click the header and select [Save](#).
5. In the Group members related list, click [Edit](#).
6. Using the [slushbucket](#), add support staff to the group.
7. Navigate to [Social IT > Chat Administration > Queues](#).
8. Select the chat queue for which the group provides support.
9. In the Assignment Group field, select the group.

---

© 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.
Chat queue group

*Make help desk chat accessible to an end user*

Users access live support from the Employee Self-Service Portal (ESS Portal).

Users access live support from the Employee Self-Service Portal (ESS Portal). To make a Help Desk Chat queue accessible to end users, add a link to the ESS Portal (requires the Content Management Plugin).

To change the default link in the ESS header:

1. Navigate to **Content Management > Headers**.
2. Open **Portal - Header**.
3. In the Chat queue field, enter the chat queue that users access by clicking the link in the ESS header. Clear the field to remove the chat queue link.
4. Click **Update**.
Chat queue link

Add a custom link elsewhere on the ESS portal
How to add a custom help desk chat link on the ESS portal.

1. Navigate to **Content Management > Static HTML**.
2. Click **New**.
3. Enter a Name.
4. In the Static content field, click **Toggle HTML Source** to edit the field in HTML source mode.

5. Create a link to the desired Help Desk Chat queue (see **Link Syntax**).
6. Click **Submit**.
7. Add the new content block to the desired location on the portal (see [Adding Content to the Page](#)).

**Link syntax**
To open a Help Desk Chat queue from a custom link on the ESS Portal, you must call the `CustomEvent.fire` method using appropriate arguments.

To open a Help Desk Chat queue from a custom link on the ESS Portal, you must call the `CustomEvent.fire` method using appropriate arguments. Details of the API call and an example that generates an anchor link are provided below.

**API Call:**
```
CustomEvent.fire(LiveEvents.LIVE_EVENT, LiveEvents.LIVE_WINDOW_JOIN_QUEUE_QUERY, CHAT_QUEUE_SYS_ID, CHAT_QUEUE_SYS_NAME);
```

where the variables are:
- **CHAT_QUEUE_SYS_ID**: Specifies the sys_id for the chat queue.
- **CHAT_QUEUE_SYS_NAME**: Specifies the name of the chat queue (must match the value the Name field of the chat queue record).

Example: This example creates an anchor link that opens the Help Desk Chat queue.

```html
<a href="#" onclick="CustomEvent.fire(LiveEvents.LIVE_EVENT,
LiveEvents.LIVE_WINDOW_JOIN_QUEUE_QUERY,
'c54f0abf0a0b452db84664f409c79c',
'Help Desk Chat'); return false;">
Help Desk Chat
</a>
```

**Monitor chat queues**

Chat queues can yield useful Key Performance Indicators (KPI) for evaluating support effectiveness.

- **Queue Wait Time**: amount of time a user waits in the queue before a help desk agent accepts the request.
- **Percentage of Chats Abandoned**: users that exit the queue before an agent responds (user stopped waiting).
- **Percentage of Chats Accepted**: requests that are answered by an agent.

---

**Note**: This information is not calculated automatically. Administrators may calculate these values based on data collected by chat queues.

**Monitor help desk chat tasks**

Help Desk Chat requests are tracked in the Chat queue entries table, which appears as a related list on the associated chat queue record.

Help Desk Chat requests are tracked in the Chat queue entries table, which appears as a related list on the associated chat queue record. Because this table extends the Task table, administrators can take advantage of core task functionality. For example, administrators can attach Service Level Agreements (SLAs) to chat queue entries to evaluate the response time of Help Desk Chat support.

---

**Live Feed**

Live Feed is a social IT application that provides a place to post and share content in a ServiceNow instance.

Live Feed content forms a searchable knowledge source for sharing information within an organization. Main features include the following:

- Users can post, reply to, and rate messages, including links and images.
- Administrators can set up automatic messages that are generated when specific records are updated throughout the system.
- Users can subscribe to receive email notifications when new messages are posted.

Live feed includes different types of feeds.
My Live Feeds

System Administrator
16 minutes ago • From Feed W0010007
WM Admin added as an approver
Like • Copy Link • Comment

System Administrator
16 minutes ago • From Feed W0010007
WM Admin added as an approver
Like • Copy Link • Comment

System Administrator
16 minutes ago • From Feed W0010007
WM Approver added as an approver
Like • Copy Link • Comment

System Administrator
16 minutes ago • From Feed W0010007
WM Approver added as an approver
Like • Copy Link • Comment
Live Feed browser support

The Live Feed v2 plugin does not support Internet Explorer 7 through 9. Users who access the instance from those browser versions can use Live Feed v1 functionality. Users who access the instance from browsers that are compatible with HTML5 can use Live Feed v2 functionality.

Activate Live Feed

Live Feed is active for all instances. An administrator can activate the Live Feed plugin if it is not already active.

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.

Administer live feed

Administrators and users with the live_feed_admin role can configure live feed security and provide access to live feed from content management pages. Administrators can also set up live feed table notifications.

Document feeds

A document feed is a live feed group that is associated with a record, such as an incident or change.

Document feeds allow users to work on tasks and other records through the live feed interface. Users can post messages in live feed that are automatically maintained as comments or work notes on the record, if the record has these journal fields.

The benefits of using document feeds include the following.

- Improving communication between users working on the same record.
- Improving visibility into progress for end users.
- Providing a single place to see updates on multiple records.
- Saving conversation history in the record so that knowledge is not lost in an email chain.

To use document feeds, activate the Live Feed Document plugin, which is active by default in new instances. See Use live feed to work on records to learn how to use this feature.

The system automatically creates a document group for the feed when a user follows or shows a record on live feed. The system also creates a document group when a user creates a new record on a table that has live feed enabled.

The following list describes features of the document feed group.

- Is unlisted; it does not appear when users view all groups on live feed.
- Automatically approves membership for every user who can access the record.
- Uses the record number as the group name.
- Uses the record short description as a group description.
- Maintains all messages posted to live feed on the record, if the record has a journal field for comments. If the record has a standard text field for comments, each live post overwrites the field value.
- Maintains all messages posted on the record in live feed if the record has a journal field for comments. When the group is created, existing messages are added to the document feed.

A user who participates in live feed becomes a member of the group.

**Add a live feed UI action on a table**

You can add UI actions on a table to allow users to follow records in live feed.

Role required: ui_action_admin or admin

1. Navigate to System Definition > UI Actions.
2. Open one of the live feed UI actions, for example, the Follow on Live Feed list UI action.
3. In the Table field, select the table name.
4. Right-click the header and select Insert to create a copy of the UI action for the desired table.
5. Repeat steps 1 – 4 for all live feed UI actions.

**Configure document feeds**

You can configure a table to support document feeds.

Role required: personalize_dictionary or admin

Configuring a table to support document feeds includes the following steps:

1. Add live feed to a form header.
2. Add Follow on Live Feed and Show Live Feed as list and form UI actions.

**Security configuration for document feeds**

Document feeds honor the access control rules (ACLs) for the associated record. Users can only view messages on the document feed if they have access to the same information on the record.

Consider the following examples.

- If an ACL allows a user to read and create comments on an incident, then the user can view and add messages posted as comments on the incident feed.
• If an ACL restricts a user from reading work notes, then the user cannot view messages posted as work notes on the incident feed.

Note: Access control rules are only checked when a user first accesses the document feed. After users view the feed, an administrator must remove them manually to change their access.

Disable a record feed
You can disable live feed functionality from the form of any table.
Role required: personalize_dictionary or admin
1. Navigate to System Definition > Dictionary.
2. Open the dictionary entry for the table.
3. Add live_feed=false in the Attributes field.
4. Click Update.

Note: If the Collaboration feature is activated, you can remove the show live feed icon from all form headers. Set the glide.live_feed.task_header_button property to collaboration.

Disable a document feed
You can disable a document feed from the form of any table.
Role required: personalize_dictionary or admin
1. Navigate to System Definition > Tables.
2. Open the table record.
3. Clear the Live feed check box.
4. Click Update.

Business rule installed with Live Feed Document
This business rule is installed with Live Feed Document. There are no tables, roles, or notifications installed with it.

<table>
<thead>
<tr>
<th>Business rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Live Feed integration</td>
<td>Writes journal comments to the live feed if there is a group for this record.</td>
</tr>
</tbody>
</table>

Record feeds
A record feed is a live feed group that is associated with a record, such as an incident or change. Record feeds allow users to work on tasks and other records through the live feed interface. Users can post messages in live feed that are automatically maintained as comments or work notes on the record if the record has these journal fields.

You can use record feeds to:
• Improve communication between users working on the same record.
- Improve visibility into progress for end users.
- Provide a single place to see updates on multiple records.
- Save feed history in the record so that knowledge is not lost in an email chain.

**Live feed document**

**Note:** Many of these features are part of live feed v2.

**Activate live feed document**

The Live Feed Document plugin is active by default.

Administrators can enable record feeds in an instance by activating the Live Feed Document plugin, which activates the Live Feed plugin, if it is not active. For upgrades, administrators must activate the 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 Only** related link on the System Plugin form.

5. Click **Activate**.

### Configure record feeds

Configure a table to support record feeds. You can add the Show Live Feed button in the form header and add the UI actions Follow on Live Feed and Show Live Feed as List and Form.

By default, the Show Live Feed icon appears on the form header for all tables that extend task, including the Incident, Change Request, and Problem tables, and in the list and form context menus for all task tables.

**Add live feed to a form header**

Add the **Live Feed** button in the form header for a table.

1. Type `sys_properties.list` in the Application Navigator.
2. Open the record for `glide.live_feed.task_header_button`.
3. In the **Value** field, change the value to `both`.

**Note:** By default, the value is `collaboration` so that the property is supported in the Collaboration (com.glide.collaboration) plugin. Changing the value to `both` allows the system property to be supported in Collaboration and Live Feed.

4. Click **Update**.
5. Navigate to **System Definition > Tables**.
6. Open the table record.
7. If the **Live feed** check box does not appear on the form, configure the form layout to add the **Live feed** field.
8. On the form, select the **Live feed** check box.
9. Click **Update**.

   Alternatively, you can add `live_feed=true` to the **Attributes** field in the dictionary entry for the table.

The **Live Feed** button appears on the overflow menu of the form header.
Add live feed to a context menu
Add live feed UI actions on a table.

1. Navigate to System Definition > UI Actions.
2. Open one of the live feed UI action, for example, Follow on Live Feed.
3. In the Table field, select the table name.
4. Right-click the header and select Insert to create a copy of the UI action for the desired table.
5. Repeat steps 1 – 4 for all live feed UI actions.

Disable a record feed
You can disable live feed functionality from the form of any table.

Role required: personalize_dictionary or admin

1. Navigate to System Definition > Dictionary.
2. Open the dictionary entry for the table.
3. Add live_feed=false in the Attributes field.
4. Click Update.

Note: If the Collaboration feature is activated, you can remove the show live feed icon from all form headers. Set the glide.live_feed.task_header_button property to collaboration.

Configure security
Record feeds honor the access control rules (ACLs) for the associated record.
Users can only view messages on the record feed if they have access to the same information on the record. For example:

- If an ACL allows a user to read and create comments on an incident, then the user can view and add messages posted as comments on the incident feed.
- If an ACL restricts a user from reading work notes, then the user cannot view messages posted as work notes on the incident feed.

**Note:** Access control rules are only checked when a user first accesses the record feed. After users view the feed, an administrator must remove them manually to change their access.

**Live feed table notifications**

Live feed table notifications generate automatic live feed messages. The Live Feed plugin must be activated to use table notifications.

When a record is inserted or updated on a specific task table and the notification conditions are met, a message is generated and posted to the specified group or to the company feed. Table notifications are supported for all task tables and all task types by default.

Administrators and users with the live_feed_admin or chat_admin roles can set up table notifications for any table in an instance.

**Set up table notifications for task tables**

You can set up a table notification for a task table to enable automatic live feed messages.

Role required: live_feed_admin or chat_admin

1. Navigate to **Collaborate > Feed Administration > Table Notifications**.
2. Click **New** or select a notification to open it.
3. Complete the form.

**Live Table Notification fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Select the table for which notifications are generated.</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 table notification.</td>
</tr>
<tr>
<td>Post to chat rooms</td>
<td>Select the check box to generate the notification in chat rooms that are associated with the record. This applies to task records only and requires that the Chat plugin is active.</td>
</tr>
<tr>
<td>Post to live feed</td>
<td>Select the check box to generate the notification on live feed. If record feeds are not set up and the <strong>Feed group</strong> field is blank, the notification is posted to the company feed.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Record Feeds</td>
<td>Select the fields to post for record feeds. This field is available only if</td>
</tr>
<tr>
<td></td>
<td>Post to live feed is selected.</td>
</tr>
<tr>
<td>Application</td>
<td>Select the application that contains this record.</td>
</tr>
<tr>
<td>Active</td>
<td>Select the check box to enable the notification.</td>
</tr>
<tr>
<td>Insert</td>
<td>Select the check box to generate the notification when a record is inserted</td>
</tr>
<tr>
<td></td>
<td>into the database.</td>
</tr>
<tr>
<td>Update</td>
<td>Select the check box to generate the notification when a record is updated.</td>
</tr>
<tr>
<td>Feed</td>
<td>Select the live feed team to which you want to post messages. This field is</td>
</tr>
<tr>
<td></td>
<td>available only if Post to live feed is selected. Clear the field to post</td>
</tr>
<tr>
<td></td>
<td>notifications on the company feed.</td>
</tr>
<tr>
<td>Conditions</td>
<td>Create the condition that must be met to generate the notification.</td>
</tr>
<tr>
<td></td>
<td>If you add a condition statement, the system evaluates the condition first</td>
</tr>
<tr>
<td></td>
<td>and parses the Before script field only if the condition is met. You may</td>
</tr>
<tr>
<td></td>
<td>choose to leave this field blank and include conditions in the script.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the table notification.</td>
</tr>
<tr>
<td>Message</td>
<td>Construct the automatic message you want to generate. You can include field</td>
</tr>
<tr>
<td></td>
<td>values as variables and a link to the record.</td>
</tr>
<tr>
<td></td>
<td>To add a variable, position the cursor in the text and then click the field</td>
</tr>
<tr>
<td></td>
<td>name in the Select variables field. To add a link to the record, enter $</td>
</tr>
<tr>
<td></td>
<td>(URI) in the message text as shown in the following example.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>High priority incident opened:</td>
</tr>
<tr>
<td></td>
<td>${URI}</td>
</tr>
<tr>
<td></td>
<td>Short description:</td>
</tr>
<tr>
<td></td>
<td>${short_description}</td>
</tr>
</tbody>
</table>

**Note:** For security reasons, any HTML code is automatically stripped out of a message before it is posted.
### Before script

Create a script that runs before a notification is generated. The script runs only if the condition evaluates to true or is empty. The following variables are available in the script.

- **current**: the GlideRecord object that triggered the notification.
- **changedFields**: an ArrayList of fields changed on submit. Use `changedFields.contains("fieldname")` to check for change.
- **answer**: set answer to false to cancel the notification.
- **profileSource**: set to a valid GlideRecord object to define the profile that is posting the message.
- **profileID**: set to a live_profile sys_id to define the profile that is posting the message; by default it is the current record. Overrides profileSource if both are specified.

Any custom variable created in the script is also exposed to the message in the form of `${myVariableName}`.

4. Click **Submit** or **Update**.

### Set up table notifications for non-task tables

Table notifications are supported for all task tables by default, and you can set up a table notification for any other table.

**Role required**: live_feed_admin or chat_admin

1. Navigate to **System Definition > Business Rules**.
2. Open the **live feed events** business rule.
3. In the Advanced section, select and copy the text in the **Script** field.
4. Click the back arrow on the top, left to exit the record and return to the Business Rules list.
5. Click **New**.
6. Enter the following values at the top of the form.
   - **Name**: Enter a name, such as `live feed events for my table`.
   - **Table**: Select the table for which you are setting up a notification.
   - **Active** and **Advanced**: Select these check boxes.

7. In the **When to run** section, enter the following values.
   - **When**: Select **before**.
   - **Insert**, **Update**, and **Delete**: Select the check boxes.

8. In the **Advanced** section, paste the script from the **live feed events** business rule into the script box.
9. Click **Submit**.
The live feed events business rule runs on the non-task table. It fires the live_feed.update event, which is associated with the Live Feed Update script action. The script action sets up variables and processes the table notifications.

After saving the business rule, create a live feed table notification record for the new table as you would for a task table.

Live feed table notification examples

The following examples demonstrate how to set up different types of table notifications that are useful for live feed.

Workaround posted
This example demonstrates a table notification that generates an automatic message on live feed whenever a workaround is added to an open problem.

- **Table**: Problem (problem)
- **Active**: Select the check box.
- **Update**: Select the check box.
- **Post to live feed**: Select the check box.
- **Conditions**: (State) (is) (Open)
- **Description**: Workaround Posted
- **Message**:

  
  `${sys_updated_by}` posted a workaround for `${URI}`.
  Short description: `${short_description}`

  
- **Before script**:

  ```java
  // only post to live feed when the Workaround field changes
  answer  = changedFields. contains ( "work_around" ) ;
  ```
Example workaround message

Problem resolved (advanced)
This advanced example demonstrates a table notification that generates an automatic message on live feed whenever a problem is closed.

It also adds a message about the assigned user and posts the message from the assignment group profile instead of the problem record.

- **Table**: Problem (problem)
- **Active**: Select the check box.
- **Update**: Select the check box.
- **Post to live feed**: Select the check box.
- **Conditions**: (Problem State) (is) (Closed/Resolved)
- **Description**: Problem Resolved
- **Message**:

  Problem ${number} - ${short_description} has been resolved. ${fixedByMsg}

- **Before script**:

  //cancel if we didn't just change the problem state if ( !changedFields.
  contains ( "problem_state" ) )
  answer  = false ;
//if we have an assigned_to value add a comment about who it was //create
//a new variable fixedByMsg that we can access from the message
fixedByMsg = ""; if (!current.assigned_to.nil())
fixedByMsg = "Thank you " + current.assigned_to.getDisplayValue();

//make the message appear to come from the assignment group if we have
//one if ( !current.assignment_group.nil() )
profileSource = current.assignment_group.getRefRecord(); // need
GlideRecord object

Example problem resolved message

Opportunity won (non-task)
This example demonstrates a table notification on a non-task table. It generates an automatic
message on live feed whenever a sales opportunity is won, if you have activated the Sales Force
Automation plugin.
Create a **business rule** on the Opportunity (sales_opportunity) table that matches the **live feed events** business rule on the task table.

Create a table notification with the following values:

- **Table**: Opportunity (sales_opportunity)
- **Active**: Select the check box.
- **Update**: Select the check box.
- **Post to live feed**: Select the check box.
- **Conditions**: (State) is (Closed Won)
- **Description**: Opportunity won
- **Message**:  
  
  ${owner} closed a sale with ${account}!

- **Before script**:  
  
  ```
  //make the message appear to come from the assigned salesperson if there is one if (!current. owner. nil ( ) )
  profileSource = current. owner. getRefRecord ( ) ; //need GlideRecord object
  ```

---

**Example opportunity won message**

**Related feeds table notification**

This example demonstrates table notifications to be sent out to related feeds.
For this example, whenever the status of a story changes to **Complete**, a table notification message is sent to the related sprint, release, or epic. Messages are posted only if the related feed already exists; this notification does not create a new feed.

- **Table**: Story (rm_story)
- **Active**: Select the check box.
- **Update**: Select the check box.
- **Post to live feed**: Select the check box.
- **Record feeds**: Move **Sprint**, **Release**, and **Epic** to the **Selected** column.
- **Conditions**: (State) (changes to) (Complete)
- **Description**: Story is done; message to Epic, Release, and Sprint
- **Message**:

```text
${URI} status changed to ${state}
```

**Live feed security and table access**

By default, administrators and users with the live_feed_admin role can configure live feed security and view all live feed tables.

You can also modify the following live feed tables.

- **Live Table Notification** (live_table_notification): set up automatic messages that are generated when specific records are updated throughout the system.
- **Live Feed Message** (live_message): modify only if necessary, such as to delete an inappropriate message or restore a message that a user accidentally deleted. This table is typically managed by system functionality.

Extending or modifying data in any live feed chat table is not recommended.

**Domain separation in live feed**

Using domain separation with the live feed application allows administrators to keep user content within a specific domain.

Parent and child domains define the live feed content that can be viewed and shared with other users.

- A user in a parent domain can see users and content within their domain and within all child domains that are lower in the domain hierarchy.
- A user in a child domain can see users and content within their domain but cannot see the parent domain or other child domains at the same level in the domain hierarchy.

**Enable domain separation for live feed**

Domain separation for the Live Feed application is available starting with the Eureka release. For users upgrading to Eureka, a **sys_domain** column is added to existing live feed-related database tables. For existing database records, the value of the **sys_domain** field is set to empty (global). This allows the domain separation feature to work with existing live feed records.

**Show or hide the live feed application for a domain**

The administrator can live feed visibility for a domain. This includes:

- Displaying live feed in the application navigator.
• Following a document feed for a record.
• Viewing live feed from a record.

Use live feed with domain separation

All of the live feed features are available to users within a domain and work the same way, with some exceptions to visibility.

• Posting and sharing content
  • Users in a child domain can interact with other users in the same domain. This includes posting and replying to messages, deleting messages, attaching files and links, and rating content.
  • Users in a parent domain can interact with other users in the same domain and with users in any child domains. Messages that are added to child threads by parent users are given the visibility of the child domain, not the parent domain.

• Viewing content
  • Users in a child domain can view content that resides within their domain. This includes filtering by feed, sorting, searching, and viewing older messages.
  • Users in a parent domain can view content that resides within their domain and within any child domains.
  • My Feed shows messages, teams, and hashtags based on the user's domain. Showing another user's feed only shows posts visible in the current user's domain.

• Using hashtags
  • Hashtags are separated by domain. Users in a child domain can use all of the hashtag functions within their domain. This includes tagging messages, viewing available hashtags, changing hashtag names, and searching and filtering by hashtag.
  • Users in a parent domain can use all of the hashtag functions within their domain and can see hashtags in any child domains.

• Using teams
  • Teams are separated across domains. Users in a child domain can join and follow teams within their domain, and can invite other users within their domain to join teams.
  • Users in a parent domain can join and follow teams that belong to their domain or to any child domains.

• Exceptions to teams
  • New teams are created in the user's domain. However, if the team has a record associated with it, the team is created in record's domain.
  • New threads in an existing team are created in the domain of the existing team.
  • When a user is creating a new team from a document, if the document domain is not empty or global, the team domain needs to be changed to be the document's domain.
  • For a document-generated team, when the domain of the document changes, the domain of all related live feed records changes as well.

• Subscribing to email notifications
  • Users can subscribe to email notifications from users and teams within their domain only.
Limit live feed access by role

All active users in the instance have access to live feed by default.
live_feed_admin and admin

1. Complete the following steps to define the roles that allow users to see the Live Feed module.
   a) Perform the appropriate action for your version of the UI:
      - UI16: Navigate to System Definition > Application Menus > Collaborate and select Live Feed.
      - UI15 or UI11: Right-click the icon beside the Live Feed module and select Edit Module.
   b) Enter the roles that have access in the Roles field.
   c) Click Update.

2. Complete the following steps to define the roles that allow users to see live feed from a mobile device.
   a) Navigate to System Definition > Applications (Mobile).
   b) Click Live Feed.
   c) Enter the roles that have access in the Roles field.
   d) Click Update.

3. Use the following settings in the Access Control form to create access control rules to limit who can view the live_feed pages.
   - Type: ui page
   - Operation: read
   - Name: create one access control rule record for each of the following pages
     - live_feed
     - live_feed_small
     - $live_feed
     - $live_feed_small
   - Requires role: in this related list, add roles to define who can access the live feed pages. Users who do not have these roles cannot access live feed.

Manage live feed message content

Users can remove their own messages from feeds. If necessary, administrators can remove inappropriate messages that are posted by any user.
live_feed_admin and admin

For security reasons, any HTML code is automatically stripped out of a message before it is posted. This measure ensures that users cannot modify any page settings by posting a message.

1. Navigate to Collaborate > Feed Administration > Messages.
2. Open the message to be removed.
3. In the State field, select deleted. You may need to configure the form to add this field.
4. Click Update.

Live feed team security

You can restrict who can create teams by modifying an access control rule.
Modify the following access control rule.

- **Table**: Live Group Profile (live_group_profile)
- **Operation**: create

**Restrict hashtag renaming**

You can restrict who can rename hashtags.

You restrict hashtag rename by modifying the following access control rule:

- **Table**: Live Tag (live_tag)
- **Operation**: write

**Provide access to live feed from CMS pages**

You can provide access to live feed from pages built in the Content Management System (CMS). For example, allow an end user to access your company feed via the ESS portal.

Role required: content_admin or admin

The ESS Portal template includes the Portal - Live page and Live Feed dynamic blocks. To provide access to live feed from CMS pages, add the Live Feed dynamic block to a CMS page or include Portal - Live page in a site.

1. Navigate to Content Management > iFrames.
2. Click New.
3. Enter the iFrame block details.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique name such as Live Frame.</td>
</tr>
<tr>
<td>Frame Name</td>
<td>Enter a frame name, such as live_frame.</td>
</tr>
<tr>
<td>URL</td>
<td><a href="https://INSTANCE/live_feed.do?sysparm_doctype=true">https://INSTANCE/live_feed.do?sysparm_doctype=true</a> where INSTANCE is your instance URL (example, {instance name}.service-now.com)</td>
</tr>
<tr>
<td>Application</td>
<td>Displays scoping information.</td>
</tr>
<tr>
<td>Sizing</td>
<td>Select Fixed Size and enter height and width pixel dimensions according to the page where you plan to display the feed (for example, width of 1024 and height of 768).</td>
</tr>
</tbody>
</table>

4. Click Submit.
5. Add the block to a page.

**Components installed with live feed**

Several types of components are installed with Live Feed.

Demo data is available with Live Feed.
Tables installed with live feed

Live Feed plugin installs the following tables.

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link attachments (live_link)</td>
<td>Stores links and attachments that are added to messages.</td>
</tr>
<tr>
<td>Live Favorite (live_favorite)</td>
<td>Stores the favorite conversations, user groups, and messages.</td>
</tr>
<tr>
<td>Live Feed Searches (live_feed_search)</td>
<td>Stores live feed text searches. Access at Collaborate &gt; Feed Administration &gt; Search Log.</td>
</tr>
<tr>
<td>Live Follows (live_follow)</td>
<td>Maintains users' follow preferences for user feeds.</td>
</tr>
<tr>
<td>Live Group Profile (live_group_profile)</td>
<td>Stores conversation properties, including name, description, and public status. Also stored are user group properties, such as name, description, and public status.</td>
</tr>
<tr>
<td>Live Group Member (live_group_member)</td>
<td>Maintains the member lists for conversation and user group.</td>
</tr>
<tr>
<td>Live Mention (live_mention)</td>
<td>Stores the profiles mentioned in a message. References sys_user table.</td>
</tr>
<tr>
<td>Live Message Tag (live_message_tag)</td>
<td>Stores messages associated with user-created tags. Appears as a related list on Live Tag records.</td>
</tr>
<tr>
<td>Live Poll (live_poll)</td>
<td>Stores a poll question.</td>
</tr>
<tr>
<td>Live Poll Cast (live_poll_cast)</td>
<td>Stores profiles of users who voted for a particular option in a poll.</td>
</tr>
<tr>
<td>Live Poll Options (live_poll_option)</td>
<td>Stores poll options.</td>
</tr>
<tr>
<td>Live Table Notification (live_table_notification)</td>
<td>Generates automatic table notifications, such as when a user reads live feed for the first time and when a high priority incident is opened. Access at Collaborate &gt; Feed Administration &gt; Table Notifications.</td>
</tr>
<tr>
<td>Live Tag (live_tag)</td>
<td>Maintains user-created tags. Access at Collaborate &gt; Feed Administration &gt; Tags.</td>
</tr>
</tbody>
</table>
User roles installed with Live Feed

Live Feed plugin installs the following user roles.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>live_feed_admin</td>
<td>Can manage live feed functions. For example, users with the live_feed_admin role can:</td>
</tr>
<tr>
<td></td>
<td>· Set up table notifications for task tables.</td>
</tr>
<tr>
<td></td>
<td>· Set up table notifications for non-task tables.</td>
</tr>
<tr>
<td></td>
<td>· Limit live feed access by role.</td>
</tr>
<tr>
<td></td>
<td>· Manage live feed message content.</td>
</tr>
<tr>
<td>chat_admin</td>
<td>Can manage chat functions (if the Chat plugin is activated). For example, users with the chat_admin role can:</td>
</tr>
<tr>
<td></td>
<td>· Change chat room message read access.</td>
</tr>
<tr>
<td></td>
<td>· Define chat room access rights.</td>
</tr>
</tbody>
</table>

Script includes installed with Live Feed

Live Feed plugin installs the following script includes.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LiveMsgUtil</td>
<td>Provides helper functions for working with live_message records.</td>
</tr>
<tr>
<td>LiveFeedFilter</td>
<td>Queries filters for working with live_feed records.</td>
</tr>
<tr>
<td>LiveFeedUtil</td>
<td>Provides helper functions for working with live_feed records.</td>
</tr>
</tbody>
</table>

Business rules installed with Live Feed

Live Feed plugin installs the following business rules.

<table>
<thead>
<tr>
<th>Business rule</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feed Group Creator Becomes Admin</td>
<td>Live Group Profile</td>
<td>Designates the group creator as the group administrator.</td>
</tr>
<tr>
<td></td>
<td>(live_group_profile)</td>
<td></td>
</tr>
<tr>
<td>live feed events</td>
<td>Task</td>
<td>Runs on task insert, update, and delete. Runs event associated with the Live Feed Update Script action that processes Live Table Notifications to auto-generate live feed messages.</td>
</tr>
<tr>
<td></td>
<td>(task)</td>
<td></td>
</tr>
<tr>
<td>Business rule</td>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Live feed member update events</td>
<td>Live Group Member (live_group_member)</td>
<td>Generates a notification event when member state changes (invited, accepted, declined, left, rejected, request, request_accepted).</td>
</tr>
<tr>
<td>Live feed integration</td>
<td>Journal Entry (sys_journal_field)</td>
<td>Writes journal comments to the live feed if there is a group for this record.</td>
</tr>
<tr>
<td>Live feed new member events</td>
<td>Live Group Member (live_group_member)</td>
<td>Generates a notification event when new members are added.</td>
</tr>
<tr>
<td>Live feed profile events</td>
<td>Live Profile (live_profile)</td>
<td>Runs on live_profile insert/update/delete, triggers event associated with the Live Feed Update script action that processes Live Table Notifications to auto-generate live feed messages.</td>
</tr>
<tr>
<td>Live Feed message events</td>
<td>Live Feed Message (live_message)</td>
<td>Runs on live_message, notification event trigger for new live messages.</td>
</tr>
<tr>
<td>Live message like events</td>
<td>Message Liked by (live_message_like)</td>
<td>Runs on live_message_like, notification event trigger for new like records.</td>
</tr>
<tr>
<td>LiveFeed Group Member Visibility 2.0</td>
<td>Live Group Member (live_group_member)</td>
<td>Ensures users can only see the members list for public groups and groups they belong to.</td>
</tr>
<tr>
<td>LiveFeed Group Profile Validation</td>
<td>Live Group Profile (live_group_profile)</td>
<td>Ensures that a public group is visible.</td>
</tr>
<tr>
<td>LiveFeed Group Profile Visibility 2.0</td>
<td>Live Group Profile (live_group_profile)</td>
<td>Ensures that the list of all groups only displays public groups, private groups that are visible, and groups the user belongs to.</td>
</tr>
<tr>
<td>LiveFeed Membership Changes</td>
<td>Live Group Member (live_group_member)</td>
<td>Ensures that only the group administrator and users with live_feed_admin role can manage membership for a group.</td>
</tr>
<tr>
<td>LiveFeed Single Group Membership</td>
<td>Live Group Member (live_group_member)</td>
<td>Ensures that a user is not added multiple times to the same group.</td>
</tr>
<tr>
<td>Live Message Likes</td>
<td>Live Message Like (live_message_like)</td>
<td>Updates the number of likes for a message.</td>
</tr>
<tr>
<td>LiveFeed Join Group Check</td>
<td>Live Group Member (live_group_member)</td>
<td>Ensures that users cannot automatically join private visible groups.</td>
</tr>
<tr>
<td>Update Follow/Follower Counts</td>
<td>Live Follow (live_follow)</td>
<td>Updates the following/followers counts.</td>
</tr>
</tbody>
</table>
### Email notifications installed with Live Feed

Live Feed plugin installs the following email notifications:

<table>
<thead>
<tr>
<th>Email notification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Live Feed Feed Member Accepted</td>
<td>Sends an email to the administrator when a user has accepted to join the feed.</td>
</tr>
<tr>
<td>Live Feed Feed Member Declined</td>
<td>Sends an email to the administrator when a user has declined to join the feed.</td>
</tr>
<tr>
<td>Live Feed Feed Member Invited</td>
<td>Sends an email to a user when they have been invited to join a feed.</td>
</tr>
<tr>
<td>Live Feed Feed Member Left</td>
<td>Sends an email to the administrators when a user has left the feed.</td>
</tr>
<tr>
<td>Live Feed Feed Member Removed</td>
<td>Sends an email to a user when they have been removed from the feed.</td>
</tr>
<tr>
<td>Live Feed Feed Member Request</td>
<td>Sends an email to administrators when an user requests to join a feed.</td>
</tr>
<tr>
<td>Live Feed Feed Member Request Accepted</td>
<td>Sends an email to the user when their request to join a feed is accepted.</td>
</tr>
<tr>
<td>Live Feed Feed Request Rejected</td>
<td>Sends an email to the user when their request to join a feed has been rejected by an administrator.</td>
</tr>
<tr>
<td>Live Feed MsgReply Subscription</td>
<td>Sends an email when a reply or reply_to_reply message is inserted into the thread of a message in a feed.</td>
</tr>
<tr>
<td>Live Feed Team Member Accepted</td>
<td>Sends an email to administrators when a user accepts an invitation to join a team.</td>
</tr>
<tr>
<td>Live Feed Team Member Declined</td>
<td>Sends an email to administrators when a user declines an invitation to join a team.</td>
</tr>
<tr>
<td>Live Feed Team Member Invited</td>
<td>Sends an email when a user is invited to join a team.</td>
</tr>
<tr>
<td>Live Feed Team Member Left</td>
<td>Sends an email when a user leaves a team.</td>
</tr>
<tr>
<td>Live Feed Team Member Removed</td>
<td>Sends an email when an administrator has removed a user from a team</td>
</tr>
<tr>
<td>Live Feed Team Member Request</td>
<td>Sends an email when a user requests to join a team.</td>
</tr>
<tr>
<td>Live Feed Team Member Request Accepted</td>
<td>Sends an email when a user's request to join a team is accepted.</td>
</tr>
<tr>
<td>Live Team Member Request Rejected</td>
<td>Sends an email when a user's request to join a team is rejected.</td>
</tr>
<tr>
<td>Email notification</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Live Message All Subscription</td>
<td>Sends an email to subscribed users when any message (new or reply) is posted.</td>
</tr>
<tr>
<td>Live Message Feed Subscription</td>
<td>Sends an email when a new message is inserted into a feed.</td>
</tr>
<tr>
<td>Live Message Liked</td>
<td>Sends an email to the creator of a message when another user likes the message.</td>
</tr>
<tr>
<td>Live Message Mention</td>
<td>Sends an email to a user when that user is mentioned in a message.</td>
</tr>
<tr>
<td>Live Message New Posts Subscription</td>
<td>Sends an email to subscribed users when a new (not reply) message is posted.</td>
</tr>
<tr>
<td>Live Message Reply</td>
<td>Sends an email to all users in a feed thread when a user posts a reply (live_message.replied event).</td>
</tr>
</tbody>
</table>

**Use Live Feed**

Live Feed provides many methods you can use to share content with others in your organization. Depending on your role, there are several different types of feeds you can access, teams you can join and share information with, and hashtags you can use for categorizing messages.
Note: Live Feed v2 is active for all new instances by default. If you are upgrading from an earlier version of ServiceNow, you need to activate Live Feed v2 to use these features.
Use hashtags in Live Feed

Hashtags are words marked with a hash symbol (#) in messages. Hashtags are a way to categorize messages by keyword or topic for improved search results. For example, to identify messages associated with VPN questions, add the hashtag #VPN in the message text.

Note: Many of these features are part of live feed v2. If you are using live feed v1, or have not activated live feed v2, see Legacy Live Feed.

Tag messages

To tag a keyword or topic in a message, enter a # symbol before the word. A link to the hashtag is added beneath the message and all feed users can search and filter by the hashtag to find the message.

Tips for using hashtags effectively include:

- Limit the number of hashtags per message (no more than 3 is a good guideline).
- Use hashtags only in messages that are relevant to the tagged topic.
- Write a message first, and then add hashtags only if they add value. Answer the question, "What are you working on?", rather than "What hashtags apply to what you are working on?"
- Use camel case to create a hashtag that is more than one word long. For camel case, remove the space and use an uppercase letter to start each word. For example, to create a topic about the service desk, use #ServiceDesk.
View an available hashtag

View a hashtag from any feed.

1. Navigate to Collaborate > Live Feed.
2. Click Hashtags in the sidebar.

   Any hashtags already defined are displayed. Up to 36 hashtags can be displayed, and options are available for searching and sorting the hashtags. When searching, you do not need to include the hash symbol (#).
3. Click a hashtag to view all messages containing that hashtag.

Tags multiple messages

**Change a hashtag name and merge a hashtag**

Over time, users may create many hashtags with similar names, such as competitive, competitor, and competition. To combine hashtags for better searching and filtering, change the names of similar hashtags to a standard name.

Administrators can restrict who can rename hashtags.

1. Navigate to **Collaborate > Live Feed.**
2. Click Hashtags in the sidebar to reveal the currently defined hashtags.
3. Turn off the filter to show all hashtags.
4. Point to the hashtag you want to change. If you have the rights to edit hashtags, an edit tag icon appears.
5. Click the edit tag icon.

### Hashtags

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Competitive</td>
<td>1</td>
<td>Competitor</td>
<td>3</td>
<td>joined</td>
</tr>
<tr>
<td>2</td>
<td>Lync</td>
<td>1</td>
<td>VPN</td>
<td>1</td>
<td>SAP</td>
</tr>
<tr>
<td>4</td>
<td>Email</td>
<td>1</td>
<td>WiFi</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>MacBook</td>
<td>1</td>
<td>Excel</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Edit tag

6. Enter a new hashtag name.
7. Press Enter.
   - If the new name is different than the other hashtags, the new hashtag name replaces the old hashtag name on the list and in the text of any messages that include the hashtag.
   - If the name is the same as one of the existing hashtags, the hashtags will be merged.
   
     For example, if you have two hashtags called Competitive and Competitors, and you change the name of Competitors to Competitive, all of the messages previously tagged Competitors are changed to Competitive and the Competitors hashtag is removed.

    **Note:** If a hashtag is removed from the message, renaming that hashtag does not change the message text.

#### Add an image to a hashtag

You can add an image at the domain level of already defined hashtags if you have the admin role.

1. Click Hashtags in the sidebar.
2. Select the appropriate hashtag.

### #VPN Feed

#### Tag with image icon

3. Do one of the following:
   - Locate the image in your file system, and then drag-and-drop the image onto the add an image icon.  

• Click the add an image icon ( ), select the image file, and click **Open**.

4. To change the image, simply drag-and-drop a new image onto the old one, or click on the existing one and select a new image.

When you view a message that contains a hashtag with an image, that image appears in the hashtag heading bar.

![Message with tag icon](image)

**Follow and unfollow a hashtag**

You can view all postings assigned a specific hashtag by following the hashtag. You can also unfollow the hashtag if you no longer want to view those postings.

1. Navigate to **Collaborate > Live Feed**.
2. Click **Hashtags** in the sidebar.
3. Select the hashtag you want to follow.
4. Click **Follow**.
Follow tag

A confirmation message appears.

5. Click X to dismiss the message.

To unfollow a hashtag, repeat the same steps and click Unfollow.

Bookmark hashtags

The live feed interface uses the standard bookmarking functionality for hashtags.

In UI15 and UI11, the live feed interface uses the standard bookmarking functionality for hashtags. You can drag-and-drop group feeds and hashtags from the Feed Summary section to the Edge for quick access.

© 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.
Bookmark hashtag

Remove a hashtag from a posted message

As a participant in a conversation, you can remove hashtags from messages that have already been posted.

1. Navigate to the posted message.
2. Click Hashtags in the message posting.

Hashtag in post

The hashtags associated with the message are displayed, along with the removal icon.
3. Click the removal icon.

Use teams in Live Feed

Users can be combined into teams for the purpose of subscribing to specifically-focused feeds. Teams can be created based on any criteria that makes sense for your organization. For example, you can create a team called IT Developers and subscribe the team to feeds such as Coding Standards, AngularJS Development, and ServiceNow Customization Best Practices. When a new developer is added to the IT Developers team, that user automatically has rights to participate in all of the feeds followed by the team.

Create a live feed team

When you create a team, you become the team administrator.

As team administrator, you can:

- **Modify team properties**
- **Accept or reject membership requests**
- **Remove members from the team**
- **Delete the team**

1. Navigate to **Collaborate > Live Feed**.
2. In the sidebar, click your profile picture, then select the **Teams** tab.
3. Click **Create Team**.

4. Enter a **Name** to appear at the top of the feed and in messages posted to the team. This name links to the team feed.
5. Enter a **Description** to appear at the top of the feed and under the team name in the list of all teams.

6. Select the access level for the team:
   - **Public Team**: In the list of all teams, any user can see the name of this team. Any user can also see the feed and join the team. Messages in a public team appear in the Company Feed with a link to the team feed.
   - **Private Team**: In the list of all teams, any user can see the name of this team, but not the feed. Messages in private teams do not appear on the Company Feed.

   When **Private Team** is selected, the **Show this team for anyone to find and request to join** check box is displayed. Select this check box to allow any user to search for this team and request to join it. Clear the check box to allow only invited users to see the feed and join the team.

7. Click **Create**.

   The team is created with you as the team administrator.

---

**Note**: A team administrator can create one or more group feeds specifically for the members of this team by clicking the **Group Feeds** tab and **Create Group Feed**. Additionally, the team can be invited to join a feed. Having multiple feeds for the team facilitates focused discussions on topics of interest to the team and allows the team to selectively invite other teams and members to collaborate on specific feeds.
Automatic team creation

If you create a record on a table that has live feed enabled, such as the Incident table, and click Follow/Show Live Feed for the record, a record feed is created for the record.

The record feed name is based on the table name.

Join a team

You can join a public team, accept an invitation, or request access to a team.

As a team member, you can:

- **View messages** posted to the team (team feed). Non-members can also view the feed for a public team.
- **View a list of team members**.
- **Invite another team** to join the team.
- **Subscribe to team email notifications**.
- **Leave** the team.

1. Navigate to **Collaborate > Live Feed**.
2. Click **Teams** and click **All Teams**.
   - If you received an invitation, click **Accept**. You can **Decline** the invitation if you do not want to join the team.
   - If the team is public, click **Join**.
   - If the team is private, click **Request**. The team administrator receives an email notification and must accept your request before you can join the team.

View a team feed

View a team feed to see messages belonging to that team.

1. Navigate to **Collaborate > Live Feed**.
2. In the sidebar, click your profile picture, then select the **Teams** tab.
   - To view a team you belong to, select the team name.
   - To view a public team you do not belong to, select **All Teams** and then click the team name.

   You must be a member to view the feed for a private team.

View a team member

View a list of members belonging to a live feed team.

1. Navigate to **Collaborate > Live Feed**.
2. In the sidebar, click your profile picture, then select the **Teams** tab.
3. From the team list, select the team name.

   You must be a member of the team to view the members.

4. Click **Members**.

   The list of team members appears, organized by team administrators and team members.

Invite a new member

You can invite another user to join a team.

1. Navigate to **Collaborate > Live Feed**.
2. In the sidebar, click your profile picture, then select the **Teams** tab.
3. From the team list, select the team name.
4. Click the **Pending members** tab.
5. In the **Add User** field, enter the name of the user you want to invite. The invited member's picture appears.

---

**Remove a member**

If you are team administrator, you can remove any member from the team.

1. Navigate to **Collaborate > Live Feed**.
2. In the sidebar, click your profile picture, then select the **Teams** tab.
3. From the team list, select the team name.
4. Click the **Members** tab.
5. Click Remove below the member name.
6. Click Remove again in the confirmation box that opens.

**Note:** You can remove members regardless of their current state. That is, you can remove members who have already joined the team or whose membership is pending.

---

**Subscribe to team and email notification**

Users can subscribe and unsubscribe to receive email notifications generated by feeds the team participates in.

Email notifications are generated whenever actions such as posting messages, replies, likes, polls, and @mentions are performed.

All notifications related to a top-level message, such as replies, mentions, and likes, are sent out with the same subject. The subject line defaults to Live Feed followed by the beginning of the subject line from the top-level message. For example, if the subject of the feed is IT Support, the email notification's subject will be Live Feed IT Support.

1. Navigate to Collaborate > Live Feed.
2. Click Teams and select the team name.
3. Click the subscribe icon ( ).
You can click the unsubscribe icon ( ) to stop receiving email notifications.

### Subscribe a team to feed notification

A team administrator can subscribe a team to specific feeds so the members of the team receive email notifications.

1. Navigate to Collaborate > Live Feed.
2. Click Teams and select the team name. You can use the advanced search to locate team of which you are the administrator.
3. Click Feeds.
4. Click the subscribe icon ( ) beside the feed name.

You can click the unsubscribe icon ( ) to stop receiving email notifications.

### Reply to email notifications using email

After receiving an email about a posted message or a reply, you can reply to live feed with your email client.

The body of the reply email becomes a reply to the live feed message. Any attachments included in your reply email are included in the live feed reply.

### Leave a team

You can give up membership to a team by leaving that team.

1. Navigate to Collaborate > Live Feed.
2. In the sidebar, click your profile picture, then select the Teams tab.
3. Click Leave beside the team name.

### Modify a team

If you are team administrator, you can modify an existing team.

1. Navigate to Collaborate > Live Feed.
2. In the sidebar, click your profile picture, then select the Teams tab.
3. From the team list, select the team name.
4. Click the edit icon ( ).
5. Modify the team properties as needed.
6. Click Save.

### Manage a membership request

When a user requests membership to a private team, the team administrator receives an email. If you are the team administrator, you can manage membership requests.

1. Navigate to Collaborate > Live Feed.
2. Click Teams and select the team name.

If one or more users have been invited to the team, the Pending members tab shows the number of invitations sent.
Pending members

3. Click **Pending members**.

This shows the users who have received invitations, but who have not yet accepted.
4. You can cancel a user's invitation by clicking **Remove**.
5. You can invite another user to the team by entering their name in the **Add user** field and clicking the Invite member (👤) button.

### Delete a team

If you are the team administrator, you can delete a team.

1. Navigate to **Collaborate > Live Feed**.
2. In the sidebar, click your profile picture, then select the **Teams** tab.
3. From the team list, select the team name.
4. Click the edit icon (📝).
5. Click **Delete**.
6. **Click Yes** to confirm deletion.  
The team is deleted from live feed. Messages posted to a private team are deleted; messages posted to a public team remain on the company feed without a team link.

If you delete a team that is associated with an active record, such as an incident that has not yet been closed, the team becomes active again when any user modifies that record or follows the record on live feed. The first user who modifies the record becomes the team administrator. The previous messages that existed as part of the record feed are not deleted.

---

**Use live feed to work on records**

A record feed is associated with a record, such as an incident or change.

Record feeds help users collaborate on records by providing a place for anyone who can access the record to share messages and post attachments specific to that record.

With record feeds, users can:

- Follow record feeds and post messages in live feed. These messages can also be automatically maintained in the comments or work notes journal fields on records.
- View live feed from records.
- Work on multiple records from **My Feed**.
- Access live feed team functions, such as sending invitations and subscribing to email notifications.

Any users with access to the record can also use the record feed. By default, record feeds are available on the incident, change, and problem tables. Administrators can configure record feeds for additional tables.
How Document Feeds Work

The Live Feed application creates a document group for each document feed. The document group:

- Automatically approves membership for every user who can access the record.
- Uses the record number as the group name.
- Uses the record short description as a group description.
- Maintains all messages posted on the record in live feed (if the record has a journal field for comments). When the group is created, existing messages are added to the document feed.
- Lists the group when users select View all groups on their live feed interface, unless the record associated with the document feed has been closed. When the state of the record is closed, the live feed group becomes inactive and unlisted.
- Automatically adds users to the document group when they view the record.

**Document Group Creation**

When a user follows or shows a record on live feed, a live feed group is automatically created and associated to the record (if one does not already exist). The user becomes a member of the group and can use live feed to work on the record. If the user can access work notes on the record, the user also becomes a group administrator.

A live feed group is also automatically created when a user creates a record on a table that uses document feeds, such as the Incident table. The user who creates the record becomes the administrator of the group, and any other user who modifies the same record automatically joins the group.

**Add Live Feed to a homepage**

Add live feed to a homepage so it is the first thing you see when you log in.

1. Click Add content at the top of the homepage.
2. Select Live Feed in the left panel.
3. On the bottom of the window, click Add here in the appropriate layout position, then close the window.

**Note:** Administrators can add live feed to a global homepage to make it available for all homepage users by default. By default, users with any role can add live feed to their homepage. Administrators can restrict this ability.
Modifying and deleting document feeds

The user who creates a record feed becomes the group administrator, which allows the user to modify the following record feed properties.

- **Name**: default value is the record number.
- **Description**: default value is the record short description.
- **Picture**: default value is a thumbnail image of the record.

Feed administrators can also delete the feed. When deleted, the feed is removed from live feed but messages remain in the journal field of the associated record.

Viewing Live Feed from records

Interact with the record feed in any form that has live feed enabled.
The record feed appears in a pop-up window. The record feed also appears on the record form’s activity formatter if the administrator enables the record feed system property (glide.ui.show_live_feed_activity).

To access a record feed from the form, do one of the following:

- Click the Show Live Feed button in the form header. This displays the live feed pop-up.
- Right-click the form header and select Show Live Feed. This also displays the live feed pop-up.
- Scroll down to the activity formatter area on the form. Click one of the following tabs:
  - **Live Feed**: click to show a text box to type in the feed.
  - **Activity**: click to show the activity summary. The activity filter determines the content in the activity summary.
If the activity formatter or the Live Feed and Activity tabs are not visible, administrators can do the following:

- Configure the form layout and add Activities (filtered) to the form. This adds the activity formatter.
- Personalize the form layout and add Activities (filtered) to the form. This adds the activity formatter.
• Go to **System Definition > Tables**, access the table associated with the record, and verify that the `live_feed` dictionary attribute is set to true on the form. This adds live feed to the activity formatter.

• Go to **Collaborate > Feed Administration > Properties** and enable the following property: **Toggle the display of the live feed tab in the activity formatter**

---

**Working with record feeds**

When a user follows a record, the user becomes a member of a private group for the record.

Team members can:

• View the record feed from live feed.
• View a list of group members (other users who are following the record).
• Invite another user to join the group. Only users who have access to the record have access to the record feed.
• Subscribe to email notifications.
• Leave the team to stop following the record.

**Follow a record feed from a form**

You can follow records that have a record feed associated with them from within the record form.

1. Navigate to the record in a list or form.
2. Click the **Show on Live Feed** icon in the header.
Follow Task

Follow a record feed from a list
You can follow records that have a record feed associated with them when viewing a list of records. This method allows you to select multiple records to follow.

1. Navigate to a list of records (for example, **Assigned to me**).
2. Select the **Action** check box beside each record to follow.
3. In the **Actions** choice list, select **Follow on Live Feed**.
Follow My Tasks

Post a message to a record feed
Use live feed to post a message to a record feed.

1. Open the record feed in one of the following ways:
   - From your homepage (must already be following the record)
   - As a team in live feed (must already be following the record)
   - From My Live Feed (must already be following the record)
   - From the Live Feed pop-up window
   - From the Live Feed tab on the activity formatter

   - Click the Show Live Feed button ( ) in the form header.

2. Compose the message and add images and links.
3. (My Live Feed only) In the To list, select the record where you want to post the message.
4. (Optional) Select the Work Notes check box to post the message as a work note. Only users with access to work notes on the record can post and see work notes. This option is only available for records that have a journal field.
5. Click Post.

Note: If the record has journal fields for comments or work notes, your message is automatically added to the appropriate field on the record. If the record has a standard text field for comments on the activity formatter, each live post overwrites
the field value. Comments added through live feed start with #LiveFeed on the activity formatter.

Use feeds in Live Feed

Feeds allow users to create focused discussions in Live Feed.

Live feed includes different types of feeds. The user who creates a group or record feed becomes the feed administrator. This user configures the access level for the feed:

- **Public**: any user can see the name on the list of all feeds, view the feed, and join it. Messages appear on the company feed with a link to the public feed.
- **Private**: any user can see the name on the list of all feeds, but only invited members can view the feed and join. Messages do not appear on the company feed.

**Note**: The concept of groups has changed in live feed v2 (starting with the Fuji release).

Create a group feed

Group feeds are created by users so that members with similar interests can find that information in one place. Individual users or teams can join group feeds.

1. Navigate to **Collaborate > Live Feed**.
2. Click **Group Feeds** and click **All Feeds**.
3. Click **Create Group Feed**.
4. Enter the feed name and description. These will appear in the list of group feeds.
5. Indicate how members can join the feed:
   - **Public Feed**: Select this to allow anyone to view and join the group feed.
   - **Private Feed**: Select this to restrict membership to only members invited by the administrator.
When **Private Feed** is selected, the **Show this feed for anyone to find and request to join** check box is displayed. If it is selected, any user can search for this group feed and join it. If the check box is not selected, only users who are invited can see the feed and join the group feed.

6. **Click Create.**

### Create record feeds

When a user views a record on a table that has live feed enabled, such as the **Incident** [incident] table, the user can click the **Show live feed** button at the top of the form to automatically create a record feed.

When a user who has write access to a record’s **work_notes** journal field clicks the **Show live feed** button, that user becomes the record feed administrator. If, for example, a customer calls technical support to report an incident and the customer clicks **Show live feed** on a record, a record feed is created, but the customer is not the record feed administrator. When a support representative later opens the incident and participates in the record feed, the user becomes the feed administrator.

Record feeds are, by default, private unlisted. That is, only invited members can see the name of the record feed in the list of feeds, and join it. Record feed administrators, however, have the ability to change the access level at any time. This can be helpful if, for example, a user is working on a sales opportunity and wants customers to be able to participate in a record feed without granting them access to the records.

### Control how live feed is enabled for records

A property called **glide.ui.show_live-feed_activity** controls whether live feed is automatically enabled for all records.

This glide record is disabled by default. If the property is enabled, a record feed is automatically created whenever a record is viewed, and you become a member of that feed.

A second property, **glide.live-feed.auto_join_document_group**, enables automatic membership to a record feed whenever the associated document is visited and the user clicks **Show Live Feed**.

### View the activity stream in record feeds

When you view record feeds, live feed displays the activity stream for the document.

For example, for an incident feed, the screen displays recent activity for the incident. The activity stream is updated whenever anything is changed in the associated record.
Live feed activity stream

Note: The information in the activity stream is subject to the same ACL rules as those for viewing the underlying document.
Participate in a feed

When you join a feed, you become a feed member.

Feed members can:

- View messages posted to the feed. Non-members can also view the messages for a public feed.
- View a list of feed members.
- Invite another user to join the feed.
- Subscribe to feed email notifications.
- Leave the feed.

1. Navigate to Collaborate > Live Feed.
2. Click either Group Feeds or Record Feeds, and then click All Feeds.
If you received an invitation, click **Accept**. You can **Decline** the invitation if you do not want to join the feed.

- If the feed is public, click **Join**.
- If the feed is private, click **Request**. The feed administrator receives an email notification and must accept your request before you can join the feed.

### Mark a feed as a favorite

Top-level messages in feeds can be marked as favorites on a per user basis only.
You can also search for messages marked as favorites, and remove the favorite designation as needed.

1. Navigate to Collaborate > Live Feed.
2. Click either Group Feeds or Record Feeds, and then click All Feeds.
3. In the list of feeds, click the star icon (🌟) adjacent to the feed name you want to mark as a favorite.

To unfavorite a message, click the star icon (🌟) of a message that is already a favorite.

**View a feed**

You have several options for viewing a feed.

1. Navigate to Collaborate > Live Feed.
2. Click either Group Feeds or Record Feeds.
   - This displays a list of feeds you belong to and an option to view all feeds.
     - To view a feed you belong to, select the feed name.
     - To view a public feed you do not belong to, select Show All and then click the feed name. You must be a member to view the feed for a private feed.

---

**Note:** If you navigate away from the live feed application and then back again, the system displays the feed you last visited if you are a member of it.

---

**View a feed member**

View a specific member of a group feed.

1. Navigate to Collaborate > Live Feed.
2. Click either Group Feeds or Record Feeds.
   - This displays a list of feeds you belong to and an option to view all feeds.
3. Click the feed name.
   - The list of feed members appears, organized by feed administrators and members.

**Invite a new member to a group feed**

The feed administrator can invite another user or a group to join a feed.

When a team is added to a feed, all members of the team also indirectly become members of the feed. Only users, and not teams, can be the feed administrators. A team member who is following a feed can become administrator by directly inviting another user to the feed.

1. Navigate to Collaborate > Live Feed.
2. Click either Group Feeds or Record Feeds, and then select the feed name.
3. Click the Pending members tab.
4. In the Add user or team field, begin entering a user or team name and select a user or team from the suggestion list.
   - The invited user or team members receive an email notification.

**Invite a new member to a record feed**

The feed administrator can invite another user or a team to join a record feed.
When a team is added, each of the individual members of the team become members of the feed. That is, if Team ABC is added to a feed, the feed does not show that Team ABC is a member. Instead, the feed shows each of the individual members of Team ABC as members of the feed.

When users are invited, their membership state is initially Invited. When they accept the invitation, the system checks their access to the work_notes journal field. If they have write access, they become administrator members; otherwise, they become active members.

1. Navigate to Collaborate > Live Feed.
2. Click Record Feeds and select the record feed name.
3. Click the Pending members tab.
4. In the Add user or team field, begin entering a user or team name and select a user or team from the suggestion list.

   If you invite a team, the individual members of the team are invited.

   The invited users receive an email notification.

Remove a member from a feed

The feed administrator can remove any member from the feed.

1. Navigate to Collaborate > Live Feed.
2. Click either Group Feeds or Record Feeds, and then select the feed name.
3. Click the Members tab.
4. Locate the member you want to remove and click Remove.
Remove member

Note: You can remove members regardless of their current state. That is, you can remove members who have already joined the feed or whose membership is pending.

Subscribe to a feed

Direct members of a feed can subscribe and unsubscribe to the feed in order to receive email notifications whenever any activity in the feed occurs, such as new messages being posted, replies, likes, polls, and @mentions.

Individual indirect members—that is, members of a team that is participating in a feed—cannot subscribe or unsubscribe from a feed directly. If the team administrator subscribes the team to a feed, the individual members receive an email notification for activities in the feed such as new messages being posted, replies, likes, polls and @mentions.

All notifications related to a top-level message, such as replies, mentions, and likes, are sent out with the same subject. The subject line defaults to Live Feed followed by the beginning of the subject line from the top-level message. For example, if the subject of the feed is IT Support, the email notification’s subject will be Live Feed IT Support.

1. Navigate to Collaborate > Live Feed.
2. Click either Group Feeds or Record Feeds, and then select the feed name.
3. Click the subscribe icon ( ).
You can click the unsubscribe icon ( ) to stop receiving email notifications.

**Note:** If a team is subscribed to receive email notifications for a feed, but a member of the team did not subscribe to the team, that member does not receive the email notifications.

---

### Navigate between live feed and other modules

If you are participating in a feed and navigate to another module, when you return to live feed it displays the feed you were previously viewing if it is public or if it is a private feed that you are a member of.

For example, assume you are viewing a public feed and then navigate to a particular incident record. Upon returning to live feed, the feed you were previously viewing opens. If you were last viewing a private feed that you are not a member of, returning to live feed opens the Company Feed.

---

### Leave a feed

Members can choose to leave a group feed.

1. Navigate to **Collaborate > Live Feed**.
2. Click either **Group Feeds** or **Record Feeds**, and then select the feed name.
3. Click **Leave**.

**Note:** If you leave a **feed** associated with a record, such as an incident, you automatically rejoin that feed if you modify the associated record again.

---

### Delete a feed

If you are a feed administrator, you can delete the feed.

1. Navigate to **Collaborate > Live Feed**.
2. Click either **Group Feeds** or **Record Feeds**, and then select the feed name.
3. Click **Delete**.
4. Click **Yes** to confirm deletion.

The feed is deleted from live feed. Messages posted to a private feed are deleted. Messages posted to a public feed remain on the Company Feed without a feed link.

---

### Live Feed UI overview

The Live Feed user interface provides many methods you can use to share content with others in your organization.

---

### Update your Live Feed profile

Your profile information includes a photo or image, and tabs for different types of information including messages, feeds, teams, followers, and those who are following you. You can update your profile information and picture at any time.

**Note:** The functionality described here applies to HTML5-compliant browsers, such as Chrome, Firefox, Safari and IE10 and above.

1. Navigate to **Collaborate > Live Feed**.
2. Click your name or title displayed below your picture.

![Profile]

The profile record opens.

![Profile record]

3. Click the pencil icon next to **About Me** and type a short description about yourself that you want to share with others who view your profile. This is text that you might not necessarily want to change on a regular basis.
4. You can change your profile photo using either of the following two methods:
   - Locate the photo file you want to use, and drag-and-drop it over the existing photo.
   - Hover over the existing picture (or tap the photo in the case of the smartphone or tablet interface) to display the **Upload a picture** link. Click the link, navigate to the location of the photo you want to use, and click **Open**.

   ![Upload a picture](image)

   **Note:** Your profile picture is used by the Connect and legacy chat features as well if they are activated.

### Work with Live Feed messages

This portion of the UI gives the user access to various types of messages and tools for grouping and categorizing messages. Also included are methods for identifying which user feeds you are following and which users are following you.
Tools for working with live feed messages

<table>
<thead>
<tr>
<th>Menu section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>My Live Feeds</td>
<td>These are custom feeds that allow you to customize live feed to view the</td>
</tr>
<tr>
<td></td>
<td>content that is most important to you.</td>
</tr>
<tr>
<td>Company Feed</td>
<td>This feed displays all posts, except those posted to private or unlisted</td>
</tr>
<tr>
<td></td>
<td>groups.</td>
</tr>
<tr>
<td>Group Feeds</td>
<td>These feeds are created by users. Record Feeds: These feeds are associated</td>
</tr>
<tr>
<td></td>
<td>with a record, such as an incident or change.</td>
</tr>
<tr>
<td>Record Feeds</td>
<td>These feeds help users collaborate on records by providing a place for</td>
</tr>
<tr>
<td></td>
<td>anyone who can access the record to share messages and post attachments</td>
</tr>
<tr>
<td></td>
<td>specific to that record.</td>
</tr>
<tr>
<td>People</td>
<td>This option displays people who are following the current user and people</td>
</tr>
<tr>
<td></td>
<td>the current user is following.</td>
</tr>
<tr>
<td>Teams</td>
<td>This option is used to combine users into groups for the purpose of</td>
</tr>
<tr>
<td></td>
<td>subscribing to specifically-focused conversations.</td>
</tr>
<tr>
<td>Hashtags</td>
<td>Hashtags are words marked with a hash (#) symbol in messages. Hashtags are</td>
</tr>
<tr>
<td></td>
<td>used to categorize messages by keyword or topic for improved search results</td>
</tr>
<tr>
<td></td>
<td>messages filtered from all conversations that include specific hashtags.</td>
</tr>
</tbody>
</table>

View another Live Feed user

When a requester user, one that has no ServiceNow role, is viewing a feed and points to another user’s picture, information for the user appears from the Business Card view of the User (sys_user) table.

You can customize ACLs to increase the amount of information you want displayed for users with different roles.
If you click a user's name or title, the user's profile appears. Click the tabs to view different types of information for the user.
Profile tabs

**Follow other Live Feed users**

As you use Live Feed, you can follow the message threads of other users.

1. Navigate to a thread that the user you want to follow is engaged in.
2. Click that user's name or point to the user's picture.
   A Follow link appears in the user's profile.
3. Click **Follow**.
4. To stop following the user, navigate to **People > Following**.
Unfollow

5. Click Unfollow.
6. To view people who are following you, navigate to People > Followers.

Select feeds

A feed is a stream of related messages. You can use the feed selector to switch between feed types and to view specific group feeds and record feeds.

1. Use the Search field to locate any type of feed. As you type in the Search field, the results are dynamically displayed. For example, if you type INC, records that are incidents are forced to the top of the results list.
2. You can also select the following types of feed information.

### Feeds types

<table>
<thead>
<tr>
<th>Feed</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>My Live Feeds</td>
<td>Displays the following posts:</td>
</tr>
<tr>
<td></td>
<td>• messages from users you follow</td>
</tr>
<tr>
<td></td>
<td>• messages with hashtags you follow</td>
</tr>
<tr>
<td>Company Feed</td>
<td>Displays all posts, except those posted to private or unlisted groups.</td>
</tr>
<tr>
<td>Add Group Feed</td>
<td>Allows you to add a group feed.</td>
</tr>
</tbody>
</table>
Follow feeds

You can view users who are following you or other users you are following. To view users who are following you or other users you are following, click **People** in the sidebar. The system shows 10 most recent followers or users you are following.

<table>
<thead>
<tr>
<th>People</th>
</tr>
</thead>
<tbody>
<tr>
<td>Following</td>
</tr>
<tr>
<td>--------</td>
</tr>
</tbody>
</table>

If either list contains more than 10 users, a Show More link appears.

**Note:** If you are following a particular user whose profile changes, that user moves to the front of the Following list. This alerts you to changes in the profile of a user you are following.

Bookmark feeds and hashtags

The live feed interface uses the standard bookmarking functionality for feeds and hashtags. In UI15 and UI11, you can drag-and-drop group feeds and hashtags from the Feed Summary section to the Edge for quick access.
Bookmark a hashtag

Add Live Feed to your homepage

You can add Live Feed to your own homepage or to a global homepage.

1. Navigate to a homepage.
2. Click the add content icon in the top left corner of the homepage.
3. Select Live Feed in the left panel.
4. On the bottom of the window, click Add here in the appropriate layout position, then close the window.
Note: Administrators can add live feed to a global homepage to make it available for all homepage users by default. Users with any role can add live feed to their homepage; however, administrators can restrict this ability.

Use Live Feed with UI11

Using Live Feed with UI11 requires the UI11-Navpage layout with multiple panes plugin.

1. If you do not see a gray toolbar on the left side of the screen (called your edge), click the Switch to the new UI link in the banner.
2. Navigate to Collaborate > Live Feed.
3. Drag the Live Feed module to the edge.
4. Point to the bookmark on your edge. When the tip window appears, click Edit Bookmark.
5. Select the Flyout check box.
6. Click Update.
   - You can now access live feed in a flyout window without navigating away from your working panes.
   - Notifications appear on the edge when new messages are posted in your My Feed.

   ![UI11 notification]

   - When you open the bookmark, a blue circle appears beside new messages.
Post content in Live Feed

In Live Feed, you can post new messages and replies to existing messages for all users in the feed. You can also send a reply message to a team or record.

Post a live feed message

You can post a message to open a new feed.

1. Navigate to **Collaborate > Live Feed**.
2. Click the feed to which you want to post your message, for example My Live Feed, Company Feed, and so on.
3. Enter a message in the **Share your thoughts** field. Use hashtags, if you want.
4. As needed, click to add a poll, attachment, or screenshot image, respectively.
5. Click **Post**.
Reply to a live feed message

To participate in an existing thread of a feed, you can compose and submit a reply message. By default, the message is visible to all members of the feed.

1. Navigate to Collaborate > Live Feed.
2. Locate the message you want to reply to.
3. Type your reply in the message box and click Reply.
   - As needed, you can add hashtags, attachments, links, or knowledge base articles.
4. To limit who can view the reply to a single individual, select a user from the To choice list.
5. Click Reply.
6. By default, 7 replies are visible for each message. To view additional replies, click Show all replies. Any reply to a reply includes a Threads link.
7. Click Threads to view all of the replies within the selected reply in reverse chronological order within the Message Thread pop-up window, similar to an email thread.
Message Thread

Nirupam Biswas

8 days ago

Confused for a few mins about the voting, I got

Navakanth Reddy

8 days ago

#suggestion(s) A common black vertical line just before the bars would help with this. Also, line spacing between two options should be more than single-spaced.

Also, the bar says 5 people voted and it shows up 5 people and 1 more. Is this a #bug?

Nirupam Biswas

8 days ago

I guess we need some visual distinction between the poll question and the options. After voting, I got confused for some moments why there are four options in result. See screenshot.

Shouvik Goswami

8 days ago

We have enabled polls in Live Feed. Please review and provide #suggestions and #feedbacks

How do you like the poll in Live Feed?

- Exactly what I was looking for
- Wanted something more
- Did not visualize it this way

Vote

Peter Smith

8 days ago

about a minute ago

Ryan Manuel

8 days ago

- I set up a poll
- I feel like it is a bit complicated
- Get some opinions
- It still shows 'that' results
- I tried to edit the poll
- When I view the poll, it is not showing the results

Share · Tags (2)
Attach files, links, images, and knowledge articles to messages

In addition to entering text, you can attach files, such as images, documents, and spreadsheet files in any ServiceNow supported file type to live feed messages.

Administrators can manage attachment file settings, such as supported file types and maximum attachment file size, by editing system properties.

You can also include links to user-defined URLs and knowledge articles contained in your instance’s knowledge base.

---

**Note:** The functionality described here applies to HTML5-compliant browsers, such as Chrome, Firefox, Safari and Internet Explorer 10 and above. Significant differences while using different browsers are highlighted.

---

Attach a file to a post or reply

You can attach files to a post by dragging a file into a post or pasting an image from the clipboard.

Use the paperclip icon ( ![paperclip](image)) to drag files into a post. Additionally, you can paste images into a post or reply from the clipboard.

1. Do one of the following:
   - While composing a post or reply (see Reply to a Message), locate one or more images or other supported types of files, and drag them into the message box.
   - Click the paperclip icon ( ![paperclip](image)) in the message box, navigate to the location of the files you want to attach, select them, and click Open.

2. To add more files, drag-and-drop additional files into the text box below the displayed files or images, or click the plus sign.
Attaching files

3. If you want to delete an attachment before posting the message, click the trashcan icon adjacent to the attachment.
4. Enter a comment to share your thoughts about the image.

Note: The Post button is enabled only after you add the comment.

5. Click Post or Reply.
6. If you added files that do not contain previews and then posted the message, they will be listed in the message box with a Download link.
7. Click the link to download the files.

**Copy an image from the clipboard**

In addition to adding files to a message, you can also copy images to the clipboard and paste them into a message or reply.

1. Click into the **Comment** box and add a comment.

   ![Comment box](image)

   Here is how to drag-and-drop tags in order to bookmark them.

2. Click the **Add an image** button.
   
   The **Screenshots** dialog box opens.

3. Right-click the **Paste an image here** box and select **Paste** to paste the image from the clipboard.
4. To add another image, repeat the previous steps.
5. When you finish pasting images into the message, click **Done**.
6. To change the link text, click **Pasted Image** and enter a new label.
7. When you finish, click **Post** or **Reply**.
8. To remove an image, click the trash can icon adjacent to the link.
9. To make changes to an existing image, click the edit icon (✏️).
Add a link to a post or reply

Add or modify a link to a live feed post.

1. Click into the Comment box.
   The Add a link button appears.
2. Click the Add a link button.
   The URL and Link text fields appear.

3. Enter the URL and the text you want to appear as the link.
4. To add another link, click the link icon under the URL field.
5. When you have finished entering your message, click Post or Reply.

URL Saved
To remove a link, click the trash can icon adjacent to the link. To make changes to an existing link, click the edit (✏️) icon.

**Add a knowledge article link to a post or reply**

Use the ID of a knowledge article to post it as a reply to a live feed conversation.

1. While composing a post or reply, type the ID of the knowledge article you want to link to. You do not need to identify the knowledge article ID as a hyperlink; live feed recognizes it as such and automatically converts it into a link when the message is posted.
2. When you are finished entering your message, click Post or Reply.

**Add a poll to a message**

When you are posting a message, you have the option of creating a poll in order to record your viewers' opinions. As users take the poll, their feedback statistics are displayed within the feed.

1. Open the feed where you want to create a message with a poll.
2. Enter the message with an invitation to take the poll in the Share your thoughts box.
3. Click the poll (📊) icon.
Poll

4. In the **Question** field, enter the question on which you are soliciting opinions.
5. In the **Option** fields, enter possible responses to the query.
6. To add more response options, click **Add more options**.
7. Click **Post**.

After the poll is posted, users who view the message can vote. After they vote, their pictures appear next to their response, with others who have voted for the same option.

**Note:** Only the poll creator can view results without casting a vote. Other members can see results only after casting a vote or if the poll is closed.
An email notification with the poll result is sent to all participants of the poll informing them that the poll is closed.

Add mentions to a message

An @mention is any posted update that contains @username anywhere in the body of the message.

The user’s name, with a link to that user’s feed, is inserted into the message. Additionally, the mentioned user receives an email notification about the mention. This is a great way of bringing attention to other members in a conversation. All @mentions are included in the logged-in user’s My Feed.

Note: If an @mention is used by a member of a team, only members of that team appear in the auto-suggest list.

1. While entering a message or reply in a conversation, type @username anywhere in the message. As you type, an auto-suggest list appears with names and pictures of users that
match your entries. For example, if you type @t, the auto-suggest list shows the pictures and names of all users with names that start with T.

2. Click the user you want to add. That user’s name is inserted into the @mention in the body of the message.

Note: My Feed displays @mentions of you and the teams you are a member of. Profile feeds for another user display only @mentions of that user.

Like a message
Like a message to provide feedback to the author.

1. Navigate to Collaborate > Live Feed.
2. Click Feeds.
3. Locate the feed that contains the message you want to like.
4. Under the message title, click Like.

If the message has previously been liked, the number of likes for a message displays next to the Like link.

For a top-level message, the profile pictures of the first 5 users who liked a message are displayed. Any additional users who liked the message can be viewed by hovering over the # more link. If the logged-in user has liked the message, that user’s image will appear first, followed by the image of the user who last liked the message.

For a reply, you must hover your mouse pointer over the count link to view the users who liked the message.

Note: After a message has been liked, it cannot be unliked.
Delete a message

Users can delete any of their own posts or replies. A conversation administrator can also delete messages.

1. Hover over the message you want to delete.
2. Click the trash can icon in the upper-right-hand corner of the message box.
3. Click **Delete** in the confirmation box.
   The message disappears from the feed.

Configuration Management Database (CMDB)

With the ServiceNow® Configuration Management Database (CMDB) application, build logical representations of assets, services, and the relationships between them that comprise the infrastructure of your organization. Details about these components are stored in the configuration management database (CMDB) which you can use to monitor the infrastructure, helping ensure integrity, stability, and continuous service operation.

Use core features such as CMDB Health, CMDB Identification and Reconciliation, and CMDB CI Lifecycle Management to monitor and detect health issues, reconcile data integrity issues, and manage data life cycle.

**Note:** CMDB modules, features, and wizards are not supported on mobile devices. You cannot use a mobile device to access the CI Class Manager or the Query Builder. Or to access or configure CMDB features such as Identification and Reconciliation, CMDB Health, CI Lifecycle Management, baseline CMDB, and proposed changes.

<table>
<thead>
<tr>
<th>Explore</th>
<th>Set up</th>
<th>Administer</th>
</tr>
</thead>
<tbody>
<tr>
<td>• CMDB release notes</td>
<td>• Options to populate the CMDB</td>
<td>• Baseline CMDB</td>
</tr>
<tr>
<td>• Upgrade to Jakarta</td>
<td>• Whitepaper: CMDB Design &amp; Configuration</td>
<td>• CI relationships in the CMDB</td>
</tr>
<tr>
<td>• Configuration Management and the CMDB</td>
<td>• Whitepaper: CMDB Design</td>
<td>• CMDB classifications</td>
</tr>
<tr>
<td>• CMDB Identification and Reconciliation</td>
<td>• Whitepaper: Improving Configuration Item Data Quality</td>
<td>• Video: CMDB Health dashboard</td>
</tr>
<tr>
<td>• CMDB Health</td>
<td>• Whitepaper: CMDB Design Guidance</td>
<td></td>
</tr>
<tr>
<td>• CMDB CI Lifecycle Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Activate the Extended CMDB plugins</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Use</th>
<th>Develop</th>
<th>Troubleshoot and get help</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Create a CI class</td>
<td>• Developer training</td>
<td>• Search the HI knowledge base for known error articles</td>
</tr>
<tr>
<td>• Create or edit a CI relationship</td>
<td>• Developer documentation</td>
<td>• Contact ServiceNow Technical Support</td>
</tr>
<tr>
<td>• Add a proposed change to a CI</td>
<td></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.
Configuration Management and the CMDB

The Configuration Management data base (CMDB) creates and maintains the logical configurations your network infrastructure needs to support a ServiceNow service.

These logical service configurations are mapped to the physical layout data of the supporting network and application infrastructure in each of your respective domains. They track the physical and logical state of IT service elements and associate incidents to the state of service elements, which helps in analyzing trends and reducing problems and incidents.

The configurations are stored in a configuration management database (ServiceNow CMDB) which consists of entities, called Configuration Items (CI), that are part of your environment. A CI may be:

- A physical entity, such as a computer or router
- A logical entity, such as an instance of a database
- Conceptual, such as a Requisition Service

In each case, there are attributes about the CI that you want to maintain, and there is control you want to have over the CI. There are changes that may need to be made and tracked against the CI. Also, a CI does not exist on its own. CIs have dependencies and relationship with other CIs. For example, the loss of disk drives may take a database instance down, which affects the requisition service that the HR department uses to order equipment for new employees.

It is this relationship data that makes the CMDB a powerful decision support tool. Understanding the dependencies and other relationships among your CIs can tell you, for example, exactly who and what is affected by the loss of that bank of disk drives. When you find out that a router has failed, you will be able to assess the effect of that outage. When you decide to upgrade the processor in a server, you can tell who or what will be affected during the outage.

Configuration items differ from environment to environment because each customer has unique needs. Details about the exact physical attributes of a computer may be needed by one customer, but may represent meaningless data to another. The NOW Platform provides a mechanism to easily define new classes of configuration items and new relationships that may exist between CIs. New classes can be defined that extend other classes. For example, a laptop class exists that extends the computer class. The computer class itself extends the base CI class. Customer class extensions are automatically part of the ServiceNow environment and blend seamlessly into the integration points for other ITIL processes.

You can for example, set the Used for attribute in the cmdb_ci_server table to a value such as ‘development’, ‘test’, or ‘production’. These values indicate the environment that the CI is supporting, and serve as a way of tracking a CI through its lifecycle in a changing environment.

Roles required

For viewing CMDB-related records in the user interface, the itil role is usually sufficient. For updating records and for other manipulation of records, roles with higher credentials are usually required, as noted.
**ITIL Configuration Management integration**

The CMDB has relationships with IT service management processes in the following areas: ITIL incident management, ITIL problem management, ITIL change management, ITIL service catalog management, and financial management.

**ITIL Incident Management**

Configuration management assists *Incident Management* by providing the Service Desk with immediate information on the CIs affected, and more timely resolution of faults by understanding what CIs have been affected and changed.

**ITIL Problem Management**

Configuration Management assists *Problem Management* by linking the CIs affected by problems to the Incident / Problem / Change Management processes, and ensuring the CI status is properly maintained.

**ITIL Change Management**

Configuration Management assists *Change Management* by recording which CIs have been changed and controlling the status of CIs throughout the entire CI lifecycle. Configuration Management ensures any changes made to CIs are recorded and kept accurate.

**ITIL Service Catalog Management**

With *Service Portfolio Management*, business services in the CMDB can also be managed by the Service Catalog team, and exposed to end users who can then request items from them.

**Financial Management**

With *Cost Management*, costs can be associated with configuration items, so that the cost associated with Configuration Management can be tracked and bundled into expense lines, budgets, or cost centers.

**ITIL**

The IT Infrastructure Library (ITIL) is an integrated, process-based framework for managing IT services.

It provides guidance for creating and operating a Service Desk that provides efficient communication between the user community and the IT provider. Originally initiated to improve IT service management for the UK central government, it has become a standard for many organizations; public or private sector, large or small, centralized, or distributed.

ITIL provides processes for three service concepts: design, transition, and operation.

<table>
<thead>
<tr>
<th>Service concept</th>
<th>Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- service level management</td>
</tr>
<tr>
<td></td>
<td>- availability management</td>
</tr>
</tbody>
</table>
Service concept

<table>
<thead>
<tr>
<th>Processes</th>
</tr>
</thead>
</table>
| • capacity management  
• supplier management  
• service catalog management |

Transition

<table>
<thead>
<tr>
<th>Processes</th>
</tr>
</thead>
</table>
| • change management  
• knowledge management  
• asset management  
• configuration management  
• release management |

Operation

<table>
<thead>
<tr>
<th>Processes</th>
</tr>
</thead>
</table>
| • request fulfillment management  
• event management  
• incident management  
• problem management  
• facilities service automation |

Service design

This guide provides a general overview of ITIL service design concepts.

Service level management

The service level management process is designed to ensure customer satisfaction within IT service processes. Service level agreements are made between the IT staff and the customers, and the IT desk must monitor their performance as compared to the agreements. In addition, underpinning contracts with external vendors and operational level agreements with internal vendors ensures that these service level agreements are feasible.

Availability management

The availability management process ensures that availability within a system is kept as close to 100% as possible. By both reacting to past service failures, and planning to avoid future service failures, availability management can greatly increase end-user satisfaction with services.

Capacity management

The capacity management process is designed to ensure that business services are not made unavailable by over-capacity. By analyzing past failures and planning for growth of demand of services, capacity management can increase end-user satisfaction with services.

Supplier management

Supplier management is a process that defines and monitors agreements between an IT department and an external supplier.
**Service catalog management**

The service catalog provides a front end for customers to request items and services. Service catalog management ensures that this service catalog provides accurate and useful information on the items and services.

**Service transition**

This guide provides a general overview of ITIL service transition concepts and how the Now Platform can enable these processes.

**Change management**

The change management process ensures that standardized methods and procedures are used for efficient and prompt handling of all changes to minimize the impact of change related incidents on service quality. Consequently, change management aims to improve the day-to-day operation of the organization. IT-related changes that may affect one or many customers are tracked with change management. Adding memory to one machine, getting a new server, and installing the latest Windows OS on all PCs are all examples. To find out how the ServiceNow platform implements change management, see [Change Management](#).

**Knowledge management**

The knowledge management process ensures that important information flows freely throughout the IT organization. Knowledge management keeps the CMDB and knowledge base of an organization up-to-date, and uses a knowledge-centered support approach to reduce repeat incidents and problems. For more information on how the ServiceNow platform implements knowledge management, see [Knowledge Management](#).

**Asset management**

Asset management enables a process of monitoring processes, organizations, people, information, applications, infrastructure, and financial capital within an organization. This allows the organization to collect accurate records of these business components, making them available for both internal and external auditing processes. To find out how the Now Platform implements asset management, see [Asset Management](#).

**Configuration management**

Configuration management provides a logical model of the infrastructure or a service by identifying, controlling, maintaining and verifying the Configuration Items in existence. To find out how the Now Platform implements configuration management, see [Configuration Management](#).

**Release management**

This discipline of IT service management is the management of all software configuration items within the organization. It is responsible for the management of software development, installation and support of an organization's software products. Software Control & Distribution procedures include the management of the software Configuration Items and their distribution and implementation into a production environment. This involves the definition of a release
program suitable for the organization, the definition of how version control is implemented, and the procedures surrounding how software is built, released and audited. To find out how the Now Platform implements release management, visit Release Management.

Options to populate the CMDB

You can populate the CMDB by using Discovery, by importing information from another source, by integrating with an existing external CMDB, or by manually creating a CI.

When you populate the CMDB with information, you create a record for each configuration item in the cmdb_ci table or on one of the tables that extend that table.

ITIL configuration management auto-discovery

The key to any configuration management business practice is the initial and on-going inventory or discovery of what you own. The ServiceNow platform provides three options for auto-discovery:

- The separate and highly robust Discovery product.
- A lightweight native discovery tool, called Help the Help Desk, as part of the overall CMDB. Help the Help Desk enables organizations to proactively scan their network to discover all Windows-based PCs and the software packages installed on those PCs. This WMI-based discovery is included in the core ServiceNow functionality, in the Self Service application, at no additional cost.
- For organizations that want to leverage the discovery technologies they already have deployed (SMS, Tally NetCensus, LanDesk, and so on), the ServiceNow platform supports integrations to those technologies via web services. Scanned data can be mapped directly into the CMDB.

For further information on designing, constructing, and maintaining the CMDB, see white papers CMDB Design & Configuration and CMDB Design.

Use Discovery

The Discovery product automatically populates the CMDB. Discovery runs probes and sensors to collect information on hardware on the network, software running on that hardware, and the relationships between all the items found. This information is sent back to the ServiceNow instance, and is used to populate the CMDB.
Import information from another source

Information can be imported to the CMDB using import sets. Import sets find files of information (in formats such as XML, Excel, or CSV), import them, and transform them onto the required table. This process can be scheduled or performed on demand.

To import relationships between CIs, use import sets to populate the table (cmdb_rel_ci) with information on the parent, the child, and the nature of the relationship. The (cmdb_rel_ci) table displays a list of all CI relationships and is useful when importing CI data.

Integrate with an existing external CMDB

If the data required for the CMDB is already being collected by another CMDB, it is possible to collect the information from that CMDB in an automated process.
Manually create a CI

Create a single CI for a specific class.

1. Locate the table for which you want to create a CI, and display the list view for the class:
   - Navigate to and expand Configuration. Then, select one of the classes such as Business Services.
   - In the navigation filter of the application navigator, enter the table label (such as 'Linux'), or the table name in the format of <table name>.list (such as 'cmdb_ci_linux_server.list'). Then, press Enter.

2. In the list view of the table click **New** and fill out the form fields for the table.

3. Click **Submit**.
Baseline CMDB

CMDB baseline provides capabilities that help you understand and control the changes that have been made to your configuration items (CIs) in the CMDB.

- You can create a baseline, which is a snapshot of your configuration items in the CMDB. You can review the changes that have been made to that configuration item since a previous baseline. Multiple baselines may be created and the system tracks the changes that have been made per baseline.

Creating a baseline captures the attributes of the CI as well as all first-level relationships for the CI. Any changes to the base CI or to any related CIs are captured and displayed. Newly created CIs are not automatically added to a baseline.

- Associate a configuration item with a task, a change or change task, and to propose changes to the CI after the change is complete. You can record changes, and these changes are not applied to the CI immediately but are delayed until the change is complete.

When the change is complete, you can choose to apply the proposed changes which makes all changes previously proposed and associates the changes with the task.

Create a CMDB baseline

You can create a baseline for a CI to track updates to the CI over time.

Role required: ecmdb_admin and itil

1. Navigate to Configuration > Baselines > Baselines.
   
   If the Baselines module is not visible in the Configuration application, the module is inactive. In that case append /sys_app_module.do?sys_id=f4463879a9fe3dba01b30bc100cbf404 to the instance URL, and in the Module - Baselines form, ensure that the module is Active.

2. Click New.

3. Enter a Name for the baseline.
   
   By default, the cmdb_ci table is selected so that the record creates the baseline for all configuration items in the system.

4. Optional: To limit the baseline to specific CIs, select a different Table or choose Conditions that a CI must meet for it to have a baseline entry.
   
   For example, you might create a baseline for the Database table with the condition (Location) (is) (<configured location>).

5. Click Submit.

   The creation of a baseline is time consuming and occurs in the background. A message at the top of the record list notifies you that your baseline has been scheduled and you will receive an email when the process is complete.

Display baseline differences

You can see the changes that have been made to a CI or any first level related CIs by configuring the CI form layout to display the CMDB Baseline diff field. This field is labeled Baseline differences on the form.

Role required: itil

1. Open a CI record.

2. Select the baseline you want to see for this CI from the choice list.
   
   The field displays the details of any changes that were made to the current record for the selected baseline, or indicates that no changes were made.
3. To add a relationship to the CI, click the green plus icon in the Related Items toolbar. The new relationship appears below the toolbar. For more information about the Related Items toolbar and how to control the display, see CI relations formatter.

4. Update a related CI and see the changes displayed as Basic attribute changes in the current CI record.

### Proposed changes

The proposed changes feature allows you to pre-configure changes to configuration items and their associated relationships. These pre-configured changes are prepared to be implemented, but do not actually happen until they are applied at a later time.

When you view a CI, the proposed changes can be displayed so that you can see what is planned.

This feature is useful when you want to make modifications while a change process is in the approval stage, and only implement the changes after the approvals are complete. If the change is never approved, no changes to records have to be reversed. If the change is approved, a quick command applies all the proposed changes.

You can make the following proposed changes to a CI:

- Modify any field on the CI form.
- Add or delete a relationship to that CI.

To modify a relationship, you must delete the current relationship and add a new relationship. You cannot delete a proposed change.
View CI history

You can view the history of changes to a CI in a list, calendar, or timeline format.

View the proposed changes of a CI

You can view the proposed changes so that you can see what is planned for the CI.

Role required: personalize_form

To view any proposed changes, configure the CI form layout to display the CMDB Scheduled Changes field. Proposed changes are not displayed in a CI form by default.

1. Navigate to Change > Open and open a change request.
2. In the Affected CIs related list, open the Configuration Item.
   You may also navigate directly to the CI form.
3. Right-click the form header bar.
4. Select Configure > Form Layout.
5. Move the CMDB Scheduled Changes field to the Selected pane.
6. Click Save.
   The CI form shows the details of any proposed changes in the Scheduled changes area.

Add a proposed change to a CI

Proposed changes to a CI can be made while viewing a change request or any task-related record.

Role required: itil

1. In the Change Request form, go to the Affected CIs related list.
   If there are no CIs in the Affected CIs list, click Edit to add CIs that are affected by this change request.
2. Right-click the CI that you want to configure for a proposed change, and select Proposed Change.
3. Complete the form to make the proposed changes, and click Save Proposed Change.
   Click Update to apply the changes immediately. Click Delete to delete the CI.
4. To propose an addition or a removal of a CI relationship:
   a) Click the plus icon in the Related Items section.
   b) In the Relationships section, add or delete a relationship. For information about using the relationship editor, see Create or edit a CI relationship.
   c) Click Save Propose Change.
   d) Confirm saving the proposed change.

Click Update or Delete to commit the changes immediately.

**Note:** Use only with CI relationships. Proposing additions or removal of relationships is not valid for user relationships and group relationships.

After the proposed changes are saved, the Apply Proposed Changes button appears on the Change Request form. This button lets the user commit the proposed changes to the CI. Your business processes determine the appropriate time to commit the changes. The CI retains
the existing data until the proposed changes are committed. However, users can see that changes have been proposed.

Apply a proposed change to a CI

When you apply the proposed changes, all the proposed changes for that change request are applied to the configuration item. You can apply proposed changes without verification, or if verification tests of the proposed changes have failed.

Role required: itil

After you apply the proposed changes, the Scheduled changes part of the form displays No scheduled changes found. You can configure proposed change verification rules which you can use to verify proposed changes before applying the changes.

1. Navigate to the Change Request form.
2. Click the Apply Proposed Changes button.
   You may have to right-click the form header and select the Reload Form option to see the changes.

Create or edit a proposed change verification rule

Ensure that proposed changes meet business requirements and do not introduce invalid data to the CMDB, create a rule that includes a script to verify the proposed changes.

Role required: asset or itil

When you configure proposed change verification rules for a CI, you have an option to verify that the proposed changes pass the verification test script in the rule. The verification test results are logged as passed or failed, and you can view the results. Running the verification test is not mandatory, and a failed verification test does not prevent you from applying proposed changes.

1. Navigate to Configuration > Change Verification > Proposed Change Verification Rules.
2. Click New or select an existing rule to edit.
3. Fill in the fields, as appropriate.

Proposed Change Verification Rules form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule name</td>
<td>The name of this rule.</td>
</tr>
<tr>
<td>Table name</td>
<td>The table to which the rule applies.</td>
</tr>
<tr>
<td>Filter condition</td>
<td>Conditions to apply this rule to specific CIs.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box to activate this rule.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Rule script</td>
<td>A verification Java script that needs to return true or false. For example:</td>
</tr>
</tbody>
</table>
|              | ```javascript
validateRule()
{
  var os =
current.getValue("os");
  var cpu =
current.getValue("cpu_count");

  //Use
current.getValue(fieldName)
to get the proposed
change value, eg. var os =
current.getValue("os");
  //Your verification code

  if (os != "SunOS" || cpu < 2)
    return false;
  //Return true to pass the
verification and false if the
verification failed
    return true;
}
``` |

4. Click Submit or Update.

On the Change Request form, you can click Verify Proposed Changes to verify proposed changes for the affected CIs.

**Verify proposed changes**

Before applying proposed changes to affected CIs, use proposed change verification rules to verify that the changes meet business requirements and do not add invalid data to the CMDB.

Create or edit the rules used to verify proposed changes. For details, see [Create or edit a proposed change verification rule](#).

Role required: none

You can apply proposed changes even if they are unverified or fail a verification test.

1. Open the Change Request form that affects the CI.
2. Click Verify Proposed Changes.
   The proposed changes are verified against any proposed change verification rules in which the CI meets the Filter condition criteria.
3. Review the message that appears at the top of the form after the verification process is finished.
   The message states whether the verification tests passed or failed.

To view the details of any verification tests that were performed for the change request in the past two days, click the Proposed Change Verification Log related link.
Create or edit a planned change validation script

Create a custom script that checks if a change to a class was valid according to business requirements, and whether the change was planned or not. A planned change validation script is used whenever a CI change is viewed in the CI timeline or change history.

Role required: admin or itil

The system attempts to validate each CI change as follows:

- If a custom script exists for the CI or one of the CI parents, then the script is executed and the results are used to flag the change as valid or invalid. Parent CIs are examined in the hierarchical order.
- If a custom script does not exist for the CI or any of its parents, then a predefined validation script is used. The change is determined as a planned change if the change occurred between the Work start and Work end dates of the change request associated with the changed CI.

However, this check is not always reliable because a user might have manually modified the CI within the work dates, which flags the change as valid even if it is invalid.

The script needs to return a boolean, true or false, which depends on meeting the test criteria in the script. You can define a separate script for each CI class, and you can define multiple planned change validation scripts for a single class. For example, to maintain different versions of the script. Only one script can be active for a CI class at any given time.

These are the parameters that uniquely characterize a change:

- The fields that were changed
- The data source that performed the change
- The time stamp of the change

To correctly determine the validity of a change, examine the parameters and apply business logic to evaluate if the validation tests are met. A planned change validation script can test any of these characteristics and determine when a change meets pre-established criteria. For example, the custom script can check if the mode of the CI is operational or maintenance, or who initiated the change.

1. Navigate to Configuration > Change Verification > Planned Change Validation Script.
2. Click New or select a validation script to edit.
3. Complete the form.

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Check box to activate this script for validating changes.</td>
</tr>
<tr>
<td>Applies to</td>
<td>Class that this script applies to.</td>
</tr>
<tr>
<td>Script</td>
<td>Script to run to validate a change. If the script does not return a boolean value, then it is configured to false.</td>
</tr>
</tbody>
</table>

The script has a template which displays the input variables of the script.
### Template script input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>current</td>
<td>GlideRecord</td>
<td>Current record that is being processed.</td>
</tr>
<tr>
<td>updatedOn</td>
<td>GlideDateTime</td>
<td>Time stamp of the change.</td>
</tr>
<tr>
<td>updatedBy</td>
<td>String</td>
<td>Entity responsible for the change.</td>
</tr>
<tr>
<td>fieldsChanged</td>
<td>String</td>
<td>Comma-separated list of the names of all fields that were changed.</td>
</tr>
</tbody>
</table>

This sample script checks who initiated the record update. It returns true if admin initiated the record update. Otherwise, the script returns false.

```javascript
isValidChange();

function isValidChange(/*GlideRecord current, GlideDateTime updatedOn, String updatedBy, String changedFields*/) {
  // Return true if the user that updated the record has an admin role
  return isUserAdmin(updatedBy);
}

function isUserAdmin(userName) {
  var grUser = new GlideRecord("sys_user");
  grUser.addQuery('name', userName);
  grUser.query();
  if(grUser.next()) {
    var roles = new GlideRecord("sys_user_has_role");
    roles.addActiveQuery();
    roles.addQuery('user', grUser.sys_id);
    roles.query();
    while(roles.next()) {
      if(roles.role.name == 'admin')
        return true;
      }
  }
  return false;
}
```

4. Click Submit.

### CI relationships in the CMDB

The CMDB, in contrast to a static asset list, helps you track not only the configuration items (CIs) within your system, but also the relationships between those items.

A relationship in the CMDB consists of two CIs and a relationship type:

- Parent CI
- Child CI
- Type of the relationship that links both CIs

For example, in the (Server1) (Managed by) (Server2) relationship:
- Server1 is the child CI
- Server2 is the parent CI
- (Managed by) is the relationship type

For example, a web application might read data from an instance of Oracle, which in turn might depend on a piece of underlying hardware. Most CIs in a CMDB have multiple relationships to other CIs, users, and groups.

The relationships between CIs can be automatically discovered. If you use Discovery, many relationships can be automatically loaded into the system through the discovery process. If you import your data from another system, you get some form of relationships.

You can add to automatically discovered relationships, create relationships, or edit relationships for a CI by launching the CI relationship editor from the CI form.

**Suggested CI relationships**

The system keeps a table of relationship types that are appropriate for a CI type, based on its class. You can view these relationships by navigating to Configuration > Suggested Relationships. You can also create additional suggested relationships.

**Suggestion model**

The relationship editor has a base CI. The base CI designates the CI that a user was on before launching the editor, as the base CI in the new relationship. If you launched the relationship editor from the Inux100 CI, then Inux100 becomes the base CI. Also, every CI in the system has a type (class). For example, bond Inux100 is of the Linux server type.

Many CI types are children of other types in the hierarchy. For example, the class hierarchy for a Linux server is:

```
cmdb_ci -> cmdb_ci_computer -> cmdb_ci_server -> cmdb_ci_linux_server
```

Looking at a Linux server, the suggestion model works by analyzing the suggested relationship table for all relationships whose base class is the current base class of the user or any one of its parent classes. For example, when looking at a Linux server, the suggestion model would retrieve any relationships whose base class was:

```
cmdb_ci_linux_server, cmdb_ci_server, cmdb_ci_computer, or cmdb_ci
```

**Suggested CI relationships in the relationship editor**

The CI relationship editor uses the suggestion model to help users select reasonable relationships for configuration items.

For example, consider these relationship types in the system:
- Provides Power for :: Receives Power From
- Runs on :: Hosts

Typically, a user uses these relationships to defines the following reasonable relationships between two items as follows:
- a database runs on a server
• a rack provides power for a server

Typically, neither of the following definitions would be appropriate:
• a rack runs on a server
• a server runs on a database

Add a suggested CI relationship

You can define suggested relationships that can be selected when new CI relationships are created.

Role required: admin

2. Click New.
3. Complete the form.

Suggested Relationship fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base class</td>
<td>The base class in the relationship, which depending on the relationship type, is either the parent or the child in the relationship.</td>
</tr>
<tr>
<td>Relationship</td>
<td>Relationship type.</td>
</tr>
<tr>
<td>Dependent class</td>
<td>The dependent class in the relationship, which depending on the relationship type, is either the parent or the child in the relationship.</td>
</tr>
</tbody>
</table>

You can add suggested relationships such as the following

<table>
<thead>
<tr>
<th>Base Class</th>
<th>Relationship</th>
<th>Dependent Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle</td>
<td>Is Hosted On</td>
<td>Linux Server</td>
</tr>
<tr>
<td>Oracle</td>
<td>Is Hosted On</td>
<td>Solaris Server</td>
</tr>
</tbody>
</table>

Note: The same parent class and relationship can appear more than once.

You may need to delete a suggested relationship, for example, to limit the choice of available relationships in the CI relationship editor. Removing a suggested relationship does not affect relationships that are created or updated by Discovery.

CI relations formatter

The default CI form includes a CI relations formatter from which you can examine a CI and its relationships in various views. From the CI relations formatter, you can also launch the CI relationship editor for the CI.

If the domain separation plugin is activated, then only relationships in which the logged on user is authorized to view both CIs, are displayed.

The CI relations formatter contains a list of related CIs and a toolbar with controls for viewing the relationships between the current CI and related CIs. You can configure the controls in this
formatter to modify varying aspects of the view. For more information about formatters, see Create a formatter and add it to the form.

**Note:**
- If an endpoint is a child in one relationship and the same endpoint is a parent in another relationship, then that endpoint is hidden and does not appear in the relations formatter view. Similarly, relationship qualifier chains are also hidden and do not appear in the relationship formatter view.
  - Example: CI1 > endpoint > CI2
    In this example, CI1 is related to CI2 through relationships with endpoint. A single relationship appears in the relations formatter:
    CI1 > CI2 (These relationships appear as a direct relationship without endpoint, because endpoint is a parent in one relationship and a child in another relationship)
- Example: CI1 > endpoint1 > CI2 > endpoint2
  Two relationships appear in the relations formatter:
  CI1 > CI2 (endpoint1 is hidden because it is a parent in one relationship and a child in another relationship)
  CI1 > CI2 > endpoint2 (appears as level 2 relationship – endpoint1 is hidden and endpoint2 appears as a child and not a parent in any other relationship)
- On instances that do not meet the internet browser requirements for the CI relations formatter, the default CI form includes the legacy CI relations formatter instead. For more information, see Legacy CI relations formatter.
- CIs not extended from the Configuration Item [cmdb_ci] table, are not displayed in Dependency Views maps and in CI relation formatters.
- The **Applicative Flow To::Application Flow From** relationship is a special relationship type used only between Service Mapping endpoints. This relationship type is not intended for use in the CMDB as a relationship between CIs and therefore it is not displayed in the relations formatter.

### Controls for viewing related CIs

<table>
<thead>
<tr>
<th>Control</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Add CI relationship" /></td>
<td>Starts the relationship editor to manually create CI relationships. For more information, see Create or edit a CI relationship.</td>
</tr>
<tr>
<td>Show dependency views</td>
<td>Launches a Dependency Views map in another window or tab. The CI is the central node in the map, with a configurable number of levels above and below that node in the hierarchy. Map indicators next to the nodes indicate the number of tasks, incidents, problems, changes, or outages related to that node. Right-click to expand collapsed nodes or display a list of related tasks or problems. For more information, see Dependency Views map.</td>
</tr>
<tr>
<td>Search for CI</td>
<td>Filters the CIs included in the display.</td>
</tr>
</tbody>
</table>
Click the **Settings** (⚙️) icon to configure additional view settings that filter the data displayed. Settings are preserved through logging out and logging back in.

### Related items settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Show Relations in Flat/Tree Layout</strong></td>
<td>To view a flat list of related CIs that are grouped by relationship type in alphabetical order, click <strong>Flat</strong>.</td>
</tr>
<tr>
<td></td>
<td>To view groups of related CIs in a hierarchical tree, click <strong>Tree</strong>. If you select the tree view, you cannot configure any other settings for viewing related CIs. A single list of upstream and downstream relationships is displayed.</td>
</tr>
<tr>
<td><strong>Show Relations in Split/Merge Layout</strong></td>
<td>To view separate lists for upstream and downstream relationships, click <strong>Split</strong>.</td>
</tr>
<tr>
<td></td>
<td>To view a single list that includes both upstream and downstream relationships, click <strong>Merge</strong>. Relationships are grouped by relationship type.</td>
</tr>
<tr>
<td><strong>Filter Relations by Max Level</strong></td>
<td>Select the number of levels in the hierarchy to include when displaying CIs in a flat view.</td>
</tr>
<tr>
<td><strong>Filter Relations by Relationship Type</strong></td>
<td>Select the types of relationships to view.</td>
</tr>
<tr>
<td><strong>Filter Relations by CMDB View</strong></td>
<td>Filter by tables specified in CMDB views, if any relationship filters exist.</td>
</tr>
</tbody>
</table>

The relations formatter uses the following icons to provide additional information about changes, problems, and outages related to CIs in the relationship:

### Icons related to CIs

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checkmark</td>
<td>Recently closed changes</td>
</tr>
<tr>
<td></td>
<td>Planned changes</td>
</tr>
<tr>
<td></td>
<td>Currently open changes</td>
</tr>
<tr>
<td></td>
<td>Recently closed outages</td>
</tr>
<tr>
<td>Alarm symbol</td>
<td>Problems</td>
</tr>
<tr>
<td></td>
<td>Incidents</td>
</tr>
<tr>
<td></td>
<td>Planned outages</td>
</tr>
</tbody>
</table>
In large networks, a list of related CIs might be excessively long, which can slow performance when a CI form is rendered. You can configure these properties to control the amount of data that is displayed. To find a property, enter `sys_properties.list` in the left navigation filter and search for the property.

### Properties related to performance

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.ecmdb.find_relationship_issues</td>
<td>Hides or displays an icon in the CI relations formatter that links to open issues for the CI. This property defaults to true (displays the icon).</td>
</tr>
<tr>
<td>glide.ui.max_relation_levels</td>
<td>Specifies the maximum level for displaying CIs in flat view before reaching the maximum relations limit. The default value is 5.</td>
</tr>
<tr>
<td>glide.ui.max_relations</td>
<td>Specifies the maximum number of related CIs to display. When exceeded, a notification is displayed indicating that the limit has been reached, and that not all relations are displayed. The default value is 1000.</td>
</tr>
</tbody>
</table>

---

### Create or edit a relationship filter

Create a custom relationship filter to display CI relationships from selected tables in the CI relations formatter.

Role required: ecmdb_admin

The CI relations formatter displays related CIs for the base CI, and the relationships between the CIs. You can use relationship filters on the CI relations formatter to customize CI relationship views.

1. Navigate to **Configuration > Relationships > Relationship Filters**.
2. Click **New** or select a filter to edit.
3. Enter or edit the relationship filter name.
4. Right-click the form header and click **Save**.
5. In the **Configuration Types** section, click **Edit**.
6. On the **Edit Members** form, select the tables of the CIs that you want to show with the filter and then move the tables to the **Configuration Types list**.
7. Click **Save**.

On a CI form, in the relations formatter settings, you can select the newly defined relationship filter from the **Filter Relations by CMDB View** list.

In the legacy CI relations formatter, you can click **View** and select the newly defined relationship filter.

After you select a filter, the relations formatter displays only CIs from the tables specified in the filter or from descending tables.

---

### Exclude relationships from the relations formatter view

Create a list of relationships that should not appear in the relations formatter view on CI forms.
Role required: ecmdb_admin

1. Navigate to Configuration > Relationships > Relationship Type Exclusion List.
2. In the CI Relation Filters list view, click New.
3. Fill out the CI Relation Filter form to specify the relationship that you want to exclude from view.
4. Click Submit.
   Excluded relationships do not appear in Related Items on CI forms.

Legacy CI relations formatter

On instances that do not meet the internet browser requirements for the latest CI relations formatter, the default CI form includes the legacy CI relations formatter instead.

This element contains the list of related CIs and a toolbar with controls for viewing the relationships between the current CI and related CIs.

Related Items field

Note: The legacy BSM map provides a more complete view of CI relationships.

Configure the controls in this formatter with two properties that restrict varying aspects of the view.

Flat layout

Click the flat layout icon (≡) to group the related CIs by relationship.
Flat layout view

Tree layout
Click the tree layout icon ( ) to group the related CIs in a hierarchical tree.

Tree Layout View

CI relationship editor
Use the CI relationship editor to create CI relationships.
When you use the relationship editor, the CI from which the editor was launched is designated as the base CI. You can then select one or more CIs as a second CI for the relationship. Depending on the selected relationship type, the base CI can become the parent CI or the child CI in the new relationship.
The relationship editor operates differently, depending on whether you select the **Use suggested relationship** check box.

- With suggested relationships, the relationship editor lists all available relationship types for the base CI. To define a new relationship, select a relationship type, and then select a second CI for the relationship.

  Suggested relationships are highlighted for you. These relationships are displayed in blue with a prefix of (Suggested).

- Without suggested relationships, you define a new relationship by first selecting a second CI for the relationship and then selecting a parent or a child relationship type.

---

**Note:** The following relationship types are used only for Service Mapping endpoints, and you cannot use them as a relationship type between two CIs:

- **Implement End Point To:** Implement End Point From
- **Use End Point To:** Use End Point From
- **Applicative Flow To:** Applicative Flow From

---

**Suggested relationships**

If you select the **Use suggested relationship** check box in the editor, the **Suggested relationship** list appears. It displays all available CI, user and group relationship types for the base CI. Relationship types have a suffix of (Parent) or (Child) to note the relationship descriptor, and suggested relationship types are displayed in blue and have a '*' prefix.

When you select a relationship, you are also designating the base CI as being the parent or the child CI in the new relationship. For example, if you select the 'Feeds' relationship type, the base CI becomes the designated parent CI, and the second CI that you select becomes the child CI in this relationship.

**Downstream relationships**

If you do not select the **Use suggested relationship** check box in the editor, the **Downstream relationships** list appears. It displays all relationships in which the base CI is the parent CI. The child CI of the relationship is displayed in the Child column.

**Upstream relationships**

If you do not select the **Use suggested relationship** check box in the editor, the **Upstream relationships** list appears. It displays all relationships in which the base CI is the child CI. The parent CI in each relationship is displayed in the Parent column.

**Supported browsers for the relationship editor**

You must use supported browser versions in order to use the latest CI relationship editor. If you do not use a supported browser version, the instance provides the legacy CI relationship builder.

- Firefox version 20 and up
- Chrome version 25 and up
- Safari version 6 and up
- Internet Explorer version 9 and up
Create or edit a CI relationship

Use the relationship editor to view, create or modify CI relationships. You can open the relationship editor from the CI Relations formatter.

Role required: asset, itil, or admin

The relationship editor operates differently, depending on whether you check the Use suggested relationship option or not.

1. Launch the relationship editor:
   a) Open a CI form.
   b) Locate the Related Items section near the center of the form.
   c) Click the plus (+) icon on the Related items section.

2. To use suggested relationships, first select a relationship type, and then select one or more CIs to be the child CIs in the relationship:
a) Select **Use suggested relationship**.
b) From the **Suggested relationship type** list, select a relationship type. You can filter the list of suggested relationships by using the filter check boxes.

<table>
<thead>
<tr>
<th>Filter option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hide CI relationship</td>
<td>Hides any relationships between the base CI and another CI (such as &quot;Receives data from&quot;). Default filter is stored in the <code>ci_manage_relationships_filter_hint.cmdb_ci</code> user preference.</td>
</tr>
<tr>
<td>Hide user relationship</td>
<td>Hides any relationships between the base CI and a user (such as &quot;Logs reviewed by&quot;). The default filter is stored in the <code>ci_manage_relationships_filter_hint.sys_user</code> preference.</td>
</tr>
<tr>
<td>Hide group relationship</td>
<td>Hides any relationships between the base CI and a group (such as &quot;Backups done by&quot;). Default filter is stored in the <code>ci_manage_relationships_filter_hint.sys_user_group</code> user preference.</td>
</tr>
</tbody>
</table>

The **Configurations Items** list displays all the CIs that are appropriate for the base CI and the selected relationship type. The **Relationships** list at the bottom of the editor, displays all existing relationships of the selected relationship type, in which the base CI is a parent CI or a child CI.

c) From the **Configuration Items** list, select one or more CIs as a second CI for the relationship.

You can filter the list of **Configurations Items** by adding conditions in the **Filter** section and clicking **Run filter**.

If you selected a parent relationship type, these CIs becomes the child CI in the relationship, and if you selected a child relationship type, then the selected CIs become the parent CI in the relationship.

d) In the **Relationships** section, click the plus icon (+) to add the new relationships.

Alternatively, you can drag the selected CIs to the **Relationships** list. Each new relationship will consist of the base CI, the selected relationship type, and a selected second CI.

3. To not use suggested relationships, first select one or more CIs to be the child CIs in the relationship, and then select the relationship type:
a) Clear **Use suggested relationship**.

b) In the **Configuration Items** list, select one or more CIs as a second CI for the relationship. You can filter the list of **Configurations Items** by adding conditions in the **Filter** area and clicking **Run filter**.

Depending on the relationship type that you will select, the selected CIs might become a parent or a child CI in the relationship.

c) With at least one CI selected in the **Configuration Items** list, click the ‘+’ sign in the **Downstream Relationships** section or the **Upstream Relationships** section to create the relationship.
• Add the relationship to **Downstream Relationships** to create a relationship in which the base CI is the parent CI and the selected CI is the child CI.

• Add the relationship to **Upstream Relationships** to create a relationship in which the base CI is the child CI and the selected CI is the parent CI.

d) For each newly created relationship in either the **Downstream Relationships** or the **Upstream Relationships** lists, click *Please select a relationship* and select a relationship type.

• The list of available relationship types in the **Downstream Relationships** list contains parent relationships only, in which the base CI is the parent CI.

• The list of available relationship types in the **Upstream Relationships** list contains child relationships only, in which the base CI is the child CI.

e) Click **Save** or **Save and Exit**.

Only after you enter all the information that is necessary for creating the relationship, these buttons light up indicating that there are pending updates that require saving.

---

**Legacy CI relationship builder**

Used to define CI relationships manually, this page is a sophisticated version of the standard slushbucket. In the legacy CI relations formatter, click the CI relationship builder icon (⊕) to display the legacy Define Relationships page.

**Select a CI relationship type**

The top half of the legacy relationship editor contains a large option box that allows you to select which type of relationship you want to manipulate. Click the particular type of relationship you are interested in working with.

**Filter the list of CI relationships**

In the legacy relationship editor, the checkboxes along the right hand edge of the select box provide a quick way to filter down the list of available relationships.

By default, the system displays a list of all suggested relationships for the type of CI you selected. For example, if you selected a Database instance, a relationship of ’Runs on’ makes sense, but a relationship of ’Provides HVAC for’ does not. The default filter is stored in the user preferences cimanagerelationships_filter_hint.cmdb_cici_manage_relationships_filter_hint.sys_user, and cimanagerelationships_filter_hint.sys_user_group.

• **Hide CI relationship** -- Hides any relationships between this CI and another CI (e.g. ”Receives data from”).

• **Hide user relationships** -- Hides any relationships between this CI and a user (e.g. ”Logs reviewed by”).

• **Hide group relationships** -- Hides any relationships between this CI and a group (e.g. ”Backups done by”).

• **Show all relationships** -- If you have the appropriate role (out of the box this is itil_admin) you will have an additional checkbox labeled ”Show all relationships.” If you click that checkbox, the system will let you choose any relationship defined in the system, regardless of where it is on the ”suggested” list for this type of CI.
Select CI relationship targets

In the legacy relationship editor, users can link or unlink CIs for a relationship type.

As soon as you pick a relationship type, the system will fill in the two select boxes at the bottom of the screen with CIs that are appropriate for the relationship you suggested. The left hand select box will contain a list of CIs that might reasonably be linked via this relationship, while the right hand box contains a list of those CIs which are already linked.

1. Link or unlink items.

<table>
<thead>
<tr>
<th>Link new items</th>
<th>Move that CI from the left hand box to the right hand box.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unlink existing items</td>
<td>Move them from the right hand box to the left.</td>
</tr>
</tbody>
</table>

**Result:** When you make either type of change, a message appears indicating that you have pending changes.

2. Apply or cancel your changes.

<table>
<thead>
<tr>
<th>Click the Save button.</th>
<th>This will save your set of changes, and go back to the previous screen (either a CI or the BSM map depending on how you got here).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click the Cancel button.</td>
<td>This causes you to exit without saving your changes.</td>
</tr>
</tbody>
</table>

Relation qualifier

A relation qualifier, which is a CI of the Qualifier (cmdb_ci_qualifier) type, stores important information about the CI relationships.

In a relation qualifier, you can annotate arbitrary unique information about the relationship between two CIs. You can define multiple qualifiers for a single relationship, resulting in a qualifier chain. But, there can be only a single qualifier chain for a specific relationship type between two CIs.

For example, for a relationship between a parent CI and a child CI, you can add a relation qualifier to note that the relationship was discovered based on traffic (such as cmdb_ci_qualifier_trafficbased). This results in having two records in the CI Relationship (cmdb_rel_ci) table for the relationship.

- A record that links the parent CI and the new qualifier
- A record that links the new qualifier and the child CI

For this relationship, there is a parent CI and a child CI, and a relation qualifier of type cmdb_ci_qualifier_trafficbased.

For information about usage of relation qualifiers in the identification process, see CMDB identification rules.
**CI relationship security**

When applying security to CI relationships, it is important to apply the access controls both to the CI Relationship (cmdb_rel_ci) table and to create an operation editCIRelations to the * table as well.

If the current instance has defined security for editCIRelations, it will be applied to edit_ci_relations automatically in the process of upgrading, and the out-of-date security will be removed.

**Create a CI relation rollup**

A CI relation rollup allows you to sum, count, max, min, or mean a relationship type. You can create CI relation rollups.

Role required: ecmdb_admin

CI relation rollup can be useful for tracking and for receiving notifications. For example:

- In a sum roll up, add up fields from multiple CIs and display the result on another CI to which they are related. So, if you have four configuration items in a rack that are all consuming power, create a CI relation rollup to add all the power usage together and display the result in one field on the rack CI form.
- If a certain level of power consumption in a rack is exceeded, send a notification.
- With a rack that has 10 slots, send a notification when 9 slots are filled.

CI relation rollups use the `cmdb synch event` business rule on the (cmdb_ci) table. Although this business rule is active by default, you must modify the rule slightly before it will run.

1. Navigate to Configuration > Relationships > CI Relation Rollups.
2. Click New.
3. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CI Relationship Type</td>
<td>Select a relationship type from the list to use with the rollup. For example, Members::Member contains the parent descriptor Members and the child descriptor Member of.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the type of rollup from the drop-down list: COUNT, MAX, MEAN, MIN, or SUM.</td>
</tr>
<tr>
<td>Parent field</td>
<td>The target field on which the operation will be done.</td>
</tr>
<tr>
<td>Child field</td>
<td>The input to the equation type. The Parent field is affected by the selections in the child field.</td>
</tr>
<tr>
<td>Rollup class</td>
<td>The classes that can use the relationship. For example, you can specify that the relationship only applies to racks.</td>
</tr>
</tbody>
</table>

4. To run the `cmdb synch event` business rule, navigate to Business Rules.
5. Use the search box to find the (cmdb synch event) table.
6. Click the `cmdb synch event` business rule to go to the Business Rule page.
7. Select the Update, Delete, and Query check boxes.
Additionally, if you wish CI relation rollups to recalculate when there is a change to a relationship, use a similar procedure to select the **Active** check box on the `cmdb_rel_ci synch event` business rule.

**CMDB classifications**

CMDB classifications are groups of configuration items (CIs) that share attributes and are stored in their own table. Classifications allow administrators to define the hierarchy of CIs within the CMDB. A CI class refers to the actual table name in the instance database. In that context, CI Type is a friendly name that a CI is known by, such as computer, router, or printer.

As good practice, keep CI classifications as simple as possible.

**Configuration Management Database**

The Configuration Management Database (CMDB) is a series of tables that contain all the assets and business services controlled by a company and its configurations.

This information includes computers and devices on the network, software contracts and licenses, business services, and more. The IT desk can use the CMDB to better understand their network users' equipment, and the relationships between them. The CMDB can also be referenced by other processes within the system.

The CMDB can be populated using the Discovery product. Discovery searches the network for all attached computers and devices, then populates the CMDB with information on each computer/device's configuration, provisioning, and current status. Discovery also reports on any software which is running, and the TCP connections between computer systems, thereby establishing their relationships.

Applications such as Asset Management and Contract Management, operate in conjunction with the CMDB. Asset Management and Software Asset Management link to CMDB all assets, hardware, software, assets in stock, as well as records for manufacturers and vendors. The Contract Management application contains information about contracts, including leases, service contracts, purchase orders, warranties, and software licenses. The Configuration Management application has a focus on operation.

**CMDB tables**

Key tables in the configuration management database (CMDB):

- The Base Configuration Item (cmdb) table, which is the core CMDB table for non IT CIs (descending classes are non IT CIs).
- The core Configuration Item (cmdb_ci) table, which stores the basic attributes of all the CIs. The admin, itil, or asset user role is required to access this table (descending classes are IT CIs).
- The CI Relationship (cmdb_rel_ci) table, which defines all relationships between CIs.

The Configuration Item table is extended to other tables, such as Database (cmdb_ci_database) and Computer (cmdb_ci_computer). The Computer table is extended to the Server (cmdb_ci_server) table, which is extended to the UNIX Server (cmdb_ci_unix_server) table, and so on.

**Note:** The Base Configuration Item (cmdb) table uses the table per partition extension model, which has different inheritance and replication behaviors than other extended tables. See Table extension and classes.
You can use the schema map to view more details of tables and their relationships:

1. Navigate to **System Definition > Tables & Columns**.
2. Select a table and click **Schema Map**.

---

**Note:** CIs not extended from the Configuration Item (cmdb_ci) table, are not displayed in Dependency Views maps and in CI relation formaters.
CI attributes

Attributes apply to all the CIs in a classification. To change attributes for a CI, you must extend the table and create a new classification for that CI.

The position of a CI in a classification hierarchy is determined by the attributes it shares with the CIs below it. Each time a CI has a single different attribute from its parent, the classification hierarchy branches.

For example, servers have different attributes from computers, which include workstations and laptops. Linux servers and UNIX servers have different attributes from the parent server classification and from each other, so they occupy separate branches in the hierarchy.

CMDB table attributes descriptions

Descriptions of the attributes in the Base Configuration Item (cmdb) table, and in its first level extended table Configuration Item (cmdb_ci).

Attention: Do not modify any of these attributes in the dictionary. For example, do not modify the type of the location attribute from reference to list. Such modifications may prevent features that use the CMDB, from functioning properly.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset</td>
<td>Reference field to the Asset table</td>
</tr>
<tr>
<td>Asset Tag</td>
<td>Asset tag/service tag for the specific asset</td>
</tr>
<tr>
<td>Assigned</td>
<td>Date and time of assignment to user</td>
</tr>
<tr>
<td>Assigned To</td>
<td>Reference field to the User table</td>
</tr>
<tr>
<td>Assignment Group</td>
<td>Reference field to the Group table</td>
</tr>
<tr>
<td>Checked In</td>
<td>Date and time of checking in</td>
</tr>
<tr>
<td>Checked out</td>
<td>Date and time of checking out</td>
</tr>
<tr>
<td>Class</td>
<td>System class name</td>
</tr>
<tr>
<td>Company</td>
<td>Reference field to the Company table</td>
</tr>
<tr>
<td>Cost</td>
<td>Financial value in local currency (as defined in the Cost Currency field)</td>
</tr>
<tr>
<td>Cost Center</td>
<td>Reference field to the Cost Center table</td>
</tr>
<tr>
<td>Cost Currency</td>
<td>Name of currency (such as dollars, pounds, Euros)</td>
</tr>
<tr>
<td>Created</td>
<td>Date and time record was created</td>
</tr>
<tr>
<td>Created By</td>
<td>Name of person/data source which initially created the record</td>
</tr>
<tr>
<td>Department</td>
<td>Reference field to the Department table</td>
</tr>
<tr>
<td>Domain</td>
<td>ID of the domain to which the instance belongs</td>
</tr>
<tr>
<td>Domain Path</td>
<td>Path of the domain to which the instance belongs</td>
</tr>
<tr>
<td>Due</td>
<td>Date and time instance was due</td>
</tr>
<tr>
<td>Due In</td>
<td>Description of the manner of which the instance was due</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>GL Account</td>
<td>General Ledger account name/number</td>
</tr>
<tr>
<td>Installed</td>
<td>Date and time instance was most recently installed</td>
</tr>
<tr>
<td>Invoice Number</td>
<td>Invoice number used in acquisition process</td>
</tr>
<tr>
<td>Justification</td>
<td>Description of the justification for the instance</td>
</tr>
<tr>
<td>Lease Contract</td>
<td>Number of current leasing contracts</td>
</tr>
<tr>
<td>Location</td>
<td>Reference field to the Location table</td>
</tr>
<tr>
<td>Managed by</td>
<td>Reference field to the User table</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>Reference field to the Company table</td>
</tr>
<tr>
<td>Model ID</td>
<td>Reference field to the Product Model table</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the CI instance</td>
</tr>
<tr>
<td>Order Received</td>
<td>Date and time instance was initially received</td>
</tr>
<tr>
<td>Ordered</td>
<td>Date and time instance was initially ordered</td>
</tr>
<tr>
<td>Owned by</td>
<td>Reference field to the User table</td>
</tr>
<tr>
<td>PO Number</td>
<td>Purchase order number used in acquisition process</td>
</tr>
<tr>
<td>Purchased</td>
<td>Date instance was purchased</td>
</tr>
<tr>
<td>Requires verification</td>
<td>Flag indicating whether verification is required for the instance</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Serial number of the instance</td>
</tr>
<tr>
<td>Skip sync</td>
<td>Flag indicating whether synchronization between Asset Management and CMDB can be skipped</td>
</tr>
<tr>
<td>Status</td>
<td>Configurable choice list with values for current functional states</td>
</tr>
<tr>
<td>Support Group</td>
<td>Reference field to the Group table</td>
</tr>
<tr>
<td>Sys ID</td>
<td>ServiceNow Sys ID (GUID)</td>
</tr>
<tr>
<td>Tags</td>
<td>Related tags</td>
</tr>
<tr>
<td>Updated</td>
<td>Date and time instance was last updated</td>
</tr>
<tr>
<td>Updated By</td>
<td>Person/data source which last updated the record</td>
</tr>
<tr>
<td>Updates</td>
<td>Configurable choice list with values for update states</td>
</tr>
<tr>
<td>Vendor</td>
<td>Reference field to the Company table</td>
</tr>
<tr>
<td>Warranty Expiration</td>
<td>Date current warranty expires</td>
</tr>
</tbody>
</table>

**Configuration Item (cmdb_ci) table**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approval Group</td>
<td>Reference field to the Group table</td>
</tr>
<tr>
<td>Attributes</td>
<td>Description of usage of attributes for the instance</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Can Print</td>
<td>Indicates whether the instance can print</td>
</tr>
<tr>
<td>Category</td>
<td>Name of category applicable to the instance</td>
</tr>
<tr>
<td>Comments</td>
<td>Comments related to the instance</td>
</tr>
<tr>
<td>Correlation ID</td>
<td>ID of the instance from another data source</td>
</tr>
<tr>
<td>DNS Domain</td>
<td>Name of the DNS domain to which the instance belongs</td>
</tr>
<tr>
<td>Description</td>
<td>Fit (how deployed) and function (purpose) of the instance</td>
</tr>
<tr>
<td>Discovery source</td>
<td>Name of primary (most trusted) discovery source</td>
</tr>
<tr>
<td>Fault Count</td>
<td>Number of faulty recorded against the instance to date</td>
</tr>
<tr>
<td>First Discovered</td>
<td>Date and time instance was initially discovered</td>
</tr>
<tr>
<td>Fully Qualified Domain Name</td>
<td>Full path name of domain to which the instance belongs</td>
</tr>
<tr>
<td>IP Address</td>
<td>Primary IP address used by the instance</td>
</tr>
<tr>
<td>MAC Address</td>
<td>MAC address of the instance</td>
</tr>
<tr>
<td>Maintenance Schedule</td>
<td>Reference field to the Schedule table</td>
</tr>
<tr>
<td>Model Number</td>
<td>Manufacturer original model number</td>
</tr>
<tr>
<td>Monitor</td>
<td>Indicates whether the instance is monitored</td>
</tr>
<tr>
<td>Most Recent Discovery</td>
<td>Date and time instance was last discovered</td>
</tr>
<tr>
<td>Operational Status</td>
<td>Configurable choice list for current operational states</td>
</tr>
<tr>
<td>Schedule</td>
<td>Reference field to the Schedule table (for normal processing)</td>
</tr>
<tr>
<td>Start Date</td>
<td>Date and time the instance was last started</td>
</tr>
<tr>
<td>Subcategory</td>
<td>Name of Subcategory applicable to the instance</td>
</tr>
</tbody>
</table>

**CMDB record types**

The CMDB contains the following major record types.

**CMDB record types**

<table>
<thead>
<tr>
<th>Record types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Item (CI)</td>
<td>Any computer, device, or service in the CMDB. A CI’s record includes all of the relevant data, such as manufacturer, vendor, location, etc. Configuration items can be created or maintained either using tables, lists, and forms within the platform, or using the Discovery application.</td>
</tr>
<tr>
<td>Record types</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Relation Type</td>
<td>A defined relationship between a CI and either another CI, a user, or a group. Relation types are defined twice, once from the perspective of the child CI and once from the parent CI's perspective. For example, a parent CI that powers a child CI uses relation type <code>Powers::Is Powered By</code>. Example relation types include <code>In Rack::Rack contains</code>, <code>Log Reviewed by::Reviews logs</code> for, or <code>Backup done by::Does backups</code> for. CMDB relationships can be established using Discovery or using the tables, lists, and forms within the platform. The CMDB form has a specific Related Items toolbar optimized for modifying relationships.</td>
</tr>
</tbody>
</table>

**Related Lists of CI components**

Related Lists in CI records display additional components contained by that CI, such as disk drives on a server and the rules that control the behavior of a network router.

When Discovery runs, the Related List is populated with the components that Discovery finds running on the CI. The CI record might show different lists from scan to scan, depending on whether or not Discovery found the component.

By default, the Related Lists only display those components that are associated with that CI in the CMDB that have been discovered by the last scan. Components that are recorded in the CMDB but are not discovered in a scan, are deemed absent and do not appear in the list.

There are two types of components that appear in the Related List: those that are CIs themselves (such as hard disks), and those that are not (serial numbers and rules). The default filter condition in the breadcrumbs for components that are CIs is `(Status) (!=) (Absent)`. The filter condition for components that are not CIs is `(Absent) (=) (false)`.

In the following example, the `snc-tc01` router has several Related Lists affected by these filter conditions, including routing rules, disk drives, interfaces, and network adapters. Only those components found during the last Discovery appear in these Related Lists.
Create a CI class

Use the CI Definition form view to create a new CI class (table) that is an extension of an existing CI class.

Role required: itil_admin (on top of itil) or admin. Or personalize_dictionary if using the CI Class Manager.

The CI Definition view serves as a centralized location from which you can create a new table that is derived from the CMDB table, and configure additional CMDB-related configurations for the CI.

Alternatively, you can extend a class by following a prescribed step-by-step in-product guidance:

1. Navigate to Guided Setup > ITOM Guided Setup and click Continue.
2. Scroll to Configuration (CMDB), and click Continue.
3. Scroll to Class Extension and click Configure.

1. Use the CI Class Manager:
   a) Navigate to Configuration > CI Class Manager.
   b) In the Class Hierarchy, click the context menu for the class that the new class will be extended from. Click Extend.

   On the Table form, Extends table is populated with the class that was extended.
2. Fill out the Table form. The table that you specify in Extends table can for example, be an extension of the CMDB table.
   See Create a table for details about the Table form.
3. Click Submit, and wait for the new class to be added to the Class Hierarchy.
4. Scroll to the bottom of the Table view to use any of the CI Definition form view specific controls, such as CI Identifiers, Reconciliation Definition, or Icon.

**Reclassify a CI**

You can upgrade, downgrade, or switch the class of a CI by modifying its Class attribute.

Role required: itil or asset (In general, the roles required to update a CI)

Each class is defined with a unique set of attributes. This set consists of attributes that were derived from the parent class, and additional attributes defined for the class.

When you reclassify a class, the following occurs.

1. The set of attributes is adjusted to match the set of attributes of the newly assigned class. Attributes are added or removed as needed.
2. If any attributes are unique to the current class and are not defined in the newly reclassified class, they are lost.
3. A new record with the CI's sys_id is inserted to the table of the new class, with the appropriate set of attributes for the class.

Depending on the reclassification, the following occurs.

**Downgrade**

The CI class is updated to a class that is lower in class hierarchy, and the newly assigned class is a parent of the current class. For example, reclassifying a CI from the cmdb_ci_server class to the cmdb_ci_computer class.

For example, the cmdb_ci_server class has attributes that the cmdb_ci_computer class does not have. During the downgrade, these attributes and their respective values are not included in the new CI record that is inserted into the cmdb_ci_computer class.

**Upgrade**

The CI class is updated to a class that is higher in class hierarchy, and the newly assigned class is a derived child of the current class and has additional attributes. For example, reclassifying a CI from the cmdb_ci_computer class to the cmdb_ci_server.

**Switch**

The newly assigned class is in a different branch in the class hierarchy and has a different set of attributes than the current class. For example, reclassifying a CI from the cmdb_ci_linux_server class to the cmdb_ci_win_server class.

A switch is a combination of a downgrade and an upgrade. For example if the CI is downgraded to the cmdb_ci_server, and then upgraded to the cmdb_ci_win_server class. Therefore, attributes are lost in the same manner as in a downgrade operation.

**Note:** Avoid the CI class downgrade and CI class switch operations as those can lead to data loss. When automatic CI reclassification is enabled (which is by default), the identification process can result in some automatic reclassifications which lead to data loss.

For more information about system properties that control system-wide behavior of automatic CI reclassification, see CI reclassification.

1. Locate the CI that you want to reclassify and display it in a list view.
You can use the application navigator. Or for example, if the CI is a server, then in the navigation search box, type `cmdb_ci_server.list` to display the CI in the Servers view.

2. Ensure that the Class field is displayed in the list.
   If you do not see this attribute, personalize the list to add the Class field.

3. Double-click the Class value for the CI, and select a new class.

4. Click the green check box to confirm your selection.

View table definitions

Use the CI Class Manager as a central location to explore tables and CI definitions, and to search through the CI class hierarchy. View the details of each table such as the table's label and field definitions, and all related definitions and scorecards.

For each table, you can directly access additional CMDB health metrics and scorecards such as datasource precedence rules, orphan scorecard and certificate template defined for the table class.

1. Navigate to Configuration > CI Class Manager.
2. Select a class from the Class Hierarchy list to display its table columns and other details.
   See control descriptions in Create a table.
3. Check Advanced at the top of the right sidebar and ensure that Fields is selected.

Querying the CMDB

The CMDB Query Builder allows you to easily build complex infrastructure and service queries that span multiple CMDB classes, and that involve many CIs that are connected by different relationships.

The CMDB Query Builder provides a canvas into which you drag the CI classes and other artifacts that you want to include in a query. Then you add relationships, AND/OR operators between the CI classes, and define the relationship properties to query for. You can use saved queries to populate a CMDB group with CIs, and then use scriptable APIs to retrieve the CI list and apply actions collectively to all the CIs in the group.

There are two query types: CMDB Query and a Service Mapping query, which you can use separately or in combination to create queries such as:

- All CIs of a certain type in a business service. For example, all Apaches/Web Servers/Linux servers per service.
- All virtual servers and the physical servers that host them.
- All servers that are not mapped to any business service.
- All Servers with a database.
- All database servers that are included in any business service or in a particular business service.
- All business services and their associated servers and the cost of each server. This query helps evaluate the cost of technology for each business service.

The Query Builder uses the concept of start node which is the starting point of the query and is noted by gray background in its query node. The first class that you drag to the canvas becomes automatically the start node of the query and you cannot select a different start node. In a complex query, the start node must always be the only node connected to an AND/OR operator. If you try to connect a second node to an operator that the start node is connected to, the query fails to run and you will be prompted to select a different start node.
CMDB Query

A query type that queries the infrastructure for CI classes, and the relationships and references that connect them.

Service Mapping Query

A query type that queries business services and technical services, and thus requires that Service Mapping is activated. The query is framed within a business service map. You define a pattern, and query for business service maps that have that pattern in their definition. The relationships in Service Mapping queries are matched by single-level direct relationships which is similar to the CMDB queries, and in addition, they are also matched by multi-level indirect relationships if they exist. A query for a relationship between two CI classes is satisfied even if the two CI classes are connected by intermediate CI classes that are not specified in the query.

Combination Query

You can combine the two query types by incorporating a saved Service Mapping query into a CMDB query. For example, create a CMDB query for Windows Servers that are connected to Tomcat WAR. Then connect the Tomcat WAR CI class to a Service Mapping query. This changes the query to find Windows Servers that are connected to Tomcat WAR which is included in the services that returned by the Service Mapping query. You can inverse that query by choosing - Does Not Belong To Service. This changes the query to find Windows Servers that are connected to Tomcat WAR that is not included in services returned by the Service Mapping query.

Relationship properties

When you connect CI classes on the canvas, the CMDB Query Builder displays the Connection Properties dialog box where you can choose from a list of relationships that exist between these two CI classes including relationships to descendent classes. For Service Mapping queries, only related and not-related connections are displayed.

The relationship arrow on the canvas shows the direction of the query, but the connection properties for the relationship determine what the relationship is queried for.

Connection properties include:

- Parent/child direction: Which CI class is the parent and which CI class is the child in the relationship.
- No relations: Query for a CI class which has no relation to the class it is connected to.
- References fields: A field that the parent and ancestor parent CI classes use to reference the child CI class.

Newly added relationships between CI classes may take up to 30 minutes to appear in the relationship list.

Build a CMDB query using the CMDB Query Builder

Build a CMDB query in the CMDB Query Builder.

Role required: cmdb_query_builder (contained for itil and asset)

Build the query by dragging the CI classes that you want to include in the query, dropping them as nodes on the canvas, and then defining relationship properties between them. For every class
node in the query, you can filter on its attributes to narrow down the results to a specific set of CIs of that class or to a single specific CI, and you can select the property columns that display in the query results. Query filters use related list conditions which allow the inclusion of a relationship with another table in the filter. For more information, see Add related list conditions.

Authorized users can update and delete a query created by another user.

1. Navigate to Configuration and click CMDB Query Builder.
2. On the CMDB Query Builder page do either of the following:
   a) Click Create new. Type in a Name, choose CMDB Query as the Query type, and click Create.
   b) Click on a widget of a saved query to continue building an existing query. Search saved queries first if needed.
   c) Point to the upper right corner of a saved query widget, and click the Duplicate Query icon to edit a copy of a saved query. The new query's default name contains the string 'copy'.
3. Do any of the followings on the canvas:
   - Add CI classes to the query: Select classes from the class hierarchy under CMDB Artifacts and drag them to the canvas.
   - Add connections between two nodes on the canvas:
     1. On the first node in the relationship, click the small square at the center of the right side to toggle its color to blue.
     2. On the second node in the relationship, click the small square at the center of the left side to toggle its color to blue.
   - In the Connection Properties dialog box:
     - Choose the parent/child roles in the relationship and then configure the properties in the respective section of the connection properties.
     - Click Add Relations and select a relationship from the list of existing relationships between the CIs (including descendant classes).
     - Select No Relations to query for classes that do not have any relationships with each other. For example, query for all Tomcat WAR CIs which are not connected to a Windows Server.
   - Click Add Reference to choose a field that the parent class (including ascendant parent classes) uses to reference the child.
4. Click Confirm.

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full line</td>
<td>A relationship in a CMDB query.</td>
</tr>
<tr>
<td>Dotted line</td>
<td>A relationship in a Service Mapping query.</td>
</tr>
<tr>
<td>Red asterisk at the center of the connection line</td>
<td>Information such as relationship type is missing, invalidating the query.</td>
</tr>
</tbody>
</table>

- Add filters to the query:
The initial elements of a query are classes. Applying filters, you can narrow a class down to a specific set of CIs or to a single specific CI.

1. Point to the node to add a filter to.
2. Click the **Apply Filters** icon that pops up above the node.
3. Add attribute and related list conditions.
4. Close the **Filters** section on the canvas.

For example add a filter for database location to query for databases located in Seattle.

Click **Applied Filters** in the navigation bar on the right to view all filters that were added for each node on the canvas. When you select a set of filters in the navigation bar, the respective node that these filters apply to, is highlighted. And, if you select a node, the respective set of filters that apply to that node, is highlighted.

- Add AND/OR operations to the query:
  1. Connect one node to two other nodes.
  2. Click the **AND** box that appears to toggle between the And and the Or operations.

For example C1 is Tomcat WAR, C2 is Linux Server, and C3 is Windows Server. Query for all Tomcat WAR CIs which are connected either to Linux Server Or to a Windows Server.

- Add property columns to display in the query results:

  | **Note:** For a relationship, the query results display the parent, child, and type columns. You cannot add any other columns from the `cmdb_rel_ci` table. |
  |---|---|---|
  | 1. Click the node to add properties to. |
  | 2. Click the **Properties** tab, and then click **Add Columns**. |
  | 3. Select the properties to display and then click outside the properties list to close it. |

- Select columns and add filters that will be applied to the resulting set of services:
  1. Ensure that **Properties** is selected at the top on the right hand-side navigation bar, and then click an empty space on the canvas to ensure that nothing is selected.
  2. Click **Add Columns** at the bottom of the right hand-side navigation bar and select columns to add.

- Create a combination query by integrating a Service Mapping query into a CMDB query:
  1. Click **Saved Service Queries**.
  2. Select a Service Mapping query and drag it to the canvas.

This query returns all CIs that satisfy the CMDB query, and that are included in the services returned by the Service Mapping query.

- Add a search tag that can then be used as a search criteria for saved queries:
  1. Click the **Add Tags** icon.
  2. Click **Add Tag**, and enter the tag string.
  3. Click the **Add Tags** icon again to close the **Query Tags** dialog box.
4. Modify the query:
   - Apply filters: Click a node and then click the **Apply filters** icon to add or edit the node's filters.
   - Modify relationship properties: Click the line that represents the relationship between two nodes to display the **Connection Properties** on the right hand side pane.
   - Modify Query Builder settings: Click the (Settings) icon to open the **Query Builder Settings** dialog box.

   - Click **Save**.

   In the **Saved Queries** tab, you can hover over a saved query widget and click the 'i' icon to view query information such as the query type, last update date, CMDB groups associated with the query, and the query schedules.

   - Click **Run**.

   **Note:** When a query is running, wait for it to complete or to timeout before opening or running another query.

The query results pane displays only the first 100 results of the query. Click **Load More Results** to display the next set of 100 results. Also, in the query results pane you can click a CI to open its CI form, and on the CI form you can click **Dashboard** to view CI health in the CI dashboard.

   - **Create a schedule** to run the query at a future time, and to email the results to interested parties.
   - **Click the Export icon in the query results pane.** Even if the **Load More Results** button is visible, indicating that there are additional query results, only the results that are visible are exported.

   The exported file contains the query results with the addition of the CIs and relationship sys_ids.

   - **Populate a CMDB group** using the saved query.

### Build a Service Mapping query using the CMDB Query Builder

Build a Service Mapping query in the CMDB Query Builder. A Service Mapping query is a pattern consisting of classes and relationships between those classes. After you build the pattern and run the query, the query returns all the Service Mapping services that contain that pattern.

Service Mapping must be activated.

Role required: cmdb_query_builder (contained for itil and asset)

Build the query by dragging the CI classes that you want to include in the query, dropping them as nodes on the canvas, and then defining relationship properties between them. For every class node in the query, you can filter on its attributes to narrow down the results to a specific set of CIs of that class or to a single specific CI, and you can select the property columns that display in the query results. Query filters use related list conditions which allow the inclusion of a relationship with another table in the filter. For more information, see **Add related list conditions**.

Authorized users have the ability to update and delete a query that was created by another user.

1. Navigate to **Configuration** and click **CMDB Query Builder**.
2. On the **CMDB Query Builder** page do either of the following:
   a) Click **Create new**. Type in a **Name**, choose **Service Mapping Query** as the **Query type**, and click **Create**.
b) Click on a widget of a saved query to continue building an existing query. Search saved queries first if needed.

c) Point to the upper right corner of a saved query widget, and click the Duplicate Query icon to edit a copy of a saved query. The new query’s default name contains the string ‘copy’.

3. Do any of the followings on the canvas:
   - Add CI classes to the query: Select classes from the class hierarchy under CMDB Artifacts and drag them to the canvas.
   - Add connections between two nodes on the canvas:
     1. On the first node in the relationship, click the small square at the center of the right side to toggle its color to blue.
     2. On the second node in the relationship, click the small square at the center of the left side to toggle its color to blue.
   - In the Connection Properties dialog box:
     • Choose the parent/child roles in the relationship and then configure the properties in the respective section of the connection properties.
     • Click Add Relations and select a relationship from the list of existing relationships between the CIs (including descendant classes).
     • Select No Relations to query for a pattern in which the two classes have no relationships with each other. For example, all Tomcat WAR CIs which are not connected to a Windows Server.
     • Click Add Reference to choose a field that the parent class (including ascendant parent classes) uses to reference the child.

4. Click Confirm.

**Relationship UI Notations**

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dotted line</td>
<td>A relationship in a Service Mapping query.</td>
</tr>
<tr>
<td>Red asterisk at the center of the connection line</td>
<td>Information such as relationship type is missing, invalidating the query.</td>
</tr>
</tbody>
</table>

- Add filters to the query:

  The initial elements of a query are classes. Applying filters, you can narrow a class down to a specific set of CIs or to a single specific CI.
   1. Point to the node to add a filter to.
   2. Click the Apply Filters icon that pops up above the node.
   3. Add attribute and related list conditions.
   4. Close the Filters section on the canvas.

For example add a filter for business criticality to query for businesses that are ‘most critical’.

Click Applied Filters in the navigation bar on the right to view all filters that were added for each node on the canvas. When you select a set of filters in the navigation bar, the
respective node that these filters apply to, is highlighted. And, if you select a node, the respective set of filters that apply to that node, is highlighted.

- Add AND/OR operations to the query:
  1. Connect one node to two other nodes.
  2. Click the AND box that appears to toggle between the And and the Or operations.

For example C1 is Tomcat WAR, C2 is Linux Server, and C3 is Windows Server. Query for all Tomcat WAR CIs which are connected either to Linux Server Or to a Windows Server.

- Add property columns to display in the query results:

  Note: For a relationship, the query results display the parent, child, and type columns. You cannot add any other columns from the (cmdb_rel_ci) table.

  1. Click the node to add properties to.
  2. Click the Properties tab, and then click Add Columns.
  3. Select the properties to display and then click outside the properties list to close it.

- Select columns and add filters that will be applied to the resulting set of services:

  1. Ensure that Properties is selected at the top on the right hand-side navigation bar, and then click an empty space on the canvas to ensure that nothing is selected.
  2. Click Add Columns at the bottom of the right hand-side navigation bar and select columns to add.
  3. Click the Apply Service Mapping Query Filters icon at the top of the canvas and add filters.

- Disable Services Including This Pattern to inverse the entire query and search for all Service Mapping services that do not include the query pattern.

- Add a search tag that can then be used as a search criteria for saved queries:

  1. Click the Add Tags icon.
  2. Click Add Tag, and enter the tag string.
  3. Click the Add Tags icon again to close the Query Tags dialog box.

4. Modify the query:

- Apply filters: Click a node and then click the Apply filters icon to add or edit the node’s filters.
- Modify relationship properties: Click the line that represents the relationship between two nodes to display the Connection Properties on the right hand side pane.
- Modify Query Builder settings: Click the (Settings) icon to open the Query Builder Settings dialog box.

- Click Save. A saved Service Mapping query can be built into a CMDB query.

  In the Saved Queries tab, you can hover over a saved query widget and click the ’i’ icon to view query information such as the query type, last update date, CMDB groups associated with the query, and the query schedules.

- Click Run.
Note: When a query is running, wait for it to complete or to timeout before opening or running another query.

The query results pane displays only the first 100 results of the query. Click Load More Results to display the next set of 100 results. Also, in the query results pane you can click a CI to open its CI form, and on the CI form you can click Dashboard to view CI health in the CI dashboard.

- Create a schedule to run the query at a future time, and to email the results to interested parties.
- Click the Export icon in the query results pane. Even if the Load More Results button is visible, indicating that there are additional query results, only the results that are visible are exported.

The exported file contains the query results with the addition of the CIs and relationship sys_ids.

- Populate a CMDB group using the saved query.

Sample CMDB queries
Use the following sample queries to build your own CMDB queries.

CMDB query sample
Use this example to build a CMDB query.

All servers with a connection to a database
1. Navigate to Configuration and click CMDB Query Builder
2. Click Create new. Enter a Name - All servers with a connection to a DB. Choose CMDB Query, and click Create.
3. In the CMDB Artifacts list, locate the Server class, and drag it to the canvas.
4. Locate the Database class, and place it to the right of the Server class node on the canvas.
5. Click at the center of the right side of Server, and then at the center of the left side of Database to create a connection.
6. In the Connection Properties dialog, in the Add Relations for Server 1 section - one by one, select all the listed relationships.
   Note that the added relationships are displayed in the navigation bar on the right, underneath Server 1.
7. Click Save, and then click Saved Queries on the left to see the tile for the saved query.
8. Click the query tile to return to the canvas in edit mode.
9. Click Run to execute the query.
   Review the query results. Each row displays the name of a server CI, the name of a database CI, and the relationship type between them.
10. Add columns to the query results:
    a. Click Server 1 on the canvas.
    b. On the right navigation bar, underneath Server 1 Report Columns, click Add Columns.
    c. Select Manufacturer.
    d. Click Run.
Review the query results which now include the **Manufacturer** column.

e. Click **Save** again to save all your customization for this query.

---

**Service Mapping query sample**

Use this example to build a Service Mapping query.

**Linux server in services**

Note: To build and run a Service Mapping query, Service Mapping must be activated.

1. Navigate to **Configuration** and click **CMDB Query Builder**
2. Click **Create new**. Enter a Name - *Linux server in services*. Choose **Service Mapping Query**, and click **Create**.
3. In the **CMDB Artifacts**, locate **Linux Server**, and drag it to the canvas.
4. Click **Run**.

Review the query results. Each row displays the name of a Service Mapping Service and the name of a Linux Server that is a member of that service.

5. On the right navigation bar, click **Disable Service Including This Pattern**, and then click **Run** again.

Review the query results. Now, each row displays the name a Service Mapping Service that does not include the specified Linux Server.

---

**Run a partial CMDB query**

You can run a partial query in the CMDB Query Builder by defining a section of a query, and then running it.

Role required: cmdb_query_builder (contained for itil and asset)

While building a query or reviewing a saved query, you can run only a section of the query. On the canvas in the CMDB Query Builder, highlight a section of the query which contains the nodes and relationships of the partial query that you want to run. You can then examine the results of the partial query, and update the query if needed.

1. Navigate to **Configuration** and click **CMDB Query Builder**.
2. On the CMDB Query Builder page, click a tile to open an existing query.
3. Click the selection tool under the navigation tool to switch to a section selection mode.
4. Border a section of the query:
   a) Click the mouse device on the upper left corner of the section that you want to create.
   b) Drag the mouse device to the bottom right corner of the section that you want to create. As you drag the mouse device, the selected section is highlight in light blue.
   c) Release the mouse device. The query nodes that are included in the partial query, appear with a blue border.

5. Click **Run**.
6. In the Pick Starting Node dialog box, select the starting node for the partial query, and click Confirm.

The results of the partial query appear in the Results pane.

### Settings in CMDB Query Builder

Use settings to control some aspects of the CMDB Query Builder behavior.

Open the Query Builder Settings dialog box:

1. Navigate to Configuration and click CMDB Query Builder.

2. On the CMDB Query Builder page, click the (Settings) icon.

3. Click the Settings icon again to close the dialog box.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Relationships in Results</td>
<td>Enable to display the relationship between CIs in the query results.</td>
</tr>
<tr>
<td>Display Suggested Connections</td>
<td>Enable to filter the class hierarchy in the left pane to display only classes that the selected class on the canvas has a relationship with. You can then drag any class from the filtered list to the canvas, and connect it to the selected class on the canvas. This setting applies only to CMDB queries.</td>
</tr>
</tbody>
</table>

### Navigation in CMDB Query Builder

Use the navigation tools to enlarge or shrink the query, to move the query, or to border a section of the query to run.

Use the buttons in the navigation tool as follows:

- Use the plus sign (+) to increase magnification of the query.
- Use the minus sign (-) to decrease magnification of the query.
- Click the center dot to center the query on the canvas.
- Use the direction arrows to move the query in that direction.
- Use the selection tool under the navigation tool to toggle between two states:
  - Moving the entire query on the canvas.
  - Bordering a section of the query, which you can then run as a partial query.
Search saved queries

The CMDB Query Builder allows you to search for a specific saved query using any combination of search criteria based on the query’s title, type, custom tags, and who created or updated the query.

To locate a saved query using a **Query Tags** search criteria, the query must have a query tag associated with it. For more information see [*Build a CMDB query using the CMDB Query Builder*](#), or [*Build a Service Mapping query using the CMDB Query Builder*](#).

Role required: cmdb_query_builder (contained for itil and asset)

1. Navigate to **Configuration > CMDB Query Builder**.
2. In the **Search Saved Queries** box on the **Saved Queries** tab, enter a string to search for.
   - The resulting list displays all search categories that can be applied using the search string.
3. Select an item from the list to add it as a search criteria.
4. Refine the search string or select additional search criteria as needed.

Create a schedule for a CMDB query

Schedule a CMDB query to run once at a scheduled time or on a recurring schedule, and to email the query results to specified users.

Role required: cmdb_query_builder (contained for itil and asset)

A saved CMDB query that was built in the CMDB Query Builder.

The query results are attached to the email as a `.csv` file identical to the file generated when exporting the query results. By default, the maximum result rows that can be attached is 10,000. This is controlled by a system property.

1. If need to, navigate to **Configuration**, click **CMDB Query Builder**, and then click a saved query.
2. Click **Create Schedule** and fill out the form.

  **Scheduled Email of Query Builder form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query</td>
<td>The query to run.</td>
</tr>
<tr>
<td>Users</td>
<td>Users who should receive query results email.</td>
</tr>
<tr>
<td></td>
<td>To receive emails, users must have an Email address defined and have Notifications set to Enable in their user records.</td>
</tr>
<tr>
<td>Groups</td>
<td>Groups to email the query results to.</td>
</tr>
<tr>
<td>Zip output</td>
<td>Indicates whether the report should be sent as a zip file.</td>
</tr>
<tr>
<td>Active</td>
<td>Indicates whether to run the query according to the specified schedule.</td>
</tr>
<tr>
<td>Run</td>
<td>Frequency for running the query.</td>
</tr>
<tr>
<td>Time</td>
<td>Time of day to run the query.</td>
</tr>
<tr>
<td>Conditional</td>
<td>Indicates whether to display the Condition field, which allows you to specify conditions under which the query runs.</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>
<tbody>
<tr>
<td>Omit if not records</td>
<td>Indicate whether to distribute email if the query returns zero results.</td>
</tr>
<tr>
<td>Email addresses</td>
<td>Email addresses of users who should receive the email but who are not in the system.</td>
</tr>
<tr>
<td>Subject</td>
<td>Text that appears in the subject line of the distribution email.</td>
</tr>
<tr>
<td>Introductory message</td>
<td>Additional message that is delivered with the query results.</td>
</tr>
<tr>
<td>Condition</td>
<td>User-created script that checks for certain conditions to be true before running the query. This field is visible only when Conditional is checked.</td>
</tr>
</tbody>
</table>

### System properties associated with the CMDB Query Builder

CMDB Query Builder uses the following system properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| glide.cmdb.query.max_results_limit           | Limits the number of results of a scheduled query and in the results section in the Query Builder when you click Load All Results.  
• Type: integer  
• Default value: 10000  
• Location: System Property (sys_properties) table. |
| glide.cmdb.query.batch_time_limit_in_sec     | Time limit (in seconds) for running one batch to get one batch of query results (100 results).  
• Type: integer  
• Default value: 300  
• Location: System Property (sys_properties) table. |
| glide.cmdb.query.query_time_limit_in_sec     | Time limit (in seconds) for running an entire query to get all results.  
• Type: integer  
• Default value: 1800  
• Location: System Property (sys_properties) table. |

### CMDB CI Lifecycle Management

From the time of its creation to the time that it is no longer needed, a CMDB CI would typically transition through several operational states while undergoing various operations. CI Lifecycle Management provides the mechanism to define states and actions for a CI and lets you apply
appropriate actions based on a CI’s state to tailor the management of CI lifecycle to business needs.

Terms associated with CI Lifecycle Management:

**Operational states**
A set of states that a CI can be at such as 'Operational' or 'Repair in Progress'. A CI can be associated with only a single operational state at any given time. The choices for operational states are based on the `operational_status` field in the `cmdb_ci` table. There are several operational states that are defined in the base system such as 'Retired' and 'Repair in Progress'. You can modify this list to reflect operational states that are relevant in your business.

**Note:** By default, Service Mapping is configured to ignore all host CIs for which the value of Operational status (`operational_status`) is not 1 (Operational) or the value of status (`install_status`) is 100 (absent). For additional information about this behavior, see Preparing customized ServiceNow deployments to work with Service Mapping (KB0647574) in the HI Knowledge Base.

CI Lifecycle Management allows multiple operators and automations to simultaneously set different operational states of a CI. Since a CI cannot be associated with multiple operational states, it is important to configure each operational state with a priority. These priorities are then used in such situation to determine which of the operational states is the cumulative operational state.

**CI actions**
A set of actions that can be applied to a CI during its lifetime. You can define CI actions that are relevant in your business.

**Compatible CI Actions**
CI Lifecycle Management allows a CI to have multiple active CI actions simultaneously, however they must be specifically defined as compatible. By default, there are no two actions for a CI that are compatible with each other. You can change this behavior by specifying pairs of actions that are compatible and thus allowed to be applied simultaneously to a CI. For example, you can specify that the 'Patching' and the 'Provisioning' CI actions are compatible making it possible to apply both simultaneously to a CI.

**Not Allowed CI Actions**
By default, any CI action can be applied to any CI. You can restrict this behavior by defining a rule that an action is not allowed for a CI when it is in a specific operational state. For example, you can define a Not Allowed CI Action in which it is not allowed to apply the 'Provisioning' action to a Linux Server that is in a 'Non-Operational' state.

**Not Allowed Operational Transitions**
By default, transitions are allowed from any operational state to another. You can restrict this behavior by defining a rule that for a specified CI, a transition from a certain operational state to another operational state is not allowed. For example, you can define that for a Linux Server it is not allowed to transition from 'Repair in progress' to 'Non-Operational'.

**Requestor**
A requestor can be a workflow or a non-workflow operator that is trying to set operational states and apply CI actions. Each requestor has an associated requestor ID that is a GUID and that can be an active workflow context or a non-workflow registered operator ID.

**Lease time**
A time period that each requestor (especially non-workflow operators) can provide, during which a specified CI action is allowed to be active for a specified CI.
CMDB CI Lifecycle Management provides a set of APIs to manage CI operational states and CI actions. And the UI where you define a set of rules to restrict certain operational state transitions and to restrict actions based on operational states. It also provides a mechanism to audit CI operational state and CI actions during the entire CI lifecycle.

Providers such as automation, workflows, or Change Management can use CI Lifecycle Management as a mechanism to manage CI operational states and apply CI actions. By default, the behavior of CI Lifecycle Management has no restrictions on some operations, and full restrictions on other operations. The CI Lifecycle Management UI lets you modify this default behavior by specifying Not Allowed CI Actions, Compatible CI Actions, and Not Allowed Operational Transitions that restricts some operations and enables for others.

With CI Lifecycle Management you can:
- Manage CI operational states and CI actions throughout the entire CI lifecycle.
- Manage CI operational state transitions.
- Restrict certain operational state transitions.
- Associate certain actions for certain CI types that are in specific operational state.
- Restrict IT Service Management applications based on CI operational state.
- Audit CI operational states and CI actions during the entire CI lifecycle.

Lifecyle management APIs

CI Lifecycle Management provides a set of APIs to manage CI operational state and CI actions during the entire CI lifecycle. All restrictions and allowances specified by rules in the UI are enforced when state management APIs run, and if an API attempts to perform a restricted operation, the operation is blocked and an error is logged.

Registering requestors

When using the lifecycle management APIs to apply CI actions, requestors are required to be registered and to obtain a requestor ID which is unique within the lifecycle management tables. To register and to obtain a requestor ID, non-workflow users should call the registerOperator API. Workflow users can use the active Workflow context as the requestor ID, and they do not need to explicitly call registerOperator.

After completing the CI lifecycle operations, the requestor should call the unregisterOperator API to unregister. All the state management records associated with that specific requestor ID are then marked as inactive or they are removed by the CI Lifecycle Management - Restore Internal State Management Tables scheduled job.

Integration with Incident Management and Problem Management

A base instance includes the pre-defined CI action CreateTask used for creating a task for a CI. New instances have a pre-defined Not Allowed CI Action, specifying that the CreateTask action is not allowed for any CI with a Retired operational state. This restriction is integrated with Incident Management and with Problem Management to prevent the creation of incident or problem tasks for retired CIs. The CreateTask CI action is used as a reference qualifier to the Configuration Item field of the Incident/Problem tables. In a new incident or problem, CIs in which Operational Status is Retired – are filtered out from the Configuration Item list on the form. For more information about reference qualifiers, see Reference qualifiers.
Integration with Asset Management

In a base system, a CI's Operational Status field and the Status/Hardware Status (if its hardware) fields are kept synchronized if one of the two fields' values is Retired. When Operational Status of a CI is set to Retired, then the Status/Hardware Status field is automatically set to Retired. In the opposite direction, when the Status/Hardware Status field of a CI is set to Retired, Operational Status is then automatically set to Retired too. When an Operational Status field changes from Retired to another status, the CI’s Status/Hardware Status field is set to Installed. And when a CI’s Status/Hardware Status field changes from Retired to another status, the Operational Status field is automatically set to Non-Operational.

Whenever CI’s Status/Hardware Status changes, it is synchronized to the CI’s corresponding Asset State field, and vice versa - keeping the CI’s Operational Status and the CI’s corresponding Asset State synchronized.

For more information about mapping Asset State and Substate fields to a CI’s Status/Hardware Status (if its hardware) field, see Map asset state and CI hardware status. And for more information about retiring assets, see Retire assets.

Get started with CI Lifecycle Management

Follow these high level steps to get started and to track activities of the CI Lifecycle Management module of the CMDB application.

1. Activate the base system CI Lifecycle Management - Restore Internal State Management Tables scheduled job that continuously checks and maintains data integrity of all internal CI Lifecycle Management tables.
2. Define CI actions.
3. Define compatible CI actions rules.
   Navigate to Configuration > CI Lifecycle Management > CMDB CI Actions to display currently active/inactive CI actions in the CMDB.
4. Define not-allowed CI actions rules.
5. Define not-allowed operational state transitions rules.
6. Define new operational states by modifying the operational_status field in the [cmdb_ci] table in the system dictionary.
   Navigate to Configuration > CI Lifecycle Management > View Internal Operational States to display available operational states set by each requestor.
7. Set priority for operational states.
8. Call APIs to apply CI actions.
   Navigate to Configuration > CI Lifecycle Management > CMDB CI Actions to display which actions were submitted and thier active/inactive state in the CMDB.
9. Navigate to Configuration > CI Lifecycle Management > View CI State Registered Users to display currently registered operators that were registered via the registerOperator API.
10. Review Renew Lease tasks and extend leases as needed: Navigate to Configuration > CI Lifecycle Management > Renew Lease Tasks. These tasks are created automatically by the CI Lifecycle Management - Restore Internal State Management Tables scheduled job for CI action records in which the lease for a valid requester has expired. The Requestor should use the lifecycle management API ExtendCIActionLease to extend the lease. Otherwise, if the lease remains expired for a specified grace period, the CI Lifecycle Management - Restore Internal State Management Tables scheduled job marks the respective CI action record as 'inactive'.

   The grace period for expired lease time is configurable by the system property glide.cmdb.statemgmt.max_lease_expired_days.
11. Navigate to Configuration > CI Lifecycle Management > State Management Logs to display logs of CI Lifecycle Management operations.

Lifecycle management APIs

CI Lifecycle Management provides a set of state management APIs for manipulating CI operational states, and applying CI actions. State management APIs adhere to restrictions and allowances specified by Not Allowed CI Actions, Compatible CI Actions, and Not Allowed Operational Transitions. If an API attempts to perform a restricted operation, the operation is blocked, an error is logged, and a task is automatically created if appropriate.

Lifecycle management APIs can set operational states and CI actions to CMDB groups by utilizing lifecycle management bulk APIs.

Registration APIs

- registerOperator() - Method to register operator with state management for non-workflow user.
- unregisterOperator(String requestorId) - Method to unregister operator for non-workflow users.
- isValidRequestor(String requestorId) - Method to determine if the specified requestor is a valid active workflow user or a registered user.
- isLeaseExpired(String requestorId, String ciSysId, String ciActionName) - Method to check if registered user lease expired.
- extendCIActionLease(String requestorId, String ciSysId, String ciActionName, String leaseTime) - Method to extend CI Action Lease time, for registered users. If previous lease already expired, extend lease from now.

Operational State APIs

- setBulkCIOperationalState(String requestorId, String sysIdList, String opsLabel, String opsStateListOld) - Method to set Operational State for an array of CIs.
- getOperationalState(String ciSysId) - Method to get CI Operational State.

CI Actions APIs

- addBulkCIAction(String requestorId, String sysIdList, String ciActionName, String ciActionListOld, String leaseTime) - Method to add CI Action for an array of CIs.
- removeBulkCIAction(String requestorId, String sysIdList, String ciActionName) - Method to remove a CI Action for a list of CIs.
- getCIActions(String ciSysId) - Method to get CI Actions.

Not Allowed Action Based on Operational State API

- isNotAllowedAction (String ciType, String opsLabel, String actionName) - Method to check if a specific CI action is not allowed for specific Operational State on a CI Type.
Not Allowed Operational State Transition API

- `isNotAllowedOpsTransition(String ciType, String opsLabel, String transitionOpsLabel)` - Method to check if specific operational state transition is not allowed on a CI Type.

Compatible Action API

- `isCompatibleCIAction(String actionName, String otherActionName)` - Method to check if two specific actions are compatible with each other.

Using state management APIs

```java
// 1. Register Operator with State Mgmt
var output = SNC.StateManagementScriptableApi.registerOperator();
var jsonUntil = new JSON();
var result = jsonUntil.decode(output);
var requestorId = result.requestorId;

// Get list of sys_ids to update
var sys_ids;

// 2. Set list of sys_ids's Operational State to 'Repair in Progress'
output = SNC.StateManagementScriptableApi.setBulkCIOperationalState(requestorId,
sys_ids,'Repair in Progress');
gs.print(output);

// 3. Set list of sys_ids's CI Action State to 'Patching'
output = SNC.StateManagementScriptableApi.addBulkCIAction(requestorId,
sys_ids, 'Patching');
gs.print(output);
```

System properties associated with CI Lifecycle Management

CI Lifecycle Management uses the following system properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.cmdb.statemgmt.max_bulk_count</td>
<td>Maximum number of CIs that CI Lifecycle Management can process in a bulk update operation.</td>
</tr>
<tr>
<td></td>
<td><strong>Type</strong>: integer</td>
</tr>
<tr>
<td></td>
<td><strong>Default value</strong>: 1000</td>
</tr>
<tr>
<td></td>
<td><strong>Location</strong>: System Property (sys_properties) table.</td>
</tr>
<tr>
<td>glide.cmdb.statemgmt.max_lease_expired_days</td>
<td>Maximum number of days that lease expiration can be set with for CI Actions.</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>· <strong>Type:</strong> integer</td>
<td></td>
</tr>
<tr>
<td>· <strong>Default value:</strong> 15</td>
<td></td>
</tr>
<tr>
<td>· <strong>Location:</strong> System Property (sys_properties) table.</td>
<td></td>
</tr>
</tbody>
</table>

### Tables installed with CI Lifecycle Management

CI Lifecycle Management adds the following tables.

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CI State Registered Users</td>
<td>All currently active registered users that were created via the <code>registerOperator</code> API. You cannot manually add new records to this table.</td>
</tr>
<tr>
<td>(statemgmt_register_users)</td>
<td></td>
</tr>
<tr>
<td>CI Actions</td>
<td>A set of CI actions that can be applied to a CI during its lifetime.</td>
</tr>
<tr>
<td>(statemgmt_ci_actions)</td>
<td></td>
</tr>
<tr>
<td>CMDB CI Actions</td>
<td>Active/inactive CI actions set by a specific requestor for a specific CI. You cannot manually add new records to this table.</td>
</tr>
<tr>
<td>(statemgmt_cmdb_actions)</td>
<td></td>
</tr>
<tr>
<td>Compatible CI Actions</td>
<td>Set of rules that define pairs of CI actions that are compatible for a CI and can be applied simultaneously.</td>
</tr>
<tr>
<td>(statemgmt_compat_actions)</td>
<td></td>
</tr>
<tr>
<td>Not Allowed CI Actions</td>
<td>Set of rules that define specific actions that are not allowed for a CI when its in a specific operational state.</td>
</tr>
<tr>
<td>(statemgmt_not_allow_actions)</td>
<td></td>
</tr>
<tr>
<td>Internal Operational States</td>
<td>Internal operational states set by a specific active requestor for a specific CI. You cannot manually add new records to this table.</td>
</tr>
<tr>
<td>(statemgmt_ops_state)</td>
<td></td>
</tr>
<tr>
<td>Renew Lease Task</td>
<td>Set of tasks that were automatically created to renew the lease of CI actions whose lease has expired. You cannot manually add new records to this table.</td>
</tr>
<tr>
<td>(statemgmt_renew_lease_task)</td>
<td></td>
</tr>
<tr>
<td>Operational State Priorities</td>
<td>Priorities of operational states which determine precedence when multiple operational states are set for same CIs by different requestors.</td>
</tr>
<tr>
<td>(statemgmt_ops_state_pri)</td>
<td></td>
</tr>
<tr>
<td>Not Allowed Operational Transitions</td>
<td>Set of rules that define specific operational state transitions that are not allowed.</td>
</tr>
<tr>
<td>(statemgmt_not_allow_ops)</td>
<td></td>
</tr>
</tbody>
</table>

### Activate the CI Lifecycle Management scheduled job

When starting to use the CI Lifecycle Management module, ensure to activate the **CI Lifecycle Management - Restore Internal State Management Tables** scheduled job which is disabled by default. This scheduled job continuously checks and maintains the data integrity of all internal CI Lifecycle Management tables.

When CI Lifecycle Management operations do not complete properly, for example due to a failure of the requestor or a requestor whose lease has expired, the integrity of tables related to CI...
Lifecycle Management might be compromised. The **CI Lifecycle Management - Restore Internal State Management Tables** scheduled job scans tables related to CI Lifecycle Management, and does the following:

- De-activates or removes all internal lifecycle management records with invalid requestors, and closes any corresponding Renew Lease Tasks if present.
- Detects records associated with a valid requestor whose lease has expired, and automatically creates a Renew Lease Task to notify the user and to provide details for extending the lease. If the requestor takes no action and the lease remains expired for a specified grace period (default 15 days), automatically de-activates the corresponding CI action record, and closes any corresponding Renew Lease Task if present.

1. Navigate to **System Definition**, and click **Scheduled Jobs**.
2. Search for the **CI Lifecycle Management - Restore Internal State Management Tables** job.
3. In the respective **Active** column, double-click the value **false**, and select **true**.
4. Click the **Save** icon.

**Define a CI action**

Define a CI Lifecycle Management CI action that can be later applied to CIs.

You can view a list of all the actions that are currently applied to CIs by navigating to **Configuration** and clicking **CMDB CI Actions**.

1. Navigate to **Configuration > CI Lifecycle Management > CI Actions**.
2. On the **CI Actions** page, click **New**. Fill in **Name** and **Description**, and then click **Submit**.

**Define compatible CI actions**

Allow a CMDB CI Lifecycle Management operation in which two specified CI actions can be applied simultaneously to a CI.

By default, it is not allowed to apply more than a single action to a CI. You can change that behaviour by defining pairs of CI actions as compatible and therefore these actions can be applied simultaneously to a CI. For example you can specify that Provisioning and Patching are compatible CI actions, which lets you apply both to a CI at the same time.

1. Navigate to **Configuration**, and click **Compatible CI Actions**.
2. On the **Compatible CI Actions** page click **New** and fill out the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>First action in the compatibility actions pair.</td>
</tr>
<tr>
<td>Compatible Action</td>
<td>Second action in the compatibility actions pair.</td>
</tr>
</tbody>
</table>

An API can successfully apply the two specified actions simultaneously to a CI.

**Define a not-allowed CI action**

Define a restriction for CI Lifecycle Management in which a specified action is not allowed for a CI that is in a specified operational state.
By default, there are no restrictions in the CMDB CI Lifecycle Management on applying CI actions. You can restrict this behaviour by not allowing a specified action to be applied to a CI when it is in a specified operational state. For example, you can define a restriction in which the provisioning action cannot be applied to a Linux Server that is in a non-operational state.

1. Navigate to Configuration > CI Lifecycle Management > Not Allowed CI Actions.
2. Click New on the Not Allowed CI Actions page, and fill out the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Allowed Action</td>
<td>The action that is being restricted.</td>
</tr>
<tr>
<td>CI Type</td>
<td>The CI type for which the restriction applies to. To apply a rule to all CIs, select Configuration Item.</td>
</tr>
<tr>
<td>Operational State</td>
<td>The operational state that the CI must be at in order to apply the restriction.</td>
</tr>
</tbody>
</table>

3. Click Submit.

If an API attempts to apply the specified action to the specified CIs, while it is in the specified operational state, the operation fails and an error is logged.

**Set priority for an operational state**

CI Lifecycle Management allows multiple operators or automations to simultaneously set different operational states for a CI. A CI can have only a single operational state, so in this case, the cumulative operational state of the CI is set to the one with the highest priority. It is recommended that you specify a priority for each operational state that you define so that a cumulative state can be correctly calculated.

1. Navigate to Configuration > CI Lifecycle Management > Operational State Priority.
2. On the Operational State Priority page, click the operational state for which you want to set or update priority.
3. Enter a Priority and click Update.

Smaller numbers represent higher priority.

**Define a non-allowed operational transition**

Define a restriction for CI Lifecycle Management in which a specified CI cannot transition from one operational state to another.

By default, CI Lifecycle Management has no restrictions for transitioning CIs from one operational state to another. You can restrict this behaviour by defining transitions that are not allowed for a specified CI. For example, you can define a restriction on transitioning a Linux server from non-operational state to repair in progress state.

1. Navigate to Configuration > CI Lifecycle Management > Not Allowed Operational Transitions.
2. On the Not Allowed Operational Transitions page, click New and fill out the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CI Type</td>
<td>The CI type for which the restriction applies.</td>
</tr>
<tr>
<td>Not Allowed Transition</td>
<td>The CI state into which transitioning is restricted.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Operational State</td>
<td>The operational state that the CI must be in for the restriction to apply.</td>
</tr>
</tbody>
</table>

If an API attempts to transition a CI that is in the specified operational state to a state that is not allowed, the operation fails and an error is logged.

CMDB groups

A CMDB group is a collection of CIs that lets you apply CI actions collectively to all the CIs that are members in the group. For example, a CMDB CI Lifecycle Management API can use a CMDB group scriptable API to retrieve the group's list of CIs, and then apply a CI Lifecycle Management action collectively to all the CIs.

Group type

A CMDB group is configured with a group type. If a CMDB group is set with the Health group type, then the CIs in the group can be monitored by CMDB Health, and the aggregated health is reported for the group as a whole in the CMDB group view dashboard. For example, you can monitor health only for CIs in a specific location.

Populate a CMDB group

Depending on the group type, you can populate a CMDB group by manually adding individual CIs, selecting saved CMDB queries, or building encoded queries in the CMDB group itself. The resulting CIs from each query are added as members to the group.

Roles required:

- To use a CMDB saved query - cmdb_query_builder
- To manually add CIs - itil or asset

Also, to populate a CMDB group using a CMDB query, a saved CMDB query must exist.

1. Navigate to Configuration > CMDB Group.
2. In the CMDB Groups pane click New.
3. Fill out the form, right-click the title bar and select Save.

CMDB Group form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>A unique name for the group.</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
Group type | - **Default**: Basic group type which can be populated by manually adding CIs, saved queries, and encoded queries.
- **Health**: Sets CMDB Health to monitor the health of the group CIs and aggregate health results for the group as a whole. Can be populated only by encoded queries.

**Note**: Dynamic filters are not supported when populating this type of CMDB groups.

4. To use saved CMDB queries:
   a) Click **CMDB Group Contains Saved Queries** and then click **Add Query**.
   b) Select a query from the **Query Builder Saved Query** list.
   c) Click **Submit**.

   The query that is used returns a list of CIs of the class in the start node of the query.

5. To manually add CIs:
   a) Click **CMDB Group Contains Configuration Items** and then click **Edit Manual CI**.
   b) Optionally add filters.
   c) Select CIs in the **Configuration Item** list and click the '+' icon at the bottom.
   d) In the **Group members** list, select the CIs to add to the group.
   e) Click **Save** or **Save and Exit**.
   f) In the **Save Confirmation** dialog box, click **OK**.
   g) Click **Submit**.

6. To use queries:
   a) Click **CMDB Group Contains Encoded Queries** and then click **New**.
   b) Select a class for which the encoded query applies to and add conditions to build a query. The resulting CIs are included in the group.

   **Note**: Dynamic filters are not supported for CMDB health-type groups, even though it is possible to add them in a condition clause.

   c) Click **Submit**.

   Click **Show All CI** to display all CI members of the group.

**Show CI Lifecycle Management details for CMDB group CIs**

Display CI Lifecycle Management operational state and CI actions that apply to the CIs that are members of a CMDB group.
If the CMDB group is based on a CMDB query, then the query runs in real-time and displays the resulting CIs. If the query does not complete successfully due to timing out or for other reasons, then appropriate error messages are displayed.

1. Navigate to Configuration > CMDB Groups.
2. On the CMDB Groups page, click on a CMDB group.
3. Click Show All CI.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Item</td>
<td>CI group member.</td>
</tr>
<tr>
<td>Class</td>
<td>Class of CI group member.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>CI Lifecycle Management operational state of the CI such as 'Repair in Progress' or 'Operational'. Possible operational states are defined in the choice list of the Operational status field in the cmdb_ci table.</td>
</tr>
<tr>
<td>Actions</td>
<td>CI Lifecycle Management actions that apply to the CI such as 'Cloning' and 'Provision'. Possible actions are defined in the CMDB CI Actions (statemgmt_cmdb_actions) table.</td>
</tr>
</tbody>
</table>

**CMDB Identification and Reconciliation**

The Identification and Reconciliation module provides a centralized framework for identifying and reconciling data from different data sources. It helps maintain the integrity of the CMDB when multiple data sources such as EventManagement, Discovery, ImportSets, and ManualEntry are used to create and update CI records.

The use of multiple sources increases the risk of introducing inconsistencies through duplicate records. To maintain the integrity of the database, it is important to correctly identify CIs and services so that new records are created only for CIs that are truly new to the CMDB. Identification and Reconciliation helps you prevent duplication of CI records, reconcile CI attributes, reclassify CIs, and allow only authoritative data sources to update the CMDB.

**Guided setup**

You can configure and get started with Identification and Reconciliation following a prescribed step-by-step in-product guidance:

1. Navigate to Guided Setup > ITOM Guided Setup and click Continue.
2. Scroll to Configuration (CMDB), and click Continue.
3. Scroll to Identification and Reconciliation and click Configure.

**Domain Separation**

The identification process is domain aware. If the domain separation plugin has been activated, then identification processes only those CIs in which the domain ID is identical to the domain of the currently logged on user. If duplicate CIs exist across domains (including parent and child domains), then those CIs are not considered duplicate CIs because their domain IDs do not match.
Identification and reconciliation components and process

The CMDB identification and reconciliation functionality is supported by identification rules, reconciliation rules, de-duplication tasks, and reclassification tasks.

Components of Identification and Reconciliation

Identification

Identification is the process of uniquely identifying CIs, to determine if the CI already exists in the CMDB or if it is a newly discovered CI that must be added to the CMDB. The identification engine performs identification processes, relying on identification rules.

Reconciliation

Reconciliation is the process of reconciling CIs and CI attributes by allowing only designated authoritative data sources to write to the CMDB at the CI table and attribute level. The CMDB is updated in real time as records are being processed. There is no staging area to verify the reconciliation activities before they are committed. The process relies on reconciliation rules.

De-duplication tasks

If the instance encounters duplicate CIs during the identification and reconciliation process, it groups each set of duplicate CIs into a de-duplication task. Review the information in these tasks to see how it was determined that these CIs are duplicates.

Reclassification tasks

During the CI identification process, a matched CI might need to be upgraded, downgraded, or switched to another CI class. If automatic reclassification is disabled, then the system generates a reclassification task. Review the information in these tasks, and decide whether a manual reclassification of the CI is appropriate.

APIs

The Identification and Reconciliation APIs are a centralized set of APIs that can be used with different sources of data such as Discovery, Monitoring, or Import Sets. You can use it to enforce identification and reconciliation before data is stored in the CMDB. Data sources do not directly write to the CMDB. Instead, they call the APIs first to ensure that the data being written does not introduce inconsistencies.

Identification engine APIs are accessible in scoped apps. See Activate Configuration Management For Scoped Apps (CMDB) for information about how to activate the plugin, and how to script a scoped app to access those APIs.

- **createOrUpdateCI()**: A scriptable API that creates or updates a CI based on identification and reconciliation rules.
- **IdentifyCI()**: Similar to the createOrUpdateCI API, but does not commit the result to the database. Use this API with a given payload to find out if the identification engine will perform insert or update operations, without committing the operation.
- **CMDBTransformUtil**: An API to be used exclusively with Import Sets to apply identification and reconciliation processes to data imported by Import Sets.

Predefined identification and reconciliation rules are included for tables that are in the base instance. You can customize these rules for your organization. When a new table is created in the CMDB, it derives identification and reconciliation rules from its parent table if these rules exist. To
apply identification and reconciliation rules to a new table, create the rules either at the child level or at its parent level.

Process flow of Identification and Reconciliation

Apply CI Identification and Reconciliation to Import Sets
You can apply CMDB Identification and Reconciliation processes when Import Sets are used to import CIs into the CMDB. CI identification can prevent duplicate CIs in the CMDB, which Import Sets might otherwise cause.

Populating CMDB tables using Import Sets can inadvertently result in duplicate CIs when multiple imported records are identical to an existing CI. To minimize this duplication, you can apply CMDB Identification and Reconciliation processes to Import Sets when importing new records into CMDB tables.
Transform map script

In the onBefore transform map script for an import set, add a call to the `CMDBTransformUtil` API, similar to the following code sample:

```javascript
(function runTransformScript(source, map, log, target) {
  // Call CMDB API to do Identification and Reconciliation of current row
  var cmdbUtil = new CMDBTransformUtil();
  cmdbUtil.identifyAndReconcile(source, map, log);
  ignore = true;

  if (cmdbUtil.hasError()) {
    var errorMessage = cmdbUtil.getError();
    log.error(errorMessage);
  } else {
    log.info('IE Output Payload: ' + cmdbUtil.getOutputPayload());
    log.info('Imported CI: ' + cmdbUtil.getOutputRecordSysId());
  }
})(source, map, log, target);
```

The `ignore = true` code phrase prevents Import Sets from creating the same record again after it is processed by the identification engine.

Process

The identification engine performs identification of each source record before it is inserted into the CMDB. The identification engine determines if the record is a duplicate of an existing CI, and then:

- If not duplicate: Inserts the record to the target table.
- If duplicate: Updates the existing CI in the CMDB, with data from the source record.

The CMDBTransformUtil API pre-processes the source data. Then passes the input values to the identification engine with import set being the data source by default. The CMDBTransformUtil API supports a target field that is a reference field in the same manner that Import Sets supports it. The CMDBTransformUtil API also supports a source script, evaluating source scripts to determine the target value which is then passed to the identification engine. For more information, see Create a field map.

Restrictions

The following restrictions apply:

- An import set should be associated with a single transform map. While adding a call to the CMDBTransformUtil API, ensure that still a single transform map exists for the import set.
- The CMDBTransformUtil API does not check if mandatory fields have values when used with Import Sets. Regardless of how enforce mandatory fields is set in the transform map, data import fails if a mandatory field does not have a value.
- CI Identification and Reconciliation cannot be applied to Import Sets for dependent CIs (CIs with dependent identification rules).
Activate Configuration Management For Scoped Apps (CMDB)

You can activate the Activate Configuration Management For Scoped Apps (CMDB) plugin (com.snc.cmdb.scoped) to allow a scoped app in scripts to use the prefix 'sn_cmdb.IdentificationEngine.<method>' to access identification engine APIs. This plugin does not include 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.

CMDB identification rules

The CMDB identification process relies on identification rules. Each identification rule consists of one or more identification entries and related entries.

Identification rules apply to a CI class and comprises of one or more identifier entries and related entries, each with a different priority. Each identifier entry defines a unique attribute set with a specific priority and each related entry defines rules for identifying related items. Create strong identification rules that give the highest priority to the strongest identifier entries and related entries.

The identification process and identification rules use the CIs attributes for identification:

Unique attributes

Designated sets of criterion attribute values of a CI, that can be used to uniquely identify the CI. Unique attributes can be from the same table or from derived tables.

Required attributes

Designated attributes of a CI that cannot be empty.
Identification rule types

The steps for identifying dependent CIs can be different from the steps for identifying independent CIs. This difference is reflected in the differences between dependent identification rules and independent identification rules.

Independent identification rule

A rule that identifies a CI based on the CI’s own attributes, independently of other CIs or relationship.

Dependent identification rule

A rule in which identifying a CI requires identifying a dependent CI first. A CI can have dependency on one or more CIs, and a dependent CI can have only a single parent CI with dependency. The relationship types between the CI and its dependent CIs are also included in the identification process. To assist in the identification process of dependent CIs, add CMDB metadata rules that define the dependency structure of CI types and the relationship types.

The payload used for identification of a dependent CI, can include a relationship with a qualifier chain. For such relationship, if there is a matching parent/child pair, the system compares the qualifier chain in the payload, with the qualifier chain of the CIs in the database. If there is a difference, the qualifier chain in the database is updated to match the qualifier chain in the payload for that relationship.

Identifier entries

You can configure an identifier entry to match a CI not only based on the CI’s own attributes (field based identification) but also based on the CI’s related list (lookup based identification) such as Serial Numbers or Network Adapters. The lookup based table that is used for identification, needs to have a reference field that points to cmdb_ci.

There are two types of identifier entries:

Regular identifier entry

Based on CI’s attributes that uniquely identify the CI.

Lookup identifier entry

Uses a related table (lookup table) which can be any table that has a reference to the CI that is being identified. After you select a related table in the lookup identifier entry, the list in Referenced field is populated with fields from the related table that reference either the cmdb_ci table itself, or one of its descendants.

Guidelines for lookup tables

Follow these guidelines when specifying a lookup table in an identifier entry.

1. Ensure that lookup tables reference the cmdb_ci table.

2. It is preferable to enforce exact count match (check box Enforce exact count match (Lookup)) for a stronger identification rule. During lookup identification, this option enforces matching only on exact lookup records count match.

3. Do not create conflicting identification rules especially for lookup based rule.

Example: In a CI Identifier for the Hardware class you specify a lookup based rule for the Network Adapter class, and you also define a CI Identifier for the Network Adapter class.
Duplicates might potentially be created in the Network Adapter table, because there are contradicting rules to identify a unique CI in that table:

- One rule that looks only at criterion attributes (CI identifier rule)
- Another rule that looks at criterion attributes and referenced sys_id (lookup rule).

Example: CI with related items that needs to be inserted - sysId is available.

```json
var payload = {
  items: [{
    className:'cmdb_ci_linux_server',
    related: [{
      className:'cmdb_ci_spkg',
      values: {
        name:'package1',
        version:'version1'
      }
    }],
    values: {
      sys_id:'194876usytrr65378098'
    }
  }]
};
```

**Related entries**

You can also define related entries which are rules that are based on related CIs. A related entry is based on a related table which can be any table that has a reference to the CI that is being identified. After you select a related table for the rule, the list in **Referenced field** is populated with fields from the related table that reference either the cmdb_ci table itself, or one of its descendants.

**Create or edit a CI identification rule**

Identification rules are used to uniquely identify CIs in the CMDB, as part of the identification and reconciliation process. Each table in the CMDB can be associated with a single identification rule.

Role required: admin, or itil_admin (on top of itil)

**Note:** Users with the itil role have read access to the CI identification rules.

In a CI identification rule, specify identifier entries and related entries that uniquely identify the CI. Review the following before creating identification rules:

- [CMDB identification rules](#)
- [Effective usage of CMDB Identification](#)

1. Use the CI Class Manager:
   a) Navigate to **Configuration > CI Class Manager**.
   b) Select a class in the **Class Hierarchy**.
   c) On the right, click **Advanced** and expand **Correctness**.
   d) Select **CI Metadata Editor**, and click the **Identification** tab.

2. Or, navigate to **Configuration > Identification/Reconciliation > CI Identifiers**.

3. Click **New, Add New Rule**, or select an existing rule.
4. Complete the form.

**Identifier form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of CI identifier.</td>
</tr>
<tr>
<td>Applies to</td>
<td>Class that this CI identifier applies to.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the CI identifier.</td>
</tr>
<tr>
<td>Independent</td>
<td>Check box indicating that the CI identifier can identify the CI independently of other CIs. See CMDB identification rules and Effective usage of CMDB Identification for more information.</td>
</tr>
</tbody>
</table>

5. Click **Submit**, and then click the identification rule to load its related lists.

6. In the **Identifier Entries** related list, click **New** or open an existing entry to specify criteria for matching the CI. Fill out the form, and then click **Submit**.

**Identifier Entry form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Check box that specifies the identifier entry is active.</td>
</tr>
<tr>
<td>Criterion attributes</td>
<td>The set of attributes to uniquely identify the CI. Attributes can belong to the current class, or to a parent class. Click the lock icon to view, add, or remove attributes from the identification rule. It is not possible to add reference fields as a criterion attribute. Reference fields store sys_ids that point to a record in another table, and thus is considered a weak criterion attribute (in terms of uniqueness) for the current table.</td>
</tr>
<tr>
<td>Identifier</td>
<td>The CI identifier to which this identifier entry belongs to. By default it is set to the identifier you previously selected.</td>
</tr>
<tr>
<td>Priority</td>
<td>Priority of the identifier entry. Identifier entries are applied based on priority. Rules with lower priority numbers are given higher priority. Identifier entries of identical priorities are applied randomly. It is recommended that you keep gaps between the priority numbers, so you can assign the unused priority numbers to new entries without modifying the existing priority order.</td>
</tr>
</tbody>
</table>
### Field Description

**Search on table**
- The lookup table:
  - For a regular identifier entry: Select the same table as the table specified in **Applies to** on the Identifier form.
  - For a lookup identifier entry: Select a table that is different from the **Applies to** table specified on the Identifier form. Also, the lookup table must have a reference field to **cmdb_ci**, otherwise the identifier entry is considered invalid.

**Allow fallback to parent’s rules**
- Check box to specify that the identification rules of the CI’s parent are used if a match is not found for this identification rule. Applies only for dependent identification rules.

**Allow null attribute**
- Check box to allow null values for criterion and unique attributes.

---

**Note:** If criterion attributes have only two attributes and **sys_class_name** is one of them (for example (name, sys_class_name), (ip_address, sys_class_name)), then the other attribute cannot be NULL, even if **Allow null attribute** is enabled. This restriction is due to **sys_class_name** being considered a special system matching attribute.

Additionally, you can add the following advanced fields by customizing the form view:

### Field Description

**Enforce exact count match (Lookup)**
- Check box for specifying that for lookup identification, match only on exact lookup records count match.

**Optional condition**
- Use the **Add Filter Condition** and the **Add “OR” Clause** buttons to construct a filter to narrow the set of records that will be searched for a matching CI. Applied only to lookup based identification.

---

7. In the **Related Entries** related list, click **New** or open an existing entry to specify a related entry for matching the related item. Fill out the form, and then click **Submit**.

### Related Entry form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>The CI identifier for which this related entry belongs to. By default it is set to the identifier you previously selected.</td>
</tr>
<tr>
<td>Related table</td>
<td>A related table that references the CI that is being matched.</td>
</tr>
<tr>
<td>Referenced field</td>
<td>A referenced field in <strong>Related table</strong> that should store the referenced CI. This field always reference the cmdb_ci table, or a descendant of the cmdb_ci table.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criterion attributes</td>
<td>The set of attributes to uniquely identify the related item. Attributes can belong to the current class, or to a parent class. Click the lock icon to view, add, or remove attributes from the identification rule.</td>
</tr>
<tr>
<td>Optional condition</td>
<td>Use the Add Filter Condition and the Add &quot;OR&quot; Clause buttons to construct a filter to narrow the set of records that will be searched for a matching related item.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box that specifies that the related entry is active.</td>
</tr>
<tr>
<td>Allow null attribute</td>
<td>Check box to allow null values for criterion and unique attributes.</td>
</tr>
<tr>
<td>Priority</td>
<td>Priority of the related entry for the specified Related table. Rules with lower priority numbers are given higher priority while matching a related item for specific related table. Related entries for the specified related table with identical priorities are applied randomly. It is recommended that you keep gaps between the priority numbers, so you can assign the unused priority numbers to new entries without modifying the existing priority order.</td>
</tr>
</tbody>
</table>

**Note:** If criterion attributes have only two attributes and `sys_class_name` is one of them (for example (name, sys_class_name), (ip_address, sys_class_name)), then the other attribute cannot be NULL, even if Allow null attribute is enabled. This restriction is due to `sys_class_name` being considered a special system matching attribute.

For example, the pre-defined Hardware Rule applies to the Hardware (cmdb_ci_hardware) table. It has an identifier entry with the criterion attribute Serial Number, Serial Number Type and its Search on table field is set to Serial Number.

The following payload snippet adds a CI to the cmdb_ci_linux_server class, that is a child of the Hardware class. It also shows how you can add related items in the payload for which you should create Related Entries on the CI Identifier page for the Hardware (cmdb_ci_hardware) table:

```json
{
  "items": [
    {
      "className": "cmdb_ci_linux_server",
      "lookup": [
        {
          "className": "cmdb_serial_number",
          "values": {
            "serial_number": "VMware-42 21 e3 da 44 14 5a a6-56 48 2b 0a 28 53 42 4c",
```

© 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 the **Hardware Rule** is applied, the Serial Number (cmdb_serial_number) table is searched for a match with the values specified within the lookup key. Unless **Enforce exact count match (Lookup)** is checked, it is not necessary for every lookup key to return a match, as long as there is at least one match. If all matches reference the same CI, then that CI is considered to be the existing CI record. If no match is found, then the identification search continues to the next rule entry. If after all the rules are exhausted without finding a match, a new CI record is created in the database.
Create identification inclusion rule

You can narrow the scope of CIs that are included in the identification process by creating identification inclusion rules. If any identification inclusion rules exist, then they are automatically used also by the CMDB Health duplicate metric, in the same manner that health inclusion rules are used for other metrics.

Role required: itil_admin (on top of itil)

During duplication detection of independent CIs, the identification engine processes only the CIs that satisfy the identification inclusion rules. For example, you can include only CIs whose operational state is operational. When no identification inclusion rules exist, all CIs are included in the identification process and in the CMDB Health duplicate metric calculations. In the base system, there are no predefined identification inclusion rules. Identification inclusion rules are defined at the class level.

Note: Be careful when creating Identification inclusion rules. Identification inclusion rules can prevent the identification of certain types of CIs, affecting some features of Discovery and Service Mapping.

1. Navigate to Configuration > CI Class Manager.
2. Select Advanced, expand Correctness and then click CI Metadata Editor.
3. On the Configuration Item page, click the Identification tab.
4. Select a class in the Class Hierarchy for which to edit or create the rule for.
5. In the Identification Inclusion Rules section, click on an existing rule to edit, or click New.
6. On the Identification Inclusion Rules form, specify the criteria that CIs must meet to be included in the identification process, and in the duplicate CMDB Health metric.
7. Click Submit.

Navigate to Configuration > Identification/Reconciliation > Identification Inclusion Rules > to see the list of all identification inclusion rules.

Reconciliation rules

Reconciliation rules specify which data sources can update a table or a set of table attributes, and they can be defined at the parent and the child table level. Ensure that there is a reconciliation rule for each data source that is authorized to update an attribute - multiple reconciliation rules can exist for the same set of attributes.

Data sources are used with the createOrUpdateCI() API to simulate manual updates to CIs. EventManagement, ImportSet, ManualEntry, and Tivoli are examples of data sources.

As you create reconciliation rules, keep the following principles and guidelines in mind. These principles are designed for flexibility and the refinement of rules at the attributes level.

Example reconciliation rules

For example, you might have the following reconciliation rules. The rules are created for the cmdb_ci_computer table and one of its child tables, the cmdb_ci_linux_server table. The rules specify the following:

1. Discovery is exclusively authorized to update the name attribute in the cmdb_ci_computer table.
Because reconciliation rules are derived by child tables from parent tables, this rule also authorizes Discovery to update the name attribute in any child tables for the cmdb_ci_computer table.

2. ServiceWatch is exclusively authorized to update the name attribute in the cmdb_ci_linux_server table.

3. ServiceWatch is exclusively authorized to update all attributes in the cmdb_ci_linux_server table, as configured by leaving the Attributes field empty in the rule.

Authorization for all attributes in a table

If you want to authorize a data source to update all attributes in a table, leave the attribute list empty in the reconciliation rule for the data source. However, this authorization can be overridden for some of the attributes by rules for child tables in which specific attributes are listed.

For example, if only example rules #1 and #3 are created, then Discovery is authorized to update the name attribute in the cmdb_ci_linux_server table. ServiceWatch is authorized to update all other attributes in the table except for the name attribute.

To override the authorization of Discovery to update the name attribute, example rule #2 is added to specifically authorize ServiceWatch to update the attribute.

Authorization to only specific attributes in a table

If you want to authorize a data source to update specific attributes in a table, list these attributes in the reconciliation rule for the data source. A rule that grants access to specific attributes in a table overrides other rules with an empty attribute list that grants access to the entire table.

Example rule #1 grants Discovery with exclusive authority to update the name attribute of the cmdb_ci_computer table. All other data sources are prevented from updating the name attribute of any CI in the cmdb_ci_computer table.

Child table rules overrides parent table rules

Any reconciliation rules defined for a child table override the rules defined for its parent table.

For example, rule #1 lets Discovery update the name attribute in the cmdb_ci_computer table and all of its child tables. However, rule #2 for the cmdb_ci_linux_server child table, which overrides rule #1 for the parent table, explicitly authorizes ServiceWatch to update this attribute in the child table.

As a result:

- Discovery cannot update the name attribute of the child cmdb_ci_linux_server table. Only ServiceWatch is authorized to update this attribute.
- Discovery is authorized to update the name attribute of CI records in all other child tables of the cmdb_ci_computer table.

Overlapping rules

Rules that authorize different data sources for the same attributes of the same table can coexist and do not exclude each other.
For example, assume the following rule is added. It is similar to example rule #1 but authorizes a different data source:

- ServiceWatch is authorized to update the name attribute in the cmdb_ci_computer table.

Like example rule #1, this new rule applies to the name attribute in the cmdb_ci_computer table so both Discovery and ServiceWatch can update the attribute. Any applicable data source precedence rules are enforced to prevent the data sources from overwriting each other's updates.

**Domain separation**

If Domain Separation is enabled, then you can scope reconciliation rules to specific domains. Rules of the parent domain, if not overridden, apply to CIs of child domain. All rules that are visible to a domain are applied, and a rule overriding the parent domain displays the child domain version.

**Create or edit a CI reconciliation rule**

A reconciliation rule specifies the attributes that a data source is authorized to update for a given table and prevents unauthorized data sources from overwriting the attributes' values. If an attribute does not have any reconciliation rules created for it, data sources are allowed to overwrite each other's updates to the attribute's value.

Role required: admin or itil_admin (on top of itil)

Reconciliation rules are used in conjunction with data source refreshness rules and data source precedence rules to determine reconciliation steps for a CI. These rules determine if, when, and by which data source a CI can be updated.

**Note:** Users with the itil role have read access to the CI identification rules.

1. Use the CI Class Manager:
   a) Navigate to Configuration > CI Class Manager.
   b) Select a class in the Class Hierarchy.
   c) On the right, click Advanced and expand Correctness.
   d) Select CI Metadata Editor, and click the Reconciliation tab.

2. Or, navigate to Configuration > Identification/Reconciliation > Reconciliations Definitions.

3. Click New to create a new reconciliation rule, or select an existing rule to edit. Fill in the fields as appropriate.

**Reconciliation Definition form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data source</td>
<td>The data source that you are configuring this rule for.</td>
</tr>
<tr>
<td>Applies to</td>
<td>The table that the selected data source can update.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Filter condition</td>
<td>Conditions that the CI must meet, in order for the rule to apply to specific CIs. For example, to apply this rule only to CIs that are associated with the Finance department, select this condition: ( \text{Department} \equiv \text{Finance} )</td>
</tr>
<tr>
<td>Attributes</td>
<td>Attributes that the data source is authorized to update. You can select attributes from the current class, or a parent class. To authorize the data source to update all table attributes, leave this field empty.</td>
</tr>
<tr>
<td>Update with null</td>
<td>Attributes that the data source can update with a null value. By default, authorized data sources cannot overwrite a non-null value with a null value. Attributes in this list, which are not in the Attributes list, are not included with the attributes that the data source can update with a null value.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain that the reconciliation rule is enforced in, if the Domain Support domain separation plugin is enabled.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box to activate this reconciliation rule.</td>
</tr>
</tbody>
</table>

4. Click Submit.

**Define or edit data source precedence**

If multiple data sources are authorized to update the same table or the same table attributes in the CMDB, assign a priority to each of these data sources to prevent them from overwriting each other's updates. Without data source precedence rules, data sources can overwrite each other's modifications.

Role required: admin, or itil_admin (on top of itil)

Data source precedence rules are used along with data source refreshness rules and reconciliation rules to determine reconciliation steps for a CI. These rules determine if, when, and by which data source a CI can be updated.

After an authorized data source updates an attribute, subsequent updates are accepted only from the same data source or from a data source with a higher priority. Updates from a data source with a lower priority are rejected, unless these two conditions are met:

- The lower propriety source is the first source updating the CI.
- The CI became stale based on data source refreshness rules for the CI class.

Information about the last data source that updates each attribute is stored in the Data Source History (cmdb_datasource_last_update) table.

Data source precedence rules affect reconciliation of stale CI attributes. During reconciliation, the information in the Data Source History table is considered along with the data source refreshness rules for the CI's class, to determine if a CI attribute is stale. A CI attribute is determined to be stale if it was not updated by the latest data source to update the CI, within a time period. The time period is specified by the Effective Duration time in the data source refreshment rule for
the class for the data source. In this case, if another authorized data source, with a lower priority attempts to update the stale CI attribute, the update is allowed.

**Note:** Users with the itil role have read access to the CI identification rules.

1. Use the CI Class Manager:
   a) Navigate to Configuration > CI Class Manager.
   b) Select a class in the Class Hierarchy.
   c) On the right, select Advanced and expand Correctness.
   d) Select CI Metadata Editor and click the Reconciliation tab.

2. Or, navigate to Configuration > Identification/Reconciliation > Datasource Precedences.
3. Click New to create a new data source precedence definition, or select an existing data precedence definition.
4. Complete the form.

**Data Source Precedence form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applies to</td>
<td>The table that this precedence rule applies to.</td>
</tr>
<tr>
<td>Data source</td>
<td>The data source that this precedence rule applies to. EventManagement, ImportSet, ManualEntry, or an application such as Tivoli are examples of a data source.</td>
</tr>
<tr>
<td>Order</td>
<td>Priority of this precedence rule within the set of precedence rules for the specified table. Smaller numbers designate higher priority. Data sources without a precedence rule are assigned the lowest priority.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box to activate this precedence rule.</td>
</tr>
</tbody>
</table>

5. Click Submit.

**Create data source refreshness rule**

Specify data source refreshness rules to determine if a CI is stale for a specific data source. Such CIs can then be updated by a lower-priority authorized data source.

Role required: admin

Data source refreshness rules are used in conjunction with data source precedence rules and reconciliation rules to determine reconciliation steps for a CI. These rules determine if, when, and by which data source a CI can be updated.

1. Navigate to Configuration > CI Class Manager.
2. Select Advanced and then expand the Correctness strip.
3. Click CI Metadata Editor and then click the Reconciliation tab.
4. In the Data Source Refreshness section select an existing rule to edit, or click New.
5. Complete or edit the form.
### Data Source Staleness Definition form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applies to</td>
<td>The class for which the rule applies.</td>
</tr>
<tr>
<td>Effective Duration</td>
<td>The time period that is used for the staleness test.</td>
</tr>
<tr>
<td></td>
<td>If the fields specified in the reconciliation rule for the CI's class were not updated by the specified data source within the specified time period - the CI is determined to be stale for that data source.</td>
</tr>
<tr>
<td></td>
<td>If you enter a value with a prefix that is valid and a suffix that is not, such as 15 x - the valid portion of the value is used (15). If the entire value is invalid - the default value of 0 is used.</td>
</tr>
<tr>
<td>Data Source</td>
<td>Data source of the class.</td>
</tr>
<tr>
<td>Active</td>
<td>Specifies that the rule is active.</td>
</tr>
</tbody>
</table>

6. Click **Submit** or **Update** to save the rule.

### Generate and simulate payload execution using identification simulation

Identification simulation is a central location for automatically constructing a payload that is guaranteed to be complete and valid. You can then simulate the processing of the payload by the identification engine and examine the results before actually submitting it for execution by the identification engine.

Use identification simulation to construct an input payload, and simulate processing of the payload by the identification engine. You can then examine the results, adjust identification rules if needed, and re-run the simulation of the updated payload.

Use the identification simulation to:

- Automatically construct input payload that is based on existing identification rules, hosting and containment rules.
- Simulate execution of a payload (automatically constructed by identification simulation, or manually created).
- Browse payload output and execution log messages for a simulated run.

**Note:** Identification simulation does not commit any updates to the CMDB, other than setting the `discovery_source` attribute to **Duplicate** for a CI that is determined to be duplicate.

### Automatically generate payload using identification simulation

Use identification simulation to automatically construct an input payload for a specified class. The constructed payload is complete with any required dependent CIs, correctly structured, and syntactically valid for processing by the identification engine.

Role required: itil
The payload that is constructed during identification simulation is for the specified class. For a dependent CI class, you will be prompted for information about all dependencies. After you provide the required details, identification simulation constructs the payload based on your input.

1. Navigate to Configuration > Identification/Reconciliation, and click Identification Simulation.
2. In the Start with CI Class box click Start.
3. On the Payload Information form, in the Source field, select the data source that is associated with this class update.
   For the ServiceNow Discovery data source, select ServiceNow.
4. Select the Class in the payload.
   a) In the Criterion Attributes area select the CI identifier attributes and then specify the values that uniquely identify a CI.
   b) In the Additional Attributes area specify attributes and values that matching CIs will be updated with.
5. For dependent CIs associated with dependent identification rules, fill out the Criterion Attributes and Additional Attributes sections in all Container level sections that display.
6. Click Generate. If any errors indicate that there are missing fields, fill in the missing fields and then click Generate again.
7. You can optionally click Execute to simulate processing of the payload by the identification engine.

Examine the results of the simulation, fine-tune the payload as needed, and combine with other payloads for other classes as desired. After finalizing the payload, use the createOrUpdateCI() API to execute the payload by the identification engine which will result in actual updates to the CMDB.

Simulate payload processing using identification simulation

Use identification simulation to simulate the identification engine process of CI identification for an input payload. Provide a valid payload, which was constructed using identification simulation or that was created manually.

Role required: itil

1. Navigate to Configuration > Identification/Reconciliation, and click Identification Simulation.
2. To execute an existing payload:
   a) Click Start in the Start with Existing Payload tile.
   b) In the Source field, select the data source that is associated with this class update.
   c) Paste the JSON payload into the empty canvas.
3. Or, to construct a new payload click Start in the Start with CI Class tile. See Automatically generate payload using identification simulation for more information.
4. Click Execute to simulate processing of the payload by the identification engine.

1. Examine the results of the simulation in the results pane, and fine-tune the payload as needed:
   a. Click Run #1 to display the Context ID and the Run ID of the simulated run.
   b. Click the drop down arrow next to Run #1 to display additional details.
      • Input: Displays the payload for the simulation.
      • Logs: Displays all the logged messages that the identification engine generated while simulating processing of the payload, according to the specified logging level.
• **Output**: Displays the output payload returned by the identification engine.

2. After finalizing the payload, use the `createOrUpdateCI()` API to execute the payload by the identification engine which will result in actual updates to the CMDB.

### Set logging level for identification simulation

Identification simulation logs each step of a simulated payload processing. You can then examine these run logs to determine if a payload was processed as expected, and if identification rules are effective. You can adjust the level of logging so it is helpful, and so that the amount of messages is not excessive or insufficient.

Role required: itil

1. Navigate to **Configuration > Identification/Reconciliation**, and click **Identification Simulation**.
2. Click the **Settings** icon.
3. Select logging level for the identification engine under **IE Log Level** and for the service cache under **Service Cache Log Level**.
   - The logging levels are displayed in ascending order, from the minimum level to the maximum level of logging.
4. Click on the **Settings** icon again to close the **Settings** dialog box.

### Resolve de-duplication tasks

When the instance encounters duplicate CIs during identification and reconciliation, it groups each set of duplicate CIs into a de-duplication task for review. Use de-duplication tasks to track the duplicate CIs until they can be resolved. A large number of duplicate CIs might be due to weak identification rules.

De-duplication tasks provide details about the duplication, including a list of all the duplicate CIs and the internal payload used during the identification process. Review the details of each duplicate CI in the task and the data that was used to determine that the CI is a duplicate.

If the duplicate CI is a dependent CI, then you can view the details of the dependent relationship, the Depend on CI, and any relation qualifier chain. If the dependent CI has a lookup table, then you can see the details of the respective lookup table.

### Skip duplication

Processing of sets of duplicate CIs depends on the system properties `glide.identification_engine.skip_duplicates` (set to true by default) and `glide.identification_engine.skip_duplicates.threshold` (set to 5 by default), and on the number of duplicate CIs in a set.

- If `glide.identification_engine.skip_duplicates` is true, and the number of duplicate CIs is less than the threshold specified by `glide.identification_engine.skip_duplicates.threshold`, then the oldest of the duplicate CIs is picked as a match and gets updated. The rest of the duplicate CIs are tagged as duplicates by setting the `cmdb_ci.cdiscovery_source` field as 'Duplicate'.
- If `glide.identification_engine.skip_duplicates` is false, then matching of duplicate CIs fails with an error, and none of the duplicate CIs is updated.

**Note:** In either case, de-duplication tasks are always created.

To modify these properties, you need to first add them to the System Properties (sys_properties) table. For more information, see *Properties installed with Identification and Reconciliation.*
Role required: admin or itil

1. Navigate to Configuration > Identification/Reconciliation > De-duplication Tasks.
2. Select a task.

### De-duplication Task fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>A unique task number.</td>
</tr>
<tr>
<td>Assigned to</td>
<td>A person that is responsible for resolving the task.</td>
</tr>
<tr>
<td>Short description</td>
<td>A short description for the task.</td>
</tr>
<tr>
<td>Internal payload</td>
<td>Payload that was used in the identification process, during which the de-duplication task was generated.</td>
</tr>
<tr>
<td>Description</td>
<td>Full description for the task.</td>
</tr>
<tr>
<td>Work notes</td>
<td>Notes to keep track of the decisions and steps of resolving the task.</td>
</tr>
<tr>
<td>Priority</td>
<td>Task priority.</td>
</tr>
<tr>
<td>State</td>
<td>State of the de-duplication task as it progresses through resolution.</td>
</tr>
</tbody>
</table>

3. In the Duplicate Audit Results section, click a CI in the Duplicate CI column to view the details about how the CI was identified as a duplicate.

### Duplicate Audit Results list columns

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duplicate CI</td>
<td>Reference to the duplicate CI.</td>
</tr>
</tbody>
</table>

**Note:** This field is a document ID type, which means that it can reference any record on any table. If the referenced CI is deleted as part of resolving duplicate tasks, then this field will be empty.

<table>
<thead>
<tr>
<th>Depend on</th>
<th>If the duplicate CI is a dependent CI, then this field displays the depend on CI.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qualifier chain</td>
<td>If the duplicate CI is a dependent CI, then this field shows a list of sys_ids of qualifier CIs, if it exists.</td>
</tr>
<tr>
<td>Follow on task</td>
<td>The associated de-duplication task that captures the duplication.</td>
</tr>
<tr>
<td>Relationship</td>
<td>For a duplicate CI that is a dependent CI, this field shows the relationship between the duplicate CI and depend on CI.</td>
</tr>
</tbody>
</table>

Based on your analysis of de-duplication tasks, you can determine which CI should remain active and which of the duplicate CIs in the Duplicate Audit Results records are stale or incorrect. Determine if it is appropriate to delete or inactivate any of these CIs.
CI reclassification

During the CI identification process, a CI might need to be reclassified to a different `sys_class_name` type. By default, CIs are reclassified automatically. If automatic reclassification is disabled, then the CI is not reclassified and the system generates a reclassification task for your review.

A CI can be upgraded to a higher class, downgraded to a lower class, or switched to a different branch in the class hierarchy. For more details about reclassification operations, see "Reclassify a CI." You can configure CI reclassification behavior at a system-wide level or individually per CI.

Enabling and disabling automatic CI reclassification

You can use the `glide.class.upgrade.enabled`, `glide.class.downgrade.enabled`, and `glide.class.switch.enabled` properties to configure system-wide behavior for CI reclassification. These properties are set to `true` by default, enabling automatic reclassification. To disable automatic CI reclassification, set the respective properties to `false`.

Alternatively, you can control the reclassification behavior for individual CIs in the input payload of the `createOrUpdateCI()` API. In the payload, you can set these properties to `true` or `false` to temporarily override the respective property setting.

- `classUpgrade`
- `classDowngrade`
- `classSwitch`

The following sample JSON payload enables automatic reclassification for the specified CI:

```
{ items: [{className: 'cmdb_ci_server', classUpgrade: true, classDowngrade: true, classSwitch: true, values: {name: 'linux123', serial_number: '12srt567', ip_address: '10.2.3.4'}}, ]}
```

View a reclassification task

When automatic CI reclassification is disabled, reclassification tasks are created for CIs that could not be automatically reclassified during the identification process. Review these tasks to locate the CIs and decide if to reclassify them.

Role required: admin or itil

1. Navigate to Configuration > Identification/Reconciliation > Reclassification Tasks.
2. Select a reclassification task.
3. Examine the details on the Reclassification Task form.

Reclassification Task form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Item</td>
<td>The CI that must be reclassified.</td>
</tr>
<tr>
<td>Short description</td>
<td>Short description noting that CI reclassification was not allowed.</td>
</tr>
<tr>
<td>Description</td>
<td>Description noting the current class of the CI and the class that the CI must be changed to.</td>
</tr>
<tr>
<td>Internal payload</td>
<td>Payload used in the identification process.</td>
</tr>
</tbody>
</table>
After examining the task details, you can locate the CI that is noted in the task Description and manually reclassify it. For details, see Reclassify a CI.

**CMDB metadata rules**

Service definitions consist of CI types and relationship types. Metadata rules define the dependency structure of the CI types and the relationship types in these service definitions, assisting in CI identification and in the construction of business service maps.

The dependencies that are defined by metadata rules are used when identifying dependent CIs to prioritize the order of CI identification, and to match CIs and respective dependent CIs in a payload. Metadata rules are also used by Service Mapping and can be defined for custom CI types. After defining a new CI type, you can define metadata rules that specify how the new CI type is related to existing types in the CMDB.

Metadata rules consist of hosting rules and containment rules, each type modeling the data from a different perspective of the CI. Containment rules represent CIs configuration hierarchy, describing which CI contains which other CIs. Hosting rules represent CIs placement in a business definition, describing what CIs run on.

Both hosting and containment rules describe a relationship type between two CI types and the same relationship type can be used in a hosting rule and in a containment rule. It is the context in which the relationship is used that distinguishes between a containment and hosting rule.

Use the Metadata Editor to configure and manage metadata rules:

- Navigate to Configuration > Identification/Reconciliation > Metadata Editor to use the Metadata Editor.
- Or, to access metadata rules at the class level, navigate to Configuration > CI Class Manager, click Advanced and then expand Correctness to use the CI Metadata Editor.

The plugins that have been activated on an instance determine which hosting and containment rules exist out-of-box.

**Hosting rules**

Hosting rules represent all the possible valid combinations of pairs of hosting and hosted CIs in the service definition. Hosting rules are a flat set of rules that can be only one level deep, and which always involve resources, typically physical or virtual hardware. Each hosting rule is a stand-alone rule between two CI types, describing either a valid CI type that another CI type can host, or by which another CI type can be hosted. A hosting rule consists of a parent CI type, a relationship type (such as Hosted On::Hosts) and a child CI type. For example, you can have a hosting rule that specifies that the CI type ‘Application’ ‘Runs On::Runs’, the CI type ‘Hardware’.

A CI can be hosted on multiple resources (such as Windows and Linux). This will be represented by a hosting rule for the CI with each resource that the CI can be hosted on. During CI identification, the pair of CIs that are being examined, need to satisfy at least one hosting rule.

Hosting rules are stored in the CMDB Metadata Hosting Rules (cmdb_metadata_hosting) table.

**Reference rules**

Reference rules represent all of the possible valid combinations of pairs of referencing and referenced CIs in the service definition.

- Reference rules are a flat set of rules that can be only one level deep.
Reference rules always involve resources, typically virtual entities. Each reference rule is a stand-alone rule between two CI types, describing either a valid CI type that another CI type can reference, or by which another CI type can be referenced. Both the CI classes should be able to live independent of each other.

A referencing rule consists of a parent CI type, a relationship type (such as `Provisioned From::Provisioned`) and a child CI type. For example, you can have a referencing rule that specifies that the CI type `Virtual Machine` `Provisioned From::Provisioned`, the CI type `Image`.

A CI can reference multiple resources (for example, a VM instance can have a reference relation with both the Image and the Hardware templates). This CI is represented by a referencing rule for the CI with each resource that the CI can be referenced from.

The reference rule cannot be part of the CI identification.

Reference rules are stored in the CMDB Metadata Reference Rules (cmdb_metadata_reference) table.

Containment rules

Containment rules represent the containment hierarchy for a CI type, describing valid objects that a CI type can contain in the service definition, and valid objects that can be contained by the CI type. Containment rules are chained to each other in a containment rules group, with a CI type that is the top-level (root) parent of the group. The collection of containment rules construct a hierarchy-like map of containment relationships. Containment rules are logical concepts, and used to represent logical CIs for example to describe software that runs on a server. A containment rule consists of a parent CI type, a relationship type (such as `Contained By::Contains`) and a child CI type. For example, you might have a containment rule specifying that the CI type `Tomcat` `Contains::Contains By` CI type `WAR File`.

Endpoints are special containment rules that specify incoming or outgoing connections in the model, designating the CI types that data of some specified type flows in to or out from the service definition. After adding an endpoint to a containment rule you cannot add any child rules to the endpoint rule.

Containment rules are stored in the CMDB Metadata Containment Rules (cmdb_metadata_containment) table.

Rules requirements

The rules that you create are bound by the following requirements which narrow the relationships and ensure that only valid options are available in the drop down lists in the Metadata Editor.

- Given a CI type that is as a child in a containment rule: It cannot be a top-level (root) parent of any other containment rule, and it cannot be in any hosting rule, either as a parent or as a child.
- Given a CI type that is a top-level (root) parent of a containment rule: It cannot be a child in a hosting rule (for example, you can’t be hosted on Tomcat, if Tomcat has any containment rules)
- Given a CI type that is a child in a hosting rule: It cannot be in any containment rule, either as a parent or a child.
- Given a CI type that is a parent in a hosting rule: It cannot be a child in any containment rule.
- Hosting rules can not create loops such as Tomcat –runs_on- VMWare –runs_on- Tomcat.
Hosting and containment rules model

Hosting rules that model the diagram:
- Tomcat ‘Runs on’ Hardware

Containment rules that model the diagram:
- Tomcat ‘Contains’ Configuration File
- Tomcat ‘Contains’ WAR
- WAR has two endpoints for JDBC with MySQL:
  - Inbound
  - Outbound

Valid set of rules

<table>
<thead>
<tr>
<th>Tomcat Hosted Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux Hosted Computer</td>
</tr>
</tbody>
</table>

The second metadata entry triggers the 3rd. requirement, which is satisfied (it’s a hosting rule, not a containment rule).

Create or edit metadata containment rule

Create metadata containment rule for CIs to assist in correctly identifying dependent CIs during the business discovery process and service mapping. Discovery calls the identification API that applies metadata rules.

Role required: admin
A containment rule is a relationship definition between two CIs, structured as: CIType1 RelationshipType CIType2. The first CI type that you add becomes the top level CI of a containment rules group which is a chain of containment rules. The entire set of containment rules is organized as groups according to top-level CIs.

To create a containment rules group for a new CI type, you need to first add the CI Type1 of the relationship. To add a child containment rule for a CI type that exists, you need to select that CI type, and define the second portion of the relationship rule which is the relationship type and CI Type2.

To each rule within a containment rules group you can add inbound or outbound endpoints, which are noted by blue up and down arrows. After adding an endpoint, you can not add a containment rule in that branch of the containment rules hierarchy.

1. Navigate to Configuration > CI Class Manager
2. On the right, click Advanced, expand Correctness, and select CI Metadata Editor.
3. Select the Metadata Information tab, and use the Containment Rules section.
4. Click Add New Rule to add a top-level rule. Or, point to a rule for which you want to add a child rule and click the green ‘+’ icon that appears on the right.
5. Complete the Add Containment Rule to <class> form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Item Type</td>
<td>The CI class that the rule applies to.</td>
</tr>
<tr>
<td>Relationship Type</td>
<td>The relationship type for the rule.</td>
</tr>
<tr>
<td>Reverse Relationship Direction</td>
<td>Enable to use the reverse relationship in the rule.</td>
</tr>
<tr>
<td>Always include in Service Model</td>
<td>Enable to always include the CIs of the specified class in the Service Map if their parent CI (based on the containment relationship) is present in the Service Map.</td>
</tr>
</tbody>
</table>

6. Click Create.
7. Add an endpoint to a child rule:
   a) Point to a child rule for which you want to add an endpoint.
   b) Click the blue “+” icon that appears on the right.
   c) Complete the Add Endpoint To <class> form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Type</td>
<td>The type of endpoint.</td>
</tr>
<tr>
<td>Inbound or Outbound</td>
<td>The direction of the endpoint.</td>
</tr>
</tbody>
</table>

   d) Click Create.

Create or edit a metadata hosting rule

Create metadata hosting rule for CIs to assist in correctly identifying dependent CIs during the business discovery process and service mapping. Discovery calls the identification API that applies metadata rules.

A hosting rule is a relationship definition between two CIs, structured as: <CI Type1> <relationship type> <CI Type2>. To create a hosting rule, you need to add a CI type as <CI Type1> in the relationship rule, and then define the second portion of the relationship rule which is the
relationship type and <CI Type2>. The entire set of hosting rules is organized as groups according to the top-level hosted CIs.

A hosting rule implicitly contains two rules, which are the reversal of each other. When you create the rule '<CI Type1> <relationship type> <CI Type2>', the rule '<CI Type2> <reversed relationship type> <CI Type1>' is automatically added.

Role required: admin

1. Navigate to Configuration > CI Class Manager
2. Select a class (CI Type1) from the Class Hierarchy for which to create a hosting rule.
3. On the right, click Advanced, expand Correctness, and select CI Metadata Editor.
4. Select the Metadata Information tab, and use the Hosting Rules section.
5. Click Add New Rule to add a top-level rule. Or, point to a rule for which you want to add a child rule and click the green '+' icon that appears on the right.
6. Complete the Add Hosted/Hosting Rule to <class> form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Item Type</td>
<td>The &lt;CI Type2&gt; in the rule.</td>
</tr>
<tr>
<td>Relationship Type</td>
<td>The relationship type for the rule.</td>
</tr>
<tr>
<td>Reverse Relationship Direction</td>
<td>Check to reverse relationship in the rule.</td>
</tr>
</tbody>
</table>

7. Click Create.

Effective usage of CMDB Identification

Use CMDB Identification effectively for optimal accuracy and performance.

Identification rules

An independent identification rule identifies a CI based on the CI’s attributes, independently of other CIs.

A dependent identification rule identifies a CI by its dependent CIs and the relationships of the identified CI with those dependent CIs. Identification with a dependent identification rule is based on the dependent CIs and the relationships and qualifiers between the identified CI and its dependent CIs. Identification then requires more time than with an independent identification rule and is prone to some identification errors. Usage of dependent rules should therefore be minimized.

CI modeling determines which type of identification rules are required for proper CI identification.

Create identification rules using the following order of importance:

1. Independent identification rules — It is always preferable to create independent identification rules rather than dependent identification rules. When you model a CI, define the CI with a complete set of attributes that lend themselves to independent identification, eliminating the need to use additional CIs for identification.

2. Dependent identification rules — If it is necessary to create dependent identification rules, then define a single level of dependency. Two is the maximum number of dependency levels that is supported.

3. Avoid creating lookup identifier entries. The use of lookup identifier entry is highly discouraged for performance reasons. If unavoidable, ensure to first review class definitions and consider updates that allow usage of independent identification rules.
4. Limit the number of identifier entries within an identification rule, ideally to 1. A second
identifier entry reduces performance, as will each additional identifier entry.

5. Create strong identification rules in which the strongest identifier entries and related entries
are set with the highest priority.

6. Ensure that the identification rule is at the class level that it needs to be.

Payload

Create the payload using the following order of importance:

1. Payload size — Limit the number of CIs per payload to 500.
2. Avoid duplicate entries in the payload.

   Example: If an identification rule has a criterion attribute for the name field, then the following
   payload has duplicate items resulting in failure:

```javascript
var payload = {
  items: [{
    className:'cmdb_ci_linux_server',
    values: {
      name:'Win Server 200',
      ram:'2048'
    }
  },
  {
    className:'cmdb_ci_linux_server',
    values: {
      name:'Win Server 200',
      ram:'4096'
    }
  }
};
```

3. Do not pass system data such as the following in the payload.

```javascript
var payload = {
  items: [{
    className:'cmdb_ci_linux_server',
    values: {
      name:'Win Server 200',
      sys_domain:'global',
      sys_domain_path:'xyz',
      sys_updated_on:'2017-06-15 16:25:11',
      sys_mod_count:23
    }
  }
};
```

4. Provide the minimum necessary set of criterion attributes for each payload item, according to
what is specified in the corresponding identification rules.

5. When matching CIs, use CIs’ sysIds if available.

   • Example: Independent CI that needs to be updated — sysId is available.

```javascript
var payload = {
  items: [{
    className:'cmdb_ci_linux_server',
    values: {
      sys_id:'194876usytrr65378098',
      ram:'2048'
    }
  }
};
```
ServiceNow Jakarta Now Platform Capabilities

- Example: Dependent CI that needs to be inserted. Tomcat War CI depends on Tomcat CI, and Tomcat CI depends on Linux Server CI. SysIds for the Tomcat and the Linux CIs are available.

```javascript
var payload = {
  items: [{
    className: 'cmdb_ci_app_server_tomcat_war',
    values: {
      name: 'war1',
      short_description: 'my description'
    }
  }, {
    className: 'cmdb_ci_app_server_tomcat',
    values: {
      sys_id: '194876usytrr65378098'
    }
  }, {
    className: 'cmdb_ci_linux_server',
    values: {
      sys_id: '09876tysueyt6345lakiu'
    }
  }],
  relations: [{
    parent: 1,
    child: 0,
    type: 'Contains::Contained by'), {
    parent: 1,
    child: 2,
    type: 'Runs on::Runs'
  }]
};
```

- Example: Dependent CI that needs to be updated — sysId is available.

```javascript
var payload = {
  items: [{
    className: 'cmdb_ci_app_server_tomcat_war',
    values: {
      sys_id: '039387euey637465sytet',
      short_description: 'my description new'
    }
  }]
};
```

6. When inserting many CIs, all of which depend on the same CI, you should serialize your API calls. Otherwise, attempting to concurrently process many CIs can clog the system, significantly degrading overall system performance.

Installed with Identification and Reconciliation

CMDB Identification and Reconciliation adds tables, properties, and script includes.

Tables installed with Identification and Reconciliation

Identification and Reconciliation uses the following tables.
<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier (cmdb_identifier)</td>
<td>Identification rule sets defined for different classes of CIs.</td>
</tr>
<tr>
<td>Reconciliation Definition (cmdb_reconciliation_definition)</td>
<td>Reconciliation rules defined for different classes of CIs at the table and field level.</td>
</tr>
<tr>
<td>Identifier Entry (cmdb_identifier_entry)</td>
<td>Rule entries with different priorities assigned to each identifier.</td>
</tr>
<tr>
<td>Data Source Precedence (cmdb_datasource_precedence)</td>
<td>Priorities of data sources that are authorized to update the same CI types or CI type with same sets of attributes.</td>
</tr>
<tr>
<td>Duplicate Audit Result (duplicate_audit_result)</td>
<td>Duplicate audit results corresponding to a specific duplicate task. These results are generated automatically during the identification process and should not be added manually.</td>
</tr>
<tr>
<td>Reconcile Duplicate Task (reconcile_duplicate_task)</td>
<td>Task to address duplication that is detected during the identification process. Records are generated automatically, and users should not add records manually.</td>
</tr>
<tr>
<td>Reclassification Task (reclassification_task)</td>
<td>Reclassification tasks that were generated during the identification process.</td>
</tr>
<tr>
<td>Data Source History (cmdb_datasource_last_update)</td>
<td>Information about the last data source that updated each attribute. Used to determine if a data source can update a stale CI.</td>
</tr>
<tr>
<td>Data Source Staleness Definition (cmdb_datasource_staleness)</td>
<td>Effective duration per data source. When effective duration is exceeded, then CMDB Health determines that the information provided by that data source is stale.</td>
</tr>
<tr>
<td>Identification Engine Context (cmdb_ie_context)</td>
<td>Input payload, and data source (cmdb_ci’s discovery_source) that will be used as input for a specific identification engine API. Also information about which specific identification engine API will be called (identifyCI or createOrUpdateCI API). <strong>Note:</strong> Internal table used by identification simulation.</td>
</tr>
<tr>
<td>Identification Engine Run (cmdb_ie_run)</td>
<td>Specific cmdb_ie_context record that was used to run against the identification engine. Also details about the output payload returned by APIs, such as start and end time of the run and whether the run was successful. <strong>Note:</strong> Internal table used by identification simulation.</td>
</tr>
</tbody>
</table>
### Identification Engine Log (cmdb_ie_log)

Identification engine logs for a specific cmdb_ie_run simulated in the identification simulation. Also details about logs level and order.

**Note:** Internal table used by identification simulation.

### Properties installed with Identification and Reconciliation

Identification and Reconciliation uses the following properties. Updating these properties requires users to have the admin role.

**Note:** To open the System Property (sys_properties) table, enter `sys_properties.list` in the navigation filter.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.required.attribute.enabled</td>
<td>Flag for enforcing required attributes during identification and reconciliation so that attributes cannot be null.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Type:</strong> true</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default value:</strong> true</td>
</tr>
<tr>
<td></td>
<td>• <strong>Location:</strong> System Properties (sys_properties) table.</td>
</tr>
</tbody>
</table>

| glide.class.upgrade.enabled      | Flag for allowing class upgrade during identification and reconciliation. |
|                                  | • **Type:** true | false  |
|                                  | • **Default value:** true  |
|                                  | • **Location:** System Properties (sys_properties) table.  |

| glide.class.downgrade.enabled    | Flag for allowing class downgrades during identification and reconciliation. |
|                                  | • **Type:** true | false  |
|                                  | • **Default value:** true  |
|                                  | • **Location:** System Properties (sys_properties) table.  |

<p>| glide.class.switch.enabled       | Flag for allowing class switching during identification and reconciliation. |
|                                  | • <strong>Type:</strong> true | false  |
|                                  | • <strong>Default value:</strong> true  |
|                                  | • <strong>Location:</strong> System Properties (sys_properties) table.  |</p>
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| glide.reconciliation.override.null | Flag for allowing the update of an empty field by a lower priority data source.  
  - **Type**: true | false  
  - **Default value**: true  
  - **Location**: System Properties (sys_properties) table. |
| glide.identification_engine.skip_duplicates | Controls how identification processes a small set of duplicate CIs.  
  - When true: If the number of duplicate CIs is less than the threshold specified by glide.identification_engine.skip_duplicates.threshold, then the oldest of the duplicate CIs is picked as a match and gets updated. For the rest of the duplicate CIs, the CMDB_CIs' discovery_source field is set to 'Duplicate'.  
  - When false: Matching a CI fails, and an error is logged.  
  - **Type**: true | false  
  - **Default value**: true  
  - **Location**: Add to the System Properties (sys_properties) table. |
| glide.identification_engine.skip_duplicates.threshold | The 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.  
  - **Type**: Integer  
  - **Default value**: 5  
  - **Location**: Add to the System Properties (sys_properties) table. |
| glide.cache.size.service_cache | The max cache size (in MB) that is used by the identification engine for inbound and outbound relations. When the limit is reached, the least recently used cached data is discarded, releasing space for new data.  
  - **Note**: You cannot disable the service cache.  
  - **Type**: Integer  
  - **Default value**: 20  
  - **Location**: Add to the System Properties (sys_properties) table. |
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| glide.identification_engine.distributed_locking | By default, identification/reconciliation processes acquire a global lock. Enable this property to allow acquiring mutex lock faster, and at a more granular level. This lock optimization is mostly beneficial for scenarios with update operations rather than insert operations.  
  - **Type**: true | false  
  - **Default value**: false  
  - **Location**: System Properties (sys_properties) table. |
| glide.identification_logs.max_run_ids | Determines how many log runs can be displayed when navigating to Configuration > Identification Logs.  
  - **Type**: integer  
  - **Default value**: 1000  
  - **Location**: System Properties (sys_properties) table. |
| glide.cmdb.logger.source.identification_engine | Enable and configure what type of details the system logs when using IRE outside the scope of identification simulation. For example, when using an API, ECC queue or scheduled jobs.  
  - **Type**: string  
  - **Values**: info, warn, error, debug, or debugVerbose  
  - **Location**: Add to System Properties (sys_properties) table. |

### Script includes installed with Identification and Reconciliation

Identification and Reconciliation uses this script include.

<table>
<thead>
<tr>
<th>Script include</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMDBTransformUtil</td>
<td>Performs identification and reconciliation.</td>
</tr>
</tbody>
</table>

### Examine identification engine run logs

Applications that use the identification engine (such as Discovery) can provide a URL to viewing identification engine run logs. To view results and for debugging purposes, you can use these links to examine the details of logs generated by the identification engine for payload runs.

**Role required**: admin

These URLs link to a central page where the identification engine payload output logs appear in a user friendly format. Logging is in the context of a specific run of the identification engine, and you can filter the log list by a specific data source and time range. Up to 1000 run logs that are up to 2 months old appear, grouped by Context IDs, and run times. You can use the glide.identification_logs.max_run_ids system property to modify the 1000 limit.
You can control the logging level by using the `glide.discovery.identification.log_level` Discovery system property, setting the value to one of the following:

- Info
- Warn
- Error
- Debug
- DebugVerbose
- DebugObnoxious

1. Navigate to Configuration > Identification/Reconciliation > Identification Logs.
2. Filter the runs list as follows:
   a) **Source**: Select the data source for which to display run logs.
   b) **Time Range**: Specify a time range for which to display run logs.

The Runs list displays all runs for the specified data source, during the specified time range.

3. In the Runs list, click a Run # to display its Context ID and Run ID.
   A unique Context ID is associated with each specific payload that is run. Each run of that payload, is associated with a unique Run ID. A single Context ID for a payload that is run multiple times is associated with multiple Run IDs.

4. Click the drop down arrow for a Run # to display additional details.
   - **Input**: Displays the payload for the run.
   - **Logs**: Displays all the logged messages that the identification engine generated while running the payload, according to the specified logging level.
   - **Output**: Displays the output payload returned by the identification engine.

**Identification engine error messages**

The identification engine generates the following errors, which are displayed in the Identification Logging pane and in the system logs.

For information about lookup-based CI identification and qualifier chains, see [Create or edit a CI identification rule](#).

**Error: IDENTIFICATION_RULE_MISSING**

<table>
<thead>
<tr>
<th>Message</th>
<th>Description and Resolution</th>
</tr>
</thead>
</table>
| Identity Rule Missing for table (xyz) | **Description:**
|                        | Identification rule is missing for a class. |
|                        | **Resolution:**
|                        | Ensure that there is an identification rule for table (xyz), and that the rule is active. |
### MISSING_MATCHING_ATTRIBUTES

<table>
<thead>
<tr>
<th>Message</th>
<th>Description and Resolution</th>
</tr>
</thead>
</table>
| In payload missing minimum set of input values for criterion (matching) attributes from identify rule for table (xyz). Add these input values in payload item 'abc' | Description: Missing minimum set of values for criterion attributes for an identification rule.  
Resolution: In the payload, add minimum set of values for criterion attributes for CI Identifier for table (xyz). Open the CI Class Manager, click Hierarchy and select the (xyz) class. Check the identification rule and the identifier entries for table (xyz). |

### Error: NO_CLASS_NAME_FOR_INDEPENDENT_CI

<table>
<thead>
<tr>
<th>Message</th>
<th>Description and Resolution</th>
</tr>
</thead>
</table>
| Cannot have 'sys_class_name' as a key field in an Independent Identity Rule on xyz | Description: The class attribute was added to the CI identifier which is not supported.  
Resolution: Remove the class attribute from CI Identifier for table (xyz). |

### Error: IDENTIFICATION_RULE_FOR_LOOKUP_MISSING

<table>
<thead>
<tr>
<th>Message</th>
<th>Description and Resolution</th>
</tr>
</thead>
</table>
| Identity Rule for table (xyz) missing Lookup Rule for class (abc)       | Description: The payload has a lookup class name, but the corresponding lookup rule is missing.  
Resolution: Add lookup identifier entry with (Search on table) as (abc) for CI Identifier for table (xyz). |
### Error: IDENTIFICATION_RULE_FOR_RELATED_ITEM_MISSING

<table>
<thead>
<tr>
<th>Message</th>
<th>Description and Resolution</th>
</tr>
</thead>
</table>
| Identity Rule for table (xyz) missing Related Rule for class (abc) | **Description:** The payload has a related class name, but the corresponding related rule is missing.  
**Resolution:** Add related entry with (Related table) as (abc) within CI Identifier for table (xyz). |

### Error: NO_LOOKUP_RULES_FOR_DEPENDENT_CI

<table>
<thead>
<tr>
<th>Message</th>
<th>Description and Resolution</th>
</tr>
</thead>
</table>
| Cannot have Lookup Rule for a Dependent Identity Rule on (xyz) | **Description:** Cannot have Lookup Rule for a Dependent Identity Rule.  
**Resolution:** Remove lookup identifier entry from dependent CI Identifier for table (xyz). |
Error: INVALID_INPUT_DATA

<table>
<thead>
<tr>
<th>Message</th>
<th>Description and Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Found invalid sys_id in payload. No record with sys_id (xyz) exist in table (abc)</td>
<td>Description: The payload has a reference to an invalid sys_id. Resolution: Remove the referenced sys_id, or provide a valid sys_id.</td>
</tr>
<tr>
<td>In payload no data source exist. You need to provide choice value from choice field (discovery_source) in table (cmdb_ci)</td>
<td>Description: In payload no data source exists. Resolution: In the payload, provide a valid choice value from choice field (discovery_source) from table (cmdb_ci).</td>
</tr>
<tr>
<td>In payload invalid data source (xyz) exist. You need to provide a valid choice value from field (discovery_source) in table (cmdb_ci)</td>
<td>Description: The payload contains an invalid data source. Resolution: In the payload, provide a valid choice value from choice field (discovery_source) from table (cmdb_ci).</td>
</tr>
<tr>
<td>No such relationship with name (xyz) exist in table (cmdb_rel_type). If out-of-box relationship for (xyz) has been removed or renamed, it should be restored</td>
<td>Description: The payload is referencing a relationship that does not exist in the (cmdb_rel_type) table. Resolution: Verify that the reference to the relationship is accurate. Or, if it is a new relationship, add it to the (cmdb_rel_type) table. Or, if out-of-box relationship for (xyz) has been removed or renamed, restore it.</td>
</tr>
<tr>
<td>Payload relations 'xyz' has invalid parent record index: (0)</td>
<td>Description: Payload references invalid parent indexes. Resolution: Check payload indexes and ensure that they are all valid.</td>
</tr>
<tr>
<td>Payload relations 'xyz' has invalid child record index: (0)</td>
<td>Description: Payload references invalid child indexes. Resolution: Check payload indexes and ensure that they are all valid.</td>
</tr>
<tr>
<td>The record with sys_id (xyz) in table (abc) is a duplicate record and has (discovery_source) field marked as Duplicate.</td>
<td>Description: The payload has a reference to an invalid sys_id.</td>
</tr>
</tbody>
</table>
Error: DUPLICATE_RELATIONSHIP_TYPES

<table>
<thead>
<tr>
<th>Message</th>
<th>Description and Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duplicate relationship type records exists with name ( xyz ) in table {cmdb_rel_type} having sys_ids: ( abc )</td>
<td>Description: There are duplicate records in the {rel_ci_type} table for the relationship.</td>
</tr>
<tr>
<td></td>
<td>Resolution: Remove the duplicate records.</td>
</tr>
</tbody>
</table>

Error: DUPLICATE_PAYLOAD_RECORDS

<table>
<thead>
<tr>
<th>Message</th>
<th>Description and Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Found duplicate items in the payload (index 0 and 1), using className ( xyz ) and fields ( abc ). Remove duplicate items from payload</td>
<td>Description: The payload contains two items whose criterion attributes have identical values.</td>
</tr>
<tr>
<td></td>
<td>Resolution: Remove one of the duplicate items.</td>
</tr>
</tbody>
</table>

Error: LOCK_TIMEOUT

<table>
<thead>
<tr>
<th>Message</th>
<th>Description and Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed to acquire synchronization lock for ( xyz )</td>
<td>Description: Failed to acquire the system mutex lock.</td>
</tr>
<tr>
<td></td>
<td>Resolution: Increase the mutex expiration time by adding the system property \texttt{glide.identification_engine.mutex_expiration_time} and setting to an integer value that is greater than the default value (15 min).</td>
</tr>
</tbody>
</table>
## Error: MULTIPLE_DUPLICATE_RECORDS

<table>
<thead>
<tr>
<th>Message</th>
<th>Description and Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Found duplicate records in table (xyz) using fields (abc)</td>
<td><strong>Description:</strong> Found duplicate records in the specified table.</td>
</tr>
<tr>
<td></td>
<td><strong>Resolution:</strong> Fix the duplicate records found by the identification engine. Check de-duplication tasks for information about all duplicates.</td>
</tr>
</tbody>
</table>

## Error: REQUIRED_ATTRIBUTE_EMPTY

<table>
<thead>
<tr>
<th>Message</th>
<th>Description and Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missing mandatory field (xyz) in table (abc). Add input value for mandatory field in payload</td>
<td><strong>Description:</strong> A required attribute is missing in the payload.</td>
</tr>
<tr>
<td></td>
<td><strong>Resolution:</strong> In the payload, add input value for mandatory field (xyz) in table (abc).</td>
</tr>
</tbody>
</table>

## Error: MISSING_DEPENDENCY

<table>
<thead>
<tr>
<th>Message</th>
<th>Description and Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>In payload no relations defined for dependent class (xyz) that matches any containment/hosting rules: (abc). Add appropriate relations in payload for def</td>
<td><strong>Description:</strong> No relations defined for the dependent class that matches any of its metadata rules.</td>
</tr>
<tr>
<td></td>
<td><strong>Resolution:</strong> In payload add appropriate relations for dependent class (xyz) that matches any containment/hosting rules: (abc).</td>
</tr>
</tbody>
</table>
### Error: METADATA_RULE_MISSING

<table>
<thead>
<tr>
<th>Message</th>
<th>Description and Resolution</th>
</tr>
</thead>
</table>
| No containment or hosting rules defined for dependent class *(xyz)*. Add containment/hosting rules for `abc`. | **Description:**
  There are no containment or hosting rules defined for dependent class.

  **Resolution:**
  Add containment or hosting rules for dependent class *(xyz).* |

### Error: MULTIPLE_DEPENDENCIES

<table>
<thead>
<tr>
<th>Message</th>
<th>Description and Resolution</th>
</tr>
</thead>
</table>
| Found multiple dependent relation items *(xyz)* and *(abc)* in payload. | **Description:**
  Multiple dependent relation items exist.

  **Resolution:**
  Remove one of the multiple dependent relation items *(xyz)* or *(abc).* |

| Multiple paths leading to the same destination: `xyz -> abc`.           | **Description:**
  Multiple paths leading to the same destination.

  **Resolution:**
  Remove duplicate relationship/qualifier chains that might exists between `xyz -> abc`. |
## Error: ABANDONED

<table>
<thead>
<tr>
<th>Message</th>
<th>Description and Resolution</th>
</tr>
</thead>
</table>
| Abandoning processing payload item `xyz`, since its depends on payload item `abc` has errors | **Description:**  
Dependent payload item has errors, so abandoning processing.  
**Resolution:**  
Resolve the error on the dependent payload item `abc`. |
| Can’t find matched record with sys_id `(xyz)` in table `(abc)` | **Description:**  
Matched sys_id does not exist in the corresponding table.  
**Resolution:**  
Check in table `(abc)` whether matched record is a valid record based on input payload. |
| Identification engine API got called recursively, aborting... | **Description:**  
The Identification engine API was called recursively.  
**Resolution:**  
Avoid calling the Identification engine API recursively. |
| Detected error while processing payload from `xyz` | **Description:**  
Error occurred during processing payload.  
**Resolution:**  
Resolve all errors mentioned in the output payload from `xyz`. |
| While processing relations encountered errors in payload item: `xyz` | **Description:**  
Payload item has errors.  
**Resolution:**  
Resolve errors in payload item `xyz`. |
| Error occurred during parsing input json payload: `xyz` | **Description:**  
Error occurred during parsing JSON payload.  
**Resolution:**  
Ensure that input JSON payload has correct JSON format. |
## Error: MULTI_MATCH

<table>
<thead>
<tr>
<th>Message</th>
<th>Description and Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duplicate dependent records found having relationship ( xyz ) with same CI (className: ( abc ), sysId: ( def ))</td>
<td>Description: Found duplicate dependent CIs.</td>
</tr>
<tr>
<td></td>
<td>Resolution: Check de-duplication tasks for information about all duplicates, and then delete duplicate records.</td>
</tr>
<tr>
<td>Found multiple relations between payload items: ( xyz ) and ( abc )</td>
<td>Description: Found multiple relations between payload items.</td>
</tr>
<tr>
<td></td>
<td>Resolution: Check for duplicate relationship chains and qualifier chains that might exist.</td>
</tr>
<tr>
<td>Found duplicate records in lookup table ( xyz ) using fields ( abc ) and reference field ( def )</td>
<td>Description: Found duplicate records in lookup table.</td>
</tr>
<tr>
<td></td>
<td>Resolution: Check de-duplication tasks for information about all duplicates, and then delete duplicate records.</td>
</tr>
</tbody>
</table>

## Error: QUALIFICATION_LOOP

<table>
<thead>
<tr>
<th>Message</th>
<th>Description and Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qualification chain has loop that contains relation ( xyz )</td>
<td>Description: Qualification chain has a loop.</td>
</tr>
<tr>
<td></td>
<td>Resolution: Remove the loop from the qualification chain with relation ( xyz ).</td>
</tr>
</tbody>
</table>
**Error: TYPE_CONFLICT_IN_QUALIFICATION**

<table>
<thead>
<tr>
<th>Message</th>
<th>Description and Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid payload, qualification chain has multiple possible paths for payload items: ‘xyz’ and ‘abc’</td>
<td>Description: Multiple qualification paths found. Resolution: Remove multiple possible qualification paths between items ‘xyz’ and ‘abc’.</td>
</tr>
</tbody>
</table>

**Error: RECLASSIFICATION_NOT_ALLOWED**

<table>
<thead>
<tr>
<th>Message</th>
<th>Description and Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>CI Reclassification not allowed from class: (xyz) to (abc)</td>
<td>Description: CI reclassification not allowed. Resolution: Check reclassification tasks for information about reclassification, and check if reclassification from class: (xyz) to (abc) is valid.</td>
</tr>
</tbody>
</table>

**Error: DUPLICATE_RELATED_PAYLOAD**

<table>
<thead>
<tr>
<th>Message</th>
<th>Description and Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Found duplicate Related items (0 and 1) in the payload index 1 using fields xyz</td>
<td>Description: Duplicate Related items present. Resolution: Remove one of the duplicate related items present in the payload.</td>
</tr>
</tbody>
</table>

**Error: DUPLICATE_LOOKUP_PAYLOAD**

<table>
<thead>
<tr>
<th>Message</th>
<th>Description and Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Found duplicate Lookup items (0 and 1) in the payload index 1 using fields xyz</td>
<td>Description: Duplicate lookup items present. Resolution: Remove one of the duplicate lookup items present in the payload.</td>
</tr>
</tbody>
</table>
CMDB Health

Monitoring and maintaining the health of the CMDB is essential to an effective and continuous use of the product. Health indicators such as duplicate CIs, required CI fields, and audits contribute to the calculation of health scorecards at the CI, class, and CMDB level.

The health of the CMDB data is monitored and reported for the following KPIs, each further consisting of sub metrics:

- Completeness: CIs are tested for required and recommended fields that are not populated.
- Correctness: CIs are tested against pre-defined data integrity rules such as identification rules, orphan CI rules, and stale CI rules.
- Compliance: The CMDB data is audited for adherence to pre-defined certificates.
- Relationships: The health of CI relationships is tested for indicators such as orphan and duplicate relationships. And for compliance with suggested relationships, hosting and containment rules.

After CIs are tested for various health indicators, the results are aggregated at the class level, and eventually at the overall CMDB level. You can configure how health is calculated and the weight of each KPI and each metric at every level of the aggregation. For most health tests, you can configure the health tests themselves.

CMDB Health is domain aware. If the domain separation plugin has been activated, then the CMDB dashboard displays health based on data, rules, and settings from the logged-on user domain. If rules and settings are not defined for a child domain, then the parent’s settings are applied, recursively.

CI remediation

CMDB Health provides a framework for configuring CI remediation. Remediation lets you proactively apply corrective actions to unhealthy CIs in a managed and standardized fashion.

Setup

You need to configure CMDB Health related system properties and health KPI and metric rules to customize how aggregated data is calculated, and other CMDB Health behavior. To start gathering and aggregating health data, you need to enable the CMDB Health-related jobs (CMDB Health Dashboard jobs) which are initially disabled. See Setup and configure CMDB Health for details about enabling these jobs and about configuring other CMDB Health settings.

Setup and configure CMDB Health

The data collection system is highly configurable, however, the base system is minimally configured for aggregating CMDB health data. Most importantly, the CMDB Health Dashboard jobs are disabled by default and data is not collected. To display valuable and meaningful data, you should review and adjust settings.

1. Review CMDB health KPIs and metrics to learn what CMDB Health can monitor, and what needs to be configured to enable and support each metric.
2. For each KPI and associated metric that you want monitored, define the necessary rules and fulfill other needed requirements. For example, create orphan rules for detecting orphan records, if you are interested in this metric.
3. Review and adjust the threshold ranges for best, at risk, and critical states for the CMDB health metrics scorecards - see Configure CMDB health scorecard thresholds.
4. Set metric aggregation preferences, deactivate KPI and metrics that you are not interested in reporting, set failure thresholds, and adjust weighted averages of aggregation - see Configure KPI and metrics aggregation preferences.

5. Narrow the scope of CIs that are included in health calculations - see Create health inclusion rule.

6. Enable the Health Dashboard jobs for the KPIs that you want reported - see Enable and configure a CMDB Health Dashboard job.

7. Customize the CI dashboard (optional).

Guided setup

Alternatively, you can configure and get started with CMDB Health following a prescribed step-by-step in-product guidance:

1. Navigate to Guided Setup > ITOM Guided Setup and click Continue.
2. Scroll to Configuration (CMDB), and click Continue.
3. Scroll to CMDB Health and click Configure.

CMDB health system properties

Configure the following system properties to customize how CMDB health is monitored and evaluated.

Role required: itil_admin

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| Max time in minutes for which individual metric processor will run in each scheduled cycle (glide.cmdb.health.metricProcessor.maxRunningTime) | If processing of a metric exceeds the specified time, CMDB health processing halts until the next CMDB health job is scheduled to run.  
- **Type**: integer  
- **Default value**: 120  
- **Location**: Navigate to Configuration > Health Preference. In the right hand-side navigator, click System Properties. |

For performance reasons, it is recommended not to set this property to a value greater than 120.

**Note**: If you enter an invalid value, the default value is used.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.cmdb.logger.use_syslog.CMDBHealth</td>
<td>A comma separated list that controls the level of logging of CMDB health jobs. Logging creates entries in the system logs to capture messages generated by the health auditing process each time they run. This helps debugging in case of failure. For example, to log error and info messages, set the value to ‘error,info’. - <strong>Type</strong>: String - <strong>Default value</strong>: error - <strong>Other possible values</strong>: Comma separated list with any of the following values: · info · error · warn Or ‘*’ which is equivalent to including all possible values. - <strong>Location</strong>: System Property (sys_properties) table.</td>
</tr>
</tbody>
</table>

Enable and configure a CMDB Health Dashboard job

Enable and configure the jobs that process CMDB health tests, to start calculating CMDB health scores for the **completeness**, **compliance**, **correctness**, and **relationship** KPI. These health scores are then aggregated into the overall CMDB health report.

**Role required**: admin

In the base system, CMDB Health Dashboard jobs are disabled by default. Enable and configure the respective job for the CMDB health KPI that you want data collected and aggregated for. You can schedule a job to run on a recurring schedule, or execute it once at any time.

1. **Navigate to** Configuration > CMDB Dashboard > CMDB View, and then click CMDB Health Dashboard Jobs.
2. **Select a job** that you want to enable or configure.

<table>
<thead>
<tr>
<th>CMDB Health Dashboard job</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMDB Health Dashboard - Completeness Score Calculation</td>
<td>Script for calculating the completeness KPI of CMDB health.</td>
</tr>
<tr>
<td>CMDB Health Dashboard - Compliance Score Calculation</td>
<td>Script for calculating the compliance KPI of CMDB health.</td>
</tr>
<tr>
<td>CMDB Health Dashboard - Correctness Score Calculation</td>
<td>Script for calculating the correctness KPI of CMDB health.</td>
</tr>
<tr>
<td>CMDB Health Dashboard - Relationship Score Calculation</td>
<td>Script for calculating the CI relationships KPI of CMDB health.</td>
</tr>
<tr>
<td>CMDB Health Dashboard - Relationship Compliance Processor</td>
<td>Script for calculating compliance of relationships with suggested relationships, and with hosting and containment rules.</td>
</tr>
</tbody>
</table>

3. **Review** the default configuration, and update as necessary.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Job name. It is recommended that you do not modify the job’s name.</td>
</tr>
<tr>
<td>Active</td>
<td>Select to activate the job.</td>
</tr>
<tr>
<td>Run</td>
<td>Configure recurring schedule of job execution, or select On Demand.</td>
</tr>
<tr>
<td>Time</td>
<td>If Active is selected, set the time (hour, minute, and second) to run the job.</td>
</tr>
<tr>
<td>Conditional</td>
<td>If selected, the scripted condition must evaluate to true before the job can run.</td>
</tr>
<tr>
<td>Run this script</td>
<td>The job’s script. Modifications to the script are not recommended.</td>
</tr>
</tbody>
</table>

4. Click **Execute Now** to run the job once immediately.

After you enable a CMDB Health Dashboard job, the results for the KPI are aggregated and displayed in the CMDB dashboard and CI dashboard, at the CMDB, class, and CI levels.

**Configure CMDB health scorecard thresholds**

Configure the thresholds for best, at risk and critical state definitions for the KPIs and metrics scorecards. You can configure these settings globally for the entire CMDB, or individually per class.

**Role required:** itil_admin (on top of itil)

Scorecard thresholds are used to determine overall metric state, and are defined by upper and lower thresholds:

- 0 - lower threshold: Best state
- Lower threshold - upper threshold: At risk state
- Upper threshold - 100: Critical state

In the base system, for all KPIs and metrics upper thresholds are set to 67 and lower thresholds are set to 33. You can adjust scorecard thresholds to reflect the range of failures that should be used for each health state.

For CMDB groups, you can specify a separate set of scorecard thresholds, per CMDB group/KPI or metric. See **Configure CMDB groups scorecard thresholds** for more details.

1. Navigate to **Configuration > CI Class Manager**.
2. In the CI Class Manager expand the **Class Hierarchy**:
   - To configure thresholds for the completeness, correctness and compliance KPIs, select the top-level **Configuration Item** class. When you select the top-level Configuration Item class, threshold settings to any scorecard apply to the entire class hierarchy.
   - To configure thresholds for a specific class, select that class from the list.
3. Check **Advanced** on the right-hand side bar. Expand **Correctness** and all other strip headers to display all scorecards.
4. Select a scorecard such as **Required Fields Scorecard** or **CMDB Correctness Scorecard**.
5. Double-click an existing scorecard to edit (such as the scorecard for the cmdb_ci class), or click **New** to create scorecard thresholds only for the selected class.

If you select the global metric for the cmdb_ci class, the threshold setting will apply to the entire class hierarchy.
6. Slide the threshold sliders, or enter specific numbers to increase or to decrease the threshold bars to fit your definitions for best, at risk, and critical levels for the scorecard.

7. Click Save.

Configure CMDB groups scorecard thresholds

Each CMDB group can have its unique set of scorecard thresholds for best, at risk, and critical state definitions for specific KPIs or metrics.

Role required: itil_admin (on top of itil)

Scorecard thresholds are used to determine overall metric state, and are defined by upper and lower thresholds:

- 0 - lower threshold: Best state
- Lower threshold - upper threshold: At risk state
- Upper threshold - 100: Critical state

In the base system, for all KPIs and metrics, upper thresholds are set to 67 and lower thresholds are set to 33. You can adjust scorecard thresholds for a specific CMDB group per KPI or metric, to reflect the range of failures that should be used in health reporting.

CMDB groups scorecard thresholds are stored in the (cmdb_health_scorecard_group_threshold) table.

1. In the search box in the navigation bar, enter cmdb_health_scorecard_group_threshold.list and press the Enter key.

2. In the CMDB Health Group Scorecard Thresholds list, click New.

3. Fill out the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upper threshold</td>
<td>Upper range of percentage of CIs failing the specified metric tests, that is used to calculate best and at risk states.</td>
</tr>
<tr>
<td>CMDB Group</td>
<td>The CMDB group to which this scorecard threshold setting applies to.</td>
</tr>
<tr>
<td>Lower threshold</td>
<td>Lower range of percentage of CIs failing the specified metric tests, that is used to calculate at risk and critical states.</td>
</tr>
<tr>
<td>Metric</td>
<td>The metric to which the scorecard threshold setting applies to.</td>
</tr>
</tbody>
</table>

4. Click Submit.

Configure KPI and metrics aggregation preferences

Metrics health scorecards are aggregated into their respective KPI, which in return are aggregated into the overall CMDB Health report. Set aggregation preferences for KPIs, and for each of their respective metrics, deactivate KPIs and metrics that you are not interested in reporting, and adjust weighted averages of aggregation.

To start collecting and reporting CMDB health KPIs and metrics, you must first enable and configure the CMDB health dashboard jobs.

Role required: itil_admin (on top of itil)

The completeness KPI for example, consists of the metrics required fields and recommended fields, each contributing a different weight to the sum. You can configure the proportional weight
of required fields and recommended fields within completeness to be 25 and 75 respectively. You can also configure the proportional weight of completeness, compliance and correctness within the aggregated sum of the overall CMDB health.

Note: Non-active KPI or metrics are displayed on the CMDB dashboard in faded coloring, displaying the most recent aggregations that were calculated when the KPI or metric was active.

If Domain Support - Domain Extensions is activated, then you can configure aggregation preferences per domain.

In the ServiceNow base system, the weights of KPIs have default settings, and metrics are globally set.

1. Navigate to Configuration > Health Preferences.
2. Select Health Metrics on the right-hand side navigator.
3. From the Select Metric list select one of the KPIs such as Completeness, or a metric.
   For Completeness, Compliance and Correctness:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Activate the KPI so it is included in the aggregated CMDB health report.</td>
</tr>
<tr>
<td>Weighted Averages</td>
<td>Specify the weight of each metric in the aggregated KPI health report. The sum of weighted averages of all metrics should be 100.</td>
</tr>
</tbody>
</table>

For a metric:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Activate the metric so it is included in the aggregated health report for the respective KPI.</td>
</tr>
<tr>
<td>Create Task</td>
<td>If a record fails the metric test, create a task with details about the failure. You can then view the task on the CI dashboard, and configure remediation for the task.</td>
</tr>
<tr>
<td>Failure Threshold</td>
<td>When the threshold number of CIs that fail the health metric test is reached, health processing stops for the metric for this cycle.</td>
</tr>
<tr>
<td>Task Assignee Group</td>
<td>An assignment group for the task.</td>
</tr>
</tbody>
</table>

4. Click Save.

Set a CI field to be mandatory

Configure a CI field as mandatory so it is included in the CMDB Health tests for the required metric if enabled. **Required** is a metric of the CMDB Health completeness KPI.

When a field is configured as mandatory, then if the required metric is enabled, the CMDB health tests check whether that field is populated or not. The CMDB dashboard displays the aggregated report of the percentage of CIs for which one or more required fields is empty.

1. Navigate to Configuration > CI Class Manager.
2. Select a class from the Class Hierarchy.
3. Select **Fields** on the right-side bar.
4. In the **Table Columns** tab, select a table column.
5. In the **Dictionary Entry** form, select the **Mandatory** check box.
6. 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.

---

**Note:** Mandatory fields are global. The field is marked as mandatory everywhere it appears in a form.

---

### Set a CI field to be recommended

You can define a list of CI fields as recommended, noting that it is desirable that they are populated by a data source such as Discovery. You can then configure the CMDB completeness KPI to include recommended fields in its aggregated health reports.

Use this for fields which should not be mandatory, but that might have useful information that the CI should have. For example, a field with information that might at some point help with diagnosis. Initially, a derived class is set with the recommended fields that are defined at the parent level. You can add or remove recommended fields for a derived class, setting it with its own recommended fields, without affecting the recommended fields at the parent or sibling levels. If all recommended fields for a derived class are removed, then the derived class automatically derives the recommended fields from its parent class.

1. Navigate to **Configuration > CI Class Manager**.
2. Select a class from the **Class Hierarchy**.
3. Check **Advanced** on the right-hand side bar, and select **Recommended Fields** from the **Completeness** group.
4. In the slushbucket move the fields that you want to designate as recommended, from the **Available** list to the **Selected** list.
5. Click **Save**.

### Create or edit a CMDB health orphan rule

Create an orphan rule to determine the percentage of orphan CIs in the CMDB. This sum is then aggregated into the correctness CMDB Health KPI, and weighed into the overall CMDB health report. Orphan rules are defined per class, and only a single orphan rule can be defined per class.

**Role required:** itil_admin (on top of itil)

In order for a CI to be considered an orphan CI, specify attributes that a CI must have, relationships that a CI should not have, or both. In the relationship conditions, you can either specify that the CI has no relationships, or a set of specific relationships that the CI does not have. An orphan rule can for example define that if a CI doesn’t have an owner or an asset, then it is considered an orphan CI.

1. Navigate to **Configuration > CI Class Manager**.
2. Select a class from the **Class Hierarchy**.
3. On the right-hand side navigation pane, check **Advanced**, expand the **Correctness** strip, and click **Orphan Rule**.
4. If an orphan rule exists for the selected class, double-click it to edit, or click **New**.
5. Complete or edit the form.
CMDB Health Orphan Rule form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>The class for which the orphan rule applies.</td>
</tr>
<tr>
<td>Attributes</td>
<td>Attribute conditions that a CI must satisfy to be considered an orphan CI. For example, the filter conditions in which both the Assigned to and the Owned by fields are empty, will identify the matching CIs as orphans.</td>
</tr>
<tr>
<td>Condition</td>
<td>And/Or operation between the Attributes conditions and the Relationship conditions.</td>
</tr>
<tr>
<td>Relationship</td>
<td>The relationship conditions that a CI must fail in order to be considered an orphan CI. To specify that a CI must have no relationships, choose Any Relation and Any Class respectively.</td>
</tr>
</tbody>
</table>

6. Click Submit or Update to save the rule.

Create or edit a CMDB Health staleness rule

If the staleness metric is in effect, then staleness rules are used to determine the percentage of stale CIs in the CMDB. This sum is then aggregated into the correctness KPI, and weighs into the overall CMDB health calculation. Staleness rules are defined per class.

Role required: itil_admin (on top of itil)

1. Navigate to Configuration > CI Class Manager.
2. Select a class from the Class Hierarchy.
3. On the right-hand side navigation pane, check Advanced, expand the Correctness strip, and click Staleness Rule.
4. If a staleness rule exists for the class, then double-click it to edit, or click New.
5. Complete or edit the CMDB Health Staleness Rule form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applies to</td>
<td>The class for which the rule applies.</td>
</tr>
<tr>
<td>Effective Duration</td>
<td>The time period that is used for the staleness test.</td>
</tr>
</tbody>
</table>

    If the CI was not updated (based on Updated sys_updated_on) within the specified time period - the CI is determined to be stale.

    If you enter a value with a prefix that is valid and a suffix that is not, such as 15 x - the valid portion of the value is used (’15’). If the entire value is invalid - the default value of 0 is used.

6. Click Submit or Update to save the rule.
Prepare a scripted audit for the compliance KPI

To include a scripted audit in CMDB Health compliance calculations, you need to update the audit's script so it captures the time that the audit ran last.

Role required: certification_admin

CMDB Health uses audits' Last run date to collect the results from the most recent complete audit run. These results are then aggregated into the CMDB Health compliance KPI. When scripted audits run, they do not register the runtime. Therefore, to include scripted audits in the compliance KPI health aggregation, you must update the audit script so it populates the Last run date field.

1. Create or edit a scripted audit.
2. On the Audit form, update the script in Run this script. Add the following code at the top of the script, just before the code that filters CIs:
   ```java
   SNC.CertificationProcessing().updateLastRunDate(current.sys_id);
   ```

Create health inclusion rule

You can narrow the scope of CIs that are included in health calculations by defining health inclusion rules. Health inclusion rules can be specified per domain.

Role required: itil_admin (on top of itil)

You can apply health inclusion rules only to the required, orphan, recommended, and staleness health metrics. Evaluation for these health metrics applies only to CIs that satisfy health inclusion rules. To narrow the scope of CIs that are included in the duplicate metric, use Identification inclusion rules.

Inheritance of health inclusion rules:

- If there are no health inclusion rules specified for a child class, then rules specified on a parent class are applied to the child class.
- If health inclusion rules are specified for a child class, then those rules take precedence over rules specified on a parent class.

In the base system, there are no predefined health inclusion rules, in which case all CIs are included in the CMDB Health calculations.

1. Navigate to Configuration > CI Class Manager.
2. Select Advanced and then click Health Inclusion Rules.
3. Select a class in the Class Hierarchy for which to edit or create the rule for.
4. In the CMDB Health Configuration page, click on an existing rule to edit, or click New.
5. On the Inclusion List page, select the metrics that the rule applies to. Move items in the Applies to metric slushbucket from the Available list to the Selected list.
6. Under All of these conditions must be met, specify the criteria that CIs must meet to be included in the evaluation for the specified health metrics.
7. Click Submit.

CMDB health KPIs and metrics

The overall CMDB health score consists of three Key Performance Indicators (KPIs) which are correctness, compliance and completeness, each further consisting of sub-metrics. Each KPI and metric is associated with a scorecard that determines its contribution to the aggregated health at the overall CMDB level, class, and CI level.
You can configure which KPIs and metrics are included in the aggregated calculation, and set their weight in the aggregation. In the base system, all KPIs and all metrics are included in the aggregated health report.

**Overall**

An aggregation of all three KPIs (correctness, completeness and compliance), according to their overall scorecard weight settings.

**Correctness**

A KPI which is an aggregation of the following metrics, according to the correctness scorecard weight settings.

**Orphan**

Measures the percentage of orphan CIs in the CMDB. A CI can become orphan if it was unintentionally left in the CMDB when it is no longer needed. A CI is determined to be orphan if:

- The CI satisfies the criteria in an orphan rule. This criteria checks for specific attributes that a CI must have, and for CIs that have no relationships or that don’t have specific relationships.
- Data is missing for the CI in its respective table, or in one of its parents’ table.

**Staleness**

Measures the percentage of stale CIs in the CMDB. A CI is stale if it was not updated within the Effective Duration time period that is specified in the staleness rule that applies to the class.

The base system includes a default staleness rule for the Configuration Item (cmdb_ci) class, which sets the Effective Duration time to 60 days. This rule applies to all extended CMDB classes, and can be overridden by class specific staleness rules defined by the user. To determine CI staleness, a staleness rule for the CI’s class is used if it exists, otherwise, the default staleness rule is used.

In addition, a relationship in which a stale CI is a parent or a child, is determined to be a stale relationship.

**Duplicate**

Measures the percentage of duplicate CIs in the CMDB using identification rules. Only independent CIs are evaluated for duplication. In a set of duplicate CIs, the count of duplicate CIs is the total number of CIs in the set, minus one. The detailed graphs for a duplicate set of CIs display all the CIs in the set.

**Completeness**

A KPI which is an aggregation of the following metrics, according to the completeness scorecard weight settings.

**Required**

Measures the percentage of CIs in which fields that are defined as mandatory, are not populated. Missing fields are tagged as incomplete noting that for this CI some information is missing. Required fields are equivalent to the fields that are specified as mandatory in the system dictionary.

**Recommended**
Measures the percentage of CIs in which fields that are set as recommended, are not populated. Out-of-box, no recommended fields are specified.

Compliance

Based on the results of actual CMDB audit runs.

Audit

Audit compares actual values of specified fields, against expected values defined in template and scripted audits. Based on the Last run date of audits, CMDB Health identifies the set of the most recent complete audit run, and uses those audit results. To pass the CMDB Health audit test, a CI must be in compliance with all audits for that CI. Create a compliance-type audit, for which the results are calculated into the CMDB Health compliance KPI.

When running scripted audits, the Last run date is not populated. Therefore, for the compliance KPI to include the results of a scripted audit, update the script in the audit to record the audit run time.

For more information, see Create an audit.

Relationships

Measures the health of CI relationships, consisting of the following metrics which are not-configurable:

Duplicate relationships

Relationships that have identical parent and child CIs, identical relationship type, and an identical port. Duplicate relationships are displayed per relationship type. In a set of duplicate relationships, the duplicate relationship count is the total number of duplicate relationships in the set, minus one. The detailed graphs for a duplicate set of relationships display all the relationships in the set.

Orphan relationships

A relationship that is missing either a parent CI, a child CI, or both.

Stale relationships

A relationship in which the parent CI or the child CI is a stale CI.

A single relationship can fail more than one health test. For example, a duplicate relationship can also be stale.

Also reports the following relationship-related summaries:

- Relations not compliant with suggested relations
- Relations not compliant with containment rules
- Relations not compliant with hosting rules

CMDB Health dashboards

CMDB dashboards display CMDB health reports and let you configure the CMDB health KPIs and metrics that CIs are evaluated for.
<table>
<thead>
<tr>
<th>Dashboard</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMDB Dashboard</td>
<td>Main CMDB health dashboard:</td>
</tr>
<tr>
<td><strong>Configuration &gt; CMDB Dashboard &gt; CMDB View</strong></td>
<td>• Overall CMDB and class level aggregated CI health. Aggregation is displayed from the metric level up to the overall CMDB level.</td>
</tr>
<tr>
<td></td>
<td>• Aggregated health for CI relationships, and its metrics.</td>
</tr>
<tr>
<td></td>
<td>• Displays the tasks that were generated for CIs that failed a health test.</td>
</tr>
<tr>
<td></td>
<td>• Drill down for each KPI to a detailed report of associated metrics, broken by class.</td>
</tr>
<tr>
<td></td>
<td>• Manage the CMDB Health Dashboard jobs.</td>
</tr>
<tr>
<td>CI Dashboard</td>
<td>Health reports at the CI level:</td>
</tr>
<tr>
<td><strong>&lt;CI form&gt; &gt; Dashboard</strong></td>
<td>• Pass/fail results for each metric, per CI.</td>
</tr>
<tr>
<td></td>
<td>• Displays incidents, changes, and other tasks affecting the CI, and business services affected by the CI.</td>
</tr>
<tr>
<td>CI Class Manager</td>
<td>Central location to manage CI classes and to configure CMDB health settings:</td>
</tr>
<tr>
<td><strong>Configuration &gt; CI Class Manager</strong></td>
<td>• Configure scorecard thresholds of all KPIs and associated metrics.</td>
</tr>
<tr>
<td></td>
<td>• Configure weight of KPIs and associated metrics in health aggregation.</td>
</tr>
<tr>
<td></td>
<td>• Manage rules and definitions that are used for health tests, such as orphan rules, audit certificates, and recommended fields rule.</td>
</tr>
<tr>
<td></td>
<td>• Explore the class hierarchy.</td>
</tr>
<tr>
<td></td>
<td>• Update and extend a CI class.</td>
</tr>
<tr>
<td></td>
<td>• Delete all records for a class.</td>
</tr>
<tr>
<td>CMDB Health Preferences</td>
<td>Central location for configuring CMDB Health settings:</td>
</tr>
<tr>
<td><strong>Configuration &gt; Health Preferences</strong></td>
<td>• Configure CMDB Health preferences.</td>
</tr>
<tr>
<td></td>
<td>• Manage the CMDB Health Dashboard jobs.</td>
</tr>
<tr>
<td></td>
<td>• Activate and configure weighted averages for KPIs and metrics.</td>
</tr>
<tr>
<td></td>
<td>• Set the maximum failure threshold for the KPIs.</td>
</tr>
<tr>
<td></td>
<td>• Configure creation of tasks for failed CIs.</td>
</tr>
<tr>
<td>CMDB Service Dashboard</td>
<td>Main CMDB service health dashboard:</td>
</tr>
<tr>
<td><strong>Configuration &gt; CMDB Dashboard &gt; Service View</strong></td>
<td>• Overall service aggregated health and detailed health for CIs per service. Aggregation is displayed from the metric level up to the overall services level.</td>
</tr>
<tr>
<td></td>
<td>• Displays the tasks that were generated for CIs in a service that failed a health test.</td>
</tr>
<tr>
<td></td>
<td>• Drill down for each KPI to a detailed report of associated metrics, broken by class.</td>
</tr>
<tr>
<td></td>
<td>• Manage the CMDB Health Dashboard jobs.</td>
</tr>
</tbody>
</table>
View CMDB health reports

The CMDB dashboard serves as a central location to view aggregated health reports for your CMDB at a glance which helps you understand the CMDB health status. Also, it provides functions to address health issues, and improve CMDB health.

The CMDB dashboard requires some configuration before it can display meaningful data. Once CMDB Health is configured and the CMDB Health Dashboard Jobs are enabled, the dashboard displays data that is automatically collected and calculated on a recurring schedule. The CMDB dashboard is based on the dashboard framework, and uses its capabilities. The CMDB dashboard is domain aware.

Using the CMDB dashboard requires the asset or itil role, and if the system property glide.cms.enable.responsive_grid_layout exists, then its value must be true. For more information, see Enable responsive dashboards.

Access the CMDB dashboard by navigating to Configuration > CMDB Dashboard > CMDB View.

On the CMDB dashboard:

- Click CMDB Health Dashboard Jobs to enable and manage the jobs that monitor and collect health data for CIs and CI relationships.
- Click the default CMDB Dashboard - CMDB View dashboard to list additional CMDB drill-in dashboards.

The CMDB dashboard has two viewing modes. Click CI Health or Relationship Health to toggle between them.

CMDB Health view

The CMDB Health view is the default view for the CMDB dashboard. It contains scorecards detailing the overall health of CIs in your CMDB, per health KPI and metric. Also, it contains useful reports showing a breakdown of any duplicate, orphan or stale CIs by class, and lists the top 10 incident, alert, and change generating CIs in the CMDB.

All the default widgets in the CI Class view can be filtered using the CMDB class hierarchy tree. Initially, the class hierarchy filter is set to the root class, Configuration Item (All). Click All to select a different class, filtering all widgets on the dashboard to display data only for the selected class and its child classes.

In each scorecard widget, the horizontal bar in the center and the % number are correlated, displaying the aggregated health summary for the KPI. Health results of associated metrics are displayed underneath, each contributing according to the configuration of the metric scorecard, and its threshold.

Except for the Overall health scorecard, you can drill into any widget in the CI Class view:
• In a scorecard widget: Click the large aggregated percent number or the health bar to drill into a more detailed dashboard for that KPI.
• In a charts widget: Click a bar to display a list of all the records that the bar represents.
• In lists: Click the ‘i’ icon to view a list of all the tasks or alerts related to the CI.

Relationship Health view

The Relationship Health view displays various scorecards for health indicators of CI relationships in your CMDB. It contains charts detailing any duplicate, orphan or stale relationships, broken down by relationship type. You can drill down these charts for further details.

Changing the CI Class selection while in the Relationship view has no effect on the data displayed in this view.

Color codes

Both, the CI class view and the relationship view, use color codes when displaying aggregated health status. The status definitions are based on each scorecard’s threshold limits that are defined in the CI Class Manager.

<table>
<thead>
<tr>
<th>Color code</th>
<th>Definition</th>
<th>Default threshold setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Best</td>
<td>Less than or equal to 33</td>
</tr>
<tr>
<td>Orange</td>
<td>At risk</td>
<td>More than 33 and less than or equal to 67</td>
</tr>
<tr>
<td>Red</td>
<td>Critical</td>
<td>More than 67</td>
</tr>
<tr>
<td>Gray</td>
<td>Incomplete</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Note: The icon is a notation that the maximum failure threshold for the scorecard has been reached. The tests for the metric are halted for this cycle, and all associated aggregated summaries are 0%. Review the scorecard rules which might be ineffective, or the CMDB might be in an unstable state.

Domain separation

If the Domain Support - Domain Extensions Installer plugin is activated, then the CMDB dashboard is domain aware:
• The CMDB dashboard aggregates and reports health failures and scores based on user’s domain visibility of CIs. If domain visibility lets a user see a CI, then the audit rule in that user’s domain applies to that CI, whether the CI is in the user’s domain or in a contained domain. If a CI fails health tests from different user domains, then separate failure records are created.
• Users can configure KPI and metric settings specific to the needs in their domain. So different domains can have different settings such as active/inactive, and thresholds.
• A child domain derives its immediate parent’s domain health configurations if the child domain does not configure its own. A child domain can override parent’s configurations by modifying them.
View services health reports

The CMDB service dashboard serves as a central location to view aggregated health reports for services at a glance. Also, it lets you drill into a service to perform remediation actions that address health issues, and that improve CMDB health. The CMDB service dashboard uses the Performance Analytics framework for dashboards and employs the capabilities it provides.

Requirements

- The Event Management and Service Mapping Core plugin must be activated.
- If the system property `glide.cms.enable.responsive_grid_layout` exists, then it needs to be set to true. For more information, see Enable responsive dashboards.
- Role required: asset or itil

Configuration

The CMDB service dashboard requires some configuration before it can display meaningful data, using the same settings as the CMDB dashboard. The CMDB service dashboard uses the settings for the Business Service, Manual Service, and Technical Service classes. For each CI that is included in a service, the rule settings of its respective class are applied. You can customize these settings in the CI Class Manager, and on the CMDB Health Preferences page. Once CMDB Health is configured and the CMDB Health Dashboard Jobs are enabled, the CMDB service dashboard displays data that is automatically collected and calculated on a recurring schedule.

CMDB Health is domain aware. If domain separation has been activated, then the CMDB service dashboard displays health based on data, rules, and settings from the logged-on user domain. If rules and settings are not defined for a child domain, then the parent’s settings are applied, recursively.

Access

Access the CMDB service dashboard by navigating to Configuration > CMDB Dashboard > Service View.

Report details

The CMDB service dashboard displays aggregated health for services, and also details for individual services. For a specific service, the CMDB service dashboard displays aggregated health for all the CIs in that service, including the service CI itself. Also it provides useful reports about service classes such as the Business Service class. You can drill down those reports to display further details of duplicate, orphan, or stale CIs per service and lists of the top 10 incident, alert, and change generating CIs in the service.

All default widgets can be filtered using the CMDB service hierarchy tree. Initially, the service hierarchy filter is set to Business Service. Click Business Service to expand it and to select a different class, filtering all widgets on the dashboard to display data only for the selected class, its child classes, or services of that class.

In each scorecard widget, the horizontal bar in the center and the % number are correlated, displaying the aggregated health summary for the KPI. Health results of associated metrics are displayed underneath, each contributing according to the weight configuration of the metric scorecard, and its threshold.
With the exception of the Overall health scorecard, you can drill into any widget in the service dashboard:

- In a scorecard widget: Click the large aggregated percent number or the health bar to drill into a more detailed dashboard for that KPI.
- In a charts widget: Click a bar to display a list of all the records that the bar represents.
- In lists: Click the 'i' icon to view a list of all the tasks or alerts related to the CI.

**Color codes**

The CMDB service dashboard uses color codes when displaying aggregated health status. The status definitions are based on the threshold limits for each scorecard, defined in the CI Class Manager.

<table>
<thead>
<tr>
<th>Color code</th>
<th>Definition</th>
<th>Default threshold setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Best</td>
<td>Less than or equal to 33</td>
</tr>
<tr>
<td>Orange</td>
<td>At risk</td>
<td>More than 33 and less than or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>equal to 67</td>
</tr>
<tr>
<td>Red</td>
<td>Critical</td>
<td>More than 67</td>
</tr>
<tr>
<td>Gray</td>
<td>Incomplete</td>
<td>N/A</td>
</tr>
</tbody>
</table>

The icon is a notation that the maximum failure threshold for the scorecard has been reached. The tests for the metric are halted for this cycle, and all associated aggregated summaries display 0%.

**View CMDB groups health reports**

The CMDB group view dashboard serves as a central location to view aggregated health reports for CMDB groups at a glance. Also, it lets you drill into a CMDB group to perform remediation actions that address health issues, and that improve CMDB health. The CMDB group view dashboard uses the Performance Analytics framework for dashboards and employs the capabilities it provides.

**Configuration**

The CMDB group view dashboard requires some configuration before it can display meaningful data, using the same settings as the CMDB dashboard. For each CI that is included in a CMDB group, the rule settings of its respective class are applied. You can customize these settings in the CI Class Manager, and on the CMDB Health Preferences page. Once CMDB Health is configured and the CMDB Health Dashboard Jobs are enabled, the CMDB group view dashboard displays data that is automatically collected and calculated on a recurring schedule.

If the system property `glide.cms.enable.responsive_grid_layout` exists, then it needs to be set to true. For more information, see [Enable responsive dashboards](#).

CMDB Health is domain aware. If domain separation has been activated, then the CMDB group view dashboard displays health based on data, rules, and settings from the logged-on user domain. If rules and settings are not defined for a child domain, then the parent’s settings are applied, recursively.

Role required: asset or itil

© 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.
Access

Access the CMDB group view dashboard by navigating to Configuration > CMDB Dashboard > Group View. Then, select a CMDB group from the CMDB Health Group List drop-down list.

Report details

For each CMDB group, the CMDB group view dashboard displays aggregated health for all the CIs in that group. You can drill down those reports to display further details of duplicate, orphan, or stale CIs per CMDB group. In each scorecard widget, the horizontal bar in the center and the % number are correlated, displaying the aggregated health summary for the KPI. Health results of associated metrics are displayed underneath, each contributing according to the weight configuration of the metric scorecard, and its threshold.

With the exception of the Overall health scorecard, you can drill into any widget in the CMDB group view dashboard:

- In a scorecard widget: Click the large aggregated percent number or the health bar to drill into a more detailed dashboard for that KPI.
- In a chart widget: Click a bar to display a list of all the records that the bar represents.
- In lists: Click the ‘i’ icon to view a list of all the tasks or alerts related to the CI.

Color codes

The CMDB group view dashboard uses color codes when displaying aggregated health status. The status definitions are based on the threshold limits for each scorecard, defined in the CI Class Manager.

<table>
<thead>
<tr>
<th>Color code</th>
<th>Definition</th>
<th>Default threshold setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Best</td>
<td>Less than or equal to 33</td>
</tr>
<tr>
<td>Orange</td>
<td>At risk</td>
<td>More than 33 and less than or equal to 67</td>
</tr>
<tr>
<td>Red</td>
<td>Critical</td>
<td>More than 67</td>
</tr>
<tr>
<td>Gray</td>
<td>Incomplete</td>
<td>N/A</td>
</tr>
</tbody>
</table>

The ! icon is a notation that the maximum failure threshold for the scorecard has been reached. The tests for the metric are halted for this cycle, and all associated aggregated summaries display 0%.

View CI health

The CI dashboard is a central location displaying health report for an individual CI, history of changes to the CI in a timeline view, and the relation formatter. The CI dashboard also displays incidents, changes, and other tasks affecting the CI, and business services affected by the CI. You can access the CI dashboard from a CI form, or from the CMDB dashboard.

Role required: asset or itil

The health scores are based on settings of CMDB Health KPIs and metrics. The report is calculated in real-time from data stored in health-related tables which the CMDB Dashboard jobs update on
a recurring schedule. The completeness and correctness KPIs are always up to date, but for other KPIs, it is possible that updates to the CMDB are not reflected because one of the dashboard jobs hasn’t run yet, as follows:

- **Compliance**: Depends on audit cycles and on the 'CMDB Health Dashboard - Compliance Score Calculation' job.
- **Relationships**: Depends on the 'CMDB Health Dashboard - Correctness Score Calculation' job.

To ensure that the latest updates to these KPIs are reflected on the CI dashboard, navigate to the respective dashboard job, and click **Execute Now**.

1. On a CI form click **Dashboard**.
2. Or, navigate to **CMDB Dashboard > CMDB Health** and click **CMDB Dashboard - All** to display the class hierarchy. Enter a search string and then select a CI from the **Configuration Items** group.

The search results are grouped by **Classes** and **Configuration Items** that match the search string.

Various widgets in the report display CI’s health with the following color codes:

- **Green**: The CI passed the health test (for example, it is not a duplicate).
- **Red**: The CI failed the health test (for example, it is a duplicate)
- **Grey**: The CI was not tested for this metric, because the threshold was not set for the CI (class) in the CI module.

The report displays the change history for the CI in a timeline format, that you can zoom in or out to select a time period for which to display details for. Use the related lists tabs **Change, Incident, Task, Business Services**, and **Alerts** to further drill into additional details.

**Note:**

Missing rules or other class definitions can prevent some health scores from being evaluated for a CI. The results in the CI dashboard in these situations, are described below:

**Duplicate**

- If no identification rules ([cmdb_identifier]) are defined for the CI’s class or its ancestors: A notification to that effect appears.
- If only dependent identification rules are defined: **Not applicable** notification appears.

**Orphan**

- If the CI is excluded by health inclusion rules: **Not applicable** notification appears.
- If no orphan rules ([cmdb_health_orphan_rule]) are defined for the CI’s class or its ancestors: A notification about missing a rule appears.

**Staleness**

- If the CI is excluded by health inclusion rules: **Not applicable** notification appears.
- If no staleness rules ([cmdb_health_staleness_rule]) are defined for the CI’s class or its ancestors: A notification about missing a rule appears.

**Audit**
Customize the CI dashboard

You can add, remove or re-arrange content on the CI dashboard to display the CI health statistics that are important to you.

Role required: itil_admin

On a CI form click **Dashboard** and customize the CI dashboard as follows:
- Drag a tile near its upper edge and drag it to a different location on the dashboard to rearrange the current layout.
- Click the X in the upper right side of a widget to hide the widget.
- Click the + sign in the upper left corner of the dashboard to add content. In the **Add content** dialog box, select the content to add and the location to place it.
- Click the gear icon in a widget tile to edit widget settings such as title and height.
- Click **Reset to Default** to revert to the base system settings.

See the following video on YouTube: [CMDB Health Dashboard for Helsinki | Overview](#) for information about configuring and using the CMDB dashboard.

View CI relationships health

View aggregated orphan, stale, and duplicate CI relationships in the CMDB dashboard. You can configure the relationship scorecards, but you cannot configure the underlying relationship KPI health tests.

The CMDB Health Dashboard - Relationship Compliance Processor dashboard job must run to generate data for these reports.

Role required: itil or asset

CMDB Health measures CI relationship health using a separate KPI and metrics.

**Orphan relationship**

A relationship that is missing a parent or missing a child.

**Duplicate relationship**

Relationships that have identical parent, child and relationship type.

**Stale relationship**

A relationship in which one of the CIs is stale. For a stale CI – its associated relationships are also stale.

In addition, the following relation compliance reports are generated and displayed at the bottom of the screen:

**Relations not compliant with suggested relations**

`suggested CI relationships` are used as rules to test if relationships comply with specified suggested relationships.
Relations not compliant with containment rules
Containment rules are used to test if relationships comply with specified containment relationships.

Relations not compliant with hosting rules
Hosting rules are used to test if relationships comply with specified hosting relationships.

For each of the compliance reports, to test a relationship there needs to be a rule (suggested relationship, hosting rule, or containment rule) in which the parent and child CI classes match the parent and child CI classes in the tested relationship. If the relationship types in the rule and in the tested relationship do not match, then the relationship is not in compliance. If an applicable rule is not found, then the relationship is considered to be in compliance. Rules apply to the classes specified in the rule, and also to descendant classes. Therefore, when testing a relationship, rules that apply to ascendant parents of the CIs in the tested relationship, are used. If there are multiple rules that match the parent and the child CI classes of the tested relationship, then the tested relationship needs to satisfy only one of these rules to be in compliance.

1. Navigate to Configuration > CMDB Dashboard > CMDB View.
2. Select the Relationship Health tab.
3. Scroll to the bottom of the page to examine the relation compliance reports. Report results are grouped by relationship type, and you can do the following:
   - Point to a relationship type to display its label and the % of relationships that are not in compliance.
   - Click on a relationship type to drill down to a detailed list of all the relations of that type that are not compliant. Click on a specific relationship to display more details such as the failure description. The Failure Description field lists only a single rule that the relationship did not comply with, even if there are additional rules that the relationship fails to comply with.

Explore and modify CI class
The CI Class Manager displays the entire CMDB class hierarchy in a tree-view format, consolidating class definitions into a central location. It lets you define metadata for a class, such as reconciliation rules, required and recommended fields, and audit templates. You can also select a specific class to view, to modify, or to extend its definition to create a new class.

In the CI Class Manager, you can review and manage the health rules and settings for all CMDB Health metrics, at the class level. You can configure scorecard settings for calculating overall health for a class, and overall health for the entire CMDB.

1. Navigate to Configuration > CI Class Manager.
2. Check Advanced and expand all strips that are closed.
3. Select any scorecard to review and update its setting for the class.
4. Expand the Class Hierarchy to explore the class hierarchy and to select a class to modify.
5. Modify any class detail as needed, and click Update.

Delete all records for a CMDB class
You can delete all the records for a CMDB class in the CI Class Manager.

Role required for the Configuration Item (cmdb_ci) table: itil or asset

1. Navigate to Configuration > CI Class Manager.
2. Expand the Class Hierarchy and select the class for which you want to delete all records.
3. On the **Table** form, click **Delete All Records**.

**Create CMDB remediation rule**

A CMDB remediation rule is associated with a task that was created for a failed CMDB health test. A CMDB remediation rule is applied automatically or manually to execute a remediation workflow that can, for example, delete stale CIs.

You need to first create and publish a remediation workflow that addresses the CI issue. The workflow can be a regular workflow, or an Orchestration workflow, and the table in the workflow needs to match the task type in the remediation rule. Do not configure the workflow with any filter conditions by setting **If condition matches** to **None**, so that the filters of the CMDB remediation rule will apply.

Role required: itil_admin (on top of itil)

1. Navigate to **Configuration > CMDB Remediations**.
2. Fill in the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Remediation name.</td>
</tr>
<tr>
<td>Task type</td>
<td>Type of CMDB health-related tasks to apply the remediation to.</td>
</tr>
<tr>
<td>Task filter</td>
<td>Filters tasks to apply remediation to. Also applies dot-walking on CI fields so that remediation is applied to tasks associated with matching CIs.</td>
</tr>
<tr>
<td>Execution</td>
<td>• Manual: Remediation is applied manually.</td>
</tr>
<tr>
<td></td>
<td>• Automatic: The workflow is applied once, upon the creation of a task that matches the Task type and Task filter.</td>
</tr>
<tr>
<td>Active</td>
<td>Allowing the workflow to run.</td>
</tr>
<tr>
<td>Workflow</td>
<td>The CMDB remediation workflow (regular or Orchestration) that will execute automatically or manually, depending on the Execution setting. You can click the Lookup using list icon, and then click <strong>New</strong> to create a new workflow.</td>
</tr>
</tbody>
</table>

3. Click **Submit**.

If **Execution** is set to Automatic, then the business rule ‘Run remediations for CMDBHealth task’ applies the remediation workflow to CIs that match the Task filter. If **Execution** is set to Manual, then you can manually apply the remediation workflow defined in the rule.

**Apply CMDB remediation**

Manually initiate a workflow to remediate a CI that failed a CMDB health test. For example, you can remediate CIs that are orphan or stale.

To manually apply a CMDB remediation, a CMDB remediation rule must exist, in which **Execution** is set to **Manual**.

Role required: itil_admin
Except for the duplicate and audit health metrics, you can choose to create tasks for health test failures for a metric.

To remediate failures of the duplicate metric, use de-duplication tasks.

For all metrics except for audit, each CI that failed a metric test is associated with a single task. Because a CI can fail multiple audits, a single CI can be associated with multiple audit tasks. The first of those tasks is in the Task field, and any additional tasks are in the Additional Tasks field. To remediate failures of the audit metric, refer to the audit tasks for the audits that the CI failed.

1. Navigate to Configuration > CMDB Dashboard, and then click CMDB View, Service View, or Group View.

2. Click on one of the bars in a bar chart on the page. Or, click on a metric tile that is associated with the remediation that you want to apply, and then in a detailed report click on a bar in a bar chart. For example, to remediate an orphan CI, click the Completeness tile.

3. In the Task column in the CMDB Health Results list, select the task that is associated with the CI that you want to remediate. Hover over the information icon (i) for a result record to display the CMDB Health Results dialog box with more details about the health test. The CMDB Health Results list contains records only for the CIs that failed a metric test.

<table>
<thead>
<tr>
<th>Field</th>
<th>Column</th>
</tr>
</thead>
<tbody>
<tr>
<td>CI</td>
<td>The CI associated with the test results.</td>
</tr>
<tr>
<td>Class Name</td>
<td>The CI’s class.</td>
</tr>
<tr>
<td>Description</td>
<td>Details about the reasons for the CI failing the metric test.</td>
</tr>
<tr>
<td>Last Evaluated On</td>
<td>Time that the CI was evaluated for the metric, and which resulted in failure.</td>
</tr>
<tr>
<td>Metric</td>
<td>The CMDB Health metric associated with this test result.</td>
</tr>
<tr>
<td>Source</td>
<td>Source of the health test failure:</td>
</tr>
<tr>
<td></td>
<td>· CMDB Health Audit: Corresponds to the dashboard</td>
</tr>
<tr>
<td></td>
<td>· Cloud discovery</td>
</tr>
<tr>
<td>Task</td>
<td>The task associated with the health test failure. For the audit metric, if there are multiple failures, then only the first task is listed.</td>
</tr>
<tr>
<td>Additional Tasks</td>
<td>If there are multiple tasks related to the audit metric, contains all tasks other than the first which is in the Task field.</td>
</tr>
<tr>
<td>Active</td>
<td>Used internally in combination with the To Delete field to determine the correct results set that this failure belongs to.</td>
</tr>
<tr>
<td>To Delete</td>
<td>Used internally in combination with the Active field to determine the correct results set that this failure belongs to.</td>
</tr>
</tbody>
</table>

4. On the task form, click Remediate.

5. In the Run Remediations dialog box, select the remediation rule that you want to apply.
The list of remediation rules is based on the type of health metric (such as orphan, stale), and on the filter defined in the rule.

6. Click **Execute**.

### Tables installed with CMDB Health

CMDB Health tracks and reports various KPI and metrics that monitor the health of the CMDB. CMDB Health adds the following tables.

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMDB Health Metric (cmdb_health_metric)</td>
<td>Details such as if a KPI or metric is enabled, maximum failure threshold, and other settings for all CMDB Health KPIs and metrics.</td>
</tr>
<tr>
<td>CMDB Health Result (cmdb_health_result)</td>
<td>Results from the most recent CMDB Health processing cycle.</td>
</tr>
<tr>
<td>CMDB Health Scorecard (cmdb_health_scorecard)</td>
<td>Current and historic health scores. Status of historic score records is ‘Historic’, and of latest score records is ‘Complete’.</td>
</tr>
<tr>
<td>CMDB Health Orphan Rule (cmdb_health_orphan_rule)</td>
<td>Rules for calculating orphan records per class.</td>
</tr>
<tr>
<td>CMDB Recommended Fields (cmdb_recommended_fields)</td>
<td>Recommended fields per class.</td>
</tr>
</tbody>
</table>
| CMDB Health Metric Status (cmdb_health_metric_status) | Internal table that tracks the status of each KPI and metric that is being processed. Includes status, processing time, and processing start date. State for a KPI or metric changes from ‘In Progress’ to either of:
  - Complete
  - MaxFailures
  - Daily Processing Time Out
  Processing of a timed out KPI or metric continues on the following day. |
| CMDB Health Processor Status (cmdb_health_processor_status) | Internal table that tracks the processing progress of each KPI and metric. Contains a list of tables that are processed for each KPI and metric, and processing status. Classes are processed sequentially, changing status from Draft -> In Progress -> Complete. |

### CMDB Health troubleshooting

Use the following information to track and resolve issues with the CMDB Health processes.

### Logging

By default, only error messages are logged to the syslog table, with the source name CmdbHealth. To enable logging of ‘info’ and ‘warning’ messages (which are typically
logged at the start and end of each processing cycle), update the system property glide.cmdb.logger.use_syslog.CMDBHealth. For information about using this property, see **CMDB health system properties**.

### Processing status

If scheduled jobs are enabled, but data is not displaying on the CMDB dashboard, you can check the processing status in the CMDB Health Metric Status (cmdb_health_metric_status) table. Depending on the status of the **inactive** metric, decide how to proceed.

Initially, the state of all metrics is 'In Progress'.

Possible final states of a metric:

- **Complete**
  All classes are processed and the number of failures is under the maximum failures threshold.

- **Max Failures**
  The number of failures for this metric reached the maximum failures threshold. Processing has been aborted and will start over in the next run.

- **Daily Time Out Pause**
  The processor reached the processing time limit. Processing is paused and will resume in the next run.

At the end of a processing cycle, the final state of a KPI depends on the final state of its associated metrics. Possible final state of a KPI:

- **Complete**
  All associated metrics are in Complete state and score calculation is complete.

- **Incomplete**
  Score is not calculated because one of the associated metrics reached its maximum failure thresholds.

- **Daily Time Out Pause**
  Timed out because one of the associated metrics has reached its processing time limit.

### Processing time

If processing of a metric times out, you can find out which class takes too long to process. Use this information to find out if any validation rules are weak.

The progress of each metric is tracked in the CMDB Health Processor Status table (cmdb_health_processor_status). Status for classes that have been processed for a metric is Complete, and for classes that are yet to be processed is Draft. By looking at the update time for each class, you can calculate the length of processing time for each class.

### Fixing orphan records due to broken hierarchy

Orphan rules might detect an orphan CI, which you are not able to access and delete. Or, there might be a mismatch between the list view that displays the orphan records, and the total number of records. These findings are due to records being deleted in the database from only one table in the CMDB hierarchy.
These CI records are not accessible via GlideRecord and must be deleted directly from the database. Therefore, in this case, to delete an orphan CI from the database you must get help from ServiceNow Technical Support.

Orphan test results provide the details of where exactly the hierarchy is broken. For example, the message 'This cmdb_ci_linux_server CI (91054fc24f22520053d6e1d10c713) is missing record in cmdb_ci_computer table' means that a record of that sys_id must be deleted from the CMDB, cmdb_ci, cmdb_ci_hardware, cmdb_ci_server, and the cmdb_ci_linux_server tables (the Computer class is between the Hardware and the Server classes in the hierarchy.)

**Scripted audits Skipped**

An error message is logged if the results from a scripted audit are not included in the compliance KPI. The reason can be that the script in the audit was not updated to populate its Last ran date field. Without a Last ran date value, CMDB Health is unable to identify these run results as part of a recent complete audit run, and skips those results.

See [prepare scripted audits for the compliance KPI](#) for information about how to resolve this issue.

**CMDB Health troubleshooting: failure threshold reached**

The CMDB dashboard displays the string 'failure threshold reached' when the number of CIs that are failing the metric tests, reaches the failure threshold set for the metric.

CMDB Health stops processing for this metric in the current cycle, and therefore there is no aggregated health score for the metric. Processing will be attempted again in the next cycle. Also, status in the CMDB Health Metric Status (cmdb_health_metric_status) table is set to Max Failures for this metric.

When the health score of a metric cannot be evaluated, then the processing status of the respective KPI (for example, correctness) is set to Incomplete. The CMDB dashboard displays the string Incomplete score for the respective KPI and for the CMDB Health overall score. Also, aggregated health scores for the metric are not available for any class in the CMDB hierarchy.

To troubleshoot, do any of the following:

- Review and refine the rules defined for the metric which has reached max failures. If a rule associated with the metric is too generic, resulting in large number of failures, attempt to refine it. For Example:
  - Completeness – Review the recommended fields that are causing failures and remove the ones that are not critical for the health score. For more information see [Set a CI field to be recommended](#).
  - Correctness – For the staleness metric, depending on the cause of the failures it might be helpful to increase the value of the glide.cmdb.health.staleness CMDB Health system property.
- Reduce the number of failures by fixing CI records: If after adjusting the metric test rules the max failures for some metrics is still reached, then address the failures by updating CI records with the relevant missing information.
- In this case increasing the failure threshold for the metric that is failing and check if processing for this metric completes successfully in the next cycle. Increasing the failure threshold beyond 500K might reduce overall performance.

**CMDB Health troubleshooting: incomplete score**

The CMDB dashboard displays the string 'incomplete score' for a metric when it fails to calculate the score for the metric.

'Incomplete score' is displayed when:
The number of CIs that are failing the tests of one of its sub-metric, reaches the failure threshold set for the metric. In this situation, the processing status for the respective parent metric (for example, correctness) is set to 'incomplete' in the CMDB Health Metric Status (cmdb_health_metric_status) table. Processing for the failing metric in the current cycle stops, and therefore there are no aggregated health scores for the sub-metric, the parent parent metric, or the overall CMDB Health.

To troubleshoot, resolve the underlying cause of CIs failing the sub-metric tests. See CMDB Health troubleshooting: failure threshold reached for more information about resolving the failures of the sub-metric.

An error is encountered while processing the sub-metric.

To troubleshoot, examine the system logs system logs to determine the cause of the error. After fixing the cause of the problem, restart processing by manually executing the respective parent metric dashboard job.

View CMDB benchmarks

CMDB calculates several CMDB Health benchmarks which then display in the Benchmarks dashboard. These benchmarks are based on various CMDB Health metrics, displaying monthly averages, trends, comparisons to industry averages of your ServiceNow peers, and global benchmarks.

The CMDB Health Dashboard jobs must be enabled and health data must be collected. Also, navigate to Benchmarks > Setup and ensure that the CMDB KPIs are enabled under IT Operations Management.

CMDB provides the following benchmarks:

- % of non-compliant CIs
- % of duplicate CIs
- % of stale CIs

For an instance, each of these benchmarks is the calculated monthly average for the corresponding CMDB Health metric. Calculating a monthly average requires that there is a metric result value for each day of the month. Therefore, each day on which the respective Health Dashboard job did not run, is assumed with the aggregated result from the run that is most recent to that day. The monthly average is then calculated based on the sum of all the daily aggregated results for the metric in that month, divided by the number of days of the month. For a CMDB Health Dashboard job that ran multiple times in a single day, only the results of the last run in that day are used for the monthly average calculation.

Note: The frequency of CMDB Health Dashboard job executions depend on whether the job is enabled, its schedule and on manual runs.

Global averages are based on the sum of monthly averages of all peer instances, divided by the number of instances (aside from instances for which the monthly average is 0).

1. Navigate to Benchmarks > Dashboard.
2. Click the icon and select IT Operations Management.
3. Click ALL or CMDB.
4. Click on a CMDB benchmark to drill down to trend data, and other benchmark details.
Useful related lists in CI forms

By default, the forms that display manageable configuration items (CI) - computers, printers, network gear, uninterruptible power supplies (UPS), and power distribution units (PDU) - provide a number of related lists for the form.

The following related lists are common to all forms for manageable CIs.

- Network Adapters - Displays all the NICs installed on a CI.
- CI IPs - Displays all the IP addresses on this CI:
  - Computers (workstations, laptops using various Mac and Windows operating systems)
  - Windows servers
  - Linux servers
  - AIX servers
  - Solaris servers
  - Devices discovered through SNMP.
- DNS Names for CIs - Displays all the DNS names on a CI.

The IP version information appears in all IP address related lists and forms.

Note: Since all paths here click into the IP Address to DNS Names list that associates an IP address with a DNS name, this part of the common flow was not added to the tree structure.

Discovery source

A table called Source (sys_object_source) stores information identifying the source of a discovery (by ServiceNow Discovery or another product), the ID of that source, and the date/time of the last scan. To view this information, configure a CI form and add the Sources related list. This table is populated automatically when the Discovery plugin is enabled.

Activate the Extended CMDB plugins

The Configuration Management (CMDB) application provides core functionality for the configuration management database, including modules for hardware and configuration items. The separate Extended CMDB plugin includes a collection of modules for specialized configuration items, such as radio hardware, test equipment, and voice system hardware.

Role required: admin

The Configuration Management (CMDB) plugin is automatically active for all instances. You must activate related plugins to access the modules for specialized configuration items.

- CMDB Mainframe (com.snc.cmdb.mainframe)
- CMDB Radio Category (com.snc.cmdb.radio.category)
- CMDB Telecom Category (com.snc.cmdb.telecom.category)
- CMDB Test Equipment (com.snc.cmdb.test.equipment)

Note: In Helsinki, many of the tables from the Extended CMDB plugin were moved to the core Configuration Management (CMDB) (com.snc.cmdb) plugin, or to one of the newly added plugins. See the Helsinki release notes for details about those tables.

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**.

---

**Help the Help Desk**

Help the Help Desk is a tool that allows users to populate the CMDB automatically with information about their Windows computer.

Help the Help Desk is a small web application that downloads and runs locally, using a WMI login script to gather information such as serial number, computer name, disk configuration, network configuration, installed software, memory, and much more. Users have the option of using two types of SOAP authentication for running the Help the Help Desk script.

- **Cookie-based authentication for Help the Help Desk**
- **Basic access authentication for Help the Help Desk**

**Note:** Domain separation is not supported for Help the Help Desk.

---

**User roles and user names**

Users must have the soap_ecc role to use Help the Help Desk from within an instance.

For users without access to an instance, you can configure Help the Help Desk to allow users to run the script without login credentials. Users with access to an instance can also use Help the Help Desk configured in this way, but only if they have the soap_ecc role.

User name cannot contain these characters: \n
Any user name that contains the \n characters prevents the **Assigned to** field on a computer from being populated.

---

**Help the Help Desk device identification**

Help the Help Desk uses a predefined series of queries to identify and update existing CIs in the CMDB or to create a new CI if no match is found. These queries attempt to match devices using three criteria in a certain order.

Updates to an existing CI require only a single match as the list is evaluated. For example, if a device’s name has changed, but the MAC address is the same, the CI with the matching MAC address is updated.

- Serial number in the (cmdb_ci_computer) table
- MAC address in the (cmdb_ci_network_adapter) table
- Computer name in the (cmdb_ci_computer) table

**Note:** Discovery Identifiers are incompatible with Help the Help Desk queries.
Script include

The script include `CIIdentifierForHelpDesk` provides the logic for updating existing CIs or creating a new CI if no matching device exists in the CMDB. Do not modify this script. Errors introduced into this script can result in update failures or in new CIs being created for every device found.

Configure SOAP authentication for Help the Help Desk

By default, the ServiceNow system requires SOAP authentication. This affects the way in which your browser is configured for Help the Help Desk.

Role required: admin

1. Navigate to **System Properties > Web Services**.
2. Verify the system property for **Require basic authorization for incoming SOAP requests** `glide.basicauth.required.soap` is enabled.
3. Click **Save**.

Note:

If you receive the error, *There was a problem retrieving the XML data(0): Unknown*, an authentication issue is preventing the script from sending information to your ServiceNow instance. Verify the user meets the requirements for **Cookie-based authentication for Help the Help Desk** or **Basic access authentication for Help the Help Desk**.

Cookie-based authentication for Help the Help Desk

Cookie-based authentication uses cookies generated by Windows Internet Explorer for SOAP authentication on the instance.

This type of authentication can be used to run the Help the Help Desk script at the time it is downloaded or after it has been saved to the local drive. When the script is downloaded, Internet Explorer generates a cookie using the user’s login credentials, and then shares this cookie with the script. When a user attempts to run the script, the instance checks first for this cookie. If the cookie has been created, the script can authenticate on the instance through SOAP.
Cookie-based authentication

The following setup requirements are imposed on .hta file downloads by Microsoft.

- You must use Internet Explorer and choose to run the script while you are logged in to your instance. If you choose to use a different browser and download the script file to run later, the script will not work properly unless you have an active session on your instance with Internet Explorer.
- Disable Protected Mode and User Account Control (UAC). Protected Mode is available in Internet Explorer 7 or later in Windows Vista. UAC is a feature of Windows Vista and Windows 7.
This feature requires that your logged in user session be persisted to the Help the Help Desk script. For this to occur, the Remember me check box in the login screen must be enabled and selected (the default behavior). This option enables the system to write back an HTTP cookie to your browser to be persisted across sessions.

Basic access authentication for Help the Help Desk

An alternative to cookie-based authentication for the Help the Help Desk script is basic access authentication, which employs two properties to configure the script with credentials.

When a user logs in with the proper credentials, the user accesses the instance in the soap_ecc role, which grants access to the ECC queue but limits the user’s access to other features. The administrator then configures the system properties with the user name and password for the soap_ecc user.

The values from these properties are automatically saved to the script file helpthehelpdesk.js. When this user runs the Help the Help Desk script, the instance checks for a cookie. If no cookie is found, the instance checks for the login credentials provided by the system properties, and authenticates the script automatically.

Set up basic access authentication for the Help the Help Desk script

You can set up basic access authentication for the Help the Help Desk script.

Role required: admin

1. Create a new user with the following values.

<table>
<thead>
<tr>
<th>User ID</th>
<th>Create an easily recognizable user name such as SOAPAUTH or SOAPONLY.</th>
</tr>
</thead>
<tbody>
<tr>
<td>First name</td>
<td>SOAP</td>
</tr>
<tr>
<td>Last name</td>
<td>Authentication</td>
</tr>
<tr>
<td>Password</td>
<td>Any password</td>
</tr>
</tbody>
</table>

2. Right-click the header bar and select Save.
   The record is saved, and the Related Lists appear.

3. In the Roles Related List, click Edit.

4. In the slushbucket, move the soap_ecc role from the Collection list to the Roles list, and then click Save.

5. Navigate to System Definition > Help the Help Desk.

6. Add the user name and password you created to the appropriate properties, and then click Save.
   The password is encoded when saved.

   The login credentials from these properties are saved to the helpthehelpdesk.js script. When the Help the Help Desk script is run by a user logged in with these credentials (in the soap_ecc role), the script is able to authenticate automatically on the instance.

Help the Help Desk login script

The Help the Help Desk script enables organizations to proactively scan their network to discover all Windows based hardware and the software packages installed on those devices.

This WMI-based script is included in the core ServiceNow platform functionality. This script can also be set up to run as a Windows login script and used to keep the CMDB up to date. The script is named helpthehelpdesk.js and can be downloaded from each customer’s local instance.
Install and use the login script

The login script is installed on the instance and can be downloaded directly from a module.

Role required: admin

The same script is used to perform the Help the Help Desk scan, which gathers information about a user’s Windows computer and updates the CMDB.

1. Log in to your instance with Windows Internet Explorer.
2. Navigate to System Definition > Help the Help Desk Login Script.
3. Follow the download instructions in the page that appears.
4. Put the helpthehelpdesk.js file in the following folder: %SystemRoot%\sysvol\sysvol\<domain DNS name>\scripts where %SystemRoot% is usually c:\winnt or c:\WINDOWS and <domain DNS name> is the DNS name of the domain, similar to MyDomain.com. This folder is replicated to all domain controllers in the domain.
5. Open the helpthehelpdesk.js file in a text editor, such as Wordpad.
6. Check the var server line to ensure that the URL for your ServiceNow instance is correct. The name of the instance is added automatically. It should look something like this:

```javascript
var server = "https://abctech.service-now.com/";
```

7. Ensure that basic authorization for SOAP requests is enabled in your instance, and a SOAP user is defined.
   This allows the script to connect to your instance. The entry should look something like this:

```javascript
var httpUsername = "user_on_your_instance";
var httpPassword = "user's_password";
```

8. Create a Logon.bat script to run helpthehelpdesk.js as follows.

```batch
@echo off
cscript %0\..\helpthehelpdesk.js
EXIT
```

9. Add Logon.bat to the Logon script field on the Profile tab of the user properties dialog in the Active Directory Users and Computers MMC corresponds to the scriptPath attribute of the user object.
   Logon scripts can also be configured in Group Policy. However, Group Policy only applies to clients with Windows 2000 or above. The setting in Group Policy is User Configuration, Windows

---

© 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.
Settings, Scripts (Logon/Logoff), Logon. Copy the file you want for the Logon script to the Windows clipboard.

10. Open the Logon setting in the Group Policy editor.
11. Click the Show Files button.
12. Paste the desired file in the dialog.

You can select the file and edit it in this dialog as well. This is easier than navigating in Windows Explorer to the folder where Group Policy Logon scripts are saved. However, if you do have to navigate to the folder, the path on the domain controller is:

```
%SystemRoot%\sysvol\sysvol\<domain DNS name>\<policy GUID>\user\scripts\logon
```

Again, %SystemRoot% is usually c:\winnt and <domain DNS name> is the DNS name of the domain, similar to MyDomain.com.

<policy GUID> is a hexadecimal string representing the GUID (unique identifier) of the specific Group Policy Object (GPO). Group Policies are assigned to a domain, site, or organizational unit in Active Directory.

The logon script setting applies to all users in the domain, site, or organizational unit to which the GPO applies. You will notice that you assign a logon script to all users in the container at once, rather than having to assign the scriptPath attribute for each user. This makes it much easier to assign logon scripts to many users. However, since the same Group Policy applies to all users in the domain, site, or organizational unit, you must code the logon script to accommodate all users.

Encode the Help the Help Desk password

You can use the Help the Help Desk properties to encode the password with simple base64 encoding.

Role required: admin

Configure the user name and encode the password in the properties before downloading the script. This adds the encoded password directly to the script without any further configuration.

1. Navigate to System Definition > Help the Help Desk.
2. Enter a user name and password into the properties for SOAP authentication.
3. Click Save.
The password is encoded immediately.

4. Navigate to System Definition > Help the Help Desk Login Script
5. Download the script.

```javascript
/** Required Variables ******************************************/
* The following section should be modified if the information is not correct.
* **************************************************************************/

// The variable should point to your instance URL, such as https://demo.service-now.com
var server = "https://demo.service-now.com/

// If SOAP authentication is turned on on the instance. The http authentication should be provided here.
var httpUsername = "snuser";
var httpPassword = "encrypt: cGFzc3dvcmQ=";
```

The script downloads with the encoded password in place. If you download the script before encoding the password in the properties form, you must add the variable and encoded password manually.

Run the Help the Help Desk script

You can run the Help the Help Desk script manually.

You also can configure Help the Help Desk to run automatically when users log into their computer. For more details, see Help the Help Desk login script.

1. On your instance, navigate to Self Service > Help the Help Desk.
2. Click Start the Scan to Help the Help Desk.
You are prompted to run or save the discovery.hta script.

3. Run or save the discovery.hta script.
   - If your browser is Windows Internet Explorer, run the script.
   - If you are using any other browser, click Save and save the script to the local machine. To execute the saved script, double-click the file.

The script runs a series of WMI queries to gather information about the Windows machine. When it is finished, the data is sent back to your instance and is used to populate the configuration database (CMDB).

The error message Error: Unable to parse SOAP document means that the Help the Help Desk script was unable to connect to the instance to relay the information that was discovered.

Run the discovery.hta script with browsers other than Internet Explorer

You can run the discovery.hta script with browsers other than Internet Explorer.

Browsers other than IE cannot handle files with the .hta extension. Browsers like Firefox, Safari, and Opera prompt users to download the script file, which you can then double-click to run.

However, in Windows XP (including Vista, Windows 2003 Server, and later), files downloaded from the Internet are marked with a security restriction that interferes with running the script. The typical error message introduced by this security restriction looks like this:

eccEvent(): Access Denied

To remove the security lock on the downloaded file, complete the following steps.

1. Right-click on the downloaded file and select Properties.
   The following message is displayed on the bottom of the form:
   This file came from another computer and may be blocked to protect this computer.

2. Click Unblock to remove the security restriction.
   The script will run if SOAP authentication is disabled.

Access Help the Help Desk status

Help the Help Desk displays the status of all scans in daily records. Drill down into a record for details on how the CMDB was updated within the last 24 hours from scans performed on the instance.

Role required: admin

1. Navigate to System Definition > Help the Help Desk Status.
   A new status record is created each day and displays the number of scans completed (devices scanned). The Description field shows Help the help desk as the source of the scan.
2. To view the details of individual scans, open a scan record.
3. In the scan record, select the **Devices** tab to view all the devices scanned by Help the Help Desk that day.
   Each CI displays the device class and the activity completed: **Created CI** or **Updated CI**. By default, Help the Help Desk cannot discriminate class between servers and workstations and classifies each CI as a **Computer**. However, if Discovery is activated on the instance, Help the Help Desk can classify CIs as either Windows servers or computers.

4. Select the **ECC Queue** tab to examine the data payload returned from each scan.
If Discovery is active on the instance, the Help the Help Desk status appears in the Discovery Status record list. These scan records are described as **Help the help desk** in the list to differentiate them from regular discoveries run from a schedule or a UI action. Open the status record to access the forms described in this page.

<table>
<thead>
<tr>
<th>Number</th>
<th>Created</th>
<th>Description</th>
<th>Schedule</th>
<th>Discover</th>
<th>State</th>
<th>Started</th>
<th>Completed</th>
<th>Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS0010006</td>
<td>2011-05-04 11:00:09</td>
<td>Scheduled Headquarters</td>
<td>Configuration items</td>
<td>Completed</td>
<td>500</td>
<td>500</td>
<td>2011-05-04 11:14:55</td>
<td></td>
</tr>
<tr>
<td>OS0010007</td>
<td>2011-05-03 11:00:09</td>
<td>Scheduled Headquarters</td>
<td>Configuration items</td>
<td>Completed</td>
<td>570</td>
<td>570</td>
<td>2011-05-03 11:15:24</td>
<td></td>
</tr>
<tr>
<td>OS0010008</td>
<td>2011-05-02 11:00:01</td>
<td>Scheduled Headquarters</td>
<td>Configuration items</td>
<td>Completed</td>
<td>570</td>
<td>570</td>
<td>2011-05-02 11:15:24</td>
<td></td>
</tr>
</tbody>
</table>

**Determine values for the Assigned to field**

This page explains how to set properties to determine which value appears in the **Assigned to** field when the script is run.

**Role required:** admin

Any user name that contains the \n characters prevents the **Assigned to** field on a computer from being populated.

- **Navigate to System Definition > Help the Help Desk.**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.wmi.assigned_to_always_overwrite</td>
<td>If the Help the Help Desk script is run on the same computer by different users, the platform overwrites the user name in the <strong>Assigned to</strong> field each time the script is run. To prevent this, set the <strong>For Help the Help Desk script, if the property is &quot;yes&quot;, the &quot;assigned_to&quot; field of the CI is always overwritten; otherwise the field is not overwritten unless it is empty (glide.wmi.assigned_to_always_overwrite) property to false</strong> (clear the check box).</td>
</tr>
<tr>
<td>glide.discovery.assigned_user_match_field</td>
<td>Help the Help Desk attempts to match a Windows user name it finds with the the user_name field of the User (sys_user) table. However, this might not be desirable if the user_name field from the User (sys_user) table contains formatting that is different from that found in Windows. The <strong>For Discovery and Help the Help Desk, the following field in the sys_user table is used to associate a computer CI with a user (glide.discovery.assigned_user_match_field) property enables you to select an alternative field for matching.</strong> For example, you can create a field called <strong>u_username</strong>, and then populate it with a user ID that can be matched against the Windows user name. In this case, replace the default value in the property with <strong>u_username</strong>.</td>
</tr>
</tbody>
</table>
View scan results
You can view the results of Help the Help Desk scans on an instance.
Role required: admin
These records provide access to logs, CI records, and the ECC Queue for all scans conducted each day. Help the Help Desk status reports are also accessible from the Discovery list.

1. Navigate to **System Definition > Help the Help Desk Status**.
2. Open the daily **status record**.

Help the Help Desk script troubleshooting
With the Help the Help Desk script, you can detect all system software on a 64-bit machine. You can also configure the Help the Help Desk script to run for users without prompting for a user name and password.

Allow users without a ServiceNow instance login to run Help the Help Desk script
You can configure the Help the Help Desk script to run for users without prompting for a user name and password.
Role required: admin
This setup enables users who do not have access privileges to an instance to run the script on their Windows machines without having to provide a user name and password. The script can be configured to login in automatically as a SOAP user with the soap_ecc role.

1. Log in to your instance with Windows Internet Explorer.
2. Navigate to **System Definition > Help the Help Desk Login Script**.
3. Follow the download instructions in the page that appears.
4. Put the `helpthehelpdesk.js` file in the following folder: `%SystemRoot%\sysvol\sysvol <domain DNS name>\scripts` where `%SystemRoot%` is usually `c:\winnt` or `c:\WINDOWS` and `<domain DNS name>` is the DNS name of the domain, similar to MyDomain.com. This folder is replicated to all domain controllers in the domain.
5. Open the `helpthehelpdesk.js` file in a text editor, such as Wordpad.
6. Check the var server line to ensure that the URL for your ServiceNow instance is correct.

The name of the instance is added automatically. It should look something like this:

```javascript
var server = "https://abctech.service-now.com/
```

```javascript
/* ************* Required Variables *****************************************************/
/* The following section should be modified if the information is not correct. */
/* **********************************************************************************/

// The variable should point to your instance URL, such as http://demo.service-now.com
var server = "https://abctech.service-now.com/

// If SOAP authentication is turned on on the instance. The http authentication should be provided here
var httpUsername = "";
var httpPassword = "";

/* ************* Optional Variables **********************************************************/
/* The following section can be modified for other purposes. */
/* ***********************************************************************************/
7. Ensure that basic authorization for SOAP requests is enabled in your instance and a SOAP user is defined. This allows the script to connect to your instance. The entry should look something like this:

```javascript
var httpUsername = "user_on_your_instance";
var httpPassword = "user's_password";
```

8. Make the script file available to all users.

**Detect software on 64-bit systems with Help the Help Desk**

You can detect all system software successfully on a 64-bit machine.

A 64-bit browser can detect both 64-bit and 32-bit software, but a 32-bit browser cannot detect 64-bit software.

- To detect all system software, run the Help the Help Desk script from a 64-bit browser.

**Enterprise CMDB**

The Enterprise Configuration Management Database (ECMDB) is targeted toward businesses that want to monitor, manage, measure, track, alert on change, and generally understand business systems that consist of a large number of components, business, and support personnel.

For example, a bond trading service may have multiple application, and web servers, several databases, Linux, UNIX, and Windows servers. There will be security products, network storage, disaster recovery procedures and hardware, etc. that are necessary for the service to operate properly.

The ECMDB makes it easy to either manually enter the relationships or have them populated automatically by discovery tools. In addition to the hardware, software, network, database, and storage areas, it is beneficial to know which individuals or groups are responsible for the service from both a business perspective as well as an IT perspective. Who are the line of business users and managers? Who starts and stops the application or its components? Who monitors the log files? Who is in charge of backup and restore, business continuity, and disaster recovery?

Enterprise CMDB is available with the Configuration Management (CMDB Enterprise Edition) (com.snc.cmdb.enterprise) plugin, which is active in the base system.

**CMDB Relationships**

The ECMDB lets you easily track all relationships by relationship type.

The Enterprise CMDB extends the capabilities of the ServiceNow platform CMDB in the following areas.

**Extended configuration item types**

- Clusters
- Database Instances (Oracle, MySQL, MSFT SQL Server)
- File Systems (Direct and network attached)
- Linux Servers
- Solaris Servers
- AIX Servers
Extended relationships

Accurate description of relationships between items, and between items and people or groups, is important to understand the fabric of a business service. ECMDB provides many relationship types out of the box, but it is easy to extend the number of relationship types. Example relationship types include the following.

- Connects to
- Depends on / Provides Service to
- Powered by / Powers
- Protected by / Protects
- Disaster Recovery Provided by / Provides Disaster Recovery for

Visualization

The system can show relationships as a hierarchy using a standard treeview, flattened, or graphically, all in a simple web interface.

Auditing

Auditing of changes to configuration items is turned on by default.

Federation

Federation of third party discovery and configuration data is supported through standard synchronization offerings (SMS, LAN Desk, others) and through the CMDB Discovery (cmdb_discovery) table.

Configuration item modeling (product models)

Model driven configuration management allows the definition of CI models up front that can be associated to product maintenance lifecycles, cost centers, and support organizations, as well as provides a means for capacity and inventory planning. By defining models for CIs (which have a many to one relationship to the model), you can dynamically group actual discovered or imported CIs into logical, operational, and financial models. This facilitates an organized approach to managing your assets (CIs) in their respective domains.

Enterprise Configuration Management Database (ECMDB) action icons

Any of the following icons may appear in the ECMDB lists of related items.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![X]</td>
<td>For currently active incidents against this configuration item</td>
</tr>
<tr>
<td>![P]</td>
<td>For currently active problems against the configuration item</td>
</tr>
<tr>
<td>![A]</td>
<td>For currently active changes against the configuration item that are not covered in the past, current, pending changes. For example, a request to update the operating system on a server that is currently in progress may display this icon.</td>
</tr>
</tbody>
</table>
For changes that were recently completed against the configuration item. changes with an “Actual_end_date” in the past.

For changes that are planned soon against the configuration item. changes with an “Actual start date” in the future.

For currently active changes against the configuration item.

For outages that were recently completed against the configuration item. outages with an “end” date in the past.

For outages that are planned soon against the configuration item. outages with a “begin” date in the future.

For currently active outages against the configuration item that have a “begin” date in the past and no “end” date

This will only show up in the Tree view and indicates that a configuration item that is downstream has at least one of the above issues against it.

The system looks 5 calendar days in the past and 7 calendar days in the future when looking at recent outages and changes.

**Business service tables**

In the CMDB, the Business Service table (cmdb_ci_service) stores information about business services.

A business service is work or goods that are supported by an IT infrastructure. For example, delivering email service to an employee can require services such as email servers, web servers, and the work to configure the user’s account. A business service management map graphically displays the configuration items (CI) that support a business service and the relationships between the configuration items.

The Business Service table (cmdb_ci_service) stores the business services in the CMDB.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Business criticality | The importance of this service to the business. This field can be used to determine disaster recovery strategies for this service. Default options are:  
  - 1 - most critical  
  - 2 - somewhat critical  
  - 3 - less critical  
  - 4 - not critical |
<p>| SLA                | A reference to the Agreement (sla) table.                                                   |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service classification</td>
<td>Designates the type of the service.</td>
</tr>
<tr>
<td></td>
<td>• Business Service (For more information, see Business services)</td>
</tr>
<tr>
<td></td>
<td>• Technical Service (For more information, see Create a technical service)</td>
</tr>
<tr>
<td></td>
<td>• Service Offering (For more information, see Add service offerings)</td>
</tr>
<tr>
<td></td>
<td>• Shared Service (For more information, see IT shared services)</td>
</tr>
<tr>
<td></td>
<td>• Application Service (To represent a service that is classified as a business application)</td>
</tr>
<tr>
<td></td>
<td>• Billable Service (To represents a service that is billed, or that is cost managed)</td>
</tr>
<tr>
<td>Used for</td>
<td>Designates how this service is used. Default options are:</td>
</tr>
<tr>
<td></td>
<td>• Production</td>
</tr>
<tr>
<td></td>
<td>• Staging</td>
</tr>
<tr>
<td></td>
<td>• QA</td>
</tr>
<tr>
<td></td>
<td>• Test</td>
</tr>
<tr>
<td></td>
<td>• Development</td>
</tr>
<tr>
<td></td>
<td>• Demonstration</td>
</tr>
<tr>
<td></td>
<td>• Training</td>
</tr>
<tr>
<td></td>
<td>• Disaster Recovery</td>
</tr>
<tr>
<td>Users supported</td>
<td>The users that this service supports. A reference to the Group (sys_users_group) table.</td>
</tr>
<tr>
<td>Version</td>
<td>Use this field for your own versioning processes.</td>
</tr>
</tbody>
</table>

The Service Configuration Item Association table

The Service Configuration Item Association table (svc_ci_assoc) binds a business service and a configuration item (CI) to track which CIs are part of each business service.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Item Id</td>
<td>A reference to the configuration item (cmdb_ci) table.</td>
</tr>
<tr>
<td>Service Id</td>
<td>A reference to the business service (cmdb_ci_service) table.</td>
</tr>
</tbody>
</table>

The Service Relationship Association table

The Service Relationship Association table (svc_rel_assoc) binds a business service and a relationship to track which relationships are part of a business service.
The Service Relationship Association table

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relation Id</td>
<td>A reference to the CI Relationship (cmdb_rel_ci) table.</td>
</tr>
<tr>
<td>Service Id</td>
<td>A reference to the Business Service (cmdb_ci_service) table.</td>
</tr>
</tbody>
</table>

Table form views

When you view a table definition form, you can open the context menu, and select a form view in which to display the table. The default view for a table is the Default view. For any class that is an extension of the CMDB table, you can select the CI Definition view which provides additional access to related tables and information.

The CI Definition form view is a centralized location from which you can configure and view a table. In addition to the information that the default view displays, the CI Definition form view provides the following controls,

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Icon tab</td>
<td>View and create new NG-BSM icons for CI types</td>
</tr>
<tr>
<td>CI Identifier tab</td>
<td>View and create new CI identifiers</td>
</tr>
<tr>
<td>Reconciliation Definitions</td>
<td>View and create new data source definitions</td>
</tr>
<tr>
<td>Inclusion related link</td>
<td>Links to the Metadata Editor</td>
</tr>
</tbody>
</table>

To access these additional controls on the CI Definition form view, you need to first create a new table that is derived from the CMDB table, and then view it using the CI Definition form.

Content packs for Configuration Management (CMDB)

Solutions contain preconfigured dashboards. These dashboards contain actionable data visualizations that help you improve your business processes and practices.

**Note:** To evaluate the functionality, you can activate Performance Analytics solutions and in-form analytics on instances that have not licensed Performance Analytics Premium. However, you have the following limitations:

- You cannot create new indicators.
- You cannot collect data older than 180 days.

For full functionality, license Performance Analytics Premium. For more information, see [Get started with Performance Analytics Premium](#).

Content packs

The Performance Analytics widgets on the dashboard visualize data over time, which allows you to analyze your business processes and identify areas of improvement. With content packs, you can get value from Performance Analytics for your application with minimal setup.
Note: Content packs include some dashboards that are inactive by default. You can activate these dashboards to make them visible to end users according to your business needs.

To enable the content pack for Configuration Management (CMDB), an admin can navigate to Performance Analytics > Guided Setup. Click Get Started then scroll to the section for Configuration Management (CMDB). The guided setup takes you through the entire setup and configuration process.

Dependency Views

Dependency Views graphically displays an infrastructure view for a configuration item (CI) and the business services that it is part of and that it supports. Dependency Views indicates the status of its configuration items, and allows access to CIs related alerts, incidents, problems, changes, and business services.

If Service Mapping is activated, Dependency Views maps are enhanced to display dependencies that reflect connections in service maps.

Explore
- Dependency Views release notes
- Upgrade to Jakarta

Administer
- Create or modify Dependency Views map indicators
- Create or modify map icons
- Create a predefined filter
- Create or modify Map Related Items
- Create or modify Dependency Views menu actions
- Create or edit a dependency type

Use
- Dependency Views map
- Dependency Views map menus and controls
- View a Dependency Views map
- Change the layout of Dependency Views map
- Filter the view of a Dependency Views map
- Perform actions on nodes in a Dependency Views map
- Supported browsers for Dependency Views

Develop
- Developer training
- Developer documentation
- Components installed with Dependency Views

Integration
- Display metrics for CIs in a Dependency Views map

Troubleshoot and get help
- Ask or answer questions in Now Community
- Search the Hi knowledge base for known error articles
- Contact ServiceNow Technical Support

Components installed with Dependency Views

The Dependency Views plugin adds tables and system properties.

Tables installed with Dependency Views

Dependency Views adds the following tables.
<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available CI icons (ngbsm_ci_icons)</td>
<td>Stores all available CI class icons.</td>
</tr>
<tr>
<td>Icons for CI types (ngbsm_ci_type_icon)</td>
<td>Maps icons to CI class names.</td>
</tr>
<tr>
<td>Map Script (ngbsm_script)</td>
<td>Custom scripts that run in real time and generate a custom view of a map for a specific CI.</td>
</tr>
<tr>
<td>Map View (ngbsm_view)</td>
<td>Serialized map views saved by users.</td>
</tr>
<tr>
<td>Map Filter (ngbsm_filter)</td>
<td>Filters saved by users.</td>
</tr>
<tr>
<td>Menu Action (ngbsm_context_menu)</td>
<td>Default and custom context menu actions that appear when users right click a map.</td>
</tr>
<tr>
<td>Related Item (ngbsm_related_item)</td>
<td>Stores which reference fields should be treated as relationships when building the map. This allows users to include CIs that are related via a reference field instead of a relationship.</td>
</tr>
<tr>
<td>Edge Colors (bsm_edge_color)</td>
<td>Color definitions to use when drawing the relationships between nodes based on relationship type.</td>
</tr>
<tr>
<td>Map Indicator (bsm_indicator)</td>
<td>Stores all map indicators.</td>
</tr>
<tr>
<td>BSM Saved Map (bsm_graph)</td>
<td>Details of maps.</td>
</tr>
<tr>
<td>BSM Map Actions (bsm_action)</td>
<td>Actions on the map.</td>
</tr>
<tr>
<td>BSM Map View (map_view)</td>
<td>Parents’ predefined filters.</td>
</tr>
<tr>
<td>Map View Configuration Types (map_view_ci_type)</td>
<td>Configuration type filters, limiting the CI class types to be displayed, per predefined filter.</td>
</tr>
<tr>
<td>Map View Relationship Types (map_view_rel_type)</td>
<td>Relationship type filters, limiting the links to be displayed between CIs, per each predefined filter.</td>
</tr>
<tr>
<td>(map_viewroles)</td>
<td>Roles that a specific predefined filter should be applied to.</td>
</tr>
<tr>
<td>CI Filters (map_filter)</td>
<td>CI attribute filters, limiting the CIs to be displayed, per predefined filter.</td>
</tr>
</tbody>
</table>

Properties installed with Dependency Views

Dependency Views adds the following properties.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of CIs to display on a map at once</td>
<td>The maximum number of nodes to retrieve from the database. If more nodes exist in the database, they are not displayed in the map.</td>
</tr>
</tbody>
</table>
| glide.bsm.max_nodes                                                     | - **Type:** Integer  
- **Default value:** 1000  
- **Location:** Dependency Views &gt; Map Properties                                                                                          |
| Maximum level depth from the root CI that can be initially displayed in Dependency Views. Range is 1 to 49 | Level depth is the graph distance between the root CI and a node.                                                                                                                                           |
| glide.bsm.max_levels                                                    | - **Type:** Integer  
- **Default value:** 3  
- **Other possible values:** 1-49  
- **Location:** Dependency Views &gt; Map Properties                                                                                              |
| Show children of virtual groups                                         | Display the continuation of the map underneath virtual group. Virtual links are used to connect virtual groups to their child nodes.                                                                          |
| glide.bsm.show_virtual_node_children                                   | - **Type:** Yes / No  
- **Default value:** No  
- **Location:** Dependency Views &gt; Map Properties                                                                                             |
| Maximum number of child nodes to display (the rest will be collapsed)   | Maximum number of nodes (of a similar CI type and at the same level) to display before applying virtual grouping. Nodes are collapsed for the map to meet this limit.                                              |
| glide.bsm.too_many_children                                             | - **Type:** Integer, valid values 1 or greater  
- **Default value:** 10  
- **Location:** Dependency Views &gt; Map Properties                                                                                             |
| A value of true indicates that filtered out items will be removed from the graph along with any disconnected children while a value of false indicates that the items will be dimmed in color | - **Type:** Yes / No  
- **Default value:** Yes  
- **Location:** Dependency Views &gt; Map Properties                                                                                             |
| glide.ngbsm.filters_remove_filtered_items                               |                                                                                                                                                    |
| Maximum number of relations per node                                   | The maximum number of relations to retrieve from the database. If more relations exist in the database, they are not displayed in the map.                                                              |
| glide.bsm.max_num_rels                                                  | - **Type:** Integer, valid values 1 or greater  
- **Default value:** 100  
- **Location:** Dependency Views &gt; Map Properties                                                                                             |
| A value of true indicates that when filters are changed the graph will recalculate it's layout using the currently selected layout algorithm | - **Type:** Yes / No  
- **Default value:** Yes  
- **Location:** Dependency Views &gt; Map Properties                                                                                             |
<p>| glide.ngbsm.filters_run_layout_automatically                             |                                                                                                                                                    |</p>
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| A value of true indicates that when filters are changed the graph will be fit to the screen automatically glide.ngbsm.filters_fit_to_screen_automatically | • **Type:** Yes | No  
• **Default value:** No  
• **Location:** Dependency Views > Map Properties                                  |
| A value of true allows relationship lines to be drawn using smooth curves instead of straight line segments. These curves can be more taxing on the browser, setting to false may improve fluidity of animation and interaction for Dependency Views glide.ngbsm.performance_allow_curves | • **Type:** Yes | No  
• **Default value:** Yes  
• **Location:** Dependency Views > Map Properties                                      |
| Amount of time in milliseconds a notification stays on the screen glide.ngbsm.notification_display_time | • **Type:** Integer  
• **Default value:** 5000  
• **Location:** Dependency Views > Map Properties                                        |
| The maximum amount of results displayed when searching for CIs glide.ngbsm.search_ci_limit | • **Type:** Integer  
• **Default value:** 10  
• **Location:** Dependency Views > Map Properties                                           |
| The maximum amount of results displayed when searching for Relationship Types glide.ngbsm.search_rel_type_limit | • **Type:** Integer  
• **Default value:** 5  
• **Location:** Dependency Views > Map Properties                                             |
| When available, the map should display the class labels for each CI glide.ngbsm.show_class_labels | • **Type:** Yes | No  
• **Default value:** Yes  
• **Location:** Dependency Views > Map Properties                                               |
| Truncate node labels to a single line and to fit available space (default). Disable to display entire labels on multiple lines and wrapped as needed glide.ngbsm.truncate_long_labels | If glide.ngbsm.show_class_labels is enabled, then the class label always displays on top of the CI label, and wrapping applies to both the class and the CI labels.  
• **Type:** Yes | No  
• **Default value:** No  
• **Location:** Dependency Views > Map Properties                                               |
| Minimum horizontal distance between nodes in horizontal layout glide.bsm.layout_horizontal_spacing_x | The distance is measured in pixels between one node’s center to another node’s center.  
• **Type:** Integer  
• **Default value:** 200  
• **Location:** Dependency Views > Map Properties                                               |
| Minimum vertical distance between nodes in horizontal layout glide.bsm.layout_horizontal_spacing_y | The distance is measured in pixels between one node’s center to another node’s center.  
• **Type:** Integer  
• **Default value:** 100  
• **Location:** Dependency Views > Map Properties                                               |
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum horizontal distance between nodes in vertical layout</td>
<td>The distance is measured in pixels between one node’s center to another node’s center.</td>
</tr>
<tr>
<td>glide.bsm.layout_vertical_spacing_x</td>
<td>- Type: Integer</td>
</tr>
<tr>
<td></td>
<td>- Default value: 125</td>
</tr>
<tr>
<td></td>
<td>- Location: Dependency Views &gt; Map Properties</td>
</tr>
<tr>
<td>Minimum vertical distance between nodes in vertical layout</td>
<td>The distance is measured in pixels between one node’s center to another node’s center.</td>
</tr>
<tr>
<td>glide.bsm.layout_vertical_spacing_y</td>
<td>- Type: Integer</td>
</tr>
<tr>
<td></td>
<td>- Default value: 125</td>
</tr>
<tr>
<td></td>
<td>- Location: Dependency Views &gt; Map Properties</td>
</tr>
</tbody>
</table>

### Dependency Views map

ServiceNow® Dependency Views maps graphically display configuration items that support business services and the relationships between the configuration items.

A ServiceNow business service is work or goods that are supported by an IT infrastructure. For example, delivering email service to an employee can require services such as email servers, web servers, and the work to configure the user’s account.

A Dependency Views map has one starting point, called the root CI or root node of the map. The root CI is surrounded by a darker frame that repaints itself with a pulsing effect drawing the attention to the root CI. The maps can show both upstream and downstream dependencies for the root CI. By default the Dependency Views map displays 3 levels, both upstream and downstream relationships. Administrators can configure the number of levels displayed. The map collapses and expands clusters to make them easier to view. By default, clusters are collapsed.

In a Dependency Views map, map indicators indicate if a CI has any active, pending issues. You can investigate the tasks that are connected to a CI to get more details. When you return to the map from another form, the system restores the last map viewed, using the default filter and layout settings. When you click the icon ( ) on a CI record or on a task record that identifies a CI, the map opens.

Many of the relationships in map are created through the discovery process. You can also create, define, and delete CI relationships in the map. You can display the map from different perspectives and open specific records that relate to configuration items. The system refreshes the map automatically to reflect changes to the CMDB.

---

**Note:** CIs not extended from the Configuration Item (cmdb_ci) table, are not displayed in Dependency Views maps and in CI relation formatters.

The Dependency Views module is active in all instances, and includes demo data.
Dependency Views sample map

When you click the map icon ( ) on a CI record or on a task record that identify a CI, a map opens.

Roles

Users with the itil and ecmdb_admin roles can view maps and perform all actions in the map. Actions include access to the map views and saved filters, both from the lists in the map and from the Saved Filters module.

Dependency Views map menus and controls

Dependency Views maps contain the following menus and controls.
## Map options

The following options are available across the top of the map.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Menu to save, load and export views of the map.</td>
<td>Menu to save, load and export views of the map.</td>
</tr>
<tr>
<td>&lt;Root CI&gt;</td>
<td>Next to the menu icon is the name of the current root node (CI) of the map.</td>
</tr>
<tr>
<td>Search for CI</td>
<td>Enter the name of a CI or a business service to load into the map. Alternatively, you can start typing to have the auto-complete feature present a list of CIs and businesses service that match your partial value.</td>
</tr>
<tr>
<td>Vertical</td>
<td>Display the map in vertical view.</td>
</tr>
<tr>
<td>Horizontal</td>
<td>Display the map in horizontal view.</td>
</tr>
<tr>
<td>Radial</td>
<td>Display the map in radial view.</td>
</tr>
<tr>
<td>Force</td>
<td>Centers the elements around the parent CI, regardless of upstream or downstream relationships.</td>
</tr>
<tr>
<td>Group</td>
<td>Groups the elements according to their CI type.</td>
</tr>
<tr>
<td>Details</td>
<td>Displays related lists such as Problems, Changes and Related Business Services that are associated with the selected CI.</td>
</tr>
<tr>
<td></td>
<td>• Click on a business service, to highlight the CIs that are associated with that business service.</td>
</tr>
<tr>
<td></td>
<td>• Click Related Business Services, then double-click a business service to display the business service map in the Event Management dashboard.</td>
</tr>
<tr>
<td></td>
<td>If the Event Management plugin is active, then events and alerts are also displayed.</td>
</tr>
<tr>
<td>Settings</td>
<td>Set filters for the map.</td>
</tr>
<tr>
<td></td>
<td>Use the navigation tools to increase or decrease the view of the map, rearrange the icons on the map, and move the map on the page.</td>
</tr>
<tr>
<td></td>
<td>• Use the plus sign (++) to increase magnification of the map.</td>
</tr>
<tr>
<td></td>
<td>• Use the minus sign (-) to decrease magnification of the map.</td>
</tr>
<tr>
<td></td>
<td>• Click the center dot to center the map on the page.</td>
</tr>
<tr>
<td></td>
<td>• Use the direction arrows to move the page in that direction.</td>
</tr>
<tr>
<td></td>
<td>• Use the selection tool under the navigation tool to toggle between moving the entire map or moving one CI on the map.</td>
</tr>
</tbody>
</table>
Map menu

The following options are available if you right-click the map background.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run Layout</td>
<td>Redraws the map with the current layout option.</td>
</tr>
<tr>
<td>Fit To Screen</td>
<td>Resizes the map to fit all the nodes in the map window.</td>
</tr>
<tr>
<td>Reset Filters</td>
<td>Performs the same action as the Filters &gt; Reset option.</td>
</tr>
</tbody>
</table>

Node menu

The following options are available if you right-click a node.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Form</td>
<td>Displays the CMDB record of the selected CI in a new tab of the browser.</td>
</tr>
<tr>
<td>View Map</td>
<td>Reloads the map using the selected CI as the new root node, with the currently defined layout setting. This option does not display on the root node.</td>
</tr>
<tr>
<td>View Related Tasks</td>
<td>Displays all tasks or outages associated with the selected CI, including incidents, problems, change requests, and follow-on tasks. This option is always available, even if there are no tasks associated with the CI. This option does not appear on collapsed nodes.</td>
</tr>
<tr>
<td>View Affected CIs</td>
<td>Shows a list of all tasks that have the CI listed as an Affected CI. This option is only visible when you access the map from the map icon in a task record’s Configuration item field.</td>
</tr>
<tr>
<td>View Related Outages</td>
<td>Displays all outages involving the selected CI. This option only appears when there is an outage associated with the CI. This option does not appear on collapsed nodes.</td>
</tr>
<tr>
<td>Add Relationship</td>
<td>This option displays a dotted green line that you can drag to another CI to create a relationship link. A popup dialog allows you to define the relationship type.</td>
</tr>
<tr>
<td>Expand</td>
<td>Displays all CIs and components within a clustered node, or virtual groups (virtual nodes that appear when <code>glide.bsm.too_many_children</code> is reached). This option appears only if the node is a cluster node or a virtual group node. If Load More was previously used, then Expand reverts the results of the Load More operation. The number of additional icons to display is bound by the value of the <code>glide.bsm.max_nodes</code> property.</td>
</tr>
</tbody>
</table>
### Relationship menu

The following options are available if you right-click a relationship link.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>View Relationship Form</strong></td>
<td>Opens the <strong>CI Relationship</strong> form. You can modify the <strong>Parent</strong>, <strong>Type</strong>, and <strong>Child</strong> of the relationship from this form.</td>
</tr>
<tr>
<td><strong>Modify Relationship</strong></td>
<td>Searches for and selects a new relationship for this link.</td>
</tr>
<tr>
<td><strong>Delete Relationship</strong></td>
<td>Deletes a relationship. The relationship is deleted after prompting for confirmation.</td>
</tr>
</tbody>
</table>

### Supported browsers for Dependency Views

The latest version or service pack of internet browsers are required to view and manipulate Dependency Views maps.

The Dependency Views module supports the latest version or service pack of the following browsers:

- Firefox with the latest ESR
- Chrome version 25 or later (latest version recommended)
- Safari version 6 or later
- Microsoft Internet Explorer (IE) version 9 or later

The Dependency Views module is not supported on tablets and on mobile devices.

### Cluster nodes in a Dependency Views map

Dependency Views maps can display cluster group nodes alongside individual CI nodes, and the child nodes of these cluster groups.
Clusters are CIs in the Cluster (cmdb_ci_cluster) table. A cluster CI is an organized set of computer CIs that work together as a single system. Each node in a cluster group represents a CI, typically a server, that can have referenced hardware, such as disks and network adapters.

Cluster nodes on a Dependency Views map can display in two modes:

- Collapsed mode: Displays only the cluster CI node without its child CI nodes. This mode avoids unnecessary clutter in large maps.
- Expanded mode: Displays the cluster CI node and all its child CI nodes.

Menu options available for a clustered node include **Collapse** and **Expand** which allow you to control the density on the map.

By default, Dependency Views collapses all cluster groups and displays clusters in collapsed mode on the map.

**Annotation**

Icons for cluster nodes and cluster group CI nodes are noted by the string “Cluster” and by a unique cluster icon. The system searches through all the component nodes in a cluster CI or collapsed node looking for tasks, outages, and trouble, such as incidents, problems, or change requests. This search evaluates only the number of levels that are displayed in the diagram.
An expanded cluster node displaying its child nodes
Virtual grouping of nodes in a Dependency Views map

To reduce the density on a map, Dependency Views automatically groups CIs of a similar CI type from the same level.

A large number of nodes can cause a Dependency Views map to become too dense to be helpful. Therefore, if the number of nodes with a similar CI type from same level, exceeds the value of the Maximum number of nodes (of a similar CI type and at the same level) to display before applying virtual grouping property, then those nodes are automatically grouped into a virtual group. A single node, the virtual group node is displayed to represent the virtual group, while all actual nodes in the virtual group (that are of a similar CI type), are hidden. Virtual group nodes represent CIs of a similar CI type but are not CIs by themselves and cannot have tasks assigned to them. The number of actual collapsed nodes in the virtual group is noted on the virtual group node.

By default, child nodes of a virtual group are not displayed. You can enable the Show children of virtual groups property to display child nodes underneath virtual groups.

Virtual grouping is not applied at the level underneath a virtual group even if the criteria for virtual grouping is met (the number of nodes with a similar CI type from that level exceeds the preconfigured property value). However, virtual grouping can happen at the following level if that criteria is met. This behaviour does not depend on any property settings, and you cannot change it.

Menu options for a virtual group include Expand and Collapse, which allow you to apply virtual grouping and display only the virtual group node, or to undo the virtual grouping and display all actual nodes.

Virtual links

A virtual node is connected to other nodes with a virtual link. A virtual link denotes that there such link between at least one CI in the virtual group, to another CI node on the map.

**Note:** Predefined filters do not apply to virtual groups. Therefore a virtual group displays even if it contains CIs that a predefined filter would have excluded. Upon the expansion of a virtual group, predefined filters are applied, and any or all of the CIs that were previously virtually grouped, might no longer display on the map.

Also, when using the node menu option Load More, virtual grouping is not applied at the newly loaded level even the criteria for virtual grouping is met.
An expanded virtual group
Use Dependency Views

Use the layout controls on a Dependency Views map to display elements in different configurations for easier management. Use the filter panel on the map to display fewer levels or to filter out elements you don't want to see, then save the filter for use later. Draw new relationships between elements or edit existing relationships.

View a Dependency Views map

When you display a Dependency Views map using one of the options below, the map is centered on the root CI, and displays the layout and number of levels defined in the map properties. If ITOM Metric Management is activated, then a Dependency Views map provides a mode that lets you directly access metrics information for the CIs on the map.

General role requirements:
- To access a Dependency Views map from either the navigation menu, a script API, or directly from a URL, the minimum role required is the dependency_views. Some operations that are related to icons, indicators, and menu actions require the ecmdb_admin role. Some operations that are related to properties and dependency types require the admin role.
- Dependency Views enforces ACL permissions on CIs, and visually hides them and their relationship from the map if the permission requirement is not met.

The maps generated by Dependency Views are based on D3 and Angular technology, providing a modern interactive graphical interface to visualize configuration items and their relationships.

If Service Mapping is activated, Dependency Views maps are enhanced to display dependencies that reflect connections in service maps. In addition, the list of related business services in the Details section includes business services that were discovered by Service Mapping. All CIs that are included in a business service, are displayed underneath the business service node on the map.

Maps provided by Service Mapping are for business services, including comprehensive maps from the perspective of business services. For more information, see Service Mapping.

Administrators can configure the setting for the default layout of the map and number of levels displayed. When you access the map from a saved view, the map opens using the properties in the saved view, and not the default map properties.

Navigate to Dependency Views and open one of these modules:
- View Map in New Tab: Opens the map in a new, full screen tab without the application navigator.
- View Map: Opens the map in the content pane of the current tab.
- Saved Views: Opens a view of a map that you previously saved.

Click a number in the Version column, and then click the ( ) icon.

Save or load a Dependency Views map

In the View Map module, use the menu icon to save and load Dependency Views maps.

1. Navigate to Dependency Views > View Map.
2. Click the menu icon ( ).
3. Select Save View, Load View, or Last View.

Delete a saved Dependency Views map view

Use the Saved Views module to delete a previously saved view.

1. Navigate to Dependency Views > Saved Views.
2. Use the checkbox in the first column of the table to select the map view that you wish to delete.
3. Select Delete from the Actions on selected rows drop-down menu.

Change the layout of Dependency Views map

You can select from different layout options for your Dependency Views map.

1. Navigate to Dependency Views > View Map.
2. Select one of the following layout options from the menu across the top of the view.
   - Vertical: Displays the elements in a vertical tree pattern according to their upstream and downstream relationships. This is the default value for the initial display of the map.
   - Horizontal: Displays the elements in a horizontal tree pattern according to their upstream and downstream relationships.
   - Radial: Displays the elements in a radial pattern according to their upstream and downstream relationships.
   - Force: Centers the elements around the parent CI, regardless of upstream or downstream relationships.
   - Group: Groups the elements according to their CI type.
   - Details: Displays related alerts, incidents, problems, and business services. If Service Mapping is activated, then the list of related business services includes business services that were discovered by Service Mapping.

   Click Related Business Services and then double-click a business service to display the business service map in the Event Management dashboard.

Filter the view of a Dependency Views map

You can filter a Dependency Views map to display specific types or categories of configuration items.

Use the filter panel to control which elements of the map are displayed and to save versions of a filter for later use.

1. Navigate to Dependency Views > View Map.
2. 
   
   Click the button to open Map Settings. Click a filter strip to expand or collapse it, and to set filter items.
<table>
<thead>
<tr>
<th>Filter panel strips and options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save Custom Settings</td>
<td>Configure desired custom settings, then enter a name and click <strong>Save</strong>. Custom settings can be loaded by using the <strong>Load Saved Custom Settings</strong> option. Navigate to <strong>Dependency Views &gt; Saved Settings</strong> to display all saved custom settings.</td>
</tr>
<tr>
<td>Load Custom Settings</td>
<td>Apply previously saved custom settings to the current map.</td>
</tr>
<tr>
<td>Predefined Filters</td>
<td>Apply <strong>previously defined filters</strong> consisting of configuration type, CI type, and relationship filters. You can <strong>Set a predefined filter as default</strong>. This filter is applied first, before any other filters (such as <strong>Filter CIs by Depth</strong>) are applied.</td>
</tr>
<tr>
<td>Dependency Type</td>
<td>Apply a filter that runs in real time and generates a custom view of a service map for a specific CI.</td>
</tr>
<tr>
<td>Max Levels</td>
<td>Designate how many levels from the root CI display on the map.</td>
</tr>
<tr>
<td>Filter CIs by Depth</td>
<td>Designate which levels of CI display on the map.</td>
</tr>
<tr>
<td>Filter CIs by CI Type</td>
<td>Designate what CI types display in the map.</td>
</tr>
<tr>
<td>Filter CIs By CI Location</td>
<td>Designate what CI locations display in the map.</td>
</tr>
<tr>
<td>Filter CIs By CI Manufacturer</td>
<td>Designate what CI manufacturers display in the map.</td>
</tr>
<tr>
<td>Filter CIs By Audit Failure</td>
<td>Hides CIs that failed the CMDB health staleness test. This option is available only if there are any such CIs.</td>
</tr>
<tr>
<td>Filter Relationship Types</td>
<td>Designate what relationship types display in the map.</td>
</tr>
<tr>
<td>Map Indicators</td>
<td>Designate what types of tasks display and get counted in the map.</td>
</tr>
<tr>
<td>Remove Filtered Items</td>
<td><strong>Off</strong>: Gray out filtered items on the map. <strong>On</strong>: Do not display filtered items on the map.</td>
</tr>
<tr>
<td>Run Layout Automatically</td>
<td><strong>On</strong>: The configured layout to the map is reapplied whenever the filter is changed. <strong>Off</strong>: The map layout remains static when the filter is changed.</td>
</tr>
<tr>
<td>Filter panel strips and options</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Fit to Screen Automatically | **On:** The map magnification will increase or decrease automatically to display all CIs on the map.  
**Off:** The map magnification remains unchanged when the map is reloaded. |

### Display metrics for CIs in a Dependency Views map

Operational Metrics processes metrics data for CIs, calculates statistics and aggregations, and detects metrics anomalies. A Dependency Views map lets you switch to metrics mode to directly access the Metric Explorer that displays metrics data for CIs on the map.

The ITOM Metric Management (com.snc.sa.metric) plugin must be activated to enable this functionality, and metrics data needs to be processed for the CIs on the Dependency Views map.

Open a Dependency Views map in metric mode which integrates a Dependency Views map with the Metric Explorer functionality that is tailored to the map. In this mode, you can access Metric Explorer functions directly from the map, to explore metrics data for the CIs on the map. All map CIs are accessible in the right hand side pane, from where you can drill into metrics data.

1. Navigate to **Dependency Views > View Map** to open a map.
2. Right-click on a CI on the map and select **View Metrics** to open the Dependency View map in metrics mode.

   In the panel on the right side, the CI that you selected on the Dependency View map is selected by default, and the list of all the metrics available for that CI are displayed.

3. Click the `<` sign on the left of the CI to display all the CIs that you can explore metrics for.

   The Metric Explorer is scoped for exploring only the CIs that currently display on the Dependency Views map, and you cannot add or remove CIs from the list. If you use map settings or filters to filter out CIs from the map, the same filtering will apply to the list of CIs that you can explore metrics for.

4. Click on a CI in the CIs list or right-click on a CI on the Dependency Views map, to drill down to the CI’s metrics.

5. Click the **Dependencies Map** tab or the **Metrics** tab to switch modes:
   a) **In Metrics** mode: The full functionality of the Metric Explorer is available, you can create metric charts by dragging metrics into the canvas. You can modify chart settings, select different time ranges for the charts, and perform other actions as described in [View metric values in the Metric Explorer](#).
   b) **In Dependencies Map** mode: Select a CI on the map to drill down to its metrics data, drop-down the **Layout** list to choose a different layout, or modify map settings.

### Perform actions on nodes in a Dependency Views map

You can view various related items for the nodes in a Dependency Views map.

If the node is a collapsed node or represents a cluster, the incidents, problems and change requests are for all the collapsed nodes.

1. Navigate to **Dependency Views > View Map**.
2. Click the ▼ icon next to a node or right-click a node on the map, to access the following menu items:

<table>
<thead>
<tr>
<th>Node Menu</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Form</td>
<td>Displays the CMDB record of the selected CI in a new tab of the browser.</td>
</tr>
<tr>
<td>View Map</td>
<td>Reloads the view using the selected CI as the new root node, with the currently defined layout setting. This option does not display on the root node.</td>
</tr>
<tr>
<td>View Related Tasks</td>
<td>Displays all tasks or outages associated with the selected CI, including incidents, problems, change requests, and follow-on tasks. This option is always available, even if there are no tasks associated with the CI. This option does not appear on collapsed nodes.</td>
</tr>
<tr>
<td>View Affected CIs</td>
<td>Shows a list of all tasks that have the CI listed as an Affected CI. This option is only visible when you access the view from the view icon in a task record’s Configuration item field.</td>
</tr>
<tr>
<td>View Related Outages</td>
<td>Displays all outages involving the selected CI. This option only appears when there is an outage associated with the CI. This option does not appear on collapsed nodes.</td>
</tr>
<tr>
<td>Add Relationship</td>
<td>This option displays a dotted green line that you can drag to another CI to create a relationship link. A popup dialog allows you to define the relationship type.</td>
</tr>
<tr>
<td>Expand</td>
<td>Displays all CIs and components within a cluster node or a collapsed node. This option only appears if the node is a collapsed or cluster node.</td>
</tr>
<tr>
<td></td>
<td>The number of additional icons to display is bound by the value of the glide.bsm.max_nodes property.</td>
</tr>
<tr>
<td>Collapse</td>
<td>Collapses all CIs and components within a cluster node or a collapsed node back to a single node. This option only appears if the node has been expanded using the Expand menu item.</td>
</tr>
<tr>
<td>Run Layout From Here</td>
<td>This option re-runs the chosen layout using the current node. Use this option to get a new or clearer view on the same map.</td>
</tr>
<tr>
<td>Load More</td>
<td>Starting at the selected icon, loads the next level of the map, past the setting of Max Levels.</td>
</tr>
<tr>
<td></td>
<td>The number of additional icons to display is bound by the value of the glide.bsm.max_nodes property.</td>
</tr>
</tbody>
</table>
Export a Dependency Views map

You can export a Dependency Views map to an image in PNG format.

1. Navigate to Dependency Views > View Map.
2. Configure the map view as you want the image to appear. The exported image displays the current view of the map.
3. Click the menu icon ( ).
4. Click Export Image.
5. Right-click the image and select Save Image As, Print, or any other menu option.

Note: You can not export images from a Dependency Views map using Internet Explorer as your browser.

6. Click the "X" button to close the Export Image window.

View collapsed nodes in a Dependency Views map

Cluster and virtually grouped nodes can be displayed in a collapsed mode to avoid unnecessary clutter in large maps.

1. To expand a collapsed node, right-click the CI and select Expand from the context menu.
2. To collapse an expanded cluster node with children, right-click the CI and select Collapse from the context menu.

Administer Dependency Views

Users with the admin role can control the appearance and behavior of Dependency Views by configuring map indicators, map related items, map icons, and menu actions.

Create or modify Dependency Views map indicators

Dependency Views maps uses icons to display additional information for a CI by displaying its related records such as alerts, outages, incidents and problems. These icons are called map indicator.

The default configuration includes map indicators for the following record types:
- Open incident.
- Open alert.
- Unplanned current outage.
- Planned current outage, or an open problem.
- Current, planned, or recent change request.

You can filter out the display of affected CIs, alerts, current change requests, incidents and problems from the Settings menu. Also, you can create a map indicator to define additional record types, such as trouble sources for business service CIs. You can also modify an existing map indicator, for example to use a different color scheme or to alter the priority of a task.

The Affected CI’s map indicator appears for CIs in two related but not identical situations. It appears for CIs for which tasks such as change request, incident, or problem were directly created for, and for any CIs that were added in those tasks (parent tasks) as Affected CIs (The CI for which a task is directly created for, is automatically added as an affected CI in that task).
The state of affected CI’s depends on the status of the respective parent task. For as long as the parent task is active, the associated affected CIs continue to be impacted by the task issue. In a Dependency Views map, the Affected CI’s indicator displays for all affected CIs for as long as the parent task is active. On a Dependency Views map, the Affected CI tooltip displays the details of the task records in which the CI was added as an affected CI. However, the Details pane does not contain an Affected CI’s tab, and no further details about affected CIs, or the associated tasks are displayed. After the parent task is closed, the Affected CI’s indicator no longer displays for any of the tasks’ affected CIs. For information about affected CIs in Change Management, see [Associate CIs to a change request](#).

**Note:** Details about affected CIs are derived from the task and the cmdb_ci tables and their extensions. Therefore, if you use custom tables to store CIs for incidents, problems and changes, it affects the details that are displayed for affected CIs.

For more information on how map indicators are used to show tasks and outages in clusters and collapsed nodes, see [Cluster nodes in a Dependency Views map](#).

1. Navigate to **Dependency Views > Map Indicators**.
2. Click **New** to create a new map indicator, or click the name of an indicator from the **Table** column to modify an existing map indicator.
3. Fill in the fields on the form, as appropriate.

### Map Indicator form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Table</strong></td>
<td>Name of the table represented by this map indicator. <strong>Note:</strong> The list shows only tables and database views that are in the same scope as the map indicator. Views are not supported, although included in the list.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Name of the indicator.</td>
</tr>
<tr>
<td><strong>Order</strong></td>
<td>Priority order of the task. The highest priority task is the indicator with the lowest order number. When more than one indicator is present on a CI, the displayed color is the color associated with the highest priority task. Additionally, a glyph on a CI displays the color indicator of the highest priority task attached to that CI.</td>
</tr>
<tr>
<td><strong>Icon</strong></td>
<td>File name and path of the icon image file, which can be a system image.</td>
</tr>
<tr>
<td><strong>CMDB CI field</strong></td>
<td>Name of the field on the selected table that contains the configuration item.</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>
<tbody>
<tr>
<td>Start field</td>
<td>The record property that determines the time-point on the metric chart timeline for placing records in the Metric Explorer. Possible values depend on the selected table. For example, the incident indicator has values such as Actual end, Actual Start, and Approval Set.</td>
</tr>
<tr>
<td>Description field</td>
<td>Name of the field on the selected table that contains the description of the configuration item.</td>
</tr>
<tr>
<td>Description</td>
<td>Text to display when hovering over the indicator. Alphanumeric characters and spaces are valid for this field.</td>
</tr>
<tr>
<td>Conditions</td>
<td>Condition builder that specifies for which CIs to apply this indicator. For example, a CI that has a current past outage is highlighted for 5 days. You can configure a condition to designate a different timeframe for what is considered to be current.</td>
</tr>
<tr>
<td>Active in Service Map</td>
<td>Enable to make the toggle for the specified table available in the Settings dialog box for Business Service maps. You can then toggle between displaying or not displaying the respective records on the map.</td>
</tr>
<tr>
<td>Active Dependencies</td>
<td>Enable to make the toggle for the specified table available in the Settings dialog box for Dependency Views maps. You can then toggle between displaying or not displaying the respective records on the map.</td>
</tr>
<tr>
<td>Active in Metrics</td>
<td>Enable to make the toggle for the specified table available in the Settings dialog box for the Metric Explorer. You can then toggle between displaying or not displaying the respective records on the Map Explorer.</td>
</tr>
<tr>
<td>Label</td>
<td>Text to display for the indicator on the map.</td>
</tr>
<tr>
<td>Tooltip Label</td>
<td>The prefix portion of the tooltip (Tooltip Label : Tooltip info).</td>
</tr>
<tr>
<td>Tooltip Info</td>
<td>The suffix portion of the tooltip (Tooltip Label : Tooltip info).</td>
</tr>
</tbody>
</table>

4. Click **Submit** to enter a new map indicator. Click **Update** to modify an existing map indicator.

For an indicator to appear in a Dependency Views map, a CI must meet all filter conditions, and **Active Dependencies** must be selected.

**Create or modify map icons**

You can upload new icons or modify existing icons to customize the icon displayed for a CI in maps in Dependency Views, Service Mapping, and Event Management.

The icons used in Dependency Views maps are listed in the Map Icons module. Records in the **Map Icons** list are arranged by CI classes, such as cmdb_ci_linux_server. The path to the default
image files is https://<instance name>.service-now.com/images/app.ngbsm/<image name.svg>. For information about uploading images to the database, see Storing images in the database.

Role required: admin or ecmdb_admin roles are required to access the records in this table (ngbsm_icon) to upload new icons.

1. Use the CI Class Manager:
   a) Navigate to Configuration > CI Class Manager.
   b) Select a class in the Class Hierarchy.
   c) In the sidebar on the right, select Icon.

2. Or, navigate to Dependency Views > Map Icons, and click New to create a new map icon or click the name of an existing icon from the Label column to modify an existing icon.

3. Fill in the fields on the form, as appropriate.

Map Icons form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CI Type</td>
<td>Label or the informal name of the CI table that this icon represents in the view.</td>
</tr>
<tr>
<td>Icon</td>
<td>Name of the icon.</td>
</tr>
<tr>
<td>URL</td>
<td>Path to the icon image using the following format: /image name.svg Click the lock icon to enter a new path.</td>
</tr>
</tbody>
</table>

4. Click Submit to enter a new icon. Click Update to modify an existing icon.

You can modify a Dependency Views map indicator to use the new icon.

Create a predefined filter

Create filters to narrow down the CIs that are displayed on a Dependency Views map. You can create filters that are based on CIs’ class, CIs’ attributes, or CIs’ relationships.

Role required: ecmdb_admin

Create a predefined filter that you can then select to determine the scope of the CIs that are displayed in a Dependency Views map. Configuration type filters filter by CI class, CI filters filter by CI attributes, and relationship filters filter by relationships. Only CIs that match at least one of the configuration type filters (if any exists), and at least one of the CI filters (if any exists), and at least one of the relationship type filters (if any exists) - are displayed on the map. If no filters are defined, then no filtering is applied.

Note: Predefined filters do not apply to virtual groups. Therefore a virtual group displays even if it contains CIs that a predefined filter would have not included. Upon the expansion of a virtual group, predefined filters are applied, and any or all of the CIs that were previously virtually grouped, might no longer display on the map.

1. Navigate to Dependency Views > Predefined Filters.
2. On the Predefined Filters page, click New.
3. Type in a Name for the filter. Click Roles, and in the Roles dialog box, select the roles that this filter will be available for.
4. Right-click on the page header, and click Save.
5. To create a configuration type filter:
a) Click Configuration Types, and then click Edit.

b) In the Collection slushbucket, select the classes that CIs must belong to in order to be displayed on the map, and move them to the Configuration Types List.

c) Click Save.

6. To create a CI filter:
   a) Click CI Filters, and then click New.
   b) In the CI Filters page enter conditions to filter CIs by specific attribute values.
   c) Click Submit.

7. To create a relationship type filter:
   a) Click Relationship Type, and then click New.
   b) In the Collection slushbucket, select the relationships that CIs must have in order to be displayed on the map, and move them to the Relationship Types List.
   c) Click Save.

After creating a predefined filter, you can apply it to a map:

1. Click the button to open Map Settings.

2. Select a filter from the Predefined Filters list.

3. Click Apply.

Set a predefined filter as default
You can set a custom predefined filter as the default predefined filter for viewing maps.

1. Create the custom predefined filter to be used as the default predefined filter.

2. On the predefined filter form, click the context menu and select Copy sys_id.

3. Navigate to User Administration > User Preferences.

4. Click New and create a new user preference record using these values:
   - Name: ecmdb.ciview
   - Type: String
   - Value: Paste the sys_id of the custom predefined filter
   - User: Leave blank to create a system-wide setting
   - Description: Description of the predefined filter
   - System: Selected

5. Click Submit.

In Map Settings, when you select the Default option for Predefined Filters, the custom predefined filter that was set, will be applied.

Create or modify Map Related Items
The Map Related Items module relates referenced CIs to one another, which allows them to be displayed in a Dependency Views map.
The base system configuration includes the following tables and relates them to items in the Computer (cmdb_ci_computer) and Server (cmdb_ci_server) tables.

- Disk (cmdb_ci_disk)
- Network Adapter (cmdb_ci_network_adapter)
- Database (cmdb_ci_database)

Some additional referenced CIs that can be related in this manner are file systems and running processes.

In the following example, computer nodes in the map are related to network adapter nodes if the Configuration Item field of the adapter records reference the specific CI node. Access or create a network adapter record from the Network Adapter related list in the cmdb_ci_computer record.

**Dependency Views Configuration Item field**

The Dependency Views map for the *JEMPLOYEE-IBM computer shows the network adapter attached to the computer.
You can configure Dependency Views to display CIs that have no relationship record, but are related to other CIs by reference fields.

1. Navigate to **Dependency Views > Map Related Items**.
2. Click **New** to create a new related item, or click in the row of an existing CI to modify an existing map related item.
3. Fill in the fields on the form, as appropriate.
   - See the Related Items form table.
4. Click **Submit** to enter a new map related item. Click **Update** to modify an existing map related item.

### Related Items form

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuration item</strong></td>
<td>CI that represents the base node or a CI in a table that extends the base node table. In the base system, the configuration item that represents the base node is Computer (cmdb_ci_computer), which includes all types of workstations and servers.</td>
</tr>
<tr>
<td><strong>Related item</strong></td>
<td>Table name of the related item. Only the cmdb_ci table and tables that extend it are displayed in the choice list.</td>
</tr>
<tr>
<td><strong>Related field</strong></td>
<td>Field that links this related item to the configuration item. In many cases, the appropriate value is automatically populated in the field after the first two fields are selected. Select the drop-down menu for additional options.</td>
</tr>
</tbody>
</table>
Create or modify Dependency Views menu actions

To modify an existing menu option, first you create a copy of the original menu action record, and then you modify the copy.

This ensures that your instance can update the record normally during the upgrade process and allows you to quickly restore the original menu option, if necessary.

1. To create a new menu option, navigate to Dependency Views > Map Menu Actions and click New.
   Fill in the fields on the form, as appropriate. See the Menu Action form table.
2. To modify an existing menu option, navigate to Dependency Views > Map Menu Actions.
3. Open the menu action you want to edit.
4. Right-click in the header and click Insert and Stay.
   This step creates a duplicate copy of the menu action and leaves it open for editing.
5. Change the name of the copied record to avoid confusion.
6. Modify the form fields as necessary and save the record.
7. Open the original record and disable it by clearing the Active check box.

Menu Action form

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Descriptive name that appears as the menu option.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box that allows you to enable or disable this record.</td>
</tr>
<tr>
<td>Condition</td>
<td>Condition that triggers the display of this menu option. If the condition evaluates to false the menu option does not display. Script is evaluated in JavaScript in the user's browser and does not have access to all the APIs that Business Rules do. For details on available parameters, see Condition Parameters.</td>
</tr>
<tr>
<td>Item</td>
<td>Map element for which the menu option displays. Valid values are: Canvas for the menu on the map background. Node for the menu on a CI. Relationship for the menu on a relationship link.</td>
</tr>
<tr>
<td>Order</td>
<td>Physical location of the option in the menu. The option with the lowest order number appears first in the menu. All editable and custom options appear below the permanent menu options.</td>
</tr>
</tbody>
</table>
Script

Script that is executed in the browser when the menu option is selected. Script is evaluated in JavaScript in the user's browser and does not have access to all the APIs that Business Rules do.

Type

Menu action type being created, either a menu option or a menu separator. The menu separator is a single line. When the type is a separator, the Script field is ignored.

Condition and script parameters for menu actions

You can use these condition and script parameters for menu actions.

Condition parameters

Note: The usual regular expression conventions are valid in the condition field, such as ! for NOT, && for AND, and || for OR.

The Condition field contains a boolean expression that evaluates to true or false. If the condition is true or if there is no condition, the specified option appears in the menu when you right-click a CI or a relationship link. When you select the option from the menu, ServiceNow executes the associated script.

Common Elements for Building a Condition

<table>
<thead>
<tr>
<th>Text</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>item</td>
<td>Node or reference link's data on which you performed the right-click action.</td>
</tr>
<tr>
<td>item.label</td>
<td>Label of the node.</td>
</tr>
<tr>
<td>item.ci_type</td>
<td>CI's type (table), such as cmdb_ci_service.</td>
</tr>
<tr>
<td>item.name</td>
<td>Name of CIs. CI's type name or the table label, such as Business Service.</td>
</tr>
<tr>
<td>item.location</td>
<td>Location of the CI, such as New York.</td>
</tr>
<tr>
<td>item.manufacturer_name</td>
<td>Name of the CI's manufacturer, such as Dell Inc.</td>
</tr>
<tr>
<td>item.id</td>
<td>The sys_id of the CI.</td>
</tr>
<tr>
<td>item.is_selected</td>
<td>The item that is selected in the map.</td>
</tr>
<tr>
<td>item.level</td>
<td>The current default level.</td>
</tr>
<tr>
<td>item.locationId</td>
<td>The sys_id of the CI node's location.</td>
</tr>
<tr>
<td>item.locationName</td>
<td>The full address of the location.</td>
</tr>
<tr>
<td>item.manufacturerId</td>
<td>The sys_id of the CI's manufacturer.</td>
</tr>
</tbody>
</table>
Valid Conditions for Condition Parameters

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>item.is_collapsed</td>
<td>The node is a collapsed node.</td>
</tr>
<tr>
<td>item.is_cluster</td>
<td>The node is a cluster node.</td>
</tr>
</tbody>
</table>

Script parameters

Menu action scripts are executed on the client when a user clicks the menu option. You can use the same building blocks in scripts as in conditions. Menu action scripts do not function on separators. These are some additional, useful expressions for scripts:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>item.id</td>
<td>The sys_id of the CI node or relationship link.</td>
</tr>
<tr>
<td>item.source</td>
<td>The sys_id of the relationship’s parent or child.</td>
</tr>
<tr>
<td>item.target</td>
<td>The sys_id of the relationship’s parent or child.</td>
</tr>
<tr>
<td>item.label</td>
<td>The name of the CI node, such as IronMail-SD-02.</td>
</tr>
<tr>
<td>item.location</td>
<td>The sys_id of the CI node’s location.</td>
</tr>
<tr>
<td>item.location_name</td>
<td>The full address of the location, such as 4616 Clairemont Drive, North Clairemont, San Diego CA.</td>
</tr>
<tr>
<td>item.manufacturer_id</td>
<td>The sys_id of the CI’s manufacturer.</td>
</tr>
</tbody>
</table>

Create or edit a dependency type

Use one of the dependency types provided, or create a custom dependency type with a script that will execute in real time to generate a custom view of a Dependency Views map for a specific CI.

Create a JavaScript to customize the map. The script must comply with JavaScript syntax guidelines and the directions in the default script template, and it can call platform APIs. Use a dependency type, for example:

- To narrow down and simplify a map, leaving out CIs that are not important for a specific task.
- To include only specific CIs that are hidden by default, such as qualifiers, end-points, and entry points.
- To display virtual relationships that are calculated, and that otherwise do not exist in the CMDB.
- As a tool to plan a new topology deployment that is based on existing resources.

The following dependency types are included in the base system:

**Application to Network Devices**

Returns the network devices in the network paths leading to/from the given CI.

**Network Device to Applications**

Returns the applicative CIs which are target or source of network paths containing the given network device. In addition, returns the hosts of those applicative CIs, and for an applicative CI that is an inclusion, its parent CI is returned too.

**Physical Network Connections**
Returns hosts/network devices that are physically connected to the given host or network device.

**Flow Dependencies**

Returns all the server to server connections that were discovered using the Netflow collector. The script builds a graph based on data in the (sa_flow_server_comm) table. This table contains pairs of services represented by an IP and a listening port that are communicating with each other. For more information, see Data collection and discovery using Netflow and Data collection and discovery using VPC Flow Logs.

1. Navigate to **Dependency Views > Dependency Types**.
2. In the **Load Filter Scripts** list view, select an existing dependency type, or click **New**.
3. Enter or modify a script, adhering to the guidelines and requirements in the script template that is provided.
4. Click **Submit**.

In a Dependency Views map, you can click **Use Dependency Type** to apply a custom script defined in a dependency type.

**Compliance**

Compliance is a tool set that enables administrators to certify ServiceNow data for correctness and fix any discrepancies found in the data.

Compliance offers these certification options to suit the size and requirements of your organization:

### Compliance certification options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desired State</td>
<td>Automatically compares the actual attributes and relationships of specific ServiceNow records against the desired states for those records. For example, an audit can detect a Linux database server with insufficient RAM or whose Depends on relationships with another CI is incorrect. The system then publishes any discrepancies found and automatically assigns follow-on tasks to qualified users to bring that server into compliance.</td>
</tr>
<tr>
<td>Architecture Compliance</td>
<td>Automatically compares the actual attributes of specific CIs, such as CPU count, RAM, or disk size against the expected attributes for those CIs. The system publishes any discrepancies found and automatically assigns remediation tasks to qualified users.</td>
</tr>
</tbody>
</table>

**Compliance Activation**

Compliance functionality is provided by the Certification Core plugin.

The Certification Core plugin which contains shared functionality required for certification audits. It consists of the following plugins, and is activated by default.

- Desired State (activated by default)
Installed with Compliance

These components are installed with the Certification Core plugin.

Demo data is included with the Desired State and Architecture Compliance plugins.

The Certification Core plugin adds or modifies these tables.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit (cert_audit)</td>
<td>Contains all the data required to run an audit, including the users assigned to follow-on tasks and the run schedule.</td>
</tr>
<tr>
<td>Audit Result (cert_audit_result)</td>
<td>Contains the results of specific, certification audits.</td>
</tr>
<tr>
<td>Follow On Task (cert_follow_on_task)</td>
<td>Contains the tasks that were generated from an audit discrepancy.</td>
</tr>
<tr>
<td>Certification Template (cert_template)</td>
<td>Contains the definition of the desired state of the record. The template includes a filter that identifies the records to evaluate and the expected attributes and relationship values. Contains the records to certify, the expected attributes, and the expected relationship values.</td>
</tr>
<tr>
<td>Certification Condition (cert_cond)</td>
<td>Base table that defines the desired attribute or relationship conditions used in templates.</td>
</tr>
<tr>
<td>Certification Attribute Condition (cert_attr_cond)</td>
<td>Contains the conditions that define the desired CI attribute values. This table extends the Certification Condition (cert_cond) base table.</td>
</tr>
<tr>
<td>Certification CI Relationship Condition (cert_ci_rel_cond)</td>
<td>Contains the CI to CI relationship conditions. This table extends the Certification Condition (cert_cond) base table.</td>
</tr>
<tr>
<td>Certification User Relationship Condition (cert_user_rel_cond)</td>
<td>Contains the CI to user relationship conditions. This table extends the Certification Condition (cert_cond) base table.</td>
</tr>
<tr>
<td>Certification Group Relationship Condition (cert_group_rel_cond)</td>
<td>Contains the CI to group relationship conditions. This table extends the Certification Condition (cert_cond) base table.</td>
</tr>
<tr>
<td>Certification Related List Condition (cert_related_list_cond)</td>
<td>Contains the related list conditions. This table extends the Certification Condition (cert_cond) base table.</td>
</tr>
<tr>
<td>Certification Filter (cert_filter)</td>
<td>Contains a certification filter, including the table that contains the records to audit and the filter conditions.</td>
</tr>
</tbody>
</table>
**User roles**

The certification role is automatically assigned to all users with the itil role when the Certification Core plugin is activated or when compliance applications are upgraded. Certification core installs two business rules, both called **Add Certification Role To Manager**, that perform similar tasks on different tables. One rule checks for a manager specified on the User (sys_user) table, and the other checks for the certification role on the User Role (sys_user_has_role) table. When both a manager and the certification role are specified for a user, the system automatically grants the certification role to the manager. This functionality ensures that a certification task can be escalated successfully to the next level. The system grants this automatic role to the user’s immediate manager only and not to others up the management chain.

**Note:** When a manager has only the certification role and no other role, the manager is considered a Requester and is not counted as a subscribed user (Fulfiller).

<table>
<thead>
<tr>
<th>Name</th>
<th>Contains roles</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certification</td>
<td>none</td>
<td>Can read and update certification tasks to resolve discrepancies.</td>
</tr>
<tr>
<td>certification_filter_admin</td>
<td>none</td>
<td>Can create, read, and update certification filters.</td>
</tr>
<tr>
<td>certification_admin</td>
<td>certification, certification_filter_admin</td>
<td>Can manage the entire certification process. These users can create, edit, and delete all certification records.</td>
</tr>
</tbody>
</table>

**UI policies**

**Compliance Certification Core UI policies**

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make table read only</td>
<td>Audit (cert_audit)</td>
<td>Sets the table field derived from the selected filter to read-only.</td>
</tr>
<tr>
<td>Hide Audit Type</td>
<td>Audit (cert_audit)</td>
<td>Hides the Audit type field.</td>
</tr>
<tr>
<td>Hide next scheduled run</td>
<td>Audit (cert_audit)</td>
<td>Hides the Next scheduled run date when an audit is inactive or on-demand.</td>
</tr>
<tr>
<td>Show task fields when create tasks is set to true</td>
<td>Audit (cert_audit)</td>
<td>Displays all fields related to creating tasks when the user selects the Create tasks check box.</td>
</tr>
<tr>
<td>Make name mandatory</td>
<td>Audit (cert_audit)</td>
<td>Makes Name a mandatory field.</td>
</tr>
<tr>
<td>Prevent editing of Last run date</td>
<td>Audit (cert_audit)</td>
<td>Makes Last run date field read-only.</td>
</tr>
<tr>
<td>Name</td>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Show User field                                | Audit (cert_audit)            | Shows or hides fields based on the Assignment type selected. The system shows the User field when you select the following assignment types:  
  • User Field if the Assign to empty option is Create Assigned Task.  
  • Specific User                                                                                                           |
| Show Assign to fields                          | Audit (cert_audit)            | Shows or hides fields based on the Assignment type selected. The system shows the Assign to field when the assignment type is User Field.                                                               |
| Show Assignment Fields                         | Audit (cert_audit)            | Shows or hides fields based on the Assignment type selected. The system shows the Assign to empty field when you select either of the following assignment types:  
  • User Field  
  • Group Field                                                                                                                |
| Show Group field                               | Audit (cert_audit)            | Shows or hides fields based on the Assignment type selected. The system shows the Group field when you select either of the following assignment types:  
  • Specific Group  
  • Group Field if the Assign to empty option is Create Assigned Task.                                                             |
| Hide "run" associated fields when active is set to false | Audit (cert_audit)            | Hides these scheduling fields when the audit is inactive:  
  • Run  
  • Day  
  • Time  
  • Last scheduled run                                                                                                        |
| Show script window on Scripted Audit           | Audit (cert_audit)            | Displays the Run this script field when the audit type is Scripted.                                                                                                                                       |
| Make table read only                           | Certification Condition (cert_cond) | Sets the table field derived from the selected filter to read-only.                                                                                                                                         |
Script includes

### Compliance Certification Core script includes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DesiredStateUtil</td>
<td>Utility functions for desired state, used to clone a template for Insert functionality.</td>
</tr>
<tr>
<td>CMDBRElationshipAjax</td>
<td>Tool to get all relationships for a given table.</td>
</tr>
<tr>
<td>RelationshipQueryParseAjax</td>
<td>Parses condition filters. This script include is the internal code used in generating the compliance conditions.</td>
</tr>
<tr>
<td>CertificationUtils</td>
<td>Utility functions for certification that find Next run time value, and so on.</td>
</tr>
<tr>
<td>CertTaskEscalationTimerPercentage</td>
<td>Utility method for setting escalation timer durations.</td>
</tr>
<tr>
<td>ConditionUtilsAjax</td>
<td>AJAX utilities for parsing queries into a human-readable format.</td>
</tr>
<tr>
<td>DeleteInactiveVersionsAjax</td>
<td>AJAX server-side script to delete all inactive versions of a record.</td>
</tr>
</tbody>
</table>

Client scripts

### Compliance Certification Core client scripts

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make audit type read only if not new</td>
<td>Certification Template (cert_template)</td>
<td>Sets the correct audit type for new records, and if the record is not new, sets the Audit type field to read only.</td>
</tr>
<tr>
<td>Update table name (filter)</td>
<td>Audit (cert_audit)</td>
<td>Updates the table Name field when the filter is updated.</td>
</tr>
<tr>
<td>Update table name</td>
<td>Audit (cert_audit)</td>
<td>Updates the table Name field when the template is updated.</td>
</tr>
<tr>
<td>Set table name on new</td>
<td>Audit (cert_audit)</td>
<td>Returns the table name from the template or filter.</td>
</tr>
<tr>
<td>Update table name</td>
<td>Certification Template (cert_template)</td>
<td>Updates the table Name field when a new filter is chosen and checks all existing conditions to see if they work for the new table.</td>
</tr>
<tr>
<td>Show conditions when table is set</td>
<td>Certification Template (cert_template)</td>
<td>Shows and hides conditions appropriately when the table is set.</td>
</tr>
<tr>
<td>Reset filter when audit type changes</td>
<td>Certification Template (cert_template)</td>
<td>Clears the filter and updates the lists shown when the audit type is changed.</td>
</tr>
</tbody>
</table>
## Business rules

### Compliance Certification Core business rules

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clone condition</td>
<td>Certification Condition (cert_cond)</td>
<td>Part of certification versioning. This business rule retains the original ID when a condition is changed.</td>
</tr>
<tr>
<td>Copy audit type from audit</td>
<td>Audit Result (cert_audit_result)</td>
<td>Ensures that all audit results have the same audit type as the audit that generated them.</td>
</tr>
<tr>
<td>Copy values from template</td>
<td>Audit (cert_audit)</td>
<td>When a user selects a template, and updates the table, filter, and audit type from the template.</td>
</tr>
<tr>
<td>Delete condition</td>
<td>Certification Condition (cert_cond)</td>
<td>Part of certification versioning that deletes a condition.</td>
</tr>
<tr>
<td>Prevent deletion of audit with results</td>
<td>Audit (cert_audit)</td>
<td>Prevents deletion of an audit containing results.</td>
</tr>
<tr>
<td>Prevent delete of Filter with Template</td>
<td>Certification Filter (cert_filter)</td>
<td>Prevents deletion of a filter still linked to a template or audit.</td>
</tr>
<tr>
<td>Prevent deletion of result with task</td>
<td>Audit Result (cert_audit_result)</td>
<td>Prevents deletion of an audit result with an attached task.</td>
</tr>
<tr>
<td>Prevent delete of Template with Audit</td>
<td>Certification Template (cert_template)</td>
<td>Prevents deletion of a template still being used by an audit.</td>
</tr>
<tr>
<td>Update conditions' tables</td>
<td>Certification Template (cert_template)</td>
<td>When storing template conditions, properly run all workflows and update the condition fields to contain the display version of the conditions.</td>
</tr>
<tr>
<td>Update filter version</td>
<td>Certification Filter (cert_filter)</td>
<td>Creates a version when the filter changes in any meaningful way.</td>
</tr>
<tr>
<td>Update next run time</td>
<td>Audit (cert_audit)</td>
<td>Updates the time in the Next scheduled run field when an audit is modified.</td>
</tr>
<tr>
<td>Update next run time during execution</td>
<td>Audit (cert_audit)</td>
<td>When the audit runs, update the Next scheduled run field to the next time the audit is scheduled to run.</td>
</tr>
<tr>
<td>Update table</td>
<td>Certification Template (cert_template)</td>
<td>Update the stored table to the table of the filter.</td>
</tr>
<tr>
<td>Update template version</td>
<td>Certification Template (cert_template)</td>
<td>Creates a version when the template changes in any meaningful way.</td>
</tr>
</tbody>
</table>
Compliance Templates and Audits

The Templates and Audits modules on the top level of the Compliance menu enable a certification_admin user to create, edit, and delete all template and audit types.

You can use Compliance Templates and Audits to evaluate records for any table in the ServiceNow system, not just those tables extending the Configuration Item [cmdb_ci] table. Compliance audits certify record attributes only. Compliance templates can be used in Control Test Definitions in Governance Risk and Compliance.

Compliance Overview module

The Compliance Overview module is a type of homepage.

The Compliance Overview module summarizes:

- Current audit states
- Outstanding certification tasks
- Compliance discrepancies
- Upcoming audits
- General state of compliance audits for Data Certification, Desired State, Architectural Compliance, and Scripted audits

To use the Compliance Overview:

1. Navigate to Compliance > Overview.
2. Click elements within the reports to obtain more information.
   - For example, click the Disk space (GB) bar in the Compliance Discrepancies chart to open a list of audit results filtered by disk space attributes.
Compliance Overview module roles

Only users with certain roles can access the Overview module.

The different levels of access are:

<table>
<thead>
<tr>
<th>Role</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>certification</td>
<td>View (view overview page and refresh reports)</td>
</tr>
<tr>
<td>certification_admin</td>
<td>• View (view overview page and refresh reports)</td>
</tr>
<tr>
<td></td>
<td>• Customize (refresh, add, delete, and rearrange reports)</td>
</tr>
<tr>
<td></td>
<td>View, customize</td>
</tr>
<tr>
<td>admin</td>
<td>• View (view overview page and refresh reports)</td>
</tr>
<tr>
<td></td>
<td>• Customize (refresh, add, delete, and rearrange reports)</td>
</tr>
<tr>
<td></td>
<td>• Edit (can edit gauges)</td>
</tr>
</tbody>
</table>

Architecture Compliance

Architecture Compliance performs scheduled or on-demand audits of configuration management database (CMDB) data to determine which configuration items (CI) match the expected attributes.

The compliance process checks servers to ensure that their resources, such as CPU speed or memory, comply with standards set by your organization. Audit reports show any discrepancies in the attributes of the target CIs, and ServiceNow automatically assigns follow-on tasks to qualified users who can remediate those discrepancies.

Activate Architecture Compliance

Administrators can activate the Architecture Compliance plugin to access the application.

Activating this plugin automatically activates these additional plugins.

- Certification Core plugin contains shared functionality required for certification audits.
- Version Management plugin manages certification filter and template versions.

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**.

**Architecture Compliance**

Architecture Compliance manages scheduled or on-demand reviews of CMDB data to determine which configuration items (CI) match expected attributes. The compliance audits check servers to ensure that their physical resources, such as CPU speed or memory, comply with certain standards.

The administrator responsible for compliance checking creates template definitions of expected attributes and then schedules an audit to check CIs for compliance. The audit results identify CIs that pass certification and itemize the discrepancies in those CIs that fail. ServiceNow automatically generates and assigns follow-on tasks to track the process of getting the CIs back into compliance. Users with the admin role activate Architecture Compliance.

**Architecture Compliance Process**

Perform these tasks in this order to certify configuration items with Architecture Compliance.

1. Create a filter.
   
   Create a filter that defines a subset of configuration items to certify. You can create multiple versions of a filter, and then activate the version you want to use for compliance checking. Architecture compliance only supports filters on the Configuration Item (cmdb_ci) table and all tables that extend it.

2. Create a template.
   
   Create template conditions using values from reference fields in a related list or conditions that define the expected physical attributes of each CI in an audit. The template uses a filter to determine which configuration items the system examines based on these conditions.

3. Create and run an audit.
   
   Create and schedule an audit or run an audit on demand. The audit generates a set of results based on the conditions in the template you specify.

4. View audit results.
   
   View the audit results which display any discrepancies between the expected state, as expressed by the template conditions, and the actual state of the target configuration items.

5. Correct discrepancies.
   
   Correct the discrepancies the audit found by completing the follow-on tasks created by the system.

**Architecture Compliance Overview module**

The Architecture Compliance Overview module displays various architecture compliance reports. The Overview module is a type of homepage.
Only compliance users with certain roles can access the Overview module. The different levels of access are:

### Access levels per role

<table>
<thead>
<tr>
<th>Role</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>certification</td>
<td>View (view overview page and refresh reports)</td>
</tr>
<tr>
<td>certification_admin</td>
<td>· View (view overview page and refresh reports)</td>
</tr>
<tr>
<td></td>
<td>· Customize (refresh, add, delete, and rearrange reports)</td>
</tr>
<tr>
<td>admin</td>
<td>· View (view overview page and refresh reports)</td>
</tr>
<tr>
<td></td>
<td>· Customize (refresh, add, delete, and rearrange reports)</td>
</tr>
<tr>
<td></td>
<td>· Edit (can edit reports)</td>
</tr>
</tbody>
</table>

### Using the Architecture Compliance Overview Module

To use the Architecture Compliance Overview module, navigate to Compliance > Architecture Compliance > Overview and click elements within the gauges to obtain more information. The available reports are:

### Architecture Compliance Overview Module Gauges

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>30/60/90 Day Task Aging</td>
<td>All outstanding follow-on tasks grouped by age in 30-day increments</td>
<td>Certification Task</td>
</tr>
<tr>
<td>Architecture Compliance Discrepancies</td>
<td>All audited attribute discrepancies</td>
<td>Audit Results</td>
</tr>
<tr>
<td>Hierarchical Task Roll Up</td>
<td>All follow-on tasks grouped by Assigned to user</td>
<td>Follow On Task</td>
</tr>
<tr>
<td>Outstanding Architecture Compliance Tasks</td>
<td>All follow-on tasks in the Pending, Open, or Work in Progress state</td>
<td>Follow On Task</td>
</tr>
<tr>
<td>Upcoming Architecture Compliance Audits</td>
<td>All scheduled audits</td>
<td>Audit</td>
</tr>
</tbody>
</table>
Architecture Compliance roles

To access or configure certification elements, a user must have the certification_admin role. These users can create, update, and delete filters if they have the proper access to necessary tables.

In the base ServiceNow system, certification_admin users have limited system rights and do not have access to all the necessary tables. When assigning compliance resources, make sure to grant additional roles to the certification_admin user as needed. For example, the certification administrator needs roles that grant access to these tables:

- Company [core_company]
- Cost Center [cmn_cost_center]
- Schedule [cmn_schedule]

Desired State

Desired State performs scheduled or on-demand audits of CMDB data to determine which records match the expected attributes, CI relationships, and relationships to other records in the system.

For example, desired state can determine if a computer has a license for a particular software program. The compliance process checks configuration items (CI) to ensure that their attributes and relationships comply with standards set by your organization. Audit results show any discrepancies in the desired state of a record, and ServiceNow automatically assigns follow-on tasks to qualified users who can remediate those discrepancies.

Desired State process

The Desired State application conducts scheduled or on-demand audits of CMDB data to determine which configuration items (CI) match a desired state.

The desired state certification process can mean checking servers to ensure that their physical resources, such as CPU speed or memory, comply with certain standards. This process also ensures that all critical business services have a manager, support group, and approval group assigned.

The administrator responsible for certification creates definitions of desired states and then schedules an audit to check CIs for compliance. The audit results identify CIs that pass certification and itemize the discrepancies in those CIs that fail. The ServiceNow system automatically generates follow-on tasks to track the process of adjusting the CIs to the desired state.

Desired state differs substantially from data certification. Data certification is a manual process to ensure that your data matches reality. Desired state examines the same data and determines when the configuration of each item is in the desired and approved state.

1. Create a certification filter: Create a filter that defines a subset of configuration items to certify. You can create multiple versions of a filter, and then activate the version you want to use for certification. You can create filters on the Configuration Item [cmdb_ci] table and all tables that extend it.

2. Create a template: Create a template with conditions that define the desired state of the physical attributes, related records, and relationships for a CI. The certification filter you select for the template determines which configuration items the system examines.

3. Create and run an audit: Create an audit using the template. Set the audit to run on a schedule or on demand. The audit generates a set of results based on the conditions from the template you specify. Determine usage of follow-on tasks:
4. View audit results: View the audit results which display any discrepancies between the desired state, as specified by the template, and the actual state of the target configuration items.

5. Correct discrepancies: Correct the discrepancies the audit found by completing the follow-on tasks created by the system.

**Desired State roles**

To access or configure certification elements, a user must have the certification_admin role. These users can create, update, and delete filters if they have the proper access to necessary tables.

In the base system, certification_admin users have limited system rights and do not have access to all the necessary tables. When assigning compliance resources, make sure to grant additional roles to the certification_admin user as needed. For example, the certification administrator requires roles that grant access to these tables:

- Company (core_company)
- Cost Center (cmn_cost_center)
- Schedule (cmn_schedule)

**Desired State Overview module**

The Desired State Overview module displays various desired state reports. The Overview module is a type of homepage.

The Desired State Overview module is a type of homepage.

**Use the Desired State Overview module**

The Desired State Overview module displays various desired state reports.

1. Navigate to **Compliance > Desired State > Overview**.
2. Move or add reports where needed.
3. Click elements within the reports to obtain more information.

The Desired State Overview Module in the base system contains these reports:

- Upcoming Desired State Audits: All scheduled audits.
- Outstanding Desired State Tasks: All follow-on tasks in the Pending, Open, or Work in Progress state.
- Hierarchical Task Roll Up: All follow-on tasks grouped by Assigned to user.
- Desired State Discrepancies: All audit discrepancies for attributes and relationships.
- 30/60/90 Day Task Aging: All outstanding follow-on tasks grouped by age in 30-day increments.
Desired State Overview module roles

Only compliance users with certain roles can access the Overview module.

The different levels of access are:

<table>
<thead>
<tr>
<th>Role</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>certification</td>
<td>View (view overview page and refresh reports)</td>
</tr>
<tr>
<td>certification_admin</td>
<td>• View (view overview page and refresh reports)</td>
</tr>
<tr>
<td></td>
<td>• Customize (refresh, add, delete, and rearrange reports)</td>
</tr>
<tr>
<td></td>
<td>View, customize</td>
</tr>
<tr>
<td>admin</td>
<td>• View (view overview page and refresh reports)</td>
</tr>
<tr>
<td></td>
<td>• Customize (refresh, add, delete, and rearrange reports)</td>
</tr>
<tr>
<td></td>
<td>• Edit (can edit reports)</td>
</tr>
</tbody>
</table>

Access levels

The different levels of access are:

- View: can view the overview page and refresh reports.
- Customize: can refresh, add, delete, and rearrange reports.
- Edit: can edit reports.

Desired State reporting

The Desired State application includes reports to assess your audit results.

These reports are available to all users whose role gives them access to the Reporting application. Users with the admin role can share these reports with specific users of groups or change the display options.

Navigate to Reports > View / Run. In the Reports search field, enter all or part of the report name. You can also scroll to the designated category and select one of the reports.

In addition to these reports, you can also generate other reports.
Filter and Order:

Follow on task.State is one of
Pending
Open
Work in Progress
Closed

and Audit type is Desired State
and Threshold is Exceeded

Desired State Result with Threshold Exceeded

Audit Result Count

<table>
<thead>
<tr>
<th>UPS Audit</th>
<th>UPS Chicago</th>
<th>UPS Miamisburg</th>
<th>UPS Sacramento</th>
<th>UPS San Diego</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPS Audit (3 days)</td>
<td>UPS Audit (7 days)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Desired State threshold report
## Desired state report table

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desired State Discrepancies</td>
<td>This report displays all desired state audit results that have a follow-on task that is not yet in the Closed Complete state. This report displays by column name.</td>
<td>Audit Result</td>
</tr>
<tr>
<td></td>
<td>• Type: bar chart</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Table: Audit Result (cert_audit_result)</td>
<td></td>
</tr>
<tr>
<td>Desired State Result with Stability Unstable</td>
<td>This report displays all audit results where the Stability field has the value Unstable. This report displays by CI and stacked by audit.</td>
<td>Audit Result</td>
</tr>
<tr>
<td></td>
<td>• Type: bar chart</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Table: Audit Result (cert_audit_result)</td>
<td></td>
</tr>
<tr>
<td>Desired State Result with Threshold Exceeded</td>
<td>This report displays all audit results where the Threshold field has the value Exceeded. This report displays by CI and stacks by each audit.</td>
<td>Audit Result</td>
</tr>
<tr>
<td></td>
<td>• Type: bar chart</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Table: Audit Result (cert_audit_result)</td>
<td></td>
</tr>
<tr>
<td>Upcoming Desired State Audits</td>
<td>This report displays the desired state audits that are scheduled to run in the next two quarters.</td>
<td>Audit</td>
</tr>
<tr>
<td></td>
<td>• Type: List (tabular) report</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Table: Audit (cert_audit)</td>
<td></td>
</tr>
<tr>
<td>30/60/90 Day Desired State Task Aging</td>
<td>This report displays the number of follow-on tasks that are not Closed Complete for desired state audit types. The report is grouped by aging level.</td>
<td>Follow On Task</td>
</tr>
<tr>
<td></td>
<td>• Type: Horizontal bar chart</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Table: Follow On Task (cert_follow_on_task)</td>
<td></td>
</tr>
<tr>
<td>Desired State Hierarchical Task Roll Up</td>
<td>This report displays similar data to the Task Aging report, but groups the results by manager.</td>
<td>Follow On Task</td>
</tr>
<tr>
<td></td>
<td>• Type: Horizontal bar chart</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Table: Follow On Task (cert_follow_on_task)</td>
<td></td>
</tr>
</tbody>
</table>
Certification audits

A certification audit compares the actual attributes of certain ServiceNow records. This audit selects a filter, against the expected attributes, relationships, and related record values defined by template conditions or a script.

You can configure the audit to create and assign follow-on tasks to remediate any discrepancies the audit finds. Audit records use a standard ServiceNow scheduler to determine when to run. After an audit runs, the results and follow-on tasks appear in related lists in the audit record.

Users with the certification_admin role can create, update, delete, and run audits. Users with the certification role can view audits, audit results, and follow-on tasks.

Create an audit

Compliance offers two types of audits: one uses templates to define conditions and the other uses a script.

Role required: certification_admin

1. Ensure that an appropriate template record was created for this audit.

   **Note:** Conditions in the template define the values to audit.

2. Use the CI Class Manager:
   a) Navigate to Configuration > CI Class Manager.
   b) Select a class from the Class Hierarchy.
   c) In the sidebar on the right, check Advanced. Click Audit in the Compliance group.

3. Or, navigate to one of these modules:
   - Compliance > Audits
   - Compliance > Architecture Compliance > Audits
   - Compliance > Desired State > Audits
   - Compliance > Scripted Audits > Audits

4. Click New.
   The system opens a new record for the audit type associated with the navigation path you selected. The Audit type field is read-only.

5. Complete the form using the fields described in the table below.

6. Right-click the header bar and select Save.
   The Audit Results and Follow On Tasks related lists appear on the form.

7. To run the audit immediately, click Run Audit.
When template audits run, ServiceNow updates the date and time in the Last run date field and populates the related lists. For scripted audits, the Last run date field is not populated.

8. View the records that passed and the discrepancies found by the audit in the Audit Results related list.

You can open template records and any follow-on tasks directly from this related list. Notice that the value in the Task description field appears as the Short description in the follow-on tasks.

**Note:** You cannot delete audit records that have audit results or audit results that have follow-on tasks. ServiceNow disables the Delete option in records and lists where these dependent records exist.

### Creating Audits

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Name for this audit.</td>
</tr>
<tr>
<td><strong>Filter</strong></td>
<td>Filter to use when the audit type is Scripted. This field is required for scripted audits, but is hidden for all other audit types.</td>
</tr>
<tr>
<td><strong>Template</strong></td>
<td>(Required) Template to use when this audit runs. Audit type filters the list of available templates, and only the active versions of templates are available for selection. For example, when you create an audit from Desired State, only templates of the Desired State audit type are available for selection. For the Desired State and Architecture Compliance audit types, only templates for tables that extend the Configuration Item (cmdb_ci) table are available. This field is hidden when the audit type is Scripted.</td>
</tr>
<tr>
<td><strong>Table</strong></td>
<td>(Read-only) Table for the template.</td>
</tr>
<tr>
<td><strong>Create tasks</strong></td>
<td>Option to create follow-on tasks for correcting discrepancies (selected). In a scripted audit, you can create the logic for either task state by using true to create tasks or false to not create tasks. By default, this check box is cleared (false) in a new audit record.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Assignment type | Method for assigning follow-on tasks. This field is visible only when the Create task check box is selected. Choices are:  
• User Field: Select a user reference field on the table being audited. For example, you choose the user identified in the Managed by field on the failed record to perform the tasks. This selection displays the Assigned to and Assign to empty fields. If the reference field on the record is empty, the value in the Assign to empty field is used.  
• Specific User: Select a specific user to perform the tasks. This selection displays the User field.  
• Group Field: Select a group reference field on the table being audited. For example, you choose the group identified in the Support group field on the failed record to perform the tasks. Tasks are assigned to all members of the group. This selection displays the Assign to group and Assign to empty fields. If the reference field on the record is empty, the value in the Assign to empty field is used.  
• Specific Group: Select a specific group to perform the tasks. This selection displays the Group field. All members of the selected group are assigned to the tasks. |
| User            | The specific user this audit assigns to follow-on tasks. This user must have the certification role. This field is available under these conditions:  
• Assignment type is set to Specific User.  
• Assign to empty is set to Create Assigned Task, and Assignment type is set to User Field. |
<p>| Assign to group | The group field that defines which group this audit assigns to the follow-on task. This field is available only when the Assignment type is Group Field. |
| Group           | The specific group this audit assigns to follow-on tasks. This field is available only when the Assignment type is Specific Group. |
| Assign to       | The user field that defines which user this audit assigns to the follow-on task. This field is available only when the Assignment type is User Field. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign to empty</td>
<td>The behavior to use if the field selected in <strong>Assign to</strong> or <strong>Assign to group</strong> is blank on the record being audited. For example, if a follow-on task must be assigned to a manager, but no manager is identified, the <strong>Assign to empty</strong> setting determines what happens. This field appears only when the <strong>Assignment type</strong> is <strong>User Field</strong> or <strong>Group Field</strong>. Choices are: - Do Not Create Task: No follow-on task is created when the <strong>Assign to</strong> or <strong>Assign to group</strong> field is empty. - Create Unassigned Task: Create a follow-on task, but do not assign it to any user or group. The task can be manually assigned later. - Create Assigned Task: Create a follow-on task and assign it to the user or group specified. If the assignment type is <strong>User Field</strong>, the <strong>User</strong> field becomes available. If the assignment type is <strong>Group Field</strong>, the <strong>Group</strong> field becomes available. The audit automatically creates follow-on tasks for all records that have <strong>Assign to</strong> populated, regardless of the <strong>Assign to empty</strong> setting.</td>
</tr>
<tr>
<td>Short description</td>
<td>Brief description of the purpose of the audit.</td>
</tr>
<tr>
<td>Task description</td>
<td>General description of the work required for the follow-on tasks for the audit. All follow-on tasks created by this audit inherit this description.</td>
</tr>
<tr>
<td>Active</td>
<td>Activation control for this audit record. Clear this check box to prevent this audit from running and creating follow-on tasks.</td>
</tr>
<tr>
<td>Run</td>
<td>How often to run the schedule that generates the audit. - Daily - Weekly - Monthly - Periodically - Once - On Demand</td>
</tr>
<tr>
<td>Day</td>
<td>- If <strong>Run</strong> is <strong>Weekly</strong>, the day of the week when the audit runs. - If <strong>Run</strong> is <strong>Monthly</strong>, the day of the month when the audit runs. If the day is 29, 30 or 31, for shorter months the audit runs on the last day of the month.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Repeat Interval</td>
<td>If Run is <em>Periodically</em>, the frequency that the audit runs, based on a 24-hr. clock. Enter the number of days between audits and the time of day that you want the audit to run. For example, set Days to 10 and Hours to 14:00:00 to run the audit every 10 days at 2:00pm.</td>
</tr>
<tr>
<td>Starting</td>
<td>If Run is <em>Periodically</em> or <em>Once</em>, the date and time when the audit runs.</td>
</tr>
<tr>
<td>Time</td>
<td>If Run is <em>Daily</em>, <em>Weekly</em>, <em>Monthly</em>, or <em>Once</em>, the time of day, on a 24-hour clock, when the audit runs.</td>
</tr>
<tr>
<td>Last run date</td>
<td><em>(Read-only)</em> The last date and time the audit ran, either on its regular schedule or manually. Audit previews do not update this field.</td>
</tr>
<tr>
<td>Next scheduled run</td>
<td><em>(Read-only)</em> The next date and time when the audit runs. The system recalculates this field when you change the schedule.</td>
</tr>
<tr>
<td>Audit type</td>
<td><em>(Read-only)</em> The type assigned to this audit. The system selects the audit type based on the application from which the audit is created. The type can be:</td>
</tr>
<tr>
<td></td>
<td>- Desired State</td>
</tr>
<tr>
<td></td>
<td>- Architecture Compliance</td>
</tr>
<tr>
<td></td>
<td>- Compliance</td>
</tr>
<tr>
<td></td>
<td>- Scripted</td>
</tr>
<tr>
<td>Health window</td>
<td>Duration of the evaluation period for threshold and stability. The health window value defines the number of Health window units in an evaluation period for an audit. This value is expressed as a positive integer. The default value for this field is 7.</td>
</tr>
<tr>
<td>Health window unit</td>
<td>Unit of measurement that defines the duration of a health window. The default value for this field is <em>Days</em>. Choices are:</td>
</tr>
<tr>
<td></td>
<td>- Minutes</td>
</tr>
<tr>
<td></td>
<td>- Hours</td>
</tr>
<tr>
<td></td>
<td>- Days</td>
</tr>
<tr>
<td></td>
<td>- Months</td>
</tr>
<tr>
<td>Threshold count</td>
<td>Sets the acceptable number of audit failures for the desired state field that can occur within the specified health window for a CI. The audit results indicate when a desired state field is within or has exceeded this threshold limit. The default value for the threshold is 5.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Stability count</td>
<td>Sets the acceptable number of times that audit results for a CI can switch between <strong>Certified</strong> and <strong>Failed</strong> within the specified health window. The audit results for a CI indicate whether it is stable or unstable. The default value for stability is 1.</td>
</tr>
<tr>
<td>Run this script</td>
<td>Audit script to run which contains the conditions that a CI need to comply with to pass the audit. This field is available only when the audit type is <strong>Scripted</strong>. The Audit form includes a sample script with instructions for performing the audit and generating the follow-on tasks.</td>
</tr>
</tbody>
</table>

**Audit Scheduling**

The system performs audits automatically from the schedule you configure.

Users with the certification_admin or admin role can generate on-demand audits directly from the Audit form by clicking **Run Audit**. When an audit runs, ServiceNow populates the **Audit Results** related list in the form and shows follow-on tasks, if any, in the **Follow On Tasks** related list. Click **Preview Audit Results** to generate an audit preview that tests your template conditions without generating any audit results.
Audit Running

Certification audit results
Audit results show the records that have passed or failed an audit and itemize any discrepancies detected.

A discrepancy is considered any departure from the expected conditions defined in the template or script used for the audit. Audit results provide links to the source records and to the follow-on tasks for bringing failed records into compliance. Records that pass an audit have a single entry in the results table with a state of Certified. Records that fail an audit show all discrepancies, each with a state of Failed.

ServiceNow displays results from a certification audit in these locations:

- Audit Results list
- A related list in the Audit record
• A related list in the compliance view of a CI record

View an audit result

To generate certification results, you must first create and run an audit.

1. Navigate to one of the following locations:
   - Compliance > Desired State > Audit Results
   - Compliance > Architecture Compliance > Audit Results
   - Compliance > Scripted Audits > Audit Results
   - Data Certification > Schedules > Audit results

2. From any audit results list, you can edit the filter to show the results for any audit type.

   ![Audit Type filter](image)

   The results filter by audit type and grouped by audit number. Within the groups, results list by date, from oldest to newest.

3. You can open the audit record, the CI record, or the follow-on tasks from this list.

   **Note:** The **Audit type** field was set automatically when the audit result was created and cannot be changed. For scripted audits, the audit type is set when you create the audit record.
Desired State Audit Results

Audit results show this information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created</td>
<td>Date and time the audit ran.</td>
</tr>
<tr>
<td>Document</td>
<td>Record that was certified, such as a configuration item (CI).</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>State</td>
<td>Results of certification for each condition evaluated. The three possible states are:</td>
</tr>
<tr>
<td></td>
<td>- Certified A certified record is one that passed all conditions. ServiceNow generates only one audit result for a certified record.</td>
</tr>
<tr>
<td></td>
<td>- Failed Records that are not certified have an audit result for each failed condition. The <strong>Column name, Desired value, Discrepancy value</strong>, and <strong>Follow on task</strong> are only populated for failed results.</td>
</tr>
<tr>
<td></td>
<td>- Pending A pending state indicates that the audit is incomplete. Data certification audits use this state when a result is awaiting user input.</td>
</tr>
<tr>
<td>Column name</td>
<td>Audited field, relationship, or related list column that did not match the expected state.</td>
</tr>
<tr>
<td>Desired value</td>
<td>Attribute or relationship required for this record that was not found, from the condition in the expected state template. For data certification, this column is blank if the record has a state of Failed or Pending.</td>
</tr>
<tr>
<td>Discrepancy value</td>
<td>Actual value of the attribute that did not match the expected state. The follow-on task, if provided, tracks resolution of this discrepancy. In a list of results for the Data Certification audit type, this column is blank if the record has a state of Certified or Pending.</td>
</tr>
<tr>
<td>Follow on task</td>
<td>Link to the follow-on task generated for remediating a discrepancy.</td>
</tr>
<tr>
<td>Audit</td>
<td>Link to the audit record that produced the results.</td>
</tr>
<tr>
<td>Threshold</td>
<td>State of an audited, desired state field with a defined failure threshold. This threshold is the acceptable number of failures for a desired state field within a specified health window and is configured in the Audit form. Possible threshold states for the results are:</td>
</tr>
<tr>
<td></td>
<td>- In Limit</td>
</tr>
<tr>
<td></td>
<td>- Exceeded</td>
</tr>
</tbody>
</table>
### Delete an audit result

While audit results can be deleted, you cannot delete an audit result that has a follow-on task associated with it.

1. Navigate to one of these modules:
   - Compliance > Desired State > Audit Results
   - Compliance > Architecture Compliance > Audit Results
   - Compliance > Scripted Audits > Audit Results

   The list groups by audit name.

2. Select the checkbox for a result in the list, and then select **Delete** from the **Actions on selected rows** menu at the bottom of the list.

   **Note:** If the result record has a follow-on task, the **Delete** option is not available. If you select multiple records, some with and some without tasks, the system only deletes those records that do not have tasks.
3. Click a date/time link to see the results for a specific CI.

   Note: The Delete button only appears on the form if the audit result does not have a follow-on task.

4. Click Delete.
View an audit result in the Compliance view

After an audit has run, you can view the results and follow-on tasks from the Compliance view in the records of every CI audited.

This view is available only for systems that use the default CI classes provided with the base ServiceNow system, such as Hardware, Software, and Computer. For information about creating views, see View Management.

1. Navigate to Configuration and open the record of a CI that was included in a compliance audit.
2. Select the view to configure by performing 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>Open the context menu and select View &gt; Compliance.</td>
</tr>
<tr>
<td>List v3</td>
<td>Open the context menu and select Change View, and then click Compliance.</td>
</tr>
</tbody>
</table>

List v2: select View > Compliance

The Audit Results Compliance View appears.
Audit Results Compliance View

Audit Results Compliance View List Descriptions

<table>
<thead>
<tr>
<th>Lists</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passed Audit Results</td>
<td>Lists audits for this CI that passed without discrepancies. The information includes the versions of the template and filter used. Records are grouped first by audit, and then by creation date and time.</td>
</tr>
<tr>
<td>Failed Audit Results</td>
<td>Lists all failed audits for this CI. The information includes the discrepancy data, the follow-on task, and the versions of the template and filter used. Records are grouped first by audit, and then by creation date and time.</td>
</tr>
<tr>
<td>Follow On Tasks</td>
<td>Lists all follow-on tasks generated from audit discrepancies for this CI.</td>
</tr>
</tbody>
</table>

3. Right-click the header bar and select View > Compliance from the context menu.
Results preview

You can preview an audit to view potential results without saving audit results or generating follow-on tasks. For example, use this feature to test template conditions for correctness without creating thousands of result records.

In an audit record, click Preview Audit Results under Related Links.

A summary of the potential audit results appears at the top of the audit record. Previewing does not change the Last run date field.

Health windows

A health window is a trailing time frame in which the ServiceNow system evaluates audit results from CIs that have desired state fields defined.
The Health window and Health unit fields define each window, and ends when an audit runs. For example, an audit runs on the fifteenth of the month with a seven-day window. It evaluates the threshold values of a desired state field from the eighth to the fifteenth. When the same audit runs the next day, the system evaluates the threshold from the ninth to the 16th, and so on. The audit counts backward seven days from the current day. ServiceNow evaluates a CI threshold value for each health window, without considering the results from the previous window. As a result, the health of a CI can fail for one audit and then pass in a subsequent audit that runs in a new window.

ServiceNow evaluates stability by recording the number of times a desired state threshold value for a CI switch between Failed and Certified within the health window. In the example shown here, a 5-minute health window was set for the desired state field on a UPS unit that measures the remaining battery time. The threshold was set at 2, which allows the field to fail two audits in the same health window.

![Health Window and Audit Image]

**Desired State Health Window**

In the initial audit, the system evaluated the threshold value for the Seconds on battery field within a 5-minute window. This window ran from 13:52:51 to the time of the audit at 13:57:51. The desired state field showed In Limit for that audit and the second audit conducted less than a minute later. The next two audits were conducted within five minutes of the first audit and both showed that the threshold (set at 2) was Exceeded. A subsequent audit was conducted five minutes after the audit in which the desired state field threshold was first exceeded. Since the health window had moved forward enough units, the Seconds on battery field was within limits again with only one failure in the 5-minute window being evaluated.
Desired State Health Results

Copy an audit

New audits can be created from an existing audit.

1. Open the audit record you want to copy.
2. Change the name or short description to distinguish this audit from the original.
3. Make any other changes you need.
4. Right-click in the header bar and select either Insert or Insert and Stay from the context menu.
The system clears the Last run date field and inserts the record into the database.

**Certification filters**

A certification filter creates a subset of ServiceNow records to audit, typically from configuration items (CI) of a certain type, such as all UNIX servers in a specific datacenter.

However, you can define a filter for any ServiceNow table by using any set of system-supported conditions. Audited records identified by a filter for expected attributes or relationships, depending on the audit type.

You can create multiple versions of a filter, reactivate inactive versions, and select the version you want to use in a template or a certification schedule. Only the active versions of a filter are available for selection in template records. You can use a single filter for multiple certification templates or schedules.
Certification filters

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Certification</td>
<td>Validates CMDB data.</td>
</tr>
<tr>
<td>Architecture Compliance</td>
<td>Manages reviews of CMDB data in architecture compliance audits to determine which configuration items (CIs) match expected attributes.</td>
</tr>
<tr>
<td>Desired State</td>
<td>Manages reviews of CMDB data to determine which CIs match a desired state for both attributes and relationships.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Manages reviews of records from any ServiceNow table to determine which records match an expected set of attributes and related record conditions.</td>
</tr>
<tr>
<td>IT Governance Risk and Compliance</td>
<td>Generates audits and tests to ensure that controls are being followed and creates tasks to track corrective actions.</td>
</tr>
</tbody>
</table>

Compliance filter

The compliance filter for license bases uses the following fields to define entitled users or CIs. These field values can be used independently or together to calculate compliance.

<table>
<thead>
<tr>
<th>Compliance Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entitled company</td>
<td>All users or configuration items (CI) at all locations of this company, in all departments are entitled to use this software package. Compliance at this level calculates how many licenses are purchased for the company at large and how many entitled users or CIs consume them.</td>
</tr>
<tr>
<td>Entitled location</td>
<td>CIs and users who are assigned to this company location in any department are entitled to use this software package. Compliance at this level calculates how many licenses are purchased for this company location and how many users and CIs consume them.</td>
</tr>
<tr>
<td>Entitled department</td>
<td>Only the users or CIs in this department at this company location are entitled to use this software package. Compliance is calculated for a single department only.</td>
</tr>
</tbody>
</table>

The license form can display information about all CIs or named users who are using this software package. The form indicates when license reconciliation is necessary and displays all compliant users or CIs.

Possible compliance levels are:
## Compliance

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non applicable</td>
<td>Compliance levels for all infrastructure licenses that are related to cluster licenses are set to <strong>Non applicable</strong> automatically. Compliance levels are calculated in the cluster license only, and not in the related infrastructure licenses.</td>
</tr>
<tr>
<td>Out of compliance</td>
<td>More licenses are being consumed than were purchased. There are more users or CIs using this license than the license allows, and some users or CIs are not be entitled to use this software package.</td>
</tr>
<tr>
<td>Unused</td>
<td>The licenses for this software package are currently unused.</td>
</tr>
<tr>
<td>Reconciliation required</td>
<td>CIs or users who are not entitled to use this software are consuming licenses. Licenses that require reconciliation are considered out of compliance. Reconciliation requires action to ensure that unentitled users are not using the software. Reconciliation involves uninstalling software or increasing license counts to match actual user counts.</td>
</tr>
<tr>
<td>Nearly out of compliance</td>
<td>For a software package to be at this compliance level, more than 95% of the licenses are in use by entitled users or CIs. License bases at this level are considered to be <strong>In compliance</strong>.</td>
</tr>
<tr>
<td>In compliance</td>
<td>This software package has unused licenses. All users or CIs using a license are entitled to use this software package.</td>
</tr>
</tbody>
</table>

### Copy a filter

New filters can be created from an existing filter.

1. Open the filter record you want to copy.
2. Make sure to change the filter name or description to distinguish the new filter from the original.
3. Make any other necessary changes.
4. Right-click in the header bar and select either **Insert** or **Insert and Stay** from the context menu.
Desired State Filter Clone

The system increments the record number and sets the version to 1 for the new record. Both the original filter and the copy are Active and appear in the record list. Showing all copies of a filter allows you to see the entire history of the filter.

Desired State Filter Insert
Additional Roles

In the base ServiceNow system, users with the certification_admin role have limited system rights and do not have access to the tables required for creating a filter.

When assigning compliance resources, make sure certification_admin users have any additional roles they need. For example, a user requires roles that grant access to the Company [core_company] table.

Filter versions

Versions can be displayed in a list.

The default list of filters displays only the active version of each filter. To see all filter versions in the list view, select All in the breadcrumbs.

Desired State Filter List

Create a filter

You can create as many versions of a filter as necessary. You can designate which versions are active and available for selection in Compliance template records, Governance Risk and Compliance control test definitions, or Data Certification schedule definitions.

1. Use the CI Class Manager:
   a) Navigate to Configuration > CI Class Manager.
   b) Select a class from the Class Hierarchy.
   c) In the sidebar on the right, check Advanced. Click Certification Filter in the Compliance group.

2. Or, navigate to one of these modules:
   - Compliance > Filters
   - IT GRC > Administration > Filters
   - Data Certification > Schedules > Certification Filters

3. Click New.
4. Fill in the fields (see table).
5. Click Submit.
This action saves the filter as version 1.

6. To create another version of this filter, open the record and modify the name, table, or conditions.

   **Note:** You can change a filter Description without incrementing a version.

7. Click **Update**.

   The system saves a new version of the current filter and makes it the Active version. The previous version is marked inactive. The system displays only active filter versions for selection when you create templates or schedules.

### Creating Filters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Number</strong></td>
<td>(Read-only) Displays the automatically assigned filter identification number. All versions of a filter have the same number.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>(Required) Filter name.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>(Optional) Describes this filter. You can change the description of a filter without incrementing a version.</td>
</tr>
<tr>
<td><strong>Table</strong></td>
<td>Specifies the table containing the records to select. The template or schedule that uses this filter works on this table. For example, select the ESXi Server [cmdb_ci_esx_server] table to select VMware ESX servers.</td>
</tr>
<tr>
<td><strong>Active</strong></td>
<td>Makes this filter available for use from the <strong>Filter</strong> field on the Certification Template or Schedule Definition form. Multiple versions of a filter can be active. You can activate or deactivate a filter without incrementing the version.</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>(Read-only) Indicates the version of this filter. Any changes to this filter, except to the description or the <strong>Active</strong> check box, makes it inactive. The system increments the version of the updated filter and marks it as active. The system saves all versions of the filter and makes them available for reactivation.</td>
</tr>
<tr>
<td><strong>Filter condition</strong></td>
<td>Specifies the fields, operators, and values that create the filter. The available fields are based on the table selected. The condition builder shows the number of records that match the conditions. Click the refresh icon to recalculate the number of matching records when you edit the conditions.</td>
</tr>
</tbody>
</table>
Delete a filter

Only users with the certification_admin or admin role can delete filter versions. But, you cannot delete a filter that is being used in a template or a scripted audit.

You cannot delete a filter that is being used in a template or a scripted audit.

1. To delete a single filter version, open that version record and click **Delete**.
   
The system hides the **Delete** button for filters that are in use. If you delete the latest version of a filter that is active, the previous version of that filter is reset to Active.

2. To delete all unused and inactive versions of a filter, open any version of that filter and click **Delete inactive versions** under **Related Links**.

3. When prompted, click **OK** to proceed.
   
The system deletes unused filter versions. A message in the header bar identifies filter versions that cannot be deleted because they are used in a template or scripted audit.
Manage a filter version in a form

You can view and manage all versions of a filter from the Certification Filter form.

1. Open any version of a filter.
   The Other Versions related list displays all other versions of this filter, both active and inactive. The system prevents you from editing either the filter version or the record number in the list view.

2. Click any version in the related list to display the record for that version.

3. To make an inactive filter the current version, open the filter, edit it if desired, and then click Revert.

   This action:
   - Deactivates the previous active version of the filter.
   - Copies the inactive filter.
   - Makes this new copy current and active.
Certification follow-on tasks

The ServiceNow system can automatically generate and assign follow-on tasks to correct discrepancies detected during compliance audits.

The system attribute `glide.allow.new.cert_follow_on_task` is set to true by default, allowing for new follow-on tasks to be created for the same failure, at each audit run. You can set this property to false, to configure audit to use the same follow-on task for the same audit failure across multiple runs.

You configure and assign follow-on tasks to qualified users or groups in the audit record. A user with the certification_admin role can reassign any follow-on task. The Audit Results related list in the Follow On Task form contains links to the records that failed.

Access follow-on tasks

Users with the certification role can only access follow-on tasks assigned to them but can reassign these tasks to other users.

1. Navigate to Compliance > My Follow On Tasks.

   The list contains all active follow-on tasks assigned to the logged in user.
Follow-on Task My Work

2. Open a task.

The record shows the specifics of the task, the task activity, and the failed audit results.
Follow-on Task

© 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. Open records from the **Audit Results** related list to see each discrepancy.

![Audit Result Detail](image1.png)

4. Go to the CI named in the record and perform the work to bring it into compliance.

5. Update the **State** field in the follow-on task record and add work notes as you correct each discrepancy.

When you change the state, the system updates the task activity appropriately.

![Follow-on Task Activity](image2.png)

**Follow-on Task Activity**

When the task is **Closed Complete** it no longer appears on the **My Work** list.
Manage follow-on tasks

Users with the certification_admin or admin role can see all follow-on tasks.

Tasks are pre-assigned to a user or group as specified in the audit record, but users with the certification_admin role can reassign the task.

1. Navigate to the appropriate application:
   - Compliance > Architecture Compliance > Follow On Tasks
   - Compliance > Desired State > Follow On Tasks
   - Compliance > Scripted Audits > Follow On Tasks

The list of follow-on tasks appears, filtered by audit type.

2. Open a task.
   - The Audit and Configuration item fields are read-only for all users.

3. Edit the Assignment group or the Assigned to field if necessary.

4. Edit the Short description field if necessary.
   - The short description is inherited from the Task description field in the Audit form.
Arch Comp Task

5. Use the links in the Audit Results related list to open the individual records that failed the audit.
6. If you update the follow-on task record, be sure to add work notes.

Certification templates

Certification templates can define attributes, relationships, and reference field values that indicate what a record is expected to contain.

These values are used to perform audits on ServiceNow records. The certification filter selected in the template identifies the table and records to audit, and the template conditions set the expected state for those records. The type of audit you create determines which tables and template conditions are available.

Users with the certification_admin role can create, update, and delete templates. Users with the certification role can view template versions.
Certification template audit types

When you create a template, ServiceNow assigns an Audit type that determines which tables and conditions are available in the certification template. This value is based on the application from which the template is created. Each application lists only the templates with the associated type.

Available Condition Builders

The available condition builders for each audit type:

- **Compliance**: Runs audits on any set of ServiceNow records, not only configuration items (CI).
  - **Attribute**: Sets conditions for the attributes of the records.
  - **Related List**: Runs audits on records in tables that reference the table defined in the template.

- **Architecture Compliance**: Defines the following types of conditions for tables that extend the Configuration Item (cmdb_ci) table.
  - **Attribute**: Sets conditions for physical attributes of CIs, such as memory or disk size.
  - **Related List**: Runs audits on records in tables that reference the table defined in the template.

- **Desired State**: Defines the following types of conditions for tables that extend the Configuration Item (cmdb_ci) table.
  - **Attribute**: Sets conditions for physical attributes of CIs, such as memory or disk size.
  - **CI relationship**: Defines the relationships these CIs have with other CIs. An example of a relationship is a business service, such as Outlook Web Access, that depends on a server.
  - **User relationship**: Defines the user who reviewed the log records. The only operator available with this condition builder.
  - **Group relationship**: Defines user groups who backed up this CI. The only operator available with this condition builder.
  - **Related List**: Runs audits on records in tables that point toward the table defined in the template.

Create or edit a certification template

To create a certification template, follow these instructions.

Activate the Certification Core plugin to enable the Compliance functionality. See [Compliance Activation](#) for details.

1. Ensure that you have an appropriate filter that defines the records the template evaluates.
   - The template applies its conditions to these records.
2. Use the CI Class Manager to navigate to the Certification Template form:
   a) Navigate to Configuration > CI Class Manager.
   b) Select a class from the Class Hierarchy.
   c) In the sidebar on the right, check Advanced. Click Certification Template in the Compliance group.
3. Or, navigate using one of these paths:
4. Click New or select a certification template to edit.

The following fields are completed automatically:

- **Number**: Each new template has a unique number. All versions of the same template use the same number.
- **Active**: All new templates are set to Active.
- **Version**: The version of a new template is set to 1.
- **Audit type**: The system sets the default type to Architecture Compliance, Desired State, or Compliance, depending on the application in which the template was created. You can select a different type when you create the template, but the field becomes read-only when you submit the record. The system uses audit types to filter record lists for appropriate data and determine which conditions are visible on the template form.

5. Complete the following mandatory fields:

- **Name**: Enter a descriptive name for this template. The name helps identify the purpose.
- **Filter**: Select the filter that identifies the records to be certified. You can select either active or inactive filter versions. By default, the system presents only active versions for selection. If you start typing the name of a filter, the auto-complete feature displays all versions for selection. For architecture compliance and desired state templates, only filters that use a table extended from Configuration Item [cmdb_ci] appear on the choice list. All filters appear on the choice list for a compliance template. After you select a filter, the template condition builder appears. The template operates on the table specified in the filter.

6. Enter a **Description** for this template

7. Define certification conditions using the condition builders. All conditions are AND conditions. The audit type of the template determines which conditions are available.

- **Certification Attribute Conditions**: (All audit types) Select configuration item attributes or specifications to certify, such as CPU count, memory, or disk space. Available fields in the attribute condition builder depend on the table from the filter. Typical ServiceNow conditions for attributes are available, including the between operator for setting numerical conditions with high and low boundary values. This operator was added specifically for desired state conditions.

The **Show Related Fields** item supports dot-walking, allowing you to include referenced fields in a certification attribute condition. Click **Show Related Fields** or **Remove Related**
**Fields** to add or remove referenced fields (in the form of `<field> => <field>`). Select a referenced field to drill down to the next level of referenced fields.

See [Selecting fields on related tables using dot-walking](#).

- **Certification CI Relationship Conditions**: (Desired State audit types) Define the CI relationships to certify, such as Runs on or Depends on.
- **Certification User Relationship Conditions**: (Desired State audit types) Select the desired user relationship for this configuration item. The relationship provided in the base system is Log reviewed by.
- **Certification Group Relationship Conditions**: (Desired State audit types) Select the desired group relationship for this configuration item. The relationship provided in the base system is Backed up by.
- **Certification Related List Conditions**: (All audit types) Select field values from tables that reference the template table, or user-defined related lists which are created via custom relationships in the `sys_relationship` table. To create a condition that evaluates all servers in the Server (cmdb_ci_server) table for the presence of Microsoft Word 2007, as referenced in the Software Installation (cmdb_sam_sw_install) table. The resulting condition is (Software Installation->Installed on) (Display name) (is) (Microsoft Word 2007).

Check **All** to include all records in the condition requirements of the related list. If there are no records in the related list, then:

- If **All** is checked, the condition requirement is met.
- If **All** is unchecked, the requirement is not met.
Note: By default, the condition builders for relationships display only suggested relationships. To see all possible relationships, select the Show all relationships check box on the right side of the form.

Clear Check

a) Click Insert a new row to insert a condition. You cannot insert an empty condition.
b) Click the green check mark icon to save a condition. Make sure to save the condition before performing any other operation. Updating the form does not save the condition.
c) To delete a condition, click the red X beside the condition. The system marks the condition as inactive.

The system marks the condition as inactive.
### Condition Marked as Inactive

<table>
<thead>
<tr>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;RAM (MB)&quot; greater than &quot;114,000&quot;</td>
</tr>
<tr>
<td>&quot;Disk space (GB)&quot; greater than &quot;5,000&quot;</td>
</tr>
<tr>
<td>&quot;CPU count&quot; greater than or is &quot;2&quot;</td>
</tr>
<tr>
<td>&quot;CPU count&quot; less than &quot;4&quot;</td>
</tr>
</tbody>
</table>

**Insert new row...**

**d)** To reactivate a condition, click the gray X. If another condition for the same field exists, the system prevents reactivation and warns you of the conflict.

8. **Click Submit.**
   ServiceNow saves the template as version 1.

9. To create another version of this template, change the name, edit the conditions, or select a different filter. Updating the template **Description** does not create a new version.

   **Note:** If you select a filter whose table is incompatible with the existing template conditions, the system displays a warning that the conditions cannot be applied.

10. **Click Update.**
    The system saves a new version of the current template and makes it the Active version. The previous version is marked inactive.

### Certification Template Record List

The default Templates list displays only the active version of each template, but users can update the breadcrumbs to display all template versions.

### Default Templates List

The default Templates list displays only the active version of each template, filtered by **Audit type**.
### Default Template

### All Template Versions

To view all template versions for an audit type, click the arrow before *Active=true* to remove that condition from the breadcrumbs.
All Template Versions

Manage Certification template versions

You can view and manage all versions of a template from the Template form.

1. Open any version of a template.
   The Other Versions related list displays all other versions of this template, both active and inactive.

2. Click any version in the related list to display the record for that version.

3. Update the template to create a new version. The system increments a version of the template when you edit any field except Description and Active. You can manage the template versions without returning to the list view.
### ServiceNow Jakarta Now Platform Capabilities

#### Other Templates

<table>
<thead>
<tr>
<th>Number</th>
<th>Active</th>
<th>Name: EBX Server Attributes - UK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td></td>
<td>Attributes for all EBX servers in the UK office</td>
</tr>
<tr>
<td>Filter</td>
<td></td>
<td>EBX Servers - UK/DEV2</td>
</tr>
<tr>
<td>Table</td>
<td></td>
<td>cmdt_ci_esx_server</td>
</tr>
</tbody>
</table>

#### Certification Attribute Conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>&quot;CPU count&quot; is &quot;2&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&quot;Disk space (GB)&quot; greater than &quot;40&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;RAM (MB)&quot; greater than &quot;2000&quot;</td>
</tr>
</tbody>
</table>

#### Certification CI Relationship Conditions

| Condition | Insert a new row... |

#### Certification User Relationship Conditions

| Condition | Insert a new row... |

#### Certification Group Relationship Conditions

| Condition | Insert a new row... |

#### Related Links

Delete inactive versions

<table>
<thead>
<tr>
<th>Other Versions</th>
<th>Audits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>EBX Server Attributes - UK</td>
<td>Attributes for all EBX servers in the UK office</td>
</tr>
<tr>
<td>EBX Server Attributes - UK</td>
<td>Attributes for all EBX servers in the UK office</td>
</tr>
<tr>
<td>Actions on selected rows...</td>
<td></td>
</tr>
</tbody>
</table>
4. To make an inactive template the current version, open that version, edit it if desired, and then click **Revert**.
This action does:

- Deactivates the previously active version of the template.
- Copies the inactive template.
- Makes the new copy the current, active version.

5. Select the Audits related list to view all audits configured to use this template.

6. Click New to create a new audit record with the template selection and table pre-populated.

**Clone a Certification template**

New templates can be cloned from an existing template.

1. Open the template record to be copied.
2. Make any necessary changes.
3. Change the template name or description to distinguish it from the original.
4. Click Clone.
   
   ServiceNow increments the record number above the highest template number and sets the version of the new record to 1. A message appears under the header bar naming the source record for the clone.
Desired State Template Clone

Both templates are Active and appear in the record list. The record list allows you to see the entire history of the template.
Delete a Certification template

Certification templates can be deleted.

Only users with the certification_admin or admin role can delete template versions. You cannot delete a template version that is being used for an audit.

1. To delete a single template version, open that version record and click **Delete**.
   
The system hides the **Delete** button for templates that are in use. If you delete the latest, active version of a template, the previous version of that template is reset to Active.

2. To delete all unused and inactive versions of a template, open any version of that template and click **Delete inactive versions** under **Related Links**. This control appears on all versions, whether they are used in an audit.
Template Delete

Delete unused and inactive versions of this template

Related Links
Delete inactive versions

Other Versions | New | Go to |
--- | --- | ---
**Template** | **Number** | **Description** | **Filter** | **Version**
ESX Server Attributes - UK | TEM001005 | Attributes for all ESX servers in the UK... | ESX Servers - UK - 1 | 1
ESX Server Attributes - UK | TEM001005 | Attributes for all ESX servers in the UK... | ESX Servers - UKDEV - 3 | 2
Actions on selected rows... | | | | | |
3. When prompted, click **OK** to proceed. The system deletes only template versions that are not used in an audit. All protected versions are named in a message that appears in the header bar.

![Figure](image.png)

**Used Template Delete**

**Controls and tests management**

After you identify the risks, define controls with accompanying control tests to prevent issues from occurring.

This diagram illustrates the entire IT GRC control process.
Define a control

Define a control before you define a control test.

1. Navigate to IT GRC > Controls > All.
2. Click New.
3. Fill in the form, as appropriate (see table).
4. Click Submit.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control ID</td>
<td>A unique identifier generated dynamically by the system.</td>
</tr>
<tr>
<td>Name</td>
<td>A name for the control.</td>
</tr>
<tr>
<td>Applies to</td>
<td>Number of a record from any table in the system. This value defines the scope of the control.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Classification</td>
<td>The type of control.</td>
</tr>
<tr>
<td>Purpose</td>
<td>The approach that the control takes.</td>
</tr>
<tr>
<td>Control frequency</td>
<td>The basis for determining when the control is implemented.</td>
</tr>
<tr>
<td>State</td>
<td>A workflow field that determines where in the authoring process the control is.</td>
</tr>
<tr>
<td>Key control</td>
<td>Indicator that the control is considered key to preventing material risk, when selected.</td>
</tr>
<tr>
<td>Owning group</td>
<td>A reference to the group with ownership over the control.</td>
</tr>
<tr>
<td>Owner</td>
<td>A reference to the user with ownership over the control.</td>
</tr>
<tr>
<td>Owner delegate</td>
<td>A reference to the user who has ownership over the control when the specified owner is unavailable.</td>
</tr>
<tr>
<td>Description</td>
<td>A long-form description of the control.</td>
</tr>
</tbody>
</table>

**Define a control test**

After you define a control, create control tests that run periodically and provide documented evidence of whether the associated control is operating correctly.

1. Navigate to IT GRC > Administration > Control Test Definitions.
2. Click New.
3. Fill in the form, as appropriate (see table).
4. Click Submit.
IT GRC Control Test Def
## Defining A Control Test

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Definition ID</td>
<td>A unique identifier generated dynamically by the system.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the control test.</td>
</tr>
<tr>
<td>Control</td>
<td>A reference to the control being enforced.</td>
</tr>
<tr>
<td>Method</td>
<td>One of the following choices for determining the test assignee:</td>
</tr>
<tr>
<td></td>
<td>· Assign to Group: Assignment group for the control test.</td>
</tr>
<tr>
<td></td>
<td>· Assign to Individual: User assigned to the control test.</td>
</tr>
<tr>
<td>Assign to group</td>
<td>Group assigned to this control test. This field is available only when the selected method is Assign to Group.</td>
</tr>
<tr>
<td>Assign to</td>
<td>User assigned to this control test. This field is available only when the selected method is Assign to Individual.</td>
</tr>
<tr>
<td>Remediation group</td>
<td>Group assigned to the remediation tasks when a control test fails.</td>
</tr>
<tr>
<td>State</td>
<td>A workflow field to indicate where in the drafting process this control test currently is. If the state is Active, control test instances are dynamically generated based on the record definition.</td>
</tr>
<tr>
<td>Run</td>
<td>Frequency for generating control test instances. 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></td>
<td>· On Demand</td>
</tr>
<tr>
<td>Time</td>
<td>The time that a control test instance is automatically generated when Run is set to Daily, Weekly, Monthly, or Periodically.</td>
</tr>
<tr>
<td>Day</td>
<td>Day of the week that a control test instance is generated each week when Run is set to Weekly. Day of the month if Run is set to Monthly.</td>
</tr>
<tr>
<td>Repeat interval</td>
<td>A duration, in days and hours, between the automatic generation of control test instances if Run is set to Periodically.</td>
</tr>
<tr>
<td>Starting</td>
<td>The date and time control test instances are first generated when Run is set to Periodically. The only date and time a control test instance is generated if Run is set to Once.</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>
<tbody>
<tr>
<td>Execution step</td>
<td>The steps involved in the control test.</td>
</tr>
<tr>
<td>Expected result</td>
<td>The result that occurs after these tests.</td>
</tr>
<tr>
<td>Include supporting data</td>
<td>Indicator whether sample data is taken from a particular table within the instance when the control test instance is generated.</td>
</tr>
</tbody>
</table>
| Data purpose                | The purpose of the data being sampled If Include supporting data is selected. This selection influences how the control test is performed. Choices are:  
  - None  
  - Support test execution: Returns a random sampling of records.  
  - Identifies non compliance: Returns all the records that do not match the condition or conditions specified.  
  - Identifies compliance: Returns all the records that do match the condition or conditions specified. |
| Table                       | The table from which to sample when Include supporting data is selected. This field is read-only when Template is the Condition type. When you select a template to define test conditions, the certification filter used in the template sets the table and cannot be changed. |
| Fields                      | The list of fields to pull values from when determining whether records match the conditions when Include supporting data is selected. |
| Condition type              | The type of conditions applied to the table and fields. Choices are:  
  - Basic: Applies conditions to the table in question.  
  - Advanced: Uses condition collections to apply conditions to the table and to related tables.  
  - Template: Uses certification templates to apply conditions to the specified table. Select the template to use from the Template field. |
<p>| Sample size                 | An integer number of rows for a random sample if Include supporting data is selected. A sample size of zero returns all matching records. This field is available only if Condition type is set to Basic and Data purpose is set to Support test execution. |
| Control test conditions     | A condition builder that limits the sample data when Include supporting data is selected. This field is available only if Condition type is set to Basic. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>In scope definition</td>
<td>A reference to a condition collection if Include supporting data is selected and Condition type is set to Advanced.</td>
</tr>
</tbody>
</table>
| Configuration to retrieve| Method for using the Configuration reference field if Include supporting data is selected and Condition type is set to Advanced or Template.  
  - None: Returns all records in scope.  
  - Matching: Returns all matching records in scope.  
  - Non-matching: Returns all non-matching records in scope.  
  For more information, see Defining Advanced Conditions. |
| Template                 | (Required) Certification template that defines conditions for this test definition. Only templates with an audit type of Compliance are available for selection. This field is available and mandatory when the value in the Condition type field is Template. |
| Configuration            | Condition collection to use. This field is available only if Include supporting data is selected, Condition type is set to Advanced, and Configuration to retrieve is set to anything except None. |

**Advanced conditions**

Set the Condition type to Advanced on control tests to define more flexible conditions using condition collections.

Condition collections have one primary condition, which is applied to the selected table, and one or more supplemental conditions.

When a control test is performed, advanced conditions evaluate in this order:

1. The system processes the condition collection in the In scope definition reference in this order:  
   a. The primary condition is processed on the fields specified in Table and Fields on the control test definition, returning an array of elements.  
   b. For each element in the array returned by the primary condition, supplemental conditions are processed, filtering the array of elements further.  
   c. The In Scope field is updated with the number of elements in the array.

2. The condition collection in the Configuration reference is processed on the array of elements returned from the In scope definition. The choices for Configuration to retrieve are:  
   - None: These conditions are skipped. Supporting Data is all the elements that are in scope.  
   - Matching: The control test checks the array of elements, returning any elements that match the Configuration.  
   - Non-matching: The control test checks the array of elements, returning any elements where at least one condition did not match the Configuration.
3. The final array of elements is recorded as **Supporting Data** records.

Both the **In Scope** and **Configuration** fields refer to the Condition Collection \[grc_condition_collection\] table.

To define condition collections:
1. Navigate to **IT GRC > Administration > Condition Collections**.
2. Click **New**.
3. Populate these fields:
   - **Name**: Name of the condition collection.
   - **Description**: Description of the condition collection.
   - **Type**: Which **Control Test Definition** field references the condition collection. Choices are:
     - **In Scope Definition**
     - **Configuration Definition**

4. After the condition collection is defined, use the **Add Condition** related link to add these conditions:
   - **Condition**: Predefined condition definition from the Condition \[grc_condition\] table.
   - **Condition type**: The condition collection **Type** determines the choices:
     - **In Scope Definition**
     - **Configuration Definition**

To define new condition records:
1. Navigate to **IT GRC > Administration > Conditions**.
2. Click **New**.
3. Populate these fields:
   - **Name**: Name of the condition collection.
   - **Description**: Description of the condition collection.
   - **Table**: Table on which the condition applies.
   - **Reference Field**: For supplemental conditions, the reference field for the table on which the primary condition is running.
   - **Condition**: Condition builder for defining the condition.

**Control test processing**

When performing a control test, processing dependencies are evaluated.

- If a control test definition is active, the system generates the control test instances dynamically, according to definition. To generate a control test manually:
  1. Navigate to **IT GRC > Administration > Control Test Definitions**.
2. Open a control test definition record.
3. Click **Execute Now**.

ServiceNow generates a control test instance, marks it Pending, and assigns it to the group or individual responsible for the test according to the control test definition.

- If sample data was requested in the definition, any sample data that matches the conditions is found in the Supporting Data section. The Test Complete Data Values related list holds references to the records returned by the sample data query.
- If a control test has a condition type of **Basic**, the value in the Sample size field limits the number of failures that are stored as support data. If the result is passed or compliant, all the matching data is stored.
- If a control test has advanced conditions, the system evaluates them as follows:
  1. The condition collection in the In scope definition reference is processed.
     a. The primary condition is processed on the fields specified in Table and Fields on the control test definition and returns an array of elements.
     b. For each element in the array returned by the primary condition, supplemental conditions are processed, filtering the array of elements further.
     c. The In Scope field is updated with the number of elements in the array.
  2. The condition collection in the Configuration reference is processed on the array of elements returned from the In scope definition. The choices for Configuration to retrieve are:
     - **None**: These conditions are skipped. Supporting Data includes all the elements that were in scope.
     - **Matching**: The control test checks the array of elements, returning any elements that match the Configuration.
     - **Non-matching**: The control test checks the array of elements, returning any elements where at least one condition did not match the Configuration.
  3. The final array of elements is recorded as Supporting Data records.

**Remediation Tasks**

If the control test reveals problems in the process, create a task from the Remediation Task related list. You can relate remediation tasks to any task in the system with the related items tool from the Many to Many Task Relations plugin.

**Scripted audits**

A scripted audit enables users with the certification_admin role to conduct an audit from a script rather than using restrictive template conditions.

A scripted audit uses a certification filter to select the records to audit, and then creates standard follow-on tasks for remediation of any discrepancies. Use this type of audit to query for any values or states that a script can define. A scripted audit is a specific audit type that is activated together with the Desired State plugin. ServiceNow provides a sample audit script with configuration instructions.
Create a scripted audit

A scripted audit is an audit whose conditions are defined by a script.

1. Navigate to **Compliance > Scripted Audits > Audits.**
   An audit type of Scripted filters the list.
2. Click **New.**
3. Complete the form (see table).
4. Create the audit script.
   The Run this script field includes a sample script with instructions for performing the audit and generating the follow-on tasks. This field appears only when you access audits from the Scripted Audits module.
5. Click **Submit.**

Sample script:

```javascript
/*
* ///////////////////////////////////////////////////////////////////////
* /// This script works with Data Center Zones filter ///
* ///////////////////////////////////////////////////////////////////////

var desiredFloorSpaceUsage = 30;  // Value to audit against
var assignToUser = '46d44a23a9fe19810012d100cca80666';  // Beth Anglin
var assignToGroup = '8a5055c9c61122780043563ef53438e3'; // Hardware group
var taskMsg = 'See the audit results below for the discrepancies that must be addressed';

// API call to retrieve records based on the filter
var gr = new SNC.CertificationProcessing().getFilterRecords(current.filter);

// Loop over all records defined by the filter
while(gr.next()) {
    var sysId = gr.getValue('sys_id'); // Sys ID of audited record
    var floorSpaceInUse = gr.getValue('floor_space_in_use'); // Value to audit
    // Determine if certification condition passes or fails
    if (floorSpaceInUse < desiredFloorSpaceUsage) {
        var columnNameSpace = gr.floor_space_in_use.getLabel(); // String value of column audited against
        // Call create Follow on Task API and save the returned sys_id for use in logging audit result fail
        // Params:
        // auditId - Sys id of the audit record executed
        // ciId Sys - id of the configuration item. Empty string if not a cmdb ci
        // assignedTo - Sys id of user to assign task to. Can be empty
        // assignmentGroup - Sys id of group to assign task to. Can be empty
        // shortDescr - Short description for the Follow On Task. Can be empty
        // Return value: Sys id of the created follow on task
        var followOnTask = new SNC.CertificationProcessing().createFollowOnTask(current.sys_id, sysId, assignToUser, '', taskMsg);
        // Call log failed result API
        // Params:
        // auditId - Sys id of audit record executed
        // auditedRecordId - Sys id of the record audited
```
// followOnTask - Sys id of the follow on task associated with the audited record(@see auditedRecordId). Can be empty
// columnDisplayName - Label of the column audited(ex. Disk space (GB)). Can be empty
// operatorLabel - Label of the operator used to audit the column(ex. is not empty, greater than). Can be empty
// desiredValue - Desired value of the column. Can be empty
// discrepancyValue - Discrepancy value. Can be empty
// isCI - True, if audited record is a CI. False, otherwise.
// domainToUse - Sys domain of the "cert_audit" record. Can be empty
new SNC.CertificationProcessing().logAuditResultFail(current.sys_id, sysId, followOnTask, columnNameSpace, 'greater than', desiredFloorSpaceUsage, floorSpaceInUse, true);
} else { // If certification condition pass, write a Audit Result Pass via API
// Params:
// auditId - Sys id of audit record executed
// auditedRecordId - Sys id of the record audited
// isCI - True, if audited record is a CI. False, otherwise. Can be empty.
// domainToUse - Sys domain of the "cert_audit" record. Can be empty.
new SNC.CertificationProcessing().logAuditResultPass(current.sys_id, sysId, true);
} */
Scripted audit

New scripted audit table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for this audit.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Filter</td>
<td>Filter to use when the audit type is Scripted. This field is required for scripted audits, but is hidden for all other audit types.</td>
</tr>
<tr>
<td>Template</td>
<td>(Required) Template to use when this audit runs. Audit type filters the list of available templates and only the active versions of a template are available for selection. This field is hidden when the audit type is Scripted.</td>
</tr>
<tr>
<td>Table</td>
<td>(Read-only) Displays the table for the template.</td>
</tr>
<tr>
<td>Create tasks</td>
<td>Creates follow-on tasks for correcting discrepancies when selected. In a scripted audit, you can create the logic for either task state by using true to create a task or false if no task is created. By default, this check box is cleared (false) in a new audit record.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Assignment type</td>
<td>A choice list to select how the audit assigns the follow-on tasks. This field is visible only when the Create task check box is selected. Choices are:</td>
</tr>
<tr>
<td>Choice list</td>
<td></td>
</tr>
<tr>
<td>Choice</td>
<td>Description</td>
</tr>
<tr>
<td>User Field</td>
<td>Select a user reference field on the table being audited. As an example, select the user named in the Managed by field on the failed record to perform the tasks. This selection displays the Assigned to and Assign to empty fields. If the reference field on the record is empty, the value in the Assign to empty field is used.</td>
</tr>
<tr>
<td>Specific User</td>
<td>Select a specific user to perform the tasks. This selection displays the User field.</td>
</tr>
<tr>
<td>Group Field</td>
<td>Select a group reference field on the table being audited. As an example, select the Support group from the failed record to perform the tasks. This selection displays the Assign to group and Assign to empty fields. All members of the group from the reference field on the failed record are assigned to the tasks. If the reference field on the record is empty, the value in the Assign to empty field is used.</td>
</tr>
<tr>
<td>Specific Group</td>
<td>Select a specific group to perform the tasks. This selection displays</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User</td>
<td>The specific user this audit assigns to follow-on tasks. This field is available under these conditions:</td>
</tr>
<tr>
<td></td>
<td>• Assignment type is set to Specific User.</td>
</tr>
<tr>
<td></td>
<td>• Assign to empty is set to Create Assigned Task, and Assignment type is set to User Field.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Ensure that the specified user has the certification role.</td>
</tr>
<tr>
<td>Assign to group</td>
<td>The group field that defines which group this audit assigns to the follow-on task. This field is available only when the Assignment type is Group Field.</td>
</tr>
<tr>
<td>Group</td>
<td>The specific group this audit assign to follow-on tasks. This field is available only when the Assignment type is Specific Group and you have selected Group Field as the assignment type.</td>
</tr>
<tr>
<td>Assign to</td>
<td>The user field that defines which user this audit assigns to the follow-on task. This field is available only when the Assignment type is User Field.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Assign to empty</td>
<td>The behavior to use if the field selected in Assign to or Assign to group is blank on the record being audited. For example, if a follow-on task must be assigned to a manager, but no manager is identified, the value in this field determines what happens. This field appears only when the Assignment type is User Field or Group Field. The possible selections are:</td>
</tr>
</tbody>
</table>

**Field selection**

<table>
<thead>
<tr>
<th>Selection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do Not Create Task</td>
<td>No follow-on task is created when the Assign to or Assign to group field is empty.</td>
</tr>
<tr>
<td>Create Unassigned Task</td>
<td>Create a follow-on task, but do not assign it to any user or group. The task can be manually assigned later.</td>
</tr>
<tr>
<td>Create Assigned Task</td>
<td>Create a follow-on task and assign it to the user or group specified. If you selected an assignment type of User Field, the User field becomes available. If you selected the Group Field type, the Group field becomes available.</td>
</tr>
</tbody>
</table>

The audit automatically creates follow-on tasks for all records that have Assign to populated, regardless of which selection you make for Assign to empty.

<table>
<thead>
<tr>
<th>Short description</th>
<th>Brief description of the purpose of the audit.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task description</td>
<td>General description of the work required for the follow-on tasks created by this audit. All follow-on tasks created by this audit inherit this description.</td>
</tr>
<tr>
<td>Active</td>
<td>Activates this audit schedule and generates follow-on tasks at the scheduled date and time. Clear this check box to hide scheduling fields on the form (except Last run date) and not generate follow-on tasks.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Run</td>
<td>How often to run the schedule that generates the audit.</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></td>
<td>• On demand</td>
</tr>
<tr>
<td>Day</td>
<td>• If Run is Weekly, the day of the week when the audit runs.</td>
</tr>
<tr>
<td></td>
<td>• If Run is Monthly, the day of the month when the audit runs. If the day is 29, 30 or 31, for shorter months the audit runs on the last day of the month.</td>
</tr>
<tr>
<td>Repeat Interval</td>
<td>If Run is Periodically, the frequency that the audit runs entered in time, days, or both. For example, set Days to 10 and Hours to 14:00:00 to run the audit every 10 days at 2:00pm.</td>
</tr>
<tr>
<td>Starting</td>
<td>If Run is Periodically or Once, the date and time when the audit runs.</td>
</tr>
<tr>
<td>Time</td>
<td>If Run is Daily, Weekly, Monthly, or Once, the time of day, on a 24-hour clock, when the audit runs.</td>
</tr>
<tr>
<td>Last run date</td>
<td>(Read-only) The last date and time the audit ran, either on its regular schedule or manually. Audit previews do not update this field.</td>
</tr>
<tr>
<td>Next scheduled run</td>
<td>(Read-only) The next date and time on which the audit runs. The system recalculates this field when you change the schedule.</td>
</tr>
<tr>
<td>Audit type</td>
<td>(Read-only) The type assigned to this audit. The system selects the audit type based on the application from which the audit was created and can be:</td>
</tr>
<tr>
<td></td>
<td>• Desired State</td>
</tr>
<tr>
<td></td>
<td>• Architecture Compliance</td>
</tr>
<tr>
<td></td>
<td>• Compliance</td>
</tr>
<tr>
<td></td>
<td>• Scripted</td>
</tr>
<tr>
<td>Run this script</td>
<td>Audit script to run. This field is available only when the audit type is Scripted. The Audit form includes a sample script with instructions for performing the audit and generating the follow-on tasks. See Script Methods for a list of the methods provided and the accepted parameters.</td>
</tr>
</tbody>
</table>
**Script methods**

ServiceNow provides four methods for creating the audit script.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>getFilterRecords</code></td>
<td>public GlideRecord getFilterRecords(String filterId)</td>
<td>filterId: The sys_id of the filter to use.</td>
</tr>
</tbody>
</table>
| `logAuditResultPass`      | public void logAuditResultPass(String auditId, String auditedRecordId, boolean isCI, String domainToUse) | auditId: Sys_id of audit record executed.  
auditedRecordId: Sys_id of the record audited.  
isCI: True, if the audited record is a CI, false if otherwise.  
domainToUse: Sys_domain of the cert_audit record. |
| `logAuditResultFail`      | public void logAuditResultFail(String auditId, String auditedRecordId, String followOnTask, String columnDisplayName, String operatorLabel, String desiredValue, String discrepancyValue, boolean isCI, String domainToUse) | auditId: Sys_id of audit record executed.  
auditedRecordId: Sys_id of the record audited.  
followOnTask: Sys_id of the follow-on task associated with the audited record and can be an empty string.  
columnDisplayName: Label of the column audited. For example, Disk space (GB).  
operatorLabel: Label of the operator used to audit the column. For example, is not empty or greater than can be the label.  
desiredValue: Desired value of the column.  
discrepancyValue: Discrepancy value.  
isCI: True, if the audited record is a CI, false if otherwise.  
domainToUse: Sys_domain of the cert_audit record. |
### Data Certification

Data Certification manages scheduled and on-demand validations of the configuration management database (CMDB) data.

Information is added to the CMDB by Discovery, by importing from third-party tools, or manually. For regulatory or procedural reasons, information in the CMDB requires checks for accuracy and certification. The person or team responsible for certification can define what information requires verification and a verification schedule. The schedule then generates a checklist for verifying the data. Individuals assigned to certification tasks answer a series of questions to verify the data.

Data certification can be performed against specific fields on specific tables. Based on the certification schedule, certification tasks are automatically created and assigned. For example, you can set up a certification to validate key information fields, such as Operating System and CPU count, on all Windows servers located in Chicago. You can then assign the tasks to the appropriate team member automatically.

Domain separated systems can use the Data Certification application.

### Activate Data Certification

Activate the Data Certification plugin to access the application. Activating this plugin also activates the Version Management plugin, which manages certification filter versions.

**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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>createFollowOnTask()</td>
<td>public String createFollowOnTask(String auditId, String cId, String assignedTo, String assignmentGroup, String shortDescr)</td>
<td>auditId: Sys_id of the audit record executed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cId: Sys_id of the configuration item. This string is empty when the table is not extended from the cmdb_ci table.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>assignedTo: Sys_id of the assigned user of the task. This string can be empty.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>assignmentGroup: Sys_id of the group the task is assigned to. This string can be empty.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>shortDescr: The text to use for the short description of the follow-on task.</td>
</tr>
</tbody>
</table>
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 Data Certification

Activating the Data Certification plugin installs the following components.

Demo data is available with Data Certification. The demo data provides information including filters, schedules, instances, and tasks.

### Tables

Data Certification adds the following tables:

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Audit Definition</td>
<td>Stores collections of certification schedules that can be run as a single entity.</td>
</tr>
<tr>
<td>(cert_audit_definition)</td>
<td></td>
</tr>
<tr>
<td>Certification Audit Definition Elements</td>
<td>Lists the certification schedules in each certification audit definition.</td>
</tr>
<tr>
<td>(m2m_cert_audit_def_cert_sched)</td>
<td></td>
</tr>
<tr>
<td>Certification Audit Instance</td>
<td>Stores the certification instances associated with a specific audit definition.</td>
</tr>
<tr>
<td>(cert_audit_instance)</td>
<td></td>
</tr>
<tr>
<td>Certification Element</td>
<td>Stores the data elements that are grouped into certification tasks.</td>
</tr>
<tr>
<td>(cert_element)</td>
<td></td>
</tr>
<tr>
<td>Certification Filter</td>
<td>Stores the data that requires certification using a filtering condition for the certification.</td>
</tr>
<tr>
<td>(cert_filter)</td>
<td></td>
</tr>
<tr>
<td>Certification Instance</td>
<td>Stores a collection of certification tasks representing a single instance of a scheduled certification. This table extends the Audit (cert_audit) table.</td>
</tr>
<tr>
<td>(cert_instance)</td>
<td></td>
</tr>
<tr>
<td>Certification Schedule</td>
<td>Stores certification for a specific set of information on a specific table, what user or group the tasks are assigned to, and how often this certification is done.</td>
</tr>
<tr>
<td>(cert_schedule)</td>
<td></td>
</tr>
<tr>
<td>Certification Task</td>
<td>Stores individual certification tasks. Certification Task extends the Task table.</td>
</tr>
<tr>
<td>(cert_task)</td>
<td></td>
</tr>
</tbody>
</table>
Script Includes

Data Certification adds the following script includes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CertificationAjax</td>
<td>Provides utilities that enable individual certification elements to be certified, rejected, or reverted.</td>
</tr>
<tr>
<td>CertificationTaskCreate</td>
<td>Custom code that extends the standard code for certification tasks.</td>
</tr>
<tr>
<td>CertTaskEscalationTimerPercentage</td>
<td>Updates time and percentage complete information for a certification.</td>
</tr>
<tr>
<td>CertificationUtilities</td>
<td>Provides utility functions for certification.</td>
</tr>
</tbody>
</table>

Client Scripts

Data Certification adds the following client scripts:

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert If Boxes Checked</td>
<td>Certification Task (cert_task)</td>
<td>Provides a warning if the certifier attempts to leave a record without certifying the checked elements</td>
</tr>
<tr>
<td>Check Table Name</td>
<td>Certification Schedule (cert_schedule)</td>
<td>Updates the table name when a different filter is selected.</td>
</tr>
</tbody>
</table>

UI Policies

Data Certification adds the following UI policies:

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hide next scheduled run</td>
<td>Certification Schedule (cert_schedule)</td>
<td>Hides the Next Scheduled Run field when the schedule is set to run once or on demand only.</td>
</tr>
<tr>
<td>• Hide &quot;run&quot; associated fields when active is set to false</td>
<td>Certification Schedule (cert_schedule)</td>
<td>Hides the Run field when Active is set to False.</td>
</tr>
<tr>
<td>• Hide Run When Not Active</td>
<td>Certification Schedule (cert_schedule)</td>
<td></td>
</tr>
<tr>
<td>Make table name read only</td>
<td>Certification Schedule (cert_schedule)</td>
<td>Makes the Table field read-only.</td>
</tr>
<tr>
<td>Hide Table field</td>
<td>Certification Element (cert_element)</td>
<td>Hides the Table field on the certification task form.</td>
</tr>
<tr>
<td>Make percent complete field read only</td>
<td>Certification Instance (cert_instance)</td>
<td>Makes the Percent complete field read only when the State is Work in Progress, Closed Complete, Closed Incomplete, or Cancelled.</td>
</tr>
</tbody>
</table>
### Business Rules

Data Certification adds the following business rules:

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adjust dates for cert tasks</td>
<td>Certification Instance</td>
<td>Adjusts dates for tasks belonging to the certification instance when the dates are changed for an active certification.</td>
</tr>
<tr>
<td></td>
<td>(cert_instance)</td>
<td></td>
</tr>
<tr>
<td>Cancel Instance</td>
<td>Certification Instance</td>
<td>Cancels all open certification tasks when an active certification is canceled.</td>
</tr>
<tr>
<td></td>
<td>(cert_instance)</td>
<td></td>
</tr>
<tr>
<td>certification audit instance</td>
<td>Certification Audit</td>
<td>Sends an inserted event when an active certification audit instance is created. Sends a completed event when an active certification audit instance is marked as complete or incomplete.</td>
</tr>
<tr>
<td>events</td>
<td>Instance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(cert_audit_instance)</td>
<td></td>
</tr>
<tr>
<td>certification element events</td>
<td>Certification Element</td>
<td>Sends a failed event when an element of a certification is marked as failed.</td>
</tr>
<tr>
<td></td>
<td>(cert_element)</td>
<td></td>
</tr>
<tr>
<td>certification instance events</td>
<td>Certification Instance</td>
<td>Sends an inserted event when an instance of a certification is created. Sends a completed event when an instance of a certification is completed.</td>
</tr>
<tr>
<td></td>
<td>(cert_instance)</td>
<td></td>
</tr>
<tr>
<td>Certification Instance Rollup</td>
<td>Certification Task</td>
<td>Updates the Percent complete field on the certification instance record.</td>
</tr>
<tr>
<td></td>
<td>(cert_task)</td>
<td></td>
</tr>
<tr>
<td>certification task events</td>
<td>Certification Task</td>
<td>Sends an inserted event when a task is inserted. Sends a completed event when a task is deactivated. Sends a canceled event when a task is canceled.</td>
</tr>
<tr>
<td></td>
<td>(cert_task)</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Certification Task Values</td>
<td>Certification Element (cert_element)</td>
<td>Updates the percent complete of the parent task when a certification element is updated.</td>
</tr>
<tr>
<td>Check Certification Audit Progress</td>
<td>Certification Instance (cert_instance)</td>
<td>Updates the completion status of the audit instance as a whole when a certification that is part of an audit is complete.</td>
</tr>
<tr>
<td>Clean Certification Views</td>
<td>Certification Instance (cert_instance)</td>
<td>Cleans all related records when a certification instance is deleted.</td>
</tr>
<tr>
<td>Copy certification schedule fields</td>
<td>Certification Instance (cert_instance)</td>
<td>Copies changes to the certification schedule to the certification instance.</td>
</tr>
<tr>
<td>Merge Certification Tasks</td>
<td>Certification Task (cert_task)</td>
<td>Merges two tasks together when a task is reassigned and there is another task for the same instance with the new user.</td>
</tr>
<tr>
<td>Prevent delete of Filter with Schedule</td>
<td>Certification Filter (cert_filter)</td>
<td>Prevents the deletion of a filter that is used in a schedule.</td>
</tr>
<tr>
<td>Reassign Notification</td>
<td>Certification Task (cert_task)</td>
<td>Sends out a notification to the new and previous assignees when a task is reassigned.</td>
</tr>
<tr>
<td>Rollup State</td>
<td>Certification Task (cert_task)</td>
<td>Updates all necessary parent items when task state is changed.</td>
</tr>
<tr>
<td>Update audit reference</td>
<td>Certification Task (cert_task)</td>
<td>Makes Data Certification records compatible with Desired State records. This rule makes sure that the Audit field is correctly completed when a record is inserted using Insert and Stay.</td>
</tr>
<tr>
<td>Update audit result</td>
<td>Certification Element (cert_element)</td>
<td>Makes Data Certification records compatible with Desired State records for reporting purposes. This rule puts certified values in the Desired value column when an audit is Certified. It also puts actual values in the Discrepancy value column when an audit is Failed.</td>
</tr>
<tr>
<td>Update follow_on_task &amp; audit references</td>
<td>Certification Element (cert_element)</td>
<td>Makes Data Certification records compatible with Desired State records for reporting purposes. This rule makes certification tasks compatible with follow-on tasks and displays all tasks, regardless of origin.</td>
</tr>
<tr>
<td>Update next run time</td>
<td>Certification Schedule (cert_schedule)</td>
<td>Updates the Next scheduled run field when a schedule runs Daily, Weekly, Monthly, or Periodically.</td>
</tr>
</tbody>
</table>
### Verify Fields

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify Fields</td>
<td>Certification Schedule</td>
<td>Verifies that no field is used in both Display and Certification fields when the fields of a certification schedule are changed.</td>
</tr>
<tr>
<td></td>
<td>(cert_schedule)</td>
<td></td>
</tr>
</tbody>
</table>

### Formatter

Data Certification adds the following formatter:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Task Elements</td>
<td>Enables custom user interface formatting of elements on a certification task. For example, displays the green check mark and red exclamation point to use when certifying an element.</td>
</tr>
</tbody>
</table>

### Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.ui.cert_task_activity.fields</td>
<td>System Properties (sys_properties)</td>
<td>Defines which journal field is the task activity field. Default: work_notes</td>
</tr>
</tbody>
</table>

### User Roles

Data Certification adds the following user roles:

<table>
<thead>
<tr>
<th>Role</th>
<th>Contains Roles</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certification_admin</td>
<td>certification</td>
<td>Can:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Create and configure certifications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Override provided answers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Perform certification tasks for certification task owners</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Send certification task notifications to users and owners at any time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cancel or delete certifications in any state</td>
</tr>
</tbody>
</table>
### Role Contains Roles Description

<table>
<thead>
<tr>
<th>Role</th>
<th>Contains Roles</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certification_filter_admin</td>
<td>certification</td>
<td>Can create and manage all data certification filters.</td>
</tr>
<tr>
<td>certification</td>
<td>none</td>
<td>Can update active or incomplete tasks assigned to them or to groups of which they are a member. Can also update configuration items owned by them or by groups of which they are a member. Receives email notifications when assigned certification tasks.</td>
</tr>
</tbody>
</table>

### Events

Data Certification adds the following events. The ServiceNow system uses these events to send email notifications to task owners and managers about changes in certification records.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cert_audit_instance.completed</td>
<td>A certification audit instance has been completed.</td>
</tr>
<tr>
<td>cert_audit_instance.inserted</td>
<td>A certification audit instance has been inserted.</td>
</tr>
<tr>
<td>cert_element.failed</td>
<td>A certification element has failed certification.</td>
</tr>
<tr>
<td>cert_instance.complete</td>
<td>A certification instance has been completed.</td>
</tr>
<tr>
<td>cert_instance.inserted</td>
<td>A certification instance has been inserted.</td>
</tr>
<tr>
<td>cert_task.cancelled</td>
<td>A certification task has been canceled.</td>
</tr>
<tr>
<td>cert_task.completed</td>
<td>A certification task has been completed.</td>
</tr>
<tr>
<td>cert_task.escalate</td>
<td>A certification task record has been escalated.</td>
</tr>
<tr>
<td>cert_task.inserted</td>
<td>A new certification task has been created.</td>
</tr>
<tr>
<td>cert_task.notifications</td>
<td>A certification task notification has been resent to a user.</td>
</tr>
<tr>
<td>cert_task.overdue</td>
<td>A certification task is past its specified completion date.</td>
</tr>
<tr>
<td>cert_task.reassign</td>
<td>A certification task has been reassigned.</td>
</tr>
<tr>
<td>cert_task.warning</td>
<td>A new task escalation point has been reached.</td>
</tr>
</tbody>
</table>

### Email Templates

Data Certification adds the following email templates:

<table>
<thead>
<tr>
<th>Name</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>certification.task.cancelled</td>
<td>A certification task assigned to you/your group as part of the data certification and management process has been canceled.</td>
</tr>
<tr>
<td>Name</td>
<td>Message</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>certification.task.reminder.inserted</td>
<td>A certification task that has been assigned to you/your group as part of the data certification and management process requires attention.</td>
</tr>
<tr>
<td>certification.task.reminder.outstanding</td>
<td>A certification task that has been assigned to you/your group as part of the data certification and management process requires attention.</td>
</tr>
<tr>
<td>certification.task.reminder.overdue</td>
<td>A certification task that has been assigned to you/your group as part of the data certification and management process is overdue.</td>
</tr>
</tbody>
</table>

**Certification schedules**

A certification schedule defines the information that requires certification and the frequency of execution.

At each time interval specified, or on-demand, the certification schedule generates a set of certification tasks based on set conditions. Use the Preview Certification Tasks related link to preview the certification tasks generated from a certification schedule.
Certification schedule

Unix Server in South Africa

- Name: Unix Server in South Africa
- Filter: Unix Server in South Africa
- Table: Unix Server (cmdb_ci_unix_server)
- Active: Checked
- Run: Monthly
- Day: 1
- Time: Hours: 00, Minutes: 00, Seconds: 00
- Last run date: 2012-10-29 12:22:27
- Next scheduled run: 2012-11-01 00:00:00

- Display fields: 
- Certification fields: CPU speed (MHz), RAM (MB), CPU core count
- Assignment type: Specific User
- User: Abel Tuter
- Days to complete: 2
- Task description: Ensure that all Unix Servers in South America data center meet minimum reqs
- Instructions:

The minimum requirements for Unix Servers are:
- CPU Speed: 3GHz
- RAM: 15GB
- CPU Core Count: 4
Certification tasks

A certification task represents the work of verifying the data associated with a particular record. Task owners are responsible for performing the certification tasks. Tasks have an associated workflow that sends reminders to the task owner and, if necessary, the manager of the owner at regular intervals.
Certification task

© 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.
Certification elements

Each element of each record being certified is tracked in its own certification element record. Also tracked are the date and time when the element was certified, comments, and the original and certified values of the field. You can view elements on individual certification tasks.
Certification instances

A certification instance is the collection of certification tasks for one execution of a certification schedule.

Certification audit instances

A certification audit instance is a collection of the certification instances and tasks generated by a single execution of the certification audit definition.
Certification audit instance

Certification audit definition

A certification audit definition is a collection of certification schedules that can be run at once.
Certification Audit Definition

<table>
<thead>
<tr>
<th>Name</th>
<th>Certify Servers and Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Days to complete</td>
<td>14</td>
</tr>
<tr>
<td>Description</td>
<td>Annual certification of Servers and Groups</td>
</tr>
</tbody>
</table>

### Certification Schedules (2)

<table>
<thead>
<tr>
<th>Certification Schedule</th>
<th>Certification fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certify groups</td>
<td>sys_user_group</td>
</tr>
<tr>
<td></td>
<td>cost_center,email,type,default_assignee</td>
</tr>
<tr>
<td>Certify servers</td>
<td>cmdb_ci_server</td>
</tr>
<tr>
<td></td>
<td>classification,cost_center,owned_by,support_group</td>
</tr>
</tbody>
</table>

Related Links

Create Certification Audit Instance
Data Certification Overview module

The Data Certification Overview module displays various data certification-related reports on the Data Certification Console homepage.

The Overview module is a type of homepage.

The different levels of access are:

<table>
<thead>
<tr>
<th>Role</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>certification</td>
<td>View (view overview page and refresh reports)</td>
</tr>
<tr>
<td>certification_admin</td>
<td>• View (view overview page and refresh reports)</td>
</tr>
<tr>
<td></td>
<td>• Customize (refresh, add, delete, and rearrange reports)</td>
</tr>
<tr>
<td>admin</td>
<td>• View (view overview page and refresh reports)</td>
</tr>
<tr>
<td></td>
<td>• Customize (refresh, add, delete, and rearrange reports)</td>
</tr>
<tr>
<td></td>
<td>• Edit (can edit reports)</td>
</tr>
</tbody>
</table>

Data Certification Overview Module

The Overview module includes the following reports:

<table>
<thead>
<tr>
<th>report</th>
<th>Description</th>
<th>Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>30/60/90 Day Aging</td>
<td>Groups tasks by the number of days (30, 60, 90, and 90 and over) since the task was opened.</td>
<td>Certification Task</td>
</tr>
<tr>
<td>Certification Instances</td>
<td>Lists all certification instances.</td>
<td>Certification Instance</td>
</tr>
<tr>
<td>Certification Progress Report</td>
<td>Groups tasks by task owner, indicating task progress as a percentage.</td>
<td>Certification Task</td>
</tr>
<tr>
<td>Certification Task Completed Report</td>
<td>Groups tasks by task owner, indicating tasks that are complete.</td>
<td>Certification Task</td>
</tr>
<tr>
<td>Exceptions To Date</td>
<td>Lists all task elements that have comments added and a state of Failed or In Progress.</td>
<td>Certification Element</td>
</tr>
<tr>
<td>report</td>
<td>Description</td>
<td>Table</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Functional Roll Up</td>
<td>Lists the managers that have groups with assigned certification tasks. The report is a horizontal bar chart, grouped by status, with each bar representing a manager of an assignment group.</td>
<td>Certification Task</td>
</tr>
<tr>
<td>Hierarchical Roll Up</td>
<td>Shows the managers that have employees with assigned certification tasks (task owners). The report is a horizontal bar chart, grouped by status, with each bar representing a manager of a task owner (identified in the Assigned to field).</td>
<td>Certification Task</td>
</tr>
<tr>
<td>Upcoming Schedules</td>
<td>Lists all schedules that are scheduled to run within the next 30 days.</td>
<td>Certification Schedule</td>
</tr>
</tbody>
</table>

**Use the Data Certification Overview module**

View the status of data certification tasks.

1. Navigate to Data Certification > Overview.
2. Click elements within the reports to obtain more information.
   - For example, click any of the colored bars in the Functional Roll Up bar chart and detailed information replaces the Data Certification Console screen.
3. Update some fields directly on the overview page.
   - For example, in the red box on the image shown, a certification schedule is being updated in the certification instances report.
### Data Certification Overview Module

The Data Certification Console allows users to manage certification schedules and track progress.

#### Certification Instances

<table>
<thead>
<tr>
<th>Number</th>
<th>Certification Type</th>
<th>Percent Complete</th>
<th>Created</th>
<th>Complete By</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Certifications</td>
<td>50%</td>
<td>2013-10-10 10:20:34</td>
<td>2014-03-13 15:04:47</td>
</tr>
<tr>
<td>2</td>
<td>Certifications</td>
<td>30%</td>
<td>2013-08-15 10:20:30</td>
<td>2013-08-18 10:54:22</td>
</tr>
<tr>
<td>3</td>
<td>Work Server Schedule</td>
<td>0%</td>
<td>2013-08-11 10:04:37</td>
<td>2013-12-18 14:04:37</td>
</tr>
<tr>
<td>4</td>
<td>Oracle Database Schedule</td>
<td>100%</td>
<td>2013-12-30 10:04:37</td>
<td>2014-03-13 16:04:37</td>
</tr>
<tr>
<td>5</td>
<td>Advento HR</td>
<td>100%</td>
<td>2013-03-11 16:19:23</td>
<td>2013-04-13 15:04:57</td>
</tr>
<tr>
<td>6</td>
<td>York's World</td>
<td>0%</td>
<td>2013-10-10 10:04:57</td>
<td>2014-01-18 14:04:57</td>
</tr>
<tr>
<td>7</td>
<td>York's User License Console</td>
<td>40%</td>
<td>2013-02-01 10:04:27</td>
<td>2013-02-11 16:04:57</td>
</tr>
</tbody>
</table>

#### Certification Progress Report

<table>
<thead>
<tr>
<th>Number</th>
<th>State</th>
<th>Assigned To</th>
<th>Short Description</th>
<th>Percent Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Assigned</td>
<td>Temple (1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Assigned</td>
<td>Amy (1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Assigned</td>
<td>Asset Manager (1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Assigned</td>
<td>Andrea (1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Assigned</td>
<td>Beth (1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Assigned</td>
<td>Now (1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Assigned</td>
<td>Robert (1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Assigned</td>
<td>Robert (1)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Functional Roll-Up

The functional roll-up provides a visual representation of certification tasks, with states including Work in Progress, Closed, Complete, and Cancelled.
Data Certification planning

Initial planning can make the certification process more successful. By defining certification schedules and certification audit definitions, users with the certification_admin role establish when certifications are performed, who performs it, and what data must be certified.

Required Roles

Users with the certification_admin role can view filter versions. These users can create, update, and delete filters, if they have the proper access to necessary tables. In the base ServiceNow system, certification_admin users have limited system rights and do not have access to all the tables required for creating a filter. When assigning compliance resources, make sure to grant additional roles to the certification_admin user as needed. For example, this user requires roles that grant access to these tables:

- Company [core_company]
- Cost Center [cmn_cost_center]
- Schedule [cmn_schedule]

Planning Data Certification

Planning the data certification process requires defining:

- The certification schedule defines certification for a particular set of information on a particular table. It also generates certification tasks to perform that certification. One certification task is generated per task owner and a certification instance record groups the tasks.
- The optional certification audit definition groups some certification schedules to be performed together and generates certification audit instances to perform them.

The following questions require answers for each certification schedule:

- What information requires certification?
- When is the due date for certification?
- Who must perform the certification?

Create a certification filter

A filter is a subset of configuration items from any ServiceNow table that is created with a standard condition builder.

An example is a filter that selects all UNIX servers in the Australian data center.

With filters, you can:

- Create multiple versions of a filter and then select the version you want to use.
- Use one filter on multiple certification schedules.
- View the number of records that match your filter as you create the conditions.

Note: Be sure to create certification filters before creating certification schedules.

1. Navigate to Data Certification > Certification Filters.
2. Click New.
3. Fill in the form (see table).
4. Click **Submit**.

This action saves the filter as version 1.

5. To create another filter version, modify the filter conditions and click **Update**.

The system saves the new filter and increments the version number.
Certification filter V2

By default, the Certification Filters list shows only the current version of each filter. To see all filter versions, click **All** in the breadcrumbs.
Certification Filter List

6. To make an inactive filter the current version, open the inactive filter and click **Revert**.
Certification filter revert

This action creates a new, active version of the filter and makes all previous versions inactive.

7. To delete a single filter version, open that version record and click **Delete**.

8. To delete inactive versions of a filter, click **Delete inactive versions** under **Related Links** in that filter record.

You cannot delete a filter that is used in a schedule definition. The system displays a warning and the filter is not deleted.

Creating certification filters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>(Required) Filter name.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Brief description of the filter.</td>
</tr>
<tr>
<td>Number</td>
<td>(Read-only) Automatically assigned filter identification number.</td>
</tr>
<tr>
<td>Table</td>
<td>Table containing the records to be filtered. Use of the Database View [sys_db_view] table is limited by version.</td>
</tr>
</tbody>
</table>
Field | Description
---|---
Active | Control to make the filter available for use from the Filter field on the Certification Schedule form.
Version | Current version of this filter. Any significant changes to the filter make the current version inactive. The system copies the updated filter, marks it as active, and increments the version number. The system saves all versions of the filter and makes them available to users. More than one version of a filter can be marked active.
Filter condition | Field, operator, and value to create the condition. The available options depend on the table selected. You can view the number of records that match the filter by clicking the refresh icon.

**Refresh Conditions**

If the filter does not match any records, the system marks the certification instance as Closed Complete, with the Percent complete value set to 100%.

---

**Define a certification schedule**

A certification schedule specifies the fields to display, the fields that require certification, certification task assignments, completion requirements for task owners, frequency of schedule, and detailed instructions.

Use the preview option to see what tasks are created before saving the schedule. If the tasks are not what you want, edit the schedule and preview the tasks again. The system creates certification tasks automatically when it executes a schedule.

To schedule a certification:

1. Navigate to Data Certification > Schedule Definitions.
2. Click New
3. Fill in the fields (see table).
4. Click Submit.

### Defining A Certification Schedule

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A schedule name.</td>
</tr>
<tr>
<td>Filter</td>
<td>A certification filter for this schedule.</td>
</tr>
<tr>
<td>Table</td>
<td>(Read-only) The table holding the records to be certified. To change the table name, select a different Filter or create a new Filter.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Display fields</td>
<td>The fields displayed in the Certification Task list to provide context. These do not require certification themselves. For example, although users are not required to certify the Name field of a record, it displays so that users know what record they are certifying.</td>
</tr>
<tr>
<td>Certification fields</td>
<td>The fields to certify on this certification schedule.</td>
</tr>
<tr>
<td>Assignment type</td>
<td>A choice list to select how the certification schedule assigns the certification tasks.</td>
</tr>
<tr>
<td></td>
<td>• <strong>User Field</strong>: Select a user reference field on the table being certified. As an example, select the user named in the Managed by field to identify the user who performs the task. This selection displays the Assign to and Assign to empty fields. If the reference field on the record is empty, the value in the Assign to empty field is used.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Specific User</strong>: Select a specific user to perform the tasks. This selection displays the User field.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Group Field</strong>: Select a group reference field on the table being certified. As an example, select the Support group field to identify the user who performs the task. This selection displays the Assign to group and Assign to empty fields. All members of the group from the reference field on the record are assigned to the tasks. If the reference field on the record is empty, the value in the Assign to empty field is used.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Specific Group</strong>: Select a specific group to perform the tasks. This selection displays the Group field. All members of the named group are assigned to the tasks.</td>
</tr>
<tr>
<td>User</td>
<td>This field appears when:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Assignment type</strong> is <strong>Specific User</strong>. This system assigns this user to all certification tasks for this schedule.</td>
</tr>
<tr>
<td></td>
<td>• The <strong>Assign to empty</strong> field is set to <strong>Create Assigned Task</strong>, and you have selected <strong>User Field</strong> as the assignment type. The system assigns this user to certification tasks containing unassigned records.</td>
</tr>
<tr>
<td></td>
<td>You can only select users with the certification role.</td>
</tr>
<tr>
<td>Assign to group</td>
<td>The group field that defines the group assigned to the certification tasks. This field is available only when the <strong>Assignment type</strong> is <strong>Group Field</strong>.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Group</td>
<td>The specific group to which certification tasks are assigned for this schedule. This field is available only when the <strong>Assignment type</strong> is <strong>Specific Group</strong>.</td>
</tr>
<tr>
<td>Assign to</td>
<td>The user field that defines which user is assigned to the certification task. This field is available only when the <strong>Assignment type</strong> is <strong>User Field</strong>.</td>
</tr>
<tr>
<td>Assign to empty</td>
<td>The behavior to use if the field selected in <strong>Assign to</strong> or <strong>Assign to group</strong> is blank on the record being certified. For example, if a task must be assigned to a manager, but no manager is identified, the value in this field determines what happens. This field appears only when the <strong>Assignment type</strong> is <strong>User Field</strong> or <strong>Group Field</strong>. The possible selections are:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Do Not Create Task</strong>: No task is created when the <strong>Assign to</strong> or <strong>Assign to group</strong> field is empty.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Create Unassigned Task</strong>: Create a task, but do not assign it to any user or group. The task can be manually assigned later.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Create Assigned Task</strong>: Create a task and assign it to the user or group specified. If you selected an assignment type of <strong>User Field</strong>, the <strong>User</strong> field is available. If you selected the <strong>Group Field</strong> type, the <strong>Group</strong> field is available.</td>
</tr>
<tr>
<td></td>
<td>The schedule automatically creates certification tasks for all records that do have “Assign to” populated, regardless of which selection you make for “Assign to empty.”</td>
</tr>
<tr>
<td>Days to complete</td>
<td>(Required) The number of days that task owners have to complete the certification tasks. When the certification schedule is part of a certification audit definition, the <strong>Days to Complete</strong> audit definition value overrides the value set for the certification schedule.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box to activate this certification schedule, generating certification tasks at the scheduled date and time. Clear this check box to hide scheduling fields on the form (except <strong>Last run date</strong>) and not generate certification tasks.</td>
</tr>
<tr>
<td>Run</td>
<td>How often to run the schedule that generates certification tasks:</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></td>
<td>- On Demand</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Day</td>
<td>When Run is <strong>Weekly</strong>, the day of the week when the schedule runs and generates certification tasks. When Run is <strong>Monthly</strong>, the day of the month the schedule runs and generates certification tasks. If the day is <strong>29</strong>, <strong>30</strong> or <strong>31</strong>, the certification runs on the last day of the month for shorter months.</td>
</tr>
<tr>
<td>Repeat Interval</td>
<td>When Run is <strong>Periodically</strong>, the frequency that the schedule runs to generate certification tasks, entered in time, days, or both. For example, set Days to <strong>10</strong> and Hours to <strong>14:00:00</strong> to run the schedule and generate certification tasks every 10 days at 14:00.</td>
</tr>
<tr>
<td>Starting</td>
<td>When Run is <strong>Periodically</strong> or <strong>Once</strong>, the date and time the schedule runs and generates certification tasks.</td>
</tr>
<tr>
<td>Time</td>
<td>When Run is <strong>Daily</strong>, <strong>Weekly</strong>, <strong>Monthly</strong>, or <strong>Once</strong>, the time of day, on a 24-hour clock, the schedule runs and generates certification tasks.</td>
</tr>
<tr>
<td>Last run date</td>
<td>(Read-only) The date and time that the schedule ran last, either on its regular schedule or manually, and generated certification tasks.</td>
</tr>
<tr>
<td>Next scheduled run</td>
<td>(Read-only) The next date and time the schedule runs and generates certification tasks.</td>
</tr>
<tr>
<td>Task Description</td>
<td>A description to add to the Short Description field of the certification task.</td>
</tr>
<tr>
<td>Instructions</td>
<td>An HTML field for providing instructions to the user or group performing the certification.</td>
</tr>
</tbody>
</table>

**Preview a certification task**

Previewing certification tasks saves any changes to the Certification Schedule form and displays the tasks that are created when you execute the certification schedule.

Previewing tasks is especially useful if you want to test different combinations of options in the Assignment type, Assign to, and Assign to empty fields.

1. Navigate to **Data Certification > Schedules > Schedule Definitions**.
2. Click a certification schedule **Name**.
3. In Related Links, click **Preview Certification Tasks**.
   
   The tasks to be created appear at the top of the screen.
Use a certification schedule notification

After you define a certification schedule, the system automatically sends notifications to specific users based on the information in the schedule.

The following notifications are sent automatically:

**Certification Schedule Notifications**

<table>
<thead>
<tr>
<th>Time elapsed to end date</th>
<th>Email template name</th>
<th>Notification message is sent to</th>
</tr>
</thead>
<tbody>
<tr>
<td>0% (when task is created)</td>
<td>certification.task.reminder.inserted</td>
<td>Task owner or assignment group, if specified</td>
</tr>
<tr>
<td>50%</td>
<td>certification.task.reminder.outstanding</td>
<td>Task owner or assignment group, if specified</td>
</tr>
<tr>
<td>75%</td>
<td>certification.task.reminder.outstanding</td>
<td>Task owner, assignment group, if specified, and manager of the task owner, if specified</td>
</tr>
<tr>
<td>95%</td>
<td>certification.task.reminder.outstanding</td>
<td>Task owner, assignment group, if specified, and manager of the task owner, if specified</td>
</tr>
<tr>
<td>100%</td>
<td>certification.task.reminder.overdue</td>
<td>Task owner, assignment group, if specified, and manager of the task owner, if specified</td>
</tr>
</tbody>
</table>

The email templates used in the notifications can be edited, for example, to change the email message text.

Executing a Certification Schedule

Executing a certification schedule generates certification tasks based on the schedule.

1. Navigate to Data Certification > Schedules > Schedule Definitions.
2. Click a certification schedule Name.
3. Click Execute Now.

The related lists Certification Instances and Certification Tasks display the instances or tasks generated by the schedule. The amount of time it takes to generate all certification tasks depends on the size of the table selected and how many fields require certification.
Define and create a certification audit

A certification audit is a collection of certification schedules that can be run as a single entity. Certification audits can be useful when there are multiple certification schedules. After creating a certification audit definition, you can generate a certification audit instance. The certification audit instance is a collection of the certification instances and tasks generated by a single execution of the certification audit definition.

1. Navigate to Data Certification > Audits > Audit Definitions.
2. Click New.
3. Fill in the fields (see table).
4. Right-click the header bar and select Save.
5. In the Certification Schedules related list, click Edit.
6. In the Collection list on the left, select one or more schedules and click Add.
7. Click Save.
8. In Related Links, click Create Certification Audit Instance.

The system generates an audit instance based on the certification schedules selected. All audit instances based on this audit definition are listed in the Certification Audit Instances related list.
Defining and Creating a Certification Audit

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the audit definition.</td>
</tr>
<tr>
<td>Days to Complete</td>
<td>The number of days that task owners have to complete the certification tasks created by this audit definition. Overrides the identical field on the certification schedule.</td>
</tr>
<tr>
<td>Description</td>
<td>A short description of the intended audit.</td>
</tr>
</tbody>
</table>

**Track a certification audit instance**

You can view a list of all certification audit instances at any time.

1. Navigate to Data Certification > Audits > Audit Instances.
2. View the Certification Instances related list.

   The list contains each of the associated instances generated as part of the audit.

**Data certification performance**

After the certification process has been planned, certification tasks can be performed according to defined schedules.

Users with the certification role can perform certification tasks. The certification tasks can be tracked as part of certification instances.

**Fulfill certification tasks**

After you execute a certification schedule manually or at a scheduled time, the ServiceNow system performs certain actions.

After you execute a certification schedule manually or at a scheduled time, ServiceNow performs the following actions:

- Creates tasks for any records that meet the filter requirements in the specified table, like tasks from the Configuration Item [cmdb_ci] table.
- Assigns the new tasks to the user or group identified in one of these certification schedule fields:
  - Assign to
  - User
  - Assign to group
  - Group
- Places the new tasks in the Work in Progress state.
- Adds the certification schedule Short description and Assigned to values to the corresponding fields on the certification task record.
- Adds the certification schedule Days to complete and Complete by date fields to the certification task record, based on when the task is created.
**Note:** If the certification filter does not match any CIs, the system sets the State to Closed Complete and the Percent complete to 100.

To view tasks assigned to you, navigate to **Data Certification > Tasks > My Tasks**.

The following information is tracked on the certification task record:

**Certification task record**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>An identification number for the certification task.</td>
</tr>
<tr>
<td>Assigned to</td>
<td>The user responsible for certifying the data.</td>
</tr>
<tr>
<td>Assignment group</td>
<td>The group responsible for certifying the data.</td>
</tr>
<tr>
<td>Complete by</td>
<td>(Read-only) A date field containing a deadline for the task. This field is automatically filled in based on the Days to Complete field on the certification schedule.</td>
</tr>
<tr>
<td>State</td>
<td>(Read-only) The current state of the certification task. The selections are: Work in Progress, Closed Incomplete, Closed Complete, and Cancelled.</td>
</tr>
<tr>
<td>Percent complete</td>
<td>The task progress as a percentage. This field is read-only when a task is in a Closed Incomplete, Closed Complete, or Cancelled state.</td>
</tr>
<tr>
<td>Escalation</td>
<td>(Read-only) The escalation level of the task. When 0–49% of the time to Complete By has elapsed, this field is set to Normal. At 50%, this field changes to Moderate and an email reminder is sent to the task owner. At 75%, this field changes to High and an email reminder are sent to the task owner and the manager of the task owner. At 95%, this field remains set to High, but a second email reminder is sent to the task owner and manager.</td>
</tr>
<tr>
<td>Short Description</td>
<td>A short description of the task. This field is automatically filled in with the text from the certification schedule of the Task description field.</td>
</tr>
<tr>
<td>Work notes</td>
<td>Information about work performed on the certification.</td>
</tr>
</tbody>
</table>

**Export the certification list**

Users with the certification_admin role can export the certifications list and save the list in Excel, CSV, XML, or PDF format. This list is useful when you have a long list of certification elements or if many different users are assigned to certify elements on a single certification schedule.

For general information and common export steps, see [List export](#).

1. Navigate to **Data Certification > Tasks > All Tasks**
2. Open a task.
3. Open any column context menu in the certification data list and complete the export.
Certify an element

The Certification Task form contains a list of all elements to be certified.

**Note:** After you certify all the elements in a task, no elements can be reverted.

1. Navigate to Data Certification > Tasks > My Tasks.
2. Open a certification task with a State of Work in Progress.
3. In the upper right corner of the list, select records that require certification for this task or all records that are part of this certification task.
4. Select the check box beside a certification element.
5. In Optional comment for checked elements, above the list, enter information that would be useful to others.
6. Do:
   - Click the green check mark to certify the element.
   - Click the red exclamation point to fail the element.

7. To see the certified or failed element, set the view to Show All Records.
   A green check mark or red exclamation mark appears beside the element.

8. Point to an icon to see any certification comments.

9. Ensure that all elements have the correct certification, either accepted or rejected.
   After you certify all elements, no elements can be reverted. When all elements of a certification task are certified or rejected, the task State changes to Closed Complete.

View an audit result

View audit results after you certify the elements.

1. Navigate to Data Certification > Schedules > Audit Results.
   The list of data certification audit results appears, grouped by certification instances. Certified configuration items show the Original value only. Failed CIs contain the Certified value and the Original value.

2. Click the links in the list to open any of the related records.
Data cert audit results

Reset certifications

You cannot reset any element after all elements are certified. You cannot reset any element after all elements are certified.

- To reset individual certifications, right-click the element in the certification list and select Revert Certification.
- To reset the entire task to its starting point, click the Reset all Certifications to Pending related link.

Track a task with a certification instance

The Certification Tasks related list on the certification instance record provides information about associated tasks.
The State field on the certification instance record is read-only and is based on the cumulative states of the certification tasks associated with the instance. The Percent complete column allows users with the certification_admin role to track task progress quickly. For more information, see Track Certification Tasks.

To track a certification instance:

1. Navigate to Data Certification > Schedules > Instances.
2. Click a certification instance Number.
3. View and edit the following fields as necessary:

### Certification instance

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>(Read-only) Automatically generated identification number for the instance.</td>
</tr>
<tr>
<td>Certification Schedule</td>
<td>The certification schedule used to create the certification instance.</td>
</tr>
<tr>
<td>State</td>
<td>(Read-only) Current state of the certification instance: Work in Progress, Complete, Closed Incomplete, or Cancelled. For more information, see Track Certification Tasks.</td>
</tr>
<tr>
<td>Created</td>
<td>(Read-only) Date and time the certification instance was created. Date is filled in automatically when the Execute Now button clicks the associated certification schedule.</td>
</tr>
<tr>
<td>Complete by</td>
<td>(Required) Date and time when the certification instance must be completed. The system updates this field when it executes the schedule, using the deadline specified on the instance. All certification tasks associated with the certification instance must be marked Complete, Closed Incomplete, or Cancelled before the instance is complete.</td>
</tr>
<tr>
<td>Percent complete</td>
<td>Percentage of the instance that has reached the Closed Complete state. This field is automatically filled in based on the Percent Complete fields on the associated certification tasks.</td>
</tr>
<tr>
<td>Task Description</td>
<td>Information about the certification instance. This field automatically displays the text from the Task description field of the associated certification schedule.</td>
</tr>
<tr>
<td>Instructions</td>
<td>Field for providing instructions to the user or group performing the certification. This field is automatically filled in with information from the Instructions field on the associated certification schedule.</td>
</tr>
</tbody>
</table>

### Cancel a certification instance

Users with the certification_admin role can cancel a certification instance.
The instance must have a State of Work in Progress. Canceling a certification instance:
  - Changes the certification instance State to Cancelled.
  - Changes all associated Work in Progress certification tasks to Cancelled.

To cancel a certification instance:
1. Navigate to **Data Certification > Schedules > Instances**.
2. Click a certification instance Number.
3. Click **Cancel**.

**Track a certification task**

Use the certification task state to track the progress of a task.

The available task states are Work in Progress, Closed Complete, Closed Incomplete, and Cancelled.

When the state of a certification task changes, the certification instance state also changes in the following cases:
  - If any certification task is in Work in Progress state, the certification instance is placed in Work in Progress state.
  - If all certification tasks are in Cancelled state, the certification instance is placed in Cancelled state.
  - If all certification tasks are in Cancelled or Closed Complete state, the instance is placed in a Closed Complete state. For example, if three certification tasks are Cancelled, and one task is Closed Complete, the instance state is changed to Closed Complete.
  - When one certification task is Closed Incomplete and the remainder of the tasks are Cancelled or Closed Complete, the instance is placed in Closed Incomplete.

To view the state of certification tasks:
1. Navigate to **Data Certification > Tasks** and select **My Tasks** or **All Tasks**.
2. View the State column for each task.

**Escalate a certification task**

Users with the certification_admin role can escalate a task in the Work in Progress state. To escalate a task, the task owner identified in the Assigned to field on the task record must have an associated manager.

Personalize the User form to see the Manager field.

Escalating a task:
  - Sends an email message to the task owner and the manager of the task owner stating that the task has been escalated.
  - Sets the manager as the new task owner.

The event that triggers the escalation is named cert_task.escalate and the email notification is named Escalation Notification. To edit the text of the email message that is sent, edit the Escalation Notification email notification directly.

For more information, see [Email and SMS notifications](#).

To escalate a certification task from the Certification Task form:
1. Navigate to **Data Certification > Tasks > All Tasks**.
2. Click a certification task Number.
3. Click **Escalate**. If the Escalate button is not available, the user in the Assigned to field does not have an associated Manager.

### Escalate a certification task from the certification task list

1. Navigate to **Data Certification > Tasks > All Tasks**.
2. Select the check box to the left of a certification task Number. Multiple check boxes can be selected.
3. From the Actions on Selected Rows menu below the list, select **Escalate**. If the Escalate button is not available, the user in the Assigned to field does not have an associated Manager.
   Select multiple tasks from the list. The menu option shows how many tasks are not eligible for escalation, such as Escalate (4 of 6).

### Reassign a certification task

If you have the certification_admin role, you can reassign any certification task in the Work in Progress state. Tasks in Closed Complete, Closed Incomplete, or Cancelled state cannot be reassigned. When a task is reassigned, the current task owner and the new task owner are sent a message.

Role required: certification_admin

The event associated with the reassignment is named cert_task.reassign and the email notification is named Certification Task Reassignment. To edit the text of the email message that is sent, edit the Certification Task Reassignment email notification directly.

For more information, see [Email and SMS notifications](#).

To reassign a certification task:

1. Navigate to **Data Certification > Tasks > All Tasks**.
2. Click a certification task Number.
3. Enter a new name in the Assigned to field.

### Send certification task reminders

The Certification Task Escalations workflow sends automatic email reminders.

The Certification Task Escalations workflow sends automatic email reminders to the:

- Certification task owner.
- Assignment group, if the assignment group was specified on the Certification Task form.
- Manager of the certification task owner, if necessary and if a manager was specified on the User form.

The reminders are based on the Complete by field on the certification task record. If the Complete by date is changed, the reminder schedule automatically adjusts to reflect the new date.
Certification task reminders

<table>
<thead>
<tr>
<th>Time elapsed to end date</th>
<th>Email reminder is sent to</th>
<th>Escalate field on task record reads</th>
</tr>
</thead>
<tbody>
<tr>
<td>50%</td>
<td>task owner and assignment group (if specified)</td>
<td>Moderate</td>
</tr>
<tr>
<td>75%</td>
<td>task owner, assignment group, and manager of the task owner</td>
<td>High</td>
</tr>
<tr>
<td>95%</td>
<td>task owner, assignment group, and manager of the task owner</td>
<td>High</td>
</tr>
<tr>
<td>100%</td>
<td>task owner, assignment group, and manager of the task owner</td>
<td>High</td>
</tr>
</tbody>
</table>

To set reminders for different or more intervals, edit the workflow Certification Task Escalations. In addition to the email reminders sent automatically, users with the certification_admin role can send email reminders manually at any time.

Send an email reminder from the certification task form

How to manually send email reminders from the Certification Task form.

1. Navigate to Data Certification > Tasks > All Tasks.
2. Click a certification task Number.
3. Right-click the header bar and select Resend email notifications.

Send an email reminder from the certification task list

How to manually send email reminders from the Certification Task list.

1. Navigate to Data Certification > Tasks > All Tasks.
2. Select the check box to the left of a certification task Number. Multiple check boxes can be selected.
3. From the Actions on Selected Rows menu below the list, select Resend email notifications. Select multiple tasks from the list. The menu option shows how many notifications are outstanding and how many were sent, such as Resend email notifications (15 of 18).

Mark a certification task as closed incomplete

Mark a task as closed incomplete if, for example, only some of the elements can be certified. The following users can mark a task as closed incomplete:

- Users with the certification_admin role.
- User identified in the Assigned to field on the certification task record.

To mark a task as closed incomplete:

1. Navigate to Data Certification > Tasks and select All Tasks, or My Tasks.
2. Click a certification task Number.
3. In Work Notes, enter information about why the task could not be completed.
4. Click Close Incomplete.
If at least one task on a certification instance is marked Closed Incomplete, the Completed date and Percent complete fields on the certification instance record are not updated. A user with the certification_admin role can:

- Complete the incomplete task or tasks.
- Cancel the incomplete task or tasks.

When all tasks on the certification instance are Closed Complete or Cancelled:

- The system sets the Completed date field on the certification instance record to the current date and time.
- The Percent complete field on the certification instance record is set to 100 percent.

**Certification tasks cancellation**

Users with the certification_admin role can cancel a certification task in the Work in Progress or Closed Incomplete state.

When a certification task is cancelled, a notification email is sent to the task owner or assignment group assigned to the task. The task owner or assignment group manager is not notified.

**Cancel an individual task**

1. Navigate to Data Certification > Tasks > All Tasks.
2. Find a task with a State of Work in Progress.
3. Click the task Number.
4. Click Cancel.

**Cancel all tasks in an instance**

1. Navigate to Data Certification > Schedules > Instances.
2. Find an instance with a State of Work in Progress.
3. Click the instance Number.
4. Click Cancel.

All tasks in the instance with a state of Work in Progress are cancelled. The task owner or assignment group is notified.

The email template used for the notification is named certification.task.cancelled. The email templates can be edited to change the email message text, for example.

**Content Management System**

The Content Management System (CMS) is a ServiceNow application that primarily enables users to create a custom interface for the ServiceNow platform and ServiceNow applications.

The CMS application is powerful and flexible. Customers use it for a wide variety of projects, from creating entire websites to integrating with other products. The Content Management application is active by default.

This video provides an overview of the CMS application.
A CMS typically requires a systems administrator or a web developer to set up and add features. Non-technical users can use the CMS application as a tool for website maintenance. You also want to consider the timing of the addition of content management, and the maturity level of ServiceNow data. For more information, see CMS Planning.

Following are several CMS project ideas:

- Design a company-wide service catalog that offers a collection of services.
- Present a customized UI for a knowledge base.
- Create customized login pages, search pages, views of lists, tables, charts, or graphs.
- Design a complete website.
- Integrate ServiceNow with other company applications.
- Build a tailored self-service portal for end users that is in compliance with a corporate style guide.

Example CMS sites

There are two common interface approaches within the ServiceNow community:

- An image and text-based interface similar to Amazon.com
- A search-based interface similar to Google

Both approaches have been used successfully. The approach you select depends on the needs of the people using the data and how easy it is to train them. While the two design philosophies are different, both approaches share the common goal of UI simplicity.

Content Management design

Before building a website in the CMS, it is important to have a good understanding of what to build and who the audience is.

A high volume of content can heavily influence the look and feel of the site and the site hierarchy. When deciding the content, design for ease of maintenance for the people who take care of the system. This level of planning can be time-consuming, but is important.

Review website design prerequisites to help you set expectations, scope deliverables, and define reasonable time lines. Consider both the planning and execution of site design, to understand how sites are built, and to provide a working overview of the CMS.

Timing is important when considering the addition of content management. Successful deployments of the content management system usually take place after phase 1 processes (for example, Incident, Problem, Change, Catalog, and Knowledge) are in place. This is especially true if the team has limited website design experience. Waiting until phase 2 of deployment gives administrators time to work in ServiceNow and to understand how the organization uses the system and what business needs it meets.

Also consider the maturity level of data in the ServiceNow system. Depending on the ITIL processes used, content management is only useful and effective once the data within ServiceNow is established. Ensure that hierarchies, tasks, and workflows are well-defined. For example, before creating a catalog interface, confirm that the service catalog has been in place for some time, has been used, and contains data. The same is true for a knowledge management interface, particularly when high ratings or view counts define article placement on the page.
Content organization

Before you begin to build the CMS website, list all the content that you want to include and take the time to organize it.

A site created in CMS relies on two different types of content.

- CMS site information, such as site pages, images, and menus
- System information, such as knowledge base articles and catalog items

CMS content

Begin by listing all the content you want to host on the CMS pages. Examples include help pages, My Requests, My Approvals, and specific catalog items. Think about current solutions that you can implement immediately, and note ideas for future implementation phases.

Within CMS, you group pages to define the top-down menu structure. You establish a home or starting page, and other pages in the site reference the home page in the Parent Page reference field.

There are several ways to group, such as by audience or the purpose of the website. After listing the content to host, group it logically and identify a common name for each group, as shown in the following examples.

<table>
<thead>
<tr>
<th>IT environment groups</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Content built for</strong></td>
</tr>
<tr>
<td>End user</td>
</tr>
<tr>
<td>IT professional</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>General groups</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose of site</strong></td>
</tr>
<tr>
<td>Reports</td>
</tr>
<tr>
<td>Help and knowledge</td>
</tr>
</tbody>
</table>

System content

Organize the content so the interface is easy to navigate and understandable to the user. Determine the organization based on the data that you are leveraging, both in the CMS (using sites, parent pages, pages, and navigational menus) and throughout the rest of the system. For example, within the catalog you have "category," and in the knowledge base you have "category" and "subcategory." You can use these hierarchies with filtered lists for good search results.

Organizing CMS content logically is important for long-term maintenance of the site, however, the data typically comes from other ServiceNow applications. Communicate with the administrators for these applications, such as the knowledge base, service catalog, and business service portfolio. Work with them to offer the application data appropriately through the CMS pages you create. For example, the team that created the ServiceNow corporate website in CMS began by evaluating the naming conventions used in the corporate knowledge base.
Branding elements

Branding refers to the logo, name, colors, and symbols that identify an organization. It imposes consistency in design and use of terms. Your marketing department defines branding elements and can provide them to you as you plan your CMS pages. Consider how to incorporate the following branding elements.

- Logos
- Color palette
- Tag line
- Trademarked elements
- Graphics

Site design

During planning, consider providing a core set of features with a standard appearance throughout the site. The following web design elements are often used to create a consistent look.

- Page templates
- Navigation schemes
- Header
- Breadcrumbs
- Footer
- Forms

ServiceNow features

Analyze and organize the following ServiceNow features in your instance if you plan on using any of them with CMS pages.

- Account settings
- Email
- Workflow approvals
- Filters

Team member identification

Identify the team members who assist you with website design, branding, and development.

Engage team members for each listed function before you begin to build pages for the CMS website. Each function can be performed by the same or different people.

- Gather corporate style design guidelines.
- Define the written terminology and content for the site.
- Gather and define the site flow.
- Manage the CMS project as the webmaster. The CMS webmaster is responsible for executing the design and making the site work. The following skills are required:
  - Basic ServiceNow administration skills
  - HTML
  - CSS
  - Graphic design
• Web design

After you identify the project team members, establish who is responsible to complete the tasks involved in building the CMS website.

• Determine who owns each page.
• Set a page update schedule so owners do not overwrite each other.
• Formalize content management processes, including content review and page updates.

Data preparation

It is important that there is enough data in the ServiceNow instance before you begin to build the CMS website.

Ensure that the necessary data and content are available in the instance by taking the following actions.

• Review the ITIL processes that you intend to implement in the CMS. Ensure that the data in the instance is a mature representation of the applications being used, for example, service catalog, knowledge management, and incident management.
• Review the defined hierarchies, such as the categories and subcategories for the knowledge base or service catalog. You use these categories to design the entry page into the application.

Corporate style guide

When you build a CMS website, you design the look and feel based on guidelines in the corporate style guide.

A corporate style guide provides detailed information for designing any corporate interface, including corporate websites.

Corporate design team

Many organizations have a web development team that designed the corporate website. Contact this team and involve the designers early in the planning, as they provide help and give their approval to the interface you design. Without approval, there is the risk of having to redesign the entire site because it does not adhere to the organizational guidelines.

Corporate style guide

A corporate style guide takes the guesswork out of designing the CMS website. The example style guide shown is defined down to the pixel. Creating a site with the style guide makes it easy to create clean CSS and HTML. Without the style guide, building the site can take a great deal of time.

Design considerations

Some modifications to the base design for forms may be necessary. The content area of any CMS design should be no smaller than 860px, or service catalog forms are clipped. The sample style guide entry specifies the content area to be 576px, which clips service catalog forms.
Columns and topics:

1. Navigation (levels 2–4)
2. Main content
3. Info snippets
Prototypes and rapid web design

Many user interface designers use prototypes and rapid web design techniques to visualize the final product before it is developed.

Design revisions are the most time consuming and expensive phase of site design. When the team analyzes and then uses prototypes to create pages, revisions to the published pages are minimal.

Develop the prototype and print it. Review the design with the appropriate team members and annotate the prototype, and annotate what to update on each page.

Define the following elements within the prototype.

- The site map for the entire site.
- A detailed prototype of every intended page, including elements such as links, link destinations, content, page names, and page descriptions.

Content Management navigation

After you design the hierarchical structure of the site, begin planning site navigation.

Consider the following as you plan site navigation.

- Placing navigation elements on every page.
- Locating navigation elements in the same place on every page.
- Using either text or images for navigation.
- Providing visitors with an easy way to understand where they are in the site, for example, with breadcrumbs or a specific color scheme.
- Adding a site map, which is a one-page, hyperlinked, hierarchical outline of the site.
- Providing a link to the home page from every site page, as visitors often enter the site on a page other than the home page.
- Designing navigation to help visitors find information quickly with as few clicks as possible.

In the CMS, navigation menus define your site navigation. Build menus as navigational blocks to create navigation paths. The menu chosen for the task depends on the size and complexity of your site. Available menu options include the following items.

- List menus
- Two types of tab menus
- Vertical, clickable list, usually placed on the left side
- Horizontal blocks
- Vertical blocks
- Super menu (a menu of menus)

System content management

Most of the content in a CMS site is managed in different locations throughout the system.

For example, if you are building a knowledge website, the pages and blocks exist in CMS, but the knowledge articles are authored and managed in the Knowledge application. The same is true for any other type of content you plan to leverage. It is important to take time to understand the table structure of data to become acquainted with content.

Links to content are typically static, however, take time to look at the document tree and review how field values are formatted for use within the CMS. To understand the information provided below, right-click within forms in the platform and select Show XML to view the document tree for
the referenced table. To see the table values for each field, right-click the form label and choose Show - (field name) or Configure Dictionary for reference.

Look at several internet news sites for ideas on how to format dynamic list data and also the full article detail. Research blog sites, shopping sites, and any other site you find easy to use, as layout and usability design can be time-consuming. If you find a site that inspires you, emulate it in your design.

- This New York Times example has two separate list formats.
- The CNN example has several list formats on the page.
- Several different list formats are used on the ServiceNow website.

Knowledge articles - kb_knowledge table

When you right-click and select Show XML on any form within the system, the document tree for the referenced database table becomes reference-able. Review the following selected subset of the document tree so you can acquaint yourself with the content readily available to your site design.

```
<kb_knowledge>
  <active>true</active>
  <author display_value= "First Last Name" >Use this field value if author name is important</author>
  <short_description>Use this field value as the link to the full article detail</short_description>
  <description>Provide this field value as a 1-2 sentence summary of the article</description>
  <number>Unique ID can be leveraged in a number of different ways</number>
  <published>Published time stamp of the article</published>
  <rating>This field value provides a 1 to 5 star rating similar to iTunes</rating>
  <sys_updated_on>Add to supplement article published timestamp</sys_updated_on>
  <sys_view_count>8</sys_view_count>
  <topic>Useful field value in creating hierarchical breadcrumbs</topic>
  <category>Also useful in organizing articles hierarchically</category>
  <use_count>Use this similar to Facebook's "like" feedback, answer to the question was this useful</use_count>
</kb_knowledge>
```
Activate the Content Management System

The Content Management System (CMS) application and the Service Management Portal application, which is implemented within Content Management, are automatically installed on new instances. If they are not active on your instance, administrators can activate them.

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**.
**Installed with Content Management**

Several types of components are installed with the Content Management application.

Demo data is available for this feature.

**Tables installed with Content Management**

Content Management adds the following tables.

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Page</td>
<td>Provides an inventory list of pages within the system</td>
</tr>
<tr>
<td>(content_page)</td>
<td></td>
</tr>
<tr>
<td>Content Css</td>
<td>Stores internal or external CSS for the page</td>
</tr>
<tr>
<td>(content_css)</td>
<td></td>
</tr>
<tr>
<td>Content Theme</td>
<td>Made up of a collection of CSS files</td>
</tr>
<tr>
<td>(content_theme)</td>
<td></td>
</tr>
<tr>
<td>Content Link</td>
<td></td>
</tr>
<tr>
<td>(content_link)</td>
<td></td>
</tr>
<tr>
<td>Content Page Rule</td>
<td></td>
</tr>
<tr>
<td>(content_page_rule)</td>
<td></td>
</tr>
<tr>
<td>Content Block</td>
<td></td>
</tr>
<tr>
<td>(content_block)</td>
<td></td>
</tr>
<tr>
<td>Content Block Detail</td>
<td></td>
</tr>
<tr>
<td>(content_block_detail)</td>
<td></td>
</tr>
<tr>
<td>Content Site</td>
<td>Provides and inventory list of sites within the system</td>
</tr>
<tr>
<td>(content_site)</td>
<td></td>
</tr>
<tr>
<td>Content Block Static</td>
<td></td>
</tr>
<tr>
<td>(content_block_static)</td>
<td></td>
</tr>
<tr>
<td>Content Type Detail</td>
<td></td>
</tr>
<tr>
<td>(content_type_detail)</td>
<td></td>
</tr>
<tr>
<td>Content Page Meta</td>
<td></td>
</tr>
<tr>
<td>(content_page_meta)</td>
<td></td>
</tr>
<tr>
<td>Content Config</td>
<td></td>
</tr>
<tr>
<td>(content_config)</td>
<td></td>
</tr>
<tr>
<td>Content Type</td>
<td></td>
</tr>
<tr>
<td>(content_type)</td>
<td></td>
</tr>
<tr>
<td>Content ThemeCss</td>
<td></td>
</tr>
<tr>
<td>(_content_theme_css)</td>
<td></td>
</tr>
</tbody>
</table>
# Roles installed with Content Management

Content Management adds the following roles.

<table>
<thead>
<tr>
<th>Role title (name)</th>
<th>Description</th>
<th>Contains roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content administrator (content_admin)</td>
<td>Can read, write, and configure all elements of the Content Management Application</td>
<td>none</td>
</tr>
</tbody>
</table>

# Script includes installed with Content Management

Content Management adds the following script includes.

<table>
<thead>
<tr>
<th>Script include</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMSCopyAjax</td>
<td>Support for copying CMS pages</td>
</tr>
<tr>
<td>CMSEntryPage</td>
<td>Creates an entry page</td>
</tr>
<tr>
<td>ContentPageClone</td>
<td>Copy support for CMS pages</td>
</tr>
<tr>
<td>ContentSiteClone</td>
<td>Copy support for CMS sites</td>
</tr>
<tr>
<td>CMSAjax</td>
<td>CMS Ajax utilities</td>
</tr>
</tbody>
</table>

# Client Script installed with Content Management

Content Management adds the following client script.

<table>
<thead>
<tr>
<th>Client script</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Header Color Change</td>
<td>Content Block Header (content_block_header)</td>
<td>Changes the background color of the control to what the user selected</td>
</tr>
</tbody>
</table>

# Business Rules installed with Content Management

Content Management adds the following business rules.

<table>
<thead>
<tr>
<th>Business rule</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replace Stub</td>
<td>Content Block (content_block)</td>
<td>Replaces a placeholder widget with a content widget.</td>
</tr>
<tr>
<td>Unload Page</td>
<td>Page (content_page)</td>
<td>Unloads content from the page.</td>
</tr>
</tbody>
</table>
Configure Content Management sites

Planning a CMS site involves obtaining resources, communicating with others about design, and gathering content.

Role required: content_admin or admin

The following steps are a high-level overview of how to set up a site.

1. Plan and design your content.
2. Create a site.
   - The site is the container that holds all the content. To simplify your process, you can copy an existing site and edit its components. For more information on creating a site, see Create a site. For more information on copying a site, see Copy a site.
3. Add pages to the site.
   - Pages contain blocks of information for the site. For more information, see Create a content page.
4. Create content blocks to customize the layout, headers, menu navigation, lists, and static and dynamic content.
   - Content blocks are chunks of actual HTML that make up the content page. There are various content block types available to help with your customization. For more information, see Content blocks.
5. Add style to your site using themes, style sheets, and frames.
   - Neither content sites or content pages reference style sheets directly. Configure them using the Themes or Style Sheets options. For more information, see Style in Content Management.
6. Test the site.
   - After you create or modify a site, test the site to ensure that content displays properly and all links work correctly. For more information, see Test the site.

Content sites

A content site is a group of related content pages that have the same basic theme, layout, and URL suffix.

Content sites are made up of a series of basic building blocks. The Employee Self-Service site is an out-of-box sample site that is included in the CMS activation. It provides existing, working examples or each CMS component, which you can use like a template to build your own site.

<table>
<thead>
<tr>
<th>Business rule</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bump Parent if Content</td>
<td>Portal</td>
<td>Replace content in the current page.</td>
</tr>
<tr>
<td></td>
<td>(sys_portal)</td>
<td></td>
</tr>
<tr>
<td>Remove Block from Pages</td>
<td>Content Block</td>
<td>Removes a block from pages where it is placed.</td>
</tr>
<tr>
<td></td>
<td>(content_block)</td>
<td></td>
</tr>
<tr>
<td>Validate Suffix</td>
<td>Content Page</td>
<td>Validates a suffix so that a page name or a page suffix cannot match a table name.</td>
</tr>
<tr>
<td></td>
<td>(content_page)</td>
<td></td>
</tr>
</tbody>
</table>
Create a site

Configure a site by either creating a new site with CMS or by editing a copy of either the ESS Portal or the Service Management Portal.

Role required: content_admin or admin

If you are creating a catalog site in CMS, follow the steps in Manage catalog sites in Service Catalog Management.

1. Navigate to Content Management > Sites.
2. Click New.
3. Complete the form.

   Since you have not yet created pages, you cannot select the Home, Search, Login, and Gauge target pages. Add them to the site record after you create them.

Site fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for the site.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>URL suffix</td>
<td>The URL suffix that identifies the site. The URL suffix is case-sensitive, the suffix you enter impacts the CMS site URL used to launch the site. It is incorporated into the URL as follows: http://&lt;instance name&gt;.servicenow.com/url_suffix/page.do</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Do not use portal and cms in the URL suffix. They are reserved terms and return a <strong>Page not found</strong> if you use them.</td>
</tr>
<tr>
<td>Home page</td>
<td>The page to display when the user does not specify a page name in their URL: http://&lt;instance name&gt;.servicenow.com/url_suffix/</td>
</tr>
<tr>
<td>Search page</td>
<td>The page that displays search results when a user searches from any page within the site.</td>
</tr>
<tr>
<td>Login page</td>
<td>The page to use for logging in to the site. If specified, users must log in to access the pages on the site. If left blank, no login is required to access the pages within the site.</td>
</tr>
<tr>
<td>Gauge target page</td>
<td>The page that displays gauge content. When the user clicks a gauge on the new site, the gauge target page opens to show the gauge content. The gauge target page replaces the CMS page in the current tab.</td>
</tr>
<tr>
<td>Title</td>
<td>A title for the site. The title can be the same as or different from the <strong>Name</strong>.</td>
</tr>
<tr>
<td>Description</td>
<td>A full description of the site.</td>
</tr>
<tr>
<td>Default layout</td>
<td>The layout for pages to use by default. Any page in the site that has a blank <strong>Layout</strong> field uses the layout selected in this field.</td>
</tr>
<tr>
<td>Default theme</td>
<td>The theme for pages to use by default. Any page in the site that has a blank <strong>Theme</strong> field uses the theme selected in this field.</td>
</tr>
<tr>
<td>Simple catalog display</td>
<td>Selecting this option simplifies catalog pages in the site by hiding the search bar, breadcrumbs, and the results per page choice list. It also prevents you from adding attachments from record producers to your CMS site.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Use external cart</td>
<td>Option to omit the default cart when rendering catalog pages within a site that contains catalog pages. Provide a catalog cart block somewhere on the site to allow users to make catalog requests.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you use an external cart, the no cart check box on a service catalog item has no effect. The external cart appears for all items.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

The following is the site record for the ESS Portal:
Copy a site

To create a new site quickly, you can copy an existing site.

Role required: content_admin or admin

The site copy option creates a complete standalone copy of the site and all its resources. If you are copying a site to create a second site, use this option after the first site is complete, tested, and production ready. This consideration is important because the blocks, CSS, and pages are duplicated to support the new site. There are various reasons why site copying is useful, such as site versioning, branding, or creating a backup.
Images are not included when you use the Copy Site option. They are stored separately in the `sys_attachments` table.

To copy just a few pages without duplicating all the resources (CSS, blocks, menus), use the page copy option. Page copy duplicates the page but not the resources used in the page. For more information, see Copy a page.

1. Navigate to Content Management > Sites > (Site Name).
2. On the Site form, click Copy.
3. In the dialog box that opens, type a name for the new site.
   This name is a prefix for all the site elements that are duplicated. Do not use Portal or CMS in the site name.
   A progress bar shows the copy process. When the process is complete, the Site form shows information for the new site.

Content Management security

There are several methods for securing CMS sites and pages. Site security is set in the Login page field on the site record. You can control if a page is public or private through the URL.

Every content page has its own URL that users can access outside of the platform. Depending on how the Login page or roles are defined, the URL may or may not be public.

- If the content page has no defined Read role or there is no defined Login page, any internet user can navigate to the URL and view the content page.
- If there is a defined Read role, then anyone who goes to the URL is asked to log in before they can view the site.
- If there is a defined Login page on the site record, all pages in the site are private.

Content Management URLs

The format for Content Management URLs is as follows.

```
<path to the instance> + /<site suffix> + /<page suffix> + .do
```

The `<site suffix>` is defined by the URL Suffix field on the site form. The `<page suffix>` is defined by the URL Suffix field in the page form. The URL suffix is case-sensitive.

For example, the page Austere - Site Entry has a site URL Suffix of austere and a page URL Suffix of entry. The constructed URL looks like the following URL.

```
<instance name>.service-now.com/austere/entry.do
```

If the site URL Suffix field is left blank, the `<site suffix>` is cms, as shown in this example:

```
instance.service-now.com/cms/page.do
```

If the page URL Suffix is left blank, the name of the page is used as shown in this example:

```
instance.service-now.com/austere/Page Name.do
```

Special characters in the name of the page have to be escaped.

Login pages instead of login rules

You set a login page on the site record to allow users to log in or out directly through the content site.
Login rules were used in earlier versions to dictate what users saw after logging in, based on their roles or permissions. Login rules still work, but their use is deprecated.

**Configure CMS sites to use single sign-on (SSO)**

To configure CMS to use SSO, make the view_content page private.

Because public pages do not require login, and CMS sites are public by default, CMS pages do not use SSO. Use the following procedure to turn off public-facing content pages and enable SSO.

1. Navigate to Public Pages (sys_public.list).
2. For the view_content page, set **Active** to **false**.

**Content pages in CMS**

Content pages are the core of the Content Management System. A content page is a web page that displays blocks of content.

Pages are built from content blocks and organized into sites. Pages display as regular webpages that are rendered in HTML. Constructing a content page requires a basic knowledge of HTML. Content pages are formed by arranging content blocks in predefined layouts. They can be used to present login pages, search pages, or ServiceNow content.

**Create a content page**

Pages are built from content blocks and organized into sites.

Role required: content_admin or admin

1. Navigate to **Content Management > Sites**.
2. Open the site to add the page.
3. In the **Pages** related list, click **New**.
4. Complete the form.

**Page form fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for the page. Prefix each page name with the name of the site followed by a dash and the page function. For example, <strong>ESS - Catalog Detail</strong> and <strong>ESS - Search Results</strong> are page names within the <strong>ESS</strong> site.</td>
</tr>
</tbody>
</table>
| URL suffix     | The URL suffix that identifies the page. It is incorporated into the URL as follows:  

  http://instance_name.service-now.com/site/url_suffix.do |
<p>| Parent page    | The existing page that is the parent of the current page. Parent pages keep sections sortable on the site list of pages and are used to create breadcrumbs dynamically. Use CSS to define menus that give the Parent page context within the user interface. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layout</td>
<td>The layout to use for the page. Layouts define dropzones where content blocks can be added to the page. If this field is left blank, the page inherits the default layout of the site. If the site does not have a default layout, there is a single dropzone for the entire page.</td>
</tr>
<tr>
<td>Content theme</td>
<td>The theme to use for the page. Themes bundle CSS style sheets that are applied to all content within the page. If this field is left blank, the page inherits the default theme of the site. Use the default theme unless the page requires a different set of CSS style sheets from the other pages in the site.</td>
</tr>
<tr>
<td>Frame buster</td>
<td>Select the check box to remove any restrictions placed by frames that contain the page. This way you avoid frame-within-frame issues that sometimes occur with improper linking.</td>
</tr>
<tr>
<td>Content site</td>
<td>The site associated with the content page. If you created the page from the related list in the site, the value defaults. The content site provides the <code>&lt;site_suffix&gt;</code> in the page URL, as follows: http://&lt;instance_name&gt;.service-now.com/site_suffix/page_suffix.do</td>
</tr>
<tr>
<td>Read roles</td>
<td>Users with the selected roles can view the page. Click the lock icon to select roles.</td>
</tr>
<tr>
<td>Model document</td>
<td>A document ID of a record to display by default.</td>
</tr>
<tr>
<td>Page status</td>
<td>The status for the page, such as Draft or Published.</td>
</tr>
<tr>
<td>Created by</td>
<td>The user who created the page. If your role has higher privileges than your user name and you enter your user name, the field defaults to the role. For example, if you are logged in as an Admin and you type your name, which has lower privileges, this field displays Admin.</td>
</tr>
<tr>
<td>Title</td>
<td>The title for the page. The title displays on the browser tab when the page is accessed.</td>
</tr>
<tr>
<td>Description</td>
<td>Type a description of the page that displays for users when they access the page.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.
Add content to a page

After you define the page settings, set the content of the page by adding content blocks. Setting content blocks is similar to how you add content to homepages.

Role required: content_admin or admin

Note: Do not add any type of report, such as a calendar, to iFrames. For more information on adding a report directly onto a page without using iFrames, see Embedding reports in Jelly.

2. Click Add Content.
3. Select a content block from the picker.
4. Select the dropzone where the content goes.

Create content blocks by adding one of the content blocks named *New (block type) to the page.
Copy a page

Copying pages is an efficient way to avoid duplicating the same work and to create pages quickly from a guiding master template.
Role required: content_admin or admin

1. Navigate to Content Management > Sites and select the site.
2. Select the page to copy.
3. Click Copy.
4. Rename the page.

**Note:** Do not use service_catalog to rename a page. It is already a valid page in the system.

5. Edit the page fields.
6. Click Update.

**Assign a page to a site**

If you have created multiple sites, you can add pages from one site to another site.

Role required: content_admin or admin

1. Navigate to Content Management > Sites.
2. Select a site.
3. In the Pages related list, click Edit.
4. Select other pages to include in the site.
5. Click Save.
6. Update the site.

**Add a page to an application**

Homepages and content pages are not added automatically to update sets and applications. They must be manually added.

Role required: content_admin or admin

1. Navigate to Content Management > Pages.
2. Right-click a content page record.

   The page is added to the current application and to the current update set.

**Configure a private UI page for CMS links**

With single sign-on (SSO) in place, you can generate email links that take users directly to tickets and applications through the CMS interface.

Role required: content_admin or admin

You accomplish this procedure by creating a private UI page to redirect CMS links. Because the page is not public, it requires authentication and redirects to SSO appropriately.

1. Check that your CMS site is private by completing the following steps.
   a) Navigate to Content Management > Sites > (Your Site)
   b) Verify that the Login page field has a page listed.

2. Create a new UI page by completing the following steps.
   a) Navigate to System UI > UI Pages.
   b) Click New.
c) Enter a Name, for example, redirector.
d) Enter the following Adobe Jelly code into the HTML field.

```xml
<?xml version="1.0" encoding="utf-8"?>
<j:jelly trim="true" xmlns:j="jelly:core" xmlns:g="glide" xmlns:j2="null" xmlns:g2="null"><script type="script/javascript">
window.location.href="${sysparm_uri}";</script></j:jelly>
```

The CMS now supports email links with following format:

http://<path to instance>/<UI page>.do?uri=/<CMS suffix>/<record type>.do%26sys_id=<record ID>

For example:

http://<instance name>.service-now.com/redirector.do?sysparm_uri=/ess/incident.do%26sys_id=46e3e949a9fe19810069b824ba2c761a

**Note:** If you are using SAML 2.0 update 1 for SSO, use the UI page saml_redirector instead of creating a new UI page. For example, an email link to a SAML 2.0 redirector page would use the URL format: http://<instance name>.service-now.com/saml_redirector.do?sysparm_uri=/ess/incident.do%26sys_id=46e3e949a9fe19810069b824ba2c761a.

### Content Management templates

Content Management templates are content pages that are reused to provide a consistent look and feel. Templates are useful when creating CMS sites for the following reasons.

<table>
<thead>
<tr>
<th>Create new pages rapidly without risk by copying pages</th>
<th>Using a template to create new pages saves time because you do not have to keep repeating the same steps.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide a restore point for pages within the system</td>
<td>Have a working template available if something goes wrong in one of the blocks or in the theme CSS. It is often easier to start over from the template instead of trying to undo complex changes.</td>
</tr>
<tr>
<td>Provide a functional reference for editors on the site</td>
<td>Having the template as a reference ensures that pages continue to conform to the style guide.</td>
</tr>
</tbody>
</table>

### Page templates

Every page that is part of the site needs a template.

### Critical page reference fields

When you build a new site, there are four page reference fields on the site record that are critical. Understanding these pages and how they are used helps you define page templates and site defaults.

- **Home page:** landing page for the site. A home page is mandatory.
- **Search page:** page that displays search results when a user searches from any page within the site. A search page is mandatory for your site to have a Search Results block.
- **Login page:** a standalone login page, which is useful to force authentication for the entire CMS site.
• Gauge target page: page used to display the drill-through content from a gauge. When the user clicks a gauge, the gauge target page opens showing the drill-through content for that gauge.

Critical page reference fields

Detail pages

Depending on the data or tables that you plan to use, you may need detail pages. These detail pages use one of the content types in the following list.

• Knowledge detail page: displays a full knowledge article detail (mandatory for a knowledge site).
• Incident page: detail page for an incident record.
• Catalog page: detail page for all items, content items, order guides, and record producers.

Templates for creating sections

There are two page templates you can use when creating sections:

• Parent page: keeps sections within large sites organized and sortable on the site list of pages. Parent pages are also used to create breadcrumbs dynamically.
• Detail page: differs from the parent page in that the content area displays a full article or detail instead of a selection of related content. Detail pages must have a Current Document block.

These pages are mandatory if you plan on accessing system data. For example, if you plan on showing the service catalog in your CMS, you need the following items.
- A service catalog content type that references the (sc_cat_item table).
- A detail page that provides the full view of the item.

**New templates**

If the base system sample site pages are not suitable, you can create a template from scratch. Create a page and then use it as a template. For more information, see [Create a Content Page](#).

When you save a new template, include the word "template" in the page name.

**Configure a master template**

An easy way to create a master template is to copy the existing ESS sample site and customize it to suit your own needs. You can also configure a master template from scratch.

Role required: content_admin or admin

Follow these steps to create a single master page and generate all important components within the site.

1. Design a layout.
   Regardless of the interface, a site can be distilled into a few simple layouts.
2. Create a theme.
   The theme defines the structure of the layouts in CSS and the base styles, such as fonts and colors. For more information, see [Design themes](#).
3. Build the common blocks.
   Pages are composed of content blocks. Most content blocks are reused on multiple pages. For the master template, build basic blocks such as a header, side navigation, and some basic content for the main content area of the page. More detailed content can be added later, but define content for reuse on many of the site pages here. For more information, see [Content blocks](#).
4. Build a site entry page.
   Use the common content blocks you just created to design the first page that users see when they enter the site. For more information, see [Create a content page](#).
5. Build a detail page.
   Design the detail pages to determine how pages such as knowledge articles, catalog items, and search results are displayed. You can build a detail page by copying the site entry page and adding additional content blocks. For more information, see [Copy a page](#).
6. Assign the pages created to the new site.
   Create the site and apply the layout and theme to the site defaults. Then, navigate to the All Pages list and specify the master template site in the Site column for each of the master template pages. For more information, see [Create a site](#).

**Customize a copy of a page template**

One good source for templates is the base system sample site. It is easy to copy pages and restyle them into new page templates to meet different business requirements.

The Employee Self-Service portal is provided as a working example and design template in the following procedure.

1. Navigate to Content Management > Sites > Employee Self-Service.
2. Select a page.
   For example, to copy the ESS sample site homepage, select Portal.
3. Click **Copy**.
4. Rename the page.
5. Right-click in the header and select **Save**.
7. Point your cursor to the content block to change and click the edit icon that appears on the right.
   For example, change the menus, alter the layout, or add a different logo.
8. Click **Update**.
9. Use the page in other sites you created by assigning pages to a site.

### Content types

Content types provide site-specific control of how system data defined by templates is rendered.

In the site, one page displays a list of knowledge articles, and another page displays catalog items or incidents or a combination of the two. Different themes can be used for types of content and each theme can provide different user interaction. Content types define the pages that display content from a table. Each content type corresponds to a table.

Every type of document that the CMS displays has an associated content type. Changing the content type requires knowledge of Apache Jelly scripting. However, the common content types (such as service catalog or knowledge base) come in the base system. Content types can be associated with particular sites. This association allows different sites to use different detail pages for the same content type.

Content types define three features of associated documents.

- What does a link to one of these documents look like? For example, if a list of these documents is displayed on a page, how does each entry appear?
- What does a detailed view of one of these documents look like?
- What detail page is used to display the document? This decision is important and is often an area of confusion for new CMS users.

The document content type determines the page that a list of documents points to, the list itself does not determine the page. The content from a link is displayed in a detail content block on a page. The content type determines in which detail block on a page the document content is displayed.

For example, the list block **Catalog Top 5** displays the top five items in the Service Catalog table (sc_cat_item). Because the table is (sc_cat_item), the content type **sc_cat_item** controls how the **Catalog Top 5** list is displayed. Clicking any item in the list displays the Service Catalog Detail page with the item displayed on it according to the detail template script. These content types are applied:

- in search results to link to the correct page.
- in the Current Document block to display the current record.
- in links on lists and other places that link to record types.

Several content types are available by default for tables such as Catalog Item (sc_cat_item), Gauge (sys_gauge), and Page (content_page).

Content type defaults that are set for CMS can be overridden for individual sites. Use the **Content Types** related list on the site record to customize content types.

### Configure a content type

Users with the content_admin role can create a content type.
Role required: content_admin or admin

1. Navigate to **Content Management > Content Types**.
2. Click **New**.
3. Complete the Content Type form.

### Content Type form

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select the table whose content will be rendered in Content Management.</td>
</tr>
<tr>
<td>Content site</td>
<td>Select the site that will use this content type.</td>
</tr>
</tbody>
</table>
| Media type     | Enter one of the following media types to use with this content type or leave the field blank to use the UI111 interface.  
|                | • doctype: UI15 desktop interface only                                     |
|                | • m: Smartphone interface only (not for CMS use)                           |
| Media type     | • tablet: Tablet interface only (not for CMS use)                           |
| Default detail page | Select which page loads after a user clicks a link.                      |
| Gauge page     | Select which page is the drill-through target for any gauge. If you display a gauge on a CMS page, then clicking the links loads the page specified here. |
| Summary Template | Write an XML script that determines how the list is displayed in the list block, if the link is displayed in a list block. |
| Detail Template | Write an XML script that determines how to display the associated information after a user clicks the link. |

### CMS gauge support

Gauges are a graphical way to display information from an instance.

A gauge might, for example, show a bar chart breaking down all open incidents by category. Gauges are fully supported within the CMS system. This means:

1. **You can put a gauge on a CMS page**
2. **You can control what will happen when a user clicks on a cell within that gauge**

### Put a gauge on a CMS page

You have control over the gauges on a CMS page.

1. Bring up the CMS page in edit mode.
2. Click **Add Content**.
3. Select the gauge you want to add.
4. Place the gauge on the page in the desired location.
Control what happens on a click
Since a CMS system uses multiple pages you have to tell the system which page to use to display drill through content.

In the normal (non CMS) system, when you click a bar in a bar chart or a wedge on a pie chart, you drill through and your current screen is replaced with a list of records meeting the chart's criteria. For example, if you have a gauge of Incidents by Category and you click the bar labeled Hardware you drill through to a list of all incidents with a category=hardware.

Within the CMS system, there is a similar drill through mechanism at work, but you must manually specify which page to display.

There are two different models of the drill through, use an in-place target frame to receive the content, or use another page to display the content.

Using an In-Place Target
An in-place target is a named iframe on the same CMS page as the gauge. When the gauge is clicked, the drill-through content appears within that iframe rather than changing out the CMS page. The gauge (and the rest of the page other than the target) remain in place and active.

Using a Gauge Target Page
A gauge target page is a separate CMS page that is used to display the drill-through content from a gauge. When a gauge is clicked, the current CMS page is replaced with the gauge target page and the drill-through content is rendered within that second page.

- **Gauge Target Page**
  To set a site default, select Gauge Target Page, on the site configuration page. This page is used as the drill-through target for any gauges in the system that do not have a more specific gauge page specified in their content type.

- **Gauge Page**
  To set a content-type specific page, you can specify a Gauge Page, on a content type page. Any gauges for this type of content then use that page for any drill through.

  **Note:** The gauge target on a particular content type overrides the default, site level, gauge target.

- **Gauge Target block**
  A gauge target page is a normal CMS page, with one special requirement. Somewhere on that page, there must be a Gauge Target block. This market block tells the system where to output the drill through data.

View content types
The following is an example of where you might use Content Types.

This example uses the out-of-box Employee Self-Service (ESS) site as an example.
Role required: content_admin or admin
Use any out-of-box instance of a CMS site.
The Issue Status, or incident_status CMS page contains two content blocks: Common Answer and Current Issues. These content blocks both use Content Types to render results.


This block matches the Common Answers section of the Issue Status page. The Table field describes the Content Type associated with Common Answers.

4. Use the link to view existing Content Types.

5. Click the Content Type to view the XML that determines how the list and record are rendered in CMS.

The Default Detail Page field indicates a CMS page that displays a record selected from a List of Content block.

6. Click the Information icon next to the Default Detail Page, to go to that page.

7. From the Default Detail Page, under Related Links, click Edit Page.

The Detail Block contains a content type formatter. When editing or viewing the page, it is looking for a URL to be passed to determine the record to display, which is why it says "Detail record could not be located".

8. Click the pencil icon to edit and view the Detailed Content block.

The Type drop down list has "Show the page's current document" selected, which indicates that the document_id must be passed to this block from the CMS pages, then it can display the record based on the content type listed in the document_id.

9. From the Common Answers block, on the Self Service page, select a record.

The page opens with a URL similar to: https://<instance name>.service-now.com/ess/knowledge.do?sysparm_document_key=kb_knowledge,02255450d731310013ab49547e61038e

The table sysparm_document_key=kb_knowledge and sys_id 02255450d731310013ab49547e61038e determine the record. The associated content type, kb_knowledge, renders the content on the Default Detail Page, Portal - Knowledge Detail / url_suffix=knowledge.

Content blocks

A block is a defined piece of content within the system that can be reused.

A content page is constructed by arranging customized blocks of content on a page. Content blocks are an important part of a CMS site. Existing content such as reports, gauges, and record lists are automatically available as content blocks and more can be created within the CMS.

After defining content blocks, use them on any content page by adding them to drop zones. For more information, see Add content to a page.

Create content blocks after sites and pages have been designed.

Configure a content block

To configure a content block, define it in the appropriate form.

Role required: content_admin or admin

1. Perform one of the following actions to create a content block.
   - Navigate to Content Management > Blocks > (Block type) > New. The form for creating the selected block type opens.
   - Navigate to Content Management > Blocks > All and select the type of content to create from the list.
• Edit a content page and add a stub block of the desired content block type. Click the link in the stub block.

2. Complete the content block form and save it.
3. Add the content block to any content page.

View CMS block tags

A CMS block tag is used for advanced block creation and site flexibility.

Role required: content_admin or admin

It is constructed as `<g:content_block> {{Jelly_Tags|Jelly}}` and can be used in either of the following ways.

• Blocks: to display a block inside a block.
• Layouts: to display a block inside a layout.

The tag appears in the format, `<g:content_block type="<type>" id="<sys_id>"/>`.

An example of the block tag is included in the ESS Portal sample site.

1. Navigate to Content Management > Design > Frames.
2. Click cms_admin_home_frame.
3. View the code.

```html
<style>
DIV.cms_administration_home {
    background: url(gray_${current_page.getURLSuffix()}.pngx) no-repeat right top;
}
</style>

<div class="cms_administration_home">
    ${body}
    <br/>
<!-- Would you like to pivot off of parent page instead?  try this snippet -->
    <j:if test="${current_page.getParentPage().getURLSuffix()=='administration'}">
        <g:content_block type="content_block_menu" id="7afc342def002000914304167b2256ac"/>
    </j:if>
    The defaults use the page URL suffix to define sub menus
    -->
    <j:if test="${current_page.getURLSuffix()=='administration'}">
        <g:content_block type="content_block_menu" id="7afc342def002000914304167b2256ac"/>
    </j:if>
    <j:if test="${current_page.getURLSuffix()=='community_inspired'}">
        <g:requires name="ess.portal.globals.jsdbx" />
        <g:content_block type="content_block_menu" id="ccd4b8c7efb70000914304167b22566e"/>
    </j:if>
    <br/>
</div>
```
4. To see what the page looks like, navigate to the ESS Portal administration page. For example, http://instance name.service-now.com/ess/administration.do.

Types of content blocks

Content blocks, which make up content pages, are reusable pieces of content defined within the system.

Each content block can be used for a different type of content.

Configure a header block

A header block is a visual element placed at the top of pages. It provides a place for branding and other important site-wide functionality.

Role required: content_admin or admin

Some of the options that are available in headers include, global search, text size toggle, menus for navigational purposes, and the user name with logout link.

1. Navigate to Content Management > Blocks > Headers.
2. Click New.
3. Complete the form.

Header form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a unique name for the header block.</td>
</tr>
<tr>
<td>Background</td>
<td>Select a background for the header logo and menus.</td>
</tr>
<tr>
<td></td>
<td>- None - No background is rendered.</td>
</tr>
<tr>
<td></td>
<td>- Gradient/Image - Specify an image or gradient image to serve as the background.</td>
</tr>
<tr>
<td></td>
<td>- Colored Bars - Specify colors for three different sections of the header, top, middle, and bottom.</td>
</tr>
<tr>
<td>Image</td>
<td>If Background is Gradient/Image, upload an image for the header block background. For gradients, upload a gradient image.</td>
</tr>
<tr>
<td>Top bar color</td>
<td>If Background is Colored Bars, enter a CSS color or color name to use as the background for the top menu.</td>
</tr>
<tr>
<td>Middle bar color</td>
<td>If Background is Colored Bars, enter a CSS color or color name to use as the background for the logo and text.</td>
</tr>
<tr>
<td>Bottom bar color</td>
<td>If Background is Colored Bars, enter a CSS color or color name to use as the background for the bottom menu.</td>
</tr>
<tr>
<td>Logo</td>
<td>Select a logo image. The image is also a link to the main page.</td>
</tr>
<tr>
<td>Active</td>
<td>Select this check box to make the block available for use.</td>
</tr>
<tr>
<td>Text</td>
<td>Type the text to display beside the logo.</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
Conditional | Select the check box and type any scripted conditions to apply in the **Condition** script field that appears.
Category | Select a category to provide organization for the header block. The category also determines the detail page in which header block links open. Detail pages often display information in different ways.
Top Menu | Select a navigational menu block to use as a menu above the logo.
Bottom Menu | Select a navigational menu block to use as a menu below the logo.
Height | Specify the height for the header.
Search | Select this check box to add a search element in the header.
Font sizer | Select this check box to include text sizing controls in the header.
Login | Select this check box to include a login link in the header. If the user is logged in, this element displays the user name and a logout link. If you specify a login page on the site record, it is important to include a login link so users can enter their username and password.
Chat Queue | Select the chat queue that users access by clicking the **Help Desk Chat** button in the header. Clear the field to remove the button. This field appears only if the Chat plugin is active.

**Create a navigation menu block**

Navigation menu blocks enable you to create a menu of links to different content pages.

Role required: **content_admin** or **admin**

The following three objects define navigation menus.

- **Menu block**: The menu block defines the entire menu block and how it displays.
- **Menu section**: The menu sections define groups of links displayed within the block.
- **Menu item**: The menu items define the links within each menu section.

1. Navigate to **Content Management > Navigation Menus**.
2. Click **New**.

A gallery of available navigation menu blocks displays.
CMS menu options

3. Select the desired menu block style.
4. Complete the Navigation Menu form to define the block.

Navigation Menu form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique name for the block.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the type of navigation menu, which determines how the links are displayed.</td>
</tr>
<tr>
<td>Frame</td>
<td>Select a border style for the navigation menu block.</td>
</tr>
<tr>
<td>Conditional</td>
<td>Select this check box to enable the use of scripted conditions. If selected, the <strong>Condition</strong> and <strong>Logged On</strong> fields appear.</td>
</tr>
<tr>
<td>Logged on</td>
<td>Select this check box to display the navigation menu block only if the user is logged on. This field appears only if <strong>Conditional</strong> is selected.</td>
</tr>
</tbody>
</table>
## Configure menu sections

Menu sections define groups of links displayed within the navigation menu block.

**Role required:** content_admin or admin

1. Navigate to **Content Management > Blocks > Navigation Menus** and select a block.
2. In the Menu Sections related list, click **New**.
3. Complete the Menu Section form.

### Menu Section form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique name for the menu section.</td>
</tr>
<tr>
<td>Content block menu</td>
<td>Select the navigation menu on which this menu section appears.</td>
</tr>
<tr>
<td>Redirect to</td>
<td>Select what appears when a user clicks the menu section name and icon.</td>
</tr>
<tr>
<td>URL</td>
<td>Click the lock icon to open the edit field, then enter the URL to display when a user clicks the menu section title and icon. This field is available only if <strong>Redirect to</strong> is set to <strong>The specified URL</strong>.</td>
</tr>
<tr>
<td>Detail page</td>
<td>Select the content page to open when a user clicks the menu section title or icon. This field is available only if <strong>Redirect To</strong> is set to a content page.</td>
</tr>
<tr>
<td>Left image DB</td>
<td>Select the image database where your site images are stored.</td>
</tr>
<tr>
<td>Right image DB</td>
<td>Select the image database where your site images are stored.</td>
</tr>
<tr>
<td>Left image</td>
<td>Select icons to appear on the left and on the right of the name.</td>
</tr>
<tr>
<td>Right image</td>
<td>Select icons to appear on the left and on the right of the name.</td>
</tr>
<tr>
<td>Second level text</td>
<td>Enter a description to appear beside the menu section title.</td>
</tr>
<tr>
<td>Active</td>
<td>Select this check box to make the menu section available for use.</td>
</tr>
<tr>
<td>Order</td>
<td>Enter a number to indicate where this section appears on the menu relative to other menu sections.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Logged on</td>
<td>Select this check box to display the menu section only if the user is logged on.</td>
</tr>
<tr>
<td>Roles</td>
<td>Click the lock to open a list, then select the roles that can access this menu section if you restrict access by role.</td>
</tr>
<tr>
<td>Category</td>
<td>Select the category in which the menu section belongs.</td>
</tr>
<tr>
<td>Open In</td>
<td>Select the behavior of clicked links.</td>
</tr>
<tr>
<td>iFrame</td>
<td>Enter the name of the iFrame where the link opens when a user clicks the menu section title and icon. Make sure that there is an iFrame on the page where the link opens. This field is available only if Open In is set to Named iFrame.</td>
</tr>
<tr>
<td>Header</td>
<td>Enter header information for the menu section.</td>
</tr>
<tr>
<td>Footer</td>
<td>Enter footer information for the menu section.</td>
</tr>
</tbody>
</table>

4. **Click Submit.**

Configure menu items

Menu items are the links that appear within each menu section.

Role required: content_admin or admin

Not all navigation menu sections require menu items. Use menu items to link users to other pages or additional information. These steps use the ESS sample portal site as an example.

1. Navigate to **Content Management > Blocks > Navigation Menus** and select a navigation menu.
   - For example, select the **Documentation Menu**.
2. From the **Menu Sections** related list, select a menu section.
   - For example, select **Getting Started**.
3. From the **Menu Items** related list, click **New**.
4. Complete the form.

**Menu Item form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a unique name for the menu item.</td>
</tr>
<tr>
<td>Menu section</td>
<td>Select the menu section in which this item appears.</td>
</tr>
<tr>
<td>Redirect to</td>
<td>Select what appears when the menu item name and icon are clicked.</td>
</tr>
<tr>
<td>URL</td>
<td>Click the lock icon to open the edit field, then enter the URL to open when the menu item title and icon are clicked. This field is available only if Redirect to is set to The specified URL.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Detail page</td>
<td>Select the content page to open when the name or icon is clicked. This field is available only if Redirect To is set to A content page.</td>
</tr>
<tr>
<td>Image</td>
<td>Select an icon to appear with the name.</td>
</tr>
<tr>
<td>Active</td>
<td>Select this check box to make the menu item available for use.</td>
</tr>
<tr>
<td>Order</td>
<td>Enter a number to indicate where this item appears on the menu relative to other menu items.</td>
</tr>
<tr>
<td>Logged on</td>
<td>Select this check box to display the menu item only if the user is logged on.</td>
</tr>
<tr>
<td>Roles</td>
<td>Click the lock to open a list, then select the roles that can access this menu item to restrict access by role.</td>
</tr>
<tr>
<td>Category</td>
<td>Select the category in which the menu item belongs.</td>
</tr>
<tr>
<td>Open in</td>
<td>Select the behavior of clicked links.</td>
</tr>
<tr>
<td>iframe</td>
<td>Type the name of the iframe where the link opens when a user clicks the menu item name and icon. Make sure that there is an iframe on the page. This field is available only if Open In is set to Named IFrame.</td>
</tr>
</tbody>
</table>

5. Click Submit.

Menu types

By changing the Type field on the navigation menu block, you can format the same menu in different ways.

Menu types

<table>
<thead>
<tr>
<th>Type</th>
<th>Image</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Super Menu for Headers</td>
<td><img src="image" alt="Super Menu" /></td>
<td>The super menu is a hybrid between the drop-down menu and the tabbed system. The user can use a super menu to create a menu from any number of menus.</td>
</tr>
<tr>
<td>Type</td>
<td>Image</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Drop-Down Menu for Headers</td>
<td><img src="image1.png" alt="Image" /></td>
<td>The drop-down menu renders the menu sections as drop-down list. Use the mouse to point to the menu name and view the menu items.</td>
</tr>
<tr>
<td>Tab Menu for Headers</td>
<td><img src="image2.png" alt="Image" /></td>
<td>The tab menu renders the menu sections as tabs. Use the mouse to click the tab and view the menu items.</td>
</tr>
<tr>
<td>Horizontal Blocks</td>
<td><img src="image3.png" alt="Image" /></td>
<td>The horizontal blocks menu renders the menu sections as block headings with menu items as links within the blocks. The blocks are arranged horizontally.</td>
</tr>
<tr>
<td>Type</td>
<td>Image</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Tab Content Block</td>
<td><img src="image1.png" alt="Image" /></td>
<td>The tab content block (horizontal) menu renders the menu sections as tabs with menu items as links within the block.</td>
</tr>
<tr>
<td>Vertical List</td>
<td><img src="image2.png" alt="Image" /></td>
<td>The vertical list menu renders the menu sections as headings with menu items as links below them.</td>
</tr>
<tr>
<td>Vertical Blocks</td>
<td><img src="image3.png" alt="Image" /></td>
<td>The vertical blocks menu renders the menu sections as block headings with menu items as links within the block. The blocks are arranged vertically.</td>
</tr>
</tbody>
</table>

**Menu style customization**

You can customize menu styles in the style sheets your site uses.

Navigate to **Content Management > Design > Style Sheets** to customize style sheets.
Supplementary page navigation menu example code

In the following example, look at the CSS class selectors and rules. Also, review how the block containers (div.cms_menu_section_blocks) are defined based on the outer container (TD.layout_content_submenu_column). The outer container is actually a part of the site layout.

This concept is clearer if you compare the styles to the styles used in the super menu further down in the example. This example shows that there is no need to make a completely new menu system. You can use CSS to change the look and feel of existing menus.

```html
SUB MENU VARIATIONS FOR HORIZONTAL MENUS - Section Blocks Menu
(cms_menu_section_blocks UI Macro)

TD.layout_content_submenu_column DIV.cms_menu_section_blocks {
    width: 156px;
    height: auto;
    float: left;
    position: relative;
    border-style: solid;
    margin: 0px 0px 0px 0px;
    border: 0px solid #e0e0e0;
    padding: 0px;
    background: none;
    padding: 24px 12px 0px 12px;
}

TD.layout_content_submenu_column DIV.sub_menu_section {
    width: 156px;
    height: 20px;
    float: left;
    border-style: solid;
    border: 0px solid #e0e0e0;
    padding: 0px;
    background: none;
    padding: 0px 12px 0px 12px;
}

SPAN.cms_sub_menu_list_link, TD.submenu_cell A {
    color: #FFF;
}

TD.layout_content_submenu_column IMG.menu_bullet{
    display: none;
}

TD.cms_menu_section_blocks_title h2, TD.cms_menu_section_blocks_title h2 a, TD.cms_menu_tab_blocks_text h2 {
    margin:0;
    padding: 0px;
    font-size: 11px;
    text-transform: uppercase;
    color: #42C4DD;
    font-weight: normal;
    white-space: nowrap;
}

TD.layout_content_submenu_column a.cms_menu_block_item {
    margin:0;
    padding: 0px;
    font-size:11px;
}
### Super menu sections example code

The following menu is a simple float grid. The defaults are written first. Then, below the “SUPER MENU VARIATIONS...” comment, the defaults are overwritten by adding a containing div with a unique class. In the code that renders the header for the base system, the bottom menu resides in a table cell with the class of `cms_header_bottom_menu` (refer to the `TD.cms_header_bottom_menu` CSS selector).

```html
TD.layout_content_submenu_column DIV.cms_menu_section_blocks {
  width: 156px;
  height: auto;
  float: left;
  position: relative;
  border-style: solid;
  margin: 0px 0px 0px 0px;
  border: 0px solid #e0e0e0;
  padding: 0px;
  background: none;
  padding: 24px 12px 0px 12px;
}

TD.layout_content_submenu_column DIV.sub_menu_section {
  width: 156px;
  height: 20px;
  float: left;
  border-style: solid;
  border: 0px solid #e0e0e0;
  padding: 0px;
  background: none;
  padding: 0px 12px 0px 12px;
}

SPAN.cms_sub_menu_list_link, TD.submenu_cell A {
  color: #FFF;
}

TD.layout_content_submenu_column IMG.menu_bullet{
  display: none;
}

TD.cms_menu_section_blocks_title h2, TD.cms_menu_section_blocks_title h2 a, TD.cms_menu_tab_blocks_text h2 {
  margin:0;
  padding: 0px;
  font-size: 11px;
  text-transform: uppercase;
  color: #42C4DD;
}
```
4.2 2. Super Menu Sections Example Code

This menu is essentially a simple float grid. The defaults are written first. Then, below the "SUPER MENU VARIATIONS..." comment, the defaults are overwritten by adding a containing div with a unique class. In the code that renders the header for the base system, the bottom menu resides in a table cell with the class of "cms_header_bottom_menu" (note the TD.cms_header_bottom_menu CSS selector).

/ *******************************************************************************************
| Section Blocks Menu (cms_menu_section_blocks UI Macro)
| *******************************************************************************************/

div.cms_menu_section_blocks {
    width: 260px;
    height: 260px;
    float: left;
    border-style: solid;
    margin: 0px 0px 12px 12px;
    border: 1px solid #e0e0e0;
    padding: 10px;
    background: url(blue/portal_horizontal_bkg.pngx) repeat-x center bottom;
}

p.cms_menu_separator {
    border-top:1px dotted #ccc;
    margin-top: 6px;
    margin-bottom: 6px;
}

td.cms_menu_section_blocks_title h2, td.cms_menu_section_blocks_title h2 a, td.cms_menu_tab_blocks_text h2 {
    margin:0;
    padding: 0px;
    font-size: larger;
    font-weight: normal;
    color:#444;
}

a.cms_menu_block_item {
    margin:0;
    padding: 0px;
    color:#999;
    font-size: inherit;
}
SUPER MENU VARIATIONS FOR HORIZONTAL MENUS - Section Blocks Menu
(cms_menu_section_blocks UI Macro)

TD.cms_header_bottom_menu .cms_menu_super_menu_bar { /*style the super menu drop down bar */
    z-index: 199;
    float: left;
    background: none;
    margin-left: 44px;
}

TD.cms_header_bottom_menu div.cms_menu_section_blocks {
    width: 200px;
    float: left;
    border: 0px;
    margin: 0px 0px 12px 0px;
    padding: 0px;
    background: none;
}

TD.cms_header_bottom_menu p.cms_menu_separator {
    border-top:0px dotted #ccc;
    margin-top: 0px;
    margin-bottom: 0px;
}

TD.cms_header_bottom_menu .cms_menu_super_menu_bar_item { /*style an item on the super menu drop down bar*/
    z-index: 200;
    float: left;
    padding-left: 12px;
    padding-right: 12px;
    padding-bottom: 8px;
    padding-top: 4px;
    cursor: pointer;
    cursor: hand;
    font-weight: bold;
    color: #000;
    border-left: 1px solid #FFF;
    border-top: 1px solid #FFF;
}

TD.cms_header_bottom_menu .cms_menu_super_menu_bar_item_selected { /*style a selected item on the super menu drop down bar*/
    z-index: 200;
    float: left;
    padding-left: 12px;
    padding-right: 12px;
    padding-bottom: 8px;
    padding-top: 4px;
    cursor: pointer;
    cursor: hand;
    background: #fff url(super_menu_bkg.gifx) no-repeat left top;
    font-weight: bold;
    border-right: 0px solid #CCC;
    border-bottom: 0px solid #CCC;
    border-left: 1px solid #DDD;
    border-top: 1px solid #EEE;
}
Example menu items and content links

The method for choosing a link target (current window, iFrame, or new window) and referencing the item linked (page, attachment, or URL) are similar. Review examples of how to link within these elements.

- A content page reference helps you select the desired page. For example, the value `home.do` links to the site homepage.
- An attachment reference allows you to reference a single file attached to the menu item or section record. If there is more than one attachment, only the first attachment is referenced. The link is then generated automatically and displays a Browser File Save prompt.
- The specified URL reference allows you to link to a full URL string in your instance or from another system. For example, `com.glideapp.servicecatalog_cat_item_view.do?sysparm_id=66c313e7c0a8016b008ebela8e3d97f5&sysparm_nameofstack=b654d15bef921000914304` links to the Ask a Question record producer. Use this reference to link to a page in an existing intranet system.

Menu items can be seen as featured links from each section. There are many choices in URL definitions and link options. Links within the ESS Portal open content pages within the site. In turn, each page has an iFrame or set of blocks that houses the corresponding data. This method is useful for rapid prototyping, but consider where to create dynamic detail pages and use the available linking options.
Menu Item

Menu items are similar to content links except they are called by the list block, not as part of a navigation menu block. Menu items and content links function the same as far as how they are defined and the options available for linking to items. Content links are meant to be called through a list block that calls the Content Link (content_link) table. Content links do not have the *Logged in* field or the *Roles* option used to control the UI experience for various roles.
View menu and list examples

Menu sections define groups of links and how the links behave.

Role required: content_admin or admin

For example, link behavior determines which page opens when the link is clicked and how it opens, such as in a new page or a new frame. Use the following procedure to view a sample menu section.

1. Navigate to **Content Management > Blocks > Navigation Menus**.
2. Click **Portal - Block Menu**.
3. In **Menu Sections** related list, click **Order Things**.
4. Click the reference icon next to **Detail Page** to open the page.
5. In **Related Links**, click **Edit Page**.

By default, the link goes to the Order Things page with the Portal - Order Splash Menu (Vertical Block Menu) in the page content area.

In most default CMS menus, the menu section has the menu title with secondary text, a separation line, and the links you define as menu items. Although the design is versatile and flows well between pages, there could be questions about linking and scalability to large catalogs. This practice may only be useful for a small catalog with limited items.

6. To view an example of dynamic content, follow these steps to look at the request catalog list/grid view on the ESS Portal.
   a) Add `/ess/manage.do` to your instance URL.
      For example, `https://<instance name>.service-now.com/ess/manage.do`.
   b) In the **Code Example Demos** section, click **Request Catalog List / Grid View**.
   c) Browse the catalog items.
Configure dynamic blocks
Use dynamic blocks to use scripting or to pull information from the system. Dynamic blocks are where most of your content resides.

Role required: content_admin or admin

A good use of dynamic blocks is job postings. Store the postings in knowledge articles and display the postings with a dynamic block.

Several dynamic blocks are predefined, including the following items.

- **New Content**: Each of the new content blocks allows for creating blocks while editing content pages.
- **Clean Login**: The default login page requesting user name and password, which includes a “Remember Me” check box. After the user logs in, this block triggers login rules.
- **Login**: An area that allows a logged out user to log in and a logged in user to log out. This block is especially useful on publicly available content pages.
- **Search**: The global text search field. Currently, global text search is the only form of search that can be included in a content page.
- **Search Results**: An area for displaying global text search results.

For information about Apache Jelly, see [Jelly tags](#).

1. Navigate to **Content Management > Dynamic**.
2. Click **New**.
3. Complete the Dynamic Content form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a unique name for the dynamic content block.</td>
</tr>
<tr>
<td>Category</td>
<td>Select a category to provide organization for the dynamic block. The category also determines the detail page in which dynamic block links open.</td>
</tr>
<tr>
<td>Frame</td>
<td>Select a border styling for the dynamic block. For more information, see Format a frame.</td>
</tr>
<tr>
<td>Active</td>
<td>Select this check box to make the block available for use.</td>
</tr>
<tr>
<td>Conditional</td>
<td>Enter any scripted conditions to be applied. If selected, adds a Condition script field to the form.</td>
</tr>
<tr>
<td>Two phase</td>
<td>Select this check box to allow two phase <a href="#">Jelly tags</a>.</td>
</tr>
<tr>
<td>Dynamic content</td>
<td>Enter the XML script field that determines the behavior of the dynamic block.</td>
</tr>
</tbody>
</table>

Catalog cart block
The catalog cart block is a dynamic block provided in the base system.

This block provides the same cart that is available within the service catalog. If the site definition has the **Use external cart** option selected, include this block in the site so users can interact with their catalog cart.
Catalog cart block is available when the `glide.sc.use_cart_layouts` property is set to false.

**Customize the list block**

List blocks are content blocks that dynamically generate a list of links to records within the instance. When a user clicks a link in a list block, the associated information is displayed in a detail page determined by its content type.

Role required: content_admin or admin

Make the list using a simple query on any table or by scripting a more advanced query. Lists are powerful and flexible. Here are some places that allow you to have complete control over the list display.

### List control

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frames</td>
<td>Frames provide a method to create decorative containers for content blocks and other elements within the site. When frames are used with the <strong>Type</strong> field, the designer has complete control over list placement.</td>
</tr>
<tr>
<td>List Type</td>
<td>The List Definitions module defines the type of lists available for content pages. On the List Block form, select a list definition in the <strong>Type</strong> field.</td>
</tr>
<tr>
<td>List Filtering</td>
<td>Provides every field in the referenced table for more granular results.</td>
</tr>
<tr>
<td>Max Entries</td>
<td>Limits the results from a table to fit the design of the block.</td>
</tr>
<tr>
<td>Order and Order Direction</td>
<td>Allows sorting by any field in the referenced table, in either ascending or descending order.</td>
</tr>
</tbody>
</table>

You can also use list blocks to create a list of links to information outside your instance. Create the external links as records on the Content Link (content_link) table, and then follow the steps in this procedure.

1. **Navigate to Content Management > Lists.**
2. **Click New.**
3. **Complete form.**

### List Block fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique name for the list content block. It is used to identify the record in the instance and is not displayed on the content page. Use the <strong>Title</strong> field for that purpose.</td>
</tr>
<tr>
<td>Category</td>
<td>Select a category to provide organization for the list content block.</td>
</tr>
<tr>
<td>Type</td>
<td>Select a list definition UI macro to format the list of links. For more information, see <a href="#">Configure list definitions</a>.</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>
<tbody>
<tr>
<td>Frame</td>
<td>Select a border style for the list block. For more information, see <em>Create a frame UI macro</em>.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Select this check box to enable generating a list from a script, rather than from a simple filtered query.</td>
</tr>
<tr>
<td>Query</td>
<td>Filters the results using a condition builder.</td>
</tr>
<tr>
<td>Active</td>
<td>Select this check box to make the block available for use.</td>
</tr>
<tr>
<td>Title</td>
<td>Enter the name to display at the top of the list block when it appears in a content page.</td>
</tr>
<tr>
<td>Maximum entries</td>
<td>Set the maximum number of entries to display in this list block.</td>
</tr>
<tr>
<td>Table</td>
<td>Select a table to query for the list items. The table determines which detail page displays when a user clicks a link in the list block. For more information, see <em>Configure a content type</em>.</td>
</tr>
</tbody>
</table>

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

| Conditional | Select this check box to enable the use of scripted conditions. If selected, a **Condition** script field appears. Other fields that appear include the **Logged On** and **Omit if empty** check boxes. |

4. Click **Submit**.

Configure list definitions
List definitions, similar to content management frames, are decorative containers that control the look and feel of lists.

Role required: content_admin or admin

Specifically, list definitions are UI macros that use Adobe Jelly script to define how a list is rendered inside a list block. Site design often requires multiple list styles within the layout. Lists are often the primary form of navigation within a site, so it is important to have control over their formatting.

Configuring list definitions requires a knowledge of Adobe Jelly.

1. Navigate to **Content Management > Configuration > List Definitions > ..**
2. Click **New**.
3. Complete the List Definition form.

Configure a static HTML block
Use static blocks for text that does not change. For example, use a static block for a site footer with only the company or organization name. A static HTML block allows any HTML code to be run within a page.

Role required: content_admin or admin
Anyone who edits their own HTML, Jelly, or Javascript may find the HTML editor in the static block limited. The HTML editor can also add tags or formats that advanced coders find unnecessary. For more advanced options, use dynamic blocks.

1. Navigate to **Content Management > Blocks > Static HTML**.
2. Click **New**.
3. Complete the Static Content form.

**Static content form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Input value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a unique name for the static HTML content block.</td>
</tr>
<tr>
<td>Category</td>
<td>Select a category to provide organization for the static HTML block. The category also determines the detail page in which static HTML block links open. Detail pages often display information in different ways.</td>
</tr>
<tr>
<td>Frame</td>
<td>Select a border styling for the static HTML block. For more information, see <a href="#">Format a frame</a>.</td>
</tr>
<tr>
<td>Active</td>
<td>Select this check box to make the block available for use.</td>
</tr>
<tr>
<td>Conditional</td>
<td>Enter any scripted conditions to be applied. If selected, adds a <strong>Condition</strong> script field and <strong>Logged on</strong> check box to the form.</td>
</tr>
<tr>
<td>Static Content</td>
<td>Enter <strong>HTML code</strong> that determines the behavior of the static HTML block.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

Format an image as a static HTML block

An easy way to add an image to a CMS page is to use a static HTML block. After the block is created, you can reuse it throughout the site.

Role required: content_admin or admin

1. Navigate to **Content Management > Design > Images**.
2. Click **New**.
3. Select a **Category** to help organize the images.
4. Type the file name of the image, including the extension (such as `.png`).
5. Upload the file by selecting **Click to add** and browsing for the image.
6. Click **OK**.
7. Click **Update**.
8. Navigate to **Content Management > Blocks > Static HTML** and click **New**.
9. Paste the following code into the HTML block, substituting the image name as uploaded in the previous step.

   The "x" at the end of the filename is required for image caching.

   ```html
   <img src="<image_name>.gifx"/>
   ```

Now the image is a static HTML block and you can add it to any content page. Use standard HTML code to alter the image in the content block.
Configure Flash movie blocks
Use a Flash movie block to embed any Flash movie (.swf file) as an attachment or by referencing a URL in a content page.

Role required: content_admin or admin

To add streaming video or Flash video (.flv), for example, to a knowledge article, see Embed videos in HTML fields.

1. Navigate to **Content Management > Specialty Content > Flash Movies**.
2. Click **New**.
3. Complete the Flash Movie form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Input value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a unique name for the Flash movie block.</td>
</tr>
<tr>
<td>Source</td>
<td>Specify where the Flash movie is found.</td>
</tr>
<tr>
<td></td>
<td>· <strong>Attachment</strong>: If this choice is selected, upload the Flash movie to this record.</td>
</tr>
<tr>
<td></td>
<td>· <strong>Link to External Object</strong>: If this choice is selected, a URL field appears. Specify the Flash movie URL and ensure that the Flash movie is publicly accessible.</td>
</tr>
<tr>
<td>Height</td>
<td>Enter the height of the Flash movie in pixels.</td>
</tr>
<tr>
<td>Width</td>
<td>Enter the width of the Flash movie in pixels.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

Configure content links
Content links are the predecessors to navigation menus. You can use content links to create navigational links to information outside of your instance.

Role required: content_admin or admin

After the content link is configured, it must be defined in a list block. List blocks use content links to reference information outside of your CMS.

1. Navigate to **Content Management > Specialty Content > Content Links**.
2. Click **New**.
3. Complete the Content Link form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a unique name for the content link</td>
</tr>
<tr>
<td>Redirect to</td>
<td>Select the location of the external link</td>
</tr>
<tr>
<td>Category</td>
<td>Select a category to provide organization for the list content block.</td>
</tr>
<tr>
<td>URL</td>
<td>Click the lock icon to open the edit field, then enter the site URL to open when the link is clicked. This field is available only if Redirect to is set to The specified URL.</td>
</tr>
</tbody>
</table>
4. Click Submit.
5. From Content Management > Blocks > Lists, create a list block that references the content links by selecting Content Link in the table field.
6. Create a query to determine which external links display on the page. For example, the query Category is Search displays any external links that have a category defined as Search.
7. Click Update.

**Configure iFrames**

An iFrame embeds a URL on a page within a frame. It can embed external pages or render ServiceNow content.

Role required: content_admin or admin

Configure an iFrame with forms you create in the instance and link to the page in which the iFrame resides.

**Note:** Do not add any type of report, such as a calendar, to iFrames. For more information on adding a report directly onto a page without using iFrames, see Embedding reports in Jelly.

**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.

1. Navigate to Content Management > Specialty Content > iFrames.
2. Click New.
3. Complete the iFrame form fields.

**iFrame form fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Input value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a unique name for the iFrame block.</td>
</tr>
<tr>
<td>Frame name</td>
<td>Type a name for the frame on the page. When you use iFrames to present ServiceNow content such as forms or lists, the frame name must be gsft_main. This name allows links within the iFrame to open within the iFrame.</td>
</tr>
</tbody>
</table>
**Field** | **Input value**
---|---
URL | Enter the URL to display in the iFrame. If you use the iFrame to display ServiceNow content, start with the page name and do not include the base instance part of the URL. For example, to show the list of requested items, the URL is:

```
sc_req_item_list.do
```

Queries can be applied to the URL. For instance, to display a list of open requested items, the URL is:

```
sc_req_item_list.do?sysparm_query=active=true
```

For more information, see [URL schema](#).

Sizing | Select an option for iFrame block size.

**Note:** The Expand to fit content choice only works with ServiceNow content. If Fixed Size is selected, height and width fields are displayed for you to enter the size in pixels.

---

**Integrate Live Feed with CMS**

You can provide access to Live Feed from pages built in the Content Management System (CMS). For example, allow an end user to access your company feed via the ESS portal.

The ESS Portal template includes the **Portal - Live page** and **Live Feed** dynamic block (requires the Live Feed plugin). To provide access to Live Feed from CMS pages, add the **Live Feed dynamic block** to a CMS page or include the **Portal - Live page** in a site.

1. Navigate to **Content Management > Specialty Content > iFrames**.
2. Click **New**.
3. Complete the iFrame block form with the following values.

**iFrame values**

<table>
<thead>
<tr>
<th>Field</th>
<th>Input value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a unique name: Live Frame</td>
</tr>
<tr>
<td>Frame name</td>
<td>Type a frame name: live_frame</td>
</tr>
</tbody>
</table>
4. Click Submit.
5. Complete the steps in Add the block to a page.

### iFrame methods

The following examples show how system records are pulled into an iFrame that is placed on a content page.

For system lists or forms, use the frame name `gsft_main` so that links work properly.

- **Order Hardware** is an example of linking to a catalog category.
  - URL: `com.glideapp.servicecatalog_category_view.do?sysparm_parent=d258b953c611227a0146101fb1be7c31&sysparm_view=`
  - Frame name: `gsft_main`

- **My Approvals List** is an example of linking to a list with a view filter and a JavaScript that reference the authenticated user.
  - URL: `sysapproval_approver_list.do?sysparm_query=approver=javascript:getMyApprovals()&sysparm_view=ess`
  - Frame name: `gsft_main`

- **Service Catalog Home Page (system)** references the system catalog page within the Service Catalog application. If you are satisfied with the way the catalog looks, this method is an easy way to bring the page into a CMS design.
  - URL: `catalog_home.do?sysparm_view=catalog_default`
  - Frame name: `gsft_main`

- **Problem Management Overview** references a homepage. `../` makes the URL string relative to system homepages. Without it, the URL string resolves to the default CMS homepage reference in the site.
  - URL: `../home.do?sysparm_view=problem_overview`
  - Frame name: `gsft_main`

### Configure a detailed content block

A detailed content block displays the content of an existing document, such as an incident, knowledge article, or service management request. The document type determines the page that a list of documents points to.

Role required: content_admin or admin

The block works with content types in the Default detail page field. For more information, see Configure a content type.
If you plan to use a script to find a document, configure the form to add the Script field if it is not displayed.

1. Navigate to **Content Management > Configuration > Page Detail Settings**.
2. Click **New**.
3. Complete the Detailed Content form.

### Detailed Content form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a unique name for the Detailed Content block.</td>
</tr>
<tr>
<td>Category</td>
<td>Select a category to provide organization for the detailed content block. If the block Type is Show the page's current document, the category displays content from any link of the same type.</td>
</tr>
<tr>
<td>Frame</td>
<td>Select a border styling for the detailed content block. For more information, see Format a frame.</td>
</tr>
<tr>
<td>Model Document</td>
<td>Select the document to display by default.</td>
</tr>
<tr>
<td>Active</td>
<td>Select this check box to make the block available for use.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the behavior for the block.</td>
</tr>
<tr>
<td></td>
<td>• Show a Specific Document: Displays the Model Document.</td>
</tr>
<tr>
<td></td>
<td>• Show the page's current document: Displays the currently selected document.</td>
</tr>
<tr>
<td></td>
<td>• Use a script to find a document: Uses the Script field to select a particular document.</td>
</tr>
<tr>
<td>Conditional</td>
<td>Select the check box and enter any scripted conditions to be applied. Selecting this check box adds a Condition script field and Logged on check box to the form.</td>
</tr>
<tr>
<td>Script</td>
<td>Enter a script to find an appropriate document if the Type is set to Use a script to find a document. Set the Return to the GlideRecord of the desired document.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

### Content Management and the Apache Jelly engine

Apache Jelly is a Java-based and XML-based scripting and processing engine for turning XML into executable code.

The Apache Jelly engine closely resembles XML and should be comfortable for developers familiar with JavaScript, XML, XHTML, or HTML. In the ServiceNow instance, the Apache Jelly engine renders items such as forms, lists, and UI Pages. Apache Jelly code renders well within a dynamic content block, but can have issues when used in static blocks. You can use Jelly tags, calls, and statements, but HTML acts just like XHTML.

```xml
<?xml version= "1.0" encoding= "utf-8" ?>
```
Ensure that all tags are closed. If the tag is not a naturally closing tag, then place a forward slash before the end bracket. For example, a `<BR />` or an `<IMG src="cms.png" />`.

If you are unfamiliar with Jelly scripting, review these topics:

- [Jelly tags](#)
- [Extensions to Jelly syntax](#)
- [Jelly escaping types](#)

Include the following tag with all Apache Jelly scripts.

```xml
<j:jelly trim= "false" xmlns:j= "jelly:core" xmlns:g= "glide" xmlns:j2= "null" xmlns:g2 = "null" >
</j:jelly>
```

The tag looks complex, but keep the following information in mind.

- Apache Jelly script uses multiple namespaces.
- There are two types of prefixes in tags: j and g. The j prefix is used for tags that are natively part of Apache Jelly. The g prefix is used for tags that the ServiceNow platform created and is using for platform purposes.

The j2 and g2 prefixes are just like j and g, except that they are processed in a second phase. The Apache Jelly script parser runs through each j and g tag respectively. For example:

```xml
<j:jelly trim= "false" xmlns:j= "jelly:core" xmlns:g= "glide" xmlns:j2= "null" xmlns:g2 = "null" >
<j:set var="jvar_phase1" value="Hello" />
<j2:set var="jvar_phase2" value="World" />
${jvar_phase1} ${jvar_phase2}
</j:jelly>
```

In phase 1, the parser runs through all the j and g tags. It then caches the result. Before it runs the second phase, it takes the j and g namespaces and moves the namespaces to the second phase. It looks something like the following code.

```xml
<j:jelly trim= "false" xmlns:j= "jelly:core" xmlns:g= "glide" xmlns:j2= "jelly:core" xmlns:g2 = "glide" >
<j2:set var="jvar_phase1" value="Hello" />
<j2:set var="jvar_phase2" value="World" />
Hello ${jvar_phase2}
</j:jelly>
```
For subsequent calls of this script, only phase 2 is parsed.

**Note:** If you plan to use phase 2 Jelly tags (g2 and j2) on the Content Type (content_type) or Dynamic Content (content_block_programmatic) tables, select the **Two phase** option on the content form.

Another example is to create a report of all open incidents assigned to each group. For this purpose, you could use a report and save time, but it is a good example for learning Jelly. Start with the Jelly tag:

```xml
<j:jelly trim= "false" xmlns:j= "jelly:core" xmlns:g= "glide" xmlns:j2= "null" xmlns:g2= "null">
</j:jelly>
```

First, you need a list of open incidents. Use a `g2:evaluate` tag. The evaluate tag runs the script. Anything inside the tag is parsed like a business rule, so, for example, you can call global business rules, script includes, and gliderecord.

```xml
<j:jelly trim= "false" xmlns:j= "jelly:core" xmlns:g= "glide" xmlns:j2= "null" xmlns:g2= "null">
  <g:evaluate var="jvar_groups" object="true">
    var gr = new GlideRecord("sys_user_group");
    gr.orderBy('name');
    gr.query();
    gr;
  </g:evaluate>
</j:jelly>
```

This script is in phase 1 because frequent changes to incident assignment groups are not expected. Also notice the `var` attribute on the evaluate tag. This attribute specifies what variable is set from this block. At the end of the script, there is a `gr` on a line by itself. That last line is what sets the variable.

You can omit the `jvar_groups` variable, but then all the variables in the evaluate tag become Apache Jelly variables. The `object=ture` specifies that the variable is not a primitive data type. If `object=true` is omitted, the script would break because `jvar_groups` would only be able to hold items like integers and strings.

After the evaluate tag, loop through these groups and find the incidents for each one.

```xml
<table>
<tr>
  <th>Name</th>
  <th>Incidents</th>
</tr>
<j:while test="${jvar_groups.next()}">
  <tr>
    <td>${HTML:jvar_groups.getValue('name')}</td>
    <td></td>
  </tr>
</j:while>
```

© 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.
You can include normal XML in the Apache Jelly script at any time. Since there is no namespace, the Apache Jelly script does not try to parse the XML tags. Notice the \texttt{j:while} loop. It is a normal while loop and can iterate through a GlideRecord object. Also notice that you output a value with \texttt{$(HTML:jvar\_groups.getValue('name'))$}. Here are the important elements:

- The outer brackets, $\{$\}, specify the output of the variable and the phase in which the variable is output: $\{\}$ means first phase, $\{\}$ means second phase.
- HTML before the expression is for escaping the output. The expression \texttt{jvar\_groups.getValue('name')} is being escaped for HTML. For other types of escaping, there are JS (Javascript), NS (No Script), and some other options.

To select only one record and not iterate through many records, the code looks like the following example:

```xml
<j:jelly trim="false" xmlns:j="jelly:core" xmlns:g="glide" xmlns:j2="null" xmlns:g2="null">
  <g:evaluate var="jvar\_groups" object="true">
    var gr = new GlideRecord("sys\_user\_group");
    gr.orderBy('name');
    gr.query();
    gr;
  </g:evaluate>
  <j:if test="${jvar\_groups.next()}">
    We found ${HTML:jvar\_groups.getValue('name')}
  </j:if>
</j:jelly>
```

Content management and Jelly code examples

**Code examples**

**Header Example Code**

This dynamic content block needs to be active and have the 'Two Phase' option clicked. The \texttt{g:requires} tag is including the UI script defined in the system whose name is 'servicenow\_website\_globals'. The file extension in the call is .jsdbx and is used only in the call to the UI script, not in the name of the script in the system. For JSDBX, the file being called is a JavaScript(.js) defined within the database (db) that needs to be cached (x).

```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">
  <g:requires name = "servicenow\_website\_globals.jsdbx" />
</j:jelly>
```

**Page Title and Description Example Code**

This dynamic content block needs to be active. There are two actions within this code snippet. First is a forward-looking string container that allows site translation, the $\{gs.getMessage('Your Text')\}$ string call). The second action pulls in the page title and description, $\{current\_page.getName()\}$ and $\{current\_page.getDescription()\}$.

```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">
  <j:if test = "${current\_page.getName()}=="Solutions'"">
    <h1 class = "page\_name" > <b> <a href = "solutions\_do?" title =
```
List Block Pulling From Knowledge Articles Example Code

This code example contains one of the best tricks in the CMS. Using the type field with draws from a number of defined list definitions to make slight, or very dramatic changes, to list display. Because the UI is open to configuration and innovation, this is a good opportunity to use design skills. Anyone who can use HTML and CSS knows that a basic list can be turned into a float grid or be made inline. The combinations are limited only by what the designer can dream up and code.

In the code example, there is a custom logo field (u_logo) added to the Knowledge form. The custom field displays customer logos, partner logos, and award images on the awards page. There are a number of different sections that use this list definition so efficient reuse is taking place.

- div class="cms_knowledge_list customer_success" - Begin by creating an outer container with a unique class name that can be used as a basis for CSS style selectors and rules. From the outer container, many of the child elements can be accessed for theming.
- <g:for_each_record file="${current}" max="${jvar_max_entries}"> - Loop for list creation that calls the selected table record and the entries set on the list form.
- <a href="knowledge.do?sysparm_document_key=kb_knowledge,${current.sys_id}"><img src="${current.u_logo.getDisplayValue()}" alt="${current.text}" width="110px"/> - Defines linking to the article detail in the Knowledge base. For further reference, look at content types within the site definition and you will see some similarities. The knowledge.do? portion of the URL points to the knowledge detail page which (as mentioned above) is mandatory if you plan to call the knowledge base in your CMS site. The rest of the URL represents the syntax for calling a knowledge article by its sys_id. Each and every item housed within the system has a unique sys_id.
- ${SP}-${SP}${current.author.first_name}${SP}${current.author.last_name} - This example is commented out and not used, but it is still interesting in that it has a jelly call ${SP} and it pulls the knowledge article’s author by first and last name.

<?xml version= "1.0" encoding= "utf-8" ?>
<j:jelly trim = "false" xmlns:j = "jelly:core" xmlns:g = "glide" xmlns:j2 = "null" xmlns:g2 = "null">
  <div class = "cms_knowledge_list customer_success" >
    <g:for_each_record file="${current}" max="${jvar_max_entries}" >
      <br />
      <table cellspacing = "0" cellpadding = "0" border = "0" class = "background_transparent" >
        <tr>
          <td class = "cms_knowledge_list_image" >
            <j:if test = "${current.u_logo.getDisplayValue() != ''}" >
              <div class = "knowledge_article_logo" >
                <a href = "knowledge.do?sysparm_document_key=kb_knowledge,${current.sys_id}" >
                  <img src="${current.u_logo.getDisplayValue()}" alt="${current.text}" width="110px" />
                </a>
              </div>
            </j:if>
          </td>
          <td width = "100%" >
            <a href = "knowledge.do?sysparm_document_key=kb_knowledge,${current.sys_id}" >
              <img src = "${current.u_logo.getDisplayValue()}" alt = "${current.text}" width = "110px" />
            </a>
          </td>
        </tr>
      </table>
    </g:for_each_record>
  </div>
</j:jelly>
Style in Content Management

Content pages can be styled with CSS, just like any HTML website.

Three elements control CSS styles:

- **Style Sheets** are records containing CSS declarations.
- **Themes** are groups of style sheets that can be invoked together.
- **Frames** are UI macros that define the outer border of individual content blocks as they appear on a content page. Frames work by calling on particular definitions in the style sheets.

**Style sheets**

Styles sheets are standard Cascading Style Sheets (CSS) that define the look and feel of all elements within the interface.

Cascading Style Sheets (CSS) can either be internal (stored in the database) or external (hosted on the server), based on organizational needs. To define an internal style sheet, use standard CSS in the style field. Using external CSS allows the Content Management System to use the same CSS as a corporate website or other online resource.

Use an external style sheet by defining a URL that points to the .cssx file. If you upload a .cssx file to the platform, you can reference the .cssx file using a URL.

Content pages do not reference style sheets directly. To invoke a style sheet, you assign the style sheet to a Theme using the related list on the Theme form.

**Design themes**

Design themes are the convergence of structure and styling, making them a critical tool for creating a powerful user interface.

For a successful project, review the corporate style guide and communicate with the corporate website art team. If the organization has an art or design department that maintains branding, include them in this process.

A theme is a collection of one or more style sheets (CSS files) that define a consistent look for a set of pages. In most environments, many pages share a few themes. Use multiple themes within a site to create stylistic differentiators between site areas. You can also use a single theme to create one unified look and feel for the site.

*Customize a design theme*

A theme is a collection of one or more style sheets (CSS files) that define a consistent look for a set of pages.

Role required: content_admin or admin

Themes can be invoked in any of the following ways.

- Directly by content pages.
- As the default theme of a content site.
- On the configuration page as a global default.

1. Navigate to **Content Management > Design > Themes.**
2. Click **New**.
3. Type a name for the theme and mark it as Active.
4. Right-click the form header and click **Save**
   The **Style Sheet** related list appears.
5. Use the **Style Sheet** related list to add style sheets to the theme.

**Doctypes**

The view_content html page template on which all CMS is based defaults to `doctype=html`. The code looks like the following HTML source code.

```html
<!DOCTYPE HTML>
```

If your CMS site does not render properly, remove the doctype from the page by setting the following property:

- `glide.html.doctype.pages = chat_desktop,live_feed,live_feed_small,navigator,navpage11,image_browse`

The following is the default for this property.

- `glide.html.doctype.pages = chat_desktop,live_feed,live_feed_small,navigator,navpage11,image_browse,view_content`

Setting this doctype offers these benefits for building new sites:

- Incorporating common practice: Use a practice that is becoming widely adopted across the Internet and can prevent certain browsers from running in quirks mode.
- Cleaner CSS and markup: Write more standards-based CSS and markup to promote code sharing.
- A step towards browser compatibility: Find solutions that work across browsers and avoid browser-specific workarounds.

**Format a frame**

Frames provide a way to manage decorative containers for content blocks and any other elements within the site. For example, one frame can be a container, made of div or span tags, that is styled with rounded corners.

Role required: content_admin or admin

Individual content blocks use a frame UI macro to define the frames. When viewing a content block form, the **Frame** field offers a choice between the different frame UI macros. The frame UI macro does not, however, have the definition for the frame within its Jelly script. Instead, it references a particular frame as defined in a style sheet.

Configuring a new frame is a two-step process.

1. Define the frame in a style sheet.
2. Create the frame UI macro to invoke the frame definition.

**Define a frame in a style sheet**

Add style definitions for any custom frame UI macro you create.

Role required: content_admin or admin

Each frame has its own class name.

1. Navigate to **Content Management > Design > Style Sheets**.
2. Select a style sheet to contain the frame definition. Base system themes use a separate Frames style sheet.

3. Add the following code, substituting the desired frame name and style:

```less
div.FRAME_NAME{border:STYLE;}
```

4. Click Update.

**Create a frame UI macro**

Copy an existing frame UI macro to display content in a custom frame.

Role required: content_admin or admin

Create a custom frame UI macro if you want to control the style of the frame with your own style sheet definitions.

1. Navigate to Content Management > Design > Frames and select one of the existing frame UI macros.
2. Change the name to match the FRAME_NAME you used in the style sheet.
3. Right-click the header bar and select Insert and Stay.
4. Update the frame name in the XML field as shown:

```xml
<div class="FRAME_NAME">
```

5. Click Submit.

- In any content block form, select the UI macro.
- Define the frame in a style sheet.

**Content Management meta tags**

Meta tags are special tags in web pages that contain information about the page but are not rendered with the page. You can define custom meta tags for content pages.

Meta tags are not noticeable to a page visitor unless the visitor looks at the page source code. Web search engines read meta tags as they ‘crawl’ the web, identifying and organizing content. Modern website designers often use meta tags to embed ‘hints’ to search engines about how to index or otherwise crawl the site.

Structurally, a meta tag consists of a tag and a name/content pair and looks similar to the following code.

```xml
<meta name="generator" content="MediaWiki 1.16wmf4" />
```

The Content Management System allows you to define both site level and page level tags.

**Configure a page level meta tag**

A page level tag is a meta tag defined on a specific page and included on only that page.

Role required: content_admin or admin

If an individual page has a specific tag with the same name as the site, the page tag takes precedence.

1. Navigate to Content Management > Pages.
2. Open the page.
3. If not already included, add the Meta Tags related list to the form.
4. In the Meta Tags related list, click New.
Configure a site level meta tag

A site level tag is a meta tag is defined on a site and included on every page within that site.

Role required: content_admin or admin

If an individual page has a specific tag with the same name as the site tag, the page tag takes precedence.

1. Navigate to Content Management > Sites.
2. Open the site.
3. If not already included, add the Meta Tags related list to the form.
4. In the Meta Tags related list, click New.
5. Enter a Name and Content for the tag.
6. Click Submit.

Configure DIV-based layouts

After you create your site, you can change the site layout with DIV tags.

Role required: content_admin or admin

Many web page layouts use tables for a consistent look and feel. Tables are effective for numbers and statistics, but can be limiting for designing other types of information. DIV tags are flexible block-element tags. To use DIV tags for layouts, give the tag an ID and assign attributes using CSS.

Changing to CSS and DIV tags help in the following ways:

- simplify code
- reduce the amount of code
- increase page load speed
- separate content from presentation
- help pages adapt to different device resolutions
- make pages easier for search engines to crawl
- make code more compliant with evolving web page design standards

A theme named Administration Theme - Charcoal is included as an example of CSS-driven, DIV-based layouts. To view the Administration Theme - Charcoal DIV-based layout, complete the following steps.

1. Navigate to Content Management > Design > Layouts.
2. Click Admin 1 Column
3. Review the code.

Content meta tag hierarchy

Page and site level meta tags are included in a content meta tag hierarchy.

Site and page level tags

CMS supports page level and site level tags. The system behavior is to show the sum of all page level and site level tags. For example, if you have two tags on the site and one tag on the page, all with different names, you see three tags on the page. Two are from the site and one is from the page. If both the site and the page have a tag of the same name, only the page tag is used.
**Note:** The Content Management System does not support some commonly used meta tags. For example, you cannot use the X-UA-Compatible meta tag, which allows you to specify which version of Internet Explorer a site should be rendered in.

### Example: all tags have unique names

<table>
<thead>
<tr>
<th>Site Level</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>breakfast</td>
<td>eggs</td>
</tr>
<tr>
<td>lunch</td>
<td>sandwich</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Page Level</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>dinner</td>
<td>steak</td>
</tr>
</tbody>
</table>

**Output**

<table>
<thead>
<tr>
<th>Name</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>breakfast</td>
<td>eggs</td>
</tr>
<tr>
<td>lunch</td>
<td>sandwich</td>
</tr>
<tr>
<td>dinner</td>
<td>steak</td>
</tr>
</tbody>
</table>

### Example: page level tag overrides site level tag

<table>
<thead>
<tr>
<th>Site Level</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>breakfast</td>
<td>eggs</td>
</tr>
<tr>
<td>lunch</td>
<td>sandwich</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Page Level</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>lunch</td>
<td>tacos [--- overrides site level steak ]</td>
</tr>
<tr>
<td>dinner</td>
<td>steak</td>
</tr>
</tbody>
</table>

**Output**

<table>
<thead>
<tr>
<th>Name</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>breakfast</td>
<td>eggs</td>
</tr>
<tr>
<td>lunch</td>
<td>tacos</td>
</tr>
<tr>
<td>dinner</td>
<td>steak</td>
</tr>
</tbody>
</table>

### Content Management integration points

Integration points use content blocks in CMS to link different applications together using static and dynamic methods.

By using integration points, users can connect to different systems from a single page. The power of the CMS is that it can display any data within the ServiceNow platform. The ESS portal, for example, connects users to a service catalog, a knowledge base, and a help and incident reporting site. Each section contains a set of links to additional content. List blocks offer the easiest way to display data dynamically. Content types define how lists link to the detailed data they reference.

Generating lists from the ServiceNow platform is straightforward, especially if you use filtering. When the CMS was first introduced, lists were the only method available to create navigational systems for sites. Content types define system record links using specific templates to define the list and the details.
ServiceNow Jakarta Now Platform Capabilities

- Summary template: defines the list
- Detail template: defines the detail as it is rendered in a page.

The templates work together to pass data attributes or unique record identifiers (sysid) into a single detail page that manages the data. Any attribute variations use the URL sent to the page.

Understanding how content types work can mean the difference between a site with 20 pages versus a site with 200 pages. There is a time for both types of data calls. Depending on the task, there are appropriate times to use static content and times for dynamic methods.

**View links between system elements and URLs**

You can view the links between your system elements and their URLs to render more specific content within your site.

Role required: content_admin or admin

See the URL schema page for an overview of URL syntax in the ServiceNow platform.

The Incidents list offers a quick example of viewing a form within its own tab. This viewing method illustrates how to append the URL string to render more specific content within your site.

1. Navigate to Incident > All.
2. Right-click in a blank area within the content frame and select Open Frame in New Window or Open Frame in New Tab.

   The URL returned looks similar to this example.

   `<instance_name>/incident_list.do?sysparm_userpref_module=b55b4ab0c0a80009007a9c0f03fb4da9`

   The URL is comprised of the following elements.

   - `incident_list.do?` is the call to the list with no parameters passed into it. Explore context menu options and list filtering variations to see how the URL string is appended with each action.
   - `incident_list.do?sysparm_query=&sysparm_view=ess` is an example of how the view is passed in the URL string.
   - `incident_list.do?sysparm_query=GROUPBYactive&sysparm_view=` is how the URL looks when the group by option is chosen from the context menu.
   - `incident_list.do?sysparm_query=category%3Dsoftware` is the result of applying a category is software filter to the list.

   Explore all the options available within the right-click menu. Click through to the Incident form itself (incident.do) to see what the URL string does when parameters are passed into it.

**Element link examples**

View examples that show how to create a site pointing to various system data in several different data tables.

The following examples illustrate setting up access to the following system data.

- Knowledge: building a versatile front end for a knowledge base, from overview page to variations on the list definitions used in the site.
- Catalog: ideas for a business-to-consumer shopping experience that pulls various items and forms from your service catalog.
- Service Portfolio: using the business service portfolio to contain all defined services offered by your organization.
- Featured reports: methods for linking to the most important reports.
Example links to system data

Page source view

Use the tools available in your browser to view the frame source page and understand what URL address bars pass between system frame sets.

The Firefox browser, for example, has the developer tools option. This option provides an easy way to view records that render within the main content frame (gsft_main) of the ServiceNow platform. Also, Firefox quickly builds menus and links to records within the system.

This Firefox functionality is useful when stepping through the menu items section.
Frame view

**Static methods**

Static methods in the CMS application were created for ease of use.

Form-based menu management and WYSIWYG code editing can be useful to both advanced and entry-level users. The technical ability of subject matter experts (SMEs) managing the language of your site can vary considerably. Letting SMEs write the content and having a technical resource manage the linking expedites menu and link creation within the system.
Static and dynamic methods

**Navigation Menu Links**

Use base system templates to group similar links for placement on the page. Though the terminology is different (menu sections and menu items), this type of linking behaves the same way as content links. For more information on creating a navigation menu block, see [Create a navigation menu block](#).

**Static HTML Details**

Content blocks that are useful for areas administered by developers unfamiliar with HTML or markup. Anyone familiar with markup can use dynamic blocks because they are extendable. For more information on static HTML, see [Using Content Blocks](#).

**Content Links**

The predecessors to navigation menus from when the CMS was first introduced. Use content links to make navigational links by defining several content links under the same category. Then, call the links as a list referencing the Content Link (content_link) table.

**iFrame Details**
Used both dynamically and statically throughout the system. Using them is an easy way to bring any form or list into your CMS pages. For more information on iFrame methods, see Using Content Blocks.

**Dynamic methods**

While static methods are a powerful navigational tool, you have more control over data rendering using the dynamic methods.

Reference common code in the system to make long-term maintenance of the site easier. Coding skills are useful when implementing dynamic methods.

**Static and dynamic methods**

**Dynamic Blocks**

These blocks are where the majority of your work resides. For more information, see Configure dynamic blocks.

**Frames**

Frames are meant to be decorative wrappers around any block in the system. They are mentioned with dynamic blocks because frames are essentially UI macros with the category
of Frame. Frames apply the ${body} variable to a block and define where the block is inserted when rendered on the page.

Lists

Lists generate links to records based on the filtering rules you define. Lists can be sorted for presentation by any field in the corresponding record. Lists help supplement navigation and pull data from outside the CMS. For more information, see Customize the list block.

Content Types

Content types provide site-specific control of how system data defined as templates is rendered. The rendering of lists is considered first (summary templates). The next consideration is the detail template, which allows control over the record rendering.

List Definitions

List definitions enable you to extend the summary template defaults defined on the site level. Used with frames, list definitions render the same data differently based on the placement on the page or site. For more information, see Configure list definitions.

Detailed Content

Detailed content in page detail settings) are blocks that display the content of an existing document as a block on a content page. For more information, see Configure a detailed content block.

Example integration points

Each element on the page links to a specific URL point.
**Business Services** links to a content page (CMS page referenced: Business Service Portfolio, URL: business_service_category.do) that pulls the system service catalog homepage into a frame within the content area. Each link within this section uses the browse by category page, where you pass in the name of the category to return results.

- **Target page iFrame URL:** catalog_home.do?
  sysparm_nameofstack=aabdaed07ef22100914304167b22567d&sysparm_view=business&sysparm_clean=true
- **Target page frame name:** gsft_main
  - **Desktop Computing** URL: category_browse.do?category=Desktop Computing
  - **Business Applications** URL: category_browse.do?category=Business Applications
  - **Communications Services** URL: category_browse.do?category=Communications Services
  - **Infrastructure Services** URL: category_browse.do?category=Infrastructure Services
  - **Hosting Services** URL: category_browse.do?category=Hosting Services

**Featured Services** links to a content page which pulls a small subset of services into an iFrame.

- **iFrame URL:** com.glideapp.servicecatalog_category_view.do?
  sysparm_parent=d67c446ec0a80165000335aa37efbc1&sysparm_view=
- **Frame name:** gsft_main
  - **Install Software** URL: catalog.do?
    uri=com.glideapp.servicecatalog_cat_item_view.do?
    sysparm_id=10d69689c611227600335aa37efbc1&sysparm_view=
  - **Email Account** URL: catalog.do?
    uri=com.glideapp.servicecatalog_cat_item_view.do?
    sysparm_id=d67a86b6c0a80165009386c752cd4a09
  - **Electronic Messaging** URL: catalog.do?
    uri=com.glideapp.servicecatalog_cat_item_view.do?
    sysparm_id=533798810a0a0b2600f1a03593e19058
  - **VPN RSA Token** URL: catalog.do?
    uri=com.glideapp.servicecatalog_cat_item_view.do?
    sysparm_id=d67b099ac0a8016500919c276b772502
  - **Shared Storage (SAN)** URL: catalog.do?
    uri=com.glideapp.servicecatalog_cat_item_view.do?
    sysparm_id=cedd458a0a0b8300c3b1e32e7a3ac2

**Reporting** links to a content page that pulls the reports page into an iFrame. All links within this menu leverage homepage in the system, which creates an issue with the home.do URL. Notice in the following links that ../ is used to create a relative URL outside of the CMS site home.do definition. Without this path, the site homepage would render within the iFrame.

- **iFrame URL:** report_home.do
- **Frame name:** gsft_main
  - **Cost Management Overview** URL: ../home.do?
    sysparm_userpref_homepage=fa81ae91c0a805c64c0942ab2e4b852b
  - **Administration Overview** URL: ../home.do?
    sysparm_userpref_homepage=8b7b11f6c611228901ff3fcfbd3cc8f
  - **Portfolio Overview** URL: catalog_home.do?sysparm_view=business
  - **Service Availability** URL: ../home.do?
    sysparm_userpref_homepage=8ee772000a0bad00c38eb7e68b93d0

© 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.
Content Management testing

Test your site to ensure that all pages display correctly, links go to the specified address, and images are not broken. It is important to test the site as you build it. Do not wait until just before launch to begin testing.

Also, test templates as you create them so any issues are resolved before creating other content based on the templates. Recruit as many people as possible to help you test.

Here are some general site testing guidelines:

- Test on the browsers and platforms your site visitors use
- Test on various monitors (for example, LCD and CRT)
- View pages using different screen resolutions
- View pages using different color settings
- Test all navigation and links
- Test items that can be downloaded (for example, PDF files)
- Test the search functionality
- Test site security
- If necessary, test for accessibility (for guidelines, see the W3C Website Accessibility Initiative)

Global search in Content Management

When you add global search to a CMS site, two different search result blocks can display, depending on the user role: global or no global.

Roles are defined at System Properties > Global Text Search.

- Search Results (Global): For users with permission to use the global search within the normal frame set. The normal frame set is defined as the default, non-CMS user interface with the set of frames.
- Search Results (No Global): For users without permission to use the global search. Searches only the knowledge base and the catalog.

The header search bar and the Search dynamic block in the base system both automatically handle the permissions and direct the user to the appropriate search results. In the base system, the search result blocks are deployed on the same Search Results content page.

In order for the global search to work properly, it is important to ensure that the DEFAULT directs users to a working content page. If not, the results from the global search link back to the frame set, not to pages within the CMS site.

Note: The global search is similar to the normal frame set user interface and ties to the same roles (Set global text search properties).

Search Results (Global)

Before you use the Search Results (Global) dynamic block, define content types to control the behavior a search result is clicked. If no content type is defined for a table, selecting a link on that table renders the results according to the DEFAULT content type. It is good practice to point
the **DEFAULT** content type to a page with a normal "Current Document" detailed block. Set the content type detail (**Detail Template** field) to have just an iFrame.

The **Search Results (No Global)** dynamic block does not require any additional configuration.

### CMS translation

You can translate CMS sites by activating internationalization plugins and manually translating custom interface strings.

Two tables support the translation of a CMS site into other languages.

- Translated Name / Field (sys_translated): Stores strings that are shared or commonly used within a site. These include menu section names, menu item names, site breadcrumb names, link names, and footer menu links. Internationalization plugins typically provide translations for these strings. See [Localization settings](#).
- Translated Text (sys_translated_text): Stores unique string translations which you create when you manually translate interface elements. See [Translate the interface](#).

### View a translated CMS site

Activating an internationalization plugin provides a quick way to see translated strings for CMS menus, breadcrumbs, and links. For a full translation, you must translate the instance manually.

The following example explains how to view a translated site in Japanese.

1. Navigate to **System Definition > Plugins**.
2. In the **Go to** filter, select **Name**, enter `I18N`, and then press the Enter key.
3. Activate both the `I18N - Japanese Translations` and the `I18N: Knowledge Management Internationalization Plugin v2` plugins.
4. Refresh the browser.
5. In the **Language** picker in System Settings, select **Japanese**.
6. Browse the site to see the translated language strings.
8. Browse the site to see the translated language strings in the ESS Portal.

### Credentials and connection information

Credentials and connection information are required to gain access to a computer or network device for Discovery, Service Mapping, and Cloud Management or to perform work using Orchestration.

**Explore**

- [Credentials release notes](#)
- [Upgrade to Jakarta](#)
- [Introduction to credentials](#)
- [Credential affinity for Discovery and Orchestration](#)

**Set up**

- [Create credentials](#)
- [Check IP service affinity for Discovery and Orchestration](#)
- [MID Server connection prerequisites](#)

**Integrate**

- [External credential storage](#)

**Troubleshoot and get help**

- [Credentials troubleshooting](#)
- [Search the HI knowledge base for known error articles](#)
Introduction to credentials

Several applications require credentials to access resources during discovery, including Discovery, Orchestration, Service Mapping, and Cloud Management.

Credential types

The following credential types are provided:

<table>
<thead>
<tr>
<th>Credential type</th>
<th>Description</th>
<th>Supports Test Credential option</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Applicative Credentials</strong></td>
<td>The credentials to explore the applications on a device or computer. Patterns often need applicative credentials.</td>
<td>No</td>
</tr>
<tr>
<td><strong>AWS Credentials</strong></td>
<td>The Amazon Web Services (AWS) master account, access key ID, and secret access key.</td>
<td>No</td>
</tr>
<tr>
<td><strong>Azure Service Principal</strong></td>
<td>The Azure service principals required for an Azure subscription.</td>
<td>No</td>
</tr>
<tr>
<td><strong>Basic Authentication Credentials</strong></td>
<td>A user name and password.</td>
<td>No</td>
</tr>
<tr>
<td><strong>CIM Credentials</strong></td>
<td>The user name and password required to access a CIMOM - Common Information Model Object Manager (CIM) server, which obtains information about VMware ESX servers.</td>
<td>No</td>
</tr>
<tr>
<td><strong>Cloud Management Credential</strong></td>
<td>Credentials that Orchestration uses to access cloud resources.</td>
<td>No</td>
</tr>
<tr>
<td><strong>JDBC Credentials</strong></td>
<td>A user name and password to access a Java Database Connectivity (JDBC) connection.</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>JMS Credentials</strong></td>
<td>A user name and password to access a Java Message Service (JMS).</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>SNMP Community Credentials (Password Only)</strong></td>
<td>The community string to access devices via SNMP.</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>SNMPv3 Credentials</strong></td>
<td>The user name and keys required to access devices on your SNMP v3 network.</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>SSH Credentials</strong></td>
<td>The user name and password to access Linux and Unix devices.</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>SSH Private Key Credentials</strong></td>
<td>The private key credentials to access Linux and Unix devices. SSH private key credentials are recommended over SSH password credentials for security reasons.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
## How MID Servers use credentials

By default, Windows MID Servers use the login credentials of the MID Server service on the host machine to discover Windows devices in the network. You should configure these service credentials so that they have at least local administrator privileges. For Linux and UNIX machines and network devices, the MID Server uses the SSH and SNMP credentials configured in the instance in Discovery > Credentials.

MID Servers that Orchestration uses must have access to the necessary credentials to execute commands on computers in the network as specified by the Workflow activities. Orchestration can use the same SSH and SNMP credentials as Discovery, but has two additional credentials designed for specific Workflow activities: Windows (for PowerShell) and VMware.

### Encryption and decryption

The platform stores credentials in an encrypted field on the Credentials (discovery_credentials) table. Once they are entered, they cannot be viewed.

When credentials are requested by the MID Server, the platform decrypts the credentials using the following process:

1. The credentials are decrypted on the instance with the password2 fixed key.
2. The credentials are re-encrypted on the instance with the MID Server's public key.
3. The credentials are encrypted on the load balancer with SSL.
4. The credentials are decrypted on the MID Server with SSL.
5. The credentials are decrypted on the MID Server with the MID Server's private key.

**Note:** The platform does not have separate encryption keys for multi-tenant instances.

### Credential order

Credentials can be assigned an order value in the Credentials Form, which forces the application to try all the credentials at their disposal in a certain sequence. If you do not specify an order value, the application tries the credentials in the Credentials (discovery_credentials) table randomly, until it finds one that works, such as when Orchestration attempts to run a command on an SSH server (such as a Linux or UNIX machine), or when Discovery attempts to query an SNMP device (such as a printer, router, or UPS).
After identifying the credentials for a device, Discovery and Orchestration create an affinity between the credentials and the device using the Credential Affinity [dscy_credentials_affinity] table. All subsequent discoveries or Orchestration activities attempt to match the credentials in this table with a device for which an affinity exists. If credentials for a device change, Discovery and Orchestration try all available credentials again until they create a new affinity.

**Note:** If Orchestration and Discovery are installed, and credential tagging is enabled, multiple affinities can exist. In this case, the platform looks up credentials for each affinity and inserts the credential for the affinity with the lowest order into the probe.

Ordering credentials is useful in the following situations:

- The credentials table contains many credentials, with some used more frequently than others. For example, if the table contains 150 SSH credentials, and 5 of those are used to log into 90% of the devices, it is good practice to configure those five with low order numbers, which places them at the top of the execution list. Discovery and Orchestration will work faster if they try these common credentials first. After the first successful connection, the system knows which credentials to use the next time for each device.

- The system has aggressive login security. For example, if the Solaris database servers in the network only allow three failed login attempts before they lock out the MID Server, configure the database credentials with a low order value.

**Credential tagging**

Credential tagging allows workflow creators to assign individual credentials to any activity in an Orchestration workflow or assign different credentials to each occurrence of the same activity type in an Orchestration workflow. Credential tagging also works with credential affinities.

**External credential stores**

If you do not want credentials stored in your instance, you can use external credential repositories. External credential stores save the credentials in an external site that your instance can access. Only CyberArk is supported.

**Credential synchronization with MID Servers**

Each MID server on your network synchronizes with your instance keeps what is essentially a copy of every credential that you create. This synchronization is done to speed up the reading of credentials when applications like Discovery or Service Mapping need to access multiple devices on the network. The MID Servers synch when they find a credentials_reload job in the ECC Queue. The reload job instructs the MID Server to make a SOAP call to the instance to get the entire list of credentials, including all the field values, in the Credentials [discovery_credentials] table.

The SOAP response that your instance sends to each MID Server also includes custom fields that you added to any credential form that you customized. If you added reference fields, the data in the referenced table is also sent as part of the SOAP response.

**Create credentials**

Discovery, Service Mapping, Cloud Management, and Orchestration require credentials to access hardware and software on your network.
Role required: admin

1. Navigate to one of these modules:
   - Discovery > Credentials
   - Service Mapping > Credentials
   - Orchestration > Credentials

2. Click New.
3. On the Credentials page, click a link for the credential type and complete the form.
4. Click Submit.

Test your credentials.

Applicative credentials

Some applications require credentials in addition to the credentials the that host machine requires. Credentials required to access these applications are referred to as applicative credentials.

A typical credential contains a user name and a password for logging into a device or application. While most applications require only one credential for accessing them, sometimes hosts and applications have separate credentials for extra security. For example, ABAP SAP Central Services (ASCS) requires applicative credentials in addition to the SSH or Windows host credentials for the server that hosts ASCS.

Note: In Service Mapping and Discovery, devices and applications are referred to as configuration items (CIs).

Just like with host credentials, you assign applicative credentials to MID Servers.

You create applicative credentials per CI type, for example the CI type for ASCS is SAP ASCS Application (cmdb_ci_appl_sap_ascs). The preconfigured pattern for discovering CIs belonging to this CI type contains commands that require a MID Server to use the applicative credential for this CI type. If there is more than one credential configured for this CI type, the MID Server tries using these credentials in the order you define until it finds the credential that fits.

Check the discovery requirements information in the ServiceNow documentation to determine if you need to configure applicative credentials for specific application CIs. There is no need to configure applicative credentials, if discovery prerequisites do not mention it.

Applicative credentials form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the credential. Use a descriptive name like Oracle DB or London Oracle DB (for an Oracle database).</td>
</tr>
<tr>
<td>Active</td>
<td>Select this check box to use this credential.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter the actual user name of the applicative credential.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the actual password of the applicative credential.</td>
</tr>
<tr>
<td>CI type</td>
<td>Select a CI type to which the CI belongs.</td>
</tr>
<tr>
<td>Tag</td>
<td>Enter the table name for the CI type whose applicative credentials the application uses. Applications may use applicative credentials of a CI type different from their own.</td>
</tr>
</tbody>
</table>

For this application | Select this table
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABAP SAP Central Services (ASCS)</td>
<td>cmdb_ci_appl_sap_ascs</td>
</tr>
<tr>
<td>IBM Security Access Manager appliance</td>
<td>cmdb_ci_appl_server_webseal</td>
</tr>
<tr>
<td>SAP Central Instance</td>
<td>cmdb_ci_appl_sap_ascs</td>
</tr>
<tr>
<td>SAP Central Services (SCS)</td>
<td>cmdb_ci_appl_sap_ascs</td>
</tr>
<tr>
<td>SAP Evaluated Receipt Settlement (ERS)</td>
<td>cmdb_ci_appl_sap_ascs</td>
</tr>
<tr>
<td>SAP Java Cluster</td>
<td>cmdb_ci_appl_sap_ascs</td>
</tr>
<tr>
<td>SAP NetWeaver Dialog Instance</td>
<td>cmdb_ci_appl_sap_ascs</td>
</tr>
<tr>
<td>Microsoft Exchange Mailbox (for Microsoft Exchange)</td>
<td>cmdb_ci_exchange_mailbox</td>
</tr>
<tr>
<td>Microsoft SQL Database</td>
<td>cmdb_ci_db_mssql_instance</td>
</tr>
<tr>
<td>MySQL Server</td>
<td>cmdb_ci_db_mysql_instance</td>
</tr>
<tr>
<td>Oracle Advanced Queue Queue</td>
<td>cmdb_ci_db_ora_instance</td>
</tr>
<tr>
<td>Oracle Database</td>
<td>cmdb_ci_db_ora_instance</td>
</tr>
<tr>
<td>Oracle E-Business Suite</td>
<td>cmdb_ci_db_ora_instance</td>
</tr>
<tr>
<td>Oracle WebLogic Module</td>
<td>cmdb_ci_app_server_weblogic</td>
</tr>
<tr>
<td>Tibco EMS Queue</td>
<td>cmdb_ci_appl_tibco_message</td>
</tr>
<tr>
<td>Tibco Enterprise Message Service (EMS)</td>
<td>cmdb_ci_appl_tibco_message</td>
</tr>
</tbody>
</table>

### Applies to

Select whether to apply these credentials to All MID servers in your network, or to one or more Specific MID servers. Specify the MID Servers that should use these credentials in the MID servers field.

### Order

Enter the order (sequence) in which the platform tries this credential as it attempts to log on to devices. The smaller the number, the higher in the list this credential appears. Establish credential order when using large numbers of credentials or when security locks out users after three failed login attempts. If all the credentials have the same order number (or none), the instance tries the credentials in a random order.

---

**Amazon Web Services credentials**

Amazon Web Services (AWS) credentials access services within the AWS cloud.

After you create a credential and select AWS, these fields are available on the form:

**AWS credentials form fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Input value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique and descriptive name for this credential. For example, you might call it AWS Main Account.</td>
</tr>
</tbody>
</table>
### Azure Service Principal and Enterprise Agreement credentials

Azure credentials are necessary for your instance to access a Microsoft Azure cloud. Azure Enterprise Agreement credentials are necessary for the billing functionality that the Cloud Management application provides.

These fields are available on the Azure Service Principal form:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the service principal to register with the instance.</td>
</tr>
<tr>
<td>Tenant ID and Client ID</td>
<td>Paste the values that you obtained from the Azure portal:</td>
</tr>
<tr>
<td></td>
<td>- The Tenant ID is the Directory ID in Azure.</td>
</tr>
<tr>
<td></td>
<td>- The Client ID is the ID of the application that you registered in Azure. If you do not have an application, you must create one under App registrations in the Azure portal.</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Select <strong>Client secret</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Client assertion is not supported.</td>
</tr>
<tr>
<td>Secret key</td>
<td>Paste the secret key that was generated while creating the Azure Service Principal in the Azure portal. This field appears when Authentication method is <strong>Client secret</strong>.</td>
</tr>
</tbody>
</table>

These fields are available on the Azure Enterprise Agreement Credentials 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>Enrollment number</td>
<td>Enter the enrolment number from Azure.</td>
</tr>
<tr>
<td>Access Key</td>
<td>Paste in the access key that Azure provides you.</td>
</tr>
</tbody>
</table>

### Basic authentication credentials

The Basic Auth credential type manages access to store basic authentication credentials. This credential type is available for Discovery and Orchestration.
These fields are available in the Credentials form for basic authentication.

**Basic Auth credentials form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Input value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique and descriptive name for this credential. For example, you might call it <strong>Basic Authentication</strong>.</td>
</tr>
<tr>
<td>User Name</td>
<td>Enter the user name.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password.</td>
</tr>
<tr>
<td>Credential ID</td>
<td>Enter the unique key configured for these credentials in the <em>CyberArk</em> external credential storage system. The credential ID may be used as a safe override when multiple safes are in use. By default, the syntax in the Credential ID field is this: <code>&lt;safe name&gt;:&lt;Credential ID&gt;</code>. If the safe name is omitted, there must be a safe name defined in the config.xml file. To change the separator character from the default colon to another character, override the value with the optional <code>ext.cred.safe_name</code> parameter. The Credential ID field has a limit of 40 characters. This field is only visible when the <strong>External storage</strong> check box is selected.</td>
</tr>
</tbody>
</table>

**External credential store**

Select this check box to use an external credential storage system. When you select this option the **User name** and **Password** fields are replaced with the **Credential ID** field. Currently, the only supported external storage system is *CyberArk*.

**Order**

Enter the order (sequence) in which the platform tries this credential as it attempts to log on to devices. The smaller the number, the higher in the list this credential appears. Establish credential order when using large numbers of credentials or when security locks out users after three failed login attempts. If all the credentials have the same order number (or none), the instance tries the credentials in a random order.

---

**Chef server credentials**

Chef server credentials access chef integrations with the instance.

These fields are available on the Credentials form for Chef server type credentials. This information comes from the settings you configured when you performed **Chef server installation**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique and descriptive name for this credential.</td>
</tr>
<tr>
<td>Active</td>
<td>Enable or disable these credentials for use.</td>
</tr>
<tr>
<td>Admin Name</td>
<td>Provide the administrator name that you created during Chef server installation.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Admin Key | Enter the RSA private key that the Chef server generated when you created the administrator.
Validator Name | Enter the validator.
Validator Key | Enter the RSA private key that the Chef server generated when you created an organization.
Cert Name | Enter the certification name.
Cert Key | Enter the certification key.

### CIM credentials

The CIM credential type manages access to a CIM server (also referred to as a CIMOM - Common Information Model Object Manager) for information about VMware ESX servers. This credential type is available for Discovery.

These fields are available in the Credentials form for CIM.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique and descriptive name for this credential.</td>
</tr>
<tr>
<td>Active</td>
<td>Enable or disable these credentials for use.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter the user name to create in the Credentials table. Avoid leading or trailing spaces in user names. A warning appears if the platform detects leading or trailing spaces in the user name.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password.</td>
</tr>
<tr>
<td>Credential ID</td>
<td>Enter the unique key configured for external credentials in the JAR file uploaded to the MID Server for an external credential system. The Credential ID field has a limit of 40 characters. This field is only visible when the External credential store check box is selected.</td>
</tr>
<tr>
<td>Tag</td>
<td>Allow workflow creators to assign individual credentials to any activity in an Orchestration workflow or assign different credentials to each occurrence of the same activity type in an Orchestration workflow. To use the credential for discovering CIs not belonging to this CI type using Service Mapping and Discovery patterns, enter the table name for the CI type to which the CI belongs, for example cmdb_ci_apache_web_server. For more information, see Change credentials to non-default.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>External credential store</td>
<td>Select this check box to use an external credential storage system. When you select this option the User name and Password fields are replaced with the Credential ID field. External credential storage is only available when the External Credential Storage plugin is activated.</td>
</tr>
<tr>
<td>Note:</td>
<td>Currently, the only supported external storage system is CyberArk.</td>
</tr>
<tr>
<td>Applies to</td>
<td>Select whether to apply these credentials to All MID servers in your network, or to one or more Specific MID servers. Specify the MID Servers that should use these credentials in the MID servers field.</td>
</tr>
<tr>
<td>MID servers</td>
<td>Select one or more MID Servers from the list of available MID Servers. The credentials configured in this record are available to the MID Servers in this list. This field is available only when you select Specific MID servers from the Applies to field.</td>
</tr>
<tr>
<td>Order</td>
<td>Enter the order (sequence) in which the platform tries this credential as it attempts to log on to devices. The smaller the number, the higher in the list this credential appears. Establish credential order when using large numbers of credentials or when security locks out users after three failed login attempts. If all the credentials have the same order number (or none), the instance tries the credentials in a random order.</td>
</tr>
</tbody>
</table>

**Configure NetApp storage devices for CIM credentials**

NetApp storage devices require additional configuration in order for Discovery to explore them.

Role required: admin

1. Install the SMI-S agent on the storage device host. See the Data ONTAP SMI-S Agent 5.2 Installation and Configuration Guide for instructions and requirements.

   **Note:**
   
   ServiceNow does not maintain the documentation on this site. Be aware that this document can change without notice.

2. Create a user account and password for the SMI-S agent.
3. Create a record for the SMI-S agent credentials. Set the credential type to CIM.

**Cloud Management credentials**

The Cloud Management credential type manages access to a cloud-based application. This credential type is available for Orchestration.

These fields are available in the Credentials form for cloud management.
## Cloud Management credentials form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Input value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique and descriptive name for this credential. For example, you might call it <strong>Cloud Atlanta</strong>.</td>
</tr>
<tr>
<td>Active</td>
<td>Enable or disable these credentials for use.</td>
</tr>
<tr>
<td>Type</td>
<td>Specify <strong>AWS</strong>.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter the CIM user name to create in the Credentials table. Avoid leading or trailing spaces in user names. A warning appears if the platform detects leading or trailing spaces in the user name.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the CIM password.</td>
</tr>
<tr>
<td>SSH Passphrase</td>
<td>Enter a memorable phrase for key generation. For example, you might enter <strong>Friday is a good day</strong>.</td>
</tr>
<tr>
<td>SSH private key</td>
<td>Enter the SSH private key.</td>
</tr>
<tr>
<td>Authentication protocol</td>
<td>Select the <strong>MD5</strong> or <strong>SHA</strong> authentication protocol that was used to generate the <strong>Authentication Key</strong>.</td>
</tr>
<tr>
<td>Authentication Key</td>
<td>Enter a SSH-generated authentication key.</td>
</tr>
</tbody>
</table>
| Privacy protocol       | Enter one of the following privacy protocols that describes encryption for the **Privacy Key**:
  - **3DES** for Triple Data Encryption Standard (DES)
  - **AES128** for Advanced Encryption Standard (AES) with 128 bit encryption
  - **AES192** for AES with 192 bit encryption
  - **AES256** for AES with 256 bit encryption
  - **DES** for legacy DES encryption

Enter an additional privacy key.

| Tag                    | Allow workflow creators to assign individual credentials to any activity in an Orchestration workflow or assign different credentials to each occurrence of the same activity type in an Orchestration workflow. |
| External credential store | Select this check box to use an external credential storage system. When you select this option the **User name** and **Password** fields are replaced with the **Credential ID** field. Currently, the only supported external storage system is CyberArk. |
| Applies to             | Select whether to apply these credentials to All **MID servers** in your network, or to one or more **Specific MID servers**. Specify the MID Servers that should use these credentials in the **MID servers** field. |
| Classification         | Enter the Application Classification for CI discovery.                      |
### Cloud Management (CMP) node credentials

Cloud Management (CMP) node credentials associate credentials for a virtual server that Cloud Management provisions. The Cloud Management application automatically creates these credentials.

You might need to deactivate these credentials if you no longer want them used, change the order precedence, or select a MID Server that is allowed to access them. Otherwise, you do not need to manually create or modify this type of credential.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The automatically generated name based on the datacenter where the virtual machine is located.</td>
</tr>
<tr>
<td>Active</td>
<td>If the credentials are active.</td>
</tr>
<tr>
<td>Applies to</td>
<td>Choose whether this credential is available to a specific MID Server or all MID Servers.</td>
</tr>
<tr>
<td>Order</td>
<td>Enter the order (sequence) in which the platform tries this credential as it attempts to log on to devices. The smaller the number, the higher in the list this credential appears. Establish credential order when using large numbers of credentials or when security locks out users after three failed login attempts. If all the credentials have the same order number (or none), the instance tries the credentials in a random order.</td>
</tr>
<tr>
<td>User Name and Password</td>
<td>The virtual server user name and password.</td>
</tr>
<tr>
<td>SSH passphrase and SSH private key</td>
<td>The private key and the passphrase that protects the key if the virtual server requires it.</td>
</tr>
<tr>
<td>Authentication Protocol and Authentication Key</td>
<td>The private key and the passphrase that protects the key if the virtual server requires it.</td>
</tr>
<tr>
<td>Privacy Protocol and Privacy Key</td>
<td>The encryption protocol used with the virtual server and enter the privacy key.</td>
</tr>
<tr>
<td>Tag</td>
<td>Allow workflow creators to assign individual credentials to any activity in an Orchestration workflow or assign different credentials to each occurrence of the same activity type in an Orchestration workflow.</td>
</tr>
</tbody>
</table>
Cloud Management (CMP) SSH key pair credentials

Cloud Management (CMP) SSH key pairs store the keys that the Cloud Management application automatically generates when users provision stack resources.

You might need to deactivate these credentials if you no longer want them used. Otherwise, you do not need to manually create or modify this type of credential.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The automatically generated name.</td>
</tr>
<tr>
<td>Active</td>
<td>If the credentials are active.</td>
</tr>
<tr>
<td>SSH Public Key</td>
<td>The public key.</td>
</tr>
<tr>
<td>SSH Private Key</td>
<td>A secure private key that can be used instead of a password for SSH logins.</td>
</tr>
</tbody>
</table>

Infoblox credentials

Infoblox credentials are required to set up IP pools (IPAM) in the Cloud Management application. These fields are available on the Credentials form for Infoblox type credentials.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique and descriptive name for this credential.</td>
</tr>
<tr>
<td>Active</td>
<td>Enable or disable these credentials for use.</td>
</tr>
<tr>
<td>Applies to</td>
<td>Choose whether this credential is available to a specific MID Server or all MID Servers.</td>
</tr>
<tr>
<td>Order</td>
<td>Enter the order (sequence) in which the platform tries this credential as it attempts to log on to devices. The smaller the number, the higher in the list this credential appears. Establish credential order when using large numbers of credentials or when security locks out users after three failed login attempts. If all the credentials have the same order number (or none), the instance tries the credentials in a random order.</td>
</tr>
<tr>
<td>wAPI Version</td>
<td>Enter the version of wAPI you are using.</td>
</tr>
<tr>
<td>User Name and Password</td>
<td>Enter the InfoBlox user name and password.</td>
</tr>
</tbody>
</table>

JDBC credentials

The JDBC credential type manages access to a Java Database Connectivity (JDBC) connection. This credential type is available for Discovery and Orchestration.

These fields are available in the Credentials form for JDBC type credentials.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique and descriptive name for this credential.</td>
</tr>
<tr>
<td>Active</td>
<td>Enable or disable these credentials for use.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User name</td>
<td>Enter the user name to create in the Credentials table. Avoid leading or trailing spaces in user names. A warning appears if the platform detects leading or trailing spaces in the user name.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password.</td>
</tr>
<tr>
<td>Credential ID</td>
<td>Enter the unique key configured for external credentials in the JAR file uploaded to the MID Server for an external credential system. The <strong>Credential ID</strong> field has a limit of 40 characters. This field is only visible when the <strong>External credential store</strong> check box is selected.</td>
</tr>
<tr>
<td>Tag</td>
<td>Allow workflow creators to assign individual credentials to any activity in an Orchestration workflow or assign different credentials to each occurrence of the same activity type in an Orchestration workflow. To use the credential for discovering CIs not belonging to this CI type using Service Mapping and Discovery patterns, enter the table name for the CI type to which the CI belongs, for example cmdb_ci_apache_web_server. For more information, see <a href="#">Change credentials to non-default</a>.</td>
</tr>
<tr>
<td>External credential store</td>
<td>Select this check box to use an external credential storage system. When you select this option the <strong>User name</strong> and <strong>Password</strong> fields are replaced with the <strong>Credential ID</strong> field. External credential storage is only available when the <strong>External Credential Storage plugin</strong> is activated. <strong>Note:</strong> Currently, the only supported external storage system is <strong>CyberArk</strong>.</td>
</tr>
<tr>
<td>Applies to</td>
<td>Select whether to apply these credentials to <strong>All MID servers</strong> in your network, or to one or more <strong>Specific MID servers</strong>. Specify the MID Servers that should use these credentials in the <strong>MID servers</strong> field.</td>
</tr>
<tr>
<td>MID servers</td>
<td>Select one or more MID Servers from the list of available MID Servers. The credentials configured in this record are available to the MID Servers in this list. This field is available only when you select <strong>Specific MID servers</strong> from the <strong>Applies to</strong> field.</td>
</tr>
<tr>
<td>Order</td>
<td>Enter the order (sequence) in which the platform tries this credential as it attempts to log on to devices. The smaller the number, the higher in the list this credential appears. Establish credential order when using large numbers of credentials or when security locks out users after three failed login attempts. If all the credentials have the same order number (or none), the instance tries the credentials in a random order.</td>
</tr>
</tbody>
</table>
**JMS credentials**

The JMS credentials type manages access to a Java Message Service (JMS). This credential type is available for Discovery and Orchestration.

These fields are available in the Credentials form for JMS.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique and descriptive name for this credential.</td>
</tr>
<tr>
<td>Active</td>
<td>Enable or disable these credentials for use.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter the user name to create in the Credentials table. Avoid leading or trailing spaces in user names. A warning appears if the platform detects leading or trailing spaces in the user name.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password.</td>
</tr>
<tr>
<td>Credential ID</td>
<td>Enter the unique key configured for external credentials in the JAR file uploaded to the MID Server for an external credential system. The Credential ID field has a limit of 40 characters. This field is only visible when the <strong>External credential store</strong> check box is selected.</td>
</tr>
<tr>
<td>Tag</td>
<td>Allow workflow creators to assign individual credentials to any activity in an Orchestration workflow or assign different credentials to each occurrence of the same activity type in an Orchestration workflow. To use the credential for discovering CIs not belonging to this CI type using Service Mapping and Discovery patterns, enter the table name for the CI type to which the CI belongs, for example cmdb_ci_apache_web_server. For more information, see <strong>Change credentials to non-default</strong>.</td>
</tr>
<tr>
<td>External credential store</td>
<td>Select this check box to use an external credential storage system. When you select this option the <strong>User name</strong> and <strong>Password</strong> fields are replaced with the <strong>Credential ID</strong> field. External credential storage is only available when the <strong>External Credential Storage plugin</strong> is activated. <strong>Note</strong>: Currently, the only supported external storage system is <strong>CyberArk</strong>.</td>
</tr>
<tr>
<td>Applies to</td>
<td>Select whether to apply these credentials to <strong>All MID servers</strong> in your network, or to one or more <strong>Specific MID servers</strong>. Specify the MID Servers that should use these credentials in the <strong>MID servers</strong> field.</td>
</tr>
<tr>
<td>MID servers</td>
<td>Select one or more MID Servers from the list of available MID Servers. The credentials configured in this record are available to the MID Servers in this list. This field is available only when you select <strong>Specific MID servers</strong> from the <strong>Applies to</strong> field.</td>
</tr>
</tbody>
</table>
### Order

Enter the order (sequence) in which the platform tries this credential as it attempts to log on to devices. The smaller the number, the higher in the list this credential appears. Establish credential order when using large numbers of credentials or when security locks out users after three failed login attempts. If all the credentials have the same order number (or none), the instance tries the credentials in a random order.

### SAP credentials

The SAP credential type manages access to SAP JCo systems. This credential type is available for Discovery and Orchestration.

These fields are available in the Credentials form for SAP type credentials.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique and descriptive name for this credential.</td>
</tr>
<tr>
<td>Active</td>
<td>Enable or disable these credentials for use.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter the user name to create in the Credentials table. Avoid leading or trailing spaces in user names. A warning appears if the platform detects leading or trailing spaces in the user name.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password.</td>
</tr>
<tr>
<td>Credential ID</td>
<td>Enter the unique key configured for external credentials in the JAR file uploaded to the MID Server for an external credential system. The <strong>Credential ID</strong> field has a limit of 40 characters. This field is only visible when the <strong>External credential store</strong> check box is selected.</td>
</tr>
<tr>
<td>Tag</td>
<td>Allow workflow creators to assign individual credentials to any activity in an Orchestration workflow or assign different credentials to each occurrence of the same activity type in an Orchestration workflow. To use the credential for discovering CIs not belonging to this CI type using Service Mapping and Discovery patterns, enter the table name for the CI type to which the CI belongs, for example cmdb_ci_apache_web_server. For more information, see <a href="#">Change credentials to non-default</a>.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>External credential store</td>
<td>Select this check box to use an external credential storage system. When you select this option the User name and Password fields are replaced with the Credential ID field. External credential storage is only available when the External Credential Storage plugin is activated.</td>
</tr>
<tr>
<td>Note:</td>
<td>Currently, the only supported external storage system is CyberArk.</td>
</tr>
<tr>
<td>Applies to</td>
<td>Select whether to apply these credentials to All MID servers in your network, or to one or more Specific MID servers. Specify the MID Servers that should use these credentials in the MID servers field.</td>
</tr>
<tr>
<td>MID servers</td>
<td>Select one or more MID Servers from the list of available MID Servers. The credentials configured in this record are available to the MID Servers in this list. This field is available only when you select Specific MID servers from the Applies to field.</td>
</tr>
<tr>
<td>Order</td>
<td>Enter the order (sequence) in which the platform tries this credential as it attempts to log on to devices. The smaller the number, the higher in the list this credential appears. Establish credential order when using large numbers of credentials or when security locks out users after three failed login attempts. If all the credentials have the same order number (or none), the instance tries the credentials in a random order.</td>
</tr>
</tbody>
</table>

**SNMP credentials**

Discovery explores many kinds of devices (switches, routers, printers, etc.) using the SNMP protocol. Credentials for SNMP do not include a user name, just a password, called the community string.

The default read-only community string for many SNMP devices is public, and Discovery will try that automatically. Enter the appropriate SNMP credentials if they differ from the public community string.

Discovering SNMP uses all community strings that are configured. This behavior does not apply to discovering SNMPv3.

The default Orchestration activity SNMP Query returns the object identifier (OID) of a device and requires SNMP credentials.

**SNMP community credentials**

The SNMP Community credential type manages access to discover many kinds of devices (switches, routers, printers, etc.) using the SNMP protocol. This credential type is available for Discovery, Service Mapping, and Orchestration.

Credentials for SNMP do not include a user name, just a password (the community string). The default read-only community string for many SNMP devices is public, and the system will try that automatically. Enter the appropriate SNMP credentials if they differ from the public community string.
These fields are available in the Credentials form for SNMP community.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a unique and descriptive name for this credential.</td>
</tr>
<tr>
<td><strong>Active</strong></td>
<td>Enable or disable these credentials for use.</td>
</tr>
<tr>
<td><strong>User name</strong></td>
<td>Enter the user name to create in the Credentials table. Avoid leading or trailing spaces in user names. A warning appears if the platform detects leading or trailing spaces in the user name.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Enter the password.</td>
</tr>
<tr>
<td><strong>Credential ID</strong></td>
<td>Enter the unique key configured for external credentials in the JAR file uploaded to the MID Server for an external credential system. The Credential ID field has a limit of 40 characters. This field is only visible when the External credential store check box is selected.</td>
</tr>
<tr>
<td><strong>Tag</strong></td>
<td>Allow workflow creators to assign individual credentials to any activity in an Orchestration workflow or assign different credentials to each occurrence of the same activity type in an Orchestration workflow. To use the credential for discovering CIs not belonging to this CI type using Service Mapping and Discovery patterns, enter the table name for the CI type to which the CI belongs, for example cmdb_ci_apache_web_server. For more information, see Change credentials to non-default.</td>
</tr>
<tr>
<td><strong>External credential store</strong></td>
<td>Select this check box to use an external credential storage system. When you select this option the User name and Password fields are replaced with the Credential ID field. External credential storage is only available when the External Credential Storage plugin is activated. Note: Currently, the only supported external storage system is CyberArk.</td>
</tr>
<tr>
<td><strong>Applies to</strong></td>
<td>Select whether to apply these credentials to All MID servers in your network, or to one or more Specific MID servers. Specify the MID Servers that should use these credentials in the MID servers field.</td>
</tr>
<tr>
<td><strong>MID servers</strong></td>
<td>Select one or more MID Servers from the list of available MID Servers. The credentials configured in this record are available to the MID Servers in this list. This field is available only when you select Specific MID servers from the Applies to field.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Order | Enter the order (sequence) in which the platform tries this credential as it attempts to log on to devices. The smaller the number, the higher in the list this credential appears. Establish credential order when using large numbers of credentials or when security locks out users after three failed login attempts. If all the credentials have the same order number (or none), the instance tries the credentials in a random order.

### SNMPv3 credentials

SNMP credentials accept a privacy protocol and an additional privacy key and are available for Discovery and Orchestration.

Discovering SNMP uses all community strings that are configured. This behavior does not apply to discovering SNMPv3. These fields are available in the Credentials form for SNMPv3.

#### SNMP v3 form

<table>
<thead>
<tr>
<th>Field</th>
<th>Input value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique and descriptive name for this credential. For example, you might call it <strong>SNMP Community Atlanta</strong>.</td>
</tr>
<tr>
<td>Active</td>
<td>Enable or disable these credentials for use.</td>
</tr>
<tr>
<td>Applies to</td>
<td>Select whether to apply these credentials to <strong>All MID servers</strong> in your network, or to one or more <strong>Specific MID servers</strong>. Specify the MID Servers that should use these credentials in the <strong>MID servers</strong> field.</td>
</tr>
<tr>
<td>MID servers</td>
<td>Select one or more MID Servers from the list of available MID Servers. The credentials configured in this record are available to the MID Servers in this list. This field is available only when you select <strong>Specific MID servers</strong> from the <strong>Applies to</strong> field.</td>
</tr>
<tr>
<td>Order</td>
<td>Enter the order (sequence) in which the platform tries this credential as it attempts to log on to devices. The smaller the number, the higher in the list this credential appears. Establish credential order when using large numbers of credentials or when security locks out users after three failed login attempts. If all the credentials have the same order number (or none), the instance tries the credentials in a random order.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter the SNMP user name. Avoid leading or trailing spaces in user names. A warning appears if the platform detects leading or trailing spaces in the user name.</td>
</tr>
<tr>
<td>Authentication protocol</td>
<td>Select the authentication type to use for this credential. The choices are <strong>MD5</strong> and <strong>SHA</strong>.</td>
</tr>
<tr>
<td>Authentication Key</td>
<td>Enter the authentication key to use for this credential.</td>
</tr>
<tr>
<td>Field</td>
<td>Input value</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Privacy protocol</td>
<td>Select the encryption protocol for this credential. The choices are:</td>
</tr>
<tr>
<td></td>
<td>• 3DES</td>
</tr>
<tr>
<td></td>
<td>• AES128</td>
</tr>
<tr>
<td></td>
<td>• AES192</td>
</tr>
<tr>
<td></td>
<td>• AES256</td>
</tr>
<tr>
<td></td>
<td>• DES</td>
</tr>
<tr>
<td>Privacy key</td>
<td>Enter the key associated with the selected privacy protocol.</td>
</tr>
<tr>
<td>Credential ID</td>
<td>Enter the unique key configured for external credentials in the JAR file uploaded to the MID Server for an external credential system. The <strong>Credential ID</strong> field has a limit of 40 characters. This field is only visible when the <strong>External credential store</strong> check box is selected.</td>
</tr>
<tr>
<td>Tag</td>
<td>Allow workflow creators to assign individual credentials to any activity in an Orchestration workflow or assign different credentials to each occurrence of the same activity type in an Orchestration workflow.</td>
</tr>
<tr>
<td>External credential store</td>
<td>Select this check box to use an external credential storage system. When you select this option the <strong>User name</strong> and <strong>Password</strong> fields are replaced with the <strong>Credential ID</strong> field. External credential storage is only available when the <strong>External Credential Storage plugin</strong> is activated.</td>
</tr>
</tbody>
</table>

**SSH credentials**

The SSH credential type manages access for Unix and Linux devices that use the Secure Shell (SSH).

**Note:** For increased security, ServiceNow recommends the use of SSH private key credentials rather than SSH password credentials.

These fields are available in the Credentials form for SSH.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique and descriptive name for this credential.</td>
</tr>
<tr>
<td>Active</td>
<td>Enable or disable these credentials for use.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter the user name to create in the Credentials table. Avoid leading or trailing spaces in user names. A warning appears if the platform detects leading or trailing spaces in the user name.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Credential ID | Enter the unique key configured for external credentials in the JAR file uploaded to the MID Server for an external credential system. The **Credential ID** field has a limit of 40 characters. This field is only visible when the **External credential store** check box is selected.
Tag | Allow workflow creators to assign individual credentials to any activity in an Orchestration workflow or assign different credentials to each occurrence of the same activity type in an Orchestration workflow.
To use the credential for discovering CIs not belonging to this CI type using Service Mapping and Discovery patterns, enter the table name for the CI type to which the CI belongs, for example cmdb_ci_apache_web_server. For more information, see [Change credentials to non-default](#).
External credential store | Select this check box to use an external credential storage system. When you select this option the **User name** and **Password** fields are replaced with the **Credential ID** field. External credential storage is only available when the **External Credential Storage plugin** is activated.

**Note:** Currently, the only supported external storage system is [CyberArk](#).
Applies to | Select whether to apply these credentials to **All MID servers** in your network, or to one or more **Specific MID servers**. Specify the MID Servers that should use these credentials in the **MID servers** field.
MID servers | Select one or more MID Servers from the list of available MID Servers. The credentials configured in this record are available to the MID Servers in this list. This field is available only when you select **Specific MID servers** from the **Applies to** field.
Order | Enter the order (sequence) in which the platform tries this credential as it attempts to log on to devices. The smaller the number, the higher in the list this credential appears. Establish credential order when using large numbers of credentials or when security locks out users after three failed login attempts. If all the credentials have the same order number (or none), the instance tries the credentials in a random order.

### SSH private key credentials form

These fields are available in the Credentials form for SSH private keys.

SSH private key credentials are recommended over SSH password credentials for security reasons.
**SSH private key credentials form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Input value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique and descriptive name for this credential. For example, you might call it <strong>SSH Atlanta</strong>.</td>
</tr>
<tr>
<td>Active</td>
<td>Enable or disable these credentials for use.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter a UNIX or Linux user name. Avoid leading or trailing spaces in user names. A warning appears if the platform detects leading or trailing spaces in the user name.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the UNIX or Linux password. For <strong>SSH Private Key</strong> type credentials, enter the sudo password if one is required for the user name.</td>
</tr>
<tr>
<td>SSH passphrase</td>
<td>Type a secure SSH passphrase. This field is available only for <strong>SSH Private Key</strong> credentials.</td>
</tr>
</tbody>
</table>
| SSH private key        | Enter a secure, private key that can be used instead of a password for SSH logins. The private key must be entered in the proper format to ensure it is correctly encrypted. The private key must start with the string **-----BEGIN**. Here is an example of a correctly formatted private key:  

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAsEK65scPssPSobpDFMｐR+Btv3MS4Q7NP8ERaSR2zsh3IWz+x...
...7hrxV2dbSug60FahypGWBGtPnXm5PaE2X5WP1uJ94n
-----END RSA PRIVATE KEY-----
```

The Now Platform supports private keys in the PEM format generated by the OpenSSH `ssh-keygen` utility. To convert PPK keys that were generated by PuTTY:

- Open your private key in PuTTYGen.
- Export it in OpenSSH format from the menu **Conversions > Export OpenSSH key**.
- Save the new OpenSSH key.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Allow workflow creators to assign individual credentials to any activity in an Orchestration workflow or assign different credentials to each occurrence of the same activity type in an Orchestration workflow.</th>
</tr>
</thead>
<tbody>
<tr>
<td>External credential store</td>
<td>Select this check box to use an external credential storage system. When you select this option the <strong>User name</strong> and <strong>Password</strong> fields are replaced with the <strong>Credential ID</strong> field. Currently, the only supported external storage system is CyberArk.</td>
</tr>
<tr>
<td>MID servers</td>
<td>Select one or more MID Servers from the list of available MID Servers. The credentials configured in this record are available to the MID Servers in this list. This field is available only when you select <strong>Specific MID servers</strong> from the <strong>Applies to</strong> field.</td>
</tr>
<tr>
<td>Field</td>
<td>Input value</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Applies to</td>
<td>Select whether to apply these credentials to All MID servers in your network, or to one or more Specific MID servers. Specify the MID Servers that should use these credentials in the MID servers field.</td>
</tr>
<tr>
<td>Order</td>
<td>The order (sequence) in which the platform tries this credential as it attempts to log onto devices. The smaller the number, the higher in the list this credential appears. Establish credential order when using large numbers of credentials or when security locks out users after three failed login attempts. If all the credentials have the same order number (or none), Discovery or Orchestration tries the credentials in a random order.</td>
</tr>
</tbody>
</table>

**UNIX and Linux credentials**

Discovery and Orchestration explore UNIX and Linux devices by using commands executed over Secure Shell (SSH), so they need SSH credentials.

The user can be any user. Both applications must run commands on UNIX and Linux systems with root privileges. There are two general approaches to accomplishing this:

- **Give root credentials.** These are obviously the most powerful credentials, but may not be desirable from a security perspective. If Discovery or Orchestration have the root credentials to any UNIX or Linux system, no further configuration is required.
- **Give other credentials for Discovery or Orchestration, but grant the user in those credentials the right to execute certain commands with root privileges, using sudo.** This is a secure way to grant limited privileges. Discovery or Orchestration use sudo on any probe that has the must_sudo parameter set to true (it defaults to false). However, each system must be configured to allow sudo to work. This is done by editing the /etc/sudoers file using the visudo command.

**Access Requirements for Non-Root Credentials**

If you do not provide Discovery with root access credentials, you must provide credentials with the following access requirements.

<table>
<thead>
<tr>
<th>Application</th>
<th>File or Directory</th>
<th>Access Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache</td>
<td>httpd.conf</td>
<td>Read</td>
</tr>
<tr>
<td>Hbase</td>
<td>hbase-site.xml</td>
<td>Read</td>
</tr>
<tr>
<td>JBoss</td>
<td>jboss-service.xml</td>
<td>Read</td>
</tr>
<tr>
<td></td>
<td>JBoss home directory</td>
<td>Read</td>
</tr>
<tr>
<td></td>
<td>web.xml</td>
<td>Read</td>
</tr>
<tr>
<td>MySQL</td>
<td>my.cnf</td>
<td>Read</td>
</tr>
<tr>
<td>NGINX</td>
<td>nginx.conf</td>
<td>Read</td>
</tr>
<tr>
<td>Oracle</td>
<td>oratab</td>
<td>Read</td>
</tr>
<tr>
<td></td>
<td>Associated (s) pfiles</td>
<td>Read</td>
</tr>
</tbody>
</table>
### UNIX and Linux commands requiring root privileges for Discovery and Orchestration

These commands require root privileges in Discovery and Orchestration.

The examples here assume that the user name in the credentials is `Disco`. Substitute the actual user name and ensure that the paths for the commands match the path on the systems.

**Note:** Sudo commands do not work with private key credentials, because there is no password to supply to the sudo command. A solution is to add the NOPASSWD option to the sudo configuration. For example, you might enter: `disco ALL=(root) NOPASSWD:/usr/sbin/dmidecode,/usr/sbin/lsof,/sbin/ifconfig`.

### UNIX and Linux commands requiring root privileges

<table>
<thead>
<tr>
<th>Command</th>
<th>Platform</th>
<th>Purpose</th>
<th>/etc/sudoers line example</th>
<th>Used by</th>
</tr>
</thead>
<tbody>
<tr>
<td>adb</td>
<td>HP-UX</td>
<td>Gathers CPU speed and memory.</td>
<td>Disco ALL=(root) /usr/bin/adb</td>
<td>Discovery</td>
</tr>
<tr>
<td>chage</td>
<td>All Linux and UNIX versions</td>
<td>Changes the number of days between password changes and the date of the last password change.</td>
<td>Disco ALL=(root) /usr/bin/chage</td>
<td>Orchestration</td>
</tr>
<tr>
<td>chpasswd</td>
<td>All Linux and UNIX versions</td>
<td>Changes user passwords.</td>
<td>Disco ALL=(root) /etc/chpasswd</td>
<td>Orchestration</td>
</tr>
<tr>
<td>Command</td>
<td>Platform</td>
<td>Purpose</td>
<td>/etc/sudoers line example</td>
<td>Used by</td>
</tr>
<tr>
<td>---------</td>
<td>------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>---------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>dmidecode</td>
<td>All Linux</td>
<td>Gathers several pieces of information about the hardware, including the serial number embedded within the motherboard.</td>
<td>Disco ALL=(root) /sbin/dmidecode</td>
<td>Discovery</td>
</tr>
<tr>
<td>dmsetup</td>
<td>Linux and Solaris</td>
<td>Examines a low level volume.</td>
<td>Disco ALL=(root) /usr/bin/dmsetup table * Disco ALL=(root) /usr/bin/dmsetup ls</td>
<td>Discovery</td>
</tr>
<tr>
<td>fcinfo</td>
<td>Solaris</td>
<td>Gets WWPNs for ports.</td>
<td>${sudo:fcinfo remote-port -sl -p $port}</td>
<td>Discovery</td>
</tr>
<tr>
<td>fdisk</td>
<td>All Linux</td>
<td>Gathers the disks and size information on the system.</td>
<td>Disco ALL=(root) /usr/bin/fdisk -l</td>
<td>Discovery</td>
</tr>
<tr>
<td>iscsiadm</td>
<td>Solaris</td>
<td>Gets iSCSI IQNs.</td>
<td>${sudo:iscsiadm list target -S}</td>
<td>Discovery</td>
</tr>
<tr>
<td>lsof</td>
<td>All UNIX versions</td>
<td>Determines the relationship between processes and the connections being made to the system.</td>
<td>Disco ALL=(root) /sbin/lsof</td>
<td>Discovery</td>
</tr>
<tr>
<td>multipath</td>
<td>All Linux</td>
<td>Gathers device mappings for MPIO.</td>
<td>Disco ALL=(root) /usr/bin/multipath -Il</td>
<td>Discovery</td>
</tr>
<tr>
<td>oratab</td>
<td>All Unix versions</td>
<td>Grants read access to the oratab file for locating the Oracle Home and pfile.</td>
<td>N/A</td>
<td>Discovery</td>
</tr>
<tr>
<td>prtvtoc</td>
<td>Solaris</td>
<td>Reports information about disk partitions.</td>
<td>Disco ALL=(root) /usr/bin/prtvtoc</td>
<td>Discovery</td>
</tr>
<tr>
<td>/usr/bin/ps</td>
<td>Solaris</td>
<td>Lists running process. As an alternative to running with root access, add a proc_owner role.</td>
<td>Disco ALL=(root) /usr/bin/ps</td>
<td>Discovery</td>
</tr>
</tbody>
</table>
### Privileged commands for Discovery

To discover certain information on a host server, Discovery must run SSH commands with higher privilege.

An example of information that requires elevated privileges is information about storage disks on a host server, retrieved with the `fdisk -l` command. If your system cannot use sudo commands, you must configure the hosts in your network to use one of the other privileged commands.

**Note:** You can have different privileged commands set up for different hosts. However, Discovery supports only one privileged command per host.

### SSH privileged escalation command requirements

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>sudo</strong></td>
<td></td>
</tr>
</tbody>
</table>
- Host must support the `sudo -S -p <password>` command and return the correct list of allowed SSH commands.  
- Credentials provided for Discovery must be able to run the command `sudo -S -p <password> <commands>`.
|
| **pbrun** |  
- Host must support the `pbrun -v` command and return the correct version of PowerBroker.  
- Credentials provided for Discovery must be able to run `pbrun <commands>`.  
- Discovery does not support any other `pbrun` options, such as a password prompt.  
- The instance must be able to reach the target host via SSH.  
<p>|</p>
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| pfexec  | - Host must support the `pfexec id -a` command and return the correct ID.  
- Credentials provided for Discovery must be able to run `pfexec <commands>`.
- Discovery does not support any other `pfexec` options, such as a password prompt. |
| dzdo    | - Host must support the `dzdo` command and return the path to `dzdo` in standard output.  
- Credentials provided for Discovery must be able to run `dzdo <commands>`.
- Discovery does not support any other `dzdo` options, but Discovery supports password authentication for `dzdo`. |

Add a new privileged command

Add a new privileged command to the Privileged Command (privileged_command) table that is available to your MID Servers.

Role required: admin

**Important**: Do not delete any of the supported commands.

1. Navigate to MID Server > Privileged Command and click New.
2. Complete these fields:
   - **Command**: The name of the privileged command.
   - **Password Prompt**: The password prompt displayed to the user for this privileged command, or a regular expression that matches this password prompt. If this field is empty, no password is required for this privileged command, and no prompt is displayed. SUDO commands do not require a password prompt.
3. Click Submit.

Configure the MID Server to use specific privileged commands

You can configure the MID Server to use specific commands in a defined order.

Role required: admin

1. Navigate to the list of MID Servers using one of the following paths:
   - MID Server > Servers
   - Discovery > MID Servers
   - Orchestration > MID Servers
2. Select the MID Server you want to configure.
3. Click the menu icon in the header bar and select View > Advanced from the context menu.
4. In the **Privileged Command** related list, click **Edit**.
5. Select the command you want this MID Server to use and click **Save**.

The default order of privileged commands is 100, but you can change the order as necessary. The privileged command with the smallest order number is tried first.
List of privileged commands to use for a MID Server

Create a pbrun profile privileged command

You can create a special configuration for the pbrun privileged command that allows it to run as a profile.

Role required: discovery_admin, admin

Of all the privileged commands, only the pbrun command can be configured to run as a profile, and only one of these special pbrun configurations can function on a MID Server.

Important: Edit the existing pbrun record for this purpose. The system ignores any additional commands you create for pbrun.

1. Navigate to MID Server > Privileged Command.
2. Select pbrun from the list.
3. In the Privileged Command record, edit the value in the Command field to use the format pbrun -u <profile>.
   For example, you can set pbrun -u admin as a command to run with an admin profile.
4. Click Update.

Long running commands with sudo

Configure J2SSH and ServiceNow SSH to prevent long running commands using sudo from failing when the MID Server disconnects.

ServiceNow SSH allows probes to run sudo against individual commands or an entire, long-running script. This is also supported for the pbrun and pfexec privileged commands.
Sudo for individual commands

You can run sudo against individual commands within a probe, but only if all the following sudoer configurations are performed on the target:

- The !requiretty option is required.
- Allow individual commands to be run by the user in the provided credential with NOPASSWD configured.
- The target specifies an individual sudo call in the command or referenced scripts. For example, set sudo as "sudo fdisk -I" or "${sudo:fdisk -I}" rather than "must_sudo" for the entire script.

Note: Running sudo against individual commands with ServiceNow SSH produces detailed and useful entries in the sudo logs on the target computer.

Running sudo on an entire script

If any of the required sudoer configuration requirements for individual commands is not in place, Discovery applies sudo to the initial and complete probes, and does not execute sudo remotely inside the command. This condition can be forced by setting must_sudo on the probe and eliminating any sudo commands within the probe.

This approach prevents long running commands from failing when the probe disconnects, but cannot specify individual commands in the sudoers configuration.

Logging

The logs from ServiceNow SSH sudo activity run against an entire script show cryptic entries, such as /tmp/.run.aef13123fe124123, which prevent administrators from controlling permissible commands and knowing the exact command that was run. Sudo run against individual commands produces more detailed log entries, such as /sbin/fdisk -l.

VMware credentials

The VMware credentials type manages access to vCenter credentials.

Applications that access VMware cloud resources need access to VMware credentials. For example, the VMware credential type allows Discovery to explore VMware's vCenter running on a Windows machine to discover ESX machines, virtual machines, and resource pools. The VMware Discovery and automation API (vCenter API) now provides the globally unique serial number for computer CIs. CIM credentials are not needed to allow access to each VMware host.

Note: Windows credentials are not necessary for vCenter Discovery, when valid VMware credentials are used.

Important: Do not use VMware Type credentials for Orchestration activities that perform work on the individual virtual machines cloned by vCenter (for example, restarting a Linux VM). For these activities, the credential Type depends on the operating system of the virtual machine (either SSH or Windows).
VMware credentials form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique and descriptive name for the VMware credentials.</td>
</tr>
<tr>
<td>Active</td>
<td>Enable or disable these credentials for use.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter the user name you use for your VMware account.  Avoid leading or trailing spaces in user names.  A warning appears if the platform detects leading or trailing spaces in the user name.  The VMware credentials must have the read-only role in vCenter.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the VMware account.</td>
</tr>
<tr>
<td>MID servers</td>
<td>Select one or more MID Servers from the list of available MID Servers. The credentials configured in this record are available to the MID Servers in this list. This field is available only when you select Specific MID servers from the Applies to field.</td>
</tr>
<tr>
<td>Order</td>
<td>Enter the order (sequence) in which the platform tries this credential as it attempts to log on to devices.  The smaller the number, the higher in the list this credential appears.  Establish credential order when using large numbers of credentials or when security locks out users after three failed login attempts.  If all the credentials have the same order number (or none), the instance tries the credentials in a random order.</td>
</tr>
</tbody>
</table>

Windows credentials

The Windows credential type manages access to Windows computers. This credential type is available for Discovery and Orchestration.

These fields are available in the Credentials form for Windows.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique and descriptive name for this credential.</td>
</tr>
<tr>
<td>Active</td>
<td>Enable or disable these credentials for use.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter the user name to create in the Credentials table. Avoid leading or trailing spaces in user names.  A warning appears if the platform detects leading or trailing spaces in the user name.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password.</td>
</tr>
<tr>
<td>Credential ID</td>
<td>Enter the unique key configured for external credentials in the JAR file uploaded to the MID Server for an external credential system.  The <strong>Credential ID</strong> field has a limit of 40 characters.  This field is only visible when the External credential store check box is selected.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Tag</td>
<td>Allow workflow creators to assign individual credentials to any activity in an Orchestration workflow or assign different credentials to each occurrence of the same activity type in an Orchestration workflow. To use the credential for discovering CIs not belonging to this CI type using Service Mapping and Discovery patterns, enter the table name for the CI type to which the CI belongs, for example cmdb_ci_apache_web_server. For more information, see Change credentials to non-default.</td>
</tr>
<tr>
<td>External credential store</td>
<td>Select this check box to use an external credential storage system. When you select this option the User name and Password fields are replaced with the Credential ID field. External credential storage is only available when the External Credential Storage plugin in activated. Note: Currently, the only supported external storage system is CyberArk.</td>
</tr>
<tr>
<td>Applies to</td>
<td>Select whether to apply these credentials to All MID servers in your network, or to one or more Specific MID servers. Specify the MID Servers that should use these credentials in the MID servers field.</td>
</tr>
<tr>
<td>MID servers</td>
<td>Select one or more MID Servers from the list of available MID Servers. The credentials configured in this record are available to the MID Servers in this list. This field is available only when you select Specific MID servers from the Applies to field.</td>
</tr>
<tr>
<td>Order</td>
<td>Enter the order (sequence) in which the platform tries this credential as it attempts to log on to devices. The smaller the number, the higher in the list this credential appears. Establish credential order when using large numbers of credentials or when security locks out users after three failed login attempts. If all the credentials have the same order number (or none), the instance tries the credentials in a random order.</td>
</tr>
</tbody>
</table>

**Permission requirements for Windows credentials**

Provide the proper permissions for the Windows credentials.

**User accounts**

To provide sufficient permissions, Windows credentials must be one of the following:

- A domain user with local administrator access on the target Windows hosts.
- A local account that has administrator privileges and User Access Control (UAC) disabled on the same target host.
- A user who meets the requirements of Discovery Windows probes and permissions (Discovery only).
- A user who meets the requirements of the Orchestration activity to be run (Orchestration only).

**Workgroup computers**

To run Powershell commands to discover a Workgroup computer, configure the MID Server credentials for either of these users:

- Built-in administrator account on the Workgroup computer.
- Domain user on the Workgroup computer.

**Domain requirements for Windows credentials**

To enable Windows credentials to function across multiple domains, make sure to use the correct name formats and MID Server configuration.

**Supported User Name Formats**

Discovery and Orchestration support Windows domain credentials in both User Principal Name and Down-Level Logon Name user name formats. For example, Domain\ UserName or UserName@example.domain.com. You can provide Windows workgroup credentials in the following format: WORKGROUP\ UserName.

You can also provide a local account by using the . \ user name.

For information about credential requirements, see *Permission requirements for Windows credentials*.

**Windows Domain Requirements**

Additional actions are required to enable credentials to function across multiple Windows domains.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Additional actions required</th>
</tr>
</thead>
<tbody>
<tr>
<td>MID Server host on the same domain as the Windows target.</td>
<td>None</td>
</tr>
<tr>
<td>MID Server host on a different domain than the Windows target.</td>
<td>Ensure that Powershell 2.0 or higher is installed on the MID Server host.</td>
</tr>
<tr>
<td>MID Server host on a different domain than the Microsoft SQL Server target.</td>
<td>See MSSQL server discovery.</td>
</tr>
</tbody>
</table>

**Windows credential requirements for Discovery and Orchestration**

Add Windows credentials to specific locations for Discovery and Orchestration.

Discovery and Orchestration have the following requirements for Windows credentials:

- Install a MID Server on a Windows host as a service.
- Add Windows credentials to one of these locations:
  - An entry in the Credentials [windows_credentials] table
• A MID Server service account to run as a specific Windows user or domain account.

**Configure MID Server credentials from the credentials table**

Configure the MID Server to use Windows credentials from the Credentials (discovery_credentials) table.

To have the MID Server use credentials from the Credentials (discovery_credentials) table:

1. Add individual Windows credentials to the Credentials [windows_credentials] table.
   - Verify each credential meets the permission requirements.
   - Verify each username meets the name format requirements.
   - Verify each credential meets the Windows domain requirements.

2. (Optional) Configure the MID Server to use Powershell by setting the mid.use_powershell parameter to **true**. See [MID Server Configuration](#).

3. (Optional) By default, Discovery automatically uses the MID Server service account credentials if all credentials in the Credentials table fail. If you do not want to use the MID Server service credentials as a fall back, set the mid.powershell.local_mid_service_credential_fallback parameter to **false**.

**Configure MID Server credentials from the service account**

Configure the MID Server to use the credentials of its own Windows service.

To have the MID Server use credentials from the MID Server service account:

1. Set the **MID Server service account** to a user who meets the permission requirements.
2. Verify the username meets the name format requirements.
3. Fill in the fields on the form, as appropriate.
4. Verify the credentials meet domain requirements.

**Test your credentials**

You can test your credentials directly from the Credentials record.

Role required: discovery_admin, admin

You can submit a credential record first and then test it later, or test the credential immediately before saving it.

**Note:** Credentials are encrypted at all times during the test.

Credential testing is supported for these credential types:

- SSH (including private keys)
- Windows
- SNMP (including v3)
- VMware
- JDBC
- JMS

This procedure assumes you are testing the credential before submitting it.

1. Navigate to **Discovery > Credentials**, and click **New**.
2. Select the type of credentials to create.
3. Enter your credentials in the record fields.
4. Under Related Links, click Test credential.
5. Complete the fields in the Test Credential dialog box.

### Credential test fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Credential type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target</td>
<td>Target host on which these credentials are run. This value must be an IP address for all credential types except VMware, which can be the host URL.</td>
<td>All</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For JMS, this is the provider URL. The information in this URL tells JNDI how to find and access the JMS Provider. An example value for connecting to ActiveMQ V5.1, is <code>tcp://ipAddressOrHostName:61616</code>.</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>Port on the target to use for this test. The system pre-populates this field with the default port for the selected credential type.</td>
<td>All</td>
</tr>
<tr>
<td>MID Server</td>
<td>MID Server to use for this test. You must use a Windows MID Server to test Windows credentials. Only Up and Validated MID Servers are available.</td>
<td>All</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Credential type</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>DB Type</td>
<td>Type of database on which to test these credentials.</td>
<td>JDBC</td>
</tr>
<tr>
<td>DB Name</td>
<td>Name of the database on which to test these credentials.</td>
<td>JDBC</td>
</tr>
<tr>
<td>Initial Context Factory</td>
<td>Name of the JNDI class that is used to create the InitialContext. Using this initial context factory, various JMS objects, such as JMS Connection, are created. For example, to connect to ActiveMQ V5.10, (JMS Provider), the value in this field would be org.apache.activemq.jndi.ActiveMQInitialContextFactory</td>
<td>JMS</td>
</tr>
</tbody>
</table>

6. Click OK to begin the test.

An indicator appears, showing that the system is attempting to contact the target using the credentials you have provided. When the instance connects to the target it displays a success message. If the instance encounters a problem with the test inputs you have provided, it displays the appropriate error message. The following are some common error messages.

- Incorrect target or port number:

![TCP connection failure](image)

- Incorrect user name or password:

![Authentication failure](image)

- Incorrect MID Server for Windows credentials:
7. Click **Retry** to open the test Credential dialog box and correct the input error.
8. When your credentials test is successful, click **Submit** to save the record.

---

**Important:** Testing credentials does not ensure that the credentials have the necessary privileges required for the intended Discovery or Orchestration workflow tasks.

---

### Credential affinity for Discovery and Orchestration

Credential affinity is an association between a set of credentials and a device on your network. When Discovery or Orchestration first attempts to access a device, they try all available credentials until they find the correct ones. After identifying the credentials for a device, Discovery and Orchestration create an affinity between the credentials and the device using the Credential Affinity `dscy_credentials_affinity` table. All subsequent discoveries or Orchestration activities attempt to match the credentials in this table with a device for which an affinity exists. If credentials for a device change, Discovery and Orchestration try all available credentials again until they create a new affinity.

Note: If Orchestration and Discovery are installed, and **credential tagging** is enabled, multiple affinities can exist. In this case, the platform looks up credentials for each affinity and inserts the credential for the affinity with the lowest order into the probe.
Credential tagging for Orchestration activities

Credential tagging gives an administrator more control over the credentials used in Orchestration activities.

This is useful when an activity requires specific credentials to perform a task. You can use a credential tag to assign individual credentials to any activity in an Orchestration workflow or assign different credentials to each occurrence of the same activity type in an Orchestration workflow.

Credential tagging interacts with credential affinity to determine which credentials should be used for an Orchestration activity.

How credential tagging works

A business rule called Insert Discovery Affinity (renamed from Insert Credential Affinity in the Geneva release) runs when a record is inserted into the ECC Queue. This rule determines whether a credential affinity exists for the device and identifies the proper credential_id (the sys_id of the record in the Credentials [discovery_credentials] table) to use. When the platform encounters an affinity with a credential tag value defined (credential_tag in the business rule), the business rule determines if the credential referenced by the affinity has the specified tag. If it does, the business rule selects the credential_id of the tagged credential and passes that value to the MID Server. If the credential does not have the specified tag, any other affinities that exist for the target system will be checked. If no affinity references an appropriately tagged credential, the MID Server iterates through the Credentials (discovery_credentials) table and selects the credential with the appropriate tag. The MID Server then creates a new affinity for this credential.
Orchestration credential tagging logic

Check IP service affinity for Discovery and Orchestration

You can check the IP Services table for a list of IP addresses that are associated with a protocol. Role required: admin

The IP Services table maps a port to a protocol. Several mappings are provided by default for commonly used port-protocol combinations, such as port 80 for HTTP, port 22 for SSH, and port 161 for SNMP.
A system property called `glide.discovery.ip_service_affinity` allows Discovery to remember the last port of the IP address that was discovered. This property is set to `false` by default.

**Caution:** You should not modify IP services unless your organization uses custom ports.

1. Navigate to Discovery > Discovery Definition > IP Services.
2. Filter the list to find the appropriate IP service.
3. Click the name of the service to go to that IP service page.
4. Click the IP Service Affinities tab for the list of IP addresses associated with that service.
IP Service Affinities

Name: snmp
Service name: Simple Network Management Prot
Port: 161
Protocol: UDP
Creates: -- None --

Available on:
IP Service Affinities (2)

IP service = snmp

<table>
<thead>
<tr>
<th>IP address</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.191.1</td>
<td>global</td>
</tr>
<tr>
<td>192.168.1.1</td>
<td>global</td>
</tr>
</tbody>
</table>

Actions on selected rows...
External credential storage

An instance can store credentials used by Discovery, Orchestration, and Service Mapping in an external credential repository rather than directly in a ServiceNow credentials record.

The instance maintains a unique identifier for each credential, the credential type (such as SSH, SNMP, or Windows), and any credential affinities. The MID Server obtains the credential identifier from the instance, and then uses a customer-provided JAR file to resolve the identifier from the repository into a usable credential. Currently, the ServiceNow® platform supports the use of the CyberArk vault for external credential storage.

Components installed with External Credential Storage

Business rule

The External Credential Storage business rule performs the following tasks when an administrator makes any change to the external credential storage property:

- Changes the view for the Credentials record list and form to the External Storage view. This view enables users to see the Credential ID column in the list.
- Instructs the MID Server to refresh its credentials cache in preparation for a change in the way credentials are obtained.

Property

A property called Enable External Credential Storage (com.snc.use_external_credentials) enables or disables the External Credential Storage plugin after it is activated. The property is located in Discovery Definition > Properties and Orchestration > MID Server Properties, and is enabled when you activate the plugin.

If you disable external credential storage with the system property, the system automatically sets all the external credentials to inactive in the instance. If you re-enable the feature with this property, the system does not reset the external credential records to active. You must reactivate each credential record manually.

External credential storage log

The MID Server posts log messages about external credential storage.

If the repository encounters an error while attempting to resolve a credentials request, the MID Server posts log messages with this prefix: Problem with client's CredentialResolver:

Activate external credential storage for Discovery and Orchestration

The External Credential Storage 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

| 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 timezone, 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 |
| Any information that would be helpful for the ServiceNow personnel activating the plugin such as if you need the plugin activated at a specific time instead of during one of the default activation windows. |

3. Click **Submit**.

**External credential storage architecture**

External credential storage requires a properly configured MID Server to retrieve the credentials from the external store.

**Credential process flow**

The MID Server retrieves credentials from an external store using this process:

1. MID Server downloads credential objects from the ServiceNow Credentials (discovery_credentials) table that contain the corresponding credential ID from the target vault.

2. MID Server checks to see if there are probes to execute from Discovery or Orchestration jobs.

3. MID Server determines if the relevant credentials, such as SSH, Windows or SNMP, are available for the specified probe target. If not, the MID Server uses the Credential Resolver JAR to make a call to the vault to get the actual user name and password. The details about the correct credential object to retrieve from the vault are determined by the Credential Resolver JAR file. Information such as credential ID, target IP address, or credential type are available to the JAR file. If a credential has been retrieved from a previous probe, the credential is cached and is not retrieved again, unless the MID Server is restarted or specifically directed to flush the credential cache.

4. MID Server executes the probe with the appropriate credential.

**Note:** Credential affinity still applies. The mechanism remains the same, since the only real difference from the MID Server’s perspective is that the real credential details (user name and password) come from the third party vault.
Architecture

```
© 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 AWS credentials on a CyberArk vault

Configure your CyberArk vault with the AWS credentials to be retrieved for use by your instance. Store the credentials as an SSH key on the CyberArk vault. When you configure access to the vault on your instance, the name you give to the SSH key must also be used as the credential ID.

1. In CyberArk, go to **Accounts > Add SSH Key**.
2. Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Type</strong></td>
<td>Select <strong>Cloud Service</strong>.</td>
</tr>
<tr>
<td><strong>Platform Name</strong></td>
<td>Select <strong>Amazon Web Services - AWS - Access Keys</strong>.</td>
</tr>
<tr>
<td><strong>AWS Access Key ID</strong></td>
<td>Enter the AWS Access Key, as provided by AWS.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Enter the AWS Secret Access Key, as provided by AWS.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Enter a name for this key.</td>
</tr>
</tbody>
</table>

3. Choose **Save**.

If you have not done so already, create a credential identifier on your instance to configure access to the CyberArk vault. For more details, see **Configure access to external credential storage for AWS**.

External credential storage configuration

Configure your instance to obtain credentials from a remote repository.

These procedures assume that you already have an external repository configured with the credentials you want to protect. The credential identifier configured in the ServiceNow instance must be mapped to the actual credential in the repository through the JAR file.

To configure External Credential Storage, complete these tasks in order:

Create a JAR file to resolve credentials

Create a JAR file to resolve credential identifiers sent from the MID Server into actual credentials from the repository.

Make sure to include all the credential elements that the instance expects, such as the private key.

To create a JAR file to resolve credentials:

1. Use this sample Java file as a template:

```java
package com.snc.discovery;

import java.util.*;
import java.io.*;
/**

```
public class CredentialResolver {
    
    private static String ENV_VAR = "CREDENTIAL_RESOLVER_FILE";
    private static String DEFAULT_PROP_FILE_PATH = "C:\dummycredentials.properties";

    // These are the permissible names of arguments passed INTO the resolve()
    // method.

    // the string identifier as configured on the ServiceNow instance...
    public static final String ARG_ID = "id";

    // a dotted-form string IPv4 address (like "10.22.231.12") of the target
    // system...
    public static final String ARG_IP = "ip";

    // the string type (ssh, snmp, etc.) of credential as configured on the
    // instance...
    public static final String ARG_TYPE = "type";

    // the string MID server making the request, as configured on the
    // instance...
    public static final String ARG_MID = "mid";

    // These are the permissible names of values returned FROM the resolve()
    // method.

    // the string user name for the credential, if needed...
    public static final String VAL_USER = "user";

    // the string password for the credential, if needed...
    public static final String VAL_PSWD = "pswd";

    // the string pass phrase for the credential if needed:
    public static final String VAL_PASSPHRASE = "passphrase";

    // the string private key for the credential, if needed...
    public static final String VAL_PKEY = "pkey";

    // the string authentication protocol for the credential, if needed...
    public static final String VAL_AUTHPROTO = "authprotocol";

    // the string authentication key for the credential, if needed...
    public static final String VAL_AUTHKEY = "authkey";

    // the string privacy protocol for the credential, if needed...
    public static final String VAL_PRIVPROTO = "privprotocol";

    // the string privacy key for the credential, if needed...
    public static final String VAL_PRIVKEY = "privkey";

    private Properties fProps;
    public CredentialResolver() {
        fProps = new Properties();
        fProps.load(new FileInputStream(DEFAULT_PROP_FILE_PATH));
    }
}
private void loadProps() {
    if (fProps == null)
        fProps = new Properties();

    try {
        String propFilePath = System.getenv(ENV_VAR);
        if (propFilePath == null) {
            System.err.println("Environment var "+ENV_VAR+" not found. Using default file: "+DEFAULT_PROP_FILE_PATH);
            propFilePath = DEFAULT_PROP_FILE_PATH;
        }

        File propFile = new File(propFilePath);
        if (!propFile.exists() || !propFile.canRead()) {
            System.err.println("Can't open "+propFile.getAbsolutePath());
        } else {
            InputStream propsIn = new FileInputStream(propFile);
            fProps.load(propsIn);
        }
        //
        fProps.load(CredentialResolver.class.getClassLoader().getResourceAsStream("dummycredentials.properties"));
    } catch (IOException e) {
        System.err.println("Problem loading credentials file:");
        e.printStackTrace();
    }
}

/**
 * Resolve a credential.
 */
public Map resolve(Map args) {
    loadProps();
    String id = (String) args.get(ARG_ID);
    String type = (String) args.get(ARG_TYPE);
    String keyPrefix = id+"."+type+".";

    if(id.equalsIgnoreCase("misbehave"))
        throw new RuntimeException("I've been a baaaaaaaaaad CredentialResolver!");

    // the resolved credential is returned in a HashMap...
    Map result = new HashMap();
    result.put(VAL_USER, fProps.get(keyPrefix + VAL_USER));
    result.put(VAL_PSWD, fProps.get(keyPrefix + VAL_PSWD));
    result.put(VAL_PKEY, fProps.get(keyPrefix + VAL_PKEY));
    result.put(VAL_PASSPHRASE, fProps.get(keyPrefix + VAL_PASSPHRASE));
    result.put(VAL_AUTHPROTO, fProps.get(keyPrefix + VAL_AUTHPROTO));
    result.put(VAL_AUTHKEY, fProps.get(keyPrefix + VAL_AUTHKEY));
    result.put(VAL_PRIVPROTO, fProps.get(keyPrefix + VAL_PRIVPROTO));
    result.put(VAL_PRIVKEY, fProps.get(keyPrefix + VAL_PRIVKEY));

    System.err.println("Resolving credential id/type["+id+"/"+type+"] ->"+
    "+result.get(VAL_USER)+"/"+result.get(VAL_PSWD)+"/"+result.get(VAL_PASSPHRASE)+"/"+
    "+result.get(VAL_PKEY)+"/"+result.get(VAL_AUTHPROTO)+"/"+result.get(VAL_AUTHKEY)+"/"+
    "+result.get(VAL_PRIVPROTO)+"/"+result.get(VAL_PRIVKEY));

    return result;
}
```java
/**
 * Return the API version supported by this class.
 */
public String getVersion() {
    return "1.0";
}

public static void main(String[] args) {
    CredentialResolver obj = new CredentialResolver();
    obj.loadProps();
    System.err.println("I spy the following credentials: ");
    for (Object key: obj.fProps.keySet()) {
        System.err.println(key +": " + obj.fProps.get(key));
    }
}
```
# Md5 Authorization with no Privileges
User2.snmpv3.user=user2
User2.snmpv3.authprotocol=md5
User2.snmpv3.authkey=1234567890abcdef

# Sha Authorization with no Privileges
User3.snmpv3.user=user3
User3.snmpv3.authprotocol=sha
User3.snmpv3.authkey=1234567890abcdef

# Authorization with Privileges
User4.snmpv3.user=user4
User4.snmpv3.authprotocol=md5
User4.snmpv3.authkey=1234567890abcdef
User4.snmpv3.privprotocol=aes_128
User4.snmpv3.privkey=1234567890abcdef

Import a JAR file to resolve credentials

Import a JAR file created to resolve credential identifiers sent from the MID Server into actual credentials from the repository.

After you create the JAR file, import it into the instance, where it becomes accessible to the MID Server.

1. After creating the JAR and properties files, copy the properties file to the MID Server.
2. Navigate to MID Server > JAR Files.
3. Click New.
4. Complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique and descriptive name for identifying the file in the instance.</td>
</tr>
<tr>
<td>Version</td>
<td>A version number for the file, if one is available.</td>
</tr>
<tr>
<td>Source</td>
<td>Location of the JAR file for reference purposes. Source information is not used by the system.</td>
</tr>
<tr>
<td>Description</td>
<td>Short description of the JAR file and its purpose in the instance.</td>
</tr>
</tbody>
</table>

5. Click the paper clip icon in the banner and attach the JAR file to the record.

6. Click Submit.
7. Restart the MID Server service.
The platform makes the JAR file available to any MID Server configured to communicate with the instance.

**Configure the credential identifier**

Configure the credential identifier in the instance.

Role required: admin

Verify the following items:

- The External Credential Storage plugin must be active.
- The Enable External Credential Storage Discovery property is enabled.

1. Navigate to Discovery > Credentials or Orchestration > Credentials.
2. Click New.
3. Select a credential type.
4. Select the External credential store check box.
   The User name and Password fields disappear, and the Credential ID field appears.
5. Complete the Credentials form using the fields from the table.
6. Click Submit.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique and descriptive name for this credential.</td>
</tr>
<tr>
<td>Active</td>
<td>Enable or disable these credentials for use.</td>
</tr>
</tbody>
</table>
| Credential ID | Enter the unique key configured for external credentials in the JAR file uploaded to the MID Server for an external credential system. This is the ID passed to the Java class in the parameter map:  

```java
public static final String ARG_ID   = "id";
```

The MID Server uses this identifier to resolve the actual credentials on the repository.

**Note:** This field is only visible when the External credential store check box is selected.

| Tag          | Allow workflow creators to assign individual credentials to any activity in an Orchestration workflow or assign different credentials to each occurrence of the same activity type in an Orchestration workflow. |
### Configure the credential identifier for AWS

Configure your instance to obtain credentials from a remote repository.

**Role required:** cloud_admin

Verify that the External Credential Storage plugin and Amazon Web Services plugin have been activated and the MID server has been installed.

These procedures assume that you already have an external repository configured with the credentials you want to protect. The credential identifier configured in the ServiceNow instance must be mapped to the actual credential in the repository through the JAR file.

1. Navigate to **Amazon AWS Cloud > Configuration > Accounts**.
2. Select the appropriate account.
3. In the **AWS Credentials** related list, click **New** and fill in the form, as appropriate.

#### AWS Credentials

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique and descriptive name for this credential. For example, Amazon Web Services.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Active</td>
<td>Check box to enable or disable the credential.</td>
</tr>
<tr>
<td>AWS Account</td>
<td>Master AWS account to which this credential belongs.</td>
</tr>
<tr>
<td>External credential store</td>
<td>Select this check box to use an external credential storage system. When you select this checkbox, the Access Key ID and the Secret Access Key fields disappear and are replaced by Credential ID and MID servers.</td>
</tr>
<tr>
<td>Credential ID</td>
<td>Enter the Name as stored in CyberArk.</td>
</tr>
<tr>
<td>MID servers</td>
<td>Select one or more MID Servers.</td>
</tr>
</tbody>
</table>

4. Click Submit.

**CyberArk credential storage integration**

The MID Server integration with the CyberArk vault enables Orchestration, Discovery, and Service Mapping to run without storing any credentials on the instance.

**Introduction to CyberArk**

CyberArk’s Application Identity Management (AIM) product uses the Privileged Account Security solution to eliminate the need to store application passwords embedded in applications, scripts or configuration files, and allows these highly-sensitive passwords to be centrally stored, logged and managed within the CyberArk vault. This approach enables organizations to comply with internal and regulatory requirements of periodic password replacement and to monitor activities associated with all types of privileged identities, whether on-premise or in the cloud.

The instance maintains a unique identifier for each credential, the credential type (such as SSH, SNMP, or Windows), and any credential affinities. The MID Server obtains the credential identifier, credential type, and IP address from the instance, and then uses the CyberArk vault to resolve these elements into a usable credential.

The CyberArk integration requires the ServiceNow® External Credential Storage plugin, which is available by request.

**Installed with CyberArk**

- **Business rule**: The External Credential Storage business rule performs the following tasks when an administrator makes any change to the external credential storage property:
  - Changes the view for the Credentials record list and form to the External Storage view. This view enables users to see the Credential ID column in the list.
  - Instructs the MID Server to refresh its credentials cache in preparation for a change in the way credentials are obtained.

- **System property**: A property called Enable External Credential Storage (com.snc.use_external_credentials) enables or disables the External Credential Storage plugin after it is activated. This property is located in Discovery Definition > Properties and Orchestration > MID Server Properties, and is enabled when you activate the plugin.
**Note:** If you disable external credential storage with the system property, the system automatically sets all the external credentials to inactive in the instance. If you re-enable the feature with this property, the system does not reset the external credential records to active. You must reactivate each credential record manually.

---

**Supported credential types**

The CyberArk integration supports these ServiceNow credential types:

- CIM
- JMS
- SNMP Community
- SSH
- SSH Private Key (with key only)
- VMware
- Windows

Orchestration activities that use these network protocols support the use of credentials stored on a CyberArk vault:

- SOAP (with basic authentication overrides)
- REST (with basic authentication overrides)
- JDBC
- SSH
- PowerShell
- JMS
- SFTP

**Important:** You cannot manage credentials stored on a CyberArk vault and a custom external credential storage system using the same MID Server. To use both types of external storage, install and configure a dedicated MID Server for each. The MID Server must be installed on the same machine as the CyberArk AIM API/client.
CyberArk architecture
How the MID Server handles Windows accounts

Credential lookup initially attempts to match the specified credential ID to an existing value in the CyberArk vault Name field. If a match is found, that credential is returned. If no match is found, the credential lookup attempts to find a match using the IP address. If the IP address lookup matches more than one credential, such as Windows and Tomcat on the same server, the lookup fails. To avoid this issue, set the ext.cred.typeSpecifier parameter in the MID Server config.xml file to true to force CyberArk to return credentials that match both the credential type and the IP address. For example, if an IP address is shared by both Windows and Tomcat, a credential type of Windows returns the Windows credential only.

CyberArk integration configuration

These procedures include both CyberArk and ServiceNow configuration tasks, including references to the appropriate CyberArk documentation.

The credential identifier configured in the ServiceNow instance must be mapped to the credential name in the CyberArk vault. When looking up a credential, the MID Server first tries to find the credential by name, which must be unique, and then by IP address. To identify the credential by IP address, the system looks at the credential type to ensure that there is only one credential of that type at that address. An example of this might be when a Windows server and vCenter are both running on the same IP address. To support strict credential requirements like this in an SSH environment, a MID Server configuration parameter allows you to require that the credential type requested matches the type returned by CyberArk.

To configure your instance to obtain credentials from a CyberArk vault, complete these tasks in the order in which they appear below.

Configure the CyberArk vault and install the AIM API

Configure the CyberArk vault to allow MID Server access and install the CyberArk AIM API on the MID Server machine.

Role required: admin

Before starting this procedure, ensure that the External Credential Storage plugin is activated.

1. Configure the CyberArk vault with the application ID and authentication details that all MID Servers requesting credentials will use.

   For details, refer to the CyberArk Credential Provider and ASCP Implementation Guide.
   a) Ensure that CyberArk is configured to allow the MID Server to access the vault by creating an App-ID in CyberArk called ServiceNow_MID_Server.
   b) Make sure that every credential the MID Server needs is granted access to the ServiceNow_MID_Server App-ID.

   Note: You can override the default ServiceNow_MID_Server App-ID in the MID Server config.xml file using the ext.cred.app_id parameter. If you change the value in this parameter, make sure to configure a matching value in the vault.

2. Install the CyberArk Credential Provider, including the AIM API, on each machine that hosts a MID Service server that is used to access the credential store.

3. Provision CyberArk accounts and set permissions for application access.

   For details, refer to the CyberArk Privileged Account Security Implementation Guide.
   a) In the CyberArk Password Safe, create the privileged accounts required by Discovery, Orchestration, or Service Mapping to access different devices and ensure that these accounts are members of the safes in which the necessary credentials are stored.
b) Add the Credential Provider and application users as members of the Password Safes where the application passwords are stored.

**Import the CyberArk JAR file**

Import the CyberArk JavaPasswordSDK.jar file into the instance to make it accessible to the MID Server.

Role required: agent_admin or admin

Before starting this procedure, ensure that CyberArk is configured to allow the MID Server access to credentials. Ensure that the CyberArk AIM API is installed on each server hosting a MID Server that is used to access the vault.

Use this process even if the JavaPasswordSDK.jar file already exists on the MID Server.

1. Navigate to MID Server > JAR Files.
2. Click New.
3. Complete the form using the fields in the table.

<table>
<thead>
<tr>
<th>JAR File form fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique and descriptive name for identifying the file in the instance.</td>
</tr>
<tr>
<td>Version</td>
<td>Optional version number for the file, if one is available.</td>
</tr>
<tr>
<td>Source</td>
<td>Provider of the JAR file. Source information is not used by the system.</td>
</tr>
<tr>
<td>Description</td>
<td>Optional short description of the JAR file and its purpose in the instance.</td>
</tr>
</tbody>
</table>

4. Attach the JAR file to this record.
   
   The AIM JavaPasswordSDK.jar file comes with the AIM SDK installation files and is typically located on the MID Server in the AIM installation directory at `<install_dir>/CyberArk/ApplicationPasswordSdk`.

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.

**Configure the MID Server for CyberArk**

Configure the config.xml file to grant the MID Server access to the CyberArk vault.

Role required: admin

Before starting this procedure, import the JavaPasswordSDK.jar file into the instance.

Manually configure the MID Server config.xml file with these parameters.

This configuration cannot be done from the instance.
### Required configuration parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ext.cred.safe_folder</td>
<td>NameOfFolder</td>
<td>Folder to use for all credential lookups. For example, root.</td>
</tr>
<tr>
<td>ext.cred.use_cyberark</td>
<td>true</td>
<td>Boolean parameter indicating that this MID Server is integrated with CyberArk.</td>
</tr>
</tbody>
</table>

### Optional configuration parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ext.cred.safe_timeout</td>
<td>5 (sec)</td>
<td>Timeout of each credential lookup in the vault, specified in seconds.</td>
</tr>
<tr>
<td>ext.cred.safe_name</td>
<td>NameOfSafe</td>
<td>Default safe name used for all credential lookups. If parameters are in multiple safes, the credential ID may be specified in the format <code>&lt;safeName&gt;:&lt;CredentialID&gt;</code>. When configured like this, the NameOfSafe field is ignored. If all external credentials have their credential IDs specified in this format, then leave out the NameOfSafe field.</td>
</tr>
</tbody>
</table>

**Note:** By default the separator character in this format is a colon. To assign any character you want as a separator, add this line to the CredMap.properties file:

```properties
safe.cred.split.string=<string>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ext.cred.app_id</td>
<td>ServiceNow_MID_Server</td>
<td>Specifies the App-ID used to grant permission to the MID Server to access the CyberArk vault. The default value, ServiceNow_MID_Server, must be defined in the CyberArk vault. You can use this parameter to override the default and specify your own App-ID. If you edit the App-ID in this parameter, make sure to configure CyberArk to match.</td>
</tr>
</tbody>
</table>
## ServiceNow Jakarta Now Platform Capabilities

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ext.cred.type_specifier</td>
<td>true</td>
<td>Forces the lookup to return credentials that match both the CyberArk platform ID and the IP address. For example, if an IP address is shared by both Windows and Tomcat, a credential with a platform ID starting with <strong>Win</strong> returns the Windows credential only. When this parameter is set to true, CyberArk looks for platform IDs that begin with:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Win: Windows</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Unix: SSH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- VMWare: VMware</td>
</tr>
<tr>
<td>ext.cred.check_ssh_type</td>
<td>false</td>
<td>When set to true, requires that the type of SSH credential returned from CyberArk matches the type of credential requested. For example, if a normal SSH username/password credential is requested and only SSH keys are available, the credential lookup fails.</td>
</tr>
</tbody>
</table>

### Configure CyberArk for SNMPv2 credentials

If your system uses SNMPv2, you can create a special file to map the attribute in a credential to the community string.

Role required: admin

Before starting this procedure, configure the MID Server to have access to the CyberArk vault.

**Note:** If the community string appears in the password field of the CyberArk credential, it is not necessary to perform this procedure.

SNMPv2 is not natively supported in CyberArk. If your organization has created custom SNMPv2 credentials in which the community string does not appear in the password field of the credential, use this procedure to map the attribute in the credential to the community string.

1. In a text editor, create a file called `CredMap.properties`, containing this code:
   ```properties```
   ```
   SNMPv2.Community=attribute_name
   ```
2. Save the file to the `/agent` directory of your MID Server installation.

   On credential lookup, the MID Server attempts to find this attribute for the credential. If the attribute is not found, the MID Server then looks in the password field. If the password field is empty, the credential lookup fails.

### Configure the CyberArk credential identifier

Create the unique key that CyberArk can use to identify specific credentials in the external repository.

Role required: admin
Before starting this procedure, ensure that the External Credential Storage plugin is activated, and the `com.snc.use_external_credentials` system property is set to true.

1. Navigate to Discovery > Credentials or Orchestration > Credentials.
2. Click **New**.
3. From the list of credential types, select a type that supports CyberArk external storage.
4. Complete the form using the fields from your credential type.
5. Select the **External credential storage** check box.

The **User name** and **Password** fields are replaced with the **Credential ID** field.

6. In the **Credential ID** field, enter an expression using one of these formats:
   - If all your credentials are in the same safe, configure this safe name in the MID Server `config.xml` file using the `ext.cred.safe_name` parameter, and then specify the credential ID by name only, as `<credential ID>`.
   - To name credentials for a given platform that reside in a specific safe, define the credential ID as `<safe>:<credential ID>:<platform ID>`.
   - If your credentials are in multiple safes, specify the credential ID in this format: `<safe>:\<credential ID>`.
   - If you want CyberArk to look up the credential by IP address, using an alternate safe, specify the credential ID in this format: `<safe>:`.
   - If you want CyberArk to look up the credential for an alternate platform ID in the same safe, use this format: `::<platform ID>`.
   - If you want CyberArk to look up the credential in a configured safe by the IP address rather than the credential ID, leave this field blank. Do this when handling installations in which each server has a unique credential. Without this type of lookup, you must create a credential ID record in your instance for every server in your environment.

   **Note:** The credential ID must match the value in the **Name** field of the credential in the CyberArk vault. The **Credential ID** field has a limit of 40 characters.

7. Click **Submit**.

**Configure AWS credentials on a CyberArk vault**

Configure your CyberArk vault with the AWS credentials to be retrieved for use by your instance.

Store the credentials as an SSH key on the CyberArk vault. When you configure access to the vault on your instance, the name you give to the SSH key must also be used as the credential ID.

1. In CyberArk, go to **Accounts > Add SSH Key**.
2. Enter the following information:

   **CyberArk credentials**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Type</td>
<td>Select <strong>Cloud Service</strong>.</td>
</tr>
<tr>
<td>Platform Name</td>
<td>Select <strong>Amazon Web Services - AWS - Access Keys</strong>.</td>
</tr>
<tr>
<td>AWS Access Key ID</td>
<td>Enter the AWS Access Key, as provided by AWS.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the AWS Secret Access Key, as provided by AWS.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter a name for this key.</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. Choose **Save**.

If you have not done so already, create a credential identifier on your instance to configure access to the CyberArk vault. For more details, see *Configure access to external credential storage for AWS*.

**Credentials troubleshooting**

Review the `<credentials_debug>` section of the ECC queue payload to troubleshoot issues with credentials.

Certain probes support credential debugging, starting with the Istanbul release. Credential debugging inserts a `<credentials_debug>` section in the payload that the MiD Server returns to the instance ECC queue. You can view the `<credentials_debug>` section to see detailed information about the credential lookup.

The `<credentials_debug>` section appears in the payload if:

- Credentials fail for **WMIRunner**, **PowerShell**, **JMS**, or **SSHCommand**.
- You set the `credentials_debug` parameter to `true` for the **WMIRunner**, **PowerShell** or **SSHCommand** probes. If you set the parameter to true, the `<credentials_debug>` section appears even if the credential lookup is successful.

The `<credentials_debug>` section shows:

- Information about the credential search, such as the credential types, tags, and affinities.
- The IP address targeted.
- Information about each credential (in order) that the MiD server used, including the type, classification, tag, name, Sys ID, and external credential ID if present.
Sample payload showing invalid credentials

Additional details appear for PowerShell and SSHCommand:

- For the PowerShell parameter:
  - If the local MID Server credentials were used after all the Windows credentials failed, and also if that succeeded.
  - If the credentials were skipped because you are trying to discover the same machine that the MID Server is on, or if the `mid.powershell.use_credentials` parameter is set to true.

- For the SSHCommand:
  - If the credential search was skipped because the target IP is blacklisted.
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

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-preserving 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 logging
- 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.

Note: The MID Server saves IP addresses for failed credential searches in a blacklist in cache memory. This blacklist specifies which devices the MID Server should stop trying to access. By default, the IP addresses stay on the blacklist for five minutes, or until the credentials change or the MID Server is restarted, which clears the cache. You cannot change this time length.
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.
- **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>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>token_map</td>
<td>Order-preserving encryption 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 NAE.
- 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.

- **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 system. A single Java KeyStore can store multiple keys and the keys are identified by a key alias, making it easier to manage multiple keys.
- **NAE (Network Attached Encryption) key store**: Keys are stored and retrieved with SafeNet's KeySecure key management.
- **File system**: 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.

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.

**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>
</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 customer’s 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.

#### Tables for Edge Encryption

<table>
<thead>
<tr>
<th>Table</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>
</tbody>
</table>
## Table

<table>
<thead>
<tr>
<th>Encryption Job Execution (sys_encryption_job_execution)</th>
<th>Supports mass encryption jobs.</th>
</tr>
</thead>
<tbody>
<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.

**Note:** To open the System Properties (sys_properties) table, enter `sys_properties.list` in the navigation filter.

#### 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 |
### Property Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</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>

### 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

The Edge Encryption proxy application can run on servers or virtual machines running Windows or Linux.

The Edge Encryption proxy distribution comes with JRE 1.8. The base system Edge Encryption proxy uses the JRE bundled with the distribution. You can change this by modifying the `wrapper.java.command` property in the `wrapper.conf` file in the `<installation dir>/conf` directory.

### Proxy server minimum configuration

The minimum configuration includes:

- A minimum of 4 GB of available RAM per proxy server (6 GB is recommended for most deployments).

**Note:** The host machine running the proxy server must have at least 1 more GB of RAM available for OS services than is needed to run the proxy server. Specifically, if a proxy server is set to use 4 GB of RAM, the VM or hardware must have at least 5 GB of RAM installed.

- 3+ GHz CPU, with a 4-core CPU preferred.
- Multiple proxy servers behind a load balancer. The number of proxy servers will depend on the number of application nodes, number of simultaneous users, and failover needs. See [Sizing your Edge Encryption environment](#) for considerations.
- Ability to ride-along with other services, depending on the server utilization and resource availability.
- Java 8 is required to run the installer.
Proxy server supported systems

The following systems are supported.

- Windows Server
  - All Windows Server 2012-R2 editions or later
  - Virtual machines or physical hardware
  - 64-bit systems

- Linux
  - Virtual machines or physical hardware
  - 64-bit systems

**Note:** 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 Jakarta release.

On 64-bit Linux systems, you must install the 32-bit GNU C library (glibc). The installation command for CentOS is: `yum install glibc.i686`

Proxy server connection requirements

The proxy server that runs the Edge Encryption application must be able to communicate with machines in your network. Make sure that the proxy server has these network privileges:

- **Firewall access:** Configure any firewalls between the proxy server and the client devices to allow a connection. If your network uses a DMZ, 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.

- **Network access:** Configure each client to let the proxy server 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.

- **Instance access:** Ensure network access to the instance from the proxy server. Make sure that the network used by the proxy server is configured to allow traffic over TCP port 443.

- **Network account:** Install the proxy server with the proper account, either local or domain administrator.

**Note:** Because the Edge Encryption proxy server resides in your network, its host IP and port may be subject to vulnerability scans by your network software. The Edge Encryption proxy server will forward such scan requests to your ServiceNow instance. To prevent IP scanner or similar requests from being forwarded to your ServiceNow instance, make sure to configure your network scanner to skip the Edge Encryption proxy server port or IP address. Alternatively, you can configure a firewall utility on the host machine to prevent the proxy server from forwarding requests from specific addresses to the instance.

Order-preserving and tokenization database system requirements

Order-preserving encryption and encryption patterns require a MySQL database configured for the Edge Encryption proxy. Use a dedicated machine to run the order-preserving and tokenization database. The minimum requirements include:

- **Version:** MySQL database versions 5.5 to 7.x
- **OS**: 64-bit systems
- **CPU**: 2+ GHz CPU, with a 4-core CPU preferred
- **RAM**: 16 GB
- **Disk**: SAN or local storage (RAID 10 recommended)
- **Size**: Determined by the number of potential records multiplied by record size. Calculate the order-preserving and tokenization database size.
- **Configuration**: High Availability cluster. If you are unsure of how to configure your MySQL server, contact MySQL for configuration information.

### Sizing your Edge Encryption environment

Choosing the number of proxy servers for your environment is an important task. Consider the number of users, redundancy needs, and acceptable latency.

#### Redundancy

Maintain redundant proxy servers in case of hardware failure. Proxy servers should be located behind a load balancer to provide a functional path for all users if a proxy server is unreachable. At a minimum, ensure that two proxy servers are always available.

#### Size

Size refers to the number of proxy servers required to avoid additional latency that the encryption of data produces. Depending on use, you may want to reduce the amount of latency by adding additional proxy servers. For example, if regular mass encryptions are run, add additional proxy servers to handle the load, or run the mass encryptions when the user load is light. In addition, the hardware that the proxy server runs on influences performance and latency. Proxy servers running on hardware with faster CPUs, more CPUs, and more RAM have higher throughput than slower, limited systems.

The following guidelines assume that your proxy server is running on at least the minimum hardware requirements. To determine the number of proxy servers:

- Consider setting up one proxy server for every two application nodes on the instance.
- For redundancy, set up a minimum of two proxy servers behind a load balancer.
- Add an extra proxy server for every 500 simultaneous users.
- Depending on the desired redundancy, add additional proxy servers for failover.

For example, for an instance with 2,000 users, you should have at least five proxy servers behind a load balancer. This calculation includes one proxy server for every 500 users, with an extra proxy server for failover. Determine ahead of time when you will approach a threshold of 500 users and place another proxy server in the load balancer pool.

#### Load balancers

To balance requests and improve server response time, distribute proxy servers in a load balancer pool. Configure load balancers to use the "least connections" method. This method connects requests to the proxy server with the fewest active connections, preventing the overloading of a single proxy.
CPU utilization

Because data encryption and tokenization are CPU intensive operations, CPU spikes while encrypting data are normal and expected. When CPU utilization is over 80% for several minutes at a time, it likely means that the proxy server has too much work to do. When this happens, latency increases for the period that the CPU utilization is high. If latency persists, adding another proxy server may help decrease the latency.

Memory

The proxy server must have a minimum of 4 GB of RAM available (6 GB recommended). Set the proxy server initial and upper bound memory limits to the recommended settings.

Calculate the order-preserving and tokenization database size

If using order-preserving encryption or encryption patterns, determine the size of your MySQL database by multiplying the number of potential records by record size.

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.

- Only string fields can be encrypted. Choice fields, virtual fields, journal fields, and any fields other than string fields cannot be encrypted. See Field types for more information.
- String fields that include more than five multi-byte characters cannot be encrypted.
- 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.
- Encrypted fields are not available in Go to and header filter boxes.
ServiceNow    Jakarta    Now Platform Capabilities

- 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 short description in the Incident table is marked to be encrypted, then 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, and SafeNet, 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.

© 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 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.

Integration restrictions

Restrictions on data integrations with Edge Encryption.

- Attachments uploaded via REST or SOAP cannot be uploaded to tables marked for attachment encryption.
- Importing data from or exporting data to Excel, CSV, XML, or other file types to or from fields with encryption configurations defined is not supported.

Edge Encryption installation

You can install an Edge Encryption proxy manually or using the Edge Encryption installer.

Installing Edge Encryption includes these steps.

- Install the Edge Encryption proxy application on a server in your network.
- 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>edgeencryption.proxy.host</td>
<td>hostname.mycompany.com</td>
</tr>
<tr>
<td>edgeencryption.proxy.http.port</td>
<td>8081</td>
</tr>
</tbody>
</table>

A client will access the proxy server using the following address: `http://hostname.mycompany.com:8081/`.

**Note:** DNS settings and routing rules may be used. Host and port values are determined by your network administrator.
Request Edge Encryption

The Edge Encryption plugin (com.glide.edgeencryption) is available as a separate subscription.

To purchase a subscription, contact your ServiceNow account manager. The account manager can arrange to have the plugin activated on your organization's production and 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 timezone, 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 | Any information that would be helpful for the ServiceNow personnel activating the plugin such as if you need the plugin activated at a specific time instead of during one of the default activation windows. |

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.

   ![Download Edge Encryption Proxy Server]

   **Interactive Installer:**
   Download

   Refer to using the Installer for details.

   **Manual Installation:**
   Refer to the installation instructions for details.

   ![Linux 64 bit]

   ![Windows 64 bit]

   **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 Jakarta 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 installer. If installing manually, Manually install the Edge Encryption proxy server.

**Install the Edge Encryption proxy server using the installer**

You can install the Edge Encryption proxy server on a Windows or Linux computer using the installer.

The Edge Encryption plugin must be installed and activated on your instance before you start this procedure. Ensure that Java 8 is installed on the machine running the Edge Encryption installer.
Role required: security_admin on your ServiceNow instance and local administrator on the host machine.

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.

Use the installer to install multiple proxies for your instance on multiple machines, ensuring the following criteria applies:

- 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.

**Note**: SafeNet KeySecure keystore files are not supported by the Edge Encryption installer. To use a SafeNet KeySecure keystore, manually install the proxy server.

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**

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.
      
      ![URL Example](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><em>Note:</em> Click Detect FQDN to look up the machine’s fully qualified domain name and auto-populate the Proxy Host field.</td>
</tr>
<tr>
<td></td>
<td>Along with the port, this property defines the URL used by the client to access the proxy server.</td>
</tr>
<tr>
<td>HTTP Port</td>
<td>Port on the proxy for HTTP communication.</td>
</tr>
<tr>
<td>HTTPS Port</td>
<td>Port on the proxy for HTTPS communication.</td>
</tr>
<tr>
<td>Proxy Name</td>
<td>Name of the proxy and the service. The proxy name must be unique.</td>
</tr>
<tr>
<td>Proxy Poll Interval</td>
<td>Poll interval in seconds. With the default setting, it takes 5 seconds for the proxy to learn of encryption configuration changes. Larger values cause the instance to take longer to detect proxies that have come online.</td>
</tr>
<tr>
<td></td>
<td><em>Note:</em> 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 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 128-bit encryption key

After the HTTPS certificate is configured 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 128-bit and 256-bit encryption keys, they must both use the same keystore.

1. Select the location to store the encryption key.
   - **File Store**: 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.
     
     **Note**: This step selects both the key storage and the encryption key. If **File Store** is selected, click **Next** and go to step 5.
   
   - **Create New Java KeyStore**: Create a keystore to store the encryption key.
   - **Java KeyStore File**: Store the encryption key in an existing Java KeyStore file.

2. Click **Next**.

3. Select or create the encryption key.
   - **New Key**: Create an encryption key and alias.
     
     **Note**: 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 [Java SE Documentation](https://docs.oracle.com/javase/8/docs/technotes/tools/?keytool).
   
   - **Use Existing Key**: Use an existing encryption key in the selected keystore.
   - **Import Existing Key**: Import an encryption key from a different keystore.

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 256-bit encryption key

After the 128-bit key is configured through the Edge Encryption proxy installer, you can optionally configure the AES 256-bit encryption key and set it as the default 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 128-bit and 256-bit encryption keys, they must both use the same keystore. If you do not want to configure a 256-bit encryption key, click Skip.

1. Select the encryption key location.
   - **File Store**: 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.

   **Note:** This step selects both the key storage and the encryption key. If File Store is selected, click Next and go to step 5.

   - **Create New Java KeyStore**: Create a keystore to store the encryption key.
   - **Java KeyStore File**: Store the encryption key in an existing Java KeyStore file.

2. Click Next.

3. Select or create the encryption key.
   - **New Key**: Create an encryption key and alias.
   
   **Note:** 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 Java SE Documentation.

   - **Use Existing Key**: Use an existing encryption key in the selected keystore.
   - **Import Existing Key**: Import an encryption key from a different keystore.

4. Click Next.

5. Install the Java Cryptography Extension (JCE) and overwrite the policy files on the proxy server. See Enable AES 256-bit encryption.

6. Configure the 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 (optional)

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.
Edge Encryption proxy installation tests

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.

**Manually install the Edge Encryption proxy server**

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.

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**

You can 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.

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 the appropriate command for the target machine and change the variables according to your configuration.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td><code>java -jar edgeencryption-dist-&lt;version&gt;-windows-x86-64.zip</code> <code>-m install -n &lt;ProxyName&gt; --instancehost &lt;host&gt; -p &lt;port&gt; --protocol https</code></td>
</tr>
<tr>
<td>Linux</td>
<td><code>java -jar edgeencryption-dist-&lt;version&gt;-linux-x86-64.zip</code> <code>-m install -n &lt;ProxyName&gt; --instancehost &lt;host&gt; -p &lt;port&gt; --protocol https</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>version</td>
<td>The version number of the Edge Encryption release.</td>
</tr>
<tr>
<td>ProxyName</td>
<td>The name of the encryption proxy instance.</td>
</tr>
<tr>
<td>host</td>
<td>Your instance.</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>port</td>
<td>The port of your instance. When the protocol is https, the port is normally 443.</td>
</tr>
</tbody>
</table>

To see the help screen, execute the appropriate command without arguments:
- **Windows**: `java -jar edgeencryption-dist-<version>-windows-x86-64.zip`
- **Linux**: `java -jar edgeencryption-dist-<version>-linux-x86-64.zip`

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</td>
<td>Proxy server description.</td>
</tr>
</tbody>
</table>

   If this step is not performed, the Edge Encryption proxy service installs 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`.

```
keytool -keystore keystore.jceks -storetype jceks -storepasswd -new
    <newpassword>
```

3. Create an encryption key pair.

   **Note:** Do not enter a password for the key when the keytool utility prompts for one.

   Enter this command on a single line.

```
keytool -genkeypair -alias <key alias> -keyalg rsa -keystore
    keystore.jceks -storetype jceks -storepass <keystore password> -keysize 2048
```

4. Update the encryption proxy property file (`edgeencryption.properties`).
   a) Change to the `<installation directory>/conf/` directory.
   b) Open the `edgeencryption.properties` file.
   c) Enter the properties for the `digital signature`.

   These properties must be the same for all proxies.

5. Save and close the `edgeencryption.properties` file.

**Import and configure the certificate for secure SSL connection**

To use a secure SSL connection, import a server certificate and add it to the Java KeyStore.

You must obtain the server certificate before you can add it to the Java KeyStore.

1. Add a server certificate to the Java KeyStore.

   **Table:**
<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</td>
<td>keytool -import -alias typename -file server.cert -storetype JCEKS -keysize 2048</td>
</tr>
<tr>
<td>the certificate from that key.</td>
<td>keystore keystore.jceks -storepass &lt;keystore password&gt;</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>If you have a PKCS12 (.pfx) file that contains the RSA key and the</td>
<td>keytool -importkeystore -destkeystore keystore.jceks -deststoretype jceks -keysize 2048</td>
</tr>
<tr>
<td>certificate.</td>
<td>deststoretype jceks -srcstoretype &lt;PKCS12 filename&gt; -srcstoretype pkcs12</td>
</tr>
</tbody>
</table>

Make sure that the private key password is the same as the Java KeyStore password.

You can run this command to change the password.

```
keytool -keypasswd -keystore keystore.jceks -alias <key alias>
```

For testing, you can use this command to generate a self-signed certificate.

```
keytool -genkeypair -alias cert -keystore keystore.jceks -storetype jceks -keyalg rsa
```

2. Update the `edgeencryption.properties` file.
   a) Change to the `<installation directory>/conf/` directory.
   b) Open the `edgeencryption.properties` file.
   c) Enter the properties for the `SSL certificate`.

© 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 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

If you want to use AES 256-bit encryption, you must install the Java Cryptography Extension (JCE) jurisdiction policy files by copying them into each Edge Encryption proxy installation directory.

Edge Encryption ships with the AES 128-bit policy files, which you must overwrite with the AES 256-bit policy files. It is only necessary to download the JCE once, but every Edge Encryption proxy must be updated.

1. Download the JCE policy 8 ZIP file from Oracle.
2. Unzip the file.
3. On each proxy server, copy the local_policy.jar and US_export_policy.jar files into the <proxy-dir>/java/jre/lib/security folder.

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>Java KeyStore</strong></td>
<td>A Java KeyStore:</td>
</tr>
<tr>
<td></td>
<td>• Stores keys in a Java JCEKS KeyStore.</td>
</tr>
<tr>
<td></td>
<td>• Is password protected and more secure than storing keys in a file in the file system.</td>
</tr>
<tr>
<td></td>
<td>• Can store multiple keys. A key alias represents each key, making it easier to manage multiple keys.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>NAE (Network Attached Encryption) key store</strong></td>
<td>Keys are stored and retrieved with SafeNet KeySecure key management.</td>
</tr>
<tr>
<td></td>
<td>You must secure a license with Gemalto, download the libraries, and install the SafeNet KeySecure keystore on a host machine in your network before configuring the keystore on the Edge Encryption proxy server.</td>
</tr>
<tr>
<td><strong>File system</strong></td>
<td>Keys are stored in a file in a file system accessed by the Edge Encryption proxy server.</td>
</tr>
<tr>
<td></td>
<td>Because encryption keys stored in a file are not encrypted, it is your responsibility to protect these files.</td>
</tr>
</tbody>
</table>
2. Set up the keystore and encryption keys in your local network.

Set up a Java KeyStore keystore
You can use a Java KeyStore keystore to store encryption keys.

You must use the Java 1.8 version of the keytool utility. A copy of the utility can be found in `<proxy install dir>/java/jre/bin/keytool`.

The Edge Encryption proxy ships with the Java JCEKS KeyStore file named `keystore.jceks` in the `keystore` directory. This keystore file contains the ServiceNow public key used to validate encryption rules signed by ServiceNow.

1. Set up the keystore properties.
   a) Change to the `<installation directory>/conf/` directory.
   b) Open the `edgeencryption.properties` file.
   c) Enter the properties for the Java KeyStore.

2. Save and close the `edgeencryption.properties` file.

After setting up the Java KeyStore, Create encryption keys using the Java KeyStore keytool.
Create encryption keys using the Java KeyStore keytool
You can use the keytool shipped with the encryption proxy distribution to create AES 128-bit and AES 256-bit encryption keys.

You must use the Java 1.8 version of the keytool utility. A copy of the utility can be found in `<proxy install dir>/java/jre/bin/keytool`.

To find out more about the keytool utility, see the Java SE Documentation.

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><code>keytool -genseckey -alias 128bitkey -keyalg aes -keysize 128 -keystore keystore.jceks -storetype jceks</code></td>
</tr>
<tr>
<td>AES 256</td>
<td><code>keytool -genseckey -alias 256bitkey -keyalg aes -keysize 256 -keystore keystore.jceks -storetype jceks</code></td>
</tr>
</tbody>
</table>

You add the alias on the instance when you assign default keys.
**Note:** The key password must be the same as the keystore password.

Set up a SafeNet KeySecure keystore
If you are using a SafeNet keystore, copy a set of libraries into the proxy distribution directory.
You must install and set up the SafeNet keystore before performing this step. Secure a license with Gemalto in order to download the libraries.

**Note:** On Linux, file paths use a forward slash.

1. Copy these files to `<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.

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, you must do the following.

1. Create the encryption key.
2. Make the new key available to all encryption proxies. You can accomplish this by either copying the file or Java KeyStore file to each proxy, or ensuring that each proxy has access to the Java KeyStore or NAE 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
   The Encryption Key Configuration - Created form is shown.
2. Add new keys
   Rows in the list with an X in the left column can be deleted. Keys that have been used as the default, or are in the Available state cannot be deleted.
   a) In the row that says Insert a new row... double-click.
      An edit box is shown.
   b) 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 Submit. Key aliases must be unique.
   c) In the same row, double-click in the Key size column.
      A select box is shown.
   d) 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.
      A select box is shown.
   f) Select a key type, either File, Keystore, or SafeNet, 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. The form moves to the Key Status step.

3. When the key status becomes Available, click Next Step.
The instance tracks the status of every encryption key available to any proxy. When a key alias is available on all proxies, its state becomes **Available**. If, after a few minutes, the state does not change, 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 alias.

### Encryption key states

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available</td>
<td>All online proxies have the key.</td>
</tr>
<tr>
<td>Unavailable</td>
<td>This is a new key and the proxies have not yet loaded the key, or at least one proxy failed to load the key.</td>
</tr>
</tbody>
</table>

4. On the **Change Default Keys** tab, either type in the key alias, or click the spy glass icon and select an alias, and then click **Next Step**.
   The form moves to the **Schedule Key Rotation** step.

5. If desired, create and run a mass encryption job to encrypt existing data using the new encryption key.
   If you do not run a mass encryption 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**

```java
wrapper.java.additional.1 = -Djava.io.tmpdir=../tmp
wrapper.java.additional.2 = -Dcloudedge.home.dist=..
# must ensure UTF8 encoding when running on Windows
wrapper.java.additional.3 = -Dfile.encoding=UTF8
# additional properties for heap settings
wrapper.java.additional.4 = -Xms6144m
wrapper.java.additional.5 = -Xmx6144m
```

*Start the Edge Encryption proxy.*

**Start the Edge Encryption proxy**

After an Edge Encryption proxy is installed and configured, you can start the proxy from the command line.

Before starting the encryption proxy, verify the following:

- The Edge Encryption plugin is activated on the instance.
- The `edgeencryption.properties` file on this machine has been configured.
- If using an order preserving encryption type or encryption patterns, the proxy database is running.

**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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>On a Linux machine</strong></td>
<td>1. cd to <code>ServerName_port</code></td>
</tr>
<tr>
<td></td>
<td>2. Execute ./startup.sh</td>
</tr>
</tbody>
</table>
| **On a Windows machine**      | 1. cd to `ServerName_port/bin`
|                               | 2. Execute `edgeencryption.bat start` |

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*.
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><code>wrapper.ntservice.name</code></td>
<td>Unique name of the Edge Encryption proxy service.</td>
</tr>
<tr>
<td><code>wrapper.ntservice.displayname</code></td>
<td>Edge Encryption proxy service display name.</td>
</tr>
<tr>
<td><code>wrapper.ntservice.description</code></td>
<td>(Optional) 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);
       }
   }
   ```

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 */
   ```
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.service-now.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>
### ServiceNow    Jakarta    Now Platform Capabilities

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>edgeencryption.target.protocol</code></td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>- http</td>
</tr>
<tr>
<td></td>
<td>- https</td>
</tr>
</tbody>
</table>

#### User account properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>edgeencryption.target.username</code></td>
<td>User name that the proxy uses to log in to the instance. The user must have the <code>edge_encryption</code> role. See <code>Set up an Edge Encryption user account</code>.</td>
</tr>
<tr>
<td><code>edgeencryption.target.password</code></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><code>edgeencryption.proxy.host</code></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><code>edgeencryption.proxy.name</code></td>
<td>Proxy name. It must be unique for each proxy.</td>
</tr>
<tr>
<td><code>edgeencryption.proxy.http.port</code></td>
<td>Port on the proxy for HTTP communication.</td>
</tr>
<tr>
<td><code>edgeencryption.proxy.https.port</code></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><code>edgeencryption.proxy.https.cert.alias</code></td>
<td>Alias of the certificate provided by the proxy server to connecting clients.</td>
</tr>
<tr>
<td><code>edgeencryption.proxy.https.keystore.path</code></td>
<td>Path to the keystore that contains the HTTPS certificate.</td>
</tr>
<tr>
<td><code>edgeencryption.proxy.https.keystore.password</code></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><code>edgeencryption.proxy.locked</code></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>
</tbody>
</table>
| edgeencryption.db.name        | Proxy database name. Must be the same for all encryption proxies connecting to the same instance.  
  - **Default value**: edgeencryption |
| edgeencryption.db.bootstrap.file | Bootstrap file for the proxy database. The file is relative to the sql/ directory. Must be the same for all encryption proxies connecting to the same instance. |

**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>
</tbody>
</table>
| edgeencryption.proxy.signature.keystore.password | Password. The default password is <changeme>.  
  Change the password after installing the Java KeyStore. |
| edgeencryption.proxy.signature.keystore.keyalias | The key alias given as the -alias argument  
  when the RSA key pair is generated. |

### NAE device keystore

<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 key store 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>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</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></td>
<td>\texttt{edgeencryption.keystore.path = keystore/keystore.jceks}</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. If using the Java KeyStore or a SafeNet KeySecure keystore, leave this property commented out. Example:</td>
</tr>
<tr>
<td></td>
<td>\texttt{edgeencryption.keyfile.directory=keys}</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>\textbf{Note:} 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.encryption.order_preserving.cache.enable</td>
<td>Determines whether caching is used to support order-preserving encryption types.</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>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>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</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 300.</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 10. The minimum value is 5.</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 0 (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>

**Deprecated proxy encryption properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>edgeencryption.encrypter.default.key128</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>edgeencryption.encrypter.default.key256</td>
<td>Specifies the name of the current AES 256 key. Must be the same for all proxies.</td>
</tr>
<tr>
<td>edgeencryption.encrypter.key</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>edgeencryption.encrypter.type</td>
<td>Specifies the type of encryption keystore system.</td>
</tr>
<tr>
<td>edgeencryption.encrypter.file</td>
<td>Specifies the path and file name of the text file associated with the key.</td>
</tr>
<tr>
<td>edgeencryption.encrypter.password</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. However, you must either configure the environment to return responses to the load balancer instead of the proxy server and configure load balancer iRules, or run the proxy servers on the same port as the load balancer. Otherwise, users cannot view the responses to their requests.
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 Edge Encryption instance.
4. The 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 the Virtual Server.
   - 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 on 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.
Solutions

To return responses from the load balancer to the clients in your network, determine whether to use proxy servers on the same port as the load balancer, or to configure the load balancer environment instead.

Use proxy servers on the same port as the load balancer

Because the proxy servers and load balancer use the same port, the client browser receives the response on the same port identified in the response header. This solution requires less maintenance and is more performant than configuring the load balancer environment.

Verify that the host and port properties in the edgeencryption.properties file to point to the port running both the load balancer and Edge proxies. The host must point to the load balancer. Properties to configure include:

- `edgeencryption.proxy.host`: Set the value to the load balancer host machine.
- `edgeencryption.proxy.http.port`: Set the value to the port used by both the load balancer and the Edge proxies.
- `edgeencryption.proxy.https.port`: Set the value to the port used by both the load balancer and the Edge proxies.

For more information on Edge Encryption properties, see *Edge Encryption properties*.

Configure the load balancer to rewrite the response

If the load balancer and proxy servers are using different ports, configure the load balancer to rewrite the response before forwarding it to the client browser. The load balancer must terminate the SSL connection with the Edge proxy, rewrite the response using an iRule, and recertify and forward the response to the browser. This solution enables you to configure proxy servers on different ports from the load balancer, but can cost more in maintenance and performance. In this configuration:

1. The instance sends a response to the Edge proxy, which forwards the response to the load balancer.
2. The load balancer terminates the SSL connection.
3. The load balancer uses an iRule to rewrite the response, changing the port in the response location header to the load balancer port.
4. The load balancer recertifies the response and forwards it to the client browser. To recertify the response, the load balancer must host the servicenow certificate and private key.

Configure the load balancer

If the load balancer and proxy servers are using different ports, configure the load balancer to rewrite the response before forwarding it to the client browser. The load balancer must terminate the SSL connection with the Edge proxy, rewrite the response using an iRule, and recertify and forward the response to the browser. This solution enables you to configure proxy servers on different ports from the load balancer, but can cost more in maintenance and performance.

Role required: admin

1. Add the servicenow certificate and private key to the load balancer. These files must be maintained and up-to-date.
2. Configure the load balancer to terminate the SSL connection, modify the response from the instance, and recertify and forward the response to the client browser.
Create scripts or iRules on the load balancer to rewrite the response location header to use the load balancer port. This enables the client browser communicating with the load balancer to receive the response. To learn more about iRules, see F5 load balancer documentation.

The load balancer intercepts each response from the proxy server and rewrites the response location header before forwarding it to the client.

**Edge Encryption upgrades**

You can schedule an upgrade to enable the instance to upgrade the Edge Encryption proxy server, or manually upgrade the proxy server at any time.

**Scheduled upgrade**

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
   - java/jre/lib/security/local_policy.jar file
   - java/jre/lib/security/US_export_policy.jar file

   As a result, your keys, keystores, settings, certificates, and Java Cryptography Extension (JCE) files 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`.

**Manual upgrade**

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 back to the old version to ensure that there is no downtime.

**Troubleshoot a failed scheduled upgrade**

When a scheduled 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 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](#).

### Mixed proxy-version environments

While 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 Jakarta release, your environment supports proxy servers from any Jakarta 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.

**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
- `java/jre/lib/security/local_policy.jar` file
- `java/jre/lib/security/US_export_policy.jar` 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>
<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:</td>
</tr>
</tbody>
</table>
|                    | • Pending
|                    | • Running
|                    | • Complete
|                    | • Failed                                                                      |

4. Click **Submit.**

After an upgrade is executed, you can review the upgrade details to learn more about it. If your upgrade failed, review the **Failure Reason** to determine next steps.

### Upgrade details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Version</td>
<td>The version that the server was upgraded from.</td>
</tr>
<tr>
<td>To Version</td>
<td>The version that the server was upgraded to.</td>
</tr>
<tr>
<td>Actual Start Time</td>
<td>Time that the upgrade began.</td>
</tr>
<tr>
<td>End Time</td>
<td>Time that the upgrade ended.</td>
</tr>
<tr>
<td>Failure Reason</td>
<td>Reason that the upgrade failed.</td>
</tr>
</tbody>
</table>
**Manually upgrade an Edge Encryption proxy server running on Linux**

Update a proxy running on Linux.

1. Copy the Edge Encryption update-archive file to the installation directory.
2. Change to the installation directory.
3. Run the following command:
   ```
   java -jar edgeencryption-dist-<version>-linux-x86-64.zip -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>-linux-x86-64.zip```

A new proxy directory is created with a current timestamp and the old proxy directory is maintained as a backup. 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.

Role required: admin

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>-windows-x86-64.zip -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>-windows-x86-64.zip```

A new proxy directory is created with a current timestamp and the old proxy directory is maintained as a backup. 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 Jakarta release, the proxy server will automatically roll back to the old version. The old proxy server is stored unmodified in a backup directory.

If you would like to roll back a manual upgrade, you can follow these steps.

1. Shut down the proxy.
2. Delete the new proxy directory.
3. Rename the backup directory to the proxy name.
   The backup directory is in the proxy installation directory with the name `<proxy name>_backup`.
4. Start the proxy.
5. Check the proxy log and the instance to verify that the proxy is online.

Edge Encryption configuration

After the Edge Encryption proxy server is installed and running, manage Edge Encryption through the proxy server.

You must complete all the steps in Edge Encryption installation before creating encryption configurations and encryption patterns on the instance.

Note: To access Edge Encryption configuration, you must log in through the proxy server and elevate to the security_admin role.

Rotate encryption keys

You can perform encryption key rotation from the instance. You can 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 it can be assigned as the default key.

Note: Before removing a key from the proxy, ensure that no data on the instance uses the key. You can do this by setting up and running a mass key rotation job.

Schedule a single key rotation job

You can 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, make sure you 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.
### Schedule a mass key rotation job

You can schedule a job to find data encrypted with old keys and then re-encrypt the data with the current default encryption keys. The data is decrypted before it is re-encrypted with the current default key.

**Role required:** security-admin

1. Navigate to **Edge Encryption Configuration > Maintenance > Schedule Mass Key Rotation**.
2. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name.</td>
</tr>
<tr>
<td>Job Type</td>
<td>Select <strong>Mass Key Rotation</strong>.</td>
</tr>
<tr>
<td>Active</td>
<td>Clear this check box if you want to deactivate this job.</td>
</tr>
<tr>
<td>Run</td>
<td>Select the period between job executions.</td>
</tr>
<tr>
<td>Starting</td>
<td>Enter the date and time to run the job for the first time.</td>
</tr>
</tbody>
</table>

3. Click the menu icon in the form header and select **Save**.
4. To see an estimated count of records to be updated, click **Estimate Record Count**.

### Schedule an attachment key rotation job

You can 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>Mass Key Rotation</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 the job for the first time.</td>
</tr>
<tr>
<td>Field</td>
<td>Value</td>
</tr>
<tr>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>Name</td>
<td>Enter a descriptive name.</td>
</tr>
<tr>
<td>Job Type</td>
<td>Select Attachment Key Rotation.</td>
</tr>
<tr>
<td>Active</td>
<td>Clear the check mark if you want to deactivate this job.</td>
</tr>
<tr>
<td>Table</td>
<td>Select a table.</td>
</tr>
<tr>
<td>Run</td>
<td>Select the period between job executions.</td>
</tr>
<tr>
<td>Starting</td>
<td>Enter the date and time to run the job for the first time.</td>
</tr>
</tbody>
</table>

3. Click the menu icon in the form header and select **Save**.
4. To see an estimated count of records to be updated, click **Estimated Record Count**.
5. To run the job immediately, click **Execute Now**.

**Encrypt fields using encryption configurations**

Encrypt fields by creating encryption configurations.

To configure Edge Encryption, you must be connected to the instance through the proxy. Test all changes on a non-production instance before making the changes to the production instance.

**Define encryption keys**

After setting up one or more proxies and configuring a default encryption key, the instance verifies that the keys are available to all proxies. You cannot make an encryption key the default key unless all proxies have the key. Once a default key is defined, you can create encryption configurations.

**Assign fields and attachments to be encrypted**

Assigning fields and attachments to be encrypted means assigning an encryption type to the field or attachment. Before marking a field as encrypted, evaluate these issues.

- Determine what system features might be impacted.
- Examine all scripts for use of the field.
- Make any desired adjustments to the field’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

1. Navigate to **Edge Encryption Configuration > Edge Encryption Configurations > Create New**.
2. Fill in the fields on the form, as appropriate.
**Edge Encryption configuration**

<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 Column.</td>
</tr>
<tr>
<td>Column</td>
<td>The table field to be encrypted. This field appears when the Type is Column.</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, the records are encrypted as they are saved to the instance.

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>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) before the decryption job runs, otherwise, nothing happens.

Role required: security-admin

1. Navigate to Edge Encryption Configuration > Encryption Configurations > All.
2. Click the field that you want to decrypt.
   The Scheduled Encryption Job form is shown with all fields populated. The bottom of the form shows records for previous job executions.
4. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name.</td>
</tr>
<tr>
<td>Job Type</td>
<td>Select Decryption.</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>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

1. Navigate to **Edge Encryption Configuration** > **Edge Encryption Configurations** > **Create New**.
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 <strong>Attachment</strong>.</td>
</tr>
<tr>
<td>Column</td>
<td>The table field to be encrypted. This field appears when the Type is <strong>Column</strong>, and not when Type is <strong>Attachment</strong>.</td>
</tr>
<tr>
<td>Encryption type</td>
<td>The encryption type to use. For attachments, only Standard AES128 and Standard AES256 are allowed.</td>
</tr>
</tbody>
</table>

3. Click **Submit**.

After the encryption record has been added, you can create an attachment encryption job to encrypt existing attachments. If you do not run an attachment encryption job, the system encrypts new attachments when you attach them.
Schedule an attachment encryption job

You can schedule a job to find and encrypt any unencrypted attachments for a specified table, using the default encryption key configured for the table.

Role required: security-admin

1. Navigate to Edge Encryption Configuration > Encryption Configurations > All.
2. Click the table you want to schedule an encryption job for.

   The Scheduled Encryption Job form is shown with all fields populated. The bottom of the form shows records for previous job executions.
4. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name.</td>
</tr>
<tr>
<td>Active</td>
<td>Clear this check box if you want to deactivate this job.</td>
</tr>
<tr>
<td>Job Type</td>
<td>Select Attachment Encryption.</td>
</tr>
<tr>
<td>Table</td>
<td>Select a table.</td>
</tr>
<tr>
<td>Run</td>
<td>Select the period between job executions.</td>
</tr>
<tr>
<td>Starting</td>
<td>Enter the date and time to run the job for the first time.</td>
</tr>
</tbody>
</table>

5. Click the menu icon in the form header and select Save.
6. To see an estimated count of records to be updated, click Estimate Record Count.
7. To run the job immediately, click Execute Now.

Schedule an attachment decryption job

You can schedule a job to decrypt any encrypted attachments for a specified table, to store clear attachments in the instance.

Note: You must mark the encryption record for the table as inactive (clear the Active box) before the decryption job runs, otherwise, nothing happens.

Role required: security-admin

1. Navigate to Edge Encryption Configuration > Encryption Configurations > All.
2. Click the table with the attachments that you want to decrypt.

   The Scheduled Encryption Job form is shown with all fields populated. The bottom of the form shows records for previous job executions.
4. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name.</td>
</tr>
<tr>
<td>Job Type</td>
<td>Select Attachment Decryption.</td>
</tr>
<tr>
<td>Active</td>
<td>Clear the check mark if you want to deactivate this job.</td>
</tr>
</tbody>
</table>
Field | Value
--- | ---
Table | Select a table.
Run | Select the period between job executions.
Starting | Enter the date and time to run the job for the first time.

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 specify string patterns to be replaced by tokens before being sent to and stored in the instance.

You can pick patterns provided out of the box, or create your own patterns. You can create a basic pattern by specifying a sequence of characters. You create an advanced pattern by specifying a Java RegEx expression. The out of the box patterns are advanced patterns.

Encryption pattern limitations.
- A pattern of all alpha characters is not allowed.
- The minimum pattern size is 5 characters. This can be changed using a system property.
- The * and + quantifiers are forbidden in encryption patterns.

When the proxy matches a pattern in a request going to the instance, the proxy replaces the string with a token the same size as the string being replaced, and sends the token to the instance. The string matching the pattern is not sent to the instance. When the response is sent from the instance to the browser of HTTP client, the proxy replaces the token with the string so you see the clear text.

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.
The string matching the pattern is not encrypted, it is replaced with a token. The clear text never leaves your network. If the same string is sent to the instance multiple times, it is replaced with the same token. This means that you can perform text searches for strings that have been replaced with a token. While the search happens on the instance with tokens, the query string is changed to a token when the query is sent to the instance, the search is performed on tokens, and when the search results are sent back to you, the tokens are replaced with the clear text. Searches are done on exact matches; features such as stemming do not work.

The encryption pattern feature uses the same MySQL database used for order-preserving encryption.

**Note:** Encrypted fields are not checked for encryption patterns.

### Configure basic encryption patterns

You can build a pattern character by character.

In order to use encryption patterns, you must install and set up a proxy database in your network. This is the same database used for order-preserving encryption. In order to create or edit encryption patterns, you must be connected to the instance through the proxy.

Role required: security-admin

The input type defines how you are going to enter the pattern. It does not impact how the pattern is used. To enter a series of character types use the basic input type. To enter a Java RegEx expression use the advanced input type. To use one of the preconfigured patterns, edit one of the patterns on the Advanced Patterns list.

1. Navigate to **Edge Encryption Configuration > Encryption Patterns > Create New**.
2. Enter the pattern name.
3. Create a pattern by clicking the **Add** button, and then selecting a character type.
   - The Sample pattern shows what your pattern looks like as you add characters and specify the character type.
   - You can use the **New Block** button to move the next character to the next line. This allows you to group characters in a long pattern.
   - Click the **X** button to delete the last character in the pattern.
4. Click **Submit**.

### Configure advanced encryption patterns

You can build a pattern using a Java RegEx expression.

In order to use encryption patterns, you must install and set up a proxy database in your network. This is the same database used for order-preserving encryption. In order to create or edit encryption patterns, you must be connected to the instance through the proxy.

Role required: security-admin

The input type defines how you are going to enter the pattern. It does not impact how the pattern is used. To enter a series of character types use the basic input type. To enter a Java RegEx expression use the advanced input type. To use one of the preconfigured patterns, edit one of the patterns on the Advanced Patterns list.

1. Navigate to **Edge Encryption Configuration > Encryption Patterns > Create New**.
2. Enter the pattern name.
3. In the **Edge pattern input type** list, select **Advanced**.
4. When the **Convert basic pattern to advanced** dialog is shown, click **OK**.
5. In the Sample match edit box, enter a sample pattern.
Use this sample pattern to test the RegEx expression you enter. You cannot save the pattern until the pattern matches the sample.

6. In the Pattern edit box, enter a Java RegEx expression.
7. Click the Validate button to verify that the expression matches the sample pattern.
8. Click Submit.

Configure predefined encryption patterns

Edge Encryption ships with a set of predefined encryption patterns. You can activate these patterns instead of creating your own patterns.

In order to use encryption patterns, you must install and set up a proxy database in your network. This is the same database used for order-preserving encryption. In order to create or edit encryption patterns, you must be connected to the instance through the proxy.

Role required: security-admin

The input type defines how you are going to enter the pattern. It does not impact how the pattern is used. To enter a series of character types use the basic input type. To enter a Java RegEx expression use the advanced input type. To use one of the preconfigured patterns, edit one of the patterns on the Advanced Patterns list.

1. Navigate to Edge Encryption Configuration > Encryption Patterns > Advanced Patterns.
2. Click on the pattern you want to use.
   You can change the pattern to match your specific requirements.
   The Encryption Pattern form is shown.
3. Click Active, and then click Update.
   The Encryption Patterns list is shown.

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>
</tbody>
</table>
### ServiceNow Jakarta Now Platform Capabilities

#### Schedule a proxy-database recovery job

Run this job when the proxy database has lost data. This job finds all records that have been encrypted with a token (order preserving encryption type) and sends them to the proxy so that the proxy database can be rebuilt.

Role required: security-admin

1. Navigate to **Edge Encryption Configuration > Maintenance > Schedule Database Recovery**.
2. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name for this job.</td>
</tr>
<tr>
<td>Job Type</td>
<td>Select <strong>Database Recovery</strong>.</td>
</tr>
<tr>
<td>Active</td>
<td>Clear this check box if you want to deactivate this job.</td>
</tr>
<tr>
<td>Run</td>
<td>Select the period between job executions.</td>
</tr>
<tr>
<td>Starting</td>
<td>Enter the date and time to run this job for the first time.</td>
</tr>
</tbody>
</table>

3. Click the menu icon in the form header and select **Save**.
4. To see an estimated count of records to be updated, click **Estimated Record Count**.

#### 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 Glide 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.

---

© 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 to use custom rules

A set of encryption rules is installed 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 must 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.

Encryption rule APIs

Encryption rules are written in JavaScript and utilize Edge Encryption APIs to locate and encrypt sensitive information in the body of a request. The API uses expressions similar to xPath to navigate through both JSON and XML content.

Edge Encryption APIs process the request off the stream as it is being written to the output stream. Stream parsing allows encryption rules to be network performant. However, fetching and parsing content from the body multiple times could lead to unexpected results. To account for this, requests should be processed by the action in a single pass.

When creating encryption rules, you cannot use Glide APIs, script includes, business rules, or any global parameters such as current. Because the rules are created for HTTP objects, a global request object is available.

When creating encryption rules, you cannot use APIs from the white list manager or scoped applications.
Error handling

If an encryption rule condition or action throws an exception, check the proxy log for troubleshooting information.

Inspect the client request

Before creating a custom encryption rule, you must determine the format of the client request entering the Edge Encryption proxy server.

Because encryption rules iterate over client requests and determine what, if anything, needs to be encrypted, you must understand the type of request you are creating a rule for. The format of the client request determines the structure of your encryption rule and the APIs available for use in the rule.

1. Inspect the client request.

   Depending on the source of the request, the following tools are available to inspect the request and determine the format.

<table>
<thead>
<tr>
<th>Source of request</th>
<th>Available tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client browser</td>
<td>Use the developer console in your browser to inspect the client request. Useful tools include:</td>
</tr>
<tr>
<td></td>
<td>· Firefox Network Monitor</td>
</tr>
<tr>
<td></td>
<td>· Chrome Network Panel</td>
</tr>
<tr>
<td>Third-party/external source</td>
<td>Use an HTTP protocol analyzer to inspect the request. Useful tools include:</td>
</tr>
<tr>
<td></td>
<td>· Wireshark</td>
</tr>
<tr>
<td></td>
<td>· HTTP Scoop</td>
</tr>
<tr>
<td></td>
<td>Alternatively, you can often use documentation for the external source to determine the format of the request.</td>
</tr>
</tbody>
</table>

2. From the client request, inspect the packet and determine:
   - The client request method
   - The URL path of the request
   - The URL parameters
   - The POST parameters, if any
   - The format of the request body, if included
Inspecting the request provides an understanding of the fields you need to filter for and iterate over in your encryption rule. To understand the fields in the request object, see request.

Create an encryption rule

Encryption rules are used by the proxy to find content in HTTP requests that should be encrypted.

Role required: security_admin

Before creating an encryption rule, you must inspect the client request to determine the format.

To create or edit encryption rules, you must be connected to the instance through an encryption proxy.

1. Navigate to Edge Encryption Configuration > Rules > Create New.
2. In the Name box, enter a name.
3. In the Request Type, select an HTTP method.
   - HTTP Post
   - HTTP Get
   - HTTP Put
   - HTTP Patch
   - HTTP Delete

   **Note:** Pre-Jakarta instances 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.

request
The request object is a global object available in Edge Encryption rule action and condition scripts.

The request object is a JavaScript object that represents the client request coming in to the Edge Encryption proxy server. You must build your encryption rule to parse the request object, map request object values to fields in a table on the instance, and encrypt any sensitive data in the request object.

The request object includes the following attributes and data from the client request:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>path</td>
<td>The path portion of the URL.</td>
</tr>
<tr>
<td>requestMethod</td>
<td>GET, POST, PUT, PATCH, DELETE.</td>
</tr>
<tr>
<td>contentType</td>
<td>The Content-Type header field.</td>
</tr>
<tr>
<td>urlParams</td>
<td>The parameters in the query string. This can also be evaluated to a String.</td>
</tr>
<tr>
<td>postParams</td>
<td>If this is a form post, this contains the post parameters.</td>
</tr>
</tbody>
</table>

`request.getAsJsonContent()`

Returns the request as an iterable object of type JsonNode.

This method is available only in an Edge Encryption rule if the request body is a valid JSON payload. If you are not sure what format the request body includes, check the contentType field on the request object.

Once the request is returned as a JsonNode object, you can use the JSON APIs to iterate over the object and encrypt fields.
Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>JsonNode</td>
<td>The request as an iterable JsonNode.</td>
</tr>
</tbody>
</table>

request - getAsXmlContent()

Returns the request content as an iterable object of type XMLContent.

This method is available only in an Edge Encryption rule if the request body is a valid XML payload. If you are not sure what format the request body includes, check the contentType field on the request object.

Once the request is returned as an XMLContent object, you can use the XML APIs to iterate over the object and encrypt fields.

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>XMLContent</td>
<td>The request as an iterable object of type 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>

<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>

<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>

**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>

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>XMLContent</td>
<td>The request as an iterable XMLContent.</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.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tableName</td>
<td>String</td>
<td>The table that you expect the query to run on.</td>
</tr>
</tbody>
</table>

**Returns**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>void</td>
<td></td>
</tr>
</tbody>
</table>

#### ParameterValue - valueFor(String tableName, String fieldName)

Specifies that the value of the element maps to the specified field in the specified table.

Calling this method on an element value tells the proxy that the value for this element maps to the specified field in the specified table. The proxy then checks if the field must be encrypted.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tableName</td>
<td>String</td>
<td>The table name.</td>
</tr>
<tr>
<td>fieldName</td>
<td>String</td>
<td>The field name.</td>
</tr>
</tbody>
</table>

**Returns**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>void</td>
<td></td>
</tr>
</tbody>
</table>

### XML APIs

XML APIs can be used after calling `getAsXmlContent()` on either the request object or a `ParameterValue` property.
When using XML APIs to write your encryption rule, you can follow a general format:

1. Call `getAsXmlContent()` on the `request` object or `ParameterValue` property. This returns an iterable object of the `XMLContent` underlying class.

2. Call `getIterator()` or `getIterator(String xpath)` on the `XMLContent` object. This returns an `XMLElementIterator` object that can be used to iterate over XML elements.

3. Call the `hasNext()` method on the `XMLElementIterator` object to determine whether another element is available.

4. Call `next()` on the `XMLElementIterator` object to return the next XML element. You cannot call `next()` without first calling `hasNext()`.

5. Call `valueFor(String tableName, String fieldName)` on the XML element. This method tells the proxy that the value for this element maps to the specified field in the specified table. The proxy then checks if the field must be encrypted.

   **Note:** To determine if you want to call `valueFor(String tableName, String fieldName)` on an XML element, you can use the `getName()` method to return the name of the element.

### Mapping to a known table-field on the instance

In this example, the XML payload will be processed on the instance to insert records in the `incident` table. The description field will populate `short_description` on the incident.

```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.
**Note:** This rule finds all description tags within all record tags in the XML payload. If there is only one occurrence of a tag to encrypt, the rule still uses the xPath and iterator structure. However, it iterates only once in the loop.

**Mapping to an unknown table-field on the instance**

In this example, the rule iterates over the record tags, but does not know what tags to expect within the record tag. The only known is that the tags within the record tags match the names of the columns specified in the table URL parameter.

The rule also specifies that, if the table is incident, then the data in the description tag should be encrypted and stored in the short_description field on the instance.

```javascript
function sampleXmlAction2() {
    var xmlContent = request.getAsXmlContent();
    var tableName = request.urlParam.table;
    // This first iterator will iterate over all record elements
    var xmlElementIterator = xmlContent.getIterator('data/record');
    while (xmlElementIterator.hasNext()) {
        encryptFieldsInRecord(xmlElementIterator.next());
    }
}

function encryptFieldsInRecord(xmlElement) {
    // Then, iterate over all tags representing fields in the table
    var fieldIterator = xmlElement.getIteratorOverAllChildren();
    while (fieldIterator.hasNext()) {
        var field = fieldIterator.next();
        var fieldName = childElement.getName();
        // if table is incident, then description is encrypted for the short_description field
        if (tableName == 'incident' && fieldName == 'description') {
            field.valueFor(tableName, 'short_description');
        } 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>
```
<description filter="false">'Test Record 1 Description'</description>
<query filter="true">category=1^name=edge</query>
</record>
<record>
  <name filter="false">'Test Record 2'</name>
  <description filter="false">'Test Record 2 Description'</description>
  <query filter="true">category=2^severity=3</query>
</record>
</data>

The following encryption rule action can apply:

```javascript
function sampleXmlAction3() {
  var xmlContent = request.getAsXmlContent();
  var 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>
XMLElementIterator
An object that can be used to iterate over elements in the XMLContent object.

XMLElementIterator - hasNext()
Determines if there is another element available.

XMLElementIterator - next()
Returns the next element in the iterator.

© 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.
XMLElement
Provides methods for iterating through XML elements and mapping values to fields in a table.
You get an XMLElement object by calling the next() method of an XMLElementIterator object.

XMLElement - getIterator(String xPath)
Returns an XMLElementIterator object for the XML element based on the specified parameter.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>xPath</td>
<td>String</td>
<td>An xPath-like expression that specifies where in the XMLElement object to start.</td>
</tr>
</tbody>
</table>

XMLElement - getIteratorOverAllChildren()
Returns an XMLElementIterator object that includes all sub-elements for the XML element based on the specified parameter.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>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=3D4B60165813e63a00d00abd322244b092^category=vulnerability"
  }
}
The following rule can apply:

```
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.

```
function sampleJsonAction2() {
    var jsonContent = request.getAsJsonContent();
    var tableName = request.urlParam.table;
    // This first iterator will iterate over all record elements
    var jsonNodeIterator = jsonContent.getIterator('data/records');
    while (jsonNodeIterator.hasNext()) {
        encryptFieldsInRecord(jsonNodeIterator.next());
    }
}
```

```
function encryptFieldsInRecord(jsonNode) {
    // this time we want to iterate over all nodes
    var fieldIterator = jsonNode.iterator();
    while (fieldIterator.hasNext()) {
        var field = fieldIterator.next();
        var fieldName = childElement.getName();
        if (fieldName == 'description') {
            field.valueFor(tableName, 'short_description');
        } else {
            field.valueFor(tableName, fieldName);
        }
    }
}
```

In the `encryptFieldsInRecord()` function, the `valueFor()` method is called on a table and a field that are dynamically assigned based on the request. Even though the table and field names
can change, the rule asks the proxy to check whether the field in the table must be encrypted based on the encryption configurations defined.

If the field is not configured for encryption, or if the node name does not match a field in the table, the proxy skips that node. If the node name matches a field marked for encryption, then the proxy encrypts the value.

Using an encoded query

```javascript
function sampleJsonAction3() {
    var jsonContent = request.getAsJsonContent();
    var tableName = request.urlParam.table;
    // This first iterator will iterate over all record elements
    var jsonNodeIterator = jsonContent.getIterator('data');
    while (jsonNodeIterator.hasNext()) {
        var jsonNode = jsonNodeIterator.next();
        if (jsonNode.getName() == 'records')
            encryptRecords(jsonNodeIterator.next());
        else if (jsonNode.getName() == 'query')
            jsonNode.encodedQueryFor(tableName);
    }
}
function encryptRecords(jsonNode) {
    // we iterate over all fields in the node
    var recordIterator = jsonNode.iterator();
    while (recordIterator.hasNext()) {
        encryptFieldsInRecord(recordIterator.next());
    }
}
function encryptFieldsInRecord(jsonNode) {
    // this time we want to iterate over all nodes
    var fieldIterator = jsonNode.iterator();
    while (fieldIterator.hasNext()) {
        var field = fieldIterator.next();
        var fieldName = childElement.getName();
        field.valueFor(tableName, fieldName);
    }
}
```

In this example, the rule iterates over `data`. As it finds `records`, it performs the same logic as in the second example, iterating over fields in each node. When it finds the `query` node, it calls `encodedQueryFor()` to encrypt values that should be encrypted in the query.

JsonNode

A global object that provides methods to iterate over the JSON content.

You can access a `JsonNode` object by calling `getAsJsonContent()` on a `request` object.

You access JSON content from a `POST` or `URL` parameter by calling `request.postParms.<parameter name>.getAsJsonContent()` or `request.urlParms.<parameter name>.getAsJsonContent()`.

`JsonNode - getIterator(String xpath)`

Returns a `JsonNodeIterator` object for the JSON content.

This method can only be used on the root node, but can be used to traverse deep into the JSON object. Subsequent traversals must use the `iterator()` method.
### Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>xPath</td>
<td>String</td>
<td>An xPath expression.</td>
</tr>
</tbody>
</table>

### Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>JsonNodeIterator</td>
<td>An object that can iterate over nodes in the JSON object.</td>
</tr>
</tbody>
</table>

**JsonNode - iterator()**

Returns a `JsonNodeIterator` object that iterates over all child nodes of the current node.

#### Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>JsonNodeIterator</td>
<td>An object that can iterate over nodes in the JSON object.</td>
</tr>
</tbody>
</table>

**JsonNode - getAsString()**

Returns the current node value as a string.

#### Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>The current node value.</td>
</tr>
</tbody>
</table>

**JsonNode - getAsString(String propertyName)**

Returns the string value of the specified property.

#### Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>propertyName</td>
<td>String</td>
<td>Name of the property.</td>
</tr>
</tbody>
</table>
Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>The property value.</td>
</tr>
</tbody>
</table>

JsonNode - getName()

Returns the name of the current JSON node.

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>Name of the current JSON node.</td>
</tr>
</tbody>
</table>

JsonNode - valueFor(String tableName, String fieldName)

Specifies that the JSON property maps to the specified field in the specified table.

Calling this method on a JSON property tells the proxy that the value for this property maps to the specified field in the specified table. The proxy then decides if the field must be encrypted. If the table and field names are unknown, you can call the valueFor() method on a table and a field that are dynamically assigned based on the request.

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tableName</td>
<td>String</td>
<td>The table name.</td>
</tr>
<tr>
<td>fieldName</td>
<td>String</td>
<td>The field name.</td>
</tr>
</tbody>
</table>

Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>void</td>
<td></td>
</tr>
</tbody>
</table>

JsonNode - encodedQueryFor(String tableName)

Specifies that the value of the JSON property is an encoded query for the specified table.

Calling this function on a JSON node tells the proxy that the value is an encoded query for the specified table. The proxy parses the encoded query and encrypts the values for fields in the encoded query that must be encrypted.

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tableName</td>
<td>String</td>
<td>The table that you expect the query to run on.</td>
</tr>
</tbody>
</table>
Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>void</td>
<td></td>
</tr>
</tbody>
</table>

JsonNodeIterator

You get a `JsonNodeIterator` object by calling the `getIterator()` or `iterator()` methods of the `JsonNode` class.

JsonNodeIterator - hasNext()

Determines if there is another property available.

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>None</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>None</td>
<td></td>
</tr>
</tbody>
</table>

Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>JsonNode</td>
<td>The next JsonNode.</td>
</tr>
</tbody>
</table>

`print(String message)`

Prints a message to the wrapper log file: `<proxy server directory>/logs/wrapper_<date>.log`.

This method is available only in an Edge Encryption rule action script.

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>message</td>
<td>String</td>
<td>The message to be written to the wrapper log file.</td>
</tr>
</tbody>
</table>
### Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>void</td>
<td></td>
</tr>
</tbody>
</table>

#### Prohibited keywords

The Edge Encryption proxy validates encryption rule scripts before saving the rule. Many JavaScript keywords are not allowed in encryption rule scripts.

<table>
<thead>
<tr>
<th>Keyword</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>__DIR__</code></td>
</tr>
<tr>
<td><code>__FILE__</code></td>
</tr>
<tr>
<td><code>__LINE__</code></td>
</tr>
<tr>
<td><code>__parent__</code></td>
</tr>
<tr>
<td><code>__proto__</code></td>
</tr>
<tr>
<td><code>Error</code></td>
</tr>
<tr>
<td><code>eval</code></td>
</tr>
<tr>
<td><code>getClass</code></td>
</tr>
<tr>
<td><code>getPrototypeOf</code></td>
</tr>
<tr>
<td><code>Java</code></td>
</tr>
<tr>
<td><code>javax</code></td>
</tr>
<tr>
<td><code>javafx</code></td>
</tr>
<tr>
<td><code>JavaImporter</code></td>
</tr>
<tr>
<td><code>load</code></td>
</tr>
<tr>
<td><code>loadWithNewGlobal</code></td>
</tr>
<tr>
<td><code>new</code></td>
</tr>
<tr>
<td><code>Packages</code></td>
</tr>
<tr>
<td><code>Object</code></td>
</tr>
<tr>
<td><code>prototype</code></td>
</tr>
<tr>
<td><code>RegExp</code></td>
</tr>
<tr>
<td><code>setPrototypeOf</code></td>
</tr>
<tr>
<td><code>this</code></td>
</tr>
<tr>
<td><code>throw</code></td>
</tr>
</tbody>
</table>

### 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.

Two inactive encryption rules are automatically created to encrypt data sent from the record producer to the field marked for encryption.

<table>
<thead>
<tr>
<th>Encryption rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;RecordProducerName&gt;</code></td>
<td>Rule created to process POST parameters from the Service Catalog and map variables to fields in the instance.</td>
</tr>
<tr>
<td><code>&lt;RecordProducerName&gt;Json</code></td>
<td>Rule created to process a JSON payload from the Service Portal and map variables to fields in the instance.</td>
</tr>
</tbody>
</table>

5. Activate the necessary encryption rules created by the record producer.
   a) Navigate to Edge Encryption Configuration > Rules > All.
   b) Depending on where the record producer will be used, open the associated encryption rule created by the record producer and select the Active flag.
      If using the record producer in the Service Catalog, activate the `<RecordProducerName>` encryption rule. If using the record producer in the Service Portal, activate the `<RecordProducerName>Json` encryption rule.

6. Examine the Encryption rule Action field and add any necessary field names or statements.

   If a record producer directly maps a variable to a field in a table, the encryption rule automatically maps the variable to the correct field. However, if a variable is indirectly mapped through various scripts on the platform, you may need to update the rules to map each variable to the correct field.

   The below encryption rule was created from the Report Outage record producer and processes POST parameters from the Service Catalog to map variables to fields in the instance. Replace 'FILL ME IN' with the target field.
The below encryption rule was created from the Report Outage record producer and processes a JSON payload from the Service Portal to map variables to fields in the instance. Add additional statements to map any scripted variables to the target fields.
Edge Encryption Rule
ReportOutageScenario

Name: ReportOutageScenario
Request type: HTTP Post
Active: off

Condition

```javascript
function ReportOutageScenarioCondition(request) {
    if (request.path.startsWith("/api/servicescatalog/items")) {
        if (request.path.split('/')[3] == '180f6424ab0177938a52329653c29f5ec8') {
            return true;
        } else {
            return false;
        }
    }
}
```

Action

```javascript
function ReportOutageScenarioAction(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.long_description is accessed via script from current.short_description;
    // current.issue_id is accessed via script from gw.getoverId();
    var issueContent = request.getActionsContent();
    var forLoop = issueContent.getIterator('variables');
    forLoop.hasNext();
    if (forLoop.hasNext()) {
        var element = forLoop.nextElement();
        var issueContent = element.getValue(tableName, element.getName());
    }
}
```

Order: 100
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.

```java
if (jsonElement.getName() == 'error_message')
  jsonElement.valueFor(tableName, 'short_description');
```

The value of the **Action** field becomes:

```java
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.

**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

**Edge Encryption monitoring**

You can monitor sessions that use Edge Encryption proxies.

The instance tracks all encryption proxies. Each encryption proxy registers when it starts up. The instance is notified when:

• A new encryption proxy starts up.
• An encryption proxy is intentionally shut down.

If an encryption proxy 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 file is not audited.

You can also monitor the following lists and files for information about your proxies:

<table>
<thead>
<tr>
<th>List</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Edge Encryption Configuration > Diagnostics And Troubleshooting > Invalid Insert Attempts** | 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 then logs any attempts to save this data. If you have the security-admin role, you can view the logs in the Invalid Insert Attempts list. |
| **Edge Encryption Configuration > Proxies > Online** | List of online proxies. |
| **Edge Encryption Configuration > Proxies > All** | List of all proxies. |
| **System log** | The instance periodically checks for messages from each encryption proxy, and it logs an error if a proxy has not sent a message in the required time frame. 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. |
XMLStats

<table>
<thead>
<tr>
<th>XMLStats</th>
<th>Information about the number of registered encryption proxies, and the number of pending and running mass encryption jobs.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Edge Encryption Configuration &gt; Maintenance &gt; Scheduled Jobs</strong></td>
<td>A list of jobs that are scheduled to run.</td>
</tr>
<tr>
<td><strong>Edge Encryption Configuration &gt; Maintenance &gt; Job Executions</strong></td>
<td>A list of jobs about that have run.</td>
</tr>
<tr>
<td><strong>Edge Encryption Configuration &gt; Diagnostics And Troubleshooting &gt; Job Failures</strong></td>
<td>A list of jobs that did not execute successfully.</td>
</tr>
</tbody>
</table>

**Edge Encryption logging**

Edge Encryption logs information on the instance and on each proxy server.

You can view a log file listing all cases of when an attempt was made to save unencrypted data to an encrypted field. Navigate to **Edge Encryption Configuration > Diagnostics And Troubleshooting > Invalid Insert Attempts**. An administrator can trace back to why data was not saved.

There are encryption log files on each proxy server.

**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.

**Knowledge Management**

The ServiceNow® Knowledge Management (KM) application enables the sharing of information in knowledge bases. These knowledge bases contain articles that provide users with information such as self-help, troubleshooting, and task resolution.

Knowledge Management has significantly changed with Knowledge v3, which is enabled by default for all instances starting with the Fuji release.

Knowledge Management supports processes for creating, categorizing, reviewing, and approving articles. Users can search and browse articles as well as provide feedback.
To support multiple groups, knowledge bases can be assigned to individual managers. Separate workflows can be used for publishing and retiring articles, and separate access controls can be used to control reading and contributing.

---

**Knowledge Management setup guide for admins**

Before users in your organization can start creating knowledge bases and knowledge articles, you must set up Knowledge Management. Work with stakeholders to define requirements for setting up Knowledge Management effectively to meet the needs of users. For this task, you must be an administrator with the admin role.

**Requirements**

**Role required**

admin

**Before you begin**

Meet with the following stakeholders
<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge manager</td>
<td>Defines and oversees the knowledge management processes for day-to-day operations related to content publishing and usage.</td>
</tr>
<tr>
<td>Knowledge admin</td>
<td>Configures advanced settings for specific Knowledge Management features</td>
</tr>
<tr>
<td>Content creators and reviewers</td>
<td>Create, review, and update articles in the knowledge bases.</td>
</tr>
<tr>
<td>Community managers</td>
<td>Focus on the creation and curating of social content.</td>
</tr>
<tr>
<td>Line managers</td>
<td>Manage teams that create and use knowledge articles</td>
</tr>
</tbody>
</table>

With stakeholders, determine the following requirements

- Who are the consumers of the content in the knowledge bases?
- Who are the writers, editors, and managers for the knowledge base articles?
- What are the required workflows to publish and retire articles?
- What are the unique behaviors required for your knowledge management implementation? For example, should attachments appear in search results?
- Do knowledge articles need to be translated into other languages?

What to do

Assign knowledge roles to users and groups

Determine which Knowledge Management roles are appropriate for each user, and then assign those roles.

Create custom Knowledge workflows

If the default knowledge workflows for publishing and retiring knowledge articles are not appropriate for knowledge bases, create custom workflows for those knowledge bases.

Configure Knowledge properties

If the default knowledge properties do not fulfill the requirements of users, reconfigure the properties as necessary.

Activate support for other languages besides English

If languages other than English must be supported, activate the Knowledge Management Internationalization plugins.

Coordinate with knowledge managers for knowledge base setup

Let knowledge managers and administrators know that they can start configuring their knowledge bases. For details, refer them to the Knowledge base setup guide for knowledge admins and managers.
Next steps

Depending on any other requirements for the knowledge bases, you may be asked to help with additional tasks, such as configuring knowledge homepages.

Knowledge base setup guide for knowledge admins and managers

After basic Knowledge Management setup is completed, you can set up a knowledge base for users to create and publish knowledge articles.

Multiple knowledge bases can be created for different groups within your organization to share information within and between those groups.

Administrators create knowledge bases, and assign them to individual managers responsible for controlling the behavior and organization scheme of each knowledge base.

Each knowledge base contains knowledge articles that provide information for users, such as policy, release notes, or instructions for a task. Each knowledge base can also use a separate workflow for publishing and retiring articles.

Requirements

Role required
knowledge_administrator, knowledge_manager, or admin

Before you begin

Determine the following requirements for each knowledge base that you want to set up:

- Who are the knowledge base managers that are responsible for approving articles?
- Who are the users and contributors for that knowledge base? Access for these users is defined through user criteria.
- What are the categories to be used to classify articles? Will users be able to create categories?
- Will users of the knowledge base be able to create new content?
- Will Social Q&A be leveraged for this knowledge base?

What to do

Set up the knowledge base

1. Create the knowledge base.
2. Set up which users can read, create, or edit knowledge articles by selecting user criteria for the knowledge base.
3. Define the approval process for articles using workflows.
4. Define the knowledge categories that are needed for organizing articles in the knowledge base.
5. If you want to enable users to ask and answer questions in the knowledge base, activate Social Q&A.
6. If you want a custom knowledge homepage, ask your ServiceNow administrator to create it.

Next steps

Let users in your organization know that they can start creating and searching articles in the knowledge base. For details, refer users to the Knowledge Management guide for users.

If you have the knowledge_manager role, there are many other tasks that you can perform to maintain the knowledge base. You can pin articles so they are featured prominently in the search results and on homepages. You can also assign other users as managers of a knowledge base. For details, see Knowledge manager.

Knowledge Management guide for users

After knowledge bases are set up, you can start searching and creating articles. If Social Q&A was activated for the knowledge base, you can also submit answers or answer questions for other users.

Requirements

Role required

None. All users can read, create, and edit knowledge articles in a knowledge base, unless the knowledge manager has restricted access to it.

If you need these permissions, contact the knowledge manager for the knowledge base.

What to do

Create knowledge articles

If you have the required permissions for a knowledge base, you can create articles for it. You can create articles from the Self-Service application menu or by importing Word documents.

You can also create knowledge articles from incidents and problems.

Search for knowledge articles

From the Knowledge homepage, you can select a knowledge base to search for articles and answers. You can view only the knowledge bases to which you have access.

You can also search knowledge from within an incident.

Access to knowledge using your mobile device is supported.

Ask and answer questions

If Social Q&A was activated for a knowledge base, you can ask and answer questions. You can also browse and vote on answers.
Next steps

After articles are created, you can perform the following tasks to make sure that articles are organized in the right knowledge bases and retired when appropriate. If existing knowledge bases do not fit your needs, you can request a new knowledge base.

- Move a knowledge article
- Retire a knowledge article
- Request a knowledge base

Knowledge Management roles

Certain roles are required to use Knowledge Management functionality.

### Knowledge Management roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>knowledge</td>
<td>Users with the knowledge role can contribute to the default knowledge base</td>
</tr>
<tr>
<td>knowledge_manager</td>
<td>Knowledge managers perform administrative functions for knowledge bases</td>
</tr>
<tr>
<td>knowledge_admin</td>
<td>Knowledge administrators can create new knowledge bases and manage all</td>
</tr>
<tr>
<td>admin</td>
<td>Administrators can configure knowledge workflows, set knowledge properties,</td>
</tr>
</tbody>
</table>

Administrators assign these roles to the users and groups who maintain the knowledge content.

Knowledge homepage

The Knowledge homepage displays knowledge articles and social Q&A questions organized by knowledge base and category, as well as featured content and popular articles.

To view the default knowledge homepage, navigate to **Self-Service > Knowledge**.

**Note:**

The knowledge homepage is not compatible with Internet Explorer 9 or earlier. Using one of these browsers will cause you to be redirected to the legacy knowledge portal.

The Knowledge V3 home page is not customizable. Use the Knowledge Management Service Portal for an easily configurable user experience.
The Knowledge homepage

If you access knowledge from a service management application, the knowledge homepage for the associate application opens.

From the homepage, you can import a Word document to a knowledge base using the Import Articles button. You can also create a new article using the Create An Article button, or ask a question using the Post a Question button.

- Import a Word document
- Create an article
- Ask a question
You can select a knowledge base to browse articles and questions within that knowledge base. You can view only knowledge bases you can access.

![Knowledge Base Selection](Image)

### Browsing articles by category

Articles and questions are organized by category or by tag. Categories are listed alphabetically. While browsing, you can filter content by type to view only knowledge articles, only social Q&A questions, or only unanswered questions. You can sort content by most recent update or by number of views.

An administrator can configure the knowledge homepage to display the number of articles and questions within each category. This count includes articles and questions from subcategories. To display the article and question count, set the knowledge homepage property `Display or hide the count of articles and questions in the category and child categories (glide.knowman.show_number_on_categories)` to true.

### Knowledge search

You can search for knowledge articles and social Q&A questions from the knowledge homepage using the search bar at the top of the page.
Search results include only articles and questions you are authorized to read. The search results count does not take into consideration any security rules set for the articles; therefore, the number of articles you could access may be lower than the count displayed in the search results page. Documents that are attached to articles are also listed in the search results (for those articles to which you have access).

**Note:** To change how the attachments are displayed in the search results, set the How to display attachments in Knowledge Search Results glide.knowman.search.attachment property. Attachments can be displayed with a snippet, link only, or not at all.

To use wildcards in your search, using the application navigator, navigate to **Contextual Search > Search Contexts > Knowledge Base Search** and enable wildcard search.

You can sort knowledge content by relevancy, most recent update, or number of views.

You can filter results using the check boxes that appear. Filtering options appear depending on the search text.

**Filtering options**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select if you want to view knowledge articles, social Q&amp;A questions, or both. This option is only available if Social Q&amp;A is enabled.</td>
</tr>
<tr>
<td>Knowledge Bases</td>
<td>Select a knowledge base to search. You can select only knowledge bases you can access. If you do not select a specific knowledge base, search results include articles and questions from all knowledge bases that you can access. You can also select a knowledge base from the choice list in the search bar. For pinned articles, only those in the selected knowledge base in the corresponding language appear.</td>
</tr>
<tr>
<td>Categories</td>
<td>Select one or more knowledge categories. Categories are listed alphabetically.</td>
</tr>
<tr>
<td>Authors</td>
<td>Select one or more authors.</td>
</tr>
<tr>
<td>Language</td>
<td>The multi-language search feature is available when more than one supported language is enabled. When you enable the language plugin and set the system property for multi-language search to True, the search query returns the results in all available languages simultaneously. If you set the system property for multi-language to False, the search query returns the results based on the language selected with this filter option. Refer to Knowledge search properties for more information.</td>
</tr>
</tbody>
</table>
Filtering a search

Social Q&A

If Social Q&A is activated for a knowledge base, you can ask questions and respond to questions from other users. You can also vote on helpful questions and answers.
Social Q&A extends the Knowledge application. All questions and answers are associated with a knowledge base. Social Q&A uses Knowledge access controls, search, and the knowledge homepage.

Social Q&A is available on mobile devices using the mobile knowledge interface. You can perform all Social Q&A functions on mobile, such as asking and answering questions.

**Note:** Social Q&A is not compatible with Internet Explorer 9 or earlier. Navigating to a Social Q&A page using one of these browsers will cause a browser support warning to appear.

---

**Enable social Q&A for a knowledge base**

As a knowledge manager, you can enable social Q&A for a knowledge base you manage.

Role required: knowledge_manager

You can set the limit for the number of times users can post questions, answers, and comments, or subscribe to the questions using the Knowledge Social Q&A properties.

All Social Q&A questions and answers are associated with a knowledge base. The **Enable social questions and answers** check box on the Knowledge Base form controls if users can view and ask questions.

Social Q&A uses user criteria from the knowledge base to determine which users have access to questions. A user must meet the criteria defined in the knowledge base **Can Read** related list to view or contribute to Social Q&A questions, answers, and comments associated with that knowledge base.

**Note:** The **Can Contribute** related list does not control the ability to contribute to Social Q&A. Users that meet the **Can Read** criteria for a knowledge base can also contribute questions, answers, and comments.

1. Navigate to **Knowledge > Knowledge Bases**.
2. Select a knowledge base you manage.
3. Select the **Enable social questions and answers** check box.
   
   This check box only appears if the Social Q&A plugin has been activated.
4. Click **Update**.

You can disable Q&A for a knowledge base by clearing the **Enable social questions and answers** check box. Disabling Q&A does not delete existing questions and answers associated with this knowledge base, but prevents users from browsing or searching for those questions and answers.

---

**Social Q&A questions**

Social Q&A organizes information by question.

You can browse and search for questions from the Knowledge homepage (**Self-Service > Knowledge**). Questions appear along with knowledge articles organized by knowledge base, category, and tags.

Click on a question to view the question details, as well as responses and comments. You can add responses and comments, vote on existing responses, share questions, and edit your own questions and answers from the question details.

---

**Ask a social Q&A question**

As a Social Q&A user, you can ask questions that other users can respond to.
Roles required: None

1. Navigate to **Self-Service > Knowledge**.
2. Click **Post a Question**.
3. Enter a value for the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Enter the question you have.</td>
</tr>
<tr>
<td>Question details</td>
<td>Enter additional details about the question that may help other users provide an answer.</td>
</tr>
<tr>
<td>Knowledge base</td>
<td>Select the knowledge base this question relates to. You can select only knowledge bases configured to allow Q&amp;A.</td>
</tr>
<tr>
<td>Category</td>
<td>Select the knowledge category this question relates to. You can select only categories within the selected knowledge base. Questions without a category appear on the knowledge homepage in the (empty) category.</td>
</tr>
<tr>
<td>Tags</td>
<td>Enter one or more tags that describe the question.</td>
</tr>
</tbody>
</table>

4. Click **Post Question**.

To accept the answer, click the **Accept** link from within the answer. The accepted answer moves to the top of the list of answers. You can unaccept an answer by clicking **Unaccept**.

**Note:** You must be the owner of the question or the knowledge manager to accept an answer.

**Answer a question**

As a user, you can answer a question another used has asked. The owner of the question or the knowledge manager can then accept the answer.

Roles required: None

As a knowledge manager or the owner of a question, you can accept an answer as the correct answer. That answer then appears above other answers for the question.

1. Navigate to **Self-Service > Knowledge**.
2. Select a question.
3. Enter an answer in the **Your answer** field.
4. Click **Submit**.

**Comment on a question or answer**

You can comment on a question or an answer to provide additional information relevant to that question or answer.

Roles required: None

1. Navigate to **Self-Service > Knowledge**.
2. Select a question.
3. Within the question or answer you want to comment on, click the **Comment** link.
4. Enter the comment text.
   Comments have a maximum length of 140 characters.
5. Click **Post comment** or press the Enter key.

**Edit a question, answer, or comment**

You can edit questions, answers and comments you submit, or in knowledge bases you manage.

Role required: None
1. Navigate to **Self-Service > Knowledge**.
2. Select a question.
3. Within the question, answer, or comment you want to edit, click **Edit**.
4. Edit the details as needed.
5. Optional: When editing a question, click **Advanced** to make changes to the question record.
6. Click **Update**.
   Click **Undo** to discard the changes and close the editor.

**Vote on a question or answer**

As a Social Q&A user you can vote on a question or answer to promote it.

Role required: None

Vote up questions that you want users to answer, and answers that you believe accurately resolve questions. Alternatively, vote down questions that you do not find useful, or answers that you believe are incorrect. You can vote for each question or answer only once, but you can change your vote.

Answers with a higher score appear above answers with a lower score when viewing a question. A pinned answer appears above other answers regardless of votes.

**Note:** You cannot vote for your own questions or answers.

1. Navigate to **Self-Service > Knowledge**.
2. Select a question.
3. Click the up or down arrow next to the question or answer you want to vote on.
   The score for that question or answer changes depending on your vote.

You can change your vote by clicking the other arrow.

**Subscribe to a question**

You are automatically subscribed to any question you ask, so you receive notifications when another user votes on, comments on, or answers the question. If you want to receive notifications for a question asked by another use, you can manually subscribe to the question.

Role required: None

You automatically subscribe to any question you ask.

1. Navigate to **Self-Service > Knowledge**.
2. Select a question.
3. Click the subscribe icon ( ).
If you want later to stop receiving notifications about this question, click the unsubscribe icon.

Delete a question, answer, or comment

You can delete questions, answers, or comments that you submitted.

You can delete only questions, answers, and comments you submitted. Knowledge managers can delete any question, answer, or comment within knowledge bases they manage.

Role required: none

1. Navigate to Self-Service > Knowledge.
2. Select a question or answer.
3. Within the question, answer, or comment you want to delete, click the Delete link.
   Deleting a question also deletes all answers and comments associated with that question. Deleting an answer also deletes all comments associated with that answer.

Share a question

You can generate a URL directly to a question and related answers.

Role required: None

1. Navigate to Self-Service > Knowledge.
2. Select the question that you want to share.
3. Click Share.
   Some browsers do not allow adding content directly to the clipboard. You may need to manually copy the URL from the popup that appears.

Distribute the URL to share the question.

Social Q&A internationalization support

The Social Q&A questions and answers are automatically associated with the language that is set for the interface.

You can only browse and search for questions in the language currently set for the interface. For example, if a Social Q&A user has set French as the interface language, any questions that the user asks is associated with the French language. All Social Q&A users who want to view those questions must have their interface language set to French.

Note: For Social Q&A internationalization to take effect, you must clear the platform cache and browser cache after selecting the desired language.

Social Q&A search

Users can search for specific questions from the knowledge homepage.

Social Q&A uses knowledge search to provide search results. Searching knowledge returns questions that contain the search terms in the question title or the question details, or in the accepted answer.

By default, knowledge search results include both knowledge articles and questions. You can filter results using knowledge search controls, such as filtering by knowledge base or author.

Social Q&A results also appear with knowledge articles when using global search.
Social Q&A uses the Contextual Search feature to generate search results. Questions appear in Contextual Search results, such as when creating an incident. The Social QA Question Search Context and Social QA Question Searcher records define the Social Q&A search. To ensure Social Q&A search functions as intended, do not modify these records.

**Social Q&A tags**

Tags organize questions and provide information about the question subject matter.

Social Q&A shares available tags with other applications allowing you to organize records consistently across the instance. Tags are stored on the Tags (label) table.

You can view a list of tags and filter by tag from the knowledge homepage. Clicking on a tag displays a list of knowledge articles and questions with that tag.

Only users who can edit a question can edit the associated tags. By default, only the question owner and knowledge managers can add or remove tags on questions.

**Knowledge feedback**

You can view and contribute to feedback on knowledge articles.

**Feedback options**

Enable or disable the feedback options using the Knowledge article view properties.

You can submit feedback for knowledge articles in these ways:

- Flag an article as incorrect or inappropriate.
- Provide a rating value for the article.
- Mark an article as helpful or not helpful.
- View comments, add a new comment, or reply to existing comments.

Users can view comments directly on the article. Knowledge managers can view the other types of feedback by navigating to Knowledge > Feedback.

Administrators and knowledge managers can disable some feedback options using fields on the Knowledge Base form. Administrators can configure feedback options using properties.

**Flagging articles**

You can flag an article for incorrect or inappropriate content. Click Flag Article in the article header to open a new window, allowing you to enter suggested changes.

The glide.knowman.use_live_feed property controls the display of knowledge article comments.

- If enabled, the system uses live feed to manage and display feedback on knowledge articles. Flagged comments do not appear on the Article View page. Users with the admin, knowledge_admin, and knowledge_manager roles can access flagged articles by navigating to Knowledge > Articles > All Flagged. Users with the knowledge role can access their flagged articles by navigating to Knowledge > Articles > My Flagged.
- If disabled, the author of the article and users with the admin, knowledge_admin, and knowledge_manager roles can see all flagged comments. Other users can see only their own flagged comments.
Note: You cannot disable flagging for an article until you have disabled the flagging for all feedback comments for that article.

Flagged comments are stored in the Knowledge Feedback (kb_feedback) table but not the Live Feed Messages (live_message) table.

Rating articles

The five stars below the article title allow you to indicate the article’s effectiveness on a scale of 1 to 5.

Marking articles

The question Helpful? at the bottom of the article allows you to indicate the usefulness of the article with a simple Yes or No answer.

Comments

Knowledge comments at the bottom of the article use live feed to enable a conversation around a knowledge article. For example, you can post replies to comments, add attachments, or Like comments.

Request a knowledge base

If existing knowledge bases do not fit your needs, you can request a new knowledge base through the service catalog. If the request is approved, you are added as the owner of the new knowledge base.

Role required: none

If no knowledge base exists that fit your needs, all users can request a new knowledge base.

1. Navigate to Self-Service > Service Catalog.
2. Select Can We Help You?.
3. Select the Request Knowledge Base catalog item.
4. Enter the reason you want the knowledge base, and a name for the knowledge base.
5. Click Submit.

You are notified when the request is approved or rejected. If the request is approved, you are added as the owner of the new knowledge base. You can then assign managers and manage articles in the new knowledge base.

Knowledge bases created through this request process are inactive by default, so you must activate the knowledge base to make it available for users.

Create a knowledge article

Knowledge contributors can create and edit knowledge articles within a knowledge base to share information across your organization.

Users with at least one role can create and edit knowledge. These users are known as knowledge contributors. Users without any role can read articles and submit feedback, but cannot create or edit articles.
Some knowledge bases may allow only certain users to contribute. For example, a member of the IT department can create knowledge articles in the IT knowledge base, such as desktop support information or articles describing company IT processes.

1. Navigate to **Self-Service > Knowledge**.
2. Click **Create An Article**.

3. Fill in the fields on the form, as appropriate.

**Knowledge form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge Base</td>
<td>The knowledge base selected for this article.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> An article can only be associated with one knowledge base.</td>
</tr>
<tr>
<td>Category</td>
<td>The category for this article. Select a <strong>Knowledge Base</strong> before you can select a category. Articles without a category appear on the knowledge homepage in the (empty) category.</td>
</tr>
<tr>
<td>Published</td>
<td>The date this knowledge article was published. This value is set when the article is published.</td>
</tr>
<tr>
<td>Valid to</td>
<td>The date this knowledge article expires. Articles do not appear in search results after the valid to date, or if the valid to date is empty.</td>
</tr>
<tr>
<td>Article type</td>
<td>The type of article, either HTML or wiki.</td>
</tr>
<tr>
<td>Workflow</td>
<td>(Read-Only) The publication state of the article, such as Draft or Published. When inserting a new article from an existing article, the state of the new article is reset to Draft.</td>
</tr>
<tr>
<td>Source</td>
<td>The task this knowledge article was created in response to, if any. This field is set automatically when you create the knowledge article from a task record.</td>
</tr>
</tbody>
</table>

**Note:** You must have user criteria “Can contribute” permission for at least one active knowledge base, otherwise the **Create An Article** button does not appear. See Knowledge Management v3 migration and Knowledge manager.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Attachment link     | Check box for downloading an attached file automatically when a user accesses the article, instead of opening the article view. Add one or more attachments to the article to use this option.  
  
  **Note:** You may attach multiple files, but most web browsers permit users to download only the first one. To ensure download of all the files, bundle them into an archive, such as with WinZip, and attach the archive. The Attachment link option applies to articles accessed from search links only. Articles accessed from links within other knowledge articles will not automatically download an attached file. |
| Display attachments | Check box for displaying attachments to users viewing this knowledge article. Attachments appear below the article text. Add one or more attachments to the article to use this option. |
| Short description  | The title of the article. This title appears when browsing and searching knowledge, and at the top of the article. |
| Text                | Content for the article. Use the [HTML editor](#) to create content. A preview of the content appears when browsing and searching knowledge. |

4. Click **Submit** to create the article.

After saving the article record, you can add tags to further organize the article.

Any additional steps required to publish the article, such as approvals, depend on the publishing workflow for the knowledge base.

- If there is no approval workflow set up, the article is immediately published.
- If there is an approval workflow set up: If the article is approved, it is published. If rejected, the article state is changed to Draft.

**Edit a knowledge article**

Knowledge contributors can edit/update knowledge articles within a knowledge base to update information shared across your organization.

**Role required:** knowledge

Users with at least one role can edit knowledge. These users are known as knowledge contributors. Users without any role can read articles and submit feedback, but cannot edit articles.

However, Knowledge managers can configure User Criteria to restrict access to certain Knowledge bases. For example, only members of the IT department can create or edit
knowledge articles in the IT knowledge base, such as desktop support information or articles describing company IT processes.

**Note:** If you have user criteria “Can contribute” permission for the specified knowledge base, but are not the article author, and do not have a knowledge base admin or manager role: The installed Knowledge Management Advanced Installer plugin requires the `glide.knowman.versioning.enabled` property (from the System Property (sys_properties) table) to be set to `false` to enable you to be able to make changes to unpublished articles within the knowledge base.

Edit an article using one of these options.

- **Edit published/unpublished articles with Versioning enabled:**
  1. Navigate to Knowledge > Articles
  2. Select an article from the Published or Unpublished category.
  3. From the article, click Checkout and edit the article.
  4. To save changes to:
     - an unpublished article, and to publish it at the same time, click Publish.
     - a published article, or to save changes to an unpublished article without publishing it, click Update.

- **Edit published articles from the Knowledge homepage or Service Portal:**
  1. Navigate to one of the following modules:
     - Self-Service > Knowledge
     - Knowledge > Homepage
     - Knowledge Service Portal homepage
  2. From the Knowledge homepage, search for and select the article to edit.
  3. From the article, click Edit, then from the Knowledge form record, edit the desired editable fields.
  4. Click Update to save changes.
If you edited an unpublished article, any additional steps required to publish an article, such as approvals, depend on the publishing workflow for the knowledge base.

**Select a knowledge article category**

Knowledge articles within a knowledge base are grouped by category. These groups can help you define the knowledge base taxonomy, and can help users find articles within that knowledge base.

As a knowledge contributor, when editing a knowledge article you can select categories using the Category picker, and add or edit categories if enabled for the knowledge base.

1. Click the reference lookup icon beside the **Category** field.

2. Select an existing category, or click the add category icon (+) to add a new category.
   After you select a category, you can click the pen icon to rename that category. Press the enter key or click outside the selected category to save the change.

   **Note:** Clicking **Cancel** while selecting a category cancels selecting a new category, but does not revert any changes you make to the categories such as renaming or adding new categories.

3. Fill in the fields on the form, as appropriate.
4. Optional: Select or add a subcategory.
5. Click **OK**.

**Move a knowledge article**

You can move articles between knowledge bases.

1. Edit a knowledge article.
2. Change the **Knowledge Base** field value.
   After moving an article, the Apply Default Values dialog box prompts you to populate certain fields in the article with default values from the new knowledge base. If the new knowledge base has no default values, the dialog box does not appear.
3. Click **OK** to overwrite fields with the default values, or **Cancel** to leave all fields unchanged.
A knowledge manager can define default values for articles in knowledge bases you manage using the **Set default knowledge field values** field on the Knowledge Base form.

4. Click **Update**.

**Retire a knowledge article**

Retired knowledge articles are not available to users except for administrators and knowledge administrators who can view them.

A knowledge article has an associated retirement workflow, similar to the publishing workflow. This allows administrators to configure these workflows, defining an approval and review process for retiring knowledge if appropriate.

When editing an article, click **Retire** to launch the retirement workflow associated with that article. If the article requires approval prior to retirement, the article goes to a pending approval state, and the workflow either finishes upon approval or cancels if rejected by a required approver.

**Note:** Retired knowledge articles cannot be searched for by external users or customers. To reuse a retired article, create a new article with the same content, which is published once approved.
Instant retire and Approval retire workflows

Create knowledge from an incident or problem

To create knowledge from an incident or problem, select the Knowledge check box on the incident or problem form and close the incident or problem record.
For detailed information on creating knowledge from an incident, refer to Create a knowledge article from an incident.

The short description from the incident or problem becomes the knowledge article title. Articles created this way are added to the knowledge base specified in the property glide.knowman.task_kb.

Depending on the value of the glide.knowman.submission.workflow property, knowledge created from an incident or problem may require additional approval. When this property is true, a submission record is created instead of a knowledge article. A user with the knowledge role must approve the submission to create a knowledge article.

Approving a submission creates a new knowledge article using the submission content.

1. Navigate to Knowledge > Open Submissions.
2. Select a submission record.
3. Review the submission to ensure the content and settings are correct.
4. Click Create Article.
   A new draft knowledge article is created. Articles created this way are added to the knowledge base specified in the property glide.knowman.task_kb.

You can edit the new knowledge article before publishing it, such as to select a category.

Import a Word document to a knowledge base

Import a Microsoft Word document to create a new knowledge article.

Role required: None. You must have user criteria "Can contribute" permission for at least one active knowledge base. If you cannot contribute, the Import Articles button does not appear.

| Note: | An administrator can control the visibility of the Import Articles button by setting the other knowledge property Hide the 'Import' functionality (button and drag-n-drop) for all users (glide.knowman.import.hide_import_functionality) to true. |

Importing documents to knowledge is available only from a computer browser. You cannot import documents from a mobile device.

You can import Microsoft Word .doc and .docx files.

| Note: | The file extension must be lowercase. |

When you import a document, text content from the document is used to create the knowledge article. The articles support all editing functions supported by the TinyMCE editor. All HTML supported by the TinyMCE editor such as tables, lists, and links, as well as styling such as bold and italics, are preserved. Images from the document are added as attachments to the knowledge article and embedded in the article body.

| Note: | You can import multiple files at a time. Closing the browser or navigating away cancels any in-progress uploads but does not delete articles created from completed imports. You cannot import documents to knowledge from mobile devices. |

The following styles and elements are preserved when importing a .doc or .docx file into a knowledge base. Styles and elements not included in this list may not be preserved when importing a document.

- Titles
1. Navigate to **Self-Service > Knowledge**.
2. Perform one of the following actions.
   - Click **Import Articles** and select one or more document files.
   - Drag one or more document files onto the knowledge homepage.
3. Select the **Knowledge base** to add the new article to.
   You can select only knowledge bases you can contribute to.
4. Optional: Select a **Category** from within that knowledge base.
   
   **Note:** Use the category picker to add a category. The picker does not differentiate between different category levels. You can select a category or sub category and add it to the **Category** field.
5. Optional: Select the **Publish** check box to start the publishing workflow for each imported article immediately after the import finishes.
   
   This check box applies only when importing to v3 knowledge bases and only if the **Show publish checkbox on the knowledge import pop-up** property is set to **Yes** on the Knowledge Management properties form. You cannot automatically publish articles imported to v2 knowledge bases.
   
   Knowledge v2 articles go into **Draft** state. Knowledge v3 articles go into **Review** or **Published** state, depending on the workflow attached to the knowledge base (Approval Publish or Instant Publish).
6. Click **Import**.
   
   A new article is created in the selected knowledge base and category using the content from the uploaded document. If you uploaded multiple documents, one article is created for each. If you use knowledge internationalization, the language of the new article is set to the currently selected system language.
   
   After the upload completes, a popup window appears displaying the number and short description of the newly-created articles. Click an article to view the full record.
   
   If any errors occur during the upload, a popup window appears to display the error.

---

**Knowledge manager**

Having multiple knowledge bases allows an organization to spread management responsibilities across multiple users, known as knowledge managers.

As a knowledge manager, you can assign other managers, define category structures, configure which users can read and contribute articles, move and pin articles, and modify most fields on the **Knowledge Base** form. You can also approve the publishing or retiring of knowledge articles...
those knowledge bases. You can enable Social Q&A for your knowledge bases if the Social Q&A application is active.

The primary manager of a knowledge base is the owner of that knowledge base. Each knowledge base must have one owner. There may be any number of additional managers for each knowledge base. All managers of a knowledge base, including the owner, automatically receive the knowledge_manager role.

**Pin a knowledge article**

You can pin a knowledge article to appear in the Featured content section of the knowledge homepage and at the top of knowledge search results page.

Role required: knowledge_manager, knowledge_admin, or admin

Pinning associates an article to specific keywords. You can search a keyword in the knowledge service portal or search results page to display articles in the Featured content section or at the top of the knowledge search results list.

- To display articles in the Featured content section, add a default keyword in the glide.knowman.default_keyword property Value field and add the same keyword to all articles you want to display in that section.
- To display articles at the top of the knowledge search results list, add a list of keywords to each article you want to display at the top of the list.

1. Navigate to Knowledge > Knowledge Bases.
2. Select a knowledge base.
3. In the Featured content related list, click New.
4. In the Knowledge field, search for and select the desired article.
5. In the Keywords field, click the lock/unlock toggle icon.
6. Click the lookup icon to open the Knowledge keywords list.

**Note:** Each keyword must be a single word and cannot contain spaces.

7. Select the keyword to add for this article.
   - Add the default keyword to display this article in the Featured content section during search.
   - Add all related keywords for the article to display it at the top of the knowledge search results page during search.

**Note:** You can create knowledge keywords, if it does not already exist in the list, and then add it to the article.

8. Click the lock/unlock toggle icon to add the keywords to the article.
9. Click Submit.

**Create a user criteria record in Knowledge Management**

You can create or modify a user criteria record in Knowledge Management. User criteria is used to control what users, groups, roles, companies, locations, and/or departments can access knowledge bases and articles.

Role required: user_criteria_admin

1. Navigate to Knowledge > Administration > User Criteria.
2. Click New or open a record.
3. Fill out the fields on the form as required. For field descriptions, refer to Create a user criteria record in Service Catalog

4. Click Submit.

Select user criteria for a knowledge base

You can specify user criteria to control which users can create, read, write, and retire knowledge articles within a knowledge base.

Role required: knowledge_manager, knowledge_admin, or admin

User criteria refers to knowledge base records that determine the users who can read or contribute to a knowledge base. User criteria definitions:

- **canRead**
  - users who can read all knowledge base articles

- **cantRead**
  - users who cannot read, create, or modify articles in the knowledge base

- **canContribute**
  - users who can read, create, and modify articles in the knowledge base

- **cantContribute**
  - users who cannot create or modify articles in the knowledge base

**No User Criteria**

If a knowledge base has no user criteria, all users can read its articles. Any user having at least one role can create and edit articles, unless they are members of the **cantContribute** user criteria.

If a knowledge base has **canRead** user criteria, but no **canContribute** user criteria, all users with at least one role can access and modify the knowledge base. This video demonstrates how to control Knowledge Management access through user criteria.

This video demonstrates how to control Knowledge Management access through user criteria.

1. Navigate to Knowledge > Knowledge Bases.
2. Select a knowledge base you manage.
3. Access one of these related lists, and then select or create user criteria records.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can read</td>
<td>Users who meet one of these criteria can read articles in this knowledge base.</td>
</tr>
<tr>
<td>Can contribute</td>
<td>Users who meet one of these criteria can create and edit articles in this knowledge base.</td>
</tr>
</tbody>
</table>
Can Read
Leveraging User Criteria to grant read access to Knowledge Bases & Knowledge Articles

User role: admin, knowledge_admin, KB-owner, KB-manager, CanContribute

No

Yes

User has cantRead role

No

User has canRead role, or KB requires no role

No

Yes

Can Read KBs and/or Article(s)

No Access to KB and/or Article(s)
Can Contribute
Leveraging User Criteria to grant access to Knowledge Bases & Knowledge Articles

User role: admin, knowledge_admin, KB-owner, KB-manager

No

User has cantContribute role

Yes → No Access to KB and/or Article(s)

Yes

User has canContribute role, or KB requires no role

No

Yes

Can Contribute to KB and/or Article(s)
### Order of System Validation (L->R)

<table>
<thead>
<tr>
<th>Contribute</th>
<th>Read</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>cantContribute (1)</td>
<td>cantRead (3)</td>
<td>canContribute (2)</td>
</tr>
</tbody>
</table>
| empty | empty | empty | empty | 1. All Users with role # Create  
| empty | empty | empty | User A | 2. All Users # Read  
| empty | User B | empty | empty | 3. All Users with role # Read  
| empty | User B | User A | empty | 4. All Users with role # Read  

<table>
<thead>
<tr>
<th>Contribute</th>
<th>Read</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>cantContribute (1)</td>
<td>cantContribute (2)</td>
<td>cantRead (3)</td>
</tr>
</tbody>
</table>
| empty | User C | empty | empty | 1. User C # Create  
| empty | User C | empty | User A | 2. User A # Read  

<table>
<thead>
<tr>
<th>Contribute</th>
<th>Read</th>
<th>Result</th>
<th>Permissions on KB (in the following order)</th>
</tr>
</thead>
<tbody>
<tr>
<td>cantContribute (1)</td>
<td>canContribute (2)</td>
<td>cantRead (3)</td>
<td>canRead (4)</td>
</tr>
<tr>
<td>empty</td>
<td>User C</td>
<td>User B</td>
<td>empty</td>
</tr>
<tr>
<td>1. User C # Create, Read</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. User B # Denied Read</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. All Other Users # Read</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>empty</td>
<td>User C</td>
<td>User B</td>
<td>User A</td>
</tr>
<tr>
<td>1. User C # Create, Read</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. User B # Denied Read</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. User A # Read</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Contribute</th>
<th>Read</th>
<th>Result</th>
<th>Permissions on KB (in the following order)</th>
</tr>
</thead>
<tbody>
<tr>
<td>cantContribute (1)</td>
<td>canContribute (2)</td>
<td>cantRead (3)</td>
<td>canRead (4)</td>
</tr>
<tr>
<td>User D</td>
<td>empty</td>
<td>empty</td>
<td>empty</td>
</tr>
<tr>
<td>1. User D # Denied Create</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. All Other Users with role # Create</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. All Users # Read</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User D</td>
<td>empty</td>
<td>empty</td>
<td>User A</td>
</tr>
<tr>
<td>1. User D # Denied Create, Read</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. All Other Users with role # Create</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. User A # Read</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. All Users with role # Read</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contribute</td>
<td>Read</td>
<td>Result</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>cantContribute (1)</td>
<td>cantRead (3)</td>
<td>canRead (4)</td>
<td></td>
</tr>
<tr>
<td>User D</td>
<td>empty</td>
<td>User B</td>
<td>empty</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1. User D # Denied Create</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. All Other Users with role # Create</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3. User B # Denied Read</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4. All Users # Read</td>
</tr>
</tbody>
</table>

| | | |
| | | |
| | | |

<table>
<thead>
<tr>
<th>Contribute</th>
<th>Read</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>cantContribute (1)</td>
<td>cantRead (3)</td>
<td>canRead (4)</td>
</tr>
<tr>
<td>User D</td>
<td>empty</td>
<td>User B</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| | | |
| | | |
| | | |

<table>
<thead>
<tr>
<th>Contribute</th>
<th>Read</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>cantContribute (1)</td>
<td>cantRead (3)</td>
<td>canRead (4)</td>
</tr>
<tr>
<td>User D</td>
<td>User C</td>
<td>empty</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User D</td>
<td>User C</td>
<td>empty</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contribute</td>
<td>Read</td>
<td>Result</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>canContribute (1)</td>
<td>cantRead (3)</td>
<td>empty</td>
</tr>
<tr>
<td>User D</td>
<td>User B</td>
<td>1. User D # Denied Create</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. User C # Create, Read</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. User B # Denied Read</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. All Other Users # Read</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>cantContribute (1)</th>
<th>canContribute (2)</th>
<th>cantRead (3)</th>
<th>canRead (4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>User D</td>
<td>User C</td>
<td>User B</td>
<td>User A</td>
</tr>
<tr>
<td>1. User D # Denied Create, Read</td>
<td>2. User C # Create, Read</td>
<td>3. User B # Denied Read</td>
<td>4. User A # Read</td>
</tr>
</tbody>
</table>

**Note:** In the tables of rules, an implicit last rule is: All Users # Denied Create, Read.

### Enable user criteria system property to override role read access

Add the glide.knowman.search.apply_role_based_security system property to enable user criteria to control read access of knowledge bases or articles over roles.

Role required: admin

1. Follow the steps to [Add a system property](#).
2. Add the `glide.knowman.search.apply_role_based_security` property, and set the property value to `false`. This enables specified user criteria to override canRead access specified for roles.

### Select user criteria for an article

You can specify user criteria for an article to control which users can read the article.

If an article has no user criteria selected, the article is available to all users who have access to that knowledge base (based on the user criteria for the knowledge base). Knowledge base user criteria restrictions override article-level user criteria. For example, a knowledge base that is configured to restrict user access overrides any access granted at the article level.

If a user has contribute access to the knowledge base, article-level user criteria are not evaluated and the user can read all articles in the knowledge base. If a user has read access to the knowledge base, article-level user criteria are evaluated to determine if the user has read access to the article.
On the article level, if **Can read** user criteria is defined, only those users specified can read the article. If an article has **Cannot read** user criteria defined, those users specified are denied reading the article. **Cannot read** user criteria overrides **Can read** user criteria for articles.

1. Navigate to **Self-Service > My Knowledge Articles**.
2. Select an article.
3. Select the desired user criteria for the **Can Read** and **Cannot Read** fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can Read</td>
<td>Users who meet one of these criteria can read the article.</td>
</tr>
<tr>
<td>Cannot Read</td>
<td>Users who meet one of these criteria are denied reading the article (regardless of the <strong>Can Read</strong> setting for the user).</td>
</tr>
</tbody>
</table>

**Note:** If the **Can Read** and **Cannot Read** fields are not visible, add the fields to the form by configuring the form layout (click the form context menu icon and select **Configure > Form Layout**).
<table>
<thead>
<tr>
<th>Knowledge base level</th>
<th>Article level</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Read</td>
<td>canRead</td>
</tr>
<tr>
<td>Contribute</td>
<td></td>
<td>User</td>
</tr>
<tr>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>Yes</td>
<td>empty</td>
<td>empty</td>
</tr>
<tr>
<td></td>
<td>empty</td>
<td>User</td>
</tr>
<tr>
<td></td>
<td>User</td>
<td>empty</td>
</tr>
<tr>
<td></td>
<td>User</td>
<td>User</td>
</tr>
</tbody>
</table>

**Note:**
- When article-level read access is assigned to an article, only the user who belongs to that particular user criteria can read the article. Other users are restricted.
- Users with contribute access to a knowledge base can also read articles even if they are not in the defined Can Read user criteria.
- Ownership group users who are either members or managers of groups assigned to an article will have access to contribute to articles even if they don’t have contribute access to the knowledge base.

**Define a knowledge article category**

Each knowledge base has a hierarchy of categories that organizes the articles.

You must have CanContribute access to the knowledge base or have a knowledge_admin or admin role.

You can define a hierarchy for categories by creating parent-child relationships. The category hierarchy is saved in the Full category field in the Knowledge Category (kb_category) table.

You can create and edit categories separately for each knowledge base.

1. Navigate to Knowledge > Knowledge Bases.
2. Select a knowledge base you manage.
3. Choose an option.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a top-level category.</td>
<td>Navigate to the Knowledge Categories related list and click New.</td>
</tr>
<tr>
<td>Create a child category.</td>
<td>Expand an existing category and click New within the expanded section.</td>
</tr>
</tbody>
</table>
4. Enter a **Label** for the category. The label appears as the name of the category.
5. Optional: Enter a **Value** you can use when referencing the category in scripts.
6. Click **Submit**.

In addition to using categories defined by a knowledge manager, knowledge contributors can add and edit categories when editing an article.

**Assign a knowledge base manager**

You can assign users as managers of a knowledge base.
Role required: knowledge_admin, or admin

1. Navigate to Knowledge > Knowledge Bases.
2. Select a knowledge base you manage.
3. In the Managers field, click the unlock icon.
4. Add one or more users.
5. Click Update.

After you save the knowledge base record, users selected as managers automatically receive the knowledge_manager role if they do not have it already.

You can remove a knowledge base manager by removing that user from the Managers field. If the user is not a manager of any other knowledge base, the knowledge_manager role is removed from that user.

**Knowledge administration**

As an administrator, you are responsible for setting up knowledge bases, configuring knowledge workflows, and customizing knowledge homepages. Most day-to-day management functions are performed by knowledge managers.

The following podcast offers additional information on using the Knowledge Base Application.

**Create a knowledge base**

Create a knowledge base to provide a self-service platform for users to store, share, and manage content. Configure knowledge bases into product or service categories and manage user access based on permissions. Customize workflows for publishing and retiring articles in the knowledge base.

Understand the requirements for setting up a knowledge base.

Role required: knowledge_admin or admin

1. Navigate to Knowledge > Administration > Knowledge bases.
2. In the Knowledge Bases list, click New.
3. On the form, fill in the following fields as appropriate:

<table>
<thead>
<tr>
<th>Knowledge base form</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Unique name for the knowledge base.</td>
</tr>
<tr>
<td>Icon</td>
<td>An image that provides a visual reference to describe the knowledge base. This image is displayed next to all articles from this knowledge base in the article search results page.</td>
</tr>
<tr>
<td>Disable commenting</td>
<td>Check box to disable commenting. If selected, users cannot comment on articles in the knowledge base.</td>
</tr>
<tr>
<td>Disable suggesting</td>
<td>Check box to disable edit suggestions. If selected, users cannot suggest edits to articles in the knowledge base.</td>
</tr>
<tr>
<td><strong>Title</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Disable category editing</td>
<td>Check box to disable editing of knowledge categories. If selected, only knowledge managers can add or edit knowledge categories for the knowledge base.</td>
</tr>
<tr>
<td>Checklist</td>
<td>Checklist to evaluate the quality of articles in the knowledge base.</td>
</tr>
<tr>
<td>Owner</td>
<td>The user responsible for the knowledge base. A knowledge base owner can assign other roles to the knowledge base.</td>
</tr>
<tr>
<td>Manager</td>
<td>Users who perform administrative functions on the knowledge base.</td>
</tr>
<tr>
<td>Publish workflow</td>
<td>The workflow for publishing the articles in the knowledge base.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Knowledge - Instant Publish</strong>: publishes articles in the knowledge base without requiring an approval.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Knowledge - Approval Publish</strong>: requests approval from the manager of the knowledge base before moving the articles to the published state.</td>
</tr>
<tr>
<td>Retire workflow</td>
<td>The workflow for retiring the articles in the knowledge base.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Knowledge - Instant Retire</strong>: retires articles in the knowledge base without requiring an approval.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Knowledge - Approval Retire</strong>: requests approval from the manager of the knowledge base before moving the articles to the retired state.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box to make the knowledge base visible to all users.</td>
</tr>
<tr>
<td>Enable social questions and answers</td>
<td>Check box to enable social Q&amp;A for articles in the knowledge base.</td>
</tr>
<tr>
<td>Description</td>
<td>A short description to describe the knowledge base.</td>
</tr>
<tr>
<td>Set default knowledge field values</td>
<td>Default configuration settings for the knowledge base.</td>
</tr>
<tr>
<td>Related products</td>
<td>List of products related to the knowledge base content.</td>
</tr>
</tbody>
</table>

4. Right-click the form header and click **Save**.
5. In the related list section, view or configure the following items related to the knowledge base:

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge</td>
<td>List of knowledge articles stored in this knowledge base.</td>
</tr>
<tr>
<td>Questions</td>
<td>List of Social Q&amp;A questions stored in this knowledge base.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Can Read</td>
<td>The Can Read user criteria list for this knowledge base.</td>
</tr>
<tr>
<td>Can Contribute</td>
<td>The Can Contribute user criteria list for this knowledge base.</td>
</tr>
<tr>
<td>Featured Content</td>
<td>List of knowledge articles that appear in the homepage <strong>Featured Content</strong> section based on the corresponding keyword search set for each article.</td>
</tr>
<tr>
<td>Knowledge Categories</td>
<td>List of knowledge categories associated with this knowledge base.</td>
</tr>
</tbody>
</table>

6. Click **Submit**.

**Knowledge workflows**

The publishing and retirement processes for a knowledge article are controlled by workflows defined for the knowledge base that the article belongs to.

You can assign different workflows to each knowledge base.

You can use one of the default workflows, or create your own workflows to define custom publishing and retirement processes for different types of knowledge.

For the workflows that require approval, you can configure which users can approve or reject by editing the `getApprovers()` function in the `KBWorkflow` script include.

**Default knowledge workflows**

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge - Approval Publish</td>
<td>Requests approval from a manager of the knowledge base before moving the article to the published state. The workflow is canceled and the article remains in the draft state if any manager rejects the request.</td>
</tr>
<tr>
<td>Knowledge - Approval Retire</td>
<td>Requests approval from a manager of the knowledge base before moving the article to the retired state. The workflow is canceled and the article remains in the published state if any manager rejects the request.</td>
</tr>
<tr>
<td>Knowledge - Instant Publish</td>
<td>Immediately publishes a draft article without requiring an approval.</td>
</tr>
<tr>
<td>Knowledge - Instant Retire</td>
<td>Immediately retires a published article without requiring an approval.</td>
</tr>
<tr>
<td>Knowledge - Publish Knowledge</td>
<td>A subflow that moves the knowledge article to the published state. You can use this subflow when defining your own workflow.</td>
</tr>
<tr>
<td>Knowledge - Retire Knowledge</td>
<td>A subflow that moves the knowledge article to the retired state. You can use this subflow when defining your own workflow.</td>
</tr>
</tbody>
</table>
Knowledge properties

As an administrator, you can configure the look and functionality of many knowledge base features with knowledge properties.

You can access knowledge properties by navigating to Knowledge > Properties.

Knowledge portal properties

Knowledge portal properties control the look and functionality of the legacy portal page. This portal page lists recent knowledge articles and their publishing dates, organized by topic.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of columns on Knowledge portal pages.</td>
<td>Set the number of columns for arranging topics on the knowledge portal. <strong>Note:</strong> This property applies only to Knowledge v2 pages. This property is not supported on Knowledge v3 pages.</td>
</tr>
<tr>
<td>(glide.knowman.columns)</td>
<td></td>
</tr>
<tr>
<td>Maximum number of articles per content block on the home page</td>
<td>Enter the maximum number of articles to display in the Most Useful and Most Viewed sections of the knowledge homepage. <strong>Note:</strong> This property applies only to Knowledge v2 pages. This property is not supported on Knowledge v3 pages.</td>
</tr>
<tr>
<td>(glide.knowman.content_block_limit)</td>
<td></td>
</tr>
<tr>
<td>Omit empty Knowledge topics and categories.</td>
<td>Select the Yes check box to display topic sections only if there are articles for the topic. Clear the check box to show all topic sections, even those with no assigned articles. <strong>Note:</strong> This property does not apply to the News category. <strong>Note:</strong> This property applies only to the default knowledge base and the legacy knowledge portal. Knowledge v3 articles do not specify a topic. Therefore, this property applies only to Knowledge v2 pages. This property is not supported on Knowledge v3 pages.</td>
</tr>
<tr>
<td>(glide.knowman.show_only_populated)</td>
<td></td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Show Knowledge section descriptions. (glide.knowman.show_descriptions) | Select the Yes check box to display topic descriptions in the knowledge portal. To enter these descriptions:  
1. Edit an existing knowledge article.  
2. Right-click the Topic field label and choose Show Choice List.  
3. Open the record for the topic name and enter the description into the Hint field.  
Clear the check box to omit section descriptions from the knowledge portal.  
**Note:** This property applies only to Knowledge v2 pages. This property is not supported on Knowledge v3 pages. |
| Number of Knowledge Base items to preview in a section. (glide.knowman.section_limit) | Set the maximum number of articles per topic for the knowledge portal. The specific articles shown depends on the Knowledge section sort field property setting.  
**Note:** This property applies only to Knowledge v2 pages. This property is not supported on Knowledge v3 pages. |
| Knowledge section sort field. (glide.knowman.section_sort) | Select the default order for articles within each topic section on the knowledge portal.  
- Published: uses the date published.  
- View count: uses the number of times articles have been viewed during the period specified in the Number of days used when summing article views property.  
- Alphabetically: uses the first letter of the article title (Short description field).  
**Note:** This property applies only to Knowledge v2 pages. This property is not supported on Knowledge v3 pages. |
| Knowledge Base section sort direction. (glide.knowman.section_sort_direction) | Select the order, ascending or descending, in which articles are listed within each topic section on the knowledge portal. The value used for sorting is set in the Knowledge section sort field property.  
**Note:** This property applies only to Knowledge v2 pages. This property is not supported on Knowledge v3 pages. |
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Show unpublished articles in Knowledge Base portal and topic lists.</strong> <em>(glide.knowman.show_unpublished)</em></td>
<td>Select the <strong>Yes</strong> check box to allow users to see unpublished articles in the knowledge portal and knowledge search results. Use the subsequent <strong>List of roles...</strong> properties to designated which users can see articles in various unpublished states. If this is not selected, users with appropriate roles can access unpublished articles through other modules of the <strong>Knowledge Base</strong> application.</td>
</tr>
<tr>
<td><strong>List of roles (comma separated) that can see articles in the Review workflow state in the Knowledge portal and Topic list.</strong> <em>(glide.knowman.section.view_roles.review)</em></td>
<td>Enter role names exactly as they appear in <strong>User Administration &gt; Roles.</strong> If <strong>Show unpublished articles in Knowledge Base portal and topic lists</strong> is selected, users with these roles see articles in the Review workflow state in the knowledge portal, in the topic list that appears when they click a topic title on the portal, and in knowledge search results.</td>
</tr>
<tr>
<td><strong>List of roles (comma separated) that can see articles in the Draft workflow state in the Knowledge portal and Topic list.</strong> <em>(glide.knowman.section.view_roles.draft)</em></td>
<td>Enter role names exactly as they appear in <strong>User Administration &gt; Roles.</strong> If <strong>Show unpublished articles in Knowledge Base portal and topic lists</strong> is selected, users with these roles see articles in the Draft workflow state in the knowledge portal, in the topic list that appears when they click a topic title on the portal, and in knowledge search results.</td>
</tr>
<tr>
<td><strong>Define roles that can view articles in other/custom workflow states. Do not include Draft and Review states, as they are already defined in other properties.</strong> <em>(Format - stage: [roles];)</em> For example:</td>
<td>Enter role names exactly as they appear in <strong>User Administration &gt; Roles.</strong> If <strong>Show unpublished articles in Knowledge Base portal and topic lists</strong> is selected, define the custom field and role as <strong>workflow state: [roles];</strong>. The users with these roles see articles in the custom workflow state on the knowledge portal.</td>
</tr>
<tr>
<td><strong>The number of articles that are asynchronously loaded when scrolling down in the new search results page.</strong> <em>(glide.knowman.search.articles_per_page)</em></td>
<td>Enter the number of articles to be displayed during a search. <strong>Note:</strong> This property applies only to Knowledge v3 pages. This property is not supported on Knowledge v2 pages.</td>
</tr>
<tr>
<td><strong>Show only Knowledge topic titles on portal page (no article links).</strong> <em>(glide.knowman.home_titlesonly)</em></td>
<td>Select the <strong>Yes</strong> check box to omit all article titles from the knowledge portal and show only the topic names. Users can click the topic title to see the list of related articles. <strong>Note:</strong> This property applies only to Knowledge v2 pages. This property is not supported on Knowledge v3 pages.</td>
</tr>
<tr>
<td><strong>Number of days (integer, default 30) used when summing article views. Views older than this are not considered when sorting articles based on view count. 0 means consider all views.</strong> <em>(glide.knowman.view_age.days)</em></td>
<td>Enter a number of days to consider when calculating view count. This is used only when the <strong>Knowledge section sort field</strong> property is set to <strong>View count.</strong> The <strong>view_count</strong> field in the knowledge record will be updated periodically to reflect the view count based on this property. For example, if you enter 60, the view count is the total number of views in the past 60 days. Enter 0 to have ServiceNow consider all views, regardless of date.</td>
</tr>
</tbody>
</table>
## Knowledge search properties

Knowledge search properties give you control over the search options available to users and the presentation of search results.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Automatically place cursor in Knowledge portal search box.</strong> <em>(glide.knowman.portal_search_focus)</em></td>
<td>Select the <strong>Yes</strong> check box to have ServiceNow place the cursor in the search field when a user opens the knowledge portal. Clear the check box to have users click in the search field before entering a search term. <strong>Note:</strong> This property applies only to Knowledge v2 pages. This property is not supported on Knowledge v3 pages.</td>
</tr>
</tbody>
</table>

### Knowledge search properties

Knowledge search properties give you control over the search options available to users and the presentation of search results.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Knowledge search result order.** *(glide.knowman.order.search)* | Select the order for displaying search results:  
- **Number of Views:** orders search results based on the **Number of days used when summing article views** property.  
- **Relevancy:** orders search results based on content that is similar to the search term.  
- **Last Modified:** orders search results based on modification date. |
| **Search method used when searching Knowledge from a task or directly in the Knowledge Base.** *(glide.knowman.search.operator)* | Select the search approach to use when the search term includes multiple words:  
- **OR query:** returns articles that contain at least one word from the search term.  
- **AND then OR query:** first searches for articles that include all words in the search term (an AND query). If no matches are found, an OR query is performed. |
<p>| <strong>Show author in knowledge search results.</strong> <em>(glide.knowman.search.show_author)</em> | Select this check box to include the author of each article in knowledge search results. If the article versioning feature is enabled, articles with a version number less than or equal to 1.0 display <strong>Authored by &lt;name&gt;</strong> and articles with a version number greater than 1.0 display <strong>Revised by &lt;name&gt;</strong>. |
| <strong>Show last modified date and time in knowledge search results.</strong> <em>(glide.knowman.search.show_last_modified)</em> | Select this check box to include the date and time each article was last edited in knowledge search results. |
| <strong>Show publish date in knowledge search results.</strong> <em>(glide.knowman.search.show_published)</em> | Select this check box to include the date each article was published in knowledge search results. |
| <strong>Show category in knowledge search results.</strong> <em>(glide.knowman.search.show_category)</em> | Select this check box to include the category breadcrumbs of each article in knowledge search results. |
| <strong>Show number of views in knowledge search results.</strong> <em>(glide.knowman.search.show_view_count)</em> | Select this check box to include the number of times each article was viewed in knowledge search results. |</p>
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| How to display attachments in Knowledge Search Results. (glide.knowman.search.attachment) | Select the behavior of how the attachments are shown in the search results:  
- Do not show attachment  
- Show only link for attachment  
- Show attachment with text snippet (default)  
For best performance, select **Do not show attachment**, or **Show only link for attachment**. |
| Show relevancy in knowledge search results. (glide.knowman.search.show_relevancy) | Select this check box to show how relevant each search result is based on the search string.  
**Relevancy** value is only shown when knowledge search result order property is set to **Relevancy**. |
| Enable instant search results for knowledge. (glide.knowman.search.instant_results) | Select this check box to enable instant search for search results. The default is **No**. |
| Show Knowledge Base name in Knowledge search results. (glide.knowman.search.show_knowledgebase) | Select this check box to display the knowledge base to which the knowledge base article belongs. For example, **IT**. |
| Show average rating from knowledge search results. (glide.knowman.search.show_rating) | Select this check box to display the average star ratings for knowledge base articles. |
| Show article number in knowledge search results. (glide.knowman.search.show_article_number) | Select this check box to display the article number for each article in the search result.  
If the article versioning feature is enabled, the article number and the version number are displayed for each article in the search result.  
**Note:** This property does not apply to contextual search results. |
| Specify default language for searching articles. (glide.knowman.search.default_language) | Set the property to the desired default language for searching articles.  
- **String**  
- **Default value:** user-specified  
- **Location:** System Properties  
**Note:** If the glide.knowman.enable_multi_language_search property is set to **True**, then the multi-language search capability overrides the default language search capability. |
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable multi-language search.</td>
<td>Set the property to <strong>True</strong> to enable search for multiple languages simultaneously.</td>
</tr>
</tbody>
</table>
| (glide.knowman.enable_multi_language_search)                            | - **Type**: true | false  
- **Default value**: false  
- **Location**: System Properties  

**Note:** If this property is set to **True**, it overrides the setting for the glide.knowman.search.default_language property.

---

**Knowledge article view properties**

Article view properties give you control over the meta data and rating options that appear with articles. They also enable you to grant access to individual feedback options based on user role.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show tasks to which an article has been recently attached.</td>
<td>Select the <strong>Yes</strong> check box to have article view include a list of tasks associated with the article. Knowledge articles can be attached to a task by clicking the <strong>Attach to Task</strong> button after searching from a form.</td>
</tr>
<tr>
<td>(glide.knowman.recent_tasks.display)</td>
<td></td>
</tr>
<tr>
<td>Number of attached tasks to display when viewing an article.</td>
<td>Specify the maximum number of tasks to list in article view.</td>
</tr>
<tr>
<td>(glide.knowman.recent_tasks)</td>
<td></td>
</tr>
</tbody>
</table>
| Show article rating section, which may optionally include yes/no rating, star rating, and flagging options. | Select the **Yes** check box to display the rating options for users with specific roles. Clear this check box to omit the rating section for all users, regardless of role.  
The **Feedback** field is always displayed for all users. |
| (glide.knowman.show_rating_options)                                     |                                                                                                                                                                                                              |
| List of roles (comma separated) that can see an article's rating section, which may optionally include yes/no rating, star rating, and flagging option. | Enter role names exactly as they appear in **User Administration > Roles**. If **Show article rating section**... is selected, users with the roles listed here see the yes/no rating, star rating, and flagging options, according to related property settings.  
Be sure to include all roles that should be permitted to see any of these rating options. Separate properties enable you to identify specific roles for each option separately. All roles in those properties must also be listed here. |
<p>| (glide.knowman.show_rating_options.roles)                              |                                                                                                                                                                                                              |
| Show the &quot;Was this article helpful?&quot; yes/no rating option.              | Select the <strong>Yes</strong> check box to display the &quot;Was this article helpful?&quot; rating to users with roles set in the associated property. This appears only if the <strong>Show article rating section</strong>... property is selected. |
| (glide.knowman.show_yn_rating)                                          |                                                                                                                                                                                                              |</p>
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>List of roles (comma separated) that can see yes/no &quot;Was this article helpful?&quot; rating option. (glide.knowman.show_yn_rating.roles)</td>
<td>Enter role names exactly as they appear in User Administration &gt; Roles. If both Show article rating section... and Show the &quot;Was this article helpful?&quot; properties are selected, users with the roles listed here see the &quot;Was this article helpful?&quot; rating in article view. All roles listed here must also be listed in the List of roles that can see an article's rating section...&quot; property.</td>
</tr>
<tr>
<td>Show &quot;Create Incident&quot; link after a Knowledge article is rated not helpful. (glide.knowman.create_incident_link.display)</td>
<td>Select the Yes check box to display the Create Incident link after a user rates an article as not helpful. To find the URL, open the appropriate page, then right-click the header bar and choose Copy URL. Highlight the URL that appears and use the browser's copy and paste feature to place it into this property field.</td>
</tr>
<tr>
<td>URL used for the &quot;Create Incident&quot; link after rating a Knowledge article not helpful. (glide.knowman.create_incident_link)</td>
<td>Enter the URL for the page where users can create an incident only if the Show &quot;Create Incident&quot; link...&quot; property is selected. To find the URL, open the appropriate page, then right-click the header bar and choose Copy URL. Highlight the URL that appears and use the browser's copy and paste feature to place it into this property field.</td>
</tr>
<tr>
<td>Show five-star rating option. (glide.knowman.show_star_rating)</td>
<td>Select the Yes check box to display the five-star rating to users with roles set in the associated property. This appears only if the Show article rating section... property is selected.</td>
</tr>
<tr>
<td>List of roles (comma separated) that can see five-star rating option. (glide.knowman.show_star_rating.roles)</td>
<td>Enter role names exactly as they appear in User Administration &gt; Roles. If both Show article rating section... and Show five-star rating option properties are selected, users with the roles listed here see the five-star rating option in article view. All roles listed here must also be listed in the List of roles that can see an article's rating section...&quot; property.</td>
</tr>
<tr>
<td>Show 'Flag Article' option to identify incomplete/inaccurate articles. (glide.knowman.show_flag)</td>
<td>Select the Yes check box to display the flag article option to users with roles set in the associated property. This appears only if the Show article rating section... property is selected.</td>
</tr>
<tr>
<td>List of roles (comma separated) that can flag incomplete/inaccurate articles. (glide.knowman.show_flag.roles)</td>
<td>Enter role names exactly as they appear in User Administration &gt; Roles. If both Show article rating section... and Show &quot;Flag Article&quot; option properties are selected, users with the roles listed here see the flag article option in article view. All roles listed here must also be listed in the List of roles that can see an article's rating section...&quot; property.</td>
</tr>
<tr>
<td>Show user comments on knowledge articles. (glide.knowman.show_user_feedback)</td>
<td>Select an option for showing user comments When article loads, When user clicks link to show comments, or Never for users with roles set in the associated property.</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>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>List of roles (comma separated) that can see user comments on an article. (glide.knowman.show_user_feedback.roles)</td>
<td>Enter role names exactly as they appear in User Administration &gt; Roles. If the Show user comments on knowledge articles property is selected, users with the roles listed here see user comments in article view.</td>
</tr>
<tr>
<td>Maximum number of user comments displayed on a knowledge article. (glide.knowman.feedback.display_threshold)</td>
<td>Set the maximum number of user comments to display. If no value is set, all comments are displayed. This property does not apply to live feed comments on the article view page.</td>
</tr>
</tbody>
</table>
| Use Live Feed for Knowledge feedback. (glide.knowman.use_live_feed) | Set the property to True to use live feed to manage and display feedback on knowledge articles.  
- **Type:** true | false  
- **Default value:** false  
- **Location:** System Properties |

**Knowledge homepage properties**

Knowledge homepage properties control the featured content on the knowledge homepage.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display or hide the count of articles and questions in the Knowledge Homepage. (glide.knowman.show_number_on_homepage)</td>
<td>Select to display or hide the count of knowledge articles and questions on the Knowledge homepage.</td>
</tr>
<tr>
<td>Default keyword for getting pinned articles (glide.knowman.default_keyword)</td>
<td>Enter a default keyword for pinned articles. Articles pinned with the specified keyword appear in the Featured Content section of the knowledge homepage.</td>
</tr>
<tr>
<td>Display or hide the count of articles and questions in the category and child categories (glide.knowman.show_number_on_categories)</td>
<td>Select to display the count of articles and questions within each category, including subcategories, when browsing or searching knowledge bases.</td>
</tr>
<tr>
<td>Show Knowledge Home page when user has access to only one Knowledge Base (glide.knowman.show_home_if_one_kb)</td>
<td>Select to display the Knowledge homepage when the current user has access to only one knowledge base.</td>
</tr>
<tr>
<td>Default header title for the pinned articles section on knowledge home pages. (glide.knowman.default_pinned_section_header_title)</td>
<td>Enter a title for the Featured Content section of the knowledge homepage.</td>
</tr>
</tbody>
</table>

**Other knowledge properties**

Additional knowledge properties let you control general knowledge management features.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>When attaching an article to an incident, copy the content into this field. (glide.knowman.attach.fields)</td>
<td>When a user searches knowledge from a task form (such as an incident, problem, or change) and clicks the Attach to Task button for an article, the system copies the article number and content into the field specified here. You can specify a separate field for each table you want to attach articles to as a comma-separated list. Use dot walking to copy the article content into related records. If a specified field does not exist, that field is ignored.</td>
</tr>
<tr>
<td>Knowledge Management logo to display if running out of the ServiceNow frames. (glide.knowman.frameless_logo)</td>
<td>Click the reference lookup tool (Icon Reference Lookup) and choose an image file to be displayed on knowledge pages that are used outside of the ServiceNow application frames. For example, the logo image selected here appears if you create a Content Management System site that includes knowledge pages. You can also enter the Name of an image stored in the database to use that image. Note: This property applies only to Knowledge v2 pages. This property is not supported on Knowledge v3 pages.</td>
</tr>
<tr>
<td>Hide the 'Import' functionality (button and drag-n-drop) for all users. (glide.knowman.import.hide_import_functionality)</td>
<td>Select Yes to hide the Import Articles button. If you have not yet migrated to Knowledge v3 and are using legacy Knowledge v2, you can configure the visibility of the Import Articles button to prevent users from importing articles to knowledge bases.</td>
</tr>
<tr>
<td>Show publish check box on the knowledge import pop-up.  (glide.knowman.import.show_publish_checkbox)</td>
<td>Select No to remove the Publish check box on the knowledge import form so that an article cannot be published as part of the import process. Default is yes.</td>
</tr>
<tr>
<td>Use submission workflow.  (glide.knowman.submission.workflow)</td>
<td>Select the Yes check box to use the knowledge submission workflow instead of the standard knowledge workflow. If this option is selected, each time a user creates knowledge from an incident or problem, the content is placed into a submission record instead of a draft article. Transforming knowledge submissions into articles follows a specific workflow.</td>
</tr>
<tr>
<td>The sys_id of the knowledge base when creating knowledge from task records. (glide.knowman.task_kb)</td>
<td>Enter the sys_id of the knowledge base to put new knowledge articles created from tasks in.</td>
</tr>
<tr>
<td>Before displaying an article's text in search results or the article view, check field-level ACLs on appropriate field: kb_knowledge.text (HTML article) or kb_knowledge.wiki (wiki text article). (glide.knowman.text.check_can_read)</td>
<td>Select this check box if users must have ACL-based permission to view text fields on the Knowledge (kb_knowledge) table to read article previews in knowledge search results.</td>
</tr>
</tbody>
</table>
When showing a list of articles through the Knowledge portal (using the `kb_list` UI Page), remove articles the user cannot see before building the list. (`glide.knowman.list.filter`)

Enter the value as `true` to enable removal of articles that user cannot see before building the articles list in the knowledge portal.

- **Type:** true | false
- **Default value:** false
- **Location:** System Properties

If you have large number of articles in your knowledge base, setting this property to `true` will negatively impact performance.

### Knowledge Social Q&A properties

The system administrator can set the limit for the number of times users can ask, answer, or subscribe to Social Q&A questions, or comment on the questions and answers using the Social Q&A system properties.

To open the System Properties (sys_properties) table, enter `sys_properties.list` in the navigation filter.

**Note:** If the **Value** field for the any of the Social Q&A properties is left blank, then a rate limit does not apply for that particular property.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Maximum number of Social Q&amp;A questions that can be posted per user per day.</strong>&lt;br&gt;<code>sn_kb_social_qa.max_questions_per_user_daily</code></td>
<td>Enter the maximum number of times a user can post Social Q&amp;A questions per day.</td>
</tr>
<tr>
<td><strong>Type:</strong> Integer&lt;br&gt;<strong>Default value:</strong> 500&lt;br&gt;<strong>Location:</strong> System Properties</td>
<td></td>
</tr>
<tr>
<td><strong>Maximum number of Social Q&amp;A answers that can be posted per user per day.</strong>&lt;br&gt;<code>sn_kb_social_qa.max_answers_per_user_daily</code></td>
<td>Enter the maximum number of times a user can post answers to the Social Q&amp;A questions per day.</td>
</tr>
<tr>
<td><strong>Type:</strong> Integer&lt;br&gt;<strong>Default value:</strong> 500&lt;br&gt;<strong>Location:</strong> System Properties</td>
<td></td>
</tr>
<tr>
<td><strong>Maximum number of Social Q&amp;A comments that can be posted per user per day.</strong>&lt;br&gt;<code>sn_kb_social_qa.max_comments_per_user_daily</code></td>
<td>Enter the maximum number of times a user can post comments to the Social Q&amp;A questions or answers per day.</td>
</tr>
<tr>
<td><strong>Type:</strong> Integer&lt;br&gt;<strong>Default value:</strong> 500&lt;br&gt;<strong>Location:</strong> System Properties</td>
<td></td>
</tr>
<tr>
<td><strong>Maximum number of times a user can subscribe to the questions per day.</strong>&lt;br&gt;<code>sn_kb_social_qa.max_subscriptions_per_user_daily</code></td>
<td>Enter the maximum number of times a user can subscribe to the questions per day.</td>
</tr>
<tr>
<td><strong>Type:</strong> Integer&lt;br&gt;<strong>Default value:</strong> 500&lt;br&gt;<strong>Location:</strong> System Properties</td>
<td></td>
</tr>
</tbody>
</table>
**Article versioning properties**

The knowledge administrator can set configuration properties that enable users to edit specific fields on published articles without creating new versions.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable article versioning feature. (glide.knowman.versioning.enabled) | Select the Yes check box to enable the article versioning feature.  
  - **Type**: true | false  
  - **Default value**: true  
  - **Location**: Knowledge > Administration > Properties |

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable minor edits to a published article without creating a new version. (glide.knowman.versioning.enable_minor_edits) | Select the Yes check box to enable minor edits to published articles without creating a new version.  
  - **Type**: true | false  
  - **Default value**: false  
  - **Location**: Knowledge > Administration > Properties |

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| A comma-separated list of fields that can be edited on published articles without creating a new version. (glide.knowman.versioning.minor_edit_fields) | Enter the fields in a comma-separated list that can be edited on published articles without creating a new version.  
  - **Type**: string  
  - **Default value**: valid_to  
  - **Location**: Knowledge > Administration > Properties |

**Note**: This feature is available for the following users: the knowledge administrator, the knowledge base manager, and the knowledge base owner.

**Knowledge subscription properties**

The knowledge administrator can set configuration properties that enable users to subscribe to knowledge bases and knowledge articles.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable subscribe feature for KM (glide.knowman.enable_km_subscription) | Select the Yes check box to enable the Knowledge subscription feature.  
  - **Type**: true | false  
  - **Default value**: true  
  - **Location**: Knowledge > Administration > Properties |
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| List of roles (comma-separated) who can have subscription feature (glide.knowman.enable_km_subscription.roles) | Enter the roles in a comma-separated list that can use the Knowledge subscription feature.  
- **Type**: string  
- **Default value**: knowledge  
- **Location**: Knowledge > Administration > Properties |
| List of workflow states (comma-separated) that can have subscription feature (glide.knowman.enable_km_subscription.workflow_state) | Enter the workflow states for knowledge articles in a comma-separated list that users can subscribe to.  
- **Type**: string  
- **Default value**: draft, review, published  
- **Location**: Knowledge > Administration > Properties |

### Create a custom knowledge homepage

As a system administrator, you can create a module allowing users to open a knowledge homepage for a specific knowledge base or category.

**Role required**: admin

1. Right-click the application label in the application navigator and select **Edit Application**.
2. In the **Modules** related list click **New**.
3. Enter a **Title** for the module.
4. In the **Link type** field, select **URL (from Arguments)**.
5. In the **Arguments** field, append one or more of the following values to `$knowledge.do#/search?`.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **sysparm_kb=<knowledge base sys_id>** | Enter the sys_id of a knowledge base to show knowledge articles from that knowledge base by default.  
If the specified knowledge base does not exist, the default knowledge homepage appears when accessing the custom homepage module. |
| **sysparm_category=<knowledge category sys_id>** | Enter the sys_id of a knowledge category to show knowledge articles from that category by default.  
If the specified category does not exist, the default category for the selected knowledge base appears when accessing the custom homepage module.  
**Note**: The category passed in this parameter must belong to the knowledge base passed in the **sysparm_kb** parameter. |
| **sysparm_order=<view_count, last_modified, or relevancy>** | Enter the default sort order for articles to appear in. |
To create a homepage for a *Facilities* knowledge base with a sys_id of d582764047022100158b949b6c9a7145 and sorting by last modified date, enter $knowledge.do#/search?
sysparm_kb=d582764047022100158b949b6c9a7145&sysparm_order=last_modified in the Arguments field on the Module form.

I18N - Knowledge internationalization

Organizations with knowledge users who speak multiple languages can activate the optional knowledge internationalization features.

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

Enabling any of the I18N language plugins automatically enables the I18N: Knowledge Management Internationalization Plugin v2 plugin (com.glideapp.knowledge.i18n2).

When active, knowledge internationalization enables the knowledge management team to create language-specific knowledge articles and keep translations of the same article related to each other so they are easy to manage. Users can view and search within their own language while still being able to view articles in other languages when necessary.

**Note:**

To set the default language for searching articles to a language different from the logged in language of the user, specify the desired language in the glide.knowman.search.default_language system property.

For example, if you are logged in using the French language and would like the default language for searched articles to be English, specify English in the system property. You can then switch to French from within the UI to see French articles.

If no language is specified in the system property, articles default to the logged in language of the user.

Refer to [Knowledge search](#) for information on performing a search on all available languages simultaneously.

Social Q&A does not use language-specific questions and answers. All questions and answers appear in the language they were created in. For example, a question in English is not translated when the current user’s selected language is French.

**Activate the knowledge management internationalization plugin**

To enable translation of knowledge articles, you must activate multiple plugins.

- I18N:Knowledge Management Internationalization v2 plugin
- Internationalization plugins for each appropriate language

**Activate a plugin**

**Installed Components**

Activating the Knowledge Management Internationalization plugin installs these components:
- A relationship named Translated Versions that creates a related list on the Knowledge form showing other articles that have the same parent article.
- A business rule named knowledge query that automatically filters the knowledge portal and search results based on the user's selected language.
- A UI macro named kb languages.
- Two fields, named Language and Parent, in the Knowledge [kb_knowledge] table and the Knowledge form.

Knowledge Form Changes

Activating knowledge management internationalization adds these fields to the Knowledge form.
- Language: select the language for the article.
- Parent: enter the number of the article that represents the base language. This setting keeps translations of the same article related to each other. Consider choosing the same language consistently for the parent article.

Additionally, the Translated Versions related list is automatically added to the Knowledge form after you save an article.

Create a translation for a knowledge article

Create a translation for an article from the Translated Versions related list on the knowledge article record. Before creating a translation, activate the internationalization plugin for the desired language which, in turn, activates the i18N: Knowledge Management Internationalization Plugin v2 (com.glideapp.knowledge.i18n2).

1. Open the knowledge article record.
2. In the Translated Versions related list, click New.
3. Select the desired language for the translation in the Language field.
4. Provide a description in the Short Description field.
5. Click Submit.

The translation is created and added to the Translated Versions related list.

Duplicate knowledge article numbers

Importing knowledge articles into an instance can create articles with duplicate numbers.

The Knowledge Number field is auto-generated and is incremented every time you create a new article in an instance. The initial value for the Number field is 10,000. To customize this number:

1. Navigate to System Definition > Number Maintenance.
2. Search for Knowledge in the Table column.
3. Click the Controls related list tab.
4. Enter a new Number and click Update.

Importing knowledge articles from another instance or as part of the demo data for another application may introduce an article with a number that is already in use. Because the Knowledge Number field is not uniquely indexed, the import completes without error.

© 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.
With duplicate knowledge article numbers present, links to article view pages that use the knowledge number can behave inconsistently. For example, if there are two articles with the same Knowledge number KB0000033, the following link may open either of these two articles randomly: \texttt{kb\_view.do?sysparm\_article=KB0000033}. This can happen in Knowledge search results where clicking on a result opens a different article instead of the article displayed in the search results.

**Avoiding duplicate Knowledge article numbers**

To avoid inserting Knowledge articles with duplicate numbers into a production environment:

- Do not import demo data articles in production environment.
- Verify the numbers of the articles to be inserted to make sure they are not already in use.
- Create a before insert business rule on the Knowledge table (kb\_knowledge) to ensure the new number is not already in use.

You can also update the initial value for the Knowledge **Number** field so that newly created articles do not conflict with existing articles.

1. Navigate to **System Definition** > **Number Maintenance**.
2. Search for **Knowledge** in the **Table** column.
3. Click the **Knowledge** link to open the Knowledge table form.
4. Click the **Controls** related list tab.
5. In the **Number** field, update the count to a number greater than the largest value already in the system.
6. Click **Update**.

**Enable search on all knowledge bases**

Configure the knowledge base search source in the service portal to perform a search on all knowledge bases.

Role required: admin

By default, the knowledge base search source in the service portal is set to search only a single knowledge base, which by default is set to the IT knowledge base.

1. Navigate to **Service Portal** > **Portals** > **Service Portal**.
2. Clear the entry in the **Knowledge base** field.
3. Click **Update**.
4. In the **Search Source** related list, select **Knowledge Base**.
5. In the **Data Source** tab, go to the **Data fetch script** field and delete or comment out line 7.
function(query) {
    var results = [];
    // Here goes the logic. Compute results.
    var kb = new GlideRecord('kb_knowledge_base', query);
    kb.addQuery('workflow_state', 'published');
    kb.addQuery('valid_to', '>=', (new GlideDate()).getLocalDate().getValue());
    kb.addQuery('123TEXTQUERY321', query);
    kb.setLimit(data.limit);
    kb.query();
    data.article_count = kb.getRowCount();
    var kbCount = 0;
    while (kb.next() && kbCount < data.limit) {
        // Does user have permission to see this record?
        if (!$sp.canReadRecord("kb_knowledge_base", kb)) {
            continue;
        }
        var article = {};
        $sp.getRecordDisplayValues(article, 'sys_id,number,short_description,published,article.publishedUTC = kb.getValue(article.publishedUTC)
        article.type = "kb";
        if (!article.text) {
            article.text = "";
        }
        article.text = $sp.stripHTML(article.text);
    }
}
6. Click **Update**. When you perform a keyword search in the service portal, the knowledge base search source performs the search on all knowledge bases.

**Use knowledge on mobile devices**

All users can access knowledge from mobile devices to search for and view knowledge articles and social Q&A questions.

**Browse knowledge on mobile devices**

You can browse knowledge bases using a mobile device. Navigate to **SELF-SERVICE > Knowledge Base**.

Browse Knowledge by tapping on a category and browsing articles or subcategories.
Mobile Knowledge Categories

**Note:** Select the desired category and click the close icon ( ) for the selected category to reflect in the search results.

View knowledge articles and questions on mobile devices

You can read knowledge content using a mobile device.

Tap a title to view the article or question.
Note: You cannot edit or add comments to knowledge articles on the mobile interface. If using Social Q&A, you can perform all functions such as adding and editing questions, answers, and comments through the mobile interface.

Mobile Knowledge Article View

Search knowledge on mobile devices
Find a specific article or question by searching on a particular term.
Knowledge Management v3 migration

Knowledge management has significantly changed with the introduction of knowledge v3 starting with the Fuji release.

Knowledge v3 has several key differences from knowledge v2, the version of knowledge management that was available until Eureka release. The knowledge v3 plugin is activated by default starting with the Fuji release.

The following podcast provides more information on what is new in Knowledge Management v3.

When upgrading from Eureka or earlier versions, if you intend to use the new features available in knowledge v3, you have to migrate legacy knowledge content and any customizations you have made to the Knowledge Base applications.

The following video provides more information on how to migrate from Knowledge Management v2 to v3.
Key differences

<table>
<thead>
<tr>
<th>Legacy Knowledge</th>
<th>Knowledge v3</th>
</tr>
</thead>
<tbody>
<tr>
<td>One knowledge base.</td>
<td>Multiple knowledge bases.</td>
</tr>
<tr>
<td>A single lifecycle workflow shared by all articles.</td>
<td>Separate, customizable workflows available for each knowledge base.</td>
</tr>
<tr>
<td>Two-level organizational structure with <strong>Topic</strong> and <strong>Category</strong>. A single</td>
<td>Category structure with any number of levels. Each knowledge base has a</td>
</tr>
<tr>
<td>organizational taxonomy shared by all articles.</td>
<td>unique category taxonomy.</td>
</tr>
<tr>
<td>Permissions defined per article using roles and ACLs.</td>
<td>Permissions defined per knowledge base or article using user criteria.</td>
</tr>
</tbody>
</table>

Knowledge Management v3 migration process

When you upgrade from Eureka or earlier, consider a multi-step migration process. This process ensures you can access existing knowledge content and allows you to fully migrate at your own pace.

Review automatic changes before upgrading. These changes are applied immediately when upgrading and may impact existing functionality.

1. Migrate knowledge functionality to use your customized functionality with the knowledge v3 enhancements.
2. Migrate knowledge content to use the knowledge v3 enhancements with your existing knowledge articles.

After migration to Knowledge v3

These items are relevant to getting the full range of new functionality after you migrate.

- You must configure knowledge access controls based on user criteria to ensure that users can access existing knowledge content. Since access control in knowledge v3 is intended to be based on user criteria alone, users may be unable to access v2 or v3 knowledge articles, or have restricted access, with preexisting ACLs.
- If the home page was customized in knowledge v2, custom layout and links are not saved in knowledge v3.
- Images added using the **Image** field in a knowledge article form do not display in the Knowledge v3 or Knowledge Service Portal pages. The article search results page displays the knowledge base icon next to all articles from the knowledge base.

Automatic changes after KMv3 migration

Upgrading to Knowledge v3 automatically changes knowledge functionality including the knowledge user interface and security model.

Default knowledge base

When you upgrade from Eureka or earlier, a default knowledge base is created, titled Knowledge, that contains all knowledge articles from the previous version.

After the upgrade, you can add and edit articles in this knowledge base.
Articles in the default knowledge base continue to use legacy functionality, such as role-based access controls. Any customizations you made to knowledge functionality before the upgrade are preserved in the default knowledge base.

**Knowledge search changes**

By default, the legacy knowledge portal uses knowledge v3 search with limited filtering options. You can filter results only by knowledge base. Search results include only those articles the current user can view based on user criteria. ACLs do not restrict search results.

**Knowledge security changes**

Knowledge v3 manages access to articles with user criteria rather than roles and ACLs.

Existing ACLs on the Knowledge (kb_knowledge) table are preserved, but with the following changes.

- A version of 3 indicates that a knowledge base uses the knowledge v3 functionality.
- A version of 2 indicates that a knowledge base uses legacy functionality.

New ACLs introduced by knowledge v3, such as field-level controls, apply to all knowledge bases. When you upgrade from Eureka or earlier, any custom ACLs you implemented for the Knowledge table still apply to any knowledge records in the default knowledge base. Knowledge v3 updates ACLs that exist before upgrade so they only apply to Knowledge (kb_knowledge) records where this field value is 2.

**Note:** These changes affect the default knowledge base. Even if you are not using the new knowledge functionality, the legacy knowledge behavior may change if you have made customizations to ACLs on the Knowledge (kb_knowledge) table. Ensure you configure knowledge access controls after upgrading to prevent unexpected behavior.

Because Knowledge v3 introduces ACLs for the Knowledge (kb_knowledge) table, if you do not have high security enabled, you may notice differences in default behavior. See [KB0549970](#) for information about configuring Knowledge v3 without high security.

**Knowledge article view changes**

The Knowledge application uses the kb_view UI page to display knowledge articles.

**UI page**

The following changes apply automatically when you upgrade from Eureka or earlier:

- The existing kb_view page is renamed to kb_view_customer. The kb_view_customer page is used to display articles in the default knowledge base, preserving the legacy user experience.
- A new kb_view page is used. This becomes the primary page used to display articles that are not in the default knowledge base.

You should review all customizations introduced around the legacy kb_view UI page.

- URLs should not be updated as the new kb_view page redirects to the correct page depending on the article.
- Customizations made to the kb_view UI page are automatically copied to the kb_view_customer page on upgrade.
- Other customizations that affect kb_view may need to be copied or modified to apply to kb_view_customer. For example, an ACL defined for kb_view may need to be duplicated to provide security coverage for kb_view_customer.
Feedback

Legacy feedback functionality is retained for knowledge articles displayed in the legacy article view. Users can continue to use the feedback options to view, add, and reply to comments on these legacy articles. Legacy comments are retained in the Knowledge Feedback (kb_feedback) table.

To retain the legacy comment functionality with new knowledge articles, set the Use Live Feed for Knowledge feedback property (glide.knowman.use_live_feed) to false. This property is set to false by default.

Knowledge portal changes

While the legacy knowledge portal, kb_home, has not changed in Knowledge v3, we strongly recommend that you consider moving to the new Knowledge v3 home page, $knowledge.do.

UI page

You can search articles from the knowledge portal and filter search results by knowledge base, and by language if the instance uses knowledge management internationalization. This portal also appears for users on older browsers, such as Internet Explorer 9, instead of the knowledge homepage.

Navigation add-ons are available in the legacy knowledge portal. Navigation add-ons of the Link type appear in the top-right of the portal. To add navigation add-ons of the Search type, you must customize the kb_home UI page.

Search

By default, the legacy knowledge portal uses knowledge v3 search with limited filtering options. You can filter results only by knowledge base. Search results include only those articles the current user can view.

Access a knowledge base or search engine

You can add new search engines to the advanced search function or add links at the top of knowledge pages.

Role required: admin

This feature lets you configure access to a knowledge base, either public or private, or to a public search engine.

1. Navigate to Knowledge > Administration > Navigation Add-ons.
2. Click New.
3. Complete the form.

Navigation Add-on form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the search engine name or link text.</td>
</tr>
<tr>
<td>Type</td>
<td>Select Search or Link.</td>
</tr>
<tr>
<td>Order</td>
<td>Enter a number to indicate the sequence of this search option or link.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>URL</td>
<td>For a link, enter the URL. Leave blank for a search engine.</td>
</tr>
<tr>
<td>Script</td>
<td>For a search engine, enter a script that opens the search engine's results page for the search text. Leave blank for a link.</td>
</tr>
</tbody>
</table>

4. Click Submit.

**Knowledge submissions**

Knowledge submissions created from tasks continue to work in knowledge v3 with minor changes. By default, the Topic and Category fields no longer appear on the Submission form due to the knowledge v3 category changes.

The property glide.knowman.submission.workflow no longer appears on the knowledge properties UI page. To enable knowledge submissions, set this property to true on the System Properties (sys_properties) table.

See creating knowledge from incidents and problems for instructions on using knowledge submission in knowledge v3.

**Migrating Knowledge access controls**

Access to knowledge articles is controlled based on the user criteria for the knowledge base.

**Important:** If you do not migrate existing knowledge ACLs to user criteria, users may be unable to access knowledge articles, or may be able to access restricted articles.

User criteria records, rather than ACLs, control basic create, read, update, and delete operations for knowledge articles as well as which search results appear. This may lead to unexpected behavior if your configuration depends on ACLs to control access.

To ensure users are able to access the correct knowledge articles, migrate any ACL-based security settings to user criteria. This process may include creating additional knowledge bases and moving existing content to these knowledge bases, depending on your security model. For a detailed explanation and migration examples, refer to KB0550924 Understanding User Criteria and ACLs in Knowledge v3.

This video demonstrates how to manage article-level access controls during migration from Knowledge Management v2 to v3.

**Knowledge functionality migration**

You can migrate knowledge functionality to use your customized functionality with the knowledge v3 enhancements.

**Replaced knowledge modules**

When you are ready to migrate to knowledge v3, you can activate the v3 modules and deactivate the legacy modules.

Use the tables below to identify which knowledge v3 modules to activate and which legacy modules to deactivate. When activating a knowledge v3 module, deactivate the knowledge v2 module with the same name to ensure users access the correct module.

You can use the enablev3anddisablev2menus.txt backup script to enable knowledge v3 menus and disable knowledge v2 menus.
### Knowledge v3 modules

<table>
<thead>
<tr>
<th>Title</th>
<th>Order</th>
<th>Link type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Homepage</td>
<td>100</td>
<td>URL (from Arguments:)</td>
</tr>
<tr>
<td>Articles</td>
<td>200</td>
<td>Separator</td>
</tr>
<tr>
<td>Create New</td>
<td>300</td>
<td>New Record</td>
</tr>
<tr>
<td>Unpublished</td>
<td>400</td>
<td>List of Records</td>
</tr>
<tr>
<td>Published</td>
<td>500</td>
<td>List of Records</td>
</tr>
<tr>
<td>Retired</td>
<td>600</td>
<td>List of Records</td>
</tr>
<tr>
<td>Flagged</td>
<td>800</td>
<td>List of Records</td>
</tr>
<tr>
<td>All</td>
<td>900</td>
<td>List of Records</td>
</tr>
<tr>
<td>Open Submissions</td>
<td>960</td>
<td>List of Records</td>
</tr>
<tr>
<td>Administration</td>
<td>1000</td>
<td>Separator</td>
</tr>
<tr>
<td>Knowledge Bases</td>
<td>1100</td>
<td>List of Records</td>
</tr>
<tr>
<td>Feedback</td>
<td>1300</td>
<td>List of Records</td>
</tr>
<tr>
<td>Ratings</td>
<td>1500</td>
<td>List of Records</td>
</tr>
<tr>
<td>Search Log</td>
<td>1600</td>
<td>List of Records</td>
</tr>
<tr>
<td>Navigation Add-ons</td>
<td>1700</td>
<td>List of Records</td>
</tr>
<tr>
<td>Messages</td>
<td>1800</td>
<td>List of Records</td>
</tr>
<tr>
<td>Properties</td>
<td>1900</td>
<td>URL (from Arguments:)</td>
</tr>
<tr>
<td>Overview</td>
<td>2000</td>
<td>URL (from Arguments:)</td>
</tr>
<tr>
<td>User Criteria</td>
<td>2100</td>
<td>List of Records</td>
</tr>
</tbody>
</table>

### Legacy modules

<table>
<thead>
<tr>
<th>Title</th>
<th>Order</th>
<th>Link type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New</td>
<td>100</td>
<td>New Record</td>
</tr>
<tr>
<td>Published</td>
<td>190</td>
<td>List of Records</td>
</tr>
<tr>
<td>Edit</td>
<td>200</td>
<td>List of Records</td>
</tr>
<tr>
<td>Retired</td>
<td>240</td>
<td>List of Records</td>
</tr>
<tr>
<td>Feedback</td>
<td>300</td>
<td>List of Records</td>
</tr>
<tr>
<td>View</td>
<td>400</td>
<td>URL (from Arguments:)</td>
</tr>
<tr>
<td>Submissions</td>
<td>410</td>
<td>Separator</td>
</tr>
<tr>
<td>Assigned to me</td>
<td>420</td>
<td>List of Records</td>
</tr>
<tr>
<td>Open Submissions</td>
<td>450</td>
<td>List of Records</td>
</tr>
<tr>
<td>KCS</td>
<td>460</td>
<td>List of Records</td>
</tr>
<tr>
<td>Flagged Articles</td>
<td>470</td>
<td>List of Records</td>
</tr>
<tr>
<td>Ratings</td>
<td>480</td>
<td>List of Records</td>
</tr>
<tr>
<td>Searching Log</td>
<td>495</td>
<td>List of Records</td>
</tr>
</tbody>
</table>
Knowledge article publish and retire workflows

With knowledge v3, article state is controlled by workflows.

In the legacy knowledge base, article state was controlled by UI actions. UI actions from previous versions are available only in the default knowledge base.

To preserve your article publishing and retirement process in new knowledge bases, create workflows that follow these processes. To create these workflows, copy the default workflow that best matches your process and modify that copy. After creating workflows that use your article publishing and retirement processes, use these workflows as the Publish workflow and Retire workflow for the new knowledge bases.

Knowledge article category structure

With knowledge v3, all knowledge articles are organized by category and subcategory within knowledge bases.

The default knowledge base uses the legacy category structure; knowledge articles are organized by topics and categories.

Before you migrate articles, create a category structure for these articles in the destination knowledge bases. This structure can reproduce your legacy topic and category structure or can be extended to take advantage of the knowledge v3 category functionality.

Knowledge content migration

To use the new functionality available in knowledge v3 with legacy articles, you must migrate these articles out of the default knowledge base.

To migrate knowledge content, move articles out of the default knowledge base by changing the Knowledge Base value for each article. The state of the article remains unchanged when moving articles. After selecting a new knowledge base, assign a category to each article using the category structure defined in the new knowledge base.

After you migrate a knowledge article, the legacy feedback functionality is automatically replaced with the new knowledge feedback mechanisms. Legacy feedback is copied to the Live Feed Message (live_message) table to ensure previously submitted feedback is available for knowledge v3 articles.

Content packs for Knowledge Management

Content packs contain preconfigured best practice dashboards. These dashboards contain actionable data visualizations that help you improve your business processes and practices.

Note: To evaluate the functionality, you can activate Performance Analytics solutions and in-form analytics on instances that have not licensed Performance Analytics Premium. However, you have the following limitations:

- You cannot create new indicators.

© 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.
• You cannot collect data older than 180 days.

For full functionality, license Performance Analytics Premium. For more information, see *Get started with Performance Analytics Premium*.

---

**Content packs**

The Performance Analytics widgets on the dashboard visualize data over time, which allows you to analyze your business processes and identify areas of improvement. With content packs, you can get value from Performance Analytics for your application with minimal setup.

**Note:** Content packs include some dashboards that are inactive by default. You can activate these dashboards to make them visible to end users according to your business needs.

To enable the content pack for Knowledge Management, an admin can navigate to *Performance Analytics > Guided Setup*. Click *Get Started* then scroll to the section for Knowledge Management. The guided setup takes you through the entire setup and configuration process.

**Article versioning**

Use the Knowledge Management article versioning feature to create and maintain multiple versions of a knowledge article.

Knowledge contributors can create a new version of a knowledge article from an existing published version. This existing version can be either the latest published version or an older outdated version. All changes are stored in the new version of the article and the information in the existing article remains the same.

If you import published knowledge articles from a ServiceNow instance that does not support article versioning, you must run the *Initialize Versions on Articles* fix script to enable article checkout and editing.

With the article versioning feature, knowledge users can:

• Check out the latest version of a published article and create a new version.
• Select a previously published (outdated) version of an article and make it current.
• Recall an article that is being reviewed.
• Retire the latest published version of an article.

There are two types of article revisions: major and minor. Minor revisions include updates to an article that has not yet been published. Major revisions include updates to an article that has been published and is available to customers. To track the different revisions, the article versioning feature introduces version numbering.

With the article versioning feature, the knowledge article number also includes the version number. All references to knowledge articles use this number format. For example, KB0010003 v2.0.

**Activate the Knowledge Management Advanced plugin**

You can activate the Knowledge Management Advanced plugin (com.snc.knowledge_advanced) if you have the admin role.

Role required: admin
The Knowledge Management Advanced plugin includes feature code and demo data. The Knowledge Management Advanced Installer plugin (com.snc.knowledge_advanced.installer) is used to activate the Knowledge Management Advanced features.

The Knowledge Management Advanced plugin activates the following features:

- Article Versioning: Customers must migrate to Knowledge Management V3 completely to use article versioning. For more information, see Knowledge Management v3 migration.
- Article Subscriptions: The Knowledge Management Advanced plugin activates the Subscriptions and Activity Feed Framework plugin (com.snc.activity_subscriptions).

This plugin performs two validation steps prior to activation.

- Determines if there are any active Knowledge Management v2 knowledge bases. The customer must migrate to Knowledge Management v3 completely to use article versioning.
- Determines if there is a unique database index on the Number field. If a unique constraint has been added to the Number field, the plugin activation fails. Follow the instructions listed in this KB0634959 to perform corrective steps to resolve the issue.

You need access to HI to be able to view KB articles.

---

**Note:** The Knowledge Management Advanced plugin is not automatically activated with the Knowledge Management v3 application.

Demo data is included as part of the Knowledge Management Advanced plugin. If the validation step performed by the Knowledge Management Advanced Installer plugin completes successfully, the Knowledge Management Advanced plugin is activated automatically. However, the demo data is not included in this activation. To load the demo data, go to the Knowledge Management Advanced plugin page, click the Load Demo Data Only related link, and then click OK.

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**.

---

**Manually update customized files**

If you have customized any of the files that are updated as part of the Knowledge Management Advanced Installer plugin, these files are skipped during plugin activation and must be updated manually.

---
Manually update your customization to include the article versioning-related changes.

- Add the **Version** field to the Knowledge form layout and the Knowledge list view, if it is not already present.
- Add the **outdated** choice to the **Workflow** choice list field on the Knowledge form, if it is not already present. Keep the value as **outdated** because of dependencies that article versioning functionalities have on this choice.
- Update the **Knowledge > My Flagged** and **Self-Service > My Knowledge Articles** modules to include the following condition in the **Filter** field, if these modules do not already reflect this change: **Revised by is (dynamic) me**.

If you have customized any of the Knowledge Management Overview dashboard reports, these files are also skipped during plugin activation and must be updated manually.

**Article versioning changes**

Article versioning introduces new actions that allow knowledge users to create and revise versions of existing articles. It also introduces new fields and related lists to the Knowledge form, new columns to the Knowledge list, and updates to Knowledge dashboard reports.

**New user actions**

As part of creating article versions, users can:

- Check out a published article and create a new version by clicking **Checkout** on the Knowledge form.

  **Note:** Only the author, knowledge base owner, and users with the knowledge_admin role can edit an article in the draft state.

- Recall an article that is being reviewed by clicking **Recall** on the Knowledge form.
- Select a previously published article in the Outdated state and make it the current published version by clicking **Make this current** in the Knowledge form header.

  **Note:** To edit a published article without having to create a new version, make sure the `glide.knowman.versioning.enable_minor_edits` property is enabled.

**Changes to the Knowledge list**

The article versioning feature adds the following to the Knowledge list:

- The **Version** column displays the article version number. The Knowledge list displays multiple versions of an article.
- The **Workflow** column includes the new **Outdated** state.

**Changes to the Knowledge form**

The article versioning feature adds the following to the Knowledge form:

- The **Version** field displays the article version number.
- The **Display number** field displays a combination of the article number and the version number. For example, KB0010004 v1.02. All references to a knowledge article use this display number.
The **Base Version** field displays the knowledge article number and version on which the current article is based.

The **Revised By** field displays the name of the user who checked out a published article and created a new version.

The **Article Versions** related list displays a list of all versions for an article. From this list, you can:

- Click the **Version** to view a specific version of an article.
- Click the **View Article** related link to see the article page view.

---

**Note:** If necessary, configure the form to display the fields and the related list.

---

### Changes to Knowledge modules

The article versioning feature introduces the following Knowledge module changes:

- **My Knowledge Articles**
  - For a knowledge user, this module includes records for the articles authored by the user as well as records for each article revised by the user.
  - For a knowledge reviser, this module includes records for the articles published by the user as well as records for each article revised by the user.

- **My Flagged**
  - For a knowledge user, this module includes records for each revision made to articles authored by the user.
  - For a knowledge reviser, this module includes records for each article revised by the user.

---

**Note:** Users that have customized these modules do not see these changes.

---

### Changes to Knowledge Management dashboard reports

The Knowledge Management Overview dashboard reports have been updated to include article versioning-related changes when the Knowledge Management Advanced plugin is activated.

- Articles Flagged in the Last 30 Days
- Articles Marked Not Useful in the Last 30 Days
- Articles Used per Month
- Knowledge use
- Knowledge view
- Knowledge updated in past 30 days
- Knowledge flagged in past 30 days
- Knowledge by Workflow state
- Knowledge created by Author
- Knowledge created in past 30 days
- New Knowledge Articles Created in the Last 30 Days
- Knowledge Ratings for past 30 days
Versioning information available in the Knowledge Management Service Portal

Knowledge search results show the article number and the version number for each article.

**Note:**

To display the article version number next to the article number in the search results, enable the `glide.knowman.search.show_article_number` property in the Knowledge Search Properties section of the Knowledge Management Properties page.

If you are accessing an article from the base system or knowledge service portals using the URL to a KB article, you must also include the article version number in the URL. For example, to access the KB0000005 knowledge article, instead of using the `https://<instance name>/sp?id=kb_article&sys_id=KB0000005` as the URL, you must use `https://<instance name>/sp?id=kb_article&sys_id=KB0000005%20V1.0` to view the article.

The article view page shows a version history section for articles that have been updated. This section includes the version numbers, date updated, and the name of the author or reviser.

- Click **Latest version** or the version number and current state to expand the version history section.
- Click the version number to open that particular version of the article.
- When viewing an outdated article, a message informs the user that a newer updated version is available. The message includes a link to the latest version.

Feedback on article versions

With the article versioning feature, users can view and contribute to feedback on the current versions of knowledge articles.

For more information about feedback options, see *Knowledge feedback*.

<table>
<thead>
<tr>
<th>Feedback option</th>
<th>How this option works with article versioning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rating an article</td>
<td>The average rating for an article is carried over to the checked out version. The average rating calculation updates and displays on the current version of the article.</td>
</tr>
<tr>
<td>Marking an article as helpful</td>
<td>The helpfulness percentage of a previous version of an article is also considered for a new version when displayed in the helpfulness column on the homepage.</td>
</tr>
<tr>
<td>Comments</td>
<td>The Comments section at the bottom of an article displays comments from previous versions unless Live Feed is enabled. Live Feed only shows comments for the current version.</td>
</tr>
<tr>
<td>Flagging an article</td>
<td>Checking out an article or setting a previous version to the current version resets the flagged value to false.</td>
</tr>
<tr>
<td>View count</td>
<td>The view count is carried over to the checked out article. Any view of a version of an article increments the view count of all subsequent versions. Views to a newer version of an article do not affect the view count of previous versions.</td>
</tr>
</tbody>
</table>
### Feedback option

<table>
<thead>
<tr>
<th>Use count</th>
<th>How this option works with article versioning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The use count is carried over to the checked out article. Any use of a version of an article increments the use count of all subsequent versions. Any use of a newer version of an article does not affect the use count of previous versions.</td>
</tr>
</tbody>
</table>

### Knowledge article version numbers

Knowledge article version numbers follow a specific pattern. Increments to the version number depend on the revision type.

Article version numbers follow the pattern `major.minor`. The type of revision being made to an article determines the increment. A minor revision increments the version number by 0.01. A major revision, such as publishing an article, increments the version to the next whole number, for example, from version 2.02 to 3.0.

The following example illustrates the life cycle of a versioned article and the changes to the version number.

<table>
<thead>
<tr>
<th>User action</th>
<th>Article state</th>
<th>Version number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge author creates a new article</td>
<td>Draft</td>
<td>0.01</td>
</tr>
<tr>
<td>Knowledge author makes a change and updates the article.</td>
<td>Draft</td>
<td>0.01</td>
</tr>
<tr>
<td>Knowledge author submits the article for review.</td>
<td>Review</td>
<td>0.02</td>
</tr>
<tr>
<td>Knowledge author recalls the article to make another change.</td>
<td>Draft</td>
<td>0.03</td>
</tr>
<tr>
<td>Knowledge article submits the article for review</td>
<td>Review</td>
<td>0.04</td>
</tr>
<tr>
<td>Approver rejects the article and requests a change.</td>
<td>Draft</td>
<td>0.05</td>
</tr>
<tr>
<td>Knowledge author makes the change and submits the article for review.</td>
<td>Review</td>
<td>0.06</td>
</tr>
<tr>
<td>Approver approves the article</td>
<td>Published</td>
<td>1.0</td>
</tr>
<tr>
<td>Knowledge author checks out the published article.</td>
<td>Draft</td>
<td>1.01</td>
</tr>
<tr>
<td>Knowledge author submits the article for review.</td>
<td>Review</td>
<td>1.02</td>
</tr>
<tr>
<td>Approver approves the article</td>
<td>Published</td>
<td>2.0</td>
</tr>
</tbody>
</table>

Any change to the state of an article results in a version increment, except to and from the Pending retirement, Retired, and Outdated states.
Knowledge article version information

Users can view version information for a knowledge article from the Knowledge view page.

The knowledge article number and the version number appear at the top of the article, just below the title. Clicking the version number expands the version history section, which includes a list of the available article versions. User roles determine what is included in this list:

- Users with read access to a knowledge base can see the latest published version and previous major versions.
- Users with read and contribute access to a knowledge base can see the latest published version, previous major versions, and any draft or review versions.

You can view any of the previous versions of an article by clicking the version number in the list. When you view a previous version, a message at the top of the article indicates that an updated version is available.

At the bottom of a knowledge article, you can see additional information about an article, including the name of the author or revisor and the date that the article was last modified.

Knowledge article states

A versioned knowledge article can be in one of several states as it progresses through the creation cycle.

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft</td>
<td>The article is in the process of being created.</td>
</tr>
<tr>
<td>Review</td>
<td>The draft version of the article is sent to reviewers to approve or reject.</td>
</tr>
<tr>
<td>Published</td>
<td>The article is approved and published. When the state of an article changes to Published, the state of any previous published versions of that article changes to Outdated.</td>
</tr>
<tr>
<td>Pending retirement</td>
<td>The published article is selected for retirement, pending approval.</td>
</tr>
<tr>
<td>Retired</td>
<td>The published article is retired.</td>
</tr>
<tr>
<td>Outdated</td>
<td>A more recent version of the article has been published. End users can read published articles as well as the outdated versions.</td>
</tr>
</tbody>
</table>

Article versioning properties

The knowledge administrator can set configuration properties that enable users to edit specific fields on published articles without creating new versions.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable article versioning feature. (glide.knowman.versioning.enabled)</td>
<td>Select the Yes check box to enable the article versioning feature.</td>
</tr>
<tr>
<td></td>
<td>· Type: true</td>
</tr>
<tr>
<td></td>
<td>· Default value: true</td>
</tr>
<tr>
<td></td>
<td>· Location: Knowledge &gt; Administration &gt; Properties</td>
</tr>
</tbody>
</table>
### Property: Enable minor edits to a published article without creating a new version.

- **(glide.knowman.versioning.enable_minor_edits)**
  - **Type:** true | false
  - **Default value:** false
  - **Location:** Knowledge > Administration > Properties

**Note:** This feature is available for the following users: the knowledge administrator, the knowledge base manager, and the knowledge base owner.

### Property: A comma-separated list of fields that can be edited on published articles without creating a new version.

- **(glide.knowman.versioning.minor_edit_fields)**
  - **Type:** string
  - **Default value:** valid_to
  - **Location:** Knowledge > Administration > Properties

**Check out a published article and create a new version**

Create a new version of a knowledge article by checking out the latest published version.

Users with canContribute permissions, including the knowledge owner, knowledge manager, and knowledge administrator, can check out a published article unless there is already a checked out version. If a version has been checked out, the **Checkout** button does not appear on the Knowledge form header.

**Note:** Outdated articles can be checked out by first using Make this current, provided a version has not already been checked out.

1. Navigate to **Knowledge > Articles > Published**.
2. Select the desired article from the list.
3. Click **Checkout** in the Knowledge form header.

   The system creates a new version of the knowledge article and displays a message to the user. The article number for the new version remains the same, the version number is increased by 0.01, and the state changes to **Draft**. The new version of the article is added to the Knowledge list and to the **Article Versions** related list on the Knowledge form.

**Approve an article that is being reviewed**

Approve an article that is being reviewed and create a new published version.

When an article is in the **Review** state, only those users who are included in the **Approvals** related list can modify the article.

1. Navigate to **Knowledge > Articles > Unpublished**.
2. Open an article in the **Review** state and review the text.
3. In the **Approvals** related list, click **Requested** in the **State** column to display the Approval form for the article.
4. Click Approve.
   The system displays the Knowledge form. The version number of the article increments to the
   next whole number (for example, from 2.02 to 3.0) and the state changes to Published. The
   new published version of the article is added to the Knowledge list and to the Article Versions
   related list on the Knowledge form.

Revert an outdated article to the current state

Use an outdated version of an article to create a new version.
Roles required: knowledge base owner, knowledge_manager, knowledge_admin
This action is available for earlier published version that have a state of Outdated and only when
there is no checked out version. If a version has been checked out, the Make this current button
does not appear on the Knowledge form header.
1. Navigate to Knowledge > Articles > All.
2. Open an article in the Outdated state.
3. Click Make this current in the Knowledge form header.
   The system displays the Knowledge form. The version number increments to the latest version
   number plus 0.01 and the state changes to Draft. For example, if the latest published version
   of an article is 3.0 and you select the outdated 1.0 version to become the current version, the
   version number increments to 3.01.

Recall an article that is being reviewed

Recall an article that is being reviewed to make additional changes.
When a revised article is in the Review state, only the corresponding versions reviser can recall
the article to make additional changes. When a newly created article is in the Review state, only
the author can recall the article. Recalling an article in the Review state results in a minor version
increment.
1. Navigate to Knowledge > Articles > All.
2. Open an article in the Review state.
3. Click Recall in the Knowledge form header.
   The system returns the state of the article to Draft, increments the version number by 0.01, and
displays a message to the user.

View all versions of an article

View a list of all available versions for a selected knowledge article and then view the selected
version in a new tab.
The list of all available versions for a selected knowledge article is displayed in the Article Versions
related list on the Knowledge form. Users with read access can see major versions. Users with
contribute access can see major and minor versions.
1. Navigate to Knowledge > Articles > All.
2. Open the desired article.
3. Click the Article Versions tab to display the related list.
4. Click Version to display the desired article version in a new tab.
5. If desired, click the View Version related link to see the article view page.
Compare two versions of an article

Select and compare two versions of a knowledge article.

Role required: knowledge_manager, knowledge_admin

1. Navigate to a knowledge article with multiple versions.
2. In the Article Versions related list, select two versions of the article to compare.
3. In the Actions choice list below the list, select Compare.
   The Compare Versions page opens in a new tab and lists the fields for the selected articles in a side-by-side format. Differences between the two articles are highlighted.
4. When you are finished comparing the two versions, click Done to return to the Knowledge form.

Retire a versioned article

You can retire the latest published version of a knowledge article. Retiring a knowledge article does not create a new version. It simply marks the article as Retired.

This action is available only when there is no checked out version. If a version has been checked out, the Retire button does not appear on the Knowledge form header.

Note: For the Knowledge - Approval Retire workflow, this happens only when the retire request is approved.

In addition to the knowledge administrator and the knowledge manager, the following users can retire a versioned article:

- knowledge owner
- author of the versioned knowledge article
- reviser of the versioned knowledge article

Users can still access outdated articles that have been attached to incidents by navigating to the article view page with the sys_id of the article. Outdated articles include a message that an updated article is available.

If versioning is disabled, only the latest version of the article is shown in search results and list views.

1. Navigate to Knowledge > Articles > Published.
2. Open the desired article.
3. Click Retire in the Knowledge form header.
   The system returns to the Knowledge list. The state of the article changes to Pending retirement and the state of previously published versions change to Outdated.

Note: You cannot check out or edit a retired article.

Disable the article versioning feature

Users with the system administrator role can disable the article versioning feature by setting a property.

Role required: admin

The Enable article versioning feature property controls the article versioning feature. Setting this property to false disables the article versioning feature. Once disabled:
- The **Version** field is removed from the Knowledge form. The **Version** column remains on the Knowledge list and can be removed manually.
- The **Article Versions** related list is removed from the Knowledge form.
- The **Recall**, **Checkout**, and **Make this current** buttons are removed from the Knowledge form.
- Outdated articles are removed from Knowledge list views.
- The version history does not appear on the article view page.

Articles continue to be versioned in the background. Minor versions are incremented until an article is published and then the version number is increased to the next major version.

Users can still access outdated articles that have been attached to incidents. Outdated articles include a message that an updated article is available.

1. Navigate to **Knowledge > Administration > Properties**.
2. Locate the **Enable article versioning feature** property in the Article Versioning Properties section.
3. Click the check box to disable the property.
4. Click **Save**.

### Knowledge Management Service Portal

The Knowledge Management Service Portal enables users to perform the same operations that are available with the Knowledge Management V3 plugin. From the portal, users can view knowledge bases and articles, search for information, sort and filter search results, and provide feedback.

Knowledge administrators can customize portal pages and configure widgets for searching, sorting, and filtering knowledge base information.

To use the Knowledge Management Service Portal:

1. Activate the **Knowledge Management - Service Portal plugin** (com.snc.knowledge_serviceportal).
2. Configure the **Knowledge Management Service Portal properties**, including the property that directs users to the Knowledge Management Service Portal homepage.

### Customizing the Knowledge Management Service Portal

The Knowledge Management Service Portal is comprised of **three pages** and **multiple widgets**. Users with the system administrator roles can customize the pages and widgets as desired.

- To customize this portal, navigate to **Service Portal > Portals** and click **Knowledge Portal**. See **Service Portal** for more information about creating a custom interface.
- To configure widget instance options and customize the search, sort, and filter features, see **Knowledge Management Service Portal widgets**.

### Section 508 compliance features

Users can view and interact with the Knowledge Management Service Portal article view page using Section 508 compliance features. See **Enabling accessibility features** for more information.
Activate the Knowledge Management Service Portal plugin

You can activate the Knowledge Management - Service Portal plugin (com.snc.knowledge_serviceportal) if you have the admin role.

Role required: admin

This plugin requires the following plugins:

- Knowledge Management V3 (com.snc.knowledge3)
- Service Portal for Enterprise Service Management (com.glide.service-portal.esm)

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.

Knowledge features not supported on Knowledge Management Service Portal

Several knowledge features are not yet supported on the Knowledge Management Service Portal.

These features include:

- Article import on the Search results page
- Hierarchical categories on the Article view page
- Live Feed support for Social Q&A on the Article view page
- Tags added in Social Q&A are not honored in search results

The glide.knowman.portal.enable_redirect property is not honored for the following use cases:

- Contextual search in the Incident form
- Connect

Knowledge Management Service Portal properties

Knowledge Management Service Portal properties determine how information is displayed on the Knowledge portal. You must have the admin role to set configuration properties.

The following system properties are set to direct users to the Knowledge Management Service Portal homepage, and to specify the URL suffix for the homepage.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sn_km_portal.glide.knowman.serviceportal.enable_redirect</td>
<td>Directs users to the desired Knowledge homepage.</td>
</tr>
<tr>
<td></td>
<td>• Set to <code>true</code> to direct users to the Knowledge Management Service Portal homepage.</td>
</tr>
<tr>
<td></td>
<td>• Set to <code>false</code> to direct users to the Knowledge Management v3 homepage.</td>
</tr>
<tr>
<td>sn_km_portal.glide.knowman.serviceportal.portal_url</td>
<td>The URL suffix for the Knowledge Management Service Portal. The default is <code>kb</code>.</td>
</tr>
</tbody>
</table>

The Knowledge Management Service Portal supports the Knowledge Management V3 properties. Configuring widget instance options on the portal pages can override these properties.

**Knowledge Management Service Portal pages**

The Knowledge Management Service Portal includes a homepage, a search results page, and an article view page.

**Homepage**

The Knowledge Management Service Portal landing page. This page includes a search bar, knowledge bases, and lists of knowledge articles.

- Users can search for information, explore knowledge bases, and view featured articles.
- Administrators can customize the page layout, add knowledge bases, and add article collections (for example, a list of the most viewed articles).

**Search results page**

This page displays a list of search results and includes several options for sorting and filtering the information.

- Users can sort and filter search results in multiple ways.
- Administrators can customize the page layout, configure the sort and filter widgets to use any field on the Knowledge (kb_knowledge) table, and also configure the filter widgets to use custom queries.

**Article view page**

This page displays the selected knowledge article or social Q&A item.

- Users can view articles and provide comments and ratings. If enabled, users can subscribe to articles, view article versions, and create incidents for articles that are rated as not helpful. Users can also view and edit questions and provide comments or answers.
Administrators can customize the page layout and enable or disable user actions, such as creating an incident for an article. Administrators can also activate the plugins to enable article versioning and article subscriptions.

**Knowledge Management Service Portal homepage**

The Knowledge Management Service Portal homepage displays knowledge articles and social Q&A items organized by knowledge base and category, as well as featured content and popular articles.

To view the Knowledge Management Service Portal homepage, navigate to one of the following:

- **Self Service > Knowledge**
- **Knowledge > Homepage**

**Note:** To use the Knowledge Management Service Portal, activate the Knowledge Management - Service Portal plugin (com.snc.knowledge_serviceportal) and enable the glide.knowman.serviceportal.enable_redirect property.
Welcome to

3 Knowledge Bases

Explore our Knowledge Bases

Featured

Email Interruption Tonight at 11:00 PM Eastern
Wayne Webb • 1 Views • 24d ago • ★★★★☆

Sales Force Automation is DOWN
Wayne Webb • 0 Views • 9mo ago • ★★★★★

Most Useful

Sales Force Automation
Wayne Webb • 0 Views • 9mo ago • ★★★★★
The Knowledge Management Service Portal homepage includes the following:

**Header**

The header contains a search bar and counters that display the number of available knowledge bases and the total number of knowledge articles and social Q&A items.

**Knowledge bases**

Each knowledge base is represented by a tile that includes the knowledge base icon and name. Icons and counters below the knowledge base name display the number and type of items stored in the knowledge base, such as articles and questions. By default, tiles are ordered alphabetically by knowledge base name.

**List collections**

Lists of articles, including featured, most useful, and most viewed articles. By default, these lists display articles by the article **Short description** and include information such as the author name, number of views, and average rating.

---

**Note:** The Knowledge Management Service Portal homepage is mobile responsive.

---

**Using the homepage**

From the Knowledge Management Service Portal homepage, you can do the following.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search for information</td>
<td>Use the search bar to search knowledge bases and social Q&amp;A.</td>
</tr>
<tr>
<td>View knowledge bases</td>
<td>Knowledge bases available to the user are arranged in alphabetical order.</td>
</tr>
<tr>
<td>View articles</td>
<td>Select articles from the article collection lists.</td>
</tr>
<tr>
<td>Ask a question</td>
<td>This action is available to logged in users with the knowledge role. Click <strong>Ask a Question</strong>, which opens a question page. Fill in the <strong>Question</strong> and <strong>Question details</strong> fields, and click <strong>Post question</strong> to post the question.</td>
</tr>
<tr>
<td>Create an article</td>
<td>This action is available to logged in users with the knowledge role. Click the <strong>Overflow</strong> icon (*** and select <strong>Create Article</strong>, which opens a new Knowledge record with an assigned number. Fill in the fields and click <strong>Submit</strong> to return to the Knowledge Management Service Portal.</td>
</tr>
<tr>
<td>Subscribe to a knowledge base</td>
<td>This action is available to logged in users; availability is based on knowledge subscriptions user roles. Click <strong>Subscribe</strong> at the top of a knowledge base tile to subscribe to that knowledge base. Unsubscribe by clicking <strong>Unsubscribe</strong>. See <strong>Knowledge subscriptions</strong> for more information.</td>
</tr>
</tbody>
</table>
Knowledge Management Service Portal search results page

The Knowledge Management Service Portal search results page displays a list of search results as well as options for sorting and filtering the items in the list.
The Knowledge Management Service Portal search results page includes the following:

**Search results list**

The search results list includes knowledge articles, pinned articles, and social Q&A items. For knowledge articles, the search results include articles in which the short description, text content, or attached file content includes the search term. For social Q&A items, search results include answered and unanswered questions, and questions with accepted answers. The following information displays for each list item:

- The article short description or the question.
- The knowledge base in which the item is stored.
- The first two lines of text from the article or question or surrounding the relevant keywords from your search.
- Information about the item such as the author name, the number of views, and rating information.
- An icon that represents the type of item.

**Search results list header**

The header displays the number of search results, which updates as the user selects and deselects filters. Selected filter options appear just below the number of search results. The header also includes the available sort options.

**Filter facet widgets**

A number of filter facet widgets appear to the left of the search results list. Each filter facet widget includes a list of selectable options that can be used to refine the search results.

- Knowledge Base: lists the available knowledge bases
- Category: lists the available knowledge categories
- Author: lists the names of the authors for the knowledge articles included in the search results list
- Tags: lists the available knowledge tags
- Resource: lists the types of items available, such as knowledge articles and social Q&A
- Rating: lists article ratings from 0-5 stars (clicking a rating displays articles that have the selected rating and higher)
- Last Modified: lists selections based on the timing of knowledge item modifications such as Past Month or Past Week
- View Count: lists the knowledge item view counts such as More Than 50 or Less Than 10. Set the number of days to consider when calculating view count using the `glide.knowman.view_age.days` property.

**Using the search results page**

From the Knowledge Service Portal homepage, you can do the following.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform a search</td>
<td>Use the search bar at the top of the page to search for additional information.</td>
</tr>
<tr>
<td>Sort the search results</td>
<td>Click a sort option in the search results list header to sort list items by relevance to the search term, number of views, newest, or alphabetical. Items are sorted in ascending order. Click the option again to sort in descending order.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Filter the search results</td>
<td>Select options in the filter facet widgets to filter the items in the search results list. Clear selected filter options by:</td>
</tr>
<tr>
<td></td>
<td>- Deleting a single option from the search results list header.</td>
</tr>
<tr>
<td></td>
<td>- Clicking <strong>Clear all</strong> in the search results list header.</td>
</tr>
<tr>
<td></td>
<td>- Clicking <strong>Clear</strong> in the filter facet widget header.</td>
</tr>
</tbody>
</table>

**Knowledge Management Service Portal article view page**

The Knowledge Management Service Portal article view page displays the selected knowledge article, including the article number, short description, and article content.

If users select a question, the article view page displays the question, any answers to the question, and a text box for providing an answer.
Create An Email Signature

To create a personalized email signature:

1. Open a new message. On the Message tab, in the Include group, click Signature.
2. On the E-mail Signature tab, click New.
3. Type a name for the signature, and then click OK.
4. In the Edit signature box, type the text that you want to include in the signature.
5. To format the text, select the text, and then use the style and formatting buttons.
6. To add elements besides text, click where you want the element to appear, and then:

<table>
<thead>
<tr>
<th>Options</th>
<th>How to</th>
</tr>
</thead>
<tbody>
<tr>
<td>To add an electronic business card</td>
<td>Click Business Card, and then click a contact in the Filed As section.</td>
</tr>
<tr>
<td>To add a hyperlink</td>
<td>Click Insert Hyperlink, type in the information or browse to the URL.</td>
</tr>
<tr>
<td>To add a picture</td>
<td>Click Picture, browse to a picture, click to select it, and then include .bmp, .gif, .jpg, and .png.</td>
</tr>
</tbody>
</table>

1. To finish creating the signature, click OK.

NOTE:

The signature that you just created or modified won't appear in the currently open message.
The Knowledge Management Service Portal article view page includes the following:

**Header**
For knowledge articles, the header includes the knowledge article number and enabled user actions. For questions, the header includes the question text.

**Knowledge article meta data**
Article information including the short description and author name, the date that the article was last modified, the number of views, and the average rating. If configured, it also includes article version information.

**Article or question content**
The text and images of the knowledge article or question.

**Feedback options**
Article feedback options include marking the article as helpful, rating the article, and providing a comment. Question feedback options include sharing a question, commenting on a question, providing an answer, and accepting an answer.

**List widgets**
The article view page includes the following list widgets for articles and questions:
- Most Recent Tasks
- Affected Products
- Most Viewed
- Most Useful
- Question Stats
- Recent Questions

From the Knowledge Service Portal article view page, you can do the following.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View content</td>
<td>View a knowledge article or question.</td>
</tr>
<tr>
<td>Edit an article</td>
<td>Users with contribute access can edit an article.</td>
</tr>
<tr>
<td>Flag an article</td>
<td>Users with contribute access can flag an article that contains incorrect or inappropriate content.</td>
</tr>
<tr>
<td>Subscribe to an article</td>
<td>This action is available to logged in users: availability is based on knowledge subscriptions user roles. Click <strong>Subscribe</strong> in the article header to subscribe to that knowledge article. Unsubscribe by clicking <strong>Unsubscribe</strong>. See <strong>Knowledge subscriptions</strong> for more information.</td>
</tr>
<tr>
<td>Create an incident</td>
<td>If configured, the <strong>Create Incident</strong> link appears at the bottom of the article after the article is rated as not helpful.</td>
</tr>
</tbody>
</table>

**Note:** Use the widget instance option for the article view page to enable the display of this link.
<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide feedback to an article</td>
<td>Feedback options include marking an article as helpful, providing a rating from one to five stars, and adding a comment. See Knowledge feedback for more information.</td>
</tr>
<tr>
<td>Post a question</td>
<td>All users can post a question.</td>
</tr>
<tr>
<td>Answer a question</td>
<td>All users can provide an answer to a question.</td>
</tr>
<tr>
<td>Accept an answer</td>
<td>The knowledge manager or the owner of a question can accept an answer as the correct answer.</td>
</tr>
<tr>
<td>Comment on a question or answer</td>
<td>All users can add a comment to a question or to an answer.</td>
</tr>
<tr>
<td>Edit a question, answer, or comment</td>
<td>All users can edit the questions, answers, and comments that they submit. Knowledge managers can edit questions, answers, and comments for the knowledge bases that they manage.</td>
</tr>
</tbody>
</table>

**Note:** For more information, see Social Q&A questions.

### Knowledge Management Service Portal widgets

The Knowledge Management Service Portal uses a number of widgets to enable searches, display search results, and display articles and social Q&A.

The Knowledge Management Service Portal homepage, search results page, and article view page honor the Knowledge Management V3 system properties. If configured, widget instance options can override the system properties.

Users with the knowledge_admin or admin role can configure the widget instance options used on the Knowledge Management Service Portal pages. Use the control + right-click menu to access the widget instance options and configure a widget instance.

**Note:** Before configuring widget instance options, switch to the Knowledge Management - Service Portal scope.

#### Homepage widgets:
- Knowledge Homepage Search
- Knowledge Bases Browse
- Knowledge Featured Articles
- Knowledge Most Useful Articles
- Knowledge Most Viewed Articles

#### Search results page widgets:
- Knowledge Breadcrumbs
- Knowledge Search
- Knowledge Facet Header
- Knowledge Field Facet
- Knowledge Tags Facet
- Knowledge Resource Facet
Configure search widget instance options

Configure widget instance options for the search widgets on the Knowledge Management Service Portal homepage and search results page.

Role required: knowledge_admin or admin

The homepage uses the Knowledge Homepage Search widget and the search results page uses the Knowledge Search widget. Use the widget instance options to customize the search feature for these pages.

1. Navigate to the Knowledge Management Service Portal homepage or search results page.
2. Control + right-click the search bar.
3. Click Instance Options.
4. Configure the desired settings for the search widgets.

<table>
<thead>
<tr>
<th>Instance option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>The title of the search widget. The default for the homepage is Welcome to Knowledge.</td>
</tr>
<tr>
<td>Glyph</td>
<td>An icon that appears in the search bar.</td>
</tr>
<tr>
<td>Bootstrap color</td>
<td>The color of the search widget.</td>
</tr>
<tr>
<td>Bootstrap size</td>
<td>The size of the search widget.</td>
</tr>
<tr>
<td>CSS</td>
<td>CSS used in the widget instance.</td>
</tr>
<tr>
<td>Search Placeholder</td>
<td>Default text that appears in the search bar.</td>
</tr>
<tr>
<td>Allow Empty Search</td>
<td>Allow empty knowledge base searches. The default for the homepage uses the system property. The default for the search results page is Yes. For an empty search, the search results page returns all results.</td>
</tr>
<tr>
<td>Allow Instant Search On Keypress</td>
<td>Enables instant search results as you type a search term. The default for the search results page uses the system property.</td>
</tr>
<tr>
<td>Minimum Number of Characters for Search</td>
<td>The minimum number of characters required to generate a search.</td>
</tr>
<tr>
<td>Instance option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Wait time (ms) between searches, if instant search</td>
<td>The time, in milliseconds, to wait between searches if the instant search</td>
</tr>
<tr>
<td>is enabled</td>
<td>feature is enabled. The default wait time is <strong>500 ms.</strong></td>
</tr>
<tr>
<td>Alternate URL Parameters for Search</td>
<td>Alternate parameters that appear in the search results URL. By default these</td>
</tr>
<tr>
<td></td>
<td>parameters include keyword and query.</td>
</tr>
<tr>
<td>Alternate URL Parameters for Language</td>
<td>Alternate parameters that appear in the URL denoting the selected language.</td>
</tr>
</tbody>
</table>

5. Click **Save**.

**Configure knowledge base tile widget instance options**

Configure widget instance options for the knowledge base tile widgets on the Knowledge Management Service Portal homepage.

Role required: knowledge_admin or admin

The homepage uses the Knowledge Bases Browse widget to display knowledge base tiles.

1. Navigate to the Knowledge Management Service Portal homepage.
2. Control + right-click a knowledge base tile.
3. Click **Instance Options**.
4. Configure the desired settings for the knowledge base tile widgets.

<table>
<thead>
<tr>
<th>Instance option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>The title that appears above the knowledge base tiles. The default is <strong>Explore our Knowledge Bases.</strong></td>
</tr>
<tr>
<td>Bootstrap color</td>
<td>The color of the widget.</td>
</tr>
<tr>
<td>CSS</td>
<td>CSS used in the widget instance.</td>
</tr>
<tr>
<td>Order By</td>
<td>The order in which the knowledge base tiles appear on the homepage. Use any</td>
</tr>
<tr>
<td></td>
<td>field on the Knowledge table. If this field is empty, tiles are displayed</td>
</tr>
<tr>
<td></td>
<td>in alphabetical order. Other available options include article_count.</td>
</tr>
<tr>
<td>Reverse Order</td>
<td>Enable this check box to display knowledge base tiles in the reverse order.</td>
</tr>
<tr>
<td>Post Question Label</td>
<td>The label on the button used to post a question. The default is <strong>Ask a Question.</strong></td>
</tr>
<tr>
<td>Create Article Label</td>
<td>The label on the button used to create an article. The default is <strong>Create Article.</strong></td>
</tr>
<tr>
<td>Post Question URL</td>
<td>The parameters that appear in the URL when posting a question.</td>
</tr>
<tr>
<td>Create Article URL</td>
<td>The parameters that appear in the URL when creating an article.</td>
</tr>
</tbody>
</table>

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.
Configure article list widget instance options

Configure widget instance options for the article lists on the Knowledge Management Service Portal homepage.

Role required: knowledge_admin or admin

The homepage uses the Article List widget to display different lists of articles, including Featured, Most Useful, and Most Viewed.

1. Navigate to the Knowledge Management Service Portal homepage.
2. Control + right-click one of the article list headers.
3. Click Instance Options.
4. Configure the desired settings for the article list widget.

<table>
<thead>
<tr>
<th>Instance option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>The title of the article list.</td>
</tr>
<tr>
<td>Bootstrap color</td>
<td>The color of the widget.</td>
</tr>
<tr>
<td>Glyph</td>
<td>An icon that appears in the widget.</td>
</tr>
<tr>
<td>CSS</td>
<td>CSS used in the widget instance.</td>
</tr>
<tr>
<td>Table</td>
<td>The table that stores the list articles.</td>
</tr>
<tr>
<td>Display Field</td>
<td>The title displayed for each article in the list. By default, this is the article short description.</td>
</tr>
<tr>
<td>Secondary Fields</td>
<td>Additional information displayed for each article in the list below the title. By default, this information includes the author, view count, the date that the article was last modified, and the article rating.</td>
</tr>
<tr>
<td>Max number of records to show</td>
<td>The maximum number of articles to include in the list.</td>
</tr>
<tr>
<td>Show even when empty</td>
<td>Enable this check box to display the article list even if it does not contain any articles.</td>
</tr>
<tr>
<td>Show Secondary Fields Label</td>
<td>Enable this check box to display the field labels for the additional information displayed for each article.</td>
</tr>
<tr>
<td>Knowledge Base</td>
<td>To restrict the articles that appear in this list to a specific knowledge base, select the knowledge base from the knowledge base list.</td>
</tr>
</tbody>
</table>

5. Click Save.

Configure sort widget instance options

Configure widget instance options for the knowledge sort widget on the Knowledge Management Service Portal search results page.

Role required: knowledge_admin or admin

The search results page uses the Knowledge Result Sort widget to provide sort options for the returned list of results. Use the widget instance options to customize the sort options.

1. Navigate to the Knowledge Management Service Portal search results page.
2. Control + right-click the sort options at the top of the results list.
3. Click **Instance Options**.
4. Configure the desired settings for the sort widget.

<table>
<thead>
<tr>
<th>Instance option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bootstrap color</td>
<td>The color of the search widget.</td>
</tr>
<tr>
<td>CSS</td>
<td>CSS used in the widget instance.</td>
</tr>
<tr>
<td>Hide Relevancy</td>
<td>Removes the relevancy sort option.</td>
</tr>
<tr>
<td>Table</td>
<td>The table that contains the fields used to sort the list of knowledge items. The default table is <strong>Knowledge</strong>.</td>
</tr>
<tr>
<td>Sort Fields</td>
<td>The fields used for sorting the list of knowledge items.</td>
</tr>
<tr>
<td>Sort Field Labels</td>
<td>The labels for the fields that appear in the sort options. The default is <strong>Views:desc,Newest:desc,Alphabetical</strong>. The sort order for the sort field labels is ascending. To use a descending order, denote <strong>:desc</strong>.</td>
</tr>
</tbody>
</table>

5. Click **Save**.

### Configure search results list widget instance options

Configure widget instance options for the results list widget on the Knowledge Management Service Portal search results page.

**Role required:** knowledge_admin or admin

The search results page uses the Knowledge Result widget to provide display options for the returned list of results. Use the widget instance options to customize the display options.

1. Navigate to the Knowledge Management Service Portal search results page.
2. Control + right-click the list of returned search results.
3. Click **Instance Options**.
4. Configure the desired settings for the results list widget.

<table>
<thead>
<tr>
<th>Instance option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Glyph</td>
<td></td>
</tr>
<tr>
<td>CSS</td>
<td>CSS used in the widget instance.</td>
</tr>
<tr>
<td>Show Relevancy Score</td>
<td>Shows how relevant each search result is based on the search term. The default setting uses the system property.</td>
</tr>
<tr>
<td>Breadcrumb: Hide Categories</td>
<td>Hides the category in the breadcrumb that appears below the article short description or question in the results list. The default setting uses the system property.</td>
</tr>
<tr>
<td>Breadcrumb: Knowledge Base Separator</td>
<td>The character used as a separator between the knowledge base and the category in the breadcrumb.</td>
</tr>
<tr>
<td>Breadcrumb: Category Separator</td>
<td>The character used as a separator between categories in the breadcrumb.</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>Instance option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Sort Order</td>
<td>The default sort order for the list of returned results. The default sort order is <code>sys_view_count:desc</code>, which sorts the results by the number of views in descending order.</td>
</tr>
<tr>
<td>How to Display Attachments in Knowledge Search Results</td>
<td>How attachments are shown in the list of returned results. The default uses the system property.</td>
</tr>
<tr>
<td>Label for Show Pinned Articles Link</td>
<td>The text used for the pinned articles link.</td>
</tr>
<tr>
<td>Maximum number of articles in first fetch</td>
<td>The maximum number of items included when the search results list is first displayed.</td>
</tr>
<tr>
<td>Maximum number of articles in subsequent fetches on scroll</td>
<td>The maximum number of items included when the search results list updates as the user scrolls to the bottom.</td>
</tr>
<tr>
<td>Table</td>
<td>The table that stores the information returned in the search results.</td>
</tr>
<tr>
<td>Knowledge Secondary Fields</td>
<td>Fields that display additional information for each article in the search results.</td>
</tr>
<tr>
<td>Social Secondary Fields</td>
<td>Fields that display additional information for each social Q&amp;A item in the search results.</td>
</tr>
<tr>
<td>Show Secondary Fields Label</td>
<td>Enable this check box to display the field labels for the additional information displayed for each result.</td>
</tr>
</tbody>
</table>

5. **Click Save.**

**Configure filter facet widget instance options**

Configure widget instance options for the filter facet widgets on the Knowledge Management Service Portal search results page.

Role required: knowledge_admin or admin

The homepage uses several widgets to filter the items in the search results list. There are two types of facet widgets:

- Simple field facets based on the Knowledge table fields
- Advanced query facets based on custom queries of the Knowledge table

Use the widget instance options to customize these facet widgets:

- Knowledge Field Facet (for filtering by knowledge base, knowledge category, and author)
- Knowledge Tags Facet (for filtering by tag)
- Knowledge Resource Facet (for filtering by resource, such as articles and social Q&A)
- Knowledge Query Facet (for filtering by rating, last modified, and number of views)

1. Navigate to the Knowledge Management Service Portal search results page.
2. Control + right-click a filter facet widget.
3. Click Instance Options.
4. Configure the desired settings for the selected type of facet widget.
<table>
<thead>
<tr>
<th>Instance option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Glyph</td>
<td>An icon that appears to the left of the title.</td>
</tr>
<tr>
<td>Order</td>
<td>The order in which the filter facet widgets appear on the left side of the search results page. If empty, the filter facet widgets sort alphabetically.</td>
</tr>
<tr>
<td>Bootstrap color</td>
<td>The color of the filter facet widget header.</td>
</tr>
<tr>
<td>CSS</td>
<td>CSS used in the widget instance.</td>
</tr>
<tr>
<td>Source Table</td>
<td>The table that contains the Source Field used to provide the filter facet widget options. The default table is Knowledge (kb_knowledge).</td>
</tr>
<tr>
<td>Source Field</td>
<td>The field in the Source Table that provides the filter facet widget options. Field types that can be used as a source field include string, choice, integer, reference, and boolean.</td>
</tr>
<tr>
<td>Facet Identifier</td>
<td>A unique name for the custom query facet that can be used in script code.</td>
</tr>
<tr>
<td>Facet Template</td>
<td>The selected template determines the type of facet interaction.</td>
</tr>
<tr>
<td></td>
<td>Knowledge Field Facet widget templates:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Single Select</strong>: users can select only one filter from this widget.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Multi Select</strong>: users can select more than one filter from this widget.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Dropdown Select</strong>: users can select more than one filter from a drop down menu.</td>
</tr>
<tr>
<td></td>
<td>Knowledge Query Facet widget templates</td>
</tr>
<tr>
<td></td>
<td>- <strong>Simple Query</strong>: shows a label for each facet value.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Rating</strong>: shows rating stars.</td>
</tr>
<tr>
<td>Custom Template</td>
<td>A custom template that determines facet interaction and value selection.</td>
</tr>
<tr>
<td>Facet Options</td>
<td>A custom query in JSON format for the label, ID, order, and query for each facet value. Includes the table, value (encoded query), and display value (encoded query).</td>
</tr>
<tr>
<td>Order by</td>
<td>Determines the sort order of the filter options within the facet widget. The default order is label, which sorts the options in alphabetical order. For reference fields, you can also state an order from the reference field table.</td>
</tr>
<tr>
<td>Minimum results for showing filter search bar</td>
<td>The minimum number of results required to display a search bar at the top of the filter facet widget.</td>
</tr>
<tr>
<td>Minimum results for showing scroll bar</td>
<td>The minimum number of results required to display a scroll bar in the filter facet widget.</td>
</tr>
</tbody>
</table>
## ServiceNow    Jakarta    Now Platform Capabilities

### Table: Instance Option Descriptions

<table>
<thead>
<tr>
<th>Instance option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum length for string field</td>
<td>Only fields whose maximum length is less than this value are allowed to be added as a filter facet.</td>
</tr>
<tr>
<td>Alternate URL Parameters</td>
<td>The names of the URL parameters used to initialize this filter facet, if it is used in the URL as a search parameter.</td>
</tr>
<tr>
<td>Fetch Maximum Values</td>
<td>If enabled, fetches all facet values instead of only those facets applicable for the initial load of results. Disabling this instance option can reduce the load time for the filter facet. Based on the glide.knowman.search.facet_depth property.</td>
</tr>
<tr>
<td>Show Empty Value</td>
<td>If enabled, shows an empty filter facet option that users can select to filter for articles that do not have this field set. For example, if an article does not have an assigned category, clicking the empty option lists all articles with no assigned category.</td>
</tr>
<tr>
<td>Show Only Facet Values Matching Results</td>
<td>Creates a dynamic filter facet widget that displays only those filter values that match the search results rather than showing all values. Disabling this instance option can reduce the time needed to load the filter facet data.</td>
</tr>
</tbody>
</table>

5. Click **Save**.

---

**Configure a user action for the article view page**

Configure a user action for the Knowledge Management Service Portal article view page.

**Role required:** admin

The article view page uses the Knowledge Article Content widget to provide user actions. Use the widget instance options to customize these actions.

Ensure that the application scope on the Now Platform is set to Knowledge Management Service Portal.

User actions available for the article view page appear in a menu after clicking the overflow icon (*** in the article header. These actions enable users to flag an article, edit an article, or create an incident for an article.

1. Navigate to the Knowledge Management Service Portal article view page.
2. Control + right-click the article header.
3. Click **Instance Options**.
4. Configure the desired settings for the Knowledge Article Content widget.
<table>
<thead>
<tr>
<th>Instance option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hide All Actions</td>
<td>Hides the user actions in the article header including the <strong>Subscribe/Unsubscribe</strong> button and the overflow icon.</td>
</tr>
<tr>
<td>Show Version Information</td>
<td>Displays version information for the selected article. Requires the Knowledge Management Advanced plugin (com.snc.knowledge_advanced).</td>
</tr>
<tr>
<td>Show Create Incident Action</td>
<td>Displays the <strong>Create Incident</strong> user action when a user clicks the overflow icon in the article header.</td>
</tr>
<tr>
<td>Create Incident Action Label</td>
<td>The label for the user action that appears in the overflow icon menu. The default is <strong>Create Incident</strong>.</td>
</tr>
<tr>
<td>Create Incident Action URL</td>
<td>The target URL for the <strong>Create Incident</strong> user action. If no URL is specified, the system uses the URL in the <strong>glide.knowman.create_incident_link</strong> system property.</td>
</tr>
</tbody>
</table>

5. Click **Save**.

**Knowledge Management Service Portal navigation**

Navigate to the various sections of the service portal to find the information you need.

From the homepage, navigate to:

- The search results page by entering a word or term in the search bar and pressing Enter.
- A knowledge base by clicking a knowledge base tile.
- A knowledge article by clicking the article short description in the Featured, Most Useful, or Most Viewed article lists.

From the search results page, navigate to a knowledge article or a question by clicking the short description in the search results list.

From an article view page, navigate to recent tasks, affected products, or other articles listed in the widgets to the right of the article.

**Use the breadcrumb**

The breadcrumb appears at the top of the Knowledge Service Portal search page and article view page. The breadcrumb displays the location of the page or article currently in view.

Click links in the breadcrumb to move to the homepage, knowledge base, or search results page.

**Knowledge Management Service Portal searching**

Enter one or more words in the search bar on the Knowledge Management Service Portal homepage to view all search results.

Users can enter a search term and press the Enter key, which redirects to the search results page. The search results include items in which the short description, content, or attached files include
the search term. By default, knowledge search results include articles, pinned articles, and social Q&A.

Users can search for information on the Knowledge Management Service Portal homepage as well as filter the search results.

**Search auto-correct feature**

The Knowledge Management Service Portal homepage search tool also includes an auto-correct feature. When enabled, users can auto-correct a typing error in a search term by clicking one of the suggestions.

When a search term contains a misspelling, the search tool displays the search results page and includes one or more suggested terms at the top of the page under the heading **Did you mean**. Clicking one of these suggestions shows all of the search results that match the selected term.

Users with the system administrator role can enable this feature.

1. Navigate to **System Properties > Text Search**.
2. Set the following properties to **true**:
   - Suggest alternate search spellings for knowledge or global search (glide.ts.dym.enable_spell_correct)
   - Suggest related searches for knowledge or global search (glide.ts.dym.enable_chain_suggest)
3. Click **Save**.

**Knowledge Management Service Portal sorting**

Use the sort feature on the search results list page to sort knowledge articles and social Q&A in a variety of ways.

Sort the items in a knowledge base or search results list using the **Sort by** options at the top of the list.

- **Views**: sorts by number of article views.
- **Newest**: sorts by the date created or updated.
- **Alphabetical**: sorts alphabetically by the article **Short description** field.
- **Relevancy**: sorts by relevance to the search term.

By default, the selected option sorts in descending order. Click the option again to sort in ascending order.

The system saves the last selected sort option. When you navigate away from the search results page and then return, this sort option is retained.

**Sorting by language**

You can also sort articles by language if the I18N: Knowledge Management Internationalization Plugin v2 (com.glideapp.knowledge.i18n2) is activated.

Activating this plugin adds a language link at the top of the search results page. To sort by language, click this link and select the desired language from the drop-down menu. The search results list displays items in the selected language.
Knowledge Management Service Portal filtering

Filter knowledge base information or a list of search results using the filter facet widgets on the search results page.

The search results page includes multiple ways to filter the results using filter facet widgets. These widgets are listed in a column on the left side of the page and can be expanded and collapsed as needed. Refine results by expanding a filter and selecting specific items. Selections appear at the top of the search results list. By default, you can filter by:

- **Knowledge Base**: lists the available knowledge bases
- **Category**: lists the available knowledge categories
- **Author**: lists the names of the authors for the knowledge articles included in the search results list
- **Tags**: lists the knowledge tags for the items in the search results list.
- **Resource**: lists the types of items available, such as knowledge articles and social Q&A. For social Q&A, you can also filter for unanswered and answered questions, and question with answers that have been accepted.
- **Rating**: lists article ratings from 0-5 stars (clicking a rating displays articles that have the selected rating and higher)
- **Last Modified**: lists selections based on the timing of knowledge item modifications such as Past Month or Past Week
- **View Count**: lists the knowledge item view counts such as More Than 50 or Less Than 10

The selections that you make filter the items displayed in the search results list. The search results list updates to display only those items that match your selections. Deleting a selection reverses the
filtering in the list. The number of matching results displayed at the top of the list changes as you add and remove filters.

Clear filter selections in the following ways:

- The **Clear** button at the top of a filter widget clears all of the selections in that widget.
- The **Clear all** button at the top of the search results list clears all of the widget selections.
- Clear individual filters at the top of the search results list by clicking the X in the filter name.

**Integrating new knowledge portal pages with the service portal**

Using the base system service portal, access the improved version of the knowledge portal that features an enhanced landing page with multiple knowledge bases, an article view page that includes new article widgets, and the search results page that displays global knowledge search results.

To access the *enhanced knowledge portal pages* from the service portal, as a system administrator, you can configure the following in the service portal:

**Note:** The knowledge portal page integrations described in this section can only be performed in the base system service portal.

- Link the Knowledge header menu and the Knowledge Base tile widget to point to the new Knowledge Management Service Portal homepage.
- Configure the type ahead and global knowledge search results links that currently point to the previous version of the knowledge portal article view page to point to the new Knowledge Management Service Portal article view page.
- Add a knowledge search widget to perform a highly configurable global knowledge search in the Knowledge Management Service Portal search results page.
- Replace the Top Rated article widget with one of the new widgets provided in the Knowledge portal.

**Configure the knowledge header menu and tile widget**

Access the new knowledge portal home page using the Knowledge header menu and the Knowledge Base tile widget in the service portal.

Role required: admin

1. Configure the Knowledge header link to point to the knowledge portal home page.

   **Knowledge link on service portal header**

   To configure:
   a) Navigate to **Service Portal > Portals**.
   b) In the **Service Ports** list, select the **Service Portal** record.
   c) In the **KB home page** field, enter *kb_home*.
   d) Click **Update**.

   When you click **Knowledge** in the service portal header menu, it takes you to the knowledge portal home page.
2. Configure the **Knowledge Base** tile widget to link to the knowledge portal home page.

   ![Knowledge tile widget](image)

   **To configure:**
   a) Navigate to the service portal page.
   b) Control + right-click the knowledge base tile widget and select **Instance Options**. The Knowledge Base form appears.
   c) In the **Page** field, change the value from `kb_view` to `kb_home`.
   d) Click **Save**.

   When you click the **Knowledge Base** tile widget in the service portal page, it takes you to the knowledge portal homepage.

Configure the knowledge portal URL to link to the article view page

Use the service portal to access the new knowledge portal article view page that features type ahead search and a highly configurable search results page.

Role required: admin

You must configure the type ahead knowledge portal link and knowledge global search results link in the knowledge base search source and in the service catalog search source, to point to the **Knowledge Management Service Portal article view page**.

1. Complete the following steps to configure the type ahead knowledge portal link and the knowledge global search results link in the knowledge base search source.

   a) Navigate to **Service Portal > Search Sources** and click the **Knowledge Base** search source.

   b) In the **Search page template** field, change the following line of code from:

   ```
   "?id=kb_article_view&amp;sys_kb_id={{item.sys_id}}"
   ```

   to

   ```
   "?id=kb_article&amp;sys_id={{item.sys_id}}"
   ```

© 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.
c) In the Data Source tab, go to the Data fetch script field and add the following line of code:

```javascript
article.url = '?id=kb_article_view&amp;sys_kb_id=' + kb.sys_id;
```
data.article_count = kb.getRowCount();

var kbCount = 0;
while (kb.next() && kbCount < data.article_count) {
    // Does user have permission
    if (!$sp.canReadRecord("kb_kb", kb.sys_id)) {
        continue;
    }

    var article = {};
    $sp.getRecordDisplayValues(article, kb,
        'sys_id, number, short_description, publishedUTC, type',
        article.publishedUTC = kb.get(
            article.type = "kb";
        if (!article.text) {
            article.text = "";
        article.text = $sp.stripHTML(article.text);
        article.score = parseInt(kb.
        article.label = article.short
        article.primary = article.sho
        article.url = '?id=kb_article
        results.push(article);
        kbCount++;
    }
}$sp.logSearch('kb_kb', data); return results;
d) Right-click the form header and click **Save**.

2. Complete the following steps to configure the type ahead knowledge portal link and the knowledge global search results link in the service catalog search source.
   a) Navigate to **Service Portal > Search Sources** and click the **Service Catalog** search source.
   b) In the **Search page template** field, change the href tag to the following:

   ```html
   <a ng-if="item.content_type == 'kb'" ng-href="?
   id=kb_article&sys_id={{::item.kb_article}}" class="h4 text-primary m-b-sm block">
   ```
c) In the **Data Source** tab, go to the **Data fetch script** field and change the code in line 45 to the following, as shown in image below:

```javascript
item.url = '?id=kb_article_view&sys_kb_id=' + kb.sys_id;
```
3. Click Update.
The knowledge results from type ahead and global search in the service portal point to the new knowledge portal article view page.

**Enable search on all knowledge bases.**

**Add a knowledge search widget to the Service Portal**

Create and add a new widget to the service portal search results page to navigate to the enhanced knowledge search results page.

Role required: admin

Create and add a **Search Within** knowledge widget to the service portal and link it to the Knowledge global search results page.

1. **Create a new widget** with the name **Search Within** using the following settings:

   **Field values to create a new knowledge search widget**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
</table>
   | HTML Template          | `<div role="list" class="list-group">
                             <span class="list-group-item active">${Search Within}</span>
                             <a role="link" class="list-group-item" ng-href="{{data.url}}">${Knowledge}</a>
                         </div>` |
   | Server Script          | `(function() {
                             var q = encodeURIComponent($sp.getParameter('q'));
                             var kb = $sp.getValue('kb_knowledge_base') || "";
                             data.url = '/sp?id=kb_search';
                             if(q)
                               data.url += "&keyword="+q;
                             if(kb)
                               data.url += "&kb_knowledge_base="+kb;
                       })();` |

2. **Add the widget to the service portal search results page.**

   To add the widget:
   
   a) Navigate to the service portal search page (https://<instance>.service-now.com/sp?id=search) in designer mode.
   
   b) In the **Filter Widget** search box, search for the **Search Within** widget and drag it into the container in the location you want the widget to appear in the service portal search results page.
The **Search Within** widget is added to the service portal search results page. In the service portal, when you click **Knowledge** in the **Search Within** widget, and search for a keyword, it redirects you to the knowledge global search results page.

### Add knowledge quick-access widgets

Add Featured Articles, Most Useful Articles, and Most Rated Articles knowledge widgets to the service portal page.

**Role required:** admin

Replace the existing Top Rated knowledge widget in the service portal with one or more of the knowledge quick-access widgets.

The following knowledge quick-access widgets are available to be added to the service portal:

- Featured Articles
- Most Useful Articles
- Most Viewed Articles

1. Navigate to the service portal home page in designer mode.
2. In the **Filter Widget** search box, search for the widget you had created and drag it into the container in the location you want the widget to appear in the service portal home page.

**Note:** You can click **Preview** to verify the location and appearance of the newly added widget.

When you click a link in the newly added quick-access widget from the service portal, it takes you to the knowledge portal page.
Knowledge subscriptions

Subscribe to knowledge bases and knowledge articles and receive email notifications about new articles and article revisions or comments.

- **Subscribed to a knowledge base:**
  - Knowledge base owners are auto-subscribed to all articles in the knowledge bases they own. They receive email notifications when new articles are created or revised (published) in the knowledge base.
  - Users who subscribe to a knowledge base receive email notifications when new articles are created in the knowledge base or if the existing articles are revised (published).

- **Subscribed to a knowledge article:**
  - Knowledge authors are auto-subscribed to the articles they create. They receive email notifications when the articles they created are checked out or revised (published) by other authors, and if the articles receive user comments.
  - Users who subscribe to an article receive email notifications when the article is revised (published).

Users can set their Knowledge notification preferences using **System Settings**.

The knowledge subscription feature is available for both the Knowledge Management v3 user interface and the Knowledge Management Service Portal.

Activate the Knowledge Management Advanced plugin (com.snc.knowledge_advanced) to use the knowledge subscription feature. The Knowledge Management Advanced plugin activates the Subscriptions and Activity Feed Framework plugin (com.snc.activity_subscriptions).

**Note:** The Knowledge Management Advanced plugin is not activated by default.

If the article versioning feature is enabled, the following notifications are also sent:

- An article is checked out
- An article is revised
- A new version of an article is published

Before using the article subscription feature, the system administrator must:

1. Activate the Knowledge Management Advanced plugin.
2. Configure the knowledge subscription properties.
3. If necessary, customize the article subscription email notification templates.

**Activate the Knowledge Management Advanced plugin**

You can activate the Knowledge Management Advanced plugin (com.snc.knowledge_advanced) if you have the admin role.

Role required: admin

The Knowledge Management Advanced plugin includes feature code and demo data. The Knowledge Management Advanced Installer plugin (com.snc.knowledge_advanced.installer) is used to activate the Knowledge Management Advanced features.

The Knowledge Management Advanced plugin activates the following features:
Article Versioning: Customers must migrate to Knowledge Management V3 completely to use article versioning. For more information, see Knowledge Management v3 migration.

Article Subscriptions: The Knowledge Management Advanced plugin activates the Subscriptions and Activity Feed Framework plugin (com.snc.activity_subscriptions).

This plugin performs two validation steps prior to activation.

- Determines if there are any active Knowledge Management v2 knowledge bases. The customer must migrate to Knowledge Management v3 completely to use article versioning.
- Determines if there is a unique database index on the Number field. If a unique constraint has been added to the Number field, the plugin activation fails. Follow the instructions listed in this KB0634959 to perform corrective steps to resolve the issue.

You need access to HI to be able to view KB articles.

**Note:** The Knowledge Management Advanced plugin is not automatically activated with the Knowledge Management v3 application.

Demo data is included as part of the Knowledge Management Advanced plugin. If the validation step performed by the Knowledge Management Advanced Installer plugin completes successfully, the Knowledge Management Advanced plugin is activated automatically. However, the demo data is not included in this activation. To load the demo data, go to the Knowledge Management Advanced plugin page, click the Load Demo Data Only related link, and then click OK.

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.

**Configure knowledge subscription properties**

These properties enable the knowledge subscription feature, identify the roles that can use the feature, and identify the article states that generate notifications.

Role required: knowledge_admin or admin

1. Navigate to Knowledge > Administration > Properties.
2. In the KM Subscription Properties section, configure the following properties.
Enable subscribe feature for KM
(glide.knowman.enable_km_subscription)

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable subscribe feature for KM</td>
<td>Enables or disables the Knowledge Management knowledge subscriptions feature.</td>
</tr>
<tr>
<td>List of roles (comma-separated) who can have subscription feature</td>
<td>A comma-separated list of the roles that can use the knowledge subscriptions feature and subscribe to knowledge bases and articles.</td>
</tr>
<tr>
<td>List of workflow states (comma-separated) that can have subscription feature</td>
<td>A comma-separated list of the article states for which the knowledge subscription feature is available. The default states include Draft, Review, and Published.</td>
</tr>
</tbody>
</table>

3. Click Save.

Knowledge subscription email notification templates

The knowledge subscription feature uses email notification templates to send subscription notifications to knowledge users.

<table>
<thead>
<tr>
<th>Email template</th>
<th>Subscription type</th>
</tr>
</thead>
<tbody>
<tr>
<td>KM Subscription: Article created</td>
<td>Knowledge base</td>
</tr>
<tr>
<td>KM Subscription: Article revised in KB</td>
<td>Knowledge base</td>
</tr>
<tr>
<td>KM Subscription: Article checked out</td>
<td>Knowledge article</td>
</tr>
<tr>
<td>KM Subscription: Article revised</td>
<td>Knowledge article</td>
</tr>
<tr>
<td>KM Subscription: Article commented</td>
<td>Knowledge article</td>
</tr>
</tbody>
</table>

Users with the admin or knowledge_admin role can customize these email notification templates. To locate the template, navigate to System Notifications > Email > Notifications. For more information about customizing a template, see Create an email notification.

Subscription notifications include a link at the bottom of the email to the user's Notification Preferences page.

Subscribe to a knowledge base

Subscribe to a knowledge base and receive notifications when articles are added to that knowledge base.

Role required: knowledge

Users can subscribe to a knowledge base from either the Knowledge Management v3 user interface or the Knowledge Management Service Portal.

1. Navigate to Knowledge > Homepage.
2. Click the Subscribe link on the knowledge base tile.
   The link changes to Subscribed and includes a check mark.

Subscribe to a knowledge article

Subscribe to a knowledge article within a knowledge base.

Role required: knowledge
Users can subscribe to a knowledge article from either the Knowledge Management v3 user interface or the Knowledge Management Service Portal.

**Note:**

Users who are already subscribed to a knowledge base are also subscribed to the articles within that knowledge base.

To subscribe to articles from the base service portal (https://<instance name>/sp?), you must navigate to the Knowledge Management Service Portal pages (for example: https://<instance name>/sp?id=kb_home) from the base service portal.

1. Navigate to Knowledge > Homepage.
2. Click Subscribe at the top of the knowledge article.
   The system displays an information message about the article subscription and the button toggles to Subscribed.

### Unsubscribe from a knowledge base

Unsubscribe from a knowledge base.

Role required: knowledge

Users can unsubscribe from a knowledge base from either the Knowledge Management v3 user interface or the Knowledge Management Service Portal.

**Note:** If you subscribe to an article and then subscribe to the knowledge base, unsubscribing from the knowledge base also unsubscribes you from the article.

1. Navigate to Knowledge > Homepage.
2. Point to and click the Subscribed link on the knowledge base tile, which toggles to Unsubscribe.
   After unsubscribing you from the knowledge base, the link toggles to Subscribe.

### Unsubscribe from a knowledge article

Unsubscribe from a knowledge article.

Role required: knowledge

Users can unsubscribe from a knowledge article from either the Knowledge Management v3 user interface or the Knowledge Management Service Portal.

**Note:** If you are subscribed to a knowledge base and you unsubscribe from an article in that knowledge base, you must also unsubscribe from the parent knowledge base.

1. Navigate to Knowledge > Homepage.
2. Point to and click Subscribed, which toggles to Unsubscribe.
   If you are subscribed to the knowledge article, this action results in an information message that the article subscription has been removed. If you are also subscribed to the parent knowledge base, proceed to the next step.
3. If you are subscribed to the parent knowledge base, click Yes on the Unsubscribe pop-up window.
   This action results in an information message that the knowledge base subscription has been removed.
Set knowledge subscription notification preferences

Set notification preferences for knowledge bases and knowledge articles.

Role required: knowledge

Users can set notification preferences from the Knowledge menu or from the Knowledge Management Service Portal.

1. Navigate to the Notification Settings page.

<table>
<thead>
<tr>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From the Knowledge application</td>
<td>Click the Notification Settings module.</td>
</tr>
<tr>
<td>From the Knowledge Management Service Portal</td>
<td>Click the user name in the portal header and then click Notification Settings.</td>
</tr>
</tbody>
</table>

2. Click the Notification Preferences tab.
3. Click Knowledge Base and enable or disable the knowledge base notification options.
4. Click Knowledge Articles and enable or disable the knowledge article notification options.

Manage knowledge subscriptions

Manage knowledge base and knowledge article subscriptions from the Notification Settings page.

Role required: knowledge

Users can manage knowledge subscriptions from the Knowledge application or from the Knowledge Management Service Portal.

1. Navigate to the Notification Settings page.

<table>
<thead>
<tr>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From the Knowledge application</td>
<td>Click the Notification Settings module.</td>
</tr>
<tr>
<td>From the Knowledge Management Service Portal</td>
<td>Click the user name in the portal header and then click Notification Settings.</td>
</tr>
</tbody>
</table>

2. Click the Subscriptions tab.
3. Click Knowledge Base or Knowledge Articles to see a list of current subscriptions.
4. To unsubscribe from a knowledge base or knowledge article, click Subscribed. The link toggles to Unsubscribed.

Managed Documents

Use the ServiceNow® Managed Documents application to control electronic documents within your instance.

After parameters have been set by the administrator and the Knowledge Document plugin installed, documents can move through the managed document cycle.

**Note:** Step through the process below on your test (or any non-production) instance.

Managed Document features

Managed Documents is a lightweight, ITIL-based solution for creating and managing electronic documents within your instance.
This application adds a layer of control around any document by providing workflow, storage, security, and categorization options. It can be used for a variety of internal documents, such as policies and procedures, compliance documentation, and knowledge articles. Because it is integrated within the instance, Managed Documents offers a seamless alternative to 3rd-party systems.

### Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check-in/Check-out</td>
<td>Track revisions, approval history, and automated notifications for approvers and reviewers. Useful for compliance and risk authors, policy and procedure writers, and contract administrators.</td>
</tr>
<tr>
<td>Categorization</td>
<td>Classify documents for organization and search.</td>
</tr>
<tr>
<td>Access control</td>
<td>Share documents with selected users.</td>
</tr>
<tr>
<td>Revision control</td>
<td>Track changes to documents.</td>
</tr>
<tr>
<td>Digital signature for approval</td>
<td>Integration with the Approval with E-Signature plugin.</td>
</tr>
<tr>
<td>Workflow</td>
<td>Support consistent content review and approval.</td>
</tr>
<tr>
<td>Security</td>
<td>Use high security setting.</td>
</tr>
</tbody>
</table>

### Managed Document concepts

The following concepts explain Managed Documents: Managed Document, Document Collection, Document Revisions, and Document Parameters.

<table>
<thead>
<tr>
<th>Concept</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed Document</td>
<td>The <strong>Document (dms_document)</strong> table contains the documents controlled through the managed documents process.</td>
</tr>
<tr>
<td>Document Collection</td>
<td>The <strong>Document Collection (dms_collection)</strong> table allows related documents to be grouped together.</td>
</tr>
<tr>
<td>Document Revisions</td>
<td>Because managed documents must have clear records of individual versions of a document, revisions (including the file) are attached to the master document record through a related list. Document revisions are controlled to keep a standard naming scheme and consistent version numbers. Once a document revision is ready, it can be submitted for review.</td>
</tr>
<tr>
<td>Concept</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Document Parameters</td>
<td><strong>Attention:</strong> Parameters do not control application or document security. Parameters only organize documents, they do not affect who can access documents. To grant access to the Managed Documents application, you can assign a role. To grant access to a specific document, set user and group permissions. Each document can be associated with predefined parameters. The parameters can help with grouping documents.</td>
</tr>
<tr>
<td></td>
<td>- Type: Defines the type of document being controlled. Documents of the same type use the same controls.</td>
</tr>
<tr>
<td></td>
<td>- Classification: Defines document restriction level, such as public, restricted, or confidential.</td>
</tr>
<tr>
<td></td>
<td>- Audience: Defines the groups with access to the document, such as internal or external.</td>
</tr>
<tr>
<td></td>
<td>- Name Formats: Defines the format of document names, ensuring that documents of the same type have the same name scheme assembled from name components.</td>
</tr>
<tr>
<td></td>
<td>- Name Components: Defines the document values used in the name formats.</td>
</tr>
<tr>
<td></td>
<td>- Approval Rules: Defines the approvals the document must have before it can be published.</td>
</tr>
</tbody>
</table>

**Install the Managed Documents plugin**

The Managed Documents plugin is available for activation by users with the admin role.

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**.

**Managed Documents plugin**

This page describes the applications and modules, database table structure, scripts, and roles.
Database table structure

The following tables are added:

<table>
<thead>
<tr>
<th>Display Name (Table Name)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revision (dms_revision)</td>
<td>The document revisions.</td>
</tr>
<tr>
<td>Audience (dms_audience)</td>
<td>The intended document readers.</td>
</tr>
<tr>
<td>Classifications (classification)</td>
<td>The document restriction level, such as public or confidential. (Does not define access to the document. Document security is set in user and group permissions.)</td>
</tr>
<tr>
<td>Type (dms_type)</td>
<td>The document purpose.</td>
</tr>
<tr>
<td>Component (dms_component)</td>
<td>The components of name formats. The value field is a dot-walking expression that is evaluated. An exception is made for the revision because it does not exist when the revision name is generated.</td>
</tr>
<tr>
<td>Name format (dms_name_format)</td>
<td>The composition of components to generate revision names.</td>
</tr>
<tr>
<td>Approval sequence (approval_sequence)</td>
<td>The approval sequences that users need to follow.</td>
</tr>
<tr>
<td>Approval Rule (dms_approval_rule)</td>
<td>The criteria that records of the dms_document table must match. Used to automatically add approvers to a document.</td>
</tr>
<tr>
<td>Collection (dms_collection)</td>
<td>The document groups created by the user.</td>
</tr>
</tbody>
</table>

Scripts

Business rules that are added to sys_script

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update Document</td>
<td>Changes the state of a document depending on its revisions.</td>
</tr>
<tr>
<td>Add Approvers</td>
<td>Populates the list of approvers in the document.</td>
</tr>
</tbody>
</table>

Script includes that will be added to sys_script_include

<table>
<thead>
<tr>
<th>Script include</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DocumentManagement</td>
<td>Contains the main logics for the Managed Documents plugin.</td>
</tr>
<tr>
<td>DocumentManagementDB</td>
<td>Contains methods to perform CRUD operations on the database.</td>
</tr>
<tr>
<td>DocumentManagementSecurity</td>
<td>Helps manage the security of the Managed Documents system.</td>
</tr>
</tbody>
</table>
### Script include

<table>
<thead>
<tr>
<th>Script include</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DocumentManagementAjax</td>
<td>Updates the details of the temporary revision that is created when opening the upload/check in revision form.</td>
</tr>
<tr>
<td>DocumentAttachmentAjax</td>
<td>Renames an attachment file.</td>
</tr>
<tr>
<td>DocumentRevisionWorkflowHelper</td>
<td>Helps perform basic workflow operations on a revision.</td>
</tr>
<tr>
<td>DocumentManagementApprovalMatcher</td>
<td>Helps obtain the user and group approvers for a document that matches approval rules.</td>
</tr>
<tr>
<td>DocumentApproverHelper</td>
<td>Contains logics to handle document approvers.</td>
</tr>
<tr>
<td>DocumentManagementUtils</td>
<td>Useful methods.</td>
</tr>
<tr>
<td>DocumentReferenceQualifiers</td>
<td>Static methods that return reference qualifiers.</td>
</tr>
</tbody>
</table>

### Client script that is added to sys_script_client

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document type change</td>
<td>Updates the name format field in the revision settings section of the document. Each type has a default name format.</td>
</tr>
</tbody>
</table>

### Roles

This plugin introduces two new roles:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>document_management_user</td>
<td>This role enables a user to access the Managed Documents plugin, create documents, and search for documents. Document reviewers and approvers need the document_management_user role to access the Managed Document plugin. (Please note that reviewers and approvers can also access a document revision from an approval record.)</td>
</tr>
<tr>
<td>document_management_admin</td>
<td>This role enables a user to change administrative settings for the Managed Documents plugin.</td>
</tr>
</tbody>
</table>

**Note:** Each document has individual permissions, so even if a user is given the document_management_user role and has permissions to the application, the user can only view documents to which they have been given access.

### Create a new managed document record

Configure the properties and policies for a managed document.

1. Navigate to **Managed Documents > Create New**.
2. In the **Name** field, type **Policy**.
3. In the Requested by field, add your name.
4. In the Owner field, add your name.
5. In the Reviewer field, add your name.
6. In the Type field, select Policy.
7. In the Classification field, select Confidential.
8. In the Audience field, select Internal.
9. Under Revision Settings, select the Auto increment revision option.

10. Click Submit.

Check in a document after making changes

After making changes to a document, check the revised document into Managed Documents.
1. Open the document record.
2. Click the Upload/Check in Revision related link.
3. Click Choose File, select the revised file, and click Open.
4. Check that the Name and Revision Number contain the updated number.
5. Ensure that the Check in option is selected.
6. Click OK.

The Document Revisions list updates to contain the most recent revision.

Check out a document to make changes

After a document is added to a managed document record, check the file out to make changes. Checking documents in and out keeps a record of document changes and ensures that only one person at a time is editing the document.
1. Open the document record.
2. Select the Check Out Document related link.
3. Select **Download file**.
4. Click **Check Out**.
5. Open the file and make a small change.
6. Save the document with the same name, but a new revision number. For example, `Policy_POL_02.txt`.

**Publish a document in Managed Documents**

After the document is reviewed and approved, publish the document within Managed Documents.

1. Open the document record.
2. In the Document Revisions list, click the name of the revision that was approved and is listed in the Ready for Publishing stage.
3. In the header bar, click **Publish Revision**.
4. In the Publish revision dialog box, check that the name and revision number are correct and click **Publish**.
   In the Document Revisions list, the revision you just published is now in the Published stage.
Send a document out for review and approval

When a document is ready, send it out for review and approval. If a reviewer or approver is not identified in the document record, the document is moved directly to the publishing stage.

1. In the Document Revisions list, right-click the revised document and select **Submit Revision**.

![Submit Revision](image)

Because you identified yourself as the reviewer, you receive an approve request email message.

2. In the email message, click the link next to **Click here to view Approval Request**.
3. (Optional) View the document by clicking the attachment name under **Document Revision**.
4. Click **Approve**.
   
   The Approvals page displays and lists the document you just approved.
5. Open the document record.
6. In the Document Revisions list, the revision you approved is now in the Ready for Publishing stage.

Upload a document as an attachment

After creating a document record, add the document to the record as an attachment.

1. Open the document record.
2. Select the **Upload/Check in Revision** related link.

![Upload/Check in Revision](image)

3. Click **Choose File**.
4. Select a simple document, such as a text file, and click **Open**.
5. Check that the name reads **Policy_POL_0.1**.
6. Click **OK**.

   The document is listed under Document Revisions.
**Defining Document Parameters**

Before using the Managed Documents application, the user with the `document_management_admin` role needs to set the parameters that define the kinds of documents to be managed through the application. Managed Documents provides both base and custom parameter options.

**Defining Document Parameters**

The following document parameters should be defined:

- **Type**: identifies the purpose of the document. The type also determines the default document format and name format.
- **Classification**: indicates the security level assigned to the document and determines who can view or edit the document.
- **Audience**: specifies the intended readers of the document.
- **Name format**: specifies the name format to use when a document revision is added.
- **Name components**: are individual identifiers used inside a name format. Name components define a reference path (often by dot-walking) that holds the value specific to the document.
- **Approval rules**: determine which approvers are added to documents (in addition to the Reviewers specified on the document record).

**Defining Types**

To define a new type, navigate to **Managed Documents > Administration > Type** and click **New**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for the type.</td>
</tr>
<tr>
<td>Code</td>
<td>A short code for the type. Referenced as a name component for the name format.</td>
</tr>
<tr>
<td>Label</td>
<td>A label to display in the Type choice list.</td>
</tr>
<tr>
<td>Name Format</td>
<td>The name format that documents of this type will use.</td>
</tr>
<tr>
<td>Order</td>
<td>A number indicating the type's sequence in the choice list.</td>
</tr>
</tbody>
</table>

The following types are available in the base system.

<table>
<thead>
<tr>
<th>Name</th>
<th>Code</th>
<th>Label</th>
<th>Name format</th>
<th>Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>-- None --</td>
<td>null</td>
<td>-- None --</td>
<td>null</td>
<td>1</td>
</tr>
<tr>
<td>policy</td>
<td>POL</td>
<td>Policy</td>
<td>Default Policy</td>
<td>2</td>
</tr>
<tr>
<td>guideline</td>
<td>GUI</td>
<td>Guideline</td>
<td>Default</td>
<td>3</td>
</tr>
<tr>
<td>procedure</td>
<td>PROC</td>
<td>Procedure</td>
<td>Default</td>
<td>4</td>
</tr>
<tr>
<td>contract</td>
<td>CON</td>
<td>Contract</td>
<td>Default</td>
<td>5</td>
</tr>
</tbody>
</table>
Defining Approval Rules

To define a new approval rule, navigate to Managed Documents > Administration > Approval Rules and click New.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique identifier for the approval rule.</td>
</tr>
<tr>
<td>Active</td>
<td>A check box indicating whether this approval rule is used.</td>
</tr>
<tr>
<td>Condition</td>
<td>A condition builder that determines which documents use this approval rule.</td>
</tr>
<tr>
<td>Description</td>
<td>A short description of the approval rule.</td>
</tr>
</tbody>
</table>

Once the approval rule is saved, the Approvers related list defines which approvers are added if the conditions in the Condition field are met.

The following approval rules are available in the base system.

<table>
<thead>
<tr>
<th>Name</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal policy</td>
<td>type=Policy ^ audience=Internal</td>
</tr>
<tr>
<td>Development policy</td>
<td>type=Policy ^ department=Development</td>
</tr>
</tbody>
</table>

Defining Audiences

To define a new audience, navigate to Managed Documents > Administration > Audience and click New.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audience Name</td>
<td>A unique name for the audience.</td>
</tr>
<tr>
<td>Audience Code</td>
<td>A short code for the audience. Referenced as a name component for the name format.</td>
</tr>
<tr>
<td>Label</td>
<td>A label to display in the Audience choice list.</td>
</tr>
<tr>
<td>Order</td>
<td>A number indicating this audience's sequence in the choice list.</td>
</tr>
</tbody>
</table>

The following audiences are available in the base system.

<table>
<thead>
<tr>
<th>Audience</th>
<th>Audience code</th>
<th>Label</th>
<th>Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>internal</td>
<td>INT</td>
<td>Internal</td>
<td>1</td>
</tr>
<tr>
<td>external</td>
<td>EXT</td>
<td>External</td>
<td>2</td>
</tr>
</tbody>
</table>

Defining Classifications

Define a new classification on the Classification form.
Navigate to Managed Documents > Administration > Classification and click New.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for the classification.</td>
</tr>
<tr>
<td>Code</td>
<td>A short code for the classification. Referenced as a name component for the name format.</td>
</tr>
<tr>
<td>Label</td>
<td>A label to display in the Classification choice list.</td>
</tr>
<tr>
<td>Order</td>
<td>A number indicating this classification's sequence in the choice list.</td>
</tr>
</tbody>
</table>

The following classifications are available in the base system.

<table>
<thead>
<tr>
<th>Name</th>
<th>Code</th>
<th>Label</th>
<th>Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>public</td>
<td>P</td>
<td>Public</td>
<td>1</td>
</tr>
<tr>
<td>restricted</td>
<td>R</td>
<td>Restricted</td>
<td>2</td>
</tr>
<tr>
<td>confidential</td>
<td>C</td>
<td>Confidential</td>
<td>3</td>
</tr>
</tbody>
</table>

Defining Name Components

Name components define the document values used in the name format.

For example, the name component `document.audience.code` dot-walks from the document record to the audience Code.

To define a new name component, navigate to Managed Documents > Administration > Components and click New.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique identifier for the name component.</td>
</tr>
<tr>
<td>Short Description</td>
<td>A short description of the name component value.</td>
</tr>
</tbody>
</table>
| Value          | The path to the field holding the value used for the name format. Defined relative to a current revision record. For example:  
- Enter `revision` to use the revision Number field on the revision record.  
- Enter `document.name` to use the Name field on the revision's referenced document.  
- Enter `document.audience.code` to use the Code field for the audience referenced by the document.  
This dot-walking approach makes it possible to get any value related to the revision into the name format. |

Note: The revision component is a special component replaced by the appropriate revision number (rather than querying a value related to the current record). The revision
is either automatically incremented or uses the latest revision number, depending on the setting on the document form.

The following components are defined in the base system.

<table>
<thead>
<tr>
<th>Name</th>
<th>Short description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audience code</td>
<td>Displays the code assigned to the document audience.</td>
<td>document.audience.code</td>
</tr>
<tr>
<td>Classification code</td>
<td>Displays the classification code.</td>
<td>document.classification.code</td>
</tr>
<tr>
<td>Document name</td>
<td>Displays the document name.</td>
<td>document.name</td>
</tr>
<tr>
<td>Revision</td>
<td>Displays the document revision.</td>
<td>revision</td>
</tr>
<tr>
<td>Type code</td>
<td>Displays the code assigned to the document type.</td>
<td>document.type.code</td>
</tr>
</tbody>
</table>

**Defining Name Formats**

The name format automatically generates a name for a document revision by arranging name components in a standard code to match naming conventions.

For example, a name format with the name components *Type Code*, *Document Name*, and *Revision Number* and the separator `-`, would be formatted as:

**TYPECODE-Name-RevNumber.fileformat**

In this example, a policy (code POL) named *IT Off-Boarding Policy*, with revision number *1.0*, and uploaded as a *docx* file would have the name:

**POL-IT Off-Boarding Policy-1.0.docx**

To define a new name format, navigate to **Managed Documents > Administration > Name Formats** and click **New**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for the name format.</td>
</tr>
<tr>
<td>Separator</td>
<td>A separator to put between each of the components. Hyphens <code>-</code> and underscores <code>_</code> are commonly used. Using alphanumeric characters can create a confusing name format.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the name format.</td>
</tr>
</tbody>
</table>

Use the related list to add name components. Use the **Order** field to set the sequence in which name components are used.

The following name formats are defined in the base system.

<table>
<thead>
<tr>
<th>Name</th>
<th>Separator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>_</td>
<td>The default format. Document name and revision separated by an underscore.</td>
</tr>
<tr>
<td>Default Policy</td>
<td>_</td>
<td>The format for the policy document type.</td>
</tr>
<tr>
<td>Development documentation</td>
<td>(no separator)</td>
<td>The format for the software documentation type.</td>
</tr>
<tr>
<td>Name</td>
<td>Separator</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>Development Sources</td>
<td>(no separator)</td>
<td>The format for the development and code sources type.</td>
</tr>
<tr>
<td>Intranet Improvement</td>
<td>(no separator)</td>
<td>The format for documents that describe intranet use.</td>
</tr>
</tbody>
</table>

**Defining Document Workflow**

In the base system, all managed documents use the **Managed Documents** workflow after the **Active** check box is selected.
Document workflow

The document parameters defined in the workflow are often used as conditions to trigger more specific workflows, such as type-specific workflows or classification-specific workflows. If different
kinds of documents should follow different workflows, use the Graphical Workflow Editor to create new workflows.

**Knowledge document**

The Knowledge Document plugin extends the Managed Documents plugin by providing the functionality for managed documents to be published to the knowledge base.

**Installed with knowledge document**

These elements are installed with the knowledge document plugin.

**Dependencies**

The Knowledge Document plugin depends on the Managed Documents plugin. Activating Knowledge Document activates Managed Documents.

**Tables**

<table>
<thead>
<tr>
<th>Display Name (table_name)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge Records (m2m_document_knowledge)</td>
<td>A many-to-many table storing the relationship between a document and a knowledge article.</td>
</tr>
</tbody>
</table>

**UI Actions**

<table>
<thead>
<tr>
<th>UI action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link to Knowledge</td>
<td>Creates or updates a knowledge article related to the current document, depending on whether a knowledge article already exists.</td>
</tr>
</tbody>
</table>

**Scripts**

<table>
<thead>
<tr>
<th>Script include</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KnowledgeDocument</td>
<td>Holds the main logic for the Knowledge Document plugin.</td>
</tr>
<tr>
<td>KnowledgeDocumentDB</td>
<td>Class that gets, inserts, and updates data for the Knowledge Document plugin.</td>
</tr>
</tbody>
</table>
Knowledge settings fields

These fields appear on the Managed Document form Knowledge Settings section.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behavior</td>
<td>Defines the process performed when the Link to Knowledge related link is clicked. Select <strong>Always create record</strong> to create a new knowledge article with the latest published revision attached. The knowledge article is then linked to the document. Select <strong>Update existing record</strong> to update the existing knowledge article to the latest published revision. If no knowledge articles exist for the document, a new knowledge article is created. The <strong>Update existing record</strong> option is not available when many knowledge articles are linked to a document.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the type of knowledge article. Use Knowledge or any option that extends the kb_knowledge table. For example, if you have the IT GRC plugin installed to create GRC policies, select the type Policies. Note that when a knowledge article is created, the <strong>Type</strong> field becomes read-only.</td>
</tr>
<tr>
<td>Topic</td>
<td>Defines the subject of the document. Adds the topic information to the same field in the knowledge article.</td>
</tr>
<tr>
<td>Published</td>
<td>Date that the article should be published. Adds publishing date information to the same field in the knowledge article.</td>
</tr>
<tr>
<td>Valid to</td>
<td>Date that the article expires. Adds valid to date information to the same field in the knowledge article.</td>
</tr>
<tr>
<td>Short description</td>
<td>A few words or short phrase describing the knowledge article. Adds the short description to the same field in the knowledge article.</td>
</tr>
</tbody>
</table>

View knowledge linked to a document

You can view the knowledge linked to a document from the document record.

1. Navigate to the document record.
2. Select the **Knowledge Records** related list.
3. Select the knowledge article to view.

Create a document

After Managed Documents parameters have been set by the administrator, documents can be created, requested, checked out, edited, checked in, copied, and, if necessary, rolled back to an earlier version.

Once documents have been added to the Managed Documents application, they can be grouped into document collections.

Approval process

During the approval process, the approver approves or rejects the document. A document goes through the approval process after the review process.

Approval workflow

After the document has been reviewed, submit the document for approval. If the document does not have an approver, the approval process is omitted.

When the document is Active, the workflow Document Management Default is used to manage approvals:
Document Management Default workflow
If the approver rejects the document, the author and owner are notified and the document review is cancelled. The author, owner, and approver should discuss what changes need to be made to the document. When the document is ready, a new review can be initiated.

If the final approver approves the document, the author and the owner are notified. Once final approval is successful, the document stage changes to Ready for Publishing in the Document Revisions list:

**Process modification for multiple approvers**

If there are multiple approvers, the approval process works in sequence and multiple approvers can be assigned to a single sequence. For example:

Sequence 1: approvers A and B
Sequence 2: approvers C and D
Sequence 3: approver E

Because the sequences take place in ascending chronological order, approvers A and B receive the approval request first (approvers C, D, and E are not part of the process yet). Similar to the review process, the first approver to act within a sequence dictates what happens to the document. If approver A acts first and rejects the document, the approval process stops and the state is set to Cancelled. Approver B's status is changed to No Longer Required. If approver A acts first and approves the document, the process stops and approver B's status is changed.
to No Longer Required. Then, the document moves to approval sequence 2. After at least one approver in each sequence approves the document, the author and the owner are notified that the document has been approved.

**Review process**

During the review process, the reviewer approves or rejects the document. Sometimes a document will have multiple reviewers.

If the reviewer rejects the document, the author and owner are notified and the review is cancelled. The author, owner, and reviewer should discuss what changes need to be made to the document. If the reviewer approves the document, the author and owner are notified that the review was successful and the document can move to the approval stage.

If multiple reviewers are assigned to a document, the first reviewer to act dictates what happens to the document. For example, there are two reviewers, A and B. If reviewer A acts first and rejects the document, the review process stops and the revision state is set to Cancelled. Reviewer B receives a notification email stating that the review was rejected and their status is changed to No Longer Required. If reviewer A acts first and approves the document, the review process stops and the document can move to the approval stage. Reviewer B’s status is changed to No Longer Required.

**Enable electronic signature for approval**

This topic explains how to enabling electronic signatures for approval. Electronic signatures are helpful if you must obtain a digital signature for compliance or auditing purposes.

You can activate the [Approval with e-signature](#) to require that users type in a user name and password when reviewing and approving documents.

The digital signature is not tracked or stored in the document record. Users must simply type in a user name and password after clicking the Approve or Reject button.

After activating the Approval with E-Signature plugin, ensure that a row in the e-signature registry table is created for the dms_document_revision table.

1. Navigate to [System Definition > e-Signature Registry](#).
2. Check if dms_document_revision is already listed and Enabled is set to true.
3. If not listed, click New.
4. **Table name**, select Document Revision.
5. Select Enabled.
6. Click Submit.

**Publish an approved revision**

This topic explains how to publish a document revision that has been approved.

Once a document has been created and edited, a specific revision can be submitted for draft review and final approval. After final approval, the document can be published.

Publish the approved revision from the Document Revisions list.

**Note:** Publishing documents to the Knowledge Base requires the Knowledge Document Plugin.

1. Navigate to the document record.
2. In the Document Revisions List, click the revision marked **Ready for Publishing**.
3. Click **Publish Revision** to display the Publish dialog box.

The revision number matches the latest revision number. If your standard is to change the revision number when the document is published, such as incrementing the version number to 1.1 or 1.0.1, the change can be made on this dialog box manually.

4. Click **Publish**.

The published revision is highlighted in green and the stage of previous revisions is automatically changed to Retired:
Note: If the approval and publishing process is repeated, the published revision is retired when the new revision is published. Any workflows running against previous revisions are canceled when the document is published.

Submit a revision for draft review

This topic explains how to submit a document draft for review.

Once a document has been created and edited, a specific revision can be submitted for draft review and final approval. After final approval, the document can be published.

When a draft of the document is ready, submit the draft for review. If the document does not have reviewers identified in the Reviewers field of the document record, the review process is omitted.

1. Navigate to the document record.
2. Right-click the appropriate revision.
3. Select Submit Revision.

The revision stage is set to Awaiting Review.
Create or request a new document

Once an administrator has set parameters for the Managed Documents application, you can create or request new documents.

1. Navigate to Managed Documents > Create New.
2. Complete the following fields:

   **New document fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Input value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>An identifying number for the document. Automatically generated using number maintenance.</td>
</tr>
<tr>
<td>Field</td>
<td>Input value</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Name</td>
<td>A name for the document. Note that the name for the document is combined with other naming components (as defined by the name format) to create the names for each document revision.</td>
</tr>
<tr>
<td>Requested by</td>
<td>The person asking that the document be created or updated.</td>
</tr>
<tr>
<td>Owner</td>
<td>The approver of the document request. Also responsible for setting completion date with requesters and authors.</td>
</tr>
<tr>
<td>Reviewers</td>
<td>The user or users who review the document and provide feedback to owners and authors.</td>
</tr>
<tr>
<td>Department</td>
<td>The department responsible for the document.</td>
</tr>
<tr>
<td>Type</td>
<td>The document purpose. This is a choice list derived from the type parameters.</td>
</tr>
<tr>
<td>Classification</td>
<td>The document classification, based on security, audience, and confidentiality. This is a choice list derived from the classification parameters.</td>
</tr>
<tr>
<td>Audience</td>
<td>The document readers, such as external or internal. This is a choice list derived from the audience parameters.</td>
</tr>
<tr>
<td>State</td>
<td>The current status of the document in the editing and publication process.</td>
</tr>
<tr>
<td>Checked out by</td>
<td>The user who currently has the document checked out.</td>
</tr>
<tr>
<td>Description</td>
<td>A short description of the document.</td>
</tr>
<tr>
<td>Revision Settings</td>
<td></td>
</tr>
<tr>
<td>Name format</td>
<td>The format for the name of each individual revision of the document. For more information, see Defining Name Formats.</td>
</tr>
<tr>
<td>Revision format</td>
<td>A choice between the two digit (0.x) or the three digit (0.0.x) revision format.</td>
</tr>
<tr>
<td>Auto increment revision</td>
<td>If selected, the revision number automatically increments each time the document is revised.</td>
</tr>
</tbody>
</table>

The User Permissions related list determines which users have rights to view and contribute to the document:

**User permissions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Input value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>A reference to a user who is entitled to read and contribute to the document.</td>
</tr>
</tbody>
</table>
The Group Permissions related list determines which groups have rights to view and contribute to the document:

**Group permissions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Input value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>A reference to a group of users who are entitled to read and contribute to the document.</td>
</tr>
</tbody>
</table>
| Type  | A choice list describing how group members can interact with the document. Options are:  
  - Reader - Group members can read the document versions.  
  - Editor - Group members can upload new versions.  
  - Owner - Group members can edit the document. |

### Specify an approver

You can specify approvers for a document record after you save it.

You can have one approver or multiple approvers. For example, set multiple approvers to have one person do a quality check of the document and a different individual to serve as a final approver. Approvers are assigned a number. The lowest number (usually number one) approver always goes first, then any other approvers in ascending chronological order. Multiple approvers can have the same sequence number. For example, two approvers can do a quality check and be assigned sequence number 1. Then, two individuals can be final approvers and be assigned sequence number 2.

1. Navigate to the document record.
2. Right-click in the document header bar and select **Add Approver**.
3. Add a user name.
4. Select a sequence number from the drop-down list. (Lower numbers approve before higher numbers. For example, approver number one approves before number two.)
5. Click **Add User**.
6. Repeat steps 2-5 to add more approvers.

### Check in a document

Check in the document after you revise it so other users can check out the document.

1. Navigate to the document record.
2. Select the **Upload/Check In Revision** related link.
3. Click **Browse** and navigate to the revised file.
4. Click **Open**.
5. Check the Name and Revision Number.
6. Click **OK**.

The Document Revisions related list updates to contain the most recent revision:

![Document Revisions](image)

**Document revisions**

**Copy a document**

A document can be duplicated at any time. This is useful if you have an existing document that you want to use as a base for a new document.

1. Navigate to the document record.
2. Right-click the header bar and select **Copy Document**.
   
   An information message with a link to the new document displays:
3. Click **OK**.
   
   The new document is renamed and includes the word "Copy."

**Note:** Only the latest revision is copied.

**Deactivate a document**

To change the document state to Inactive, deactivate the document. This is useful when changes to a document have been put on hold. An inactive document can be reopened at any time.

1. Navigate to the document record.
2. Right-click the header bar and select **Deactivate Document**.

**Note:** To activate a document, right-click on the header and click **Reopen Document**.

**Reopen a deactivated document**

A document that has been deactivated can be reopened.

1. Navigate to the document record.
2. Right-click the header bar and select **Reopen Document**.

**Roll back a document**

A document can be rolled back to an earlier revision at any time. Before rolling back to an earlier revision, ensure that the document is not checked out and that you have Editor or Owner permissions for the document.

1. Navigate to the document record.
2. In the Document Revisions list, click the revision to which you want to roll back.
3. Right-click the header bar and select **Rollback**. The Rollback to Revision dialog box displays. The name and revision number are new. The note specifies the revision to which you are rolling back.

4. Change any information on the Rollback to Revision dialog box as necessary.

5. Click **OK**. The latest revision is now the revision you selected for rollback.

**Cancel a document**

Change the document state to Cancelled when no more changes will be made to the document.

When canceling a document, there is no confirmation message, so ensure that you want to cancel the document.

1. Navigate to the document record.
2. Right-click the header bar and select **Cancel Document**.

   An info message confirms the cancellation:

   The State is set to Cancelled:
Check out a document

Documents in the Managed Documents application can only be revised by one user at a time. Check out the document to revise it.

1. Navigate to the document record.
2. Select the Check Out Document related link.
3. Select Download file to download the current version of the document when it is checked out.

4. Click Check Out.

After checking out a document, you can edit the document and make any necessary changes.

Create a document collection

A document collection is a set of individual documents. After documents have been uploaded into Managed Documents, organize the documents by grouping them into collections.

1. Navigate to Managed Documents > Document > My Collections.
2. Select New.
3. Type in a Name.
4. (Optional) Type in a Description.
5. Click Submit.
6. Click the name of the collection you created.
7. Click Edit.
8. On the left, double-click an available document or select a document and click **Add**.
9. Click **Save**. The Document Collection page displays and the individual documents in the collection are listed:

![Document Collection](image)

**Upload a document**

Upload a document into a saved record. You can upload text files, spreadsheets, presentations, PDF files, and more.

1. Navigate to the document record.
2. Click the **Upload/Check In Revision** related link.
3. Click **Choose File** and navigate to the file.
4. Click **Open**.
5. Check the Name and Revision Number.
6. Click **OK**.

After the initial document is uploaded, subsequent revisions can be created by checking out the document.
**MetricBase**

Use the MetricBase product to collect, retain, analyze, and visualize time series data on the Now Platform.

Time series data is a collection of values for an item taken at specific time intervals. Time series data is stored in a separate database, called the MetricBase database. An example is collecting CPU usage values for a computer every hour. You can then use the time series data to evaluate system capacity issues.

The MetricBase product is integrated with the Now Platform making it easy to handle time series data for applications on the Now Platform. The MetricBase database saves values as floating-point numbers.

The MetricBase product is available as a separate subscription. For more information, see Request the MetricBase product.

**Request the MetricBase product**

The MetricBase product requires a separate subscription and must be activated by ServiceNow personnel.

Role required: none

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.

**View time series retention policies**

The MetricBase application provides pre-defined retention policies that define the data collection interval for a metric.

Role required: admin

How often time series data is collected and how long the time series data is retained are important parameters for each metric. The MetricBase application provides pre-defined retention policies. You cannot create retention policies.

A retention policy is a series of time periods and collection rates. An example is `8d@1h`, which means for eight days data is collected at one hour intervals. A retention policy is a series of these time periods with longer intervals for each subsequent time period. For example, `8d@1m, 31d@30m, 397d@1h`.

Retention policies define the collection interval, which changes with the age of the data. Older data is compacted and stored with lower fidelity. You can see the available retention policies with the Retention Policies module. The `8d@1m, 31d@30m, 397d@1h` retention policy means

- For the last eight days, data points are available at 1-minute intervals.
- Data points from 9 through 31 days are compressed to 30-minute intervals.
- Data points older than 32 days are compressed to 1-hour intervals.
- If data is ingested at 30-second intervals in the last eight days, one data point is lost. Data in the last eight days are always stored at 1-minute intervals.
- If data is ingested at 2-minute intervals in the last eight days, the missing data points are stored as NaN. Data in the last eight days are always stored at 1-minute intervals.

1. Navigate to MetricBase > Retention Policies.
2. Click a policy to view the collection interval specification.
Create a time series metric

Create a time series metric record for each item for which time series data is to be collected. You must define the table, metric field name, and the retention policy.

Role required: admin

2. Click New.
3. Complete the time series metric definition form then click Submit.

Time series metric definition

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>Name of the metric.</td>
</tr>
<tr>
<td>Table name</td>
<td>Name of the table to contain the metric. A table can have multiple metric columns. Required.</td>
</tr>
<tr>
<td>Metric field name</td>
<td>Required. Define the name of the column to add to the target table.</td>
</tr>
<tr>
<td>Retention policy</td>
<td>Required. Retention policy to use. Select one of the available retention policies.</td>
</tr>
<tr>
<td>Application</td>
<td>Application for which this metric is defined. (Auto filled)</td>
</tr>
<tr>
<td>Display value aggregator</td>
<td>Aggregation to use for the metric field display value on the list view of the table.</td>
</tr>
<tr>
<td>Display value re-sampling duration</td>
<td>Sample interval to use for the metric field display value on the list view of the table.</td>
</tr>
</tbody>
</table>

Adds a float field with the name specified in the Metric field name field to the target table.

Store time series data

Use JavaScript, REST, or scriptable REST APIs to add time series data to a metric field.

It is recommended that you use the REST APIs to store time series data.

For information on the MetricBase REST APIs see the REST API Explorer on an instance with the MetricBase application installed, or see the Clotho Time Series API.

For information on the MetricBase JavaScript APIs, see Client, ClothoTransform, Data, DataBuilder, and DataSelector.

In practice, for performance reasons, batch multiple series of multiple data points and store them at one time, do not insert each data point individually.

Store time series data using REST APIs

curl -v "https://<your_instance.servicenow.com>/api/now/v1/clotho/put" --request POST
--header "Accept:application/json" --header "Content-Type:application/json"
--data 
{"seriesRef":{"subject":"6d499254c70232007a89aba35a976359","table":"cmdb_ci_knode"}}
Store time series data using JavaScript APIs

```javascript
// get the subject GlideRecord with which we are going to put metric data
var gr = new GlideRecord('cmdb_ci_computer');
gr.get(<sys id of record containing metric to be stored>);

// build time series data for cpu_percentage metric. time is GlideDateTime
var dataBuilder = new sn_clotho.DataBuilder(gr, 'cpu_percentage').add(time, 0.75);

// use clotho client to insert data
new sn_clotho.Client().put(dataBuilder);
```

Analyze time series data

Analyze time series data with the JavaScript APIs

This example is to get the average CPU percentage over the specified time for each XYZ computer.

```javascript
// Query the cmdb_ci_computer table for the records for
var gr = new GlideRecord('cmdb_ci_computer');
gr.addEncodedQuery('manufacturer=xyz');
gr.query();

// Create a DataSelector object and specify the metric (cpu_percentage),
// the transform (avg), and label (avg cpu)
var transform = new sn_clotho.DataSelector(gr).addMetric('cpu_percentage').avg()
    .label('avg-cpu-percentage');

// Run the transform between startTime and endTime.
// startTime and endTime are GlideDateTime
var data = new sn_clotho.Client().transform(transform, startTime, endTime);
var values = data['avg-cpu-percentage'].getValues();
```
View time series data

You can view time series data for a metric. A metric is defined for all records in a table, and you can view the time series data for all records.

Role required: admin

1. Navigate to the table containing the metric.
   In the Filter Navigator, type `<table name>.list`, and hit enter.
2. Click on the menu icon above the metric column, and select Time Series Chart.
3. Change the Time Span and Transform fields to evaluate the data.

   When you select the Add, Multiply, or Divide transforms, the Value field and Submit button are shown. Enter a value and click Submit to view the adjusted data. The adjusted data is not saved to the MetricBase database.

View MetricBase status

You can view the status of the MetricBase database.

Role required: admin

1. Navigate to MetricBase > MetriBase Status.
   A list of MetricBase statistics is shown.
2. Set up the list to show the information you want to check.
   a) Click the Update Personalized List icon.
   b) Use the slush bucket to move the desired metric to the display, and click OK.
3. Click on the metric value to view the time series data for that statistic.

Debug MetricBase

You can use session debug tools to debug issues.

Role required: admin

1. Navigate to System Diagnostics > Session Debug > Debug MetricBase.
   This starts session debug tracking for MetricBase activities.
2. Navigate to MetricBase > MetricBase Status, and scroll to the bottom of the list.
   Debug information is listed below the list.

MID Server

The ServiceNow® MID Server application facilitates communication and movement of data between the platform and external applications, data sources, and services.

Explore
- MID Server release notes
- Upgrade to Jakarta
- Introducing the MID Server

Set up
- MID Server installation
- Create the MID Server user and grant the role
- Configure a default MID Server for each application

Administer
- MID Server parameters
- MID Server properties
- MID Server cluster configuration
- Privileged commands for the MID Server
Introducing the MID Server

The Management, Instrumentation, and Discovery (MID) Server is a Java application that runs as a Windows service or UNIX daemon on a server in your local network.

The MID Server facilitates communication and the movement of data between a ServiceNow instance and external applications, data sources, and services.

This video gives you an overview of the MID Server:

Applications that use MID Servers

<table>
<thead>
<tr>
<th>ServiceNow applications</th>
<th>Other applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery</td>
<td>Import Sets</td>
</tr>
<tr>
<td>Orchestration</td>
<td>Alltirs</td>
</tr>
<tr>
<td>Service Mapping</td>
<td>Microsoft SMS/SCCM</td>
</tr>
<tr>
<td>Service Analytics</td>
<td>LANDesk Maintenance Suite</td>
</tr>
<tr>
<td>Event Management</td>
<td>HP OpenView Operations</td>
</tr>
<tr>
<td>Cloud Management</td>
<td>Microsoft System Center Operations Manager (SCOM)</td>
</tr>
<tr>
<td></td>
<td>Borland Starteam Integration</td>
</tr>
<tr>
<td></td>
<td>Microsoft MIIS</td>
</tr>
<tr>
<td></td>
<td>Service Assurance</td>
</tr>
</tbody>
</table>

Communicating with the MID Server

The MID Server initiates all communications with the ServiceNow® instance. The instance never initiates communications with the MID Server. This communication is recorded as records in the ECC queue, which is essentially the communication log between the instance and the MID Server. See The MID Server ECC queue for more information.

MID Server selection

An application can select a MID Server in these ways.
• **Auto-selection**: The application can automatically find an appropriate MID Server that meets the necessary selection criteria. The criteria is different for each application.

• **Default selection**: The application defaults to a single MID Server that you can specify for each application.

• **Manual selection**: The application selects a single MID Server that you specify. Not every application allows for manual selection.

See [MID Server selection](#) for details.

### Asynchronous Message Bus

The MID Server opens a persistent connection to the instance through the Asynchronous Message Bus (AMB) Client and listens on the `/mid/server/<mid_sys_id>` AMB channel. When an output record is inserted into the Queue (ecc_queue) table, an AMB message is sent to the MID Server's channel. The MID Server receives this message and immediately polls the ecc_queue table for work.

The MID Server polls the ECC queue on the regular interval defined in the `mid.poll.time` configuration parameter, regardless of AMB message activity. The default polling interval is set to 40 seconds, but can be reconfigured. This polling of the ECC queue at a regular interval is done in case the AMB connection is dropped.
**Note:** The AMB client on the MID Server does not work in all environments and might need to be disabled to avoid performance issues. To disable AMB in your environment, set the `mid.disable_amb` parameter to `true`. When you disable AMB, the MID Server reverts to a default polling interval of 5 seconds, unless the `mid.poll.time` parameter is set to a different value.
System clones and the MID server

See KB0547597 for information on what to do with MID Servers when you are cloning your instance.

MID Server heartbeat

The Now Platform checks the MID Server for a response every 5 minutes, using a synthetic transaction monitoring system.

Checking for a heartbeat

ServiceNow instances send a synthetic transaction via the Heartbeat probe to every MID Server every 5 minutes. The Heartbeat probe functions exactly as a normal probe does and is sent by writing an output record to the ECC queue. A MID Server retrieves the record when it queries the ECC queue for work. The MID Server processes the probe just as it would any other probe and responds back to the instance. If the instance does not detect a response from a MID Server, the instance marks that MID Server as Down. If the MID Server responds, the instance considers the MID Server to not be Down and is communicating properly with the instance.

Note: Make sure that your MID Server can communicate on port 443. See MID Server connection prerequisites and MID Server system requirements for more information.

System events

When a MID Server transitions from one state to another, one of these events is triggered:

- mid_server.up: The MID Server goes from a status of Down, Paused, or Upgrading to a status of Up.
- mid_server.down: The MID Server goes from a status of Up to a status of Down.
- mid_server.paused: The MID Server is paused.
- mid_server.upgrading: The MID Server is being automatically upgraded because the instance is being upgraded.

You can use these events to send notifications or trigger actions that you specify in scripts.

Scheduled job

To change the trigger interval for the Heartbeat probe, navigate to System Scheduler > Scheduled Jobs > Scheduled Jobs. Open the MID Server Monitor record and edit the interval.
### MID Server heartbeat trigger interval

### MID Server system requirements

Use these minimum system requirements to allocate resources for computers hosting MID Servers.
**MID Server supported systems**

The following systems support the MID Server.

  
  **Note**: .NET Framework version 3.5, 4.0, or 4.5 is required for Service Mapping support and for Windows pattern-based discovery.

- **Linux**: The MID Server was tested on Linux Red Hat 6, Ubuntu 12, and CentOS 6. Linux MID Servers support virtual machines and 64-bit systems. On 64-bit Linux systems, you must install the 32-bit [GNU C library](https://en.wikipedia.org/wiki/GNU_C_library) (glibc). The installation command for CentOS is:

  ```bash
  yum install glibc.i686
  ```

**Java version support**

The MID Server installs with JRE version 1.8. If you upgrade with a MID Server using JRE 1.6, the system automatically upgrades that MID Server to use version 1.8. Both the 32 bit and 64 bit MID Servers use JRE 1.8.

**Setting the JVM Memory size**

The MID Server installs with 1 GB of JVM memory. If the suggested memory size for your product is greater than 1 GB, see [Set the MID Server JVM memory size](#) for the procedure to override the default setting.

**Standard deployments**

System requirements for your instance are determined by the needs of the individual products you use that require a MID Server. The following products are considered "standard" because their MID Servers share the same minimum disk space and memory requirements:

- Discovery
- Event Management
- Integrations
- Orchestration
- Service Mapping

The minimum standard requirements pertain to both a single product and a combined product deployment. You can deploy a single MID Server for multiple standard products without significantly increasing the disk or memory requirements.

**High resource deployments**

Content Management Platform (CMP), Service Analytics and Operational Metrics are processing intensive and require more resources for each MID Server than the standard products. Install MID Servers for these products on dedicated hosts that do not support MID Servers for other products.
Recommended MID Server minimum requirements

All configurations listed here require a quad core processor with a speed of 2 GHz or greater and were calculated for a Windows Server 2012 R2 host.

**Note:** The MID Server minimum system requirements for 25 concurrent threads includes resource overhead that is independent of the number of threads. As a result, the system requirements for 200 threads do not require a linear increase in resources.

<table>
<thead>
<tr>
<th>Product</th>
<th>Disk space (GB)</th>
<th>Memory (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OS</td>
<td>MID Server +</td>
</tr>
<tr>
<td>Service Analytics</td>
<td>36 GB</td>
<td>10 GB</td>
</tr>
<tr>
<td>Content Management Platform</td>
<td>36 GB</td>
<td>4 GB</td>
</tr>
<tr>
<td>Operational metrics</td>
<td>36 GB</td>
<td>16 GB</td>
</tr>
<tr>
<td>Standard</td>
<td>36 GB</td>
<td>4 GB</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Product</th>
<th>Disk space (GB)</th>
<th>Memory (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OS</td>
<td>MID Server +</td>
</tr>
<tr>
<td>Service Analytics</td>
<td>36 GB</td>
<td>10 GB</td>
</tr>
<tr>
<td>Content Management Platform</td>
<td>36 GB</td>
<td>4 GB</td>
</tr>
<tr>
<td>Operational metrics</td>
<td>36 GB</td>
<td>16 GB</td>
</tr>
<tr>
<td>Standard</td>
<td>36 GB</td>
<td>4 GB</td>
</tr>
</tbody>
</table>

**Use case 1: Single MID Server deployed for multiple standard products**

In this example, Service Mapping, Discovery, and Orchestration share a MID Server with 25 threads that is installed on a dedicated host. The disk space and memory requirements specified here satisfy the minimum recommended requirements for the combined product deployment.
One MID Server for multiple standard products

<table>
<thead>
<tr>
<th>Product</th>
<th>Disk space (GB)</th>
<th>Memory (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OS</td>
<td>MID Server + product</td>
</tr>
<tr>
<td>Service Mapping + Discovery + Orchestration</td>
<td>36 GB</td>
<td>4 GB</td>
</tr>
</tbody>
</table>

Use case 2: Multiple MID Servers deployed to a single host

In this example, three MID Servers for standard products are deployed to a single host, where each MID Server has 25 threads. The required resources are calculated as follows:

- **Total disk space required**: Add the recommended disk space for the operating system from the OS column to the sum of the values in the MID Server + product column for all products mapped.
- **Total memory required**: Add the recommended memory for the operating system from the OS memory column to the sum of the values in the JVM memory column for all products mapped.

Calculating resources for multiple MID Servers on a single host

<table>
<thead>
<tr>
<th>Product</th>
<th>Disk space (GB)</th>
<th>Memory (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OS</td>
<td>MID Server + product</td>
</tr>
<tr>
<td>MID Server 1</td>
<td>36 GB</td>
<td>4 GB</td>
</tr>
<tr>
<td>MID Server 2</td>
<td></td>
<td>4 GB</td>
</tr>
<tr>
<td>MID Server 3</td>
<td></td>
<td>4 GB</td>
</tr>
<tr>
<td>Recommended</td>
<td>36 GB</td>
<td>12 GB</td>
</tr>
</tbody>
</table>

Monitoring performance

To ensure that the MID Server resource allocations are sufficient for your environment, monitor performance during peak periods of product execution from the MID Server dashboard.

MID Server version compatibility

The version of the MID Server must be compatible with the version of the instance. Otherwise, the MID Server cannot process commands or communicate with the instance.

The instance determines which version of the MID Server is allowed. The MID Server version must at minimum belong to the same major release, such as Helsinki. If the MID Server version belongs to the same major release, it can, but does not have to, belong to the same minor version, such as Helsinki Patch 1. In this case, communication with the instance might still be possible, but it is always suggested that you upgrade to the latest version.
Caution: You can pin the MID Server to a specific version using the `mid.version.override` property, but you should be aware that the version might become out of date.

For more information on upgrades, see MID Server upgrade.

Version indicators

If the version is not compatible, the MID Server status is not changed to **Down** in the MID Server dashboard. So it might still appear to be processing commands when it actually is not doing so. You must check the MID Server Version on the dashboard, which is available starting with the Istanbul release.

The icons in the Version column indicates the following:

- **Red**: Incompatible. The MID Server and instance do not belong to the same release. You must upgrade the MID Server and verify that it is not pinned to an older version with the `mid.version.override` property. The MID Server will not be upgraded until the parameter is cleared.
- **Yellow**: Compatible, but an upgrade is recommended. This indicates that the MID Server version belongs to the same family as the instance, but not the same version.
- **Green**: Compatible. No upgrade necessary.
- **Gray**: Incompatible. The instance cannot detect the version.

See KB0535181 for additional MID Server troubleshooting information.

MID Server connection prerequisites

You must install a MID Server on a local network resource and configure it to communicate with the machines it probes.

Network privileges

The local network resource must have these network privileges:

- **Firewall access**: Configure any firewalls between the MID Server and the target devices to allow a connection. If your network uses a DMZ, and if your network security protocols limit port access from within the network to the DMZ, you might have to deploy a MID Server to a machine within the DMZ to probe the devices there.
- **Network access**: Configure target devices to allow the MID Server probe to connect. If network security prevents you from configuring new machines that can connect to the targets, install the MID Server on an existing machine with connection privileges.
- **Network account**: Install the MID Server with the proper account, either local or domain administrator.

Additionally, for the MID Server to access your ServiceNow instance, satisfy these prerequisites:

- **Network access to the ServiceNow instance**: Configure the network that the MID Server uses to allow traffic over TCP port 443.
- **A MID user**: Create a ServiceNow user record for the MID Server to use. This user record must have the mid_server and import_admin roles.

**Note**: Verify that the baseline public page InstanceInfo is active for the MID Server to connect to the instance.
Security considerations

Sometimes computers or devices have additional security measures configured, and these measures may interfere with the MID Server’s ability to run commands or queries on those systems. For example, a Linux server might be configured to allow only certain IP address to connect to it via SSH. Similarly, a network router might be configured to allow only certain IP address to query SNMP on it. To allow access in such cases, use one of the following methods:

- Update the configuration of those computers or devices to allow the desired MID Server to run commands or query them. For example, a network router may be configured to only allow the network management systems to query SNMP on it. In that case, add the MID Server as though it were another network management system.
- Install a MID Server on a computer that already has access to the computers or network devices with such restrictions. For example, to use Discovery within a DMZ (where communication from outside the DMZ will be severely restricted), install a MID Server on a computer that is already in the DMZ.

External connectivity requirements

These requirements are specifically for the use of MID Servers with the ServiceNow Discovery and Orchestration products.

The MID Server communicates securely on port 443 to the instance and requires no inbound connections. In some cases, it might be necessary to allow this communication through the firewall if the MID Server fails to register on the instance. To determine if the application or a network security restriction is to blame for connection failure, attempt to telnet to the instance on port 443 from the server that is hosting the MID Server application. If this connection fails, then the problem could be a web proxy (since 443 is a https connection) or a Firewall rule preventing external TCP connections from that host. Contact network security personnel for the proxy information to add to the config.xml file, or request that the firewall be configured to allow access using one of the following syntax:

- `<source IP> to <any>`
- `<source IP> to <ServiceNow> any established`
- `<source IP> to <instance_name.service-now.com> 443`

Important: Ensure that the MID Server can connect to install.service-now.com to download and install updates.

Internal connectivity requirements

These methods are used for discovering various devices on a network and are specifically for the use of MID Servers with the ServiceNow Discovery and Orchestration products.

- **SSH**: For UNIX-like machines, Discovery and Orchestration use **SSH protocol, version 2** to access target machines. SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices. SSH communicates on port 22 within an encrypted datastream and requires a login to access the targets using two available methods of authentication: a user name and password combination and a user name and shared private key. Specify SSH authentication information and type in the **Credentials** module. If multiple credentials are entered, the platform tries one after the other until a successful connection is established or all are ultimately denied. To provide for application relationships a limited number of SUDO commands must be available to be run. Additional details to these
requirements can be found in UNIX/Linux commands requiring root privileges for Discovery and Orchestration.

- **WMI**: For Windows machines, Discovery uses the Windows Management Instrumentation (WMI) interface to query devices. Due to security restrictions for WMI, the MID Server application executing the WMI queries must run as a domain user with local (target) administrator privileges. When Discovery detects activity on port 135, it launches a WMI query. The response from the Windows device is sent over a Distributed Component Object Model (DCOM) port configured for WMI on Windows machines. This can be any port. Ensure that the MID Server application host machine has access to the targets on all ports due to the unique nature of the WMI requirements.

- **Windows PowerShell**: PowerShell is built on the Windows .NET Framework and is designed to control and automate the administration of Windows machines and applications. Orchestration uses PowerShell to run Workflow activities on Windows machines. PowerShell must be installed on any MID Server that executes these activities. MID Servers using PowerShell must be installed on a supported Windows operating system. ServiceNow supports PowerShell 2.0 and 3.0. Orchestration activities for PowerShell require a credentials Type of Windows.

- **SNMP - Network**: For network devices, Discovery uses an SNMP scan to get device specific MIBs and OIDs. SNMP is a common protocol used on most routers, switches, printers, load balancers and various other network enabled devices. Use a community string (password) for authentication when scanning a device via SNMP. Many devices have a default community string of public, until a successful query returns. In addition to the credentials, the platform also requires the ability to make SNMP requests on port 161 from the MID Server to the target. If Access Control Lists (ACLs) are in place to control the IP addresses that can make these queries, ensure that the IP address of the MID Server is in the ACL. ServiceNow Discovery supports SNMP versions 1, 2c, and 3.

- **WBEM**: Web-Based Enterprise Management (WBEM) defines a particular implementation of the Common Information Model (CIM), including protocols for discovering and accessing each CIM implementation. WBEM requires either of two ports, 5989 or 5988 and uses the HTTP transport protocol. WBEM supports SSL encryption and uses CIM user name/password credentials. ServiceNow Discovery launches a WBEM port probe to detect activity on the target ports and to append gathered data to a classification probe that explores CIM Servers.

### MID Server installation

The installation of the MID Server requires you to satisfy certain connection prerequisites and create a MID Server user before you download and install the MID Server service on a host machine.

You can perform the installation prerequisites and install the MID Server manually or use the MID Server Guided Setup utility, which streamlines the entire process and allows you to set up a basic MID Server quickly.

The manual process requires these setup tasks, performed in the order shown here:

1. **Configure communication between the MID Server and the instance on the appropriate port and enable required web services.** See Configure MID Server connection prerequisites for details.
2. **Create the MID Server user** and grant that user the mid_server role.
3. **Download the installer file** for the host machine.
4. **Install the MID Server** on a Linux or Windows host.
5. **Test the MID Server** connection to the instance.
6. Validate the MID Server to ensure that it is trusted to access credentials used by the instance for automations.

7. Configure MID Server parameters, which control several aspects of MID Server functionality, including proxy servers, debugging, and upgrade.

**Use MID Server guided setup**

MID Server guided setup provides a sequence of tasks that help you install a MID Server with the proper user account, select SNMP credentials for that MID Server, and assign IP addresses automatically.

Role required: admin

You are guided through configuration activities that create, download, and validate a MID Server. A progress indicator on each screen allows you to monitor your progress for each task.

Each configuration activity provides the following resources to help you:

- Contextual embedded help.
- Links to comprehensive documentation on the ServiceNow product documentation site.

**Important:** You must complete MID Server configuration before you can launch any other IT Operations Management guided setup.

1. Navigate to Guided Setup > ITOM Guided Setup.

The IT Operations Management Guided Setup welcome screen appears.
2. Click **Get Started**.
The IT Operations Management Guided Setup category screen appears, with controls for starting the MID Server tasks.

3. In the MID Server pane, click **Get Started**.
The MID Server task list appears with a description of each task.
MID Server

The MID Server runs as a Windows service or a UNIX daemon to facilitate communication and the movement of data between a ServiceNow instance and external applications, data sources, and services. Complete the activities in this category to create a user for the MID Server, download the installation package, and validate the MID Server after installation.

Create MID User
Not started yet
Create the user account that the MID Server needs to authenticate on the ServiceNow instance.

Download & Install MID
Unlock by completing Create MID User
Select and download the appropriate MID Server installer archive for the operating system.

Validate MID
Unlock by completing Download & Install MID
You must validate the network connection between the MID server and your instance before the MID server is permitted to access automation credentials or execute any outbound ECC probes.
4. Click **Configure** to create the MID Server user and follow the instructions in the help pane that appears on the right edge of the screen.

5. When you have provided the requested information for the MID Server user, click **Submit**, and then click **Mark as Complete** at the bottom of the help pane.

The view returns to the task list. Notice that the circular progress indicator for the category shows 20% of the MID Server configuration complete. The progress indicator on the left edge of the screen shows the completion percentage for all the IT Operations Management tasks. In the case of the MID Server, the completed task represents 3% of the MID Server setup's contribution to the whole.
6. Click **Configure** for the next task, **Download & Install MID**, and continue with the MID Server setup.

7. After you create and validate your MID Servers, configure any SNMP credentials you need and select the MID Servers to use for IP range auto-assignment.

When all the required MID Server tasks are completed, you can begin the guided setup tasks for the applications that require a MID Server.
Configure MID Server connection prerequisites

You must perform several prerequisite tasks to allow the MID Server to connect to the instance.

Role required: admin

1. Configure the network to allow MID Server network connectivity to the ServiceNow instance over TCP port 443.
2. Configure basic authentication for SOAP communications with the ServiceNow instance.
3. Navigate to System Web Services > Scripted Web Services > Scripted SOAP Services.
4. Confirm that the following web services are active:
   - GetMIDInfo
   - InstanceInfo
   - MIDAssignedPackages
   - MIDFieldForFileProvider
   - MIDFileSyncSnapshot
   - MIDServerCheck
   - MIDServerFileProvider

5. Type sys_public.list in the navigation search field and press Enter. The Public Pages record list appears.
6. Verify that the InstanceInfo public page is active, to allow the MID Server to validate its version.
7. Make sure that the MID Server computer can access install.service-now.com.

Create the MID Server user and grant the role

Create the MID Server user ID and grant this user the role it needs to communicate with the instance. Additionally, the real-time system validation of MID Server role assignments prevents incompatible settings.

Role required: admin

The MID Server connects to an instance by using the SOAP web service. To allow authentication with the instance, create a separate user account for each MID Server or share the same account across multiple MID Servers. Grant each MID Server user the mid_server role, which is required for the MID Server user on any instance on which basic authentication is enabled. The mid_server role allows the MID Server to access protected tables when strict SOAP security is in place. The system adds the necessary SOAP roles automatically with this role.

Note: The strict SOAP security feature, enabled by default for any instance that uses basic authentication, protects all tables with Access Control Lists (ACL).

1. From the instance, navigate to User Administration > Users.
2. Click New.
3. Complete the fields in the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>The same user ID that will be specified in the mid.instance.username parameter of config.xml. If you use special characters, such as an ampersand (&amp;), you must encode the special character using character references in the config.xml file.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>First name</td>
<td>The user's first name.</td>
</tr>
<tr>
<td>Last name</td>
<td>The user's last name.</td>
</tr>
<tr>
<td>Password</td>
<td>The same password that will be specified in the <code>mid.instance.password</code> parameter of <code>config.xml</code>. If you use special characters, such as an ampersand (&amp;), you must encode the special character using character references in the <code>config.xml</code> file.</td>
</tr>
</tbody>
</table>

4. To configure your MID Server to use special characters in the user name or password, such as `passw&rd`:
   a) Open the `config.xml` file and find these lines:
      `<parameter name="mid.instance.username" value="mid_user"/>
      <parameter encrypt="false" name="mid.instance.password" value="passw&rd"/>
   b) Make the following change:
      `<parameter encrypt="false" name="mid.instance.password" value="passw&amp;rd"/>
   c) Save the file.

   **Note:** For examples of the character references required for well-formed XML, see [Character Entity References](#).

5. Right-click the header and select **Save**.
6. Under the **Roles** related list, click **Edit**.
7. Select the **mid_server** role for this user.
   Each MID Server account must have this role to access protected tables.
   
   **Important:** The mid_server and security_admin roles are incompatible and cannot be assigned to the same user. For information on how the instance checks role assignments, see [MID Server role validation](#).

8. Click **Save**.
9. To see if the **Logged in user** is the same as the user in the configuration file, look in the MID Server dashboard or view the list view of MID Servers.
   
   The icon in the **Logged in user** column indicates the following:
   - **Red:** Incompatible. The user does not have the mid_server role or the user does not match the value in the `mid.instance.username` parameter (in the `config.xml` configuration file). Reconfigure the MID Server user and verify that it has the proper user and role.
   - **Green:** Compatible. The user has the mid_server role and matches the user in the configuration file.

10. Confirm that the MID Server account was created successfully and the account has connectivity to the instance.
    a) On the MID Server host, Open a supported web browser on the MID Server host and navigate to the instance.
    b) If the account is already logged into the instance, log out.
    c) Right-click the header and select **Save**.
d) Use the previously created MID Server user credentials and sign in. If the user name or password includes special characters, make sure that you edit the config.xml file to allow for well-formed XML.

**MID Server role validation**

Real-time system validation of MID Server role assignments prevents incompatible settings. To prevent MID Server validation failure and ensure that your MID Server is configured correctly, the system runs several business rules that monitor the roles and settings you select for your MID Server user. The instance displays a warning and blocks the change when you attempt to save an incompatible configuration.

**Elevated privileges not permitted**

The mid_server role cannot be configured for elevated privileges. The *Invalid MID Server settings* business rule runs on the Role (sys_user_role) table and prevents the *elevated_privileges* field from being set to true for the mid_server role.

![Warning for elevated privileges on the mid_server role](image-url)
Relationship table protection

The User Role (sys_user_has_role) table creates the relationship between the (sys_user) and the (sys_user_role) tables.

- **Incompatible role**
  The mid_server and security_admin roles are incompatible and cannot be assigned to the same user. The system determines the user's current role and runs the Security Admin incompatible with MID business rule on the User Role (sys_user_has_role) table. This rule prevents an administrator from adding the security_admin role for a user who currently has the mid_server role.

Warnings for incompatible security_admin role assignment

- **Incompatible user role and user record settings**
  The Incompatible MID Server user role business rule runs on the User Role (sys_user_has_role) table to protect its data from incompatible configurations. Validation for this related table ensures that an administrator cannot assign the mid_server role to a user who:
  
  - Already holds the security_admin role.
  - Has the web_service_access_only field set to true.
  - Has the internal_integration_user field set to true.
<table>
<thead>
<tr>
<th>User ID</th>
<th>tyree.courregue</th>
<th>Email</th>
<th><a href="mailto:tyree.courregue@example.com">tyree.courregue@example.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>First name</td>
<td>Tyree</td>
<td>Language</td>
<td>-- None --</td>
</tr>
<tr>
<td>Last name</td>
<td>Courregue</td>
<td>Calendar integration</td>
<td>Outlook</td>
</tr>
<tr>
<td>Title</td>
<td></td>
<td>Time zone</td>
<td>System [US/Pacific-New]</td>
</tr>
<tr>
<td>Department</td>
<td>Hit</td>
<td>Date format</td>
<td>System [yyyy-MM-dd]</td>
</tr>
<tr>
<td>Password</td>
<td></td>
<td>Business phone</td>
<td></td>
</tr>
<tr>
<td>Photo</td>
<td>Click to add...</td>
<td>Mobile phone</td>
<td></td>
</tr>
</tbody>
</table>

- A user with the 'Web Service Access' option set to true cannot be granted the mid_server role.
- A user cannot be granted both the mid_server and security_admin roles.
- "MD Server" role assignment rejected.
Incompatible user record settings

Certain settings in the user record are not permitted with the mid_server role. The **User settings incompatible with MID** business rule runs on the User (sys_user) table to monitor the settings of the **web_service_access_only** and **internal_integration_user** check boxes. If the user has the mid_server role, this rule prevents either of these fields from being set to true.

![User record settings](image)

**Incompatible MID Server settings**

**Note:** If you upgrade from a previous release with incompatible MID Server roles and settings, the system displays the appropriate warning messages when any change is made to the tables monitored by these business rules. If the change is unrelated to any role and settings validation, the system permits the updates and simply warns you of the existing incompatibilities. If the changes violate any compatibility rules in the Jakarta release, the business rules enforce the restrictions appropriately.

Download the MID Server files

The MID Server application is downloadable from the ServiceNow service instance.

The IP address of the MID Server download site (install.service-now.com) can change without notice. To ensure that you can download the MID Server installation package and receive automatic MID Server upgrades, allow local network access to these IP addresses:

149.96.5.98 and 149.96.6.98

You download the MID Server and then enable Discovery, Orchestration, or any integration that requires the use of the MID Server.

1. On the ServiceNow instance, navigate to **Mid Server > Downloads** on your instance.
2. Select and download the MID Server for the appropriate operating system.
   - If the download does not begin immediately, try again later when the system is not as busy.
MID Server downloads

3. Save the download file to a temporary file on the local drive.
4. Move the file into the designated MID Server folder you create for your operating system and run the installer from that location.
   - Linux
   - Windows

Install a MID Server on Linux

This MID Server installer automates the installation of a MID Server on a Linux computer.
Role required: admin, mid_server

**Important:** Verify that the computer meets the [MID Server system requirements](#).

You can install a MID Server on a 32-bit or 64-bit Linux computer. Click this link to view the installation video:

1. From the Linux command line, type `mkdir -p /servicenow/mid server name` to create the installation directory. You need to have read/write/execute permissions on this folder.
2. Extract the downloaded MID Server archive file, `mid.os.zip` into the `servicenow/mid server name/` directory. Use the MID Server name created in the instance or create a new name that you will use for this MID Server moving forward.
   The resulting directory structure is `/servicenow/<mid server name>/agent`.
3. Change to the `servicenow/mid server name /agent` directory, and enter the following command to start the MID Server installer: `./installer.sh`.
   If you prefer to manually configure the MID Server instead, skip to **this step**.
4. Use the installer to enter the following information.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServiceNow instance URL</td>
<td>Enter the full URL of your instance, for example:</td>
</tr>
<tr>
<td></td>
<td><a href="https://mycompanyinstance.service-now.com">https://mycompanyinstance.service-now.com</a></td>
</tr>
<tr>
<td>ServiceNow MID Server username</td>
<td>Enter the user name of the MID Server user that you already created.</td>
</tr>
<tr>
<td></td>
<td>The MID Server user must have the mid_server role.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ServiceNow MID Server password</td>
<td>Enter the password for the user in the ServiceNow MID Server username.</td>
</tr>
<tr>
<td>Use proxy</td>
<td>Select this check box if your MID Server communicates through a proxy to connect to the instance.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Your proxy server must use Basic Authentication for the MID server to connect to the instance.</td>
</tr>
<tr>
<td>Proxy host</td>
<td>Enter the proxy server host name or IP address. Do not include the protocol in the host name. For example, enter proxyserver.domain.com, not <a href="https://proxyserver.domain.com">https://proxyserver.domain.com</a>.</td>
</tr>
<tr>
<td>Proxy port</td>
<td>Enter the port through which the proxy server communicates. If you leave this field blank, it should use the proxy server's default port number.</td>
</tr>
<tr>
<td>Proxy username</td>
<td>Enter the user name that has administrator rights to the proxy server.</td>
</tr>
<tr>
<td>Proxy password</td>
<td>Enter the password for the user name.</td>
</tr>
</tbody>
</table>

5. Click **Test your connection** to validate the credentials and instance information. If you encounter any errors, verify the information that you input.

6. Click **Next**.

7. Configure the MID name parameters (see table).
### Configure MID name parameters

**Field** | **Description**
--- | ---
MID Server name | Enter any MID Server name.
MID Service wrapper name | Modify this field if necessary. It is populated automatically by prefixing `snc_mid_` to the MID Server name. In most cases, you do not need to modify this.
MID Server wrapper display name | Modify this field if necessary. It is populated automatically by prefixing `ServiceNow MID Server_` to the MID Server name. In most cases, you do not need to modify this.

8. Click **Next** to view the summary.
9. Click **Start MID Server**.
The local host starts the MID Server.

10. Click **Mid Servers List Page**.
The installer opens the MID Server list from your instance.

11. Select the MID Server name from the list.

   **Note:** It may take a few seconds for the MID Server time to establish a connection with your instance.

The system displays the MID Server record.

12. From **Related Links**, click **Validate**.
The MID Server **Validated** changes to **Yes**.
13. To configure the MID Server manually, change to the servicenow/mid server name /\nagent directory, and then edit the config.xml file as follows:
   a) Find the element `<parameter name="url" value="https://YOUR_INSTANCE.service-
   now.com" />` and change the value to the URL of your instance.
   b) Enter the MID user credentials in the mid.instance.username and
      mid.instance.password parameters.
      By default, the MID Server, uses basic authentication for SOAP messages. The password
      value is also encrypted authentication.
   c) Find the `<parameter name="name" value="YOUR_MIDSERVER_NAME_GOES_HERE" />` element and change the value for the MID Server name.
   d) Optional: Enter connection information for the proxy server. Remove the appropriate
      comment tags from the proxy configuration information.
      For example, you can configure these parameters:
      - mid.proxy.use_proxy
      - mid.proxy.host
      - mid.proxy.port
      - mid.proxy.username
      - mid.proxy.password

14. If you configured the MID Server manually, finalize the configuration as follows:
   a) Execute the shell script `start.sh`.
      The system starts the new MID Server.
   b) Log into the instance.
   c) Navigate to MID Servers > Servers.
      The system displays a list of MID Server records.
   d) Select the record matching your new MID Server and verify that the Status is listed as Up.

15. To configure the MID Server to restart automatically when the host is restarted, run
    `${base_install_dir}/agent/bin/mid.sh install` as root.
    This command installs the MID Server as a daemon service and adds the auto start scripts to
    the init.d directory.

    **Note:** You cannot install more than one MID Server service as a daemon on a Linux
    host. This is a limitation of the Tanuki wrapper service.

Configure **MID Server parameters**, which control several aspects of MID Server functionality,
including proxy servers, debugging, and upgrade.

**Install a MID Server on Windows**

This MID Server installer automates the installation of a MID Server on a Windows computer.

Role required: admin or mid_server

You can install one or more MID Servers on a supported Windows computer. Click this link to view
the installation video:

1. Log in to the Windows host machine where you want to install the MID Server.
2. Create a folder for the MID Server on the top level of the drive such as `ServiceNow\MID
   Server1`.
3. Download the MID archive file into the new folder.
4. Right-click the archive and select **Extract All**.

5. Navigate to the `service-now\<mid server name>\agent` folder that was created when the file was extracted.

6. Run `installer.bat` to start the MID Server installer.

   To configure the MID Server manually, skip to **this step**.

7. Use the installer to enter the following information.

   ![ServiceNow MID Server Installer Configuration](image)

   - **ServiceNow instance URL**: `https://{inst.name}.service-now.com`
   - **ServiceNow MID Server username**: `midserver`
   - **ServiceNow MID Server password**: `**********`
   - **Proxy host**: `proxyserver.domain.com`
   - **Proxy port**: `3238`
   - **Proxy username**: `proxyuser`
   - **Proxy password**: `**********`

   - **Use proxy**

   - **Test your connection**

   - **View Installer Logs**
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServiceNow instance URL</td>
<td>Enter the full URL of your instance, for example:</td>
</tr>
<tr>
<td></td>
<td><a href="https://mycompanyinstance.service-now.com">https://mycompanyinstance.service-now.com</a></td>
</tr>
<tr>
<td>ServiceNow MID Server username</td>
<td>Enter the user name of the MID Server user that you already created. The MID Server user must have the mid_server role.</td>
</tr>
<tr>
<td>ServiceNow MID Server password</td>
<td>Enter the password for the user in the ServiceNow MID Server username.</td>
</tr>
<tr>
<td>Use proxy</td>
<td>Select this check box if your MID Server communicates through a proxy to connect to the instance.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Your proxy server must use Basic Authentication for the MID server to connect to the instance.</td>
</tr>
<tr>
<td>Proxy host</td>
<td>Enter the proxy server host name or IP address. Do not include the protocol in the host name. For example, enter proxyserver.domain.com, not</td>
</tr>
<tr>
<td>Proxy port</td>
<td>Enter the port through which the proxy server communicates. If you leave this field blank, it should use the proxy server's default port number.</td>
</tr>
<tr>
<td>Proxy username</td>
<td>Enter the user name that has administrator rights to the proxy server.</td>
</tr>
<tr>
<td>Proxy password</td>
<td>Enter the password for the user name.</td>
</tr>
</tbody>
</table>

8. Click **Test your connection** to validate the credentials and instance information. If you encounter any errors, verify the information that you input.

9. Click **Next**.

10. Configure the MID name parameters (see table).
Configure MID name parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MID Server name</td>
<td>Enter any MID Server name.</td>
</tr>
<tr>
<td>MID Service wrapper name</td>
<td>Modify this field if necessary. It is populated automatically by prefixing snc_mid_ to the MID Server name. In most cases, you do not need to modify this.</td>
</tr>
<tr>
<td>MID Server wrapper display name</td>
<td>Modify this field if necessary. It is populated automatically by prefixing ServiceNow MID Server_ to the MID Server name. In most cases, you do not need to modify this.</td>
</tr>
</tbody>
</table>

11. Click **Next** to view the summary.
12. Click **Start MID Server.**
   The local host starts the MID Server.

13. Click **Mid Servers List Page.**
   The installer opens the MID Server list from your instance.

14. Select the MID Server name from the list.

   **Note:** It may take a few seconds for the MID Server time to establish a connection with your instance.

   The system displays the MID Server record.

15. From **Related Links**, click **Validate.**
   The MID Server **Validated** changes to **Yes.**
16. To configure the MID Server manually, edit the config.xml file with a text editor such as WordPad:
   a) Find the element `<parameter name="url" value="https://YOUR_INSTANCE.service-now.com" />` element and change the value to the URL of your instance.
   b) Enter the MID user credentials in the `mid.instance.username` and `mid.instance.password` parameters.
   By default, the MID Server, uses basic authentication for SOAP messages. The password value is also encrypted authentication.
   c) Optional: Find the `<parameter name="name" value="YOUR_MIDSERVER_NAME_GOES_HERE" />` element and change the value for the MID Server name.
   d) Optional: Enter connection information for the proxy server. Remove the appropriate comment tags from the proxy configuration information.
   For example, you can configure these parameters:
   - `mid.proxy.use_proxy`
   - `mid.proxy.host`
   - `mid.proxy.port`
   - `mid.proxy.username`
   - `mid.proxy.password`

17. If you configured the MID Server manually, finalize the configuration as follows:
   a) Execute the batch file `start.bat`.
      The system starts the new MID Server.
   b) Log into the instance.
   c) Navigate to MID Servers > Servers.
      The system displays a list of MID Server records.
   d) Select the record matching your new MID Server and verify that the Status is listed as Up.

Configure MID Server parameters, which control several aspects of MID Server functionality, including proxy servers, debugging, and upgrade.

Manually install a MID Server as a Windows Service

If you did not start the MID server at the end of the installation procedure, you can manually install the MID Server to run as a Windows service.

Role required: admin

You can install a MID Server as a Windows service in these operating systems:
- Windows Server 2008
- Windows Server 2012
- Windows Server 2016

1. Open the agent directory in the directory you created for the MID Server installation files. For example, the path might be `C:\ServiceNow\MID Server1\agent`.
2. Right-click the `start.bat` file and select Properties.
3. Select the option to Run as administrator.
4. Double-click the `start.bat` file to install the Windows service.
**Test MID Server connectivity**

Confirm network connectivity to the MID Server for automatic upgrades, and then ensure that the MID Server can communicate with the instance.

Role required: admin

The system that hosts the MID Server must be able to access one of these URLs to automatically upgrade:

- HTTPS: https://install.service-now.com on the default HTTPS port (443)
- HTTP: http://install.service-now.com on the default HTTPS port (80)

1. Use PING to test connectivity with the host on the network (ping<host IP>).
2. If no ping response is returned, use TRACEROUTE to see where traffic might be stopped (traceroute<host>).
3. Use TELNET to connect to any of the TCP ports (telnet<host> <port>).
4. Use an SNMP scanning tool to determine if a potential network device is responsive.
5. Resolve the most likely issues around network connectivity:
   - Routing: Confirm that the MID Server host has network access to the IP ranges you are attempting to discover.
   - Firewalls: Confirm access to the physical firewalls that protect a large environment such as the Data Center. Confirm access to any logical firewalls that protect an individual computer. MID Server communications are initiated inside the firewall and therefore do not require any special firewall rules or VPNs.
   - Access Control Lists (ACL): Confirm that ACLs contain the IP addresses based list on SNMP network devices that allows communication to a particular target.
   - Resolve all issues with your network teams to better understand your topology. Deploy additional MID Servers if necessary to help keep your network secure. Configure access from your existing MID Server host to networking components.

6. Verify that the MID Server service is running on the host:
   - Windows: In the Windows Services console, locate the **ServiceNow (MID Server name)** and confirm that each MID Server has the **Started Status** value.
   - Linux: Ensure that the **agent0.log.0.lck** appears in the `/servicenow/ MID Server name]/agent` folder.

7. After each MID Server restart, open the **agent0.log.0** and address all error messages.
8. From the ServiceNow instance, navigate to **MID Server > Servers**.
9. Review and verify that all MID Servers that are connected to the instance are listed.
10. Verify that the **Status** is **Up** for the MID Servers.

**Validate the MID Server**

You must manually validate the MID Server after it is installed to enable it to execute automation tasks. You can invalidate a MID Server you suspect has been compromised to prevent it from accessing automation credentials in the instance or executing outbound ECC probes.

Role required: **agent_admin**, **admin**

Make sure that the **MID Server version** is compatible with the instance.

Validation restricts access to automation credentials to trusted MID servers only.

Starting in the Istanbul release, you can specify that the MID should be used for all capabilities, applications, and IP ranges when you validate a MID Server. You will be prompted to set the
initial selection criteria when you validate MID Servers that do not already have capabilities, applications, or IP ranges already configured. You do not have to set the initial selection criteria to actually validate the MID Server. See MID Server selection for more information on capabilities, applications, and IP ranges.

**Note:** When you upgrade to Geneva and later releases, MID Servers that are already configured in your instance are automatically validated. This prevents the interruption of automation tasks that MID Servers might be performing. See MID Server upgrade for more information.

1. Install the MID Server using the instructions in MID Server installation. This creates a record in the MID Server (ecc_agent) table.
2. Navigate to MID Server > Servers.
3. Open the new MID Server from the list of MID Servers.
4. Under Related Links click Validate.
   The Set Initial Selection Criteria window appears if there are no records in the Supported Applications, IP Ranges, or Capabilities related lists.
5. On the Set Initial Selection Criteria window, use the switches to enable or disable selection criteria for this MID Server:
   - **Allow ALL capabilities:** Allow all capabilities for Orchestration and Event Management use this MID Server.
     **Note:** Service Mapping and Service Analytics, which used capabilities in previous releases, rely on the application for MID Server selection starting with the Istanbul release.
   - **Allow ALL applications:** Allow all applications that use MID Servers use this MID Server.
   - **Allow ALL IP ranges:** Make all IP ranges valid for this MID Server, meaning that it can target any IP address.

6. Click OK.
   The Validated field on the dashboard is set to Validating, and then set to Yes after the validation completes.
7. To invalidate a MID Server, open the record for the MID Server you suspect has a security issue.
8. Under Related Links, click Invalidate.

Invalidating a MID Server forces it to clear its memory and restart. The MID Server generates a new keypair on restart.

**Multiple MID Server deployments**

Depending upon how you use the MID Server (for an external integration, Discovery, Service Mapping or Orchestration) and the load placed on it, you might find it necessary to deploy multiple MID Servers in your network.

Factors determining the number of MID Servers your network will require to support external applications that integrate with ServiceNow include the following:

- The security constraints in your network.
- Your network policies.
- The amount of traffic between ServiceNow and the integrations.
- The reliability of the MID Server machines.

**Network policies and security**

Security policies in your network (firewalls between network segments, for example) might make direct communication impossible between your instance and an integration’s data source (JDBC, LDAP, etc.). To retrieve data for the instance, you can install a MID Server that has access to both the data source and the instance.

These network policies can determine if you need to install multiple MID Servers in your environment:

- **Access control lists (ACL):** If your security policy controls access to network devices (e.g. switches and routers) with an ACL, it might be necessary to install one or more MID Servers on a machine in the network that is already on the ACL.
- **DMZ:** Your network policy might require you to install one or more MID Servers in your DMZ to probe the devices there. This is common in networks that tightly regulate the ports that are opened on the inside firewall.
- **Probe types:** If you are conducting probes of different operating systems, your network policy might require a separate MID Server for each type of probe (e.g., one MID server for Windows WMI probes and another for SSH probes on UNIX).

**Load balancing**

Deploy multiple MID Servers where capacity is an issue, as when Discovery has to gather information about thousands of configuration items quickly. In a high volume environment, it might be necessary to deploy multiple MID Servers as load balancers for certain transactions. For example, JDBC data transfers can tie up the resources of a MID Server, making it unable to respond to other requests. The following operations between an integration might require separate MID Servers in a busy network:

- File exports
- Running scripts
- JDBC data sources
- Reading files
High availability model

Avoid installing MID Servers for critical integrations on a machine that might experience any type of planned outage or an outage caused by overloaded processes. If necessary for reliability, consider deploying these types of MID Servers to dedicated machines for high reliability.

Note: Do not integrate with an external application on a MID Server provisioned for ServiceNow Discovery or Orchestration.

Wide area network (WAN)

When determining where to deploy MID Servers in a WAN, consider the bandwidth available between your local area networks. In most cases, install a MID Server on each LAN to probe devices locally, rather than deploying MID Servers that must probe devices across slow WAN connections. An alternative to this type of deployment is to install MID Servers that probe other LANs via VPN connections that take advantage of fast Internet connections. If the bandwidth of your WAN connections is comparable to that of your Internet connection, then there is no performance impact in running MID Server probes across WAN connections.

Domain separation

In deployments where domain separation is enabled and domains are configured to form a hierarchy, place the MID Servers at the lowest domain level.
Deploying MID Servers with domain separation

Install multiple MID Servers on a single system

You can install multiple MID Servers on the same host computer.

Role required: admin, mid_server

You can install multiple MID Servers on a single host or on a virtual machine using either Linux or Windows. Installing multiple MID Servers may involve other setup steps depending on your network configuration.

1. Log in to the host system or virtual machine where you want to install multiple MID Servers.
2. Create a directory for each MID Server on the top level of the drive.

   Make sure you create a unique and descriptive name for each MID Server, such as MIDSserver_SMS_Int or MIDSserver_Disc1.
3. Extract the downloaded MID Server archive file into each MID Server directory.
When the extract completes, there should be a directory path that resembles the following for each MID Server. For example, ServiceNow<MID Server name>\agent.

4. For each MID Server, run the installer appropriate to the host's operating system.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Installer path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>/agent/installer.bat</td>
</tr>
<tr>
<td>Linux</td>
<td>/agent/installer.sh</td>
</tr>
</tbody>
</table>

5. Use the installer to enter the following information.
   - URL to your instance
   - User credentials to run the MID Server
   - Proxy server connection details
   - MID server name
   - MID server service wrapper name and display name (Windows systems only)

   **Note:** The MID Server user must have the mid_server role.

6. From the installer, click **Start MID Server**.
The local host starts the MID Server.

7. Click **Mid Servers List Page**.
   The installer opens the MID Server list from your instance.

8. Select the MID Server name from the list.

   **Note:** It may take a few seconds for the MID Server time to establish a connection with your instance.

   The system displays the MID Server record.

9. From **Related Links**, click **Validate**.
   The MID Server **Validated** changes to **Yes**.
Uninstall a MID Server

The MID Server runs as a stand-alone service. You can remove a stand-alone MID Server service to accommodate such tasks as redeploying the MID Server to another host machine or changing the unique name of a MID Server when deploying multiple MID Servers.

Role required: admin

1. Do one of the following to stop the running MID Server service.
   - Windows command line: From the MID Server home directory, for example from the agent folder, type `stop.bat`.
   - Windows Services console: From the Windows Services console, right-click the ServiceNow MID Server name and then select `stop`.
   - Linux: From the MID Server home directory, for example the agent folder, type `stop.sh`.

2. From a command prompt, go to the `\agent\bin` directory in the MID Server installation directory.

3. Do one of the following:
   - Windows: Double-click the `UninstallMID-NT.bat` file.
   - Linux: Confirm that the MID Server is stopped by executing the `bin/mid.sh status` shell script. After the MID Server stops, delete the files in the agent directory.

4. On Windows machines, check in the Windows Services console for a service named ServiceNow WMI Collector. If it is running, open a command prompt, navigate to `agent\bin\sw_wmi\tools`, double-click `uninstall_wmi.bat`.

Configure Windows MID Server service credentials

MID Server service credentials are required so the MID Server can communicate with devices on your network.

By default, the MID Server service runs as a Local System account. This account only grants access to the machine on which the MID Server is running, not to other systems on the network. Therefore, you must change the service credentials to one of the following types:

- A Domain User account. This account should have local admin rights to allow automatic MID Server upgrade.
- A specific user account that has local admin access to the MID Server machine as well as access to other systems on the network.

**Note:** Service credentials are not the same as the MID Server user credentials: the service credentials allow communication between the MID Server and your network, while the MID Server user credentials allow communication between the MID Server and the instance. You must configure both of these credentials separately. See Create the MID Server user and grant the role for instructions on MID Server user credentials.

1. Open the Windows Services console.
2. Double-click the ServiceNow <MID Server name> service for each MID Server.
3. Select the Log On tab.
4. Set Log on as privileges with the Domain User or another user account that has local admin access to the MID Server machine as well as access to other systems on the network. Whatever account you choose, verify that it has local admin access and access to other systems on the network. For local admin access, you can use Windows Explorer to grant write permissions to the MID Server agent folder.
5. In the General tab, set **Startup type** to **Automatic**.
6. Click **OK**.
7. Restart the ServiceNow <MID Server name> service, and make sure that ServiceNow\<MID Server name>\agent\logs\agent0.log does not have error messages. If the MID Server does not start, see the ServiceNow knowledge article Review the agent log for MID Server errors (article KB0535148).
8. On the instance this MID Server is connected to, navigate to **MID Server > Servers**. If Discovery is installed, navigate to **Discovery > MID Servers**.
   All MID Servers connected to this instance are listed.
9. Make sure that the Status of the MID Server you just installed is **Up**.

**Post installation MID Server administration**

You can manually start, stop, restart, and monitor the MID Server after it is installed.

The status of each MID Server activity appears in the **MID Servers** page. Additional log information appears in the following places:

- The MID Server log is available on the instance.
- The corresponding *agent0.log.0* and wrapper logs (*wrapper.log*) are available in the MID Server agent\logs folder.

**Start the MID Server**

Manually start the MID Server to initiate communication with the instance.

Role required: admin

You can manually start the MID Server.

1. Do one of the following:
   - Windows command line: From the MID Server home directory, for example the agent folder, type `start.bat`.
   - Windows Services console: From the Windows Services console, right-click the **ServiceNow MID Server name** and then select **Start**.
   - Linux: From the MID Server home directory, for example the agent folder, type `start.sh`.

2. Monitor the MID Server to ensure that it is operating properly.

**Stop the MID Server**

Stop the MID Server to terminate communication with the instance.

Role required: admin

Consider **pausing the MID Server** instead. Pausing the MID Server from the instance still allows you to run certain commands on the MID server.

1. Do one of the following:
   - Windows command line: From the MID Server home directory, for example the agent folder, type `stop.bat`.
   - Windows Services console: From the Windows Services console, right-click the **ServiceNow MID Server name** and then select **stop**.
   - Linux: From the MID Server home directory, for example the agent folder, type `stop.sh`.
2. **Restart the MID Server** when ready.

### Restart the MID Server

You can restart the MID Server if it has been stopped.

**Role required:** admin

You can manually restart the MID Server.

1. Do one of the following:
   - **MID Server instance:** Navigate to the MID Servers and click a Name. Under Related Links, click Restart MID.
   - **Windows command line:** From the MID Server home directory, for example the agent folder, type `Restart.bat`.
   - **Windows Services console:** From the Windows Services console, right-click the ServiceNow MID Server name and then select Start.
   - **Linux:** From the MID Server home directory, for example the agent folder, run the `restart-service.sh` script using one of these commands:
     - `./restart-service.sh`
     - `sh restart-service.sh`
     - `bash restart-service.sh`

2. Monitor the MID Server to ensure that it is operating properly.

### Monitor the MID Server

Monitoring MID Servers involves verifying entries in log files, confirming network connectivity, and checking MID server status.

**Role required:** agent_admin or admin

You can monitor MID Servers hosted by Windows or Linux MID servers.

1. **For Windows only**, navigate to the Windows Services console, locate the service name that matches the name that appears from the wrapper-override.conf file. If the MID Server process is the only Java process running on the host, monitor the memory used by `java.exe` and alert on less than the maximum configured memory defined in the `~\agent\conf\wrapper-override.conf` folder.

2. Ensure that the `agent0.log.0.lck` file appears in the `~\agent\logs` folder to confirm that the MID Server running and logging system activity in the `agent0.log.0` file.

3. Review the following logs for warning, critical, and severe errors:
   - `~\agent\logs\agent0.log.0`
   - `~\agent\logs\wrapper.txt`

   See [Access MID Server log entries from the ECC queue](#) to see how to open log entries from the instance.

4. **Confirm network connectivity.**

5. From the MID Server instance, navigate to the MID Servers page, and review the status of the MID Server. For additional information, click a Name.

6. Use Windows or Linux tools to monitor:
   - CPU
Set up email, SMS, and push notifications to alert you when issues occur with MID servers. The **MID Server Down** notification is enabled by default. See [Notifications](#) for details.

**MID Server upgrade**

MID Servers are automatically upgraded, but you can also manually upgrade each MID Server separately.

**Upgrade methods**

- **Automatic**: Allow the instance to automatically upgrade the MID Server. This functionality is available by default. Automatic upgrade occurs:
  - Every hour, when the MID Server checks with the instance to see if there is a different version available for upgrade. You cannot modify this time period.
  - When the instance is upgraded and the MID Server for that version is different than the version currently on the MID Server.
  - When the MID Server **pre-upgrade test** passes without an error. Any errors encountered during this automatic test prevent the upgrade from occurring until the issues are resolved. The pre-upgrade test is enabled by default, but can be disabled by adding and setting a system property.

- **Manual**: Manually start the upgrade by clicking a related link on the MID Server record. Use this method when you do not want to wait until the next hourly automatic update or if your upgrade failed and you want to force an upgrade. See [Upgrade the MID Server manually](#) for instructions.

**Upgrade version**

You can configure a property that specifies a different upgrade version if you do not want to use the default MID Server version that is determined by the instance. See [Set the MID Server version](#) for more information.

**The Upgrade state**

The instance initiates the upgrade by sending the **autoUpgrade** system command to the MID Server. Starting with MID Servers upgrading **from** an Istanbul version MID Server, the MID Server **Status** is changed to **Upgrading** while the upgrade is running. The **Upgrading** state is similar to the **Paused** state. This is done to avoid potential miscommunication between the new version of the instance and the previous version of the MID Server during upgrade. For the upgrade to run, MID servers must be in the **Up** state and must be **validated**.

While in the **Upgrading** state, you cannot resume or restart the MID Server. However, you can perform the same actions that you can when the MID Server is in the **Paused** state. After a
successful upgrade, the queued output is sent to the instance and the MID Server starts retrieving new commands to process. The status also changes to **Up**.

When the instance sends the `autoUpgrade` system command to the MID Server, if it is **Down** or **Paused**, or if it has not been validated, the command remains in the ECC Queue until the MID Server status changes to **Up**. Then the command is processed.

**Note:** If you are using an Istanbul instance but you are upgrading a pre-Istanbul MID Server to Istanbul, these upgrade states are not available. They are available only for MID Servers that are already on Istanbul.

### Failed upgrades

Failed upgrades are handled differently based on the version you are upgrading to:

- **Upgrade to another major release:** (such as Istanbul to the next full release): the status changes to **Upgrade Failed**.
- **Upgrade from a minor version within a release:** (such as Helsinki patch 1 to patch 2): the MID Server continues using the version it is currently running. It does not perform the upgrade and the status eventually changes to **Up**, assuming the MID Server was already functioning properly.

### Upgrading MID Servers in the Down state

If a MID Server is in the **Down** state, it cannot process the upgrade command. When the MID Server changes to **Up**, it immediately checks to see if an upgrade is necessary. If it does need to upgrade, the upgrade process starts before the MID Server processes any other commands.

### Upgrade error messages

The MID Server can display the following upgrade error messages.

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unable to refresh packages</td>
<td>The MID Server displays this message as a generic error when the error is not handled by a defined error message.</td>
</tr>
<tr>
<td>Failed to query instance for MID Server buildstamp</td>
<td>Instance is unavailable or there is a major version mismatch between the MID Server and the instance.</td>
</tr>
<tr>
<td>Not a valid package buildstamp</td>
<td>InstanceInfo returned an assigned buildstamp that was not in the correct format, such as a version mismatch.</td>
</tr>
</tbody>
</table>

### MID Server pre-upgrade check

The instance automatically tests the MID Server’s ability to upgrade on your system prior to the actual upgrade, to identify issues that could cause a MID Server outage or require reinstallation.

Each MID Server contains an AutoUpgrade monitor that compares the MID Server version with that of the instance to determine if the MID Server needs to upgrade. If the AutoUpgrade monitor
discovers that the MID Server version is out of date, the monitor runs pre-upgrade validation tests for that MID Server. If an issue is detected, a message is logged to the MID Server Issue (ecc-agent_issue) table, and the upgrade is blocked. The AutoUpgrade monitor continues to run every hour, until the tests all pass. If there are no blocking issues, the MID Server downloads the appropriate upgrade package and begins the upgrade process.

Failed tests leave the MID Server in one of these states:

- **Upgrade Failed**: For upgrades to a different release family, such as from Geneva to Jakarta.
- **Up**: For upgrades within the same release family, such as an upgrade to a patch.

Errors, such as insufficient disk space for the installer and lack of connectivity to install.service-now.com, are written to both the MID Server agent log and to the MID Server Issue (ecc-agent_issue) table. These errors are published before the actual MID Server upgrade occurs and must be resolved before the upgrade can continue. You can view issues from the MID Server Issue (ecc-agent_issue) table in any of these locations:

- MID Server Issues related list in a MID Server record.
- MID Server > Server Issues navigation module.
- MID Server Issues gauge on the MID Server dashboard.

### Pre-upgrade tests

The pre-upgrade validation tests check these requirements:

- At least 1GB of free disk space.
- Access to the download site at install.service-now.com.
- Permission to execute these file operations:
  - Extract a ZIP archive to a temp folder.
  - Copy files from the temp folder to the agent folder.
  - Read a text file.
  - Delete the pre-upgrade contents.
  - For Windows, ensure that the Log On As user for the Windows service is either LocalSystem or a user that is part of the local Administrator group. By default, domain administrators are added to the local Administrator group when joining a computer to a domain. If the PowerShell script that performs this test does not return the expected output, the system logs a warning to the MID Server Issue (ecc-agent_issue) table, but the test passes.

### Data provided

When the instance encounters issues during the pre-upgrade check, it populates these fields in the MID Server Issue (ecc-agent_issue) table:

#### MID Server issue fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last detected</td>
<td>Date and time the issue was last detected.</td>
</tr>
<tr>
<td>Short description</td>
<td>Contents of the generated message that specifies a possible issue with available disk space, download server access, or file permissions.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MID Server</td>
<td>Name of the MID Server affected by a pre-upgrade test failure.</td>
</tr>
<tr>
<td>Issue source</td>
<td>The process that identified the issue. For all issues with MID Server pre-upgrade testing, the source is UpgradeCheck.</td>
</tr>
<tr>
<td>State</td>
<td>The current state of the issue. Possible states are:</td>
</tr>
<tr>
<td></td>
<td>· New: Starting state when the instance creates the issue.</td>
</tr>
<tr>
<td></td>
<td>· Acknowledged: State set by the administrator when he or she first examines the issue.</td>
</tr>
<tr>
<td></td>
<td>· Resolved: Ending state, set by the instance, indicating that the issue has been resolved. If the scheduled job does not encounter the issue when it runs again, the instance automatically sets the state to this value.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain for the MID Server. For all issues derived from MID Server pre-upgrade testing, the domain value is inherited from the domain of the MID Server user.</td>
</tr>
<tr>
<td>Count</td>
<td>Number of times an issue has been detected. Each time the pre-upgrade tests run and encounter the same issue, the AutoUpgrade monitor increments this field.</td>
</tr>
</tbody>
</table>

**Errors that block the upgrade**

These messages describe issues detected by the pre-upgrade test and published to the MID Server Issue (ecc_agent_issue) table. Failure of any of these tests blocks the upgrade.

- **Not enough free disk space. The system reports <n> bytes free:** This message is displayed when less than 1GB of free disk space is detected on the MID Server host. This error is also written to the MID Server agent log.
- **Unable to download updates from install server:** This message indicates that either the MID Server host does not have permission to download the installation package from install.service-now.com or network problems prevent connection. This error is also written to the MID Server agent log.
- **Unable to extract contents of pre upgrade check zip:** This message indicates that the service account on the MID Server host does not have permission to extract the pre-upgrade ZIP archive to the temporary folder specified by the system property, java.io.tmpdir. On a UNIX host, the value for this property is typically /tmp or /var/tmp. On Microsoft Windows hosts, the path is c:\WINNT\TEMP.
- **Unable to create folder <upgrade check file path>:** This message indicates that the MID Server service account does not have permission to create the upgradeCheck folder for the pre-upgrade checking files in the agent/package path.
- **Unable to verify file permissions: <message>:** This message indicates an exception has occurred when checking file permissions, such as a file that does not exist or access failure.
- **MID Server Windows Service is not running as LocalSystem or a local Administrator:** This message warns that the Windows service is not running with the desired permissions.
Non-blocking warnings

These warnings are displayed in the MID Server Issue (ecc_agent_issue) table and do not prevent a Windows MID Server from upgrading:

- **WARN: Unable to parse $logOnAsUser**: This message warns that the Log On As User value for the Windows service is not in either of these expected formats:
  - `user@domain.company.com`
  - `domain\user`
- **WARN: Unable to look up Log On As user's groups**: When the instance attempts to look up the logged on user's group memberships, it executes the `net user <username>` command. The instance expects a certain output structure by the Windows service from this command and issues this warning if the expected output does not match the actual output.

These PowerShell warnings are written to the MID Server agent log only. Because PowerShell is not required to use a MID Server, these configuration issues do not prevent a Windows MID Server from upgrading. However, these warnings might indicate issues in your environment that require attention.

- **Skipping PowerShell upgrade checks since PowerShell is not usable**: PowerShell 2.0 (at a minimum) is not installed or `powershell.exe` is not available to the MID Server service user.
- **Continuing with upgrade, but the following issue was encountered during upgradeCheck**: `<exception message>`. This message indicates that there was an issue running the PowerShell portion of the pre-upgrade tests.

Disabling the pre-upgrade check

A MID Server configuration parameter called `mid.upgrade.run_precheck` is set to `true` by default, which allows the automatic pre-upgrade test to run. To disable these tests for a single MID Server, add this parameter to that MID Server's `config.xml` file and set it to `false`. To disable these tests for all MID Servers, add a new record to the MID Server Property (ecc_agent_property) table called `mid.upgrade.run_precheck`. Set the value of this property to `false` and leave the MID Server field blank.

Set the MID Server version

You can specify which version the MID server should upgrade to using a property.

Role required: admin

ServiceNow does not recommend pinning the MID Server to a specific version for a significant amount of time, especially if you upgrade the instance. Under most circumstances, you should let the instance determine which MID Server version to use.

These properties control the MID Server version:

- **mid.buildstamp**
  The `mid.buildstamp` property identifies the MID Server version with an identifier based on the date of the build. This property uses a date and time format of `yyyy-mm-dd-hhmm`.

  The MID Server checks for version information hourly. If no override version is configured, the MID Server looks at the `mid.buildstamp` property for the version to use. This property resets itself to the default version (the version that matches your instance version) when the instance is restarted or upgraded, so any user changes are lost at that time.

- **mid.version.override**
Use this property to set an override condition for the current MID Server version. When the MID Server checks the version each hour, it looks at the mid.version.override property first. If this property is empty, the MID Server will get its version information from the mid.buildstamp property. If an override version is configured, the MID Server uses this value and ignores the version information in the mid.buildstamp property. This override value remains when the instance is restarted and is passed to the MID Server. However, the version in the mid.version.override property is deleted during an upgrade, allowing the MID Server to reset itself to the version in the mid.buildstamp property.

The MID Server cannot be upgraded until the parameter is cleared.

---

**Note:** Downgrades are only possible within the same major release, such as Helsinki or Istanbul.

1. In the **Navigation** pane filter, type *sys_properties.list*.
   The list of system properties appears.
2. Click **New**.
3. Type `mid.version.override` in the Name field.
4. Enter a description, such as, **Set an override value for the current MID Server version**.
5. Enter a version for the MID Server to use that is different from the version ServiceNow has selected in the mid.buildstamp property. The date and time format is `yyyy-mm-dd-hhmm`.
6. Click **Submit**.

**Upgrade the MID Server manually**

You can manually upgrade MID Servers at any time if you do not want to wait for the automatic upgrade.

Role required: mid_server or admin

For the upgrade to run, MID servers must be in the **Up** state and must be **validated**.

The MID Server is upgraded to the version specified by build stamp on the instance, or by the **upgrade property** that you specify.

1. Navigate to **Discovery > MID Servers or Orchestration > MID Server Configuration > MID Servers**.
2. Open the record of the MID Server that you want to upgrade.
3. Click **Upgrade MID** under **Related Links**.
4. Confirm that you want to perform the upgrade.

**MID Server configuration**

Administrators must configure a MID Server to ensure that it has access to sufficient system resources, probes the proper data sources, and communicates with the instance as expected.

You must complete all the steps in **MID Server Installation** before attempting any of the configuration steps explained here.

Restart a MID Server after any configuration change for the changes to take effect.
Note: All new MID Servers must be validated before use. Validation ensures that the MID Server is trusted to access credentials used by the instance for automations. For instructions, see Validate and invalidate the MID Server.

MID Server Records that cannot be altered

These records cannot be modified or deleted.

<table>
<thead>
<tr>
<th>Table</th>
<th>Record</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Page (sys_public)</td>
<td>InstanceInfo</td>
</tr>
</tbody>
</table>
| Scripted Web Service (sys_web_service) | • InstanceInfo  
|                                | • GetMIDInfo                     |
|                                | • MIDAssignedPackages             |
|                                | • MIDFieldForFileProvider         |
|                                | • MIDFileSyncSnapshot             |
|                                | • MIDServerCheck                  |
|                                | • MIDServerFileProvider           |

Using special characters in an XML file

The XML specification defines five predefined entities that represent special characters, and requires that all XML processors honor them. If these characters are used in a password, you will experience unexpected results.

The following characters represent the five pre-defined entities:

- "
- \\&
- '
- <
- >

If you use the pre-defined entity characters in an XML file, such as the MID Server configuration file, you need to encode them. To encode pre-defined entities into an XML document:

- replace " with &quot;
- replace & with &amp;
- replace ' with &apos;
- replace < with &lt;
- replace > with &gt;

For example, to specify the password as test& in the MID Server config.xml file:

```
<parameter encrypt="true" name="mid.instance.password" value="test&amp;"/>
```

Use the MID Server dashboard

The MID Server dashboard is a central place for MID Server users to monitor ongoing operations. The dashboard consists of reports and gauges that display information from the MID Server Status table.
The MID Server Dashboard is available from the MID Server > Dashboard module.

**The MID Server status gauge**

The MID Server Status gauge on the dashboard displays basic information about each MID Server. This information comes from the MID Server Status (ecc_agent_status) table.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the MID Server.</td>
</tr>
<tr>
<td>Host name</td>
<td>The name of the system that hosts the MID Server.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the MID Server.</td>
</tr>
<tr>
<td>Validated</td>
<td>Whether or not the MID Server was validated.</td>
</tr>
<tr>
<td>Max memory used %</td>
<td>The highest percent usage of memory on the system that hosts the MID Server, in the configured sampling interval. The default interval is 30 minutes, but this value is user configurable. See MID Server resource threshold alerts for details.</td>
</tr>
<tr>
<td>Mean CPU used %</td>
<td>The average percent usage of CPU on the system that hosts the MID Server, in the configured sampling interval. The default interval is 30 minutes, but this value is user configurable. See MID Server resource threshold alerts for details.</td>
</tr>
<tr>
<td>Pending jobs</td>
<td>Number of pending ECC queue jobs for that MID Server.</td>
</tr>
<tr>
<td>Processing jobs</td>
<td>Number of processing ECC queue jobs for that MID Server.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Version | The version of the MID Server. An icon indicates the validity of the MID Server:  
- **Red**: Incompatible. The MID Server and instance do not belong to the same release. You must upgrade the MID Server and verify that it is not pinned to an older version with the `mid_version.override` property. The MID Server will not be upgraded until the parameter is cleared.  
- **Yellow**: Compatible, but an upgrade is recommended. This indicates that the MID Server version belongs to the same family as the instance, but not the same version.  
- **Green**: Compatible. No upgrade necessary.  
- **Gray**: Incompatible. The instance cannot detect the version. |
| User | The login name of the user. An icon indicates the validity of the user:  
- **Red**: Incompatible. The user does not have the `mid_server` role or the user does not match the value in the `mid.instance.username` parameter (in the `config.xml` configuration file). Reconfigure the MID Server user and verify that it has the proper user and role.  
- **Green**: Compatible. The user has the `mid_server` role and matches the user in the configuration file.  
  
  **Note**: The user can also have any of the SOAP roles that the `mid_server` role inherits. |

**MID Server status**

- **Up**: The MID Server is up and running and communicating heartbeats and status with the instance. This does not mean the MID Server is validated. See Validate the MID Server for instructions.  
- **Down**: The MID Server is not running. This means that you manually stopped the MID Server service or a network issue disrupted communication between the MID Server and the instance.  
- **Paused**: The MID Server has been paused by the `mid_server` user or the administrator.  
- **Upgrading**: The MID Server is upgrading to another version.  
- **Upgrade failed**: The upgrade was not possible. The MID Server will not accept tasks from instance until it is successfully upgraded. See MID Server troubleshooting and KB0596459.  

In the Validating field, the following can appear:  
- **Validating**: The MID Server is being validated.  
- **Validation failed**: Validation of the MID Server failed. See MID Server troubleshooting.  

© 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.
CPU and maximum memory usage

This graph shows the average percentage of CPU usage on all the systems that host MID Servers in the last 30 days.

This graph shows the average percentage of maximum memory used by all the systems that host MID Servers in the last 30 days.
MID Server selection

You can configure applications to select MID Servers in a variety of ways.
MID Server criteria

MID Servers offer these types of criteria that help an application determine which MID Server to use:

- **Application**: The application that you specify on the MID Server. You can designate these applications for a specific MID Server:
  - Discovery
  - Orchestration
  - Service Mapping
  - Service Analytics
  - Event Management
  - Cloud Management

  An **ALL** application option is also available. By default, this option includes all applications except Service Analytics, which requires an exclusive MID Server. You can **configure which applications** are included in the **ALL** designation.

- **IP address or range**: The IP address or the IP ranges that the MID Server is allowed to work within. You can specify an IP address or IP range in the application, such as on a Discovery schedule or an Orchestration activity, and for the MID Server. If the IP configured in the application matches the IP address or falls within the allowable IP range configured on the MID Server, a match is possible, and that MID Server passes this criteria. To have the instance automatically assign IP ranges (subnets) to available MID Servers, see **MID Server IP range auto-assigment**.

- **Capabilities**: The network capability an application needs to use, such as the PowerShell Orchestration activity. Some applications, like Cloud Management and alert aggregation and RCA, require a specific capability.

  **Note**: Discovery and Service Mapping can also use behaviors, which determine the type of port probes used during the port scan phase of Discovery. Both Discovery and Service Mapping use a behavior to discover **load balancers running on Linux**. Other applications do not use behaviors. Behaviors are not used for auto-selection, default MID Servers, or specific MID Servers as described below.

How an application selects a MID Server

If you do not specify a specific MID Server for an application to use, the application tries to select one. Each application relies on different criteria to select an appropriate MID Server.

<table>
<thead>
<tr>
<th>Application</th>
<th>Supported Application on the MID Server</th>
<th>IP address range</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery</td>
<td>The Discovery or ALL application must be specified on the MID Server.</td>
<td>Discovery uses IP ranges that you configure on the Discovery Schedule form to see if they fall within the IP ranges that you configure on the MID Server, or the ALL IP ranges option must be selected on the MID Server.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Note**: Any configured behaviors are ignored.
<table>
<thead>
<tr>
<th>Application</th>
<th>Supported Application on the MID Server</th>
<th>IP address range</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orchestration</td>
<td>The Orchestration or ALL application must be specified on the MID Server.</td>
<td>The target IP address that you configure in an Orchestration activity must fall within the IP ranges that you configure on the MID Server, or the ALL option must be selected on the MID Server.</td>
<td>The capability that is required for an Orchestration activity must match the capabilities you configure on the MID Server, or the MID Server capability must be set to ALL.</td>
</tr>
<tr>
<td>Service Analytics</td>
<td>The Service Analytics application must be specified on the MID Server.</td>
<td>N/A</td>
<td>One of these capabilities must be present on the MID Server: the RCA capability for Service Analytics and the ITOA metrics capability for operational metrics.</td>
</tr>
<tr>
<td>Service Mapping</td>
<td>The Service Mapping or ALL application must be specified on the MID Server.</td>
<td>The endpoint IP address must fall within the IP range that you configure on the MID Server, or the ALL option must be selected on the MID Server.</td>
<td>One of the supported Service Mapping capabilities (for new installs) must be configured on the MID Server, or the MID Server capability must be set to ALL.</td>
</tr>
<tr>
<td>Event Management</td>
<td>The Event Management or ALL application must be specified on the MID Server.</td>
<td>The IP configured in the event connector instances, such as HPOM, must fall within the IP range configured on the MID Server.</td>
<td></td>
</tr>
<tr>
<td>Cloud Management</td>
<td>N/A</td>
<td>N/A</td>
<td>The Cloud Management or ALL capability must be added.</td>
</tr>
</tbody>
</table>

**Using a specific MID Server**

Discovery and Event Management can use a MID Server that you specifically call out.

**Note:** Selecting a specific MID Server is not the same as specifying the default MID Server for an application. A specific MID Server is always used. If it is Down or not validated, the application does not execute commands against the MID Server. A default MID Server is fallback that is used when the auto-selection of MID Servers does not find any eligible MID Server.
How you specify a specific MID Server

<table>
<thead>
<tr>
<th>Application</th>
<th>How you specify a specific MID Server</th>
<th>Criteria that the default MID Server must meet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery</td>
<td>Choose the MID Server on the Discovery schedule.</td>
<td>You can use any MID Server as long as it does not have the discovery capability for Service Analytics. If you select a MID Server without the Discovery or ALL application, it automatically adds the Discovery application.</td>
</tr>
<tr>
<td>Orchestration</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Service Analytics</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Service Mapping</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Event Management</td>
<td>Choose one or more MID Servers on the connector instance event collection, such as HPOM.</td>
<td>N/A</td>
</tr>
<tr>
<td>Cloud Management</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Note: You can also specify a cluster of MID Servers.

<table>
<thead>
<tr>
<th>Criteria that the default MID Server must meet</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can use any MID Server as long as it does not have the Discovery or ALL application. If you select a MID Server without the Discovery or ALL application, it automatically adds the Discovery application.</td>
</tr>
</tbody>
</table>

Note: If a MID Server manages resources within defined IP ranges for Orchestration, you must map the fully-qualified domain name (FQDN) of a server with its IP address to run certain activities, such as Exchange activities.

Domain separation

If you are using domain separation, you can configure MID Servers to be in separate domains. The domain that the MID Server is in affects how the application selects the domain:

- **Discovery and Service Mapping**: On the Discovery schedule, the MID Servers and clusters that available for selection are limited to the same domain of the user who is configuring the schedule. This also applies to the auto-selection option: only MID Servers in the same domain as the user can be automatically selected.

- **Alert aggregation and RCA (Event Management)**: The metrics for a business service is done on the MID Server that is in the same domain as the business service. Otherwise, a MID Server from the global domain is used.

MID Server selection test

If Service Mapping is active, you can preview which MID Server that Service Mapping uses for a specific target device or computer. To do this, navigate to Service Mapping > MID Servers and click MID Selection Test. Enter the IP address and an optional application and capability, and then click OK. The name of the MID Server that Service Mapping will use appears in the window.

Configure a default MID Server for each application

You can configure a default MID Server on the application or MID Server record for all applications except Event Management.

Role required: agent_admin or admin

Applications are only available when their respective plugins are activated.

The default MID Server is used when applications fail to find a suitable MID Server that matches configured criteria during auto-select. The default MID Server for the ALL application is used if the default MID Server for the specific application is not available. Some applications also offer a property to set the default MID Server.
Important: If you configure a MID Server for **ALL IP ranges** (type **Include**) and also create an IP range of type: **Exclude** for the same MID Server, the system will ignore the excluded IP range for that MID Server.

The default MID Server does not need to meet any criteria (application, IP range, behavior, or capability) to be used. Specifying a default MID Server is optional, and you can use a MID Server as the default for more than one application.

<table>
<thead>
<tr>
<th>Application</th>
<th>Additional notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery</td>
<td>Discovery attempts to use the default MID Server when the Discovery schedule specifies <strong>Auto-Select MID Server</strong> and Discovery cannot find any MID Servers with the correct application and IP range.</td>
</tr>
</tbody>
</table>
| Orchestration       | Orchestration attempts to use the default MID Server when it cannot find any MID Servers with the capabilities that you define in the Orchestration activity.
You can also specify a default MID Server. The value in that property automatically synchronizes with the default MID Server you select in the Orchestration application. |
| Service Analytics   | Not applicable. The MID Server is selected if it has the RCA capability. Route to right MID by domain.                                               |
| Service Mapping     | Starting with the Istanbul release, fresh Istanbul installs use the default MID Server for the Service Mapping application. Upgrades to Istanbul still use the MID Server. |
| Event Management    | You can specify a default MID Server for Event Management using the `mid.server.connector_default` system property. Event Management does not use the default MID Server in the application record. |
| Cloud Management    | N/A                                                                                                                                              |

1. Configure the default MID Server for an application in the MID Server record.
   a) Navigate to **MID Server > Servers** and open a record.
   b) In the **Supported Applications** related list, click **Edit**.
   c) In the left column of the slushbucket, click the applications that can use this MID Server and move them to the right column.
   You can define which applications are included in the **ALL** option.
   d) Click **Save**.

2. Configure the default MID Server for an application in the application record.
   a) Navigate to **MID Server > Applications**.
   The list of installed applications that can use MID Servers appears.
   b) Click the name of an installed application.
   c) On the MID Server Application form, select the MID Server in the **Default MID Server** field.
   d) To select additional MID Servers for this application, click **Edit** in the **MID Servers** related list and select alternate MID Servers that this application is allowed to use.
   e) Click **Update**.
Configure an IP address range for the MID Server

Configure an IP address range for the MID Server to use.

Role required: agent_admin or admin

Applications, such as Discovery and Orchestration, can specify an IP range or a specific IP address of a target. When the application looks for a MID Server to use during auto-selection, it chooses a MID Server that has corresponding IP range that includes the application's IP range or specific IP address. Applications also use other criteria, such a the MID Server supported application and capabilities. See MID Server selection for more information.

Note: This is a manual configuration procedure. To learn how the system can assign IP address ranges to selected MID Servers automatically, see MID Server IP range auto-assigment.

These applications use IP ranges as follows:

- **Orchestration**: Use the IP address of the target machine (together with the capability) to select the correct MID Server for Orchestration activities. Refer to the procedure in this topic to configure the IP address.
- **Service Mapping**: Select the MID Server whose IP address range matches the IP in the discovery request. See MID Server configuration for Service Mapping for more information.
- **Discovery**: Can select an IP address range using the same criteria as Service Mapping. Discovery can also use a quick IP range that you specify in the Discovery schedule.

Tip: You can also use the ALL IP range, which allows the MID Server to be used with any range of IP addresses that an application specifies. This only allows the MID Server to access IP ranges, it does not mean that the MID Server can actually reach all of the IP ranges. To function with an application, the MID server must have access to the IP ranges that the application needs.

Valid IP address ranges can be as follows:

- An IP address in dotted decimal or hexadecimal format. The hexadecimal format can be explicitly prefixed with 0x, this is not mandatory. Here are examples:
  - 10.11.144.155
  - 0x0A0B909B
  - 0A0B909B

- An IP address range in dotted decimal or hexadecimal format. Here are examples:
  - 10.11.144.150-10.11.144.160
  - 0x0A0B9096-0x0A0B90A0
  - 10.11.144.150-0x0A0B90A0

- An IP network address with the net mask specified after a slash (/) in regular notation (0-32 inclusive) or in IP address notation. Dotted decimal or hexadecimal format is not allowed. Here are examples:
  - 10.11.144.0/24 10.11.144.0/255.255.255.0
  - 10.11.144.0/0xFFFFFFFF
  - 0x0A0B9000/24

© 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.
1. Navigate to **MID Server > IP Ranges**.
2. Click **New**.
3. Complete the form, using the fields in the table.

<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>Type</td>
<td>Select the type of range:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Include</strong>: Include the specified IP range.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Exclude</strong>: Exclude the IP address range.</td>
</tr>
<tr>
<td>Range</td>
<td>Enter the range in a valid format.</td>
</tr>
<tr>
<td>Related list</td>
<td>The MID Servers that can use this IP address range.</td>
</tr>
</tbody>
</table>

**Note:** If a MID Server is configured for **ALL** applications, any IP addresses configured for exclusion are ignored by the system. If your goal is to configure default MID Servers for separate applications in your system, see **Configure a default MID Server for each application**.

4. Click **Save**.
**Important:** IP ranges assigned manually prior to using the auto-assignment feature are affected as follows:

- Individual IP ranges are retained and appended to the ranges assigned automatically by the system for the designated MID Server.
- If the MID Server was configured with the All ranges selection, the auto-assignment feature overwrites that designation with the ranges it finds.

Open the ALL IP range record and configure the MID Servers that you want to use with any set of IP addresses.

**Configure applications included in ALL Applications**

You can narrow down the list of applications that are included in the definition of ALL.

Role required: agent_admin or admin

You can specify the ALL application for a MID Server, which means that the MID Server is allowed work with any of the applications that require MID Servers, such as Discovery, Event Management, Service Mapping, and so on. But you might not want all applications to be included in the definition of ALL. For example, you might want to exude Service Mapping from all the ALL definition if you already have a dedicated MID Server to work with Service Mapping.

1. Navigate to MID Server > Applications.
   The list of installed applications that can use MID Servers appear.
2. If you do not see the Included in application ALL column, you can personalize the list and add it.
3. For each application, double-click the value in the Included in application ALL column.
4. Change the value to true (to include) or false (to exclude).

**MID Server IP range auto-assigment**

IP ranges that represent a subnet can be automatically assigned to MID Servers.

To be automatically assigned to a subnet, a MID Server must be:

- In a running (Up) state.
- Successfully validated.
• Able to access one or more subnets in your network.

You can select MID Servers for auto assignment using either of these methods:

• **Guided Setup**: The ITOM Guided Setup module leads you through the process of installing and configuring a MID Server and automatically assigning that MID Server to a subnet range. When you use the Guided Setup to assign MID Servers to subnets, the instance runs Discovery to identify the available subnets and then makes the assignments for the MID Servers you select. To get started with Guided Setup, navigate to **Guided Setup > ITOM Guided Setup**.

• **Auto-Assign IP Ranges**: The **MID Server > Auto-Assign IP Ranges** module displays the MID Server auto assignment list. When you select one or more MID Servers for auto-assignment, the instance runs Discovery to identify the subnets in your network and completes the MID Server IP range assignments.

The subnet assignments that the instance makes for the MID Servers you select are stored in the Automation Status Set (automation_status_set) table.

**Required SNMP OIDs for MID Server IP range auto-assignment**

Customers who use network service providers must request specific SNMP access to use MID Server IP range auto-assignment.

IP range auto-assignment requires SNMP credentials for read-only access to all routers that Discovery uses to identify subnets. In addition, your service provider must grant the following SNMPWALK access:

- iso.org.dod.internet.mgmt.mib-2.ip.ipRouteTable (1.3.6.1.2.1.4.21)
  - ipRouteDest (1.3.6.1.2.1.4.21.1.1)
  - ipRouteNextHop (1.3.6.1.2.1.4.21.1.7)
  - ipRouteType (1.3.6.1.2.1.4.21.1.8)
  - ipRouteMask (1.3.6.1.2.1.4.21.1.11)

- iso.org.dod.internet.mgmt.mib-2.ip.ipForward.ipCidrRouteTable (1.3.6.1.2.1.4.24.4)
  - ipCidrRouteDest (1.3.6.1.2.1.4.24.4.1.1)
  - ipCidrRouteMask (1.3.6.1.2.1.4.24.4.1.2)
  - ipCidrRouteNextHop (1.3.6.1.2.1.4.24.4.1.4)
  - ipCidrRouteType (1.3.6.1.2.1.4.24.4.1.6)

**Select MID Servers for auto-assignment**

Select the MID Servers you want the instance to automatically assign to discovered subnets.

Role required: admin

You can auto-assign MID Servers in ITOM Guided Setup or use this procedure to select MID Servers for subnet assignments from the instance navigator.

1. Navigate to **MID Server > Auto-Assign IP Ranges**.
   - The MID Server range auto-assignment lists appear. Only validated, running MID Servers are available for selection.
2. Drag and drop MID Servers selected for assignment from the **Available** list to the **Selected** list, or use the arrow buttons to move them.

3. Click **OK** when you are done.
The instance runs a subnet Discovery and automatically assigns the MID Servers you have selected to the subnets that Discovery finds.

**View automation status sets and IP range assignments**

The Automation Status Set form shows summary details of a subnet Discovery and the subsequent IP range assignments for MID Servers selected for automatic subnet assignment.

Role required: admin

1. Navigate to MID Server > Automation Status Sets.
2. Select a status record for a subnet Discovery you want to view.

The form contains read-only status information about the selected Discovery, the subnets found, and the range assignment process for the MID Servers you selected for auto assignment.

---

**Important:** IP ranges assigned manually prior to using the auto-assignment feature are affected as follows:

- Individual IP ranges are retained and appended to the ranges assigned automatically by the system for the designated MID Server.
- If the MID Server was configured with the All ranges selection, the auto-assignment feature overwrites that designation with the ranges it finds.
The Automation Status Set shows the IP range assignments for the MID Servers selected for discovery.

This form includes summary details of the Discovery that identified the available subnets as

- **Number**: STA0001003
- **State**: Completed

Subnet Discovery Status  Range Assignment Status

This tab shows information for the currently running Subnet Discovery.

- **Number**: DIS0010022
- **Started**: 62
- **Completed**: 31
- **Duration**: 43 Minutes

Update  Delete

Related Links

Refresh

<table>
<thead>
<tr>
<th>MID Servers Used (1)</th>
<th>Subnet Queue (31)</th>
<th>Subnet ECC Queue</th>
<th>Subnets Discovered (1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Range Assignments (565)</td>
<td>Inaccessible IP Ranges (141)</td>
<td>IP Range Assignment Log (3)</td>
<td></td>
</tr>
</tbody>
</table>
3. Select the **Subnets Discovered** related list to view the list of subnets available for assignment.

4. Select the **IP Range Assignments** related list to view the IP ranges that were assigned to a MID Server.

---

**Caution:** IP ranges identified by Discovery are stored in the IP collection (ip_address_collection) table, which is only used for MID Server IP range auto-assignment in the Jakarta release. This table is intended for future development and **should not** be used in any customizations, including column additions, business rules, or scripting actions.
MID Server parameters

Parameters control the behavior of a particular MID Server. They have lower precedence compared to MID Server properties. Changes to parameters only take effect when the MID Server is started (or restarted).

Required parameters

**Note:** Using special characters in an XML configuration file requires you to encode them.

<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance URL</td>
<td>url</td>
<td>Specifies the URL to the associated ServiceNow instance. Normally the URL is similar to <a href="https://instance.service-now.com">https://instance.service-now.com</a>, where you replace instance with the instance name. If you host your own ServiceNow instance, use the URL set by your organization.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: string</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Default value: none</td>
</tr>
<tr>
<td>Label</td>
<td>Names</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MID Server ID</td>
<td>mid_sys_id</td>
<td>Records the MID Server record’s unique identifier. This parameter should be empty when you initially configure a MID Server. Do not change the value. Type: string. Default value: automatically set (GUID)</td>
</tr>
<tr>
<td>MID Server name</td>
<td>name</td>
<td>Use this parameter to supply a name that is meaningful for you. If you do not supply this parameter, the MID Server uses the default value. A set of business rules synchronizes the name in the configuration file with the name in the MID Server record. The business rules ensure that changing the name in one location also changes the name in the other location. Type: string. Default value: YOUR_MIDSERVER_NAME_GOES_HERE</td>
</tr>
<tr>
<td>Instance user name</td>
<td>mid.instance.username or glide.glidesoap.username</td>
<td>If the ServiceNow instance has authentication enabled, as it is by default, set this parameter to define the user name the MID Server should use to log in to the instance. This user should have the mid_server role on the ServiceNow instance in order to access necessary tables and fields. Type: string. Default value: none</td>
</tr>
<tr>
<td>Instance password</td>
<td>mid.instance.password or glide.glidesoap.password</td>
<td>If your ServiceNow instance has authentication enabled, as it is by default, set this parameter to define the password the MID Server should use to log in to the instance. Type: string. Default value: none</td>
</tr>
</tbody>
</table>
### CIM parameters

<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of messages sent at once to a CIM server.</td>
<td>mid.cim.batch.size</td>
<td>Specifies the maximum number of messages sent at once to a CIM server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Default value: 1</td>
</tr>
<tr>
<td>Interval to wait between requests to the same CIMOM (ms).</td>
<td>mid.cim.request.interval</td>
<td>Specifies the number of milliseconds to wait between requests to the same Common Information Model Object Manager (CIMOM).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: integer (milliseconds)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Default value: 0</td>
</tr>
<tr>
<td>The maximum amount of simultaneous connections allowed per CIMOM.</td>
<td>mid.cim.host.connection.limit</td>
<td>Specifies the maximum number of simultaneous connections to each Common Information Model Object Manager (CIMOM). A value of zero disables simultaneous connections.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: integer (number of connections)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Default value: 0</td>
</tr>
</tbody>
</table>

### Connection parameters

<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asynchronous Message Bus Client disable</td>
<td>mid.disable_amb</td>
<td>Disables the Asynchronous Message Bus (AMB) Client. When AMB is enabled, the MID Server uses a default polling interval of 40 seconds. When the AMB client is disabled, the default polling interval switches to 5 seconds. If you set a polling interval with the mid.poll.time parameter, the MID Server uses that value whether or not the AMB client is enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Default value: false</td>
</tr>
<tr>
<td>Label</td>
<td>Names</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Instance date format                      | instance.date.format        | Specifies the format the instance uses for dates and times. The primary impact of setting this parameter is to allow the MID Server to correctly refresh its start and stop times on the MID Server record in ServiceNow. The format of this date/time string is identical to that used by the Java SimpleDateFormat class.  
  - Type: string (Date format)  
  - Default value: yyyy-MM-dd HH:mm:ss |
| MID Server immediate response enable      | glide.mid.fast.responses    | Instructs the MID Server to try sending messages to the instance as soon as they are ready. Normally the MID Servers ends message to the ServiceNow instance serially (that is, one message at a time). Since many probes can be run in parallel, there can be multiple messages simultaneously transmitted to the instance. Setting this parameter to `true` may decrease the time between a probe's completion and its response arriving at the instance. However, the multiple simultaneous messages consume resources, decreasing the overall instance responsiveness. If there are communications problems, this parameter's value can also cause a logjam on the MID Server, as threads normally used for running probes may become consumed for sending messages. Generally, leave this parameter out of your configuration. Setting it to `true` is meaningful only under very special circumstances.  
  - Type: true | false  
  - Default value: false |
<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MID Server JMX enable</td>
<td>mid.jmx.enabled</td>
<td>Enables a JMX server on the MID Server, which exposes some management information to JMX consoles. Implementing JMX requires additional configuration of the Java runtime environment. Setting this parameter to <strong>true</strong> is only recommended for those with detailed knowledge of the Java security architecture and a specific need for JMX.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* Type: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* Default value: false</td>
</tr>
<tr>
<td>MID Server max transmission queue size</td>
<td>glide.mid.max.sender.queue.size</td>
<td>Places an upper limit on how large the queue is allowed to get. The MID Server starts deleting queued messages if this limit is exceeded. When the MID Server generates messages to the ServiceNow instance faster than it can send them, it queues them temporarily on the file system of the MID Server’s host. This queue is normally quite small, and is completely emptied as soon as the MID Server processing slows for a short period. However, this queue can grow in size when there are communication problems between the MID Server and the instance, and especially if there is an integration running on the MID Server. The parameter is of the form {number}{multiplier}, where {number} is any positive decimal number including non-integers, and the optional multiplier is any spelling of bytes, kilobytes, megabytes, gigabytes, or terabytes (only the first character is tested, and the test is case-insensitive). The default multiplier is bytes. White space is liberally tolerated. The following strings all represent valid parameters: “1000000000”, “0.5m”, “5 GB”, “7.67gigas”, “145.69392 meg”, and “1.1 terra”.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* Type: string</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* Default value: 0.5 GB</td>
</tr>
<tr>
<td>Label</td>
<td>Names</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| MID Server maximum number of probe threads                            | threads.max      | Controls the number of execution threads (simultaneous work) that probes may use. This parameter provides direct control over what CPU resources the MID Server consumes on the computer that hosts it. To decrease the MID Server’s CPU consumption, lower the number of threads. To make the MID Server work faster, increase the number of threads. See `Set MID Server Thread Use`.  
  - Type: integer (threads)  
  - Default value: 25                                                                                                                                                                                                 |
| Maximum amount of interactive messages to queue in memory for processing. | threads.interactive.max | Sets the maximum amount of interactive messages to queue in memory for processing.  
  - Type: integer (threads)  
  - Default value: 4                                                                                                                                                                                                 |
| Maximum amount of expedited messages to queue in memory for processing. | threads.expedited.max | Sets the maximum amount of expedited messages to queue in memory for processing.  
  - Type: integer (threads)  
  - Default value: 4 (threads)                                                                                                                                                                                                 |
| MID Server poll time in seconds when MID server is not busy.           | mid.poll.time    | Sets the default MID Server polling interval (in seconds). The polling interval is the amount of time the MID Server waits before checking the ECC queue for work when the ECC queue is not busy. The MID Server polls the ECC queue using this interval if the AMB client connection is dropped.  
  **Note:** The default polling interval resets to 5 seconds when the AMB client is disabled. If you configure the `mid.poll.time` parameter, the MID Server uses this polling interval whether or not the AMB client is connected.  
  - Type: integer (seconds)  
  - Default value: 40                                                                                                                                                                                                 |
## Credentials parameters

<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
</table>
| Credentials provider. | mid.credentials.provider | Specifies the Java class name of the credentials provider.  
  - Type: string  
  - Default value: com.service_now.mid.creds.standard.StandardCredentialsProvider |
| Class that the MID server uses to generate secure key pairs. | mid.secure_credentials.key_pairs.provider | Class that the MID server uses to generate secure key pairs.  
  - Type: String  
  - Default value: com.service_now.mid.keypairs.provider.standard.StandardKeyPairsProvider |

## Debug parameters

<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
</table>
| Debug logging enable. | debug.logging | (Deprecated) Specifies whether to enable logging of MID Server events and messages (both sent and received). Normally this parameter is only used by developers, but it is occasionally useful when troubleshooting a problem. Be aware that setting this parameter to true causes intensive logging on the MID Server, potentially using considerable disk space.  
  - Type: True | False  
  - Default value: false  
  This parameter has been replaced by the mid.log.level parameter. |
<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Debug mode enable.</td>
<td>debug</td>
<td>(Deprecated) Specifies whether to enable debug logging on the MID Server. Normally this parameter is only used by developers, but it is occasionally useful when troubleshooting a problem. Be aware that setting this parameter to true causes intensive logging on the MID Server, potentially using considerable disk space.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: True</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Default value: false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This parameter has been replaced by the mid.log.level parameter.</td>
</tr>
<tr>
<td>Debug file probe templates.</td>
<td>file.probe.template.debug</td>
<td>Specifies whether to debug file probe templates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: True</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Default: false</td>
</tr>
<tr>
<td>Enables debug logging for CIM / WBEM / SLP / SMI-S.</td>
<td>mid.cim.debug</td>
<td>Specifies whether to enable debug logging for CIM, WBEM, SLP, or SMI-S.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: True</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Default value: false</td>
</tr>
<tr>
<td>Label</td>
<td>Names</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable debug logging for ServiceNow SSH Client.</td>
<td>mid.ssh.debug</td>
<td>Enables SSH debug information in the log file. The parameter usage depends on whether the ServiceNow SSH client is enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>When the ServiceNow SSH client is enabled, the parameter functions as follows:</strong> <strong>Type:</strong> String  <strong>Default value:</strong> false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following string values are valid for the ServiceNow SSH client:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>true:</strong> Enables SSH debug information in the log file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>false:</strong> Disables SSH debug information in the log file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>&lt;IP Addresses&gt;:</strong> Specify which IP ranges to enable SSH debug information in the log file. You can enter IP addresses in the following formats:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>An IP range defined by a slash and the number of bits in the subnet:</strong> For example, the string 10.10.10.0/24 scans 24 bits of IP addresses from 10.10.10.0 to 10.10.10.254.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>An IP range defined by a dash:</strong> For example, the string 10.10.11.0-10.10.11.165 scans the IP addresses from 10.10.11.0 to 10.10.11.165.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>A comma-separated list of specific IP addresses:</strong> For example the string 10.10.11.200,10.10.11.235 scans the IP addresses 10.10.11.200 and 10.10.11.235.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>deferred:</strong> Logs SSH debug information in memory unless an error or warning occurs. If an error or warning occurs, the platform publishes the debug information to the log file. This ensures that only the part of the log file pertaining to the error is recorded.</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.
### MID Server logging level.

<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
</table>
| MID Server logging level. | mid.log.level | Specifies the logging level for the MID Server. Possible values are:  
  - debug  
  - info  
  - warn  
  - error  
  
  **Note:** Values are case insensitive.  
  - Type: String  
  - Default value: info |

Enables debug logging for the Idle Connection Monitor.

<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enables debug logging for the Idle Connection Monitor. | mid.http.idle_connection_monitor.debug | Enables debug logging for the Idle Connection Monitor.  
  - Type: True | False  
  - Default value: false |

### DNS parameters

<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
</table>
| DNS scanning regulator interval (ms) | mid.dns_scan.regulator.intervnal_ms | Specifies the interval between DNS scans in milliseconds.  
  - Type: Integer  
  - Default value: 10 |

<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
</table>
| DNS scanning regulator packets per interval | mid.dns_scan.regulator.packets_per_interval | Specifies the number of regulator packets per DNS scan.  
  - Type: Integer  
  - Default value: 1 |

<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
</table>
| DNS scanning default name servers | mid.dns_scan.default_name_servers | Specifies the host names or IP addresses of the default name servers.  
  - Type: String  
  - Default value: none |

<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
</table>
| DNS scanning additional name servers | mid.dns_scan.additional_name_servers | Specifies the host names or IP addresses of any additional name servers.  
  - Type: String  
  - Default value: none |
### DNS scanning load balancing enable

<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS scanning load balancing enable</td>
<td>mid.dns_scan.load_balancing_enable</td>
<td>Specifies whether to enable load balancing of name servers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: True</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Default value: false</td>
</tr>
</tbody>
</table>

### FTP connection parameters

<table>
<thead>
<tr>
<th>Label</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max size of the FTP Connection Pool</td>
<td>mid.ftp.max_pool_size</td>
<td>Specifies the maximum size of the FTP Connection Pool, in megabytes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: Integer</td>
</tr>
<tr>
<td>Max number of the FTP connections per target</td>
<td>mid.ftp.max_per_target</td>
<td>Specifies the maximum number of the FTP connections per target.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: Integer</td>
</tr>
<tr>
<td>Max amount of time that an FTP connection can sit idle in the pool</td>
<td>mid.ftp.max_conn_idle_time</td>
<td>Specifies the maximum amount of time, in milliseconds, that an FTP connection can sit idle in the pool.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: Integer</td>
</tr>
<tr>
<td>Max number of files that can be returned in the filesystem list directory command</td>
<td>mid.filesystem.max.ls</td>
<td>Specifies the maximum number of files that can be returned in the filesystem list directory command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: Integer</td>
</tr>
</tbody>
</table>

### Logging parameters

<table>
<thead>
<tr>
<th>Label</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable monitor checking</td>
<td>disable_monitors</td>
<td>Specifies whether to disable the MID Server from actively checking for monitors on the instance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: True</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Default value: false</td>
</tr>
<tr>
<td>Label</td>
<td>Names</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Query logging enable       | mid.show.queries                                 | Instructs the MID Server whether to log details about every query it makes to the ServiceNow instance. Typically this parameter is only used by developers, but it is occasionally useful when troubleshooting a problem. Be aware that setting this parameter to true causes intensive logging on the MID Server, potentially using considerable disk space.  
  - Type: True | False  
  - Default value: false |
| Remote logging disable     | disable.remote.logging                           | Prevents the MID Server from logging any information to the MID Server log on the instance. Relatively little information is logged on the instance in any case, but setting this parameter to true eliminates all logging to the instance.  
  - Type: True | False  
  - Default value: false |
| Status sending disable     | disable.status                                   | Prevents the MID Server from sending a status report to the instance every 10 minutes.  
  - Type: True | False  
  - Default value: false |

**Proxy server parameters**

<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
</table>
| Instance proxy enable       | mid.instance.use_proxy or mid.proxy.use_proxy | If your MID Server must go through a web proxy to access the ServiceNow instance, set this parameter to true to instruct the MID Server to use the proxy. You must also set the proxy server's host and port, and perhaps the user name and password as well.  
  - Type: True | False  
  - Default value: false |
### ServiceNow Jamaica Now Platform Capabilities

<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
</table>
| Instance proxy host    | mid.proxy.host    | If your MID Server must go through a web proxy to access the ServiceNow instance, set this parameter to define the proxy's host.  
  - Type: String  
  - Default value: none                                      |
| Instance proxy password| mid.proxy.password| If your MID Server must go through a web proxy to access the ServiceNow instance, and your proxy requires a password, set this parameter to define that password.  
  - Type: String  
  - Default value: none                                         |
| Instance proxy port    | mid.proxy.port    | If your MID Server must go through a web proxy to access the ServiceNow instance, set this parameter to define the proxy's port.  
  - Type: Integer (0-65535)  
  - Default value: 80                                             |
| Instance proxy user name| mid.proxy.username| If the MID Server must go through a web proxy to access the ServiceNow instance, and the proxy requires a user name, set this parameter to define that user name.  
  - Type: String  
  - Default value: none                                           |

### Shazzam parameters

<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
</table>
| Port probe packet interval | mid.shazzam.regulator.interval_ms | Sets the interval, in milliseconds, in which Shazzam can launch packets. This parameter works with the mid.shazzam.regulator.packets_per_interval parameter to set the number of packets allowed in this interval.  
  By default, Shazzam launches one packet each millisecond.  
  - Type: Integer  
  - Default value: 1                                           |
<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
</table>
| Port probe packets launched per regulator interval | mid.shazzam.regulator.packets_per_interval | Sets the number of packets that Shazzam can launch in the configured time interval. This parameter works with the mid.shazzam.regulator.interval_ms parameter, which sets that interval. By default, Shazzam launches one packet each millisecond.  
- Type: Integer  
- Default value: 1 |
| Shazzam chunk size | mid.shazzam.chunk_size | Specifies the maximum number of IP addresses that Shazzam scans in parallel. This parameter primarily controls outbound port consumption.  
- Type: Integer  
- Default value: 100 |

### SSH Discovery parameters

<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
</table>
| MID Server connection cache | mid.connection_cache | Specifies whether to cache connections. Set to false to disable connection caching. This parameter applies to SSH connections only.  
- Type: true | false  
- Default value: true |
| Decide if the PATH environment variable should be set for SSH commands | mid.ssh.set_path | Specifies whether to set the PATH environment variable for SSH commands.  
- Type: true | false  
- Default value: true |
| Process commands against localhost via SSH rather than console | mid.ssh.local | Specifies whether to execute commands for the MID Server host machine (localhost) via SSH rather than from a console. This allows long-running commands to execute properly. This parameter applies to the legacy SSH client only.  
- Type: true | false  
- Default value: false |
<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
</table>
| MID Server SSH connection per host                                    | mid.ssh_connections_per_host               | Controls the number of concurrent probes the MID Server can run against a given host. Lowering the number of concurrent connections can slow Discovery.  
  - Type: integer  
  - Default value:  
    - 7 for the ServiceNow client  
    - 3 for the legacy SSH client |
| Enable (or disable) sudo to preserve environment (-E) for SSH         | mid.ssh.sudo_preserve_environment          | Specifies whether to use `sudo` to preserve the environment for SSH.  
  - Type: true | false  
  - Default value: false |
| Set the PATH environment paths for SSH commands                       | mid.ssh.path_override                      | Overrides the default paths set before executing a command. Enter one or more override paths delimited by a colon (:). The default path is `/usr/sbin: /usr/bin: /bin: /sbin`.  
  The ServiceNow SSH client accepts the following prefixes in front of the `path_override` value.  
  - `append`: Appends the override path to the end of the host’s path. This is the default behavior.  
  - `replace`: Replaces the host path with the `path_override` value.  
  - `prepend`: Appends the override path to the front of the host path.  
  - Type: string (a colon-separated list of directories)  
  - Default value: None |
<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the ServiceNow SSH Client</td>
<td>mid.ssh.use_snc</td>
<td>Enables the ServiceNow SSH client (SNCSSH) on individual MID Servers. SNCSSH is a ServiceNow implementation of an SSH client and is active by default for all MID Servers on new instances, via a MID Server property. Enabling the ServiceNow SSH client disables the legacy J2SSH client.</td>
</tr>
<tr>
<td>Important:</td>
<td></td>
<td>Mixing SSH client types for MID Servers connected to the same instance is not a good practice.</td>
</tr>
<tr>
<td>· Type: true</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>· Default value: false</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The maximum number of times to retry an SSH operation after a timeout</td>
<td>mid.ssh.max_retries</td>
<td>Specifies the maximum amount of times to retry an SSH operation after a timeout. The system sleeps two seconds between each connection attempt. By default, the MID Server retries once only. Set the parameter to 0 to disable retries.</td>
</tr>
<tr>
<td>· Type: integer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>· Default value: 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sets a different remove file command to replace the default <code>/bin/rm -f</code></td>
<td>mid.ssh.alt_rm</td>
<td>Sets a different SSH remove file command.</td>
</tr>
<tr>
<td>· Type: string</td>
<td></td>
<td></td>
</tr>
<tr>
<td>· Default value: none</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delay sending any SSH commands to a server after connecting</td>
<td>mid.ssh.initial_delay_ms</td>
<td>Delays sending any SSH probe commands to a server after connecting to the target for the time specified, in milliseconds. This parameter applies to the legacy SSH client only.</td>
</tr>
<tr>
<td>· Type: integer (milliseconds)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>· Default value: 0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Suppress history file generation for SSH</td>
<td>mid.ssh.suppress_history</td>
<td>Suppresses the generation of the SSH history file. This parameter applies to the legacy SSH client only.</td>
</tr>
<tr>
<td>· Type: true</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>· Default value: false</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Label</td>
<td>Names</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Timeout in ms for SSH socket read               | mid.ssh.socket_timeout            | Specifies the timeout value for the SSH socket to prevent issues created by a socket timeout. Some devices, such as systems with embedded controllers like UPSs and PDUs, that have SSH enabled require more time to respond to an authentication request. The default value of 2 minutes ensures such requests do not timeout prematurely.  
  - Type: integer (milliseconds)  
  - Default value: 120000 (2 minutes) |
| Timeout in ms for SSH channel activity          | mid.ssh.channel_timeout           | Specifies the amount of time that the MID Server waits for activity on the SSH socket before closing the connection. If there has been no activity on the SSH socket for the specified timeout value, the MID Server closes the connection. Some devices, such as systems with embedded controllers like UPSs and PDUs, that have SSH enabled may require more time to respond to an authentication request.  
  - Type: integer (milliseconds)  
  - Default value: 120000 (2 minutes) |
| Timeout in ms for SSH socket read               | mid.ssh.session_timeout           | Specifies the amount of time that a cached session remains in memory after last use. Excessively small values tend to decrease performance. This parameter applies to the ServiceNow SSH client only.  
  - Type: integer (milliseconds)  
  - Default value: 300000 (5 minutes) |
| Timeout for SSH command execution (ms)          | mid.ssh.command_timeout_ms        | The timeout duration, in milliseconds, for the execution of an SSH command.  
  - Type: integer (milliseconds)  
  - Default value: 300000 (5 minutes) |
<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use keyboard interactive authentication for SSH</td>
<td>mid.ssh.use_keyboard_interactive</td>
<td>Uses the keyboard interactive authentication mode in SSH daemons on which it is activated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td>Min size of DH group in bits</td>
<td>mid.ssh.dh_group_length_min</td>
<td>Specifies the minimum group length in bits used for generating a &quot;shared secret&quot; key in Diffie-Hillman key exchange. The larger the key the more secure the SSH connection is but at the cost of performance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: integer (bits)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: 1024</td>
</tr>
<tr>
<td>Max size of DH group in bits</td>
<td>mid.ssh.dh_group_length_max</td>
<td>Specifies the maximum group length in bits used for generating a &quot;shared secret&quot; key in Diffie-Hillman key exchange. The larger the key the more secure the SSH connection is but at the cost of performance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: integer (bits)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: 2048</td>
</tr>
<tr>
<td>List of bourne-compatible shells</td>
<td>mid.ssh.shells_supported</td>
<td>Defines the bourne-compatible shells supported by the MID Server. This value is a comma-separated list of supported shells, such as ksh, dsh, bash and sh.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: ksh,bash,sh</td>
</tr>
<tr>
<td>Discard long running command error output, emulating legacy behavior.</td>
<td>mid.ssh.discard_lrc_error</td>
<td>Discard long running command error output, emulating legacy behavior.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: String</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: j2ssh - true, sncssh - false</td>
</tr>
<tr>
<td>Ratio of ssh session pool capacity to mid thread number in percentage.</td>
<td>mid.ssh.pool_thread_ratio</td>
<td>The ratio of SSH session pool capacity to the MID Server thread number, in percentage. The pool capacity is at least 25%.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: Integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: 75</td>
</tr>
<tr>
<td>Label</td>
<td>Names</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Disable the privilege check for SSHCommand.</td>
<td>mid.ssh.disable_privilege_check</td>
<td>This parameter has no effect if the target is using a privileged command other than 'sudo.' For more information, see Privileged commands for the MID Server. The remainder of this section only applies to targets which run sudo. When this parameter is set to true, the MID Server assumes that the user configured in the credential has the privilege to run the given command using sudo. The MID Server assumes the target user can run any command string following sudo on the target. When this parameter is set to false, the MID Server runs &quot;sudo -l&quot; on the target to verify the command which follows sudo has permission to run on the target. Regardless of this parameter's value, the MID Server always validates that &quot;sudo&quot; by itself can be run on the target. Some releases do not show this parameter in the MID Configuration Parameters pull down list. In this case, you may optionally add this parameter in MID Properties.</td>
</tr>
</tbody>
</table>
|                                                                      |                                 | - Type: true | false
|                                                                      |                                 | - Default value: false

By default, the MID Server is configured to search for SSH commands in the following paths and the logged-on user's default paths:

- /usr/sbin
- /usr/bin
- /bin
- /sbin
## Upgrade parameters

<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed MID Server version</td>
<td>mid.pinned.version</td>
<td>Name of the version to which this MID Server is pinned.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: MID buildstamp</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> To see the MID buildstamp for your instance, type stats.do in the navigation filter. An example of the buildstamp format is <code>jakarta-05-03-2017_12-17-2018_2230</code></td>
</tr>
<tr>
<td>Upgrade proxy enable</td>
<td>mid.upgrade.use_proxy</td>
<td>If your MID Server must go through a web proxy to access the upgrade URL, set this parameter to true to instruct the MID Server to use the proxy. You must also set the proxy server's host and port. If the instance proxy user name and password are set, they are used for the upgrade proxy as well.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td>Upgrade proxy host</td>
<td>glide.mid.autoupgrade.proxy_host or glide.glidesoap.proxy_host</td>
<td>If your MID Server must go through a web proxy to access the upgrade URL, define the proxy's host here.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: string (URL)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: none</td>
</tr>
<tr>
<td>Upgrade proxy port</td>
<td>glide.mid.autoupgrade.proxy_port or glide.glidesoap.proxy_port</td>
<td>If your MID Server must go through a web proxy to access the upgrade URL, define the proxy's port here.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: integer (0-65535)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: 80</td>
</tr>
<tr>
<td>Upgrade proxy user</td>
<td>glide.mid.autoupgrade.proxy_user</td>
<td>If your MID Server must go through a web proxy to access the upgrade URL, define the proxy's user name here.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: string (URL)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: none</td>
</tr>
</tbody>
</table>
## Windows Discovery parameters

<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
</table>
| Upgrade proxy password | glide.mid.autoupgrade.proxy_password | If your MID Server must go through a web proxy to access the upgrade URL, define the proxy’s password here.  
- **Type**: string  
- **Default value**: none |

<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable or disable Powershell parameter passing via the command line. | mid.powershell.command.parameter_passing | Enable this parameter to allow passing Powershell parameters from the command line.  
- **Type**: True | False  
- **Default value**: false |

<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable or disable the Powershell script parameter passing via the command line. | mid.powershell.command.script.parameter_passing | Enable this parameter to allow passing Powershell scripts from the command line.  
- **Type**: True | False  
- **Default value**: true |

<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable or disable the enforcement of UTF-8 for command output. | mid.powershell.enforce_utf8 | Enable this parameter to force commands on a target Windows system to return UTF-8 encoded output. Disabling it allows the target system to use its default encoding. This parameter is only valid when PowerShell is enabled. Setting this value to false may result in incorrect values in the CMDB when non-ASCII characters are returned by a probe.  
- **Type**: True | False  
- **Default value**: true |

<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable PowerShell for Discovery. | mid.use_powershell | Specifies whether to enable PowerShell for Discovery. The MID Server requires PowerShell version 2 to operate. If the MID Server cannot find the correct version of PowerShell, it uses WMIRunner instead.  
- **Type**: True | False  
- **Default value**: true |
<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable/Disable automatically falling back to the MID Server          | mid.powershell.local_mid_service_credential_fallback                  | Specifies the login credentials the MID Server uses if all other credentials fail.  
| service user credential if all other credentials fail.               |                                                                      |  
|                                                                      |                                                                      | Type: True | False  
|                                                                      |                                                                      | Default value: false  |
| Timeout for Windows probes.                                          | mid.windows.probe_timeout                                             | Specifies the timeout value for the Windows probe, in seconds. The default value is 5 minutes.  
|                                                                      |                                                                      | Type: Integer  
|                                                                      |                                                                      | Default value: 600 seconds  |
| Powershell use credentials table.                                    | mid.powershell.use_credentials                                         | Specifies whether PowerShell Discovery should use the Windows credentials from the credentials table. To use PowerShell Discovery on a single domain, set this parameter to false, and then restart the MID Server. In this case, the MID Server runs the probes with the credentials of the user for the MID Server process.  
|                                                                      |                                                                      | Type: True | False  
<p>|                                                                      |                                                                      | Default value: true  |</p>
<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path to Powershell executable.</td>
<td>mid.powershell.path</td>
<td>Enables an administrator to point to a specific PowerShell on a MID Server in cases where more than one PowerShell is installed. Supply the path to the directory containing the PowerShell executable, for example, C:\mypowershell or C:\mypowershell. ServiceNow automatically appends the string powershell.exe to the path. This parameter might be necessary when both 32-bit and 64-bit PowerShells are active on the same MID Server, and it becomes necessary to launch the correct PowerShell for the context. Note that 64-bit Windows employs file system redirection and the MID Server runs as a 32-bit application. If the path is in %WinDir%\System32, Windows automatically redirects to %WinDir%\SysWOW64. To avoid redirection, specify the path as %WinDir%\Sysnative. An example would be to specify C:\WINDOWS\sysnative \WindowsPowerShell\v1.0\ instead of C:\WINDOWS \system32\WindowsPowerShell \v1.0.</td>
</tr>
</tbody>
</table>
| Set the protocol MID Servers use to communicate with remote Windows hosts. | mid.windows.management_protocol | Enables administrators to select the Windows management protocol used for device and process classification. Options include:  
- WMI  
- WinRM  
Type: String  
Default value: WMI  
Note: On a 64-bit version of Windows Server 2003 or Windows XP, a Microsoft hotfix may be required to enable this capability. |
<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
</table>
| Set the port WinRM will use to connect to remote hosts.             | mid.powershell_api.winrm.remote_port                       | Specifies the communications port the MID Server uses to communicate with Windows Remote Management (WinRM) protocol.  
- Type: Integer  
- Default value: 5985                                                                 |
| Maximum number of sessions allowed in the pool per target.          | mid.powershell_api.session_pool.target.max_size            | Specifies the maximum number of sessions allowed in the pool per target host.  
**Note:** Setting or changing this parameter requires restarting the MID Server.  
- Type: Integer  
- Default value: 2                                                                 |
| Maximum number of sessions allowed in the session pool.             | mid.powershell_api.session_pool.max_size                   | Specifies the maximum number of sessions allowed in the session pool.  
**Note:** Setting or changing this parameter requires restarting the MID Server.  
- Type: Integer  
- Default value: 25                                                                 |
| Idle Powershell session timeout (seconds).                          | mid.powershell_api.idle_session_timeout                    | Specifies the timeout value of idle Powershell sessions in seconds.  
**Note:** Setting or changing this parameter requires restarting the MID Server.  
- Type: Integer  
- Default value: 60                                                                 |
<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
</table>
| Timeout for all Windows probes on a MID Server. | mid.windows.probe_timeout | Sets the timeout interval for all Windows probes on a specific MID Server. This value is overridden by the values configured for individual probes with the wmi_timeout probe parameter.  
  - Type: Integer  
  - Default value: 300 |

### SNMP configuration parameters

<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable automatic inclusion of SNMP public community string. | mid.snmp.enable_auto_public | Specifies whether to use the [SNMP public community string](#) automatically if no other SNMP credentials were successful.  
  - Type: True | False  
  - Default value: true |
| Maximum time to wait for a response for the first OID request. | mid.snmp.request.timeout | Specifies the timeout value for the first OID request, in milliseconds. For subsequent requests (for example, table OIDs), the [mid.snmp.session.timeout configuration parameter](#) (see below) takes effect.  
  - Type: Integer  
  - Default value: 1500 |

Note: You can override this parameter with the timeout SNMP probe parameter.
<table>
<thead>
<tr>
<th>Label</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
</table>
| Maximum time to wait for responses to OID requests once a session has been established. | mid.snmp.session.timeout      | Specifies the timeout value for subsequent OID request, in milliseconds. SNMP communication is stateless and does not have a session or connection in the normal sense. The system regards a positive response from the first OID request as a sign that it should expect prompt responses to subsequent requests. While the default is short, it may be useful to increase this parameter value to the same value as that used for mid.snmp.request.timeout.  

**Note:** You can override this parameter with the `establish_session_timeout` SNMP probe parameter.  
- **Type:** Integer  
- **Default value:** 500 |
| Use the Snmp4j library for SNMP communication.                      | mid.snmp.use_snmp4j           | Use the Snmp4j library for SNMP communication. This is a strict requirement for SNMPv3. This parameter should only be set to `false` based on advice from ServiceNow Technical Support.  

- **Type:** True | False  
- **Default value:** true |
| Use SNMP v1 and v2c for probes.                                     | mid.snmp.use_snmp_v1_v2c      | Attempt communication using these SNMP protocol versions. Requires configuration of SNMP community string credentials or the `mid.snmp.enable_auto_public` parameter set to true, as applicable for targeted devices.  

- **Type:** True | False  
- **Default value:** true |
| Use SNMP v3 for probes.                                             | mid.snmp.use_snmp_v3          | Attempt communication using the SNMPv3 protocol version. Requires configuration of SNMPv3 credentials.  

- **Type:** True | False  
- **Default value:** true |
### Event Management parameters

<table>
<thead>
<tr>
<th>Label</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Bulk size for sending events | mid.probe.event.bulk_size | Specifies the maximum size of an event payload, in MB.  
- Type: Integer  
- Default value: 120 |
| Waiting period on empty queue for sending events | mid.probe.event.wait_time | Waiting period on an empty queue for sending events.  
- Type: Integer  
- Default value: 1000 |
| Enables or disables sending events. | mid.probe.event.send.enabled | Enables or disables the sending of events.  
- Type: True | False  
- Default value: true |
| Maximum size of events queue allowed before events will be rejected | mid.probe.event.queue.max_size | Specifies the maximum size permitted for the event queue before incoming events are rejected.  
- Type: Integer  
- Default value: 100,000 |
| If true then bulk of events will be sent to the server instead of single event sending | mid.probe.event.queue.use_bulk | Specifies whether events are sent to the server singly or in bulk. If this parameter evaluates to true then events are sent to the server in bulk.  
- Type: True | False  
- Default value: true |
| Policy to prevent whitespace in event description field. | mid.probe.event.suppress.whitespaces | Allows line breaks in description fields for multi-line events. Apply this parameter to each MID Server used with event connector instances. Choices are:  
- all  
- leave_as_is  
- keep_newline  
- Type: String  
- Default: all |
| Limit of number of active metrics to CI mappings | mid.em.metric.metric_to_ci_map_limit | Specifies the maximum number of active metrics allowed per CI map.  
- Type:  
- Default value: 200,000 |
<table>
<thead>
<tr>
<th>Label</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of seconds to wait before resending unhandled event</td>
<td>mid.em.metric_binding_timeout_seconds</td>
<td>Specifies the number of seconds to wait before resending unhandled events.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: Integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Default value: 300</td>
</tr>
<tr>
<td>Max number of seconds to wait before resending unhandled event</td>
<td>mid.em.metric_binding_timeout_max_seconds</td>
<td>Specifies the maximum number of seconds to wait before resending unhandled events.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: Integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Default value: 10800</td>
</tr>
<tr>
<td>Max number of seconds before refreshing the metric source type cache in memory</td>
<td>mid.em.metric_max_elapsed_time_before_refresh</td>
<td>Specifies the maximum number of seconds before the metric source type cache is refreshed in memory.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: Integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Default value: 60</td>
</tr>
<tr>
<td>Max length of string used for SQL command</td>
<td>mid.em.metric_max_sql_string_length_for_types</td>
<td>Specifies the maximum length of the string (composed of types) used for an SQL command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: Integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Default value: 30000</td>
</tr>
<tr>
<td>Period, in seconds, between statistics reports to the instance.</td>
<td>mid.em.statistics_report_period_seconds</td>
<td>Specifies the period, in seconds, between statistics reports to the instance. Use 0 to disable reporting. This parameter requires a restart.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: Integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Default value: 60</td>
</tr>
<tr>
<td>Max number of seconds to collect metrics in every cycle</td>
<td>mid.em.metric_connector_max_run_time_seconds</td>
<td>Specifies the maximum number of seconds to collect metrics in every cycle.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: Integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Default value: 300</td>
</tr>
<tr>
<td>Number of minutes to go back in history to retrieve metrics</td>
<td>mid.em.metric_connector_history_min</td>
<td>Specifies the number of minutes to go back in history to retrieve metrics.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type: Integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Default value: 180</td>
</tr>
<tr>
<td>Label</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Metric/Event Log Level</td>
<td>mid.em.metric_event_logging</td>
<td>Specifies the level of metric and event logging. Choices are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• all</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• events</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• metrics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• metrics:&lt;filter&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• events:&lt;filter&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: String</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: none</td>
</tr>
<tr>
<td>Number of seconds of delay when collecting metrics</td>
<td>mid.em.metric_connector_late_arrivals_delay</td>
<td>Specifies the number of seconds to delay when collecting metrics.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: Integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: 30</td>
</tr>
</tbody>
</table>

**Add a MID Server parameter**

Use a MID Server parameter to control the behavior of a particular MID Server. You modify MID Server parameters in the Configuration Parameters related list in the MID Server record and in the config.xml file in the \agent directory of your MID Server installation.

Role required: admin

1. Navigate to **MID Server > Servers**.
2. From the list of MID Servers, select a MID Server to configure.
3. Select the **Configuration Parameters** related list.

   This related list shows all the parameters currently in the MID Server's configuration file. If there are any passwords, they are displayed in asterisks for security reasons.
Defining MID Server configuration parameters

4. To add parameters, click **New**, and then complete the form.

After the form is submitted, the configuration file for that MID Server is modified to include the new parameter. Changes to existing parameters are reflected in the MID Server configuration file as well. Changes made to the MID Server configuration file do not take place immediately, but rather the next time the MID Server is restarted. The MID Server form has a related link for restarting the MID Server.
**Note:** ServiceNow prevents you from saving changes, such as modifying or deleting parameters, that would cause the MID Server to lose communications with the instance. For example, you cannot change the url parameter. Any changes to these protected properties must be made directly in the `config.xml` file for that MID Server.

Setting Parameters from the `config.xml` File

MID Server configuration is controlled by an XML file called `config.xml`. This file is located in the \agent directory, immediately under the directory where the MID Server is installed. Edit this file directly to make any configuration changes to protected parameters. Many configuration changes, such as those that do not disrupt communication between the MID Server and the ServiceNow instance, may also be made from the instance.

The structure of the `config.xml` file is simply an outer `parameters` tag and a series of inner `parameter` tags. Each `parameter` tag has name and `value` attributes.

- To change the value of a parameter, edit the `value` attribute.
- To add a parameter, add another `parameter` tag with its name and `value`.
- To delete a parameter, delete the entire `parameter` tag.

The order of the parameters within the file is not important. Notice the green comment sections in the sample. Use these elements to add useful comments to the configuration file.

**Note:** When configuring the MID Server for use with a proxy server, be sure to remove the comment tags around the proxy sections that you configure.
MID Server properties

Properties control the behavior of all MID Servers or a particular MID Server. MID Server properties override MID Server parameters. You can add or MID Server properties from the MID Server > Properties module.

The MID Server properties are in the MID Server Property (ecc_agent_property) table and can be accessed by navigating to MID Server > Properties. You must add these properties if they are not already present.
### MID Server properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mid.discovery.max_payload_size</td>
<td>Specifies the maximum string length of Discovery results that the MID Server sends to the instance. If the Discovery probe results exceed the limit, the MID Server discards them and returns a warning message. For probes, this applies only to those probes where the Used by Discovery field is true. For patterns, this applies to the Horizontal Pattern probe. Set the value to any negative number to disable the payload limit and allow payloads of any size to be sent to the instance. For example, -1.</td>
<td>integer (bytes)</td>
<td>5000000</td>
</tr>
<tr>
<td>mid.eccq.max_payload_size</td>
<td>Specifies the maximum string length of a payload that the MID Server sends to the instance. The MID Server verifies the size of the payload before sending it to the instance. If the payload size exceeds the limit, the MID Server discards it and returns an error message in the payload.</td>
<td>integer (bytes)</td>
<td>20000000</td>
</tr>
<tr>
<td>mid.discovery.max_pattern_payload_size</td>
<td>Defines the maximum overall payload size for the payload of results that come from patterns.</td>
<td>integer (bytes)</td>
<td>300000</td>
</tr>
<tr>
<td>mid.max_ci_count_per_page</td>
<td>Defines the size of each chunk in a payload of results that come from patterns. The chunk can be greater than this parameter value, depending on the relationships of the CIs.</td>
<td>integer (bytes)</td>
<td>300000</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mid.property.jdbc_operations</td>
<td>Tells the JDBCOrchestrationProbe what JDBC operations it is allowed to execute. Edit this property value to allow JDBC Orchestration activities to perform more operations. All operations are comma separated. Select a MID Server in the MID server field to define specific operations for that MID Server, or leave the field empty to apply the list of operations to all MID Servers. This property requires the Orchestration plugin.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
|                                          | * Type: string*  
|                                          | * Default value: select,update,insert,delete,show,create,describe,begin,if,end,not,exists*                                                                                                                |
| mid.property.jms.command.allowed_factory_names | Comma delimited list of Java Messaging Service (JMS) connection factories that the MID Server requires for a custom JMS activity or action. This property requires the Orchestration plugin.                                                                 |
|                                          | * Type: string*  
|                                          | * Default value: connectionFactory, queueConnectionFactory, topicConnectionFactory*                                                                                                                        |
| mid.property.powershell.command.script.parameter_passing | Type: true | false                                                                                                                |
|                                          | * Default value: false*                                                                                                                  |
| mid.property.ssh.use_snc                 | Enables the use of the SNCSSH client for Discovery and Orchestration. Change this property to false to use J2SSH. This property applies to all MID Servers connected to the instance.                                                                 |
|                                          | * Important: If you upgrade from Dublin or earlier and want to use the SNCSSH client, you must add this property to the MID Server Properties (ecc_agent_property) table and set it to true. If you do not set this property, all the MID Servers in the upgraded system will use J2SSH.  |
|                                          | * Type: true | false                                                                                                                |
|                                          | * Default value: true*                                                                                                                                                                                    |
| mid.servicewatch.max_concurrent_connections | Defines the maximum number of concurrent tasks sent to an individual host by a single MID Server.                                                                                                        |
|                                          | * Type: integer*  
<p>|                                          | * Default value: 7*                                                                                                                                                                                      |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.stored_proc.data_type.validation</td>
<td>Stops validation of data types in stored procedure parameters. Use this property if you use Orchestration to run a stored procedure on MySQL, Oracle DB, and MS-SQL databases and you want to avoid performing data type validation. Restart the MID Server service if after you change the value of this property.</td>
</tr>
</tbody>
</table>
|                                                            | **Type:** true | false **Default value:** false

**Create a MID Server property**

Use a MID Server property to control either the behavior of all MID Servers or a particular MID Server.

Role required: admin

You set MID Server properties to override MID Server parameters. Configure MID Server properties in the MID Server plugin. Do not configure MID Server properties in the `glide.properties` file that is located in the properties folder of the agent. The `glide.properties` file gets overwritten during the upgrade process.

1. Navigate to [MID Server > Properties].
2. Click [New].
3. Fill in the fields, as appropriate (see table).

**MID Server properties field**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the property name. See <a href="https://docs.servicenow.com/index.jsp">MID Server properties</a> or <a href="https://docs.servicenow.com/index.jsp">Optional Configuration</a> parameters for a list of parameter and property names.</td>
</tr>
<tr>
<td>Value</td>
<td>You can enter the value you want the property to have.</td>
</tr>
</tbody>
</table>

**Note:** If you are amending JDBC operations through the `mid.property.jdbc_operations` properties, you can enter verbs like `BEGIN`, `END`, `IF`, or common PL/SQL block statements. This will assist in being able to run CREATE or ALTER statements. You might have to restart the MID server before running some of the statements.

| MID Server     | Leave this field blank to set a MID Server property that affects all MID Servers. To set a MID Server property for a particular MID Server, select the MID Server. |

After setting any MID Server properties, restart the MID Server to ensure the properties sync with the instance.
MID Server pause

The MID server can be put into a **Paused** state to temporarily prevent it from polling the ECC Queue for work or sending Discovery results back to the instance.

You might want to pause the MID Server when your network infrastructure is undergoing changes. This prevents applications like Discovery from throwing errors during a particular maintenance window.

A paused MID Server continues processing commands that it had already retrieved before it was paused. When you resume the MID Server, the MID Server starts retrieving new commands to process.

**Note:** Discovery continues to assign jobs to MID Servers that are **Paused**. MID Servers that are **Down** are not assigned jobs.

Unlike stopping the MID Server from the Windows or Linux server command line on the MID Server machine, pausing the MID server is something that you can do from the instance. The MID Server pause feature is available starting with the Istanbul release.

**Note:** You can only pause **validated MID Servers**.

You can still perform these actions when the MID Server is paused:

- Access the MID Server logs and delete log entries.
- View MID server statistics. While the MID Server is in the **Paused** state it stops generating statistics. But you can still view the statistics generated before you paused the MID Server.
- Retrieve the MID Server thread dump.
- Make and save **configuration changes** and property changes to the server. The changes take effect after the MID Server is resumed.
- Clear the ECC queue.

The **MID server heartbeat** continues to function while the MID Server is in the **Paused** state. If the MID Server is upgraded while it is in the **Paused** state, the MID Server state automatically changes to **Up** after successful upgrade. It does not return to the **Paused** state.

During **MID Server selection**, paused MID Server can still be selected but are prioritized below MID Servers that are not paused.

Events that occur during MID Server pause

The vCenter and SNMP event collectors, continue to run and process events when you pause the MID Server. These events are not part of the normal synchronous communication that the MID Server has with the instance that you see in the ECC queue. Events are still relayed to the instance and can even trigger actions on records in the instance, such as a CI update. For example, if vCenter detects that a virtual machine goes down or is deleted, a vCenter event makes a change to the status of the corresponding CI record for that virtual machine.

To prevent these events from being processed, stop the extensions from running. See:

- **Configure and run the vCenter event collector extension**
- **Configure the SNMP Trap Collector Extension**

Pause the MID Server

Pause the MID Server to temporarily prevent it from polling the ECC Queue for work or sending Discovery results back to the instance.
Role required: agent_admin

You can only pause validated MID Servers.

1. Open the MID server record.
2. Select a running MID Server that has been validated.
3. On the MID Server form, select Pause MID under Related Links.
   The state of the MID Server changes to Paused.

4. To resume MID Server processing, select Resume MID under Related Links.

MID Server domain separation

MID Servers can be configured in separate domains.

The records that can be read, updated, or created by a MID Server are determined by the credentials configured for that MID Server in the config.xml file. These are the user credentials that a MID Server uses to access the instance and specify which domain’s records that MID Server can access.

You can create versions of these specific MID Server policy records that only a MID Server from the same domain can use. This process separation is supported for records in tables that extend MID Server Synchronized Files (ecc_agent_sync_file):

- MID Server MIB File (ecc_agent_mib)
- MID Server JAR File (ecc_agent_jar)
- MID Server Script File (ecc_agent_script_files)

See Set up domain separation for MID servers for instructions on setting up domain separation through the MID server.

Note: Attachments on MIB or JAR file records might not appear as they did in a non-domain separated environment. The attachments do not appear because the Attachments (sys_attachment) table is data separated. When data is separated between domains, a record in a child domain cannot access records in a parent domain.

Set up domain separation for MID servers

Set up domain separation through the MID server user role and the MID Server configuration file.

Role required: admin, agent_admin

1. Configure a MID Server user within a specified domain with the proper mid_server role.
2. Specify this user within the MID Server config.xml file. When you set the MID Server user credentials in the config.xml file, make sure they are in the proper domain.
When the MID Server connects to the instance, the MID Server record is created in the proper domain.

If you must change the MID Server domain:

1. Stop the MID Server and delete the ecc_agent record.
2. Update the MID Server `config.xml` with the new user in the new domain and restart the MID Server service.

If you need to create versions of specific MID Server files that only MID Servers in your domain can use:

1. Open or create a record in one of these MID Server modules:
   - SNMP MIBs
   - JAR Files
   - Script Files
2. Update an existing domain policy or submit a new record.

---

**Note:** Attachments on MIB or JAR file records might not appear as they did in a non-domain separated environment. The attachments do not appear because the Attachments (sys_attachment) table is data separated. When data is separated between domains, a record in a child domain cannot access records in a parent domain.

---

**Privileged commands for the MID Server**

The Now Platform provides default privileged commands for the MID Server to use and the ability to add additional commands to the system.

An example of information that requires elevated privileges is information about storage disks on a host server, retrieved with the `fdisk -l` command. If your system cannot use sudo commands, you must configure the hosts in your network to use one of the other privileged commands. You can have different privileged commands set up for different hosts. However, Discovery supports only one privileged command per host.

**Important:** You can edit supported privileged commands, but do not delete them.

**SSH privileged escalation command requirements**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sudo</td>
<td>Host must support the <code>sudo -S -p &lt;password&gt;</code> command and return the correct list of allowed SSH commands. Credentials provided for Discovery must be able to run the command <code>sudo -S -p &lt;password&gt; &lt;commands&gt;</code>.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| pbrun   | • Host must support the `pbrun -v` command and return the correct version of PowerBroker.  
  • Credentials provided for Discovery must be able to run `pbrun <commands>`.  
  • Discovery does not support any other `pbrun` options, such as a password prompt.  
  • The instance must be able to reach the target host via SSH. |
| pfexec  | • Host must support the `pfexec id -a` command and return the correct ID.  
  • Credentials provided for Discovery must be able to run `pfexec <commands>`. Possible SSH commands are those listed in [Unix and Linux commands](https://en.wikipedia.org/wiki/List_of_Shell_commands).  
  • Discovery does not support any other `pfexec` options, such as a password prompt. |
| dzdo    | • Host must support the command `-v dzdo` command and return the path to dzdo in standard output.  
  • Credentials provided for Discovery must be able to run `dzdo <commands>`. Possible SSH commands are those listed in [Unix and Linux commands](https://en.wikipedia.org/wiki/List_of_Shell_commands).  
  • Discovery does not support any other `dzdo` options, but Discovery supports password authentication for dzdo. |

### Add a new privileged command

Add a new privileged command to the Privileged Command (privileged_command) table that is available to your MID Servers.

Role required: admin

**Important:** Do not delete any of the supported commands.

1. Navigate to MID Server > Privileged Command and click **New**.
2. Complete these fields:
   - **Command**: The name of the privileged command.
   - **Password Prompt**: The password prompt displayed to the user for this privileged command, or a regular expression that matches this password prompt. If this field is empty, no password is required for this privileged command, and no prompt is displayed. SUDO commands do not require a password prompt.
3. Click **Submit**.

### Create a pbrun profile privileged command

You can create a special configuration for the `pbrun` privileged command that allows it to run as a profile.

Role required: discovery_admin, admin
Of all the privileged commands, only the **pbrun** command can be configured to run as a profile, and only one of these special **pbrun** configurations can function on a MID Server.

**Important:** Edit the existing **pbrun** record for this purpose. The system ignores any additional commands you create for **pbrun**.

1. Navigate to **MID Server > Privileged Command**.
2. Select **pbrun** from the list.
3. In the Privileged Command record, edit the value in the **Command** field to use the format **pbrun -u <profile>**.
   
   For example, you can set **pbrun -u admin** as a command to run with an admin profile.
4. Click **Update**.

**Configure the MID Server to use specific privileged commands**

You can configure the MID Server to use specific commands in a defined order.

Role required: admin

1. Navigate to the list of MID Servers using one of the following paths:
   
   - **MID Server > Servers**
   - **Discovery > MID Servers**
   - **Orchestration > MID Servers**

2. Select the MID Server you want to configure.
3. Click the menu icon in the header bar and select **View > Advanced** from the context menu.
4. In the **Privileged Command** related list, click **Edit**.

5. Select the command you want this MID Server to use and click **Save**.

The default order of privileged commands is 100, but you can change the order as necessary. The privileged command with the smallest order number is tried first.
List of privileged commands to use for a MID Server

Map an IP address to a DNS name

If the MID Server manages resources within defined IP ranges, all host servers must have their DNS names mapped to an IP address.

Role required: admin

The association of an IP address to a DNS name ensures that the appropriate MID Sever is selected based on the IP Address range configuration. If this is not done, Orchestration reverts to the default MID Server.

If Discovery cannot discover the server and resolve the DNS name to an IP address, you must creating the mapping manually, using this procedure.

1. Enter `cmdb_ci_dns_name.list` in the navigation filter.
   A list of DNS names appears.
2. Check the list for your host server.
   If the server does not appear in the list, continue with this procedure.
3. Click **New**.
4. Enter the fully-qualified domain name (FQDN) of the host server in the **Name** field.
5. Right-click in the form header and select **Save** from the context menu.
6. In the **IP Address** related list, click **New**.
7. In the **IP Address** field, enter the IP address of your host server.
8. In the **Nic** field, select `eth0` or your preferred network interface controller.
9. Leave the **Netmask** field blank.
10. Click **Submit**.
MID Server security and encryption

Several options are available for you to enhance security on MID Servers, including credential and encryption security, the authorization of SOAP requests, and the establishment of secure socket layer (SSL) connections.

How MID Server encryption works

The MID Server login credentials appear in the config.xml file in clear text by default, but you can encrypt them. While the username and password are initially set in a config.xml configuration file on the MID server, once the MID server retrieves the credentials, it can replace the clear-text password with an encrypted password. For the encryption of the local MID server service account, the password is encrypted using an AES128 encryption algorithm. The MID server also maintains an encryption key that is generated each time it starts and remains in memory and not on the hard disk. When credentials need to be sent from the instance to the MID server, the following process takes place:

1. The instance retrieves the encrypted password and the unencrypted username from the instance database table.
2. The instance decrypts the encrypted password, and then re-encrypts it using the MID server encryption key.
3. The username and re-encrypted password are sent to the MID Server through the encrypted TLS session was already established between the MID server and the instance.
4. The MID server receives the credentials and decrypts the password in memory before using the credentials for remote operations. At no point is the credential password stored on the disk in an unencrypted format.

To enable this encryption, see Encrypt MID Server login credentials.

MID Server encryption keypairs

Automation credentials are secured by encrypting them in the instance with the MID Server’s trusted public key prior to transmission. When the MID Server is created, it generates a keypair, consisting of a public and private key. After the MID Server is validated, it can use the private key to decrypt automation credentials. You should occasionally rekey the MID Server to meet your organizations security requirements. See Rekey a MID Server for instructions.

SSL certificates

You can add certificates to the MID Server if you want communication to occur over SSL. You can add these certificates to the cacerts keystore file:

- Signing Certificate Authority (CA) certificate
- MID Server certificate

See Add SSL certificates for the MID Server for instructions.
Basic authentication credentials and SOAP requests

You can enforce basic authentication on each request. The MID Server is not able to communicate through a proxy server if the proxy server supports only NTLM authentication. You can use basic authentication with a proxy server or create an exception for the MID server host.

Supplying basic authentication information, regardless of whether it is required, has an added advantage. The web service invocation creates or updates data using the supplied credentials. For example, when you create an incident record, the journal fields have the user id of the basic authenticated user instead of the default Guest user. This behavior allows you to identify data added by a specific MID Server.

You can set basic authentication credentials for SOAP requests. See Require basic authorization for incoming SOAP requests for instructions. Each SOAP request contains an Authorization header as specified in the Basic Authentication protocol.

**Note:** The setting for enforcing strict security controls how the instance uses the credentials you provide for the MID Server. When the setting is enabled, you must provide a user ID with access to the tables the MID Server is trying to access. When the setting is disabled, any valid user ID allows the MID Server to access to all tables.

Encrypt MID Server login credentials

Encrypt the MID Server login credentials for added security.

**Role required:** admin

**Note:** Any field in this file can be encrypted, but once encrypted, a field can be managed only from within the instance. You should encrypt password fields only for the MID Server and any proxy server specified.

1. Navigate to the *agent* directory that was created when the MID Server was installed and open the *config.xml* file using a text editor such as WordPad.

   The instance credentials section of the *config.xml* file looks like this:

   ```xml
   <!-- If your instance has authentication enabled (the normal case), set these parameters to define the user name and password the MID Server will use to log into the instance. -->
   <parameter name="mid.instance.username" value="midsrvadmin" />
   <parameter name="mid.instance.password" value="securepassw0rd"/>
   ```

2. Add the `encrypt="true"` attribute to the password tag.

   ```xml
   <parameter name="mid.instance.username" value="midsrvadmin" />
   <parameter name="mid.instance.password" encrypt="true" value="securepassw0rd"/>
   ```

3. Save the *config.xml* file, and then restart the MID Server service.

   The password is now encrypted.

   ```xml
   <parameter name="mid.instance.username" value="midsrvadmin" />
   <parameter name="mid.instance.password" encrypt="true" value="encrypted:rhrfUNYRzZAI8/BkTtZmNA=="/>
   ```
The password cannot be decrypted, which means it is displayed in clear text again, by changing the encryption attribute to false or by deleting the attribute. If the password is changed in the config.xml file and the MID Server restarted, the new password is encrypted.

Rekey a MID Server

Rekeying a MID Server forces it to restart and generate a new private key. Typically, this is only necessary if the MID Server keystore is compromised.

Role required: admin

When the MID Server comes back online, the system automatically validates the new key, and the MID Server resumes processing automation tasks.

1. Navigate to MID Server > Servers.
2. Open the MID Server whose keypairs you want to rotate.

Add SSL certificates for the MID Server

Configure the MID Server to connect to a source over SSL.

Role required: admin

Note: The MID Server does not support SSL when importing data from an integration, such as an LDAP server.

1. Open a command prompt and navigate to the folder containing the JRE keytool. An example path might be: `C:\Program Files (x86)\ServiceNow\<MidServer(s)>\agent\jre\bin`
2. Enter the following keytool command to import a certificate into the MID Server’s cacerts keystore:

   ```
   keytool -import -alias <certificate alias> -file "<path to certificate>" -keystore "<path to MID Server(s)>\agent\jre\lib\security\cacerts"
   ```

   For example, you might enter:

   ```
   keytool -import -alias MyCA -file "C:\myca.cer" -keystore "C:\Program Files (x86)\ServiceNow\MIDserver\agent\jre\lib\-security\cacerts"
   ```

   Note: Keytool prompts for a certificate password. If the certificate is for a CA, keytool also asks whether to trust the certificate authority. To add a certificate to an instance, see Upload a certificate to an instance.

Require basic authorization for incoming SOAP requests

For added security, you can enforce basic authentication on each incoming SOAP request to the MID Server.

Role required: admin

1. Navigate to System Properties > Web Services.
2. Select the check box for Require basic authorization for incoming SOAP requests.
3. Click Save.
4. To provide basic authentication credentials for a MID Server, navigate to C:\Program Files ServiceNow\<MID Server name>\agent and edit the config.xml file, as follows:

   a) Find the element `<parameter name="mid.instance.username" value="/">` and enter the instance administrator user name as the value.
For example, you might enter `<parameter name="mid.instance.username" value="admin"/>`.  

b) Find the element `<parameter name="mid.instance.password" value=""/>` and enter the configured password for this instance as the value. For example, you might enter `<parameter name="mid.instance.password" value="abc123"/>`.

**Advanced MID Server configuration**

There are several advanced options available for you to customize and configure the MID Server.

**Enable script file synchronization for Windows browser security**

Windows Internet Explorer enhanced security blocks downloaded files that it determines are potentially dangerous.

Enhanced security in Windows browsers, such as Internet Explorer, blocks downloaded files that it determines are potentially dangerous. This would block files downloaded for use by the MID Server. You would need to unblock each file manually through the browser.

To get around this issue, use file synchronization. File synchronization requires you to proactively take script files from your instance and save them on the MID Server. The files on the instance and the MID server stay synchronized, but there is no longer any need for the MID Server to download the whole file. File synchronization also protects any updates you make in those script files from being overwritten during the upgrade of an instance.

Script files synchronized with the MID Server are stored on the instance in the MID Server Script File [ecc_agent_script_file] table, which you can access in the MID Server > Script Files module.

When the MID Server first connects to the instance, the instance creates a directory called `\scripts` in the MID Server root. The instance then creates a parent directory in the path `\scripts\<parent name>` using definitions from the ecc_agent_script_file table. Finally, the instance creates the script files themselves inside the parent directory using the records from the ecc_agent_script_file table.

The record for the parent directory looks like this:
The instance creates each script file in the parent directory on the MID Server using the record Name from the ecc_agent_script_file table as the file name and the Script field payload as the file contents. A script file record looks like this:
The synchronization of the script file continues to work as if the script was manually added to the form.

See [Attach a script file to a MID Server](#) for instructions on how to attach a script file.

**Note:** The MID Server Script File (ecc_agent_script_file) table is domain separated. You can create versions of these policies that only a MID Server from the same domain can use. For instructions, see [Set up domain separation for MID servers](#).

---

**Attach a script file to a MID Server**

Attach a script file to a MID Server to keep script files in synch with the instance without having to download the file. Do this when your browser security settings are blocking the downloading of files that your MID Server needs from the instance.

**Role required:** `admin`

You can attach multiple files, but the last attached file gets synchronized to the MID Server. If you delete the attachment, the script file becomes inactive, and the synchronized file is deleted from MID Server.

1. Navigate to **MID Server > Script Files.**
2. Open the file to which you would like to attach the script file, or click **New** to create a new file.

   **Note:** The script file attachment name must match the MID Server script file name, since the record can contain other attachments.

3. Select **Use attachment**, and then click the paperclip icon to add the attachment.

   **Note:**
   When **Use attachment** is checked, an attached script file overrides the script contained in the **Script** field. If this check box is cleared, the script in the **Script** field is used instead of the attachment.
   
   The script file attachment name must match the MID Server script file name, since the record can contain other attachments.

4. Click **Update** to initiate the synchronization process.
   Ensure that the file name matches the script name.

   **Note:** If you receive the error message: **File type not permitted or mime type does not match the file content**, request that your administrator turn off mime type validation on attachments. The system property `glide.security.file.mime_type.validation` controls this setting.

---

### Configure a MID Server for Service Analytics RCA

To activate the Service Analytics root cause analysis (RCA) feature, configure at least one dedicated MID Server with the ServiceAnalytics as a supported application, and with the RCA capability. To ensure uninterrupted services, it is recommended that you also configure a failover MID Server cluster for RCA.

If the Domain Support - Domain Extensions Installer plugin is activated, then you can configure a dedicated MID Server with the RCA capability, per domain. In this case, RCA for a business service is done on the MID Server that is in the same domain as the business service. Otherwise, a MID Server from the global domain is used.

#### Hardware requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory</td>
<td>• <strong>Minimum:</strong> 4 GB</td>
</tr>
<tr>
<td></td>
<td>• <strong>Recommended:</strong> 8 GB</td>
</tr>
<tr>
<td>Processor</td>
<td>• <strong>Minimum:</strong> Either of the following:</td>
</tr>
<tr>
<td></td>
<td>• Core 2+</td>
</tr>
<tr>
<td></td>
<td>• Xeon processor with a speed over 2 GHz</td>
</tr>
<tr>
<td></td>
<td>• <strong>Recommended:</strong> Quad-core</td>
</tr>
<tr>
<td>Disk space (for 100 discovered services)</td>
<td>• <strong>Minimum:</strong> 8 GB</td>
</tr>
<tr>
<td></td>
<td>• <strong>Recommended:</strong> 10 GB</td>
</tr>
</tbody>
</table>
Software requirements

<table>
<thead>
<tr>
<th>OS</th>
<th>Supported OS versions</th>
<th>Additional requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>32-bit and 64-bit versions:</td>
<td>For either version of the OS:</td>
</tr>
<tr>
<td></td>
<td>· Windows 2008 R2</td>
<td>· 32-bit version of the MID Server</td>
</tr>
<tr>
<td></td>
<td>· Windows Server 2016</td>
<td></td>
</tr>
<tr>
<td>Linux</td>
<td>· Red Hat Enterprise Edition Linux 6.6 or later</td>
<td>32-bit or 64-bit version of the MID Server</td>
</tr>
<tr>
<td></td>
<td>· CentOS Linux 6.6 or later</td>
<td></td>
</tr>
</tbody>
</table>

Role required: admin

The RCA MID Server supports the Service Analytics RCA process by hosting the RCA Learner and the real-time RCA query handler. On the RCA MID Server, the system builds models that support responses to root cause queries. The learner data on the RCA MID Server persists by default for a maximum of 90 days.

By default, the MID Server is set up as a dedicated MID Server for Service Analytics RCA, and an attempt to add additional supported applications to the same MID Server is prevented. It is recommended that Service Analytics Metrics is also implemented with its own dedicated Metrics MID Server. These recommendations ensure high level of performance. However, if needed, you can modify this default behavior and configure the RCA MID Server or the Metrics MID Server with additional supported applications. For information about modifying the behavior of the ALL option when selecting supported applications, see Configure applications included in ALL Applications.

1. Ensure that the MID Server is validated.
   For more information, see Validate the MID Server.
2. Navigate to MID Server > Servers.
3. Double-click the MID Server that you want to configure as an RCA MID Server.
4. Add the ServiceAnalytics application:
   a) At the center of the MID Server form, click Supported Applications.
   b) In the Supported Applications section click Edit.
   c) In the slushbucket select ServiceAnalytics and click the > add button.
   d) click Save.

If the MID Server needs to support ServiceAnalytics as well as one or more other applications, you can modify the definition of the ALL option to include these applications, and then select ALL in the slushbucket. ALL is the only option to which it is valid to add the ServiceAnalytics option. Performance might be compromised with these settings.

5. Add the RCA capability:
   a) At the center of the MID Server form, click Capabilities.
   b) In the Capabilities section click Edit.
c) In the slushbucket select **RCA** and click the ‘>’ add button.
d) click **Save**.

6. Click **Update**.

The RCA MID Server is automatically configured with a Discovery IP range set to 0.0.0.0-0.0.0.0.

Create a failover cluster for RCA. In this cluster, add the MID Servers that were configured for RCA.
For more information, see **Configure a MID Server cluster**.

**MIDSystem methods**

MIDSystem variables (referred to by the variable name ms.) provide a variety of methods to get information about the MID Server.

<table>
<thead>
<tr>
<th>Method summary</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>log(String message)</td>
<td>Logs the given message with a standard prefix to indicate that the message was generated by JavaScript.</td>
</tr>
<tr>
<td>getConfigParameter(String parameter name)</td>
<td>Returns the value of the named configuration parameter.</td>
</tr>
<tr>
<td>include(String script include)</td>
<td>Include the MID Server script include with the given name into the current context.</td>
</tr>
<tr>
<td>getName()</td>
<td>Returns the name of the MID Server.</td>
</tr>
<tr>
<td>getSysID()</td>
<td>Returns the sys_id of the MID Server.</td>
</tr>
<tr>
<td>toJavaScript(Object)</td>
<td>Converts the given Java object into the equivalent JavaScript object.</td>
</tr>
</tbody>
</table>

This example writes a message to the log:

```javascript
ms.log('Attempting to log in with user: ' + this.getParameter('user'));
```

**Synchronize a JAR file to MID Servers**

You can upload a JAR file to an instance and synchronize it to all MID Servers, or write custom probes that use the synchronized JAR file.

Role required: admin, agent_admin

The MID Server JAR File (ecc_agent_jar) table is domain separated. You can create versions of these policies that only a MID Server from the same domain can use. For instructions, see **Set up domain separation for MID servers**.

---

**Caution:** Synchronizing a JAR file with this procedure causes all MID Servers connected to the instance to restart automatically.

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.

5. In the Attachments dialog box, click **Browse** and select the file you want to attach.
   
   The platform attaches the JAR file to the record and restarts the MID Servers to synchronize the file. It is not necessary to update the record to attach the file.

Set the MID Server JVM memory size

The MID Server starts with a default JVM memory allocation, but you can modify this setting in the configuration file.

Role required: admin

In the base system, the MID Server JVM memory is set to 1024MB, which is configured in the `\agent\conf\wrapper-override.conf` file in the MID Server installation directory. This setting might not be appropriate for the way your organization uses the MID Server. If you want the MID Server to work harder, allocate more resources to it. If the MID Server is located in a small branch office and runs in an environment where memory allocation is shared between a print server, mail server, or web proxy server, the allocation might have to be reduced.

---

**Note:** For a complete list of minimum MID Server requirements, see [MID Server system requirements](#).

1. Open the `\ServiceNow\<MID Server name>\agent\conf\wrapper-override.conf` file in a text editor.
   
   For more information about this file, see [Installing Multiple MID Servers on a Single System](#).

2. Locate the following lines in the file:

   ```
   # OPTIONAL: Maximum Java Heap Size (in MB)
   # wrapper.java.maxmemory=1024
   ```

3. Edit the memory allocation.

4. Remove the comment tag (`#`) from the memory allocation parameter.

5. Save the file.

6. Restart the MID Server service.
Set MID Server thread use

If the MID Server is running on a host containing many other programs that must compete for CPU time, fewer threads than the default of 25 might be necessary.

Role required: admin

You can set the MID Server to use as few as 5 threads without issues. If the MID Server needs more speed, and the host is powerful enough or lightly loaded with other programs, raise the thread setting. The thread limit depends on the hardware and the operating system of the host. You might have to experiment to find the optimal value for your situation. The following general observations may be useful:

- Most MID Server tasks require file handles to do their job.
- Windows: On the Windows operating system, file handles are available in a fixed quantity. If you configure too many MID Server threads on a Windows host, the MID Server can consume all the file handles before approaching maximum CPU usage. This situation appears as an Out of file handles error in the MID Server log and indicates that the MID Server is trying to use too many threads.
- UNIX and Linux: UNIX and Linux hosts have a much different scheme for allocating file handles. Generally, you can increase MID Server thread use on these operating systems until the CPU of the host is overloaded. See your OS documentation for monitoring CPU usage.
- Each thread on the MID Server requires some memory. Exactly how much memory varies considerably from task to task and depends on the equipment being discovered. To increase the number of threads, you might have to increase the amount of memory that Java uses. If you configure insufficient memory, an Out of memory error appears in the MID Server log.

Follow the steps below to change the config.XML file. Alternatively, use the threads.max connection parameter.

1. Open the \agent\config.xml file using any text editor.
2. Locate the following lines:
   ```xml
   <!-- MID Server Threads -->
   <parameter name="threads.max" value="25"/>
   ```
3. Edit the value. Keep in mind the cautions described above.
4. Save the record.
5. Restart the MID Server service.

ECC queue retry policy

Define retry policies for outbound Web Services that are executed via the ECC Queue table.

Retry policies specify a matching error condition for ECC Queue input records that are a result or response of an output queue record, the interval for retry, and the maximum number of retries. Because it matches on the input queue record, the retry policies only work when an input ECC Queue record is expected, and therefore requires that the outbound messages are queued on the ECC Queue table as well. Advanced matching criteria may be specified using script.

Retry activity

The retry activity records document each attempt to retry the output queue record.

When the current policy is being retried, the Status of the activity will indicate Retrying. When all retries are exhausted, e.g. the maximum number of retries have occurred and the output queue
still failed, the **Status** field will indicate a Failed state. Otherwise, at anytime during the retry, if the request then becomes successful, it indicates Succeeded.

![Queue Retry Activity](image)

Queue Retry Activity

You may also display the current list of retry activities and their states by selecting the **Queue Retry Activity** module.
### Queue Retry Activities

<table>
<thead>
<tr>
<th>ID</th>
<th>Created</th>
<th>Policy</th>
<th>Input queue</th>
<th>Retry queue entry</th>
<th>Retry count</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2011-03-04 11:11:52</td>
<td>VZ Faulted</td>
<td><a href="https://putwebvortage.com:443/Trou">https://putwebvortage.com:443/Trou</a>...</td>
<td><a href="https://putwebvortage.com:443/Trou">https://putwebvortage.com:443/Trou</a>...</td>
<td>1</td>
<td>Retrying</td>
</tr>
<tr>
<td>4</td>
<td>2011-03-04 11:25:02</td>
<td>SOAPClient java net.UnknownHostException</td>
<td><a href="http://www.webservices.net/stockquote.asmx">http://www.webservices.net/stockquote.asmx</a></td>
<td><a href="http://www.webservices.net/stockquote.asmx">http://www.webservices.net/stockquote.asmx</a></td>
<td>1</td>
<td>Retrying</td>
</tr>
<tr>
<td>6</td>
<td>2011-03-04 11:33:12</td>
<td>SOAPClient java net.UnknownHostException</td>
<td><a href="http://www.webservices.net/stockquote.asmx">http://www.webservices.net/stockquote.asmx</a></td>
<td><a href="http://www.webservices.net/stockquote.asmx">http://www.webservices.net/stockquote.asmx</a></td>
<td>1</td>
<td>Retrying</td>
</tr>
<tr>
<td>8</td>
<td>2011-03-04 11:34:10</td>
<td>SOAPClient java net.UnknownHostException</td>
<td><a href="http://www.webservices.net/stockquote.asmx">http://www.webservices.net/stockquote.asmx</a></td>
<td><a href="http://www.webservices.net/stockquote.asmx">http://www.webservices.net/stockquote.asmx</a></td>
<td>3</td>
<td>Failed</td>
</tr>
<tr>
<td>15</td>
<td>2011-03-07 00:00:58</td>
<td>SOAPClient java net.UnknownHostException</td>
<td><a href="http://www.webservices.net/stockquote.asmx">http://www.webservices.net/stockquote.asmx</a></td>
<td><a href="http://www.webservices.net/stockquote.asmx">http://www.webservices.net/stockquote.asmx</a></td>
<td>1</td>
<td>Retrying</td>
</tr>
<tr>
<td>16</td>
<td>2011-03-07 00:01:29</td>
<td>SOAPClient java net.UnknownHostException</td>
<td><a href="http://www.webservices.net/stockquote.asmx">http://www.webservices.net/stockquote.asmx</a></td>
<td><a href="http://www.webservices.net/stockquote.asmx">http://www.webservices.net/stockquote.asmx</a></td>
<td>2</td>
<td>Retrying</td>
</tr>
<tr>
<td>17</td>
<td>2011-03-07 00:01:58</td>
<td>SOAPClient java net.UnknownHostException</td>
<td><a href="http://www.webservices.net/stockquote.asmx">http://www.webservices.net/stockquote.asmx</a></td>
<td><a href="http://www.webservices.net/stockquote.asmx">http://www.webservices.net/stockquote.asmx</a></td>
<td>3</td>
<td>Succeeded</td>
</tr>
<tr>
<td>18</td>
<td>2011-03-07 00:04:00</td>
<td>SOAPClient java net.UnknownHostException</td>
<td><a href="http://www.webservices.net/stockquote.asmx">http://www.webservices.net/stockquote.asmx</a></td>
<td><a href="http://www.webservices.net/stockquote.asmx">http://www.webservices.net/stockquote.asmx</a></td>
<td>1</td>
<td>Retrying</td>
</tr>
<tr>
<td>19</td>
<td>2011-03-07 00:04:29</td>
<td>SOAPClient java net.UnknownHostException</td>
<td><a href="http://www.webservices.net/stockquote.asmx">http://www.webservices.net/stockquote.asmx</a></td>
<td><a href="http://www.webservices.net/stockquote.asmx">http://www.webservices.net/stockquote.asmx</a></td>
<td>2</td>
<td>Retrying</td>
</tr>
<tr>
<td>20</td>
<td>2011-03-07 00:04:49</td>
<td>SOAPClient java net.UnknownHostException</td>
<td><a href="http://www.webservices.net/stockquote.asmx">http://www.webservices.net/stockquote.asmx</a></td>
<td><a href="http://www.webservices.net/stockquote.asmx">http://www.webservices.net/stockquote.asmx</a></td>
<td>3</td>
<td>Succeeded</td>
</tr>
<tr>
<td>21</td>
<td>2011-03-07 00:11:21</td>
<td>SOAPClient java net.UnknownHostException</td>
<td><a href="http://www.webservices.net/stockquote.asmx">http://www.webservices.net/stockquote.asmx</a></td>
<td><a href="http://www.webservices.net/stockquote.asmx">http://www.webservices.net/stockquote.asmx</a></td>
<td>1</td>
<td>Retrying</td>
</tr>
<tr>
<td>22</td>
<td>2011-03-07 00:11:31</td>
<td>SOAPClient java net.UnknownHostException</td>
<td><a href="http://www.webservices.net/stockquote.asmx">http://www.webservices.net/stockquote.asmx</a></td>
<td><a href="http://www.webservices.net/stockquote.asmx">http://www.webservices.net/stockquote.asmx</a></td>
<td>2</td>
<td>Succeeded</td>
</tr>
</tbody>
</table>
Retry policy example

This retry policy defines the matching criteria when an UnknownHostException response is received during a SOAPClient (outbound SOAP message invocation) call.

<table>
<thead>
<tr>
<th>Name:</th>
<th>SOAPClient java.net.UnknownHostException</th>
<th>Agent:</th>
<th>SOAPClient</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum retry:</td>
<td>3</td>
<td>Topic:</td>
<td></td>
</tr>
<tr>
<td>Retry interval:</td>
<td>Days 0 Hours 00:00:15</td>
<td>ECC name:</td>
<td></td>
</tr>
<tr>
<td>Active:</td>
<td>✓</td>
<td>Source:</td>
<td></td>
</tr>
<tr>
<td>Description:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**SOAP connection fails due to java.net.UnknownHostException**

Condition:

State: is error

Condition script:

```java
answer = current.error_string.toString().startsWith('java.net.UnknownHostException');
```

Default Queue Retry Policy

The policy will only match if the **Agent**, **Topic**, **ECC Name** (matches the **Name** field), and **Source** fields match that of an input ECC queue record. Additionally, the **Condition** and **Condition script** criteria will also have to match "State == error" and the **error_string** field contains the text `java.net.UnknownHostException`.

When these conditions are met, and an input record is matched, it will retry the originating output queue record after 15 seconds, and for a maximum of 3 times.

The MID Server ECC queue

The External Communication Channel (ECC) Queue is a connection point between an instance and the MID Server. Jobs that the MID Server needs to perform are saved in this queue until the MID Server is ready to handle them.

The MID Server subscribes to messages published by the Asynchronous Message Bus (AMB), which notifies the MID Server that it has pending tasks in the ECC queue. If a job exists in the ECC Queue
for that MID Server, the MID Server sets the status to "I'm working on it." When finished working on a requested job, the MID Server reports back to the ECC queue with the results.

Access the ECC queue

Open ECC queue records to see details of the details of a discovery. You can view ECC queue records while a discovery is in process.

Role required: admin

1. Navigate to one of the following:
   - Discovery > Output and Artifacts > ECC Queue
   - Discovery > Discovery Schedules > {schedule name} > {Discovery status record}
   - ECC > Queue
   - {Discovery Status record} > ECC Queue

2. Sort the list by any column that interests you, such as Created or Queue.
3. Open an ECC queue record (see table for field descriptions).

### ECC queue fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Input value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>The name of the external system that this messages is either from or to. If</td>
</tr>
<tr>
<td></td>
<td>the message is from or to a MID Server, the agent name is in the form mid.</td>
</tr>
<tr>
<td></td>
<td>server.xxx, where xxx is the name of a particular MID Server.</td>
</tr>
<tr>
<td>Topic</td>
<td>The name of the probe the MID server ran. If you are using a pattern for</td>
</tr>
<tr>
<td></td>
<td>discovery, HorizontalDiscoveryProbe appears.</td>
</tr>
<tr>
<td>Name</td>
<td>The actual command the probe ran. For example, if Topic is SSHCommand, then</td>
</tr>
<tr>
<td></td>
<td>the Name field contains the actual shell command to run. If you are using a</td>
</tr>
<tr>
<td></td>
<td>pattern for discovery, the following appears: Pattern Launcher: followed by</td>
</tr>
<tr>
<td></td>
<td>the name of the pattern and the multipage number.</td>
</tr>
<tr>
<td>Source</td>
<td>The IP address that the discovery is to run against. A few probes run run</td>
</tr>
<tr>
<td></td>
<td>against multiple IP addresses; in those cases, this field contains a</td>
</tr>
<tr>
<td></td>
<td>human-readable description.</td>
</tr>
<tr>
<td>Response to</td>
<td>This optional field contains a reference (sys_id) to the ECC Queue message</td>
</tr>
<tr>
<td></td>
<td>that this message is in response to. Discovery makes extensive use of this</td>
</tr>
<tr>
<td></td>
<td>field to track the hierarchy of messages that result from a given</td>
</tr>
<tr>
<td></td>
<td>scheduled Discovery. Click the record icon for the value in this field to</td>
</tr>
<tr>
<td></td>
<td>open the ECC Queue record for the activity that spawned the current probe</td>
</tr>
<tr>
<td></td>
<td>or sensor record.</td>
</tr>
<tr>
<td>Queue</td>
<td>An indicator of whether this message was an input message or an output</td>
</tr>
<tr>
<td></td>
<td>message.</td>
</tr>
</tbody>
</table>
### Field | Input value
--- | ---
**State** | The state of the current ECC queue record. States update automatically. See [The ECC queue for Discovery](#) for a brief overview of the process flow.

**Processed** | The time when this message was processed.

**Created** | The time when this message was created.

**Sequence** | The unique sequence number for this message. This value is automatically generated when an ECC Queue record is inserted. Its use is deprecated.

**Error string** | An error message, if an error occurred during processing. This field is hidden on the standard form unless there was an error.

**Payload** | The body of the message in XML format. The returned XML has a root tag of `<results>` containing one or more `<result>` tags and a single `<parameters>` tag. The parameters are simply an echo of those sent to the MID server in the probe; they vary from probe to probe, but in general they tell the probe the details of what it is to do and how it should behave. The result tags are the most interesting ones: they contain the actual data generated by the probe.

---

4. Click any of these related links:

| Related link | Description |
--- | ---|
**Run again** | Runs the probe again. You can re-run probes when you encounter a failed discovery or other unexpected results.|
**Go to CMDB item** | Open the CI record for the CI that was updated during the discovery.|
**Go to Sensor** | Open the record for the associated sensor.|

---

**Create an ECC Queue message**

One of the capabilities of the MID Server is to be able to send remote commands through the MID Server to the hosting device, and then gather the response.

This feature enables an administrator to issue remote commands directly from the ECC Queue without running Discovery.

1. Navigate to Discovery > Outputs and Artifacts > ECC Queue.
2. Click New.
3. Create a message with the following settings:

   - **Agent**: The name of the MID Server that executes the command
   - **Topic**: Command
   - **Name**: The actual command that you want to process. For Windows, this is expressed in a DOS command line structure. For Linux, the structure could be a bash command line entry.
   - **Queue**: Output

---
Payload: With proper XML tags, you can specify the command here instead of in the Name field. The advantage to this is that the command is not restricted by the Name field length of 120 characters. Use the following XML format for the command:

```xml
<parameters>
  <parameter name="name" value="ACTUAL_COMMAND_LINE"/>
</parameters>
```

The MID Server takes the XML entry in the ECC Queue and processes the command-line call locally. The STDOUT is returned to the ECC Queue as an Input queue entry.

**Note:** The command specified through the Payload field takes precedence over the command specified in the Name field.

### Access MID Server log entries from the ECC queue

You can access entries in the ECC Queue that show `agent0.log.0` logs and `wrapper.log` logs for an individual MID Server.

Role required: admin or mid_user

After you install and configure your MID Servers, there are several tasks you can perform to monitor the MID server, including viewing the logs to find warnings and errors.

1. Open a MID Server record.
2. Under Related Links, click Grab MID Logs.
   
   ECC queue records appear in the list using the following filter:
   
   - **Topic** is SystemCommand
   - **Source** is grabLog
   - **Agent** is {your MID Server}

   Only `agent0.log.0` and `wrapper.log` entries appear. These logs are also accessible in the `\agent\logs\` file path.
3. To open a log entry, click the link under the Created column.

### View MID Server statistics

You can access entries in the ECC Queue that belong to the `queue.stats` topic for an individual MID Server. Use these statistics for monitoring and troubleshooting your MID Server.

Role required: admin or mid_user

Useful MID Server statistics include memory and CPU usage data.

1. Open a MID Server record.
2. Under Related Links, click MID Statistics.
   
   ECC queue records appear in the list using the following filter:
   
   - **Topic** is queue.stats
   - **Agent** is {your MID Server}
**MID Server cluster configuration**

MID Server clusters enable multiple MID Servers with the appropriate capabilities to be grouped together for load balancing and fail-over protection.

**External data sources**

For performance and reliability reasons, these data sources should not be used with MID Server clusters:

- LDAP
- Export sets
- JDBC data sources

These external data sources should only be used with dedicated MID Servers.

**How clusters work**

MID Servers in clusters must be able to connect to the instance and to all the devices with which they are expected to communicate. If all MID Servers in a cluster are down, the discovery is canceled. Make sure all the MID Servers are added to any Access Control List (ACL) in use. MID Server clusters are managed by a business rule called MID Server Cluster Management, which checks to see if the MID Server assigned to a job in the ECC Queue belongs to a cluster.

**Load balancing**

If the cluster business rule determines that a MID Server is part of a load balancing cluster, the application using the MID Server automatically balances the work between the MID Servers in that cluster. It is good practice to put MID Servers with the same capabilities in a load balancing cluster.

**Fail-over protection**

MID Servers in a fail-over cluster each have a configured order that the platform uses to determine which MID Server to use next in case of failure. MID Servers in a fail-over cluster work independently and do not load balance with other MID Servers in that cluster (although they might also be members of load balancing clusters). When a MID Server fails, the MID Server Cluster Management business rule selects the highest available MID Server in the order to take over the work. The selected MID Server checks the ECC Queue and starts with jobs that are either Processing or Ready.

**Note:** MID Server clustering does not support the ECC queue topics **Command** or **SystemCommand**. If these commands are received, the clustered MID Servers do not redirect the ECC queue to another MID Server. The ECC queue records stay on the ECC queue without being processed.

Configure a fail-over MID Server with at least the same capabilities as the MID Server it is intended to relieve.

**Note:** If a MID Server fails while the **Shazzam probe** is running and auto-selection is configured, failover is not available. The Shazzam discovery stops. Discovery does not automatically choose another MID Server.
### MID Server cluster event

The following event is triggered when the platform cannot find a MID Server with the appropriate capabilities to replace a MID Server in a fail-over cluster. Use this event to create an email to notify appropriate users that the cluster has failed.

<table>
<thead>
<tr>
<th>Event</th>
<th>Table</th>
<th>Description</th>
<th>Business Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>mid_server.cluster.down</td>
<td>MID Server Cluster</td>
<td>A MID Server cluster has failed</td>
<td>MID Server Cluster Management</td>
</tr>
</tbody>
</table>

### Combining clusters

A MID Server can be added to both types of clusters at the same time. This diagram shows a scenario in which a MID Server from a load balancing cluster (MID Server D) is also present in a fail-over cluster. If MID Server D fails, MID Server E in the failover cluster is available to the load balancing cluster to perform the tasks previously assigned to MID Server D.

![MID Server failover example](image)

### Specifying a specific MID Server cluster

You can specify a specific MID Server cluster for a Discovery schedule. The discovery process uses that cluster only. You cannot chain clusters or specify a single MID Server that belongs to multiple clusters.

### Configure a MID Server cluster

Configure a cluster of MID Servers for either failover or load balancing.

Role required: admin

You can select a MID Server cluster from the Discovery Schedule form.

1. Navigate to MID Server > Clusters.
2. Click New.
3. Name the cluster and select the cluster type: Failover or Load Balance.
4. Right click in the header bar and select Save from the context menu.
5. Click Edit in the Includes MID Servers Related List.
6. Select appropriate MID Servers for this cluster from the slushbucket.

**Note:** All MID Servers in a cluster should have capabilities defined. Ensure that each MID Server has the appropriate capabilities for the job. A MID Server in a fail-over cluster must have the same capabilities (or expanded capabilities) as the MID Server it is expected to replace.

### MID Server capabilities

MID Server capabilities define the specific functions of a MID Server within an IP address range. Several applications, such as Discovery, Service Mapping, and Orchestration can use capabilities, IP ranges, and the supported application to narrow the pool of MID Servers it uses. At least one capability is required for each MID Server used by Orchestration. See [MID Servers for Orchestration](#) for more information.

The following capabilities are available by default with Discovery:

- SSH
- SNMP
- VMware
- PowerShell
- WMI
- SOAP
- REST
- JDBC
- Resolve DNS
- AWS
- Azure
- Cloud Management
- All

### MID Server capability values

Capabilities provided in the base system do not have a defined Value string. A MID Server configured to use a capability that has no Value can locate any device using that capability’s protocol. If a capability has a defined value, the MID Server using that capability finds only those devices using that protocol that match the value string exactly. The exception to this is the Resolve DNS capability, which is configured to resolve any DNS name into an IP addresses for devices whose names end with a specified domain name. The capability Value entered is automatically prefaced with a dot during processing to match domain syntax. This value can contain one or more sub-domains, but must include the end of the domain string. Matching devices must end with the identical syntax. The script for the Resolve DNS capability determines if a device name matches the criteria defined by **Value**.

### Scripted MID Server capability value matching

You can use value tests to create capabilities that find devices using values without requiring exact string matching. Action on these values is controlled by a user-defined script.

The Resolve DNS capability is provided in the base system and is configured to resolve DNS names into IP addresses for devices whose names end with a specified domain name. The capability Value entered is automatically prefaced with a dot during processing to match domain syntax. This value can contain one or more sub-domains, but must include the end of the domain string. Matching devices must end with the identical syntax. The script for the Resolve DNS capability determines if a device name matches the criteria defined by **Value**.
a match exists, the platform performs the address resolution automatically. For example, if the value for the Resolve DNS capability is `service-now.com`, the MID Server with this capability finds `lnxlab01.sandiego.service-now.com` and `dbsrv101.sanjose.service-now.com`. If the value is changed to `sandiego.service-now.com`, then the MID Server finds only `lnxlab01`.

**Note:** If Value in the Resolve DNS capability is blank, then all domains match.

To view the script for evaluating this capability, navigate to **MID Server > Capability Value Tests** and select **Resolve DNS** from the list.

**Configure MID Server capabilities**

A capability is required for each MID Server to work with Orchestration, Service Mapping, Cloud Management, and Service Analytics.

Role required: admin or sm_admin

1. Navigate to **MID Server > Capabilities**.
2. Select an existing capability. You can also select **ALL** to include all capabilities.
3. Create a new capability:
   a) Click New.
   b) Configure the value for a custom capability.
      An example is a capability for DOMAIN, with a value of service-now.
   c) Click Submit.

4. Click Edit in the MID Servers related list to add MID Servers to the capability.
5. Select one or more MID Servers for this capability from the slushbucket.
6. Click Save.

   The capability defined here also appears in the primary record for this MID Server.

**MID Server troubleshooting**

The Knowledge Base on Hi contains several articles to help you troubleshoot MID Server issues.

```| The MID Server Troubleshooting Guide |
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>KB0597571</td>
</tr>
<tr>
<td>Start here if you are experiencing symptoms such as the MID Server going down or not responding, or CIs being duplicated during discovery.</td>
</tr>
</tbody>
</table>
```

You can also see the following video on NOWsupport YouTube channel:

- **How to set up a MID Server**

**MID Server active issues**

The ServiceNow® instance has a dedicated table that publishes active issues with MID Servers and alerts administrators when a MID Server is in danger of exceeding its resources.

The MID Server Issue (ecc_agent_issue) table displays a number of common issues that a MID Server can experience, as they occur. Error checking processes attempt to pinpoint the most likely cause of the issue. Informative error messages name the affected MID Server and explain the possible cause of the issue. The ecc_agent_issue table retains its records for 30 days.

To access records in this table, navigate to MID Server > Server Issues.

Supported MID Server active issues:
- Bad user credentials after instance cloning.
- Approaching resource thresholds for CPU usage and JVM memory.
- Errors detected during **pre-upgrade testing**.
- User authentication and authorization failures.
- Network connectivity interruptions and role configuration errors.
Example MID Server Issue record

Active MID Server post-cloning credential issues

The system provides automatic processes to detect and notify you of possible MID Server credential issues after instance cloning.

During an instance clone, the MID Server (ecc_agent) table is not copied from the source instance, but the User (sys_user) table is copied. As a result, the source MID Server user credentials copied into the target instance might not match those used by the existing set of MID Servers used by the target. Bad credentials can cause those MID Servers to be down for the target instance. Processes on the instance notify you if a MID Server is down from suspected bad credentials following an instance clone.

Table for post-cloning credential issues

The MID Server Issue (ecc_agent_issue) table stores active MID Server issues after an instance clone. Records in this table show a MID Server's current state, evaluation times, and the issue.
source. For cases in which a MID Server for a cloned instance is down because of possible bad credentials, the Issue source is InstanceClone. Data from the MID Server Issue (ecc_agent_issue) table are displayed in a related list on a MID Server record. Records in this table are removed after 10 days, regardless of their state. Ongoing issues reappear as they occur.

Post-cloning cleanup script and scheduled jobs

A cleanup script called Bad MID Server credentials after clone runs on the target instance after cloning and calls a script include called BadMIDCredentialAfterClone. This script include schedules the execution of the following jobs on the Schedule Item (sys_trigger) table:

- BadMIDCredentialAfterClone-1: Runs 15 minutes after clone execution.
- BadMIDCredentialAfterClone-2: Runs 75 minutes after clone execution.

These jobs log to the MID Server Issue (ecc_agent_issue) table any MID Servers that existed on the target instance prior to the clone that are in the Down state. These MID Servers are not ready for normal processing and might be down due to invalid credentials resulting from the cloning process. The state of MID Servers added to the target instance after the clone is not evaluated.

Note: The MID Server log shows that the MID Server user associated with the target instance could not be authenticated or was missing the proper role.

Business rule that checks for bad credentials

The Check for bad MID credential after clone business rule monitors the MID Server (ecc_agent) table for MID Servers that are transitioning from Down to Up. If the business rule finds a MID Server making that transition, the rule attempts to find a matching MID Server in the MID Server Issue (ecc_agent_issue) table that has an issue source of InstanceClone and a state other than Resolved. If a match is found, the business rule updates the state of the MID Server in the (ecc_agent_issue) table to Resolved.

Resolving MID Server issues

The error message in the MID Server Issue (ecc_agent_issue) table names the affected MID Server user. This message appears each time the business rule runs and finds a MID Server that is down from suspected bad credentials:

MID Server not operational (status: Down), possibly due to recent clone. Verify credentials for logged in User 'local-midserver'.

Attempt to resolve the issue first by comparing the user's credentials with the credentials that the affected MID Server is expecting. If the credentials are incorrect, fix the problem and check the MID Server status again. If the credentials are correct, but the MID Server remains down, check the Knowledge Base for other possible causes.

MID Server resource threshold alerts

The instance displays warnings when a MID Server breaches its resource thresholds for CPU and JVM memory usage, enabling users to create email notifications or custom scripts when a breach occurs.

The MID Server Issue (ecc_agent_issue) table warns users when a MID Server exceeds configured thresholds of its allocated CPU and memory resources. These warnings are published before the MID Server experiences performance degradation or an out-of-memory error, enabling the administrator to increase resources and avoid downtime. Administrators can use a registered
event to send email notification to selected recipients, advising them of any threshold breaches, or to create a custom script to do some other type of work. The instance continues to update the MID Server Issue (ecc_agent_issue) table to keep unresolved issues current.

By default, CPU and memory threshold alerts are disabled and no alerts are published to the MID Server Issue (ecc_agent_issue) table. To enable both types of alerting, add these properties to the System Property (sys_properties) table, and then set their values to `true`:

- `mid.threshold.resource.breach.enable.cpu.alerts`
- `mid.threshold.resource.breach.enable.memory.alerts`

For details on adding system properties to the platform, see [Add a property using sys_properties.list](#).

**Evaluation process**

This processing occurs whether or not alerting is enabled:

1. Every 10 minutes, each MID Server transmits its CPU and memory consumption metrics to the instance. The instance inserts CPU metrics into the **Mean CPU used %** field of the ECC Agent Scalar Metrics (ecc_agent_scalar_metric) table and memory metrics into the **Max memory used %** field of the ECC Agent Memory Metrics (ecc_agent_memory_metric) table.

2. After a successful insert, the following business rules run on each table, invoking a script include that calls an appropriate function. Each function takes an average of the metric sets inserted into the tables, based on the configured sampling intervals.

    - **Update cpu mean on MID Server Status**: Calls the `MIDResourceThresholdBreach.checkCpuUsage()` script include.
    - **Update max memory on MID Server Status**: Calls the `MIDResourceThresholdBreach.checkMemoryUsage` script include.

Each function takes an average of the metric sets inserted into the tables, based on the configured thresholds and sampling intervals. The instance first looks at each MID Server for configuration parameters that set custom threshold values or sampling intervals for that MID Server. If no configuration parameters for these attributes are found, the instance looks in the System Properties (sys_properties) table for custom values to use. If no properties are found, the instance uses the default threshold and interval values from the code.

**Note:** Both the threshold percentages and the sampling intervals are configurable. See [Configuring thresholds and sampling intervals](#) for details.

**Alerting process**

When alerting for CPU or memory thresholds is enabled, this processing occurs:

1. If the aggregated average metric value equals or exceeds the configured percent threshold, the instance triggers the `mid.threshold.resource.breach` event. Administrators can use this event to create email notifications for threshold breach alerts or to create a custom script.

2. The instance inserts a record of the breach into the MID Server Issue (ecc_agent_issue) table with a **State** value of **New** and a **Count** of **1**, and then publishes a message containing all the pertinent details of the breach. An example of this message is **Mean CPU used % has exceeded threshold (96>=91) for a 40 minute interval span, occurring after start date 2017-01-11 14:25:19.** This message appears in the **Short description** field of
the MID Server issue form and in the event. You can copy any part of the message into your email notifications.

**MID Server issue states**

When the administrator first examines an issue in the MID Server Issue (ecc_agent_issue) table, the administrator can change the State of the issue to **Acknowledged** to indicate that the issue is being addressed. Each time the instance detects a breach, it attempts to match the breach with an existing issue. If a MID Server already has an issue record for that breach in a **State** of **New** or **Acknowledged**, the instance updates the **Last Detected** field with the current date/time and increments the **Count** field in the existing record. This prevents the creation of duplicate records in the MID Server Issue (ecc_agent_issue) table and records the number of times after the initial incident that the breach reoccurred. The administrator can increase MID Server resources gradually and watch the effect on the **Count** field. When the counter stops incrementing, the administrator knows that the MID Server has adequate resources. When the MID Server resource have been adjusted appropriately, the administrator sets the **State** to **Resolved**. If a new threshold breach is logged that matches a MID Server issue with a **State** of **Resolved**, the instance creates a new issue record.

---

**Note:** Any record in the MID Server Issue (ecc_agent_issue) table that has not been updated in 30 days is deleted, regardless of its state.

**Recommendations for resolving resource issues**

Administrators have the opportunity to resolve any resource issues with a MID Server when they receive notification of the event. Follow these recommendations for reducing the strain on MID Server resources:

- **JVM memory:**
  - Allocate more max memory to the MID Server. For more information, see [Set the MID Server JVM memory size](#).
  - Add additional MID Servers to share the workload. For more information, see [MID Server cluster configuration](#).
  - Reduce the amount of concurrent processing for the MID Server. This includes segmenting IP Address ranges into smaller segments for a Discovery schedule or loading smaller segments of data within an import job.

- **CPU:** Reduce the activity on the host or migrate the MID Server to a new host with more available resources.
### Tables used for resource threshold evaluation

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
</table>
| MID Server Issue (ecc_agent_issue)  | Stores data on various types of MID Server issues, including breaches of configured CPU and memory thresholds. Fields used for resource threshold breaches are:  
  - **count**: Number of times a previously reported threshold breach occurs, if the event is not marked `Resolved`.  
  - **last_detected**: Current date and time a threshold breach is detected. This field is updated each time a previously detected breach is found, if it is not marked `Resolved`.  
  - **message**: Descriptive message summarizing the conditions that triggered the threshold breach event. This message includes the actual percentage of CPU and memory calculated and the configured thresholds that were breached.  
  - **mid_server**: Name of the MID Server experiencing the resource threshold breach.  
  - **source**: The issue source for the breach. These are the possible sources:  
    - `CpuMIDResourceThresholdBreach`: CPU threshold issue sources.  
    - `MemoryMIDResourceThresholdBreach`: Memory threshold issue sources.                                                                                                                                                                                                                          |
| MID Server Status (ecc_agent_status)| Stores the percentages used for the CPU and memory resources, averaged over configurable intervals for each resource. The fields used are:  
  - Mean CPU used %  
  - Max Memory used %                                                                                                                                                                                                                                                                                                                                 |
| ECC Agent Scalar Metric (ecc_agent_scalar_metric) | Stores the CPU usage data inserted by each MID Server every 10 minutes. The table field used by resource threshold alerting is `mean`.                                                                                                                                                                                                                       |
| ECC Agent Memory Metric (ecc_agent_memory_metric) | Stores the memory usage data inserted by each MID Server every 10 minutes. The table field used by resource threshold alerting is `max_used_pct`.                                                                                                                                                                                                          |
Business rules that check for threshold breaches

<table>
<thead>
<tr>
<th>Business rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update cpu mean on MID Server Status</td>
<td>Runs after the MID Server inserts a record into the ECC Agent Scalar Metric (ecc_agent_scalar_metric) table. This business rule triggers the MIDResourceThresholdBreach script include function that evaluates threshold settings to determine if the MID Server has breached its configured CPU resource thresholds.</td>
</tr>
<tr>
<td>Update max memory on MID Server Status</td>
<td>Runs after the MID Server inserts a record into the ECC Agent Memory Metric (ecc_agent_memory_metric) table. This business rule triggers the MIDResourceThresholdBreach script include function that evaluates threshold settings to determine if the MID Server has breached its configured memory resource thresholds.</td>
</tr>
</tbody>
</table>

Configuring thresholds and sampling intervals

You can use the default threshold percentages and sampling intervals or configure custom values using either of these methods:

- Add system properties to the instance and change the default values for all MID Servers.
- Add configuration parameters to change the default resource values for individual MID Servers.

The system properties and the configuration parameters use the same names.

<table>
<thead>
<tr>
<th>Property/configuration parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mid.threshold.mean_cpu.aggregate_interval_span</td>
<td>Number of 10 minute units in the interval for sampling CPU usage data. The default interval is 30 minutes (3 x 10 min.)&lt;br&gt;&lt;br&gt;&lt;strong&gt;Default:&lt;/strong&gt; 3</td>
</tr>
<tr>
<td>mid.threshold.mean_cpu.percent</td>
<td>Usage percentage of the total CPU resources that initiates a threshold breach alert.&lt;br&gt;&lt;br&gt;&lt;strong&gt;Default:&lt;/strong&gt; 95</td>
</tr>
<tr>
<td>mid.threshold.mean_max_memory.aggregate_interval_span</td>
<td>Number of 10 minute units in the interval for sampling memory usage data. The default interval is 30 minutes (3 x 10 min.)&lt;br&gt;&lt;br&gt;&lt;strong&gt;Default:&lt;/strong&gt; 3</td>
</tr>
<tr>
<td>mid.threshold.mean_max_memory.percent</td>
<td>Usage percentage of the total memory resources that initiates a threshold breach alert.&lt;br&gt;&lt;br&gt;&lt;strong&gt;Default:&lt;/strong&gt; 95</td>
</tr>
</tbody>
</table>
MID Server resource reporting

The MID Server dashboard contains two reports that give you views into the consumption of CPU and JVM memory resources. These reports show usage over the previous 30 days.

- **Avg Percentage of CPU Used:** Trending the daily average on CPU usage helps illustrate the amount of CPU processing that the MID Server host consumes. MID Servers deployed on the same host will report the same CPU usage.

- **Avg Percentage of Max Memory Used:** The maximum used percentage (max_used_pct) is a useful metric for determining if the MID Server has enough memory resources. This metric is a percentage of the max used memory over the total available memory. Trending this over time provides a visualization of how much memory is needed by the MID Server.

MID Server user connectivity issues

The instance writes issues involving MID Server user logins and network connectivity to the MID Server Issue (ecc_agent_issue) table and creates events you can use to send email notifications or to write custom scripts.

Records in the MID Server Issue (ecc_agent_issue) table can provide insight into why your MID Server user cannot log in or why a MID Server cannot connect to the instance. The system displays records for connectivity problems in this table that include informative error messages suggesting possible causes. By default, a scheduled job called MIDUserConnectivity runs every four hours and launches the MIDUserConnectivity script include to evaluate MID Server connection activity. Records in the MID Server Issue (ecc_agent_issue) table reflect the status of MID Server login attempts and connectivity at the time the scheduled job runs.

From the perspective of the instance, the MID Server is **Down** when:

- User authentication fails
- User authorization fails.
- Network issues prevent MID Server from establishing a TCP/IP connection.

**Note:** To associate a user with a MID Server, navigate to the servicenow/<mid server name>/agent/config.xml file and enter the user credentials in the mid.instance.username and mid.instance.password parameters. Make sure to restart the MID Server to activate your changes.

How issues are logged

User authentication failures and authorization issues are logged automatically to the MID Server agent log file. The message for both is the same: **User cannot be authenticated or is missing the proper roles.** If the issue is related to authorization, the agent.log file shows the list of missing roles.

When debugging is enabled, MID Server issues are logged to the system log (syslog) and are available for display in either a summary or a detailed format. You can also change the sampling interval from the default 4 hours to something shorter for tracking your remediation efforts. For instructions on enabling and configuring debugging for MID Server user issues, see [Test remediation efforts for MID Server user connectivity issues](#).

Data provided

When the instance encounters user connectivity issues, it opens a record in the MID Server Issue (ecc_agent_issue) table.

© 2019 ServiceNow, Inc. All rights reserved.
Example user authentication error message

The MID Server Issue table contains these fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last detected</td>
<td>Date and time the issue was last detected.</td>
</tr>
<tr>
<td>Short description</td>
<td>Contents of the generated message that specifies a possible issue with the named user or the MID Server.</td>
</tr>
<tr>
<td>MID Server</td>
<td>Empty in the Jakarta release.</td>
</tr>
<tr>
<td>Issue source</td>
<td>The process that identified the issue. For all issues with MID Server user connectivity, the source is MIDUserConnectivity.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>State</td>
<td>The current state of the issue. Possible states are:</td>
</tr>
<tr>
<td></td>
<td>· <strong>New</strong>: Starting state when the instance creates the issue.</td>
</tr>
<tr>
<td></td>
<td>· <strong>Acknowledged</strong>: State set when the administrator first examines the issue.</td>
</tr>
<tr>
<td></td>
<td>· <strong>Resolved</strong>: Ending state, set by the instance, indicating that the issue has been resolved. If the scheduled job does not encounter the issue when it runs again, the instance automatically sets this value.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain associated with the MID Server user account.</td>
</tr>
<tr>
<td>Count</td>
<td>Number of times an issue has been detected. Each time the scheduled job runs and encounters the same issue, it increments this field.</td>
</tr>
</tbody>
</table>

**User authentication failure**

The credentials that the instance uses to authenticate a MID Server user are configured in the MID Server Configuration Parameters (ecc_agent_config) table. If the MID Server user attempts to log into the instance with invalid credentials, the instance rejects the connection, and writes the `login.failed` event to the Events (sysevents) table for the user. Administrators can use this event to create email notifications for authentication failure or to create a custom script.

**Note:** If user authentication fails, user authorization is not attempted.

**User accounts associated with a MID Server**

Either of the following messages in the MID Server Issue (ecc_agent_issue) table indicate authentication failure for user accounts that are associated with a MID Server:

- Login authentication failure for User `<user name>` associated with 1 down MID Server. Check password on MID server.
- Login authentication failure for User `<user name>` associated with `<n>` down MID Servers. Check password on MID servers.

The necessary conditions for these messages to appear are:

- The **Status** field in the MID Servers (ecc_agent) table that is associated with the MID Server indicates that the MID Server is **Down**.
- The user identified in the MID Server Configuration Parameters (ecc_agent_config) table is the user that one or more MID Servers is configured to use for authentication and authorization when connecting to the instance. The record in the (ecc_agent_config) table must have these values:
  - Parameter name (param_name) field set to `mid.instance.username`.
  - Value (value) field set to the user’s name, corresponding to the User ID (user_name) field in Users (sys_user) table.
- The Events (sysevent) table contains posts showing that the last login attempt associated with the user failed during the scheduled time period. The record created in the (sysevent) table contains these field values:
- Event Name (name) field is set to \texttt{login.failed}.
- Parm1 (parm1) field is set to the user’s name.

\begin{center}
\textbf{Note:} The MID Server (mid_server) field in the MID Server Issues (ecc_agent_issue) table is empty (=NULL).
\end{center}

### User accounts with the mid-server role not associated with a MID Server

The following message appears when a user with the mid_server role who is not associated with a MID Server fails to authenticate: \texttt{Login authentication failure for User <user name> with mid_server role not associated with a MID Server.}

The necessary conditions for this message to appear are:

- The User Roles (sys_user_has_role) table contains a record linking the sys_id associated with the user record stored in the (sys_user) table, with the sys_id associated with the mid_server role record stored in the (sys_user_role) table.
- The user is not identified in the MID Server Configuration Parameters (ecc_agent_config) table as the user whom one or more MID Servers are configured to use for authentication and authorization when connecting to the instance.
- The Events (sysevent) table contains posts showing that the last login attempt associated with the user failed during the scheduled time period.

- The (sysevent) table contains a record with the Event Name (name) field set to \texttt{login.failed}.
- The Parm1 (parm1) field is set to the user’s name, corresponding to the User ID (user_name) field in Users (sys_user) table.

\begin{center}
\textbf{Note:} The MID Server (mid_server) field in the MID Server Issues (ecc_agent_issue) table is empty (=NULL).
\end{center}

### User authorization failure

The user authorization check occurs after the MID Server has successfully authenticated on the instance. In this step, the system ensures that the user account associated with a MID Server is granted the minimum roles required. A SOAP web service called MIDServerCheck performs the role checking on the instance. If the MID Server user has the proper roles, the connection is allowed and a \texttt{login} event is written to the Events (sysevents) table. If the user does not have the proper roles, the instance writes a \texttt{login.authorization.failed} event to the Events (sysevents) table. This event provides a comma separated list of the user’s missing roles. Administrators can use this event to create email notifications for authorization failure or to create a custom script.

Authorization can fail if a user is missing the mid_server role or any of the important SOAP roles, as in these cases:

- If the user has the soap_script role, the MIDServerCheck SOAP web service runs to check for the appropriate MID Server roles. If the user lacks the mid_server role or any of the other SOAP roles, authorization fails, and the \texttt{login.authorization.failed} event is created.
- If the user is missing the soap_script role, that user is not authorized to launch the MIDServerCheck SOAP web service, which checks for all required MID Server roles. Authorization fails, but the \texttt{login.authorization.failed} event is not created. When this occurs,
the instance displays this message: **Connectivity of MID Server user <user name> cannot be detected by the instance.**

Users associated with one or more down MID Servers

Either of the following messages in the MID Server Issue (ecc_agent_issue) table indicate authorization failure for user accounts that are associated with a MID Server that is Down:

- Login authorization failure for User <user name> associated with 1 down MID Server. Re-assign mid_server role to grant all required roles.
- Login authorization failure for User <user name> associated with <n> down MID Servers. Re-assign mid_server role to grant all required roles.

The **MIDUserConnectivity** script include identifies active users associated with one or more down MID Servers whose last login attempt within the reporting period failed user authorization. This message is generated when user authorization failures are detected and reported by the MIDServerCheck scripted web service. However, user authorization failures are not reported for users who are not assigned the soap_script role. Should this occur, problems with the user are reported by the network connectivity message.

This message appears in the MID Server Issue (ecc_agent_issue) table when:

- The user may or may not have the mid_server role.
- The user is identified in the MID Server Configuration Parameters (ecc_agent_config) table as the user whom one or more MID Servers are configured to use for authentication and authorization when connecting to the instance.
- The Events (sysevent) table contains posts showing that the last login attempt associated with the user failed during the scheduled time period. The (sysevent) table contains a record with these settings:
  - Event Name (name) field set to login.authorization.failed.
  - Parm1 (parm1) field set to the user’s name, corresponding to the User ID (user_name) field in Users (sys_user) table.

**Note:** The MID Server (mid_server) field in the MID Server Issues (ecc_agent_issue) table is empty (=NULL).

Users with the proper role not associated with a MID Server

The following message appears when a user with the mid_server role who is not associated with a MID Server fails authorization: **Login authorization failure for User <user name> with mid_server role not associated with a MID Server.**

This message is generated when user authorization failures are detected in which the user account, with the mid_server role, is not identified as a configured MID Server user in the (ecc_agent_config) table. It is possible that the user account was associated with a MID Server at the time of the failure.

This message appears in the MID Server Issue (ecc_agent_issue) table when:

- The user has the mid_server role. The User Roles (sys_user_has_role) table has a record linking the sys_id associated with the user record stored in the (sys_user) table, with the sys_id associated with the mid_server role record stored in the (sys_user_role) table.
- The user is not identified in the MID Server Configuration Parameters (ecc_agent_config) table as the user whom one or more MID Servers are configured to use for authentication and authorization when connecting to the instance.
The Events (sysevent) table contains posts showing that the last login attempt associated with the user failed during the scheduled time period. The (sysevent) table contains a record with these settings:

- Event Name (name) field set to `login.authorization.failed`.
- Parm1 (parm1) field set to the user’s name, corresponding to the User ID (user_name) field in Users (sys_user) table.

**Note:** The MID Server (mid_server) field in the MID Server Issues (ecc_agent_issue) table is empty (=NULL).

### Network issues

A network issue can prevent the MID Server from connecting to the instance’s TCP/IP server to begin a session. In this case, the instance marks the MID Server as **Down**, because the instance failed to receive the MID Server heartbeat within the prescribed 5 minute interval.

#### Users associated with down MID Servers who have not attempted to log in

Either of the following messages in the MID Server Issue (ecc_agent_issue) table name users associated with MID Servers who have not attempted to log in during the reporting period:

- **User <user name> is associated with 1 down MID Server. No login attempts within reporting period.**
- **User <user name> is associated with <n> down MID Servers. No login attempts within reporting period.**

The MIDUserConnectivity script include reports active users associated with down MID Servers where network connectivity cannot be detected by the instance.

This message appears in the MID Server Issue (ecc_agent_issue) table when:

- The user may or may not have the mid_server role.
- The user is identified in the MID Server Configuration Parameters (ecc_agent_config) table as the user which one or more MID Servers are configured to use for authentication and authorization when connecting to the instance.
- There are no login attempts, either failed or successful, recorded in the Events (sysevent) table for the user during the scheduled reporting period.

**Note:** The MID Server (mid_server) field in the MID Server Issues (ecc_agent_issue) table is empty (=NULL).

#### Users not associated with MID Servers who have not attempted to log in

The following message appears when a user with the mid_server role who is not associated with a MID Server has not attempted to login during the configured reporting interval: **User <user name> with mid_server role is not associated with a MID Server. No login attempts within reporting period.**

The MIDUserConnectivity script include reports active users with the mid_server role not associated with a MID Server, where connectivity cannot be detected by the instance.

This message appears in the MID Server Issue (ecc_agent_issue) table when:

- The user has the mid_server role. The User Roles (sys_user_has_role) table has a record linking the sys_id associated with the user record stored in the (sys_user) table, with the sys_id associated with the mid_server role record stored in the (sys_user_role) table.
- The user is not identified in the MID Server Configuration Parameters (ecc_agent_config) table as the user whom one or more MID Servers are configured to use for authentication and authorization when connecting to the instance.
- There are no login attempts, either failed or successful, recorded in the Events (sysevent) table for the user during the scheduled reporting period.

**Note:** The MID Server (mid_server) field in the MID Server Issues (ecc_agent_issue) table is empty (=NULL).

### Configuration issues

Any of the following messages, discussed above, can indicate a configuration issue:

- Login authentication failure for User `<user name>` with mid_server role not associated with a MID Server.
- Login authorization failure for User `<user name>` with mid_server role not associated with a MID Server.
- User `<user name>` with mid_server role is not associated with a MID Server. No login attempts within reporting period.

These are some common configuration errors:

- An administrator neglected to associate the user record with the MID Server record as shown in the MID Server Configuration Parameters (ecc_agent_config) table. This table is read-only and cannot be updated directly. To associate a user with a MID Server, configure the user name and password in the MID Server's `config.xml` file and restart the MID Server.
- During the process of reconfiguring a MID Server to use a different account for TCP/IP connection, the administrator has not yet removed the mid_server role from the account or deleted the account.
- A multipurpose user account was created and granted a large number of roles, including the mid_server role, although this account was never intended to be used as a MID Server account.

### User who successfully authenticates and authorizes but might not need mid_server role

The following message appears when a user with the mid_server role who is not associated with a MID Server successfully logs in: **User `<user name>` with mid_server role successfully connected but not associated with a MID Server. The mid_server role should be reserved for MID Server use only.**

The MIDUserConnectivity script include reports active users with the mid_server role who are not identified as a configured MID Server user, and whose last login attempt was successful during the scheduled time period. This message suggests that the user’s credentials are being used by a system administrator or a process that is not running on a MID Server. The assumption here is that the mid_server role should only be used for applications deployed to a MID Server. The presence of this message reminds the system administrator to remove extraneous mid_server roles from user accounts that do not require them.

This message appears in the MID Server Issue (ecc_agent_issue) table when:

- The user has the mid_server role.
- The user is not identified in the MID Server Configuration Parameters (ecc_agent_config) table as the user whom one or more MID Servers are configured to use for authentication and authorization when connecting to the instance.
- The Events (sysevent) table contains posts showing that the last login attempt associated with the user succeeded during the scheduled time period. The (sysevent) table contains a record with these settings:

© 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 (name) field set to `login`.
- Parm1 (parm1) field set to the user’s name, corresponding to the User ID (user_name) field in Users (sys_user) table.

**Note:** The MID Server (mid_server) field in the MID Server Issues (ecc_agent_issue) table is empty (=NULL).

### Test remediation efforts for MID Server user connectivity issues
After attempting to resolve a user connectivity issue that appears in the MID Server Issue (ecc_agent_issue) table, you can test your remediation efforts without having to wait until the next scheduled reporting period by shortening the sampling interval.

**Role required:** admin

Reconfigure the sampling interval using this procedure and then examine the results in the MID Server Issue (ecc_agent_issue) table. You can set any time span for the sample, but you should define a window of not less than 5 minutes, since this is the default interval of the MID Server heartbeat that reports its status. The recommended method for configuring a shorter sampling interval is to copy and modify the code from the MIDUserConnectivity scheduled job, and then run it manually in the background script utility.

**Caution:** Avoid editing the script in the MIDUserConnectivity schedule record. If you make any change to this record, it will not be updated when you upgrade the instance.

1. Navigate to **System Definition > Scheduled Jobs**.
2. Open the MIDUserConnectivity scheduled job.
3. Copy this line from the **Run this script** field:
   ```java
   MIDUserConnectivity(0).checkConnectivity(4 * (60 * 60 *1000));
   ```
   This code sets the 4 hour sampling interval in milliseconds and turns debugging off with the `MIDUserConnectivity(0)` value.
4. Navigate to **System Maintenance > Scripts - Background**.
5. Paste the code from the scheduled job into the **Run script** field.
6. Set the sampling interval to 5 minutes by changing the time calculation to `(5 * 60 *1000)`.
   The modified command looks like this: `MIDUserConnectivity(0).checkConnectivity (5 * 60 *1000);`
7. Click **Run script**.
8. Open the record of the MID Server that had the issue and select the **MID Server Issues** related list.
   The issue is updated as follows:
   - If the issue persists, the **Count** column is incremented, and the **Last detected** column shows the current date and time.
   - If the issue no longer exists, the system changes the **State** to **Resolved**.
9. Optionally, you can enable debugging by selecting a level, and then run the script again to see the breakdown for each condition evaluated.
   Use these settings to select a debugging level:
   - For a summary view, enter `MIDUserConnectivity(1)`.
   - For a detailed view, enter `MIDUserConnectivity(2)`.

For details about the type of debugging information provided, see [Interpreting MID Server user debugging output](#).
Interpreting MID Server user debugging output

Debugging output from the system log is available in either a summary or detailed view for MID Server user issues, but must be enabled manually.

To enable debugging and display all connectivity issues in either of the available formats, you must run a method manually on your instance. For instructions on enabling debugging, see Test remediation efforts for MID Server user connectivity issues. For information about each error condition and how records are created in the MID Server issue (ecc_agent_issue) table, see MID Server user connectivity issues.

Available formats

You can configure the instance to generate a simple summary of the issue or a detailed output that identifies users and MID Servers. Summaries provide a quick look at the issue conditions, by count, while the detailed view allows you to examine roles, MID Server associations, and login activity by named users.

In this summary example of an authorization issue, the instance evaluates each condition and indicates how many users met that condition. You can see that a MID Server is down and that one of two users configured for a MID Server failed authorization. Because this is a summary, neither the MID Server nor the users are named.

Sample summary debug output

```
[0:00:00.014] Script completed in scope global: script

*** Script: Log Object: MIDUserConnectivity: jobSchedulerDateTime
Java Object: com.glide.glideobject.GlideDateTime = 2017-02-21 17:35:08
Java Object: java.lang.String = 2017-02-21 09:55:08
*** Script: MIDUserConnectivity: found (1) user(s) with the mid_server role defined
*** Script: MIDUserConnectivity: found (1) down MID Servers with a configured 'mid.instance.username' parameter
*** Script: MIDUserConnectivity: found (2) configured MID Server UserIds
*** Script: MIDUserConnectivity: found (0) user(s) with the MID Server role NOT also associated with a configured MID Server user
*** Script: MIDUserConnectivity: found (0) user(s) whose most recent login attempt during the reporting period failed
*** Script: MIDUserConnectivity: found (1) user(s) whose most recent login attempt during the reporting period failed due to user authentication
*** Script: MIDUserConnectivity: found (0) user(s) whose most recent login attempt during the reporting period succeeded
*** Script: MIDUserConnectivity: found (0) configured MID Server users where connectivity to the MID by the instance can not be detected
*** Script: MIDUserConnectivity: found (1) new message(s) skipped by the auto-resolver
*** Script: MIDUserConnectivity: processing completed
```

Authentication failure

When a MID Server user cannot authenticate on the instance, the system displays these error messages in the detailed output:

- Login authentication failure for User <user name> associated with 1 down MID Server. Check password on MID server.
• Login authentication failure for User <user name> associated with <n> down MID Servers. Check password on MID servers.
• Login authentication failure for User <user name> with mid_server role not associated with a MID Server.

In this example, three users with the mid_server role, midserver2, local-midserver, and ardis.maison, failed to authenticate. Two of these users were configured for MID Servers that were Down, and the other user was not configured for any MID Servers. Each of these users has an authentication failure and is named in the appropriate error message.
ServiceNow Jakarta Now Platform Capabilities

*** Script: Log Object: MIDUserConnectivity; activeUserIDsWithMIDServerRole
Array of 3 elements
[0]: string = ardis.maison
[1]: string = midserver2
[2]: string = local-midserver

*** Script: Log Object: MIDUserConnectivity; downMIDServerConfiguredUserIDs
Array of 2 elements
[0]: string = midserver2
[1]: string = local-midserver

*** Script: Log Object: MIDUserConnectivity; userXMIUserServerMap
Object
acris.maison: Object
  ssys_domain: string = global
  mid_server: Array of 0 elements
midserver2: Object
  ssys_domain: string = global
  mid_server: Array of 1 elements
  [0]: string = 7fa7f1541b503200be67d3b3217f6a9
local-midserver: Object
  ssys_domain: string = global
  mid_server: Array of 2 elements
  [0]: string = 7b8a6f141f422f2d65db217f699b
  [1]: string = 1ae2867b102a6b709599f0b9764f9
  [2]: string = 1a2b7c0f301e70790e9f764f9
  string = uno_rba_mig
  7fa7f1541b503200be67d3b3217f6a9
  string = MIDServer44VM-10.11.145.205-2-local
  7b8a6f141f422f2d65db217f699b
  string = xano_rba_mig

*** Script: Log Object: configuredMIDServerUserIDs
Array of 2 elements
[0]: string = midserver2
[1]: string = local-midserver

*** Script: Log Object: MIDUserConnectivity; activeUserIDsWithMIDServerRoleNotAssociatedWithConfiguredMIDServer
Array of 1 element
[0]: string = ardis.maison

*** Script: Log Object: MIDUserConnectivity; userIDsWithIssues
Array of 3 elements
[0]: string = midserver2
[1]: string = local-midserver
[2]: string = ardis.maison

*** Script: Log Object: MIDUserConnectivity; userIDsMostRecentLoginAttemptsFailed
Array of 3 elements
[0]: string = midserver2
[1]: string = local-midserver
[2]: string = ardis.maison

*** Script: Log Object: MIDUserConnectivity; userIDsMostRecentLoginAttemptsAuthorizationFailed
Array of 0 elements

*** Script: Log Object: MIDUserConnectivity; userIDsMostRecentLoginAttemptsSuccessful
Array of 0 elements

*** Script: Log Object: MIDUserConnectivity; userIDsWhereConnectivityToMIDCanBeDetectedByInstance
Array of 0 elements

*** Script: Log Object: MIDUserConnectivity; doNotAutoResolveMessage
Array of 3 elements
[0]: string = Login authentication failure for User midserver2 associated with 1 down MID Server. Check password on MID server.
[1]: string = Login authentication failure for User local-midserver associated with 2 down MID Servers. Check password on MID servers.
[2]: string = Login authentication failure for User ardis.maison with mid_server role not associated with a MID Server.

*** Script: MIDUserConnectivity; processing completed
MID Server ID map

The debugging output lists all MID Servers that are marked as Down and maps them to their user accounts by the MID Server sys_id. This map includes all user accounts that have the mid_server role, whether or not they are associated with a MID Server. If there are no Down MID Servers, the map is not displayed in the debugging output.

The map is presented in three sections:

- User accounts not associated with any MID Servers.
- User accounts associated with Down MID Servers, identified by their sys_id.
- The sys_id of each Down MID Server, identified by name.

Authorization failure

If a user is missing any of the required roles, the instance generates these authorization failure messages:

- Login authorization failure for User <user name> associated with 1 down MID Server. Re-assign mid_server role to grant all required roles.
- Login authorization failure for User <user name> associated with <n> down MID Servers. Re-assign mid_server role to grant all required roles.
- Login authorization failure for User <user name> with mid_server role not associated with a MID Server.

In this example, three users with the mid_server role, midserver2, local-midserver, and ardis.maison have failed authorization. One user is not associated with any MID Server, but the other two users are. The system has logged an authorization failure, indicating that the user is missing at least one critical role. To see what roles are missing, look at the comma separated list in
the Parm2 field in the `login.authorization.failed` event record. This record is the most recent login attempt in the Event (sysevent) table for the user account within the reporting period.
Network issues

Network issues may exist for these users who are associated with MID Servers, but who have not attempted to log in during the reporting period:

- User `<user name>` is associated with 1 down MID Server. No login attempts within reporting period.
- User `<user name>` is associated with `<n>` down MID Servers. No login attempts within reporting period.

Network issues may also exist for these users who are NOT associated with MID Servers, and who have not attempted to log in during the reporting period: **User `<user name>` with mid_server role is not associated with a MID Server. No login attempts within reporting period.**

In this example, no login attempts have been detected for `midserver2`, `local-midserver`, and `ardis.maison`, all of whom have the mid_server role. Two of those users are associated with MID Servers that are marked **Down**. The other user is not associated with any MID Server. None of these users has attempted to log in to the system within the configured reporting interval. The system assumes that these users would make an attempt to log in unless network issues prevented them from doing so.

**Note:** By default, the sampling period is 4 hours. However, during debugging or remediation, the sampling period can be reset to a value that matches the MID Server heartbeat interval of 5 minutes, or greater.
**Script:** Log Object: MIDUserConnectivity; activeUserIdsWithMIDServerRole

Array of 3 elements
[0]: string = aridis.maison
[1]: string = midserver2
[2]: string = local-midserver

**User with mid_server role**

**Script:** Log Object: MIDUserConnectivity; downMIDServerConfiguredUserIds

Array of 2 elements
[0]: string = midserver2
[1]: string = local-midserver

**Users associated with Down MID Servers**

**Script:** Log Object: MIDUserConnectivity; userINMIDServerMap

Object

mid_server: Object
  sys_domain: string = global
  mid_servers: Array of 0 elements
  local-midserver: Object
    sys_domain: string = global
    mid_servers: Array of 1 elements
      [0]: string = 7aaf7154b0232001b78cd3b217669a6
  is_midserver: Object
    sys_domain: string = global
    mid_servers: Array of 2 elements
      [0]: string = 7aaf7154b0232001b78cd3b217669a6
      [1]: string = 1a2c23c303232001b78cd3b217669a6

**Users configured to MID Server**

**Script:** Log Object: MIDUserConnectivity; activeUserIdsWithMIDServerRoleNotAssociatedWithConfiguredMIDServer

Array of 1 elements
[0]: string = aridis.maison

**User not associated with MID Server**

**Script:** Log Object: MIDUserConnectivity; userINMIDServerIssues

Array of 3 elements
[0]: string = midserver2
[1]: string = local-midserver
[2]: string = aridis.maison

**Users with issues**

**Script:** Log Object: MIDUserConnectivity; userIDMostRecentLoginAttemptFailed

Array of 0 elements

**Script:** Log Object: MIDUserConnectivity; userIDMostRecentLoginAttemptAuthorizationFailed

Array of 0 elements

**Script:** Log Object: MIDUserConnectivity; userIDMostRecentLoginAttemptSuccessful

Array of 0 elements

**Script:** Log Object: MIDUserConnectivity; userIDWhereConnectivityNoMIDCanBeDetectedByInstance

Array of 3 elements
[0]: string = midserver2
[1]: string = local-midserver
[2]: string = aridis.maison

**Users with no network activity**

**Script:** Log Object: MIDUserConnectivity; doNotAutoResolveMessages

Array of 3 elements
[0]: string = User midserver2 associated with 1 down MID Server, no login attempts within reporting period.
[1]: string = User local-midserver associated with 2 down MID Servers, no login attempts within reporting period.
[2]: string = User aridis.maison with mid_server role not associated with a MID Server, no login attempts within reporting period.

**Network issues involving these users**

**Script:** MIDUserConnectivity; processing completed
Configuration issues

Any of the following messages can indicate a user configuration issue:

- Login authentication failure for User <user name> with mid_server role not associated with a MID Server.
- Login authorization failure for User <user name> with mid_server role not associated with a MID Server.
- User <user name> with mid_server role successfully connected but not associated with a MID Server. The mid-server role should be reserved for MID Server use only.
- User <user name> with mid_server role is not associated with a MID Server. No login attempts within reporting period.

In this example, a user with the mid_server role has logged in successfully within the configured sampling interval. However, this user is not configured for a MID Server and might have the role in error.

```plaintext
*** Script: Log Object: MIDUserConnectivity: activeTenantRolesWithMidServerRole
Array of 3 elements
   [0]: string = alice.maison
   [1]: string = midserver2
   [2]: string = inactive-midserver
*** Error: MIDUserConnectivity: no MIDServers are down
*** Error: Log Object: configuredMIDServerUserIDS
Array of 2 elements
   [0]: string = midserver2
   [1]: string = inactive-midserver
*** Error: Log Object: MIDUserConnectivity: activeTenantRolesWithoutAssociatedMIDConfiguredMIDServer
Array of 1 elements
   [0]: string = alice.maison
*** Error: Log Object: MIDUserConnectivity: userInKnownTenantLoginAttemptAuthorizationFailed
*** Error: Log Object: MIDUserConnectivity: userInKnownTenantLoginAttemptSuccessful
Array of 1 elements
   [0]: string = alice.maison
*** Error: Log Object: MIDUserConnectivity: userInKnownTenantNotDetectedByMIDServer
Array of 8 elements
*** Error: Log Object: MIDUserConnectivity: demarcatingEnabledMessages
Array of 1 elements
   [0]: string = User alice.maison with mid_server role is not associated with a MID Server. The mid_server role should be reserved for MID Server use only.
*** Script: MIDUserConnectivity: processing completed
```

Detailed debugging log for MID Server user account login
Orchestration

ServiceNow® Orchestration extends the workflow engine to manage processes and to automate things outside of a ServiceNow instance.

Orchestration is available as a separate subscription from the rest of the ServiceNow platform. See Activate Orchestration for details.

**Explore**
- Introduction to Orchestration
- Orchestration release notes
- Orchestration applications
- Orchestration ROI
- Orchestration examples

**Set up**
- Activate Orchestration
- MID Servers for Orchestration
- Available activity packs
- Setup Client Software Distribution

**Administer**
- List of Orchestration plugins
- Orchestration Runtime plugin

**Use**
- Orchestration activity packs
- Password Reset and Password Change applications
- Client Software Distribution

**Develop**
- Orchestration activity designer
- Orchestration custom activity templates
- Client software distribution extension framework
- Developer training

**Troubleshoot and get help**
- Ask or answer questions in the Orchestration forum
- Search the HI knowledge base for known error articles
- Contact ServiceNow Technical Support

**Introduction to Orchestration**

Orchestration automates simple or complex multi-system tasks on remote services, servers, applications, and hardware.

An Orchestration process can cross all management disciplines and interact with hosted services and all types of infrastructure elements. These capabilities provide a powerful system for managing IT and Business processes quickly and reliably.

Orchestrated solutions aide collaboration among teams by providing reusable data and versioning for both the workflows and the activities within them. Subject matter experts can create activities that are reusable to numerous workflow developers. When an activity requires a change, developers can see the downstream implication of the change immediately by knowing which workflows use the activity. Well-designed orchestrations never fail and apply human tasks to address errors as they arise.

**Orchestration tools**

Orchestration can make calls outside of a ServiceNow instance, directly to web services or through a MID Server to systems within corporate firewall. Orchestration also enables the creation reusable activities that wrapper Java Script functions for manipulating things inside the platform. Orchestration extends the Workflow editor by providing these features:

- **Activity packs** containing ready-to-use activities.
- **Activity Designer**, which enables developers to create custom activities without an over dependence to create scripts to orchestrate to third-party systems.
- Ability to create activity packs using Scoped Applications.
- A **Databus** for following the flow of data across orchestration activities.

© 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.
Orchestration Core provides entitlements to use specific applications:

**Client Software Distribution**

An application that automates software delivery from the Service Catalog. Provides OOB support for SCCM. Partner solutions support Macs using JAMF. Other third-party solutions provide support through the extension framework.

**Password Reset**

An application for users to reset their password in Active Directory. It can expand to communicate with other third-party systems.

**Orchestration ROI**

Enables users to evaluate estimated costs and actual costs for tasks, automate these tasks, and track the ROI of these tasks.

**Systems that Orchestration can automate**

Orchestration can automate tasks such as employee onboarding, user access rights, server management, managed file transfers, and Security Operations Orchestration activities. For example, you might use the Active Directory and Exchange activities provided in the base Orchestration system to set up network accounts and mailboxes for new employees.

If Orchestration does not provide the activities you need for an integration, create the necessary activities using the templates in the Orchestration Activity Designer. The external systems that Orchestration can automate for:

- Any system exposing web services (SOAP, REST)
- Any system accessible from the command line (such as a UNIX system accessible through SSH, a Windows system enabled for PowerShell remoting or WMI)
- Numerous proprietary services: Windows Active Directory, Microsoft Exchange mail servers, InfoBlox, and F5 Networks.

**Note:** For a full list of Activity Pack service offerings, see Orchestration Core Activity Packs.

- Any filesystem accessible by SFTP
- Any database with a compliant JDBC driver
- Additional Activity Packs are also available with other ServiceNow products, such as Security Operations
Orchestration capabilities

Orchestration workflow

When an Orchestration activity starts within a workflow, Orchestration launches a probe and writes a probe record to the ECC Queue. The workflow pauses as the MID Server picks up the
request and executes the probe. When the probe reports back, the workflow resumes as the results are analyzed. The workflow can exit or continue at this point.

**Orchestration workflow**

**Orchestration video tutorial**

Watch the introductory video for Orchestration.

**Activate Orchestration**

The Orchestration (com.snc.runbook_automation) plugin is available as a separate subscription from the rest of the ServiceNow platform.

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>
<tr>
<td>Reason/Comments</td>
<td>Any information that would be helpful for the ServiceNow personnel activating the plugin such as if you need the plugin activated at a specific time instead of during one of the default activation windows.</td>
</tr>
</tbody>
</table>

Note: Plugins are activated in two batches each business day in the Pacific timezone, 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**.

### List of Orchestration plugins

This table lists all plugins available for Orchestration and their dependencies. These Orchestration plugins are available for purchase or can be requested as part of your Orchestration subscription. Contact your account representative for details.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Dependencies</th>
</tr>
</thead>
</table>
| Orchestration (com.snc.runbook_automation)              | Main plugin for the Orchestration feature. This plugin extends Workflow to automate operations with external systems. Use this plugin to orchestrate business services, applications, and infrastructure. This plugin automates operations such as deployments, configurations, and information gathering. Orchestration can automate Web Services and uses MID Servers to execute commands on devices inside an enterprise's network. | • Orchestration - ROI  
• Orchestration - Runtime                                      |
| Orchestration - Active Directory (com.snc.orchestration.ad) | Installs the **Active Directory** activity pack. These activities create, delete, and manage objects in Windows Active Directory. | Orchestration                  |
| Orchestration - Asset Lease Management (com.snc.orchestration.asset_lease_management) | Provides the software lease functionality for Client Software Distribution. Allows users to specify start and end dates of software leases and to request an extension of a lease.  
**Note:** This plugin is not automatically enabled when Orchestration is active. | None                         |
| Orchestration - Azure Active Directory (com.snc.orchestration.azure.ad) | Installs the **Azure AD** activity pack. These activities automate employee onboarding and offboarding functions on Azure Active Directory and manage Office 365 licensing. | Orchestration                  |
| Orchestration - Client Software Distribution (com.snc.orchestration.client_sf_distribution) | Allows the **distribution of software** from the service catalog using third party distribution systems, such as Microsoft System Center Configuration Manager (SCCM)  
**Note:** This plugin is not automatically enabled when Orchestration is active. | • Orchestration - System Center Configuration Manager  
• Orchestration - Asset Lease Management  
• Service Catalog Scoped API  
• Software Asset Management |
<p>| Orchestration - Exchange (com.snc.orchestration.exchange) | Installs the <strong>Exchange</strong> activity pack. These activities manage Microsoft Exchange mail systems. | Orchestration                  |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orchestration - F5 network management (com.snc.orchestration.f5)</td>
<td>Installs the F5 Network Management activity pack. These activities configure elements of an F5 load balancer, including pools, pool members, and the virtual servers contained in the pool.</td>
<td>Orchestration</td>
</tr>
<tr>
<td>Orchestration - Infoblox DDI Activity Pack (com.snc.orchestration.infoblox)</td>
<td>Installs the Infoblox DDI activity pack. These activities support Infoblox DDI management.</td>
<td>Orchestration</td>
</tr>
<tr>
<td>Orchestration - PowerShell (com.snc.orchestration.powershell)</td>
<td>Installs the PowerShell activity pack. These activities control and automate the administration of Windows machines and applications, using the Windows .NET Framework.</td>
<td>Orchestration</td>
</tr>
<tr>
<td>Orchestration - Probe (com.snc.orchestration.probe)</td>
<td>Installs the Probe activity pack. These activities run ServiceNow® probes on target hosts to return specific information.</td>
<td>Orchestration</td>
</tr>
<tr>
<td>Orchestration - ROI (com.snc.runbook_automation.roi)</td>
<td>Installs an Orchestration application that estimates savings resulting from automated tasks in an instance and computes actual savings. Orchestration - ROI is activated automatically with a base Orchestration subscription.</td>
<td>Performance Analytics, Cost Management</td>
</tr>
</tbody>
</table>
| Orchestration - ROI Premium (com.snc.runbook_automation.roi_premium) | Installs a premium dashboard that displays detailed reports on calculated savings for automated tasks over time. The Orchestration - ROI Premium plugin requires purchase and activation of the Performance Analytics - Premium plugin to display its reports.  

**Note:** This plugin is not automatically enabled when Orchestration is active. | Orchestration - ROI, Performance Analytics - Premium |
| Orchestration - Runtime (com.snc.runbook_automation.runtime) | Enables other applications on the ServiceNow® platform to distribute and use orchestration content without requiring an Orchestration subscription. The Orchestration - Runtime plugin displays the Orchestration activities shipped with these applications in the Workflow Editor and allows customers to modify the activities without requiring an Orchestration license. | Workflow Runtime Engine, Core Automation |
| Orchestration - SFTP (com.snc.orchestration.sftp) | Installs the SFTP File Transfer activity pack. These activities manage files and directories on an SFTP server and move files from one SFTP server to another. | Orchestration |
| Orchestration - SSH (com.snc.orchestration.ssh) | Installs the SSH activity pack. These activities read, write, and copy files, and reset user passwords on Linux computers. | Orchestration |
| Orchestration - System Center Configuration Manager (com.snc.orchestration.sccm_mgmt) | Installs the System Center Configuration Manager (SCCM) activity pack. These activities manage software deployments and collections on an SCCM server. | Orchestration |
Orchestration Runtime plugin

The Orchestration - Runtime plugin enables other applications on the ServiceNow® platform to automate tasks, without requiring an Orchestration subscription.

The Orchestration - Runtime plugin can be activated as part of another plugin or application. It is used by strategic technology partners and ServiceNow applications to distribute activity packs to customers who may not own Orchestration. For example, the Security Incident Response Management (SIRM) application provides orchestration content, which includes activities that are available from the Packs tab in the Workflow Editor. Customers who purchase SIRM can consume and modify the activities that SIRM ships without having to purchase an Orchestration license.

Included with the plugin

The Orchestration - Runtime plugin provides access to the Packs and Data tabs in the Workflow Editor, which gives users access to custom activities for their applications and allows them to reuse data from the databus. This plugin does not provide access to custom Orchestration activity packs or to the activity designer. The Custom tab in the Workflow Editor is not available without an Orchestration subscription.
Dependencies

The Orchestration - Runtime plugin is activated by these application plugins:

- Security Incident Response Orchestration
- Service Release Automation

Access to activities

Custom activities shipped with ServiceNow® applications are available in the Packs tab of the Workflow Editor for use in workflows. To edit these activities, navigate to Orchestration > Activity Designer Activities and select the activity you want to modify. For information about the provider templates used to create these activities, see Orchestration custom activity templates.

List of Orchestration activities

Orchestration provides the following activities for use in workflows:

Several Orchestration activities have been rewritten as scoped activities using the activity designer and grouped into activity packs. Other non-scoped activities are deprecated and may or may not appear in the Workflow Editor. However, all deprecated activities still function in existing workflows that use them.

Global activities

These activities run in the global scope only. Any activities you create in the global scope are organized in the Global category in the Packs and Custom tabs in the Workflow Editor.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Server Alive</td>
<td>Runs a command (including shell scripts) on a Linux or UNIX computer via SSH to validate whether the target system is alive.</td>
</tr>
</tbody>
</table>

Active Directory (AD) activities

All AD Orchestration activities were rewritten in the Geneva release as scoped activities and are available in the Active Directory activity pack. All previous version AD activities that were built on activity definitions are deprecated and are unavailable for use in new workflows.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create AD Object</td>
<td>Creates a user account in Windows Active Directory when a user account is created in a ServiceNow instance.</td>
</tr>
<tr>
<td>Disable AD User Account</td>
<td>Marks a Windows Active Directory user account disabled, making it inactive.</td>
</tr>
<tr>
<td>Enable AD User Account</td>
<td>Enables a Windows Active Directory user account, making it active.</td>
</tr>
<tr>
<td>Query AD</td>
<td>Retrieves entries from the Windows Active Directory based on a search filter.</td>
</tr>
</tbody>
</table>
### ServiceNow

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove AD Object</td>
<td>Deletes a user account from Windows Active Directory.</td>
</tr>
<tr>
<td>Reset AD User Password</td>
<td>Resets the password of a user account in Windows Active Directory.</td>
</tr>
<tr>
<td>Change AD User Password</td>
<td>Changes the password of a user account in Windows Active Directory.</td>
</tr>
<tr>
<td>Update AD Object</td>
<td>Updates a user account in Windows Active Directory.</td>
</tr>
<tr>
<td>Is AD Account Locked</td>
<td>Determines if an Active Directory user account is locked.</td>
</tr>
<tr>
<td>Unlock AD Account</td>
<td>Unlocks a locked Active Directory user account.</td>
</tr>
</tbody>
</table>

### Azure AD

All these activities are scoped and part of the Azure AD activity pack. They do not have legacy versions.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add User to Group</td>
<td>Adds a user to an existing security group in Azure Active Directory.</td>
</tr>
<tr>
<td>Assign User License</td>
<td>Assigns an extra Office 365 software license to the named user.</td>
</tr>
<tr>
<td>Create User</td>
<td>Creates a user for the Azure Active Directory tenant.</td>
</tr>
<tr>
<td>Delete User</td>
<td>Deletes the named user's account from the Azure Active Directory tenant.</td>
</tr>
<tr>
<td>Get User Info</td>
<td>Returns the named user's information from the Azure Active Directory.</td>
</tr>
<tr>
<td>Remove User from Group</td>
<td>Removes an existing user from a security group in Azure Active Directory.</td>
</tr>
<tr>
<td>Remove User License</td>
<td>Revokes the specified Office 365 software license for the named user.</td>
</tr>
<tr>
<td>Reset User Password</td>
<td>Changes the named user's Azure Active Directory password.</td>
</tr>
</tbody>
</table>

### F5 Network Management activities

All these activities are scoped and part of the F5 Network Management activity pack. They do not have legacy versions.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add F5 Pool</td>
<td>Creates the load balancer pool.</td>
</tr>
<tr>
<td>Check F5 Pool</td>
<td>Checks the status of a pool to validate whether it is available to accept traffic.</td>
</tr>
</tbody>
</table>
## ServiceNowJakarta Now Platform Capabilities

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Delete F5 Pool</strong></td>
<td>Deletes an F5 pool.</td>
</tr>
<tr>
<td><strong>Add F5 Pool Member</strong></td>
<td>Adds a member to an F5 pool.</td>
</tr>
<tr>
<td><strong>Get F5 Pool Member</strong></td>
<td>Returns the pool members and verifies the pool status.</td>
</tr>
<tr>
<td><strong>Delete F5 Pool Member</strong></td>
<td>Deletes an F5 pool member.</td>
</tr>
<tr>
<td><strong>Add F5 Virtual Server</strong></td>
<td>Adds a virtual server.</td>
</tr>
<tr>
<td><strong>Modify F5 Virtual Server</strong></td>
<td>Configures a virtual server assigned to an F5 pool with irules and a vlan.</td>
</tr>
<tr>
<td><strong>Delete F5 Virtual Server</strong></td>
<td>Deletes a virtual server from an F5 pool.</td>
</tr>
<tr>
<td><strong>Add F5 Profile to Virtual Server</strong></td>
<td>Adds a profile to a virtual server assigned to an F5 pool.</td>
</tr>
</tbody>
</table>

### Infoblox activities

All these activities are scoped and part of the Infoblox DDI activity pack. They do not have legacy versions.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DHCP Reserve IP v4 Address Range</strong></td>
<td>Reserves an IP address range for DHCP use.</td>
</tr>
<tr>
<td><strong>DHCP Delete IP Reservation</strong></td>
<td>Deletes IP reservations in DHCP using either an IPv4 or IPv6 address range.</td>
</tr>
<tr>
<td><strong>DHCP List IP Reservations</strong></td>
<td>Generates a list of all the DHCP range reservations on a specific Infoblox server.</td>
</tr>
<tr>
<td><strong>List DNS C-records</strong></td>
<td>Retrieves all canonical (CNAME) records from a specified Infoblox server.</td>
</tr>
<tr>
<td><strong>Register DNS A-record</strong></td>
<td>Creates a DNS A record on a specified Infoblox server.</td>
</tr>
<tr>
<td><strong>Register DNS C-Record</strong></td>
<td>Creates a DNS canonical (CNAME) record on a specified Infoblox server.</td>
</tr>
<tr>
<td><strong>List DNS Record</strong></td>
<td>Generates a list of all the DNS entries on a specific Infoblox server.</td>
</tr>
<tr>
<td><strong>DNS Delete</strong></td>
<td>Deletes DNS records of any type from in Infoblox server, such as C and A records.</td>
</tr>
<tr>
<td><strong>IPAM Register IP Address</strong></td>
<td>Registers an IP address in a network using Infoblox IPAM.</td>
</tr>
<tr>
<td><strong>IPAM Reserve IP Address</strong></td>
<td>Reserves an IP address in a network using Infoblox IPAM.</td>
</tr>
<tr>
<td><strong>IPAM List IP Reservations</strong></td>
<td>Returns an array of all IP Address within the named Infoblox Server.</td>
</tr>
<tr>
<td><strong>IPAM Delete</strong></td>
<td>Deletes an IP Address within a named Infoblox server.</td>
</tr>
<tr>
<td><strong>Create Network</strong></td>
<td>Creates networks on a specified Infoblox server.</td>
</tr>
<tr>
<td><strong>Get Network Details</strong></td>
<td>Retrieves the information about a specific network on an Infoblox server.</td>
</tr>
<tr>
<td><strong>Delete Network</strong></td>
<td>Deletes a network from an Infoblox server.</td>
</tr>
<tr>
<td>Activity</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>List Registered Networks</td>
<td>Retrieves all the networks associated with an Infoblox server.</td>
</tr>
</tbody>
</table>

**Microsoft Exchange activities**

All Exchange Orchestration activities were rewritten in the Geneva release as scoped activities and are available in the Exchange activity pack. All previous version Exchange activities that were built on activity definitions are deprecated and are unavailable for use in new workflows.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Address List</td>
<td>Creates an address list that acts as an alias for emailing all users in the group. This alias cannot be used to manage user permissions.</td>
</tr>
<tr>
<td>Delete Address List</td>
<td>Removes an existing address list from an Exchange server.</td>
</tr>
<tr>
<td>Get Address List</td>
<td>Retrieves all attributes from the specified Exchange address list.</td>
</tr>
<tr>
<td>Move Address List</td>
<td>Moves an Exchange address list to another location in the address hierarchy.</td>
</tr>
<tr>
<td>Set Address List</td>
<td>Modifies an Exchange address list.</td>
</tr>
<tr>
<td>Update Address List</td>
<td>Adds or removes users from the specified address list and immediately applies any cached address list changes to the server.</td>
</tr>
<tr>
<td>Create Mailbox</td>
<td>If a user does not exist, creates a new Active Directory user and associated Exchange mailbox.</td>
</tr>
<tr>
<td>Delete Mailbox</td>
<td>Deletes the Exchange mailbox of an Active Directory user.</td>
</tr>
<tr>
<td>Disable Mailbox</td>
<td>Disables the mailbox associated with a specified Active Directory account.</td>
</tr>
<tr>
<td>Enable Mailbox</td>
<td>Creates a mailbox for an existing Active Directory user.</td>
</tr>
<tr>
<td>Get Mailbox</td>
<td>Gets the mailbox for the specified user or all mailboxes on an Exchange server.</td>
</tr>
<tr>
<td>Set Mailbox</td>
<td>Modifies the settings of an existing Exchange mailbox.</td>
</tr>
</tbody>
</table>

**PowerShell activities**

These PowerShell activities were rewritten as scoped activities and are available in the PowerShell activity pack. All previous version PowerShell activities that were built on activity definitions are deprecated and are unavailable for use in new workflows.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Windows App</td>
<td>Installs an application on a Windows target machine.</td>
</tr>
<tr>
<td>Join Domain</td>
<td>Joins a Windows machine to a domain.</td>
</tr>
</tbody>
</table>
## ServiceNow July blogger round-up

### Activity

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uninstall Windows App</td>
<td>Uninstalls an application from a Windows target machine.</td>
</tr>
<tr>
<td>Change Service State</td>
<td>Starts or stops a Windows service on a remote system.</td>
</tr>
</tbody>
</table>

### Probe activities

These probe activities were rewritten as scoped activities and are available in the Probe activity pack. All previous versions of these activities that were built on activity definitions are deprecated and are unavailable for use in new workflows.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resolve DNS Name</td>
<td>Resolves an IP address or a fully qualified domain name (FQDN) into one or more IP addresses.</td>
</tr>
<tr>
<td>SNMP Query</td>
<td>Queries an SNMP device.</td>
</tr>
</tbody>
</table>

### SCCM activities

All these activities are scoped and part of the SCCM activity pack. They do not have legacy versions.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add to Device Collection</td>
<td>Adds a device to a Microsoft System Center Configuration Manager (SCCM) device collection.</td>
</tr>
<tr>
<td>Add to User Collection</td>
<td>Adds a user to a Microsoft System Center Configuration Manager (SCCM) user collection.</td>
</tr>
<tr>
<td>Get Applications</td>
<td>Returns a list of all the applications available on a Microsoft System Center Configuration Manager (SCCM) server.</td>
</tr>
<tr>
<td>Get Deployments</td>
<td>Returns the list of deployments performed by Orchestration using a Microsoft System Center Configuration Manager (SCCM) server.</td>
</tr>
<tr>
<td>Get Device Collections</td>
<td>Returns the list of available device collections on a Microsoft System Center Configuration Manager (SCCM) host.</td>
</tr>
<tr>
<td>Get User Collections</td>
<td>Returns the list of available user collections on a Microsoft System Center Configuration Manager (SCCM) host.</td>
</tr>
<tr>
<td>Remove from Device Collection</td>
<td>Removes a device from a Microsoft System Center Configuration Manager (SCCM) device collection.</td>
</tr>
<tr>
<td>Remove from User Collection</td>
<td>Removes a user from a Microsoft System Center Configuration Manager (SCCM) user collection.</td>
</tr>
</tbody>
</table>
### SSH activities

These SSH activities were rewritten as scoped activities and are available in the SSH activity pack. The SSH activities not converted to scoped activities were moved to the Orchestration - Deprecated category, but are still available for all workflows.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File Copy</strong></td>
<td>Copies a file on a Linux or Unix computer, via SSH.</td>
</tr>
<tr>
<td><strong>File Read</strong></td>
<td>Reads a file on a Linux or Unix computer, via SSH.</td>
</tr>
<tr>
<td><strong>File Write</strong></td>
<td>Writes a file on a Linux or UNIX computer.</td>
</tr>
<tr>
<td><strong>File Replace String</strong></td>
<td>Finds and replaces a string in a file on a Linux or UNIX computer.</td>
</tr>
<tr>
<td><strong>Files Compare</strong></td>
<td>Compares two files on a Linux or Unix computer, via SSH.</td>
</tr>
<tr>
<td><strong>Reset Linux User Password</strong></td>
<td>Resets the password for a given user on a Linux computer.</td>
</tr>
<tr>
<td><strong>Secure Copy</strong></td>
<td>Copies a file from one host to another, without storing the copied file on the MID Server.</td>
</tr>
</tbody>
</table>

### SFTP activities

All these activities are scoped and part of the SFTP File Transfer activity pack. They do not have legacy versions.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Copy File</strong></td>
<td>Copies a file from an SFTP server (source host) to another SFTP server (target host).</td>
</tr>
<tr>
<td><strong>Create Directory</strong></td>
<td>Creates a directory on an SFTP server.</td>
</tr>
<tr>
<td><strong>Get File List</strong></td>
<td>Returns a list of files from a given directory and its subdirectories on an SFTP server (source host).</td>
</tr>
<tr>
<td><strong>Remove File or Directory</strong></td>
<td>Removes a file or a directory on an SFTP server, including subdirectories, when configured.</td>
</tr>
<tr>
<td><strong>Rename File or Directory</strong></td>
<td>Renames a file or directory to a new name on an SFTP server.</td>
</tr>
<tr>
<td><strong>Set File Attributes</strong></td>
<td>Sets common file attributes, such as timestamps, size, permissions, and UID/GID, for a file or directory on an SFTP server.</td>
</tr>
</tbody>
</table>
Deprecated activities

These activities have been removed from the Workflow Editor and are not available for new workflows, but continue to work normally in existing workflows. You can reactivate the deprecated activity or duplicate the functionality of a deprecated activity as a scoped activity by recreating it using the activity designer.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run Probe</td>
<td>Launches a MID Server probe on behalf of a document.</td>
</tr>
<tr>
<td>SOAP Request</td>
<td>Executes a SOAP request on a target server. The SOAP Message activity replaces this activity.</td>
</tr>
<tr>
<td>Run Command</td>
<td>Runs a command (including shell scripts) on a Linux or UNIX computer.</td>
</tr>
<tr>
<td>Run SCP</td>
<td>Uses Secure Copy Protocol (SCP) to copy a file from one computer to another, including the directory in which the file resides. The Secure Copy activity replaces the Run SCP activity.</td>
</tr>
<tr>
<td>Run Powershell</td>
<td>Executes Windows PowerShell commands on a MID Server.</td>
</tr>
</tbody>
</table>

Available activity packs

Activity packs are available with your subscription to Orchestration.

Role required: admin

The following activity packs are available and active with your Orchestration subscription:

- Orchestration - Active Directory (com.snc.orchestration.ad)
- Orchestration - Azure Active Directory (com.snc.orchestration.azure.ad)
- Orchestration - Exchange (com.snc.orchestration.exchange)
- Orchestration - SFTP (com.snc.orchestration.sftp)
- Orchestration - Infoblox DDI Activity Pack (com.snc.orchestration.infoblox)
- F5 Network Management activity pack (com.snc.orchestration.f5)
- Orchestration - SSH (com.snc.orchestration.ssh)
- Orchestration - PowerShell (com.snc.orchestration.powershell)
- Orchestration - System Center Configuration Manager (com.snc.orchestration.sccm_mgmt)

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 timezone, 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

<table>
<thead>
<tr>
<th>Reason/Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any information that would be helpful for the ServiceNow personnel activating the plugin such as 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.

**Deprecated Orchestration activities**

These Orchestration activities have been deprecated.

**Run Probe**

The Run Probe activity launches a MID Server probe on behalf of a document. All Orchestration activities that launch a probe on a target machine are based on the Run Probe activity. Your ServiceNow instance must have access to a MID Server configured to use SSH to run this activity.

**Attention:** This activity is deprecated and is unavailable for new workflows. To replace the functionality of this probe, use the **Probe activity template** to create a custom activity. Workflows from a previous release that use the Run Probe activity can continue to do so.

**Run Probe input variables**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probe</td>
<td>Select a MID Server probe from the list. This is the name of the probe as it appears in the <code>discovery_probes</code> table.</td>
</tr>
<tr>
<td>Source for probe</td>
<td>Enter the IP address of the host system against which the probe runs (the probe's target).</td>
</tr>
<tr>
<td>Sensor script</td>
<td>The script to run using the results of the probe. The output from the probe is contained in a variable called <code>output</code>. Any error from the probe is contained in a variable called <code>error</code>.</td>
</tr>
</tbody>
</table>

**SOAP Request**

The SOAP Request activity executes a SOAP request on a target server.

**Attention:** This activity is deprecated and is replaced by the **SOAP Message workflow activity** activity. Workflows from a previous release that use the SOAP Request activity can continue to do so. However, this activity is not available for new workflows.

**SOAP Request input variables**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOAP URL</td>
<td>The SOAP endpoint.</td>
</tr>
<tr>
<td>Username</td>
<td>User name for basic authentication credentials.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for basic authentication credentials.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Envelope Script</td>
<td>Script for setting up parameters for the web service.</td>
</tr>
<tr>
<td>Sensor Script</td>
<td>The script to execute after the request has been made and a response has been received.</td>
</tr>
</tbody>
</table>

**Reactivate a deprecated activity**

Orchestration activities that were converted to activity packs are deprecated for upgraded and new instances but can be reactivated for use in new workflows.

Role required: workflow_admin, admin

**Note:** Reactivation of deprecated activities for use in new workflows is discouraged. Legacy activities cannot use the unique features of the scoped applications, such as reuse of data from the `databus` and input variable testing.

1. Navigate to **Workflow > Administration > Activity Definitions**.
2. In the list of activities, clear the condition `Category ! = deprecated` from the filter.

3. Open the definition record for the activity you want to reactivate.
4. Select the **What to Display** tab.
5. In the **Category** field, replace the value `deprecated` with another category. This can be an arbitrary string.
6. Click **Update**.

The system creates a new category using the value provided and reactivates the activity, which becomes available in the **Core** tab of the workflow editor.

**SOAP Message workflow activity**

The **SOAP Message** activity uses SOAP messages defined in the System Web Services plugin and can call the messages using a MID Server.

Your instance must have access to a MID Server configured to use SOAP.

**Input variables**

**SOAP Message activity input variables**

<table>
<thead>
<tr>
<th>Field</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOAP Message</td>
<td>soap_message</td>
<td>The SOAP Message defined under the System Web Services plugin's Outbound SOAP Message (sys_soap_message) table. (System Web Services &gt; Outbound &gt; SOAP Message)</td>
</tr>
<tr>
<td>Field</td>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SOAP Message Function</td>
<td>soap_message_function</td>
<td>The function to call that is defined in the SOAP Message. Functions are listed in the <em>SOAP Message Functions</em> related list in each SOAP Message record.</td>
</tr>
<tr>
<td>SOAP Endpoint</td>
<td>soap_endpoint</td>
<td>Endpoint to use instead of the <em>SOAP endpoint</em> value in the SOAP Message Function record. Leave this field blank to use the defined endpoint in the SOAP Message Function record.</td>
</tr>
</tbody>
</table>
| Variables                | variables      | Variables to substitute into the SOAP Envelope defined in the SOAP Message Function record. Use this format for the string:  

\[
\text{name1=value1, name2=value2, ...}
\]

If either the name or value contains a comma or equal sign, escape these characters with a backslash.                                                                                                                                 |
| Use MID Server           | use_midserver  | Check box for using a MID Server to send the SOAP message. A MID Server might be necessary to reach an endpoint within a firewall or a sub-network that is not visible from the instance. If this check box is selected (true), but no MID Server is defined in the MID Server field, workflow automatically attempts to find a MID Server. |
| MID Server               | midserver      | Name of the MID Server to use. This field appears when you select the *Use MID Server* check box. The workflow ignores this parameter if the *use_midserver* parameter is disabled.                                                                                                                                           |
Probes used by Orchestration

Certain probes, controlled by MID Servers, perform Orchestration tasks on remote computers, such as restarting a server or creating virtual machines from templates.

How Orchestration probes work

When a Workflow executes an Orchestration activity, that activity launches a probe, which writes an output record to the ECC Queue. The MID Server selected for the activity checks the ECC Queue for assignments, and then executes the appropriate probe to do the work on the target machine. The information about the activity (machine restarted, files copied, etc.) that is returned from the target machine by the probe is written to the ECC Queue as an input record. This information is then sent from the ECC Queue to a sensor that is built into the Workflow activity. The Workflow is updated, and the next activity is executed.

Note: The probe parameters are set by the activities that launch the probe.

How Orchestration uses probes

Probe List

The base system includes the following Orchestration probes (Orchestration > Definition > Probes).

<table>
<thead>
<tr>
<th>Probe Name</th>
<th>ECC Queue Topic</th>
<th>ECC Queue Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>Command</td>
<td></td>
<td>A probe that runs a local command on the MID server.</td>
</tr>
<tr>
<td>Probe Name</td>
<td>ECC Queue Topic</td>
<td>ECC Queue Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DNS Name Resolver</td>
<td>DNSNameResolver</td>
<td></td>
<td>A probe that resolves a fully qualified domain name (FQDN) into an IP address.</td>
</tr>
<tr>
<td>SCPCommand</td>
<td>SCPCommand</td>
<td></td>
<td>A probe that copies files securely from one machine to another. The copy function is performed using the MID Server as a tunnel.</td>
</tr>
<tr>
<td>Shazzam</td>
<td>Shazzam</td>
<td></td>
<td>A probe that identifies active devices.</td>
</tr>
<tr>
<td>SNMPProbe</td>
<td>SNMP</td>
<td>SNMP Query</td>
<td>This is a generic SNMP probe.</td>
</tr>
<tr>
<td>SOAPProbe</td>
<td>SOAPProbe</td>
<td></td>
<td>A probe that sends a SOAP request to target machine.</td>
</tr>
<tr>
<td>SSHCommand</td>
<td>SSHCommand</td>
<td></td>
<td>A probe that executes shell scripts from a command line after logging in to a target machine via SSH.</td>
</tr>
<tr>
<td>SSHCommandLong</td>
<td>SSHCommandLong</td>
<td></td>
<td>A probe that executes long running shell scripts from a command line after logging in to a target machine via SSH.</td>
</tr>
<tr>
<td>VMWare</td>
<td>VMWareProbe</td>
<td></td>
<td>A generic VMware probe that executes the MID Server script include in the ECC queue name that is set by a VMware Orchestration activity. This probe can run any MID Server script include.</td>
</tr>
</tbody>
</table>
PowerShell activities

PowerShell is built on the Windows .NET Framework and is designed to control and automate the administration of Windows machines and applications.

PowerShell must be installed on any MID Server that uses these activities. MID Servers using PowerShell must be installed on a supported Windows operating system. ServiceNow supports PowerShell 2.0 and above. PowerShell 3.0 does not support Windows 2003 Server.

The ServiceNow Orchestration plugin adds these basic PowerShell activities to workflows. For instructions on using activities from the PowerShell activity pack, see PowerShell activity pack.

Legacy Run PowerShell activity

The Run PowerShell activity executes Windows PowerShell commands on a MID Server.

**Attention:** This activity is deprecated and is unavailable for new workflows. To replace the functionality of this activity, use the PowerShell activity template to create a custom, scoped activity. Workflows from a previous release that use the Run PowerShell activity can continue to do so.

Result Values

The workflow designer can assign a result value using activity.result from within a script field of the activity. By default, the success or failure of the PowerShell commands used determines the result value of the Run PowerShell activity. Possible result values are:

- Success
- Failure
Scratchpad Entries

Information written to stdout by the executing script is captured and returned to the activity in the activity.output variable. This information can be parsed, processed, or saved (to a scratchpad variable, for example) for future processing in the activity’s sensor script.

An example would be to run the get-date command to get the MID Server’s current time. This sensor script saves the full output received, but we can process it to return and save only the time.

```
Hostname: $workflow.inputs.hostname
Command: get-date

// save full output for a later processing in scratchpad variable ‘currentdatetime’
workflowscratchpad.currentdatetime = activity.output;

// Process the output and fetch the time and store it in a scratchpad variable ‘time’
var time = /\d{1,2}[a-p][m]{0,1}/.exec(output);
workflowscratchpad.time = time[1] ? 'No time found';
```

PowerShell activity

**Note:** This is an over-simplified example. In most cases, the script operates against some remote Windows computer. However, the principal is the same – whatever is written to stdout is returned in activity.output and available to process.

Input Variables

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>IP address of the target Windows machine. This value is mapped to the $computer variable for use in commands (see the example in the Command field). A PowerShell credential variable called $cred that is based on information in the ServiceNow Credentials table will authenticate on the computer pointed to by Hostname.</td>
</tr>
</tbody>
</table>
## Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Command                    | Enter the PowerShell command to run. For example, to execute a simple WMI query against a remote machine pointed to by the `hostname` variable, the command is:  
  ```powershell
  get-wmiobject <class> -computer $computer -credential $cred
  ```  
  If no credentials authenticate on the computer, the command runs in the context of the MID Server user.  
  You cannot run both a command and a script file. Specifying a command hides the `Script file` variable. |
| Sensor script              | The script to run using the results of the probe. The output from the probe is contained in a variable called `output`. Any error from the probe is contained in a variable called `error`. |
| Script file                | The [MID Server script file to run](#). You cannot run both a script file and a command. Selecting a script file hides the `Command` variable. |
| PowerShell script variables| Additional parameters, in JSON format, used by the specified script file.                                                                 |

## States

The activity state tells the workflow engine what to do with the activity.

### States

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executing</td>
<td>The workflow engine knows to start the <code>onExecute</code> function of the activity.</td>
</tr>
<tr>
<td>Finished</td>
<td>The activity finished running. See the result value for the outcome of the activity.</td>
</tr>
<tr>
<td>Cancelled</td>
<td>This activity, or the workflow that contains this activity, was cancelled.</td>
</tr>
</tbody>
</table>

## Example

Add workflow variables for the command line using the normal workflow variable syntax. In the example above, if the `<class>` was in a workflow input variable called `myclass`, the command would look like:

```powershell
get-wmiobject $ {workflow. inputs. myclass } -computer $computer -credential $cred
```

Similarly, if the variable is a scratchpad variable named `myclass`, the command would look like:

```powershell
get-wmiobject $ {scratchpad. myclass } -computer $computer -credential $cred
```
get -wmiobject $ {workflow. scratchpad. myclass } -computer $computer – credential $cred

HResult codes
When a PowerShell script encounters an error, the Windows machine may return an HResult code as part of the error message.

PowerShell activities can read and interpret this code. Not all PowerShell errors include an HResult code. In the event of a failed PowerShell script, you can use the HResult code to move the workflow through a specific condition.

For example, when resetting an Active Directory password to a password that does not meet policy requirements, such as minimum length or complexity, the PowerShell script returns the HResult code -2146022651. To use this code, create an activity condition with the Condition value of activity.hresult = -2146022651. If the PowerShell script returns this code when the activity runs, the workflow transitions through this new condition.

SSH activities
SSH activities allow workflows to perform operations on Linux and Unix computers.

Your ServiceNow instance must have access to a MID Server configured to use SSH to run these Orchestration activities.

Run Command activity
The Run Command activity runs a command (including shell scripts) on a Linux or UNIX computer.

Attention: The Run Command activity is deprecated in this release. If you have a workflow created in a previous version that uses this activity, your workflow will continue to work normally after upgrading to Helsinki. However, to use this functionality in a new workflow, you must create a custom activity using the SSH activity template in the ServiceNow® activity designer.

Input variables

Run command input variables

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Long running</td>
<td>Select this check box to disable the SSH connection timeout if you think the command will take longer to run than the default 60 seconds. Orchestration periodically checks the running process to determine its status until it is finished.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Hostname or IP address of destination server for SSH activity.</td>
</tr>
<tr>
<td>Directory</td>
<td>Name of the working directory.</td>
</tr>
<tr>
<td>Command</td>
<td>The command to run from this activity.</td>
</tr>
<tr>
<td>Sudo</td>
<td>Select this check box to use sudo to run the command on the host machine.</td>
</tr>
<tr>
<td>Sensor script</td>
<td>The script to run using the results of the probe. The output from the probe is contained in a variable called output. Any error from the probe is contained in a variable called error.</td>
</tr>
</tbody>
</table>
Run SCP activity
The Run SCP activity uses Secure Copy Protocol (SCP) to copy a file from one computer to another, including the directory in which the file resides.

Note: This activity is deprecated in the Geneva release and is not available for use in new workflows. If you have a workflow created in a previous version that uses this activity, your workflow will continue to work normally after upgrading. The custom Secure Copy activity replaces the Run SCP activity in the Geneva release.

Input variables

Run SCP input variables

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Host</td>
<td>Hostname or IP address of the source computer.</td>
</tr>
<tr>
<td>From File</td>
<td>Absolute path to the file to copy. This value can be a directory.</td>
</tr>
<tr>
<td>To Host</td>
<td>Hostname or IP address of the target computer.</td>
</tr>
<tr>
<td>To File</td>
<td>Path to the target file. This path can be absolute or relative to the logged in user’s home directory. The specified directory must already exist on the target computer.</td>
</tr>
<tr>
<td>Copy Directory</td>
<td>Check box to copy a directory defined in the From File variable and all files contained in that directory.</td>
</tr>
</tbody>
</table>

Orchestration applications
Orchestration provides several applications with your subscription.

Orchestration ROI
The Orchestration ROI application allows you to estimate and compute cost savings for tasks in your system that could be automated with Orchestration.

After you automate the tasks, you can track cost savings by associating Orchestration workflows with corresponding task areas. Configuration in the application allows you to select the hourly rate for performing the task manually, the rules the system uses to select tasks for evaluation, and the time period of the evaluation. Orchestration ROI estimates your savings by multiplying the cost of performing repetitive tasks manually by the estimated number of times the system performs those tasks automatically during a specific date/time range. The system also calculates the actual savings of your automations. Orchestration ROI is included with the base Orchestration subscription.

Orchestration ROI reports offer a number of views of the comparative data and allow you to access the associated records directly from the reports. The standard reports included with the Orchestration - ROI plugin provide summaries, estimated costs, and calculated costs for automated processes. The ROI premium dashboard uses Performance Analytics to provide detailed reports on calculated savings over time. Performance Analytics requires a different plugin and subscription.
Note: When Orchestration ROI is activated as a dependent plugin of Orchestration, demo data is not installed. If you want to use demo data as a template for your own ROI evaluation, submit a request to ServiceNow® technical support for an Orchestration ROI plugin upgrade with demo data selected.

To set up Orchestration ROI, complete the configuration tasks in the order shown here.

Create Orchestration ROI labor rate cards

Before calculating your Orchestration ROI, you must create labor rate cards for the manual work that would be required to complete the tasks correlated to the ROI calculations.

Role required: orchestration_manager

The hourly rates defined in the rate cards are used to determine the savings from your orchestrated tasks.

1. Navigate to Orchestration > ROI > Labor Rate Cards.
2. Complete the fields in the form using the descriptions in Manage a labor rate card.
3. Click Submit.
4. Create additional rate cards as needed.

Create an Orchestration ROI automation entry record

The ROI automation entry record couples the cost of performing a task with the specific workflow that automates the task, for the purpose of calculating the resulting savings.

Role required: orchestration_manager

Before starting this procedure, verify that the appropriate labor rate cards were created.

Use this record to apply a manual hourly rate to a task that is performed automatically by your instance. To determine the savings realized from orchestrating a task, the system can evaluate whether those savings were estimated or calculated.

- **Estimated savings**: Uses the labor rate, the time estimates for completion of the task, and the number of automations that have been run to determine savings.
- **Calculated savings**: Uses the labor rate, the time calculated for completion of the task, based on the configured evaluation period, and the number of automations that have been run to determine savings.

1. Navigate to Orchestration > ROI > Automation Entry Form.
2. Fill in the fields on the form, as appropriate.
### Automation Entry Form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Category of the selected workflow automation. The following categories are provided in the base Orchestration - ROI system:</td>
</tr>
<tr>
<td></td>
<td>• Access &amp; Identity Management</td>
</tr>
<tr>
<td></td>
<td>• Datacenter Automation</td>
</tr>
<tr>
<td></td>
<td>• IT Service Management</td>
</tr>
<tr>
<td></td>
<td>• Other</td>
</tr>
</tbody>
</table>

**Note:** To create a category, open the dictionary record for the Automation Entry Form (automation_entry_form) table and add an option to the choice list.

<table>
<thead>
<tr>
<th>Item</th>
<th>Unique name for the specific task within the category. This value represents the work to which the labor rate card applies, such as Password Reset.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource</td>
<td>Labor rate card to apply to this automation entry. You must have IT Cost Management active on the instance for this field to appear.</td>
</tr>
<tr>
<td>Associated Workflows</td>
<td>Workflow automations created to automate this manual task. The system uses this field to identify the number of automations that have been run.</td>
</tr>
<tr>
<td>Estimated Duration (min) per Task</td>
<td>Estimated time to perform this task manually.</td>
</tr>
<tr>
<td>Estimated Volume per Month</td>
<td>Estimated number of times needed to perform this task manually per month.</td>
</tr>
</tbody>
</table>

**Read-only fields**

<table>
<thead>
<tr>
<th>Start time</th>
<th>Start time for the evaluation period. Configure this value in the Time Range for Calculated Averages module.</th>
</tr>
</thead>
<tbody>
<tr>
<td>End time</td>
<td>End time of the evaluation period. Configure this value in the Time Range for Calculated Averages module.</td>
</tr>
<tr>
<td>Calculated average duration per task (min)</td>
<td>Actual time required to perform this task manually.</td>
</tr>
<tr>
<td>Calculated average volume per month</td>
<td>Actual average number of times this task is performed manually per month.</td>
</tr>
</tbody>
</table>

3. Select one of these submission options:

- **Submit:** Saves the record to the table without running any calculations.
- **Submit and process now:** Saves the record and calculates the savings based on the hourly rate and the number of workflow contexts for this automation entry.
Create an Orchestration ROI correlated task rule

The correlated task rule applies configurable conditions to fields in a selected table that tell the instance which manual tasks correspond to an automation entry record.

Role required: orchestration_manager

Before starting this procedure, make sure you have created labor rate cards and the appropriate automation entry records for the automated tasks you want to evaluate.

Create conditions that the system can use to correlate manual tasks to the automation entry. For example, a rule on the Incident (incident) table uses these conditions to correlate the employee on-boarding task to values configured in the Employee OnBoarding automation entry record:

- (Subcategory) (is) (Employee OnBoarding)
- (Sort description) (contains) (new employee)

When a new employee opens an incident to request services or assets which are typically handled manually, Orchestration applies the usual labor rate for the manual work to the potential automated solution, and then computes the actual savings.

1. Navigate to Orchestration > ROI Task Correlation > Correlated Tasks Rules.
2. Click New.
3. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automation entry</td>
<td>Automation entry record that correlates to the manual task defined by these conditions. The entry record names the workflow used to automate the task and defines the labor rate used to calculate the cost of the task.</td>
</tr>
<tr>
<td>Table</td>
<td>Table to filter, using these conditions. The rule selects records from this table that match the conditions. Information from these records is used to calculate the actual time to perform a manual task and the actual volume for that manual task.</td>
</tr>
<tr>
<td>Condition</td>
<td>Condition builder to use to filter records for this table. Use these conditions to identify all manual tasks correlated to this automation entry.</td>
</tr>
<tr>
<td>Processed on</td>
<td>Date and time that the system performs the matching records lookup. The system automatically searches for new manual tasks matching these conditions.</td>
</tr>
</tbody>
</table>

4. Select one of these submission options:
   - Submit: Saves the record to the table without running any calculations.
   - Submit and process now: Saves the record, looks up all matching tasks, and saves matching record information to the Correlated Tasks (manual_mapping_records) table.

5. To view a rule, select the link in the Table column of the Correlated Tasks Rules related list for the automation entry you want to see.
6. To view the list of tasks that match all correlated rules in the system, navigate to Orchestration > ROI Task Correlation > Correlated Tasks.

7. To view the list of tasks that match this rule in the system, click Correlated Tasks under Related Links in this form.

**Configure the time range for Orchestration ROI calculations**

Select a date range to calculate the average number of tasks and the duration per month for the correlated tasks.

Role required: orchestration_manager

By default, the system creates a range ending at the current date and time and extending back over the previous month. You can change this range at any time and recalculate the ROI instantly.

1. Navigate to Orchestration > ROI Task Correlation > Time Range for Calculated Averages.
2. Enter a new start or end date and time or click the icon to select a date using the calendar.
3. Click Calculate to recalculate the ROI based on the new time range and to save your settings.

**Installed with Orchestration ROI**

Several types of components are installed with the Orchestration - ROI plugin (com.snc.runbook_automation.roi).

**Tables installed with Orchestration ROI**

Orchestration - ROI adds the following tables.

<table>
<thead>
<tr>
<th>Tables for Orchestration - ROI</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Table</strong></td>
</tr>
<tr>
<td>Expense and Savings</td>
</tr>
<tr>
<td>(run_rate_predicted_savings)</td>
</tr>
<tr>
<td>Savings Report</td>
</tr>
<tr>
<td>(savings_report)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Detailed Savings Report</td>
</tr>
<tr>
<td>(detailed_savings_report)</td>
</tr>
</tbody>
</table>
### Table

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automation Entries (automation_entry_form)</td>
<td>Contains automation entries that couple labor resources to specific manual tasks. You can specify the estimated duration to perform a task manually and the estimated number of times that a task is performed per month. If this automation entry already has workflow automations implemented, you can specify the associated workflows. The system calculates the savings, based on the labor rate card and the number of workflow automations that have been performed.</td>
</tr>
<tr>
<td>Roadmap Planning (roadmap_planning)</td>
<td>Contains roadmap planning for each automation entry to be implemented. You can provide estimated hours to implement a workflow automation, the automation percentage anticipated by the end of the year, and the starting month to implement the workflow.</td>
</tr>
<tr>
<td>Correlated Tasks (manual_mapping_records)</td>
<td>Contains all matching manual tasks for each automation entry. Each task’s information is stored in this table for the system to use to calculate the actual duration and volume for each manual task.</td>
</tr>
<tr>
<td>Correlated Tasks Rules (manual_mapping_conditions)</td>
<td>Contains the correlated task rules the system uses to look up manual tasks corresponding to each automation entry.</td>
</tr>
</tbody>
</table>

### Plugins installed with Orchestration ROI

These plugins are installed with the Orchestration - ROI plugin, if they are not already active.

#### Plugins for Orchestration ROI

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost Management (com.snc.cost_management)</td>
<td>Provides the labor rate cards Orchestration ROI uses to determine the savings for each automated task. See Cost Management for more information.</td>
</tr>
</tbody>
</table>

### User roles installed with Orchestration ROI

These roles are installed with the Orchestration - ROI plugin.

Orchestration - ROI adds the following roles.

#### Roles for Orchestration - ROI

<table>
<thead>
<tr>
<th>Role title (name)</th>
<th>Description</th>
<th>Contains Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orchestration manager (orchestration_manager)</td>
<td>Manages all activities in the Orchestration ROI module.</td>
<td>pa_admin, report_admin</td>
</tr>
</tbody>
</table>

### UI actions installed with Orchestration ROI

Orchestration - ROI adds the following UI actions.
## UI actions for Orchestration - ROI

<table>
<thead>
<tr>
<th>UI action</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Savings Report</td>
<td>Automation Entry Form</td>
<td>Displays the savings report specific to this automation entry, if the associated workflows are not empty.</td>
</tr>
<tr>
<td>Estimated and Projected Savings</td>
<td>Automation Entry Form</td>
<td>Displays the estimated savings, based on the estimated duration of the task, and calculated savings, based on the calculated duration of the task.</td>
</tr>
<tr>
<td>Show Workflow Context</td>
<td>Detailed Savings Report</td>
<td>Shows the related workflow context.</td>
</tr>
<tr>
<td>Submit AND process now</td>
<td>Automation Entry Form</td>
<td>Processes this new entry</td>
</tr>
<tr>
<td>Correlated Tasks</td>
<td>Correlated Tasks Rules</td>
<td>Displays all matching tasks from the Correlated Tasks (manual_mapping_records) table.</td>
</tr>
<tr>
<td>Detailed Savings Report</td>
<td>Automation Entry Form</td>
<td>Displays the list of automations that have been run, based on associated workflows.</td>
</tr>
<tr>
<td>Task</td>
<td>Correlated Tasks Rules</td>
<td>Displays the task record.</td>
</tr>
<tr>
<td>Submit AND process now</td>
<td>Correlated Tasks Rules</td>
<td>Processes a correlated task rule. This action performs matching on the specified table and the filter conditions.</td>
</tr>
</tbody>
</table>

### Script includes installed with Orchestration ROI

Orchestration - ROI adds the following script includes:

### Script includes for Orchestration ROI

<table>
<thead>
<tr>
<th>Script include</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OrchestrationROIAjax</td>
<td>Script that calculates the actual duration and volume of a task.</td>
</tr>
<tr>
<td>OrchestrationROI</td>
<td>Script that calculates the number of workflow contexts, looks up all matching tasks, calculates savings, and other functions used in the UI actions.</td>
</tr>
<tr>
<td>ROIDemoDataUtil</td>
<td>Script that updates demo data timestamps.</td>
</tr>
</tbody>
</table>

### Client scripts installed with Orchestration ROI

Orchestration ROI adds the following client scripts.

---

© 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.
Client scripts for Orchestration ROI

<table>
<thead>
<tr>
<th>Client script</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display info for processing rules</td>
<td>Correlated Tasks Rules</td>
<td>Displays annotation on the Correlated Task Rule form advising that new task rules are not evaluated until the time specified in the ROI schedule.</td>
</tr>
</tbody>
</table>

Business rules installed with Orchestration ROI

Orchestration ROI adds the following business rules.

Business rules for Orchestration ROI

<table>
<thead>
<tr>
<th>Business rule</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete corresponding records</td>
<td>Automation Entry Form</td>
<td>When a record is deleted from the Automation Entry Form (automation_entry_form) table, this business rule deletes all records in other ROI tables that reference this entry.</td>
</tr>
<tr>
<td>Insert into Run Rate &amp; Savings</td>
<td>Automation Entry Form</td>
<td>When a new automation entry is provided, this business rule calculates the estimated savings, based on the estimated duration of a task and its associated labor rate card.</td>
</tr>
<tr>
<td>Insert into Savings Reports</td>
<td>Automation Entry Form</td>
<td>When a new automation entry is provided, this business rule inserts a new record into the Savings Report (savings_report) table with the automations_run field set to 0.</td>
</tr>
</tbody>
</table>

Orchestration ROI reports

Orchestration ROI provides a collection of standard and premium reports to help you calculate savings from automating services in your organization.

The ROI standard reports are included with Orchestration ROI. The premium reports provide enhanced views generated with Performance Analytics and require the Orchestration - ROI Premium plugin.

Orchestration ROI standard reports

The dashboard of standard ROI reports provides summaries, estimated costs, and calculated costs for automated processes.

To access the ROI standard dashboard, navigate to Orchestration > ROI Reports > Dashboard.

Summary tab

The Summary tab contains four reports on automation categories.
### Standard ROI summaries by category

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Type</th>
<th>Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual Tasks by Category Over Time</td>
<td>Trend of manual tasks by category over time. For example, if you use automations to perform a portion of the necessary tasks, the report shows the number of tasks still executed manually, decreasing over time.</td>
<td>Line chart</td>
<td>Detailed Savings Report</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(detailed_savings_report)</td>
</tr>
<tr>
<td>Automations by Category Over Time</td>
<td>Trend of automated tasks by category over time. For example, this chart can show the increase in the number of automated tasks as a workflow automation rolls out slowly over time.</td>
<td>Line chart</td>
<td>Detailed Savings Report</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(detailed_savings_report)</td>
</tr>
<tr>
<td>Automation Savings by Category Over Time (Uses Estimated Duration)</td>
<td>Amount of savings from automated tasks over time, based on the estimated duration of the task, the number of automations performed, and the cost from the labor rate card.</td>
<td>Line chart</td>
<td>Detailed Savings Report</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(detailed_savings_report)</td>
</tr>
<tr>
<td>Automation Savings by Category Over Time (Uses Calculated Duration)</td>
<td>Amount of savings from automated tasks over time, based on the calculated duration of the task, the number of automations performed, and the cost from the labor rate card.</td>
<td>Line chart</td>
<td>Detailed Savings Report</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(detailed_savings_report)</td>
</tr>
</tbody>
</table>

### Estimated Costs tab

The Estimated Costs tab contains eight reports on estimated time and expense for automations.
Estimated Time Spent by Task Category

- Datacenter Automation = 450.00 (68.70%)
- IT Service Management = 150.00 (22.90%)
- Access & Identity Management = 55.00 (8.40%)
<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Estimated Time Spent by Task Category</td>
<td>Total estimated time spent, in minutes, on all tasks by task category.</td>
</tr>
</tbody>
</table>
|                                                                       | **Type:** Pie chart  
|                                                                       | **Table:** Automation Entry Form (automation_entry_form)                                                                                                                                             |
| Estimated Volume of Manual Tasks per Month by Category                | Total estimated volume of all tasks per month by task category.                                                                                                                                       |
|                                                                       | **Type:** Pie chart  
|                                                                       | **Table:** Automation Entry Form (automation_entry_form)                                                                                                                                             |
| Predicted Hours Spent Monthly by Category (Uses Estimated Duration & Volume) | Total predicted hours spent monthly on all manual tasks by category, using the estimated duration of each task and the estimated volume of each task per month.  
|                                                                       | **Type:** Bar chart  
|                                                                       | **Table:** Expense and Savings (run_rate_predicted_savings)                                                                                                                                           |
| Predicted Monthly Expense by Category (Uses Estimated Duration & Volume) | Total predicted monthly expense for all manual tasks by category, using the estimated duration of each task, estimated volume of each task per month, and the cost from the labor rate card.  
|                                                                       | **Note:** This report uses negative numbers to express an expense.                                                                                                                                 |
|                                                                       | **Type:** Bar chart  
|                                                                       | **Table:** Expense and Savings (run_rate_predicted_savings)                                                                                                                                           |
| Predicted Hours Spent Quarterly by Category (Uses Estimated Duration & Volume) | Total predicted hours spent quarterly on all manual tasks by category, using the estimated duration of each task and the estimated volume of each task per month.  
|                                                                       | **Type:** Bar chart  
|                                                                       | **Table:** Expense and Savings (run_rate_predicted_savings)                                                                                                                                           |
| Predicted Quarterly Expense by Category (Uses Estimated Duration & Volume) | Total predicted quarterly expense for all manual tasks by category, using the estimated duration of each task, estimated volume of each task per month, and the cost from the labor rate card.  
|                                                                       | **Note:** This report uses negative numbers to express an expense.                                                                                                                                 |
|                                                                       | **Type:** Bar chart  
<p>|                                                                       | <strong>Table:</strong> Expense and Savings (run_rate_predicted_savings)                                                                                                                                           |</p>
<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
</table>
| Predicted Hours Spent Annually by Category (Uses Estimated Duration & Volume) | Total predicted hours spent annually on all manual tasks by category, using the estimated duration of each task and the estimated volume of each task per month.  
- **Type**: Bar chart  
- **Table**: Expense and Savings  
  (run_rate_predicted_savings) |
| Predicted Annual Expense by Category (Uses Estimated Duration & Volume) | Total predicted annual expense for all manual tasks by category, using the estimated duration of each task, estimated volume of each task per month, and the cost from the labor rate card.  
  Note: This report uses negative numbers to express an expense.  
- **Type**: Bar chart  
- **Table**: Expense and Savings  
  (run_rate_predicted_savings) |

**Costs from Correlated Tasks tab**

The Costs from Correlated Tasks tab contains eight reports on time and expense for automations based on actual calculations.
ROI calculated time and expense report sample

© 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.
### Standard ROI calculated time and expense of automations

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Spent by Task Category</td>
<td>Total actual time spent, in minutes, on all tasks by task category.</td>
</tr>
<tr>
<td></td>
<td><strong>Type:</strong> Pie chart</td>
</tr>
<tr>
<td></td>
<td><strong>Table:</strong> Automation Entry Form (automation_entry_form)</td>
</tr>
<tr>
<td>Volume of Manual Tasks per Month by Category</td>
<td>Total actual volume of all tasks per month by task category.</td>
</tr>
<tr>
<td></td>
<td><strong>Type:</strong> Pie chart</td>
</tr>
<tr>
<td></td>
<td><strong>Table:</strong> Automation Entry Form (automation_entry_form)</td>
</tr>
<tr>
<td>Projected Hours Spent Monthly by Category (Uses Calculated Duration &amp; Volume)</td>
<td>Total projected hours spent monthly on all manual tasks by category, using the calculated duration of each task and the calculated volume of each task per month.</td>
</tr>
<tr>
<td></td>
<td><strong>Table:</strong> Expense and Savings (run_rate_predicted_savings)</td>
</tr>
<tr>
<td>Projected Monthly Expense by Category (Uses Calculated Duration &amp; Volume)</td>
<td>Total projected monthly expense for all manual tasks by category using the calculated duration of each task, the calculated volume of each task per month, and the cost from the labor rate card.</td>
</tr>
<tr>
<td></td>
<td><strong>Type:</strong> Bar chart</td>
</tr>
<tr>
<td></td>
<td><strong>Table:</strong> Expense and Savings (run_rate_predicted_savings)</td>
</tr>
<tr>
<td>Projected Hours Spent Quarterly by Category (Uses Calculated Duration &amp; Volume)</td>
<td>Total projected hours spent quarterly on all manual tasks by category, using the calculated duration of each task and the calculated volume of each task per month.</td>
</tr>
<tr>
<td></td>
<td><strong>Table:</strong> Expense and Savings (run_rate_predicted_savings)</td>
</tr>
<tr>
<td>Projected Quarterly Expense by Category (Uses Calculated Duration &amp; Volume)</td>
<td>Total projected quarterly expense for all manual tasks by category using the calculated duration of each task, the calculated volume of each task per month, and the cost from the labor rate card.</td>
</tr>
<tr>
<td></td>
<td><strong>Type:</strong> Bar chart</td>
</tr>
<tr>
<td></td>
<td><strong>Table:</strong> Expense and Savings (run_rate_predicted_savings)</td>
</tr>
</tbody>
</table>
Projected Hours Spent Annually by Category (Uses Calculated Duration & Volume)

Total projected hours spent annually on all manual tasks by category, using the calculated duration of each task and the calculated volume of each task per month.

- **Type:** Bar chart
- **Table:** Expense and Savings (run_rate_predicted_savings)

Projected Annual Expense by Category (Uses Calculated Duration & Volume)

Total projected annual expense for all manual tasks by category using the calculated duration of each task, the calculated volume of each task per month, and the cost from the labor rate card.

<table>
<thead>
<tr>
<th>Note: This report uses negative numbers to express an expense.</th>
</tr>
</thead>
</table>

- **Type:** Bar chart
- **Table:** Expense and Savings (run_rate_predicted_savings)

Schedule Orchestration ROI calculations for standard reports

The scheduled job that calculates Orchestration ROI standard reports is active by default and controlled by system properties.

**Role required:** orchestration_manager, admin

The system provides a default scheduled job called Processing ROI Schedule that allows you to configure when Orchestration calculates the ROI for standard reports. This schedule allows scripting for advanced conditions. To modify the schedule or write a script to run, open Processing ROI Schedule from **System Scheduler > Scheduled Jobs > Scheduled Jobs** and click **Configure Job Definition**. To execute the schedule directly from the job definition, click **Execute Now**.

To control the running of the schedule job with the Orchestration properties:

1. Navigate to **Orchestration ROI > Properties**.
2. Configure the following properties:

**ROI schedule properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roi.processing.active</td>
<td>Activate scheduled job for ROI processing. This property activates the Processing ROI Schedule scheduled job.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Type:</strong> true</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default:</strong> true</td>
</tr>
<tr>
<td>roi.processing.interval</td>
<td>Scheduled ROI processing interval (hours). This property sets the repeat interval for the scheduled job that processes savings reports and correlated tasks.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Type:</strong> integer</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default:</strong> 24</td>
</tr>
</tbody>
</table>
3. Click **Save** to save your changes.

**Orchestration ROI premium reports**

The premium dashboard provides detailed reports on calculated savings over time.

The ROI premium reports require the Orchestration - ROI Premium plugin and are built using [Performance Analytics concepts](#). The Orchestration - ROI Premium plugin is dependent on the [Performance Analytics - Premium](#) plugin which requires a separate subscription.

**Important:** You must activate the Performance Analytics [scheduled collection job](#) before Orchestration ROI premium can display data.

To access the ROI premium dashboard, navigate to **Orchestration > ROI Reports > Premium Dashboard**.

**ROI By Category tab**

The ROI By Category tab contains three reports showing the calculated savings over time by category.

![Calculated savings monthly by category](image)
### Premium reports for calculated savings over time by category

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROI - Monthly By Category</td>
<td>Shows the calculated savings each month by category. The chart displays the total calculated savings against the calculated savings for each category.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Type</strong>: Column chart</td>
</tr>
<tr>
<td></td>
<td>- <strong>Table</strong>: Detailed Savings Report (detailed_savings_report)</td>
</tr>
<tr>
<td>ROI - By Category</td>
<td>Shows the trend of calculated savings by category.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Type</strong>: Spline chart</td>
</tr>
<tr>
<td></td>
<td>- <strong>Table</strong>: Detailed Savings Report (detailed_savings_report)</td>
</tr>
<tr>
<td>ROI - Running Sum 12 month period</td>
<td>Shows the running sum of calculated savings for all categories in the last 12 months.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Type</strong>: Area chart</td>
</tr>
<tr>
<td></td>
<td>- <strong>Table</strong>: Detailed Savings Report (detailed_savings_report)</td>
</tr>
</tbody>
</table>

### ROI By Automation Entry

The ROI By Automation Entry tab contains two reports showing the calculated savings over time by automation entry.
Calculated savings for the current month by automation entry

Calculated savings over time by automation entry

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROI By Automation Entry</td>
<td>Shows the current month’s calculated savings for each automation entry.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Type</strong>: Column</td>
</tr>
<tr>
<td></td>
<td>• <strong>Table</strong>: Detailed Savings Report (detailed_savings_report)</td>
</tr>
<tr>
<td>ROI - By Automation Entry Top 10 List</td>
<td>Shows the top 10 automation entries that have the most calculated savings in the current month.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Type</strong>: Scorecard</td>
</tr>
<tr>
<td></td>
<td>• <strong>Table</strong>: Detailed Savings Report (detailed_savings_report)</td>
</tr>
</tbody>
</table>

Activate Orchestration ROI premium reports

To view the Orchestration ROI premium reports, you must activate the Orchestration - ROI Premium (com.snc.runbook_automation.roi_premium) plugin.

The Orchestration - ROI Premium plugin requires the **Performance Analytics - Premium** plugin, which must be purchased separately.

Role required: admin

The Orchestration - ROI Premium plugin is included with an Orchestration subscription, but must be activated by request.

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></td>
<td>Note: Plugins are activated in two batches each business day in the Pacific timezone, 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>

| Reason/Comments | Any information that would be helpful for the ServiceNow personnel activating the plugin such as if you need the plugin activated at a specific time instead of during one of the default activation windows. |

3. Click Submit.

Schedule Orchestration ROI calculations for premium reports

Orchestration ROI premium reports use a Performance Analytics job that must be activated before premium reports can be generated.

Role required: orchestration_manager, admin

The scheduled job required to calculate premium ROI reports is called (PA ROI) Historic Data Collection and is installed with the Orchestration - ROI Premium (com.snc.runbook_automation.roi_premium) plugin. This job is not active by default.

1. Navigate to Performance Analytics > Data Collector > Jobs.
2. Search for the (PA ROI) Historic Data Collection job.
3. Select the Active check box.
4. The scheduling options appear for the value selected in the Run field.
   For instructions on creating a schedule, see Schedule a data collection job.
5. To execute the schedule directly from the job definition, click Execute Now.
6. Click Update.

Client Software Distribution

The Client Software Distribution (CSD) application allows administrators to distribute software from the service catalog using third-party management systems.

CSD allows an administrator to create all the records necessary to deploy software from service catalog requests, including software models and catalog items. You can use the CSD application to automate the deployment and revocation of software from an SCCM host using the custom SCCM activity pack. You can define lease periods for software distributed from the Service Catalog and allow lease extensions in some cases, pending approvals. Deployment is accomplished using Orchestration activities and workflows.

CSD also integrates with Software Asset Management to manage license counts for deployed software.
CSD process flow using SCCM

Activate client software distribution

Client software distribution requires the Orchestration - Client Software Distribution plugin (com.snc.orchestration.client_sf_distribution), which is available by request with a subscription to Orchestration.
The Orchestration - Client Software Distribution plugin activates the Orchestration - System Center Configuration Manager plugin that contains the custom SCCM activities used to deploy or revoke software using an SCCM server. For additional plugin dependencies, see Plugins installed with client software distribution.

**Note:** The Orchestration - Client Software Distribution plugin runs in its own application scope.

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 timezone, 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>
<th>Any information that would be helpful for the ServiceNow personnel activating the plugin such as if you need the plugin activated at a specific time instead of during one of the default activation windows.</th>
</tr>
</thead>
</table>

3. Click Submit.

**Installed with client software distribution**

Several types of components are installed with client software distribution (CSD).

**Tables installed with client software distribution**

These tables are installed with the Orchestration - Client Software Distribution plugin (com.snc.orchestration.client_sf_distribution).

**Client software distribution tables**

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Software Distribution Catalog Item (sn_client_sf_dist_cat_item)</td>
<td>Contains all catalog items created for client software distribution. This table extends the Catalog Item (sc_cat_item) table.</td>
</tr>
<tr>
<td>Client Software Distribution Software Request (sn_client_sf_dist_req_software)</td>
<td>Contains all requested software, and their statuses.</td>
</tr>
<tr>
<td>Client Software Distribution Application (sn_client_sf_dist_application)</td>
<td>Contains all discovered CSD applications.</td>
</tr>
<tr>
<td>Client Software Distribution Provider (sn_client_sf_dist_provider)</td>
<td>Contains all software distribution providers.</td>
</tr>
<tr>
<td>Client Software Distribution Extension Key (sn_client_sf_dist_extension_key)</td>
<td>Contains the predefined CSD extension keys.</td>
</tr>
</tbody>
</table>
### Table

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Software Distribution Extension Point (sn_client_sf_dist_extension_point)</td>
<td>Contains the customization script for the extension keys.</td>
</tr>
<tr>
<td>Client Software Distribution Software Configuration (sn_client_sf_dist_software_config)</td>
<td>Base table for all software provider configurations.</td>
</tr>
<tr>
<td>SCCM Server Instance (sn_client_sf_dist_cmdb_ci_sccm_server)</td>
<td>Contains all SCCM server instances. This table extends the Configuration Item (cmdb_ci) table.</td>
</tr>
<tr>
<td>SCCM Application (sn_client_sf_dist_sccm_application)</td>
<td>Contains all discovered SCCM applications. This table extends the Client Software Distribution Application (sn_client_sf_dist_application) table.</td>
</tr>
<tr>
<td>SCCM Application Catalog Item (sn_client_sf_dist_sccm_app_cat_item)</td>
<td>Contains all catalog items created for SCCM applications. This table extends the Client Software Distribution Catalog Item (sn_client_sf_dist_cat_item) table.</td>
</tr>
<tr>
<td>SCCM Collection (sn_client_sf_dist_sccm_collection)</td>
<td>Contains all discovered SCCM collections.</td>
</tr>
<tr>
<td>SCCM Deployment (sn_client_sf_dist_sccm_deployment)</td>
<td>Contains all discovered SCCM deployments.</td>
</tr>
<tr>
<td>SCCM Configuration (sn_client_sf_dist_sccm_config)</td>
<td>Contains the SCCM application, install and uninstall collections, and Discovery model. This table extends the Client Software Distribution Software Configuration (sn_client_sf_dist_software_config)</td>
</tr>
</tbody>
</table>

---

### Plugins installed with client software distribution

These plugins are installed with the Orchestration - Client Software Distribution plugin, if they are not already active.

For instructions on requesting activation of Client Software Distribution (CSD) see [Activate client software distribution](#).

### Plugins for Orchestration - Client Software Distribution

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orchestration - System Center Configuration Manager (com.snc.orchestration.sccm_mgnt)</td>
<td>Installs the custom SCCM Orchestration activities that do work on the SCCM target host.</td>
</tr>
<tr>
<td>Orchestration - Asset Lease Management (com.snc.orchestration.asset_lease_management)</td>
<td>Installs the <a href="#">lease functionality</a> for software distributed through the Service Catalog. This includes starting, stopping, and extending leases.</td>
</tr>
<tr>
<td>Service Catalog Scoped API (com.glideapp.servicecatalog.scoped.api)</td>
<td>Installs the API to support application creation in the Service Catalog.</td>
</tr>
<tr>
<td>Software Asset Management (com.snc.software_asset_management)</td>
<td>Provides the ability to manage software assets, including the reconciliation of entitlements to licenses for named users, workstation, and enterprise software agreements.</td>
</tr>
</tbody>
</table>

---

### Roles installed with client software distribution

These roles are installed with the Orchestration - Client Software Distribution plugin.

© 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.
### Roles for Orchestration - Client Software Distribution

<table>
<thead>
<tr>
<th>Role title (name)</th>
<th>Description</th>
<th>Contains Roles</th>
</tr>
</thead>
</table>
| Client software distribution admin (sn_client_sf_dist.csd_admin) | Administrator role for managing client software distribution application. | • sam  
• agent_admin  
• report_admin  
• catalog_admin  
• itil  
• workflow_admin |

### Script includes installed with client software distribution
These script includes are installed with the Orchestration - Client Software Distribution plugin

### Script includes for Orchestration - Client Software Distribution

<table>
<thead>
<tr>
<th>Script include</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSDExtensionPoint</td>
<td>Execute the CSD provider's specific code</td>
</tr>
<tr>
<td>CSDUtil</td>
<td>Utility functions for the CSD application.</td>
</tr>
<tr>
<td>RefQualsCSD</td>
<td>Reference qualifier filter. This script provides the filter functions for the CSD providers, devices, SCCM application, install collections, and uninstall collections.</td>
</tr>
<tr>
<td>SCCMCatItemHandler</td>
<td>Sets the field values of specific SCCM catalog items. These values are the SCCM catalog item table name, catalog item name, SCCM provider, and SCCM software configuration.</td>
</tr>
<tr>
<td>SoftwareCatItemCreator</td>
<td>Creates software catalog items</td>
</tr>
<tr>
<td>CSDCatItemHandler</td>
<td>Base class for CSD catalog item creation. This script is used by the Create Catalog Item UI action to create an application catalog.</td>
</tr>
<tr>
<td>CSDDemoDataUtil</td>
<td>Populates demo data.</td>
</tr>
<tr>
<td>CSDDemoDataUtilAjax</td>
<td>Populates demo data.</td>
</tr>
</tbody>
</table>

### Properties installed with client software distribution
Properties for client software distribution (CSD) manage the installation status of requested software deployments and configure scheduled Discoveries.

To access CSD properties, navigate to **Client Software Distribution > Properties.** The following properties are available:
### Client software distribution properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Status check expiration interval (days)       | sn_client_sf_dist.softwareInstallExpDays | Controls how many days the system waits before ignoring the software installation status. The default time limit for installing software is 30 days before the system stops checking the installation status of a deployment. Installation statuses are:  
  - **Not installed:** User has not installed requested software prior to the expiration of the configured time limit.  
  - **Installed:** Software was installed within the configured time limit.  
  - **Status check expired:** Time limit has expired for the user to install the requested software. The system no longer checks the status of this deployment.  
  - **Revoked:** Software was revoked by the administrator.  
  - **Type:** integer  
  - **Default value:** 30 |
| Reconcile software installation status interval (hours) | sn_client_sf_dist.softwareInstallIntervalHour | Determines when the scheduled job runs that determines the installation status. By default, the system checks the installation status every hour.  
  - **Type:** integer  
  - **Default value:** 24 |
| Set scheduled application Discovery interval (days) | sn_client_sf_dist.discoveryExeDay | Sets the repeat interval for the scheduled job that runs application Discovery. By default, Discovery runs at midnight on the day set with this value.  
  - **Type:** integer  
  - **Default value:** 5 |
| Set lease execution schedule job interval (minutes) | sn_client_sf_dist.lease_execution_interval | Interval in which the CSD Lease Schedule scheduled job checks for requested software leases to start, stop, or extend.  
  - **Type:** integer  
  - **Default value:** 1 |
<table>
<thead>
<tr>
<th>Property</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set time prior to lease end to notify requester (days)</td>
<td>sn_client_sf_dist.lease_end_notification</td>
<td>Determines how many days prior to the end of a software lease to notify the requester. If lease extensions are allowed, ensure that this period provides enough time for the approval process to complete before the lease expires.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Type</strong>: integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Default value</strong>: 5</td>
</tr>
</tbody>
</table>

**Workflows installed with client software distribution**

These workflows are installed with the Orchestration - Client Software Distribution plugin

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discover SCCM</td>
<td>Retrieves lists of applications, collections, and deployments from SCCM servers using custom CSD orchestration activities. An administrator runs this workflow from a UI action in a SCCM Server Instance record.</td>
</tr>
<tr>
<td>Order Client Software</td>
<td>Runs automatically when a user orders software from the service catalog.</td>
</tr>
<tr>
<td>Deploy SCCM Application</td>
<td>Triggered by the Order Client Software workflow to deploy software through SCCM server. This workflow adds either the user or the device into the SCCM collection.</td>
</tr>
<tr>
<td>Revoke Client Software</td>
<td>Begins the software revocation process for software deployed by an external provider. Administrators run this workflow from a UI action on the Requested Software record and the Installed Software Not Entitled record. This workflow triggers the appropriate provider workflow that performs the actual revocation. For example, this workflow triggers the Revoke SCCM Application workflow for applications in SCCM uninstall collections.</td>
</tr>
<tr>
<td>Revoke SCCM Application</td>
<td>Revokes SCCM applications that are members of an uninstall collection. The Revoke Client Software workflow triggers this workflow to revoke software deployed by an SCCM server. This workflow moves either the user or the device from the SCCM collection into the appropriate uninstall collection.</td>
</tr>
</tbody>
</table>

**Create licenses and counters for distributed software**

Licenses and software counters are associated with the software model and must be created if you want to track the license for software deployed by client software distribution (CSD).

Role required: sam or admin
You can create software licenses and counters in Software Asset Management for software items deployed from the service catalog by CSD. CSD depends on the software counter result to determine if the license is available for the requested software. If the license Valuation is greater than 0, and the license type is Not allocated, CSD assumes that the license is available for the software.

1. Navigate to Software Asset > Software Licenses.
2. Add a new software license for the software model you used in CSD.
3. Navigate to Software Asset > Reconciliation > Software Counters.
4. Create a software counter for the software model you created.
5. Run the counter to retrieve the software license information.

Client software distribution ordering process
Software deployed by Client Software Distribution (CSD) can be ordered from the service catalog by individual users or by approved users on behalf of others.

Client Software Distribution catalog items have different options, depending on how ordering is configured.

Lease start and end dates

All software deployed by CSD requires users to specify the beginning date for the lease. This is enforced by the Orchestration - Asset Lease Management plugin that is activated automatically with CSD. The system prepopulates the Lease start field with the current date and time.

If the catalog item is configured for revocation (uninstall), the form displays the Lease end field, which allows the requester to define an end date and time for the lease. The system validates user input in these fields to ensure that the dates selected define a future window. The Lease end field is not mandatory and can be left blank to order software with no end date.

**Note:** For systems deploying software from Microsoft System Center Configuration Management (SCCM), the Lease end field is only available if the SCCM configuration specifies an uninstall collection.

Software offered only to the logged in user

If the software catalog item is configured with the Order on behalf of check box cleared, the User field does not appear on the order form. The logged in user selects the device on which to deploy the software from the Device to install this software on field. Only those devices assigned to the logged in user appear in the list.

In this example, a user has logged into the service catalog to order Firefox for a computer that is assigned to her. She selects the machine from a list of devices she owns and selects the date and time the lease should begin. This software is deployed through Microsoft System Center Configuration Management (SCCM), but does not have an uninstall collection configured and cannot be revoked automatically by the system. As a result, the Lease end field is not available.
Ordering software as the logged in user

Software ordered on behalf of another user

If the software catalog item is configured with the Order on behalf of check box selected, the User field appears on the form. The logged in user can select any user from this field. The Device to install this software on field only lists the devices assigned to the user selected in the User field. If an approval is required for software ordered on behalf of another user, the system automatically sends an approval request to the manager of the user receiving the software. The approval is skipped if the requester is the named user's manager.

In this example, a manager is ordering Google Chrome for a contractor. The manager selects the contractor from the User field and then chooses a computer from the list of devices assigned to the contractor. This software has an SCCM uninstall collection configured, which allows the manager to select an end date for the lease that coincides with the end of the user's contract. When the lease expires, SCCM automatically uninstalls the software from the device.
Defining software lease window

Extend a software lease

Users of software deployed by Client Software Distribution (CSD) can request the extension of a lease window, if the software is revocable by a software distribution system.

Role required: Any system user

If your software has a lease end date defined, and the software status is **Installed**, you can request an extension of the lease, pending any approvals your organization requires.

1. Navigate to **Service Catalog > My Requested Software**.
   - The list shows only the software you have requested from the service catalog.
2. Select the record for the installed software whose lease you want to extend.
3. Under **Related Links** click **Extend Lease**.
4. In the dialog box that appears, select a new lease end date in the calendar and click **OK**. You must select a date later than the current date.

If the lease extension is subject to manager approval, you are notified of the decision. If the request is approved, a notification shows the new lease end date. If the new end date is within 5 days (the default notification period) of the date when you made the request, CSD sends an immediate end-of-lease notification.

**Important:** If lease extensions in your organization require approval, make sure the approver is available and has enough time to process your extension request. If the extension cannot be approved before the original end date expires, the software is revoked.
Client software distribution from SCCM

You can use Client Software Distribution (CSD) to deploy and revoke software deployments from Microsoft System Center Configuration Management (SCCM) and manage distributions on SCCM hosts.

The **SCCM activity pack** contains Orchestration activities that CSD uses to deploy software from a service catalog request and manage user and device collections on SCCM servers. In addition, CSD can manage license counts for deployed software using ServiceNow Software Asset Management, revoke software deployed by SCCM without user interaction, and manage lease periods.

**Configuring SCCM**

Follow the SCCM configuration procedures in the order shown.

Configure the Application Administrator role on the SCCM server

To deploy software using ServiceNow® Client Software Distribution (CSD), ensure that an SCCM administrative user has the correct permissions to deploy software and that PowerShell is properly configured.

SCCM role required: Application Administrator

These instructions are for Microsoft 2012 R2 Server.

1. In the System Center Configuration Manager console, navigate to **Administration > Security > Administrative Users**.
2. Right-click the user to whom you want to grant the Application Administrator role.
3. Select **Properties** from the drop-down menu.
4. In the Properties dialog box, select the **Security Roles** tab.
5. Ensure that the user has the Application Administrator role.
6. If the user does not already have this role, click **Add**, select this role from the list, and click **OK**.
Granting the Application Administrator role on the SCCM server
7. Log into SCCM as the user with the Application Administrator role.
8. Open the menu from the upper left corner of the console and select **Connect via Windows PowerShell**.

9. Ensure that the user can access the CM console.
   This action establishes the environment path to PowerShell for the logged in Application Administrator user.

**Update the SCCM cmdlet libraries**

Ensure that the System Center Configuration Manager SCCM Cmdlet Library is up-to-date.

SCCM role required: Either current user or system administrator, depending on settings.

The System Center Configuration Manager SCCM Cmdlet Library installs and updates the Windows PowerShell module for SCCM. SCCM checks for library updates on a daily basis. Out-of-date libraries can cause Discovery of the SCCM server to fail, because the system cannot parse the SCCM activity output. This warning message appears in the ECC queue input records for the SCCM GET activities:

```
WARNING: An update to the System Center 2012 Configuration Manager Cmdlet Library is available. Please go to 'http://go.microsoft.com/fwlink/?LinkID=528947' to download the latest version.
```
Running cmdlet version: 5.0.8231.1004 Latest cmdlet version: 5.0.8328.1155


If you elect to use an earlier version library, use this procedure to disable the CM update check, which allows Discovery to proceed without issues.

1. Log into the SCCM console as an administrator.
2. Open the menu from the upper left corner of the console.
4. Run one of these commands to disable the update check:
   - **Per-user**: Set-CMCmdletUpdateCheck -CurrentUser -IsUpdateCheckEnabled 0
   - **Per-system**: Set-CMCmdletUpdateCheck -System -IsUpdateCheckEnabled 0

   **Important**: The per-system cmdlet must run in an elevated Windows PowerShell session.

5. Run the Get-CMCmdletUpdateCheck command to refresh the console and check the settings.
6. Ensure that the value of the IsEnabled configuration variable has changed to False. This indicates that the warning for an out of date cmdlet library is disabled for the users specified.
7. To re-enable the update check, run the -IsUpdateCheckEnabled 1 command for either the current user or for the system.

Configure the MID Server for SCCM activities
To use a MID Server with Microsoft System Center Configuration Management (SCCM) activities, configure it to communicate with the SCCM server.

Role required: admin

1. In the navigation filter, enter cmdb_ci_dns_name.list.
2. Click New.
3. Enter the fully-qualified domain name (FQDN) of the SCCM server in the Name field.
4. Right-click in the form header and select Save.
5. In the IP Address related list, click New.
6. In the IP Address field, enter the IP address of the SCCM server.
7. In the Nic field, select eth0 or your preferred network interface controller.
8. Leave the Netmask field blank.
9. Click Submit.

Create Windows credentials for SCCM deployments
Microsoft System Center Configuration Manager (SCCM) requires the appropriate credentials to deploy applications using the Client Software Distribution application.

Role required: sn_client_sf_dist.csd_admin or admin

Client software distribution requires Windows credentials that have administrative rights on the SCCM server.

1. Navigate to Orchestraton > Credentials.
2. Click New.
3. In the list of credential types, select Windows Credentials.
4. Provide a user name and password with administrative rights on the SCCM server.
Important: Ensure the following:

- This user must have the Application Administrator role on the SCCM server.
- Use the credentials to log into the SCCM Server and connect via Windows PowerShell from the System Center Configuration Manager console at least once to set the path variable for that credential.

5. Fill in the other fields on the form, as appropriate.
   For details, see Windows credentials.
6. Click Submit.

Retrieve SCCM data for client software distribution

Retrieve the collections and the list of applications available for deployment from your SCCM servers.

Role required: sn_client_sf_dist.csd_admin or admin

Before starting this procedure:

- Set up your Microsoft System Center Configuration Manager (SCCM) server, create the applications and collections, and configure the deployments you need. For information, see your SCCM documentation.
- Configure a user with the Application Deployment Manager role on the SCCM server.
- Set up the MID Server to communicate with the SCCM server.
- Add Powershell credentials to the ServiceNow Credentials (discovery_credentials) table for the SCCM user who has the Application Deployment Manager role.

To populate the Client Software Distribution application with SCCM data:

1. Navigate to Client Software Distribution > SCCM > SCCM Server Instance.
2. Click New.
3. In the SCCM Server Instance form, identify the server by name and provide the fully qualified domain name.
4. Click Submit.
   The new SCCM server appears in the list.
5. Open the new SCCM record and click Discover now under Related links.
   The system runs the Discover SCCM workflow that retrieves the application, collection, and deployment data from the SCCM server.
Retrieving SCCM data with Discovery

SCCM server Discovery for client software distribution

A Discovery workflow populates ServiceNow tables with collection, application, and deployment data retrieved from SCCM servers.

Users run the Discover SCCM workflow from an SCCM Server Instance record to populate the following ServiceNow tables:

**SCCM data populated in ServiceNow tables**

<table>
<thead>
<tr>
<th>Table</th>
<th>Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCCM Application  (sn_client_sf_dist_sccm_application)</td>
<td>name, publisher, version, model, sccm_server</td>
</tr>
<tr>
<td>SCCM Collection  (sn_client_sf_dist_sccm_collection)</td>
<td>name, type, sccm_server</td>
</tr>
<tr>
<td>SCCM Deployment (sn_client_sf_dist_sccm_deployment)</td>
<td>application, collection, type</td>
</tr>
</tbody>
</table>
Note: For details about the custom activities used in this workflow to extract data from an SCCM server, see Orchestration SCCM activity pack.

Set up a software model for an SCCM application

Using the applications discovered on the SCCM server, set up a software model used by the Software Asset Management application to manage licenses.

Role required: sn_client_sf_dist.csd_admin or admin

Before creating software models, you must discover the applications available for deployment on the SCCM server. See Retrieve SCCM data for client software distribution for details.

You can link an SCCM application to an existing software model or create a new model.

1. Navigate to Client Software Distribution > SCCM > SCCM Applications.
   A list of applications discovered on the SCCM server appears.

2. Open an SCCM application record.

3. To link to an existing model, click the magnifying glass icon in the Model field and select a model from the list.<info>

4. To create a model, click Create Software Model under Related Links.
   a) Complete the software model fields.
      See for details.

   b) Click Submit.
      The view returns to the SCCM Applications form.

Define an SCCM configuration
To create catalog items for SCCM software deployment or to configure your instance to revoke software through SCCM, you must first associate that software with a collection through an SCCM configuration.

Before you create an SCCM configuration record, make sure you have discovered the SCCM applications, collections, and deployments and set up the necessary software models.

Role required: sn_client_sf_dist.csd_admin or admin

The SCCM configuration process associates software with SCCM collections. To deploy software from an SCCM server, the user or device must be a member of an SCCM collection associated with an install deployment. Client Software Distribution (CSD) allows you to revoke unentitled software using an SCCM server when that software can be removed using an uninstall collection. Users requesting revokable software from the Service Catalog also have the ability to define lease start and stop dates and request lease extensions.
SCCM table references

1. Navigate to Client Software Distribution > SCCM > SCCM Applications.
2. Open an application that has a configured software model.
3. Under Related Links, click Create Software Configuration.
4. Complete the form, using the fields in the table.
### SCCM configuration form

#### SCCM configuration fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Recognizable name for this SCCM software configuration.</td>
</tr>
<tr>
<td>SCCM application</td>
<td>Name of an application hosted on the SCCM server.</td>
</tr>
<tr>
<td>SCCM collection</td>
<td>Name of the collection associated with the <strong>install</strong> deployment for the selected application on the SCCM server. Only those collections associated with the application are available for selection.</td>
</tr>
<tr>
<td>SCCM uninstall collection</td>
<td>Name of the collection associated with the <strong>uninstall</strong> deployment for the selected application on the SCCM server. You must specify an uninstall collection to:</td>
</tr>
<tr>
<td></td>
<td>* Define a lease end date for deployed software.</td>
</tr>
<tr>
<td></td>
<td>* Allow lease extensions.</td>
</tr>
<tr>
<td></td>
<td>* Revoke software from a user’s machine.</td>
</tr>
</tbody>
</table>
Create a catalog item for an SCCM application

Using the applications discovered on the SCCM server, create a catalog item for an application you want to offer for distribution from the service catalog.

Role required: sn_client_sf_dist.csd_admin or admin

Before creating a catalog item, you must link the application to a software model and create at least one software configuration.

1. Navigate to Client Software Distribution > SCCM > SCCM Applications.
   A list of applications discovered on the SCCM server appears.
2. Open a record for an SCCM application.
3. Under Related Links, click Create Catalog Item.
   A new SCCM Application Catalog Item record appears with preconfigured information. For information about common service catalog fields, see .
4. Add price information and complete the following fields added to the Client Software Distribution Catalog Item (sn_client_sf_dist_cat_item) table by the Orchestration - Client Software Distribution plugin:

**SCCM fields in the catalog item form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skip approval (skip_approval)</td>
<td>Check box that allows skipping approval for this item by the requester's manager when a user orders it from the service catalog. Use this field in conjunction with the <strong>Order on behalf of</strong> field to ensure that software ordered by a logged in user on behalf of another user is subject to approval. By default, this check box is cleared, requiring manager approval for all new catalog items.</td>
</tr>
<tr>
<td>Check license compliance</td>
<td>Check box that forces the system to determine if deploying this item is allowed under the current license.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Order on behalf of         | Check box that allows the logged-in user to order this software from the service catalog for another user. This permits service desk personnel to order SCCM deployments for other users in the system. By default, this feature is enabled. To prevent unauthorized users from ordering software, ensure that approvals are required for this type of deployment by clearing the Skip approval check box. If an approval is required for software ordered on behalf of a user, the system automatically sends an approval request to the manager of the user receiving the software. The approval is skipped if the requestor is the named user's manager. Software items requested from the service catalog on behalf of a different user require the following information:  
  • **User**: User selected for deployment. This field is automatically populated with the name of the logged in user. You can select another user from the list.  
  • **Device to install this software on**: Device belonging to the selected user on which to deploy the software. Only devices belonging to that user appear in the choice list.  
  • **Lease start**: Date and time to deploy the software. This is the start time for the lease. A lease can be open-ended or have a lease end time. |
| SCCM configuration         | Name of the SCCM configuration record for this application. This record defines the collection and uninstall collection for this application. This configuration is required for all deployments, revocations, and leases performed by the SCCM server. |

5. If the catalog item requires approval because of cost, be sure to configure an approval group in the Approved By Group related list. By default, the Service Catalog Request workflow runs when an item costing more than $1000 is ordered and looks for an appropriate approval group. If no approval group is configured for the item, this workflow skips approval altogether and ends. The system then runs the Order Client Software workflow, which evaluates the Skip approval check box to determine if approval by the requester's manager is required.

6. Click **Update**. The view returns to the SCCM Applications list.

7. To see all client software distribution (CSD) catalog items, navigate to **Client Software Distribution > Maintain Items > Software Items**.

**Workflow process for SCCM deployment**

Ordering an SCCM application from a client software distribution (CSD) catalog item in the service catalog triggers the Order Client Software workflow.
This process deploys an SCCM application to a user or device through a service catalog order:

1. If the **Skip approval** check box is cleared in the software catalog item, the Order Client Software workflow sends the catalog request to the requesting user’s manager for approval.

2. If the **Check license compliance** check box is selected in the software catalog item, the workflow performs a software license check. If there is no license available, the workflow creates a catalog task to procure more licenses and assigns the task to the Client Software Distribution Administrators group.

3. The Order Client Software workflow triggers the Deploy SCCM Application workflow as a subflow. This workflow adds either the user or the device to the SCCM collection using the Add to User Collection or Add to Device Collection SCCM activity.

4. If the software configuration specifies **SCCM uninstall collection** in the software catalog item, the Deploy SCCM Application workflow checks if the user or device exists in the uninstall collection. The workflow uses the Is Device in Collection or Is User in Collection SCCM activity. If the user or device exists in the uninstall collection, the workflow removes the device or user. The workflow uses the Remove from Device Collection or Remove from User Collection SCCM activity before adding it to the SCCM install collection.

**Client software distribution validation process**

After SCCM deploys software to a target computer, client software distribution (CSD) detects the installation and validates its status.

Client software distribution uses the following methods for detecting software installed on the target machine:

- **Discovery**: CSD is configured to leverage Discovery to detect software installations. You can run Discovery manually at any time, or by a scheduled job.
- **Microsoft SCCM Integration**: You can import SCCM data into the CMDB using the features in the Integration - Microsoft SCCM plugin if Discovery is not active on the instance.

The instance uses the data gathered by Discovery or the SCCM integration plugin to populate the Software Installation (cmdb_sam_sw_install) table. To validate installations using this data, CSD runs a scheduled job called Reconcile Requested Software that uses **CSD property** settings. This process reconciles the software installation data accumulated in the CMDB and makes these status updates:

- **Not installed** to **Installed**: The user has installed the requested software within the time limit configured in the sn_client_sf_dist.softwareInstallExpDays property.
- **Not installed** to **Status check expired**: The time limit has expired for the user to install the requested software. The system stops checking for installation when the time limit expires.

**SCCM software revocation**

An administrator can revoke software without any user interaction using Microsoft System Center Configuration Manager (SCCM) if the software configuration specifies an SCCM uninstall collection, even if the software was installed by some other process or user.

Revoke software deployed through the service catalog

Software deployed by SCCM can be revoked, but only when the software’s status is **Installed** and the application associated with the software configuration has an uninstall collection configured.

- Create an **SCCM configuration record** for the application that names an appropriate uninstall collection.
- Associate the **CSD catalog item** for the application with the SCCM configuration that specifies the uninstall collection.

Role required: sn_client_sf_dist.csd_admin or admin
A workflow called **Revoke SCCM Application** moves either the user or the device from its respective collection and adds it to the appropriate uninstall collection. When SCCM performs an internal policy check and finds the user or device in the uninstall collection, SCCM removes the related software package from the client computer.

1. Navigate to **Client Software Distribution > Reports > Requested Software**.
2. Open the record for the SCCM software package you want to revoke.
   The package must have a **Status** of **Installed** to be revocable.
3. Under **Related Links**, click **Revoke software**.
   
   This action runs the Revoke Client Software workflow, which triggers the Revoke SCCM Application subflow that moves the user or device from the install collection to the uninstall collection. When SCCM performs an internal policy check and finds the user or device in the uninstall collection, SCCM removes the related software package from the client computer.

**Revoke unentitled software**

An administrator can revoke software using Microsoft System Center Configuration Manager (SCCM) that a user is not entitled to use even if the software was installed by some other process or user.

To revoke software using SCCM, you must create an **SCCM configuration record** for the application, in which the appropriate software Discovery model is defined. See [Software discovery models](#).

Role required: **sn_client_sf_dist.csd_admin** or **admin**

Client Software Distribution (CSD) uses **Software Asset Management** (SAM) to identify unentitled software installations. Discovery detects the software on the user's machine, and SAM determines if the user or device is entitled to use that software. This might include software that was not installed through a catalog request or software that the user installed without approval. If the software installation's Discovery model is associated with an SCCM software configuration that has an uninstall collection defined, then an administrator can use CSD to revoke that software from the user's machine without involving the user.

1. Navigate to **Client Software Distribution > Reports > Installed Software Not Entitled**.
2. Select the record for the installation that has unentitled users.
3. Under **Related Links**, click **Revoke software**.
   
   This action runs the Revoke Client Software workflow, which triggers the Revoke SCCM Application subflow that moves the user or device from the install collection to the uninstall collection. When SCCM performs an internal policy check and finds the user or device in the uninstall collection, SCCM removes the related software package from the client computer.
SCCM software revocation workflow
The Revoke SCCM Application workflow moves a user or device from an install collection to an uninstall collection to revoke software installed from Microsoft System Center Configuration Manager (SCCM).
For the revocation workflow to run, the software package must have a status of **Installed** and must be pre-configured for an appropriate uninstall collection. See *Revoke software deployed through the service catalog* for configuration instructions. When an administrator initiates the revocation process, the system launches the Revoke SCCM Application workflow to move the user or device collection associated with installation to the appropriate SCCM uninstall collection. When the SCCM server performs a policy check, it finds the additions to the user or device uninstall collection and revokes the software package associated with that collection.

The workflow employs two custom activities, *Remove from User Collection* and *Remove from Device Collection*, to remove either the user or the device from its original collection. The workflow then adds the user or device to the appropriate uninstall collection on the SCCM server with the *Add to User Collection* or *Add to Device Collection* activity.

**Note:** This workflow is triggered by the Revoke Client Software workflow as a subflow.

**Client software distribution dashboard**

The CSD dashboard provides a collection of visual reports for the Client Software Distribution application.

To access the CSD dashboard, navigate to **Client Software Distribution > Requested Software > Dashboard.**

![Sample report from CSD dashboard](image)

**Client software distribution reports**

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open Tasks</td>
<td>Displays all open tasks grouped by the requested item's stage value.</td>
</tr>
<tr>
<td></td>
<td>• Type: <em>List reports</em></td>
</tr>
<tr>
<td></td>
<td>• Table: Catalog Task (sc_task)</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>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 10 Applications Installed</td>
<td>Displays the top 10 applications installed by request count.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Type</strong>: Bar chart</td>
</tr>
<tr>
<td></td>
<td>• <strong>Table</strong>: Requested Software (sn_client_sf_dist_req_software)</td>
</tr>
<tr>
<td>Total Software Request Item Over Time</td>
<td>Displays the total software items requested each month.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Type</strong>: Line chart</td>
</tr>
<tr>
<td></td>
<td>• <strong>Table</strong>: Requested Software (sn_client_sf_dist_req_software)</td>
</tr>
<tr>
<td>Requests Completed Report</td>
<td>Displays the total of software requests completed each month.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Type</strong>: Line chart</td>
</tr>
<tr>
<td></td>
<td>• <strong>Table</strong>: Requested Software (sn_client_sf_dist_req_software)</td>
</tr>
<tr>
<td>Installed Software Not Entitled</td>
<td>Displays installed software that users or devices are not entitled to use. This can be software deployed through CSD or by another process that does not comply with licensing. This report is on a Software Asset Management table.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Type</strong>: List reports</td>
</tr>
<tr>
<td></td>
<td>• <strong>Table</strong>: Software Installation (cmdb_sam_sw_install)</td>
</tr>
<tr>
<td>Software Installation Status</td>
<td>Displays the count of requested software, grouped by installation status, for each month.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Type</strong>: Line chart</td>
</tr>
<tr>
<td></td>
<td>• <strong>Table</strong>: Requested Software (sn_client_sf_dist_req_software)</td>
</tr>
<tr>
<td>Software Requested Item Stage Report</td>
<td>Displays the sum of all requested items, grouped by the requested item’s stage, for each month.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Type</strong>: Line chart</td>
</tr>
<tr>
<td></td>
<td>• <strong>Table</strong>: Requested Software (sn_client_sf_dist_req_software)</td>
</tr>
<tr>
<td>License Counts Available</td>
<td>Displays the license counts for all available applications.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Type</strong>: List reports</td>
</tr>
<tr>
<td></td>
<td>• <strong>Table</strong>: SCCM Application Catalog Item (sn_client_sf_dist_sccm_app_cat_item)</td>
</tr>
</tbody>
</table>

**Client software distribution extension framework**

Client software distribution (CSD) provides built-in extension points for integrating a ServiceNow instance with client software distribution providers, such as Casper, Altiris, or LANDesk.
Caution: The use of CSD extension points is an advanced procedure intended for use by experienced Now Platform developers only. Instructions for customizing your instance to deploy and revoke software from a software distribution provider can be found in the CSD Extension Implementation Guide.

Configure client software distribution providers
Identify the provider and specify the workflows and extension points for a customized software distribution process.

Perform the development tasks described in the CSD Extension Implementation Guide before attempting this procedure.

Role required: sn_client_sf_dist.csd_admin, admin

1. Navigate to Client Software Distribution > Extensions > Providers.
2. Click New.
3. Complete the form using the fields in the table.

Provider information for Casper integration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Descriptive name of the provider.</td>
</tr>
<tr>
<td>Provider server</td>
<td>Table name of the provider server. You must create this table as an extension of the Configuration Item (cmdb_ci) table. For example, you might call your table Casper Server Instance (cmdb_ci_casper_server_instance).</td>
</tr>
<tr>
<td>Discovery workflow</td>
<td>Workflow that discovers the provider server and returns the data from that server back to the instance. This is the workflow you create with custom activities that query the provider server.</td>
</tr>
<tr>
<td>Software configuration</td>
<td>Table name of the software configuration for this provider. You create this table as an extension of the Client Software Distribution Software Configuration (sn_client_sf_dist_software_config) table. For example, you might create a table called Casper Software Configuration (sn_client_sf_dist_casper_sf_config).</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Deployment extension key</td>
<td>The SetDeploymentData key provided with CSD. This key sets up the data for the software ordering and deployment workflow.</td>
</tr>
<tr>
<td>Deployment workflow</td>
<td>Workflow that deploys software from the provider server. This is the workflow you created with custom activities that tells the provider where to deploy an application requested from the service catalog.</td>
</tr>
<tr>
<td>Revocation extension key</td>
<td>The SetRevocationData key provided with CSD. This key sets up the data for installation revocation.</td>
</tr>
<tr>
<td>Revocation workflow</td>
<td>Workflow that revokes an installation from a provider server. This is the workflow you created with custom activities that tells the provider which application to remove from a device.</td>
</tr>
</tbody>
</table>

**Client software distribution extension keys**

Client software distribution (CSD) extension keys allow you to customize the deployment and revocation of software from distribution providers.

These pre-defined keys allow you to generate input variables for workflows that deploy and revoke software from external distribution providers:

- **SetDeploymentData**: Sets the software order information and generates the input variables for the deployment workflow.
- **SetRevocationData**: Generates the input variables for the revocation workflow.
- **CheckRevocable**: Specifies the conditions that determine if an installation can be revoked. If the software configuration associated with the installed software allows uninstallation, the installed software can be revoked.

**Client software distribution extension points**

The client software distribution (CSD) extension points create the customization code for the specific provider and the extension keys.

The purpose of the extension points is to associate extension keys with a specific provider, and then create a script that sets input variables for your custom deployment and revocation workflows. Another extension point script tells CSD if the provider has the capability to revoke software. If this is the case, CSD enables the UI action that triggers revocation from the provider.

**SetDeploymentData**

The script associated with this extension key must set the csdExtensionResult object with these attributes:

- **deploymentWorkflowInputs**: Object that specifies the deployment workflow input variables.
- **softwareModel**: Software model sys_id.
- **deploymentType**: An integer. Use 1 for deployment to a user and 2 for deployment to a device.
- **softwareApplication**: Software application sys_id.
CheckRevocable

The script associated with this extension key gets the input parameter `csdExtensionInputs.softwareConfiguration`, which is a Client Software Distribution record in the Software Configuration (sn_client_sf_dist_software_config) table. All providers’ software configurations are extended from this table, but may have different attributes.

This script must set the `csdExtensionResult` object to true or false, depending on whether the software configuration specifies uninstallation.

SetRevocationData

The script associated with this extension key gets the input parameter `csdExtensionInputs.softwareConfiguration`, which is a Client Software Distribution record in the Software Configuration (sn_client_sf_dist_software_config) table. All providers’ software configurations are extended from this table, but may have different attributes.

The script must set the `csdExtensionResult` object with these attributes:
- `revocationWorkflowInput`: Object that specifies the revocation workflow input variables.
- `softwareModel`: Software model sys_id.
- `deploymentType`: An integer. Use 1 for deployment to a user and 2 for deployment to a device.

Password Reset and Password Change applications

The ServiceNow® Password Reset application enables an end user to use a self-service process to reset the password. Alternatively, your organization can implement a process that requires a service desk agent to reset passwords for end users.

Explore
- Password Reset release notes
- Upgrade to Jakarta

Set up
- Password Reset setup guide

Administer
- Password Reset admin guide

Use
- Service desk: Reset a password for a user
- Service desk: Unblock a Password Reset user
- Users: Reset your password on Windows systems

Develop
- Developer training
- Developer documentation

Integrate
- Integrate Password Reset with a CMS integration
- Password Reset Windows Application

Troubleshoot and get help
- Ask or answer questions in the Change Management forum
- Search the HI Knowledge Base for known error articles
- Contact ServiceNow Technical Support

Password Reset setup guide

A simple version of the Password Reset application is active by default. You can install a plugin to extend functionality.
Requirements

Role required: admin

What is installed

- Password Reset is active by default and includes example verifications. The base system enables connections only to the Local ServiceNow Instance credential store type. For details, see Credential stores for Password Reset. To enable connections to Active Directory (AD) and Remote (SOAP) ServiceNow Instance credential store types, you must activate the Password Reset - Orchestration Add-on plugin. The plugin also activates the Password Reset Windows Application (com.glideapp.password_reset_desktop). No other components are installed. Orchestration is available as a separate subscription. See Activate the Password Reset - Orchestration Add-on plugin.

Next steps

Plan and configure the Password Reset processes for your organization. See the Password Reset admin guide.

Activate the Password Reset - Orchestration Add-on plugin

The Password Reset - Orchestration Add-on plugin activates the Password Reset Windows Application (com.glideapp.password_reset_desktop) and enables connections to the Active Directory (AD) and Remote (SOAP) ServiceNow instance credential store types. No other components are installed.

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 timezone, 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**.

*Installed with Password Reset*

Tables, roles, business rules, scripts, and workflows are installed with the Password Reset application.

### Password Reset tables

<table>
<thead>
<tr>
<th>Table name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Reset Active Answer (pwd_active_answer)</td>
<td>Security questions and associated answers, in an encrypted state, that users have selected while going through the enrollment process.</td>
</tr>
<tr>
<td>Password Reset Active Question (pwd_active_question)</td>
<td>Security questions that users have selected while going through the enrollment process.</td>
</tr>
<tr>
<td>Password Reset Activity Log (pwd_reset_activity)</td>
<td>All Password Reset requests.</td>
</tr>
<tr>
<td>Password Reset Activity Monitor (pwd_activity_monitor)</td>
<td>Password Reset lockout activity.</td>
</tr>
<tr>
<td>Password Reset Credential Store (pwd_cred_store)</td>
<td>Password Reset credential stores that are available.</td>
</tr>
<tr>
<td>Password Reset Credential Store Parameters (pwd_cred_store_param)</td>
<td>User-created credential store parameters.</td>
</tr>
<tr>
<td>Password Reset Credential Store Types (pwd_cred_store_type)</td>
<td>Password Reset credential store types that are available.</td>
</tr>
<tr>
<td>Password Reset Desktop Access Control (pwd_access_control)</td>
<td>Password Reset Windows Application access control.</td>
</tr>
<tr>
<td>Password Reset Desktop Access Log (pwd_access_log)</td>
<td>Password Reset Windows Application access logs.</td>
</tr>
<tr>
<td>Password Reset Device Enrollment Code (pwd_dvc_enrollment_code)</td>
<td>Device enrollment codes that have been sent to users during SMS code enrollment.</td>
</tr>
<tr>
<td>Password Reset Devices (pwd_device)</td>
<td>User SMS devices that are in a state of verified.</td>
</tr>
<tr>
<td>Password Reset Enrollment for Verification (pwd_enrollment)</td>
<td>Information about user enrollment by verification.</td>
</tr>
<tr>
<td>Password Reset Enrollment Snapshot (pwd_enrollment_snapshot)</td>
<td>Snapshot of user enrollment by verification. This table is regenerated daily by a scheduled job named Password Reset Enrollment Snapshot.</td>
</tr>
<tr>
<td>Table name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Password Reset Extension Type (pwd_extension_type)</td>
<td>Extension types that are available.</td>
</tr>
<tr>
<td>Password Reset Identification Type (pwd_identification_type)</td>
<td>Password Reset identification types that are available.</td>
</tr>
<tr>
<td>Password Reset Process (pwd_process)</td>
<td>Password Reset processes that are available.</td>
</tr>
<tr>
<td>Password Reset Process Credential Store (pwd_map_proc_to_cred_store)</td>
<td>Credential stores and the associated Password Reset processes that the application is using.</td>
</tr>
<tr>
<td>Password Reset Process User Group (pwd_map_proc_to_group)</td>
<td>Groups and the associated Password Reset processes that the application is using.</td>
</tr>
<tr>
<td>Password Reset Process Verification (pwd_map_proc_to_verification)</td>
<td>Verifications and the associated Password Reset processes that the application is using.</td>
</tr>
<tr>
<td>Password Reset Question (pwd_question)</td>
<td>Questions that the application uses for security question verifications.</td>
</tr>
<tr>
<td>Password Reset Request (pwd_reset_request)</td>
<td>Information about Password Reset requests.</td>
</tr>
<tr>
<td>Password Reset SMS Verification Code (pwd_sms_code)</td>
<td>SMS verification codes that have been sent to users for a password reset.</td>
</tr>
<tr>
<td>Password Reset User Lockout (pwd_user_lockout)</td>
<td>Users that are locked out of Password Reset.</td>
</tr>
<tr>
<td>Password Reset Verification (pwd_verification)</td>
<td>Verifications that are available.</td>
</tr>
<tr>
<td>Password Reset Verification Param (pwd_verification_param)</td>
<td>User-created verification parameters.</td>
</tr>
<tr>
<td>Password Reset Verification Type (pwd_verification_type)</td>
<td>Password Reset verification types that are available.</td>
</tr>
</tbody>
</table>

### Password Reset roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>password reset administrator (password_reset_admin)</td>
<td>Configures and maintains Password Reset and Password Change.</td>
</tr>
<tr>
<td>service desk agent (password_reset_service_desk)</td>
<td>Resets passwords on behalf of users, tracks password reset requests, and views logs.</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>credentials manager  &lt;br&gt; (password_reset_credential_manager)</td>
<td>Determines which credential stores are valid for use with Password Reset.</td>
</tr>
</tbody>
</table>

### Password Reset business rules

<table>
<thead>
<tr>
<th>Business rule</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add default parameters QA verification</td>
<td>Password Reset Verification (pwd_verification)</td>
<td>If no parameters for Security Question verifications are specified, generates parameters.</td>
</tr>
<tr>
<td>Add default parameters SMS verification</td>
<td>Password Reset Verification (pwd_verification)</td>
<td>If there are no parameters specified, generates SMS code verifications parameters.</td>
</tr>
<tr>
<td>Add params personal confirm verification</td>
<td>Password Reset Verification (pwd_verification)</td>
<td>If there are no parameters specified, generates personal data confirmation verifications parameters.</td>
</tr>
<tr>
<td>Add params personal verification</td>
<td>Password Reset Verification (pwd_verification)</td>
<td>If there are no parameters specified, generates parameters for personal data verification.</td>
</tr>
<tr>
<td>Check unique verifications</td>
<td>Password Reset Process Verification (pwd_map_proc_to_verification)</td>
<td>Prevents a verification from being assigned multiple times to a specific Password Reset process.</td>
</tr>
<tr>
<td>Clear parameters for Mock verification</td>
<td>Password Reset Verification (pwd_verification)</td>
<td>Clears parameters for the Mock verification.</td>
</tr>
<tr>
<td>Deactivate process with no group</td>
<td>Password Reset Process User Group (pwd_map_proc_to_group)</td>
<td>Deactivates the process if it does not apply to all users or if the groups associated with it are removed.</td>
</tr>
<tr>
<td>Deactivate process with no min ver</td>
<td>Password Reset Process Verification (pwd_map_proc_to_verification)</td>
<td>Deactivates the process if the verifications associated with the process are less than the minimum value for the process.</td>
</tr>
<tr>
<td>Deactivate process with no verification</td>
<td>Password Reset Process Verification (pwd_map_proc_to_verification)</td>
<td>Deactivates the process if the verifications associated with it are removed.</td>
</tr>
<tr>
<td>Google Auth Enabled Check</td>
<td>Password Reset Process (pwd_process)</td>
<td>Deactivates the process with Google Authenticator verification if the Google authenticator is disabled.</td>
</tr>
<tr>
<td>Handle req_enroll validation/ default val</td>
<td>Password Reset Process Verification (pwd_map_proc_to_verification)</td>
<td>Handles requires_enrollment and auto_enroll values for the process.</td>
</tr>
<tr>
<td>Business rule</td>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Order must be unique</td>
<td>Password Reset Desktop Access Control</td>
<td>Enforces order to be unique.</td>
</tr>
<tr>
<td>(pwd_access_control)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter Names Cannot Be Updated</td>
<td>Password Reset Verification Param</td>
<td>Prevents parameter name changes.</td>
</tr>
<tr>
<td>(pwd_verification_param)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password Reset Activity Monitor</td>
<td>Password Reset User Lockout</td>
<td>Creates an event when the number of users locked out of Password Reset during a specific interval exceeds the threshold value.</td>
</tr>
<tr>
<td>(pwd_user_lockout)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password Reset Validate Autogenerate</td>
<td>Password Reset Process</td>
<td>Checks that either Email password or Display password is selected when the Autogenerate password check box is selected.</td>
</tr>
<tr>
<td>(pwd_process)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal Data Confirm Param Validation</td>
<td>Password Reset Verification Param</td>
<td>Checks that a column exists in the sys_user table for the parameter used in a personal data confirmation verification.</td>
</tr>
<tr>
<td>(pwd_verification_param)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal Data Param Validation</td>
<td>Password Reset Verification Param</td>
<td>Checks that a column exists in the sys_user table for the parameter used in a personal data verification.</td>
</tr>
<tr>
<td>(pwd_verification_param)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prevent against deletion</td>
<td>Password Reset Credential Store</td>
<td>Checks whether the credential store is part of an active process before allowing deletion.</td>
</tr>
<tr>
<td>(pwd_cred_store)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prevent against deletion</td>
<td>Password Reset Identification Type</td>
<td>If an identification type is part of an active process, prevents the identification type from being deleted.</td>
</tr>
<tr>
<td>(pwd_identification_type)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prevent against deletion</td>
<td>Password Reset Verification</td>
<td>If the verification is part of an active process, prevents it from being deleted.</td>
</tr>
<tr>
<td>(pwd_verification)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prevent against deletion when in use</td>
<td>Password Reset Credential Store Types</td>
<td>Prevents deletion when the type is in use.</td>
</tr>
<tr>
<td>(pwd_cred_store_type)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prevent against deletion when in use</td>
<td>Password Reset Verification Type</td>
<td>Prevents deletion when the type is in use.</td>
</tr>
<tr>
<td>(pwd_verification_type)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Questions Param Validation</td>
<td>Password Reset Verification Param</td>
<td>Checks for valid parameters in security question verifications.</td>
</tr>
<tr>
<td>(pwd_verification_param)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send SMS code</td>
<td>Password Reset Device Enrollment Code</td>
<td>Sends an enrollment code to a device.</td>
</tr>
<tr>
<td>(pwd_dvc_enrollment_code)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business rule</td>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Set new record flag</td>
<td>Password Reset Process (pwd_process)</td>
<td>Sets a new record flag for the client to take appropriate action.</td>
</tr>
<tr>
<td>Send SMS Verification Code Via Notify</td>
<td>Password Reset SMS Verification Code (pwd_sms_code)</td>
<td>Sends out SMS authentication code via Notify if the Notify plugin is active.</td>
</tr>
<tr>
<td>Single credential store per process</td>
<td>Password Reset Process Credential Store (pwd_map_proc_to_cred_store)</td>
<td>Prevents having more than one credential store per process.</td>
</tr>
<tr>
<td>SMS Code Param Validation</td>
<td>Password Reset Verification Param (pwd_verification_param)</td>
<td>Checks for valid parameters in SMS code verifications.</td>
</tr>
<tr>
<td>Update action based on access conditions</td>
<td>Password Reset Desktop Access Log (pwd_access_log)</td>
<td>Updates the &quot;action&quot; field of this log record based on the access control conditions.</td>
</tr>
<tr>
<td>Update proc_to_cred_store</td>
<td>Password Reset Process (pwd_process)</td>
<td>Enforces a one-to-one relation between a Password Reset process and a credential store.</td>
</tr>
<tr>
<td>Validate Process</td>
<td>Password Reset Process (pwd_process)</td>
<td>Verifies that a Password Reset process is configured correctly.</td>
</tr>
<tr>
<td>Validate Pwd Cred Store Name</td>
<td>Password Reset Credential Store (pwd_cred_store)</td>
<td>Enforces the name to be unique.</td>
</tr>
<tr>
<td>Validate Pwd Cred Store Type Name</td>
<td>Password Reset Credential Store Types (pwd_cred_store_type)</td>
<td>Enforces the name to be unique.</td>
</tr>
<tr>
<td>Validate Pwd Extension Type Name</td>
<td>Password Reset Extension Type (pwd_extension_type)</td>
<td>Enforces the name to be unique.</td>
</tr>
<tr>
<td>Validate Pwd Identification Type Name</td>
<td>Password Reset Identification Type (pwd_identification_type)</td>
<td>Enforces the name to be unique and not empty.</td>
</tr>
<tr>
<td>Validate Pwd Process Name</td>
<td>Password Reset Process (pwd_process)</td>
<td>Enforces the name to be unique.</td>
</tr>
<tr>
<td>Validate Pwd Verification Name</td>
<td>Password Reset Verification (pwd_verification)</td>
<td>Enforces the name to be unique.</td>
</tr>
<tr>
<td>Validate Pwd Verification Type Name</td>
<td>Password Reset Verification Type (pwd_verification_type)</td>
<td>Enforces the name to be unique.</td>
</tr>
<tr>
<td>Validate Security Question</td>
<td>Password Reset Question (pwd_question)</td>
<td>Validates rules for security questions such as no duplicates or empty questions.</td>
</tr>
</tbody>
</table>
## Business rule

<table>
<thead>
<tr>
<th>Business rule</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify Account Lookup Script</td>
<td>Password Reset Credential Store (pwd_cred_store)</td>
<td>Checks whether the account lookup script has the correctly named function.</td>
</tr>
<tr>
<td>VerifyAutoEnroll</td>
<td>Password Reset Verification Type (pwd_verification_type)</td>
<td>Checks whether auto-enroll is selected and ensures that an enrollment check script is provided.</td>
</tr>
</tbody>
</table>

## Password Reset UI pages

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$pwd_reset</td>
<td>First page of self-service reset process (asks for user ID).</td>
</tr>
<tr>
<td>$pwd_reset_serviceDesk</td>
<td>First page of service desk assisted reset process (asks for user ID).</td>
</tr>
<tr>
<td>$pwd_verify</td>
<td>Second page of reset process (asks user to verify identity).</td>
</tr>
<tr>
<td>$pwd_new</td>
<td>Last page of password change process (asks for new password).</td>
</tr>
<tr>
<td>$pwd_success</td>
<td>Page that appears when password is reset successfully.</td>
</tr>
<tr>
<td>$pwd_error</td>
<td>Page that appears on error during reset process.</td>
</tr>
<tr>
<td>$pwd_confirm</td>
<td>For processes configured to email password reset URL: After successful verification, this page displays message about sending link to user.</td>
</tr>
<tr>
<td>$pwd_change</td>
<td>Page for changing password.</td>
</tr>
<tr>
<td>$pwd_change_success</td>
<td>Page that appears when password is changed successfully.</td>
</tr>
<tr>
<td>$pwd_change_error</td>
<td>Page that appears on error during password change process.</td>
</tr>
<tr>
<td>$pwd_enrollment_form_container</td>
<td>Enrollment page for all verifications.</td>
</tr>
<tr>
<td>$pwd_enrollment_success</td>
<td>Page that appears when enrollment is successful.</td>
</tr>
<tr>
<td>$pwd_enroll_error</td>
<td>Page that appears when any error happens during enrollment.</td>
</tr>
<tr>
<td>$pwd_unlock_success</td>
<td>Page that appears when locked user is successfully unlocked.</td>
</tr>
<tr>
<td>$pwd_reset_downloads_ui</td>
<td>Page for downloading Password Reset Windows Application.</td>
</tr>
</tbody>
</table>
Password Reset UI macros

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$pwd_csrf_validation</td>
<td>CSRF validation for Password Reset Application. If violation is detected, the page will be redirected to the error page.</td>
</tr>
<tr>
<td>$pwd_display_password</td>
<td>Displays a temporary password on the success page if the process is configured to auto-generate.</td>
</tr>
<tr>
<td>$pwd_enroll_questions_ui</td>
<td>UI for question and answer security validation enrollment.</td>
</tr>
<tr>
<td>$pwd_enroll_questions_ui_js</td>
<td>JavaScript code that requires server-side data for security question and answer enrollment.</td>
</tr>
<tr>
<td>$pwd_enroll_sample_ui</td>
<td>Sample UI macro for enrollment for Mock Verification Type.</td>
</tr>
<tr>
<td>$pwd_enroll_sms_ui and $pwd_verify_sms_ui</td>
<td>UI for SMS enrollment and verification.</td>
</tr>
<tr>
<td>$pwd_enrollment_form_title</td>
<td>Jelly macro function that prints the title for the enrollment form. A verification ID is mandatory.</td>
</tr>
<tr>
<td>$pwd_error_message</td>
<td>UI for displaying error messages.</td>
</tr>
<tr>
<td>$pwd_process_flow</td>
<td>UI for indicating current stage.</td>
</tr>
<tr>
<td>$pwd_process_footer</td>
<td>JavaScript code to get the footer macro name.</td>
</tr>
<tr>
<td>$pwd_verify_personal_data_ui and $pwd_verify_personal_data_confirmation_ui</td>
<td>UI for verifying personal data and for confirming personal data.</td>
</tr>
<tr>
<td>$pwd_verify_questions_ui</td>
<td>UI for verifying questions.</td>
</tr>
<tr>
<td>$pwd_verify_simple_ui</td>
<td>Input section for a simple verification method. This field is a single input field.</td>
</tr>
</tbody>
</table>

UI scripts installed with Password Reset

You can create a UI script and reference the script from a UI macro or UI page by using a `<g:include_script>` Jelly tag. The following example shows how the $pwd_enroll_questions_ui UI macro can reference the $pwd_enroll_questions_ui script. In the example, `[UI Script Name]".jsdbx"` is the name of the script:

```
<g:include_script src="$pwd_enroll_questions_ui.jsdbx" />
```

By referencing an external script, you can maintain separation between client JavaScript code and Jelly code, which simplifies maintenance. You can use the following installed scripts with Password Reset UI macros:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$pwd_csrf_common_ui_script</td>
<td>Common UI script for handling a Cross-site Request Forgery (CSRF).</td>
</tr>
<tr>
<td>$pwd_enroll_questions_ui</td>
<td>JavaScript code for the $pwd_enroll_questions_ui UI macro.</td>
</tr>
<tr>
<td>$pwd_enroll_sample_ui</td>
<td>Included sample client JavaScript for the $pwd_enroll_sample_ui UI macro.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>$pwd_enroll_sms_ui</td>
<td>SMS enrollment UI script.</td>
</tr>
<tr>
<td>$pwd_enrollment_submit_event</td>
<td>UI script for an enrollment submission event.</td>
</tr>
<tr>
<td>$pwdWfManager</td>
<td>Helper class to handle workflow activities and post-processing.</td>
</tr>
</tbody>
</table>

### Password Reset workflows

The Password Reset plugin adds workflows that you can use as examples to create custom workflows for Password Reset processes.

**Workflows that connect to a credential stores**

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pwd Reset - AD</td>
<td>Connects to an AD server.</td>
</tr>
<tr>
<td>Pwd Reset - Local ServiceNow</td>
<td>Current (local) instance.</td>
</tr>
<tr>
<td>Pwd Reset - Master</td>
<td>Password Reset master workflow.</td>
</tr>
<tr>
<td>Pwd Reset - Mock Fatal</td>
<td>Example workflow to use in Password Reset testing to simulate a fatal error. No retries.</td>
</tr>
<tr>
<td>Pwd Reset - Mock Non Fatal</td>
<td>Example workflow to use in Password Reset testing to simulate a non-fatal error.</td>
</tr>
<tr>
<td>Pwd Reset - Mock Success</td>
<td>Example workflow to use in Password Reset testing to simulate a successful completion.</td>
</tr>
<tr>
<td>Pwd Reset - Remote ServiceNow</td>
<td>Connects to a remote(SOAP) ServiceNow instance.</td>
</tr>
</tbody>
</table>

**Workflows that test the connection to a credential store**

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pwd Connection Test - AD</td>
<td>Tests connection to an AD server.</td>
</tr>
<tr>
<td>Pwd Connection Test - Local SN</td>
<td>Tests connection to local instance.</td>
</tr>
<tr>
<td>Pwd Connection Test - Master</td>
<td>Master workflow to test credential store connectivity.</td>
</tr>
<tr>
<td>Pwd Connection Test - Mock Failure</td>
<td>Example credential store connection test that simulates a failed connection.</td>
</tr>
<tr>
<td>Pwd Connection Test - Mock Success</td>
<td>Example credential store connection test that simulates a successful connection.</td>
</tr>
<tr>
<td>Pwd Connection Test - Remote SN</td>
<td>Tests connection to a remote(SOAP) ServiceNow instance.</td>
</tr>
</tbody>
</table>

**Workflows that determine the lock state of a user account**

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pwd Get Lock State - AD</td>
<td>Gets a user account lock state for the AD server.</td>
</tr>
</tbody>
</table>
### Workflows that get a user account lock state

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pwd Get Lock State - Local SN</td>
<td>Workflow to get a user account lock state for the local instance.</td>
</tr>
<tr>
<td>Pwd Get Lock State - Master</td>
<td>Master workflow to get a user account lock state.</td>
</tr>
<tr>
<td>Pwd Get Lock State - Remote SN</td>
<td>Gets a user account lock state for the remote(SOAP) ServiceNow instance.</td>
</tr>
</tbody>
</table>

### Workflows that unlock a user account

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pwd Unlock Account - AD</td>
<td>Unlocks a user account for a local instance.</td>
</tr>
<tr>
<td>Pwd Unlock Account - Local SN</td>
<td>Workflow to unlock a user account for a local instance.</td>
</tr>
<tr>
<td>Pwd Unlock Account - Master</td>
<td>Master workflow to unlock a user account.</td>
</tr>
<tr>
<td>Pwd Unlock Account - Remote SN</td>
<td>Unlocks a user account for a remote(SOAP) ServiceNow instance.</td>
</tr>
</tbody>
</table>

### Workflows that change a password

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pwd Change - Master</td>
<td>Password change master workflow.</td>
</tr>
<tr>
<td>Pwd Change – Local ServiceNow</td>
<td>Connects to a local instance to change a password.</td>
</tr>
<tr>
<td>Pwd Change – AD</td>
<td>Connects to an AD server to change a password.</td>
</tr>
<tr>
<td>Pwd Change – Remote ServiceNow</td>
<td>Connects to a remote(SOAP) ServiceNow instance to change a password.</td>
</tr>
</tbody>
</table>

### Password Reset notifications

<table>
<thead>
<tr>
<th>Name</th>
<th>Fired by event name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Reset – Send SMS Code</td>
<td>pwd.send_sms_code.trigger</td>
<td>Sends out SMS authentication code for verification.</td>
</tr>
<tr>
<td>Password Reset – New Password Confirmation</td>
<td>pwd.email.trigger</td>
<td>For the Email Password process, sends an email that includes the new password.</td>
</tr>
<tr>
<td>Password Reset URL</td>
<td>password.reset.url</td>
<td>For the Email Password Reset URL process: Sends email that includes a link to the password reset URL.</td>
</tr>
</tbody>
</table>
SOAP messages for Password Reset

<table>
<thead>
<tr>
<th>SOAP Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Password</td>
<td>When the Orchestration Add-on plugin is active, the system can use the SOAP protocol to change passwords on remote credential stores such as a remote ServiceNow instance.</td>
</tr>
<tr>
<td>Password Reset Request</td>
<td>When the Orchestration Add-on plugin is active, the system can use the SOAP protocol to reset passwords on remote credential stores such as a remote ServiceNow instance.</td>
</tr>
</tbody>
</table>

REST API

Name: Pwd Reset
API ID: pwd_reset
Base API path: /api/now/pwd_reset

Resources (Version v1)

<table>
<thead>
<tr>
<th>Name</th>
<th>Resource path</th>
<th>API Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pwd_init</td>
<td>/api/now/v1/pwd_reset/init</td>
<td>v1</td>
<td>Initial request to establish session, write logs, and fetch UI messages.</td>
</tr>
<tr>
<td>pwd_identify</td>
<td>/api/now/v1/pwd_reset/identify</td>
<td>v1</td>
<td>Get identification page components.</td>
</tr>
<tr>
<td>pwd_verify</td>
<td>/api/now/v1/pwd_reset/verify</td>
<td>v1</td>
<td>Get verification page components.</td>
</tr>
<tr>
<td>pwd_new</td>
<td>/api/now/v1/pwd_reset/reset</td>
<td>v1</td>
<td>Get resetting password page components.</td>
</tr>
<tr>
<td>pwd_success</td>
<td>/api/now/v1/pwd_reset/success</td>
<td>v1</td>
<td>Get success page components.</td>
</tr>
<tr>
<td>pwd_failure</td>
<td>/api/now/v1/pwd_reset/failure</td>
<td>v1</td>
<td>Get failure page components.</td>
</tr>
</tbody>
</table>

Password Reset Windows Application
If a user forgets the password or is locked out of a Windows computer, the user can reset the password directly from the Windows login screen.

Installer and documentation

Download the installer and installation instructions from KB0542328 in the ServiceNow Knowledge Base. The installer uninstalls any earlier version of the Password Reset Windows Application.
How the Password Reset Windows Application works

Administrators download and run an EXE or MSI file to install or distribute the application to user computers. The application installs a link on the Windows login screen. The user clicks the link (Forgot Password? in the examples on various Windows versions) and is then guided through the process of resetting the password.
By default, when a user requests a reset, the instance sends the user a URL with a user-specific token. After the user opens the URL, the instance prompts the user to enter and confirm the new password. The instance does not send a temporary password.

**Restrictions on the Password Reset Windows Application**

- The Password Reset Windows Application does not support custom verifications.
- The Password Reset Windows Application uses the base-system CAPTCHA service even if the Password Reset application is configured to use Google reCAPTCHA with the web interface. See the section titled "Settings on the Details tab" in [Configure your Password Reset or Password Change process](#).
- The Password strength indicator is not supported. See [Configure and test the Password Reset connection to a credential store](#).
- For some verification types, you can use only one verification. Custom verifications are not supported. See [Password Reset verifications](#) for details.
- Custom UI macros configured on the Process > Advanced page are not supported (for example, entry, success, or failure macros). The system displays only the default success and failure messages.
- The Password Reset Windows Application supports newline characters in the Password rule hint text. Other formatting is not supported (bold, underline, hyperlink, and so on). See [Configure and test the Password Reset connection to a credential store](#).

**Password Reset Windows Application installation requirements**

You must [activate the Password Reset Orchestration Add-on plugin](#) to use the Password Reset Windows Application.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required ServiceNow release</td>
<td>Password Reset Windows Application version 4.0 is supported on Kingston, London, and Madrid releases. Jakarta and earlier releases are not supported.</td>
</tr>
<tr>
<td>Requirement</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Required hardware</td>
<td>· 1 GHz or faster processor</td>
</tr>
<tr>
<td></td>
<td>· 512 MB of RAM</td>
</tr>
<tr>
<td></td>
<td>· 10 MB of available hard disk space (x86)</td>
</tr>
<tr>
<td></td>
<td>· 10 MB of available hard disk space (x64)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required software</td>
<td>Version of Password Reset Windows Application</td>
</tr>
<tr>
<td></td>
<td>4.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported operating systems</td>
<td>· Windows 7</td>
</tr>
<tr>
<td></td>
<td>· Windows 8.1</td>
</tr>
<tr>
<td></td>
<td>· Windows 10 Enterprise</td>
</tr>
<tr>
<td></td>
<td>· Windows 10 Pro</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported processor architecture</td>
<td>· X86</td>
</tr>
<tr>
<td></td>
<td>· X64</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported network architecture</td>
<td>· Password Reset Windows Application clients must have direct access to both the Internet and the ServiceNow instance where the Password Reset Windows Application is configured</td>
</tr>
<tr>
<td></td>
<td>· The ServiceNow SHA certificate must not be blocked by the corporate network. Information on the ServerCertificateSHA256 file appears in the documentation for Password Reset Windows Application.</td>
</tr>
<tr>
<td></td>
<td>· To reset an AD password, the client must be on the corporate network.</td>
</tr>
</tbody>
</table>

**Password Reset admin guide**

The Password Reset application enables an end user to reset or change a password using a self-service process. Alternatively, your organization can implement a process that requires a service desk agent to reset passwords for end users.

Watch the video: *Introducing Password Reset (Video)*

**Password Reset processes**

Users with the password_reset_admin role configure how the process of resetting a password works for an end user.

- **Self-service process**: Users reset passwords over the Internet using a browser on any supported interface, including mobile devices.

© 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.
- **Service desk-assisted process:** A user requests the assistance of a service desk agent, over the phone or in person. Users do not reset passwords.

**End-user experience of the self-service process**

The following example is typical:

1. On the login page, the user clicks the *Forgot Password?* link to start the process.

2. The Identify page opens and the user enters their identifying information (typically username or email address). The example includes the default CAPTCHA security feature:

![Login page screenshot](image-url)
3. On the Verify page, the user verifies their identity by providing information that proves that they are who they say they are. You, the admin, configure the method of verification and you can require multiple verifications. In the example, the admin has configured the Security Question verification. The user must answer a question to prove identity. (The user had earlier selected the question and provided a secure private answer while enrolling for the password reset process.) Other possible verifications require the user to enter a code number that was sent to a mobile device by SMS text, through the Google Authenticator app, or by email.

4. The system checks the credential store to verify identity and then displays the new password on the Reset page.
Elements of a password reset process

You configure the following elements of the process for your organization:

- A connection to the credential store for your organization where user credentials (like username/password) are securely stored.
- One or more user groups on the ServiceNow instance that can use the password reset process.
- The type of identification that users must enter to identify themselves (typically username or email address).
- One or more verifications — methods to verify the identity of the user. Examples:
  - Answer a question that only the user knows how to answer — the QA Verification (based on the Security Question verification type).
  - Enter a code number that was texted to a mobile device — the SMS verification.
How you implement a password reset process

1. Plan your implementation: Ensure that all applicable organizational guidelines, security policies, and areas of the organization are considered.

2. Set up the elements of the password reset and password change processes according to the plan:
   - Connection to the credential store.
   - User groups that will use the password reset process.
   - Identification type to use.
   - Verifications to use.

3. In the service desk-assisted model, assign service desk agents to monitor and reset passwords as needed.

4. Monitor password reset activity to identify security threats and to ensure compliance with the password policy requirements of your organization.

Password Reset Windows Application

If a user forgets the password or gets locked out of a Windows computer, the user can reset the password directly from the Windows login screen. The user clicks the Forgot Password? link and is then guided through the process of resetting the password. To learn more, see Password Reset Windows Application.

Password Change application

The Password Change application extends the Password Reset application by letting admins define how users change their passwords. Only a self-service process is supported and an admin must publish the URL to the password change form.

1. The user logs in to the instance and then selects the Change Password module or link from the user profile record.

2. On the Change Password page, the user selects the credential store where the password resides.

3. The user enters the old password and then enters and confirms a new password.

4. Workflows validate the old password and then implement the new password.

5. The system notifies the user that the password was changed.

What to do next

Plan your Password Reset processes

To ensure security and efficiency, take the time to plan your Password Reset implementation.

Role required: password_reset_admin or admin

1. Decide on the password reset process:
   - **Self-service process:** Users reset their password over the Internet using a browser on any supported interface, including mobile devices. To make the Password Reset application
with Orchestration available to all users publicly, create a new Password Reset process only for this purpose and make it accessible to all users by setting the Public access property.

- **Service desk-assisted process:** Users reset passwords by requesting the assistance of a service desk agent, over the phone or in person. Only service desk agents with the password_reset_service_desk role can reset user passwords. Watch the videos: *Resetting User Passwords (Video)* and *How to Set Up a Service Desk-Assisted Password Reset Process (Video)*.

2. Understand how groups and roles differ in their access and security needs.
   Analyze and assess how members of each group in your organization access the system. For example, if members of the sales group primarily access the system remotely, consider using a stronger method or multiple methods to verify the identity of each user.

   Identify user roles that have access to critical information and resources. For example, stronger verifications might be required for roles that have access to employee data, accounting information, or network configurations.

   Based on your analysis of groups and roles, determine the number and variety of verifications needed for the different Password Reset processes.

3. Consider how to manage credentials.
   Determine whether single sign-on is enabled with the type of directory service or other credential store used. If the directory service is configured for single sign-on, consider increasing the level of security by using multiple methods to verify identity of a user. A compromised user name and password can easily allow access to associated systems in a single sign-on environment.

4. Consider how to implement enrollment in the Password Reset program.
   For example, will enrollment be optional or required? Will users be auto-enrolled? How will users be notified to enroll in the program? The answers to these questions will help you determine the appropriate verification types to use.

5. Consider which Password Reset options to offer to users.
   - If your organization uses single sign-on, how will users reset their password if they are unable to log on?
   - What options are available to users working off-site?

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).

   Preview email

   Hello
   A password reset was requested for your user account on the ServiceNow instance https://demonightyplatformsecurity.service-now.com/
   Click here to reset your password. If you do not want to reset your password, please disregard this email.
   
   The link will expire in 12 hours.
   If you did not request this password reset, please notify your company's ServiceNow administrator.

6. The Reset Password page guides the user to reset the password.
The default self-service Password Reset process (com.glideapp.password_reset) defines:

- The URI that specifies where users are redirected when they click Forgot Password. By default, this value is /$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.

---

**Configure your Password Reset or Password Change process**

To implement the process, you configure credentials, verifications, and users.

Role required: password_reset_admin or admin

1. Be sure to Plan your Password Reset processes.
2. Create the credential store record for user names and passwords that are managed.

**Note:** For LDAP integrations: If the Active Directory settings require users to reset the password when logging in, the results depend on the password reset plugin that is installed.
• The Password Reset plugin cannot change an AD password. End users will not be able to log in to the instance.
• The Self Service Password Reset plugin depends on the Password Reset Basic plugin. Self-service is intended for password reset only on the local ServiceNow instance and cannot change an AD password.
• The Password Reset Orchestration Add-on plugin is built on top of Orchestration AD activities. The plugin supports changing the AD password.

3. Define the verifications that the process will use.

A Password Reset process consists of the following elements:
• The credential store that contains user login credentials.
• Optionally, the user groups that are authorized to use the Password Reset process.
• The verifications (extension script includes) that verify the identity of the requesting user and that enable the service desk agents to authorize reset of the password.

1. Navigate to Password Reset > Processes.
2. Click New and then specify a meaningful Name and Description for the process.
3. Select the Credential store that contains the user credentials that the process applies to.
4. Specify the process that you are defining: Select the Password Reset check box and/or the Password change check box.
5. Specify the Apply to all users setting.

<table>
<thead>
<tr>
<th>Apply to all users setting</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selected</td>
<td>All users use the process that you are defining. This setting is useful only if all users have access to the authentication methods that are defined in this process.</td>
</tr>
<tr>
<td>Not selected</td>
<td>Only the users in the groups that you specify use the process. You specify the groups in the Groups related list.</td>
</tr>
</tbody>
</table>

6. If you selected Password Reset, fill in the Password Reset Details tab and, optionally, the Advanced tab. See Settings on the Password Reset Details tab and Settings on the Password Reset Advanced tab.
7. Save the form. The form refreshes and additional related lists appear.
8. From the Password Reset Process Verifications related list, select one or more verifications. See Password Reset verifications.
9. Optional: From the Password Reset Process Groups related list, select the user groups that will use the process that you are defining.
The Password Reset Process Groups related list appears only if the Apply to all users check box is not selected.
10. Select the Active check box to enable the Password Reset process that you configured. The check box is available only after the record has been saved.
11. Click Update.
12. Navigate to Password Reset > Properties to set the properties that configure the Password Reset experience for end users.

Credential stores for Password Reset
Credential stores hold user information such as user names and passwords that can be used as login credentials. Examples include the User (sys_user) table or an Active Directory server.
Users with the password_reset_admin or password_reset_credential_manager role can create and modify connections to credential stores.

**Credential store types installed with the base system**

A credential store type is a set of workflows that specify how to connect to a credential store. Navigate to Password Reset > Credential Stores to view the list of example credential stores that are based on the base-system types. The base system includes the following credential store types:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local ServiceNow Instance</td>
<td>Represents the current (local) ServiceNow instance.</td>
</tr>
<tr>
<td>AD Credential Store</td>
<td>Represents an Active Directory credential store. Installed with the Orchestration Add-on plugin.</td>
</tr>
<tr>
<td>Remote (SOAP) ServiceNow instance</td>
<td>Represents a remote ServiceNow Instance. Installed with the Orchestration Add-on plugin.</td>
</tr>
</tbody>
</table>

**Remote credential stores**

A remote credential store refers to any credential store other than the local ServiceNow instance. Remote credential stores, such as Active Directory, manage user names and passwords outside of the local instance. A remote credential store can also be a remote ServiceNow instance, a UNIX or Linux server, or any other directory-like service that relies on the SOAP protocol. The Password Reset Orchestration Add-on plugin is required to connect to remote credential stores. Review the information in the section on credential store types before you create, test, or delete credential stores.

**Connection workflows for credential store types**

A credential store type workflow requires a subflow that defines how to connect to the store, and can include an optional subflow that defines how to test the connection. Use the Pwd reset – AD and Pwd Reset - Local subflows as models for your custom connection workflows.
Pwd Reset Local sub workflow
Creating a custom credential store type

You can use a credential store type as a model to create a custom type. See Create a credential store type for Password Reset.

Configure and test the Password Reset connection to a credential store

You specify a credential store to access during the Password Reset or Password Change process and configure other settings that control the process.

Role required: password_reset_admin or password_reset_credential_manager

**Note:** The Password Reset Windows Application supports only Active Directory (AD) credential stores.

1. Navigate to **Password Reset > Credential Stores**.
2. Click **New**, enter a unique and meaningful **Name** and **Description**, and then fill in the form.

<table>
<thead>
<tr>
<th>Type</th>
<th>You can use credential store types (templates that provide a desired set of capabilities). Credential stores inherit the functionality of the credential store type.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong></td>
<td>The Password Reset Windows Application supports only AD Credential Store.</td>
</tr>
</tbody>
</table>

Installed credential store types:

- **Local ServiceNow Instance** installed with Password Reset.
- **AD Credential Store** installed with the Orchestration Add-on.
- **Remote (SOAP) ServiceNow** installed with the Orchestration Add-on.
| **Auto-generate password** | Script include that generates a temporary password for use during the reset process.  

**Note:** If you select the **Enforce history policy** check box, then you must specify a value for **Auto-generate password**. |

| **Enforce history policy** | **Note:** This option appears only if you select a credential store **Type of AD Credential Store**.  

To enforce the history policy that is configured for the credential store:  
1. Select the **Enforce history policy** check box.  
2. Follow the procedure that appears after this table.  

**Note:** Active Directory domains can be configured to include a history policy that ensures that users do not reuse passwords. For example, the history policy might be configured to not allow the user to reuse any of the previous three passwords when resetting a password. |

| **Hostname** | URL or IP address of the credential store that contains the user credential (for example, user names and passwords). |
| **User account lookup** | Script include that maps the user ServiceNow platform ID to the user credential store ID. A default script, `PwdDefaultUserAccountLookup`, returns the user ServiceNow platform user name. |
| **Password rule hint** | Text that appears on the password reset page to help the user to create a password that meets all requirements. The **Password rule script** enforces the requirements.  

**Note:** The Password Reset Windows Application supports newline characters in the hint. Other formatting is not supported (bold, underline, hyperlink, and so on). |
| **Password rule** | Client script that validates the password that the user enters. The script is invoked when the user enters a new password and clicks **Password Reset**. You can use the script to enforce password strength/complexity requirements. |
| **Enable Password Strength** | Select the check box to:  
- Display the text box for the **Strength rule script** so you can update the script.  
- Display the graphical **Password Strength** bar to the user while the user changes or resets the password.  

**Note:** The Password Reset Windows Application does not support **Password Strength**. |
3. Click **Submit**.
   The connection is created. You should test the connection to a credential store after you configure a new credential store or when users experience problems that might involve the connection.

4. Navigate to **Password Reset > Credential Stores** and then open the credential store.

5. In the header bar, click **Save and Test Connection**.
   A progress page displays the result of the test.

If you selected the **Enforce history policy** check box, then follow these steps:

1. Open the associated Password Reset process definition: **Password Reset > Processes**.

2. On the Details tab of the Password Reset Process form, clear the **Auto-generate password** check box and then save the process definition.

3. On the domain controller, set **Password Aging** (MIN_PASSWORD_AGE) to zero.

4. On the domain controller, set the history policy to twice the desired number of passwords. For example, to enforce that the last three passwords are not repeated, set the history policy to six.

   **Note:** To enforce the history policy that is configured for the credential store, the system auto-generates a new temporary password for each reset cycle. The system auto-generates the temporary password even though you have cleared the **Auto-generate password** check box on the Password Reset Process form. Because the user immediately replaces the temporary password with a new password, two passwords are created for each reset cycle.

**Set up SOAP credentials for Password Reset**

© 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 the Orchestration Add-on plugin is activated, the ServiceNow platform can use the SOAP protocol to interact with remote credential stores such as a remote ServiceNow instance.

Role required: admin or web_service_admin

1. Navigate to **System Web Services > Outbound > SOAP Message**.
2. Click **Password Reset Request**.
3. From the **Soap Message Functions** related list, configure both the **password_reset** and **sys_user_get_record** functions by completing the following steps.
   a) In **Basic auth user ID**, enter the user ID for the remote system user who has privileges to update records on the User [sys_user] table.
   b) In **Basic auth user password**, enter the password for the remote system user who has privileges to update records on the User [sys_user] table.
   c) Select **Use basic auth**.
   d) Click **Update**.

You do not need to enter a value in the **SOAP endpoint** field. The field shows the name of the ServiceNow instance used for Password Reset.

**Configure Password Reset for Active Directory**

When the Orchestration Add-on plugin is activated, the Password Reset application can change passwords on an Active Directory credential store. The application changes passwords by referencing an Active Directory user role with the appropriate password change privileges.

Active Directory must have a user role with the following privileges:

**Descendent User objects:**
- Reset password
- Read/Write pwdlastset
- Read/Write UserAccountcontrol
- Write Account Restrictions
- Read/Write lockouttime
- Read MemberOf

**Descendent Group objects:**
- Read Members
- Read MemberOf

1. **Install MID Server** on a Windows computer that can connect to Active Directory.
2. **Configure the MID Server**.
3. In the ServiceNow instance, navigate to **Orchestration > Credentials**.
4. Click **New** and then complete the form with the following values for the credential.
   - **Type**: Select Windows.
   - **User name**: Enter your Active Directory domain user. For example, domain\admin.
   - **Password**: Enter your Active Directory domain user password.
   - **Applies to**: Select the MID Server that is used to access the Active Directory server.
5. Click **Submit**.
6. Create a credential store for Active Directory.

Delete a connection to a credential store for Password Reset.
Important: Before you delete the connection to a credential store, check all Password Reset processes to ensure that the credential store is not in use. If the credential store is being used by a process, update the process before deleting the credential store.

Role required: password_reset_admin or password_reset_credential_manager

1. Navigate to Password Reset > Credential Stores and then select the check box for the credential store.
2. In the Actions choice list, select Delete.

Password Reset verifications

Each verification specifies the method and process for verifying the identity of the user that is requesting password reset.

Verifications included with Password Reset

The Password Reset application includes the following verifications in the base system. You can create a verification based on either a base-system verification or a verification type (a template).

---

### Note:
The Password Reset Windows Application does not support custom verifications.

<table>
<thead>
<tr>
<th>Verification</th>
<th>Description</th>
</tr>
</thead>
</table>
| QA verification | Implements a self-service Password Reset model with questions that are included with the base system or custom questions that the admin defines. While enrolling for the process, the user decides which questions to provide answers for. 

When a user requests password reset, the system poses a specified number of the questions that the user selected during enrollment. The user must answer all questions correctly to verify identity.

This verification is based on the Security Questions verification type. 
For information on the user enrollment experience, see Users: Enroll in the Password Reset program using questions and answers. |
| SMS verification | Implements a self-service or service desk-assisted Password Reset model that relies on auto-generated code numbers. 

When a user requests password reset, the system sends a code to an SMS-capable device that the user has authorized. To verify identity, the user then submits the code on the Password Reset Verify page.

You can use the ServiceNow Notify feature to send the codes.

This verification is based on the SMS Code verification type. 
For information on the user enrollment experience, see Users: Enroll in the Password Reset program using SMS codes. |
| Personal Data — Confirm Email Address | Implements a self-service Password Reset model that relies on user information that is available in the user profile on the instance. 

This verification is based on the Personal Data Confirmation verification type. |
| Personal Data — Enter User Name | Implements a self-service Password Reset model that relies on user information that is available in the user profile on the instance. 

This verification is based on the Personal Data verification type. |
Verifications included with the demo data

The following demo data is based on the Mock verification type:
- Sample Mock verification #1
- #2

Personal data identification types and confirmation type verifications

Personal data verifications allow users to verify their identity by providing answers to questions that are generated from personal information stored in the User table [sys_user].

Personal data identification types

The Password Reset application provides the email and username identification types. You can use either type as provided or as a model to create a custom identification type.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Identification</td>
<td>Identifies users by their email addresses.</td>
</tr>
<tr>
<td>Username Identification</td>
<td>Identifies users by their user names.</td>
</tr>
</tbody>
</table>

Personal data confirmation verifications

- **Personal data verification**: If users are associated with a Password Reset process that uses a personal data verification, the users are typically not required to enroll for Password Reset.
- **Personal data confirmation verifications** allow employees with the password_reset_service_desk role to access personal data from the sys_user table when assisting a user with a password reset request.

To configure personal data and personal data confirmation verifications, you specify parameters as name/value pairs that correspond to a particular piece of user information. For example, to verify users by their email address:

1. Set the **label** parameter (the text that the end user should see) to Email (that is, label=Email).
2. Set the **column** parameter (the column in the table that holds the verification data) to email (that is, column=email).

   **Note**: You can use only one set of name/value pair parameters per verification. Additional parameters are ignored.

To use multiple pieces of personal information for user verification, create more personal data or personal data confirmation verifications and add the verifications to the related Password Reset process.
Personal data and personal data confirmation type verifications

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| label          | Label that the user sees during the password reset request.  
|                | Data Type: string  
|                | Default Value: n/a |
| column         | Column of the sys_user table that provides the data that is used to verify the identity of the user.  
|                | Data Type: string  
|                | Default Value: n/a |

SMS Code Verification type for Password Reset

Using the Simple Message Service (SMS) Code Verification type, a user can verify identity through any SMS-enabled device, like a cell phone that accepts text messages. When a user requests password reset, the system sends a numerical code to the device and the user enters the code on the password reset page.

You can change the default behavior of an SMS code verification using either of the following methods:

- Set parameter values, as shown in the table
- Update property settings for the Password Reset application

**Note:** The system allows only one instance of each SMS code parameter.

SMS Code Verification type parameters

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Description</th>
</tr>
</thead>
</table>
| expiry         | Number of minutes the verification code is valid.  
|                | **Data Type:** integer (any positive integer)  
|                | **Default Value:** 5 |
| complexity     | Number of digits in the numerical verification code.  
|                | **Data Type:** integer (any positive integer)  
|                | **Default Value:** 4 |
| pause_window   | Number of minutes before the user can request another SMS code for verification.  
|                | **Data Type:** integer (any positive integer)  
|                | **Default Value:** 2 |
| max_per_day    | Maximum number of codes sent for verification in one day.  
|                | **Data Type:** integer (any positive integer)  
|                | **Default Value:** 10 |

Use NotifyNow to send SMS codes for enrollment and verification
You can configure the Password Reset application to send SMS codes for enrollment and verification using ServiceNow NotifyNow (via Twilio SMS Messaging). NotifyNow is tightly integrated with the workflow engine and business rules and delivers a highly configurable and trusted way to deliver SMS messages.

Role required: admin

NotifyNow requires a separate contract with Twilio.

1. Enroll for a Twilio account and telephone number at [https://www.twilio.com/](https://www.twilio.com/)
2. Activate the Notify plugin.
3. Associate the Twilio account with Notify.

No other configuration is required. Users who request password change or reset receive SMS codes through NotifyNow.

Settings on the Password Reset Details tab
The settings define the user experience when resetting or changing a password.

The Password Reset Details tab appears when you are configuring a Password Reset process (Password Reset > Processes).

**Password Reset Details tab**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public access</td>
<td>The check box is available only when Password reset is selected.</td>
</tr>
<tr>
<td></td>
<td>• Clear the check box to define a service desk-assisted process in which only service desk agents and not users can reset a password.</td>
</tr>
<tr>
<td></td>
<td>• Select the check box to enable a self-service process with public user access to the Password Reset or Password Change form through a URL.</td>
</tr>
<tr>
<td>Public URL</td>
<td>This field is available only when Public access is selected.</td>
</tr>
<tr>
<td></td>
<td>URL of the page where users go to reset or change the password. The value from the URL suffix field is appended to the URL when you tab out of the URL suffix field. For the Default self-service Password Reset process, this value must be /$pwd_reset.do?sysparm_url=ss_default.</td>
</tr>
<tr>
<td>URL suffix</td>
<td>This field is available only when Public access is selected.</td>
</tr>
<tr>
<td></td>
<td>Suffix used to create a unique URL for the Password Reset or Password Change form.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Display CAPTCHA     | This check box is available only when **Public access** is selected. Select the check box to display a CAPTCHA on the user identification page. The Password Reset application uses Google reCAPTCHA as the default CAPTCHA service. See *Configure Google reCAPTCHA*.  
  **Note:** The Password Reset Windows Application uses the base-system CAPTCHA service even if the Password Reset application is configured to use Google reCAPTCHA.  
  To use the CAPTCHA service that is provided with the base system, change the `password_reset.captcha.google.enabled` system property to `false`.  
  **Note:** Because on-premises instances do not have access to the Internet, they cannot use the Google reCAPTCHA service. Set the `password_reset.captcha.google.enabled` property to `false` for on-premises instances. |
| Identification type | Method that the user employs to claim their identity for the public Password Reset or Password Change process. Any selection overrides the default identification that is associated with the process.  
  The base system includes the **Email** and **Username Identification** identification types. You can create a custom identification type (some knowledge of JavaScript is recommended).  
  See *Personal data identification types and confirmation type verifications*. |
| Minimum verifications | Number of verifications that a user must successfully submit to reset the password.  
  If the number exceeds the number of mandatory verifications, then the user must submit enough additional optional verifications to meet the number specified for **Minimum verifications**.  
  By default during the password reset process, the system presents optional verifications to the user based on the **Order** values for the verifications.  
  **Note:** Each user must submit all mandatory verifications regardless of the number specified. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Password Reset URL</td>
<td>Select the check box to enable users to reset the password by clicking a link in an email that the instance sends to them. By default, the self-service Password Reset processes enable this option. When you select this option, the <strong>Auto-generate password</strong> check box is not available.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> See <em>Example: The default self-service Password Reset process</em> for an outline of the process that is enabled by default.</td>
</tr>
<tr>
<td>Enable account unlock</td>
<td>This check box is available only when <strong>Password reset</strong> is selected. Select the check box to allow user accounts on credential stores to be unlocked without resetting the password.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Not supported by the default self-service Password Reset process.</td>
</tr>
<tr>
<td>Unlock user account</td>
<td>Select the check box to unlock user accounts on credential stores after a password reset.</td>
</tr>
</tbody>
</table>
| Auto-generate password        | This check box is available only when:  
· The **Password reset** check box is selected.  
· The **Email Password Reset URL** check box is not selected  
Select the check box to auto-generate a new password for the user. When this check box is selected, you must select the **Email password** or **Display password** check box, or both. This setting is useful for service desk-assisted processes.                                                                                           |
<p>|                               | <strong>Note:</strong> Clear the check box to enable the <strong>Enforce history policy</strong> option for a credential store. See <em>Configure and test the Password Reset connection to a credential store</em>.                                                                                                                                                  |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User must reset password</td>
<td>This check box is available only when Auto-generate password is selected. Select the check box to require users to reset their password immediately after logging in with the auto-generated password.</td>
</tr>
<tr>
<td>Note:</td>
<td>Users whose credentials are held in the local ServiceNow instance credential store are prompted to change their password the first time that they log in. Users whose credentials are held in an Active Directory credential store are not prompted to change their passwords in the instance. Such users must change their passwords from a computer on the domain.</td>
</tr>
</tbody>
</table>

| Display password       | This check box is available only when Auto-generate password is selected. Select the check box to display the new password on the screen. In a self-service process, the password appears on the user screen. In a service desk-assisted process, the password appears on the service desk agent screen. |

| Email password         | This check box is available only when Auto-generate password is selected. Select the check box to email the new password to the user. The setting is useful in both self-service and service desk-assisted processes. The setting can add a layer of security by requiring that users access their email to view the password. In a service desk-assisted process, emailing the password to users ensures that only the user requesting the password reset can view the password. |

| Related lists          |                                                                                                                                                                                                     |
| Verifications          | This related list is available only after the record has been saved. One or more verifications that the process uses. See Password Reset verifications.                                                   |
| Groups                 | The Groups related list is available only after the record has been saved and if the Apply to all users check box is cleared. ServiceNow user groups to associate with the Password Reset process. |

Configure Google reCAPTCHA

To use the Google reCAPTCHA service, instances that are running on a domain other than service-now.com require an API key pair from Google. The process described in this topic is optional for instances that are running on the service-now.com domain.

Role required: admin
Note:

Because on-premises instances do not have access to the Internet, they cannot use the Google reCAPTCHA service. Do not follow the process described in this topic. Instead, set the `password_resetcaptcha.google.enabled` system property to `false`. This setting enables the CAPTCHA service that is provided with the base system.

The Password Reset Windows Application uses the base-system CAPTCHA service even if the Password Reset application is configured to use Google reCAPTCHA.

1. Request an API key pair (a site key and a secret) from Google at [https://www.google.com/recaptcha](https://www.google.com/recaptcha)
2. Set the following system properties:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| `password_resetcaptcha.google.enabled` | Set to `true`.  
Type: string  
Default: `true` |
| `google.captcha.site_key`           | Set to the site key that Google provided.  
Type: string  
Default: A site key that Google provided to ServiceNow |
| `google.captcha.secret`             | Set to the secret that Google provided.  
Type: password2  
Default: An encrypted secret that Google provided to ServiceNow |

Settings on the Password Reset 'Advanced' tab

UI macros and script includes can extend the basic functionality of a Password Reset process.

The Advanced tab appears when you are configuring a Password Reset process (**Password Reset > Processes**).

**Advanced tab**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry UI macro</td>
<td>UI macro that displays a customized message to users when they access the initial Password Reset screen.</td>
</tr>
<tr>
<td>Success UI macro</td>
<td>UI macro that displays a customized message to users on the final Password Reset screen when their password is successfully reset.</td>
</tr>
<tr>
<td>Failure UI macro</td>
<td>UI macro that displays a customized message to users on the final Password Reset screen when their password reset fails.</td>
</tr>
<tr>
<td>Post reset script</td>
<td>Script include that performs actions after the Password Reset process completes whether the outcome is success or failure. For more information on customizing post processor scripts, see the Post reset script category as described in [Password Reset extension scripts](Password Reset extension scripts).</td>
</tr>
</tbody>
</table>

Configure the number of questions for a 'Security Questions' verification

When designing a Security Questions verification for Password Reset, you can specify the number of questions to display when users enroll and the number to display when a user requests password reset.
Role required: password_reset_admin or admin

1. Navigate to **Password Reset > Verifications** and then open a verification that uses the **Security Questions Verification Type**.
2. Configure the parameters in the **Password Reset Verification Parameters** related list.

### Parameters for Security Questions Verification

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| num_enroll     | Number of security questions that are displayed while a user is enrolling for Password Reset.  
**Data Type:** Positive integer that does not exceed the number of questions in the security questions list (**Password Reset > Security Questions**).  
**Default Value:** 5 |
| num_reset      | Number of security questions that are displayed while a user is attempting to reset the password. The questions are selected at random and are presented in random order.  
**Data Type:** Positive integer that does not exceed the value of the num_enroll parameter  
**Default Value:** 3 |

3. Click **Update**.

### Configure the required strength for passwords

The password that a user defines must meet certain requirements — it must contain at least eight characters, it must include a numeral, and so on. You can configure the requirements as needed for your organization.

Role required: password_reset_admin

The base system includes example credential stores with various password requirements. You can modify password requirements and provide users with hints for creating password. The default requirements for a new password are:

- At least eight characters
- At least one uppercase and one lower case letter
- At least one numeral

**Note:** This topic describes the procedure for configuring password strength requirements only. You can configure several other settings for the credential store, as described in **Configure and test the Password Reset connection to a credential store**.

1. Navigate to **Password Reset > Credential Stores**.
2. Select the credential store in the list and then configure the following settings:
Password rule hint

Text that appears on the password reset page to help the user to create a password that meets all requirements. The Password rule script enforces the requirements.

**Note:** The Password Reset Windows Application supports newline characters in the hint. Other formatting is not supported (bold, underline, hyperlink, and so on).

Password rule

Client script that validates the password that the user enters. The script is invoked when the user enters a new password and clicks Password Reset. You can use the script to enforce password strength/complexity requirements.

Enable Password Strength

Select the check box to:
- Display the text box for the Strength rule script so you can update the script.
- Display the graphical Password Strength bar to the user while the user changes or resets the password.

**Note:** The Password Reset Windows Application does not support Password Strength.

Strength rule

This text box appears only if you select Enable Password Strength.

**Note:** The Password Reset Windows Application does not support Password Strength.

Client script that calculates the strength/complexity of the password that the user enters. The script is invoked when the user begins to enter a new password during the reset process.

Default settings:
- Selected for local ServiceNow credential stores
- Not selected for other credential stores

**Note:**
To guide the user during the reset process, the system displays a graphical bar labeled Password Strength under the New password field.

---

3. Click **Submit**.
   You should test the connection to a credential store after you configure a new credential store or when users experience problems that might involve the connection.

4. Navigate to **Password Reset > Credential Stores** and then open the credential store.

5. In the header bar, click **Save and Test Connection**. A progress page displays the result of the test.
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.

<table>
<thead>
<tr>
<th>SNC User Lockout Check with Auto Unlock</th>
<th>Uses the value of the <code>glide.user.max_unlock_attempts</code> property to set the limit for failed login attempts.</th>
</tr>
</thead>
<tbody>
<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.

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 three 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 five and seven.

1. Navigate to **Password Reset > Properties**.
2. Update settings as needed and then click **Save**.

### Password Reset properties

<table>
<thead>
<tr>
<th>Label on the Password Reset Properties page</th>
<th>Property name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Reset Global properties</td>
<td><code>password_reset.wf.refresh_rate</code></td>
<td>Time period in milliseconds between checks on status of the workflow.</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>Label on the Password Reset Properties page</th>
<th>Property name</th>
<th>Description</th>
</tr>
</thead>
</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.

Password Reset Request properties

| Number of unsuccessful attempts allowed to reset/change password | password_reset.request.max_attempt | Number of password reset attempts a user has before they are locked out for a period determined by the value in max_attempt_window.  
  - Type: integer  
  - Default value: 3 (attempts) |
| 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) |
| 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) |
<table>
<thead>
<tr>
<th>Label on the Password Reset Properties page</th>
<th>Property name</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 that a user is allowed to perform the Password Reset process.  
- Type: integer  
- Default value: 10 minutes |
| 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 |
| Number of security questions required during the password reset request | password_reset.qa.num_reset | Number of questions that a user must answer to verify identity during the Password Reset process.  
- Type: integer  
- Default value: 3 questions  
- Possible values: Integers that are less than the number specified for the num_enroll property. |

**Note:** You can override this security question property by adding the num_reset parameter in the security question verification.
<table>
<thead>
<tr>
<th>Label on the Password Reset Properties page</th>
<th>Property name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Number of security questions required during enrollment | password_reset.qa.num_enroll | During the enrollment process, the number of questions that a user must answer to be enrolled in the Password Reset program.  
- Type: integer  
- Default value: 5 (questions)  

**Note:** You can override this security question property by adding the `num_enroll` parameter in the security question verification. |

<table>
<thead>
<tr>
<th>Password Reset SMS Code properties</th>
<th>Property name</th>
<th>Maximum number of SMS codes sent for verification per day</th>
<th>Description</th>
</tr>
</thead>
</table>
|                                   | password_reset.sms.max_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. |
<table>
<thead>
<tr>
<th>Label on the Password Reset Properties page</th>
<th>Property name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of digits in the SMS code sent to the user</td>
<td>password_reset.sms.default_complexity</td>
<td>Number of characters required for a user to reset their password.</td>
</tr>
<tr>
<td>Time interval, in minutes, for counting blocked users</td>
<td>password_reset.activity_monitor.incident_window</td>
<td>Time window to count the number of blocked users.</td>
</tr>
<tr>
<td>Number of blocked users, in the defined time interval, that triggers a system log event</td>
<td>password_reset.activity_monitor.incident_threshold</td>
<td>Number of blocked (or locked) users, within the specified time window, that triggers a system log event.</td>
</tr>
</tbody>
</table>

**Note:** Several components in the Self Service Password Reset (com.snc.password_reset) plugin and the Password Reset (com.glideapp.password_reset) plugin control the password reset flow. The following properties affect Password Reset, but do not appear on the Password Reset > Properties page:

- You can add the glide.pwd_reset.onetime.token.validity property to the System Properties (sys_properties) table to specify the number of hours that the Password Reset token should be valid. Default: 12.
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.

**Customizing Password Reset processes**

Password Reset scripting enables you to customize Password Reset by creating your own credential store, verification, and identification types, and extend them by defining extension scripts. You can also create a custom credential store type, custom verification type, or verification.

Password Reset scripting is available to users with the `password_reset_admin` role. The easiest way to customize Password Reset is:

1. Create custom types and scripts as described in **Password Reset extension scripts**.
2. Follow the configuration steps described in **Configure your Password Reset or Password Change process**.
3. Select the new types that you created. You can customize the following components:
   - Credential store types: Define new types for how to connect to your credential stores by creating custom workflows for connection and testing. See **Create a credential store type for Password Reset**.
   - Verification types: Define new types for how users are verified. See **Create a custom Password Reset verification type**.
   - Identification types: Define new types for how users can identify themselves. See **Create a custom identification type for Password Reset**.

**Extension scripts**

Extension scripts enable you to extend Password Reset functionality by defining custom scripts that can be used in a credential store, verification, or identification type, or as a post-processor in a process. Extension scripts are predefined hooks within the Password Reset application that perform specific types of behavior defined by the extension category, which refers to where the script will be used. See **Password Reset extension scripts**.

Create a credential store type for Password Reset

You can create a custom credential store type if the base-system types do not meet your needs.

Role required: `password_reset_admin` or `password_reset_credential_manager`

1. Navigate to **Password Reset > Extensions > Credential Store Types**.
2. Click **New**, enter a unique and meaningful **Name** and **Description**, and then fill in the form.

**Note:** You may need to configure the form to see the **Get user lock state** workflow and the **Unlock user** workflow.
3. **Click Submit.**

Create a custom question for a 'Security Questions' verification

To enroll for the 'Security Questions' verification, the user selects several questions and supplies answers that only the user knows. You can add a custom question to the set of questions that are included with the base system.

Role required: password_reset_admin or admin

The default language is English, and you can create a custom question in a non-English language. If you create the appropriate non-English language questions, then the questions appear in the language that the user requested during login.

1. Navigate to **Password Reset > Security Questions** and then click **New**.
2. Enter the English language question in the **Security question** field and then click **Submit**. The question appears in the Translations related list.
3. To add the same question in another language, complete the following steps.
   a) Click the English language question to translate.
   
   **Note:** Do not change the **Language** value for the default questions that come with the base system.

   b) On the Password Reset Question page, in the Translations related list, click **New**.
   c) Select the language in the **Language** field.
d) Enter the non-English text in the **Security question** field.
e) Click **Submit**.

The question appears in the Translations related list on the Password Reset Question page. If a user selects the language while logging in, then the verification question appears in that language.

Create a custom identification type for Password Reset

A custom identification type enables the user to enter alternative verification information such as an employee ID while resetting the password.

Role required: password_reset_admin or admin

1. Navigate to **Password Reset > Extensions > Identification Types**.
2. Click **New**, enter a unique and meaningful **Name** and **Description**, and then fill in the form.

<table>
<thead>
<tr>
<th>Identification field label</th>
<th>Text to display as a label for the Identification field.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification processor</td>
<td>Identification processor script. Choose an existing script, or create your own using the Identification form processor category (extension script).</td>
</tr>
</tbody>
</table>

3. Click **Submit**.

Create a Password Reset verification from an existing verification

The Password Reset application includes several example verifications that you can use as they are or as the basis for a custom verification. If the verification types in the base system do not meet your needs, you can create a custom verification type.

Role required: password_reset_admin

---

**Note:** The Password Reset Windows Application does not support custom verifications. Custom verifications might work, but you must test and verify.

1. Navigate to **Password Reset > Verifications** and select a verification.
2. If needed, modify the parameters on the **Password Reset Verification Parameters** tab. The parameters are described in the instructions for the type of verification that you are working on.
3. Click **Submit**.
4. Each verification type has properties that control the user experience. Review the property settings and update as needed.

Create a custom Password Reset verification type

If the verification types in the base system do not meet your needs, you can create a custom verification type.

Review the verification types that are provided in the base system to determine whether to create a custom verification type. Then review the verification type components to develop.

Role required: password_reset_admin or admin

1. Navigate to **Password Reset > Extensions > Verification Types**.
2. Click **New**, enter a unique and meaningful **Name** and **Description**, and then fill in the form.
ServiceNow  Jakarta  Now Platform Capabilities

<table>
<thead>
<tr>
<th>Enrollment check</th>
<th>Script to check whether a user is enrolled for verification. Automatic enrollment requires an enrollment check. If no script is specified when Automatic Enrollment is selected, a default script is provided.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic enrollment</td>
<td>Indicator for whether users are auto-enrolled. If Automatic enrollment is not selected, then you must provide an enrollment UI macro and enrollment processor script.</td>
</tr>
<tr>
<td>Enrollment UI</td>
<td>Enrollment UI macro that provides the UI for the enrollment.</td>
</tr>
<tr>
<td>Enrollment processor</td>
<td>Enrollment processor script that processes the enrollment.</td>
</tr>
<tr>
<td>Verification UI</td>
<td>Verification UI macro that provides the UI for the verification.</td>
</tr>
<tr>
<td>Verification processor</td>
<td>Verification processor script (extension scripts) that processes the verification.</td>
</tr>
</tbody>
</table>

3. Click Submit.

Create a custom Password Reset verification

Use a verification type in the base system as a template to design a custom verification. The Password Reset Windows Application does not support custom verifications.

Role required: password_reset_admin

Verification types in the base system

<table>
<thead>
<tr>
<th>Personal Data Confirmation Verification Type</th>
<th>Verifies user identity using data from the User (sys_user) table. The user data is displayed to a service desk agent. The agent verifies the data. Enrollment is not required for this type. Recommended for service desk-assisted processes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note: The Password Reset Windows Application does not support the Personal Data Confirmation Verification type.</td>
<td></td>
</tr>
<tr>
<td>See Personal data identification types and confirmation type verifications.</td>
<td></td>
</tr>
<tr>
<td>Personal Data Verification Type</td>
<td>Verifies user identity using data from the User (sys_user) table. The user is required to answer questions. Enrollment is not required for this type.</td>
</tr>
<tr>
<td>Note: The Password Reset Windows Application allows you to define and use multiple verifications of the Personal Data type.</td>
<td></td>
</tr>
<tr>
<td>See Personal data identification types and confirmation type verifications.</td>
<td></td>
</tr>
<tr>
<td>Security Questions Verification Type</td>
<td>Verifies user identity by presenting personal security questions that the user must answer correctly.</td>
</tr>
<tr>
<td>Note: The Password Reset and Password Reset Windows Application support only a single verification of the Security Questions type.</td>
<td></td>
</tr>
<tr>
<td>See Create a custom question for a 'Security Questions' verification.</td>
<td></td>
</tr>
</tbody>
</table>
| SMS Code Verification Type | When a user requests password reset, the system sends a code to an SMS-capable device that the user has authorized. To verify identity, the user then enters the code on the Password Reset web page.  

**Note:** The Password Reset and Password Reset Windows Application support only a single verification of the SMS Code type.  

See [SMS Code Verification type for Password Reset](#). |
| --- |
| Mock Verification Type | Not a functional identity verification. Demonstrates how to add a verification type in a Password Reset process.  

**Note:** The Password Reset Windows Application does not support the Mock verification type.  

- The enrollment UI macro for this verification gets the user input and returns the entered value in the enrollment processor.  
- The Password Reset UI macro for this verification gets input from the user and returns the entered value through the verification processor. |

1. Navigate to **Password Reset > Extensions > Verification Types**.  
2. Click **New**, enter a unique and meaningful **Name** and **Description**, and then fill in the form.  

| Type | Create verifications based on one of the verification types in the base system.  

Password Reset supports the following types. You can create multiple instances of any type.  

- Personal Data Confirmation Verification  
- Personal Data Verification  
- Security Question Verification  
- SMS Code Verification  

The Password Reset Windows Application supports the following types:  

- Personal Data Verification. You can create only a single instance.  
- Security Question Verification. You can create multiple instances.  
- SMS Code Verification. You can create only a single instance.  

<table>
<thead>
<tr>
<th>Order</th>
<th>Position of the verification as it appears on the Enrollment form and Password Reset form.</th>
</tr>
</thead>
</table>
| Password Reset Verification Parameters | Parameters used by a verification to configure specific behaviors, like number of questions required to enroll, request expiration time, and columns used. Set parameters for any behavior that should be different from the default specified in the Password Reset properties.  

The available parameters are described separately for each verification type. |

3. Click **Submit**.  
4. Each verification type has properties that control the user experience. Review the property settings and update as needed.  

Enrollment options for the Password Reset service  
You can configure the Password Reset process to enroll users automatically, or you can define an enrollment check.
To define an enrollment check, you must define:

- An enrollment processor script, which specifies how enrollment is processed
- A corresponding enrollment UI macro, which specifies how the enrollment information is displayed to the user

The following example uses `PwdEnrollSMSProcessor` as the enrollment processor script and `pwd_enroll_sms_ui` as the enrollment UI macro.

![Password Reset Verification Type](image)

A verification type must also define a verification processor script and a corresponding verification UI macro. The example uses `PwdVerifySMSProcessor` as the verification processor.
script and `pwd_verify_sms_ui` as the verification UI macro. The following shows the verification processor script:

```javascript
var PwdVerifySMSProcessor = Class.create();
PwdVerifySMSProcessor.prototype = {
    category: "password_reset.extension.verification_form_processor", // DO NOT REMOVE THIS LINE!

    initialize: function () {
        // Initialization stuff here...
        initialize:
    },

    process the verification form request, and return whether the user was successfully verified

    *param params.resetRequestId The sys-id of the current password-reset request (table: pwd_reset_request)
    *param params.userid The sys-id of the user trying to be verified (table: sys_user)
    *param params.verificationId The sys-id of the verification to be processed (table: pwd_verification)
    *param request The form request object. Fields in the form can be accessed using:
    request.getParameter('<element-id>')

    // Verify if the user is successfully verified

    return true;
};
```

**Verification type SMS processor**

The following is the corresponding UI macro:
Password Reset script includes

The Password Reset plugin installs script includes that implement password reset processes. To enable you to extend functionality, each base-system script include provides extension points that you can use to invoke "extension scripts" that you have customized.
The extension script category refers to the specific types of behavior for an extension script (for example, credential store, verification, identification type, or as a post-processor).

**'Enrollment check' script includes**

All enrollment check script includes take the following parameters and return a boolean indicating whether the user is enrolled for Password Reset.

- `params.userId`: The sys_id of the user being checked (table: [sys_user]).
- `params.verificationId`: The sys_id of the verification being checked (table: [pwd_verification]).

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PwdAlwaysEnrolled</td>
<td>Default check of whether a user is enrolled that always returns true.</td>
</tr>
<tr>
<td>PwdMockIsEnrolled</td>
<td>Default check of whether a user is enrolled that always returns true.</td>
</tr>
<tr>
<td>PwdQuestionsEnrollmentCheck</td>
<td>Determines whether a user has enrolled for Password Reset using security question verification.</td>
</tr>
<tr>
<td>PwdSMSEnrollmentCheck</td>
<td>Determines whether a user has enrolled for Password Reset using SMS verification.</td>
</tr>
</tbody>
</table>

**'Identification form processor' script includes**

Identification form processor script includes provide functionality for extending identification processing.

All identification form processor script includes take the following parameters, and return the sys_id of the user that corresponds to the requested input. If the user was not identified, it returns null.

- `params.processId`: The sys_id of the calling Password Reset process (table: [pwd_process]).
- `param request`: The form request object. Fields in the form can be accessed with `request.getParameter('<element-id>')`. The supported request parameter is `sysparm_user_id`, the user identifier value entered in the form.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PwdIdentifyViaEmail</td>
<td>Verifies a user's identity by checking the email address.</td>
</tr>
<tr>
<td>PwdIdentifyViaUsername</td>
<td>Verifies a user's identity by checking the user name.</td>
</tr>
</tbody>
</table>

**'Enrollment form processor' script includes**

Enrollment form processor script includes provide functionality for extending enrollment form processing.

All enrollment form processor script includes take the following parameters, and return a boolean indicating whether the user was successfully enrolled.
- **params.userId**: The sys_id of the user trying to enroll (table: [sys_user]).
- **params.verificationId**: The sys_id of the verification used to enroll (table: [pwd_verification]).
- **params.enrollmentId**: The sys_id of this enrollment process.
- **request**: The form request object. Fields in the form can be accessed with `request.getParameter('<element-id>')`.

You should add the following information to the state of the enrollment process:

- `gs.getSession().putProperty("result.status", status)`: Whether the user was successfully enrolled.
- `gs.getSession().putProperty("result.message", message)`: An associated message to be returned to the UI, such as a detailed error message.
- `gs.getSession().putProperty("result.value", value)`: A custom value associated with the enrollment.

### Name | Description
--- | ---
PwdEnrollQuestionsProcessor | Handles questions and answers for verification.
PwdEnrollSampleProcessor | Provides an enrollment processor for sample verification.
PwdEnrollSMSProcessor | Provides an enrollment processor for SMS verification.

### 'User account lookup' script includes

User account lookup script includes return the credential store account_id for a given user.

The following parameter returns the credential store account_id for a given user.
- **params.userId**: The sys_id of the user being checked (table: [sys_user]).

### Name | Description
--- | ---
PwdDefaultUserAccountLookup | Provides a default script for user account lookup from a user_id to the account in a credential store. The default mapping is to use the user name as the account name.

### 'Password generator' script includes

Password generator script includes take the following parameter, and return an auto-generated string password.
- **params.credentialStoreId**: The sys_id of the calling Password Reset process (table: [pwd_process]).

### Name | Description
--- | ---
PwdDefaultAutoGenPassword | Generates a password from a random word and 4 digits.
‘Verification processor’ script includes

If the user identity is verified, the verification processor script includes return true.

Verification processor script includes take the following parameters:

- **params.resetRequestId**: The sys_id of the current Password Reset request (table: [pwd_reset_request]).
- **params.userId**: The sys_id of the user to be verified (table: [sys_user]).
- **params.verificationId**: The sys_id of the verification (table: [pwd_verification]).
- **request**: The form request object. Access the fields in the form with request.getParameter('element-id').

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PwdVerifyPersonalDataConfirmationProcess</td>
<td>Verifies that the user accepts the answer.</td>
</tr>
<tr>
<td>PwdVerifyPersonalDataProcessor</td>
<td>Verifies that the user’s answers match the expected data in the system.</td>
</tr>
<tr>
<td>PwdVerifyQuestionsProcessor</td>
<td>Provides question and answer verification of user input on the second page of the verification form.</td>
</tr>
<tr>
<td>PwdVerifySimpleProcessor</td>
<td>Provides simple verification of user input on the second page of the verification form.</td>
</tr>
<tr>
<td>PwdVerifySMSProcessor</td>
<td>Provides SMS verification of user input on the second page of the verification form.</td>
</tr>
</tbody>
</table>

‘Post processor’ script includes

Post processor script includes execute custom actions after the Password Reset process has completed.

All post processor script includes take the following parameters.

- **params.resetRequestId**: The sys_id of the current Password Reset request (table: [pwd_reset_request]).
- **params.wfSuccess**: A flag indicating whether the workflow completed successfully: True if, and only if, successful.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PwdPostProcessor</td>
<td>Executes actions after the process completes for success, failure, or both conditions.</td>
</tr>
</tbody>
</table>

Example custom scripts for Password Reset

The example scripts perform a user account lookup and processes an identification form, define a credential store, and create an identification type.
Perform a user account lookup and process an identification form

The main script calls two extension scripts, one to perform the user account lookup, and the other to process the identification form.

```javascript
// User account lookup
var lookupExtensionSysId =
  getExtensionScriptSysId('SampleUserAccountLookupExtension', 'user_account_lookup');
var lookupExtension = new SNC.PwdExtensionPoint(lookupExtensionSysId);

// Setup parameters required for this extension type - userId
var params = new SNC.PwdExtensionPointParameter();
params.userId = 'joe.employee';

// Invoke the extension
var answer = lookupExtension.process(params);
gs.print('user: ' + answer);

// Form processor sample - Identification form processor
var identExtensionSysId =
  getExtensionScriptSysId('SampleIdentificationProcessorExtension', 'identification_form_processor');
var identificationExtension = new SNC.PwdExtensionPoint(identExtensionSysId);

// Setup parameters required for this extension type - processId
var params = new SNC.PwdExtensionPointParameter();
params.processId = 'pwdreq1234';

// Simulate the posted form parameter for the indentification processor
var request = new SNC.PwdExtensionPointParameter(); // A real life case will inject it's own request object
request.setParameter('sysparm_user_id', 'joe.employee');

var userIdentity = identificationExtension.processForm(params, request);
gs.print('identity: ' + userIdentity);
```

Define a credential store

The following is an example of an extended process function in the User Account Lookup category used to define a credential store. To create this extension script, go to Password Reset >
Extensions > New extension script and create a new script as described in Create an Extension Script. To configure the User Lookup in a Password Reset process, see Credential Stores.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<record_update table="sys_script_include">
    <sys_script_include action="INSERT_OR_UPDATE">
        <active>true</active>
        <client_callable>false</client_callable>
        <description>Simple account lookup that returns the supplied user id</description>
        <name>SampleUserAccountLookupExtension</name>
        <script><![CDATA[
var SampleUserAccountLookupExtension = Class.create();

SampleUserAccountLookupExtension.prototype = {
    category: 'password_reset.extension.user_account_lookup', // DO NOT REMOVE THIS LINE!

    process: function(params) {
        return params.userId;
    },

type: 'SampleUserAccountLookupExtension'
};]]></script>
    </sys_script_include>
</record_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.
Create an identification type

The following is an example of an extended processForm function in the Identification Form Processor category that can be used to create an identification type. To create this extension script, go to Password Reset > Extensions > New extension script and create a new script as described in Create an Extension Script.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<record_update table="sys_script_include">
  <sys_script_include action="INSERT_OR_UPDATE">
    <active>true</active>
    <client_callable>false</client_callable>
    <description>Script that processes an identification form. Returns the sys-id of the user that corresponds to the requested input; if no user was found, null should be returned.</description>
    <name>SampleIdentificationProcessorExtension</name>
    <script><![CDATA[
        var SampleIdentificationProcessorExtension = Class.create();
        SampleIdentificationProcessorExtension.prototype = {
            category: 'password_reset.extension.identification_form_processor', // DO NOT REMOVE THIS LINE!
            processForm: function(params, request) {
                var sysparm_user_id = request.getParameter('sysparm_user_id');
                var processId = params.processId;

                // Process the identification form request, and returns the user's sys_id.
                // if user was not identified return null.
                return sysparm_user_id + '_' + processId;
            },
            type: 'SampleIdentificationProcessorExtension'
        };
    ]]></script>
  </sys_script_include>
</record_update>
```
Use the `process` and `processForm` extensions

This example shows a script that uses two sample extensions, one `process` extension and one `processForm` extension.

```javascript
// User account lookup
var lookupExtensionSysId =
  getExtensionScriptSysId('SampleUserAccountLookupExtension','user_account_lookup');
var lookupExtension =
  new SNC.PwdExtensionPoint(lookupExtensionSysId);

// Setup parameters required for this extension type - userId
var params =
  new SNC.PwdExtensionPointParameter();
params.userId = 'joe.employee';

// Invoke the extension
var answer = lookupExtension.process(params);
gs.print('user: ' + answer);

// Form processor sample - Identification form processor
var identExtensionSysId =
  getExtensionScriptSysId('SampleIdentificationProcessorExtension','identification_form_processor');
var identificationExtension =
  new SNC.PwdExtensionPoint(identificationExtensionSysId);

// Setup parameters required for this extension type - processId
var params =
  new SNC.PwdExtensionPointParameter();
params.processId = 'pwdreq1234';

// Simulate the posted form parameter for the indentification processor
var request =
  new SNC.PwdExtensionPointParameter();
request.setParameter('sysparm_user_id', 'joe.employee');

var userIdentity = identificationExtension.processForm(params, request);
gs.print('identity: ' + userIdentity);

// Simple helper to return the sys-id for a given extension script
function getExtensionScriptSysId(scriptName, category){
  var result;
  var gr =
    new GlideRecord('sys_script_include');
  gr.addQuery('name', scriptName);
  gr.addQuery('script', 'CONTAINS', 'category: \"password_reset.extension.\" + category + \\
');
  gr.query();

  return result;
}
```
if(gr.next()){
    result = gr.getValue('sys_id');}return result;}

process function:

<?xml version="1.0" encoding="UTF-8"?><record_update
  table="sys_script_include"><sys_script_include
  action="INSERT_OR_UPDATE"><active>true</active><client_callable>false</client_callable><description>Simple account lookup that returns the supplied user id</description><name>SampleUserAccountLookupExtension</name><script><![CDATA[var SampleUserAccountLookupExtension =Class.create();
    SampleUserAccountLookupExtension.prototype={
        category:'password_reset.extension.user_account_lookup',// DO NOT REMOVE THIS LINE!
        process:function(params){return params.userId;},
>sys_source_deleted>false</sys_source_deleted><sys_source_id>2df5a103d73201002bb9af728e610333</sys_source_id><sys_source_table>sys_script_include</sys_source_table><sys_type>code</sys_type><sys_update_name>SampleUserAccountLookupExtension</sys_update_name><sys_updated_by>admin</sys_updated_by><sys_updated_on>2013-07-30 16:46:00</sys_updated_on></sys_app_file></record_update>

processForm function:

<?xml version="1.0" encoding="UTF-8"?><record_update
  table="sys_script_include"><sys_script_include
  action="INSERT_OR_UPDATE"><active>true</active><client_callable>false</client_callable><description>Script that processes an identification form. Returns the sys-id of the user that corresponds to the requested input; if no user was found, null should be returned.&amp;#13;</description><name>SampleIdentificationProcessorExtension</name><script><![CDATA[var SampleIdentificationProcessorExtension =Class.create();
    SampleIdentificationProcessorExtension.prototype={
        process:function(params){return params.userId;},
        type:'SampleIdentificationProcessorExtension';}}]]></script><sys_created_by>admin</sys_created_by><sys_created_on>2013-07-30 16:44:55</sys_created_on><sys_id>8306e143d73201002bb9af728e6103d3</sys_id><sys_mod_count>0</sys_mod_count><sys_name>SampleIdentificationProcessorExtension</sys_name><sys_parent/><sys_path>!!1W4/</sys_path><sys_policy/>
>sys_source_deleted>false</sys_source_deleted><sys_source_id>2df5a103d73201002bb9af728e610333</sys_source_id><sys_source_table>sys_script_include</sys_source_table><sys_type>code</sys_type><sys_update_name>SampleIdentificationProcessorExtension</sys_update_name><sys_updated_by>admin</sys_updated_by><sys_updated_on>2013-07-30 16:46:00</sys_updated_on></sys_app_file></record_update>
category:'password_reset.extension.identification_form_processor',// DO NOT REMOVE THIS LINE!

**********
* Process the identification form request, and returns the user's sys_id.
  if user was not identified return null.
* @param params.processId The sys-id of the calling password-reset
  process (table: pwd_process)
* @param request The form request object. fields in the form
  can be accessed using: request.getParameter('<element-id>')
  * Supported request parameters:
  * sysparm_user_id - the user identifier
  value entered in the form.
  * @return The sys-id of the user that corresponds to the requested input;
    if no user was found, null should be returned.
  **********/
processForm:function(params, request){return
  request.getParameter('sysparm_user_id')+'_'+ params.processId;},
type:'SampleIdentificationProcessorExtension'
};]]></script><sys_created_by>admin</sys_created_by><sys_created_on>2013-07-30 17:00:28</sys_created_on><sys_id>3a79a503d73201002bb9af728e610349</sys_id><sys_mod_count>1</sys_mod_count><sys_updated_by>admin</sys_updated_by><sys_updated_on>2013-07-30 17:00:28</sys_updated_on><sys_script_include><sys_app_file action="INSERT_OR_UPDATE"><customer_update>false</customer_update><publish_override/><replace_on_upgrade>false</replace_on_upgrade><restore/><sys_app><sys_code>!!1W5/</sys_code><sys_created_by>admin</sys_created_by><sys_created_on>2013-07-30 17:00:28</sys_created_on><sys_id>4799ed03d73201002bb9af728e610333</sys_id><sys_mod_count>0</sys_mod_count><sys_name>SampleIdentificationProcessorExtension</sys_name><sys_parent/><sys_path>!!1W5/</sys_path><sys_policy/><sys_source_deleted>false</sys_source_deleted><sys_source_id>3a79a503d73201002bb9af728e610349</sys_source_id><sys_source_table>sys_script_include</sys_source_table><sys_type>code</sys_type><sys_update_name>sys_script_include_3a79a503d73201002bb9af728e610349</sys_update_name><sys_updated_by>admin</sys_updated_by><sys_updated_on>2013-07-30 17:08:41</sys_updated_on></sys_app_file></record_update>

Password Reset extension script categories
You can use a custom extension script to extend Password Reset functionality for credential store,
verification, or identification types.

Note: To use a script include as an extension script, you must set it to Active status.

Password Reset extension script categories
Extension scripts must specify a category that indicates which script include is being extended,
for example, category: 'password_reset.extension.enrollment_check'. The ServiceNow
platform installs several scripts in each category. A script in the Enrollment check category can
perform the enrollment check for a verification. Detailed information on each extension script
appears in Password Reset extension scripts.
<table>
<thead>
<tr>
<th>Extension script category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enrollment check</td>
<td>Defines how to check that a user is enrolled in the Password Reset process. Scripts of this category are available in the Enrollment check field when you define a verification type (Password Reset Verification Type form).</td>
</tr>
<tr>
<td>Enrollment form processor</td>
<td>Defines how an enrollment form is processed (if automatic enrollment is not configured). Scripts of this category are available in the Enrollment form processor field when you define a verification type (Password Reset Verification Type form).</td>
</tr>
<tr>
<td>Identification form processor</td>
<td>Defines how a user identification is processed. Scripts of this category are available in the Identification processor field when you define a verification type (Password Reset Identification Type form).</td>
</tr>
<tr>
<td>Password generator</td>
<td>Defines how to generate a password. Scripts of this category are available in the Auto generate password field when you configure a credential store (Password Reset Credential Store Type form).</td>
</tr>
<tr>
<td>Post reset script</td>
<td>Executes at the end of a Password Reset process. Scripts of this category are available in the Post reset script field when you configure a process (Password Reset Process form).</td>
</tr>
<tr>
<td>User account lookup</td>
<td>Defines how to look up a user account. Scripts of this category are available in the User account lookup field when you configure a credential store (Password Reset Credential Store form).</td>
</tr>
<tr>
<td>Verification form processor</td>
<td>Defines how a verification form is processed. Scripts of this category are available in the Verification processor field when you define a verification type (Password Reset Verification Type form).</td>
</tr>
</tbody>
</table>

Password Reset extension scripts
Extension scripts allow you to extend Password Reset functionality in credential store, verification, or identification types.

Password Reset extension script includes

Each script include is associated with a specific category, which is available in the appropriate field of a Password Reset form.

**Note:** Create extension scripts only from the Password Reset Extension Script form (Password Reset > Extensions > New extension script). Extension scripts are special purpose script includes that are not created in the System Definition > Script Includes interface. To use a script include as an extension script, you must set it to Active status.
'Enrollment Check' script include category

<table>
<thead>
<tr>
<th>Script include category</th>
<th>Description</th>
<th>Method signature</th>
<th>Input fields</th>
<th>Output fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enrollment Check</td>
<td>Checks whether a user is enrolled for a given verification.</td>
<td>process(params)</td>
<td>Parameters:</td>
<td>Returns: (boolean)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>· params.userId - The sys_id of the user to check (table: sys_user).</td>
<td>true, if the user is enrolled in the specified verification; otherwise, false.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>· params.verificationId - The sys_id of the verification to check (table: pwd_verification).</td>
<td></td>
</tr>
</tbody>
</table>

This Enrollment Check example signals that the user is enrolled if both expected parameters are supplied. The code would be contained in the `Script` field of an extension script named `SampleEnrollmentCheck`:

```javascript
var SampleEnrollmentCheck = Class.create();
SampleEnrollmentCheck.prototype = {
    category : 'password_reset.extension.enrollment_check', // DO NOT REMOVE THIS LINE!

    process : function (params) { return (params.userId && params.verificationId) ? true : false; },

type : 'SampleEnrollmentCheck'
};
```

© 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.
**Enrollment Form Processor** script include category

<table>
<thead>
<tr>
<th>Script include category</th>
<th>Description</th>
<th>Method signature</th>
<th>Input fields</th>
<th>Output fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enrollment Form Processor</td>
<td>Checks whether all necessary information has been collected from the user. Stores the information so it can be used for verification when the user resets their password.</td>
<td>process(params)</td>
<td>Parameters:</td>
<td>Returns: (boolean)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- params.resetRequestId - The sys_id of the current Password Reset request (table: pwd_reset_request).</td>
<td>true, if the user is enrolled in the specified verification; otherwise, false.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- params.userId - The sys_id of the user to be verified (table: sys_user).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- params.verificationId - The sys_id of the verification to be processed (table: pwd_verification).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- request - The form request object. Fields in the form can be accessed with request.getParameter(&lt;element-id&gt;).</td>
<td></td>
</tr>
</tbody>
</table>

The following information should be added to the state of the enrollment process:

- gs.getSession().putProperty("result.status",status) - Whether the user was successfully enrolled.
- gs.getSession().putProperty("result.message",message) - An associated message to be returned to the UI, such as a detailed error message.
- gs.getSession().putProperty("result.value",value) - A custom value associated with the enrollment.
This example processes an enrollment form submission successfully if the user-submitted response was success. The code would be contained in the **Script** field of an extension script named `SampleEnrollmentProcessor`:

```javascript
var SampleEnrollmentProcessor = Class.create();
SampleEnrollmentProcessor.prototype = {
    category: 'password_reset.extension.enrollment_form_processor', // DO NOT REMOVE THIS LINE!

    processForm: function (params, request) {
        var verificationId = params.verificationId;
        var sampleInput = request.getParameter('sample_input');

        if (gs.nil(verificationId) || (sampleInput != 'success')) {
            return false;
        }

        var gr = new GlideRecord('sys_user');
        gr.get(params.userId);
        gs.print('User: ' + gr.getValue('user_name') + ' successfully enrolled');
        return true;
    },

    type: 'SampleEnrollmentProcessor'};
```
### 'Identification Form Processor' script include category

<table>
<thead>
<tr>
<th>Script include category</th>
<th>Description</th>
<th>Method signature</th>
<th>Input fields</th>
<th>Output fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification Form Processor</td>
<td>Processes an identification form request.</td>
<td>processForm(params, request)</td>
<td>Parameters:</td>
<td>Returns: the sys_id of the user that corresponds to the requested input. Returns null, if no user was found.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- params.processId - The sys_id of the calling Password Reset process (table: pwd_process).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- request - The form request object. Fields in the form can be accessed with request.getParameter('sysparm_user_id'). Use request.getParameter('sysparm_user_id') to get the user ID that was entered into the form.</td>
<td></td>
</tr>
</tbody>
</table>

This example attempts to identify the user within the sys_user table given a user name submitted from the identification form. The code would be contained in the `Script` field of an extension script named `PwdIdentifyViaUsername`:

```javascript
var PwdIdentifyViaUsername = Class.create();
PwdIdentifyViaUsername.prototype = {
    initialize : function () { },

    //**********
    // Process the identification form request, and returns the user's sys_id.
    // If user was not identified return null.
    //**********
    processForm : function (params , request ) {
        var processId = params.processId; 
        var sysparm_user_id = request.getParameter('<element-id>');
        var gr = new GlideRecord('sys_user');
        gr.addQuery('user_name', sysparm_user_id);
        if (!gr.next()) { return null; } return gr.sys_id;
    }
};
```

© 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.
**Password Generator** script include category

<table>
<thead>
<tr>
<th>Script include category</th>
<th>Description</th>
<th>Method signature</th>
<th>Input fields</th>
<th>Output fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Generator</td>
<td>Returns an auto-generated password.</td>
<td>process(params)</td>
<td>Parameters:</td>
<td>Returns: (String) an auto-generated password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- params.processId</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- The sys_id of the calling Password Reset process (table: pwd_process).</td>
<td></td>
</tr>
</tbody>
</table>

This example randomly generates a password from a base word and numbers. The base word is selected depending on the credential store. The code would be contained in the **Script** field of an extension script named `SamplePasswordGenerator`:

```javascript
var SamplePasswordGenerator = Class.create();
SamplePasswordGenerator.prototype = {
    category : 'password_reset.extension.password_generator', // DO NOT REMOVE THIS LINE!

    process : function (params) {
        var basePassword;
        var gr = new GlideRecord('pwd_cred_store');
        gr.addQuery('name', 'Local ServiceNow Instance');
        gr.query(); if (gr.next()) {
            if (params.credentialStoreId == gr.getValue('sys_id')) {
                basePassword = "Password";
            } else {
                basePassword = "Dorwssap";
            }
        } return this.generateSimple(basePassword);
    },

    generateSimple : function (base) {
        var pwd = base;
        var numbers = '0123456789';
        var length = 4;
        for (var i = 0, n = numbers.length; i < length; i++) {
            pwd += numbers.charAt(Math.floor(Math.random() * n) + 1);
        }
        return pwd;
    },

    type : 'SamplePasswordGenerator'
};
```

© 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.
'Post Reset' script include category

<table>
<thead>
<tr>
<th>Script include category</th>
<th>Description</th>
<th>Method signature</th>
<th>Input fields</th>
<th>Output fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Post Reset</td>
<td>Performs additional operations after the completion of the Password Reset process.</td>
<td>process(params)</td>
<td>Parameters:</td>
<td>Returns: void</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>params.resetRequestId - The sys_id of the calling Password Reset process (table: pwd_process).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>params.wfSuccess - A flag indicating whether the workflow completed successfully. True if, and only if, successful.</td>
<td></td>
</tr>
</tbody>
</table>

This example adds failed reset requests to the system log. The code would be contained in the Script field for an extension script named `PwdPostProcessor`:

```javascript
var PwdPostProcessor = Class. create( );

PwdPostProcessor.prototype = {
    category : 'password_reset.extension.post_reset_script', // DO NOT REMOVE THIS LINE!
    initialize : function ( ) {} ,
    /**********
    * Execute custom actions after the Password Reset process has completed.
    * @param params.resetRequestId The sys_id of the current Password Reset request (table: pwd_reset_request)
    * @param params.wfSuccess A flag indicating if the workflow completed successfully.
    * True if (and only if) successful.
    * @return no return value
    *******
    process : function (params) { if ( !params.wfSuccess ) {
        gs. log ( '[' + params.resetRequestId + ']' ) ;
    } // We could place actions here that we always want executed return ; },
    type : 'PwdPostProcessor' }
```

© 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.
### 'User Account Lookup' script include category

<table>
<thead>
<tr>
<th>Script include category</th>
<th>Description</th>
<th>Method signature</th>
<th>Input fields</th>
<th>Output fields</th>
</tr>
</thead>
</table>
| User Account Lookup     | Gets the credential store account ID for a given user. | process(params) | Parameters:  
  - params.userId - The sys_id of the user being checked (table: sys_user). | Returns: (String) the credential store account ID for the given user. |

This example gets the credential store account for a user. This code would be contained in the `Script` field of an extension script named `SampleUserAccountLookupExtension`:

```javascript
var SampleUserAccountLookupExtension  = Class. create ( ) ;
SampleUserAccountLookupExtension. prototype = {
    category : 'password_reset.extension.user_account_lookup' , // DO NOT REMOVE THIS LINE!

    process : function (params) { return params. userId ; },
    type : 'SampleUserAccountLookupExtension' }
```
'Verification Form Processor' script include category

<table>
<thead>
<tr>
<th>Script include category</th>
<th>Description</th>
<th>Method signature</th>
<th>Input fields</th>
<th>Output fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verification Form Processor</td>
<td>Processes a verification form request and indicates whether the user was verified or not.</td>
<td>processForm(params, request)</td>
<td>Parameters:</td>
<td>Returns: (boolean)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>· params.resetRequestId</td>
<td>true, if the user is verified; otherwise, false.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>· params.userId</td>
<td>The sys_id of the user to be verified (table: sys_user).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>· params.verificationId</td>
<td>The sys_id of the verification to be processed (table: pwd_verification).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>· request</td>
<td>The form request object. Fields in the form can be accessed with request.getParameter('&lt;element-id&gt;').</td>
</tr>
</tbody>
</table>

This example shows a verification processor that returns true only if the user sent `ok` in the input field; otherwise, it returns false. The code would be contained in the Script field of an extension script named `SampleVerificationFormProcessor`:

```javascript
var SampleVerificationFormProcessor = Class.create();
SampleVerificationFormProcessor.prototype = {
    category : 'password_reset.extension.verification_form_processor', // DO NOT REMOVE THIS LINE!

    processForm: function(params, request) {
        /* Process the verification form request, and return whether the user was successfully verified. 
         * This is a sample verification processor returns true only if the user sent "ok" in the input field;
         * otherwise, it returns false.
         */

        @param params.resetRequestId The sys_id of the current Password Reset request (table: pwd_reset_request)
        @param params.userId The sys_id of the user trying to be verified (table: sys_user)
        @param params.verificationId The sys_id of the verification to be processed (table: pwd_verification)
        @param request The form request object. Fields in the form can be accessed with request.getParameter('<element-id>').

        return request.getParameter('ok') === 'true';
    }
};
```
Create a Password Reset extension script

Create extension scripts only from the Password Reset Extension Script form. Do not create extension scripts in the System Definition > Script Includes interface.

Role required: password_reset_admin or admin

**Note:** To use a script include as an extension script, you must set it to Active status.

1. Navigate to Password Reset > Extensions > New extension script.
2. Enter a name in the Extension script name field.
   Use CamelCase to construct a name without spaces, for example, PwdEnrollmentCustom.
3. Select an Extension script category.
   - Enrollment check
   - Enrollment form processor
   - Identification form processor
   - Password generator
   - User account lookup
   - Verification form processor
4. Click Submit.
   A new instance of the script include for the selected category opens.
5. Edit the script by providing an implementation in the body of the process or processForm function, depending on the script category. You can add additional functions as long as the process or processForm function accepts the defined parameters and returns the expected results.

**Note:** Do not edit or delete the Category declaration.
6. Click Update.

Service desk: Reset a password for a user
In a service desk-assisted Password Reset process, service desk agents with the password_reset_service_desk role reset user passwords. Users do not reset passwords. Watch a video example of service desk agents resetting passwords: Resetting User Passwords (Video).

Role required: password_reset_admin or password_reset_service_desk

Note: You must set the Public access property to enable the service desk-assisted process. See Settings on the Password Reset Details tab.

1. Navigate to **Password Reset > Service Desk**.
2. Select a user and the Password Reset process to use.
3. Click **Verify Identity**.
4. On the Verify Identity form, enter the answers that the user provides and then click **Continue**. If the user identity is verified, the Reset Password form displays identity verification and status of the account lock.
5. Perform one of the following actions.
   - If the user is not locked, the form displays the **Reset password** button. Enter the new password and click **Reset password**.
   - If the user is locked, the form displays the **Reset password** and **Unlock account** buttons. You can enter a new password and click **Reset password** to reset the password and unlock the
6. To reset the password for a different user, you must first navigate out of the Service Desk and then navigate to Password Reset > Service Desk.

Service desk: View user requests for password reset

The Reset Requests module displays the status of each password reset request from the Password Reset Request table (pwd_reset_request).

Role required: password_reset_admin or password_reset_service_desk

Navigate to Password Reset > Reset Requests.

Password Reset request fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>The user whose password is being reset or changed.</td>
</tr>
<tr>
<td>Process</td>
<td>The process that implements this password reset request.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of Password Reset request:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Change Password</strong>: Request to change a password.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Help Desk</strong>: Request opened on behalf of the requesting user by a service desk agent.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Self Service</strong>: Requesting user opened the reset request.</td>
</tr>
<tr>
<td>Action Type</td>
<td>The corrective action performed during the Password Reset request:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Change Password</strong>: Update the credential store with the new password.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Reset and Unlock Account</strong>: Generate a new password for the user and unlock the user account.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Reset Password</strong>: Generate a new password for the user.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Unlock Account</strong>: Unlock the user account.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Status</td>
<td>The result of the Password Reset request:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Completed With Failure</strong>: User completed all steps in the Password Reset process, but the password was not reset in the credentail store.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Completed With Success</strong>: User completed all steps in the Password Reset process and the password was reset in the credentail store.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Expired</strong>: User did not complete all steps in the Password Reset process in the time allowed.</td>
</tr>
<tr>
<td></td>
<td>- <strong>In Progress</strong>: User is working through the steps to reset the password.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Max Number of Attempts</strong>: User failed to answer the security questions correctly during the identity verification step and has exceeded the maximum number of attempts allowed.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Verified</strong>: User has completed the identity verification step and is verified. The user can move to the Password Reset step.</td>
</tr>
<tr>
<td>Active</td>
<td>Whether the request is open or closed.</td>
</tr>
<tr>
<td>Retry</td>
<td>The total number of times the user has attempted to complete a password reset request.</td>
</tr>
</tbody>
</table>

Service desk: Unblock a Password Reset user

If a user is manually banned or flagged as exceeding max attempts, the user can be blocked (not allowed to use the Password Reset application). You can unblock a blocked user.

Role required: password_reset_admin or password_reset_service_desk

Blocking events include:
- The user exceeded the limit for the number of failed password attempts.
- The most recent password reset occurred before the wait time required until the next reset.
- The user failed to provide the correct information while attempting to reset the password.

If the number of blocked or locked users exceeds the limit within a defined time interval, it triggers a system log event. You can configure the number of blocked, or locked, users and the time interval required to generate the log event by setting the `password_reset.activity_monitor.incident_threshold` and `password_reset.activity_monitor.incident_window` properties.

1. To view the list of blocked users, navigate to **Password Reset > Blocked Users**.
2. To unblock a self-service user:
   a) Navigate to **Password Reset > Blocked Users**.
   b) Select a user from the list.
   c) Select **Delete** on the **Actions on selected rows** list.
3. To unblock a user whose password was reset by a service desk agent:
If a user is manually banned or flagged as exceeding max attempts, the user can be blocked (not allowed to use the Password Reset application). When the password reset request is made through self-service, the user is unblocked when the password is successfully reset.

In contrast, service desk agents are allowed any number of retries. The max_attempt_reached limit does not apply and the Blocked status for the user is not reset after the password is reset. As a result, after you successfully reset a user password, you must unblock the user manually.

If the user is not unblocked manually, then the system resets the blocked state only when the max_attempt_window time period elapses and the user tries to reset the password using self-service.

a) After you successfully reset a user password, navigate to Password Reset > Blocked Users.

b) Change the Blocked setting for the user from true to false.

Integrate Password Reset with a CMS integration
You can configure a site in the ServiceNow content management (CMS) application to define a single-site access point that includes the Password Reset service. For example, you can create an employee self-service site that provides Password Reset service.

Role required: content_admin

Each Password Reset process requires a separate CMS page.

1. Navigate to Content Management > Specialty Content > iFrames and create an iFrame record.

2. Go to Content Management > Sites and create a site that has no login page.
3. Go to **Content Management > Pages** and create a password reset page.
4. Enter the name of the site that you created in the **Content site** field (**Password Reset self-service** in the example).
5. Right-click the form header and click **Save**.
6. Click the **Edit Page** related link and then click **Add content**.
7. In the **Content Blocks** section, select the iFrame that you created. Add more content as needed.
8. Click **Update**.

**Password Reset and Password Change reports and logs**
The Password Reset application provides several tools for monitoring and troubleshooting password reset activities.

Users with the **password_reset_credential_manager** or **password_reset_admin** role can view the status of password reset activities, identify potential security threats, and monitor for compliance with password security policies.

The Reset Requests, Activity Log, and Blocked Users modules are useful for monitoring password reset activities and for troubleshooting password reset issues. They also provide access to more detailed information than is provided on the Overview module.
To make room for new data, the system periodically purges the data that is used for password reset monitoring and reporting.

**Password Reset Overview module**

The **Password Reset > Overview** module displays reports on password reset and password change activities. Users with the `password_reset_admin` role can customize the layout of the reports that appear in the Overview module.

**Password Reset reports**

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Requests (last 7 days)</td>
<td>Number of password reset requests by type during the last 7 days.</td>
</tr>
<tr>
<td>Blocked Users (last 7 days)</td>
<td>Number of users blocked over the last 7 days.</td>
</tr>
<tr>
<td>Password Reset Request Status (last 7 days)</td>
<td>The status of all password reset requests by process.</td>
</tr>
<tr>
<td>Password Reset Request by Action (last 30 days)</td>
<td>Number of password reset requests by action type: Reset Password, Unlock Account, or Reset and Unlock.</td>
</tr>
<tr>
<td>Password Reset Top Users (last 30 days)</td>
<td>Number of password reset requests per user. Many password reset requests from a single user could indicate a security issue.</td>
</tr>
<tr>
<td>Password Reset Failed Verifications (last 7 days)</td>
<td>Number of failed verification attempts, by verification instance. A failed verification occurs when a user attempts to reset the password, but fails for one reason or another, during the identity verification step. Many failed verification attempts for a specific type of verification could indicate that the process is too complicated or unclear.</td>
</tr>
<tr>
<td>Password Reset Enrollment By Verification</td>
<td>Number of users by verification type who have and have not enrolled in the password reset program. A large number for users who have not enrolled could indicate a compliance or communication issue within the organization.</td>
</tr>
<tr>
<td>Password Change Top Users (last 30 days)</td>
<td>Number of password change requests per user. Many password change requests from a single user could indicate a security issue.</td>
</tr>
</tbody>
</table>

**Password Reset activity log**

The activity log (**Password Reset > Activity Log**) provides detailed information that you can use to troubleshoot and to generate reports on password reset metrics. Information contained in the activity log is stored in the Password Reset activity log `pwd_reset_activity` table.

You must have the `password_reset_credential_manager` or `password_reset_admin` role to view the log.
Password Reset event log

The event log is a valuable resource for troubleshooting. On the Start menu, click Programs (or All Programs) > Administrative Tools > Event Viewer.

If the log does not appear, then, on the Windows Logs menu, click Applications > Service Logs.

You must have the admin role to view the log.

To write to the Password Reset event log

Edit the DebugFlag registry key entry at: Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Windows > CurrentVersion > Authentication > Credential Providers > {B6EFF27D-C1C4-481F-B81B-F3547C47D58A}

By default, the key is set to 0. Set the key to 1 to write log entries to the ServiceNowPwdReset event log.

You must have the password_reset_credential_manager or password_reset_admin role to write to the log.

Password Reset blocked user notification

You can receive email notifications when the number of users that are blocked or locked exceeds the password blocked threshold. Notifications can alert you to suspicious activities. The default threshold is 10.

To subscribe: Add an email notification device or modify an existing device and then subscribe to the Password Reset-Activity Monitor Lockout notification.

You must have the password_reset_credential_manager or password_reset_admin role to subscribe.

Schedule for purging Password Reset data

To make room for new data, the system periodically purges the data that is used for password reset monitoring and reporting. Information contained in reports and monitoring tools could change dramatically immediately after a data purge. Contact ServiceNow Technical Support to modify purge intervals.

<table>
<thead>
<tr>
<th>Table name</th>
<th>Purge interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>(pwd_reset_request)</td>
<td>90 days (7,776,000 seconds). Depending on your organizational data monitoring requirements, you could configure the rule to:</td>
</tr>
<tr>
<td></td>
<td>• Purge successful requests after 90 days</td>
</tr>
<tr>
<td></td>
<td>• Keep failed requests for 120 days</td>
</tr>
<tr>
<td>Table name</td>
<td>Purge interval</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------</td>
</tr>
</tbody>
</table>
| (pwd_user_lockout)               | 90 days (7,776,000 seconds). Depending on your organizational data monitoring requirements, you could configure the rule to:  
|                                  | • Purge successful requests after 90 days  
|                                  | • Keep failed requests for 120 days               |
| (pwd_reset_activity)             | 90 days (7,776,000 seconds).                       |
| (pwd_activity_monitor)           | 90 days (7,776,000 seconds).                       |
| (pwd_dvc_enrollment_code)        | 1 day (86,400 seconds).                            |
| (pwd_sms_code)                   | 1 day (86,400 seconds).                            |

**Users: Reset your password on Windows systems**

If your organization uses the Password Reset Windows Application, you can reset your password directly from your Windows login screen.

Role required: none

1. Start your computer or press **Ctrl+Alt+Delete** to go to the Windows login screen.
2. Click the **Forgot Password?** link. (Your administrator may have configured different text for the link.)

3. On the **Identify** page, enter the requested information and then click **Next**.

4. On the **Verify** page, enter the requested information, and then click **Next**.

   **Note:** You might be given the option to choose the method used to verify your identity.

If your identity is verified, the **Reset** page displays whether you were successfully verified and the state of your account (either locked or unlocked).

5. Based on your locked/unlocked state, perform one of the following actions:
   - If your account is not locked, the page displays the **Reset Password** button. Enter and reenter the new password and then click **Reset Password**.
   - If your account is locked, the page displays the **Reset Password** and **Unlock Account** buttons.
     - You can enter a new password and click **Reset password** to reset the password and unlock the account.
- If your administrator has selected **Enable account unlock** for the password process, you can unlock the account without resetting the password by clicking **Unlock account**.

**Users: Enroll in the Password Reset program**

Some organizations auto-enroll users in a Password Reset program. Your organization could offer you the option to enroll for one or more methods of verifying your identity when you reset your password. You might enroll for any combination of the following methods:

**Verify your identity using security questions (QA verification)**

To enroll, you choose multiple questions that only you can answer (like the name of your first pet) and then supply answers. The system stores your answers securely. Later, when you want to reset your password, the system presents one or more of the questions. You answer the questions to verify your identity.

**Verify your identity using an SMS code (SMS verification)**

To enroll, you authorize a device like a cellular phone for SMS verification. Later, when you want to reset your password, you get a code number on the device and enter the code on the web page to verify your identity.

**Users: Enroll in the Password Reset program using questions and answers**

Your organization might ask you to select the questions to use when resetting your password. You select the questions and provide answers that only you know. At another time, when you reset your password, your answers verify your identity.

**Role required: none**

1. Navigate to **Password Reset > Enroll** and then click the **QA Verification** tab.
   - If you are required to enroll for the QA verification method, then the tab is marked with an asterisk (*).
2. For each **Question** field, select a question from the list and then enter the answer in the **Answer** field. Repeat the process until the required number of **Question** and **Answer** fields are filled in.
3. Click **Submit**.
4. Optional: Enroll for an extra identity verification using any of the other methods that your organization offers. See:
   - **Users: Enroll in the Password Reset program using SMS codes**

**Users: Enroll in the Password Reset program using SMS codes**

To prove that you are who you say you are (verify your identity) while resetting your password, you can use a code number (the SMS code) that was delivered to your mobile phone or device.

**Role required: none**

1. Navigate to **Password Reset > Enroll** and then click the **SMS Verification** tab.
   - If your organization requires you to enroll for the SMS verification method, then the tab is marked with an asterisk (*).
2. If you had previously added an SMS-enabled device to your Password Reset profile, the device is listed. To add and verify a device, click **Add Device** and then follow the instructions.

---

Note: You cannot enroll for this program on a mobile device.
Provide a meaningful **Name** for each device. Repeat the process for as many devices as you need.

3. After you have verified each device, select the **Authorized** check box for each device that you expect to use to change or reset your password.

   **Note:** You can deauthorize a device at any time by clearing the **Authorized** check box.

4. Click **Submit**.

5. Optional: Enroll for an additional identity verification using any of the other methods that your organization offers. See:
   - *Users: Enroll in the Password Reset program using questions and answers*

**Orchestration examples**

These examples demonstrate how Orchestration can be used to automate common tasks.

**Active Directory automation example**

A set of six Orchestration Active Directory activities enables organizations to automate their on-boarding/off-boarding processes with auditable, self-documenting workflows that save time and eliminate mistakes.

The activities in the **Active Directory activity pack** are designed to manage user accounts and reset user passwords. The following activities cover the most common use cases administrators encounter when managing Active Directory user accounts:

- Create AD User Account
- Update AD User Account
- Remove AD User Account
- Disable AD User Account
- Query AD
- Reset AD User Password.

These activities share a common design, have complementary functionality, and share a common set of parameters. They can be used singly or together to create consistent workflows for provisioning and de-provisioning user accounts.

**Update Active Directory with Orchestration**

An organization plans to make their ServiceNow instance the single system of record for user account data and wants to update Active Directory with the latest changes.

The solution is to create an Orchestration workflow that pushes changes from the ServiceNow user record down to the Active Directory to create a new user record or update an existing record. This is accomplished by creating an Orchestration workflow that can create and update records in Active Directory based on the data in the ServiceNow User (sys_user) table.

**Note:** This example workflow assumes that ServiceNow is configured for LDAP and an LDAP server is configured to accept the new user accounts. The Active Directory user management activities are not dependent on LDAP, but the presence of LDAP makes this example workflow much easier. You must provide the domain controller's IP address to the...
workflow, either by hardcoding it, adding another workflow input, or using a script to look it up from the CMDB.

1. Navigate to Workflow > Workflow Editor.
2. In the Workflow tab, click the + icon to create a new workflow using these variables:
   - Name: Sync AD User
   - Table: Global (global)
3. Click Submit.
   A basic workflow with a Begin and End point appears on the canvas.
4. Click the menu icon in the upper left corner of the canvas and select Edit Inputs from the context menu.

   ![Workflow Editor](image)

   **Editing workflow inputs**

5. In the Workflow Inputs form, click New in the Variables record list, and create a new variable, using the fields in the table.
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Reference</td>
</tr>
<tr>
<td>Label</td>
<td>User</td>
</tr>
<tr>
<td>Column name</td>
<td>u_user</td>
</tr>
<tr>
<td>Reference Specification &gt; Reference</td>
<td>User (sys_user)</td>
</tr>
</tbody>
</table>

6. **Click Submit.**
7. In the **Custom** tab, expand **Custom Activities > Active Directory**.
8. Drag and drop the Update AD Object activity onto the transition line between the Begin and End points of the new workflow.
This action automatically links the activity with the end point and opens the Workflow Activity property form.
9. Complete the form using the fields in the table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a logical name such as <strong>Update user data.</strong></td>
</tr>
<tr>
<td>Domain controller</td>
<td>The ServiceNow LDAP integration adds a reference to the LDAP server to which the user's account is linked. To identify the LDAP server, enter the following statement: <code>${workflow.inputs.u_user.ldap_server.server_url}</code></td>
</tr>
<tr>
<td>Type</td>
<td>Type of AD object. In this case, the type is <strong>User</strong>, which is the default.</td>
</tr>
<tr>
<td>Object name</td>
<td>This example assumes that the ServiceNow user name matches the Active Directory sAMAccountName. Enter the following: <code>${workflow.inputs.u_user.user_name}</code></td>
</tr>
<tr>
<td>Object data</td>
<td>Updates the user's account inActive Directory, if the user exists. In this example, the user's title is updated: <code>{&quot;title&quot; : &quot;QA&quot;}</code></td>
</tr>
</tbody>
</table>

10. **Click Submit.**
The workflow looks like this:
11. Attach both activity outcomes (Success and Failure) to the end point.
At this point, the workflow takes a ServiceNow user record as input and updates the First Name, Last Name, and Title of the corresponding Active Directory account. If the account does not exist in Active Directory, the workflow fails.

Note: In a normal workflow, some type of alternate action is desirable upon failure. For example, you might send an email notification if the workflow failed to update the record.

12. To prevent the workflow from failing, add a Create AD Object activity to the transition lines between Begin and the Update AD Object activity.

13. Complete the Workflow Activity property form using the fields in the table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a logical name such as Create user data.</td>
</tr>
<tr>
<td>Domain controller</td>
<td>Same as for the update activity. ${workflow.inputs.u_user.ldap_server.server_url}</td>
</tr>
<tr>
<td>Ou</td>
<td>The organizational unit to which this object belongs. For the purpose of this example, you can enter <strong>OU=HQ,OU=Managed Objects</strong></td>
</tr>
<tr>
<td>Object name</td>
<td>Same as for the update activity. ${workflow.inputs.u_user.user_name}</td>
</tr>
<tr>
<td>Object data</td>
<td>Creates an account with only the user name in it. For the purpose of this example, you can enter <code>{&quot;givenName&quot; : &quot;$\{workflow.inputs.u_user.first_name\}&quot;}, &quot;SN&quot; : &quot;$\{workflow.inputs.u_user.last_name\}&quot; } </code></td>
</tr>
</tbody>
</table>

14. Click Submit.

15. Connect the Failure outcome of the Create AD Object activity to End.
   For this example, we are ignoring errors. The workflow now looks like this:
Creating an AD user

This procedure builds a simple workflow that creates a bare-bones Active Directory account consisting of a user name only. The workflow then updates that account with additional information provided by the ServiceNow User (sys_user) table. However, we do not want to execute the Create AD Object activity if the user account already exists. The workflow needs to query Active Directory for matching user records and then branch the workflow based on the results of the query. If an account already exists, then the workflow should update the account. If the account does not exist, then the workflow should create the account in Active Directory.

16. Drag and drop the Query AD activity onto the transition between Begin and Create AD Object.

17. Complete the Workflow Activity property form using the fields in the table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a logical name such as Search for existing account.</td>
</tr>
<tr>
<td>Domain controller</td>
<td>${workflow.inputs.u_user.ldap_server.server_url}</td>
</tr>
<tr>
<td>Properties</td>
<td>A comma-separated list of Active Directory properties to return. For example, givenName, SN, title. If the parameter field is blank, then all properties are returned. In this workflow, we leave the field blank.</td>
</tr>
<tr>
<td>Search filter</td>
<td>An LDAP filter string that defines the search parameters. Use any valid LDAP filtering criteria. To find user accounts matching the input record, we use: (samaccountname=${workflow.inputs.u_user.user_name})</td>
</tr>
</tbody>
</table>

18. Click Submit.

19. Connect the Failure outcome for the query activity to the End point. Remember that we are ignoring errors in this workflow.
20. Connect the Success outcome of the query activity to the Update AD Object activity. The workflow now looks like this:

![](image)

Querying AD for user accounts

The Query AD activity returns its results as a JSON string in the workflow data bus. This JSON string is always an array of objects. Each object corresponds to an Active Directory entry that matched the query. Our workflow should branch, whether that array is empty or not.

21. Drag a standard If activity from the Conditions folder in the Core tab and drop it onto the transition between Query AD and Update AD Object.

22. Complete the Workflow Activity properties form using the fields in the table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a logical name such as Account exists.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Select this check box to open the Script field.</td>
</tr>
<tr>
<td>Script</td>
<td>For the If activity to work correctly, we must return a yes or no in the answer variable (var) which corresponds to the Yes and No outcomes of the query activity. Line 1 converts the Query AD results from a JSON string into a Javascript array called queryResults. Line 2 checks the length of that array. If the array is more than 0, a match to the account was found, and we set our answer to yes. Otherwise, the answer is no. var queryResults=new JSON().decode(data.get(5).output); answer = (queryResults.length&gt;0 ? 'yes' : 'no');</td>
</tr>
</tbody>
</table>
**Note:** The expression `data.get(5)` in this script identifies the Query AD output in the Databus by order number, since it was the fifth activity added to the workflow.

---

**Query AD outputs in the Databus**

23. **Click Submit**.
24. In the canvas, create a transition from the Yes outcome of the If activity to the Update AD Object activity.
25. Create a transition from the No outcome of the If activity to the Create AD Object activity.
This is the final step. This workflow will query Active Directory to determine if an account already exists. If an account exists, the workflow updates that account. If an account does not exist, the workflow creates the account and then updates the Active Directory with the configured user data set.

Creating the conditional paths

**Orchestration activity packs**

The base Orchestration system includes packs of custom activities you can use to automate typical IT and business processes in your network.

Activity packs allow you to automate several common business processes, such as managing Active Directory accounts and Exchange server mailboxes. Activity packs can also automate IT functions such as starting and stopping Windows servers, joining domains, assigning IP addresses, and configuring load balancers.

**Use an activity pack**

The Packs tab of the Workflow Editor contains any activity packs downloaded from the ServiceNow Store and any activity packs that you create.

**Roles required**: admin, activity_admin, activity_creator

You can organize custom activities into packs and upload them to the ServiceNow Store. Your custom packs do not appear in the tree until at least one activity in the pack is published. Activities added to an existing pack are not displayed until they are published. Activity packs from any application scope can appear in the Packs tab, regardless of the current scope setting for the instance.

1. In the Workflow Editor palette, select the Packs tab.
2. Click the download icon.
The hierarchy in the tab organizes packs by vendor, scope, category, and activity.

**Active Directory activity pack**

The Active Directory (AD) activity pack enables an administrator to create, delete, and manage objects in Windows Active Directory, such as users, groups, and computers, using a ServiceNow Orchestration workflow.

Activities in this pack can reset a password automatically from a user request or manage any user account in Active Directory, whether or not it was created by an Orchestration workflow.

Domain controllers are identified by the IP address of the host machine. To use the hostname of the domain controller, add the Resolve DNS Name activity to resolve the hostname into an IP, and then pass the IP into the Active Directory activity.

Your instance must have access to a MID Server configured to use PowerShell to run these activities.

**Note:** All Active Directory activities pass through error messages returned from Active Directory. To view these error messages, point to the failed activity in the workflow canvas or select the Workflow Log tab in a Workflow Context record.
Custom Active Directory activities

Orchestration provides custom Active Directory activities that were created with the Orchestration Create a PowerShell activity, starting with the Geneva release. These activities perform the same functions as AD activities by the same name from previous releases and replace those activities for all new workflows. Existing workflows from earlier versions that were created with legacy AD activities continue to function normally after an upgrade to Istanbul. However, all new workflows must use these custom AD activities. The Powershell activity template gives workflow administrators the ability to store input and output variables from the Query AD activity in the databus.

Note: To use the Active Directory custom activities, you must request activation of the Orchestration - Active Directory plugin.

Active Directory credentials with LDAP

If you are using an LDAP Server with MID Servers, note that Orchestration and Active Directory activities do not use the user name and password configured on LDAP Servers. You must create a Windows type orchestration credential record. The username and password in the credentials record is used for LDAP queries that Orchestration and workflow activities perform.

Connection port used by AD Orchestration activities

All Active Directory activities use port 389 for LDAP access. If you are using AD activities with Oracle Virtual Directory (OVD) as a proxy, set up pass-through on port 389 only.

Add User to Group AD activity

The Add User to Group activity adds a user to a group in Windows Active Directory.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Active Directory.

Input variables

<table>
<thead>
<tr>
<th>Add User to Group input variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Variable</td>
</tr>
<tr>
<td>DomainController</td>
</tr>
<tr>
<td>UserName</td>
</tr>
<tr>
<td>GroupName</td>
</tr>
</tbody>
</table>

Output variables

<table>
<thead>
<tr>
<th>Add User to Group output variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Variable</td>
</tr>
<tr>
<td>result</td>
</tr>
</tbody>
</table>
ServiceNow    Jakarta    Now Platform Capabilities

Variable                     Description
errorMessage                 The `executionResult.errorMessages` from the Activity designer parsing sources.

Conditions

Add User to Group conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>User was successfully added to group.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to add the user to the group. Additional details may be available in the workflow log.</td>
</tr>
</tbody>
</table>

Change AD User Password activity

The Change AD User Password activity changes the password for an Active Directory user account.

This activity requires the user's current password to run, unlike the Reset AD User Password activity. If the new password violates any Active Directory password requirements, such as length or character combinations, the activity fails and returns the appropriate error message. This error message appears in the ECC queue and in hint text when a user points to the activity in the workflow editor.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Active Directory.

Note: This activity replaces an AD activity by the same name available in prior releases. If you have a workflow that uses the deprecated activity, your workflow will continue to work normally after upgrading to Instanbul. However, all new workflows must use the custom version of this activity, which was built with the PowerShell activity designer.

Input variables

Change AD User Password input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainController</td>
<td>IP address of the domain controller machine.</td>
</tr>
<tr>
<td>User</td>
<td>The sAMAccountName of the Active Directory user account.</td>
</tr>
<tr>
<td>New_password</td>
<td>The new password to assign this user.</td>
</tr>
<tr>
<td>Old_password</td>
<td>The user's current password.</td>
</tr>
</tbody>
</table>
Output variables

Change AD User Password output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>One of the following outcomes:</td>
</tr>
<tr>
<td></td>
<td>· failure</td>
</tr>
<tr>
<td></td>
<td>· success</td>
</tr>
<tr>
<td></td>
<td>· Policy Failure</td>
</tr>
<tr>
<td></td>
<td>· Incorrect old password</td>
</tr>
<tr>
<td>errorMessage</td>
<td>The <code>executionResult.errorMessages</code> from the Activity designer parsing sources.</td>
</tr>
<tr>
<td>hresult</td>
<td>Powershell command result.</td>
</tr>
</tbody>
</table>

Conditions

The activity provides the following conditions:

Change AD User Password conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Password successfully reset.</td>
</tr>
<tr>
<td>Policy Failure</td>
<td>Password does not comply with the organization's Active Directory requirements.</td>
</tr>
<tr>
<td>Incorrect old password</td>
<td>Password being changed was not entered correctly.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to change the password. Additional details may be available in the workflow log.</td>
</tr>
</tbody>
</table>

Active Directory credentials with LDAP

If you are using an LDAP Server with MID Servers, note that Orchestration and Active Directory activities do not use the user name and password configured on LDAP Servers. You must create a Windows type orchestration credential record. The username and password in the credentials record is used for LDAP queries that Orchestration and workflow activities perform.

Create AD Object activity

The Create AD Object activity creates an object in Windows Active Directory.

This activity fails if it finds an existing object with matching input variables.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Active Directory.

**Note:** This activity replaces an AD activity by the same name available in prior releases. If you have a workflow that uses the deprecated activity, your workflow will continue to work
normally after upgrading to Instanbul. However, all new workflows must use the custom version of this activity, which was built with the PowerShell activity designer.

### Input variables

**Create AD Object input variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainController</td>
<td>IP address of the domain controller machine.</td>
</tr>
<tr>
<td>Type</td>
<td>The object type to create: user, group, or computer.</td>
</tr>
<tr>
<td>OU</td>
<td>The organizational unit to which this object belongs.</td>
</tr>
<tr>
<td>ObjectName</td>
<td>The sAMAccountName of the Active Directory object.</td>
</tr>
<tr>
<td></td>
<td><strong>ObjectName</strong> is also used for the <strong>name</strong> attribute in Active Directory.</td>
</tr>
<tr>
<td></td>
<td>This behavior is available in <strong>ActiveDirectory.psm1</strong>.</td>
</tr>
<tr>
<td></td>
<td>Whatever is passed as the <strong>Object name</strong> becomes both the</td>
</tr>
<tr>
<td></td>
<td><strong>samAccountName</strong> and the <strong>name</strong> of the new user in Active Directory.</td>
</tr>
<tr>
<td>ObjectData</td>
<td>A JSON object containing Active Directory property names and their</td>
</tr>
<tr>
<td></td>
<td>corresponding values.</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>```</td>
</tr>
<tr>
<td></td>
<td>{</td>
</tr>
<tr>
<td></td>
<td>&quot;givenName&quot; : &quot;John&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;SN&quot; : &quot;Doe&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;title&quot; : &quot;Sr. Account Specialist&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;allowLogin&quot; : true</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>This example sets the first name (givenName), last name (SN), and title</td>
</tr>
<tr>
<td></td>
<td>on the Active Directory user account and allows that user to log in</td>
</tr>
<tr>
<td></td>
<td>(allowLogin). This field allows expression evaluation via the ${} syntax.</td>
</tr>
</tbody>
</table>

### Output variables

**Create AD Object output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Either <strong>success</strong> or <strong>failure</strong>.</td>
</tr>
<tr>
<td>errorMessage</td>
<td>The <strong>executionResult.errorMessages</strong> from the</td>
</tr>
<tr>
<td></td>
<td><strong>Activity designer parsing sources</strong>.</td>
</tr>
</tbody>
</table>
Conditions

Create AD Object conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>A Windows Active Directory object was created successfully.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to create the AD object. Additional details may be available in the workflow log.</td>
</tr>
</tbody>
</table>

Disable AD User Account activity

The Disable AD User Account activity disables a Windows Active Directory user account, making it inactive.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Active Directory.

Note: This activity replaces an AD activity by the same name available in prior releases. If you have a workflow that uses the deprecated activity, your workflow will continue to work normally after upgrading to Instanbul. However, all new workflows must use the custom version of this activity, which was built with the PowerShell activity designer.

Input variables

Disable AD User Account input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainController</td>
<td>IP address of the domain controller machine.</td>
</tr>
<tr>
<td>User</td>
<td>The sAMAccountName of the Active Directory user account.</td>
</tr>
</tbody>
</table>

Output variables

Disable AD User Account output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Either success or failure.</td>
</tr>
<tr>
<td>errorMessage</td>
<td>The executionResult.errorMessages from the Activity designer parsing sources.</td>
</tr>
</tbody>
</table>
Conditions

Disable AD User Account conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>AD user account was successfully disabled.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to disable the account. Additional details may be available in the workflow log.</td>
</tr>
</tbody>
</table>

Enable AD User Account activity

The Enable AD User Account activity enables a Windows Active Directory user account, making it active.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Active Directory.

**Note:** This activity replaces an AD activity by the same name available in prior releases. If you have a workflow that uses the deprecated activity, your workflow will continue to work normally after upgrading to Instanbul. However, all new workflows must use the custom version of this activity, which was built with the PowerShell activity designer.

Input variables

Enable AD User Account input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>The sAMAccountName of the Active Directory user account.</td>
</tr>
<tr>
<td>DomainController</td>
<td>IP address of the domain controller machine.</td>
</tr>
</tbody>
</table>

Output variables

Enable AD User Account output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Either success or failure.</td>
</tr>
<tr>
<td>errorMessage</td>
<td>The executionResult.errorMessages from the Activity designer parsing sources.</td>
</tr>
</tbody>
</table>
Conditions

Enable AD User Account conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>AD user account was successfully enabled.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to enable the AD user account. Additional details may be available in the workflow log.</td>
</tr>
</tbody>
</table>

Is AD Account Locked activity

The Is AD Account Locked activity determines whether an Active Directory user account is locked. An account may be locked automatically if a user enters an incorrect password more times than allowed by the Active Directory security policy. You can unlock an account using the Unlock AD User Account activity.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Active Directory.

Note: This activity replaces an AD activity by the same name available in prior releases. If you have a workflow that uses the deprecated activity, your workflow will continue to work normally after upgrading to Instanbul. However, all new workflows must use the custom version of this activity, which was built with the PowerShell activity designer.

Input variables

Is AD Account Locked input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainController</td>
<td>IP address of the domain controller machine.</td>
</tr>
<tr>
<td>User</td>
<td>The sAMAccountName of the Active Directory user account.</td>
</tr>
</tbody>
</table>

Output variables

Is AD Account Locked output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Either success or failure.</td>
</tr>
<tr>
<td>errorMessage</td>
<td>The executionResult.errorMessages from the Activity designer parsing sources.</td>
</tr>
<tr>
<td>output</td>
<td>The query result.</td>
</tr>
</tbody>
</table>
Conditions

Is AD Account Locked conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locked</td>
<td>The AD account is locked.</td>
</tr>
<tr>
<td>Unlocked</td>
<td>The AD account is unlocked.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while processing the query. Additional details may be available in the workflow log.</td>
</tr>
</tbody>
</table>

Query AD activity

The Query AD activity retrieves entries from the Windows Active Directory based on an LDAP search filter and stores the results as a JSON string that can be used in the data bus.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Active Directory >.

Note: This activity replaces an AD activity by the same name available in releases prior to Geneva. If you have a workflow that uses the deprecated activity, your workflow will continue to work normally after upgrading to Instanbul and will continue to save query results to the scratchpad. However, all new workflows must use the custom version of this activity. This activity was built with the Create a PowerShell activity, which stores input and output variables in the databus instead of the scratchpad.

Input variables

Query AD input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainController</td>
<td>IP address of the domain controller machine.</td>
</tr>
<tr>
<td>Properties</td>
<td>A comma-separated list of Active Directory properties to return. For example, givenName,SN,title. If this field is blank, then all properties are returned.</td>
</tr>
</tbody>
</table>
| SearchFilter | An LDAP filter string that defines the search parameters. Use any valid LDAP filtering criteria. For example, to find user accounts matching the ServiceNow input record, use:  

(samaccountname=${workflow.inputs.u_user.user_name})
Output variables

Query AD output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Either success or failure.</td>
</tr>
<tr>
<td>errorMessage</td>
<td>The <code>executionResult.errorMessages</code> from the <code>Activity designer parsing sources</code>.</td>
</tr>
<tr>
<td>output</td>
<td>The query result.</td>
</tr>
</tbody>
</table>

Conditions

Query AD conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The query completed as expected.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while processing the query. Additional details may be available in the workflow log.</td>
</tr>
</tbody>
</table>

Remove AD Object activity

The Remove AD Object activity deletes an object from Windows Active Directory.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Active Directory.

**Note:** This activity replaces an AD activity by the same name available in prior releases. If you have a workflow that uses the deprecated activity, your workflow will continue to work normally after upgrading to Instanbul. However, all new workflows must use the custom version of this activity, which was built with the PowerShell activity designer.

Input variables

Remove AD Object input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainController</td>
<td>IP address of the domain controller machine.</td>
</tr>
<tr>
<td>ObjectName</td>
<td>The <code>sAMAccountName</code> of the Active Directory object.</td>
</tr>
<tr>
<td>Type</td>
<td>The object type to remove:</td>
</tr>
<tr>
<td></td>
<td>• user</td>
</tr>
<tr>
<td></td>
<td>• group</td>
</tr>
<tr>
<td></td>
<td>• computer</td>
</tr>
</tbody>
</table>
Output variables

Remove AD Object output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Either success or failure.</td>
</tr>
<tr>
<td>errorMessage</td>
<td>The executionResult.errorMessages from the Activity designer parsing sources.</td>
</tr>
</tbody>
</table>

Conditions

Remove AD Object conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>AD object was successfully removed.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to remove the AD object. Additional details may be available in the workflow log.</td>
</tr>
</tbody>
</table>

Remove User from Group AD activity

The Remove User from Group activity removes a user from a group in Windows Active Directory. To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Active Directory.

Input variables

Remove User from Group input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainController</td>
<td>IP address of the domain controller machine.</td>
</tr>
<tr>
<td>UserName</td>
<td>Name of the user to remove from the group.</td>
</tr>
<tr>
<td>GroupName</td>
<td>Name of the group from which this user is removed.</td>
</tr>
</tbody>
</table>

Output variables

Remove User from Group output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Either success or failure.</td>
</tr>
<tr>
<td>errorMessage</td>
<td>The executionResult.errorMessages from the Activity designer parsing sources.</td>
</tr>
</tbody>
</table>
Conditions

Remove User from Group conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>User was successfully removed from the group.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to remove the user from the group. Additional details may be available in the workflow log.</td>
</tr>
</tbody>
</table>

Reset AD User Password activity

The Reset AD User Password activity resets the password of a user account in Windows Active Directory.

If the new password violates any Active Directory password requirements, such as length or character combinations, the reset activity fails and returns the appropriate error message. This error appears in the ECC Queue and when you point to the activity in the workflow editor.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Active Directory.

**Note:** This activity replaces an AD activity by the same name available in prior releases. If you have a workflow that uses the deprecated activity, your workflow will continue to work normally after upgrading to Instanbul. However, all new workflows must use the custom version of this activity, which was built with the PowerShell activity designer.

Input variables

Reset AD User Password input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainController</td>
<td>IP address of the domain controller machine.</td>
</tr>
<tr>
<td>User</td>
<td>The sAMAccountName of the Active Directory user account.</td>
</tr>
<tr>
<td>Password</td>
<td>The new password for the user. This password must comply with the organization's Active Directory requirements.</td>
</tr>
<tr>
<td>ForceChange</td>
<td>Makes this password temporary by forcing the user to change it at the next login.</td>
</tr>
<tr>
<td>Unlock</td>
<td>Unlock the account if the account is locked.</td>
</tr>
</tbody>
</table>
Output variables

Reset AD User Password output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>One of the following outcomes:</td>
</tr>
<tr>
<td></td>
<td>• failure</td>
</tr>
<tr>
<td></td>
<td>• success</td>
</tr>
<tr>
<td></td>
<td>• Policy Failure</td>
</tr>
<tr>
<td>errorMessage</td>
<td>The <code>executionResult.errorMessages</code> from the</td>
</tr>
<tr>
<td></td>
<td><code>Activity designer parsing sources</code>.</td>
</tr>
<tr>
<td>hresult</td>
<td>Powershell command result.</td>
</tr>
</tbody>
</table>

Conditions

Reset AD User Password conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Password was successfully reset.</td>
</tr>
<tr>
<td>Policy Failure</td>
<td>New password does not comply with the organization's Active Directory</td>
</tr>
<tr>
<td></td>
<td>requirements.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to reset the password. Additional</td>
</tr>
<tr>
<td></td>
<td>details may be available in the workflow log.</td>
</tr>
</tbody>
</table>

Unlock AD Account activity

The Unlock AD Account activity unlocks a locked Active Directory user account.
You can use the `Is AD Account Locked activity` activity to determine if an account is locked.
To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Active Directory.

Note: This activity replaces an AD activity by the same name available in prior releases. If you have a workflow that uses the deprecated activity, your workflow will continue to work normally after upgrading to Instanbul. However, all new workflows must use the custom version of this activity, which was built with the PowerShell activity designer.

Input variables

Unlock AD Account input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainController</td>
<td>IP address of the domain controller machine.</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User</td>
<td>The sAMAccountName of the Active Directory user account.</td>
</tr>
</tbody>
</table>

### Output variables

**Unlock AD Account output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Either success or failure.</td>
</tr>
<tr>
<td>errorMessage</td>
<td>The executionResult.errorMessages from the Activity designer parsing sources.</td>
</tr>
</tbody>
</table>

### Conditions

**Unlock AD Account conditions**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The account was successfully unlocked.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to unlock the account. Additional details may be available in the workflow log.</td>
</tr>
</tbody>
</table>

### Update AD Object activity

The Update AD Object activity updates an object in Windows Active Directory.

This activity only replaces existing values with new values. It cannot add new values to AD records such as adding a new group member to an AD group. For complex AD operations, use the Run PowerShell activity instead. The activity fails if it cannot find an existing account with matching object name and data.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Active Directory.

**Note:** This activity replaces an AD activity by the same name available in prior releases. If you have a workflow that uses the deprecated activity, your workflow will continue to work normally after upgrading to Instanbul. However, all new workflows must use the custom version of this activity, which was built with the PowerShell activity designer.

### Input variables

**Update AD Object input variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainController</td>
<td>IP address of the domain controller machine.</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------------------------------------------------------</td>
</tr>
<tr>
<td>ObjectName</td>
<td>The sAMAccountName of the Active Directory object.</td>
</tr>
<tr>
<td>ObjectData</td>
<td>A JSON object containing Active Directory properties and their values. For example, to set the first name, last name, and title of a user, clear the user's manager, and set the VIP flag to true, the Object Data specifies:</td>
</tr>
<tr>
<td></td>
<td>{ &quot;givenName&quot; : &quot;John&quot;, &quot;SN&quot; : &quot;Doe&quot;, &quot;title&quot; : &quot;Sr. Account Specialist&quot;, &quot;manager&quot; : null, &quot;msTSAllowLogon&quot; : false }</td>
</tr>
<tr>
<td>Type</td>
<td>The object type to update: user, group, or computer.</td>
</tr>
</tbody>
</table>

**Output variables**

**Update AD Object output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Either <strong>success</strong> or <strong>failure</strong>.</td>
</tr>
<tr>
<td>errorMessage</td>
<td>The <code>executionResult.errorMessages</code> from the <code>Activity designer parsing sources</code>.</td>
</tr>
</tbody>
</table>

**Conditions**

**Update AD Object conditions**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>AD object was successfully updated.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to update an AD object. Additional details may be available in the workflow log.</td>
</tr>
</tbody>
</table>

**Azure AD activity pack**

The Azure AD activity pack enables an administrator to automate employee onboarding and offboarding functions on Azure AD and manage Office 365 licensing.

Use the Azure AD activities to add and remove users to Azure Active Directory, manage security group membership, and assign or remove Office 365 licenses for individual users.

The Azure AD activities were created with the Orchestration [REST Web Service activity template](https://www.snow.com).

**Add User to Group Azure AD activity**

The Add User to Group activity adds a user to an existing security group in Azure Active Directory.
To access this activity in the workflow editor, select the **Custom** tab, and then navigate to **Custom Activities > Azure AD**. This activity was built with the **REST web service activity template**.

**Important:** The REST message used for this activity must be configured to use **OAuth2 authentication**.

### Input variables

**Add User to Group input variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user_id</td>
<td>Object ID (GUID) of the member to be added.</td>
</tr>
<tr>
<td>group_id</td>
<td>Object ID (GUID) of the target group.</td>
</tr>
</tbody>
</table>

### Output variables

**Add User to Group output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>error</td>
<td>Returns the error string from the REST message. If there are no errors, this variable returns a null value.</td>
</tr>
<tr>
<td>body</td>
<td>Contains a string value representing the output from the REST message.</td>
</tr>
<tr>
<td>status_code</td>
<td>Contains the status code returned from the Web service.</td>
</tr>
</tbody>
</table>

### Conditions

**Add User to Group conditions**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully added the object ID to the security group.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to update the group's membership, or the activity failed to connect to Azure AD.</td>
</tr>
</tbody>
</table>

### Assign User License Azure AD activity

The Assign User License activity assigns an additional Office 365 software license to the named user.

To access this activity in the workflow editor, select the **Custom** tab, and then navigate to **Custom Activities > Azure AD**. This activity was built with the **REST web service activity template**.

**Important:** The REST message used for this activity must be configured to use **OAuth2 authentication**.
Input variables

Assign User License input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user_id</td>
<td>The object ID (GUID) or the user principal name of the target user. An example of a user principal name is <a href="mailto:someuser@a830edad9050849NDA1.onmicrosoft.com">someuser@a830edad9050849NDA1.onmicrosoft.com</a>.</td>
</tr>
<tr>
<td>sku_id</td>
<td>Subscription SKU ID associated with the tenant’s enterprise agreement.</td>
</tr>
</tbody>
</table>

Output variables

Assign User License output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>error</td>
<td>Returns the error string from the REST message. If there are no errors, this variable returns a null value.</td>
</tr>
<tr>
<td>body</td>
<td>Contains a string value representing the output from the REST message.</td>
</tr>
<tr>
<td>status_code</td>
<td>Contains the status code returned from the Web service.</td>
</tr>
</tbody>
</table>

Conditions

Assign User License conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully assigned an Office 365 license to a user.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to assigned an Office 365 license to a user, or the activity failed to connect to Azure AD.</td>
</tr>
</tbody>
</table>

Create User Azure AD activity

The Create User activity creates a user for the Azure Active Directory tenant.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Azure AD. This activity was built with the REST web service activity template.

Important: The REST message used for this activity must be configured to use OAuth2 authentication.
# Input variables

## Create User input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>display_name</td>
<td>Name of the Azure AD user in the accepted display format, such as jacinto.gawron.</td>
</tr>
<tr>
<td>user_principal_name</td>
<td>User principal name (UPN) in an email format. For example, you might enter <a href="mailto:jacinto.gawron@khitomer.com">jacinto.gawron@khitomer.com</a>.</td>
</tr>
<tr>
<td>mailNickname</td>
<td>User's email alias that redirects to the user's full address.</td>
</tr>
<tr>
<td>password</td>
<td>User's Azure AD password. This password must be passed as a workflow input with a type of Password (2 Way Encrypted) and must meet the password policy set in Azure AD.</td>
</tr>
<tr>
<td>change_password</td>
<td>Control that requires the user to change his or her password at the next login, if set to true.</td>
</tr>
<tr>
<td>account_enabled</td>
<td>Control that sets the user's account is enabled, if set to true.</td>
</tr>
<tr>
<td>given_name</td>
<td>First name of the user.</td>
</tr>
<tr>
<td>surname</td>
<td>Last name of the user.</td>
</tr>
<tr>
<td>other_mails</td>
<td>List of additional email addresses for the user. For example, you might enter &quot;<a href="mailto:jac@home.com">jac@home.com</a>&quot;, &quot;<a href="mailto:jgawron@fabrikam.com">jgawron@fabrikam.com</a>&quot;.</td>
</tr>
<tr>
<td>country</td>
<td>The country or region in which the user is located. For example, you might enter US or UK. The default value is set to US.</td>
</tr>
<tr>
<td>city</td>
<td>City in which the user is located.</td>
</tr>
<tr>
<td>department</td>
<td>Name of the department in which the user works.</td>
</tr>
<tr>
<td>mobile</td>
<td>User's primary cell phone number.</td>
</tr>
<tr>
<td>job_title</td>
<td>User's job title.</td>
</tr>
<tr>
<td>physical_delivery_office_name</td>
<td>Office location in the user place of business.</td>
</tr>
<tr>
<td>postal_code</td>
<td>Postal code of the user's address.</td>
</tr>
<tr>
<td>preferred_language</td>
<td>Language in which the user prefers to communicate. This value must follow the ISO 639-1 Code. For example, you might enter en-US. The default value is set to en-US.</td>
</tr>
<tr>
<td>state</td>
<td>State or province for the user's address.</td>
</tr>
<tr>
<td>street_address</td>
<td>Street address of the user's place of business.</td>
</tr>
<tr>
<td>telephone_number</td>
<td>Primary telephone number of the user's place of business.</td>
</tr>
<tr>
<td>usage_location</td>
<td>Two letter country code that is required for users who are assigned Office 365 licenses. The default value is US.</td>
</tr>
</tbody>
</table>
Output variables

Create User output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>error</td>
<td>Returns the error string from the REST message. If there are no errors, this variable returns a null value.</td>
</tr>
<tr>
<td>status_code</td>
<td>Contains the status code returned from the Web service.</td>
</tr>
<tr>
<td>user_exists</td>
<td>Output variable mapped to the JSON message that contains the User already exists error.</td>
</tr>
<tr>
<td>user_info</td>
<td>The user_info array contains attributes that can be leveraged by other activities as inputs. For example, the user objectid output (GUID) can be passed to the Add User to Group activity as the user_id input.</td>
</tr>
<tr>
<td></td>
<td>· objectid: User’s Azure AD identifier.</td>
</tr>
<tr>
<td></td>
<td>· accountEnabled: Boolean variable indicating whether the user’s account is active or inactive.</td>
</tr>
<tr>
<td></td>
<td>· displayName: Users display name, such as jacinto.gawron.</td>
</tr>
<tr>
<td></td>
<td>· userPrincipalName: User’s name in email format, such as <a href="mailto:jacinto.gawron@wammo.com">jacinto.gawron@wammo.com</a>.</td>
</tr>
<tr>
<td></td>
<td>· mailNickname: User’s email alias.</td>
</tr>
</tbody>
</table>

Conditions

Create User conditions

<table>
<thead>
<tr>
<th>Conditions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created user</td>
<td>Activity successfully created the user.</td>
</tr>
<tr>
<td>User already exists</td>
<td>User already exists in the tenant domain.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to connect to Azure AD, or an input value was invalid.</td>
</tr>
</tbody>
</table>

Delete User Azure AD activity

The Delete User activity deletes the named user’s account from the Azure Active Directory tenant. To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Azure AD. This activity was built with the REST web service activity template.

Important: The REST message used for this activity must be configured to use OAuth2 authentication.
Input variables

Delete User input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user_id</td>
<td>The object ID (GUID) or the user principal name of the target user. An example of a user principal name is <a href="mailto:someuser@a830edad9050849NDA1.onmicrosoft.com">someuser@a830edad9050849NDA1.onmicrosoft.com</a>.</td>
</tr>
</tbody>
</table>

Output variables

Delete User output variables

<table>
<thead>
<tr>
<th>Variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>error</td>
<td>Returns the error string from the REST message. If there are no errors, this variable returns a null value.</td>
</tr>
<tr>
<td>body</td>
<td>Contains a string value representing the output from the REST message.</td>
</tr>
<tr>
<td>status_code</td>
<td>Contains the status code returned from the Web service.</td>
</tr>
</tbody>
</table>

Conditions

Delete User conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deleted user</td>
<td>Activity deleted the specified user.</td>
</tr>
<tr>
<td>User does not exist</td>
<td>Specified user does not have an account in the tenant domain.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to connect to Azure AD.</td>
</tr>
</tbody>
</table>

Get User Info Azure AD activity

The Get User Info activity returns the named user's information from the Azure Active Directory. To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Azure AD. This activity was built with the REST web service activity template.

Important: The REST message used for this activity must be configured to use OAuth2 authentication.
### Input variables

**Check If User Exists input variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
</table>
| user_id  | The object ID (GUID) or the user principal name of the target user. An example of a user principal name is `someuser@a830edad9050849NDA1.onmicrosoft.com`.  
**Note:** Version 2 of this activity enforces input validation. If empty, the following message appears: *Mandatory input 'user_id' is empty*. |

### Output variables

**Check If User Exists output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>error</td>
<td>Returns the error string from the REST message. If there are no errors, this variable returns a null value.</td>
</tr>
<tr>
<td>body</td>
<td>Contains a string value representing the output from the REST message.</td>
</tr>
<tr>
<td>status_code</td>
<td>Contains the status code returned from the Web service.</td>
</tr>
</tbody>
</table>
| user_info | The `user_info` array contains attributes that can be leveraged by other activities as inputs. For example, the user `objectid` output (GUID) can be passed to the Add User to Group activity as the `user_id` input.  
- **objectid**: User's Azure AD identifier.  
- **accountEnabled**: Boolean variable indicating whether the user's account is active or inactive.  
- **displayName**: Users display name, such as `jacinto.gawron`.  
- **userPrincipalName**: User's name in email format, such as `jacinto.gawron@wammo.com`.  
- **mailNickname**: User's email alias. |
Conditions

Check If User Exists conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User exists</td>
<td>Activity found the named user.</td>
</tr>
<tr>
<td>User does not exist</td>
<td>Activity was unable to find the named user in the customer tenant domain.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to connect to Azure AD.</td>
</tr>
</tbody>
</table>

Remove User from Group Azure AD activity

The Remove User from Group activity removes an existing user from a security group in Azure Active Directory.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Azure AD. This activity was built with the REST web service activity template.

**Important:** The REST message used for this activity must be configured to use OAuth2 authentication.

Input variables

Remove User from Group input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user_id</td>
<td>Object ID (GUID) of the user to be removed.</td>
</tr>
<tr>
<td>group_id</td>
<td>Object ID (GUID) of the target group.</td>
</tr>
</tbody>
</table>

Output variables

Remove User from Group output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>error</td>
<td>Returns the error string from the REST message. If there are no errors, this variable returns a null value.</td>
</tr>
<tr>
<td>body</td>
<td>Contains a string value representing the output from the REST message.</td>
</tr>
<tr>
<td>status_code</td>
<td>Contains the status code returned from the Web service.</td>
</tr>
</tbody>
</table>
Conditions

Remove User from Group conditions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity removed the object ID from the security group.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to update the group's membership, or the activity failed to connect to Azure AD.</td>
</tr>
</tbody>
</table>

Remove User License Azure AD activity

The Remove User License activity revokes the specified Office 365 software license for the named user.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Azure AD. This activity was built with the REST web service activity template.

**Important:** The REST message used for this activity must be configured to use OAuth2 authentication.

Input variables

Remove User License input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user_id</td>
<td>The object ID (GUID) or the user principal name of the target user. An example of a user principal name is <a href="mailto:someuser@a830edad9050849NDA1.onmicrosoft.com">someuser@a830edad9050849NDA1.onmicrosoft.com</a>.</td>
</tr>
<tr>
<td>sku_id</td>
<td>Subscription SKU ID associated with the tenant's enterprise agreement.</td>
</tr>
</tbody>
</table>

Output variables

Remove User License output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>error</td>
<td>Returns the error string from the REST message. If there are no errors, this variable returns a null value.</td>
</tr>
<tr>
<td>body</td>
<td>Contains a string value representing the output from the REST message.</td>
</tr>
<tr>
<td>status_code</td>
<td>Contains the status code returned from the Web service.</td>
</tr>
</tbody>
</table>
Conditions

Remove User License conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity removed an Office 365 license from the named user.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to remove an Office 365 from a user, or the activity failed to connect to Azure AD.</td>
</tr>
</tbody>
</table>

Reset User Password Azure AD activity

The Reset User Password activity changes the named user’s Azure Active Directory password.

The Azure password policy imposes constraints on the complexity, length, and re-use of a password.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Azure AD. This activity was built with the REST web service activity template.

Important: The REST message used for this activity must be configured to use OAuth2 authentication.

Input variables

Reset User Password input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user_id</td>
<td>The object ID (GUID) or the user principal name of the target user. An example of a user principal name is <a href="mailto:someuser@a830edad9050849NDA1.onmicrosoft.com">someuser@a830edad9050849NDA1.onmicrosoft.com</a>.</td>
</tr>
<tr>
<td>password</td>
<td>User’s Azure AD password. This password must be passed as a workflow input with a type of Password (2 Way Encrypted) and must meet the password policy set in Azure AD.</td>
</tr>
<tr>
<td>change_password</td>
<td>Control that requires the user to change his or her password at the next login, if set to true.</td>
</tr>
</tbody>
</table>

Output variables

Reset User Password output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>error</td>
<td>Returns the error string from the REST message. If there are no errors, this variable returns a null value.</td>
</tr>
<tr>
<td>body</td>
<td>Contains a string value representing the output from the REST message.</td>
</tr>
</tbody>
</table>
### Variable Table

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status_code</td>
<td>Contains the status code returned from the Web service.</td>
</tr>
</tbody>
</table>

### Conditions

#### Reset User Password conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity reset the named user's password.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to reset the named user's password, or the activity failed to connect to Azure AD.</td>
</tr>
</tbody>
</table>

### Exchange activity pack

The Exchange activity pack allows workflows to manage Microsoft Exchange mail systems. The use of Orchestration Exchange activities requires the following:

- Microsoft Exchange 2010 or 2013.
- A MID Server configured to run Powershell 2.0
- A target Exchange server in the same Active Directory domain as the instance.
- Powershell Remoting enabled on the target Exchange server.

**Note:** These activities cannot be used to interact with Microsoft Exchange Online.

Orchestration provides custom Exchange activities that were created with the Orchestration activity designer template. These activities perform the same functions as Exchange activities by the same name from previous releases and replace those activities for all new workflows. The custom Exchange activities were built with a [Powershell activity template](#), which gives workflow administrators the ability to store input and output variables in the [databus](#).

**Note:** Existing workflows from earlier versions that were created with legacy Exchange activities continue to function normally after an upgrade to Geneva. However, all new workflows must use these custom Exchange activities.

To use the Microsoft Exchange custom activities, you must request activation of the Orchestration - Exchange plugin. The custom Exchange activities are available in the Workflow Editor on the Custom tab. Expand the Custom Activities tree and select the Exchange category for the activity you want to use.
Accessing custom Exchange activities

Configure MID Server for Exchange

Configure a MID Server with defined IP ranges to use Exchange.
If the MID Server manages resources within defined IP ranges, instead of all computers on your network, you must perform additional configuration steps to run Exchange activities. You do not need to perform these steps if your MID Server uses the default configuration.

1. In the navigation filter, enter cmdb_ci_dns_name.list.
2. Click New.
3. Enter the fully-qualified domain name (FQDN) of your Exchange server in the Name field.
4. Right-click the form header and select Save.
5. In the IP Address related list, click New.
6. In the IP Address field, enter the IP address of your Exchange server.
7. In the Nic field, select eth0 or your preferred network interface controller.
8. Leave the Netmask field blank.
9. Click Submit.

Pass multivalued properties with an Exchange activity

To set a multivalued property using an Exchange activity, you must use a specific parameter format.

The Optional parameters shared input variable allows you to set multivalued properties.

- To set a multivalued property, replacing any existing values, use this format:
  "PropertyName":"(value1,value2,value3)"
- To add values, use this format: "PropertyName":"+(value1,value2,value3);"
- To remove values, use this format: "PropertyName":"-{value1,value2,value3};"
- To both add and remove values, use this format: "PropertyName":"-{value1,value2,value3};
  +(value1,value2,value3);"

Create Address List activity

The Create Address List activity creates a new address list that acts as an alias for emailing all users in the group.

This alias cannot be used to manage user permissions. This activity implements the Microsoft Exchange New-AddressList command.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Exchange > Address List.

**Note:** This activity replaces an Exchange activity by the same name available in releases prior to Geneva. If you have a workflow created in a previous version that uses the deprecated activity, your workflow will continue to work normally after upgrading to Geneva. However, all new workflows must use the custom version of this activity. This activity was built with the PowerShell activity designer, which gives workflow administrators the ability to store input and output variables in the databus.

Input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>The hostname of the Exchange server with which the activity interacts. Do not enter an IP address in this variable.</td>
</tr>
</tbody>
</table>
### Variable Description

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain</td>
<td>The name of the Exchange server's assigned domain.</td>
</tr>
<tr>
<td>name</td>
<td>Name of the new address list to create.</td>
</tr>
<tr>
<td>parameters</td>
<td>Optional parameters to pass to the Exchange server written in JavaScript Object Notation (JSON). Exchange activities cannot pass parameters that reference an object, such as a PSCredential object. Plain text is automatically converted to SecureString objects for parameters that require that data type. Attempting to save an activity that specifies duplicate parameters, including parameters from activity variables, or incorrectly formatted JSON causes a warning message to appear. <strong>Note:</strong> When passing a switch parameter, such as ForceUpgrade, you must use the format &quot;parameter&quot;: &quot;true&quot;.</td>
</tr>
</tbody>
</table>

### Output variables

**Create Address List output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Either success or failure.</td>
</tr>
<tr>
<td>error</td>
<td>Error message if the operation fails.</td>
</tr>
<tr>
<td>output</td>
<td>Raw XML payload from the Exchange server. This data includes all Exchange attributes.</td>
</tr>
</tbody>
</table>

### Conditions

**Create Address List conditions**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The activity succeeded in creating a new address list.</td>
</tr>
<tr>
<td>Failure</td>
<td>The activity failed to create a new address list.</td>
</tr>
</tbody>
</table>

### Delete Address List activity

The Delete Address List activity removes an existing address list from an Exchange server. This activity implements the Microsoft Exchange *Remove-AddressList* command.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Exchange > Address List.
Note: This activity replaces an Exchange activity by the same name available in releases prior to Geneva. If you have a workflow created in a previous version that uses the deprecated activity, your workflow will continue to work normally after upgrading to Geneva. However, all new workflows must use the custom version of this activity. This activity was built with the PowerShell activity designer, which gives workflow administrators the ability to store input and output variables in the databus.

### Input variables

**Delete Address List input variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>The hostname of the Exchange server with which the activity interacts. Do not enter an IP address in this variable.</td>
</tr>
<tr>
<td>domain</td>
<td>The name of the Exchange server’s assigned domain.</td>
</tr>
<tr>
<td>identity</td>
<td>Name of the address list to remove.</td>
</tr>
<tr>
<td>domainController</td>
<td>Fully-qualified domain name (FQDN) of the domain controller that writes to Active Directory.</td>
</tr>
<tr>
<td>recursive</td>
<td>Check box that indicates if the activity should delete Active Directory elements that are children of the specified address list.</td>
</tr>
<tr>
<td>whatif</td>
<td>Check box that indicates if the activity should stage the changes without applying them. Use this variable to test your activity settings before using the activity in a live workflow. When this variable is selected, the Exchange server does not make any changes but indicates if the command would succeed or fail. You can review any messages from the Exchange server using the ECC queue.</td>
</tr>
</tbody>
</table>

### Output variables

**Delete Address List output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Either <strong>success</strong> or <strong>failure</strong>.</td>
</tr>
<tr>
<td>error</td>
<td>Error message if the operation fails.</td>
</tr>
</tbody>
</table>
Conditions

Delete Address List conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The activity succeeded in removing the address list from the Exchange server.</td>
</tr>
<tr>
<td>Failure</td>
<td>The activity failed to remove the address list from the Exchange server.</td>
</tr>
</tbody>
</table>

Get Address List activity

The Get AddressList activity retrieves all attributes from the specified Exchange address list.

This activity implements the Microsoft Exchange `Get-AddressList` command.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Exchange > Address List.

**Note:** This activity replaces an Exchange activity by the same name available in releases prior to Geneva. If you have a workflow created in a previous version that uses the deprecated activity, your workflow will continue to work normally after upgrading to Geneva. However, all new workflows must use the custom version of this activity. This activity was built with the PowerShell activity designer, which gives workflow administrators the ability to store input and output variables in the databus.

Input variables

Get Address List input variables

<table>
<thead>
<tr>
<th>Variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>The hostname of the Exchange server with which the activity interacts. Do not enter an IP address in this variable.</td>
</tr>
<tr>
<td>domain</td>
<td>The name of the Exchange server's assigned domain.</td>
</tr>
<tr>
<td>domainController</td>
<td>Fully-qualified domain name (FQDN) of the domain controller that writes to Active Directory.</td>
</tr>
<tr>
<td>identity</td>
<td>Name of the address list to get attributes from. If you enter a value in this variable, leave the container and searchText variables blank.</td>
</tr>
<tr>
<td>organization</td>
<td>Organization to which the specified address list belongs.</td>
</tr>
<tr>
<td>searchText</td>
<td>Filter text that causes the activity to return only results that contain this text. This variable can only be used with Exchange 2013 servers. If you enter a value in this variable, leave the container and identity variables blank.</td>
</tr>
</tbody>
</table>
Output variables

Get Address List output variables

<table>
<thead>
<tr>
<th>Variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Either success or failure.</td>
</tr>
<tr>
<td>error</td>
<td>Error message if the operation fails.</td>
</tr>
<tr>
<td>output</td>
<td>Raw XML payload from the Exchange server. This data includes all Exchange attributes.</td>
</tr>
</tbody>
</table>

Conditions

Get Address List conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The activity succeeded in retrieving the attributes from the address list.</td>
</tr>
<tr>
<td>Failure</td>
<td>The activity failed to retrieve the attributes from the address list.</td>
</tr>
</tbody>
</table>

Move Address List activity

The Move Address List activity moves a Microsoft Exchange address list to another location in the address hierarchy.

This activity implements the Microsoft Exchange Move-AddressList command.

The Exchange server caches the changes from this activity but does not immediately apply them. Use the Update Address List activity after this activity to apply the changes or wait for the Exchange server to automatically apply cached changes.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Exchange > Address List.

Note: This activity replaces an Exchange activity by the same name available in releases prior to Geneva. If you have a workflow created in a previous version that uses the deprecated activity, your workflow will continue to work normally after upgrading to Geneva. However, all new workflows must use the custom version of this activity. This activity was built with the PowerShell activity designer, which gives workflow administrators the ability to store input and output variables in the databus.
Input variables

Move Address List input variables

<table>
<thead>
<tr>
<th>Variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>The hostname of the Exchange server with which the activity interacts. Do not enter an IP address in this variable.</td>
</tr>
<tr>
<td>domain</td>
<td>The name of the Exchange server’s assigned domain.</td>
</tr>
<tr>
<td>identity</td>
<td>Name of the address list to move.</td>
</tr>
<tr>
<td>target</td>
<td>Path to the address list’s new location.</td>
</tr>
<tr>
<td>domainController</td>
<td>Fully-qualified domain name (FQDN) of the domain controller that writes to Active Directory.</td>
</tr>
<tr>
<td>whatif</td>
<td>Check box that indicates if the activity should stage the changes without applying them. Use this variable to test your activity settings before using the activity in a live workflow. When this variable is selected, the Exchange server does not make any changes but indicates if the command would succeed or fail. You can review any messages from the Exchange server using the ECC queue.</td>
</tr>
</tbody>
</table>

Output variables

Move Address List output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Either success or failure.</td>
</tr>
<tr>
<td>error</td>
<td>Error message if the operation fails.</td>
</tr>
</tbody>
</table>

Conditions

Move Address List conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The activity succeeded in moving the address list to another location.</td>
</tr>
<tr>
<td>Failure</td>
<td>The activity failed to move the address list to another location.</td>
</tr>
</tbody>
</table>

Set Address List activity

The Set Address List activity modifies a Microsoft Exchange address list.
Use the Optional parameters variable to pass specific values to the Microsoft Exchange server. This activity implements the Microsoft Exchange Set-AddressList command.

The Exchange server caches the changes from this activity but does not immediately apply them. Use the Update Address List after this activity to apply the changes or wait for the Exchange server to automatically apply cached changes.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Exchange > Address List.

**Note:** This activity replaces an Exchange activity by the same name available in releases prior to Geneva. If you have a workflow created in a previous version that uses the deprecated activity, your workflow will continue to work normally after upgrading to Geneva. However, all new workflows must use the custom version of this activity. This activity was built with the PowerShell activity designer, which gives workflow administrators the ability to store input and output variables in the databus.

### Input variables

**Set Address List input variables**

<table>
<thead>
<tr>
<th>Variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>The hostname of the Exchange server with which the activity interacts. Do not enter an IP address in this variable.</td>
</tr>
<tr>
<td>domain</td>
<td>The name of the Exchange server’s assigned domain.</td>
</tr>
<tr>
<td>identity</td>
<td>Name of the address list to modify.</td>
</tr>
<tr>
<td>parameters</td>
<td>Optional parameters to pass to the Exchange server written in JavaScript Object Notation (JSON). Exchange activities cannot pass parameters that reference an object, such as a PSCredential object. Plain text is automatically converted to SecureString objects for parameters that require that data type. Attempting to save an activity that specifies duplicate parameters, including parameters from activity variables, or incorrectly formatted JSON causes a warning message to appear. <strong>Note:</strong> When passing a switch parameter, such as ForceUpgrade, you must use the format “parameter”:“true”.</td>
</tr>
</tbody>
</table>

### Output variables

**Set Address List output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Either success or failure.</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>error</td>
<td>Error message if the operation fails.</td>
</tr>
</tbody>
</table>

**Conditions**

**Set Address List conditions**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The activity succeeded in modifying the specified address list.</td>
</tr>
<tr>
<td>Failure</td>
<td>The activity failed to modify the specified address list.</td>
</tr>
</tbody>
</table>

**Update Address List activity**

The Update Address List activity adds or removes users from the specified address list and immediately applies any cached address list changes to the server.

Use the optional parameters variable to specify which users to add or remove. This activity implements the Microsoft Exchange `Update-AddressList` command.

To access this activity in the workflow editor, select the **Custom** tab, and then navigate to **Custom Activities > Exchange > Address List**.

**Note:** This activity replaces an Exchange activity by the same name available in releases prior to Geneva. If you have a workflow created in a previous version that uses the deprecated activity, your workflow will continue to work normally after upgrading to Geneva. However, all new workflows must use the custom version of this activity. This activity was built with the PowerShell activity designer, which gives workflow administrators the ability to store input and output variables in the **databus**.

**Input variables**

**Update Address List input variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>The hostname of the Exchange server with which the activity interacts. Do not enter an IP address in this variable.</td>
</tr>
<tr>
<td>domain</td>
<td>The name of the Exchange server's assigned domain.</td>
</tr>
<tr>
<td>identity</td>
<td>Name of the address list to update.</td>
</tr>
<tr>
<td>domainController</td>
<td>Fully-qualified domain name (FQDN) of the domain controller that writes to Active Directory.</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>whatif</td>
<td>A check box that indicates if the activity should stage the changes without applying them. Use this variable to test your activity settings before using the activity in a live workflow. When this variable is selected, the Exchange server does not make any changes but indicates if the command would succeed or fail. You can review any messages from the Exchange server using the ECC queue.</td>
</tr>
</tbody>
</table>

**Output variables**

**Update Address List output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Either <strong>Success</strong> or <strong>Failure</strong>.</td>
</tr>
<tr>
<td>error</td>
<td>Error message if the operation fails.</td>
</tr>
</tbody>
</table>

**Conditions**

**Update Address List conditions**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The activity succeeded in adding or removing users from the specified address list.</td>
</tr>
<tr>
<td>Failure</td>
<td>The activity failed to add or remove users from the specified address list.</td>
</tr>
</tbody>
</table>

**Create Mailbox activity**

The Create Mailbox activity creates a new Active Directory user, if that user does not already exist, and a Microsoft Exchange mailbox for that user.

This activity implements the Microsoft Exchange **New-Mailbox** command.

To access this activity in the workflow editor, select the **Custom** tab, and then navigate to **Custom Activities > Exchange > Mailbox**.

**Note:** This activity replaces an Exchange activity by the same name available in releases prior to Geneva. If you have a workflow created in a previous version that uses the deprecated activity, your workflow will continue to work normally after upgrading to Geneva. However, all new workflows must use the custom version of this activity. This activity was built with the **PowerShell activity designer**, which gives workflow administrators the ability to store input and output variables in the **databus**.
### Input variables

**Create Mailbox input variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>The hostname of the Exchange server with which the activity interacts. Do not enter an IP address in this variable.</td>
</tr>
<tr>
<td>domain</td>
<td>The name of the Exchange server's assigned domain. Important: The MID Server must be in the same domain as the Exchange server.</td>
</tr>
<tr>
<td>first_name</td>
<td>First name of the user.</td>
</tr>
<tr>
<td>middle_initial</td>
<td>Middle initial of the user.</td>
</tr>
<tr>
<td>last_name</td>
<td>Last name of the user.</td>
</tr>
<tr>
<td>alias</td>
<td>The display name for the mailbox address, the part of the email address to the left of the @ symbol. If no alias is specified, the activity uses First name.Last name as the alias. The alias is also used as the user's principal name (UPN) if none is specified in the optional parameters.</td>
</tr>
<tr>
<td>password</td>
<td>Password to use for the new mailbox. The password is encrypted when it is sent to the target host.</td>
</tr>
<tr>
<td>parameters</td>
<td>Optional parameters to pass to the Exchange server written in JavaScript Object Notation (JSON). Exchange activities cannot pass parameters that reference an object, such as a PSCredential object. Plain text is automatically converted to SecureString objects for parameters that require that data type. Attempting to save an activity that specifies duplicate parameters, including parameters from activity variables, or incorrectly formatted JSON causes a warning message to appear. Note: When passing a switch parameter, such as ForceUpgrade, you must use the format &quot;parameter&quot;: &quot;true&quot;.</td>
</tr>
</tbody>
</table>

### Output variables

**Create Mailbox output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Either success or failure.</td>
</tr>
<tr>
<td>error</td>
<td>Error message if the operation fails.</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>output</td>
<td>Raw XML payload from the Exchange server. This data includes all Exchange attributes.</td>
</tr>
</tbody>
</table>

### Conditions

#### Create Mailbox conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The activity succeeded in creating a new mailbox for the specified user. If no Active Directory account existed for that user, this activity succeeded in creating a new account.</td>
</tr>
<tr>
<td>Failure</td>
<td>The activity failed to create a new mailbox or an Active Directory account for the specified user.</td>
</tr>
</tbody>
</table>

#### Delete Mailbox activity

The Delete Mailbox activity deletes the Microsoft Exchange mailbox of an Active Directory user. Optional parameters determine how the Exchange server handles the mailbox after deleting the user. This activity implements the Microsoft Exchange Remove-Mailbox command.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Exchange > Mailbox.

**Note:** This activity replaces an Exchange activity by the same name available in releases prior to Geneva. If you have a workflow created in a previous version that uses the deprecated activity, your workflow will continue to work normally after upgrading to Geneva. However, all new workflows must use the custom version of this activity. This activity was built with the PowerShell activity designer, which gives workflow administrators the ability to store input and output variables in the databus.

### Input variables

#### Delete Mailbox input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>The hostname of the Exchange server with which the activity interacts. Do not enter an IP address in this variable.</td>
</tr>
<tr>
<td>domain</td>
<td>The name of the Exchange server’s assigned domain.</td>
</tr>
<tr>
<td>user</td>
<td>Active Directory user to delete. The activity passes this value to Exchange as the Identity Exchange variable.</td>
</tr>
</tbody>
</table>
Variable | Description
--- | ---
parameters | Optional parameters to pass to the Exchange server written in JavaScript Object Notation (JSON). Exchange activities cannot pass parameters that reference an object, such as a PSCredential object. Plain text is automatically converted to SecureString objects for parameters that require that data type.

Attempting to save an activity that specifies duplicate parameters, including parameters from activity variables, or incorrectly formatted JSON causes a warning message to appear.

**Note:** When passing a switch parameter, such as ForceUpgrade, you must use the format "parameter": "true".

Output variables

Delete Mailbox output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Either success or failure.</td>
</tr>
<tr>
<td>error</td>
<td>Error message if the operation fails.</td>
</tr>
</tbody>
</table>

Conditions

Delete Mailbox conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The activity succeeded in deleting the specified user's mailbox.</td>
</tr>
<tr>
<td>Failure</td>
<td>The activity failed to delete the specified user's mailbox.</td>
</tr>
</tbody>
</table>

Disable Mailbox activity

The Disable Mailbox activity disables the mailbox associated with a specified Active Directory account.

This activity implements the Microsoft Exchange Disable-Mailbox command.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Exchange > Mailbox.

**Note:** This activity replaces an Exchange activity by the same name available in releases prior to Geneva. If you have a workflow created in a previous version that uses the deprecated activity, your workflow will continue to work normally after upgrading to Geneva. However, all new workflows must use the custom version of this activity. This
activity was built with the *PowerShell activity designer*, which gives workflow administrators the ability to store input and output variables in the *databus*.

## Input variables

**Disable Mailbox input variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>The hostname of the Exchange server with which the activity interacts. Do not enter an IP address in this variable.</td>
</tr>
<tr>
<td>domain</td>
<td>The name of the Exchange server's assigned domain.</td>
</tr>
<tr>
<td>user</td>
<td>Active Directory user who's mailbox should be disabled. The activity passes this value to Exchange as the Identity Exchange variable.</td>
</tr>
<tr>
<td>parameters</td>
<td>Optional parameters to pass to the Exchange server written in JavaScript Object Notation (JSON). Exchange activities cannot pass parameters that reference an object, such as a PSCredential object. Plain text is automatically converted to SecureString objects for parameters that require that data type. Attempting to save an activity that specifies duplicate parameters, including parameters from activity variables, or incorrectly formatted JSON causes a warning message to appear.</td>
</tr>
</tbody>
</table>

*Note:* When passing a switch parameter, such as ForceUpgrade, you must use the format `"parameter":"true"`.  

## Output variables

**Disable Mailbox output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Either <em>success</em> or <em>failure</em>.</td>
</tr>
<tr>
<td>error</td>
<td>Error message if the operation fails.</td>
</tr>
</tbody>
</table>

## Conditions

**Disable Mailbox conditions**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The activity succeeded in disabling the specified mailbox.</td>
</tr>
</tbody>
</table>
Enable Mailbox activity

The Enable Mailbox activity creates a new mailbox for an existing Active Directory user.

This activity implements the Microsoft Exchange `Enable-Mailbox` command.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Exchange > Mailbox.

**Note:** This activity replaces an Exchange activity by the same name available in releases prior to Geneva. If you have a workflow created in a previous version that uses the deprecated activity, your workflow will continue to work normally after upgrading to Geneva. However, all new workflows must use the custom version of this activity. This activity was built with the PowerShell activity designer, which gives workflow administrators the ability to store input and output variables in the databus.

Input variables

Enable Mailbox input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>The hostname of the Exchange server with which the activity interacts. Do not enter an IP address in this variable.</td>
</tr>
<tr>
<td>domain</td>
<td>The name of the Exchange server's assigned domain.</td>
</tr>
<tr>
<td>user</td>
<td>Active Directory user who's mailbox should be enabled. The activity passes this value to Exchange as the Identity Exchange variable.</td>
</tr>
<tr>
<td>parameters</td>
<td>Optional parameters to pass to the Exchange server written in JavaScript Object Notation (JSON). Exchange activities cannot pass parameters that reference an object, such as a PSCredential object. Plain text is automatically converted to SecureString objects for parameters that require that data type. Attempting to save an activity that specifies duplicate parameters, including parameters from activity variables, or incorrectly formatted JSON causes a warning message to appear. <strong>Note:</strong> When passing a switch parameter, such as ForceUpgrade, you must use the format “parameter”:true”.</td>
</tr>
</tbody>
</table>
Output variables

Enable Mailbox output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Either success or failure.</td>
</tr>
<tr>
<td>error</td>
<td>Error message if the operation fails.</td>
</tr>
</tbody>
</table>

Conditions

Enable Mailbox conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The activity succeeded in creating a new mailbox for the specified user.</td>
</tr>
<tr>
<td>Failure</td>
<td>The activity failed to create a new mailbox for the specified user.</td>
</tr>
</tbody>
</table>

Get Mailbox activity

The Get Mailbox activity gets the mailbox for the specified user or all mailboxes on a Microsoft Exchange server.

This activity implements the Microsoft Exchange Get-Mailbox command.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Exchange > Mailbox.

Note: This activity replaces an Exchange activity by the same name available in releases prior to Geneva. If you have a workflow created in a previous version that uses the deprecated activity, your workflow will continue to work normally after upgrading to Geneva. However, all new workflows must use the custom version of this activity. This activity was built with the PowerShell activity designer, which gives workflow administrators the ability to store input and output variables in the databus.

Input variables

Get Mailbox input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>The hostname of the Exchange server with which the activity interacts. Do not enter an IP address in this variable.</td>
</tr>
<tr>
<td>domain</td>
<td>The name of the Exchange server's assigned domain.</td>
</tr>
</tbody>
</table>
### Variable Description

- **user**: User whose mailbox this activity should retrieve. If no user is specified, the activity gets all mailboxes on the Exchange server. The activity passes this value to Exchange as the Identity Exchange variable.

- **parameters**: Optional parameters to pass to the Exchange server written in JavaScript Object Notation (JSON). Exchange activities cannot pass parameters that reference an object, such as a PSCredential object. Plain text is automatically converted to SecureString objects for parameters that require that data type. Attempting to save an activity that specifies duplicate parameters, including parameters from activity variables, or incorrectly formatted JSON causes a warning message to appear.

  **Note**: When passing a switch parameter, such as ForceUpgrade, you must use the format `"parameter":"true"`. 

### Output variables

**Get Mailbox output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Either <strong>success</strong> or <strong>failure</strong>.</td>
</tr>
<tr>
<td>error</td>
<td>Error message if the operation fails.</td>
</tr>
<tr>
<td>output</td>
<td>Raw XML payload from the Exchange server. This data includes all Exchange attributes.</td>
</tr>
</tbody>
</table>

### Conditions

**Get Mailbox conditions**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The activity succeeded in retrieving the attributes of the specified mailbox.</td>
</tr>
<tr>
<td>Failure</td>
<td>The activity failed to retrieve the attributes of the specified mailbox.</td>
</tr>
</tbody>
</table>

### Set Mailbox activity

The Set Mailbox activity modifies the settings of an existing Microsoft Exchange mailbox.

Use the optional parameters variable to pass specific values to the Exchange server. This activity implements the Microsoft Exchange **Set-Mailbox** command.
To access this activity in the workflow editor, select the **Custom** tab, and then navigate to **Custom Activities > Exchange > Mailbox**.

**Note:** This activity replaces an Exchange activity by the same name available in releases prior to Geneva. If you have a workflow created in a previous version that uses the deprecated activity, your workflow will continue to work normally after upgrading to Geneva. However, all new workflows must use the custom version of this activity. This activity was built with the **PowerShell activity designer**, which gives workflow administrators the ability to store input and output variables in the **databus**.

### Input variables

**Set Mailbox input variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>The hostname of the Exchange server with which the activity interacts. Do not enter an IP address in this variable.</td>
</tr>
<tr>
<td>domain</td>
<td>The name of the Exchange server's assigned domain.</td>
</tr>
<tr>
<td>user</td>
<td>Active Directory user whose mailbox you want to modify. The activity passes this value to Exchange as the Identity Exchange variable.</td>
</tr>
<tr>
<td>parameters</td>
<td>Optional parameters to pass to the Exchange server written in JavaScript Object Notation (JSON). Exchange activities cannot pass parameters that reference an object, such as a PSCredential object. Plain text is automatically converted to SecureString objects for parameters that require that data type. Attempting to save an activity that specifies duplicate parameters, including parameters from activity variables, or incorrectly formatted JSON causes a warning message to appear. <strong>Note:</strong> When passing a switch parameter, such as ForceUpgrade, you must use the format &quot;parameter&quot;:&quot;true&quot;.</td>
</tr>
</tbody>
</table>

### Output variables

**Set Mailbox output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Either <strong>success</strong> or <strong>failure</strong>.</td>
</tr>
<tr>
<td>error</td>
<td>Error message if the operation fails.</td>
</tr>
</tbody>
</table>
Conditions

Set Mailbox conditions

<table>
<thead>
<tr>
<th>Conditions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The activity succeeded in modifying the settings of the specified mailbox.</td>
</tr>
<tr>
<td>Failure</td>
<td>The activity failed to modify the settings of the specified mailbox.</td>
</tr>
</tbody>
</table>

F5 Network Management activity pack

Orchestration provides custom activities for configuring elements of an F5 load balancer, including pools, pool members, and the virtual servers contained in the pool.

All F5 custom activities are in the F5 Network Management Application scope and are activated by the Orchestration - F5 network management plugin, which must be activated by request.

ServiceNow provides custom F5 activities, built from the REST web service activity template, that you can use to perform the following tasks:

- Add, delete, or verify pools.
- Add, delete, or identify pool members.
- Add or delete virtual servers.
- Add a profile to a virtual server.
- Configure the virtual server for vlans, irules, pool, and persistence.

Add F5 Pool Member activity

The Add F5 Pool Member activity adds a member to an F5 load balancer pool.

This activity was built using the REST web service activity template. To access the activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Active Directory.

REST settings

- **REST message**: F5 POOL Membership Management
- **REST function**: post

Input variables

Add F5 Pool Member input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PoolName</td>
<td>Name of this pool, such as testPool.</td>
</tr>
<tr>
<td>F5IPAddress</td>
<td>IP address of the F5 console.</td>
</tr>
<tr>
<td>MemberName</td>
<td>Pool member IP address and port, such as 192.168.2.19:80.</td>
</tr>
</tbody>
</table>
Output variables

Add F5 Pool Member output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Success or failure.</td>
</tr>
<tr>
<td>status_code</td>
<td>The HTTP status code.</td>
</tr>
<tr>
<td>error</td>
<td>The REST error.</td>
</tr>
<tr>
<td>output</td>
<td>The REST output.</td>
</tr>
</tbody>
</table>

Conditions

Add F5 Pool Member conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully added an F5 load balancer pool member.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to add an F5 load balancer pool member.</td>
</tr>
</tbody>
</table>

Get F5 Pool Member activity

The Get F5 Pool Member activity returns the pool members and verifies the pool's status.

Use this activity to verify that a pool member was created properly.

This activity was built using the REST web service activity template. To access the activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Active Directory.

REST settings

- REST message: F5 POOL Membership Management
- REST function: get

Input variables

Get F5 Pool Member input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PoolName</td>
<td>Name of this pool, such as testPool.</td>
</tr>
<tr>
<td>F5IPAddress</td>
<td>IP address of the F5 console.</td>
</tr>
</tbody>
</table>
Output variables

Get F5 Pool Member output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MembersArray</td>
<td>Array for the returned pool member IP address and port, such as 192.168.2.19:80.</td>
</tr>
<tr>
<td>status_code</td>
<td>The HTTP status code.</td>
</tr>
<tr>
<td>error</td>
<td>The REST error.</td>
</tr>
<tr>
<td>result</td>
<td>Success or failure.</td>
</tr>
<tr>
<td>output</td>
<td>The REST output.</td>
</tr>
</tbody>
</table>

Conditions

Get F5 Pool Member conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully returned the F5 load balancer pool members.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to return the F5 load balancer pool members</td>
</tr>
</tbody>
</table>

Delete F5 Virtual Server activity

The Delete F5 Virtual Server activity deletes a virtual server from an F5 load balancer pool.
This activity was built using the REST web service activity template. To access the activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Active Directory.

REST settings

- **REST message**: F5 VIP Management
- **REST function**: delete

Input variables

Delete F5 Virtual Server input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F5IPAddress</td>
<td>IP address of the F5 console.</td>
</tr>
<tr>
<td>name</td>
<td>The virtual server's name, such as testVIP.</td>
</tr>
</tbody>
</table>
Output variables

**Delete F5 Virtual Server output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Success or failure.</td>
</tr>
<tr>
<td>status_code</td>
<td>The HTTP status code.</td>
</tr>
</tbody>
</table>

Conditions

**Delete F5 Virtual Server conditions**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully deleted the virtual server from the F5 load balancer pool.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to delete the virtual server from the F5 load balancer pool.</td>
</tr>
</tbody>
</table>

Check F5 Pool activity

The Check F5 Pool activity checks the status of a pool to determine if it is available to accept traffic.

Use this activity to determine if a pool you just created is up and running with the proper configuration.

This activity was built using the *REST web service activity template*. To access the activity in the workflow editor, select the **Custom** tab, and then navigate to **Custom Activities > Active Directory**.

**REST settings**

- **REST message**: F5 POOL Management
- **REST function**: get

Input variables

**Check F5 Pool input variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F5IPAddress</td>
<td>IP address of the F5 console.</td>
</tr>
<tr>
<td>PoolName</td>
<td>Name of this pool, such as <code>testPool</code>.</td>
</tr>
</tbody>
</table>
Output variables

Check F5 Pool output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Success or failure.</td>
</tr>
<tr>
<td>status_code</td>
<td>The HTTP status code.</td>
</tr>
<tr>
<td>error</td>
<td>The REST error.</td>
</tr>
</tbody>
</table>

Conditions

Check F5 Pool conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully returned the status of the F5 load balancer pool.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to return the status of the F5 load balancer pool.</td>
</tr>
</tbody>
</table>

Add F5 Profile to Virtual Server activity

The Add F5 Profile to Virtual Server activity adds a profile to a virtual server assigned to an F5 load balancer pool.

This activity was built using the REST web service activity template. To access the activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Active Directory.

REST settings

- **REST message**: F5 VIP Profile Management
- **REST function**: post

Input variables

Add F5 Profile to Virtual Server input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The virtual server's name, such as testVIP</td>
</tr>
<tr>
<td>F5IPAddress</td>
<td>IP address of the F5 console.</td>
</tr>
<tr>
<td>VirtualServerName</td>
<td>Name of the virtual server, such as testVIP.</td>
</tr>
</tbody>
</table>
Output variables

Add F5 Profile to Virtual Server output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Success or failure.</td>
</tr>
<tr>
<td>output</td>
<td>The REST output.</td>
</tr>
<tr>
<td>status_code</td>
<td>The HTTP status code.</td>
</tr>
</tbody>
</table>

Conditions

Add F5 Profile to Virtual Server conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully added the F5 load balancer profile to the virtual server.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to add the F5 load balancer profile to the virtual server.</td>
</tr>
</tbody>
</table>

Modify F5 Virtual Server activity

The Modify F5 Virtual Server activity configures a virtual server assigned to an F5 load balancer pool with irules and a vlan.

This activity was built using the REST web service activity template. To access the activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Active Directory.

REST settings

- REST message: F5 VIP Management
- REST function: put

Input variables

Modify F5 Virtual Server input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The virtual server's name, such as testVIP.</td>
</tr>
<tr>
<td>F5IPAddress</td>
<td>IP address of the F5 console.</td>
</tr>
<tr>
<td>irules</td>
<td>The irules for the virtual server, such as _sys_https_redirect.</td>
</tr>
<tr>
<td>pool</td>
<td>Name of the pool for the virtual server, such as testPool.</td>
</tr>
<tr>
<td>persistent</td>
<td>Persistent profile for the virtual server, such as cookie.</td>
</tr>
</tbody>
</table>
Output variables

Modify F5 Virtual Server output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Success or failure.</td>
</tr>
<tr>
<td>status_code</td>
<td>The HTTP status code.</td>
</tr>
<tr>
<td>output</td>
<td>The REST output.</td>
</tr>
</tbody>
</table>

Conditions

Modify F5 Virtual Server conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully configured a virtual server assigned to an F5 load balancer pool.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to configure a virtual server assigned to an F5 load balancer pool.</td>
</tr>
</tbody>
</table>

Add F5 Virtual Server activity

The Add F5 Virtual Server activity adds a virtual server.

This activity was built using the REST web service activity template. To access the activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Active Directory.

REST settings

- **REST message**: F5 POOL Membership Management
- **REST function**: post

Input variables

Add F5 Virtual Server input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The virtual server's name, such as testVIP.</td>
</tr>
<tr>
<td>description</td>
<td>Description of this virtual server.</td>
</tr>
<tr>
<td>ipProtocol</td>
<td>Protocol used for this virtual server, such as tcp.</td>
</tr>
<tr>
<td>destination</td>
<td>Virtual server IP address and port number, such as 192.168.4.20:80.</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>mask</td>
<td>Subnet mask for this virtual server, such as 255.255.255.255.</td>
</tr>
<tr>
<td>F5IPAddress</td>
<td>IP address of the F5 console.</td>
</tr>
<tr>
<td>sourceAddressTranslation</td>
<td>Source address translation mode.</td>
</tr>
</tbody>
</table>

**Output variables**

Add F5 Virtual Server output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Success or failure.</td>
</tr>
<tr>
<td>status_code</td>
<td>The HTTP status code.</td>
</tr>
<tr>
<td>error</td>
<td>The REST error.</td>
</tr>
<tr>
<td>output</td>
<td>The REST output.</td>
</tr>
</tbody>
</table>

**Conditions**

Add F5 Virtual Server conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully added a virtual server.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to add a virtual server.</td>
</tr>
</tbody>
</table>

**Delete F5 Pool Member activity**

The Delete F5 Pool Member activity deletes an F5 load balancer pool member.

This activity was built using the REST web service activity template. To access the activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Active Directory.

**REST settings**

- REST message: F5 POOL Membership Management
- REST function: delete

**Input variables**

Delete F5 Pool Member input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PoolName</td>
<td>Name of this pool, such as testPool.</td>
</tr>
<tr>
<td>F5IPAddress</td>
<td>IP address of the F5 console.</td>
</tr>
</tbody>
</table>
### Output variables

**Delete F5 Pool Member output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Success or failure.</td>
</tr>
<tr>
<td>status_code</td>
<td>The HTTP status code.</td>
</tr>
<tr>
<td>error</td>
<td>The REST error.</td>
</tr>
</tbody>
</table>

### Conditions

**Delete F5 Pool Member output variables**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity succeeded in deleting an F5 load balancer pool member.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to delete an F5 load balancer pool member.</td>
</tr>
</tbody>
</table>

### Delete F5 Pool activity

The Delete F5 Pool activity deletes an F5 load balancer pool.

This activity was built using the **REST web service activity template**. To access the activity in the workflow editor, select the **Custom** tab, and then navigate to **Custom Activities > Active Directory**.

### REST settings

- **REST message**: F5 POOL Management
- **REST function**: delete

### Input variables

**Delete F5 Pool input variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F5IPAddress</td>
<td>IP address of the F5 console.</td>
</tr>
<tr>
<td>PoolName</td>
<td>Name of this pool, such as testPool.</td>
</tr>
</tbody>
</table>
Output variables

Delete F5 Pool output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Success or failure.</td>
</tr>
<tr>
<td>error</td>
<td>The REST error.</td>
</tr>
<tr>
<td>status_code</td>
<td>The HTTP status code.</td>
</tr>
</tbody>
</table>

Conditions

Delete F5 Pool conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully deleted the F5 load balancer pool.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to delete the F5 load balancer pool.</td>
</tr>
</tbody>
</table>

Add F5 Pool activity

The Add F5 Pool activity creates the F5 load balancer pool.

Use this activity to verify that a pool member was created properly.

This activity was built using the REST web service activity template. To access the activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Active Directory.

REST settings

- REST message: F5 POOL Management
- REST function: post

Input variables

Add F5 Pool input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PoolName</td>
<td>Name of this pool, such as testPool.</td>
</tr>
<tr>
<td>F5IPAddress</td>
<td>IP address of the F5 console.</td>
</tr>
<tr>
<td>MemberName</td>
<td>Pool member IP address and port, such as 192.168.2.19:80.</td>
</tr>
</tbody>
</table>
Output variables

Add F5 Pool output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Success or failure.</td>
</tr>
<tr>
<td>status_code</td>
<td>The HTTP status code.</td>
</tr>
<tr>
<td>error</td>
<td>The REST error.</td>
</tr>
<tr>
<td>output</td>
<td>The REST output.</td>
</tr>
</tbody>
</table>

Conditions

Add F5 Pool conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity succeeded in creating the F5 load balancer pool.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to create the F5 load balancer pool.</td>
</tr>
</tbody>
</table>

Infoblox DDI activity pack

This activity pack supports Infoblox DDI management through ServiceNow Orchestration. The Infoblox DDI activity pack manages the IP addresses used in a network by integrating DNS and DHCP. Custom Orchestration activities use Infoblox Web API (WAPI) REST web services to access the Infoblox GRID server.

Important: Managing IP addresses through the Infoblox server requires a fully functional MID Server.

Starting with the Jakarta release, the Infoblox activity pack updates to version 2. This update supports Infoblox network views, which can restrict the visibility of network data. The view parameter can be passed as a query parameter or payload content, to do operations in a specific view. Version 2 also supports specifying the version of WAPI to use in integration endpoints.

Supported for Infoblox:
- WAPI version 2.0 for REST messages
- NIOS appliance version 7.0

Note: To use the Infoblox DDI activities and workflow, you must request activation of the Orchestration - Infoblox DDI Activity Pack plugin.

Create a REST credential for Infoblox activities

All Infoblox activities require a REST credential to manage IP addresses from the Infoblox DDI server.

Before starting this procedure, make sure you have the following:
- A properly configured and running Infoblox DDI Grid Server.
- REST credentials defined on the Infoblox DDI server.

Role required: admin

You must create a REST credential record on the ServiceNow instance that each Infoblox activity can use to access management features on the Infoblox server.

1. Navigate to Orchestration > Credentials and click New.
2. In the list of credential types, select Basic Auth Credentials.
3. Create the credential record with a logical name, such as InfobloxCred.
4. Right-click in the header bar of your new credential record and select Copy sys_id from the context menu. Follow browser instructions to copy the sys_id if browser security measures restrict this function.
5. Paste the sys_id into the restCredentials input field of each activity you use.

Infoblox workflows

The Infobox DDI activity pack includes two default workflows, one that reserves and registers IP addresses and another that releases IP addresses.

To access these workflows, navigate to Workflow > Workflow Editor and select the Workflows tab. Click on a workflow to open it, and then click the information icon in the workflow header to display the properties dialog box.

Infoblox Reserve/Register IP in IPAM

Use this workflow to register IPv4 addresses or request the next available IP address on IPAM. Optionally, you can use it to register IP addresses on DNS. The custom Infoblox activities used in this workflow are:

- IPAM Register IP Address
- IPAM Reserve IP Address
- Register DNS A-Record
- Get Network Details

### Infoblox Reserve/Register IP input variables

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infoblox Server</td>
<td>IP address of the Infoblox DDI server.</td>
</tr>
<tr>
<td>Network</td>
<td>Network containing the target IP address.</td>
</tr>
<tr>
<td>Zone</td>
<td>The DNS zone for the IP address being registered.</td>
</tr>
<tr>
<td>Rest Credentials</td>
<td>The sys_id of the REST credentials from the ServiceNow instance.</td>
</tr>
<tr>
<td>DNS Host Name</td>
<td>Name of the DNS server machine on which the IP address is being registered.</td>
</tr>
<tr>
<td>IPv4 Address</td>
<td>IP address being reserved or registered.</td>
</tr>
</tbody>
</table>
**Infoblox Release IPAM Reservations**

Use this workflow to release (delete) all the IPAM reservations associated with an IPv4 address. The custom Infoblox activities used in this workflow are:

- [IPAM List IP Reservations](#)
- [List DNS Record](#)
- [DNS Delete](#)
- [IPAM Delete](#)

### Infoblox Release IPAM Reservations input variables

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rest Credentials</td>
<td>The sys_id of the REST credentials from the ServiceNow instance.</td>
</tr>
<tr>
<td>IP to Delete</td>
<td>IP address to release.</td>
</tr>
<tr>
<td>Infoblox Server</td>
<td>IP address of the Infoblox DDI server.</td>
</tr>
</tbody>
</table>

### Infoblox roles and permissions

Define the roles and permissions that the Infoblox activities need to access the various resources on the Infoblox server.

#### Admin groups

There are three types of admin groups on an Infoblox server:

- Superuser
- Default
- Limited Access

To perform specific operations on the Infoblox server, the Limited Access user must have a minimum set of privileges for the desired resources, using either the user interface or an API. These privileges are based on read and read/write access. For more information, refer to the “About Admin Groups” section in the Infoblox NIOS Administrator Guide.

#### Permission hierarchy

1. **User**: A user can be part of multiple groups.
2. **Group**: A group can have many roles.
3. **Role**: Each role consists of specific resource permissions.

#### Required permissions

The ServiceNow Infoblox activity pack requires appropriate read and read/write privileges for these resources:

- Network
- DHCP
- DNS
- IPAM

This example shows a default DHCP admin role, its resources, and the related permissions for each.
### Infoblox permissions

<table>
<thead>
<tr>
<th>Group/Role</th>
<th>Permission Type</th>
<th>Resource Type</th>
<th>Permission Type</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Admin</td>
<td>DHCP Permissions</td>
<td>All DHCP Devices</td>
<td>DHCP Policies</td>
<td>RW</td>
</tr>
<tr>
<td>DHCP Admin</td>
<td>DHCP Permissions</td>
<td>DHCP IPv4 Lease History</td>
<td>IPv4 Lease History</td>
<td>RD</td>
</tr>
<tr>
<td>DHCP Admin</td>
<td>DHCP Permissions</td>
<td>DHCP IPv6 Lease History</td>
<td>IPv6 Lease History</td>
<td>RD</td>
</tr>
<tr>
<td>DHCP Admin</td>
<td>DHCP Permissions</td>
<td>IPv4 DHCP Policies</td>
<td>IPv4 DHCP Policies</td>
<td>FW</td>
</tr>
<tr>
<td>DHCP Admin</td>
<td>DHCP Permissions</td>
<td>DHCP IPv4 Lease History</td>
<td>IPv4 Lease History</td>
<td>RD</td>
</tr>
<tr>
<td>DHCP Admin</td>
<td>DHCP Permissions</td>
<td>All IPv4 DHCP Templates</td>
<td>IPv4 Template</td>
<td>RD</td>
</tr>
<tr>
<td>DHCP Admin</td>
<td>DHCP Permissions</td>
<td>All DNS Keys</td>
<td>DNS Keys</td>
<td>FW</td>
</tr>
<tr>
<td>DHCP Admin</td>
<td>DHCP Permissions</td>
<td>All HTTP Server Keys</td>
<td>HTTP Server Keys</td>
<td>FW</td>
</tr>
<tr>
<td>DHCP Admin</td>
<td>DHCP Permissions/IPAM Permissions</td>
<td>All Network Views</td>
<td>Network View</td>
<td>FW</td>
</tr>
<tr>
<td>DHCP Admin</td>
<td>DHCP Permissions/IPAM Permissions</td>
<td>All IPv4 DHCP Templates</td>
<td>IPv4 Template</td>
<td>RD</td>
</tr>
</tbody>
</table>
Infoblox DHCP activities

The Infoblox DHCP activities manage the IP addresses reserved for DHCP in your network. Use these activities to reserve, list, or delete IP addresses that are used for DHCP assignment in your network.

**DHCP Reserve IP v4 Address Range activity**

The DHCP Reserve IP v4 Address Range activity reserves an IP address range for DHCP use.

The DHCP activities use the REST web service activity template to manage IP addresses using an Infoblox DDI Grid Server. These activities are configured to use a MID Server with REST capabilities.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Infoblox DDI > DHCP.

**Input variables**

**DHCP Reserve IP v4 Address Range input variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InfobloxServer</td>
<td>Name of the Infoblox DDI Grid Server.</td>
</tr>
<tr>
<td>startIpAddress</td>
<td>Beginning IPv4 address of the range to reserve.</td>
</tr>
<tr>
<td>endIpAddress</td>
<td>Ending IPv4 address of the range to reserve.</td>
</tr>
<tr>
<td>restCredentials</td>
<td>The sys_id of the REST credentials from the ServiceNow instance.</td>
</tr>
<tr>
<td>api_version</td>
<td>Defines the version of WAPI to use for the integration endpoints. The default value is 2.0.</td>
</tr>
</tbody>
</table>

**Note:** This field is mandatory. If the field is empty, the orchestration activity will fail.

<table>
<thead>
<tr>
<th>variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>view</td>
<td>Name of the Infoblox network view. The default value is default.</td>
</tr>
</tbody>
</table>

**Note:** If the field is empty, the operation is treated as happening in the default view.

**Output variables**

**DHCP Reserve IP v4 Address Range output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcpIPv4AddressRange</td>
<td>Range of reserved IPv4 addresses.</td>
</tr>
<tr>
<td>error</td>
<td>Displays the message for any REST error encountered.</td>
</tr>
</tbody>
</table>
Conditions

**DHCP Reserve IP v4 Address Range conditions**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully reserved the specified IPv4 address range.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to reserve the specified IPv4 address range.</td>
</tr>
</tbody>
</table>

**DHCP Delete IP Reservation activity**

The DHCP Delete IP Reservation activity deletes IP reservations in DHCP using either an IPv4 or IPv6 address range.

An automation can obtain an Infoblox DHCP object to delete from either of these activities:
- [DHCP List IP Reservations](#)
- [DHCP Reserve IPv4 Address Range](#)

The DHCP activities use the [REST web service activity template](#) to manage IP addresses using an Infoblox DDI Grid Server. These activities are configured to use a MID Server with REST capabilities.

To access this activity in the workflow editor, select the [Custom tab](#), and then navigate to Custom Activities > Infoblox DDI > DHCP.

**Input variables**

**DHCP Delete IP Reservation input variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InfobloxServer</td>
<td>Name of the Infoblox DDI Grid Server.</td>
</tr>
<tr>
<td>ipToDelete</td>
<td>IP address range to delete, in the form: range/&lt;encrypted code&gt;:&lt;start range&gt;/&lt;end range&gt;/default</td>
</tr>
<tr>
<td>restCredentials</td>
<td>The sys_id of the REST credentials from the ServiceNow instance.</td>
</tr>
<tr>
<td>api_version</td>
<td>Defines the version of WAPI to use for the integration endpoints. The default value is 2.0.</td>
</tr>
</tbody>
</table>

*Note: This field is mandatory. If the field is empty, the orchestration activity will fail.*

**Output variables**

**DHCP Delete IP Reservation output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPDeletedIpRange</td>
<td>Range of deleted IP addresses.</td>
</tr>
</tbody>
</table>
### Variable Description

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>error</td>
<td>Displays the message for any REST error encountered.</td>
</tr>
</tbody>
</table>

### Conditions

#### DHCP Delete IP Reservation conditions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully deleted the specified IP address range.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to delete the specified IP address range.</td>
</tr>
</tbody>
</table>

#### DHCP List IP Reservations activity

The DHCP List IP Reservations activity generates a list of all the DHCP range reservations on a specific InfoBlox server.

The DHCP activities use the [REST web service activity template](#) to manage IP addresses using an Infoblox DDI Grid Server. These activities are configured to use a MID Server with REST capabilities.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Infoblox DDI > DHCP.

### Input variables

#### DHCP List IP Reservations input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InfobloxServer</td>
<td>Name of the Infoblox DDI Grid Server.</td>
</tr>
<tr>
<td>restCredentials</td>
<td>The sys_id of the REST credentials from the ServiceNow instance.</td>
</tr>
<tr>
<td>api_version</td>
<td>Defines the version of WAPI to use for the integration endpoints. The default value is 2.0.</td>
</tr>
</tbody>
</table>

**Note:** This field is mandatory. If field is empty, the orchestration activity will fail.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>view</td>
<td>Name of the Infoblox network view. The default value is default.</td>
</tr>
</tbody>
</table>

**Note:** If the field is empty, the operation is treated as happening with no view and returns the values with data from all views.
Output variables

DHCP List IP Reservations output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reference</td>
<td>Reference value for an array of DHCP address ranges in this format: range/&lt;encrypted code&gt;:&lt;start range&gt;/&lt;end range&gt;/default</td>
</tr>
<tr>
<td>network</td>
<td>Address of the network containing the IP address range.</td>
</tr>
<tr>
<td>network_view</td>
<td>Routing domain associated with the network returned.</td>
</tr>
</tbody>
</table>

Conditions

DHCP List IP Reservations conditions

<table>
<thead>
<tr>
<th>Variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully returned an array of DHCP IP address ranges.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to return an array of DHCP IP address ranges.</td>
</tr>
</tbody>
</table>

Infoblox DNS activities

The Infoblox DNS activities manage DNS records in your network using an Infoblox DDI Grid Server. Use these activities to register, list, or delete DNS records managed on an Infoblox server.

List DNS C-records activity

The List DNS C-records activity retrieves all canonical (CNAME) records from a specified Infoblox server.

The DNS activities use the REST web service activity template to manage DNS records using an Infoblox DDI Grid Server. These activities are configured to use a MID Server with REST capabilities.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Infoblox DDI > DNS.

Input variables

List DNS C-records input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InfobloxServer</td>
<td>Name of the Infoblox DDI Grid Server.</td>
</tr>
<tr>
<td>restCredentials</td>
<td>The sys_id of the REST credentials from the ServiceNow instance.</td>
</tr>
</tbody>
</table>
### ServiceNow Jakarta Now Platform Capabilities

#### Variable Description

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
</table>
| api_version   | Defines the version of WAPI to use for the integration endpoints. The default value is **2.0**.  
  **Note:** This field is mandatory. If field is empty, the orchestration activity will fail. |
| view          | Name of the Infoblox network view. The default value is **default**.  
  **Note:** If the field is empty, the operation is treated as happening with no view and returns the values with data from all views. |

#### Output variables

**List DNS C-records output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>error</td>
<td>Displays the message for any REST error encountered.</td>
</tr>
<tr>
<td>reference</td>
<td>Reference value for a DNS CNAME record, such as: <code>record:cname/</code></td>
</tr>
</tbody>
</table>
  `ZG5zLmJpbmRfY25hbWUkL19kZWZhdWx0LmNvbS50ZXN0LmNuYW1l:cname.test.com/` |
| cannonicalName| CNAME record.                                                                |
| name          | Name of the network option returned, such as `domain-name-server`.         |
| view          | The assigned view of the DNS data. A given zone can have multiple views, which are accessed depending on the IP address of the source of the query. The `default` view of DNS data for this activity is the network view. |

#### Conditions

**List DNS C-records conditions**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully listed the DNS C records.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to list the DNS C records.</td>
</tr>
</tbody>
</table>

---

**Register DNS A-record activity**
The Register DNS A-record activity creates a DNS A record on a specified Infoblox server.

The DNS activities use the [REST web service activity](#) template to manage DNS records using an Infoblox DDI Grid Server. These activities are configured to use a MID Server with REST capabilities.
Input variables

Register DNS A-record input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InfobloxServer</td>
<td>Name of the Infoblox DDI Grid Server.</td>
</tr>
<tr>
<td>network</td>
<td>Address of the network containing the IP address to register in the record.</td>
</tr>
<tr>
<td>hostName</td>
<td>Name of the actual server machine associate with the IP address in this record.</td>
</tr>
<tr>
<td>zone</td>
<td>The DNS zone associated with the record being created.</td>
</tr>
<tr>
<td>ipAddress</td>
<td>Specific IP address registered in this record.</td>
</tr>
<tr>
<td>restCredentials</td>
<td>The sys_id of the REST credentials from the ServiceNow instance.</td>
</tr>
<tr>
<td>api_version</td>
<td>Defines the version of WAPI to use for the integration endpoints. The default value is 2.0.</td>
</tr>
</tbody>
</table>

**Note:** This field is mandatory. If the field is empty, the orchestration activity will fail.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>view</td>
<td>Name of the Infoblox network view. The default value is default.</td>
</tr>
</tbody>
</table>

**Note:** If the field is empty, the operation is treated as happening in the default view.

Output variables

Register DNS A-record output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>error</td>
<td>Displays the message for any REST error encountered.</td>
</tr>
<tr>
<td>DNSAResult</td>
<td>Name of the record registered, expressed in the format: record:host/&lt;encrypted code&gt;:&lt;network name&gt;/default.</td>
</tr>
</tbody>
</table>
Conditions

Register DNS A-record conditions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully created the DNS A record.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to create the DNS A record.</td>
</tr>
</tbody>
</table>

Register DNS C-Record activity

The Register DNS C-Record activity creates a DNS canonical (CNAME) record on a specified Infoblox server.

The DNS activities use the REST web service activity template to manage DNS records using an Infoblox DDI Grid Server. These activities are configured to use a MID Server with REST capabilities.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Infoblox DDI > DNS.

Input variables

Register DNS C-Record input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InfobloxServer</td>
<td>Name of the Infoblox DDI Grid Server.</td>
</tr>
<tr>
<td>cname</td>
<td>The DNS canonical record to create, as expressed by the c_name value.</td>
</tr>
<tr>
<td>recordName</td>
<td>Name of the record to create.</td>
</tr>
<tr>
<td>zone</td>
<td>The DNS zone containing the canonical record to create.</td>
</tr>
<tr>
<td>restCredentials</td>
<td>The sys_id of the REST credentials from the ServiceNow instance.</td>
</tr>
<tr>
<td>api_version</td>
<td>Defines the version of WAPI to use for the integration endpoints. The default value is 2.0.</td>
</tr>
<tr>
<td><strong>Note:</strong> This field is mandatory. If the field is empty, the orchestration activity will fail.</td>
<td></td>
</tr>
<tr>
<td>view</td>
<td>Name of the Infoblox network view. The default value is default.</td>
</tr>
<tr>
<td><strong>Note:</strong> If the field is empty, the operation is treated as happening in the default view.</td>
<td></td>
</tr>
</tbody>
</table>
Output variables

Register DNS C-Record output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>error</td>
<td>Displays the message for any REST error encountered.</td>
</tr>
<tr>
<td>DNSCRecord</td>
<td>Name of the CNAME record registered, expressed in the format: record:cname/&lt;encrypted code&gt;:&lt;network name&gt;/default.</td>
</tr>
</tbody>
</table>

Conditions

Register DNS C-Record conditions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully created the canonical DNS record.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to create the canonical DNS record.</td>
</tr>
</tbody>
</table>

List DNS Record activity

The List DNS Record activity generates a list of all the DNS entries on a specific InfoBlox server.

The DNS activities use the REST web service activity template to manage DNS records using an Infoblox DDI Grid Server. These activities are configured to use a MID Server with REST capabilities.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Infoblox DDI > DNS.

Input variables

List DNS Record input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InfobloxServer</td>
<td>Name of the Infoblox DDI Grid Server.</td>
</tr>
<tr>
<td>restCredentials</td>
<td>The sys_id of the REST credentials from the ServiceNow instance.</td>
</tr>
<tr>
<td>api_version</td>
<td>Defines the version of WAPI to use for the integration endpoints. The default value is 2.0.</td>
</tr>
</tbody>
</table>

Note: This field is mandatory. If field is empty, the orchestration activity will fail.
### Output variables

**List DNS Record output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reference</td>
<td>Reference value for a DNS record, such as: record:cname/</td>
</tr>
<tr>
<td></td>
<td>ZG5zLmJpbmRfY25hbWUkL19kZWZhdWx0LmNVbS50ZXN0Lm5v</td>
</tr>
<tr>
<td>configure_for_dhcp</td>
<td>Returns the status of a DHCP fixed address object.</td>
</tr>
<tr>
<td>host</td>
<td>Host machine with which the DNS record is associated.</td>
</tr>
<tr>
<td>ipv4addr</td>
<td>The reserved IPv4 address associated with a DNS record.</td>
</tr>
<tr>
<td>name</td>
<td>Name of the network option returned. For example, the name of the DNS record object from the <code>reference</code> example is <code>cname.test.com</code>.</td>
</tr>
<tr>
<td>view</td>
<td>The assigned view of the DNS data. A given zone can have multiple views, which are accessed depending on the IP address of the source of the query. The <code>default</code> view of DNS data for this activity is the network view.</td>
</tr>
<tr>
<td>error</td>
<td>Displays the message for any REST error encountered.</td>
</tr>
</tbody>
</table>

### Conditions

**List DNS Record conditions**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully listed all the available DNS record.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to list the available DNS record.</td>
</tr>
</tbody>
</table>

**DNS Delete activity**

The DNS Delete activity deletes DNS records of any type from in Infoblox server, such as C and A records.
The DNS activities use the *REST web service activity* template to manage DNS records using an Infoblox DDI Grid Server. These activities are configured to use a MID Server with REST capabilities.

To access this activity in the workflow editor, select the **Custom** tab, and then navigate to **Custom Activities > Infoblox DDI > DNS**.

**Note:** It is faster to create a new record than recover one that has been deleted.

### Input variables

**DNS Delete input variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InfobloxServer</td>
<td>Name of the Infoblox DDI Grid Server.</td>
</tr>
<tr>
<td>RecordToDelete</td>
<td>Name of the DNS record to delete. The record is expressed in this format:</td>
</tr>
<tr>
<td></td>
<td><code>record:cname/ ZG5zLmJpbmRfY25hbWUkLi9kZWZhdWx0LmNvbS50ZXN0LmNuYW1l:cname.test.com/ default</code></td>
</tr>
<tr>
<td>restCredentials</td>
<td>The sys_id of the REST credentials from the ServiceNow instance.</td>
</tr>
<tr>
<td>api_version</td>
<td>Defines the version of WAPI to use for the integration endpoints. The default value is <strong>2.0</strong>.</td>
</tr>
</tbody>
</table>

**Note:** This field is mandatory. If the field is empty, the orchestration activity will fail.

### Output variables

**DNS Delete output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeletedRecord</td>
<td>Name of the deleted DNS record.</td>
</tr>
<tr>
<td>error</td>
<td>Displays the message for any REST error encountered.</td>
</tr>
</tbody>
</table>

### Conditions

**DNS Delete conditions**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully deleted the specified DNS record.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to delete the specified DNS record.</td>
</tr>
</tbody>
</table>
Infoblox IPAM activities

The Infoblox IPAM activities manage IP addresses in your network using an Infoblox DDI Grid Server. Use these activities to register, reserve, list, or delete IP addresses.

IPAM Register IP Address activity

The IPAM Register IP Address activity registers an IP address in a network using Infoblox IPAM.

The output of this activity produces an InfoBlox IP address record that can be used for other IPAM functions in the format fixedaddress/<encrypted key>:<reserved ip address>/<view>.

The IPAM activities use the REST web service activity template to manage IP addresses using an Infoblox DDI Grid Server. These activities are configured to use a MID Server with REST capabilities.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Infoblox DDI > IPAM.

Input variables

**IPAM Register IP Address input variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InfobloxServer</td>
<td>Name of the Infoblox DDI Grid Server.</td>
</tr>
<tr>
<td>macAddress</td>
<td>Mac address of the computer for which this IP address is registered.</td>
</tr>
<tr>
<td>ipAddress</td>
<td>Specific IP address to register.</td>
</tr>
<tr>
<td>network</td>
<td>Address of the network containing the registered IP address.</td>
</tr>
<tr>
<td>restCredentials</td>
<td>The sys_id of the REST credentials from the ServiceNow instance.</td>
</tr>
</tbody>
</table>
| api_version       | Defines the version of WAPI to use for the integration endpoints. The default value is 2.0.  
   **Note:** This field is mandatory. If the field is empty, the orchestration activity will fail. |
| view              | Name of the Infoblox network view. The default value is default.             
   **Note:** If the field is empty, the operation is treated as happening in the default view. |

Output variables

**IPAM Register IP Address output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>error</td>
<td>Displays the message for any REST error encountered.</td>
</tr>
</tbody>
</table>
### Conditions

**IPAM Register IP Address conditions**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully registered the specified IP address.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to register the specified IP address.</td>
</tr>
</tbody>
</table>

**IPAM Reserve IP Address activity**

The IPAM Reserve IP Address activity reserves an IP address in a network using Infoblox IPAM. The output of this activity produces an InfoBlox IP address record that can be used for other IPAM functions in the format `fixedaddress/<encrypted key>:<reserved ip address>/<view>`. The IPAM activities use the [REST web service activity template](#) to manage IP addresses using an Infoblox DDI Grid Server. These activities are configured to use a MID Server with REST capabilities. To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Infoblox DDI > IPAM.

### Input variables

**IPAM Reserve IP Address input variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InfobloxServer</td>
<td>Name of the Infoblox DDI Grid Server.</td>
</tr>
<tr>
<td>macAddress</td>
<td>Mac address of the computer for which this IP address is reserved.</td>
</tr>
<tr>
<td>network</td>
<td>Address of the network containing the reserved IP address. The Infoblox server reserves the next available IP address from this network.</td>
</tr>
<tr>
<td>restCredentials</td>
<td>The sys_id of the REST credentials from the ServiceNow instance.</td>
</tr>
<tr>
<td>api_version</td>
<td>Defines the version of WAPI to use for the integration endpoints. The default value is 2.0.</td>
</tr>
</tbody>
</table>

**Note:** This field is mandatory. If the field is empty, the orchestration activity will fail.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>view</td>
<td>Name of the Infoblox network view. The default value is default.</td>
</tr>
</tbody>
</table>

**Note:** If the field is empty, the operation is treated as happening in the default view.
Output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>error</td>
<td>Displays the message for any REST error encountered.</td>
</tr>
<tr>
<td>IPAddressRecord</td>
<td>IPAM record of the reserved IP address.</td>
</tr>
<tr>
<td>IPAddress</td>
<td>Selected IP address to reserve.</td>
</tr>
</tbody>
</table>

Conditions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully reserved the specified IP address.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to reserve the specified IP address.</td>
</tr>
</tbody>
</table>

**IPAM List IP Reservations activity**

The IPAM List IP Reservations activity returns an array of all IP Address within the named InfoBlox Server.

The IPAM activities use the REST web service activity template to manage IP addresses using an Infoblox DDI Grid Server. These activities are configured to use a MID Server with REST capabilities.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Infoblox DDI > IPAM.

Input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InfobloxServer</td>
<td>Name of the Infoblox DDI Grid Server.</td>
</tr>
<tr>
<td>restCredentials</td>
<td>The sys_id of the REST credentials from the ServiceNow instance.</td>
</tr>
<tr>
<td>api_version</td>
<td>Defines the version of WAPI to use for the integration endpoints. The default value is 2.0.</td>
</tr>
</tbody>
</table>

Note: This field is mandatory. If field is empty, the orchestration activity will fail.
### Variable Description

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
</table>
| view     | Name of the Infoblox network view. The default value is *default*.  
  **Note:** If the field is empty, the operation is treated as happening with no view and returns the values with data from all views. |

### Output variables

The output of this activity produces an array of reserved IP addresses in the format *fixedaddress/<encrypted key>:<reserved ip address>/<view>*.

#### IPAM List IP Reservations output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reference</td>
<td>Reference value of a reserved IP address contained in an array of addresses, such as <em>fixedaddress/2G5zLm2peGVkX2FKZlJc3MkMTAuMC4xMDMuMTEuMC4u:0.0.0.11</em> ipv4addr: <em>0.0.0.11</em></td>
</tr>
<tr>
<td>ipv4addr</td>
<td>The reserved IPv4 address.</td>
</tr>
<tr>
<td>network_view</td>
<td>Routing domain associated with the network returned.</td>
</tr>
<tr>
<td>error</td>
<td>Displays the message for any REST error encountered.</td>
</tr>
</tbody>
</table>

### Conditions

#### IPAM List IP Reservations conditions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully retrieved the list of reserved IP addresses from the Infoblox server.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to retrieve the list of reserved IP addresses from the Infoblox server.</td>
</tr>
</tbody>
</table>

**IPAM Delete activity**

The IPAM Delete activity deletes an IP Address within a named InfoBlox server.

The IPAM activities use the [REST web service activity template](https://example.com) to manage IP addresses using an Infoblox DDI Grid Server. These activities are configured to use a MID Server with REST capabilities.

To access this activity in the workflow editor, select the **Custom** tab, and then navigate to **Custom Activities > Infoblox DDI > IPAM**.
Input variables

IPAM Delete input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InfobloxServer</td>
<td>Name of the Infoblox DDI Grid Server.</td>
</tr>
<tr>
<td>itemToDelete</td>
<td>The IP address to delete, in the format fixedaddress/&lt;encrypted key&gt;:&lt;reserved ip address&gt;/view.</td>
</tr>
<tr>
<td>restCredentials</td>
<td>The sys_id of the REST credentials from the ServiceNow instance.</td>
</tr>
<tr>
<td>api_version</td>
<td>Defines the version of WAPI to use for the integration endpoints. The default value is 2.0.</td>
</tr>
</tbody>
</table>

Note: This field is mandatory. If the field is empty, the orchestration activity will fail.

Output variables

IPAM Delete output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeletedRecord</td>
<td>IPAM record of the deleted IP address.</td>
</tr>
<tr>
<td>error</td>
<td>Displays the message for any REST error encountered.</td>
</tr>
</tbody>
</table>

Conditions

IPAM Delete conditions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully deleted the specified IP address.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to delete the specified IP address.</td>
</tr>
</tbody>
</table>

Infoblox network activities

The Infoblox network activities manage networks using an Infoblox DDI Grid Server. Use these activities to create, list, or delete networks on an Infoblox server.

Create Network activity
The Create Network activity creates new networks on a specified Infoblox server.

The network activities use the REST web service activity template to manage network addresses using an Infoblox DDI Grid Server. These activities are configured to use a MID Server with REST capabilities.
To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Infoblox DDI > Network.

Input variables

Create Network input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InfobloxServer</td>
<td>Name of the Infoblox DDI Grid Server.</td>
</tr>
<tr>
<td>network</td>
<td>Address of the network to create.</td>
</tr>
<tr>
<td>restCredentials</td>
<td>The sys_id of the REST credentials from the ServiceNow instance.</td>
</tr>
</tbody>
</table>
| api_version     | Defines the version of WAPI to use for the integration endpoints. The default value is 2.0.  
  *Note:* This field is mandatory. If the field is empty, the orchestration activity will fail. |
| view            | Name of the Infoblox network view. The default value is default.             
  *Note:* If the field is empty, the operation is treated as happening in the default view. |

Output variables

Create Network output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetworkCreated</td>
<td>Address of the network created.</td>
</tr>
<tr>
<td>error</td>
<td>Displays the message for any REST error encountered.</td>
</tr>
</tbody>
</table>

Conditions

Create Network conditions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully created the network.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to create the network.</td>
</tr>
</tbody>
</table>

Get Network Details activity

The Get Network Details activity retrieves the information about a specific network on an Infoblox server.
The network activities use the REST web service activity template to manage network addresses using an Infoblox DDI Grid Server. These activities are configured to use a MID Server with REST capabilities.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Infoblox DDI > Network.

**Input variables**

**Get Network Details input variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InfobloxServer</td>
<td>Name of the Infoblox DDI Grid Server.</td>
</tr>
<tr>
<td>network</td>
<td>Address of the network whose details you want to see.</td>
</tr>
<tr>
<td>restCredentials</td>
<td>The sys_id of the REST credentials from the ServiceNow instance.</td>
</tr>
<tr>
<td>api_version</td>
<td>Defines the version of WAPI to use for the integration endpoints. The default value is 2.0.</td>
</tr>
<tr>
<td>view</td>
<td>Name of the Infoblox network view. The default value is default.</td>
</tr>
</tbody>
</table>

**Note:** This field is mandatory. If the field is empty, the orchestration activity will fail.

**Note:** If the field is empty, the operation is treated as happening in the default view.

**Output variables**

The output variables from this activity are objects on the Infoblox server used to identify network details. For more information, refer to the Infoblox documentation.

**Get Network Details output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>error</td>
<td>Displays the message for any REST error encountered.</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>NetworkOptions</td>
<td>The <code>NetworkOptions</code> array contains these attributes:</td>
</tr>
<tr>
<td></td>
<td>- <code>reference</code>: Reference value for the network requested. This value is in the form of <code>network/\ZG5zLm5ldHdvcmxkMTAuMS4wLjAvMTYvMA:10.1.0.0%2F1</code>.</td>
</tr>
<tr>
<td></td>
<td>- <code>options</code>: The <code>options</code> array contains these attributes:</td>
</tr>
<tr>
<td></td>
<td>- <code>name</code>: Name of the network option returned, such as <code>domain-name-server</code>.</td>
</tr>
<tr>
<td></td>
<td>- <code>num</code>: Index number of the option. For example, the index for <code>domain-name-server</code> is 6.</td>
</tr>
<tr>
<td></td>
<td>- <code>use_option</code>: Indicates whether a DHCP option is used at that level in the network hierarchy. Set this value to <code>True</code> to override the Grid Level DHCP option with this option at the network level.</td>
</tr>
<tr>
<td></td>
<td>- <code>value</code>: Value to use for this option. For example, the value for the <code>domain-name-server</code> option is the IP address of the server machine.</td>
</tr>
<tr>
<td></td>
<td>- <code>vendor_class</code>: The class of the network object. The options are <code>DHCP</code>, <code>DNS</code>, or <code>IPAM</code>.</td>
</tr>
</tbody>
</table>

**Conditions**

**Get Network Details conditions**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully retrieved network details from the Infoblox server.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to retrieve network details from the Infoblox server.</td>
</tr>
</tbody>
</table>

**Delete Network activity**

The Delete Network activity deletes a network from an Infoblox server.

The network activities use the *REST web service activity template* to manage network addresses using an Infoblox DDI Grid Server. These activities are configured to use a MID Server with REST capabilities.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Infoblox DDI > Network.
**Input variables**

### Delete Network input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InfobloxServer</td>
<td>Name of the Infoblox DDI Grid Server.</td>
</tr>
<tr>
<td>networkToDelete</td>
<td>Reference number of the network to delete from the Infoblox server. You can obtain this value either by using the List Registered Networks activity or when creating a network with the Create Network activity. An example of the network reference value is: <code>network/ZG5zLm5idHdvcmkMTUuMC40NS4wLz10LzA:15.0.45.0/24/default</code>.</td>
</tr>
<tr>
<td>restCredentials</td>
<td>The sys_id of the REST credentials from the ServiceNow instance.</td>
</tr>
<tr>
<td>api_version</td>
<td>Defines the version of WAPI to use for the integration endpoints. The default value is 2.0.</td>
</tr>
</tbody>
</table>

**Note:** This field is mandatory. If the field is empty, the orchestration activity will fail.

### Output variables

#### Delete Network output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeletedNetwork</td>
<td>Reference number of the deleted network from the Infoblox server.</td>
</tr>
<tr>
<td>error</td>
<td>Displays the message for any REST error encountered.</td>
</tr>
</tbody>
</table>

### Conditions

#### Delete Network conditions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully deleted the network.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to delete the network.</td>
</tr>
</tbody>
</table>

**List Registered Networks activity**

The List Registered Networks activity retrieves all the networks associated with an Infoblox server.

The network activities use the `REST web service activity template` to manage network addresses using an Infoblox DDI Grid Server. These activities are configured to use a MID Server with REST capabilities.
To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Infoblox DDI > Network.

Input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InfobloxServer</td>
<td>Name of the Infoblox DDI Grid Server.</td>
</tr>
<tr>
<td>restCredentials</td>
<td>The sys_id of the REST credentials from the ServiceNow instance.</td>
</tr>
<tr>
<td>api_version</td>
<td>Defines the version of WAPI to use for the integration endpoints. The default value is 2.0. Note: This field is mandatory. If field is empty, the orchestration activity will fail.</td>
</tr>
<tr>
<td>view</td>
<td>Name of the Infoblox network view. The default value is default. Note: If the field is empty, the operation is treated as happening with no view and returns the values with data from all views.</td>
</tr>
</tbody>
</table>

Output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reference</td>
<td>Reference value of a registered network.</td>
</tr>
<tr>
<td>network</td>
<td>Network address.</td>
</tr>
<tr>
<td>network_view</td>
<td>Routing domain associated with the network returned.</td>
</tr>
<tr>
<td>error</td>
<td>Displays the message for any REST error encountered.</td>
</tr>
</tbody>
</table>

Conditions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully retrieved the list of registered networks available on the Infoblox server.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to retrieve the list of registered networks available on the Infoblox server.</td>
</tr>
</tbody>
</table>
PowerShell activity pack

PowerShell is built on the Windows .NET Framework and is designed to control and automate the administration of Windows machines and applications.

Orchestration provides custom PowerShell activities that were created with the PowerShell activity designer template. These activities perform the same functions as PowerShell activities by the same name from previous releases and replace those activities for all new workflows. These custom activities give workflow administrators the ability to store input and output variables in the databus.

Note: Existing workflows from earlier versions that were created with legacy PowerShell activities continue to function normally after an upgrade to Geneva. However, all new workflows must use these custom PowerShell activities.

To use the PowerShell custom activities, you must request activation of the Orchestration - PowerShell plugin. These activities are available in the workflow editor on the Custom tab. Expand the Custom Activities tree and select the PowerShell category for the activity you want to use.

ServiceNow supports PowerShell 2.0 and above. PowerShell 3.0 does not support Windows 2003 Server.

PowerShell activity designer

PowerShell activities are configured to return data to a workflow from a host using Microsoft PowerShell.

You must purchase Orchestration to use this template. For specific information about using the tools in the activity designer, refer to these resources:

- Orchestration activity designer
- Create input variables
- Create a parsing rule

ServiceNow supports PowerShell 2.0 and above. PowerShell 3.0 does not support Windows 2003 Server.

PowerShell protocols and troubleshooting

PowerShell uses the Windows Management Instrumentation (WMI) and Windows Remote Management (WinRM) protocols to enable Orchestration activities to run commands on remote Windows hosts.

Windows Management Instrumentation (WMI)

WMI provides a uniform interface for any local or remote applications or scripts that obtain management data from a computer system, a network, or an enterprise. WMI contains these components:

- Managed objects and WMI providers: A WMI provider is a COM object that monitors one or more managed objects for WMI. A managed object is a logical or physical enterprise component, such as a hard disk drive, network adapter, database system, operating system, process, or service.
- WMI infrastructure: The WMI infrastructure is a Microsoft Windows operating system component know as the WMI service (wimmgmt). The WMI infrastructure is composed of the WMI Core and the WMI repository. The WMI repository is organized by WMI namespaces. The WMI service creates namespaces, such as root\default, root\cimv2, and root\subscription, at system startup and preinstalls a default set of class definitions, including the Win32 Classes, the
WMI System Classes, and others. The remaining namespaces found on your system are created by providers for other parts of the operating system or products.

- **WMI consumers:** A WMI consumer is a management application or script that interacts with the WMI infrastructure. A management application can query, enumerate data, run provider methods, or subscribe to events by calling either the COM API or the Scripting API for WMI.

**WMI installation and configuration**

For the MID Server to successfully make a remote connection to the target host, TCP port 135 must be open. The Windows firewall automatically creates an inbound rule for WMI connectivity called Windows Management Instrumentation (DCOM-In).

**Windows Remote Management (WinRM)**

WinRM is the Microsoft implementation of WS-Management Protocol, a standard Simple Object Access Protocol (SOAP) protocol that allows hardware and operating systems from different vendors to interoperate.

WinRM contains these components:

- **WinRM Scripting API:** This scripting API enables Orchestration to obtain data from remote computers, using scripts that perform WS-Management protocol operations.
- **WMI Service:** The WMI service continues to run side-by-side with WinRM and provides requested data or control through the WMI plug-in. You can continue to obtain data from standard WMI classes, such as Win32_Process.

**WinRM configuration**

WinRM is automatically installed on Windows 2008 R2 and above operating systems, but must be configured before use.

1. In a command prompt, enter `winrm quickconfig`. This command is not case sensitive.
2. When the console displays *Make these changes (y/n)?*, enter `y`.

The `winrm quickconfig` command performs the following operations:

- Starts the WinRM service, and sets the service startup type to `auto start`.
- Configures a listener for the ports that send and receive WS-Management protocol, using either HTTP or HTTPS on any IP address.
- Creates a firewall exception for the current user profile.

**MID Server PowerShell files**

PowerShell functions are stored in script files (*.ps1) that use a PowerShell Script module (*.psm1) file name extension.

The PowerShell functions are used by the PowerShell MID Server script files included in these activity packs:

- Active Directory
- Exchange
- SCCM
- PowerShell
PSScript.ps1

This script performs a number of tasks, such as credential testing, password encryption, and the execution of scripts configured in the Orchestration Activity Designer or in MID Script Files. However, this document focuses on how PSScript.ps1 uses the credential.psm1 module for testing access to remote hosts.

The PowerShell variables are generally used directly in the PowerShell execution command or as arguments in the MID Server script file you specify. There are special variables that are passed to PSScript.ps1, such as credType.
Using `credType` in execution parameters

<table>
<thead>
<tr>
<th>Input</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ABC <code>scmServer</code></td>
<td></td>
</tr>
<tr>
<td>ABC <code>collection</code></td>
<td></td>
</tr>
<tr>
<td>ABC <code>device</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Target host</th>
<th><code>$(activityInput.scmServer)</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Script type</td>
<td>MID Server script file</td>
</tr>
<tr>
<td>MID Server script file</td>
<td><code>AddToDeviceCollection.ps1</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PowerShell variables</th>
<th>Name</th>
<th>Value</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>collection</code></td>
<td><code>$(activityInput.collection)</code></td>
<td>Plain</td>
</tr>
<tr>
<td></td>
<td><code>device</code></td>
<td><code>$(activityInput.device)</code></td>
<td>Plain</td>
</tr>
<tr>
<td></td>
<td><code>credType</code></td>
<td><code>SCCM</code></td>
<td>Plain</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Credential tag</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Required MID Server capabilities</td>
<td></td>
</tr>
</tbody>
</table>

| Required PowerShell Server capabilities |  |

© 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.
PowerShell credTypes

The PowerShell credential types:

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WMI</td>
<td>testCredentialWMI</td>
</tr>
<tr>
<td>Exchange</td>
<td>testCredentilExchange</td>
</tr>
<tr>
<td>AD</td>
<td>testCredentialAD</td>
</tr>
<tr>
<td>SCCM</td>
<td>testCredentialSCCM</td>
</tr>
</tbody>
</table>

If no credential type is passed to the PSScrip.ps1 script, the MID Server defaults to the WMI test function to test access to the target host. If there is a credential type used, the MID Server runs the corresponding test function for that credential type.

Exit codes

These exit codes are returned from the PSScript.ps1 script and logged in the MID Server log file.

<table>
<thead>
<tr>
<th>Type</th>
<th>Test function</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>PowerShell command/script ran successfully.</td>
</tr>
<tr>
<td>1</td>
<td>Test finished successfully, but the command/script failed to execute.</td>
</tr>
<tr>
<td>2</td>
<td>Incorrect syntax passed to script.</td>
</tr>
<tr>
<td>3</td>
<td>All credentials including MID Server service account failed to execute the command/script.</td>
</tr>
<tr>
<td>4</td>
<td>Passed test and executed the activity, but an error was returned. Example user cannot be found.</td>
</tr>
</tbody>
</table>

Credentials.psm1

The MID Server uses this module file to test access to a target host. The MID Server loops through all Windows credentials stored in its credentials table using the following access type functions, unless the PowerShell activity has a credential type (credType) defined. All ServiceNow® authored PowerShell activities are hardcoded to use a specific credential type. As a result, the MID Server only tests credential access against the designated function.

PowerShell test functions

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>testCredentialWMI</td>
<td>Tests the given user and password on the target host using the Get-WMI object.</td>
</tr>
<tr>
<td>testCredentialAD</td>
<td>Tests the given user and password on the target host using the built-in DirectoryEntry object.</td>
</tr>
<tr>
<td>Function</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>testCredentialExchange</td>
<td>Tests the given user and password to create a session on an Exchange host. This test uses the built-in PowerShell remoting feature on a remote host. WinRM is configured on Exchange servers by default.</td>
</tr>
<tr>
<td>testCredentialSCCM</td>
<td>Tests the given user and password to create a session on an SCCM server. This test uses the built-in PowerShell remoting feature on a remote host. This requires WinRM to be configured.</td>
</tr>
<tr>
<td>testNoCredentialAccessWMI</td>
<td>Tests the given user and password on the target host, using the <code>Get-WMI</code> object. This test is used when no <code>credType</code> is used.</td>
</tr>
</tbody>
</table>

**Note:** If the test passes using one of these functions, that credential is used to run the PowerShell script/command. If the tests fail to access the target host using these functions, the MID Server runs the PowerShell script/command under the account of the MID Server service.

This diagram illustrates the dependency of the credential selection behavior on the host being targeted by the PowerShell activity. If the target host is the IP address or host name of the MID Server, the MID Server bypasses all credentials in the Credentials table and uses the account of the MID Server service. If the target host is not the MID Server, then all Windows credentials are used first. If all credentials in the Credentials table are unsuccessful in running the PowerShell activity, then the MID Server uses the MID Server service account.
PowerShell credential selection criteria
ActiveDirectory.psm1

This module file stores the functions used by the PowerShell scripts shipped with the Active Directory activity pack.

Exchange.psm1

This module file stores the functions used by the PowerShell scripts shipped with the Exchange activity pack.

SCCM.psm1

This module file stores the functions used by the PowerShell scripts shipped with the SCCM activity pack.

Set up credential tags for a PowerShell activity

Credential tagging gives an administrator more control over the credentials used in a PowerShell activity.

Role required: admin, activity_creator or workflow_admin

Tagging is useful when the activity requires specific credentials to perform a task. By populating the Credential tag field you are telling the activity to use a credential that has a specific tag set for it. Additionally, credential tagging allows you to use a different underlying credential in development, testing, and production systems without having to change the activity for a given target system. For example, you can use the SCCMCred tag and have it point to both a development and test instance.

1. Navigate to Orchestration > Credentials.
2. Select the credential you want to tag.
3. Enter a unique name in the Tag field that is descriptive of the credentials purpose.
Credential tag definition

4. Click **Update**.
5. Open the Workflow Editor and select the PowerShell activity you want to tag.
6. In the activity's Execution Command, add the name of the tag you created to the **Credential tag** field.
PowerShell troubleshooting

Authentication and access denied errors can prevent PowerShell activities from running a command on a target host.

Use these procedures for troubleshooting authentication failures with Orchestration PowerShell activities and when the Remote Procedure Call (RPC) server is unavailable or when access is denied. The authentication failure error displays when all credentials, including those of the local MID Server service account, do not have the correct permissions to run the PowerShell script/command. The same error displays when the target host is unreachable.

Authentication error message

Authentication failure in an Active Directory activity

This example uses the Create AD Object activity to illustrate troubleshooting authentication failure in PowerShell.

Role required: Permissions to access and create accounts on Active Directory

Validate that the account you are using has the proper permissions to run the activity.

1. Log on to the target machine using the account under which you want to run the activity.
   Active Directory tools must be installed on this machine.
2. Launch the Active Directory Users and Computers application.
3. Navigate to the OU under which you want to create the Active Directory object.
4. Attempt to create the object.

If this procedure is successful under the specified user, the following might be the cause of the authentication failure:

- User name is invalid.
- Password entered incorrectly.
- Domain controller is unreachable.

Note: The majority of the return codes listed in the MID Server log for this error are 1s and 3s. This is because the Active Directory activities use the ADSI provider and not WMI or WinRM. An error code of 1 means the account was able to connect with the test account, but running the script failed.
An error code of 3 means that the MID Server attempted to run the PowerShell activity under the MID Server service account but failed.

Authentication failure in an Exchange activity
This example uses the Create Mailbox activity to illustrate troubleshooting authentication failure in PowerShell.

Role required: Permissions to access and create mailboxes on the Exchange server

1. Validate that the account you are using has the proper permissions to run the PowerShell activity.
2. Log on to a machine that has the Exchange Management Shell (EMS) installed.
3. Create a user using the New-mailbox Exchange commandlet.
Creating a new user in Exchange

If this procedure is successful under the specified credential, the following is the likely cause of the failure:

- User name is invalid.
- Password entered incorrectly.
- Exchange server is unreachable.

4. If the Exchange server is unreachable, examine the MID Server logs.
Because the Exchange activities use WinRM to access the Exchange server, the logs can provide more troubleshooting information.

Note: Ensure that the error is NOT WinRM cannot process the request.

Remote Procedure Call (RPC) server unavailable or access denied
Typically, this error is logged when running a PowerShell script/command that uses WinRM or WMI.

Possible causes of error

The target host might have one of these issues:

- WinRM isn’t configured.
- Firewall is blocking access to the host over TCP port 135 (WMI) or HTTP/HTTPs and TCP port 5985 (WinRM).
- Kerberos issue, caused by hopping to multiple hosts using WMI.
Example WinRM error

The Create Mailbox activity from the Exchange activity pack has generated an error in the ECC queue involving authentication using the MID Server service credential. This occurred because the MID Server credential is the last to be used if the targeted host is not the MID Server.

Authentication failure error message

The MID Server log shows that the MID Server tried to run the activity under specific credentials, but wasn’t successful and received an exit code of 1.
Join Domain activity

The Join Domain activity joins a Windows computer to a domain.

If the computer is already a member of a domain, this activity completes without modifying the computer. Joining a domain requires a username and password. This user must have domain administration privileges or privileges to join a computer to the domain.

Note: This activity replaces a PowerShell activity by the same name available in releases prior to Geneva. If you have a workflow created in a previous version that uses the deprecated activity, your workflow will continue to work normally after upgrading to Geneva. However, all new workflows must use the custom version of this activity. This activity was built with the PowerShell activity designer, which gives workflow administrators the ability to store input and output variables in the databus.

Input variables

Join Domain input variables

<table>
<thead>
<tr>
<th>Variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>Hostname or IP address of the Windows server that is joining the domain.</td>
</tr>
<tr>
<td>Domain</td>
<td>Name of the domain to join.</td>
</tr>
<tr>
<td>Domain_user</td>
<td>The name of a user who has domain administration privileges or privileges to join a computer to the domain.</td>
</tr>
<tr>
<td>Domain_user_password</td>
<td>The password for the user who has domain administration privileges or privileges to join a computer to the domain.</td>
</tr>
</tbody>
</table>

Output variables

Join Domain output variables

<table>
<thead>
<tr>
<th>Variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Either success or failure.</td>
</tr>
<tr>
<td>errorMessage</td>
<td>The executionResult.errorMessages from the Activity designer parsing sources. If this variable is not null, the operation has failed.</td>
</tr>
</tbody>
</table>

Conditions

Join Domain conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The activity succeeded in joining the computer to the domain.</td>
</tr>
<tr>
<td>Condition</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Failure</td>
<td>The activity failed to join the computer to the domain.</td>
</tr>
</tbody>
</table>

### Install Windows App activity

The Install Windows App activity installs an application from an MSI package on a Windows target machine.

**Note:** This activity replaces a Powershell activity by the same name available in releases prior to Geneva. If you have a workflow created in a previous version that uses the deprecated activity, your workflow will continue to work normally after upgrading to Geneva. However, all new workflows must use the custom version of this activity. This activity was built with the [PowerShell activity designer](https://www.servicenow.com), which gives workflow administrators the ability to store input and output variables in the [databus](https://www.servicenow.com).

### Input variables

**Install Windows App input variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>Hostname or IP address of the target Windows machine on which the service is installed. Use the Resolve DNS <a href="https://www.servicenow.com">MID Server capability</a> to resolve hostnames into IP addresses.</td>
</tr>
<tr>
<td>installerpath</td>
<td>Path to the installer. The installer can be on any machine that is visible to both the MID Server and the target machine (local drive, UNC path, mapped drive, etc.).</td>
</tr>
<tr>
<td>installer</td>
<td>Name of the installer file, such as winzip150.msi. The installer must be an MSI package.</td>
</tr>
<tr>
<td>arguments</td>
<td>The parameter that contains the command line arguments to the MSI package. These are name=value pairs, separated by a space. For example, the argument might appear as: INSTALLDIR=c:\myinstallfolder ADDDESKTOPICON=0. These arguments are dependent on the what the actual MSI being installed defines. If there are no arguments, leave the field empty.</td>
</tr>
</tbody>
</table>

### Output variables

**Install Windows App output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Either <strong>success</strong> or <strong>failure</strong>.</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>errorMessage</td>
<td>The <code>executionResult.errorMessages</code> from the <code>Activity designer parsing sources</code>.</td>
</tr>
</tbody>
</table>

**Conditions**

The activity state tells the workflow engine what to do with the activity.

**Install Windows App conditions**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The Windows application was successfully installed on the target machine.</td>
</tr>
<tr>
<td>Failure</td>
<td>The Windows application failed to install on the target machine.</td>
</tr>
</tbody>
</table>

**Enable WMI Windows Installer provider**

To install software on Windows machines using the Install Windows App activity, enable WMI Windows Installer provider on all target machines.

- It is recommended that the MID Server, the target machine, and the installer source machine be on the same Active Directory domain. However, if these computers are on separate domains, those domains must have a trust relationship established between them.
- If the installer path is a UNC file sharing machine, the Active Directory account of the target computer must be trusted for delegation. For instructions on this configuration, see the posting on the community for installing and uninstalling Windows applications.

**Note:** See [WMI Providers](#) for a list of Windows operating systems that provide this tool by default.

1. Open the Control Panel.
2. Go to Add or Remove Programs.
3. Select Add/Remove Windows Components.
   This action opens a secondary window displaying additional selections.
5. Select WMI Windows Installer Provider check box.
6. Click OK to return to the Windows Components Wizard window.
7. Click Next.
   You might be asked for the Windows installation CD to complete this process.

**Change Service State activity**

The Change Service State activity starts or stops a Windows service on a remote system.

This activity replaces a Powershell activity by the same name available in releases prior to Istanbul. If you have a workflow created in a previous version that uses the deprecated activity, your workflow will continue to work normally after upgrading to Istanbul. However, all new workflows must use the custom version of this activity. This activity was built with the [Powershell activity template](#), which gives workflow administrators the ability to store input and output variables in the databus.
Input Variables

Change Service State input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>Hostname or IP address of the target Windows machine on which the service is installed. Use the Resolve DNS activity to resolve hostnames into IP addresses.</td>
</tr>
<tr>
<td>service</td>
<td>Name of the Windows service to start or stop. The service parameter is the service name, not the display name of the service affected.</td>
</tr>
<tr>
<td>state</td>
<td>There are two actions to select for a service state change: StartService or StopService.</td>
</tr>
</tbody>
</table>

Output variables

Change Service State output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>errorMessage</td>
<td>The executionResult.errorMessages from the Activity designer parsing sources. If there is no error, this value is null.</td>
</tr>
</tbody>
</table>

Conditions

Change Service State conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The target service was successfully started or stopped.</td>
</tr>
<tr>
<td>Failure</td>
<td>The update to the target service was unsuccessful, or the service was not found on the target system.</td>
</tr>
</tbody>
</table>

Restart Windows Server activity

The Restart Windows Server activity stops and then restarts a Windows server using Powershell.

Note: This activity replaces a Powershell activity by the same name available in releases prior to Geneva. If you have a workflow created in a previous version that uses the deprecated activity, your workflow will continue to work normally after upgrading to Geneva. However, all new workflows must use the custom version of this activity. This activity was built with the Powershell activity template, which gives workflow administrators the ability to store input and output variables in the databus.
Input variables

Restart Windows Server input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>Hostname or IP address of the Windows server to restart.</td>
</tr>
</tbody>
</table>

Output variables

Restart Windows Server output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Either success or failure.</td>
</tr>
<tr>
<td>errorMessage</td>
<td>The executionResult.errorMessages from the Activity designer parsing sources. If this variable is not null, the operation has failed.</td>
</tr>
</tbody>
</table>

Conditions

Restart Windows Server conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The activity succeeded in restarting the Windows server.</td>
</tr>
<tr>
<td>Failure</td>
<td>The activity failed to restart the Windows server.</td>
</tr>
</tbody>
</table>

Uninstall Windows App activity

The Uninstall Windows App activity uninstalls an application from a Windows target machine. The only applications that can be uninstalled using this activity are those that were installed by a Windows Installer.

Note: This activity replaces a Powershell activity by the same name available in releases prior to Geneva. If you have a workflow created in a previous version that uses the deprecated activity, your workflow will continue to work normally after upgrading to Geneva. However, all new workflows must use the custom version of this activity. This activity was built with the Powershell activity template, which gives workflow administrators the ability to store input and output variables in the databus.
### Input variables

**Uninstall Windows App input variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>Hostname or IP address of the Windows target machine on which to uninstall an application.</td>
</tr>
<tr>
<td>product</td>
<td>The name of the application to uninstall exactly as it appears in the Windows Add/Remove Programs list.</td>
</tr>
</tbody>
</table>

### Output variables

**Uninstall Windows App output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Either success or failure.</td>
</tr>
<tr>
<td>errorMessage</td>
<td>The <code>executionResult.errorMessages</code> from the Activity designer parsing sources. If this variable is not null, the operation has failed.</td>
</tr>
</tbody>
</table>

### Conditions

**Uninstall Windows App conditions**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The activity succeeded in uninstalling the application from the Windows server.</td>
</tr>
<tr>
<td>Failure</td>
<td>The activity failed to uninstall the application from the Windows server.</td>
</tr>
</tbody>
</table>

### Probe activity pack

Orchestration provides an activity pack customized using the ServiceNow activity designer that runs probes on target hosts to return specific information.

These custom activities were built with the [Create a probe activity](#), which gives workflow administrators the ability to store input and output variables in the databus.

To use the custom probe activities, you must [request activation](#) of the Orchestration - Probe plugin.

### Resolve DNS Name activity

The Resolve DNS Name activity takes an IP address or a fully qualified domain name (FQDN), which it resolves into one or more IP addresses.

The domain name is sent through the MID Server to the domain name system (DNS) to resolve the name. If a single IP address is returned, it is stored in two variables: `resolved_ip` and `resolved_ips`.
If multiple IP addresses are returned, the first IP address is stored in the `resolved_ip` variable, and all the addresses are stored in the `resolved_ips` variable. If an IP address is provided instead of an FQDN, this address is output directly to both variables. Your ServiceNow instance must have access to a MID Server configured to use Resolve DNS to run this activity.

This activity replaces an activity by the same name available in releases prior to Istanbul. If you have a workflow created in a previous version that uses the deprecated activity, your workflow will continue to work normally after upgrading to Istanbul. However, all new workflows must use the custom version of this activity. This activity was built with the `Probe activity template`, which gives workflow administrators the ability to store input and output variables in the `databus`.

### Input variables

**Resolve DNS Name input variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FQDN</td>
<td>The fully qualified domain name to resolve or an IP address.</td>
</tr>
</tbody>
</table>

### Output variables

**Resolve DNS Name output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>The first IP address of the resolved DNS name.</td>
</tr>
<tr>
<td>ips</td>
<td>Comma separated list of resolved IP addresses.</td>
</tr>
</tbody>
</table>
| result   | One of the following:  
- `resolved`: Able to resolve the specified DNS name.  
- `unresolved`: Unable to resolve the specified DNS name. |

### Conditions

**Resolve DNS Name conditions**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully resolved the DNS name.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to resolve the DNS name.</td>
</tr>
</tbody>
</table>

### SNMP Query activity

The SNMP Query activity queries an SNMP device.

Your ServiceNow instance must have access to a MID Server configured to use SNMP to run this activity.
This activity replaces an activity by the same name available in releases prior to Istanbul. If you have a workflow created in a previous version that uses the deprecated activity, your workflow will continue to work normally after upgrading to Istanbul. However, all new workflows must use the custom version of this activity. This activity was built with the Probe activity template, which gives workflow administrators the ability to store input and output variables in the databus.

Input variables

**SNMP Query input variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>Hostname or IP address of the SNMP device being queried.</td>
</tr>
<tr>
<td>oids</td>
<td>A list of unique object identifiers used to identify SNMP devices.</td>
</tr>
</tbody>
</table>

Output variables

**SNMP Query output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>Description of the SNMP object.</td>
</tr>
<tr>
<td>timeout</td>
<td>Boolean value indicating whether or not the query timed out.</td>
</tr>
<tr>
<td>error</td>
<td>Indicates any error that occurred. If no error occurred, this value is null.</td>
</tr>
<tr>
<td>oid_data</td>
<td>An array of data objects for all unique object identifiers.</td>
</tr>
</tbody>
</table>

Conditions

**SNMP Query conditions**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully ran the query on the target device.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to run the query on the target device. Failure could be caused by invalid credentials or a device that is not accessible.</td>
</tr>
</tbody>
</table>

SCCM activity pack

The Microsoft System Center Configuration Management (SCCM) activity pack provides Orchestration activities you can use to manage software deployments and collections on an SCCM server.
You can use SCCM Orchestration activities to deploy and revoke software from an SCCM server or manage user and device collections. The system manages software on an SCCM server using Orchestration activities and workflows.

Client software distribution requires:

- SCCM 2012 R2.
- Powershell 3.x.
- Powershell Remoting enabled.
- The Windows PowerShell x86 execution policy must be set to unrestricted mode.
- Latest version of the SCCM cmdlet library installed on the SCCM server.
- Use the credentials to log onto the SCCM Server and connect via Windows PowerShell from the System Center Configuration Manager console at least once to set the path variable for that credential.

**Activate SCCM activities**

The Orchestration - System Center Configuration Manager plugin installs the SCCM activity pack that deploys software from an SCCM host and manages user and device collections.

The SCCM plugin is activated automatically when the Orchestration - Client Software Distribution [com.snc.orchestration.sccm_mgnt] plugin is activated, but can be activated separately.

**Note:** The activities in the SCCM plugin run in the System Center Configuration Manager scope.

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>Specify the date and time you would like this plugin to be enabled</th>
<th>Date and time must be at least 2 business days from the current time.</th>
</tr>
</thead>
</table>

**Note:** Plugins are activated in two batches each business day in the Pacific timezone, 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 | Any information that would be helpful for the ServiceNow personnel activating the plugin such as if you need the plugin activated at a specific time instead of during one of the default activation windows. |

3. Click Submit.

**Configure the MID Server for SCCM activities**

To use a MID Server with Microsoft System Center Configuration Management (SCCM) activities, configure it to communicate with the SCCM server.

Role required: admin

1. In the navigation filter, enter cmdb_ci_dns_name.list.
2. Click **New**.
3. Enter the fully-qualified domain name (FQDN) of the SCCM server in the **Name** field.
4. Right-click in the form header and select **Save**.
5. In the **IP Address** related list, click **New**.
6. In the **IP Address** field, enter the IP address of the SCCM server.
7. In the **Nic** field, select **eth0** or your preferred network interface controller.
8. Leave the **Netmask** field blank.
9. Click **Submit**.

**Add to Device Collection activity**

The Add to Device Collection activity adds the specified device into a Microsoft System Center Configuration Manager (SCCM) device collection.

The Add to Device Collection activity uses the **Powershell activity template** to add a specified device to an SCCM device collection. The activity is configured to use a MID Server with Powershell capabilities and to run a MID Server script called **AddToDeviceCollection.ps1** to edit the collection.

To access this activity in the workflow editor, select the **Custom** tab, and then navigate to **Custom Activities > System Center Configuration Manager (SCCM)**.

---

**Note:** The Add to Device Collection activity does not use pre-processing or post processing scripts.

**Input variables**

Add to Device Collection input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sccmServer</td>
<td>The fully qualified domain name (FQDN) of the SCCM server.</td>
</tr>
<tr>
<td>collection</td>
<td>Name of the device collection.</td>
</tr>
<tr>
<td>device</td>
<td>Name of the device to add to the collection.</td>
</tr>
</tbody>
</table>

**Output variables**

Add to Device Collection output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>output</td>
<td>Variable that contains a value that is passed to other activities in the workflow.</td>
</tr>
<tr>
<td>error</td>
<td>Variable that contains the activity output error message.</td>
</tr>
</tbody>
</table>
Conditions

Add to Device Collection conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully added the device to the SCCM device collection.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to add the device to the SCCM device collection.</td>
</tr>
</tbody>
</table>

Add to User Collection activity

The Add to User Collection activity adds a user to a Microsoft System Center Configuration Manager (SCCM) user collection.

The Add to User Collection activity uses the Powershell activity template to access the SCCM server. The activity is configured to use a MID Server with Powershell capabilities and to run a MID Server script called AddToUserCollection.ps1 to edit the collection.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > System Center Configuration Manager (SCCM).

Note: The Add to User Collection activity does not use pre-processing or post processing scripts.

Input variables

Add to User Collection input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sccmServer</td>
<td>The fully qualified domain name (FQDN) of the SCCM server.</td>
</tr>
<tr>
<td>collection</td>
<td>Name of the user collection.</td>
</tr>
<tr>
<td>user</td>
<td>Name of the user to add to the collection.</td>
</tr>
</tbody>
</table>

Output variable

Add to User Collection output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>output</td>
<td>Variable that contains a value that is passed to other activities in the workflow.</td>
</tr>
<tr>
<td>error</td>
<td>Variable that contains the activity output error message.</td>
</tr>
</tbody>
</table>
Conditions

<table>
<thead>
<tr>
<th>Add to User Collection conditions</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully added a user to the SCCM user collection.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to add a user to the SCCM user collection.</td>
</tr>
</tbody>
</table>

Get Applications activity

The Get Applications activity returns a list of all the applications available on a Microsoft System Center Configuration Manager (SCCM) server.

The Get Applications activity uses the [Powershell activity template](#) to access the applications on the SCCM server. The activity is configured to use a MID Server with Powershell capabilities and to run a MID Server script called `GetApplications.ps1`. This script filters the results of the GET, so that only specific attributes are returned for the applications on the SCCM server. Filtering the results in this manner controls the size of the payload, while providing the most desirable application data. The list of available applications is returned as an array in a JSON object.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > System Center Configuration Manager (SCCM).

**Note:** The Get Applications activity does not use a pre-processing script.

Input variables

**Get Applications input variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sccmServer</td>
<td>The fully qualified domain name (FQDN) of the SCCM server.</td>
</tr>
</tbody>
</table>

Output variables

The output variables for the Get Applications activity contain an array of objects called applications and an error message. Each object in the array contains the attributes in this table.
Get Applications output variables

<table>
<thead>
<tr>
<th>Variables</th>
<th>Description</th>
</tr>
</thead>
</table>
| applications| The applications array contains these attributes:  
  - id: Primary key of the SCCM application.  
  - ciUniqueId: Unique ID of the SCCM application.  
  - name: Name of the application.  
  - manufacturer: Manufacturer of the application.  
  - version: Version of the application.  
  - isDeployable: True/false value indicating if this application is deployable.  
  - isDeployed: True/false value indicating if this application is already deployed.  
  - numberOfUsersWithApp: Count of users with this application installed.  
  - numberOfDevicesWithApp: Count of devices on which this application is installed.  
  - application: Object containing the data set listed above for this application. Use the script to parse additional data from this set that you might need. |
| error       | Variable that contains the activity output error message. |

Conditions

Get Applications conditions

<table>
<thead>
<tr>
<th>Variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully retrieved the list of applications available on the SCCM host.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to retrieve the list of applications available on the SCCM host.</td>
</tr>
</tbody>
</table>

Get Deployments activity

The Get Deployments activity returns the list of deployments performed by Orchestration using a Microsoft System Center Configuration Manager (SCCM) server.

The Get Deployments activity uses the Powershell activity template to access the deployments on the SCCM server. The activity is configured to use a MID Server with Powershell capabilities and to run a MID Server script called GetDeployments.ps1 that returns the deployments on the host. This script filters the results of the GET, so that only specific attributes are returned for the deployments on the SCCM server. Filtering the results in this manner controls the size of the payload, while providing the most desirable deployment data. The list of available deployments is returned as an array in a JSON object.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > System Center Configuration Manager (SCCM).
Note: The Get Deployments activity does not use pre-processing scripts.

## Input variables

### Get Deployments input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sccmServer</td>
<td>The fully qualified domain name (FQDN) of the SCCM server.</td>
</tr>
</tbody>
</table>

## Output variables

### Get Deployments output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deployments</td>
<td>The <code>deployments</code> array contains these attributes:</td>
</tr>
<tr>
<td></td>
<td>- <strong>id</strong>: Primary key of the SCCM application.</td>
</tr>
<tr>
<td></td>
<td>- <strong>applicationId</strong>: Primary key of the SCCM application.</td>
</tr>
<tr>
<td></td>
<td>- <strong>softwareName</strong>: Name of the software that will be deployed.</td>
</tr>
<tr>
<td></td>
<td>- <strong>collectionId</strong>: Primary key of the SCCM collection.</td>
</tr>
<tr>
<td></td>
<td>- <strong>collectionName</strong>: Name of the SCCM collection.</td>
</tr>
<tr>
<td></td>
<td>- <strong>desiredConfigType</strong>: Possible values are: <strong>Install</strong> (1) and <strong>Uninstall</strong> (2).</td>
</tr>
<tr>
<td></td>
<td>- <strong>deploymentIntent</strong>: Intended purpose of the deployment. Possible values are: <strong>Available</strong> (1) and <strong>Required</strong> (2).</td>
</tr>
<tr>
<td></td>
<td>- <strong>numberSuccess</strong>: Number of clients that successfully installed the deployment.</td>
</tr>
<tr>
<td></td>
<td>- <strong>numberErrors</strong>: Number of clients with an error when installing the deployment.</td>
</tr>
<tr>
<td></td>
<td>- <strong>deployment</strong>: Object containing the data set of attributes listed here for this deployment. Use the post-processing script to parse additional data from this set that you might need.</td>
</tr>
<tr>
<td>error</td>
<td>Variable that contains the activity output error message.</td>
</tr>
</tbody>
</table>
Conditions

Get Deployments conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully retrieved the list of deployments performed by Orchestration using an SCCM host.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to retrieve the list of deployments performed by Orchestration using an SCCM host.</td>
</tr>
</tbody>
</table>

Get Device Collections activity

The Get Device Collections activity returns the list of available device collections on a Microsoft System Center Configuration Manager (SCCM) host.

The Get Device Collections activity uses the **Powershell activity template** to access the collections on the SCCM server. The activity is configured to use a MID Server with Powershell capabilities and to run a MID Server script called `GetDeviceCollections.ps1` that returns the device collections on the server. This script filters the results of the GET, so that only specific attributes are returned for the device collections on the SCCM server. Filtering the results in this manner controls the size of the payload, while providing the most desirable device collection data. The list of available collections is returned as an array in a JSON object.

To access this activity in the workflow editor, select the **Custom** tab, and then navigate to **Custom Activities > System Center Configuration Manager (SCCM)**.

Note: The Get Device Collections activity does not use pre-processing scripts.

Input variables

Get Device Collections input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sccmServer</td>
<td>The fully qualified domain name (FQDN) of the SCCM server.</td>
</tr>
</tbody>
</table>
Output variables

Get Device Collections output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deviceCollections</td>
<td>The <code>deviceCollections</code> array contains these attributes:</td>
</tr>
<tr>
<td></td>
<td>· id: Primary key of the SCCM device collection.</td>
</tr>
<tr>
<td></td>
<td>· name: Name of the SCCM device collection.</td>
</tr>
<tr>
<td></td>
<td>· collectionType: Type of SCCM collection. In this case, the value is <code>device</code>.</td>
</tr>
<tr>
<td></td>
<td>· localMemberCount: Count of device collection members visible at the local SCCM site.</td>
</tr>
<tr>
<td></td>
<td>· memberCount: Count of all device collection members.</td>
</tr>
<tr>
<td></td>
<td>· deviceCollection: Object containing the data set of attributes listed here for this device collection. Use the post-processing script to parse additional data from this set to use.</td>
</tr>
<tr>
<td>error</td>
<td>Variable that contains the activity output error message.</td>
</tr>
</tbody>
</table>

Conditions

Get Device Collections conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully retrieved a list of device collections available on the SCCM host.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to retrieve a list of device collections available on the SCCM host.</td>
</tr>
</tbody>
</table>

Get User Collections activity

The Get User Collections activity returns the list of available user collections on a Microsoft System Center Configuration Manager (SCCM) server.

The Get User Collections activity uses the PowerShell activity template to access the user collections on the SCCM server. The activity is configured to use a MID Server with PowerShell capabilities and to run a MID Server script called `GetUserCollections.ps1` that returns the user collections on the host. This script filters the results of the GET, so that only specific attributes are returned for the user collections on the SCCM server. Filtering the results in this manner controls the size of the payload, while providing the most desirable user collection data. The list of available collections is returned as an array in a JSON object.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > System Center Configuration Manager (SCCM).

Note: The Get User Collections activity does not use pre-processing scripts.
Input variables

### Get User Collections input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sccmServer</td>
<td>The fully qualified domain name (FQDN) of the SCCM server.</td>
</tr>
</tbody>
</table>

Output variables

### Get User Collections output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>userCollections</td>
<td>The userCollections array contains these attributes:</td>
</tr>
<tr>
<td></td>
<td>• id: Primary key of the SCCM user collection.</td>
</tr>
<tr>
<td></td>
<td>• name: Name of the SCCM user collection.</td>
</tr>
<tr>
<td></td>
<td>• collectionType: Type of SCCM collection. In this case, the value is user.</td>
</tr>
<tr>
<td></td>
<td>• localMemberCount: Count of user collection members visible at the local SCCM site.</td>
</tr>
<tr>
<td></td>
<td>• memberCount: Count of all user collection members.</td>
</tr>
<tr>
<td></td>
<td>• userCollection: Object containing the data set of attributes listed here for this user collection. Use the post-processing script to parse additional data from this set to use.</td>
</tr>
<tr>
<td>error</td>
<td>Variable that contains the activity output error message.</td>
</tr>
</tbody>
</table>

Conditions

### Get User Collections conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully retrieved the list of available user collections on an SCCM host.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to retrieve the list of available user collections on an SCCM host.</td>
</tr>
</tbody>
</table>

Is Device in Collection activity

This activity verifies if a device exists in an SCCM device collection.

The Is Device in Collection activity uses the PowerShell activity template to verify if a specific device exists in an SCCM device collection. The activity is configured to use a MID Server with PowerShell capabilities and to run a MID Server script called IsDeviceInCollection.ps1 to perform the test.
To access this activity in the workflow editor, select the **Custom** tab, and then navigate to **Custom Activities > System Center Configuration Manager (SCCM)**.

**Input variables**

**Is Device in Collection input variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sccmServer</td>
<td>The fully qualified domain name (FQDN) of the SCCM server.</td>
</tr>
<tr>
<td>collection</td>
<td>Name of the device collection.</td>
</tr>
<tr>
<td>device</td>
<td>Name of the device to verify is in the collection.</td>
</tr>
</tbody>
</table>

**Output variables**

**Is Device in Collection output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>output</td>
<td>Variable that contains the test result: True/False</td>
</tr>
<tr>
<td>errorMessage</td>
<td>Variable that contains the activity output error message.</td>
</tr>
</tbody>
</table>

**Conditions**

**Is Device in Collection conditions**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exist</td>
<td>The device exists in the collection.</td>
</tr>
<tr>
<td>Not exist</td>
<td>The device does not exist in the collection.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed.</td>
</tr>
</tbody>
</table>

**Is User in Collection activity**

This activity verifies if a user exists in an SCCM user collection.

The Is User in Collection activity uses the **PowerShell activity template** to verify if a specific user exists in an SCCM user collection. The activity is configured to use a MID Server with PowerShell capabilities and to run a MID Server script called **IsUserInCollection.ps1** to perform the test.

To access this activity in the workflow editor, select the **Custom** tab, and then navigate to **Custom Activities > System Center Configuration Manager (SCCM)**.
Input variables

Is User in Collection input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sccmServer</td>
<td>The fully qualified domain name (FQDN) of the SCCM server.</td>
</tr>
<tr>
<td>collection</td>
<td>Name of the user collection.</td>
</tr>
<tr>
<td>user</td>
<td>Name of the user to verify is in the collection.</td>
</tr>
</tbody>
</table>

Output variables

Is User in Collection output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>output</td>
<td>Variable that contains the test result: True/False</td>
</tr>
<tr>
<td>errorMessage</td>
<td>Variable that contains the activity output error message.</td>
</tr>
</tbody>
</table>

Conditions

Is User in Collection conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exist</td>
<td>The user exists in the collection.</td>
</tr>
<tr>
<td>Not exist</td>
<td>The user does not exist in the collection.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed.</td>
</tr>
</tbody>
</table>

Remove from Device Collection activity

The Remove from Device Collection activity removes a device from a Microsoft System Center Configuration Manager (SCCM) device collection.

The Remove from Device Collection activity uses the PowerShell activity template to remove a device from a device collection on a Microsoft SCCM server. The activity is configured to use a MID Server with Powershell capabilities and to run a MID Server script called RemoveFromUserCollection.ps1 to edit the collection.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > System Center Configuration Manager (SCCM).
Input variables

Remove from Device Collection input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sccmServer</td>
<td>The fully qualified domain name (FQDN) of the SCCM server.</td>
</tr>
<tr>
<td>collection</td>
<td>Name of the device collection.</td>
</tr>
<tr>
<td>device</td>
<td>Name of the device to add to the collection.</td>
</tr>
</tbody>
</table>

Output variables

Remove from Device Collection output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>output</td>
<td>Variable that contains a value that is passed to other activities in the workflow</td>
</tr>
<tr>
<td>error</td>
<td>Variable that contains the activity output error message.</td>
</tr>
</tbody>
</table>

Conditions

Remove from Device Collection conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully removed the device from the SCCM device collection.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to remove the device from the SCCM device collection.</td>
</tr>
</tbody>
</table>

Remove from User Collection activity

The Remove from User Collection activity removes a user from a Microsoft System Center Configuration Manager (SCCM) user collection.

The Remove from User Collection activity uses the Powershell activity designer template to access a user collection on a Microsoft SCCM target host. The activity is configured to use a MID Server with Powershell capabilities and to run a MID Server script called RemoveFromUserCollection.ps1 to edit the collection.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > System Center Configuration Manager (SCCM).
Input variables

Remove from User Collection input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sccmServer</td>
<td>The fully qualified domain name (FQDN) of the SCCM server.</td>
</tr>
<tr>
<td>collection</td>
<td>Name of the user collection.</td>
</tr>
<tr>
<td>user</td>
<td>Name of the user to add to the collection.</td>
</tr>
</tbody>
</table>

Output variables

Remove from User Collection output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>output</td>
<td>Variable that contains a value that is passed to other activities in the workflow.</td>
</tr>
<tr>
<td>error</td>
<td>Variable that contains the activity output error message.</td>
</tr>
</tbody>
</table>

Conditions

Remove from User Collection conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully removed the user from the SCCM user collection.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to remove the user from the SCCM user collection.</td>
</tr>
</tbody>
</table>

SFTP File Transfer activity pack

Use the SFTP File Transfer activities to manage files and directories on an SFTP server and to move files from one SFTP server to another.

The SFTP activity pack includes scoped activities for common file transfer tasks and a ready-to-use workflow that includes these activities. Use the SFTP workflow to control which files are going to be moved, what conditions the files need to meet, the order in which the files are moved, and which overwrite options are executed.

Note: To use the SFTP File Transfer activities and workflow, you must request activation of the Orchestration - SFTP plugin.

SFTP File Transfer workflow

The SFTP File Transfer activity pack includes a scoped workflow that uses multiple activities to manage files on SFTP servers.
The maximum activity count for the SFTP File Transfer workflow is set to 10,000. This allows the workflow to move up to 1000 files from one server to another.

Accessing the workflow

- Navigate to Workflow > Workflow Editor and select the Workflows tab.
- Click on the SFTP File Transfer workflow to open it.
- Click the information icon in the workflow header to display the properties dialog box.

Input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source host</td>
<td>Name or IP address of the server containing the files you want to move.</td>
<td></td>
</tr>
<tr>
<td>Source port</td>
<td>Port number to use to communicate with the source server.</td>
<td>22</td>
</tr>
<tr>
<td>Source directory</td>
<td>Full path to the directory where the source files are located.</td>
<td></td>
</tr>
<tr>
<td>Source files</td>
<td>Names of specific source files to move. Separate the file names in this list with semi-colons. This field supports the use of wild cards. For information about how the values in this field are affected by options in other fields, see the section below the table.</td>
<td></td>
</tr>
<tr>
<td>Excluded files</td>
<td>Names of specific source files to exclude from the move. The system moves all other files found in the source directory or subfolders. Separate the file names in this list with semi-colons. This field supports the use of wild cards. For information about how the values in this field are affected by options in other fields, see the section below the table.</td>
<td></td>
</tr>
<tr>
<td>Target host</td>
<td>Name or IP address of the server to which the files are being moved.</td>
<td></td>
</tr>
<tr>
<td>Target port</td>
<td>Port number to use to communicate with the target host.</td>
<td>22</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
<td>Default value</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td><strong>Datetime format</strong></td>
<td>Timestamp format to apply when the $[DateTime]$ variable is used in the <strong>Target directory</strong> or <strong>Target files</strong> field. The system uses the current time from the instance to create timestamp values.</td>
<td>yyyy-MM-dd</td>
</tr>
<tr>
<td><strong>Target directory</strong></td>
<td>Path to the directory in the target host where the files are being moved. You can specify a target directory whose name includes the timestamp by adding the $[DateTime]$ variable to the directory name. For example, you might enter this path to a target directory: /user/jacinto.gawron/documents/projects_ $[DateTime]$. This produces the projects_20150505 directory. When the timestamp variable is used, the system uses the format specified in the <strong>Datetime format</strong> field.</td>
<td></td>
</tr>
</tbody>
</table>
| **Target file**   | Format to use for target file names when a timestamp is added. You can configure the system to add the timestamp as a prefix to the file name or insert the timestamp into the name, using these variables:  
  - $[DateTime]$: Current timestamp, using the format defined in the **Datetime format** field.  
  - $[SourceFile]$: Complete file name.  
  - $[SourceFile:Base]$: Base file name without the extension.  
  - $[SourceFile:Ext]$: File extension only.  
  A target file name with the timestamp added as a prefix is expressed as: $[DateTime]_ $[SourceFile]. This produces a file name that looks like this: 20150505_file1.txt  
  A target file name with the timestamp inserted into the name is expressed as: $[SourceFile:Base]_ $[DateTime]$[SourceFile:Ext]. This produces a file name that looks like this: file1_20150505.txt |               |
<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply move conditions</td>
<td>Check box to apply conditions to the file transfer. If this check box is selected, additional fields appear for setting conditions.</td>
<td>false</td>
</tr>
<tr>
<td>Minimum file size, in bytes</td>
<td>Condition that defines a target file’s minimum size requirement. This setting can help determine if the file is valid. This field appears when the Apply move conditions check box is selected.</td>
<td>0</td>
</tr>
<tr>
<td>Maximum file size, in bytes</td>
<td>Condition that defines a target file’s maximum size requirement. This field appears when the Apply move conditions check box is selected.</td>
<td>-1</td>
</tr>
<tr>
<td>File is not older than</td>
<td>Condition that sets the earliest acceptable date for this file’s age range. The range starts at 00:00 (midnight) on the date specified. This field appears when the Apply move conditions check box is selected.</td>
<td></td>
</tr>
<tr>
<td>File is not newer than</td>
<td>Condition that sets the latest acceptable date for this file’s age range. The range ends at 23:59 on the date specified. This field appears when the Apply move conditions check box is selected.</td>
<td></td>
</tr>
<tr>
<td>Include subfolders</td>
<td>Check box to move the files from subfolders in the source directory. For information about how your selection affects other fields in the form, see the section below the table.</td>
<td></td>
</tr>
<tr>
<td>Move order</td>
<td>Order in which the files are moved from the source to the target. The possible options are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- None (same order as files in the source directory)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- By timestamp</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- By file name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- By file size</td>
<td></td>
</tr>
<tr>
<td>Sort order</td>
<td>Order in which the files are sorted in the target directory, using the option selected in the Move order field. Sorting options are Ascending and Descending.</td>
<td>desc</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
<td>Default value</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Maximum number of retries</td>
<td>Number of attempts the activity can make to connect to the target host or to move a file before timing out. When the retry limit to move a file or to connect to the host is exceeded, the system logs a failure. If the maximum number of failures is not exceeded, the system attempts to connect again or to move the next file named.</td>
<td>2</td>
</tr>
<tr>
<td>Time between retries, in seconds</td>
<td>Time, in seconds, between repeat attempts to connect to the target or to begin moving a file.</td>
<td>10</td>
</tr>
<tr>
<td>Maximum number of failures</td>
<td>Acceptable number of times the system can fail to connect to the target host or to move a file before it quits trying. A failure occurs when the number of configured retries is exceeded. Using the default settings, failure occurs when the system cannot connect to the target or move a file after two retries.</td>
<td>0</td>
</tr>
<tr>
<td>Duplicate file action</td>
<td>Action to take if a file being moved already exists in the target directory. The choices are:</td>
<td>overwrite</td>
</tr>
<tr>
<td></td>
<td>• Overwrite if file exists (default)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rename with index</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Do not move</td>
<td></td>
</tr>
<tr>
<td>Preserve file attributes</td>
<td>Check box to use the time stamp and mode information from the source files for the copied files. If this check box is cleared, the copied files have a current time stamp and mode.</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This timestamp is a file attribute and is not appended to the file name.</td>
<td></td>
</tr>
<tr>
<td>Upon success, remove files from source</td>
<td>Check box to delete original files from the source directory when they are copied to the new location. Clear this check box to keep the source files in their current location in the source host.</td>
<td>false</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
<td>Default value</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Upon failure, keep moved files on target</td>
<td>Check box to keep any files on the target that were moved successfully, even if the entire file transfer operation ended in failure. If this check box is cleared, the system removes all successfully transferred files from the target when general failure occurs.</td>
<td>true</td>
</tr>
<tr>
<td>Credential tag for source</td>
<td>Specific credential tag this activity must use to run SSH commands on the source host.</td>
<td></td>
</tr>
<tr>
<td>Credential tag for target</td>
<td>Specific credential tag this activity must use to run SSH commands on the target host.</td>
<td></td>
</tr>
</tbody>
</table>

### File selection logic

When selecting the files to move from the source host, the system uses this logic:

- If the **Source files** and **Excluded files** fields are empty, the system moves all the files in the source directory.
- When the **Include subfolders** check box is selected, the following dependencies exist:
  - If no files are specified in the **Source files** and **Exclude files** fields, the system moves all files in the source directory and all files in all subfolders of the source directory.
  - If the **Source files** field contains file names, the system moves those files from their location on either the source directory or any of its subfolders.
  - If the **Exclude files** field contains file names, the system moves all the files from the source directory and its subfolders except those excluded files.
- When the **Include subfolders** check box is cleared, the system looks only in the source directory for files to move or exclude.

### Copy File activity

The Copy File activity copies a file from an SFTP server (source host) to another SFTP server (target host).

### Input variables

**Copy File input variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceHost</td>
<td>Name or IP address of the server containing the files you want to transfer.</td>
<td></td>
</tr>
<tr>
<td>sourcePort</td>
<td>Port number to use to communicate with the source server. The default port number is 22.</td>
<td></td>
</tr>
<tr>
<td>sourceFilePath</td>
<td>Full path to the file to copy from the source host.</td>
<td></td>
</tr>
</tbody>
</table>
### Variable Description

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>targetHost</td>
<td>Name or IP address of the server to which you want to move the files.</td>
</tr>
<tr>
<td>targetPort</td>
<td>Port number to use to communicate with the target server. The default port number is 22.</td>
</tr>
<tr>
<td>targetFilePath</td>
<td>Full path to the copied file on the target host.</td>
</tr>
<tr>
<td>tempFileSuffix</td>
<td>Temporary suffix to use when moving a file. If this field contains a value, the activity deletes the duplicate target file, if it exists, and then copies the source file to a temporary file using targetFilePath + tempFileSuffix as the name. Upon completion, the activity renames the file to the actual target file name. If this field is blank, the activity copies the source file directly to the target file and overwrites it, if it already exists.</td>
</tr>
<tr>
<td>sourceCredentialTag</td>
<td>Specific credential tag this activity must use to run SSH commands on the source host.</td>
</tr>
<tr>
<td>targetCredentialTag</td>
<td>Specific credential tag this activity must use to run SSH commands on the target host.</td>
</tr>
</tbody>
</table>

### Output variables

#### Copy File output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>errorMessages</td>
<td>The executionResult.errorMessages from the Activity designer parsing sources. If this variable is not null, the operation has failed.</td>
</tr>
<tr>
<td>result</td>
<td>Text message advising that the command was executed successfully.</td>
</tr>
</tbody>
</table>

### Conditions

#### Copy File conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The activity succeeded in copying the file.</td>
</tr>
<tr>
<td>Failure</td>
<td>The activity failed to copy the file.</td>
</tr>
</tbody>
</table>

### Create Directory activity

The Create Directory activity creates a new directory on an SFTP server.
### Input variables

#### Create Directory input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceHost</td>
<td>Name or IP address of the server containing the files you want to move.</td>
</tr>
<tr>
<td>sourcePort</td>
<td>Port number to use to communicate with the source server. The default port number is 22.</td>
</tr>
<tr>
<td>sourceDirectory</td>
<td>Path to the target directory to create.</td>
</tr>
<tr>
<td>sourceCredentialTag</td>
<td>Specific <a href="#">credential tag</a> this activity must use to run SSH commands on the host.</td>
</tr>
</tbody>
</table>

### Output variables

#### Create Directory output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>errorMessage</td>
<td>The <code>executionResult.errorMessages</code> from the Activity designer parsing sources. If this variable is not null, the operation has failed.</td>
</tr>
<tr>
<td>result</td>
<td>Text message advising that the command was executed successfully.</td>
</tr>
</tbody>
</table>

### Conditions

#### Create Directory conditions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The activity succeeded in creating the directory.</td>
</tr>
<tr>
<td>Failure</td>
<td>The activity failed to create the directory.</td>
</tr>
</tbody>
</table>

### Get File List activity

The Get File List activity returns a list of files from a given directory and its subdirectories on an SFTP server (source host).

### Input variables

#### Get File List input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceHost</td>
<td>Name or IP address of the server containing the files you want to list.</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>sourcePort</td>
<td>Port number to use to communicate with the target server. The default port number is 22.</td>
</tr>
<tr>
<td>sourceDirectory</td>
<td>Path to the target directory containing the files to list.</td>
</tr>
<tr>
<td>sourceFiles</td>
<td>List of target files to return. This is a comma separated list that accepts wildcards, such as *.txt.</td>
</tr>
<tr>
<td>excludedFiles</td>
<td>List of target files to exclude. This is a comma separated list that accepts wildcards, such as *.txt.</td>
</tr>
<tr>
<td>includeSubfolders</td>
<td>True/false variable that determines if files from subfolders are included in the list. The default value for this variable is false.</td>
</tr>
<tr>
<td>sourceCredentialTag</td>
<td>Specific credential tag this activity must use to run SSH commands on the host.</td>
</tr>
</tbody>
</table>

Output variables

Get File List output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>errorMessage</td>
<td>The executionResult.errorMessages from the Activity designer parsing sources. If this variable is not null, the operation has failed. An activity can examine the error message to customize a condition. For example, if the error message contains NO_SUCH_FILE, the activity can be considered successful, depending on circumstances.</td>
</tr>
<tr>
<td>result</td>
<td>List of requested files, returned as a JSON string.</td>
</tr>
</tbody>
</table>

Conditions

Get File List conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The activity succeeded in listing the requested files.</td>
</tr>
<tr>
<td>Failure</td>
<td>The activity failed to list the requested files.</td>
</tr>
</tbody>
</table>

Remove File or Directory activity

The Remove File or Directory activity removes a file or a directory on an SFTP server, including subdirectories, when configured.
## Input variables

### Remove File or Directory input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceHost</td>
<td>Name or IP address of the server containing the files you want to remove.</td>
</tr>
<tr>
<td>sourcePort</td>
<td>Port number to use to communicate with the target server. The default port number is 22.</td>
</tr>
<tr>
<td>sourceFilePath</td>
<td>Full path to the file or directory to remove. To remove multiple files or directories using a single activity, enter a semicolon-separated list of paths in this field.</td>
</tr>
<tr>
<td>isDirectory</td>
<td>True/false variable that determines if the specified file path is a directory. The default value for this variable is false.</td>
</tr>
<tr>
<td>includeSubfolders</td>
<td>True/false variable that determines if the given directory and all of its subfolders should be removed. The default value for this variable is false. If the value for this field is false, then the activity can only remove an empty directory. This field appears when the isDirectory checkbox is selected.</td>
</tr>
<tr>
<td>sourceCredentialTag</td>
<td>Specific credential tag this activity must use to run SSH commands on the host.</td>
</tr>
</tbody>
</table>

## Output variables

### Remove File or Directory output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>errorMessage</td>
<td>The executionResult.errorMessages from the Activity designer parsing sources. If this variable is not null, the operation has failed.</td>
</tr>
<tr>
<td>result</td>
<td>Either success or failure.</td>
</tr>
<tr>
<td>deletionResults</td>
<td>The deletionResults array contains these attributes:</td>
</tr>
<tr>
<td></td>
<td>- <strong>fullPath</strong>: Full path to the file or directory targeted.</td>
</tr>
<tr>
<td></td>
<td>- <strong>status</strong>: Either succeeded or failed.</td>
</tr>
<tr>
<td></td>
<td>- <strong>reason</strong>: Text message describing the cause of a failure.</td>
</tr>
</tbody>
</table>
Conditions

Remove File or Directory conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The activity succeeded in removing the file or directory specified.</td>
</tr>
<tr>
<td>Failure</td>
<td>The activity failed to remove the file or directory specified.</td>
</tr>
</tbody>
</table>

Rename File or Directory activity

The Rename File or Directory activity renames a file or directory to a new name on an SFTP server.

Input variables

Rename File or Directory input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceHost</td>
<td>Name or IP address of the server containing the file or directory you want to rename.</td>
</tr>
<tr>
<td>sourcePort</td>
<td>Port number to use to communicate with the target server. The default port number is 22.</td>
</tr>
<tr>
<td>sourceFilePath</td>
<td>Full path to the file or directory to rename.</td>
</tr>
<tr>
<td>targetFilePath</td>
<td>Full path to the renamed file or directory.</td>
</tr>
<tr>
<td>sourceCredentialTag</td>
<td>Specific [credential tag] this activity must use to run SSH commands on the host.</td>
</tr>
</tbody>
</table>

Output variables

Rename File or Directory output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>errorMessages</td>
<td>The executionResult.errorMessages from the Activity designer parsing sources. If this variable is not null, the operation has failed.</td>
</tr>
<tr>
<td>result</td>
<td>A message saying that the operation has been successful. For example, you might see: Rename /tmp/sftp_test/subdir1 to /tmp/sftp_test/subdir2 complete.</td>
</tr>
</tbody>
</table>
Conditions

Rename File or Directory conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The activity succeeded in renaming the file or directory.</td>
</tr>
<tr>
<td>Failure</td>
<td>The activity failed to rename the file or directory.</td>
</tr>
</tbody>
</table>

Set File Attributes activity

The Set File Attributes activity sets common file attributes, such as timestamps, size, permissions, and UID/GID, for a file or directory on an SFTP server.

A good practice is to use the Get File List activity to return a list of files and their attributes first. Then, when you moved a file from a source host to a target host, use the Set File Attributes activity to set the source file attributes on the target file. This is demonstrated in the SFTP File Transfer workflow.

Input variables

Set File Attributes input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceHost</td>
<td>Name or IP address of the server containing the file or directory whose attributes you want to change.</td>
</tr>
<tr>
<td>sourcePort</td>
<td>Port number to use to communicate with the target server. The default port number is 22.</td>
</tr>
<tr>
<td>sourceFilePath</td>
<td>Full path to the file or directory whose attributes you want to change.</td>
</tr>
<tr>
<td>userID</td>
<td>User ID attribute to apply to the file or directory. The UID and GUID variables must be set together as a pair.</td>
</tr>
<tr>
<td>groupID</td>
<td>Group ID attribute to apply to the file or directory. The UID and GUID variables must be set together as a pair.</td>
</tr>
<tr>
<td>permissions</td>
<td>File or directory permissions to set for the user and group specified. This value must be expressed as an integer, such as 16877, which defines these permissions: rwxr-xr-x. Note: The permissions number is an internal value returned by the Get File List activity.</td>
</tr>
<tr>
<td>accessTimestamp</td>
<td>Override the timestamp when the file or directory was last accessed. The access and modification timestamps must be set together as a pair.</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>modificationTimestamp</td>
<td>Override the timestamp when the file or directory was last modified. The access and modification timestamps must be set together as a pair.</td>
</tr>
<tr>
<td>sizeInBytes</td>
<td>Size of the file or directory, expressed in bytes.</td>
</tr>
<tr>
<td>sourceCredentialTag</td>
<td>Specific credential tag this activity must use to run SSH commands on the host.</td>
</tr>
</tbody>
</table>

**Output variables**

Set File Attributes output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>errorMessage</td>
<td>The <code>executionResult.errorMessages</code> from the [Activity designer parsing sources](https:// servicenow.com/help.html). If this variable is not null, the operation has failed.</td>
</tr>
<tr>
<td>result</td>
<td>Text message advising that the command was executed successfully.</td>
</tr>
</tbody>
</table>

**Conditions**

Set File Attributes conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The activity succeeded in changing the attributes of the specified file or directory.</td>
</tr>
<tr>
<td>Failure</td>
<td>The activity failed to change the attributes of the specified file or directory.</td>
</tr>
</tbody>
</table>

**SSH activity pack**

Orchestration provides an activity pack of SSH activities that were customized using the ServiceNow activity designer.

These activities perform the same functions as SSH activities by the same name from previous releases and replace those activities for all new workflows. The custom SSH activities were built with the [Create an SSH activity](https://servicenow.com/help.html), which gives workflow administrators the ability to store input and output variables in the databus.

**Note:** Existing workflows from earlier versions that were created with legacy SSH activities continue to function normally after an upgrade to Geneva. However, all new workflows must use these custom SSH activities.

To use the SSH custom activities, you must request activation of the Orchestration - SSH plugin.

**Secure Copy activity**

The Secure Copy activity copies a file from one host to another, without storing the copied file on the MID Server.
This activity replaces an SSH activity by the same name available in releases prior to Geneva. If you have a workflow created in a previous version that uses the deprecated activity, your workflow will continue to work normally after upgrading to Geneva. However, all new workflows must use the custom version of this activity. This activity was built with the [SSH activity designer template](#), which gives workflow administrators the ability to store input and output variables in the databus.

### Input variables

**Secure Copy input variables**

<table>
<thead>
<tr>
<th>Input variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>from_host</td>
<td>Host name or IP address of the source machine.</td>
</tr>
<tr>
<td>from_scp_file</td>
<td>Name of the file to copy, including the absolute path.</td>
</tr>
<tr>
<td>to_host</td>
<td>Host name or IP address of the target machine.</td>
</tr>
<tr>
<td>to_scp_file</td>
<td>Path to the target file. This path can be absolute or relative to the logged in user’s home directory.</td>
</tr>
<tr>
<td>debug_mid</td>
<td>Check box that enables debug logging when selected.</td>
</tr>
<tr>
<td>debug_ssh</td>
<td>Check box that enables J2SSH debug logging when selected.</td>
</tr>
</tbody>
</table>

### Output variables

**Secure Copy output variables**

<table>
<thead>
<tr>
<th>Output variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>payload</td>
<td>The <code>executionResult.payload</code> from the <a href="#">Activity designer parsing sources</a>.</td>
</tr>
<tr>
<td>output</td>
<td>The <code>executionResult.output</code> from the parsing sources.</td>
</tr>
</tbody>
</table>

### Conditions

**Secure Copy conditions**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully copied the file from one host to another.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to copy the file from one host to another.</td>
</tr>
</tbody>
</table>

### Files Compare activity

The Files Compare activity compares two files on a Linux or UNIX computer.
This activity replaces an SSH activity by the same name available in releases prior to Geneva. If you have a workflow created in a previous version that uses the deprecated activity, your workflow will continue to work normally after upgrading to Geneva. However, all new workflows must use the custom version of this activity. This activity was built with the [SSH activity designer template](#), which gives workflow administrators the ability to store input and output variables in the databus.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Global > Orchestration - SSH.

### Input variables

#### Files Compare input variables

<table>
<thead>
<tr>
<th>Input variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>Hostname or IP address of the destination server for SSH activity.</td>
</tr>
<tr>
<td>Directory</td>
<td>Name of the working directory.</td>
</tr>
<tr>
<td>OldFile</td>
<td>Name of the first file to compare.</td>
</tr>
<tr>
<td>NewFile</td>
<td>Name of the second file to compare.</td>
</tr>
</tbody>
</table>

### Output variables

#### Files Compare output variables

<table>
<thead>
<tr>
<th>Output variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>contents</td>
<td>File comparison result. This is the difference of the two compared files.</td>
</tr>
<tr>
<td>result</td>
<td>Either success or failure.</td>
</tr>
<tr>
<td>return-code</td>
<td>Either 0, if the two files are the same, or 1, if the two files are different.</td>
</tr>
<tr>
<td>errorMessage</td>
<td>The <code>executionResult.errorMessages</code> from the <code>Activity designer parsing sources</code>.</td>
</tr>
</tbody>
</table>

### Conditions

#### Files Compare conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully compared the specified files.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity could not compare the specified files.</td>
</tr>
</tbody>
</table>

### File Read activity

The File Read activity reads a file on a Linux or UNIX computer.
This activity replaces an SSH activity by the same name available in releases prior to Geneva. If you have a workflow created in a previous version that uses the deprecated activity, your workflow will continue to work normally after upgrading to Geneva. However, all new workflows must use the custom version of this activity. This activity was built with the SSH activity designer template, which gives workflow administrators the ability to store input and output variables in the databus.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Global > Orchestration - SSH.

**Input variables**

**File read input variables**

<table>
<thead>
<tr>
<th>Input variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>Hostname or IP address of the destination server for SSH activity.</td>
</tr>
<tr>
<td>Directory</td>
<td>Name of the working directory.</td>
</tr>
<tr>
<td>File</td>
<td>The name of the file to read.</td>
</tr>
</tbody>
</table>

**Output variables**

**File read output variables**

<table>
<thead>
<tr>
<th>Output variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>contents</td>
<td>Content of the file to read.</td>
</tr>
<tr>
<td>result</td>
<td>Either success or failure.</td>
</tr>
<tr>
<td>errorMessage</td>
<td>The executionResult.errorMessages from the Activity designer parsing sources.</td>
</tr>
</tbody>
</table>

**Conditions**

**File Read conditions**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully read the contents of the specified file.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity could not read the contents of the specified file.</td>
</tr>
</tbody>
</table>

**File Write activity**

The File Write activity writes a file on a Linux or UNIX computer.

The source file can be an absolute or relative path from the Directory. If an absolute path is used, then no value is required in the Directory field.
This activity replaces an SSH activity by the same name available in releases prior to Istanbul. If you have a workflow created in a previous version that uses the deprecated activity, your workflow will continue to work normally after upgrading to Istanbul. However, all new workflows must use the custom version of this activity. This activity was built with the SSH activity template, which gives workflow administrators the ability to store input and output variables in the databus.

**Input variables**

**File Write input variables**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>Hostname or IP address of destination server for SSH activity.</td>
</tr>
<tr>
<td>directory</td>
<td>Name of the working (target) directory.</td>
</tr>
<tr>
<td>file</td>
<td>Name of the file to be written.</td>
</tr>
<tr>
<td>behavior</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• overwrite: Creates the file if it does not exist and overwrites the file if it does exist.</td>
</tr>
<tr>
<td></td>
<td>• append: Creates the file if it does not exist and appends the new content to an existing file.</td>
</tr>
<tr>
<td></td>
<td>• create only: Creates the file if it does not exist and fails if the file does exist.</td>
</tr>
<tr>
<td>contents</td>
<td>What to write or append (depending on the behavior) to the file</td>
</tr>
</tbody>
</table>

**Output variables**

**File Write output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return_code</td>
<td>Indicates whether or not the file write operation was successful.</td>
</tr>
<tr>
<td>error_message</td>
<td>Message that indicates if an error has occurred. Any value other than 0 indicates a failure.</td>
</tr>
</tbody>
</table>

**Conditions**

**File Write conditions**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The activity wrote a file in the target directory.</td>
</tr>
<tr>
<td>Failure</td>
<td>The activity failed to write a file in the target directory.</td>
</tr>
</tbody>
</table>
File Copy activity

The custom File Copy activity copies a file on a Linux or UNIX computer. This activity replaces an SSH activity by the same name available in releases prior to Geneva. If you have a workflow created in a previous version that uses the deprecated activity, your workflow will continue to work normally after upgrading to Geneva. However, all new workflows must use the custom version of this activity. This activity was built with the SSH activity designer template, which gives workflow administrators the ability to store input and output variables in the databus.

To access this activity in the workflow editor, select the Custom tab, and then navigate to Custom Activities > Global > Orchestration - SSH.

Input variables

File Copy input variables

<table>
<thead>
<tr>
<th>Input variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>Hostname or IP address of destination server for SSH activity.</td>
</tr>
<tr>
<td>directory</td>
<td>Name of the working directory.</td>
</tr>
<tr>
<td>src_file</td>
<td>Name of the source file.</td>
</tr>
<tr>
<td>dst_file</td>
<td>The name of the destination file.</td>
</tr>
</tbody>
</table>

Output variables

File Copy output variables

<table>
<thead>
<tr>
<th>Output variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Either success or failure.</td>
</tr>
</tbody>
</table>

Conditions

File Copy conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully copied the file on the specified host.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to copy the file on the specified host.</td>
</tr>
</tbody>
</table>

File Replace String activity

The File Replace String activity finds and replaces a string in a file on a Linux or UNIX computer. This activity replaces an SSH activity by the same name available in releases prior to Istanbul. If you have a workflow created in a previous version that uses the deprecated activity, your
workflow will continue to work normally after upgrading to Istanbul. However, all new workflows
must use the custom version of this activity. This activity was built with the SSH activity template,
which gives workflow administrators the ability to store input and output variables in the databus.

## Input variables

### File Replace String input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>Hostname or IP address of destination server for SSH activity.</td>
</tr>
<tr>
<td>directory</td>
<td>Name of the working (target) directory.</td>
</tr>
<tr>
<td>file</td>
<td>Name of the file in which the string is to be replaced.</td>
</tr>
<tr>
<td>find_pattern</td>
<td>A regular expression of the text to replace.</td>
</tr>
<tr>
<td>replace_string</td>
<td>The replacement string for the text found by the expression in the find_pattern variable.</td>
</tr>
<tr>
<td>options</td>
<td>Replacement options:</td>
</tr>
<tr>
<td></td>
<td>- first: Replaces the first occurrence of the pattern.</td>
</tr>
<tr>
<td></td>
<td>- all:  Replaces all occurrences of the pattern.</td>
</tr>
</tbody>
</table>

## Output variables

### File Replace String output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return_code</td>
<td>Indicates whether or not the string was replaced successfully in the target file.</td>
</tr>
<tr>
<td>error_message</td>
<td>Message that indicates if an error has occurred. Any value other than 0 indicates a failure.</td>
</tr>
</tbody>
</table>

## Conditions

### File Replace String conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The activity has successfully replaced the string in the file.</td>
</tr>
<tr>
<td>Failure</td>
<td>The activity has failed to replaced the string in the file.</td>
</tr>
</tbody>
</table>
**Reset Linux User Password activity**

The Reset Linux User Password activity resets the password for a given user on a Linux computer.

This activity requires that the user executing the command be able to run the `chpasswd` command and, if expiring the password immediately, to run `chage` with `sudo privileges`.

This activity replaces an SSH activity by the same name available in releases prior to Istanbul. If you have a workflow created in a previous version that uses the deprecated activity, your workflow will continue to work normally after upgrading to Istanbul. However, all new workflows must use the custom version of this activity. This activity was built with the [SSH activity template](https://www.service-now.com), which gives workflow administrators the ability to store input and output variables in the [databus](https://www.service-now.com).

### Input variables

**Reset Linux User Password input variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>IP address of the target Linux machine.</td>
</tr>
<tr>
<td>user</td>
<td>Name of the user whose password is being reset.</td>
</tr>
<tr>
<td>password</td>
<td>New password set for this user. The password is a workflow variable that is encrypted either as a <code>password2</code> field or by calling the encryption method of a <code>Packages.com.glide.util.Encrypter</code> object.</td>
</tr>
<tr>
<td>force_change</td>
<td>Indicates if this password is temporary and to force the named user to change the password at login.</td>
</tr>
</tbody>
</table>

### Output variables

**Reset Linux User Password output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return_code</td>
<td>Indicates whether or not the user password reset action was successful.</td>
</tr>
<tr>
<td>error_message</td>
<td>Describes any error that occurred during password reset. If no error occurred, this value is null.</td>
</tr>
</tbody>
</table>

### Conditions

**Reset Linux User Password conditions**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity successfully changed specified user's password</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to change specified user's password.</td>
</tr>
</tbody>
</table>

**Global activities**

Global activities are Orchestration activities created in the global scope. Any activities you create in the global scope are listed in the Global category in the Packs and Custom tabs of the Workflow Editor.
The Test Server Alive activity determines if a target system is alive by its response to a particular protocol.

This activity replaces an activity by the same name available in releases prior to Istanbul. If you have a workflow created in a previous version that uses the deprecated activity, your workflow will
continue to work normally after upgrading to Istanbul. However, all new workflows must use the custom version of this activity. This activity was built with the Probe activity template, which gives workflow administrators the ability to store input and output variables in the databus.

Input variables

Test Server Alive input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port_probes</td>
<td>A comma separated list of protocols to use to check for signs of activity on the target machine (example: wmi,wins,https,ssh,http,https,snmp,dns)</td>
</tr>
<tr>
<td>hostname</td>
<td>Hostname or IP address of the target system to check.</td>
</tr>
</tbody>
</table>

Output variables

Test Server Alive output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alive</td>
<td>Code that indicates whether or not the server is alive. If any value but ‘1’ is returned, the server is not alive.</td>
</tr>
</tbody>
</table>

Conditions

Test Server Alive conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Activity determined that the device is running.</td>
</tr>
<tr>
<td>Failure</td>
<td>Activity failed to determine if the target device is running. Failure could be caused by a missing protocol or a device that is not accessible.</td>
</tr>
</tbody>
</table>

Orchestration activity designer

The Orchestration activity designer enables a user with either the workflow_admin or activity_creator and workflow_creator roles to construct reusable activities that suit an organization’s business needs.

Activities created by the activity designer offer the following advantages over core activities offered in previous releases:

- Reuse custom activities in multiple workflows.
- Upload and download custom activities from the ServiceNow Store.
- Parse data from standard input formats.
- Test input variables against a target host or endpoint and inspect the payload.
• Automatically map values from a test payload to an activity's output variables.
• Share data between activities.
• View previous versions of an activity.

Access to the activity designer requires activation of ServiceNow Orchestration. For instructions about managing transitions and conditions for all activities, see Workflow activities.

Orchestration provides numerous pre-defined activities, which are reusable components that can be used in numerous workflows without having to understand the complexities of the underlying system. These activities are grouped into activity packs, which address specific business needs, such as: Active Directory, Azure AD, Exchange, Infoblox DDI, and PowerShell. There are other ServiceNow applications which provide and maintain their own separate activity packs, such as Security Incident Response, Cloud Management, or Release Automation.

Customers can also build their own activities and activity packs. You can construct custom activities with a specified template through the Orchestration Activity Designer. Custom-built activities built with the Activity Designer are referred to as activity elements. Activity elements provide optimal operations, enable code reuse, and minimize the need to write code. They also enable you to follow the flow of data within a given workflow across orchestration activities. Incorporating activity elements limits the dependency on the scratchpad which reduces problems in complex workflows. Limit the use of core activities, like ‘Run Script’, unless you need direct access the scratchpad, for example, for a counter. Activity elements do not have direct access to the scratchpad. You can, however, pass scratchpad variables as inputs into your activities.

Orchestration activities created by the activity designer:
• Can be uploaded and shared in the ServiceNow App Store
• Use the databus, which allows the activity to have well-defined inputs and outputs
• Share data across activities within a workflow
• Use versioning
• Provide a consistent approach for activity development regardless protocol

Note: Prior to the Fujirelease, activities were built with Activity Definitions. In Fuji, a new architecture was introduced using the Activity Designer. Orchestration Core activities, built originally as Activity Definitions, have been converted to use the new template format (Activity Elements) and the databus offered with the activity designer. Workflows in upgraded instances that use legacy activities continue to work normally.

For instructions on using activities to construct a workflow, see Add an activity to a workflow.

Using credentials with Orchestration

Orchestration activities require credentials to their respective applications to access resources.

Before you can execute Orchestration activities, you must create and configure the corresponding credentials. The type of activity template you use can present different options for your credential configuration. For example, a REST or SOAP activity can use the credentials on the REST or SOAP message record. You can also override certain credentials with credentials configured in the central credential store. If support for OAuth or WS-Security is required, you must use the credentials on the SOAP or REST message record.

Some activity templates, such as PowerShell, SSH, JMS, and SFTP, provide support for resolving credentials through credential tagging. Tagging decouples the credential from an Activity Definition, the credential then resolves based on your environment configuration. This facilitates an easier experience to promote content to a production environment, share content, or publish content to the ServiceNow store. You should always employ credential tagging if it is available.
Syncing to MID: Any change to credential triggers a notification to MID to download latest credentials. This happens almost immediately but as always with any syncing mechanism expect a little bit of delay MID server service account vs Remote credentials. For AD/exchange activities, use credentials of user with right access to domain controller.

You should use the central Credentials table, when possible. The Credentials table provides security through ACLs, which require a credential_admin role to access the credentials table. There is also support for on-premise credential stores. The table stores the following:

- Basic authentication credentials (REST and SOAP activities)
- Cloud Management credentials (AWS communications)
- JDBC credentials (Database communications through JDBC driver)
- JMS credentials
- SNMPv3 credentials
- SSH credentials (Target instance communications)
- SSH private key credentials form
- VMware credentials
- Windows credentials (PowerShell communications)

**Credential tagging for Orchestration activities**

Credential tagging gives an administrator more control over the credentials used in Orchestration activities.

This is useful when an activity requires specific credentials to perform a task. You can use a credential tag to assign individual credentials to any activity in a Orchestration workflow or assign different credentials to each occurrence of the same activity type in an Orchestration workflow.

Credential tagging interacts with credential affinity to determine which credentials should be used for an Orchestration activity.

**How credential tagging works**

A business rule called Insert Discovery Affinity (renamed from Insert Credential Affinity in the Geneva release) runs when a record is inserted into the ECC Queue. This rule determines whether a credential affinity exists for the device and identifies the proper credential_id (the sys_id of the record in the Credentials [discovery_credentials] table) to use. When the platform encounters an affinity with a credential tag value defined (credential_tag in the business rule), the business rule determines if the credential referenced by the affinity has the specified tag. If it does, the business rule selects the credential_id of the tagged credential and passes that value to the MID Server. If the credential does not have the specified tag, any other affinities that exist for the target system will be checked. If no affinity references an appropriately tagged credential, the MID Server iterates through the Credentials (discovery_credentials) table and selects the credential with the appropriate tag. The MID Server then creates a new affinity for this credential.
Create custom activities using custom activity designer templates

You can create and update different types of custom activities in the Workflow Editor using a custom template.

Roles required: workflow_admin or activity_creator
The Activity Designer contains common steps which are applicable to all the activities that you create. This procedure guides you through the common steps and the order they should be set up. You specify an activity template before you create a custom activity.

1. Navigate to Orchestration > Workflow Editor. The Welcome tab of the Workflow Editor opens.
2. On the Custom tab in the palette, click + to create a new activity select the appropriate template from the list.

The Activity Designer form appears, with a stage indicator at the top. All new activities start at the General stage. The current stage shows with a blue underscore.

3. Add the general properties. This information is standard for each custom activity, include a name, description, and other related information.
4. Create the template **Create input variables** for the template.
   Create the variables to pass into the activity in the Inputs form of the activity designer.

5. Optional: Add a **pre-processing script**.
   For input validation or transforming input data, you might need a pre-processing script.
   
   **Note:** This step is not included in the Run Script activity.

6. Click **Continue** to open the **Execution Command** form, then fill out the **Execution Command** step based on the corresponding execution templates:
   - Create a SOAP web service activity
   - Create a JDBC activity
   - Create a JavaScript Probe activity
   - Create a PowerShell activity
   - Create a REST web service activity
   - Create a Probe activity
   - Create an SFTP activity
   - Create a Run Script activity
   - Create an SSH activity
   - Create a JMS activity

7. Optional: **Test your inputs**.

8. Optional: In the **Outputs** form, define local and/or output variables.
   Local variables can be used for temporary storage when cascading parsing rules. For example, you might extract an XML payload from within a JSON payload. A local variable can access the XML document and use that as a source for another parsing rule. The graphic shows a **Local1** variable source to parse data for **Output2**.

   ![Define local variable]

9. Use one of the options to assign values to Outputs:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parsing rule</td>
<td>You can create a parsing rule and map them to the output fields by dragging and dropping the variables into the parsing rules structure. The REST, SOAP, and JDBC templates provide auto-mapping to create the parsing rules automatically. If available from the test inputs form, auto-mapping should be used when possible.</td>
</tr>
</tbody>
</table>
Post-processing

Post-processing scripts allow you to code your own output data validation, output parsing code, and related tasks. Post-processing executes after the execution command results have been returned and before the parsing rules and conditions are run. Click Go to Post-Processing (Advanced) to create a post-processing script.

Note: If you create a script, this step reflects as a stage in the indicator.

10. Click Continue to open the Conditions form to create exit condition rules for your activity and then click Save.

General properties for activity designer templates

The following General Property fields are common to all activity designer templates.

General Property fields common to all activity designer templates

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Descriptive name of the activity. Select a unique name that makes the activity easily identifiable in the palette. If you do not name the activity, it is identified in the Data tab of the workflow editor with an index number when it is added to a workflow. This index reflects the order in which the custom activity was added to the workflow. Only custom activities and their output variables appear in the Data tab.</td>
</tr>
<tr>
<td>Short description</td>
<td>Brief description of what the activity does.</td>
</tr>
<tr>
<td>Image</td>
<td>Icon that identifies an activity of this type in the workflow palette.</td>
</tr>
<tr>
<td>Execution template</td>
<td>Predefined template selected for this activity.</td>
</tr>
<tr>
<td>Application</td>
<td>Current scope set on the instance. To view the scope, click the gear icon on the right side of the title bar in any record or list and look at the value in the Application field. The activity runs in this scope within a workflow. You cannot view or change the scope for the instance in the workflow editor.</td>
</tr>
<tr>
<td>Accessible from</td>
<td>Accessibility setting for this activity, by scope. The following options are available:</td>
</tr>
<tr>
<td></td>
<td>• All application scopes: This activity is available to all application scopes.</td>
</tr>
<tr>
<td></td>
<td>• This application scope only: Use of this activity is restricted to the scope named in the Application field.</td>
</tr>
<tr>
<td>Category</td>
<td>Category for this activity in the Custom and Packs tabs. All categories are listed under their scope in the collapsible hierarchy.</td>
</tr>
<tr>
<td>Description</td>
<td>Detailed description of the activity.</td>
</tr>
</tbody>
</table>
Create input variables

Create the variables to pass into the activity in the Inputs form of the activity designer. You must name your activity in the General form before you can advance to the Inputs stage. Roles required: workflow_admin or activity_creator

Note: Variable strings in the Inputs form have a 255 character limit.

1. Click the + icon to create a new input variable.
   The designer creates a default variable called Input1.

2. Type your new variable name in the field.
3. To change the name of a variable or any of its attributes, double-click the value and then select or enter a new value in the field that appears.
4. Configure your variable using these fields:
Variable configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Data type for this variable. Double-click on the field to display the choice list. In addition to the usual data types, you can create input arrays and encrypt individual variables that contain sensitive data. Encrypted variables are passed to the ECC Queue and then decrypted by the MID Server when they run on the target host. Sensitive data returned from running these variables on the host can then be passed to another activity through encrypted output variables.</td>
</tr>
<tr>
<td>Mandatory</td>
<td>Marks an input variable as mandatory. Variables marked as mandatory are required fields in the properties form for the activity in the workflow. The input testing feature allows you to filter on mandatory variables.</td>
</tr>
<tr>
<td>Default</td>
<td>Default value for this input variable. Default values are prepopulated for variables in the properties form for the activity in the workflow. You can override this value when you test the variables.</td>
</tr>
</tbody>
</table>

5. To reorder the variable list, select a row and then drag the row to its new location.
   When you select a row to move it, the pointer icon changes to an up/down arrow icon (\(\uparrow/\downarrow\)).

6. To delete a variable, click the delete icon (\(-\)) in the row.

7. Click **Continue** to advance to the **Execution Command** stage or click **Go to Pre-Processing (Advanced)** to create a script that runs before the activity executes.

Map an input variable
After you create the input variables, map them to the fields in the Execution Command form.

Role required: activity_admin, activity_creator

These fields contain values required by the target host or endpoint to authenticate and query for data. Included in this example are fields for a command to run on the target and the MID Server to use, if one is required.

To map a variable, drag it into the appropriate field.

The designer automatically expresses the variable in the syntax the system requires.
Configure the PowerShell execution command

Use the input variables you created to configure the command that Orchestration executes on the Windows target machine.

Create the input variables you need in the Inputs form before you can advance to the Execution Command stage.

Role required: activity_creator, admin

**Note:** You can test the PowerShell connection between the MID Server and the target computer without having to run the activity in a workflow context. For details, see *test template outputs*.

1. Drag variables from the list of inputs and drop them into command fields. The system formats the variable in the proper syntax for the command.
PowerShell execution command

2. Complete the fields shown in the table.

### Powershell command fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>Input variable builder. Create variables to map to available fields.</td>
</tr>
<tr>
<td>Target host</td>
<td>Host name or IP address of the target server for this PowerShell activity.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Script type            | Type of script to run on the PowerShell host. Available options are:  
|                        | - Custom Powershell command  
|                        | - MID Server script file                                                             |
| MID Server script file | MID Server script file to run. This field is available when the Script type selected is MID Server script file.                          |
| Command                | Command that this activity runs on the target host. This field is available when the Script type selected is Custom Powershell command. You can drag and drop input variables from the variable builder into this field to create your command. |
| Powershell variables   | Name-value pairs to pass to the host with Powershell. You can create these variables manually, or drag input variables into the Value field. Encrypted input variables retain their encryption, regardless of the data type settings in this field. If you type in a value and select the Encrypted data type, your value appears in plain text in this field and is only encrypted when it passes to the ECC Queue. |
| Use MID service account| Forces this activity to authenticate on the target host using the credentials of the MID Server service account only, without trying any other credentials. When this check box is selected, the Credential tag field is not available. |
| Credential tag         | Specific credential tag this activity must use to run Powershell commands on the host. If this field is left blank, the MID Server tries all the available credentials until it finds a valid one, ending with the MID Server service account. If a credential tag is defined, the MID Server tries the credentials for that tag only and does not try the MID Server service account. This field is not available when the Use MID service account check box is selected. |
| Required MID Server capabilities | MID Server to use for querying Powershell, by capabilities. By default, the system selects a Powershell MID Server. |

3. Click **Save**.
4. Click **Continue** to advance to the **Outputs** stage.

**Test activity template inputs**

You can test the input parameters of a custom activity during its development without having to run the activity in a workflow context.

Create input variables and map them to fields in the **Execution Command** form or provide actual values for these fields.

Role required: web_service_admin, activity_admin, activity_creator
An input test executes only the input parameters against an endpoint and not the pre-processing or post-processing scripts. You need to use a workflow to test a pre-processing or post-processing script. You do not need to check out the activity to test it, and you can test input variables from any stage in the activity designer, if your activity is properly configured. Typically, the **Execution Command** stage is the point at which your inputs are ready for testing.

**Note:** If you intend to use auto-mapping, you must test your input variables.

1. **Click Test Inputs.**

   The list of input source variables appears. If you added default values for these variables, those values appear in the **Substitute Value** column. Mandatory variables are marked with a red star. In this example, a SOAP endpoint returns a value for a stock quote variable.

   ![Fill in your test values](image)

2. Filter the variable list with these controls:
   - **All Inputs**: Displays all input variables. This is the default view.
   - **Mandatory Inputs**: Displays only mandatory input variables.
   - **Inputs Without Defaults**: Shows input variables that do not have assigned default values.

3. Reset values as needed.
   - **Reset default values**: Replaces any test values set in this form with the default values, if they are present.
   - **Clear values**: Clears all values in the input variable list, even if default values exist.

4. When your test values are configured correctly, click **OK**.

   The system runs the values for all the inputs configured against the specified target and returns the resulting payload. The buttons in the Response form display different views of the payload. The entire payload appears in the **Raw Output** window.
5. To map appropriate parameter values in the payload to variables in the Outputs stage automatically, select an auto-mapping option.
6. Alternately, you can click Save for parsing rules to copy the entire payload to the parsing rules.
This allows you to manually select values for the output variables directly from the payload. This action completely overwrites any previous payload that existed in the parsing rules.

7. Click the X in the upper right corner of the window to close it.

Data encryption for activity variables

You can protect sensitive data passed from Orchestration activities by encrypting input and output variables.

The system never stores encrypted variables as clear text. If the MID Server is used to fulfill the activity, the corresponding ECC Queue’s input payload is encrypted if an encrypted output variable is defined in the template. Output variables passed to a downstream activity as input variables maintain their encryption throughout processing.

Inputs that require data encryption come from one of these sources:

- Workflows: These inputs are provided through the Workflow Editor and must be in the password2 format for two-way encryption.
- Service catalog requests: These input values are provided to an activity as encrypted variables from a service catalog item.
- GlideRecord: These are variables attached to any ServiceNow table. The source column in the table must be a password2 type variable.
- Activity outputs: These are variables passed as outputs from one activity to a downstream activity as inputs, through the data bus.
- Empty string: The system allows you to define encrypted input variables but never pass a value into the variable.

Activity designer template pre-processing fields

Use the Pre Processing form of the activity designer to define a script to run before the activity executes.

Pre-processing fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input process script</td>
<td>Script to run before the activity executes.</td>
</tr>
<tr>
<td>Variables</td>
<td>Input variables that are available to use as building blocks in the input process script. Click the arrow above the field to open the variables list. Click an item in the tree to add it to your script in the appropriate syntax. The list displays execution parameters and input variables you passed into the activity on the Inputs form. All activity variables added in the Inputs form are read-only and are expressed in the pre-processing script with this syntax: activityInput.variable. Before the activity executes and makes a call to the service or host, you can override the effective execution value of this variable by assigning values to the executionParam.variable_name execution parameter. Refer to the specific execution parameters for your template.</td>
</tr>
</tbody>
</table>
Logging

Activity designers can add logging to the pre-processing using the `ActivityLogger` API, which works for scoped or global applications. Logged data from the script appears in the Workflow Log related list in the context records for any workflow that uses the activity. The `Source` for these messages in the workflow log is `ACTIVITY`.

**Important:** To display the debug messages in the workflow log, set the `glide.workflow.log.debug` property to `true`.

The supported messages are:

- `ActivityLogger.debug("Pre Processing Log Message");`
- `ActivityLogger.info("Pre Processing Log Message");`
- `ActivityLogger.warn("Pre Processing Log Message");`
- `ActivityLogger.error("Pre Processing Log Message");`

Template post-processing fields

From the Post Processing form in the activity designer you can define a script to run after the activity executes.

**Post-processing fields**

To use the results returned by the activity, append the `executionResult.` prefix to these parameters.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output process script</td>
<td>Script to run after the activity executes.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Variables</td>
<td>Input variables that are available to use as building blocks in the output process script. Click the arrow above the field to open the variables list. Click an item in the tree to add it to your script in the appropriate syntax. The list displays execution results and the variables you passed into the activity on the Inputs form. All activity variables added in the Inputs form are read-only and are expressed in the post-processing script with this syntax: activityInput.variable. For parameter descriptions, refer to the table in the post-processing parameters topic for this activity.</td>
</tr>
</tbody>
</table>

### Logging

Activity designers can add logging to the post-processing script using the `ActivityLogger` API, which works for scoped or global applications. Logged data from the script appears in the Workflow Log related list in the context records for any workflow that uses the activity. The Source for these messages in the workflow log is ACTIVITY.

**Important:** To display the debug messages in the workflow log, set the `glide.workflow.log.debug` property to true.

The supported messages are:

- `ActivityLogger.debug("Post Processing Log Message");`
- `ActivityLogger.info("Post Processing Log Message");`
- `ActivityLogger.warn("Post Processing Log Message");`
- `ActivityLogger.error("Post Processing Log Message");`

Enter a script to run after the activity executes but before conditions are processed. Click on various places to add elements.

Output process script

```
ActivityLogger.error("Post Processing Log Message");
```
Auto-map activity output variables

You can map parameter values in a test payload to variables in the Outputs tab automatically.

Role required: admin

1. From the Execution Command in the template, select the Inputs tab.
2. Click Test Inputs to test the input parameters.
   
   If you added actual values for the parameters and fields, the system runs those values against the specified target and returns the resulting payload. If you mapped input variables to fields and parameters, the system displays a dialog box for assigning test values to those variables.

3. Provide test values, if requested, and click OK to display the payload.
   
   The entire payload appears in the Raw Output tab of the Response form.

   ![Response Form](image)

4. Select an auto-mapping option:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-Map to Local</td>
<td>Translates the entire payload into a JSON object and places it in the data bus. This allows for post-processing manipulation in JavaScript. This selection causes the entire data field on the right to disappear and the inputs structure to be auto-populated with these default variables: output, totalRows, errorMessage, eccSysId</td>
</tr>
<tr>
<td>Auto-Map to Output</td>
<td>Automatically populates the output variables in the activity with the same default variables used as inputs for the local variable.</td>
</tr>
</tbody>
</table>

   **Note:** No parsing rules are available with auto-mapping selections.

Create an output variable

The Outputs form in the designer contains a variable builder for creating data structures of objects and arrays.

Roles required: activity_admin, activity_creator
Elements in this structure are mapped with a parsing rule to specific data contained in payloads returned from an endpoint or host. These variables and their values are then made available locally or for reuse in other activities.

1. Click the + icon in the Outputs column to create a local or output variable.

   Local variables are only available within an activity and are not visible in the data structures displayed in the Custom tab. Output variables are available for reuse in other activities, either individually or as an entire data structure. When you create a new variable of either type, the designer provides a default name of Local1 or Output1.

2. Type your new variable name in the field and select a data type.

   Variable names must be unique within an array or an object. You can assign a data type of Encrypted to output variables that contain sensitive data. Data protected by encryption is passed to other activities or processes encrypted and is never displayed in plain text.

3. To change the name of a variable or any of its attributes, double-click the value, type a new value in the editing field, and then press Enter.

   The icon to the left of the name reflects the data type of the variable.

4. To reorder the variable list, select a row and then drag the row to its new location.

   When you select a row to move it, the pointer icon changes to an up/down arrow icon.

5. Drag and drop the row into another location.

6. To reuse a variable from another activity, drag it from the Custom tab in the palette and drop it onto the Local or Output heading at the top of the variable list. To copy an entire data structure, drag the parent object or array into the variable list header.

   The designer duplicates the copied data structure in the outputs variable builder.
Reuse of data structures

7. To delete a variable, click the delete icon (−) in the row.

Activity designer template outputs
Output variables contain messages returned from a destination that are available to other activities in a workflow or internally to the activity.

Activity designer output fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Variable name</td>
<td>Name of a variable, either <strong>Local</strong> or <strong>Output</strong>, that this activity passes.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Local</td>
<td>Variable that contains a value used within an activity. For example, use a local variable to identify metadata that is processed within an activity before the final value is exported to an output variable.</td>
</tr>
<tr>
<td>Output</td>
<td>Variable that contains a value that is passed to other activities in the workflow.</td>
</tr>
</tbody>
</table>

**Map an output field**

Mapping is configured with parsing rules that allow you to build expressions in the appropriate data format for the selected payload.

Role required: activity_admin, activity_creator

When you are finished creating the output data structure, map each variable to the specific data you want to extract from the target host.

To map a variable, drag it from the Outputs variable builder and drop it into an empty **Variable name** field in the Parsing rules section.

See [create a parsing rule](#) for instructions on configuring parsing for output variables.
Create a parsing rule

Populate output variables defined in a custom activity with payload data returned from an inputs test on an external host or endpoint.

Roles required: activity_admin, activity_creator

1. Navigate to **Workflow > Workflow Editor**.
2. From the **Custom** tab in the palette, open a custom activity.
3. In the Activity Designer form, advance to the **Output** stage.
4. Drag an output variable from the data structure builder into the **Variable name** field in the Parsing rules builder.
Mapping variables to parsing rules

The parsing rules form appears for the selected variable. By default, the parsing type is set to **Direct**, which populates the variable with all the data from the selected payload, without parsing the contents. Each template has a specific default **parsing source**.

5. Complete the form using the fields in the table.

In this example, the parsing type selected is **XML**, which allows you to select specific parameters from the payload to parse.
Parsing rule for localBody

Parsing source: executionResult.body

Variable Name: activityLocal.localBody

Parsing Type: XML

Expression: $age

Parse sample data

Sample payload data:

```xml
<xml version="1.0"?>
<data>
  <user>
    <name>user one</name>
    <age>42</age>
  </user>
  <user>
    <name>user two</name>
    <age>27</age>
  </user>
  <user>
    <name>user three</name>
  </user>
</data>
```

Parsing result:
27
### Parsing rules fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parsing source</td>
<td>Source of the data returned from the target host or endpoint. Each template opens to a specific, default payload. Available choices depend on the execution template selected for the activity. You can also use local variables as a parsing source if a parsing rule has previously been defined for them. For a list of the available payloads for each template, see <a href="https://docs.servicenow.com/app/doc/activity-designer-parsing-sources">Activity designer parsing sources</a>.</td>
</tr>
<tr>
<td>Expression</td>
<td>Expression used to extract specific data from the selected parsing source. This expression is created from clickable data in the sample payload and appears in the format selected in the Parsing type field. When testing, the expression can return multiple results. Discern which choice gives reliable or predictable results before choosing your expression. Note: The system cannot generate clickable RegEx expressions from sample data. You must write all regular expressions manually.</td>
</tr>
<tr>
<td>Variable name</td>
<td>Revised variable name as it is used in the final output expression. The system adds the activityOutput or activityLocal prefix to the variable you specify.</td>
</tr>
<tr>
<td>Parsing type</td>
<td>The language to use for querying the target host’s payload. The selections are:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Direct</strong>: Maps to the entire content of the payload selected in the Parsing source field, without any parsing. This is the default parsing type.</td>
</tr>
<tr>
<td></td>
<td>- <strong>XML</strong>: XPath query used for selecting nodes from an XML payload.</td>
</tr>
<tr>
<td></td>
<td>- <strong>JSON</strong>: JSONPath query for selecting parts of a JSON payload.</td>
</tr>
<tr>
<td></td>
<td>- <strong>RegEx</strong>: Parsing method that uses a regular expression to extract data from a payload. The RegEx parsing type does not support multi-line parsing and is not case sensitive.</td>
</tr>
<tr>
<td>Short description</td>
<td>Brief description of this parsing rule.</td>
</tr>
<tr>
<td>Sample payload data</td>
<td>Sample data from the source containing the data requested. This field is not available for Direct parsing types. After you click Parse sample data, the data in this field cannot be edited, but becomes clickable for the purpose of creating expressions. Click Edit sample data to make the field editable again.</td>
</tr>
</tbody>
</table>
6. To retest the inputs, click **Get sample payload from test**. This action reopens the test form, allowing you to substitute different test values and create a different payload.

7. Click **Save** to have the parsing rules overwrite the previous payload with the one you just created.

8. To create an expression for the parsing rule, click the specific parameter you want to see in the sample payload. The value for that parameter appears in the Parsing result field, and the system creates the appropriate expression in the Expression field.

9. Click **Submit** to save the parsing rule for that variable.

**Activity designer parsing sources**
This table lists the parsing sources available with each execution template.

<table>
<thead>
<tr>
<th>Parsing sources</th>
</tr>
</thead>
</table>

### Template | Source |
|-------------|--------|
| SOAP Web Service | executionResult.body (Default)  
executionResult.status_code  
executionResult.header  
executionResult.error |
| JDBC | executionResult.output (Default)  
executionResult.errorMessages  
executionResult.probeCompletedEccId  
executionResult.totalRows |
| JavaScript Probe | executionResult.payload (Default)  
executionResult.output  
executionResult.eccSysId  
executionResult.errorMessages |
| Powershell | executionResult.output (Default)  
executionResult.tags  
executionResult.hresult  
executionResult.eccSysId  
executionResult.errorMessages |
| REST Web Service | executionResult.body (Default)  
executionResult.status_code  
executionResult.header  
executionResult.error |

© 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.
## Activity designer parsing rule example

In this example, the parsing rule is configured to populate the `activityOutput.ipv4` variable with the value for the IP address from a domain server, using PowerShell.

**Role required:** activity_creator, activity_admin

To generate the sample data, the administrator must actually run the command on the host and then paste the data returned into the **Sample payload data** field when creating the parsing rule. The administrator can then create an expression that returns IP addresses from that sample in two formats: `ipv4` and `ipv6`. In this example, the system produces two expressions to use for the parsing rule.

1. Navigate to **Workflow > Workflow Editor** and open the activity that runs on the host.
2. Click the **Inputs** tab, and note the **Command**.

### Template | Source
---|---
SFTP | • executionResult.output (Default)  
            • executionResult.eccSysId  
            • executionResult.errorMessages  
            • executionResult.tags  

Probe | • executionResult.output (Default)  
               • executionResult.payload  
               • executionResult.eccSysId  

SSH | • executionResult.output (Default)  
           • executionResult.eccSysId  
           • executionResult.errorMessages  
           • executionResult.tags  

JMS | • executionResult.status  
           • executionResult.standardHeaders  
           • executionResult.customHeaders  
           • executionResult.messagePayload  
           • executionResult.eccSysId  
           • executionResult.errorMessages
3. In a PowerShell console, run the **Command** on the host to extract the XML sample that contains the values you need.

4. Copy the data that is returned to the clipboard.

5. In the activity designer, click the **Outputs** tab and paste the returned data into the **Sample payload data** field.

   In this example, the data includes IP addresses in two different formats and the domain name.

6. Select the parsing type for the source. In this example, select **XML**.
7. Click **Parse sample data**.

The system displays the XML in the proper format, and it becomes clickable. In this view, the system can translate clicked data from the sample into an expression.
8. To create the expression, click the elements in the data sample you want to map to the variable.

Based on the sample data you clicked, the system creates two expressions.
9. Select an expression from the list.

The desired result is the IP address that has a \textit{type} attribute of \texttt{ipv4}. The system populates the \texttt{Expression} field with this choice.
10. **Click Test expression.**

The system parses the payload using the selected expression and returns the requested data in the **Parsing result** field.
11. Click **Submit**.

The view returns to the **Outputs** tab of the activity designer. The new parsing rule is listed, and a blank row is available for another rule.
Activity conditions

Create the exit conditions for your activity in the Condition column and set the order for each..

The system evaluates the condition with the lowest order number first and stops when it finds the first true condition. The system delays evaluation of conditions with an Else value set to true until all conditions with an Else value set to false are evaluated. If the system does not find a true condition, it looks for a default condition in which the value for Else is true and takes this exit. You must have at least one default exit condition, or the activity hangs when the workflow runs.

The following are possible conditions you might create for an activity:

Sample activity conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Tests for a success condition. Else is set to false and the Order is set to 100. If this condition is true, the activity takes the Success exit. If this condition is false, the system evaluates the next condition in order.</td>
</tr>
<tr>
<td>Retry</td>
<td>Tests for a condition that runs the activity again. Else is set to false. If this condition is true, the activity runs again. If this condition is false, the system takes the default Failure exit.</td>
</tr>
<tr>
<td>Failure</td>
<td>Default condition that allows the workflow to continue if the other conditions in the activity are false. Else is set to true.</td>
</tr>
</tbody>
</table>
Orchestration custom activity templates

Orchestration provides customizable activity templates to create and manage custom activities in the workflow editor.

You create and update different types of Orchestration activities with the Activity Designer using activity templates for SSH, PowerShell, REST, SOAP, JMS, SFTP, JDBC, JavaScript Probes, and Probes.

Hundreds of workflows can share these activities simultaneously. Before you change an activity, you should check the workflows that they are part of by clicking the form menu icon and selecting Used In. Any central change to a versioned activity automatically updates across workflows unless you have pinned that activity.

All the Orchestration Core activities are built using the Activity Designer in scoped applications. Custom activities can be developed in the global scope or their own application scope even if that scope is different from the scope of the workflow. Use Activity scoping when build your own activity packs.

Create a JDBC activity

Create a custom JDBC activity to automate SQL commands and stored procedure calls to relational databases from workflow.

Role required: activity_admin, activity_creator

The JDBC activity template allows you to execute ANSI SQL statements or stored procedures on a target database. Support for stored procedures with IN, OUT, and INOUT parameters are available in Jakarta. To learn how to set up these parameters, see JDBC stored procedure parameters.

Note: If you are transferring bulk data into a ServiceNow instance from an external data source, use Import sets. The JDBC activities allow you to transfer data between external...
data sources and ServiceNow within a workflow. It is not intended to replace the bulk import features of data sources.

1. Create or verify your **JDBC credential**.
   Your JDBC credentials must have permission for the target database and proper configuration for the corresponding JDBC connection. Credentials must be set up before you can create a JDBC activity.

2. Create or verify your **JDBC connection**.
   Your JDBC connection must be configured with valid JDBC credentials set up before you can create a JDBC activity.

3. Create a **custom activity**.
   This action creates a custom activity using a template.

4. After setting up general properties and creating input variables, configure the JDBC Execution Command:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>JDBC Connection</strong></td>
<td>Configure or reference the appropriate JDBC Connection for the database. The connection selected provides the activity with the following information:</td>
</tr>
<tr>
<td></td>
<td>• Target database information (server and database names)</td>
</tr>
<tr>
<td></td>
<td>• Connection URL</td>
</tr>
<tr>
<td></td>
<td>• Target database port (if different from standard port number)</td>
</tr>
<tr>
<td></td>
<td>• Database instance name</td>
</tr>
<tr>
<td><strong>Credential</strong></td>
<td>JDBC credential to use for your JDBC connection.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SQL statement</td>
<td>Input the ANSI SQL to execute on the JDBC target database.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This field is hidden when the Stored Procedure check box is selected.</td>
</tr>
<tr>
<td></td>
<td>You can map the input variables you created to configure the SQL statements. By default, you can run the following SQL statements.</td>
</tr>
<tr>
<td></td>
<td>- select</td>
</tr>
<tr>
<td></td>
<td>- insert</td>
</tr>
<tr>
<td></td>
<td>- update</td>
</tr>
<tr>
<td></td>
<td>- delete</td>
</tr>
<tr>
<td></td>
<td>- show</td>
</tr>
<tr>
<td></td>
<td>- create</td>
</tr>
<tr>
<td></td>
<td>- describe</td>
</tr>
<tr>
<td></td>
<td>For added security measure, a MID Server property controls the operations that this JDBCOrchestrationProbe executes, which restricts the SQL commands used. This property protects against potentially destructive commands, such as drop database. The mid.property.jdbc_operations contains the MID Server property controls.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You cannot run multiple statements of different types. For example, you cannot run a select statement and an update statement together, but you can run two insert statements. However, you cannot run multiple select statements in this activity.</td>
</tr>
<tr>
<td>Maximum rows</td>
<td>Maximum number of records to retrieve from database. The default is 1000.</td>
</tr>
<tr>
<td>Maximum payload size (KB)</td>
<td>You can set a limit on the maximum payload size of data retrieved from the database. The default is 64 kilobytes.</td>
</tr>
<tr>
<td>Connection timeout</td>
<td>How long the activity waits to make the connection. This field is populated automatically from the data source, but can be changed for this activity.</td>
</tr>
<tr>
<td>Query timeout</td>
<td>Elapsed time to wait after running the query until the data is returned. This field is populated automatically from the data source, but can be changed for this activity.</td>
</tr>
<tr>
<td>Required MID Server capabilities</td>
<td>MID Server to use for querying JDBC, by capabilities. By default, the system selects a MID Server that has JDBC capability.</td>
</tr>
<tr>
<td>Use stored procedure</td>
<td>If checked, you can run a stored procedure on MySQL, Oracle, or SQL Server databases by entering the procedure name and parameters. See JDBC stored procedure parameters.</td>
</tr>
</tbody>
</table>
**Note:** You can map parameter values in a test payload to variables in the Outputs tab automatically. See [automap output variables](#).

- Test JDBC activity inputs
- Use auto-mapping to generate outputs and parsing rules (recommended for JDBC)
- If you do not use auto-mapping, you can manually create output variables and create parsing rules

Create a JDBC connection for an Orchestration activity

The JDBC Connection (jdbc_connection) table provides the information custom JDBC Orchestration activities use to connect to various target databases.

You must have an appropriate JAR file, whether it is supplied with the instance or a custom JAR file.

**Note:** The ServiceNow instance supplies mysql-connector-java-5.1.21.jar, sql-server-jdbc-4.0.jar, and ojdbc6.jar files as part of the current release, which supports MySQL, SQLServer, and Oracle databases. Other databases, such as Sybase or DB2 Universal, must use a custom JAR file that must be uploaded to the instance before setting the JDBC connection.

Role required: activity_admin, activity_creator

JDBC credentials are retrieved separately by the activity designer template and support external credential storage, such as CyberArk.

1. Navigate to Orchestration > Credentials & Connections > JDBC Connections and click New.
2. Complete the form using the fields in the table.

The database selection in the Format field determines which fields are available.

### JDBC connection fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Database Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>All</td>
<td>Unique name of this JDBC connection. For example, you might enter JDBC MySQLProd.</td>
</tr>
<tr>
<td>Query timeout</td>
<td>All</td>
<td>Maximum elapsed time the JDBC query is allowed to run without a response.</td>
</tr>
<tr>
<td>Connection timeout</td>
<td>All</td>
<td>Maximum elapsed time for the JDBC activity to wait while attempting to connect to the target database.</td>
</tr>
<tr>
<td>Application</td>
<td>All</td>
<td>Scope for this table. By default, the JDBC Connection (jdbc_connection) table runs in the Global scope.</td>
</tr>
<tr>
<td>Domain</td>
<td>All</td>
<td>Domain for this table. By default, the JDBC Connection (jdbc_connection) table runs in the global domain.</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>Database Format</th>
<th>Description</th>
</tr>
</thead>
</table>
| Format        | All             | Database type for this connection. The default choices are:  
|               |                 | • MySQL  
|               |                 | • Oracle  
|               |                 | • SQLServer  
|               |                 | • None  
|               |                 | You can add Sybase or DB2 Universal to the choice list by uploading the appropriate JDBC driver JAR file to the instance. Orchestration automatically recognizes these drivers when they are loaded into the system and adds them to this list. |
| Server        | Oracle, MySQL, SQLServer | Host name or IP address of the database server.                                                                                                          |
| Oracle sid    | Oracle          | The Oracle database site identifier. The default value is orcl.                                                                                     |
| Oracle port   | Oracle          | Port that the Oracle database is using. The default value is 1521.                                                                                |
| Database name | MySQL, SQLServer | Name of the database.                                                                                                                               |
| Database port | MySQL, SQLServer | Port that the selected database is using.                                                                                                           |
| Instance name | SQLServer       | Instance name for the selected SQLServer                                                                                                             |
| Connection URL | All             | URL that the MID Server uses to connect to the specified database. The URL is created automatically when you save the form, and is read-only for the default databases. |
|               |                 | **Note:** If the format selected is not one of the default databases, you must create the connection URL manually so that the MID Server knows how to create the connection. |
| JDBC driver   | None, DB2 Universal, Sybase | The JDBC driver to use for this connection when it is not a default database.                                                                      |
|               |                 | **Note:** If you add a Sybase or DB2 Universal database, you must enter the driver name in this field and upload the driver JAR file to the instance. |
JDBC connection to Oracle example

3. Click **Submit**.

**Auto-map JDBC activity output variables**

The ServiceNow activity designer allows you to map parameter values in a JDBC test payload to variables in the **Outputs** tab automatically.

Role required: **admin**

1. In the JDBC provider template form, select the **Inputs** tab.
2. Click **Test Activity** to test the input parameters.
   - If you added actual values for the parameters and fields, the system runs those values against the specified target and returns the resulting payload. If you mapped input variables to fields and parameters, the system displays a dialog box for assigning test values to those variables.
3. Provide test values, if requested, and click **OK** to display the payload.
   - The entire payload appears in the Raw Output tab of the Response form.
4. Select one of these auto-mapping options.
   - **Auto-Map to Local**: Directly maps values to a local variable for use within the activity.
   - **Auto-Map to Output**: Directly maps values to the output variable to pass to other activities in the workflow. Auto-mapping to an output variable creates an array of objects, each of which contains the column names from the query result.

**JDBC stored procedure parameters**
You can use Orchestration to run a stored procedure on MySQL, Oracle DB, and MS-SQL databases.

There is support of multiple data types, with the following limitations:
- Only one result-set is returned.
- The order of input and output data types in the stored procedure parameters must match the activity definition.
- Binary, Blob, Varbinary, and LongBinary should be base64 encoded.
- Date, Time, and Timestamp have a specific format:
  - **Date format**: `yyyy-mm-dd`
    `yyyy-mm-dd` is the supported format.
  - **Time format**: `hh:mm:ss.(sss)`
    `hh:mm:ss.(sss)` is the supported format. Precision is in milliseconds only, microseconds or nanoseconds cannot be handled.

**Note:** `10:30:59` and `10:30:59.999000` are correct but `10:30:59.` is incorrect.

- **Timestamp format**: `yyyy-mm-dd hh:mm:ss(.ffffff)`
  `yyyy-mm-dd hh:mm:ss(.ffffff)` is the supported format. Precision is to microseconds.
- ResultSet is the first result set coming back from database server.
- MS-SQL does not support INOUT parameters. If you use INOUT parameters, the Activity Template transparently maps them to OUT parameters.

**Note:** If you do not want to do a validation of data types in stored procedure parameters, like the legacy behavior, you set the `glide.stored_proc.data_type.validation` as false. See *MID Server properties* for instructions.
### Stored procedure parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Mode** | Type of stored procedure parameter. Supported parameters:  
- IN  
- OUT  
- INOUT |
| **Sql Type** | A SQL data type. Supported data types:  
- ARRAY  
- BIGINT  
- BINARY  
- BIT  
- BLOB  
- CHAR  
- CLOB  
- DATE  
- DECIMAL  
- DISTINCT  
- DOUBLE  
- FLOAT  
- INT  
- INTEGER  
- JAVA_OBJECT  
- LONGVARBINARY  
- LONGVARCHAR  
- NULL  
- NUMERIC  
- OTHER  
- REAL  
- REF  
- REF_CURSOR  
- SMALLINT  
- STRUCT  
- TIME  
- TIMESTAMP  
- TINYINT  
- VARBINARY  
- VARCHAR |
| **Name/Value** | Name-value pairs to pass to the host. You can create these parameters manually, or drag and drop input variables into the parameter fields and assign a value. |

**Note:** Not all database providers support the entire realm of JDBC data types. Reference your database reference manual to understand the supported datatypes for your installation.

---

**Test JDBC activity template inputs**

You can test the input parameters of a custom JDBC activity during its development without having to run the activity in a workflow context.
Create input variables and map them to fields in the Execution Command form or provide actual values for these fields. Role required: web_service_admin, activity_admin, activity_creator

This test executes only the input parameters against an endpoint and not the pre-processing or post-processing scripts. It is not necessary to check out the activity to test it.

**Note:** If you provide enough information for Orchestration to contact the endpoint or host and return data, you can test the input variables. You can test from any stage in the activity designer. Typically, the Execution Command stage is the point at which your inputs are ready for testing.

1. From the JDBC Execution Command, click **Test Inputs**.
   
   The list of input source variables appears. If you added default values for these variables, those values appear in the **Substitute Value** column. Mandatory variables are marked with a red star.

   **Note:** The test fails if the MID Server cannot be found or if it cannot connect to the target.

   ![Fill in your test values](image)

   **JDBC input test values**

   2. Filter the variable list with these controls:
- **All Inputs**: Displays all input variables. This control is the default view.
- **Mandatory Inputs**: Displays only mandatory variables.
- **Inputs Without Defaults**: Shows input variables that do not have assigned default values.

3. Reset values as needed.
   - **Reset default values**: If values are present, this control replaces any test values set in this form with the default values.
   - **Clear values**: Clears all values in the input variable list, even if default values exist.

4. When your test values are configured correctly, click **OK**.
   The system runs the values for all the inputs configured against the specified target and returns the resulting payload. The buttons in the Response form display different views of the payload. The entire payload appears in the **Raw Output** window.
5. To map appropriate parameter values in the payload to variables in the Outputs stage automatically, select an **auto-mapping option**.

6.
7. Click the X in the upper right corner of the window to close it.

Create a SOAP web service activity

Use this template to create a custom SOAP activity.
Role required: web_service_admin, activity_admin, activity_creator
For instructions on using the activity template process flow, see create custom activities.

1. Create a custom activity.
   This action creates a custom activity using a template.

2. After setting up general properties and creating input variables, configure the SOAP web service Execution Command:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Map the input variables</td>
<td>Use the variables you created to configure the command that Orchestration executes on the SOAP web service.</td>
</tr>
<tr>
<td>Web service message</td>
<td>Specify the SOAP web service message to use for this activity. If you need information on SOAP web services messages, see SOAP message.</td>
</tr>
<tr>
<td>Web service message function</td>
<td>Specify the SOAP message function available in conjunction with the SOAP web service.</td>
</tr>
<tr>
<td>Endpoint</td>
<td>If you enter an endpoint in this field, it overrides the endpoint URL configured in the SOAP message web service. Click the lock icon to open the input field and add the endpoint.</td>
</tr>
<tr>
<td>SOAP message parameters</td>
<td>Name-value pairs to pass to the SOAP endpoint. You can create these parameters manually, or drag input variables into the parameter fields and then assign a value. Parameters defined in the SOAP message that use ${ } can be assigned data from this activity template. Use the Additional attribute column to configure the system to not escape the text. By default, text sent to the SOAP message is escaped. The Name column is auto-populated if the users have provided variables using variable substitution in the SOAP message.</td>
</tr>
<tr>
<td>Use MID Server</td>
<td>Check box that determines if a MID Server must be used to invoke the SOAP web service. If the SOAP web service message function defines a MID Server, that MID Server is used instead of the one selected here.</td>
</tr>
<tr>
<td>Required MID Server capabilities</td>
<td>MID Server with the appropriate capabilities for connecting to the SOAP endpoint. By default, the system selects a MID Server with SOAP capabilities. This field is available when the Use MID Server check box is selected.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Allowed duration of the SOAP web service request before it times out, in seconds. The default is 10.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>Determines what type of authentication is required for the endpoint. The options are:</td>
</tr>
<tr>
<td>Use existing credentials in SOAP message</td>
<td>Uses credential definitions from the SOAP message definition.</td>
</tr>
<tr>
<td>Override with Basic Authentication credentials</td>
<td>Uses basic authentication credentials. Overrides the credentials in the SOAP message definition. Basic authentication credentials must be provisioned before they are available for selection.</td>
</tr>
<tr>
<td>Override with Certificate Authentication credentials</td>
<td>Overrides the credentials in the SOAP message definition with certificate authentication credentials.</td>
</tr>
<tr>
<td>Override with Both Basic and Certificate Authentication credentials</td>
<td>Overrides the credentials in the SOAP message definition with both basic authentication or certificate authentication credentials.</td>
</tr>
<tr>
<td>Override with WS-Security Username profile</td>
<td>Overrides the credentials in the SOAP message definition with credentials defined a WS Security Profile.</td>
</tr>
</tbody>
</table>

| **Credentials**                             | Required REST endpoint basic authentication credentials. This field is available when **Override with Basic Authentication credentials** is selected in the **Authentication** field. Only basic authentication credentials appear in the selection list, which includes credentials stored on the instance and credential IDs from an external storage system. If you are using credentials stored in a CyberArk safe, you can override the **default safe** defined in the MID Server configuration file by adding the name of a different safe as a prefix to the credential ID, separated by a colon. For example, newsafe:orch-test-f5. |

| **Protocol Profile**                        | Protocol profile to use for authentication. This field is available when the authentication type is either **Override with Certificate Authentication credentials** or **Override with Both Basic and Certificate Authentication credentials**. |

**Note:** You can map parameter values in a test payload to variables in the **Outputs** tab automatically. See automap output variables.

- Use **auto-mapping** to generate outputs and parsing rules (recommended for JDBC)
- If you do not use auto-mapping, you can manually create output variables and create parsing rules

**Auto-map SOAP activity output variables**

The ServiceNow activity designer allows you to map parameter values in a SOAP test payload to variables in the **Outputs** stage automatically.

Role required: web_service_admin, activity_admin, activity_creator
1. In the activity designer, proceed to the Execution Command stage.
2. Define an appropriate MID Server, if requested.
   The test fails if the MID Server cannot be found or if it cannot connect to the target.
3. Click Test Activity to test the input parameters.
   If you added actual values for the parameters and fields, the system runs those values against
   the specified target and returns the resulting payload. If you mapped input variables to fields
   and parameters, the system displays a dialog box for assigning test values to those variables.
4. Provide test values, if requested, and click OK to display the payload.
   The entire payload appears in the Raw Output tab of the Response form.

5. Select one of these auto-mapping options.
   - Auto-Map to Local: Directly maps values to a local variable for use within the activity.
   - Auto-Map to Output: Directly maps values to the output variable to pass to other activities
     in the workflow. Auto-mapping to an output variable creates an array of objects, each of
     which contains the column names from the query result.

Provide credentials to access a SOAP message WSDL
   If the SOAP WSDL you are requesting in a test payload requires authentication, you must provide
   basic auth credentials in either the SOAP message or the SOAP activity.
   Role required: web_service_admin, activity_admin, activity_creator
   The ServiceNow instance only supports basic auth credentials for accessing a WSDL. If the SOAP
   function or the SOAP message does not provide these credentials, you must configure them in the
   SOAP activity template. Orchestration uses these priorities for deciding which basic authentication
   credentials to use:
   - SOAP message: Credentials for a SOAP message are used if no other credentials are defined.
   - SOAP function: Credentials for a SOAP function override the credentials configured for the
     SOAP message.
   - SOAP activity template: Credentials for a SOAP activity template override both the SOAP
     function and SOAP message credentials.

1. Navigate to System Web Services > Outbound > SOAP Message.
2. Select the SOAP message you want the activity to use.
3. In the SOAP Message record, select the Download WSDL check box.
4. In the Authentication type field, select Basic.
The **Basic auth profile** field appears.

5. Select the basic auth profile to use with this SOAP message.
6. Alternately, you can configure basic authentication credentials in Configure the SOAP execution command.
   a) In the Authentication field, select **Override with Basic Authentication credentials**. The Credentials field appears.
   b) Select the basic auth credentials to use to access the WSDL. This setting overrides any credentials configured in the SOAP message.
Configure the SOAP execution command
Use the input variables you created to configure the command that Orchestration executes on the SOAP endpoint.

Create the input variables you need in the Inputs form before you can advance to the Execution Command stage.

Role required: web_service_admin, activity_admin, activity_creator

---

**Note:** You can test the SOAP connection between the MID Server and the endpoint without having to run the activity in a workflow context. For details, see test template outputs.

---

1. Drag variables from the list of inputs and drop them into command fields. The system formats the variable in the proper syntax for the command.
2. Complete the fields shown in the table.
## SOAP template execution command fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>Input variable builder. <a href="#">Create input variables</a> to map to available fields.</td>
</tr>
<tr>
<td>Web service message</td>
<td><a href="#">SOAP message</a> to use for this activity. Users must have the web_service_admin role to configure this field.</td>
</tr>
<tr>
<td>Web service message function</td>
<td>SOAP message <a href="#">function</a> to use for this activity. Users must have the web_service_admin role to configure this field.</td>
</tr>
<tr>
<td>Endpoint</td>
<td>Endpoint URL for the SOAP web service this activity uses. Enter an endpoint in this field to override the endpoint configured in the SOAP message. Click the lock icon to open the input field.</td>
</tr>
<tr>
<td>SOAP message parameters</td>
<td>Name-value pairs to pass to the SOAP endpoint. You can create these parameters manually, or drag input variables into the parameter fields and then assign a value. Parameters defined in the SOAP message that use ${() } can be assigned data from this activity template. Use the <a href="#">Additional attribute</a> column to configure the system to not escape the text. By default, text sent to the SOAP message is escaped. The Name column is auto-populated if the users have provided variables using <a href="#">variable substitution</a> in the SOAP message.</td>
</tr>
<tr>
<td>Use MID Server</td>
<td>Check box that determines if a MID Server must be used to invoke the SOAP web service.</td>
</tr>
</tbody>
</table>

### Note:

If the SOAP web service message function defines a MID Server, that MID Server is used instead of the one selected here.

<p>| Required MID Server capabilities | MID Server with the appropriate <a href="#">capabilities</a> for connecting to the SOAP endpoint. By default, the system selects a MID Server with SOAP capabilities. This field is available when the <a href="#">Use MID Server</a> check box is selected. |
|Timeout                      | Allowed duration of the SOAP web service request before it times out, in seconds. The default is 10. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Determines what type of authentication is required for the endpoint. The options are:</td>
</tr>
<tr>
<td></td>
<td>• Use existing credentials in SOAP message: Uses credential definitions from the SOAP message definition.</td>
</tr>
<tr>
<td></td>
<td>• Override with Basic Authentication credentials: Uses basic authentication credentials. Overrides the credentials in the SOAP message definition. Basic authentication credentials must be provisioned before they are available for selection.</td>
</tr>
<tr>
<td></td>
<td>• Override with Certificate Authentication credentials: Overrides the credentials in the SOAP message definition with certificate authentication credentials.</td>
</tr>
<tr>
<td></td>
<td>• Override with Both Basic and Certificate Authentication credentials: Overrides the credentials in the SOAP message definition with both basic authentication or certificate authentication credentials.</td>
</tr>
<tr>
<td></td>
<td>• Override with WS-Security Username profile: Overrides the credentials in the SOAP message definition with credentials defined a WS Security Profile.</td>
</tr>
<tr>
<td>Credentials</td>
<td>Required REST endpoint basic authentication credentials. This field is available when Override with Basic Authentication credentials is selected in the Authentication field. Only basic authentication credentials appear in the selection list, which includes credentials stored on the instance and credential IDs from an external storage system. If you are using credentials stored in a CyberArk safe, you can override the default safe defined in the MID Server configuration file by adding the name of a different safe as a prefix to the credential ID, separated by a colon. For example, newsafe:orch-test-f5.</td>
</tr>
<tr>
<td>Protocol Profile</td>
<td>Protocol profile to use for authentication. This field is available when the authentication type is either Override with Certificate Authentication credentials or Override with Both Basic and Certificate Authentication credentials.</td>
</tr>
</tbody>
</table>

3. Click Save.
4. Click Continue to advance to the Outputs stage.

SOAP template execution parameters
You use execution parameters to create the input process script in the Pre processing form of the activity designer.

For descriptions of the SOAP web service command fields, see the table in Configure the SOAP execution command.
Note: You must use the `executionParam` prefix with all variables in this table.

### SOAP execution parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Variable</th>
<th>Type</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web service message</td>
<td><code>web_service_message</code></td>
<td>Reference</td>
<td>The sys_id of the corresponding SOAP message.</td>
</tr>
<tr>
<td>Web service message function</td>
<td><code>web_service_message_function</code></td>
<td>Reference</td>
<td>The sys_id of the SOAP message function.</td>
</tr>
<tr>
<td>Web service endpoint</td>
<td><code>web_service_endpoint</code></td>
<td>String</td>
<td>URL of the SOAP endpoint.</td>
</tr>
</tbody>
</table>
| Parameters                  | `parameters`              | Array of JavaScript objects | Array of JavaScript objects, expressed with the `executionParam` prefix. For instructions on creating arrays using this parameter, see [Create a JavaScript array in a SOAP template](#). For more information, see [Set up domain separation for MID servers](#). Use this example to customize the MID Server selection if there are additional capabilities that are assigned by value:  

```
var valueCapability = {'NEW_MID_CAPABILITY': 'NEW_MID_CAPABILITY_VALUE'};
executionParam.valueCapabilities.push(valueCapability);
```

| Use mid server              | `use_mid_server`          | Boolean              | When true, indicates that a MID Server is used.                     |
| MidCapabilities             | `midCapabilities`         | String (comma separated) | List of references to required MID Server capabilities.             |
| Time out                    | `time_out`                | String               | Allowed duration of the SOAP web service request before it times out, in seconds. The default is **10**. |
| ValueCapabilities           | `valueCapabilities`       | Array of hashmap     | Capability values used to select the MID Server. For more information, see [Set up domain separation for MID servers](#). Use this example to customize the MID Server selection if there are additional capabilities that are assigned by value:  

```
var valueCapability = {'NEW_MID_CAPABILITY': 'NEW_MID_CAPABILITY_VALUE'};
executionParam.valueCapabilities.push(valueCapability);
```
Create a JavaScript array in a SOAP template

These are instructions for creating JavaScript arrays using SOAP execution parameters.

Role required: web_service_admin, activity_admin, activity_creator

To add more name-value pairs to the parameter's array, append the values to the existing array.

1. Create a JavaScript object with the following syntax, and add it to the executionParam.parameter array:

   ```javascript
   var newParameter = {
   "name": "parameterName",
   "value": "parameterValue",
   "additional_attribute": "none"
   }
   executionParam.parameters.push(newParameter);
   ```

   By adding the new parameter JavaScript object to the array, you ensure that any elements already available in the array are not impacted.

2. Make sure to set the value in the Additional attribute column in the SOAP message parameters input field to Do not escape text.

   In this case, the system does not escape the value specified for the value attribute. An example of this is:

   ```javascript
   var newParameter = {
   "name": "parameterName",
   "value": "parameterValue",
   "additional_attribute": "do_not_escape_text"
   }
   executionParam.parameters.push(newParameter);
   ```

   **Note:** If the value for the additional_attribute field is None, then the system escapes the value specified by the value attribute. In the first example, parameterValue is escaped.

SOAP template post-processing parameters

Use these parameters to create a post-processing script.

Activity designer post-processing parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Variable</th>
<th>Type</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status code</td>
<td>status_code</td>
<td>Integer</td>
<td>Contains the status code returned from the web service.</td>
</tr>
<tr>
<td>Name</td>
<td>Variable</td>
<td>Type</td>
<td>Usage</td>
</tr>
<tr>
<td>-------</td>
<td>----------</td>
<td>--------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Header</td>
<td>header</td>
<td>Hashmap of JavaScript</td>
<td>Contains the key value paired hashmap associated with the header values passed into the web service. You can access each value with <code>executionResult.header[keyName]</code>.</td>
</tr>
<tr>
<td>Body</td>
<td>body</td>
<td>String</td>
<td>Contains a string value representing the output from the SOAP message</td>
</tr>
<tr>
<td>Error</td>
<td>error</td>
<td>String</td>
<td>Returns the error string from the SOAP web service, unless there are no errors, in which case it returns <code>null</code>.</td>
</tr>
</tbody>
</table>

**Create a JavaScript Probe activity**

Create a JavaScript Probe activity to instruct a MID server to execute server-side javascript.

Role required: activity_creator or workflow_admin

The JavascriptProbe activity has the same functionality as making ‘Packages’ calls into standard Java libraries. It allows you to have more control over the Java libraries on the MID Server. You can load your own JAR files on the MID Server and have the JavascriptProbe make Package calls into those java files.

1. Create a **custom activity**.
   This action creates a custom activity using a template.

2. After setting up **general properties** and **creating input variables**, configure the JavaScript probe activity Execution Command:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Map the input variables</strong></td>
<td>Use the variables you created to configure the command that Orchestration executes on the MID server.</td>
</tr>
<tr>
<td><strong>Script type</strong></td>
<td>Select the type of script to include. Available options are:</td>
</tr>
<tr>
<td></td>
<td>• Custom JavaScript</td>
</tr>
<tr>
<td></td>
<td>• MID Server script include</td>
</tr>
<tr>
<td><strong>Script</strong></td>
<td>Custom JavaScript to run with this probe.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This field is available when the Script type selected is <strong>Custom JavaScript</strong>.</td>
</tr>
<tr>
<td><strong>MID Server script include</strong></td>
<td>Script for the MID Server to run with this probe.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This field is available when the Script type selected is <strong>MID Server script include</strong>.</td>
</tr>
<tr>
<td><strong>Select MID Server by host</strong></td>
<td>MID Server on which the probe runs.</td>
</tr>
<tr>
<td><strong>Required MID Server capabilities</strong></td>
<td>MID Server to use, by capabilities.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Parameters</td>
<td>Name-value pairs to pass to the host with this probe. You can create these parameters manually, or drag input variables into the Parameters fields and assign a value.</td>
</tr>
</tbody>
</table>

**Note:** You can map parameter values in a test payload to variables in the Outputs tab automatically. See [automap output variables](#).

Finish creating your JavaScript probe activity by creating output variables, creating a parsing rule, or creating template conditions. Refer to the create custom activities topic to know your template options.

### JavaScript probe template execution parameters

You use execution parameters to create the input process script in the Preprocessing form of the activity designer.

For descriptions of the JavaScript Probe command fields, see the table in [Configure the JavaScript Probe execution command](#).

**Note:** You must use the executionParam. prefix with all variables in this table.

### JavaScript template execution parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Variable</th>
<th>Type</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Script Type</td>
<td>script_type</td>
<td>Enumerated</td>
<td>Type of script to run. The possible types are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- customJavascript_type</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- mid_script_include_type</td>
</tr>
<tr>
<td>Script</td>
<td>script</td>
<td>String</td>
<td>Script that runs custom JavaScript when the script_type is customJavascript_type.</td>
</tr>
<tr>
<td>Mid script include</td>
<td>mid_script_include</td>
<td>Reference</td>
<td>The sys_id reference associated with the MID Server script include to call, when the script_type is mid_script_include_type.</td>
</tr>
<tr>
<td>Source</td>
<td>source</td>
<td>String</td>
<td>Target host on which to run the script.</td>
</tr>
<tr>
<td>MidCapabilities</td>
<td>midCapabilities</td>
<td>String (comma separated)</td>
<td>List of required MID Server capabilities.</td>
</tr>
<tr>
<td>Name</td>
<td>Variable</td>
<td>Type</td>
<td>Usage</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------</td>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Parameters</td>
<td>parameters</td>
<td>Array of JavaScript</td>
<td>objects, expressed with the executionParam. prefix. To add more name-value pairs to the parameters array, append them to the existing array. Create a JavaScript object with the following syntax, and add it to the executionParam.parameters array. This assigns additional parameters to the message:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>object</td>
<td>var newParameter = {&quot;name&quot;:&quot;parameterName&quot;,&quot;value&quot;:&quot;parameterValue&quot;}; executionParam.parameters.push(newParameter);</td>
</tr>
<tr>
<td>ValueCapabilities</td>
<td>valueCapabilities</td>
<td>Array of hashmap</td>
<td>Capability values used to select the MID Server. For more information, see Set up domain separation for MID servers. If there are additional capabilities that are assigned by value, use this example to customize the MID Server selection:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>var valueCapability = {'NEW_MID_CAPABILITY': 'NEW_MID_CAPABILITY_VALUE' }; executionParam.valueCapabilities.push(valueCapability);</td>
</tr>
</tbody>
</table>

**JavaScript probe template post-processing parameters**

Use these parameters to create a post-processing script.

**JavaScript probe post-processing parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Variable</th>
<th>Type</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payload</td>
<td>payload</td>
<td>String</td>
<td>Contains raw payload returned from the JavaScript Probe.</td>
</tr>
<tr>
<td>Output</td>
<td>output</td>
<td>String</td>
<td>Contains output data returned from the JavaScript Probe.</td>
</tr>
<tr>
<td>Name</td>
<td>Variable</td>
<td>Type</td>
<td>Usage</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td>---------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>EccSysId</td>
<td>eccSysId</td>
<td>String</td>
<td>Contains the reference ID associated with the ECC Queue input message.</td>
</tr>
<tr>
<td>Error Messages</td>
<td>errorMessages</td>
<td>String</td>
<td>Contains the error messages returned from the JavaScript probe. If no error messages are returned, this value is null.</td>
</tr>
</tbody>
</table>

**Configure the JavaScript Probe execution command**

Use the input variables you created to configure the command that Orchestration executes on the JavaScript Probe target host.

Create the input variables you need in the **Inputs** form before you can advance to the **Execution Command** stage.

Role required: activity_creator, admin

---

**Note:** You can test the JavaScript Probe connection between the MID Server and the target without having to run the activity in a workflow context. For details, see [test template outputs](https:// servicenow.com).

---

1. Drag variables from the list of inputs and drop them into command fields. The system formats the variable in the proper syntax for the command.
2. Complete the fields shown in the table.

**JavaScript Probe execution command fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>Input variable builder. Create input variables to map to available fields.</td>
</tr>
<tr>
<td>Script type</td>
<td>Select the type of script to include. Available options are:</td>
</tr>
<tr>
<td>Script</td>
<td>Custom JavaScript</td>
</tr>
<tr>
<td>MID Server script include</td>
<td>MID Server script include</td>
</tr>
<tr>
<td>Select MID Server by host</td>
<td>MID Server on which the probe runs.</td>
</tr>
<tr>
<td>Required MID Server capabilities</td>
<td>MID Server to use, by capabilities.</td>
</tr>
<tr>
<td>Parameters</td>
<td>Name-value pairs to pass to the host with this probe. You can create these parameters manually, or drag input variables into the Parameters fields and assign a value.</td>
</tr>
</tbody>
</table>

3. Click **Save**.

4. Click **Continue** to advance to the **Outputs** stage.

**Create a PowerShell activity**

Create a custom PowerShell activity return data to a workflow from a host using Microsoft PowerShell.

Role required: activity_creator or workflow_admin

ServiceNow supports PowerShell 2.0 and above. PowerShell 3.0 does not support Windows 2003 Server.

1. Create a **custom activity**.
   This action creates a custom activity using a template.

2. After setting up **general properties** and **creating input variables**, configure the PowerShell Execution Command:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Map the input variables</strong></td>
<td>Use the variables you created to configure the command that Orchestration executes on the MID Server.</td>
</tr>
<tr>
<td><strong>Target host</strong></td>
<td>Host name or IP address of the target server for this PowerShell activity.</td>
</tr>
<tr>
<td><strong>Script type</strong></td>
<td>Type of PowerShell script to run on the PowerShell host. Available options are:</td>
</tr>
<tr>
<td></td>
<td>Custom PowerShell command</td>
</tr>
<tr>
<td></td>
<td>MID Server script file</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MID Server script file</td>
<td>The MID Server script file contains the PowerShell scripts. This field is available when the <strong>Script type</strong> selected is MID Server script file.</td>
</tr>
<tr>
<td>Command</td>
<td>PowerShell command the activity executes. This field is available when the <strong>Script type</strong> selected is Custom PowerShell command. You can create your commands by dragging and dropping input variables from the variable builder into this field.</td>
</tr>
<tr>
<td>PowerShell variables</td>
<td>Name-value pairs to pass to the host with PowerShell. You can create these variables manually, or drag input variables into the <strong>Value</strong> field. Encrypted input variables retain their encryption, regardless of the data type settings in this field. If you type in a value and select the <strong>Encrypted</strong> data type, your value appears in plain text. It is only encrypted when it passes to the ECC Queue.</td>
</tr>
<tr>
<td>Use MID Service Account</td>
<td>If checked, this activity authenticates on the target host using the credentials of the MID Server service account only, without trying any other credentials.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The <strong>Credential tag</strong> field is not available.</td>
</tr>
<tr>
<td>Credential tag</td>
<td>Credential tag this activity must use to run PowerShell commands on the host. If this field is left blank, the MID Server tries all the available credentials until it finds a valid one, ending with the MID Server service account. If a credential tag is defined, the MID Server tries the credentials with that tag specified only and does not try the MID Server service account.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This field is not available when the <strong>Use MID service account</strong> check box is selected.</td>
</tr>
<tr>
<td>Required MID Server capabilities</td>
<td>MID Server to use for querying PowerShell, by capabilities. By default, the system selects a PowerShell MID Server.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You can map parameter values in a test payload to variables in the <strong>Outputs</strong> tab automatically. See <a href="https://www.servicenow.com">automap output variables</a>.</td>
</tr>
</tbody>
</table>

Finish creating your PowerShell activity by creating output variables, creating a parsing rule, or creating template conditions. Refer to the create custom activities topic to know your template options.

_PowerShell template execution parameters_

You use execution parameters to create the input process script in the **Pre Processing** form of the activity designer.

For descriptions of the Powershell command fields, see the table in Configure the PowerShell execution command.
**Note:** You must use the `executionParam` prefix with all variables in this table.

### Powershell execution parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Variable</th>
<th>Type</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>source</td>
<td>String</td>
<td>Target host on which to execute the command.</td>
</tr>
<tr>
<td>Script type</td>
<td>script_type</td>
<td>Enumeration</td>
<td>Type of script to run. The possible types are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- <strong>command:</strong> Custom PowerShell command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- <strong>file:</strong> Identifies the MID Server script file to run.</td>
</tr>
<tr>
<td>Command</td>
<td>command</td>
<td>String</td>
<td>Command sent to the MID Server for it to run on the target host.</td>
</tr>
<tr>
<td>MidScriptFile</td>
<td>midScriptFile</td>
<td>Reference</td>
<td>Reference sys_id of the MID Server script file to execute, when the script type is <code>file</code>.</td>
</tr>
<tr>
<td>PoweershellVariables</td>
<td>powershellVariables</td>
<td>Array of hashmap</td>
<td>Hashmap of JavaScript objects with <code>name</code>, <code>value</code>, and <code>type</code> for each object. The type of each object can be one of <code>plain</code>, <code>encrypted</code>, <code>boolean</code>, or <code>null</code>, corresponding to the PowerShell variable type selected in the inputs tab. For example, you might enter:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><code>var newParameter = { &quot;name&quot;:&quot;parameterName&quot;,&quot;value&quot;: &quot;parameterValue&quot;,&quot;type&quot;: &quot;plain&quot; };</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><code>executionParam.powershellVariables.push(newParameter);</code></td>
</tr>
<tr>
<td>Credential tag</td>
<td>credential_tag</td>
<td>String</td>
<td>Specific credential tag this activity must use to run PowerShell commands on the host.</td>
</tr>
<tr>
<td>MidCapabilities</td>
<td>midCapabilities</td>
<td>String (comma separated)</td>
<td>List of required MID Server capabilities.</td>
</tr>
<tr>
<td>Name</td>
<td>Variable</td>
<td>Type</td>
<td>Usage</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------</td>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ValueCapabilities</td>
<td>valueCapabilities</td>
<td>Array of hashmap</td>
<td>Capability values used to select the MID Server. For more information, see <a href="#">Set up domain separation for MID servers</a>. If there are additional capabilities that are assigned by value, use this example to customize the MID Server selection: var valueCapability = {'NEW_MID_CAPABILITY':'NEW_MID_CAPABILITY_VALUE'}; executionParam.valueCapabilities.push(valueCapability);</td>
</tr>
</tbody>
</table>

*PowerShell post-processing parameters and payload parsing*

Use these parameters to create a post-processing script, payload parsing, and tagging.
### PowerShell post-processing parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Variable</th>
<th>Type</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tags</td>
<td>tags</td>
<td>Hashmap of tag values to return from the PowerShell command.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Contains the tags used to extract output using the PowerShell commands. The tag output is delimited by double percentage signs, as in <code>%%tagname</code> ... <code>%%</code>. Set up the command using the format in this example:</td>
</tr>
</tbody>
</table>
|          |          |          | **Write-Host** %%
tagname1%% output1 line 1 output1 line 2 ... Write-Host%%                                                 |
|          |          |          | **Write-Host** %%
tagname2%% output2 line 1 output2 line 2 ... Write-Host%%                                                 |
|          |          |          | The tags returned are JavaScript hashmap objects in which each key is prefixed with `tag` appended with the `tagname`.              |
|          |          |          | `{"__text__":"
",
"tagtagname1":"output1 line1
output1 line2\n",
"tagtagname2":"output2 line1
output2 line2\n"}`                                                                       |
| Hresult  | hresult  | String   | Contains any hresult returned from the PowerShell command. If no hresult is returned, this parameter is null.                         |
| Output   | output   | String   | Contains the raw output from the PowerShell command.                                                                                |
| EccSysID | eccSysID | String   | Contains the reference ID associated with the ECC Queue input message returned by the activity.                                      |
ServiceNow    Jakarta    Now Platform Capabilities

<table>
<thead>
<tr>
<th>Name</th>
<th>Variable</th>
<th>Type</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>ErrorMessages</td>
<td>errorMessages</td>
<td>String</td>
<td>Contains any error messages retrieved from the PowerShell command. This value is null if there are no error messages.</td>
</tr>
</tbody>
</table>

**Create a REST web service activity**

Use this procedure to create a custom REST web service Orchestration activity.

Role required: web_service_admin, activity_admin, activity_creator

To create and use a REST web service workflow activity:

- Create a **REST message** if an appropriate one is not already configured.
- Assign the web_service_admin role to any user who must create or edit a custom REST activity.
- Determine an application, or **scope**, for this activity.
- Determine the **REST endpoint** to use for the activity. Use this value to override the endpoint configured in the REST message.
- Optionally, create basic authentication credentials. Use this value to override the credentials configured in the SOAP message.

1. Create a custom activity.
   This action creates a custom activity using a template.

2. After setting up general properties and creating input variables, configure the REST web service Execution Command:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Map the input variables</td>
<td>Use the variables you created to configure the command that Orchestration executes.</td>
</tr>
<tr>
<td>REST message</td>
<td>Name of an existing REST message to use in this activity.</td>
</tr>
<tr>
<td>REST message function</td>
<td>REST message function to use for this activity.</td>
</tr>
<tr>
<td>Endpoint</td>
<td>Endpoint URL for the REST web service this activity uses. Enter an endpoint in this field to override the endpoint configured in the REST message. Click the lock to open the input field.</td>
</tr>
<tr>
<td>Variable substitutions</td>
<td>Name-value pairs to pass to the REST endpoint. You can create these parameters manually, or drag input variables into the parameter fields, and then assign a value. Parameters defined in the REST message that use {} can be assigned data from this activity template. Use the Additional attribute column to configure the system to not escape the text. By default the text sent to the REST message is escaped. If the users have provided variables using variable substitution in the REST message, then the Name column is automatically populated.</td>
</tr>
<tr>
<td>Additional Headers</td>
<td>Additional HTTP header parameters for the REST message selected. You can also use these values to override parameters inherited from the REST message.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Additional Query Parameters</td>
<td>Additional query parameters for the REST message selected. You can also use these values to override parameters inherited from the REST message.</td>
</tr>
<tr>
<td>Use MID Server</td>
<td>Check box that determines if a MID Server should be used to invoke the REST web service.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If the REST web service message function defines a MID Server, that MID Server is used instead of the one selected here.</td>
</tr>
<tr>
<td>Required MID Server capabilities</td>
<td>MID Server with the appropriate <strong>capabilities</strong> for connecting to the REST endpoint. By default, the system selects a MID Server with REST capabilities. This field is available when the <strong>Use MID Server</strong> check box is selected.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Allowed duration of the REST web service request before it times out, in seconds. The default is 10.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Determines what type of authentication is required for the endpoint. The options are:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Use existing credentials in REST message:</strong> Uses credential definitions from the REST message definition.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Override with Basic Authentication credentials:</strong> Uses basic authentication credentials to override the credentials in the REST message definition. Basic authentication credentials must be provisioned before they are available for selection.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Override with Certificate Authentication credentials:</strong> Uses a certificate, such as a private key, to override the credentials in the REST message definition.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Override with Both Basic and Certificate Authentication credentials:</strong> Uses both basic authentication and certificate authentication to override the credentials in the REST message definition.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Override with OAuth Authentication credentials:</strong> Uses OAuth 2.0 credentials to override the credentials in the REST message definition. The REST message selected for this activity must have its <strong>Authentication type</strong> set to OAuth 2.0 and its <strong>OAuth profile</strong> configured appropriately.</td>
</tr>
</tbody>
</table>
### ServiceNow Jakarta Now Platform Capabilities

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Credentials</strong></td>
<td>Required REST endpoint basic authentication credentials. This field is available when <strong>Override with Basic Authentication credentials</strong> is selected in the <strong>Authentication</strong> field. Only basic authentication credentials appear in the selection list, which includes credentials stored on the instance and credential IDs from an external storage system. If you are using credentials stored in a CyberArk safe, you can override the default safe defined in the MID Server configuration file. Add the name of a different safe as a prefix to the credential ID, separated by a colon. For example, <code>newsafe:orch-test-f5</code>.</td>
</tr>
<tr>
<td><strong>Protocol Profile</strong></td>
<td>Certificate authentication to use. This field is available when the selections in the <strong>Authentication</strong> are either <strong>Override with Certificate Authentication credentials</strong> or <strong>Override with Both Basic and Certificate Authentication credentials</strong>.</td>
</tr>
<tr>
<td><strong>OAuth profile</strong></td>
<td>Profile for the OAuth provider for this REST message. See <a href="#">Specify an OAuth profile</a> for more information.</td>
</tr>
</tbody>
</table>

**Note:** You can map parameter values in a test payload to variables in the **Outputs** tab automatically. See [automap output variables](#).

---

Finish creating your Rest web service activity by [creating output variables](#), [creating a parsing rule](#), or [creating template conditions](#). Refer to the [create custom activities](#) topic to know your template options.

**Auto-map REST activity output variables**

The ServiceNow activity designer allows you to map parameter values in a REST test payload to variables in the **Outputs** stage automatically.

Role required: web_service_admin, activity_admin, activity_creator

**Note:** You can test input variables from any stage in the activity designer if you have provided enough information for Orchestration to contact the endpoint and return data. Typically, the **Execution Command** stage is the point at which your inputs are ready for testing.

1. In the activity designer, proceed to the **Execution Command** stage.
2. Define an appropriate MID Server, if requested.
   The test fails if the MID Server cannot be found or if it cannot connect to the target.
3. **Click Test Activity** to test the input parameters.
   If you added actual values for the parameters and fields, the system runs those values against the specified target and returns the resulting payload. If you mapped input variables to fields and parameters, the system displays a dialog box for assigning test values to those variables.
4. **Provide test values, if requested, and click OK** to display the payload.
   The entire payload appears in the **Raw Output** tab of the Response form.
5. Select one of these auto-mapping options.
   - **Auto-Map to Local**: Directly maps values to a local variable for use within the activity.
   - **Auto-Map to Output**: Directly maps values to the output variable to pass to other activities in the workflow. Auto-mapping to an output variable creates an array of objects, each of which contains the column names from the query result.

**REST template execution parameters**

You use execution parameters to create the input process script in the **Pre Processing** form of the activity designer.

For descriptions of the REST web service command fields, see [Configure the REST execution command](#).

**Note**: You must use the `executionParam.` prefix with all variables in this table.

### REST template execution parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Variable</th>
<th>Type</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web service message</td>
<td>web_service_message</td>
<td>Reference</td>
<td>The sys_id of the corresponding web service message.</td>
</tr>
<tr>
<td>Web service message function</td>
<td>web_service_message_function</td>
<td>Reference</td>
<td>The sys_id of the REST message function.</td>
</tr>
<tr>
<td>Web service endpoint</td>
<td>web_service_endpoint</td>
<td>String</td>
<td>URL of the REST endpoint.</td>
</tr>
</tbody>
</table>
| Parameters          | parameters           | Array of JavaScript objects | Array of JavaScript objects, expressed with the `executionParam.` prefix. For instructions on creating arrays using this parameter see [Create a JavaScript array in a REST template](#).
<p>| Use mid server      | use_mid_server       | Boolean            | Selects whether or not to use the MID Server. A value of <code>true</code> uses the MID Server, and a value of <code>false</code> does not use the MID Server. |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Variable</th>
<th>Type</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>MidCapabilities</td>
<td>midCapabilities</td>
<td>String (comma separated)</td>
<td>List of references to required MID Server capabilities.</td>
</tr>
<tr>
<td>Time out</td>
<td>time-out</td>
<td>String</td>
<td>Allowable time out duration, expressed in seconds.</td>
</tr>
<tr>
<td>ValueCapabilities</td>
<td>valueCapabilities</td>
<td>Array of hashmap</td>
<td>Capability values used to select the MID Server. For more information, see Set up domain separation for MID servers. Use this example to customize the MID Server selection if there are additional capabilities that are assigned by value: var valueCapability = {'NEW_MID_CAPABILITY': 'NEW_MID_CAPABILITY_VALUE'}; executionParam.valueCapabilities.push(valueCapability);</td>
</tr>
<tr>
<td>Auth Type</td>
<td>auth-type</td>
<td>Boolean</td>
<td>Type of credentials to use. The choices are: basic_auth_pick_credentials, use_existing_credentials</td>
</tr>
<tr>
<td>Credentials</td>
<td>credentials</td>
<td>Reference</td>
<td>Contains the credentials to use for this REST message when the auth_type selected is basic_auth_pick_credentials.</td>
</tr>
</tbody>
</table>

Create a JavaScript array in a REST template
These are instructions for creating JavaScript arrays using REST execution parameters.

Role required: web_service_admin, activity_admin, activity_creator

To add more name-value pairs to the parameter’s array, append the values to the existing array.

1. Create a JavaScript object with the following syntax, and add it to the executionParam.parameter array:

```javascript
var newParameter = {
  "name": "parameterName",
  "value": "parameterValue",
  "additional_attribute": "none"
};
executionParam.parameters.push(newParameter);
```

By adding the new parameter JavaScript object to the array, you ensure that any elements already available in the array are not impacted.

2. Make sure to set the value in the Additional attribute column in the REST message parameters input field to Do not escape text.
In this case, the system does not escape the value specified for the **value** attribute. An example of this is:

```javascript
var newParameter = {
    "name":"parameterName","value":"parameterValue","additional_attribute":"do_not_escape_text";
}
executionParam.parameters.push(newParameter);
```

**Note:** If the value for the **additional_attribute** field is **None**, then the system escapes the value specified by the **value** attribute. In the first example, `parameterValue` is escaped.

REST template post-processing parameters

Use these parameters to create a post-processing script.

### Activity designer post-processing parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Variable</th>
<th>Type</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status code</td>
<td>status_code</td>
<td>Integer</td>
<td>Contains the status code returned from the REST web service.</td>
</tr>
<tr>
<td>Header</td>
<td>header</td>
<td>Hashmap of JavaScript object</td>
<td>Hashmap of key value pairs associated with the header values passed into the web service. You can access each value with <code>executionResult.header[keyName]</code>.</td>
</tr>
<tr>
<td>Body</td>
<td>body</td>
<td>String</td>
<td>Contains a string value representing the output from the REST message</td>
</tr>
<tr>
<td>Error</td>
<td>error</td>
<td>String</td>
<td>Returns the error string from the REST web service, unless there are no errors, in which case it returns <code>null</code>.</td>
</tr>
</tbody>
</table>

Configure the REST execution command

Use the input variables you created to configure the command that Orchestration executes on the REST endpoint.

Create the input variables you need in the **Inputs** form before you can advance to the **Execution Command** stage.

Role required: web_service_admin, activity_admin, activity_creator

**Note:** You can test the REST connection between the MID Server and the endpoint without having to run the activity in a workflow context. For details, see test template outputs.

1. Drag variables from the list of inputs and drop them into command fields. The system formats the variable in the proper syntax for the command.
2. Complete the fields shown in the table.

REST execution command fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input</strong></td>
<td>Input variable builder. Create input variables to map to available fields.</td>
</tr>
<tr>
<td><strong>REST message</strong></td>
<td>Name of an existing REST message to use in this activity. Users must have the web_service_admin role to configure this field.</td>
</tr>
<tr>
<td><strong>REST message function</strong></td>
<td>REST message function to use for this activity. Users must have the web_service_admin role to configure this field.</td>
</tr>
<tr>
<td><strong>Endpoint</strong></td>
<td>Endpoint URL for the REST web service this activity uses. Enter an endpoint in this field to override the endpoint configured in the REST message. Click the lock to open the input field.</td>
</tr>
<tr>
<td><strong>Variable substitutions</strong></td>
<td>Name-value pairs to pass to the REST endpoint. You can create these parameters manually, or drag input variables into the parameter fields, and then assign a value. Parameters defined in the REST message that use $() can be assigned data from this activity template. Use the Additional attribute column to configure the system to not escape the text. By default the text sent to the REST message is escaped. If the users have provided variables using variable substitution in the REST message, then the Name column is automatically populated.</td>
</tr>
<tr>
<td><strong>Additional Headers</strong></td>
<td>Additional HTTP header parameters for the REST message selected. You can also use these values to override parameters inherited from the REST message.</td>
</tr>
<tr>
<td><strong>Additional Query Parameters</strong></td>
<td>Additional query parameters for the REST message selected. You can also use these values to override parameters inherited from the REST message.</td>
</tr>
<tr>
<td><strong>Use MID Server</strong></td>
<td>Check box that determines if a MID Server should be used to invoke the REST web service.</td>
</tr>
<tr>
<td>Note:</td>
<td>If the REST web service message function defines a MID Server, that MID Server is used instead of the one selected here.</td>
</tr>
<tr>
<td><strong>Required MID Server capabilities</strong></td>
<td>MID Server with the appropriate capabilities for connecting to the REST endpoint. By default, the system selects a MID Server with REST capabilities. This field is available when the Use MID Server check box is selected.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Timeout</td>
<td>Allowed duration of the REST web service request before it times out, in seconds. The default is 10.</td>
</tr>
</tbody>
</table>
| Authentication        | Determines what type of authentication is required for the endpoint. The options are:  
  - **Use existing credentials in REST message**: Uses credential definitions from the REST message definition.  
  - **Override with Basic Authentication credentials**: Uses basic authentication credentials to override the credentials in the REST message definition. Basic authentication credentials must be provisioned before they are available for selection.  
  - **Override with Certificate Authentication credentials**: Uses a certificate, such as a private key, to override the credentials in the REST message definition.  
  - **Override with Both Basic and Certificate Authentication credentials**: Uses both basic authentication and certificate authentication to override the credentials in the REST message definition.  
  - **Override with OAuth Authentication credentials**: Uses OAuth 2.0 credentials to override the credentials in the REST message definition. The REST message selected for this activity must have its **Authentication type** set to OAuth 2.0 and its **OAuth profile** configured appropriately. |
| Credentials           | Required REST endpoint basic authentication credentials. This field is available when **Override with Basic Authentication credentials** is selected in the Authentication field. Only basic authentication credentials appear in the selection list, which includes credentials stored on the instance and credential IDs from an external storage system. If you are using credentials stored in a CyberArk safe, you can override the default safe defined in the MID Server configuration file. Add the name of a different safe as a prefix to the credential ID, separated by a colon. For example, newsafe:orch-test-f5. |
| Protocol Profile      | Certificate authentication to use. This field is available when the selections in the Authentication field are either **Override with Certificate Authentication credentials** or **Override with Both Basic and Certificate Authentication credentials**.                                                                                                                                   |
| OAuth profile         | Profile for the OAuth provider for this REST message. See **Specify an OAuth profile** for more information.                                                                                                                                                                                                                               |
3. Click **Save**.
4. Click **Continue** to advance to the **Outputs** stage.

### Create an SFTP activity

Create an activity that executes basic SFTP commands on a remote server.

**Roles required:** activity_creator or workflow_admin

You can create a custom activity that manages files and directories on a target host or copies a file from one SFTP server to another. The file content is streamed through a MID Server, which avoids having to store the data on the hard drive of the MID Server host machine.

**Note:** This activity requires the credentials of a user who can execute SFTP commands on the source host. The **Copy File** activity, provided in the activity pack, requires separate credentials to access the target host.

1. Create a **custom activity**.
   This action creates a custom activity using a template.

2. After setting up **general properties** and **creating input variables**, configure the SFTP Execution Command:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>Type of activity to create. The choices are:</td>
</tr>
<tr>
<td></td>
<td>- Copy file</td>
</tr>
<tr>
<td></td>
<td>- Create directory</td>
</tr>
<tr>
<td></td>
<td>- Get file list</td>
</tr>
<tr>
<td></td>
<td>- Remove file or directory</td>
</tr>
<tr>
<td></td>
<td>- Rename file or directory</td>
</tr>
<tr>
<td></td>
<td>- Set file attributes</td>
</tr>
</tbody>
</table>

**Note:** The fields that display on the form depend on the command you select.

<table>
<thead>
<tr>
<th>Source host</th>
<th>Name or IP address of the server containing the files targeted by the activity.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source port</td>
<td>Port number to use to communicate with the source server. The default port number is 22.</td>
</tr>
<tr>
<td>Source file path</td>
<td>Full path to a file (/temp/test_data_file.txt) or directory (/temp/test_dir) on a source host depending on the selected command. Field available on following commands:</td>
</tr>
<tr>
<td>Source directory</td>
<td>Path to the directory where the source files are located. Field available on following commands:</td>
</tr>
<tr>
<td></td>
<td>- Copy file</td>
</tr>
<tr>
<td></td>
<td>- Remove file or directory</td>
</tr>
<tr>
<td></td>
<td>- Set file attributes</td>
</tr>
<tr>
<td></td>
<td>- Create directory</td>
</tr>
<tr>
<td></td>
<td>- Get file list</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Source files</td>
<td>Names of specific source files to include in the file transfer. Separate the file names with semi-colons. This field supports a semi-colon separated list of wild-card patterns. For example: *.txt; a?cd.pdf. If this field is blank, all files are included. Field available on following command: • Get file list</td>
</tr>
<tr>
<td>Is a directory</td>
<td>If checked, specifies the file path is a directory. Field available on following command: • Remove file or directory</td>
</tr>
<tr>
<td>Credential tag for source</td>
<td>Specific credential tag this activity must use to run SFTP commands on the source host.</td>
</tr>
<tr>
<td>Credential tag for target</td>
<td>Specific credential tag this activity must use to run SFTP commands on the target host. Field available on following command: • Copy file</td>
</tr>
<tr>
<td>Excluded files</td>
<td>Names of specific source files to exclude from the file transfer. The activity acts on all other files found in the source directory or subfolders. Separate the file names with commas. This field supports comma-separated list of wild-card patterns. For example: *.txt, a?cd.pdf.. Field available on following command: • Get file list</td>
</tr>
<tr>
<td>Include subfolders</td>
<td>If checked, includes the files from subfolders in the source directory. Field available on following command: • Get file list</td>
</tr>
<tr>
<td>Target host</td>
<td>Name or IP address of the server to which the files are being transferred. Field available on following command: • Copy file</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Target port</td>
<td>Port number to use to communicate with the target host. The default port number is 22. Field available on following command:</td>
</tr>
<tr>
<td></td>
<td>- Copy file</td>
</tr>
<tr>
<td>Target file path</td>
<td>Full path to a file on a target host. Field available on following commands:</td>
</tr>
<tr>
<td></td>
<td>- Copy file</td>
</tr>
<tr>
<td></td>
<td>- Rename file or directory</td>
</tr>
<tr>
<td>Suffix for temporary file</td>
<td>If a file exists on a target host, this command enables a temporary suffix to use for a file name. If this field contains a value, the activity first copies the source file to a temporary file on the target host using targetFilePath + tempFileSuffix as the name. Upon completion, the activity renames the file to the actual target file name. If this field is blank, the activity copies the source file directly to the target file and overwrites it, if it exists. Field available on following command:</td>
</tr>
<tr>
<td></td>
<td>- Copy file</td>
</tr>
<tr>
<td>UID</td>
<td>User ID attribute to apply to a file or directory. The UID and GID values must be set together as a pair or they are ignored. The UID and GID numbers are internal values returned by the Get File List activity. Typically, you first use the Get File List activity to return a list of files and their attributes. Then you can move a file from a source host to a target host and set the source file attributes on the target file. This flow is demonstrated in the SFTP File Transfer workflow. Field available on following command:</td>
</tr>
<tr>
<td></td>
<td>- Set file attributes</td>
</tr>
<tr>
<td>GID</td>
<td>Group ID attribute to apply to a file or directory. The UID and GID values must be set together as a pair or they are ignored. The UID and GID numbers are internal values returned by the Get File List activity. Typically, you first use the Get File List activity to return a list of files and their attributes. Then you can move a file from a source host to a target host and set the source file attributes on the target file. This flow is demonstrated in the SFTP File Transfer workflow. Field available on following command:</td>
</tr>
<tr>
<td></td>
<td>- Set file attributes</td>
</tr>
</tbody>
</table>
### Option | Description
--- | ---
**Permissions** | File or directory permissions to set for the user and group specified. This value must be expressed as an integer, such as 16877, which defines these permissions: `rwxr-xr-x`. The permissions numbers are internal values returned by the Get File List activity. Typically, you first use the Get File List activity to return a list of files and their attributes. Then you can move a file from a source host to a target host and set the source file attributes on the target file. This flow is demonstrated in the [SFTP File Transfer workflow](https://example.com). Field available on following command:
- Set file attributes

**Access timestamp** | Override the timestamp when the file or directory was last accessed. The access and modification timestamps must be set together as a pair. Field available on following command:
- Set file attributes

**Modification timestamp** | Override the timestamp when the file or directory was last modified. The access and modification timestamps must be set together as a pair. Field available on following command:
- Set file attributes

**Size in bytes** | Size of a file, expressed in bytes. Field available on following command:
- Set file attributes

**Required MID Server capabilities** | MID Server with the appropriate capabilities for connecting to the source and target servers.

The system uses this logic to determine which files to move from the source host:
- If the Source files field is empty, the system selects all the files in the source directory. Otherwise, it only selects those files whose names match one of the file name patterns given in the field.
- If the Excluded files field is empty, the system excludes nothing. Otherwise, it excludes those files whose names match one of the file name patterns given in the field.
- The exclude rule has a higher preference than the include rule. If a file name matches one of the file name patterns in the Excluded files field, it does not get into the selection regardless of the include rule.
- When the Include subfolders check box is cleared, the system looks only in the source directory for files to include or exclude. Otherwise, it looks in the source directory and any of its subfolders for files to include or exclude.

**Note:** You can map parameter values in a test payload to variables in the Outputs tab automatically. See [automap output variables](https://example.com).

- Use **auto-mapping** to generate outputs and parsing rules (recommended for JDBC)
- If you do not use auto-mapping, you can manually [create output variables](https://example.com) and [create parsing rules](https://example.com)
SFTP template execution parameters

You use execution parameters to create the input process script in the Preprocessing form.

For descriptions of the command fields, see Configure the SFTP execution command.

**Note:** You must use the executionParam. prefix with all variables in this table.

### SFTP execution parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Variable</th>
<th>Type</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>command</td>
<td>String</td>
<td>Identifies the function of this activity. The possible commands are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Copy file</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Create directory</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Get file list</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Remove file or directory</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Rename file or directory</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Set file attributes</td>
</tr>
<tr>
<td>Source</td>
<td>source</td>
<td>String</td>
<td>Identifies the source host.</td>
</tr>
<tr>
<td>Source port</td>
<td>source_port</td>
<td>Integer</td>
<td>Identifies the port used to communicate with the source host.</td>
</tr>
<tr>
<td>Source directory</td>
<td>source_directory</td>
<td>String</td>
<td>Path to the source directory of the files to be moved.</td>
</tr>
<tr>
<td>Source files</td>
<td>source_files</td>
<td>String</td>
<td>Names of the files on the source to be moved.</td>
</tr>
<tr>
<td>Excluded files</td>
<td>excluded_files</td>
<td>String</td>
<td>Lists the files excluded from the operation.</td>
</tr>
<tr>
<td>Source file path</td>
<td>source_file_path</td>
<td>String</td>
<td>Path to the source files to be moved.</td>
</tr>
<tr>
<td>Target host</td>
<td>target_host</td>
<td>String</td>
<td>Identifies the target host.</td>
</tr>
<tr>
<td>Target port</td>
<td>target_port</td>
<td>Integer</td>
<td>Identifies the port used to communicate with the target host.</td>
</tr>
<tr>
<td>Target directory</td>
<td>target_directory</td>
<td>String</td>
<td>Full path to the target directory on the target host.</td>
</tr>
<tr>
<td>Target file path</td>
<td>target_file_path</td>
<td>String</td>
<td>Full path to a file or directory on the source host or on the target host. For example, this value is used in the Rename File or Directory activity in the activity pack.</td>
</tr>
<tr>
<td>Name</td>
<td>Variable</td>
<td>Type</td>
<td>Usage</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------</td>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Temp file postfix</td>
<td>temp_file_postfix</td>
<td>String</td>
<td>Temporary file name extension used by the Copy File activity when moving a file. If this field contains an extension, the source file is copied to a temporary file using <strong>target file name + temp_file_postfix</strong>, before being renamed to the actual target file. If this field is blank, the source file is copied directly to the target file.</td>
</tr>
<tr>
<td>Is directory</td>
<td>is_directory</td>
<td>Boolean</td>
<td>Indicates whether the given file path is a directory.</td>
</tr>
<tr>
<td>Include subfolders</td>
<td>include_subfolders</td>
<td>Boolean</td>
<td>Indicates whether the system looks into subfolders of the source directory for files to include and exclude.</td>
</tr>
<tr>
<td>File attribute uid</td>
<td>file_attribute_uid</td>
<td>Integer</td>
<td>User ID associated with a file or directory.</td>
</tr>
<tr>
<td>File attribute gid</td>
<td>file_attribute_gid</td>
<td>Integer</td>
<td>Group ID associated with a file or directory.</td>
</tr>
<tr>
<td>File attribute permissions</td>
<td>file_attribute_permissions</td>
<td>Integer</td>
<td>File or directory permissions for the user and group specified.</td>
</tr>
<tr>
<td>File attribute atime</td>
<td>file_attribute_atime</td>
<td>Integer</td>
<td>Access time stamp from the file attributes.</td>
</tr>
<tr>
<td>File attribute mtime</td>
<td>file_attribute_mtime</td>
<td>Integer</td>
<td>Modification time stamp from the file attributes.</td>
</tr>
<tr>
<td>File attribute size</td>
<td>file_attribute_size</td>
<td>Integer</td>
<td>Size of the file, in bytes.</td>
</tr>
<tr>
<td>Source credential tag</td>
<td>source_credential_tag</td>
<td>String</td>
<td><strong>Credential tag</strong> used to run the command on the source host.</td>
</tr>
<tr>
<td>Target credential tag</td>
<td>target_credential_tag</td>
<td>String</td>
<td>Credential tag used to run the command on the target host.</td>
</tr>
<tr>
<td>MidCapabilities</td>
<td>midCapabilities</td>
<td>String (comma separated)</td>
<td>List of required MID Server capabilities.</td>
</tr>
</tbody>
</table>

*SFTP post-processing parameters and payload parsing*

Use these parameters to create a post-processing script, payload parsing, and tagging.
## SFTP post-processing parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Variable</th>
<th>Type</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output</td>
<td>output</td>
<td>String</td>
<td>Contains output data returned by the query.</td>
</tr>
<tr>
<td>EccSysId</td>
<td>eccSysId</td>
<td>String</td>
<td>Contains the Reference ID associated with the ECC Queue input message.</td>
</tr>
<tr>
<td>ErrorMessages</td>
<td>errorMessages</td>
<td>String</td>
<td>Contains the error messages returned from the query. If no error messages are returned, this value is null.</td>
</tr>
</tbody>
</table>
| Tags            | tags     | Hashmap of tag values returned from the SSH command | Contains the tags used to extract output using the SSH commands. The tag output is delimited by double percentage signs, as in `%tagname % ... %`. Set up the command using the following format:  

| %tagname1%%  
output1 line 1  
output1 line 2  
...  
% |
| %tagname2%%  
output2 line 1  
output2 line 2  
...  
% |

The tags returned are JavaScript hashmap objects in which each key is prefixed with `tag appended with the tagname`.  

```javascript
{"__text__":  
"",  
"tagtagname1":"output1 line1
output1 line2\n",  
"tagtagname2":"output2 line1
output2 line2\n"}
```

---

### Configure the SFTP execution command

Use the input variables you created to configure the command that Orchestration executes on the SFTP target.

Create the input variables you need in the Inputs form before you can advance to the Execution Command stage.
Role required: activity_creator, admin

**Note:** You can test the JDBC connection between the MID Server and the target without having to run the activity in a workflow context. For details, see [test template outputs](#).

1. Drag variables from the list of inputs and drop them into command fields. The system formats the variable in the proper syntax for the command.

![Diagram of variable drag and drop]

**SFTP execution command**

2. Complete the fields shown in the table.
### SFTP command fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Command</th>
</tr>
</thead>
</table>
| Command                  | Type of activity to create. The choices are:  
  - Copy file  
  - Create directory  
  - Get file list  
  - Remove file or directory  
  - Rename file or directory  
  - Set file attributes                                                                                                           | All                          |
| Note: The fields displayed on the form depend on the command selected.  
| Source host              | Name or IP address of the server containing the files targeted by the activity.                                                                                                                             | All                          |
| Source port              | Port number to use to communicate with the source server. The default port number is 22.                                                                                                                   | All                          |
| Source file path         | Full path to a file on a source host.                                                                                                                                                                         | • Copy file  
  • Remove file or directory  
  • Set file attributes                               |
| Source directory         | Path to the directory where the source files are located.                                                                                                                                                   | • Create directory  
  • Get file list                                  |
| Source files             | Names of specific source files to include in the management action. Separate the file names in this list with semi-colons. This field supports the use of wild cards. If this field is blank, all files are included. For information about how the values in this field are affected by options in other fields, see the section below the table. | Get file list                  |
| Is a directory           | Check box that determines if the specified file path is a directory.                                                                                                                                          | Remove file or directory       |
| Credential tag for source| Specific [credential tagging](<link_to_credential_tagging>) this activity must use to run SFTP commands on the source host.                                                                                       | All                          |
| Field                        | Description                                                                                                                                                                                                 | Command        |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------========================================================================================================================================|----------------|
| Credential tag for target    | Specific credential tag this activity must use to run SFTP commands on the target host.                                                                                                                                                                      | Copy file      |
| Excluded files               | Names of specific source files to exclude from the management action. The activity acts on all other files found in the source directory or subfolders. Separate the file names in this list with semicolons. This field supports the use of wild cards. For information about how the values in this field are affected by options in other fields, see the section below the table. | Get file list  |
| Include subfolders           | Check box to manage the files from subfolders in the source directory. For information about how your selection affects other fields in the form, see the section below the table.                                                                                                     | Get file list  |
| Target host                  | Name or IP address of the server to which the files are being transferred.                                                                                                                                                                                      | Copy file      |
| Target port                  | Port number to use to communicate with the target host. The default port number is 22.                                                                                                                                                                             | Copy file      |
| Target file path             | Full path to a file on a target host.                                                                                                                                                                                                                        | Copy file      |
|                              | • Copy file  
<p>|                              | • Rename file or directory                                                                                                                                                                                                                                 |                |
| Suffix for temporary file    | Temporary suffix to use for a file name if the file already exists on a target host. If this field contains a value, the activity deletes the duplicate target file if it exists, and then copies the source file to a temporary file using <code>targetFilePath + tempFileSuffix</code> as the name. Upon completion, the activity renames the file to the actual target file name. If this field is blank, the activity copies the source file directly to the target file and overwrites it, if it already exists. | Copy file      |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>UID</td>
<td>User ID attribute to apply to a file or directory. The UID and GID values must be set together as a pair or they are ignored.</td>
<td>Set file attributes</td>
</tr>
<tr>
<td>GID</td>
<td>Group ID attribute to apply to a file or directory. The UID and GID values must be set together as a pair or they are ignored.</td>
<td>Set file attributes</td>
</tr>
<tr>
<td>Permissions</td>
<td>File or directory permissions to set for the user and group specified. This value must be expressed as an integer, such as 16877, which defines these permissions: <code>rwxr-xr-x</code>. The permissions number is an internal value returned by the Get File List activity. Typically, you first use the Get File List activity to return a list of files and their attributes. Then you can move a file from a source host to a target host and set the source file attributes on the target file. This is demonstrated in the SFTP File Transfer workflow.</td>
<td>Set file attributes</td>
</tr>
<tr>
<td>Access timestamp</td>
<td>Override the timestamp when the file or directory was last accessed. The access and modification timestamps must be set together as a pair.</td>
<td>Set file attributes</td>
</tr>
<tr>
<td>Modification timestamp</td>
<td>Override the timestamp when the file or directory was last modified. The access and modification timestamps must be set together as a pair.</td>
<td>Set file attributes</td>
</tr>
<tr>
<td>Size in bytes</td>
<td>Size of a file, expressed in bytes.</td>
<td>Set file attributes</td>
</tr>
<tr>
<td>Required MID Server capabilities</td>
<td>MID Server with the appropriate <code>capabilities</code> for connecting to the source and target servers. By default, the system selects an SSH MID Server.</td>
<td>All</td>
</tr>
</tbody>
</table>

The system uses this logic to determine which files to move from the source host:

- If the **Source files** field is empty, the system select all the files in the source directory. Otherwise, it only selects those files whose names match one of the file name patterns given in the field.
• If the Excluded files field is empty, the system excludes nothing. Otherwise, it excludes those files whose names match one of the file name patterns given in the field.
• The exclude rule has a higher preference than the include rule. A file whose name matches one of the file name patterns in the Excluded files field does not get into the selection, even though it would be selected by the include rule.
• When the Include subfolders check box is cleared, the system looks only in the source directory for files to include or exclude. Otherwise, it looks in the source directory and any of its subfolders for files to include or exclude.

3. Click Save.
4. Click Continue to advance to the Outputs stage.

Create a probe activity
Create an activity that runs a probe on the target host that is configured to return specific information.

Role required: activity_creator or workflow_admin
For instructions on using the activity template process flow, see create custom activities.

1. Create a custom activity.
This action creates a custom activity using a template.
2. After setting up general properties and creating input variables, configure the Probe Execution Command:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Map the input variables</td>
<td>Use the variables you created to configure the command that Orchestration executes.</td>
</tr>
<tr>
<td>Probe</td>
<td>Probe to run with this activity, from the list of probes in the system</td>
</tr>
<tr>
<td>Target host</td>
<td>Host name or IP address of the target server for this activity.</td>
</tr>
<tr>
<td>Parameters</td>
<td>MID Server to use, by capabilities.</td>
</tr>
<tr>
<td>Required MID Server capabilities</td>
<td>Name-value pairs to pass to the host with this probe. You can create these parameters manually, or drag and drop input variables into the parameter fields and assign a value.</td>
</tr>
</tbody>
</table>

**Note:** You can map parameter values in a test payload to variables in the Outputs tab automatically. See automap output variables.

• Use auto-mapping to generate outputs and parsing rules
• If you do not use auto-mapping, you can manually create output variables and create parsing rules

Probe template execution parameters
You use execution parameters to create the input process script in the Pre Processing form.
For descriptions of the command fields, see Configure the Probe execution command.

**Note:** You must use the executionParam. prefix with all variables in this table.
### Probe activity execution parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Variable</th>
<th>Type</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probe</td>
<td>probe</td>
<td>Reference</td>
<td>The sys_id of the MID Server probe.</td>
</tr>
<tr>
<td>Source</td>
<td>source</td>
<td>String</td>
<td>Intended target host</td>
</tr>
<tr>
<td>Parameters</td>
<td>parameters</td>
<td>Array of JS object</td>
<td>Array of JavaScript objects, expressed with the executionParam. prefix. To add more name-value pairs to the parameters array, append them to the existing array. Create a JavaScript object with the following syntax, and add it to the executionParam.parameter array. This assigns additional parameters to the message:</td>
</tr>
<tr>
<td>MidCapabilities</td>
<td>midCapabilities</td>
<td>String (comma separated)</td>
<td>List of required MID server capabilities.</td>
</tr>
<tr>
<td>ValueCapabilities</td>
<td>valueCapabilities</td>
<td>Array of hashmap</td>
<td>Capability values used to select the MID Server. For more information, see Set up domain separation for MID servers. If there are additional capabilities that are assigned by value, use this example to customize the MID Server selection:</td>
</tr>
</tbody>
</table>

**Probe template post-processing parameters**

Use these parameters to create a post-processing script.
### Probe post-processing parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Variable</th>
<th>Type</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payload</td>
<td>payload</td>
<td>String</td>
<td>Contains raw payload returned from the probe.</td>
</tr>
<tr>
<td>Output</td>
<td>output</td>
<td>String</td>
<td>Contains output data returned from the probe.</td>
</tr>
<tr>
<td>EccSysId</td>
<td>eccSysId</td>
<td>String</td>
<td>Contains the reference ID associated with the ECC Queue input message.</td>
</tr>
</tbody>
</table>

**Configure the Probe execution command**

Use the input variables you created to configure the command that Orchestration executes on the target.

Create the input variables you need in the Inputs form before you can advance to the Execution Command stage.

Role required: activity_creator, admin

**Note:** You can test the activity connection between the MID Server and the target without having to run the activity in a workflow context. For details, see test template outputs.

1. Drag variables from the list of inputs and drop them into command fields.
   The system formats the variable in the proper syntax for the command.
2. Complete the fields shown in the table.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>max_discovery_payload_size</td>
<td>$(activityInput.maxDiscoveryPayload)</td>
</tr>
<tr>
<td>max_http_payload_size</td>
<td>$(activityInput.maxHttpPayload)</td>
</tr>
<tr>
<td>must_sudo</td>
<td>$(activityInput.mustSudo)</td>
</tr>
<tr>
<td>string/ai</td>
<td>$(activityInput.string/ai)</td>
</tr>
</tbody>
</table>
Probes execution command fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>Input variable builder. <a href="#">Create input variables</a> to map to available fields.</td>
</tr>
<tr>
<td>Probe</td>
<td>Probe to run with this activity, from the list of probes in the system.</td>
</tr>
<tr>
<td>Target host</td>
<td>Host name or IP address of the target server for this activity.</td>
</tr>
<tr>
<td>Required MID Server capabilities</td>
<td>MID Server to use, by capabilities.</td>
</tr>
<tr>
<td>Parameters</td>
<td>Name-value pairs to pass to the host with this probe. You can create these parameters manually, or drag and drop input variables into the parameter fields and assign a value.</td>
</tr>
</tbody>
</table>

3. Click **Save**.
4. Click **Continue** to advance to the **Outputs** stage.

**Create an SSH activity**

Create an activity that extracts data from a target host that uses the SSH network protocol.

Role required: activity_creator or workflow_admin

For instructions on using the activity template process flow, see [create custom activities](#).

1. Create a **custom activity**.
   This action creates a custom activity using a template.

2. After setting up **general properties** and **creating input variables**, configure the SSH Execution Command:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Map the input variables</strong></td>
<td>Use the variables you created to configure the command that Orchestration executes.</td>
</tr>
<tr>
<td><strong>Target host</strong></td>
<td>Host name or IP address of the target server for this activity.</td>
</tr>
<tr>
<td><strong>Command</strong></td>
<td>Command this activity runs on the target host. You can invoke a MID Server script from this field using any script type that the SSH command line supports. For more information, see <a href="#">Advanced SSH script options</a> below the table.</td>
</tr>
<tr>
<td><strong>Directory</strong></td>
<td>Directory on the target host where the command is run.</td>
</tr>
<tr>
<td><strong>Credential tag</strong></td>
<td>The Orchestration credential tag to use when running the command.</td>
</tr>
<tr>
<td><strong>Required MID Server capabilities</strong></td>
<td>MID Server with the appropriate capabilities for connecting to the host. By default, the system selects a MID Server with SSH capabilities.</td>
</tr>
<tr>
<td><strong>Long running</strong></td>
<td>If checked, disables the SSH connection timeout for commands that might take longer to run than the default 60 seconds. Orchestration periodically checks the running process to determine its status until it is finished.</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>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Must Sudo</td>
<td>If checked, enables the use of <code>sudo</code> to run commands.</td>
</tr>
</tbody>
</table>

**Note:** You can map parameter values in a test payload to variables in the **Outputs** tab automatically. See automap output variables.

### Advanced SSH script options

To run a MID Server script on the target host, specify the script type and pass the name of the script into the `${syncFile()}` parameter. The system uses this parameter to locate the named script in the MID Server Script File (ecc_agent_script_file) table and run it on the target host. For example, a bash script can be expressed as:

```bash
bash `${syncFile("<MID script name>")}` argument1 argument2 argument3
```

A base script (`main_script.bash`) can reference another script (`my_include.bash`) as well as a separate file (`.my_profile`) located on the target host. Both scripts and the file referenced must be synced to the MID Server, using the `${syncFile()}` parameter, to execute properly.

```bash
source `${syncFile(".my_profile")}`
cp `${syncFile("my_include.bash")}` /usr/ssmith/my_include.bash
bash `${syncFile("main_script.bash")}` one two three four five six
rm /usr/ssmith/my_include.bash
```

A Python example with inline comments might look like this:

```python
set $LIB_DIR=/usr/bin;
# Sync a file that is referenced inside myF5CreateLBPool.py
cp `${syncFile("specialFunctions.py")}` ~/specialFunctions.py
# set up environment variables
source `${syncFile(".python_profile")}`
# call script that sets up dependencies on the box from remote package repos
python `${syncFile("setupPythonDependencies.py")}` pycontrol
# call a script that requires functions from the package as well as a function from myIncludedFile
python `${syncFile("myF5CreateLBPool.py")}` snow_pool myActualValue
# user is responsible for their own cleanup
rm ~/specialFunctions.py
```

- Use **auto-mapping** to generate outputs and parsing rules
- If you do not use auto-mapping, you can manually create output variables and create parsing rules

**SSH template execution parameters**

Use execution parameters to create the input process script in the **Pre Processing** form of the activity designer.

For descriptions of the command fields, see Configure the SSH execution command.
Note: You must use the `executionParam` prefix with all variables in this table.

### SSH execution parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Variable</th>
<th>Type</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td><code>source</code></td>
<td>String</td>
<td>Intended target or host.</td>
</tr>
<tr>
<td>Command</td>
<td><code>command</code></td>
<td>String</td>
<td>Comment to run on the host.</td>
</tr>
<tr>
<td>Directory</td>
<td><code>directory</code></td>
<td>String</td>
<td>Directory on the host in which to run the command.</td>
</tr>
<tr>
<td>Credential tag</td>
<td><code>credential_tag</code></td>
<td>String</td>
<td>Orchestration credential tag to use when running the command.</td>
</tr>
<tr>
<td>MidCapabilities</td>
<td><code>midCapabilities</code></td>
<td>String (comma separated)</td>
<td>List of required MID Server capabilities.</td>
</tr>
<tr>
<td>ValueCapabilities</td>
<td><code>valueCapabilities</code></td>
<td>Array of hashmap</td>
<td>Capability values used to select the MID Server. For more information, see <a href="#">Set up domain separation for MID servers</a>. If there are additional capabilities that are assigned by value, use this example to customize the MID Server selection:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><code>var valueCapability = {'NEW_MID_CAPABILITY': 'NEW_MID_CAPABILITY_VALUE'};</code> executionParam.valueCapabilities.push(valueCapability);</td>
</tr>
<tr>
<td>Long running</td>
<td><code>long_running</code></td>
<td>Boolean</td>
<td>Indicates whether or not the command is long running. A value of true indicates that the command is long running.</td>
</tr>
<tr>
<td>Must sudo</td>
<td><code>must_sudo</code></td>
<td>Boolean</td>
<td>Indicates whether or not this activity must use sudo to run root commands. A value of true indicates that <code>sudo</code> must be used.</td>
</tr>
</tbody>
</table>

### SSH post-processing parameters and payload parsing

Use these parameters to create a post-processing script, payload parsing, and tagging.
**SSH post-processing parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Variable</th>
<th>Type</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output</td>
<td>output</td>
<td>String</td>
<td>Contains the output returned from the SSH command.</td>
</tr>
<tr>
<td>EccSysID</td>
<td>eccSysID</td>
<td>String</td>
<td>Contains the reference ID associated with the ECC Queue input message returned by the activity.</td>
</tr>
<tr>
<td>ErrorMessages</td>
<td>errorMessages</td>
<td>String</td>
<td>Contains the error messages retrieved from the SSH command. This value is null if there are no error messages.</td>
</tr>
<tr>
<td>Tags</td>
<td>tags</td>
<td>Hashmap of tag values returned from the SSH command</td>
<td>Contains the tags used to extract output using the SSH commands. The tag output is delimited by double percentage signs, as in %tagname %% ... %%. Set up the command using the following format:</td>
</tr>
</tbody>
</table>
|          |          |            | %tagname1%%
output1 line 1
output1 line 2
...
%%

%tagname2%%
output2 line 1
output2 line 2
...
%%

The tags returned are JavaScript hashmap objects in which each key is prefixed with tag appended with the tagname.

```javascript
{"__text__":
"",
"tagtagname1":"output1 line1\noutput1 line2\n",
"tagtagname2":"output2 line1\noutput2 line2\n"}
```
Configure the SSH execution command
Use the input variables you created to configure the command that Orchestration executes on the host target.

Create the input variables you need in the Inputs form before you advance to the Execution Command stage.

Role required: activity_creator, admin

**Note:** You can test the SSH connection between the MID Server and the target without having to run the activity in a workflow context. For details, see test template outputs.

1. Drag variables from the list of inputs and drop them into command fields.
   The system formats the variable in the proper syntax for the command.
SSH execution command

2. Complete the fields shown in the table.
### SSH activity inputs

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>Input variable builder. <a href="#">Create input variables</a> to map to available fields.</td>
</tr>
<tr>
<td>Target host</td>
<td>Host name or IP address of the target server for this activity.</td>
</tr>
<tr>
<td>Command</td>
<td>Command this activity runs on the target host. You can invoke a MID Server script from this field using any script type that is supported by the SSH command line. For more information, see <a href="#">Advanced SSH script options</a> below the table.</td>
</tr>
<tr>
<td>Directory</td>
<td>Directory on the target host where the command is run.</td>
</tr>
<tr>
<td>Credential tag</td>
<td>The Orchestration <a href="#">credential tag</a> to use when running the command.</td>
</tr>
<tr>
<td>Select MID Server by capabilities</td>
<td>MID Server with the appropriate capabilities for connecting to the host. By default, the system selects a MID Server with SSH capabilities</td>
</tr>
<tr>
<td>Long running</td>
<td>Check box to disable the SSH connection timeout for commands that might take longer to run than the default 60 seconds. Orchestration periodically checks the running process to determine its status until it is finished.</td>
</tr>
<tr>
<td>Must Sudo</td>
<td>Check box to allow the use of <a href="#">sudo</a> to run commands.</td>
</tr>
</tbody>
</table>

3. Click **Save**.
4. Click **Continue** to advance to the **Outputs** stage.

### Create a run script activity

Create an activity that runs any script.

Role required: activity_creator or workflow_admin

1. Create a [custom activity](#).
   This action creates a custom activity using a template.
2. After setting up [general properties](#) and [creating input variables](#), configure the Run Script Execution Command:
   Create a script for this activity to execute.

   **Note:** You can map parameter values in a test payload to variables in the Outputs tab automatically. See [automap output variables](#).

   - Use [auto-mapping](#) to generate outputs and parsing rules
Run Script template processing script
Use the Run Script custom template Script form to enter a script to call and use with other activities.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processing script</td>
<td>Script that the activity runs.</td>
</tr>
<tr>
<td>Variables</td>
<td>Input variables that are available to use as building blocks in the input process script. Click the arrow above the field to open the variables list. Click an item in the tree to add it to your script in the appropriate syntax. The list displays input variables you passed into the activity on the Inputs form. All activity variables added in the Inputs form are read-only and are expressed in the processing script with this syntax: activityInput.variable.</td>
</tr>
</tbody>
</table>

Create a JMS activity
Create a custom JMS activity to retrieve or send messages to external systems using the Java Messaging Service.

Role required: activity_creator or workflow_admin

The JMS activity supports third party JMS providers whose JMS client application is written with a typical Java EE pattern and can support these operations:

- Using JNDI to find aConnectionFactory object.
- Using JNDI to find one or more destination objects.
- Using the ConnectionFactory to create a JMS connection object.
- Using the JMS connection to create one or more JMS session objects.
- Using a JMS session and the destinations to create the MessageProducer and MessageConsumer objects.
- Starting the JMS connection to enable delivery or consumption of messages.

Note: The JMS activity designer has been tested with the JMS providers ActiveMQ and Tibco EMS. When connecting to a JMS provider, refer to your third party user documentation.

1. Create or verify your JMS credential.
   Your JMS credentials must have permission for the target database and proper configuration for the corresponding JMS connection. Credentials must be set up before you can create a JMS activity.
2. Create or verify your JMS connection.
   Your JMS connection must be configured with valid JMS credentials set up before you can create a JMS activity.
3. Create a custom activity.
   This action creates a custom activity using a template.
4. After setting up general properties and creating input variables, configure the JMS Execution Command:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure your credential</td>
<td>Fill in the fields necessary for your database connection.</td>
</tr>
<tr>
<td><strong>Connection Factory</strong></td>
<td>Name of the JMS Connection Factory. You should create or verify your JMS connection. This configuration links the name of the Initial Context Factory with the URL of the JMS provider.</td>
</tr>
<tr>
<td><strong>Destination Type</strong></td>
<td>Type of destination used for this message:</td>
</tr>
<tr>
<td>- Queue</td>
<td>Message is queued for point-to-point communications.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>The GET operation is only supported for the Queue destination type.</td>
</tr>
<tr>
<td>- Topic</td>
<td>Message is used for publish and subscribe communication.</td>
</tr>
<tr>
<td><strong>Destination Name</strong></td>
<td>Name of the queue or topic destination that is configured on the JMS provider.</td>
</tr>
<tr>
<td><strong>Message Type</strong></td>
<td>The JMS message type value. Only the Text Message type is supported. The queue or topic destination must be configured to receive or send only Text Message. Other message types are dropped, since the JMS Activity cannot process them.</td>
</tr>
<tr>
<td><strong>Operation</strong></td>
<td>The programmatic operation to perform on the destination. The choices are PUT or GET.</td>
</tr>
<tr>
<td><strong>Timeout (Secs)</strong></td>
<td>Allowed time to wait for a message in the message queue before it times out, in seconds. The default is 30.</td>
</tr>
<tr>
<td><strong>Custom message headers</strong></td>
<td>The custom header values in a name/value pair format, that is available on the JMS destination.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>This is only supported for a PUT operation.</td>
</tr>
<tr>
<td><strong>Message payload</strong></td>
<td>Actual message content or payload that is sent to the JMS destination.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>This is only supported for a PUT operation.</td>
</tr>
<tr>
<td><strong>Credential tag</strong></td>
<td>A tag for an individual credential for a JMS activity in an Orchestration workflow.</td>
</tr>
<tr>
<td><strong>Required MID Server capabilities</strong></td>
<td>MID Server to use, by capabilities.</td>
</tr>
</tbody>
</table>

- Use **auto-mapping** to generate outputs and parsing rules
- If you do not use auto-mapping, you can manually create output variables and create parsing rules

Create a JMS connection for an Orchestration activity
Configure your system to use Java Messaging Service (JMS) with a custom Orchestration JMS activity.
Role required: admin

The MID Server must have the correct JMS connection factories for your organization. Configure those values in the `mid.property.jms.command.allowed_factory_names` property, found in MID Server > Properties. The default values for this property can be changed to any value or comma-separated list of values that the third-party JMS provider advertises.

1. Navigate to MID Server > JAR Files.
2. Click New and add:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique and descriptive name for identifying the file in the instance.</td>
</tr>
<tr>
<td>Version</td>
<td>A version number for the file, if one is available.</td>
</tr>
<tr>
<td>Source</td>
<td>Location of the JAR file for reference purposes. Source information is not used by the system.</td>
</tr>
<tr>
<td>Description</td>
<td>Short description of the JAR file and its purpose in the instance.</td>
</tr>
</tbody>
</table>

3. Click the paper clip icon in the banner and attach the JMS driver jar file.

The JMS driver jar file should be available as part of JMS provider installation. Few JMS vendors make them available as a separate product. Refer to the JMS provider documentation to determine which JMS client driver jar files require the client applications to connect to the JMS provider. For example, if you are trying to connect to ActiveMQ V5.10 (JMS provider), you need the `activemq-all-5.10.1.jar` file.

5. Click New, add the following, and click Submit:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name of this connection factory.</td>
</tr>
<tr>
<td>Initial Context Factory</td>
<td>Name of the JNDI class that is used to create the InitialContext.</td>
</tr>
<tr>
<td>Note: For example, to connect to ActiveMQ V5.10 (JMS Provider), the value is org.apache.activemq.jndi.ActiveMQInitialContextFactory.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Provider URL</th>
<th>Location of the running JMS provider installation.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note: For example, to connect to ActiveMQ V5.1: tcp://ipAddressOrHostName:61616.</td>
<td></td>
</tr>
</tbody>
</table>

6. Navigate to Orchestration > Credentials.
7. Click New, select JMS Credentials, and provide the user name and password the MID should use to communicate with the JMS provider.

For more information, see JMS credentials.

8. Click Submit.

You are ready to create a custom JMS activity.

**JMS template execution parameters**

You use execution parameters to create the input process script in the Preprocessing form.

You must use the `executionParam.` prefix with all variables in this table.
### JDBC execution parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Variable</th>
<th>Type</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jms ds</td>
<td>jms_ds</td>
<td>Reference</td>
<td>Selected JMS data source.</td>
</tr>
<tr>
<td>Destination type</td>
<td>destination_type</td>
<td>Enumerated</td>
<td></td>
</tr>
<tr>
<td>Destination name</td>
<td>destination_name</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>Message type</td>
<td>message_type</td>
<td>Enumerated</td>
<td></td>
</tr>
<tr>
<td>Operation</td>
<td>operation</td>
<td>Enumerated</td>
<td></td>
</tr>
<tr>
<td>Time out</td>
<td>time_out</td>
<td>Integer</td>
<td>Length of time to wait for the query to return results.</td>
</tr>
<tr>
<td>Custom headers</td>
<td>custom_headers</td>
<td>Array of JavaScript objects</td>
<td></td>
</tr>
<tr>
<td>Message payload</td>
<td>message_payload</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>Credential tag</td>
<td>credential_tag</td>
<td>String</td>
<td>List of required MID Server capabilities.</td>
</tr>
<tr>
<td>MidCapabilities</td>
<td>midCapabilities</td>
<td>String (comma separated)</td>
<td></td>
</tr>
<tr>
<td>ValueCapabilities</td>
<td>valueCapabilities</td>
<td>Array of hashmap</td>
<td>Capability values used to select the MID Server. For more information, see <a href="#">Set up domain separation for MID servers</a>. If there are additional capabilities that are assigned by value, use this example to customize the MID Server selection:</td>
</tr>
</tbody>
</table>

```javascript
var valueCapability = {'NEW_MID_CAPABILITY': 'NEW_MID_CAPABILITY_VALUE'};
executionParam.valueCapabilities.push(valueCapability);
```

### JMS template post-processing parameters

Use these parameters to create a post-processing script.

#### JMS post-processing parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Variable</th>
<th>Type</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>status</td>
<td>String</td>
<td>Status of the operation (Put or Get) on the JMS destination.</td>
</tr>
<tr>
<td>Name</td>
<td>Variable</td>
<td>Type</td>
<td>Usage</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------</td>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>StandardHeaders</td>
<td>standardHeaders</td>
<td>String</td>
<td>All the standard headers, as specified by JMS, that are obtained as part of the JMS message during a Get operation. This field is applicable only for Get operations.</td>
</tr>
<tr>
<td>CustomHeaders</td>
<td>customHeaders</td>
<td>String</td>
<td>All custom headers added by a producer or publisher application that are obtained as part of the JMS message during a Get operation. This field is applicable only for Get operations.</td>
</tr>
<tr>
<td>MessagePayload</td>
<td>messagePayload</td>
<td>String</td>
<td>Message payload that is obtained as part of the JMS message during a Get operation. This field is applicable only for Get operations.</td>
</tr>
<tr>
<td>EccSysID</td>
<td>eccSysID</td>
<td>String</td>
<td>Contains the reference ID associated with the ECC Queue input message returned by the activity.</td>
</tr>
<tr>
<td>ErrorMessages</td>
<td>errorMessages</td>
<td>String</td>
<td>Contains any error messages retrieved from the JMS command. This value is <strong>null</strong> if there are no error messages.</td>
</tr>
</tbody>
</table>

### Activity scoping

Custom activities run in their own scope, even if it is different from that of the workflow.

Any script that runs inside a custom activity with a scope can only access outside artifacts that are within the scope of that activity or artifacts that are configured to run in any scope. Conversely, an outside artifact can only access the script inside that private activity if the outside artifact is running in the same scope. Activities with public scopes can interact with outside artifacts in any application scope.

You can use private activities as part of a workflow that has a public application scope. These activities are protected from reaching outside of the workflow or from being reached from outside the workflow. For details about setting application scoping for custom activities, see the field description table for the appropriate activity template.

**Note:** Custom activities uploaded to the ServiceNow Store must be configured as accessible to all application scopes.
Publish a custom activity

When a user creates a custom activity and saves or submits it, that activity appears in the Custom and Packs tabs of the designer palette, but is visible only to the user who created it.

Roles required: admin, activity_admin, activity_creator

1. When you finish configuring the activity, click Publish.
   
   This makes the activity accessible to other users on the instance with the workflow_admin or activity_creator role. Published activities are available for upload to the ServiceNow Store, can be added to workflows, and can be edited by any user with the proper roles.

2. To edit a published activity, click Checkout.

   When an activity is checked out by a user, only that user can modify it. The fields of a checked out activity are read-only for all other users.

3. When you are finished editing the checked out activity, publish it again.

   The system adds a new version of this activity to the Custom tab in the workflow editor palette.

   **Note:** Activities you create and publish are visible in the Packs tab only if they were created in the current application scope.

Return a locked activity to a published state

Problems can arise if an activity version is checked out by a user and not checked back in. An activity in this state cannot be checked out for update.

**Role required:** admin, activity_admin, activity_creator

An administrator can return a locked activity to a published state.

1. Open the workflow editor.

2. From the Custom tab, open the activity that is locked.

3. Click the menu icon in the title bar and select Versions from the context menu.

   A list of all the versions of that activity appears. The locked version displays the user who checked it out.
4. Select the checked out version.
   The system opens the record in the activity designer.

5. Click the menu icon again and select **Force Checkout** from the context menu.
   The activity fields become editable.

6. Click **Publish**.
   The activity becomes available to users with the appropriate roles.

**Copy a custom activity**

You can copy activities for reuse from the **Custom** tab in the global scope.

Role required: admin, activity_admin, activity_creator

**Note:** You cannot copy an activity in a private scope.

1. To reuse an activity in the global scope, expand the parent category to display the activities.
2. Right-click the activity you want to copy and select one of these options:
   - Copy into global scope as new activity: Copies the activity with the new name you provide, uses the same version number as the original activity, and moves it to the global scope in the **Custom** tab.
Naming an activity copy

- Copy into global scope as new version: Copies the activity using the same name, increments the version number, and moves it to the global scope in the Custom tab. The system automatically adds the parent category to the Custom tab if it does not already exist. This action will overwrite another activity with the same name and version number.

Creating a new activity version

**Note:** If the activity is in any other scope but global, the system displays this message: Cannot copy privately scoped activity.

Orchestration databus

The databus allows workflow designers to track the flow of data through an Orchestration workflow and provides access to output data that can be consumed by other custom activities.

Data is made available in a workflow when you use activities created with the Orchestration activity designer. The activity designer provides the ability to specify well defined inputs and outputs for your activities. When you use those activities on the workflow canvas, the outputs appear in the Data tab and are available for use as inputs in subsequent activities.

**Note:** Orchestration does not filter the data you are given for reuse in the Data tab. You must make sure an activity in the workflow canvas has executed before you consume its output data.

When you drop a custom activity onto the workflow canvas, the system assigns it an index. If you delete an activity from the canvas and add a new one, the indexes are not reused. This ensures that you don’t accidentally start subscribing to data you did not intend to use. If you update an activity in the activity designer, the system automatically updates the activity on the canvas to ensure the data you are subscribing to downstream is not affected.
Reuse data in the activity designer

The Data tab in the Workflow Editor lists all custom activities used in the current workflow that produce data and displays that data for reuse in other custom activities.

Roles required: workflow_creator

Activities are categorized by application in this tab and are available for use as data sources for other activities. The Data tab is a graphical representation of the workflow databus, which manages all the temporary data used by the current workflow.

1. Drag output variables from an activity in this tab into the inputs of another activity on the workflow canvas to link the activities together.

   You can use any of the outputs in the structure, regardless of the application to which they belong. An index number in parenthesis after the activity name provides a unique identifier for the parameters that you use as input data in other activities. If you do not name a custom activity, the only identifier for that activity in the Data tab is the index number. Index numbers indicate the sequence in which custom activities were added to the workflow and are not reused. When you drag a custom activity onto the workflow canvas, the system adds that activity and its output data to the structure. Conversely, if you remove a custom activity from the canvas, that activity and its outputs disappear from the data list.

2. Point to an activity to display information about it in a pop-up window.

   Any output data reused by the activity is listed in the Databus Output field of the pop-up window.
MID Servers for Orchestration

Orchestration automatically selects an appropriate MID Server based on the capabilities that you configure in activities, the IP addresses of target devices, and the application that the MID Server is allowed to use.

To allow a MID Server to work with Orchestration, it must have the Orchestration application or the All application assigned to it. See Configure a default MID Server for each application for instructions.

You can have MID Servers focus on different capabilities and separate sections of your network. See:

- MID Server capabilities
- Map an IP address to a DNS name

You can also specify a default MID Server to use if no MID Servers meet the capability and IP range criteria for an activity. See Select the default MID Server for Orchestration.

MID Server capabilities

MID Server capabilities define the specific functions of a MID Server within an IP address range.

Several applications, such as Discovery, Service Mapping, and Orchestration can use capabilities, IP ranges, and the supported application to narrow the pool of MID Servers it uses. At least one capability is required for each MID Server used by Orchestration. See MID Servers for Orchestration for more information.

The following capabilities are available by default with Discovery:

- SSH
- SNMP
MID Server capability values

Capabilities provided in the base system do not have a defined Value string. A MID Server configured to use a capability that has no Value can locate any device using that capability’s protocol. If a capability has a defined value, the MID Server using that capability finds only those devices using that protocol that match the value string exactly. The exception to this is the Resolve DNS capability, which is configured to resolve any DNS name into an IP address using a partial string match.

Scripted MID Server capability value matching

You can use value tests to create capabilities that find devices using values without requiring exact string matching. Action on these values is controlled by a user-defined script.

The Resolve DNS capability is provided in the base system and is configured to resolve DNS names into IP addresses for devices whose names end with a specified domain name. The capability Value entered is automatically prefaced with a dot during processing to match domain syntax. This value can contain one or more sub-domains, but must include the end of the domain string. Matching devices must end with the identical syntax. The script for the Resolve DNS capability determines if a device name matches the criteria defined by Value. If a match exists, the platform performs the address resolution automatically. For example, if the value for the Resolve DNS capability is service-now.com, the MID Server with this capability finds lnxlab01.sandiego.service-now.com and dbsrv101.sanjose.service-now.com. If the value is changed to sandiego.service-now.com, then the MID Server finds only lnxlab01.

Note: If Value in the Resolve DNS capability is blank, then all domains match.

To view the script for evaluating this capability, navigate to MID Server > Capability Value Tests and select Resolve DNS from the list.
Configure MID Server capabilities

A capability is required for each MID Server to work with Orchestration, Service Mapping, Cloud Management, and Service Analytics.

Role required: admin or sm_admin

1. Navigate to **MID Server > Capabilities**.
2. Select an existing capability. You can also select **ALL** to include all capabilities.

   **Note:** Ensure that each IP address range has MID Servers with the necessary capabilities to complete the Orchestration activities on that network segment.

3. Create a new capability:
   a) Click **New**.
   b) Configure the value for a custom capability. An example is a capability for **DOMAIN**, with a value of **service-now**.
   c) Click **Submit**.

4. Click **Edit** in the MID Servers related list to add MID Servers to the capability.
5. Select one or more MID Servers for this capability from the slushbucket.
6. Click Save.

The capability defined here also appears in the primary record for this MID Server.

**Select the default MID Server for Orchestration**

Orchestration uses the default MID Server if it cannot find a MID Server with the correct IP range and capability.

Specify the default MID Server in either of these locations:

- The **Default MID Server** field on the Orchestration application record. See [Configure a default MID Server for each application](#) for instructions.
- The **Default MID Server to use for Orchestration Activities** property. Navigate to Orchestration > MID Server Properties to set this value.

These two values are automatically kept in synch. You can change the default MID Server in either location.

**Use the Orchestration Usage dashboard**

This dashboard shows an overview of Orchestration usage metrics to show customers how their organization uses Orchestration and to support license compliance.

Role required: orchestration_manager

1. To view the dashboard, navigate to Orchestration > Operations & Troubleshooting > Orchestration Usage Dashboard.

   The Orchestration Usage dashboard displays. The tabs on the dashboard include Licensable Usage and Orchestration Usage. Reports on these tabs include:

   **Orchestration Usage Metrics**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction Summary Last 12 months</td>
<td>A running transaction count of all Orchestration transactions over the last 12 months. Includes:</td>
</tr>
<tr>
<td></td>
<td>- The count of orchestration transactions associated with the HR Application</td>
</tr>
<tr>
<td></td>
<td>- The count of Orchestration transactions associated with the Security Operations Application</td>
</tr>
<tr>
<td>Transaction Summary YTD</td>
<td>Cumulative count of all transactions since the time the Orchestration plugin was activated or the customer upgraded to Geneva.</td>
</tr>
<tr>
<td>365 day Running Average of Server</td>
<td>The running average over the last 365 days for cmdb_ci_computer - cmdb_ci_server. This includes all physical and virtual client nodes and excludes server nodes from the count.</td>
</tr>
<tr>
<td>365 day Running Average of Client</td>
<td>The running average over the last 365 days for cmdb_ci_server. This includes all physical and virtual server nodes.</td>
</tr>
</tbody>
</table>
### ServiceNow® Jakarta Now Platform Capabilities

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orchestration Transactions by Month for Last 12 Months</td>
<td></td>
</tr>
<tr>
<td>Average Client Nodes Orchestrated Last 365 Days</td>
<td></td>
</tr>
<tr>
<td>Average Server Nodes Orchestrated Last 365 Days</td>
<td></td>
</tr>
<tr>
<td>Number of Orchestration Activities Developed Last 365 Days</td>
<td>The aggregate number of activity definitions you have developed and OOB activity definitions you have modified. This number includes activity elements (Activities build with the Activity Designer) you have developed and OOB activity definitions you have modified.</td>
</tr>
<tr>
<td>Cumulative Client Nodes Orchestrated by Month</td>
<td></td>
</tr>
<tr>
<td>Cumulative Server Nodes Orchestrated by Month</td>
<td></td>
</tr>
<tr>
<td>Usage by Provider Last 12 Months</td>
<td>Breaks down emphasis by provider, such as PowerShell, JDBC, SSH, etc.</td>
</tr>
<tr>
<td>Top 10 Orchestration Activities</td>
<td></td>
</tr>
</tbody>
</table>

2. Optional: You can add more widgets to the dashboard by clicking the **Add Content** icon in the upper right corner of the dashboard.

**Note:** You should not modify the first tab in this Dashboard. If you want a different dashboard experience, add a tab and customize that with your usage reports.

---

### Password Reset and Password Change applications

The ServiceNow® Password Reset application enables an end user to use a self-service process to reset the password. Alternatively, your organization can implement a process that requires a service desk agent to reset passwords for end users.

**Explore**
- **Password Reset release notes**
- **Upgrade to Jakarta**

**Set up**
- **Password Reset setup guide**

**Administer**
- **Password Reset admin guide**

**Use**
- **Service desk: Reset a password for a user**

**Develop**
- **Developer training**

**Integrate**
- **Integrate Password Reset with a CMS integration**

© 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.
password reset setup guide

A simple version of the Password Reset application is active by default. You can install a plugin to extend functionality.

Requirements

Role required: admin

What is installed

- Password Reset is active by default and includes example verifications. The base system enables connections only to the Local ServiceNow Instance credential store type. For details, see Credential stores for Password Reset.

- To enable connections to Active Directory (AD) and Remote (SOAP) ServiceNow Instance credential store types, you must activate the Password Reset - Orchestration Add-on plugin. The plugin also activates the Password Reset Windows Application (com.glideapp.password_reset_desktop). No other components are installed. Orchestration is available as a separate subscription. See Activate the Password Reset - Orchestration Add-on plugin.

Next steps

Plan and configure the Password Reset processes for your organization. See the Password Reset admin guide.

Activate the Password Reset - Orchestration Add-on plugin

The Password Reset - Orchestration Add-on plugin activates the Password Reset Windows Application (com.glideapp.password_reset_desktop) and enables connections to the Active Directory (AD) and 'Remote (SOAP) ServiceNow instance' credential store types. No other components are installed.

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>
<tr>
<td>Reason/Comments</td>
<td>Any information that would be helpful for the ServiceNow personnel activating the plugin such as 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**.

**Installed with Password Reset**

Tables, roles, business rules, scripts, and workflows are installed with the Password Reset application.

**Password Reset tables**

<table>
<thead>
<tr>
<th>Table name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Reset Active Answer (pwd_active_answer)</td>
<td>Security questions and associated answers, in an encrypted state, that users have selected while going through the enrollment process.</td>
</tr>
<tr>
<td>Password Reset Active Question (pwd_active_question)</td>
<td>Security questions that users have selected while going through the enrollment process.</td>
</tr>
<tr>
<td>Password Reset Activity Log (pwd_reset_activity)</td>
<td>All Password Reset requests.</td>
</tr>
<tr>
<td>Password Reset Activity Monitor (pwd_activity_monitor)</td>
<td>Password Reset lockout activity.</td>
</tr>
<tr>
<td>Password Reset Credential Store (pwd_cred_store)</td>
<td>Password Reset credential stores that are available.</td>
</tr>
<tr>
<td>Password Reset Credential Store Parameters (pwd_cred_store_param)</td>
<td>User-created credential store parameters.</td>
</tr>
<tr>
<td>Table name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Password Reset Credential Store Types (pwd_cred_store_type)</td>
<td>Password Reset credential store types that are available.</td>
</tr>
<tr>
<td>Password Reset Desktop Access Control (pwd_access_control)</td>
<td>Password Reset Windows Application access control.</td>
</tr>
<tr>
<td>Password Reset Desktop Access Log (pwd_access_log)</td>
<td>Password Reset Windows Application access logs.</td>
</tr>
<tr>
<td>Password Reset Device Enrollment Code (pwd_dvc_enrollment_code)</td>
<td>Device enrollment codes that have been sent to users during SMS code enrollment.</td>
</tr>
<tr>
<td>Password Reset Devices (pwd_device)</td>
<td>User SMS devices that are in a state of verified.</td>
</tr>
<tr>
<td>Password Reset Enrollment for Verification (pwd_enrollment)</td>
<td>Information about user enrollment by verification.</td>
</tr>
<tr>
<td>Password Reset Enrollment Snapshot (pwd_enrollment_snapshot)</td>
<td>Snapshot of user enrollment by verification. This table is regenerated daily by a scheduled job named Password Reset Enrollment Snapshot.</td>
</tr>
<tr>
<td>Password Reset Extension Type (pwd_extension_type)</td>
<td>Extension types that are available.</td>
</tr>
<tr>
<td>Password Reset Identification Type (pwd_identification_type)</td>
<td>Password Reset identification types that are available.</td>
</tr>
<tr>
<td>Password Reset Process (pwd_process)</td>
<td>Password Reset processes that are available.</td>
</tr>
<tr>
<td>Password Reset Process Credential Store (pwd_map_proc_to_cred_store)</td>
<td>Credential stores and the associated Password Reset processes that the application is using.</td>
</tr>
<tr>
<td>Password Reset Process User Group (pwd_map_proc_to_group)</td>
<td>Groups and the associated Password Reset processes that the application is using.</td>
</tr>
<tr>
<td>Password Reset Process Verification (pwd_map_proc_to_verification)</td>
<td>Verifications and the associated Password Reset processes that the application is using.</td>
</tr>
<tr>
<td>Password Reset Question (pwd_question)</td>
<td>Questions that the application uses for security question verifications.</td>
</tr>
<tr>
<td>Password Reset Request (pwd_reset_request)</td>
<td>Information about Password Reset requests.</td>
</tr>
<tr>
<td>Password Reset SMS Verification Code (pwd_sms_code)</td>
<td>SMS verification codes that have been sent to users for a password reset.</td>
</tr>
<tr>
<td>Password Reset User Lockout (pwd_user_lockout)</td>
<td>Users that are locked out of Password Reset.</td>
</tr>
<tr>
<td>Password Reset Verification (pwd_verification)</td>
<td>Verifications that are available.</td>
</tr>
</tbody>
</table>
### Password Reset roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>password reset administrator</td>
<td>Configures and maintains Password Reset and Password Change.</td>
</tr>
<tr>
<td>(password_reset_admin)</td>
<td></td>
</tr>
<tr>
<td>service desk agent</td>
<td>Resets passwords on behalf of users, tracks password reset requests, and views logs.</td>
</tr>
<tr>
<td>(password_reset_service_desk)</td>
<td></td>
</tr>
<tr>
<td>credentials manager</td>
<td>Determines which credential stores are valid for use with Password Reset.</td>
</tr>
<tr>
<td>(password_reset_credential_manager)</td>
<td></td>
</tr>
</tbody>
</table>

### Password Reset business rules

<table>
<thead>
<tr>
<th>Business rule</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add default parameters QA verification</td>
<td>Password Reset Verification (pwd_verification)</td>
<td>If no parameters for Security Question verifications are specified, generates parameters.</td>
</tr>
<tr>
<td>Add default parameters SMS verification</td>
<td>Password Reset Verification (pwd_verification)</td>
<td>If there are no parameters specified, generates SMS code verifications parameters.</td>
</tr>
<tr>
<td>Add params personal confirm verification</td>
<td>Password Reset Verification (pwd_verification)</td>
<td>If there are no parameters specified, generates personal data confirmation verifications parameters.</td>
</tr>
<tr>
<td>Add params personal verification</td>
<td>Password Reset Verification (pwd_verification)</td>
<td>If there are no parameters specified, generates parameters for personal data verification.</td>
</tr>
<tr>
<td>Check unique verifications</td>
<td>Password Reset Process Verification (pwd_map_proc_to_verification)</td>
<td>Prevents a verification from being assigned multiple times to a specific Password Reset process.</td>
</tr>
<tr>
<td>Clear parameters for Mock verification</td>
<td>Password Reset Verification (pwd_verification)</td>
<td>Clears parameters for the Mock verification.</td>
</tr>
<tr>
<td>Deactivate process with no group</td>
<td>Password Reset Process User Group (pwd_map_proc_to_group)</td>
<td>Deactivates the process if it does not apply to all users or if the groups associated with it are removed.</td>
</tr>
<tr>
<td>Business rule</td>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Deactivate process with no min ver</td>
<td>Password Reset Process Verification</td>
<td>Deactivates the process if the verifications associated with the process are less than the minimum value for the process.</td>
</tr>
<tr>
<td>Deactivate process with no verification</td>
<td>Password Reset Process Verification</td>
<td>Deactivates the process if the verifications associated with it are removed.</td>
</tr>
<tr>
<td>Google Auth Enabled Check</td>
<td>Password Reset Process</td>
<td>Deactivates the process with Google Authenticator verification if the Google authenticator is disabled.</td>
</tr>
<tr>
<td>Handle req_enroll validation/ default val</td>
<td>Password Reset Process Verification</td>
<td>Handles requires_enrollment and auto_enroll values for the process.</td>
</tr>
<tr>
<td>Order must be unique</td>
<td>Password Reset Desktop Access Control</td>
<td>Enforces order to be unique.</td>
</tr>
<tr>
<td>Parameter Names Cannot Be Updated</td>
<td>Password Reset Verification Param</td>
<td>Prevents parameter name changes.</td>
</tr>
<tr>
<td>Password Reset Activity Monitor</td>
<td>Password Reset User Lockout</td>
<td>Creates an event when the number of users locked out of Password Reset during a specific interval exceeds the threshold value.</td>
</tr>
<tr>
<td>Password Reset Validate Auto-generate</td>
<td>Password Reset Process</td>
<td>Checks that either <strong>Email password</strong> or <strong>Display password</strong> is selected when the <strong>Auto-generate password</strong> check box is selected.</td>
</tr>
<tr>
<td>Personal Data Confirm Param Validation</td>
<td>Password Reset Verification Param</td>
<td>Checks that a column exists in the sys_user table for the parameter used in a personal data confirmation verification.</td>
</tr>
<tr>
<td>Personal Data Param Validation</td>
<td>Password Reset Verification Param</td>
<td>Checks that a column exists in the sys_user table for the parameter used in a personal data verification.</td>
</tr>
<tr>
<td>Prevent against deletion</td>
<td>Password Reset Credential Store</td>
<td>Checks whether the credential store is part of an active process before allowing deletion.</td>
</tr>
<tr>
<td>Prevent against deletion</td>
<td>Password Reset Identification Type</td>
<td>If an identification type is part of an active process, prevents the identification type from being deleted.</td>
</tr>
<tr>
<td>Prevent against deletion</td>
<td>Password Reset Verification</td>
<td>If the verification is part of an active process, prevents it from being deleted.</td>
</tr>
<tr>
<td>Business rule</td>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Prevent against deletion when in use</td>
<td>Password Reset Credential Store Types (pwd_cred_store_type)</td>
<td>Prevents deletion when the type is in use.</td>
</tr>
<tr>
<td>Prevent against deletion when in use</td>
<td>Password Reset Verification Type (pwd_verification_type)</td>
<td>Prevents deletion when the type is in use.</td>
</tr>
<tr>
<td>Security Questions Param Validation</td>
<td>Password Reset Verification Param (pwd_verification_param)</td>
<td>Checks for valid parameters in security question verifications.</td>
</tr>
<tr>
<td>Send SMS code</td>
<td>Password Reset Device Enrollment Code (pwd_dvc_enrollment_code)</td>
<td>Sends an enrollment code to a device.</td>
</tr>
<tr>
<td>Set new record flag</td>
<td>Password Reset Process (pwd_process)</td>
<td>Sets a new record flag for the client to take appropriate action.</td>
</tr>
<tr>
<td>Send SMS Verification Code Via Notify</td>
<td>Password Reset SMS Verification Code (pwd_sms_code)</td>
<td>Sends out SMS authentication code via Notify if the Notify plugin is active.</td>
</tr>
<tr>
<td>Single credential store per process</td>
<td>Password Reset Process Credential Store (pwd_map_proc_to_cred_store)</td>
<td>Prevents having more than one credential store per process.</td>
</tr>
<tr>
<td>SMS Code Param Validation</td>
<td>Password Reset Verification Param (pwd_verification_param)</td>
<td>Checks for valid parameters in SMS code verifications.</td>
</tr>
<tr>
<td>Update action based on access conditions</td>
<td>Password Reset Desktop Access Log (pwd_access_log)</td>
<td>Updates the “action” field of this log record based on the access control conditions.</td>
</tr>
<tr>
<td>Update proc_to_cred_store</td>
<td>Password Reset Process (pwd_process)</td>
<td>Ensures a one-to-one relation between a Password Reset process and a credential store.</td>
</tr>
<tr>
<td>Validate Process</td>
<td>Password Reset Process (pwd_process)</td>
<td>Verifies that a Password Reset process is configured correctly.</td>
</tr>
<tr>
<td>Validate Pwd Cred Store Name</td>
<td>Password Reset Credential Store (pwd_cred_store)</td>
<td>Ensures the name to be unique.</td>
</tr>
<tr>
<td>Validate Pwd Cred Store Type Name</td>
<td>Password Reset Credential Store Types (pwd_cred_store_type)</td>
<td>Ensures the name to be unique.</td>
</tr>
<tr>
<td>Validate Pwd Extension Type Name</td>
<td>Password Reset Extension Type (pwd_extension_type)</td>
<td>Ensures the name to be unique.</td>
</tr>
<tr>
<td>Validate Pwd Identification Type Name</td>
<td>Password Reset Identification Type (pwd_identification_type)</td>
<td>Ensures the name to be unique and not empty.</td>
</tr>
<tr>
<td>Business rule</td>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Validate Pwd Process Name</td>
<td>Password Reset Process (pwd_process)</td>
<td>Enforces the name to be unique.</td>
</tr>
<tr>
<td>Validate Pwd Verification Name</td>
<td>Password Reset Verification (pwd_verification)</td>
<td>Enforces the name to be unique.</td>
</tr>
<tr>
<td>Validate Pwd Verification Type Name</td>
<td>Password Reset Verification Type (pwd_verification_type)</td>
<td>Enforces the name to be unique.</td>
</tr>
<tr>
<td>Validate Security Question</td>
<td>Password Reset Question (pwd_question)</td>
<td>Validates rules for security questions such as no duplicates or empty questions.</td>
</tr>
<tr>
<td>Verify Account Lookup Script</td>
<td>Password Reset Credential Store (pwd_cred_store)</td>
<td>Checks whether the account lookup script has the correctly named function.</td>
</tr>
<tr>
<td>VerifyAutoEnroll</td>
<td>Password Reset Verification Type (pwd_verification_type)</td>
<td>Checks whether auto-enroll is selected and ensures that an enrollment check script is provided.</td>
</tr>
</tbody>
</table>

### Password Reset UI pages

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$pwd_reset</td>
<td>First page of self-service reset process (asks for user ID).</td>
</tr>
<tr>
<td>$pwd_reset_serviceDesk</td>
<td>First page of service desk assisted reset process (asks for user ID).</td>
</tr>
<tr>
<td>$pwd_verify</td>
<td>Second page of reset process (asks user to verify identity).</td>
</tr>
<tr>
<td>$pwd_new</td>
<td>Last page of password change process (asks for new password).</td>
</tr>
<tr>
<td>$pwd_success</td>
<td>Page that appears when password is reset successfully.</td>
</tr>
<tr>
<td>$pwd_error</td>
<td>Page that appears on error during reset process.</td>
</tr>
<tr>
<td>$pwd_confirm</td>
<td>For processes configured to email password reset URL: After successful verification, this page displays message about sending link to user.</td>
</tr>
<tr>
<td>$pwd_change</td>
<td>Page for changing password.</td>
</tr>
<tr>
<td>$pwd_change_success</td>
<td>Page that appears when password is changed successfully.</td>
</tr>
<tr>
<td>$pwd_change_error</td>
<td>Page that appears on error during password change process.</td>
</tr>
<tr>
<td>$pwd_enrollment_form_container</td>
<td>Enrollment page for all verifications.</td>
</tr>
<tr>
<td>$pwd_enrollment_success</td>
<td>Page that appears when enrollment is successful.</td>
</tr>
<tr>
<td>$pwd_enroll_error</td>
<td>Page that appears when any error happens during enrollment.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>$pwd_unlock_success</td>
<td>Page that appears when locked user is successfully unlocked.</td>
</tr>
<tr>
<td>$pwd_reset_downloads_ui</td>
<td>Page for downloading Password Reset Windows Application.</td>
</tr>
</tbody>
</table>

### Password Reset UI macros

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$pwd_csrf_validation</td>
<td>CSRF validation for Password Reset Application. If violation is detected, the page will be redirected to the error page.</td>
</tr>
<tr>
<td>$pwd_display_password</td>
<td>Displays a temporary password on the success page if the process is configured to auto-generate.</td>
</tr>
<tr>
<td>$pwd_enroll_questions_ui</td>
<td>UI for question and answer security validation enrollment.</td>
</tr>
<tr>
<td>$pwd_enroll_questions_ui_js</td>
<td>JavaScript code that requires server-side data for security question and answer enrollment.</td>
</tr>
<tr>
<td>$pwd_enroll_sample_ui</td>
<td>Sample UI macro for enrollment for Mock Verification Type.</td>
</tr>
<tr>
<td>$pwd_enroll_sms_ui and $pwd_verify_sms_ui</td>
<td>UI for SMS enrollment and verification.</td>
</tr>
<tr>
<td>$pwd_enrollment_form_title</td>
<td>Jelly macro function that prints the title for the enrollment form. A verification ID is mandatory.</td>
</tr>
<tr>
<td>$pwd_error_message</td>
<td>UI for displaying error messages.</td>
</tr>
<tr>
<td>$pwd_process_flow</td>
<td>UI for indicating current stage.</td>
</tr>
<tr>
<td>$pwd_process_footer</td>
<td>JavaScript code to get the footer macro name.</td>
</tr>
<tr>
<td>$pwd_verify_personal_data_ui and $pwd_verify_personal_data_confirmation_ui</td>
<td>UI for verifying personal data and for confirming personal data.</td>
</tr>
<tr>
<td>$pwd_verify_questions_ui</td>
<td>UI for verifying questions.</td>
</tr>
<tr>
<td>$pwd_verify_simple_ui</td>
<td>Input section for a simple verification method. This field is a single input field.</td>
</tr>
</tbody>
</table>

### UI scripts installed with Password Reset

You can create a UI script and reference the script from a UI macro or UI page by using a `<g:include_script>` Jelly tag. The following example shows how the $pwd_enroll_questions_ui UI macro can reference the $pwd_enroll_questions_ui script. In the example, `[UI Script Name]+".jsdbx"` is the name of the script:

```xml
<g:include_script src='$pwd_enroll_questions_ui.jsdbx' />
```

By referencing an external script, you can maintain separation between client JavaScript code and Jelly code, which simplifies maintenance. You can use the following installed scripts with Password Reset UI macros:
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$pwd_csrf_common_ui_script</td>
<td>Common UI script for handling a Cross-site Request Forgery (CSRF).</td>
</tr>
<tr>
<td>$pwd_enroll_questions_ui</td>
<td>JavaScript code for the $pwd_enroll_questions_ui UI macro.</td>
</tr>
<tr>
<td>$pwd_enroll_sample_ui</td>
<td>Included sample client JavaScript for the $pwd_enroll_sample_ui UI macro.</td>
</tr>
<tr>
<td>$pwd_enroll_sms_ui</td>
<td>SMS enrollment UI script.</td>
</tr>
<tr>
<td>$pwd_enrollment_submit_event</td>
<td>UI script for an enrollment submission event.</td>
</tr>
<tr>
<td>$pwdWfManager</td>
<td>Helper class to handle workflow activities and post-processing.</td>
</tr>
</tbody>
</table>

**Password Reset workflows**

The Password Reset plugin adds workflows that you can use as examples to create custom workflows for Password Reset processes.

**Workflows that connect to a credential stores**

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pwd Reset - AD</td>
<td>Connects to an AD server.</td>
</tr>
<tr>
<td>Pwd Reset - Local ServiceNow</td>
<td>Current (local) instance.</td>
</tr>
<tr>
<td>Pwd Reset - Master</td>
<td>Password Reset master workflow.</td>
</tr>
<tr>
<td>Pwd Reset - Mock Fatal</td>
<td>Example workflow to use in Password Reset testing to simulate a fatal error.</td>
</tr>
<tr>
<td></td>
<td>No retries.</td>
</tr>
<tr>
<td>Pwd Reset - Mock Non Fatal</td>
<td>Example workflow to use in Password Reset testing to simulate a non-fatal error.</td>
</tr>
<tr>
<td>Pwd Reset - Mock Success</td>
<td>Example workflow to use in Password Reset testing to simulate a successful completion.</td>
</tr>
<tr>
<td>Pwd Reset - Remote ServiceNow</td>
<td>Connects to a remote(SOAP) ServiceNow instance.</td>
</tr>
</tbody>
</table>

**Workflows that test the connection to a credential store**

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pwd Connection Test - AD</td>
<td>Tests connection to an AD server.</td>
</tr>
<tr>
<td>Pwd Connection Test - Local SN</td>
<td>Tests connection to local instance.</td>
</tr>
<tr>
<td>Pwd Connection Test - Master</td>
<td>Master workflow to test credential store connectivity.</td>
</tr>
<tr>
<td>Pwd Connection Test - Mock Failure</td>
<td>Example credential store connection test that simulates a failed connection.</td>
</tr>
<tr>
<td>Pwd Connection Test - Mock Success</td>
<td>Example credential store connection test that simulates a successful connection.</td>
</tr>
<tr>
<td>Pwd Connection Test - Remote SN</td>
<td>Tests connection to a remote(SOAP) ServiceNow instance.</td>
</tr>
</tbody>
</table>
### Workflows that determine the lock state of a user account

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pwd Get Lock State - AD</td>
<td>Gets a user account lock state for the AD server.</td>
</tr>
<tr>
<td>Pwd Get Lock State - Local SN</td>
<td>Workflow to get a user account lock state for the local instance.</td>
</tr>
<tr>
<td>Pwd Get Lock State - Master</td>
<td>Master workflow to get a user account lock state.</td>
</tr>
<tr>
<td>Pwd Get Lock State - Remote SN</td>
<td>Gets a user account lock state for the remote(SOAP) ServiceNow instance.</td>
</tr>
</tbody>
</table>

### Workflows that unlock a user account

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pwd Unlock Account – AD</td>
<td>Unlocks a user account for a local instance.</td>
</tr>
<tr>
<td>Pwd Unlock Account - Local SN</td>
<td>Workflow to unlock a user account for a local instance.</td>
</tr>
<tr>
<td>Pwd Unlock Account - Master</td>
<td>Master workflow to unlock a user account.</td>
</tr>
<tr>
<td>Pwd Unlock Account – Remote SN</td>
<td>Unlocks a user account for a remote(SOAP) ServiceNow instance.</td>
</tr>
</tbody>
</table>

### Workflows that change a password

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pwd Change - Master</td>
<td>Password change master workflow.</td>
</tr>
<tr>
<td>Pwd Change – Local ServiceNow</td>
<td>Connects to a local instance to change a password.</td>
</tr>
<tr>
<td>Pwd Change – AD</td>
<td>Connects to an AD server to change a password.</td>
</tr>
<tr>
<td>Pwd Change – Remote ServiceNow</td>
<td>Connects to a remote(SOAP) ServiceNow instance to change a password.</td>
</tr>
</tbody>
</table>

### Password Reset notifications

<table>
<thead>
<tr>
<th>Name</th>
<th>Fired by event name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Reset – Send SMS Code</td>
<td>pwd.send_sms_code.trigger</td>
<td>Sends out SMS authentication code for verification.</td>
</tr>
<tr>
<td>Password Reset - New Password</td>
<td>pwd.email.trigger</td>
<td>For the Email Password process, sends an email that includes the new password.</td>
</tr>
<tr>
<td>Confirmation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password Reset URL</td>
<td>password.reset.url</td>
<td>For the Email Password Reset URL process; Sends email that includes a link to the password reset URL.</td>
</tr>
</tbody>
</table>
SOAP messages for Password Reset

<table>
<thead>
<tr>
<th>SOAP Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Password</td>
<td>When the Orchestration Add-on plugin is active, the system can use the SOAP protocol to change passwords on remote credential stores such as a remote ServiceNow instance.</td>
</tr>
<tr>
<td>Password Reset Request</td>
<td>When the Orchestration Add-on plugin is active, the system can use the SOAP protocol to reset passwords on remote credential stores such as a remote ServiceNow instance.</td>
</tr>
</tbody>
</table>

REST API

Name: Pwd Reset
API ID: pwd_reset
Base API path: /api/now/pwd_reset

Resources (Version v1)

<table>
<thead>
<tr>
<th>Name</th>
<th>Resource path</th>
<th>API Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pwd_init</td>
<td>/api/now/v1/pwd_reset/init</td>
<td>v1</td>
<td>Initial request to establish session, write logs, and fetch UI messages.</td>
</tr>
<tr>
<td>pwd_identify</td>
<td>/api/now/v1/pwd_reset/identify</td>
<td>v1</td>
<td>Get identification page components.</td>
</tr>
<tr>
<td>pwd_verify</td>
<td>/api/now/v1/pwd_reset/verify</td>
<td>v1</td>
<td>Get verification page components.</td>
</tr>
<tr>
<td>pwd_new</td>
<td>/api/now/v1/pwd_reset/reset</td>
<td>v1</td>
<td>Get resetting password page components.</td>
</tr>
<tr>
<td>pwd_success</td>
<td>/api/now/v1/pwd_reset/success</td>
<td>v1</td>
<td>Get success page components.</td>
</tr>
<tr>
<td>pwd_failure</td>
<td>/api/now/v1/pwd_reset/failure</td>
<td>v1</td>
<td>Get failure page components.</td>
</tr>
</tbody>
</table>

Password Reset Windows Application

If a user forgets the password or is locked out of a Windows computer, the user can reset the password directly from the Windows login screen.

Installer and documentation

Download the installer and installation instructions from KB0542328 in the ServiceNow Knowledge Base. The installer uninstalls any earlier version of the Password Reset Windows Application.
How the Password Reset Windows Application works

Administrators download and run an EXE or MSI file to install or distribute the application to user computers. The application installs a link on the Windows login screen. The user clicks the link (Forgot Password? in the examples on various Windows versions) and is then guided through the process of resetting the password.
By default, when a user requests a reset, the instance sends the user a URL with a user-specific token. After the user opens the URL, the instance prompts the user to enter and confirm the new password. The instance does not send a temporary password.

Restrictions on the Password Reset Windows Application

- The Password Reset Windows Application does not support custom verifications.
- The Password Reset Windows Application uses the base-system CAPTCHA service even if the Password Reset application is configured to use Google reCAPTCHA with the web interface. See the section titled "Settings on the Details tab" in Configure your Password Reset or Password Change process.
- The Password strength indicator is not supported. See Configure and test the Password Reset connection to a credential store.
- For some verification types, you can use only one verification. Custom verifications are not supported. See Password Reset verifications for details.
- Custom UI macros configured on the Process > Advanced page are not supported (for example, entry, success, or failure macros). The system displays only the default success and failure messages.
- The Password Reset Windows Application supports newline characters in the Password rule hint text. Other formatting is not supported (bold, underline, hyperlink, and so on). See Configure and test the Password Reset connection to a credential store.

Password Reset Windows Application installation requirements

You must activate the Password Reset Orchestration Add-on plugin to use the Password Reset Windows Application.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required ServiceNow release</td>
<td>Password Reset Windows Application version 4.0 is supported on Kingston, London, and Madrid releases. Jakarta and earlier releases are not supported.</td>
</tr>
<tr>
<td>Requirement</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Required hardware            | • 1 GHz or faster processor  
• 512 MB of RAM  
• 10 MB of available hard disk space (x86)  
• 10 MB of available hard disk space (x64) |
| Required software            | | **Version of Password Reset Windows Application** | **Microsoft .NET Framework** | **Microsoft Visual C++** |
|                             | | 4.0 | 4.7.1 and newer | Redistributable Visual Studio 2017 |
| Supported operating systems  | • Windows 7  
• Windows 8.1  
• Windows 10 Enterprise  
• Windows 10 Pro |
| Supported processor architecture | • X86  
• X64 |
| Supported network architecture | • Password Reset Windows Application clients must have direct access to both the Internet and the ServiceNow instance where the Password Reset Windows Application is configured  
• The ServiceNow SHA certificate must not be blocked by the corporate network. Information on the ServerCertificateSHA256 file appears in the documentation for Password Reset Windows Application.  
• To reset an AD password, the client must be on the corporate network. |

**Password Reset admin guide**

The Password Reset application enables an end user to reset or change a password using a self-service process. Alternatively, your organization can implement a process that requires a service desk agent to reset passwords for end users.

Watch the video: [Introducing Password Reset (Video)](Watch the video: [Introducing Password Reset (Video)](video))

**Password Reset processes**

Users with the password_reset_admin role configure how the process of resetting a password works for an end user.

- **Self-service process:** Users reset passwords over the Internet using a browser on any supported interface, including mobile devices.
• **Service desk-assisted process**: A user requests the assistance of a service desk agent, over the phone or in person. Users do not reset passwords.

**End-user experience of the self-service process**

The following example is typical:

1. On the login page, the user clicks the **Forgot Password?** link to start the process.

![Login page](service-now-login-page.png)

2. The Identify page opens and the user enters their identifying information (typically username or email address). The example includes the default CAPTCHA security feature:
3. On the Verify page, the user verifies their identity by providing information that proves that they are who they say they are. You, the admin, configure the method of verification and you can require multiple verifications. In the example, the admin has configured the Security Question verification. The user must answer a question to prove identity. (The user had earlier selected the question and provided a secure private answer while enrolling for the password reset process.) Other possible verifications require the user to enter a code number that was sent to a mobile device by SMS text, through the Google Authenticator app, or by email.

4. The system checks the credential store to verify identity and then displays the new password on the Reset page.
Elements of a password reset process

You configure the following elements of the process for your organization:

- A connection to the credential store for your organization where user credentials (like username/password) are securely stored.
- One or more user groups on the ServiceNow instance that can use the password reset process.
- The type of identification that users must enter to identify themselves (typically username or email address).
- One or more verifications — methods to verify the identity of the user. Examples:
  - Answer a question that only the user knows how to answer — the QA Verification (based on the Security Question verification type).
  - Enter a code number that was texted to a mobile device — the SMS verification.
How you implement a password reset process

1. Plan your implementation: Ensure that all applicable organizational guidelines, security policies, and areas of the organization are considered.

2. Set up the elements of the password reset and password change processes according to the plan:
   - Connection to the credential store.
   - User groups that will use the password reset process.
   - Identification type to use.
   - Verifications to use.

3. In the service desk-assisted model, assign service desk agents to monitor and reset passwords as needed.

4. Monitor password reset activity to identify security threats and to ensure compliance with the password policy requirements of your organization.

Password Reset Windows Application

If a user forgets the password or gets locked out of a Windows computer, the user can reset the password directly from the Windows login screen. The user clicks the Forgot Password? link and is then guided through the process of resetting the password. To learn more, see Password Reset Windows Application.

Password Change application

The Password Change application extends the Password Reset application by letting admins define how users change their passwords. Only a self-service process is supported and an admin must publish the URL to the password change form.

1. The user logs in to the instance and then selects the Change Password module or link from the user profile record.

2. On the Change Password page, the user selects the credential store where the password resides.

3. The user enters the old password and then enters and confirms a new password.

4. Workflows validate the old password and then implement the new password.

5. The system notifies the user that the password was changed.

What to do next

Plan your Password Reset processes

Plan your Password Reset processes

To ensure security and efficiency, take the time to plan your Password Reset implementation.

Role required: password_reset_admin or admin

1. Decide on the password reset process:
• **Self-service process:** Users reset their password over the Internet using a browser on any supported interface, including mobile devices. To make the Password Reset application with Orchestration available to all users publicly, create a new Password Reset process only for this purpose and make it accessible to all users by setting the **Public access** property.

• **Service desk-assisted process:** Users reset passwords by requesting the assistance of a service desk agent, over the phone or in person. Only service desk agents with the password_reset_service_desk role can reset user passwords. Watch the videos: *Resetting User Passwords (Video)* and *How to Set Up a Service Desk-Assisted Password Reset Process (Video)*.

2. Understand how groups and roles differ in their access and security needs.
   Analyze and assess how members of each group in your organization access the system. For example, if members of the sales group primarily access the system remotely, consider using a stronger method or multiple methods to verify the identity of each user.

   Identify user roles that have access to critical information and resources. For example, stronger verifications might be required for roles that have access to employee data, accounting information, or network configurations.

   Based on your analysis of groups and roles, determine the number and variety of verifications needed for the different Password Reset processes.

3. Consider how to manage credentials.
   Determine whether single sign-on is enabled with the type of directory service or other credential store used. If the directory service is configured for single sign-on, consider increasing the level of security by using multiple methods to verify identity of a user. A compromised user name and password can easily allow access to associated systems in a single sign-on environment.

4. Consider how to implement enrollment in the Password Reset program.
   For example, will enrollment be optional or required? Will users be auto-enrolled? How will users be notified to enroll in the program? The answers to these questions will help you determine the appropriate verification types to use.

5. Consider which Password Reset options to offer to users.
   - If your organization uses single sign-on, how will users reset their password if they are unable to log on?
   - What options are available to users working off-site?

Example: The default self-service Password Reset process

The default self-service Password Reset process enables a user to reset the password without assistance from service desk agents.

**The default self-service password reset flow**

1. If a user does not remember the password, the user can click the **Forgot Password?** link on the login screen.
2. The Password Reset application starts. On the **Identity** page, the user identifies himself or herself by entering a **Username**.

3. On the **Verify** page, the user proves that they are the person who is associated with the username. In this example, the user enters the email address that is associated with the user profile. The admin can configure a different verification method or can require additional verifications, for example, a personal question that only the user can answer.

4. The **Reset** page tells the user to check email for instructions.

5. The user opens the email and clicks the **here** link to reset the password. The link is valid for a period that you specify (use the `password_reset.request.expiry` property).
6. The **Reset Password** page guides the user to reset the password.

The default self-service Password Reset process (com.glideapp.password_reset) defines:

- The URI that specifies where users are redirected when they click **Forgot Password**. By default this value is `/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.
Configure your Password Reset or Password Change process

To implement the process, you configure credentials, verifications, and users.

Role required: password_reset_admin or admin

1. Be sure to Plan your Password Reset processes.
2. Create the credential store record for user names and passwords that are managed.

   **Note:** For LDAP integrations: If the Active Directory settings require users to reset the password when logging in, the results depend on the password reset plugin that is installed.
   - The Password Reset plugin cannot change an AD password. End users will not be able to log in to the instance.
   - The Self Service Password Reset plugin depends on the Password Reset Basic plugin. Self-service is intended for password reset only on the local ServiceNow instance and cannot change an AD password.
   - The Password Reset Orchestration Add-on plugin is built on top of Orchestration AD activities. The plugin supports changing the AD password.

3. Define the verifications that the process will use.

A Password Reset process consists of the following elements:
- The credential store that contains user login credentials.
- Optionally, the user groups that are authorized to use the Password Reset process.
- The verifications (extension script includes) that verify the identity of the requesting user and that enable the service desk agents to authorize reset of the password.

1. Navigate to Password Reset > Processes.
2. Click New and then specify a meaningful Name and Description for the process.
3. Select the Credential store that contains the user credentials that the process applies to.
4. Specify the process that you are defining: Select the Password Reset check box and/or the Password change check box.
5. Specify the Apply to all users setting.

<table>
<thead>
<tr>
<th>Apply to all users setting</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selected</td>
<td>All users use the process that you are defining. This setting is useful only if all users have access to the authentication methods that are defined in this process.</td>
</tr>
<tr>
<td>Not selected</td>
<td>Only the users in the groups that you specify use the process. You specify the groups in the Groups related list.</td>
</tr>
</tbody>
</table>

6. If you selected Password Reset, fill in the Password Reset Details tab and, optionally, the Advanced tab. See Settings on the Password Reset Details tab and Settings on the Password Reset Advanced tab.
7. Save the form. The form refreshes and additional related lists appear.
8. From the Password Reset Process Verifications related list, select one or more verifications. See Password Reset verifications.
9. Optional: From the Password Reset Process Groups related list, select the user groups that will use the process that you are defining.
The Password Reset Process Groups related list appears only if the Apply to all users check box is not selected.

10. Select the Active check box to enable the Password Reset process that you configured. The check box is available only after the record has been saved.

11. Click Update.

12. Navigate to Password Reset > Properties to set the properties that configure the Password Reset experience for end users.

Credential stores for Password Reset

Credential stores hold user information such as user names and passwords that can be used as login credentials. Examples include the User (sys_user) table or an Active Directory server.

Users with the password_reset_admin or password_reset_credential_manager role can create and modify connections to credential stores.

Credential store types installed with the base system

A credential store type is a set of workflows that specify how to connect to a credential store. Navigate to Password Reset > Credential Stores to view the list of example credential stores that are based on the base-system types. The base system includes the following credential store types:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local ServiceNow Instance</td>
<td>Represents the current (local) ServiceNow instance.</td>
</tr>
<tr>
<td>AD Credential Store</td>
<td>Represents an Active Directory credential store. Installed with the Orchestration Add-on plugin.</td>
</tr>
<tr>
<td>Remote (SOAP) ServiceNow instance</td>
<td>Represents a remote ServiceNow instance. Installed with the Orchestration Add-on plugin.</td>
</tr>
</tbody>
</table>

Remote credential stores

A remote credential store refers to any credential store other than the local ServiceNow instance. Remote credential stores, such as Active Directory, manage user names and passwords outside of the local instance. A remote credential store can also be a remote ServiceNow instance, a UNIX or Linux server, or any other directory-like service that relies on the SOAP protocol. The Password Reset Orchestration Add-on plugin is required to connect to remote credential stores. Review the information in the section on credential store types before you create, test, or delete credential stores.

Connection workflows for credential store types

A credential store type workflow requires a subflow that defines how to connect to the store, and can include an optional subflow that defines how to test the connection. Use the Pwd reset – AD and Pwd Reset - Local subflows as models for your custom connection workflows.
Pwd Reset Local sub workflow
Creating a custom credential store type

You can use a credential store type as a model to create a custom type. See Create a credential store type for Password Reset.

Configure and test the Password Reset connection to a credential store
You specify a credential store to access during the Password Reset or Password Change process and configure other settings that control the process.

Role required: password_reset_admin or password_reset_credential_manager

Note: The Password Reset Windows Application supports only Active Directory (AD) credential stores.

1. Navigate to Password Reset > Credential Stores.
2. Click New, enter a unique and meaningful Name and Description, and then fill in the form.

<table>
<thead>
<tr>
<th>Type</th>
<th>You can use credential store types (templates that provide a desired set of capabilities). Credential stores inherit the functionality of the credential store type.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note:</td>
<td>The Password Reset Windows Application supports only AD Credential Store.</td>
</tr>
</tbody>
</table>

Installed credential store types:
- Local ServiceNow Instance installed with Password Reset.
- AD Credential Store installed with the Orchestration Add-on.
- Remote (SOAP) ServiceNow installed with the Orchestration Add-on.
<table>
<thead>
<tr>
<th><strong>Auto-generate password</strong></th>
<th>Script include that generates a temporary password for use during the reset process.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enforce history policy</strong></td>
<td><strong>Note:</strong> This option appears only if you select a credential store Type of AD Credential Store.</td>
</tr>
<tr>
<td></td>
<td>To enforce the history policy that is configured for the credential store:</td>
</tr>
<tr>
<td></td>
<td>1. Select the <strong>Enforce history policy</strong> check box.</td>
</tr>
<tr>
<td></td>
<td>2. Follow the procedure that appears after this table.</td>
</tr>
<tr>
<td><strong>Hostname</strong></td>
<td>URL or IP address of the credential store that contains the user credential (for example, user names and passwords).</td>
</tr>
<tr>
<td><strong>User account lookup</strong></td>
<td>Script include that maps the user ServiceNow platform ID to the user credential store ID. A default script, <code>PwdDefaultUserAccountLookup</code>, returns the user ServiceNow platform user name.</td>
</tr>
<tr>
<td><strong>Password rule hint</strong></td>
<td>Text that appears on the password reset page to help the user to create a password that meets all requirements. The <strong>Password rule</strong> script enforces the requirements.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The Password Reset Windows Application supports newline characters in the hint. Other formatting is not supported (bold, underline, hyperlink, and so on).</td>
</tr>
<tr>
<td><strong>Password rule</strong></td>
<td>Client script that validates the password that the user enters. The script is invoked when the user enters a new password and clicks <strong>Password Reset</strong>. You can use the script to enforce password strength/complexity requirements.</td>
</tr>
<tr>
<td><strong>Enable Password Strength</strong></td>
<td>Select the check box to:</td>
</tr>
<tr>
<td></td>
<td>· Display the text box for the <strong>Strength rule</strong> script so you can update the script.</td>
</tr>
<tr>
<td></td>
<td>· Display the graphical <strong>Password Strength</strong> bar to the user while the user changes or resets the password.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The Password Reset Windows Application does not support Password Strength.</td>
</tr>
</tbody>
</table>
Strength rule: This text box appears only if you select **Enable Password Strength**.

**Note:** The Password Reset Windows Application does not support Password Strength.

Client script that calculates the strength/complexity of the password that the user enters. The script is invoked when the user begins to enter a new password during the reset process.

Default settings:
- Selected for local ServiceNow credential stores
- Not selected for other credential stores

**Note:**
To guide the user during the reset process, the system displays a graphical bar labeled **Password Strength** under the **New password** field.

3. Click **Submit**.

   The connection is created. You should test the connection to a credential store after you configure a new credential store or when users experience problems that might involve the connection.

4. Navigate to **Password Reset > Credential Stores** and then open the credential store.

5. In the header bar, click **Save and Test Connection**.

   A progress page displays the result of the test.

If you selected the **Enforce history policy** check box, then follow these steps:

1. Open the associated Password Reset process definition: **Password Reset > Processes**.

2. On the Details tab of the Password Reset Process form, clear the **Auto-generate password** check box and then save the process definition.

3. On the domain controller, set **Password Aging** (MIN_PASSWORD_AGE) to zero.

4. On the domain controller, set the history policy to twice the desired number of passwords. For example, to enforce that the last three passwords are not repeated, set the history policy to six.

**Note:** To enforce the history policy that is configured for the credential store, the system auto-generates a new temporary password for each reset cycle. The system auto-generates the temporary password even though you have cleared the **Auto-generate password** check box on the Password Reset Process form. Because the user immediately replaces the temporary password with a new password, two passwords are created for each reset cycle.
**Set up SOAP credentials for Password Reset**

When the Orchestration Add-on plugin is activated, the ServiceNow platform can use the SOAP protocol to interact with remote credential stores such as a remote ServiceNow instance.

**Role required:** admin or web_service_admin

1. Navigate to **System Web Services** > **Outbound** > **SOAP Message**.
2. Click **Password Reset Request**.
3. From the **Soap Message Functions** related list, configure both the `password_reset` and `sys_user_get_record` functions by completing the following steps.
   a) In **Basic auth user ID**, enter the user ID for the remote system user who has privileges to update records on the User `[sys_user]` table.
   b) In **Basic auth user password**, enter the password for the remote system user who has privileges to update records on the User `[sys_user]` table.
   c) Select **Use basic auth**.
   d) Click **Update**.

You do not need to enter a value in the **SOAP endpoint** field. The field shows the name of the ServiceNow instance used for Password Reset.

**Configure Password Reset for Active Directory**

When the Orchestration Add-on plugin is activated, the Password Reset application can change passwords on an Active Directory credential store. The application changes passwords by referencing an Active Directory user role with the appropriate password change privileges.

Active Directory must have a user role with the following privileges:

**Descendent User objects:**
- Reset password
- Read/Write pwdlastset
- Read/Write UserAccountcontrol
- Write Account Restrictions
- Read/Write lockouttime
- Read MemberOf

**Descendent Group objects:**
- Read Members
- Read MemberOf

1. **Install MID Server** on a Windows computer that can connect to Active Directory.
2. **Configure the MID Server**.
3. In the ServiceNow instance, navigate to **Orchestration** > **Credentials**.
4. Click **New** and then complete the form with the following values for the credential.
   a) **Type**: Select Windows.
   b) **User name**: Enter your Active Directory domain user. For example, `domain\admin`.
   c) **Password**: Enter your Active Directory domain user password.
   d) **Applies to**: Select the MID Server that is used to access the Active Directory server.

5. Click **Submit**.
6. Create a credential store for Active Directory.
Delete a connection to a credential store for Password Reset

Important: Before you delete the connection to a credential store, check all Password Reset processes to ensure that the credential store is not in use. If the credential store is being used by a process, update the process before deleting the credential store.

Role required: password_reset_admin or password_reset_credential_manager

1. Navigate to Password Reset > Credential Stores and then select the check box for the credential store.
2. In the Actions choice list, select Delete.

Password Reset verifications

Each verification specifies the method and process for verifying the identity of the user that is requesting password reset.

Verifications included with Password Reset

The Password Reset application includes the following verifications in the base system. You can create a verification based on either a base-system verification or a verification type (a template).

<table>
<thead>
<tr>
<th>Verification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QA verification</td>
<td>Implements a self-service Password Reset model with questions that are included with the base system or custom questions that the admin defines. While enrolling for the process, the user decides which questions to provide answers for. When a user requests password reset, the system poses a specified number of the questions that the user selected during enrollment. The user must answer all questions correctly to verify identity. This verification is based on the Security Questions verification type. For information on the user enrollment experience, see Users: Enroll in the Password Reset program using questions and answers.</td>
</tr>
<tr>
<td>SMS verification</td>
<td>Implements a self-service or service desk-assisted Password Reset model that relies on auto-generated code numbers. When a user requests password reset, the system sends a code to an SMS-capable device that the user has authorized. To verify identity, the user then submits the code on the Password Reset Verify page. You can use the ServiceNow Notify feature to send the codes. This verification is based on the SMS Code verification type. For information on the user enrollment experience, see Users: Enroll in the Password Reset program using SMS codes.</td>
</tr>
<tr>
<td>Personal Data — Confirm Email Address</td>
<td>Implements a self-service Password Reset model that relies on user information that is available in the user profile on the instance. This verification is based on the Personal Data Confirmation verification type.</td>
</tr>
</tbody>
</table>
Verifications included with the demo data

The following demo data is based on the Mock verification type:

- Sample Mock verification #1
- #2

*Personal data identification types and confirmation type verifications*

Personal data verifications allow users to verify their identity by providing answers to questions that are generated from personal information stored in the User table [sys_user].

### Personal data identification types

The Password Reset application provides the email and username identification types. You can use either type as provided or as a model to create a custom identification type.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Identification</td>
<td>Identifies users by their email addresses.</td>
</tr>
<tr>
<td>Username Identification</td>
<td>Identifies users by their user names.</td>
</tr>
</tbody>
</table>

### Personal data confirmation verifications

- **Personal data verification**: If users are associated with a Password Reset process that uses a personal data verification, the users are typically not required to enroll for Password Reset.
- **Personal data confirmation verifications** allow employees with the password_reset_service_desk role to access personal data from the sys_user table when assisting a user with a password reset request.

To configure personal data and personal data confirmation verifications, you specify parameters as name/value pairs that correspond to a particular piece of user information. For example, to verify users by their email address:

1. Set the **label** parameter (the text that the end user should see) to Email (that is, `label=Email`).
2. Set the **column** parameter (the column in the table that holds the verification data) to email (that is, `column=email`).

**Note**: You can use only one set of name/value pair parameters per verification. Additional parameters are ignored.

To use multiple pieces of personal information for user verification, create more personal data or personal data confirmation verifications and add the verifications to the related Password Reset process.
**Personal data and personal data confirmation type verifications**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>label</td>
<td>Label that the user sees during the password reset request.</td>
</tr>
<tr>
<td></td>
<td>Data Type: string</td>
</tr>
<tr>
<td></td>
<td>Default Value: n/a</td>
</tr>
<tr>
<td>column</td>
<td>Column of the sys_user table that provides the data that is used to verify the identity of the user.</td>
</tr>
<tr>
<td></td>
<td>Data Type: string</td>
</tr>
<tr>
<td></td>
<td>Default Value: n/a</td>
</tr>
</tbody>
</table>

**SMS Code Verification type for Password Reset**

Using the Simple Message Service (SMS) Code Verification type, a user can verify identity through any SMS-enabled device, like a cell phone that accepts text messages. When a user requests password reset, the system sends a numerical code to the device and the user enters the code on the password reset page.

You can change the default behavior of an SMS code verification using either of the following methods:

- Set parameter values, as shown in the table
- Update property settings for the Password Reset application

**Note:** The system allows only one instance of each SMS code parameter.

**SMS Code Verification type parameters**

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>expiry</td>
<td>Number of minutes the verification code is valid.</td>
</tr>
<tr>
<td></td>
<td><strong>Data Type:</strong> integer (any positive integer)</td>
</tr>
<tr>
<td></td>
<td><strong>Default Value:</strong> 5</td>
</tr>
<tr>
<td>complexity</td>
<td>Number of digits in the numerical verification code.</td>
</tr>
<tr>
<td></td>
<td><strong>Data Type:</strong> integer (any positive integer)</td>
</tr>
<tr>
<td></td>
<td><strong>Default Value:</strong> 4</td>
</tr>
<tr>
<td>pause_window</td>
<td>Number of minutes before the user can request another SMS code for verification.</td>
</tr>
<tr>
<td></td>
<td><strong>Data Type:</strong> integer (any positive integer)</td>
</tr>
<tr>
<td></td>
<td><strong>Default Value:</strong> 2</td>
</tr>
<tr>
<td>max_per_day</td>
<td>Maximum number of codes sent for verification in one day.</td>
</tr>
<tr>
<td></td>
<td><strong>Data Type:</strong> integer (any positive integer)</td>
</tr>
<tr>
<td></td>
<td><strong>Default Value:</strong> 10</td>
</tr>
</tbody>
</table>

Use NotifyNow to send SMS codes for enrollment and verification
You can configure the Password Reset application to send SMS codes for enrollment and verification using ServiceNow NotifyNow (via Twilio SMS Messaging). NotifyNow is tightly integrated with the workflow engine and business rules and delivers a highly configurable and trusted way to deliver SMS messages.

Role required: admin

NotifyNow requires a separate contract with Twilio.

1. Enroll for a Twilio account and telephone number at https://www.twilio.com/
2. Activate the Notify plugin.
3. Associate the Twilio account with Notify.

No other configuration is required. Users who request password change or reset receive SMS codes through NotifyNow.

**Settings on the Password Reset Details tab**

The settings define the user experience when resetting or changing a password.

The Password Reset Details tab appears when you are configuring a Password Reset process (Password Reset > Processes).

### Password Reset Details tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Public access    | The check box is available only when **Password reset** is selected.  
|                  | - Clear the check box to define a service desk-assisted process in which only service desk agents and not users can reset a password.  
|                  | - Select the check box to enable a self-service process with public user access to the Password Reset or Password Change form through a URL. |
| Public URL       | This field is available only when **Public access** is selected.  
|                  | URL of the page where users go to reset or change the password. The value from the URL suffix field is appended to the URL when you tab out of the URL suffix field.  
|                  | For the Default self-service Password Reset process, this value must be /$pwd_reset.do?sysparm_url=ss_default. |
| URL suffix       | This field is available only when **Public access** is selected.  
<p>|                  | Suffix used to create a unique URL for the Password Reset or Password Change form. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display CAPTCHA</td>
<td>This check box is available only when Public access is selected. Select the check box to display a CAPTCHA on the user identification page. The Password Reset application uses Google reCAPTCHA as the default CAPTCHA service. See Configure Google reCAPTCHA.</td>
</tr>
<tr>
<td>Note:</td>
<td>The Password Reset Windows Application uses the base-system CAPTCHA service even if the Password Reset application is configured to use Google reCAPTCHA.</td>
</tr>
<tr>
<td></td>
<td>To use the CAPTCHA service that is provided with the base system, change the password_reset.captcha.google.enabled system property to false.</td>
</tr>
<tr>
<td>Note:</td>
<td>Because on-premises instances do not have access to the Internet, they cannot use the Google reCAPTCHA service. Set the password_reset.captcha.google.enabled property to false for on-premises instances.</td>
</tr>
<tr>
<td>Identification type</td>
<td>Method that the user employs to claim their identity for the public Password Reset or Password Change process. Any selection overrides the default identification that is associated with the process. The base system includes the Email and Username Identification identification types. You can create a custom identification type (some knowledge of JavaScript is recommended). See Personal data identification types and confirmation type verifications.</td>
</tr>
<tr>
<td>Minimum verifications</td>
<td>Number of verifications that a user must successfully submit to reset the password. If the number exceeds the number of mandatory verifications, then the user must submit enough additional optional verifications to meet the number specified for Minimum verifications. By default during the password reset process, the system presents optional verifications to the user based on the Order values for the verifications.</td>
</tr>
<tr>
<td>Note:</td>
<td>Each user must submit all mandatory verifications regardless of the number specified.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Email Password Reset URL</td>
<td>Select the check box to enable users to reset the password by clicking a link in an email that the instance sends to them. By default, the self-service Password Reset processes enable this option. When you select this option, the <strong>Auto-generate password</strong> check box is not available. <strong>Note:</strong> See <a href="#">Example: The default self-service Password Reset process</a> for an outline of the process that is enabled by default.</td>
</tr>
<tr>
<td>Enable account unlock</td>
<td>This check box is available only when <strong>Password reset</strong> is selected. Select the check box to allow user accounts on credential stores to be unlocked without resetting the password. <strong>Note:</strong> Not supported by the default self-service Password Reset process.</td>
</tr>
<tr>
<td>Unlock user account</td>
<td>Select the check box to unlock user accounts on credential stores after a password reset.</td>
</tr>
</tbody>
</table>
| Auto-generate password | This check box is available only when:  
- The **Password reset** check box is selected.  
- The **Email Password Reset URL** check box is not selected  
Select the check box to auto-generate a new password for the user. When this check box is selected, you must select the **Email password** or **Display password** check box, or both. This setting is useful for service desk-assisted processes. **Note:** Clear the check box to enable the **Enforce history policy** option for a credential store. See [Configure and test the Password Reset connection to a credential store](#). |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User must reset password</td>
<td>This check box is available only when Auto-generate password is selected. Select the check box to require users to reset their password immediately after logging in with the auto-generated password.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Users whose credentials are held in the local ServiceNow instance credential store are prompted to change their password the first time that they log in. Users whose credentials are held in an Active Directory credential store are not prompted to change their passwords in the instance. Such users must change their passwords from a computer on the domain.</td>
</tr>
<tr>
<td>Display password</td>
<td>This check box is available only when Auto-generate password is selected. Select the check box to display the new password on the screen. In a self-service process, the password appears on the user screen. In a service desk-assisted process, the password appears on the service desk agent screen.</td>
</tr>
<tr>
<td>Email password</td>
<td>This check box is available only when Auto-generate password is selected. Select the check box to email the new password to the user. The setting is useful in both self-service and service desk-assisted processes. The setting can add a layer of security by requiring that users access their email to view the password. In a service desk-assisted process, emailing the password to users ensures that only the user requesting the password reset can view the password.</td>
</tr>
<tr>
<td>Related lists</td>
<td></td>
</tr>
<tr>
<td>Verifications</td>
<td>This related list is available only after the record has been saved. One or more verifications that the process uses. See Password Reset verifications.</td>
</tr>
<tr>
<td>Groups</td>
<td>The Groups related list is available only after the record has been saved and if the Apply to all users check box is cleared. ServiceNow user groups to associate with the Password Reset process.</td>
</tr>
</tbody>
</table>

**Configure Google reCAPTCHA**

To use the Google reCAPTCHA service, instances that are running on a domain other than service-now.com require an API key pair from Google. The process described in this topic is optional for instances that are running on the service-now.com domain.

Role required: admin
Note:

Because on-premises instances do not have access to the Internet, they cannot use the Google reCAPTCHA service. Do not follow the process described in this topic. Instead, set the `password_reset.captcha.google.enabled` system property to `false`. This setting enables the CAPTCHA service that is provided with the base system.

The Password Reset Windows Application uses the base-system CAPTCHA service even if the Password Reset application is configured to use Google reCAPTCHA.

1. Request an API key pair (a site key and a secret) from Google at [https://www.google.com/recaptcha](https://www.google.com/recaptcha)
2. Set the following system properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>password_reset.captcha.google.enabled</code></td>
<td>Set to <code>true</code>. Type: string Default: <code>true</code></td>
</tr>
<tr>
<td><code>google.captcha.site_key</code></td>
<td>Set to the site key that Google provided. Type: string Default: A site key that Google provided to ServiceNow</td>
</tr>
<tr>
<td><code>google.captcha.secret</code></td>
<td>Set to the secret that Google provided. Type: password2 Default: An encrypted secret that Google provided to ServiceNow</td>
</tr>
</tbody>
</table>

**Settings on the Password Reset ‘Advanced’ tab**

UI macros and script includes can extend the basic functionality of a Password Reset process. The Advanced tab appears when you are configuring a Password Reset process (Password Reset > Processes).

### Advanced tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry UI macro</td>
<td>UI macro that displays a customized message to users when they access the initial Password Reset screen.</td>
</tr>
<tr>
<td>Success UI macro</td>
<td>UI macro that displays a customized message to users on the final Password Reset screen when their password is successfully reset.</td>
</tr>
<tr>
<td>Failure UI macro</td>
<td>UI macro that displays a customized message to users on the final Password Reset screen when their password reset fails.</td>
</tr>
<tr>
<td>Post reset script</td>
<td>Script include that performs actions after the Password Reset process completes whether the outcome is success or failure. For more information on customizing post processor scripts, see the Post reset script category as described in Password Reset extension scripts.</td>
</tr>
</tbody>
</table>
Configure the number of questions for a 'Security Questions' verification

When designing a Security Questions verification for Password Reset, you can specify the number of questions to display when users enroll and the number to display when a user requests password reset.

Role required: password_reset_admin or admin

1. Navigate to Password Reset > Verifications and then open a verification that uses the Security Questions Verification Type.
2. Configure the parameters in the Password Reset Verification Parameters related list.

Parameters for Security Questions Verification

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>num_enroll</td>
<td>Number of security questions that are displayed while a user is enrolling for Password Reset. <strong>Data Type:</strong> Positive integer that does not exceed the number of questions in the security questions list (Password Reset &gt; Security Questions). <strong>Default Value:</strong> 5</td>
</tr>
<tr>
<td>num_reset</td>
<td>Number of security questions that are displayed while a user is attempting to reset the password. The questions are selected at random and are presented in random order. <strong>Data Type:</strong> Positive integer that does not exceed the value of the num_enroll parameter <strong>Default Value:</strong> 3</td>
</tr>
</tbody>
</table>

3. Click Update.

Configure the required strength for passwords

The password that a user defines must meet certain requirements — it must contain at least eight characters, it must include a numeral, and so on. You can configure the requirements as needed for your organization.

Role required: password_reset_admin

The base system includes example credential stores with various password requirements. You can modify password requirements and provide users with hints for creating password. The default requirements for a new password are:

- At least eight characters
- At least one uppercase and one lower case letter
- At least one numeral

**Note:** This topic describes the procedure for configuring password strength requirements only. You can configure several other settings for the credential store, as described in Configure and test the Password Reset connection to a credential store.

1. Navigate to Password Reset > Credential Stores.
2. Select the credential store in the list and then configure the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password rule hint</strong></td>
<td>Text that appears on the password reset page to help the user to create a password that meets all requirements. The Password rule script enforces the requirements.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>The Password Reset Windows Application supports newline characters in the hint. Other formatting is not supported (bold, underline, hyperlink, and so on).</td>
</tr>
<tr>
<td><strong>Password rule</strong></td>
<td>Client script that validates the password that the user enters. The script is invoked when the user enters a new password and clicks Password Reset. You can use the script to enforce password strength/complexity requirements.</td>
</tr>
<tr>
<td><strong>Enable Password Strength</strong></td>
<td>Select the check box to:</td>
</tr>
<tr>
<td></td>
<td>· Display the text box for the Strength rule script so you can update the script.</td>
</tr>
<tr>
<td></td>
<td>· Display the graphical Password Strength bar to the user while the user changes or resets the password.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>The Password Reset Windows Application does not support Password Strength.</td>
</tr>
<tr>
<td><strong>Strength rule</strong></td>
<td>This text box appears only if you select Enable Password Strength.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>The Password Reset Windows Application does not support Password Strength.</td>
</tr>
<tr>
<td></td>
<td>Client script that calculates the strength/complexity of the password that the user enters. The script is invoked when the user begins to enter a new password during the reset process.</td>
</tr>
<tr>
<td>Default settings</td>
<td>· Selected for local ServiceNow credential stores</td>
</tr>
<tr>
<td></td>
<td>· Not selected for other credential stores</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>To guide the user during the reset process, the system displays a graphical bar labeled Password Strength under the New password field.</td>
</tr>
</tbody>
</table>

3. Click Submit. You should test the connection to a credential store after you configure a new credential store or when users experience problems that might involve the connection.

4. Navigate to Password Reset > Credential Stores and then open the credential store.

5. In the header bar, click Save and Test Connection.
A progress page displays the result of the test.

**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.

<table>
<thead>
<tr>
<th>SNC User Lockout Check with Auto Unlock</th>
<th>Uses the value of the <code>glide.user.max_unlock_attempts</code> property to set the limit for failed login attempts.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SNC User Lockout Check</th>
<th>Tracks the number of failed login attempts and locks the user account after a specified number of failed login attempts (default: 5).</th>
</tr>
</thead>
<tbody>
<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.

**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 three 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 five and seven.

1. Navigate to **Password Reset > Properties**.
2. Update settings as needed and then click **Save**.

**Password Reset properties**

<table>
<thead>
<tr>
<th>Label on the Password Reset Properties page</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>Label on the Password Reset Properties page</td>
<td>Property name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Workflow polling frequency | password_reset.wf.refresh_rate | Time period in milliseconds between checks on status of the workflow.  
  - Type: integer  
  - Default value: 500 |
| 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 |
| Password Reset Request properties | | |
| Number of unsuccessful attempts allowed to reset/change password | password_reset.request.max_attempt | Number of password reset attempts a user has before they are locked out for a period determined by the value in max_attempt_window.  
  - Type: integer  
  - Default value: 3 (attempts) |
| 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><strong>Label on the Password Reset Properties page</strong></th>
<th><strong>Property name</strong></th>
<th><strong>Description</strong></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 that a user is allowed to perform the Password Reset process.  
- Type: integer  
- Default value: 10 (minutes) |

**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 |
| **Number of security questions required during the password reset request** | `password_reset.qa.num_reset` | Number of questions that a user must answer to verify identity during the Password Reset process.  
- Type: integer  
- Default value: 3 (questions)  
- Possible values: Integers that are less than the number specified for the `num_enroll` property. |

**Note:** You can override this security question property by adding the `num_reset` parameter in the security question verification.
<table>
<thead>
<tr>
<th>Label on the Password Reset Properties page</th>
<th>Property name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Number of security questions required during enrollment | password_reset.qa.num_enroll | During the enrollment process, the number of questions that a user must answer to be enrolled in the Password Reset program.  
- Type: integer  
- Default value: 5 (questions)  
  
  **Note:** You can override this security question property by adding the num_enroll parameter in the security question verification. |
| Password Reset SMS Code properties         |                                |                                                                                                                                                                                                            |
| 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. |
<table>
<thead>
<tr>
<th>Label on the Password Reset Properties page</th>
<th>Property name</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
| 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.

<table>
<thead>
<tr>
<th>Password Reset Monitoring and Reporting properties</th>
<th></th>
</tr>
</thead>
</table>
| 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) |

**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.
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.

---

**Customizing Password Reset processes**

Password Reset scripting enables you to customize Password Reset by creating your own credential store, verification, and identification types, and extend them by defining extension scripts. You can also create a custom credential store type, custom verification type, or verification.

Password Reset scripting is available to users with the `password_reset_admin` role. The easiest way to customize Password Reset is:

1. Create custom types and scripts as described in **Password Reset extension scripts**.
2. Follow the configuration steps described in **Configure your Password Reset or Password Change process**.
3. Select the new types that you created. You can customize the following components:
   - Credential store types: Define new types for how to connect to your credential stores by creating custom workflows for connection and testing. See **Create a credential store type for Password Reset**.
   - Verification types: Define new types for how users are verified. See **Create a custom Password Reset verification type**.
   - Identification types: Define new types for how users can identify themselves. See **Create a custom identification type for Password Reset**.

---

**Extension scripts**

Extension scripts enable you to extend Password Reset functionality by defining custom scripts that can be used in a credential store, verification, or identification type, or as a post-processor in a process. Extension scripts are predefined hooks within the Password Reset application that perform specific types of behavior defined by the extension category, which refers to where the script will be used. See **Password Reset extension scripts**.

---

**Create a credential store type for Password Reset**

You can create a custom credential store type if the base-system types do not meet your needs.

Role required: `password_reset_admin` or `password_reset_credential_manager`

1. Navigate to **Password Reset > Extensions > Credential Store Types**.
2. Click **New**, enter a unique and meaningful **Name** and **Description**, and then fill in the form.

**Note:** You may need to configure the form to see the **Get user lock state** workflow and the **Unlock user** workflow.
New credential store fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Reset workflow</td>
<td>Subflow that defines the credential store processing. Password Reset workflows are available to use as a model. Provide scripts for each of the activities defined for the subflow. For more information about how to create a workflow, see Create a workflow. For installed workflows, see Installed with Password Reset.</td>
</tr>
<tr>
<td>Connection test workflow</td>
<td>Subflow that defines how to test the connection. Connection test workflows are available to use as a model. If you create a connection test subflow, provide scripts for each of the activities defined for the subflow. For more on how to create a workflow, see Create a workflow. For installed workflows, see Installed with Password Reset.</td>
</tr>
<tr>
<td>Get user lock state workflow</td>
<td>Subflow that defines how to get the user lock state. Get user lock state workflows are available to use as a model. Provide scripts for each of the activities defined for the subflow. For more on how to create a workflow, see Create a workflow. For installed workflows, see Installed with Password Reset.</td>
</tr>
<tr>
<td>Unlock user workflow</td>
<td>Subflow that defines how to unlock a user. Unlock user workflows are available to use as a model. If you create a connection test subflow, provide scripts for each of the activities defined for the subflow. For installed workflows, see Installed with Password Reset.</td>
</tr>
</tbody>
</table>

3. Click Submit.

Create a custom question for a ‘Security Questions’ verification

To enroll for the ‘Security Questions’ verification, the user selects several questions and supplies answers that only the user knows. You can add a custom question to the set of questions that are included with the base system.

Role required: password_reset_admin or admin

The default language is English, and you can create a custom question in a non-English language. If you create the appropriate non-English language questions, then the questions appear in the language that the user requested during login.

1. Navigate to Password Reset > Security Questions and then click New.
2. Enter the English language question in the Security question field and then click Submit. The question appears in the Translations related list.
3. To add the same question in another language, complete the following steps.
   a) Click the English language question to translate.
      
      **Note:** Do not change the Language value for the default questions that come with the base system.

   b) On the Password Reset Question page, in the Translations related list, click New.
c) Select the language in the Language field.
d) Enter the non-English text in the Security question field.
e) Click Submit.

The question appears in the Translations related list on the Password Reset Question page. If a user selects the language while logging in, then the verification question appears in that language.

Create a custom identification type for Password Reset

A custom identification type enables the user to enter alternative verification information such as an employee ID while resetting the password.

Role required: password_reset_admin or admin

1. Navigate to Password Reset > Extensions > Identification Types.
2. Click New, enter a unique and meaningful Name and Description, and then fill in the form.

<table>
<thead>
<tr>
<th>Identification field label</th>
<th>Text to display as a label for the Identification field.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification processor</td>
<td>Identification processor script. Choose an existing script, or create your own using the Identification form processor category (extension script).</td>
</tr>
</tbody>
</table>

3. Click Submit.

Create a Password Reset verification from an existing verification

The Password Reset application includes several example verifications that you can use as they are or as the basis for a custom verification. If the verification types in the base system do not meet your needs, you can create a custom verification type.

Role required: password_reset_admin

Note: The Password Reset Windows Application does not support custom verifications. Custom verifications might work, but you must test and verify.

1. Navigate to Password Reset > Verifications and select a verification.
2. If needed, modify the parameters on the Password Reset Verification Parameters tab. The parameters are described in the instructions for the type of verification that you are working on.
3. Click Submit.
4. Each verification type has properties that control the user experience. Review the property settings and update as needed.

Create a custom Password Reset verification type

If the verification types in the base system do not meet your needs, you can create a custom verification type.

Review the verification types that are provided in the base system to determine whether to create a custom verification type. Then review the verification type components to develop.
Role required: password_reset_admin or admin

1. Navigate to Password Reset > Extensions > Verification Types.
2. Click New, enter a unique and meaningful Name and Description, and then fill in the form.

<table>
<thead>
<tr>
<th>Enrollment check</th>
<th>Script to check whether a user is enrolled for verification. Automatic enrollment requires an enrollment check. If no script is specified when Automatic Enrollment is selected, a default script is provided.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic enrollment</td>
<td>Indicator for whether users are auto-enrolled. If Automatic enrollment is not selected, then you must provide an enrollment UI macro and enrollment processor script.</td>
</tr>
<tr>
<td>Enrollment UI</td>
<td>Enrollment UI macro that provides the UI for the enrollment.</td>
</tr>
<tr>
<td>Enrollment processor</td>
<td>Enrollment processor script that processes the enrollment.</td>
</tr>
<tr>
<td>Verification UI</td>
<td>Verification UI macro that provides the UI for the verification.</td>
</tr>
<tr>
<td>Verification processor</td>
<td>Verification processor script (extension scripts) that processes the verification.</td>
</tr>
</tbody>
</table>

3. Click Submit.

Create a custom Password Reset verification

Use a verification type in the base system as a template to design a custom verification. The Password Reset Windows Application does not support custom verifications.

Role required: password_reset_admin

Verification types in the base system

<table>
<thead>
<tr>
<th>Personal Data Confirmation Verification Type</th>
<th>Verifies user identity using data from the User (sys_user) table. The user data is displayed to a service desk agent. The agent verifies the data. Enrollment is not required for this type. Recommended for service desk-assisted processes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note: The Password Reset Windows Application does not support the Personal Data Confirmation Verification type.</td>
<td></td>
</tr>
<tr>
<td>See Personal data identification types and confirmation type verifications.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Personal Data Verification Type</th>
<th>Verifies user identity using data from the User (sys_user) table. The user is required to answer questions. Enrollment is not required for this type.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note: The Password Reset Windows Application allows you to define and use multiple verifications of the Personal Data type.</td>
<td></td>
</tr>
<tr>
<td>See Personal data identification types and confirmation type verifications.</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.
Security Questions Verification Type

Verifies user identity by presenting personal security questions that the user must answer correctly.

**Note:** The Password Reset and Password Reset Windows Application support only a single verification of the Security Questions type.

See [Create a custom question for a Security Questions verification](#).

SMS Code Verification Type

When a user requests password reset, the system sends a code to an SMS-capable device that the user has authorized. To verify identity, the user then enters the code on the Password Reset web page.

**Note:** The Password Reset and Password Reset Windows Application support only a single verification of the SMS Code type.

See [SMS Code Verification type for Password Reset](#).

Mock Verification Type

Not a functional identity verification. Demonstrates how to add a verification type in a Password Reset process.

**Note:** The Password Reset Windows Application does not support the Mock verification type.

- The enrollment UI macro for this verification gets the user input and returns the entered value in the enrollment processor.
- The Password Reset UI macro for this verification gets input from the user and returns the entered value through the verification processor.

1. Navigate to **Password Reset > Extensions > Verification Types**.
2. Click **New**, enter a unique and meaningful **Name** and **Description**, and then fill in the form.

<table>
<thead>
<tr>
<th>Type</th>
<th>Create verifications based on one of the verification types in the base system. Password Reset supports the following types. You can create multiple instances of any type.</th>
</tr>
</thead>
</table>
|      | - Personal Data Confirmation Verification  
|      | - Personal Data Verification  
|      | - Security Question Verification  
|      | - SMS Code Verification  
|
|      | The Password Reset Windows Application supports the following types:  
|      | - Personal Data Verification. You can create only a single instance.  
|      | - Security Question Verification. You can create multiple instances.  
|      | - SMS Code Verification. You can create only a single instance.  
|
| Order | Position of the verification as it appears on the Enrollment form and Password Reset form.  
|
| Password Reset Verification Parameters | Parameters used by a verification to configure specific behaviors, like number of questions required to enroll, request expiration time, and columns used. Set parameters for any behavior that should be different from the default specified in the Password Reset properties. The available parameters are described separately for each verification type.  
|
3. Click Submit.
4. Each verification type has properties that control the user experience. Review the property settings and update as needed.

Enrollment options for the Password Reset service

You can configure the Password Reset process to enroll users automatically, or you can define an enrollment check.

To define an enrollment check, you must define:

- An enrollment processor script, which specifies how enrollment is processed
- A corresponding enrollment UI macro, which specifies how the enrollment information is displayed to the user

The following example uses PwdEnrollSMSProcessor as the enrollment processor script and pwd_enroll_sms_ui as the enrollment UI macro.
Verification type example

A verification type must also define a verification processor script and a corresponding verification UI macro. The example uses PwdVerifySMSProcessor as the verification processor script and pwd_verify_sms_ui as the verification UI macro. The following shows the verification processor script:
**Verification type SMS processor**

The following is the corresponding UI macro:
Password Reset UI macro

The Password Reset plugin installs script includes that implement password reset processes. To enable you to extend functionality, each base-system script include provides extension points that you can use to invoke "extension scripts" that you have customized.
The **extension script category** refers to the specific types of behavior for an extension script (for example, credential store, verification, identification type, or as a post-processor).

**'Enrollment check' script includes**

All enrollment check script includes take the following parameters and return a boolean indicating whether the user is enrolled for Password Reset.

- **params.userId**: The sys_id of the user being checked (table: (sys_user)).
- **params.verificationId**: The sys_id of the verification being checked (table: (pwd_verification)).

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PwdAlwaysEnrolled</td>
<td>Default check of whether a user is enrolled that always returns true.</td>
</tr>
<tr>
<td>PwdMockIsEnrolled</td>
<td>Default check of whether a user is enrolled that always returns true.</td>
</tr>
<tr>
<td>PwdQuestionsEnrollmentCheck</td>
<td>Determines whether a user has enrolled for Password Reset using security question verification.</td>
</tr>
<tr>
<td>PwdSMSEnrollmentCheck</td>
<td>Determines whether a user has enrolled for Password Reset using SMS verification.</td>
</tr>
</tbody>
</table>

**'Identification form processor' script includes**

Identification form processor script includes provide functionality for extending identification processing.

All identification form processor script includes take the following parameters, and return the sys_id of the user that corresponds to the requested input. If the user was not identified, it returns null.

- **params.processId**: The sys_id of the calling Password Reset process (table: (pwd_process)).
- **param request**: The form request object. Fields in the form can be accessed with `request.getParameter('<element-id>')`. The supported request parameter is `sysparm_user_id`, the user identifier value entered in the form.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PwdIdentifyViaEmail</td>
<td>Verifies a user's identity by checking the email address.</td>
</tr>
<tr>
<td>PwdIdentifyViaUsername</td>
<td>Verifies a user's identity by checking the user name.</td>
</tr>
</tbody>
</table>

**'Enrollment form processor' script includes**

Enrollment form processor script includes provide functionality for extending enrollment form processing.

All enrollment form processor script includes take the following parameters, and return a boolean indicating whether the user was successfully enrolled.
- params.userId: The sys_id of the user trying to enroll (table: [sys_user]).
- params.verificationId: The sys_id of the verification used to enroll (table: [pwd_verification]).
- params.enrollmentId: The sys_id of this enrollment process.
- request: The form request object. Fields in the form can be accessed with request.getParameter('<element-id>').

You should add the following information to the state of the enrollment process:

- gs.getSession().putProperty("result.status",status): Whether the user was successfully enrolled.
- gs.getSession().putProperty("result.message",message): An associated message to be returned to the UI, such as a detailed error message.
- gs.getSession().putProperty("result.value",value): A custom value associated with the enrollment.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PwdEnrollQuestionsProcessor</td>
<td>Handles questions and answers for verification.</td>
</tr>
<tr>
<td>PwdEnrollSampleProcessor</td>
<td>Provides an enrollment processor for sample verification.</td>
</tr>
<tr>
<td>PwdEnrollSMSProcessor</td>
<td>Provides an enrollment processor for SMS verification.</td>
</tr>
</tbody>
</table>

'User account lookup' script includes

User account lookup script includes return the credential store account_id for a given user.

The following parameter returns the credential store account_id for a given user.
- params.userId: The sys_id of the user being checked (table: [sys_user]).

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PwdDefaultUserAccountLookup</td>
<td>Provides a default script for user account lookup from a user_id to the account in a credential store. The default mapping is to use the user name as the account name.</td>
</tr>
</tbody>
</table>

'Password generator' script includes

Password generator script includes take the following parameter, and return an auto-generated string password.
- params.credentialStoreId: The sys_id of the calling Password Reset process (table: [pwd_process]).

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PwdDefaultAutoGenPassword</td>
<td>Generates a password from a random word and 4 digits.</td>
</tr>
</tbody>
</table>
'Verification processor' script includes

If the user identity is verified, the verification processor script includes return true.
Verification processor script includes take the following parameters:

- params.resetRequestId: The sys_id of the current Password Reset request (table: (pwd_reset_request)).
- params.userId: The sys_id of the user to be verified (table: (sys_user)).
- params.verificationId: The sys_id of the verification (table: (pwd_verification)).
- request: The form request object. Access the fields in the form with request.getParameter('element-id').

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PwdVerifyPersonalDataConfirmationProcess</td>
<td>Verifies that the user accepts the answer.</td>
</tr>
<tr>
<td>PwdVerifyPersonalDataProcessor</td>
<td>Verifies that the user's answers match the expected data in the system.</td>
</tr>
<tr>
<td>PwdVerifyQuestionsProcessor</td>
<td>Provides question and answer verification of user input on the second page of the verification form.</td>
</tr>
<tr>
<td>PwdVerifySimpleProcessor</td>
<td>Provides simple verification of user input on the second page of the verification form.</td>
</tr>
<tr>
<td>PwdVerifySMSProcessor</td>
<td>Provides SMS verification of user input on the second page of the verification form.</td>
</tr>
</tbody>
</table>

'Post processor' script includes

Post processor script includes execute custom actions after the Password Reset process has completed.

All post processor script includes take the following parameters.

- params.resetRequestId: The sys_id of the current Password Reset request (table: (pwd_reset_request)).
- params.wfSuccess: A flag indicating whether the workflow completed successfully: True if, and only if, successful.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PwdPostProcessor</td>
<td>Executes actions after the process completes for success, failure, or both conditions.</td>
</tr>
</tbody>
</table>

Example custom scripts for Password Reset
The example scripts perform a user account lookup and processes an identification form, define a credential store, and create an identification type.
Perform a user account lookup and process an identification form

The main script calls two extension scripts, one to perform the user account lookup, and the other to process the identification form.

```javascript
// User account lookup
var lookupExtensionSysId =
    getExtensionScriptSysId('SampleUserAccountLookupExtension',
    'user_account_lookup');
var lookupExtension = new SNC.PwdExtensionPoint(lookupExtensionSysId);

// Setup parameters required for this extension type - userId
var params = new SNC.PwdExtensionPointParameter();
params.userId = 'joe.employee';

// Invoke the extension
var answer = lookupExtension.process(params);
gs.print('user: ' + answer);

// Form processor sample - Identification form processor
var identExtensionSysId =
    getExtensionScriptSysId('SampleIdentificationProcessorExtension',
    'identification_form_processor');
var identificationExtension = new
    SNC.PwdExtensionPoint(identExtensionSysId);

// Setup parameters required for this extension type - processId
var params = new SNC.PwdExtensionPointParameter();
params.processId = 'pwdreq1234';

// Simulate the posted form parameter for the indentification processor
var request = new SNC.PwdExtensionPointParameter(); // A real life case will inject it's own request object
request.setParameter('sysparm_user_id', 'joe.employee');

var userIdentity = identificationExtension.processForm(params, request);
gs.print('identity: ' + userIdentity);
```

Define a credential store

The following is an example of an extended process function in the User Account Lookup category used to define a credential store. To create this extension script, go to Password Reset >
**Extensions** > **New extension script** and create a new script as described in [Create an Extension Script](#). To configure the User Lookup in a Password Reset process, see [Credential Stores](#).

```xml
<?xml version="1.0" encoding="UTF-8"?>
<record_update table="sys_script_include">
  <sys_script_include action="INSERT_OR_UPDATE">
    <active>true</active>
    <client_callable>false</client_callable>
    <description>Simple account lookup that returns the supplied user id</description>
    <name>SampleUserAccountLookupExtension</name>
    <script><![CDATA[var SampleUserAccountLookupExtension = Class.create();
SampleUserAccountLookupExtension.prototype = {
  category: 'password_reset.extension.user_account_lookup', // DO NOT REMOVE THIS LINE!

  **********
  * Returns the credential-store account id for a given user
  *
  * @param params.userId The sys-id of the user being checked (table: sys_user)
  * @return The credential-store account-id (string) for a given user
  **********/
  process: function(params) {
    return params.userId;
  },

type: 'SampleUserAccountLookupExtension'
}]]></script>
  <sys_created_by>admin</sys_created_by>
  <sys_created_on>2013-07-30 16:44:55</sys_created_on>
  <sys_id>2df5a103d73201002bb9af728e610333</sys_id>
  <sys_mod_count>1</sys_mod_count>
  <sys_updated_by>admin</sys_updated_by>
  <sys_updated_on>2013-07-30 16:46:00</sys_updated_on>
</sys_script_include>
</record_update>
```
Create an identification type

The following is an example of an extended processForm function in the Identification Form Processor category that can be used to create an identification type. To create this extension script, go to Password Reset > Extensions > New extension script and create a new script as described in Create an Extension Script.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<record_update table="sys_script_include">
    <sys_script_include action="INSERT_OR_UPDATE">
        <active>true</active>
        <client_callable>false</client_callable>
        <description>Script that processes an identification form.  
        Returns the sys-id of the user that corresponds to the requested input; if no user was found, null should be returned.</description>
        <name>SampleIdentificationProcessorExtension</name>
        <script><![CDATA[
            var SampleIdentificationProcessorExtension = Class.create();
            SampleIdentificationProcessorExtension.prototype = {
                category: 'password_reset.extension.identification_form_processor', // DO NOT REMOVE THIS LINE!
                processForm: function(params, request) {
                    return request.getParameter('sysparm_user_id') + '_' + params.processId;
                },
                type: 'SampleIdentificationProcessorExtension'
            };
        ]]]>
    </sys_script_include>
</sys_app_file>
```

© 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.
Use the `process` and `processForm` extensions

This example shows a script that uses two sample extensions, one `process` extension and one `processForm` extension.

```java
// User account lookup var lookupExtensionSysId =
getExtensionScriptSysId('SampleUserAccountLookupExtension','user_account_lookup');
var lookupExtension =new SNC.PwdExtensionPoint(lookupExtensionSysId);

// Setup parameters required for this extension type - userId
var params =new SNC.PwdExtensionPointParameter();
params.userId='joe.employee';

// Invoke the extension var answer = lookupExtension.process(params);
gs.print('user: ' + answer);

// Form processor sample - Identification form processor
var identExtensionSysId =
getExtensionScriptSysId('SampleIdentificationProcessorExtension','identification_form_processor');
var identificationExtension =new SNC.PwdExtensionPoint(identificationExtensionSysId);

// Setup parameters required for this extension type - processId
var params =new SNC.PwdExtensionPointParameter();
params.processId='pwdreq1234';

// Simulate the posted form parameter for the identification processor
var request =new SNC.PwdExtensionPointParameter();
var userIdentity = identificationExtension.processForm(params, request);
gs.print('identity: ' + userIdentity);
```

A simple helper to return the sys-id for a given extension script function

```java
function getExtensionScriptSysId(scriptName, category){
  var result;

  var gr = new GlideRecord('sys_script_include');
  gr.addQuery('name', scriptName);
  gr.addQuery('script','CONTAINS','category: \\password_reset.extension.' + category + '\');
  gr.query();

  if (gr.get()) {
    result = gr.getValue('sys_id');
  }

  return result;
}
```
if(gr.next()){
    result = gr.getValue('sys_id');
}return result;}

process function:

```xml
<record_update
    table="sys_script_include" action="INSERT_OR_UPDATE">
    <client_callable>false</client_callable><description>Simple account lookup that returns the supplied user id</description><name>SampleUserAccountLookupExtension</name><script><![CDATA[
        var SampleUserAccountLookupExtension = Class.create();
        SampleUserAccountLookupExtension.prototype={
            category:'password_reset.extension.user_account_lookup',// DO NOT REMOVE THIS LINE!
            process:function(params){return params.userId;},
            type:'SampleUserAccountLookupExtension'
        };]]>
    </script><sys_script_include>
</record_update>
```

processForm function:

```xml
<record_update
    table="sys_script_include" action="INSERT_OR_UPDATE">
    <client_callable>false</client_callable><description>Script that processes an identification form.
    Returns the sys-id of the user that corresponds to the requested input; if no user was found, null should be returned.&amp;#13;&lt;/description><name>SampleIdentificationProcessorExtension</name><script><![CDATA[
        var SampleIdentificationProcessorExtension = Class.create();
        SampleIdentificationProcessorExtension.prototype={
            category:'password_reset.extension.user_account_lookup',// DO NOT REMOVE THIS LINE!
    processForm:function(){
    return null;},
            type:'SampleIdentificationProcessorExtension'
        };]]>
    </script><sys_script_include>
</record_update>
```
Password Reset extension script categories
You can use a custom extension script to extend Password Reset functionality for credential store, verification, or identification types.

**Note:** To use a script include as an extension script, you must set it to **Active** status.

Password Reset extension script categories
Extension scripts must specify a category that indicates which script include is being extended, for example, category: 'password_reset.extension.enrollment_check'. The ServiceNow platform installs several scripts in each category. A script in the **Enrollment check** category can perform the enrollment check for a verification. Detailed information on each extension script appears in **Password Reset extension scripts**.
<table>
<thead>
<tr>
<th>Extension script category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enrollment check</td>
<td>Defines how to check that a user is enrolled in the Password Reset process. Scripts of this category are available in the Enrollment check field when you define a verification type (Password Reset Verification Type form).</td>
</tr>
<tr>
<td>Enrollment form processor</td>
<td>Defines how an enrollment form is processed (if automatic enrollment is not configured). Scripts of this category are available in the Enrollment form processor field when you define a verification type (Password Reset Verification Type form).</td>
</tr>
<tr>
<td>Identification form processor</td>
<td>Defines how a user identification is processed. Scripts of this category are available in the Identification processor field when you define a verification type (Password Reset Identification Type form).</td>
</tr>
<tr>
<td>Password generator</td>
<td>Defines how to generate a password. Scripts of this category are available in the Auto generate password field when you configure a credential store (Password Reset Credential Store Type form).</td>
</tr>
<tr>
<td>Post reset script</td>
<td>Executes at the end of a Password Reset process. Scripts of this category are available in the Post reset script field when you configure a process (Password Reset Process form).</td>
</tr>
<tr>
<td>User account lookup</td>
<td>Defines how to look up a user account. Scripts of this category are available in the User account lookup field when you configure a credential store (Password Reset Credential Store form).</td>
</tr>
<tr>
<td>Verification form processor</td>
<td>Defines how a verification form is processed. Scripts of this category are available in the Verification processor field when you define a verification type (Password Reset Verification Type form).</td>
</tr>
</tbody>
</table>

**Password Reset extension scripts**

Extension scripts allow you to extend Password Reset functionality in credential store, verification, or identification types.

**Password Reset extension script includes**

Each script include is associated with a specific category, which is available in the appropriate field of a Password Reset form.

**Note:** Create extension scripts only from the Password Reset Extension Script form (Password Reset > Extensions > New extension script). Extension scripts are special purpose script includes that are not created in the System Definition > Script Includes interface. To use a script include as an extension script, you must set it to Active status.
This Enrollment Check example signals that the user is enrolled if both expected parameters are supplied. The code would be contained in the `Script` field of an extension script named `SampleEnrollmentCheck`:

```javascript
var SampleEnrollmentCheck = Class.create();
SampleEnrollmentCheck.prototype = {
    category: 'password_reset.extension.enrollment_check', // DO NOT REMOVE THIS LINE!

    process: function (params) {
        return (params.userId && params.verificationId) ? true : false;
    },

    type: 'SampleEnrollmentCheck'
};
```
### Enrollment Form Processor' script include category

<table>
<thead>
<tr>
<th>Script include category</th>
<th>Description</th>
<th>Method signature</th>
<th>Input fields</th>
<th>Output fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enrollment Form Processor</td>
<td>Checks whether all necessary information has been collected from the user. Stores the information so it can be used for verification when the user resets their password.</td>
<td>process(params)</td>
<td></td>
<td>Returns: (boolean) true, if the user is enrolled in the specified verification; otherwise, false.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Parameters:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>· params.resetRequestId - The sys_id of the current Password Reset request (table: pwd_reset_request).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>· params.userId - The sys_id of the user to be verified (table: sys_user).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>· params.verificationId - The sys_id of the verification to be processed (table: pwd_verification).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>· request - The form request object. Fields in the form can be accessed with request.getParameter(&lt;element-id&gt;).</td>
<td></td>
</tr>
</tbody>
</table>

The following information should be added to the state of the enrollment process:

- gs.getSession().putProperty("result.status", status) - Whether the user was successfully enrolled.
- gs.getSession().putProperty("result.message", message) - An associated message to be returned to the UI, such as a detailed error message.
- gs.getSession().putProperty("result.value", value) - A custom value associated with the enrollment.
This example processes an enrollment form submission successfully if the user-submitted response was success. The code would be contained in the `Script` field of an extension script named `SampleEnrollmentProcessor`:

```javascript
var SampleEnrollmentProcessor = Class.create();
SampleEnrollmentProcessor.prototype = {
    category : 'password_reset.extension.enrollment_form_processor' , // DO NOT REMOVE THIS LINE!

    processForm : function (params , request ) { var verificationId = params.verificationId; var sampleInput = request.getParameter('sample_input');
        if (gs.nil(verificationId) || (sampleInput != 'success')) { return false; }

        var gr = new GlideRecord('sys_user');
        gr.get(params.userId);
        gs.print('User: ' + gr.getValue('user_name') + ' successfully enrolled'); return true;
    },

    type : 'SampleEnrollmentProcessor'
};
```

© 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.
### Identification Form Processor script include category

<table>
<thead>
<tr>
<th>Script include category</th>
<th>Description</th>
<th>Method signature</th>
<th>Input fields</th>
<th>Output fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification Form Processor</td>
<td>Processes an identification form request.</td>
<td><code>processForm(params, request)</code></td>
<td>Parameters:</td>
<td>Returns: the sys_id of the user that corresponds to the requested input. Returns null, if no user was found.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- <code>params.processId</code> - The sys_id of the calling Password Reset process (table: pwd_process).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- <code>request</code> - The form request object. Fields in the form can be accessed with <code>request.getParameter('&lt;element-id&gt;')</code>. Use <code>request.getParameter('sysparm_user_id')</code> to get the user ID that was entered into the form.</td>
<td></td>
</tr>
</tbody>
</table>

This example attempts to identify the user within the sys_user table given a user name submitted from the identification form. The code would be contained in the `Script` field of an extension script named `PwdIdentifyViaUsername`:

```javascript
var PwdIdentifyViaUsername = Class.create( );
PwdIdentifyViaUsername.prototype = {
    category : 'password_reset.extension.identification_form_processor', // DO NOT REMOVE THIS LINE!
    initialize : function () { },

    // Process the identification form request, and returns the user's sys_id. If user was not identified return null.
    processForm : function (params , request ) { var processId = params.processId ; var sysparm_user_id = request.getParameter('sysparm_user_id') ;
        gr = new GlideRecord ('sys_user') ;
        gr.addQuery ('user_name', sysparm_user_id ) ;
        gr.query () ; if ( !gr.next () ) { return null ; } return gr.sys_id ; },

    // Supported request parameters: sysparm_user_id - the user identifier value entered in the form
};
```

© 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.
'Password Generator' script include category

<table>
<thead>
<tr>
<th>Script include category</th>
<th>Description</th>
<th>Method signature</th>
<th>Input fields</th>
<th>Output fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Generator</td>
<td>Returns an auto-generated password.</td>
<td>process(params)</td>
<td>Parameters:</td>
<td>Returns: (String) an auto-generated password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- params.processId - The sys_id of the calling Password Reset process (table: pwd_process).</td>
<td></td>
</tr>
</tbody>
</table>

This example randomly generates a password from a base word and numbers. The base word is selected depending on the credential store. The code would be contained in the Script field of an extension script named SamplePasswordGenerator:

```javascript
var SamplePasswordGenerator = Class.create();
SamplePasswordGenerator.prototype = {
    category: 'password_reset.extension.password_generator', // DO NOT REMOVE THIS LINE!

    process: function (params) {
        var basePassword;

        var gr = new GlideRecord('pwd_cred_store');
        gr.addQuery('name', 'Local ServiceNow Instance');
        gr.query();
        if (gr.next()) {
            if (params.credentialStoreId == gr.getValue('sys_id')) {
                basePassword = "Password";
            } else {
                basePassword = "Dorwssap";
            }
        }
        return this.generateSimple(basePassword);
    },

    generateSimple: function (base) {
        var pwd = base;
        var numbers = '0123456789';
        var length = 4;

        for (var i = 0, n = numbers.length; i < length; i++) {
            pwd += numbers.charAt(Math.floor(Math.random() * n) + 1);
        }
        return pwd;
    },

    type: 'SamplePasswordGenerator'
};
```

© 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.
### 'Post Reset' script include category

<table>
<thead>
<tr>
<th>Script include category</th>
<th>Description</th>
<th>Method signature</th>
<th>Input fields</th>
<th>Output fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Post Reset</td>
<td>Performs additional operations after the completion of the Password Reset process.</td>
<td>process(params)</td>
<td>Parameters:</td>
<td>Returns: void</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- params.resetRequestId - The sys_id of the calling Password Reset process (table: pwd_process).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- params.wfSuccess - A flag indicating whether the workflow completed successfully. True if, and only if, successful.</td>
<td></td>
</tr>
</tbody>
</table>

This example adds failed reset requests to the system log. The code would be contained in the **Script** field for an extension script named `PwdPostProcessor`:

```javascript
var PwdPostProcessor = Class.create();

PwdPostProcessor.prototype = {
    category: 'password_reset.extension.post_reset_script', // DO NOT REMOVE THIS LINE!
    initialize: function() { },
    process: function(params) {
        if (!params.wfSuccess) {
            gs.log('[PwdPostProcessor.process] failure post processing for request [' + params.resetRequestId + '])
        }
        // We could place actions here that we always want executed
        return
    },
    type: 'PwdPostProcessor'
};
```
'User Account Lookup' script include category

<table>
<thead>
<tr>
<th>Script include category</th>
<th>Description</th>
<th>Method signature</th>
<th>Input fields</th>
<th>Output fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Account Lookup</td>
<td>Gets the credential store account ID for a given user.</td>
<td>process(params)</td>
<td>Parameters:</td>
<td>Returns: (String) the credential store account ID for the given user.</td>
</tr>
</tbody>
</table>

This example gets the credential store account for a user. This code would be contained in the *Script* field of an extension script named `SampleUserAccountLookupExtension`:

```javascript
var SampleUserAccountLookupExtension  = Class. create ( ) ;
SampleUserAccountLookupExtension. prototype = {
    category : 'password_reset.extension.user_account_lookup' , // DO NOT REMOVE THIS LINE!
    process : function (params ) { return params. userId ; } ,
    type : 'SampleUserAccountLookupExtension' }
```
‘Verification Form Processor’ script include category

<table>
<thead>
<tr>
<th>Script include category</th>
<th>Description</th>
<th>Method signature</th>
<th>Input fields</th>
<th>Output fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verification Form Processor</td>
<td>Processes a verification form request and indicates whether the user was verified or not.</td>
<td>processForm(params, request)</td>
<td>Parameters:</td>
<td>--</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>params.resetRequestId - The sys_id of the current Password Reset request (table: pwd_reset_request).</td>
<td>true, if the user is verified; otherwise, false.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>params.userId - The sys_id of the user to be verified (table: sys_user).</td>
<td>true, if the user is verified; otherwise, false.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>params.verificationId - The sys_id of the verification to be processed (table: pwd_verification).</td>
<td>true, if the user is verified; otherwise, false.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>request - The form request object. Fields in the form can be accessed with request.getParameter(&lt;element-id&gt;).</td>
<td>true, if the user is verified; otherwise, false.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>true, if the user is verified; otherwise, false.</td>
</tr>
</tbody>
</table>

This example shows a verification processor that returns true only if the user sent `ok` in the input field; otherwise, it returns false. The code would be contained in the Script field of an extension script named `SampleVerificationFormProcessor`:

```javascript
var SampleVerificationFormProcessor = Class.create();
SampleVerificationFormProcessor.prototype = {
    category : 'password_reset.extension.verification_form_processor', // DO NOT REMOVE THIS LINE!

    processForm: function (params, request)
    {
        /* Process the verification form request, and return whether the user was successfully verified.
         * This is a sample verification processor returns true only if the user sent "ok" in the input field;
         * otherwise, it returns false.
         *
         * @param params.resetRequestId The sys_id of the current Password Reset request (table: pwd_reset_request)
         * @param params.userId The sys_id of the user trying to be verified (table: sys_user)
         * @param params.verificationId The sys_id of the verification to be processed (table: pwd_verification)
         * @param request The form request object. Fields in the form can be accessed with request.getParameter(<element-id>)
         */
        return request.getParameter('ok') == 'ok';
    }
};
```

© 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 a Password Reset extension script
Create extension scripts only from the Password Reset Extension Script form. Do not create extension scripts in the System Definition > Script Includes interface.

Role required: password_reset_admin or admin

Note: To use a script include as an extension script, you must set it to Active status.

1. Navigate to Password Reset > Extensions > New extension script.
2. Enter a name in the Extension script name field.
   Use CamelCase to construct a name without spaces, for example, PwdEnrollmentCustom.
3. Select an Extension script category.
   - Enrollment check
   - Enrollment form processor
   - Identification form processor
   - Password generator
   - User account lookup
   - Verification form processor
4. Click Submit.
   A new instance of the script include for the selected category opens.
5. Edit the script by providing an implementation in the body of the process or processForm function, depending on the script category. You can add additional functions as long as the process or processForm function accepts the defined parameters and returns the expected results.

Note: Do not edit or delete the Category declaration.
6. Click Update.

Service desk: Reset a password for a user

In a service desk-assisted Password Reset process, service desk agents with the password_reset_service_desk role reset user passwords. Users do not reset passwords. Watch a video example of service desk agents resetting passwords: [Resetting User Passwords (Video)](https://service-now.com/). Note: You must set the Public access property to enable the service desk-assisted process. See [Settings on the Password Reset Details tab](https://service-now.com/).

Role required: password_reset_admin or password_reset_service_desk

---

1. Navigate to Password Reset > Service Desk.
2. Select a user and the Password Reset process to use.
3. Click Verify Identity.
4. On the Verify Identity form, enter the answers that the user provides and then click Continue. If the user identity is verified, the Reset Password form displays identity verification and status of the account lock.
5. Perform one of the following actions.
   - If the user is not locked, the form displays the Reset password button. Enter the new password and click Reset password.
• If the user is locked, the form displays the **Reset password** and **Unlock account** buttons. You can enter a new password and click **Reset password** to reset the password and unlock the account. If the **Enable account unlock** check box is selected for the password process, you can unlock the account without resetting the password by clicking **Unlock account**.

6. To reset the password for a different user, you must first navigate out of the Service Desk and then navigate to **Password Reset > Service Desk**.

**Service desk: View user requests for password reset**

The **Reset Requests** module displays the status of each password reset request from the Password Reset Request table (pwd_reset_request).

Role required: password_reset_admin or password_reset_service_desk

Navigate to **Password Reset > Reset Requests**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>The user whose password is being reset or changed.</td>
</tr>
<tr>
<td>Process</td>
<td>The process that implements this password reset request.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of Password Reset request:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Change Password</strong>: Request to change a password.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Help Desk</strong>: Request opened on behalf of the requesting user by a service desk agent.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Self Service</strong>: Requesting user opened the reset request.</td>
</tr>
<tr>
<td>Action Type</td>
<td>The corrective action performed during the Password Reset request.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Change Password</strong>: Update the credential store with the new password.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Reset and Unlock Account</strong>: Generate a new password for the user and unlock the user account.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Reset Password</strong>: Generate a new password for the user.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unlock Account</strong>: Unlock the user account.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Status</td>
<td>The result of the Password Reset request:</td>
</tr>
<tr>
<td></td>
<td>* <strong>Completed With Failure</strong>: User completed all steps in the Password Reset process, but the password was not reset in the credential store.</td>
</tr>
<tr>
<td></td>
<td>* <strong>Completed With Success</strong>: User completed all steps in the Password Reset process and the password was reset in the credential store.</td>
</tr>
<tr>
<td></td>
<td>* <strong>Expired</strong>: User did not complete all steps in the Password Reset process in the time allowed.</td>
</tr>
<tr>
<td></td>
<td>* <strong>In Progress</strong>: User is working through the steps to reset the password.</td>
</tr>
<tr>
<td></td>
<td>* <strong>Max Number of Attempts</strong>: User failed to answer the security questions correctly during the identity verification step and has exceeded the maximum number of attempts allowed.</td>
</tr>
<tr>
<td></td>
<td>* <strong>Verified</strong>: User has completed the identity verification step and is verified. The user can move to the Password Reset step.</td>
</tr>
<tr>
<td>Active</td>
<td>Whether the request is open or closed.</td>
</tr>
<tr>
<td>Retry</td>
<td>The total number of times the user has attempted to complete a password reset request.</td>
</tr>
</tbody>
</table>

**Service desk: Unblock a Password Reset user**

If a user is manually banned or flagged as exceeding max attempts, the user can be blocked (not allowed to use the Password Reset application). You can unblock a blocked user.

Role required: password_reset_admin or password_reset_service_desk

Blocking events include:

- The user exceeded the limit for the number of failed password attempts.
- The most recent password reset occurred before the wait time required until the next reset.
- The user failed to provide the correct information while attempting to reset the password.

If the number of blocked or locked users exceeds the limit within a defined time interval, it triggers a system log event. You can configure the number of blocked, or locked, users and the time interval required to generate the log event by setting the `password_reset.activity_monitor.incident_threshold` and `password_reset.activity_monitor.incident_window` properties.

1. To view the list of blocked users, navigate to **Password Reset > Blocked Users**.
2. To unblock a self-service user:
   a) Navigate to **Password Reset > Blocked Users**.
   b) Select a user from the list.
   c) Select **Delete** on the **Actions on selected rows** list.
3. To unblock a user whose password was reset by a service desk agent:
If a user is manually banned or flagged as exceeding max attempts, the user can be blocked (not allowed to use the Password Reset application). When the password reset request is made through self-service, the user is unblocked when the password is successfully reset.

In contrast, service desk agents are allowed any number of retries. The max_attempt_reached limit does not apply and the Blocked status for the user is not reset after the password is reset. As a result, after you successfully reset a user password, you must unblock the user manually.

If the user is not unblocked manually, then the system resets the blocked state only when the max_attempt_window time period elapses and the user tries to reset the password using self-service.

a) After you successfully reset a user password, navigate to Password Reset > Blocked Users.

b) Change the Blocked setting for the user from true to false.

Integrate Password Reset with a CMS integration

You can configure a site in the ServiceNow content management (CMS) application to define a single-site access point that includes the Password Reset service. For example, you can create an employee self-service site that provides Password Reset service.

Role required: content_admin

Each Password Reset process requires a separate CMS page.

1. Navigate to Content Management > Specialty Content > iFrames and create an iFrame record.

2. Go to Content Management > Sites and create a site that has no login page.
3. Go to **Content Management > Pages** and create a password reset page.

4. Enter the name of the site that you created in the **Content site** field (**Password Reset self-service** in the example).

5. Right-click the form header and click **Save**.

6. Click the **Edit Page** related link and then click **Add content**.

7. In the **Content Blocks** section, select the iFrame that you created. Add more content as needed.

8. Click **Update**.

**Password Reset and Password Change reports and logs**

The Password Reset application provides several tools for monitoring and troubleshooting password reset activities.

Users with the **password_reset_credential_manager** or **password_reset_admin** role can view the status of password reset activities, identify potential security threats, and monitor for compliance with password security policies.
The Reset Requests, Activity Log, and Blocked Users modules are useful for monitoring password reset activities and for troubleshooting password reset issues. They also provide access to more detailed information than is provided on the Overview module.

To make room for new data, the system periodically purges the data that is used for password reset monitoring and reporting.

**Password Reset Overview module**

The **Password Reset > Overview** module displays reports on password reset and password change activities. Users with the password_reset_admin role can customize the layout of the reports that appear in the Overview module.

**Password Reset reports**

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Requests (last 7 days)</td>
<td>Number of password reset requests by type during the last 7 days.</td>
</tr>
<tr>
<td>Blocked Users (last 7 days)</td>
<td>Number of users blocked over the last 7 days.</td>
</tr>
<tr>
<td>Password Reset Request Status (last 7 days)</td>
<td>The status of all password reset requests by process.</td>
</tr>
<tr>
<td>Password Reset Request by Action (last 30 days)</td>
<td>Number of password reset requests by action type: Reset Password, Unlock Account, or Reset and Unlock.</td>
</tr>
<tr>
<td>Password Reset Top Users (last 30 days)</td>
<td>Number of password reset requests per user. Many password reset requests from a single user could indicate a security issue.</td>
</tr>
<tr>
<td>Password Reset Failed Verifications (last 7 days)</td>
<td>Number of failed verification attempts, by verification instance. A failed verification occurs when a user attempts to reset the password, but fails for one reason or another, during the identity verification step. Many failed verification attempts for a specific type of verification could indicate that the process is too complicated or unclear.</td>
</tr>
<tr>
<td>Password Reset Enrollment By Verification</td>
<td>Number of users by verification type who have and have not enrolled in the password reset program. A large number for users who have not enrolled could indicate a compliance or communication issue within the organization.</td>
</tr>
<tr>
<td>Password Change Top Users (last 30 days)</td>
<td>Number of password change requests per user. Many password change requests from a single user could indicate a security issue.</td>
</tr>
</tbody>
</table>

**Password Reset activity log**

The activity log (**Password Reset > Activity Log**) provides detailed information that you can use to troubleshoot and to generate reports on password reset metrics. Information contained in the activity log is stored in the Password Reset activity log (pwd_reset_activity) table.

You must have the password_reset_credential_manager or password_reset_admin role to view the log.
Password Reset event log

The event log is a valuable resource for troubleshooting. On the Start menu, click Programs (or All Programs) > Administrative Tools > Event Viewer.

If the log does not appear, then, on the Windows Logs menu, click Applications > Service Logs. You must have the admin role to view the log.

To write to the Password Reset event log

Edit the DebugFlag registry key entry at: Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Windows > CurrentVersion > Authentication > Credential Providers > {B6EFF27D-C1C4-481F-B81B-F3547C47D58A}

By default, the key is set to 0. Set the key to 1 to write log entries to the ServiceNowPwdReset event log.

You must have the password_reset_credential_manager or password_reset_admin role to write to the log.

Password Reset blocked user notification

You can receive email notifications when the number of users that are blocked or locked exceeds the password blocked threshold. Notifications can alert you to suspicious activities. The default threshold is 10.

To subscribe: Add an email notification device or modify an existing device and then subscribe to the Password Reset-Activity Monitor Lockout notification.

You must have the password_reset_credential_manager or password_reset_admin role to subscribe.

Schedule for purging Password Reset data

To make room for new data, the system periodically purges the data that is used for password reset monitoring and reporting. Information contained in reports and monitoring tools could change dramatically immediately after a data purge. Contact ServiceNow Technical Support to modify purge intervals.

Purge intervals for Password Reset tables

<table>
<thead>
<tr>
<th>Table name</th>
<th>Purge interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>(pwd_reset_request)</td>
<td>90 days (7,776,000 seconds). Depending on your organizational data monitoring requirements, you could configure the rule to:</td>
</tr>
<tr>
<td></td>
<td>• Purge successful requests after 90 days</td>
</tr>
<tr>
<td></td>
<td>• Keep failed requests for 120 days</td>
</tr>
<tr>
<td>Table name</td>
<td>Purge interval</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>(pwd_user_lockout)</td>
<td>90 days (7,776,000 seconds).</td>
</tr>
<tr>
<td></td>
<td>Depending on your organizational data</td>
</tr>
<tr>
<td></td>
<td>monitoring requirements, you could</td>
</tr>
<tr>
<td></td>
<td>configure the rule to:</td>
</tr>
<tr>
<td></td>
<td>• Purge successful requests after 90</td>
</tr>
<tr>
<td></td>
<td>days</td>
</tr>
<tr>
<td></td>
<td>• Keep failed requests for 120 days</td>
</tr>
<tr>
<td>(pwd_reset_activity)</td>
<td>90 days (7,776,000 seconds).</td>
</tr>
<tr>
<td>(pwd_activity_monitor)</td>
<td>90 days (7,776,000 seconds).</td>
</tr>
<tr>
<td>(pwd_dvc_enrollment_code)</td>
<td>1 day (86,400 seconds).</td>
</tr>
<tr>
<td>(pwd_sms_code)</td>
<td>1 day (86,400 seconds).</td>
</tr>
</tbody>
</table>

**Users: Reset your password on Windows systems**

If your organization uses the Password Reset Windows Application, you can reset your password directly from your Windows login screen.

Role required: none

1. Start your computer or press **Ctrl+Alt+Delete** to go to the Windows login screen.
2. Click the **Forgot Password?** link. (Your administrator may have configured different text for the link.)

3. On the **Identify** page, enter the requested information and then click **Next**.

4. On the **Verify** page, enter the requested information, and then click **Next**.

**Note:** You might be given the option to choose the method used to verify your identity.

If your identity is verified, the **Reset** page displays whether you were successfully verified and the state of your account (either locked or unlocked).

5. Based on your locked/unlocked state, perform one of the following actions:
   - If your account is not locked, the page displays the **Reset Password** button. Enter and reenter the new password and then click **Reset Password**.
   - If your account is locked, the page displays the **Reset Password** and **Unlock Account** buttons.
     - You can enter a new password and click **Reset password** to reset the password and unlock the account.
• If your administrator has selected Enable account unlock for the password process, you can unlock the account without resetting the password by clicking Unlock account.

Users: Enroll in the Password Reset program

Some organizations auto-enroll users in a Password Reset program. Your organization could offer you the option to enroll for one or more methods of verifying your identity when you reset your password.

You might enroll for any combination of the following methods:

Verify your identity using security questions (QA verification)

To enroll, you choose multiple questions that only you can answer (like the name of your first pet) and then supply answers. The system stores your answers securely. Later, when you want to reset your password, the system presents one or more of the questions. You answer the questions to verify your identity.

Verify your identity using an SMS code (SMS verification)

To enroll, you authorize a device like a cellular phone for SMS verification. Later, when you want to reset your password, you get a code number on the device and enter the code on the web page to verify your identity.

Users: Enroll in the Password Reset program using questions and answers

Your organization might ask you to select the questions to use when resetting your password. You select the questions and provide answers that only you know. At another time, when you reset your password, your answers verify your identity.

Role required: none

1. Navigate to Password Reset > Enroll and then click the QA Verification tab.
   If you are required to enroll for the QA verification method, then the tab is marked with an asterisk (*).
2. For each Question field, select a question from the list and then enter the answer in the Answer field. Repeat the process until the required number of Question and Answer fields are filled in.
3. Click Submit.
4. Optional: Enroll for an extra identity verification using any of the other methods that your organization offers. See:
   • Users: Enroll in the Password Reset program using SMS codes

Users: Enroll in the Password Reset program using SMS codes

To prove that you are who you say you are (verify your identity) while resetting your password, you can use a code number (the SMS code) that was delivered to your mobile phone or device.

Role required: none

Note: You cannot enroll for this program on a mobile device.

1. Navigate to Password Reset > Enroll and then click the SMS Verification tab.
If your organization requires you to enroll for the SMS verification method, then the tab is marked with an asterisk (*).

2. If you had previously added an SMS-enabled device to your Password Reset profile, the device is listed. To add and verify a device, click **Add Device** and then follow the instructions. Provide a meaningful **Name** for each device. Repeat the process for as many devices as you need.

3. After you have verified each device, select the **Authorized** check box for each device that you expect to use to change or reset your password.

   **Note:** You can deauthorize a device at any time by clearing the **Authorized** check box.

4. Click **Submit**.

5. Optional: Enroll for an additional identity verification using any of the other methods that your organization offers. See:

   - **Users: Enroll in the Password Reset program using questions and answers**

**Self-service**

The Self-Service application gives supported end users a clean, simple front end to their IT support organization.

By default, the Self-Service application provides access to common actions, such as viewing your homepage, accessing the Service Catalog, viewing knowledge articles, working with incidents, and taking surveys.

**Service catalog requests**

This page contains links to content on service catalog requests.

**Add new request items**

Use ServiceNow’s web-based interface to add new items to a request.

Roles required: Only an administrator or a user with the catalog_admin role can add a new item to a submitted request.

Modifying a request does not resubmit it to the approval process.

1. Navigate to **Service Catalog > Open Records > Requests** and open an existing request.
2. Click **Add New Item**.
3. In the dialog box that appears, choose an item and a quantity to add.
4. Click **OK**.

**Amazon EC2 instance request from the Service Catalog**

Users can request the provisioning and deletion of virtual computers (Linux or Windows) in the Amazon EC2 virtual computing environment through the ServiceNow Service Catalog.

The Amazon EC2 offering requires the purchase and activation of ServiceNow Orchestration Automaton.
Request an instance

Request the provisioning of a new Amazon EC2 instance through the service catalog.

1. Navigate to **Self-Service > Service Catalog**.
2. Select **Amazon EC2 Instance** from the **Request Application Infrastructure** category.

3. Select the operating system, the type of instance (Large or Small), and the number of instances requested.

   See the specifications for Large and Small instances in Amazon EC2 Instance Types.

4. Type a reason for the request.
EC2 Service Catalog

5. Click **Order Now** to order the instance.

The Order Status form appears, summarizing the request. A status bar tracks the progress of the approval and provisioning of the EC2 instance.
Upon successful creation of the instance, you receive an email containing the instance ID, IP address, and the public DNS for the instances created.

**Terminate an instance**

Shut down an Amazon EC2 instance through the service catalog.

1. Navigate to **Service Catalog > Routine Changes > Terminate Amazon EC2 Instance**.
   
   A list appears displaying the instances that are assigned to you.

2. Select an instance from the list and click **Order**.
   
   This list does not support multi-line selection, and there is no **undo** feature.

**Check-out redirect property**

A property called One-step checkout redirect (**glide.vm.checkout_redirect**) controls the view presented to virtual machine requesters in the service catalog.

By default, this property is set to **false**, which redirects the view to the Order Status form when the requester clicks **Order Now**. When this property is set to **true**, ServiceNow redirects the requester to his or her My Virtual Assets portal. This property is located in **Cloud Management > Administration > Properties**.

**Delete request items**

Use ServiceNow’s web-based interface to delete items from a request.

All users can delete items from their own requests any time prior to delivery. Modifying a request does not resubmit it to the approval process.

1. Navigate to **Service Catalog > Open Records > Requests** and open an existing request.

2. In the **Requested Items** related list, select the check box beside the item to delete.
3. In the Actions choice list, select Delete. ServiceNow recalculates the price and delivery date for the order.

**Place a request**

Use ServiceNow’s web-based interface for ordering predefined goods and services.

1. Navigate to **Self-Service > Service Catalog**.

   The default catalog view organizes items in categories and subcategories.

   ![Service Catalog](image)

   **Default catalog view**

2. Select an item to order.

   **Note**: Some items are order guides, which combine related items for easier ordering. For example, an order guide called **New Employee Hire** presents a list of items that new employees typically receive (desk, phone, computer, email account). After you select the items you want to order, the order guide requests the information required and shows a separate time to delivery for each item ordered.

   The order screen requests any additional information that’s needed, such as the requester’s name or location and the date the item is needed. It also displays the item’s delivery time after approval.
Delivery time

3. Enter complete and accurate information to expedite your order.
4. Order any other items required.
5. Click **Order Now** when the order is complete.

ServiceNow displays a confirmation screen for your order:
Order submitted

You can view the order's progress in the Stage column.

Note: It may be useful to note the order number for future reference.

ServiceNow automatically notifies the approvers if approval is required and creates work orders to fulfill the order according to your organization's process. For example, if you order a new notebook computer, the purchasing group might receive a work order to order the computer, and the desktop services group might receive a work order to configure the new computer and deliver it to your office after it arrives.

Create incidents and change requests from a requested item

To quickly open an incident or a change request from a requested item, use the Create Change or the Create Incident UI action from the context menu of the requested item. It also maintains a linked relationship between the requested item, and its associated incidents or change requests.

The Create Change or Create Incident UI actions should be enabled by setting the Active field to true when you edit these UI actions.
Role required: itil

1. Navigate to **Self-Service > Requested Items**.
2. Open a requested item.
3. From the **Additional Actions** menu, select the **Create Change** or **Create Incident** UI action. By default, these UI actions are inactive.

**View request status**

Use ServiceNow's web-based interface to view the status of a request.

1. Navigate to **Self-Service > Requested Items**.
2. Click your order number to view details.
3. View the order's progress in the **Stage** field.
Customize homepages

If you are assigned at least one role in the system, you can create a customized homepage that you can see when you log in.

The content on your homepage comes from a variety of sources, such as graphs and charts generated from a report, application modules, a service catalog category, the scrolling news widget, which is the News knowledge category.

1. Navigate to **Self-Service > Homepage**.
2. Add any item to the homepage by clicking the add content icon (+) or the Add content link at the top.

A window will open that lets you select from a number of different homepage items you can add. Some items pertain to specific features and applications, such as CMS content blocks and the Work Management dispatch map. So the list of items varies depending on what is active on your system.

3. Reposition elements on your homepage by dragging and dropping them to a new location.

4. To remove a homepage item, click the (X) on the right side of the item's header.

Delete custom homepages

You can delete any of your custom homepages if you no longer need them.

1. Click the Delete page link at the bottom of the homepage.

2. Click Ok to confirm the deletion.

How Help the Help Desk identifies devices

Help the Help Desk uses a predefined series of queries to identify and update existing CIs in the CMDB or to create a new CI if no match is found.

These queries attempt to match devices using the three criteria listed here, in this order. Updates to an existing CI require only a single match as the list is evaluated. For example, if a device's name has changed, but the MAC address is the same, the CI with the matching MAC address is updated.

- Serial number in the `cmdb_ci_computer` table
- MAC address in the `cmdb_ci_network_adapter` table
- Computer name in the `cmdb_ci_computer` table
Note: Discovery Identifiers are incompatible with Help the Help Desk queries.

Script Include

The script include CIIdentifierForHelpDesk provides the logic for updating existing CIs or creating a new CI if no matching device exists in the CMDB. Do not modify this script. Errors introduced into this script can result in update failures or in new CIs being created for every device found.

Running Help the Help Desk

Help the Help Desk is a tool that enables users to populate the CMDB automatically with information about their Windows computer. Help the Help Desk is a small Web application that downloads and runs locally, using a login script to gather information such as serial number, computer name, disk configuration, network configuration, installed software, memory, and much more.

To detect all system software successfully on a 64-bit machine, make sure to run the Help the Help Desk script from a 64-bit browser. A 64-bit browser can detect both 64-bit and 32-bit software, but a 32-bit browser cannot detect 64-bit software.

1. On your instance, navigate to Self Service > Help the Help Desk.
2. Click Start the Scan to Help the Help Desk.
   You are prompted to run or save the discovery.hta script.
3. If your browser is Internet Explorer, run the script. If you are using any other browser, click Save and save the script to the local machine.
4. To execute the saved script, double click the file.
   The script runs a series of WMI queries to gather information about the Windows machine. When it is done, the data is sent back to your ServiceNow instance and used to populate the configuration database (CMDB).

Service Delegation

Service delegation is the ability to designate other users to view and interact with approvals sent or tasks assigned to you, and to receive copies of all email notifications sent to you.

Note: Users to whom you delegate responsibility see all pending tasks and approvals regardless of the delegation period.

Note: Delegation does not cascade. When a user acts as a delegate for another user, the delegate cannot in turn delegate to a third party. The original delegate is the only user who receives assignments and notifications. Delegation does not grant the delegate access to tasks where the caller or requester is the user for whom the delegate was created.

Add the Delegates related list to a user profile

To delegate approvals and tasks to another user, configure your user profile form to display the Delegates related list.

Role required: personalize_form or admin.

1. Navigate to Self-Service > My Profile.
2. On the form context menu, navigate to **Configure > Related Lists**, and then add the **Delegate->User** related list.

The Delegates related list displays at the bottom of the user profile form.

**Delegate approvals and tasks to another user**

If a user is out of the office, that user can delegate responsibilities to other users for a period of time.

1. Navigate to **Self Service > My Profile**.
2. In the **Delegates** related list, click **New**.

![Image of Delegates related list](image)

**Delegates Related List**

If the list is not visible, configure the form to add the **Delegate->User** related list.
3. Select the Delegate (User).
4. Set the period of time.
5. Specify the responsibilities the delegate will assume using the following check boxes. You can delegate:
   - **Approvals**: The delegate can approve items on your behalf.
   - **Assignments**: The delegate can view and work on tasks assigned to you.
   - **CC notifications**: The delegate receives a copy of email notifications sent to you, except those marked as Meeting Invitation.

   **Note:** If the **Approvals** check box is selected but **CC notifications** is not, the delegate does not receive approvals.

   - **Meeting invitations**: The delegate receives a copy of email notifications sent of the type Meeting Invitation.

   **Note:** You must select an active user as your delegate. The instance only delegates to active users.

A sample delegation looks like this:

![Delegation Options](image)

**Delegation Options**

**Note:** If your delegate gets email notifications, they will be the same email notifications sent to you. The delegate may be confused to see 'Incident assigned to you' emails, so make sure they know they are a delegate.
Service administration

Configure settings for services that support business applications or the platform.

Assessments

Use assessments to evaluate, score, and rank records from any table in the system.

You can assess projects that executives want to evaluate for effective management, or rate and compare a vendor's goods and services. Use assessments to send custom questionnaires to selected users or write scripts that query the database directly. You can then compare assessment results for the records using unique graphical views designed to highlight key performance information. Share an assessment between ServiceNow instances by using update sets, which is the recommended way to move assessment data from one instance to another.

The Assessments plugin is enabled by default.

Domain separation for assessments

Assessments support domain separation. If the metric type is global:

- All the categories and metric should be global
- Assessable records can be from different domains
- When the assessment is assigned to a user, then:
  - Users in the global domain can see all assessable records
  - Users in a particular domain can see assessable records in the global domain, in their domain, and in any child domains
  - If the user does not have access to any of the assessable records (for example, the metric type is global, but all assessable records are in acme domain and a user in the XYZ domain is assigned the assessment), the assessment instance will not be created and an "Instance could not be created" error is thrown.

If the metric type is not global:

- All categories and metrics must be in the same domain as the metric type
- All assessable records must be in the same domain as the metric type
- You can assign assessments to users that are in the global domain, in the domain of the metric type, or in any parent of the domain of the metric type

Installed with Assessments

- Demo data is available for assessments and surveys.
- Vendor Performance offers an additional set of vendor assessment demo data.

Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description: Assessments</th>
<th>Description: Surveys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessable Record</td>
<td>Stores all assesseable records.</td>
<td>For system use only.</td>
</tr>
<tr>
<td>(asmt_assessable_record)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Table</td>
<td>Description: Assessments</td>
<td>Description: Surveys</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Assessment Category Result</td>
<td>Stores all category results.</td>
<td>For system use only.</td>
</tr>
<tr>
<td>(asmt_category_result)</td>
<td></td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Assessment Category User</td>
<td>Stores associations between users and metric categories they can assess. A user that is</td>
<td>Stores associations between users and surveys. A user that is associated to a category is a survey user and is automatically associated to all the survey's categories.</td>
</tr>
<tr>
<td>(asmt_m2m_category_user)</td>
<td>category user.</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Assessment Group</td>
<td>Stores all assessment groups.</td>
<td>For system use only.</td>
</tr>
<tr>
<td>(asmt_assessment)</td>
<td></td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Assessment Instance</td>
<td>Stores all assessment instances.</td>
<td>Stores all survey instances.</td>
</tr>
<tr>
<td>(asmt_assessment_instance)</td>
<td></td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Assessment Instance Question</td>
<td>Stores all assessment instance questions, each of which represents one question on one assessment instance.</td>
<td>Stores all survey instance questions, each of which represents one question on one survey instance.</td>
</tr>
<tr>
<td>(asmt_assessment_instance_question)</td>
<td></td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Assessment Metric</td>
<td>Stores all metrics.</td>
<td>Stores all survey questions.</td>
</tr>
<tr>
<td>(asmt_metric)</td>
<td></td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Assessment Metric Definition</td>
<td>Stores all metric definitions.</td>
<td>Stores all answer options for survey questions.</td>
</tr>
<tr>
<td>(asmt_metric_definition)</td>
<td></td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Assessment Metric Template</td>
<td>Stores all metric templates.</td>
<td>Stores all question templates.</td>
</tr>
<tr>
<td>(asmt_template)</td>
<td></td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Assessment Metric Type</td>
<td>Stores all metric types.</td>
<td>Stores all survey definitions.</td>
</tr>
<tr>
<td>(asmt_metric_type)</td>
<td></td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Assessment Stakeholders</td>
<td>Stores associations between assessable records and category users. A category user that is associated to an assessable record is a stakeholder.</td>
<td>Not used for surveys.</td>
</tr>
<tr>
<td>(asmt_m2m_stakeholder)</td>
<td></td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Assessment Template Definition</td>
<td>Stores all metric template definitions.</td>
<td>Stores all question template definitions.</td>
</tr>
<tr>
<td>(asmt_template_definition)</td>
<td></td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Assessment X Category Matrix</td>
<td>Allows users to specify metric categories as the X axis of a decision matrix.</td>
<td>Not used for surveys.</td>
</tr>
<tr>
<td>(asmt_m2m_xcategory_matrix)</td>
<td></td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Assessment Y Category Matrix</td>
<td>Allows users to specify metric categories as the Y axis of a decision matrix.</td>
<td>Not used for surveys.</td>
</tr>
<tr>
<td>(asmt_m2m_ycategory_matrix)</td>
<td></td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Bubble Chart</td>
<td>Stores all bubble chart definitions.</td>
<td>Not used for surveys.</td>
</tr>
<tr>
<td>(asmt_bubble_chart)</td>
<td></td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Category Assessable Records</td>
<td>Stores associations between assessable records and metric categories.</td>
<td>For system use only.</td>
</tr>
<tr>
<td>(asmt_m2m_category_assessment)</td>
<td></td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
### Table

<table>
<thead>
<tr>
<th>Table</th>
<th>Description: Assessments</th>
<th>Description: Surveys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decision Matrix (asmt_decision_matrix)</td>
<td>Stores all <a href="#">decision matrixes</a></td>
<td>Not used for surveys.</td>
</tr>
<tr>
<td>Metric Category (asmt_metric_category)</td>
<td>Stores all <a href="#">metric categories</a></td>
<td>Stores all survey categories.</td>
</tr>
<tr>
<td>Metric Result (asmt_metric_result)</td>
<td>Stores all <a href="#">metric results</a></td>
<td>Stores all <a href="#">survey responses</a>.</td>
</tr>
<tr>
<td>Signature (asmt_signature)</td>
<td>Stores all <a href="#">signature records</a> for assessments and ([Attestations</td>
<td>Stores all signature records for surveys.</td>
</tr>
<tr>
<td>Trigger Condition (asmt_condition)</td>
<td>Stores all <a href="#">assessment trigger conditions</a></td>
<td>Stores all <a href="#">survey trigger conditions</a>.</td>
</tr>
</tbody>
</table>

### Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sn_portal_surveys.sp_survey.email_redirection</td>
<td>Allow a survey accessed from a link in an email to open in the Service Portal (applies only for surveys).</td>
</tr>
<tr>
<td></td>
<td>- <strong>Type</strong>: Yes/No</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default value</strong>: no</td>
</tr>
<tr>
<td></td>
<td>- <strong>Location</strong>: Assessments &gt; Admin &gt; Assessment Properties, Survey Management &gt; Administration &gt; Properties</td>
</tr>
<tr>
<td></td>
<td>- <strong>Learn more</strong>: <a href="#">Customize the appearance of a survey</a></td>
</tr>
<tr>
<td>com.snc.assessment.signature_authentication</td>
<td>Require authentication for user signature. When Yes is selected, this property requires credentials for a full name signature.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Type</strong>: True/False</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default value</strong>: true</td>
</tr>
<tr>
<td></td>
<td>- <strong>Location</strong>: Assessments &gt; Admin &gt; Assessment Properties, Survey Management &gt; Administration &gt; Properties</td>
</tr>
<tr>
<td></td>
<td>- <strong>Learn more</strong>: <a href="#">Signatures</a></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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>- <strong>Type:</strong> color</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default value:</strong> #767676</td>
</tr>
<tr>
<td></td>
<td>- <strong>Location:</strong> Assessments &gt; Admin &gt; Assessment Properties</td>
</tr>
<tr>
<td></td>
<td>- Survey Management &gt; Administration &gt; Properties</td>
</tr>
<tr>
<td></td>
<td>- <strong>Learn more:</strong> <a href="#">Customize the appearance of a survey</a></td>
</tr>
<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>- <strong>Type:</strong> color</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default value:</strong> #eee</td>
</tr>
<tr>
<td></td>
<td>- <strong>Location:</strong> Assessments &gt; Admin &gt; Assessment Properties</td>
</tr>
<tr>
<td></td>
<td>- Survey Management &gt; Administration &gt; Properties</td>
</tr>
<tr>
<td></td>
<td>- <strong>Learn more:</strong> <a href="#">Customize the appearance of a survey</a></td>
</tr>
<tr>
<td>com.snc.assessment.decision_matrix_filter_max_entries</td>
<td>Maximum number of items to show for a decision matrix field filter.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Type:</strong> integer</td>
</tr>
<tr>
<td></td>
<td>- <strong>Default value:</strong> 1000</td>
</tr>
<tr>
<td></td>
<td>- <strong>Location:</strong> Assessments &gt; Admin &gt; Assessment Properties</td>
</tr>
<tr>
<td></td>
<td>- Survey Management &gt; Administration &gt; Properties</td>
</tr>
<tr>
<td></td>
<td>- <strong>Learn more:</strong> <a href="#">Customize the appearance of a survey</a></td>
</tr>
</tbody>
</table>
### Name: css.assessment.caption.font.color

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

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

**Learn more:** Customize the appearance of a survey

### User roles

<table>
<thead>
<tr>
<th>Role title (name)</th>
<th>Description</th>
<th>Contains roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>assessment administrator (assessment_admin)</td>
<td>Can administer the Assessments application. Can access all the modules of the Assessments application.</td>
<td>None</td>
</tr>
</tbody>
</table>

**Note:** The assessment_admin role is contained by the itil_admin role. It is also contained by the survey_admin role.

### Script includes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AssessmentUtils</td>
<td>Core code for assessment functionality.</td>
</tr>
<tr>
<td>AssessmentUtilsAJAX</td>
<td>AJAX based code for displaying scorecard data.</td>
</tr>
<tr>
<td>MigrateSurveyToAssessment</td>
<td>Code for migrating legacy surveys to assessment surveys.</td>
</tr>
<tr>
<td>RatingUtilsAJAX</td>
<td>Reserved for future use.</td>
</tr>
<tr>
<td>SurveyUtils</td>
<td>Core code for survey functionality.</td>
</tr>
</tbody>
</table>
## Client scripts

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calculate Assessable Record Field choice list</td>
<td>Trigger Condition (asmt_condition)</td>
<td>Limits the Assessable Record Field choices to those that are compatible with the selected assessment.</td>
</tr>
<tr>
<td>Check survey schedule period</td>
<td>Trigger Condition (asmt_condition)</td>
<td>Checks the selected survey definition's Schedule period. If Schedule period is set to Only Once, this client script displays a warning message that each user can only take the selected survey once.</td>
</tr>
<tr>
<td>Clear display_when when depends changed</td>
<td>Assessment Metric (asmt_metric)</td>
<td>Shows the Display when field when the Depends on field is set. Clears the Display when field when the Depends on field changes and the options need to change.</td>
</tr>
<tr>
<td>Conditionally Set Type for Surveys</td>
<td>Group (sys_user_group)</td>
<td>Sets the user group Type to survey if you create a new group from the User Groups module.</td>
</tr>
<tr>
<td>Data type -- Hide choices for surveys</td>
<td>Assessment Metric (asmt_metric)</td>
<td>Ensures only Data type options that are valid for surveys are available on the Survey Question form.</td>
</tr>
<tr>
<td>Data type -- Show/Hide Not Applicable</td>
<td>Assessment Metric (asmt_metric)</td>
<td>Hides the Allow not applicable field and sets its value to false if the metric method is Assessment and the data type is Percentage, Checkbox, Date, Date/Time, Number, or String.</td>
</tr>
<tr>
<td>Datatype defaults to String for surveys</td>
<td>Assessment Metric (asmt_metric)</td>
<td>Sets the default Data type field value to String on the Survey Question form.</td>
</tr>
<tr>
<td>Fetch Min/Max</td>
<td>Assessment Metric (asmt_metric)</td>
<td>Updates the Min and Max fields to match the least and greatest metric template definition values if an assessment administrator selects or changes the Template value.</td>
</tr>
<tr>
<td>Hide Assessable Record Field</td>
<td>Trigger Condition (asmt_condition)</td>
<td>Hides the Assessable Record field unless the evaluation method of the metric type selected in the Assessment field is Assessment.</td>
</tr>
<tr>
<td>Hide assessment if empty</td>
<td>Survey (survey_master)</td>
<td>Hides the Assessment field on the Survey form unless it contains a value. The system populates the Assessment field when you migrate a survey.</td>
</tr>
<tr>
<td>Name</td>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Hide Survey Instance Trigger ID if Empty</td>
<td>Assessment Instance</td>
<td>Hides the Trigger ID field and makes it read-only unless it contains a value.</td>
</tr>
<tr>
<td></td>
<td>(asmt_assessment_instance)</td>
<td></td>
</tr>
<tr>
<td>Hide user lists</td>
<td>Assessable Record</td>
<td>Hides the Category users related list if the associated metric type schedule type is On demand.</td>
</tr>
<tr>
<td></td>
<td>(asmt_assessable_record)</td>
<td></td>
</tr>
<tr>
<td>Hide user related lists</td>
<td>Metric Category</td>
<td>Hides the User related list if the associated metric type schedule type is On demand and the Evaluation method is not Survey.</td>
</tr>
<tr>
<td></td>
<td>(asmt_metric_category)</td>
<td></td>
</tr>
<tr>
<td>Hide value or String value</td>
<td>Assessment Instance Question</td>
<td>Hides the Value field and shows the String value field if the associated metric data type is Date, Date/Time, or String. Does the opposite if the data type is anything else.</td>
</tr>
<tr>
<td></td>
<td>(asmt_assessment_instance_question)</td>
<td></td>
</tr>
<tr>
<td>Live feed deletion warning</td>
<td>Assessable Record</td>
<td>Displays a warning message if an assessment administrator clears the Live feed check box.</td>
</tr>
<tr>
<td></td>
<td>(asmt_assessable_record)</td>
<td></td>
</tr>
<tr>
<td>Method -- Show/Hide Not Applicable</td>
<td>Assessment Metric</td>
<td>Hides the Mandatory and Allow not applicable fields and sets both values to false if the metric method is Script. Shows the Mandatory field if the metric method is Assessment. Shows the Allow not applicable field if the method is Assessment except when the data type is Percentage, Checkbox, Date, Date/Time, Number, or String.</td>
</tr>
<tr>
<td></td>
<td>(asmt_metric)</td>
<td></td>
</tr>
<tr>
<td>Min/Max Control</td>
<td>Assessment Metric</td>
<td>Makes the Min and Max fields mandatory except when the data type is Template.</td>
</tr>
<tr>
<td></td>
<td>(asmt_metric)</td>
<td></td>
</tr>
<tr>
<td>Min/Max Read-only</td>
<td>Assessment Metric</td>
<td>Makes the Min and Max fields read-only when the data type is Choice or Likert Scale.</td>
</tr>
<tr>
<td></td>
<td>(asmt_metric)</td>
<td></td>
</tr>
<tr>
<td>Populate Groups</td>
<td>Assessment Metric Type</td>
<td>Populates the available values for the Filter field with fields from the selected metric type table.</td>
</tr>
<tr>
<td></td>
<td>(asmt_metric_type)</td>
<td></td>
</tr>
<tr>
<td>Read only Type</td>
<td>Metric Category</td>
<td>Makes the Type field read-only when it contains a value.</td>
</tr>
<tr>
<td></td>
<td>(asmt_metric_category)</td>
<td></td>
</tr>
<tr>
<td>Reload Decision Matrix Filter Columns</td>
<td>Assessment Metric Type</td>
<td>Populates the available choices for the Default matrix filter as appropriate if the Filter field value changes.</td>
</tr>
<tr>
<td></td>
<td>(asmt_metric_type)</td>
<td></td>
</tr>
<tr>
<td>Reload default filters</td>
<td>Assessment Metric Type</td>
<td>Populates the available choices for the Default filter as appropriate if the Display all filters value changes.</td>
</tr>
<tr>
<td></td>
<td>(asmt_metric_type)</td>
<td></td>
</tr>
<tr>
<td>Set scale factor</td>
<td>Assessment Metric Type</td>
<td>Reserved for future use.</td>
</tr>
<tr>
<td></td>
<td>(asmt_metric_type)</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Set table field</td>
<td>Metric Category (asmt_metric_category)</td>
<td>Sets the category Table value to that of the metric type.</td>
</tr>
<tr>
<td>Show and Hide Scheduled Job</td>
<td>Assessment Metric Type (asmt_metric_type)</td>
<td>Hides the Scheduled job field if the Schedule type is On demand and shows the Scheduled job field if the Schedule type is Scheduled.</td>
</tr>
<tr>
<td>Show and Hide Scheduled Job</td>
<td>Assessment Metric Type (asmt_metric_type)</td>
<td>Shows the Scheduled job field on the Survey Definition form if the Schedule period is Daily, Weekly, Monthly, or Yearly.</td>
</tr>
<tr>
<td>Survey View</td>
<td>Assessment Metric Type (asmt_metric_type)</td>
<td>Shows the Scheduled job field on the Survey Definition form if the Schedule period is Daily, Weekly, Monthly, or Yearly.</td>
</tr>
<tr>
<td>Toggle Metric Definitions (Load)</td>
<td>Assessment Metric (asmt_metric)</td>
<td>Displays the Assessment Metric Definitions related list if the data type is Choice or Likert Scale.</td>
</tr>
<tr>
<td>Toggle Metric Definitions (Update)</td>
<td>Assessment Metric (asmt_metric)</td>
<td>Displays the Assessment Metric Definitions related list if the data type is Choice or Likert Scale. Sets the Method field to the appropriate value if the data type is compatible with one method only.</td>
</tr>
<tr>
<td>Update Min And Max Default Values</td>
<td>Assessment Metric (asmt_metric)</td>
<td>Sets reasonable default values for the Min and Max fields, based on the data type.</td>
</tr>
<tr>
<td>Validate Probability</td>
<td>Survey Trigger Condition (asmt_condition)</td>
<td>Ensures that the Probability (%) value is a whole number between 1 and 100.</td>
</tr>
<tr>
<td>Verify Max</td>
<td>Assessment Metric (asmt_metric)</td>
<td>Verifies that the Max value is greater than the Min value and greater than or equal to zero if the metric method is Assessment.</td>
</tr>
<tr>
<td>Verify Min</td>
<td>Assessment Metric (asmt_metric)</td>
<td>Verifies that the Min value is less than the Max value and greater than or equal to zero if the metric method is Assessment.</td>
</tr>
<tr>
<td>Verify Value</td>
<td>Assessment Metric Definition (asmt_metric_definition)</td>
<td>Verifies that the Value is greater than or equal to zero.</td>
</tr>
<tr>
<td>Verify Value</td>
<td>Assessment Template Definition (asmt_template_definition)</td>
<td>Verifies that the Value is greater than or equal to zero.</td>
</tr>
</tbody>
</table>
## Business rules for Assessments

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessable domain matches type</td>
<td>Assessable Record (asmt_assessable_record)</td>
<td>Ensures that all new assessable records are in the same domain as the metric type. This is a special requirement of assessment domain separation, that all records must be in the same domain.</td>
</tr>
<tr>
<td>Auto stakeholder creation</td>
<td>Assessment Category User</td>
<td>Assigns new category users as stakeholders automatically for assessable records if the associated category has the Create stakeholders check box selected.</td>
</tr>
<tr>
<td>Auto stakeholder creation</td>
<td>Category Assessable Records</td>
<td>Creates stakeholders from all of a category's category users automatically for new assessable records if:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The Create stakeholders check box is selected for the metric category.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The same metric category is associated to the new assessable record.</td>
</tr>
<tr>
<td>Auto stakeholder creation</td>
<td>Metric Category (asmt_metric_category)</td>
<td>Assigns all of a category's category users as stakeholders for each assessable record associated to the category when the Create stakeholders check box is selected for the category.</td>
</tr>
<tr>
<td>Calculate category max weight</td>
<td>Assessment Metric (asmt_metric)</td>
<td>Calculates the sum of all metric weights in a category.</td>
</tr>
<tr>
<td>Cancel notification workflow</td>
<td>Assessment Instance (asmt_assessment_instance)</td>
<td>Cancels the workflow that generates assessment email notifications when an assessment instance is deleted or changes state to Complete or Canceled.</td>
</tr>
<tr>
<td>Category domain matches type</td>
<td>Metric Category (asmt_metric_category)</td>
<td>Ensures that all new categories are in the same domain as the metric type. This is a special requirement of assessment domain separation, that all records must be in the same domain.</td>
</tr>
<tr>
<td>Name</td>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Check Live Feed Groups</td>
<td>Assessable Record (asmt_assessable_record)</td>
<td>Selects the Live feed check box if a live feed group is associated with the source record. If the Live feed check box is selected and no live feed group is associated with the source record, this business rule clears the check box.</td>
</tr>
<tr>
<td>Check only one default</td>
<td>Bubble Chart (asmt_bubble_chart)</td>
<td>Ensures there is only one default bubble chart for a metric type.</td>
</tr>
<tr>
<td>Check only one default</td>
<td>Decision Matrix (asmt_decision_matrix)</td>
<td>Ensures there is only one default decision matrix for a metric type.</td>
</tr>
<tr>
<td>Create actual results</td>
<td>Assessment Instance (asmt_assessment_instance)</td>
<td>Generates assessment and category results from the user responses if a user completes an assessment.</td>
</tr>
<tr>
<td>Create Business Rule on Remote table</td>
<td>Assessment Metric Type (asmt_metric_type)</td>
<td>Generates the following business rules if an assessment administrator creates or updates a metric type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Business rule called Auto business rule for Assessments, which monitors the Table selected for the metric type. When someone adds a record that meets the metric type conditions, this business rule generates an assessable record. If someone changes the metric type’s Table or conditions, the Create Business Rule on Remote table business rule updates the automatic business rule script to reflect the changes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Business rule called Auto deletion rule for Assessments, which prevents users from deleting a record on the metric type’s Table if the record is associated to metric or category results. If the record has no associated results and a user deletes it, this business rule deletes any associated assessable records.</td>
</tr>
</tbody>
</table>

The Create Business Rule on Remote table business rule generates automatic business rules only for metric types with Evaluation method set to Assessment.
<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
</table>
| Create Scheduled Job                      | Assessment Metric Type (asmt_metric_type) | Assessments: Generates a scheduled job for the creation of assessment components if either of these conditions is met:  
- Someone creates a new metric type with the schedule type set to Scheduled.  
- The schedule type changes from On demand to Scheduled.  
Surveys: Generates a scheduled job for the creation of survey components if the schedule period for a survey definition is set to Daily, Weekly, Monthly, or Yearly. |
<p>| Create Survey Records                     | Assessment Metric Type (asmt_metric_type) | Generates various records and populates certain fields on those records when someone creates a new survey definition, which is a metric type with Evaluation method set to Survey. More specifically, this business rule generates a survey category and assessable record, both associated to the survey definition. |
| Create UI Action on Remote table          | Assessment Metric Type (asmt_metric_type) | Reserved for future use.                                                                                                                                                                                     |
| decision_matrix_axis                      | Global (global)                      | Limits available categories for X- and Y-axes to those that belong to the type if there is a metric type specified on the Decision Matrix form.                                                                |
| Delete Live Feed Group                    | Assessable Record (asmt_assessable_record) | Deletes the assessable record’s live feed group, if there is one, when an assessment administrator deletes an assessable record.                                                                               |
| delete related users                      | Category Assessable Records (asmt_m2m_category_assessment) | Deletes any stakeholders for the assessable record and category when an assessment administrator dissociates a category from an assessable record.                                                      |
| Do not allow category to change           | Assessment Metric (asmt_metric)       | Prevents the Category field from being changed if there are any conditional question dependencies related to the current record.                                                                            |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not allow datatype to change</td>
<td>Assessment Metric (asmt_metric)</td>
<td>Prevents the Data type and Template fields from being changed if there are any conditional questions that depend on the current record.</td>
</tr>
<tr>
<td>Ensure Types Match</td>
<td>Assessment Metric (asmt_metric)</td>
<td>Sets the type of a metric to the type of the associated category.</td>
</tr>
<tr>
<td>Ensure types match</td>
<td>Assessment Stakeholders (asmt_m2m_stakeholder)</td>
<td>Ensures users can only create a stakeholder from a category user and assessable record of the same type.</td>
</tr>
<tr>
<td>Ensure types match</td>
<td>Category Assessable Records (asmt_m2m_category_assessment)</td>
<td>Prevents users from associating categories of one type to an assessable record of a different type.</td>
</tr>
</tbody>
</table>
| Evaluate filters                    | Assessable Record (asmt_assessable_record) | Performs the following after the system generates a new assessable record:  
  - Checks all filter conditions for categories in the type.  
  - Automatically associates the new assessable record to all categories for which it meets the category filter conditions.                                                                                                                                                                                                                             |
| Generate assessment trigger condition | Trigger Condition (asmt_condition) | Generates a business rule the survey or assessment trigger condition uses to send surveys or assessments.                                                                                                                                                                                                                                                                                                                  |
| getStakeholders                     | Global (global)               | Ensures that only category users for categories associated with the assessable record are available on the Assessable Record form when users edit the Category users related list.                                                                                                                                                                                                                                              |
| Link assessable record and category | Metric Category (asmt_metric_category) | Sets these hidden fields as follows for a newly created survey category:  
  - Table: Assessment Metric Type (asmt_metric_type)  
  - Filter: `<sys_id of the survey definition the new survey category is associated with>`                                                                                                                                                                                                                                                                         |
<p>| Live Feed Group                     | Assessable Record (asmt_assessable_record) | Creates a live feed group for the assessable record, if one does not exist, when the record is saved with the Live feed check box selected. If the check box is then cleared and the record saved, this business rule deletes an existing live feed group.                                                                                                                        |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metric domain matches category</td>
<td>Assessment Metric (asmt_metric)</td>
<td>Ensures that all new metrics are in the same domain as the category to which they belong. This is a special requirement of assessment domain separation, that all records must be in the same domain.</td>
</tr>
<tr>
<td>Notify assessment user</td>
<td>Assessment Instance (asmt_assessment_instance)</td>
<td>Starts a workflow that sends an email notification to the assigned user when an assessment instance changes to the Ready state or the user to which it is assigned changes. The workflow generates other assessment email notifications at later stages.</td>
</tr>
<tr>
<td>Prevent recursive dependencies</td>
<td>Assessment Metric (asmt_metric)</td>
<td>Prevents the Depends on field from being set in a way that creates a recursive conditional question dependency.</td>
</tr>
<tr>
<td>Publish Survey</td>
<td>Assessment Metric Type (asmt_metric_type)</td>
<td>Generates survey instances and assigns them to the associated survey users when the survey definition state changes from Draft to Published.</td>
</tr>
<tr>
<td>Remove auto create Business Rules</td>
<td>Assessment Metric Type (asmt_metric_type)</td>
<td>Deletes the automatically created business rule for a metric type when an assessment administrator deletes that metric type.</td>
</tr>
<tr>
<td>Remove auto create UI Actions</td>
<td>Assessment Metric Type (asmt_metric_type)</td>
<td>Reserved for future use.</td>
</tr>
<tr>
<td>Remove auto created business rule</td>
<td>Survey Trigger Condition (asmt_condition)</td>
<td>Deletes the automatically created business rule when someone deletes the survey trigger condition.</td>
</tr>
</tbody>
</table>
| Remove Scheduled Job                             | Assessment Metric Type (asmt_metric_type) | Assessments: Deletes the scheduled job for a metric type if either of these conditions is met:  
• Someone deletes the metric type.  
• Someone changes the schedule type from Scheduled to On demand.  
Surveys: Deletes the scheduled job for a survey definition if the schedule period is set to Only Once or No Limit. |
<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset Min/Max for metric</td>
<td>Assessment Metric Definition (asmt_metric_definition)</td>
<td>Updates the Min and Max fields for metrics and survey questions based on the metric definition Value.</td>
</tr>
<tr>
<td>Set Domain for M2M Cat Assessable Recs</td>
<td>Category Assessable Records (asmt_m2m_category_assessment)</td>
<td>Ensures that assessable records are only associated to categories in the same domain. This is a special requirement of assessment domain separation, that all records must be in the same domain.</td>
</tr>
<tr>
<td>Set Domain for M2M Category Users</td>
<td>Assessment Category User (asmt_m2m_category_user)</td>
<td>Ensures that users are only linked to categories in the same domain. This is a special requirement of assessment domain separation, that all records must be in the same domain.</td>
</tr>
<tr>
<td>Set Domain for M2M Stakeholders</td>
<td>Assessment Stakeholders (asmt_m2m_stakeholder)</td>
<td>Ensures that assessable records are only linked to category users in the same domain. This is a special requirement of assessment domain separation, that all records must be in the same domain.</td>
</tr>
<tr>
<td>Set scratchpad fields</td>
<td>Assessment Metric Type (asmt_metric_type)</td>
<td>Caches field values for use by other scripts that run on the Assessment Metric Type form.</td>
</tr>
<tr>
<td>Store view type</td>
<td>Metric Category (asmt_metric_category)</td>
<td>Ensures that the Type field only allows users to select metric types used for assessments.</td>
</tr>
<tr>
<td>Synchronize category survey users</td>
<td>Assessment Category User (asmt_m2m_category_user)</td>
<td>Ensures that the same users are associated with all of a survey’s categories.</td>
</tr>
<tr>
<td>Synchronize survey users and stakeholder.</td>
<td>Metric Category (asmt_metric_category)</td>
<td>Adds all users associated with a survey’s existing categories to any newly created category for that survey.</td>
</tr>
<tr>
<td>Update Category Count</td>
<td>Assessment Metric (asmt_metric)</td>
<td>Updates the value in the Total metrics field on the Metric Category form when metrics are added to and deleted from the category.</td>
</tr>
<tr>
<td>Name</td>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Update records that match filter</td>
<td>Metric Category (asmt_metric_category)</td>
<td>Automatically performs these tasks when an assessment administrator edits the Filter field:&lt;br&gt;  - Associates the category to assessable records that meet the filter conditions.&lt;br&gt;  - Disassociates the category from assessable records that do not meet the filter conditions.&lt;br&gt;The Assessable records related list reflects these changes when the record is saved.</td>
</tr>
<tr>
<td>Update scheduled job on schedule change</td>
<td>Assessment Metric Type (asmt_metric_type)</td>
<td>Updates the survey creation scheduled job to reflect schedule period changes.</td>
</tr>
<tr>
<td>Validate mandatory and not applicable</td>
<td>Assessment Metric (asmt_metric)</td>
<td>Sets the Mandatory and Allow not applicable fields to false if the metric method is Script. If the metric data type is Percentage, the business rule sets the Allow not applicable field to false.</td>
</tr>
<tr>
<td>Verify min/max</td>
<td>Assessment Metric (asmt_metric)</td>
<td>Ensures that the Min is greater than or equal to zero and less than the Max. Sets the Min to 0 and the Max to 1 if the data type is Checkbox or Yes/No.</td>
</tr>
<tr>
<td>Verify value</td>
<td>Assessment Template Definition (asmt_template_definition)</td>
<td>Ensures that the metric template definition Value is:&lt;br&gt;  - Greater than or equal to zero.&lt;br&gt;  - Different from the Value for all other metric template definitions related to the template.</td>
</tr>
<tr>
<td>Verify value</td>
<td>Assessment Metric Definition (asmt_metric_definition)</td>
<td>Ensures that users can only enter a metric definition Value greater than or equal to zero. Ensures that the metric definition Value is different from the Value for all other metric definitions related to the metric.</td>
</tr>
</tbody>
</table>

**Assessment Administrator tasks**

Before you create assessments, assign the assessment_admin role to the appropriate users in your organization and determine your objectives for the assessment.

Decide which sets of records in the system to assess, which themes you are interested in, and which traits to measure. Consider your organization’s options for obtaining the data to compare. If you intend to use assessment questionnaires, consider which people can answer the questions.
## Assessment terminology

Assessment admins use several terms when working with assessments.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metric type</td>
<td>A <em>metric type</em> defines a set of records to evaluate, such as vendors, projects, or employees.</td>
</tr>
<tr>
<td>Assessable record</td>
<td>An <em>assessable record</em> links a record to evaluate, such as the company record for Amazon or the user record for a sales representative, to a metric type, such as vendors or employees. You define sets of assessable records when you create metric types.</td>
</tr>
<tr>
<td>Metric category</td>
<td>A <em>metric category</em> represents a theme for evaluating assessable records. Categories contain one or more individual metrics, which define specific traits or values that comprise the theme. Examples of categories include overall vendor performance or quality of delivery services. You can also set filter conditions that control which assessable records to evaluate for the metrics in a category.</td>
</tr>
<tr>
<td>Metric</td>
<td>A <em>metric</em> is a trait or value used to evaluate assessable records. A metric can measure subjective values in an assessment questionnaire, or gather objective values in a database query run by a script. Examples of metrics include perceived courtesy of sales representatives or number of incidents per vendor.</td>
</tr>
<tr>
<td>Category user</td>
<td>A <em>category user</em> is a person who knows about a specific category. One person can be a category user for multiple categories. Examples of category users include a vendor manager who oversees all purchasing operations or a supervisor of a sales team.</td>
</tr>
<tr>
<td>Stakeholder</td>
<td>A <em>stakeholder</em> is a category user who knows about a specific assessable record. Examples of stakeholders include a vendor manager who coordinates purchases from Amazon or a supervisor of a sales team who manages a specific employee.</td>
</tr>
</tbody>
</table>
| Assessment instance | An *assessment instance* represents one assessment questionnaire assigned to one user. The system generates a new assessment instance for each assigned user when:  
  - The assessment generation scheduled job runs.  
  - An assessment administrator creates an on-demand assessment. |
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scorecard</td>
<td>A scorecard provides a visual illustration of an assessable record’s performance, based on assessment results. Use scorecards to view a variety of data summaries for one assessable record and to compare the ratings with other assessable records.</td>
</tr>
<tr>
<td>Decision matrix</td>
<td>A decision matrix is a graph with two axes that plots the assessment results for multiple assessable records. Use decision matrices to determine the relative standing of assessable records in selected categories.</td>
</tr>
<tr>
<td>Bubble chart</td>
<td>A bubble chart is a graph with three axes that plots the assessment results for multiple assessable records. Use bubble charts to determine the relative standing of assessable records in selected categories, with an emphasis on one category.</td>
</tr>
</tbody>
</table>

**Assessment roles**

The Assessments application requires certain roles to perform assessment tasks. No role is required to take assessment questionnaires that are assigned to you.

<table>
<thead>
<tr>
<th>Role Title</th>
<th>Role Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment administrator</td>
<td>assessment_admin</td>
<td>Assessment administrators set up assessments. They know which records to evaluate, the criteria on which to evaluate the records, and who to assign assessments to.</td>
</tr>
</tbody>
</table>

*Note:* By default, users with the assessment_admin role have limited system rights and might not have access to all source records to assess. When planning assessments, grant additional roles to assessment administrators as needed. For example, to create and manage vendor assessments, the assessment administrator must also have the vendor_manager role, which grants access to the Company table and other relevant tables.

© 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.
### Role Title | Role Name | Description
--- | --- | ---
ITIL user | itil | ITIL users perform basic technician operations in the system. In the Assessments application, they have read access to the Assessable Record table.

Administrator | admin | Administrators have access to all aspects of the assessment process. Only administrators can set up assessment schedules.

#### Assessment methods

The available methods are **Assessment**, for non-scripted metrics, and **Script**, for scripted metrics. Each method serves a different function and can be used with certain data types.

Use the **Method** field to specify how to use the metric.

#### Assessment method

Metrics with the Method set to Assessment are called non-scripted metrics. Use each non-scripted metric to define a question for assessment questionnaires. Non-scripted metrics are useful if you want to obtain subjective data like personal opinions.

You can use the Assessment method with these **Data type** values:

- Attachment
- Checkbox
- Choice
- Date
- Date/Time
- Likert Scale
- Number
- Percentage
- String
- Template
- Yes/No

#### Script method

Metrics with the Method set to Script are called scripted metrics. Use each scripted metric to define a custom script for database queries. Scripted metrics are useful if your system contains reliable data for the traits you want to evaluate.

You can use the Script method with these **Data type** values:

- Duration
- Number
- Percentage
Use the Script field to write JavaScript code. By default, the field contains information about available variables and an example, which you can use as the basis of your script or replace entirely:

```
1 // The following variables are available:
2 // - primary: contains the sys_id of the record being evaluated
3 // - actual_result: the script sets the actual value for this metric to this variable
4 // - scaled_result: the script sets the scaled value (used in calculations) for this metric to this variable
5 // For example:
6 // var gr = new GlideRecord('cmdh_ci');
7 // gr.addquery('manufacturer', primary);
8 // gr.query();
9 // actual_result = gr.getRowCount();
10 // if (actual_result > 100) scaled_result = 5;
11 // else scaled_result = 1;
```

**Metric form script field**

You must use the following variables in your script:

- **primary**: Input variable used to access the sys_id of the record being assessed.
- **actual_result**: Output variable that contains the actual value for this metric. The system uses this variable to populate the Actual value field on the Metric Result form. For each actual_result, you must specify a corresponding **scaled_result** value.
- **scaled_result**: Output variable that contains a numerical scaled value to represent an actual value. The system uses this variable to populate the Scaled value field on the Metric Result form. Ensure the scaled values you specify are between or equal to the Min and Max values for the metric. The Scale definition field determines how the system uses the scaled value. A scale definition of **Low** means smaller numbers are better, such as for a metric that measures the number of incidents for a vendor. **High** means larger numbers are better, such as for a metric that measures user satisfaction on a scale of one to five.

**Script example**

The metric Number of active devices uses the script pictured below. The primary variable is used to find CIs that are associated to the vendor record being assessed. The script retrieves the actual_result, the number of CIs associated to the vendor, then calculates the correct scaled_result. The script uses a series of scaled values, from the Min to the Max value, to represent actual values. Because the Scale definition is set to **High**, the greatest scaled values are best, meaning a vendor associated to the most CIs scores highest. The system stores the actual and scaled values in a metric result record for the vendor.
Scripted metric example

Data types for assessments
Metric data types have functions that depend on the method that you select.

### Assessment data types

<table>
<thead>
<tr>
<th>Data type</th>
<th>Compatible methods</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachment</td>
<td>Assessment</td>
<td>On questionnaires, users attach one or more files to a question.</td>
</tr>
<tr>
<td>Data type</td>
<td>Compatible methods</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Checkbox</td>
<td>Assessment</td>
<td>On questionnaires, users select a check box next to a statement or leave it cleared. Set the <strong>Scale definition</strong> field to <strong>High</strong> if a selected check box equates to a good score.</td>
</tr>
<tr>
<td>Choice</td>
<td>Assessment</td>
<td>On questionnaires, users select a value from a list of custom answer options. Create a metric definition for each answer option.</td>
</tr>
<tr>
<td>Date</td>
<td>Assessment</td>
<td>On questionnaires, users select a date.</td>
</tr>
<tr>
<td>Data type</td>
<td>Compatible methods</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Date/Time</td>
<td>Assessment</td>
<td>On questionnaires, users select a date and time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="https://via.placeholder.com/150" alt="Example of selecting date" /></td>
</tr>
<tr>
<td>Duration</td>
<td>Script</td>
<td>When the script runs, the system populates the <strong>Duration value</strong> and <strong>Scaled value</strong> fields on the Metric Result form with the appropriate values from the <code>actual_result</code> and <code>scaled_result</code> variables in the metric script.</td>
</tr>
<tr>
<td>Data type</td>
<td>Compatible methods</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Likert Scale</td>
<td>Assessment</td>
<td>On questionnaires, users select a value from a custom scale of answer options. Create a metric definition for each answer option, which is represented by a radio button on the scale. A Likert scale metric that evaluates an application's ease of use might have the metric definitions Easy, Average, and Difficult. If you want to reuse a series of answer options for multiple metrics, create a metric template and use the Template data type instead of the Likert Scale data type.</td>
</tr>
<tr>
<td>Number</td>
<td>Assessment, Script</td>
<td><strong>Assessment</strong>: On questionnaires, users enter a number. <strong>Script</strong>: When the script runs, the system populates the Actual value and Scaled value fields on the Metric Result form with the appropriate values from the actual_result and scaled_result variables in the metric script.</td>
</tr>
<tr>
<td>Data type</td>
<td>Compatible methods</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Percentage         | Assessment, Script | **Assessment** On questionnaires, users enter a number.  

Approximately what percent of the time are your incidents resolved in a week or less?  
%   

**Script** When the script runs, the system populates the *Actual value* and *Scaled value* fields on the Metric Result form with the appropriate values from the `actual_result` and `scaled_result` variables in the metric script.  

| String             | Assessment         | On questionnaires, users enter text. The size of the string field depends on the String option you select:  

Additional comments  

String single line wide data type  

Additional comments
### Data type | Compatible methods | Description
--- | --- | ---
Template | Assessment | On questionnaires, users select a value from a predefined series of answer options. There must be at least one template defined to use this data type. For a template, there is a template definition for each answer option, which is represented by a radio button.

<table>
<thead>
<tr>
<th>Data type</th>
<th>Compatible methods</th>
<th>Description</th>
</tr>
</thead>
</table>
| Yes/No | Assessment | On questionnaires, users select Yes or No from a list. Set the **Scale definition** field to **High** if selecting Yes equates to a better score.

**Assessment generation**

In the Assessments application, administrators or assessment administrators can trigger the system to generate scheduled assessments or on-demand assessments when all the prerequisite steps are completed.

An assessment administrator must publish the metric type to enable assessment generation.

The system performs these tasks when it generates assessments:

- Creates assessment questionnaires from non-scripted metrics and assigns the questionnaires to users. When users complete their assigned questionnaires, the system uses their responses to calculate assessment results.
- Runs scripted metrics from each category to query the database and calculate assessment results.

Each time the system generates assessments, it creates some or all of the following components. Consider having an administrator set a schedule for recurring data cleanup, as the system can potentially generate a considerable amount of assessment data.

- **Assessment group**
- **Assessment instances**
- **Assessment results**

**Assessment groups**

An assessment group is a container for assessment instances and assessment results generated in a single occurrence.
The system generates an assessment group every time the scheduled job runs or the API is called, when there is at least one assessable record associated to a category in the type. You can find assessment group records in Assessments > Assessments > Assessment Groups.

The Assessment Group form displays the group Number, the associated Metric type, and these related lists:

- **Assessment Instances**: Lists all assessment instances within this group. There may be no records in this related list. The system does not generate assessment instances if there are only scripted metrics for the type.
- **Metric Results**: Lists all metric results for this group. There may be no records in this related list initially. The system generates metric results immediately for scripted metrics, but not for non-scripted metrics, which appear as questions on assessments and require user response. The system dynamically updates the records in this list as users complete assessment questionnaires.
- **Assessment Category Results**: Lists all category results for this group. There may be no records in this related list initially. The system generates category results immediately if there are only scripted metrics in a category. Otherwise, the system does not calculate category results until a user completes an assessment questionnaire that contains questions from the category.

**Note**: To prevent the loss of important assessment data, you cannot delete an assessment group if it contains any assessment instances, metric results, or category results.

Create an assessment category

Assessment categories are used with assessment metric types and assessment metrics to generate bubble charts.

Role required: assessment_admin or admin

The Demand Management application comes with the Demand assessment metric type, five assessment metric categories, and assessment metrics. From the Assessment Categories section of the application menu, you can modify existing assessment categories and create ones.

1. Navigate to Demand > Settings > Assessments.
2. Click Create New to create a new record.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>Assesses demand size relative to the size of other demands.</td>
</tr>
<tr>
<td>Strategic Alignment</td>
<td>Assesses how closely the demand aligns with strategic goals of the organization compared to other demands.</td>
</tr>
<tr>
<td>Risk</td>
<td>Assesses demand risks compared to other demands.</td>
</tr>
<tr>
<td>ROI</td>
<td>Assesses demand return on investment compared to other demands.</td>
</tr>
<tr>
<td>Cost</td>
<td>Assesses demand cost compared to other demands.</td>
</tr>
</tbody>
</table>

**Assessment metric categories**

In the Assessments application, a metric category represents a theme for evaluating assessable records in a given metric type.
Each category has a numeric weight value to indicate its importance relative to other categories. Within a category, records called metrics are the traits or values used to evaluate assessable records. For example, there are many categories within the Vendor metric type, including Support Rating, which contains metrics that measure the quality of vendors’ customer support services. Assessable records must be associated to categories to be eligible for evaluation. Assessment administrators create categories and manage which assessable records each category is associated to.

Weight categories and metrics

When you create a metric category or metric, you must specify a weight, a numeric value that indicates the importance of the category or metric relative to other categories and metrics. The greater the weight value, the more important the item is. The system uses weight values in assessment result calculations. Consider these recommendations when choosing weight values.

- Determine a weighting scale and use it consistently. In general, use a scale with a small numeric range. A standard 1-10 scale is usually appropriate, where 1 is least and 10 most important. Understand that increasing the maximum value of a weighting scale impacts all related result calculations.
- Use the same weighting scale for metric categories and metrics. Though there is no limitation, consider using the same or very similar weighting scales for both categories and metrics to make it easier to remember which values to use. A scale of 1-10 is an effective and simple weighting system, but may not be suitable for all organizations.

Note: If you do not want to use weighting, set the same weight value for all categories and metrics. The default weight value is 10.

Create a category for assessable records

After you create a metric type and generate assessable records, create categories for the themes you are interested in using to evaluate the assessable records.

Role required: none

1. Navigate to Assessments > Metric Definition > Categories.
2. Click New to create a new metric category and then complete the Metric Category form:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the metric category. The name appears on assessment questionnaires.</td>
</tr>
<tr>
<td>Type</td>
<td>(Required) Metric type this category is used for. Metrics in this category are used to evaluate assessable records for the type you select. This field becomes read-only after you save the record.</td>
</tr>
<tr>
<td>Create stakeholders</td>
<td>Check box that enables (selected) or disables (cleared) automatic stakeholder creation for this category. When the check box is selected, the system makes all associated category users stakeholders for each assessable record associated to this category. This saves the time required to manually create stakeholders. For more information, see Create Stakeholders Automatically. Existing stakeholders are not impacted if you clear the check box.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Table</td>
<td>(Read-Only) Table that contains the records to evaluate with metrics in this category. The system automatically populates this field with the same table as the metric type selected. The table does not appear in the field until you save the form. This field is visible depending on whether a <strong>Type</strong> is selected.</td>
</tr>
<tr>
<td>Weight</td>
<td>(Required) Numerical value that represents the importance of this category relative to other categories. A greater value indicates greater importance. For more information, see <a href="weight_categories_and_metrics">weight categories and metrics</a>. The default value is 10.</td>
</tr>
<tr>
<td>Scoring type</td>
<td>Scoring method for an attestation category. This field appears only when the <strong>metric type</strong> is an attestation with a <strong>Scoring type</strong> of <strong>Percent</strong>. Use this field to configure different scoring types for specific attestation categories. Possible selections are:</td>
</tr>
<tr>
<td></td>
<td>· <strong>Percent</strong>: Attestation score as a weighted percentage of correct answers for scored questions.</td>
</tr>
<tr>
<td></td>
<td>· <strong>All or nothing</strong>: All answers for attestation type questions must be correct or the score is zero for the entire category.</td>
</tr>
<tr>
<td>Total metrics</td>
<td>(Read-Only) Number of metrics associated to this category.</td>
</tr>
<tr>
<td>Filter</td>
<td>Filter conditions that assessable records must meet to be evaluated using metrics in this category. The filter operates on fields on the selected table. If you specify a filter condition, the system automatically associates matching assessable records to the category when you save the record. If you change the filter conditions, the system removes and creates assessable record associations as needed. The system also deletes stakeholders for assessable records it disassociates. The system does not remove assessable record associations created by users, even if the assessable records do not match the filter conditions. This field is visible only when a <strong>Type</strong> is selected.</td>
</tr>
<tr>
<td>Description</td>
<td>Descriptive information about the category that appears on assessment questionnaires.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Roles                 | Only those users with the specified roles can perform the assessment for this category. If no role is specified, then users with any role can perform the assessment for this category.  
                        | **Note:** If the Roles property does not appear on the form, ask your admin to add the property.                                                                                                           |
| Details               | Text field containing an HTML editor. Use this field to present important details about this category to assessment recipients. Details can include formatted lists, images, videos, or links to external websites. You may need to configure the form to see this field. |
| Related Lists         |                                                                                                                                                                                                             |
| Assessment Metrics    | All metrics associated to this category. There must be at least one metric associated to the category to use any assessments with the category.                                                            |
| Assessable records    | All assessable records associated to this category. There must be at least one assessable record associated to the category to use any assessments with the category.  
                        | **Note:** This related list is hidden if the Evaluation method is Attestation.                                                                                                                               |
| Users                 | All users associated to this category. There must be at least one category user to create scheduled assessments using metrics in this category.  
                        | This related list is available only when the associated metric type has schedule type set to Scheduled. Category users are not a part of the on-demand assessment process. |

**Assessable record associations**

Only the assessable records associated to a category can be evaluated using metrics in that category. Manage which assessable records you evaluate for each category by creating and removing the associations.

Only the assessable records associated to a category can be evaluated using metrics in that category. Manage which assessable records you evaluate for each category by creating and removing the associations.

**Note:** You can also manage which categories an assessable record is associated to using the Assessable Record form.

**Manage an assessable record automatically**

You must define at least one filter condition in the Metric Category form to automatically associate assessable records with the category.
Role required: assessment_admin or admin

1. Navigate to **Assessments > Metric Definition > Categories**.
2. Open a category.
3. In the **Filter** field, create a condition statement that defines the records you want to associate to this category. The available fields are from the table defined for the metric type.

For example, for a category in the **Vendor** type, you might create the condition **(Country) (is) (Germany)**. Metrics in the category will be used only to evaluate vendors that meet this condition.

4. Save the record.

The system associates this category to all assessable records that match the filter condition. As the system generates new assessable records that match the condition, it associates them to this category. If you change the filter condition, the system removes and creates assessable record associations, as appropriate. Note the following:

- The system does not remove assessable record associations created manually, even if the assessable records do not match the filter conditions.
- The system deletes any related stakeholders, if applicable, when it disassociates assessable records from a category.
- The system does not create or remove assessable record associations if the related source records change. For example, consider the previous example in which all assessable records for vendors based in Germany were associated to a particular category. Assume that a user changes the **Country** of one of the vendor records from **Germany** to **Canada**. The system does not disassociate the related assessable record from the category, even though it no longer matches the filter condition.

---

**Note:** To configure the system to automatically associate all assessable records from a metric type to a category, use the same category condition as the metric type condition. For example, if the **Vendor** metric type has the condition **(Vendor) (is) (true)**, create the same condition for the category. If the metric type does not have a condition specified, you can use the category condition **(Sys ID) (is not empty)**, which includes all records from any table.

---

Manage an assessable record manually

You can manually create and remove assessable record associations for a category using a related list on the Metric Category form.

Role required: assessment_admin or admin

Keep in mind that when you disassociate an assessable record from a category, the system deletes any related stakeholders, if applicable, and you can no longer evaluate the assessable record using metrics in that category.

1. Navigate to **Assessments > Metric Definition > Categories**.
2. Open a category.
3. In the **Assessable records** related list, click **Edit** and use the slushbucket to add or remove one or more assessable records.

   Only assessable records associated to this category’s metric type are available for selection.

Delete a category

When you delete a category, the system also deletes the associated category users and stakeholders.

Role required: assessment_admin or admin

1. Navigate to **Assessments > Metric Definition > Categories**.
Alternatively, navigate to a record that contains a related list for categories.

2. Open a record from the list.
3. On the Metric Category form, click Delete.
4. Click OK when asked to confirm the action.

The system displays messages at the top of the form describing the actions taken.

**Assessment metrics**

In the Assessments application, a metric is a trait or value used to evaluate assessable records. Depending on the metric method, a metric can be used as either of the following:

- A question on assessment questionnaires, to obtain a subjective value such as how much people enjoy using each cell phone offered in the service catalog.
- A script that queries the database, to obtain an objective value such as the number of incidents related to each cell phone.

Each metric is associated to one `metric category` and can be used to evaluate assessable records for that category only. For example, the Support Rating category contains metrics that measure the quality of vendors’ customer support services. One metric addresses the quality of product documentation. Others address the strength of the user community, self-service options, online training, and other support services. Each metric has a numeric weight value to indicate its importance relative to other metrics in the same category.

Assessment administrators can create and administer metrics and `metric templates`, which define reusable sets of answer options for metrics used as assessment questions. If you decide to use metric templates, you may want to create them before you create metrics.

**Note:** Changes to assessment metrics and metric templates are reflected in assessment questionnaires and results, even if users have saved responses already. If possible, avoid changing the original meaning of a metric question, the data type, or any metric templates in use by existing assessments.

Create a metric for a category

After you create a category, create metrics you can use to evaluate the assessable records for that category.

Role required: assessment_admin or admin

When you create metrics, consider the focus of the category and what characteristics you want to measure for the items you will assess. If you plan to use metrics for assessment questionnaires, you may want to review tips for writing good questions.

1. Navigate in one of the following ways:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessments &gt; Metric Definition &gt; Categories</td>
<td>Open a category, and locate the Assessment Metrics related list.</td>
</tr>
<tr>
<td></td>
<td>This is the suggested navigation path, as the system links metrics to the category from which they are created.</td>
</tr>
<tr>
<td>Assessments &gt; Metric Definition &gt; Metrics</td>
<td></td>
</tr>
</tbody>
</table>

2. Click New.
3. Fill in the fields, as appropriate.
### Assessment Metric form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the metric.</td>
</tr>
<tr>
<td>Category</td>
<td>Metric category that the metric belongs to. The system automatically populates this category if you create a new metric from the Metric Category form.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>You cannot change the category if the Depends on field is set or if another metric depends on this metric.</td>
</tr>
<tr>
<td>Method</td>
<td>Determines how to use the metric.</td>
</tr>
<tr>
<td><strong>Assessment</strong>: Non-scripted metric. Make the metric available as a question on an assessment questionnaire. The Assessment method is compatible with all data types except Duration.</td>
<td></td>
</tr>
<tr>
<td><strong>Script</strong>: Scripted metric. Obtain values by writing a custom script. The Script method is compatible with the Duration, Number, and Percentage data types.</td>
<td></td>
</tr>
<tr>
<td><strong>Default answer from field</strong>: This option appears only if you have selected an Assessment Metric Type that contains a table. The General tab adds two fields:</td>
<td></td>
</tr>
<tr>
<td><strong>Default answer</strong>: Select the default answer for the question. The list comes from the selected table.</td>
<td></td>
</tr>
<tr>
<td><strong>Ask question</strong>: Specifies when to ask the question: always or only if the default answer is empty.</td>
<td></td>
</tr>
<tr>
<td><strong>Default answer from script</strong>: The General tab adds a field:</td>
<td></td>
</tr>
<tr>
<td><strong>Ask question</strong>: Specifies when to ask the question: always or only if the script does not contain a default answer. The script is defined on the Field Type tab.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong>: If you select a Data type that is incompatible with the selected Method, the system automatically changes the Method to the correct value.</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Weight</td>
<td>Numeric value that represents the importance of this metric relative to other metrics in the same category. By default, the weight is 10. For weighting suggestions, see <a href="#">weight categories and metrics</a>. This field is visible and required unless the <strong>Data type</strong> is <strong>Date</strong>, <strong>Date/Time</strong>, or <strong>String</strong>. These data types are not included in results calculations.</td>
</tr>
<tr>
<td>Order</td>
<td>Numeric value that determines the order of the metric question on assessment questionnaires, relative to other metric questions in the same category. The metric with the smallest order value appears as the first question in the category section. By default, the order is 100. For more information about questionnaire layout, see <a href="#">Complete Assessment Questionnaires</a>. Note: It does not matter which order value you use for metrics with the Script method, as they do not appear on questionnaires.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box that determines whether this metric is used to gather assessment results. If a non-scripted metric (Assessment method) is inactive, the question does not appear on assessment questionnaires generated after the metric becomes inactive. If a scripted metric (Script method) is inactive, the script does not run.</td>
</tr>
<tr>
<td>Mandatory</td>
<td>Check box that makes the metric question mandatory (selected) or optional (cleared) on assessment questionnaires. Users cannot submit questionnaires until they provide valid responses to all mandatory questions, which display a red <strong>field status indicator</strong>. This field is visible only if the <strong>Method</strong> is <strong>Assessment</strong>, the <strong>Depends on</strong> field is empty, and the data type is not <strong>Checkbox</strong>.</td>
</tr>
</tbody>
</table>
### Field

<table>
<thead>
<tr>
<th>Allow not applicable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check box that determines whether to include a <strong>Not Applicable</strong> answer option for this metric question on assessment questionnaires. Users can select <strong>Not Applicable</strong> if they do not have sufficient information to respond to a question or if a question does not apply to a particular assessable record. User responses of <strong>Not Applicable</strong> are excluded from results calculations. This field is visible only if the <strong>Method</strong> is <strong>Assessment</strong> and certain data types are selected.</td>
</tr>
</tbody>
</table>

### Additional fields you can add by customizing the form

<table>
<thead>
<tr>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text field containing an HTML editor. Use this field to present important details about this metric to assessment recipients. Details can include formatted lists, images, videos, or links to external websites.</td>
</tr>
</tbody>
</table>

### General Section
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Question</td>
<td>Text to use as the question on assessment questionnaires. Enter a clear, straightforward question that is easy to answer, such as <em>How likely are you to recommend this vendor for the purchase of office supplies?</em></td>
</tr>
<tr>
<td>Description</td>
<td>Information about the metric and what it evaluates. If the Method is Assessment, include details that help users understand how to answer the question. This text appears as a hint when a user points to the question text on the questionnaire.</td>
</tr>
<tr>
<td>Depends on</td>
<td>Setting used to make this metric a conditional question. Select an existing metric question from the list, which displays Checkbox, Choice, Likert Scale, Template, and Yes/No metrics of the same category as this metric. Then, use the Displayed when field to set the conditions that display this metric question on questionnaires. The system prevents the creation of recursive dependencies between metrics. For example, if Metric A depends on Metric B, Metric B cannot depend on Metric A. This field is visible only if the Method is Assessment.</td>
</tr>
<tr>
<td>Displayed when</td>
<td>Answer options for the selected Depends on metric question that, when chosen on questionnaires, display this metric question. This field is visible and required only if the Depends on field is set.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Data type</td>
<td>(Required) Format of the expected response data. The function of the data type depends on the selected Method. If the method is Assessment, the data type determines how users answer the corresponding question on questionnaires. If the method is Script, the data type determines how the system calculates assessment results. Note: If another metric depends on this metric, you cannot change the data type.</td>
</tr>
<tr>
<td>Randomize answers</td>
<td>Check box that determines whether to present the answer options for this metric question in a random order. The order of answer options can influence users, which creates biased results. Randomizing answer options can help prevent this bias. This field is visible only if a data type that requires metric definitions is selected. Note: Randomizing answer options for certain questions can make those questions confusing for the person answering. In general, only randomize answer options that do not follow a logical order. For example, the following question is confusing when randomization is enabled:</td>
</tr>
<tr>
<td>Template</td>
<td>Metric template to use for the metric question. A metric template is a set of predefined answer options. This field is visible and required only if the Data type is Template. Note: If another metric depends on this metric, you cannot change the template.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Dependent plugin</td>
<td>Plugin that contains the tables queried in the script. The system executes</td>
</tr>
<tr>
<td></td>
<td>the metric script only if the plugin is active. The default available</td>
</tr>
<tr>
<td></td>
<td>values are <strong>Asset Management</strong>, <strong>CMDB</strong>, <strong>Core</strong>, <strong>Cost Management</strong>,</td>
</tr>
<tr>
<td></td>
<td><strong>Procurement</strong>, and <strong>Software Asset Management</strong>. If the <strong>Method</strong> is</td>
</tr>
<tr>
<td></td>
<td><strong>Script</strong>, select a plugin.</td>
</tr>
<tr>
<td></td>
<td>This field is visible only if the <strong>Method</strong> is <strong>Script</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: An administrator may need to add more <strong>choices</strong> of plugins to the</td>
</tr>
<tr>
<td></td>
<td>field.</td>
</tr>
<tr>
<td>Scale definition</td>
<td>Setting that determines whether lesser or greater numerical values equate</td>
</tr>
<tr>
<td></td>
<td>to a good score in assessment result calculations. Select <strong>Low</strong> if lesser</td>
</tr>
<tr>
<td></td>
<td>numerical values are better, such as for a metric that measures the number</td>
</tr>
<tr>
<td></td>
<td>of incidents for a vendor. Select <strong>High</strong> if greater numerical values are</td>
</tr>
<tr>
<td></td>
<td>better, such as for a metric that measures user satisfaction on a scale of</td>
</tr>
<tr>
<td></td>
<td>one to five. The default value is <strong>High</strong>.</td>
</tr>
<tr>
<td></td>
<td>This field is visible and required unless the <strong>Data type</strong> is <strong>Date</strong>, **</td>
</tr>
<tr>
<td></td>
<td>Date/Time**, or <strong>String</strong>. The results for these data types are not included</td>
</tr>
<tr>
<td></td>
<td>in results calculations.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: For information about how to set the scale definition for data</td>
</tr>
<tr>
<td></td>
<td>types that do not require you to set a numerical value, see <strong>Data Types</strong>.</td>
</tr>
<tr>
<td>Min</td>
<td>Lowest numerical value to be used as an answer option on assessments or as a</td>
</tr>
<tr>
<td></td>
<td>scaled value in a scripted metric.</td>
</tr>
<tr>
<td></td>
<td>This field is visible and required only if certain data types are selected.</td>
</tr>
<tr>
<td></td>
<td>If the data type is <strong>Choice</strong> or <strong>Likert Scale</strong>, this field is read-only</td>
</tr>
<tr>
<td></td>
<td>and is set automatically based on the smallest metric definition <strong>Value</strong>.</td>
</tr>
<tr>
<td>Max</td>
<td>Highest numerical value to be used as an answer option or scaled value.</td>
</tr>
<tr>
<td></td>
<td>This field is visible and required only if certain data types are selected.</td>
</tr>
<tr>
<td></td>
<td>If the data type is <strong>Choice</strong> or <strong>Likert Scale</strong>, this field is read-only</td>
</tr>
<tr>
<td></td>
<td>and is set automatically based on the largest metric definition <strong>Value</strong>.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Script    | Script that obtains the desired system information.  
This field is visible and required only if the Method is Script.  
For more information about using this field, see Script methods. |

### Related List

| Assessment Metric Definitions | Lists all metric definitions, which appear as answer options for questions on assessment questionnaires. Click New to create a new metric definition.  
This related list is available only if the Data type is Choice or Likert Scale. |

4. **Save the record.**

When you create a **Choice** or **Likert Scale** question, reopen the Assessment Metric form after you submit it to create a metric definition. If you distribute a questionnaire without creating the answers for questions with these data types, recipients are unable to answer the questions. If the questions are mandatory, the recipients are unable to submit their questionnaires.

**Create a metric definition**

Metrics with Choice or Likert Scale data types must have metric definitions defined to represent answer options on questionnaires.

Role required: assessment_admin or admin

Each metric definition appears as one answer option for a question on an assessment questionnaire. For example, a metric for the question "How satisfied are you with the quality of this vendor?" has three metric definitions to create these answer options: **Very satisfied**, **Somewhat satisfied**, and **Not at all satisfied**.

1. **Open the metric record you want to edit.**
2. **In the Assessment Metric Definitions related list, click New to create a new metric definition.**
3. **Fill in the fields:**
   - **Display**: Enter the text you want to appear as the answer option.
   - **Value**: Enter the numeric value, greater than or equal to zero, to which the answer option equates. Values are used to calculate metric results. When you view assessment questions, metric definitions appear in order from least to greatest value.
     - **The system sets the minimum and maximum values according to the metric definition values.**
     - **To prevent reporting confusion, no two metric definitions for a given metric should have the same Value.**

4. **Click Submit.**

**Change the order of an answer**

By default, the order of answer options is established when a question is created with a data type of **Choice** or **Likert Scale**.

Role required: assessment_admin or admin
The system creates an Order value for each choice based on where it appears in the original list when you submit it. This order corresponds to the Value setting you give the answer. The choice with the lowest order number appears first, and the choice with the highest order number appears last. If you want to reconfigure the order of the answer options, you must do so by editing the Order field and not the Value field.

The Order column is hidden in the base system.

To edit these records, configure the Assessment Metric Definitions related list in the question record to show the Order column, and then edit the order number in the list. The Value setting remain the same for each answer option after reorganization.

Metric types and assessable records

In the Assessments application, assessment administrators create and administer metric types and assessable records.

A metric type defines a set of records an organization wants to evaluate, such as vendors, projects, or employees. For each type, the system generates unique assessable records that link the type to records that need to be evaluated, such as the individual records for the vendors Amazon and Intel. There may be multiple assessable records for the same source record if the source record meets the criteria for more than one type. For example, you might want to evaluate a record on the Company table, such as Intel, as a vendor and as a manufacturer, with different categories and metrics.

For configuration suggestions, see Assessment Administrator tasks.

Assessable records

An assessable record links a source record you want to evaluate, such as the company record for Amazon or the user record for a sales representative, to a metric type, such as vendors or employees.

You use assessments to evaluate the assessable record. The system generates assessable records from the source records that match the table and conditions set on the Assessment Metric Type form. You evaluate the assessable records with metric categories and metrics, which define traits and values to assess. For metric types with the On demand schedule type, you can generate on-demand assessments from the Assessable Record form. This method of assessment generation makes it easy to create and preview short questionnaires or to quickly obtain assessment results for specific assessable records.

You can set up an assessment description that includes information from multiple fields on an assessable record and is displayed on multiple lines. This provides the user who is taking the assessment with a more detailed and understandable description of the information being
requested on the assessment questionnaire. Create a multi-line description using table titles, which can be defined to use one or more fields from the selected table. See Define a new smartphone table title for more information.

Create metric types and generate assessable records
Each metric type sets a table and filter conditions that define a set of records to evaluate.

Role required: assessment_admin or admin

For example, the Vendor Performance application provides the Vendor metric type, which defines an assessable record for each source record in the Company (core_company) table that has the Vendor field selected. Create a metric type for each set of records you want to evaluate, such as vendors, users within an organization, or projects.

In addition to defining assessable records, metric types also determine how to filter decision matrix data and set the schedule type, which determines whether assessments are on-demand or scheduled.

1. Navigate to Assessments > Metric Definition > Types.
2. Click New.
3. Fill in the fields, as appropriate (see table).
4. When you are satisfied with the type settings, click Generate Assessable Records to save the record and create assessable records. The page redirects to the list of assessable records created.

You must click Generate Assessable Records to create the initial set of assessable records based on the table and conditions specified on the type record. After that, the system creates an assessable record each time a new matching record is created. Generate Assessable Records is located under Related Links.

Note: Clicking Generate Assessable Records can trigger the deletion of existing assessable records under certain circumstances. For more information, see Enforce a condition to delete an assessable record.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>(Required) Name of the type. It may be practical to give the type a name that indicates which records it defines.</td>
</tr>
<tr>
<td>Assessment duration</td>
<td>Amount of time assessors have to complete their assigned questionnaires, starting from the time the assessment is generated. The assessment duration sets the Due date that appears on assessment instances. Changes made to the duration of an attestation in the GRC Control Test Definition form are updated dynamically in this field. The default duration is 14 days.</td>
</tr>
<tr>
<td>Live feed</td>
<td>Check box that determines whether to enable (selected) or disable (cleared) the Live Feed view in scorecards for all assessable records created from this type.</td>
</tr>
<tr>
<td>Notify manager if overdue</td>
<td>Check box that determines whether to send (selected) email notifications a user's manager when that user fails to submit an assigned questionnaire on time.</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>
<tbody>
<tr>
<td>Assessment manager</td>
<td>Manager for this assessment metric type. These users are responsible only for managing the assessment process and not the results. The system notifies the assessment manager when an assessment for this metric type is past due.</td>
</tr>
<tr>
<td>Scoring type</td>
<td>Scoring method to use for questions with a data type of attestation. The possible selections are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Percent</strong>: Attestation score as a weighted percentage of correct answers for scored questions. When you select this scoring type, categories can be scored as <strong>Percent</strong> or <strong>All or nothing</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>All or nothing</strong>: Requires all answers for attestation type questions to be correct, or the score is zero for the entire attestation. When you select this scoring type, all categories are scored automatically as <strong>All or nothing</strong>.</td>
</tr>
<tr>
<td>Scale factor</td>
<td>(Required) Number to represent the best possible score for assessment results. All results for assessments of this type are scaled to this number. 10 is generally a good scale factor.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: This field becomes read-only when it contains a value and you save the metric type. Choose a scale factor you are satisfied with before you save the metric type.</td>
</tr>
</tbody>
</table>
### Field

Pagination setting for Service Portal view

Specify how the user will see pages on the desktop or tablet view in Service Portal.

- **Category**: Display each category on a separate page. The categories appear in the following order:
  - Each category appears in sequence on a separate page for the first assessable record
  - Then each category appears in sequence on a separate page for the next assessable record
  - and so on

- **Question**: Display each question on a separate page. Questions appear on separate pages for mobile devices regardless of this setting. Each question appears for each category as described for the **Category** setting.

- **None**: All items on a single page—no pagination

**Default**: Category

**Note**: This field appears only when Service Portal is installed.

### Roles

Additional user roles that can view the results and access records associated with this type. Users with the specified roles have read access to this type record as well as to associated categories, metrics, assessable records and scorecards, category users, stakeholders, and decision matrixes.

**Note**: Users with these roles do not have access to Assessments modules unless they are also assessment administrators. Users with these roles can navigate to the records by other means, such as from reference fields on assessment instances. This field provides the option to easily grant certain users access to specific assessment data in special cases. For example, the **Vendor** metric type provides access to users with the vendor_manager role so they can view results and compare assessable records when they open scorecards or decision matrixes in the Vendor Performance application.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature</td>
<td>(Optional) Acknowledgement by a survey recipient of requirements, admonitions, or expectations related to an assessment. For more information, see Create an assessment signature.</td>
</tr>
<tr>
<td>Return URL</td>
<td>Destination address of a web page that is presented to users after they submit an assessment for this metric type. When a return URL is configured, the end note content does not appear.</td>
</tr>
<tr>
<td>State</td>
<td>(Read-Only) Status of the assessment: Draft or Published.</td>
</tr>
<tr>
<td>Business rule</td>
<td>(Admin only) Business rule the system creates to monitor the specified table. When a new record is added to the table that meets the metric type conditions, the business rule generates a corresponding assessable record. If someone changes the table or conditions of the metric type, the system updates the business rule to reflect the changes. Existing assessable records associated with the metric type are not affected.</td>
</tr>
<tr>
<td>Schedule type</td>
<td>Setting that determines which assessment process to use. Select On demand or Scheduled.</td>
</tr>
<tr>
<td>Scheduled job</td>
<td>(Admin only) Scheduled job the system creates to generate assessments for this metric type. This field is populated the first time you save the record. The scheduled job name follows the format &lt;type name&gt; Assessment Creation. Administrators can configure a recurring assessment generation schedule for the metric type. This field is visible only when the schedule type is Scheduled.</td>
</tr>
</tbody>
</table>

**Note:** If you change the schedule type from Scheduled to On demand, the system deletes the scheduled job. If you change the schedule type back to Scheduled, the system creates a new scheduled job. The previous assessment generation schedule is not saved, but can be reconfigured if desired.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluation method</td>
<td>(Admin only) Indicates the evaluation method for this metric type. The system sets this field based on how the metric type is created. The possible evaluation methods are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Assessment</strong>: Default filter value for metric types. Only this evaluation method uses assessable records, conditions, and stakeholders.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Attestation</strong>: For details, see.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Survey</strong>: For details, see Survey definitions.</td>
</tr>
<tr>
<td>Scale factor</td>
<td>(Required) Number to represent the best possible score for assessment results. All results for assessments of this type are scaled to this number. 10 is generally a good scale factor.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: This field becomes read-only when it contains a value and you save the metric type. Choose a scale factor that you are satisfied with before you save the metric type.</td>
</tr>
<tr>
<td>Allow retake</td>
<td>Check box that allows users to modify their answers to a completed assessment, quiz, survey, or attestation. After the due date, the system removes the assessment from the user's My Assessments and Surveys page.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box that determines whether the metric type is active. When the metric type is inactive (cleared), assessment generation is disabled and users cannot take existing assessments.</td>
</tr>
<tr>
<td>Description</td>
<td>Helpful information about this type. Enter a clear description of the type and its purpose.</td>
</tr>
<tr>
<td>Introduction</td>
<td>Introductory content to display on assessment questionnaires. Consider adding a company logo, a welcome message, background information about the survey, or instructions. You may need to configure the form to see this field.</td>
</tr>
<tr>
<td>End note</td>
<td>Content to display on the screen that appears when someone submits an assessment questionnaire. Consider adding a thank you message, followup instructions, or other applicable information. You may need to configure the form to see this field. End notes are not displayed if a Return URL is specified.</td>
</tr>
<tr>
<td>Send notifications</td>
<td>Select the check box to send notifications for this assessment, survey, or attestation. You may need to configure the form to see this field.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Condition section</strong></td>
<td></td>
</tr>
<tr>
<td>Table</td>
<td>(Required) Table that contains the records you want to evaluate. The system creates assessable records for records on this table that meet the conditions you specify, if any. The number of matching records appears as a link by the <strong>Condition</strong> field. The link dynamically updates if you change the table selection. Click the link to open the list of matching records in a new tab or window. <strong>Note:</strong> Additional roles are required to view the records on certain tables. If you select a table that you do not have access to, a warning message appears by the <strong>Condition</strong> field where the number of matching records would be. You cannot generate assessable records for tables you do not have sufficient roles for.</td>
</tr>
<tr>
<td>Enforce condition</td>
<td>Check box that determines what happens to assessable records when you change the selected table or conditions.</td>
</tr>
<tr>
<td>Condition</td>
<td>Condition builder that defines specific records to assess from the selected table. If you do not specify any conditions, the system creates assessable records for all records on the selected table. Click the refresh icon to update the adjacent record count. <strong>Note:</strong> If you change the table or conditions, you must click Generate Assessable Records to create new assessable records.</td>
</tr>
<tr>
<td>Decision Matrix section</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Filter field  | (Required) Field on the selected table that can be used to filter results on decision matrixes and scorecards. For example, if the selected table is Company [core_company] and you choose Vendor type as the filter field:  
  - When you view decision matrixes for this type, the decision matrix menu to filter plotted items lists vendor types: Applications, Hardware, Services, and Software.  
  - On scorecards for this type, the Averages view displays ratings by vendor type.  |
<p>| Filter condition | Condition builder that defines which records from the table are available as choices on the filter menu. For example, if the filter field is Vendor type and you create the filter condition (Name) (does not contain) (Hardware), only records with vendor types of Applications, Services, and Software are possible choices as decision matrix filters. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default matrix filter</td>
<td>Record to use as the default filter choice on decision matrixes and scorecards. The selected <strong>Filter field</strong> and <strong>Filter condition</strong> control the available record choices. To see the records, if any, click the refresh icon next to the field. Consider the case that the filter field is <strong>Vendor type</strong> and you select <strong>Applications</strong> as the default matrix filter. The filter choice on decision matrixes for this type is set to <strong>Applications</strong> by default. If you change the value of the <strong>Table</strong> or <strong>Filter condition</strong> field, you must click the refresh icon to view the updated <strong>Default matrix filter</strong> choices. If you do not, the system selects the first available choice from the updated field choices when you save the record.</td>
</tr>
</tbody>
</table>

**Related Lists**

<table>
<thead>
<tr>
<th>Metric Categories</th>
<th>All metric categories associated with the type.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessable Records</td>
<td>All assessable records associated with the type. This related list is hidden in the Attestation view of this form.</td>
</tr>
</tbody>
</table>

**Note:** The **Generate Assessments** button is visible to administrators in certain cases for scheduled assessments. Do not click the button until after completing the prerequisite tasks.

---

Delete a metric type

Deleting a metric type entails deleting many related records.

Role required: assessment_admin or admin

You must delete some of these records manually before deleting the type, while the system deletes others automatically with the type.

1. Delete the records associated with the type to delete:
   - **Assessment results** (metric and category results)
   - **Assessment instance** (questions and assessment instances, in that order)
   - **Assessment groups**

2. Delete the type.
   A confirmation dialog box appears and alerts you that certain records associated with the type will also be deleted.

3. Click **OK** to delete the type and these related records:
   - Scheduled job for assessment generation
   - Business rule for assessable record generation
   - Assessable records
   - Metric categories
   - Category users
   - Stakeholders
   - Metrics
• Metric definitions
• Decision matrixes

Export an assessment
You can share assessments between ServiceNow instances by exporting an assessment and then importing the assessment on another instance.
Role required: assessment_admin or admin

Note: Update sets are available in the Helsinki release and should be used to move data from one instance to another. For information about update sets, see System update sets.

Note: The system exports a single XML file that does not contain result data.

The XML file contains a metric type [asmt_metric_type] and the following records that are associated with the type:
• Assessable records [asmt_assessable_record]
• Metric categories [asmt_metric_category]
• Metrics [asmt_metric]
• Metric definitions [asmt_metric_definition]
• Category users [asmt_m2m_category_user]
• Stakeholders [asmt_m2m_stakeholder]
• Decision matrixes [asmt_decision_matrix], [asmt_m2m_xcategory_matrix], and [asmt_m2m_ycategory_matrix]

1. Navigate to Assessments > Metric Definition > Types.
2. Right-click the record and select Export Assessment.
3. Save the XML file.

Import an assessment
Share assessments between ServiceNow instances by importing a previously exported assessment.
Role required: admin

Note: Update sets are available in the Helsinki release and should be used to move data from one instance to another. For information about update sets, see System update sets.

1. Ensure that the target instance has assessments enabled.
2. Follow the procedure detailed in Import a Record as XML Data.

Use update sets for surveys and assessments
Use an update set to capture changes to surveys and assessments.
Role required: admin or survey_admin

When developing surveys and assessments, you can use an update set to capture the changes and move them from a development instance to a production instance. Once an update set is created and marked current, all of the updates to the following tables are recorded in the update set.

The following tables are now update set enabled and also extend the application file:
• Assessment Metric Templates (asmt_template)
• Assessment Template Definitions (asmt_template_definition)
• Assessment Metric Definitions (asmt_metric_definition): survey question answer options
- Schedule (sys_trigger): scheduled jobs associated with the survey
- Assessment Metric Categories (asmt_metric_category): survey categories
- Assessment Metrics (asmt_metric): survey questions
- Assessment Category Users (asmt_m2m_category_user): survey users
- Trigger Conditions (asmt_condition)

Create an assessment signature

A signature on an assessment questionnaire contains assertions that can communicate directions, a legal statement, or any text that you want the recipient to consider.

Role required: assessment_admin or admin

You can require the recipient to select a check box or provide a full signature to acknowledge acceptance of the assertion before submitting the form. You can display assertions without requiring a signature. An assessment property called Require authentication for user signature allows you to require users to provide their user name and password when an assessment asks for a full name signature.

1. Navigate to Assessments > Metric Definition > Signatures.

   All signatures in the system appear in this list.

2. Click New.

3. Complete and submit the form using the fields in the table.

### Assessment signature fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Descriptive name for this signature</td>
</tr>
<tr>
<td>Signature type</td>
<td>Type of signature required. The selections are Checkbox, Full name, or Assertion only. If Assertion only is selected, no signature is required to submit the questionnaire. By default, the system requires user authentication for a full name entry.</td>
</tr>
<tr>
<td>Assertion</td>
<td>Text to present to recipients that requires acknowledgement.</td>
</tr>
</tbody>
</table>

### Assessable records

An assessable record links a source record you want to evaluate, such as the company record for Amazon or the user record for a sales representative, to a metric type, such as vendors or employees.

You use assessments to evaluate the assessable record. The system generates assessable records from the source records that match the table and conditions set on the Assessment Metric Type form. You evaluate the assessable records with metric categories and metrics, which define traits and values to assess. For metric types with the On demand schedule type, you can generate on-demand assessments from the Assessable Record form. This method of assessment generation makes it easy to create and preview short questionnaires or to quickly obtain assessment results for specific assessable records.

You can set up an assessment description that includes information from multiple fields on an assessable record and is displayed on multiple lines. This provides the user who is taking the assessment with a more detailed and understandable description of the information being requested on the assessment questionnaire. Create a multi-line description using table titles, which can be defined to use one or more fields from the selected table. See Define a new smartphone table title for more information.
View an assessable record
View the Assessable Record form to edit preferences and perform various actions.

Role required: assessment_admin or admin

1. Navigate to Assessments > Assessable Records.
2. Open a record from the list.
   By default, the list displays only assessable records with Active metric types.
3. On the Assessable Record form, edit fields and perform other actions as necessary (see table).

Viewing Assessable Records

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>(Read-Only) Assessable record name based on the display value of the source record. The name appears on assessment questionnaires.</td>
</tr>
<tr>
<td>Source</td>
<td>(Read-Only) Source record the assessable record is linked to. The Source reflects the table name and source record display value. For example, if the Name field is the display value for the Company table, the assessable record for a company record named Amazon has the Source value Company: Amazon.</td>
</tr>
<tr>
<td>Live feed</td>
<td>Check box that, when selected, creates a live feed group for the assessable record, which appears on the scorecard. If you clear the check box after a live feed group has been created, the system deletes the live feed group and all its messages.</td>
</tr>
<tr>
<td>Type</td>
<td>(Read-Only) Metric type from which the assessable record was generated.</td>
</tr>
<tr>
<td>Decision matrix</td>
<td>Check box that, when selected, enables this assessable record’s results data to appear on decision matrixes of the same metric type. Decision matrixes are graphs that plot the assessment results for multiple assessable records. If you clear the check box, the assessable record still appears on the default decision matrixes if you click the View Matrix related link on the assessable record’s scorecard.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Live feed group</td>
<td>(Read-Only) Live feed group for this assessable record. When you select the Live feed check box and save the record, the system populates this field.</td>
</tr>
</tbody>
</table>

**Related Links**

**View Scorecard**

Opens the scorecard for the assessable record.

**Related Lists**

**Category**

All metric categories associated with the assessable record. An assessable record must be associated to a category to be evaluated. Click **Edit** to add or remove category associations. Note that it is often more efficient to associate assessable records to categories using the Metric Category form.

**Category users**

All stakeholders who can take assessment questionnaires about this assessable record. Click **Edit** to create and delete stakeholders. For more information about this and other methods of creating stakeholders, see **Stakeholders**.

This related list is available only when the associated metric type has the **Scheduled** schedule type.

---

**Enforce a condition to delete an assessable record**

By default, the system does not delete assessable records, even if you change the table or conditions for the type and the existing assessable records no longer match.

**Role required:** assessment_admin or admin

The system can be configured so you can trigger the deletion of assessable records that do not match the type table and conditions.

1. On the Assessment Metric Type form, select the **Enforce condition** check box to enable deletion of existing assessable records of this type that do not match the table or conditions specified.

   When the check box is cleared, the system retains existing assessable records of this type, even if they do not match the table and conditions specified.

2. Click **Generate Assessable Records** to delete all assessable records associated with the type that do not match the current table and conditions.

   The system does not automatically delete assessable records, even if the **Enforce condition** check box is selected. You must click **Generate Assessable Records** with the check box selected every time you want the system to delete non-matching assessable records.

**Delete an assessable record**

When you delete an assessable record, the system deletes any stakeholders for the record.

**Role required:** assessment_admin or admin
Note: If a source record is deleted, the system deletes the associated assessable record. To delete the source record, you must first delete all associated metric results and category results.

Delete the assessable record:
- To delete a single record, open the record and click **Delete**.
- To delete multiple records, use the Assessable Records list.

Create a metric template

Create a metric template to define reusable rating scales for evaluating non-scripted metrics.

Role required: assessment_admin or admin

1. Navigate to **Assessments > Metric Definition > Templates**.
2. Click **New**.
3. Fill in the **Name** field on the Assessment Metric Template form.
4. To use images for template choices, such as for image scale questions, select **Allow Image**.
5. Click **Submit**.
6. Under the **Assessment Template Definitions** related list, click **New**.
   Create a template definition for each answer option you want to appear on an assessment question.
7. Fill in the following fields:
   - **Display**: Enter the text to appear as the answer option.
   - **Value**: Enter a numeric value, equal to or greater than zero, that you want the answer option to equate to. Values are used in results calculations.
   - **Selected Image**: Click to add the image to use for selected state.
   - **Unselected Image**: Click to add the image to use for unselected state.

When you view assessment questions that use templates, answer options appear in order from least to greatest Value.

**Tip**: To prevent reporting confusion, no two template definitions for a given template should have the same Value.

8. Click **Update**.

Metric templates

Metric templates define reusable rating scales for evaluating non-scripted metrics.

Each answer option on the scale is defined as a template definition, much like a metric definition. For example, the metric template named Satisfaction contains the template definitions: **Very Satisfied, Satisfied, Neutral, Dissatisfied**, and **Very Dissatisfied**.

Metric templates are available for metrics that have **Template** as the Data type. The following metric templates are available by default.

<table>
<thead>
<tr>
<th>Name</th>
<th>Assessment template definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Likert 5</td>
<td>Strongly Disagree, Disagree, Neutral, Agree, Strongly Agree</td>
</tr>
<tr>
<td>Satisfaction</td>
<td>Very Dissatisfied, Dissatisfied, Neutral, Satisfied, Very Satisfied</td>
</tr>
<tr>
<td>Name</td>
<td>Assessment template definition</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------------</td>
</tr>
<tr>
<td>Frequency</td>
<td>Never, Seldom, Sometimes, Most of the time, All of the time</td>
</tr>
<tr>
<td>Amount</td>
<td>None, Few or little, Average amount, Many, Quite a lot</td>
</tr>
<tr>
<td>Size</td>
<td>Very Small, Small, Average, Large, Very Large</td>
</tr>
<tr>
<td>Quality</td>
<td>Very Poor, Poor, Average, Good, Very Good</td>
</tr>
<tr>
<td>Complexity</td>
<td>Very Complex, Complex, Moderate, Simple, Very Simple</td>
</tr>
</tbody>
</table>

Update a metric minimum and maximum value to match a template

For assessment results to be properly calculated, the Min and Max values of a metric that uses a template must be equal to the smallest and largest template definition Value, respectively.

Role required: assessment_admin or admin

The system sets the Min and Max fields automatically when you create a metric of the Template data type, based on the template definition values. However, the system does not update these fields for existing metrics if you add a new template definition to a template or if you update the Value of an existing template definition. If the new Value is less than the minimum value of any metrics that use the template or greater than the maximum value, update the metrics accordingly.

To edit the minimum and maximum values for a question that has the Template data type:

1. Navigate to Assessments > Metric Definition > Metrics.
2. Configure the list to show the Min and Max columns.
3. Run the following list filter condition: [Template] [is] [<select the template you updated>]
4. Ensure the Min and Max values match the smallest and largest template definition Value for the selected template, respectively.
   If the values do not match, edit the Min and Max directly from the list.

    Note: When the data type is Template, a UI policy prevents the editing of Min and Max from the form.

Category users and stakeholders

Users who take assessments are individuals in your organization who have specific knowledge of the assessment categories and the records being assessed. A person who is qualified to answer assessment questions from metrics in a specific category becomes a category user when associated to that category. A category user then becomes a stakeholder when associated to a specific assessable record.

The system determines which assessable records and questions a user receives by looking at the metric categories and assessable records for which those users are stakeholders. Assessment administrators can create and manage category users and stakeholders.

Note: Category users and stakeholders are used only for scheduled assessments.
Category users

Category users are users who can potentially answer assessment questions about a particular metric category for scheduled assessments. Category users should have special knowledge of the categories and the metrics those categories contain. A category user becomes a stakeholder when associated to an assessable record. Create at least one category user for each category you want to use for assessment questionnaires. There is no need for category users if the category contains only scripted metrics.

Stakeholders

A stakeholder is a category user with specific product or service knowledge, who is associated to an assessable record. A stakeholder is familiar with the assessable record and all the metrics within a specific category. The same category user can be associated to multiple assessable records, in which case the system creates a stakeholder record for each association.

There are multiple ways to create stakeholders:

- Configure the system to create stakeholders automatically.
- Associate multiple category users to multiple assessable records.
- Associate multiple category users to one assessable record.
- Associate one category user to one assessable record.

Note: Ensure you establish the desired user and assessable record associations to categories before attempting to creating stakeholders.

Create a category user

Create category users by associating users in the system to metric categories.

Role required: assessment_admin or admin

When you create category users, choose users who are knowledgeable and can answer questions from that category. For example, a purchasing agent is a good category user for metrics that evaluate a vendor’s discount practices.

1. Navigate to Assessments > Metric Definitions > Categories.
2. Open a category record.
3. In the Users related list, click Edit.
4. Select the appropriate users for this category.

Note: The category must be associated to a metric type that has the Schedule type set to Scheduled.

Create stakeholders automatically

You can configure the system to create stakeholders automatically from all category users and assessable records associated with a category using the Create stakeholders check box on the Metric Category form.

Role required: assessment_admin or admin

If you associate a user to the category, the system makes the resulting category user a stakeholder for all the assessable records associated to the category. Similarly, if you associate a new assessable record to the category, the system makes all category users stakeholders for that record if they are not already stakeholders.

Note: Use the Create stakeholders check box with caution. You can end up with more stakeholders than you want and a large amount of unnecessary assessment data.
Automatic stakeholder creation is best suited to assessment implementations in which category users are knowledgeable about all or most of the assessable records associated to each category.

1. Navigate to Assessments > Metric Definition > Categories.
2. Select a category.
3. Associate category users and assessable records to the category.
4. Select the Create stakeholders check box.
5. Click Update.
   All the category users are associated to all the assessable records as stakeholders.
6. In the Assessable Records related list, click Edit.
7. Using the slushbucket, associate an assessable record to the category.

8. Click Save.
   The system makes all category users stakeholders for the new assessable record.
9. Delete stakeholders as needed.

Associate multiple category users to multiple assessable records
The stakeholder list helper in the create stakeholders module is the most efficient way to associate multiple category users to multiple assessable records in a single interface.

Role required: assessment_admin or admin

You can select category users from one category at a time.

Note: You cannot edit or delete stakeholders using the list helper.

1. Navigate to Assessments > Advanced > Create Stakeholders.
The stakeholder list helper appears.
2. Select a metric type from the list of available types.

   **Note:** Only metric types for scheduled assessments are available. On-demand assessments do not use category users or stakeholders.

3. Select a category from the list of available categories.

   **Note:** Only categories within the selected metric type are available.

   The system populates the **Category User** and **Assessable Records** lists with category users and assessable records associated to the selected category.

4. Select one or more category users from the **Category Users** list.
5. Select one or more assessable records from the **Assessable Records** list.
6. Click the **Associate** arrow between the lists to complete the association.

   A message above the list helper advises you that the selected category users are now stakeholders for the selected assessable records.

**Delete a stakeholder for multiple assessable records**

You can delete stakeholders for multiple assessable records.

Role required: assessment_admin or admin

1. Navigate to **Assessments > Advanced > Assessment Stakeholders**.
2. Sort the list by **Assessable Record** or **Category User** depending on the perspective you want.
3. Select the check box for each stakeholder you want to delete.
4. Select **Delete** in the **Actions** choice list.
5. Click **OK** to confirm the action.

   The system deletes the stakeholders.
Associate one category user to one assessable record
You can create a single stakeholder using the list in the Assessment Stakeholders module.

Role required: assessment_admin or admin

Associate any category user to any assessable record.

1. Navigate to Assessments > Advanced > Assessment Stakeholders.
2. Click New. On the Assessment Stakeholders form, fill in these fields:
   - Category user: Select a category user.
   - Assessable record: Select an assessable record.

3. Click Submit.
   The selected category user becomes a stakeholder for the selected assessable record. To verify the association, navigate to the assessable record and note that the selected category user is on the Category users related list.

   ![Assessment Stakeholders](image)

   **Note:** Do not create stakeholders from category users and assessable records of different metric types.

Associate multiple category users to one assessable record
You can create many stakeholders for a single assessable record from the Assessable Record form.

Role required: assessment_admin or admin

You can also edit or delete stakeholders from the form.

1. Navigate to Assessments > Assessable Records.
2. Open a record from the list.
3. In the Category users related list, click Edit.
   These category users are the stakeholders for this assessable record.
4. Use the slushbucket to edit the category users associated to this assessable record. Add category users to create stakeholders. Remove category users to delete stakeholders. The system only shows category users for categories associated to the assessable record. For example, if an assessable record is only associated to the Compliance Score and Support Rating categories, you do not see User Satisfaction category users.

Delete a stakeholder for one assessable record
You can delete stakeholders for one assessable record.

Role required: assessment_admin or admin

1. Navigate to **Assessments > Assessable Records**.
2. Open an assessable record.
3. In the **Category Users** related list, select the check box for each stakeholder you want to delete.
4. Select **Delete** in the **Actions** choice list.
5. Click **OK** to confirm the action. The system deletes the stakeholders.

### Generate an on-demand assessment

Use on-demand assessments to familiarize yourself with the basic assessment process and test your questionnaires using minimal configuration.

**Role required:** assessment_admin or admin

Select the **assessable records** to evaluate, create the categories and questions, and then assign an assessment to a user in the system. Pre-configured **stakeholders** are not used for on-demand assessments.

1. Create a **metric type** and set the **Schedule type** to **On demand** to allow for testing of your assessment configuration.
2. Generate the **assessable records** for the metric type you created.
3. Create the **metric category** required to evaluate the assessable records selected.
4. Create one or more assessment questions, or **metrics**, for each category.
5. **Publish the assessment**.
6. Perform an **on-demand assessment** to test your categories and metrics.
7. Analyze the assessment ratings in an **assessment scorecard** or **decision matrix**.

#### On-demand assessments

On-demand assessments can be generated for metric types with the Schedule type field set to **On demand**.

For the system to properly generate on-demand assessments, the metric type must be active and published. The metric type must also be associated to at least one metric category. That metric category must be associated to one or more of each of the following items:

- Assessable record
- Metric

By default, an assessment administrator can generate an on-demand assessment for one assessable record or **multiple assessable records**.

#### Generate an on-demand assessment for one assessable record

When you generate an on-demand assessment from the Assessable Record form, the resulting assessment contains questions from the categories associated to the assessable record.

**Role required:** assessment_admin or admin

1. Navigate to **Assessments > Assessable Records**.
2. Open an assessable record associated to a metric type that has the **On demand** schedule type.
3. On the Assessable Record form, click **Assign Assessment**.
The Select Assessor dialog box appears.

4. Select a user from the Recent Assessors list or select a different user.
5. Click **OK**.

The system generates an assessment instance assigned to the selected user.

*Generate an on-demand assessment for multiple assessable records*

When you generate an on-demand assessment from the Assessment Metric Type form, the resulting assessment contains questions from all categories associated to any assessable records for the metric type.

**Role required:** assessment_admin or admin

For example, if there are 15 assessable records associated to at least one category with assessment metrics, the assessment contains questions for all 15 assessable records.

1. Navigate to **Assessments > Metric Definition > Types**.
2. Open a metric type that has the **On demand** schedule type.
3. On the Assessment Metric Type form, click **Assign Assessment**.
   
   The Select Assessor dialog box appears.
   
   4. Select a user from the Recent Assessors list or select a different user.
   5. Click **OK**.

The system generates an assessment instance assigned to the selected user.

*Generate an assessment with the on-demand API*

The Assign Assessment buttons call an API to generate on-demand assessments.

**Role required:** assessment_admin or admin

1. To generate an assessment, call the from any script in the system, such as a business rule or client script.
2. Use the sys_ids of these items:
   - An assessable record to evaluate. The assessable record must be associated with an on-demand type and at least one category that contains non-scripted metrics.
   - One or more users who should perform the assessment. The API generates a questionnaire about the specified assessable record for each user.
Schedule an assessment

After you have evaluated your questionnaires using on-demand assessments, edit your categories and metrics as needed, reset your metric type record, and select the users who are qualified to evaluate the assessable records.

Role required: assessment_admin or admin

1. Open the metric type you created for the on-demand assessment and set the Schedule type to Scheduled.
2. Make sure the categories and metrics you created for the on-demand assessment are correct.
3. Create category users who have special knowledge of your categories.
4. Create stakeholders by associating category users to specific assessable records.
5. Set a schedule for automatic assessment generation or generate the assessment manually. This procedure must be done by a system administrator.
6. Configure email notifications to remind users of their assigned assessments and to report to managers when an employee misses an assessment deadline.
7. Analyze the assessment ratings in an assessment scorecard or decision matrix.

Schedule types

You can schedule assessments for preconfigured users or send them to any user on demand.

On-demand assessments require less setup. Scheduled assessments define users, or stakeholders, who have specific knowledge of the records being evaluated, and automatically send out assessment questionnaires to those users at scheduled intervals. The best practice is to configure an on-demand assessment first to familiarize yourself with the process and test your questionnaires. When you are satisfied with your categories and questions, reconfigure for a scheduled assessment. These configuration paths are the easiest for both assessment types. Refer to Key Terms for definitions of the terms used in these procedures.

Set an assessment generation schedule

You can set assessment generation schedules. You must set a schedule for each metric type individually.

Role required: assessment_admin or admin

1. Navigate to Assessments > Metric Definition > Types.
2. Open the appropriate metric type record.
3. Click the reference icon next to the Scheduled job field to open the Schedule Item record.
4. Locate the Trigger type field and set a recurring schedule for the scheduled job.

   For example, if you want to generate assessment components each month, select the Interval or Repeat trigger type and specify a Repeat value of 30 days. Alternatively, select Day in Month and specify a Run time and Run day of month.

   The optimal frequency of assessment generation is subjective. When you set the schedule, keep in mind the number of records to evaluate, how often your organization requires updated assessment results, the time and effort required of users to complete assessments, and other relevant factors.

Publish a metric type

Before it is possible to generate assessments, an assessment administrator must publish the associated metric type.

Role required: assessment_admin or admin
The **State** field on the Assessment Metric Type form indicates whether the type is published. The default state is **Draft**, which disables the system from generating assessments.

1. Navigate to **Assessments > Metric Definition > Types**.
2. Open a metric type record, and click **Publish**.

   The **Publish** button is available only if the state is **Draft** and there is at least one metric associated with the type.

   **Note:** A metric type cannot be moved back to the **Draft** state after it has been published.

---

**Scheduled assessments**

The system generates a unique scheduled job for each metric type with the **Schedule type** field set to **Scheduled**.

The system generates a unique scheduled job for each metric type with the **Schedule type** field set to **Scheduled**. Each scheduled job generates assessment components for the related metric type. By default, the scheduled job runs when an administrator executes it manually, but administrators can set a schedule to generate assessments automatically on a recurring basis.

For the system to properly generate scheduled assessments, the metric type must be active and **published**. The metric type must also be associated to at least one metric category. That metric category must be associated to one or more of each of the following items:

- **Assessable record**
- **Stakeholder** associated to one of the assessable records
- **Metric**

**Generate a scheduled assessment manually**

Administrators can generate scheduled assessments manually.

Role required: assessment_admin or admin

Use this option, for example, if you have set a schedule but want to generate assessments before the next scheduled run date.

1. Navigate to **Assessments > Metric Definition > Types**.
2. Open the appropriate metric type record.
3. Click **Generate Assessments** to trigger the scheduled job immediately.

   **Note:** Be careful to click **Generate Assessments**, not **Generate Assessable Records**.

---

**Generate a vendor type assessment manually**

The Vendor Performance feature provides a direct method of generating assessments for the Vendor metric type.

Role required: admin

1. Navigate to **Vendor Performance > Admin > Generate Assessments**.
2. Click **Generate Assessments** to execute the scheduled job for the **Vendor** type.

---

**Clean up assessment data**

The assessment process generates a considerable amount of data, some of which is not useful after a short time.

Role required: assessment_admin or admin

The assessment process generates a considerable amount of data, some of which is not useful after a short time. Assessments include a scheduled job called **Remove Old Assessment Data** that
is available to administrators only. The scheduled job removes these items if they are more than a year old:

- Assessment instance questions
- Assessment instances
- Metric results

By default, the scheduled job is executed manually. Administrators can configure the scheduled job to run automatically on a recurring schedule.

1. Navigate to **System Scheduler > Scheduled Jobs > Scheduled Jobs**.
2. Open the **Remove Old Assessment Data** record.
3. On the Schedule Item form, set the **Trigger type** field to run the scheduled job on a recurring schedule.

   It is recommended to set the scheduled job to run on a weekly or monthly basis.
4. Optional: Click **Execute Now** to run the scheduled job.

**Assessment instances**

An assessment instance represents one occurrence of a questionnaire assigned to one user.

The system generates assessment instances only when the required conditions are met, as described in **Scheduled assessments** and **On-demand assessments**, and there are non-scripted metrics in at least one category.

When the system generates scheduled assessments for a metric type, each assessment instance contains questions about assessable records and categories related to the stakeholder to which it is assigned.

**Example:**

Recall that there can be multiple stakeholder records associated with one user record. Minh Leclare is a stakeholder for these items related to the **Vendor** metric type:

<table>
<thead>
<tr>
<th>Assessable record</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon</td>
<td>User Satisfaction</td>
</tr>
<tr>
<td>Acme</td>
<td>User Satisfaction</td>
</tr>
<tr>
<td>Acme</td>
<td>Reliability</td>
</tr>
<tr>
<td>Cisco</td>
<td>Reliability</td>
</tr>
</tbody>
</table>

When the system generates a scheduled assessment, Minh is assigned one assessment instance. Minh must evaluate Amazon, Acme, and Cisco by answering questions from the categories for which she is a stakeholder. Assuming that there are three questions in the User Satisfaction category and six questions in Reliability, Minh's questionnaire contains three questions about Amazon, nine questions about Acme, and six questions about Cisco.

When the system generates an on-demand assessment **for a specific assessable record**, the assessment instance contains questions about that assessable record and all its associated categories. When the system generates an on-demand assessment **for a metric type**, the assessment instance contains questions about all that metric type's assessable records and their associated categories.

**View an assessment instance**

An assessment instance represents one occurrence of a questionnaire assigned to one user.
Role required: none

1. Navigate to Assessments > Assessments > Assessment Instances.
2. Click an assessment instance number to open the record.
3. View the record, which displays the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Auto-generated record number.</td>
</tr>
<tr>
<td>Metric type</td>
<td>Metric type of this assessment.</td>
</tr>
<tr>
<td>Assessment group</td>
<td>Assessment group to which this assessment belongs.</td>
</tr>
<tr>
<td>Due date</td>
<td>Date by which the assessment instance must be completed. The system populates the due date from the value in the metric type Assessment duration field. The system generates email notifications related to the due date.</td>
</tr>
<tr>
<td>State</td>
<td>State of the assessment. The possible states are Ready to take, In progress, Complete, and Canceled.</td>
</tr>
<tr>
<td>Assigned to</td>
<td>User this assessment is assigned to. This field becomes read-only when the state is In progress, Complete, or Canceled.</td>
</tr>
<tr>
<td>Signature</td>
<td>Name of the signature record attached to this assessment. A signature requires that assessment recipients acknowledge that they have read any assertions attached to a questionnaire.</td>
</tr>
<tr>
<td>Signature result</td>
<td>Verification provided by the recipient when a signature is required. This value is either the recipient’s full name from the User (sys_user) table or checked, indicating that the recipient acknowledged reading the assertion by selecting a check box.</td>
</tr>
</tbody>
</table>

4. Click Take assessment to open the questionnaire.

This button is available if all the following conditions are true for the assessment instance:

- It is Assigned to you.
- The State is Ready to take or In progress.
- The associated metric type is Active.

Configure trigger conditions for an assessment

Trigger conditions specify when to send a particular assessment and who to send the assessment to.
ServiceNow    Jakarta    Now Platform Capabilities

Role required: assessment_admin or admin

1. Navigate to **Assessments > Admin > Trigger Conditions.**
2. Complete the fields as described in the table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment</td>
<td>(Required) Metric type to generate assessment instances for. Triggered assessments only work if the metric type is set to the <strong>On demand</strong> schedule type.</td>
</tr>
<tr>
<td>Table</td>
<td>(Required) Table to run the trigger condition on. You can select only tables in the current application scope. The table must have a connection to the assessable records for the selected Assessment. For example, you might want to send a vendor assessment when incidents close that are related to vendors you assess. In this case, select the Incident (incident) table. After you select a table, ensure there is at least one option for the Assessable Record Field. If there is not, select a different table.</td>
</tr>
<tr>
<td>User field</td>
<td>(Required) Field that stores the users you want to send the assessment. You can select any field, on the selected Table or on a related table, that references the User (sys_user) table. Use the tree picker to select a field.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Repeat Interval</td>
<td>Minimum period that must pass before the trigger condition can resend the assessment to the same user. For example, assume the repeat interval is set to 30 days. Even if the same user is eligible for multiple assessments from this trigger condition, the system can only send the user one assessment every 30 days.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box that determines whether this trigger condition is active (selected).</td>
</tr>
<tr>
<td>Business rule</td>
<td>(Admin only) Business rule the system creates to monitor the selected table. When the condition is met, the business rule sends the assessment to the correct user. No configuration is necessary for this business rule.</td>
</tr>
<tr>
<td>Trigger randomly</td>
<td>Check box that determines whether to send the assessment to the appropriate user every time the condition is met (cleared) or only a percentage of the time (selected), as specified in the Probability (%) field.</td>
</tr>
<tr>
<td>Probability (%)</td>
<td>Probability out of 100 that the assessment will be sent each time the condition is met. For example, if the probability is set to 50, the system sends the assessment approximately 50% of the time the conditions are met, assuming there are no repeat interval restrictions. This field is visible and required only when the Trigger randomly check box is selected.</td>
</tr>
</tbody>
</table>
### ServiceNow Jakarta Now Platform Capabilities

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessable Record Field</td>
<td>(Required) Field on the selected Table that determines which assessable record will be the subject of the assessment. Only appropriate reference fields on the selected Table are available to select. If there are no Assessable Record Field options available, you must select a different Table. If the selected Assessment evaluates records on the Company [core_company] table and the selected Table is Incident, the only Assessable Record Field options are fields on the Incident table that reference the Company table. For example, Company or, if vendor ticketing is enabled, Vendor. If you select Vendor, the trigger condition sends an assessment about the Vendor for the incident, assuming there is an assessable record for the associated company. The assessment contains questions from all metric categories associated with the assessable record. <strong>Note:</strong> This field is not available if the selected Assessment is a metric type used for surveys. See <a href="#">Survey trigger conditions</a>.</td>
</tr>
<tr>
<td>Related Field 1 – Related Field 4</td>
<td>Field that contains a value you want to store for reporting purposes. You can pick any reference field on the selected Table. When the trigger condition generates an assessment instance, the system stores the value from the triggering record. Select up to four fields. For example, if you select the Incident table, you might select Caller and Vendor as related fields. That stores the caller and vendor associated with the incident as Related record 1 and Related record 2 in the assessment instance record. To view these fields, configure the Assessment Instance form.</td>
</tr>
<tr>
<td>Description</td>
<td>Summary information to identify the trigger condition.</td>
</tr>
<tr>
<td>Condition</td>
<td>(Required) Condition builder that defines the criteria that must be true to send the assessment. For example, if you want to send an assessment whenever an incident closes, create the condition (State) (is) (Closed).</td>
</tr>
</tbody>
</table>

---

**Assessment trigger conditions**

A trigger condition tells the system who to send a designated assessment to and when, based on specific conditions.
With trigger conditions, assessment administrators can configure the system to generate assessments each time a specific action occurs, such as when an incident or change request closes. The trigger condition sends the assessment to specified users who are related to the triggering record, such as incident callers or change request assignees. You can choose to send the assessment every time the condition is met, or set a probability for the system to send the assessment at random when the condition is met.

### Trigger condition configuration

<table>
<thead>
<tr>
<th>Assessment</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Incident [incident]</td>
</tr>
<tr>
<td>User field</td>
<td>Assigned to</td>
</tr>
<tr>
<td>Repeat Interval</td>
<td>30 days</td>
</tr>
<tr>
<td>Active</td>
<td>true</td>
</tr>
<tr>
<td>Trigger randomly</td>
<td>false</td>
</tr>
<tr>
<td>Assessable Record Field</td>
<td>Vendor</td>
</tr>
<tr>
<td>Related Field 1</td>
<td>Caller</td>
</tr>
<tr>
<td>Related Field 2</td>
<td>Vendor</td>
</tr>
<tr>
<td>Condition</td>
<td>(State) (is) (Closed) and (Vendor) (is not empty)</td>
</tr>
</tbody>
</table>

### Trigger condition example

Modesto Scroggie is the caller on an incident that is assigned to Boris Catino, a service desk technician. Boris contacts a vendor to resolve Modesto©s issue and sets the Vendor field to Microsoft. When the incident closes, the system creates an assessment instance assigned to Boris so he can evaluate Microsoft as a vendor.

Because two related fields were selected as part of the trigger condition, the assessment instance stores the following information from the incident:

- **Related record 1**: User: Modesto Scroggie
- **Related record 2**: Company: Microsoft

**Note**: Even though the trigger condition is set to be triggered every time the conditions are met, the Repeat interval setting ensures that Boris does not receive another assessment if another vendor incident assigned to him closes within 30 days of the first one.

### Enable manager notifications

Users with the assessment_admin role can enable the Notify manager assessment is overdue email notification.

Role required: assessment_admin or admin

This notification sends emails to assessors' managers when assessors do not complete their assigned assessments on time. For more information, see the table of assessment notifications. You must enable or disable this email notification separately for each metric type.

1. Navigate to Assessments > Metric Definition > Types.
2. Open a metric type.
3. Select the Notify if overdue check box.
To disable manager notifications, clear the check box.

4. Save the record.

**Note:** The assessor's user record must have a manager specified in the **Manager** field to use this notification. You might need to configure the form to use this field.

Assessment notifications

You can configure the system to send email notifications for assessments.

You can configure any of the following types of notification during the process of generating assessable records:

- **Notify assessment user:** This message notifies you of an assigned assessment and includes the **type**, the due date, and basic instructions. The message also contains a link to the record where you take the assessment.

  **Note:** If a user has a pending assessment, then the system will not generate another instance of the same assessment.

- **Remind assessment user:** This message reminds you of the due date if half the time passes and you have not completed the assessment. The message content is the same as the first notification.

- **Notify manager assessment is overdue:** If you do not complete an assessment by the due date, the system may send a notification to your manager, depending on configuration.

  **Note:** By default, the system runs a script every 30 days to cancel expired assessment and survey instances that are in the **Work in progress** or **Ready to take** states.

Assessment notification workflow

The system sends assessment notifications according to the Notify assessment user workflow. Users with the workflow_admin, workflow_creator, or workflow_publisher roles can view workflows.

1. To open the graphical workflow editor, navigate to **Workflow > Workflow Editor**.

2. In the activity menu, click the link to choose an existing workflow.
3. **Select Notify assessment user** from the Workflow Versions list.

   The workflow appears.
View a metric result

Metric results contain values that represent an evaluated record’s performance for a specific metric, based on a single evaluation from one user or from the execution of a script. Metric results contain actual values as well as calculated values. The system uses values from metric results to calculate category results.

Role required: assessment_admin or admin

If there is an active scripted metric when the assessment is generated, the system automatically produces a metric result for each associated assessable record. The system produces an additional metric result for each question a user answers on a completed assessment questionnaire. If multiple users complete questionnaires with the same questions on the same assessable records, the system produces metric results for each user’s responses. For example, three users complete questionnaires that contain the same four questions about the Acme Corporation record. The system produces 12 metric results: one per user for each question.

1. Navigate to Assessments > Results > Metric Results.
2. Open the metric result record you want to view.
All fields on the form except **Updated** and **String value** are read-only.

### Metric Result form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment group</td>
<td>Assessment group to which the metric result is associated.</td>
</tr>
<tr>
<td>Metric</td>
<td>Name of the metric to which these metric result values apply.</td>
</tr>
<tr>
<td>Data type</td>
<td>Data type of the metric.</td>
</tr>
<tr>
<td>Method</td>
<td>Method of the metric.</td>
</tr>
<tr>
<td>Updated</td>
<td>Date and time the metric result was last updated.</td>
</tr>
<tr>
<td>Source</td>
<td>Source record of the assessable record evaluated.</td>
</tr>
<tr>
<td>Assigned to</td>
<td>User who completed the assessment questionnaire. This field is blank when the method is <strong>Script</strong>.</td>
</tr>
<tr>
<td>Instance</td>
<td>Assessment instance completed by the <strong>Assigned to</strong> user. This field is blank when the method is <strong>Script</strong>.</td>
</tr>
<tr>
<td>Actual value</td>
<td>Unscaled value from a user response or script, depending on the method:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Assessment</strong>: Value obtained from the user response to the assessment instance question. The actual value is determined by the metric data type:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Checkbox</strong>: The actual value is 0 if the check box is cleared and 1 if it is selected.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Choice</strong> or <strong>Likert Scale</strong>: The actual value is equal to the Value of the metric definition associated with the chosen answer option.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Date</strong>, <strong>Date/Time</strong>, or <strong>String</strong>: The actual value is -1 to indicate that these data types do not contribute to category result calculations.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Template</strong>: The actual value is equal to the Value of the <strong>template definition</strong> associated with the chosen answer option.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Yes/No</strong>: The actual value is 0 if the response is <strong>No</strong> and 1 if it is <strong>Yes</strong>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Script</strong>: Value the script placed in the <strong>actual_result</strong> variable.</td>
</tr>
</tbody>
</table>

This field is hidden and left blank when the data type is **Duration**.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration value</td>
<td>Specific kind of actual value that is only applicable if the data type is Duration. The duration value is the value obtained by the script query from the actual_result parameter, such as the average duration of outages for a vendor.</td>
</tr>
<tr>
<td>Scaled value</td>
<td>Appropriate value from the scaled_result variable in the associated metric script. The code in a scripted metric defines a scaling scheme for the actual values it obtains. For example, a scripted metric queries the CMDB to return the number of configuration items (CIs) for a vendor. The code includes this scaling scheme, where actual_result is the number of CIs, and scaled_result is a representation of the quantity of CIs:</td>
</tr>
</tbody>
</table>
|               | if (actual_result < 1)  
scaled_result = 0;  
else if (actual_result < 1000)  
scaled_result = 1;  
else if (actual_result < 10000)  
scaled_result = 2;  
else if (actual_result < 25000)  
scaled_result = 3;  
else if (actual_result < 100000)  
scaled_result = 4;  
else  
scaled_result = 5;                                                                                                                                  |
<p>|               | If the script detects 315 CIs for the vendor, the Actual value is 315 and the Scaled value is 1 for this metric result.                                                                                                                                                                                                                      |
|               | <strong>Note:</strong> Although this field is visible only when the method is Script, the system populates the field with the Actual value when the method is Assessment, as the scaled value is used in the Normalized value calculation.                                                                                                                                         |
| Normalized value| Adjusted value that accounts for weights, scale definition, minimum and maximum values, and other factors that impact the metric (like the survey responses or the input value—the actual value given by the user). See the example for Normalized value in View an assessment category result.                                                                                                                   |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String value</td>
<td>Value that displays the response as it appears on a questionnaire. In some cases this is the same as the Actual value, such as when the metric data type is Percentage. The string value is N/A for unanswered questions of certain data types. For the Attachment data type, the names of the attached files are displayed as comma-separated values.</td>
</tr>
</tbody>
</table>

**Assessment results**

In the Assessments application, when the system processes completed questionnaires or gathers values returned from scripted metric queries, it generates assessment result records called metric and category results.

Assessment administrators can view assessment results.

The system calculates metric results first, normalizes the scores, and then calculates category results. Each metric and category result record stores data from one assessment group, for a particular category and source record evaluated. Specifically:

- Metric results: store data calculated from one evaluation of one metric.
- Category results: store data calculated from a weighted average of all metrics in the category.

**Note:** Although results data is available to view in the form of metric and category result records, the most meaningful way to view results is in scorecards and decision matrixes. These tools display only the most pertinent data in graphical, comparative formats.

**Excluded Responses**

The system creates metric results for responses but does not include them in category result calculations if any of the following are true:

- The user selects the Not Applicable answer option on a questionnaire.
- The user does not answer the question and the data type is not Checkbox.
- The question data type is one of the following: Date, Date/Time, or String.
- The metric result Actual value, Scaled value, and Normalized value fields are set to -1.

**Metric Attachments**

After a survey or assessment is submitted, any attachments that have been added by a user are moved to the metric result record. The names of the attached files are added to the String value field on the Metric Result form.

**Note:** You cannot add or remove attachments from a metric result.

**Assessments overview module**

The assessment overview module is a type of homepage that displays various assessment reports, such as results by category and assessments by state.
Prerequisites

You can view the overview page and refresh, add, delete, and rearrange report widgets.
Role required: assessment_admin
To use the Assessments Overview module, navigate to **Assessments > Overview** and click elements within the reports to obtain more information.

The available reports are:

Assessments overview module reports descriptions

<table>
<thead>
<tr>
<th>Report</th>
<th>Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assesable Records by Type</td>
<td>Assessable Record</td>
</tr>
<tr>
<td>Assessment Instances by Assessment Group</td>
<td>Assessment Instance</td>
</tr>
<tr>
<td>Assessments by State</td>
<td>Assessment Instance</td>
</tr>
<tr>
<td>Answered Questions by Assigned User</td>
<td>Assessment Instance Question</td>
</tr>
<tr>
<td>Average Rating by Type</td>
<td>Assessment Category Result</td>
</tr>
<tr>
<td>Category Result Ratings by Category</td>
<td>Assessment Category Result</td>
</tr>
<tr>
<td>Metrics by Data Type</td>
<td>Assessment Metric</td>
</tr>
<tr>
<td>Stakeholders per Category</td>
<td>Assessment Stakeholders</td>
</tr>
<tr>
<td>Top Rated Items</td>
<td>Metric Result</td>
</tr>
<tr>
<td>Total Metrics by Metric Type</td>
<td>Assessment Metric</td>
</tr>
<tr>
<td>Unanswered Questions by Assigned User</td>
<td>Assessment Instance Question</td>
</tr>
</tbody>
</table>

**Assessment results calculation**

For every assessment group, there are assessment results.

Data calculated from an evaluation of one metric is classified as a metric result. Data calculated from the weighted average of all metric results in a category is classified as a category result. The system calculates some assessment results when the assessment is generated, and others when users complete questionnaires.

**View a bubble chart for assessments**

Assessment administrators can view bubble charts to compare the relative standing of assessable records in three metric categories.

Role required: assessment_admin or admin

1. Navigate to **Assessments > Admin > Bubble Charts**.
2. Click a **Name** to open the bubble chart record.
3. Under **Related Links**, click **View Bubble Chart**.

---

**Note:** Demand managers and vendor managers can view bubble charts through the Demand Management and Vendor Performance applications. See **Project Portfolio Suite** for more information.

**Bubble charts for assessments**

A bubble chart is a dynamically updated graph that plots assessment results for multiple assessable records.

Assessment administrators can create and use bubble charts to compare the relative standing of assessable records in three metric categories. The X- and Y-axes each represent a different category. Assessable records are plotted on the chart as circular markers, or bubbles, which vary in size according to scores for the third category.

Create a bubble chart
Assessment administrators can create bubble charts to compare the relative standing of assessable records in three metric categories.

To create a bubble chart, navigate to **Assessments > Admin > Bubble Charts** and create a record (see table for field descriptions).

**Note:** For color fields, either HTML color names or hexadecimal (hex) values are acceptable. For hex values, the # character is optional. Values are not case-sensitive. For example, all of the following values are valid: LightGray, lightgray, #D3D3D3, d3d3d3.
## Bubble Chart form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Descriptive name for the bubble chart. Bubble Chart is appended to the name when you view the bubble chart.</td>
</tr>
<tr>
<td></td>
<td><strong>Top left label</strong>&lt;br&gt;<strong>Top right label</strong>&lt;br&gt;<strong>Bottom left label</strong>&lt;br&gt;<strong>Bottom right label</strong>&lt;br&gt;Label text for the top left, top right, bottom left, and bottom right quadrants, respectively. Choose labels that help interpret results. For example, a bubble chart that displays vendor assessment results might have the following quadrant labels, where vendors in the top right quadrant have the best scores:&lt;br&gt;- <strong>Top left label</strong>: Resource&lt;br&gt;- <strong>Top right label</strong>: Essential Partner&lt;br&gt;- <strong>Bottom left label</strong>: Poor Performer&lt;br&gt;- <strong>Bottom right label</strong>: Reevaluate</td>
</tr>
<tr>
<td>Top left color</td>
<td>Border colors for the top left, top right, bottom left, and bottom right quadrants, respectively. Bubbles are the color of the quadrant they are in.</td>
</tr>
<tr>
<td></td>
<td><strong>Top left color</strong>&lt;br&gt;<strong>Top right color</strong>&lt;br&gt;<strong>Bottom left color</strong>&lt;br&gt;<strong>Bottom right color</strong>&lt;br BORDER colors for the top left, top right, bottom left, and bottom right quadrants, respectively. Bubbles are the color of the quadrant they are in.</td>
</tr>
<tr>
<td>Type</td>
<td>Metric type associated with this bubble chart. Only results for assessable records of the selected metric type are plotted on the bubble chart.</td>
</tr>
<tr>
<td></td>
<td><strong>X-Axis label</strong>&lt;br&gt;<strong>Y-Axis label</strong>&lt;br&gt;<strong>Z-Axis label</strong>&lt;br&gt;Label text for the X-, Y-, and Z-axis categories of the bubble chart. These labels appear along the X- and Y-axes, if applicable, and in bubble score summary windows. The metric category name is usually a good label. If these fields are left empty, the bubble chart automatically displays the selected category names as the labels.</td>
</tr>
<tr>
<td>Metric X category</td>
<td>Metric category each axis represents. Results for the Z-axis category determine the size of each bubble. The Z-axis should generally represent the most important category out of the three.</td>
</tr>
<tr>
<td>Metric Y category</td>
<td></td>
</tr>
<tr>
<td>Metric Z category</td>
<td></td>
</tr>
<tr>
<td>Quadrant label color</td>
<td>Color of the label text for the quadrant borders.</td>
</tr>
<tr>
<td>Default</td>
<td>Check box that enables (selected) or disables (cleared) the bubble chart as the default. There can be only one default bubble chart per metric type.</td>
</tr>
</tbody>
</table>

### Bubble chart components

The X- and Y-axes each represent a different metric category. Assessable records are plotted on the chart as circular markers, or bubbles, which vary in size according to scores for the third category.

The bubble chart page has these components:

- **Bubble Chart**
- **X- and Y-axes**: Each axis represents a metric category.
• **Bubbles**: Each labeled bubble represents an average of category result data for an assessable record. Point to a bubble to view an assessable record score summary. Click a bubble or bubble label to view the scorecard for the assessable record.

• **Source record list**: List of all records defined by the **Table** and **Condition** fields for the associated **metric type**. Note that the bubble chart only plots records for which there are assessment results. The assessment results are actually associated with the assessable records for each of the listed source records.
Assessable record score summaries
Point to a bubble to display a score summary for the assessable record the bubble represents.
The summary displays the assessable record’s average score for each category in the following order: X-axis category, Y-axis category, Z-axis category. The scores are based on data from the last 12 months.

View an assessment scorecard
The Assessments application prepares printable scorecards. A scorecard displays easy-to-interpret assessment results, in which the current calculated ratings for an assessable record are compared to previous ratings or to the ratings of other records.
Role required: assessment_admin or admin
Users can examine ratings over time, compare ratings for one assessable record with all assessable records in a table, or compare the ratings of two assessable records. All ratings are averages for the time range selected. The system dynamically updates a scorecard each time you view it, so the ratings reflect recently completed assessments and scripted metrics.
Administrators can display a scorecard for any table by creating a Related Link on assessable records. The system provides this link on the Company form by default when Vendor Performance is active.
The Vendor Performance application provides an enhanced scorecard view for vendors.
See Vendor Performance in Project Portfolio Suite.
1. Navigate to Assessments > Assessable Records.
2. Open a record.

Create a link to a scorecard
Users with the admin role can create UI actions that allow users to view scorecards from tables.
Role required: assessment_admin or admin

1. Generate **assessable records** you want to evaluate.
   For example, you might create a metric type called **Project** to assess project management records.

2. Navigate to **System Definition > UI Actions**.

3. Open the View Scorecard record.

4. Right-click the header bar and select **Insert and Stay** from the context menu to create a duplicate record.

5. Change the **Table** name to the table on which you want the UI action to appear.
   For example, you might select Project (pm_project).

6. Do not edit the **Action name** field or the **Condition** script.

7. Save the record.

8. Navigate to the table on which you created the UI action and open an assessable record.
   a) In this example, navigate to **Project > Projects > All**.
   b) Open any record in the list.
   c) Click **View Scorecard** under **Related Links** to open the scorecard for that assessable record.
The scorecard appears with the title in the form of `<table display name> Scorecard`. For example, a scorecard for an assessable record in the Project `pm_project` table is named `Project Scorecard`.

**Note:** Content does not appear in the scorecard unless the associated assessable record has assessment results or related live feed conversations.

9. Insert a new View Scorecard UI action record for each table where you want the related link to appear.

**Export a scorecard as an image**
You can export scorecards as images.

Role required: assessment_admin or admin

1. Click the menu icon and select Save as PNG or Save as JPEG as the download format.
2. When the export is complete, select Download to save the scorecard image to a storage location.

---

**Assessment scorecard averages**
The Averages view compares the current ratings for an assessable record in each metric category with the average, minimum, and maximum values from all assessable records in the filter. All ratings are from assessments generated over the trailing twelve months (TTM).

---

© 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.
Select a filter option to compare the current record against all assessable records in that filter. An assessment administrator configures these options in the **Filter field** field in the Assessment Metric Type form.

Rating variances are highlighted as follows:
- **Red**: Ratings are below average in this category. The **Diff** value displays a negative number.
- **Green**: Ratings are above average in this category. The **Diff** value displays a positive number.
- **White**: Ratings are average in this category. The **Diff** value is 0.0.

In the following example, the ratings of the current group are compared against other groups for which Don Goodliffe is the manager.

![Group scorecard with ratings filter](image)

**Group scorecard with ratings filter**

**Assessment scorecard categories**
The Categories view displays a bar chart showing the average ratings for each category in the selected time interval.

Select from these reporting periods:
- All History
- Last 3 Months
- Last 12 Months
Scorecard categories

Assessment scorecard category metrics
The Category Metrics view displays the weighted average results for each metric within a category. Use this view to learn how individual metrics affect the overall rating for the category.

Select a metric category from the choice list to display the chart.
Scorecard category metrics

Assessment scorecard head-to-head compare view
The Head to Head Compare view allows you to compare the ratings of two assessable records of the same type. Select an assessable record from the choice list to compare against the current record’s trailing twelve month (TTM) ratings.

Head to head compare

The Diff column displays the difference between each assessable record’s most recent TTM ratings. By default, the system selects the first assessable record in the list when you open this view. The scorecard displays three years of ratings for the comparison record. All ratings are expressed as averages.
Scorecard head to head compare

Overall Rating
The Overall Rating is calculated as:

\[
\frac{\text{sum of normalized values in category result}}{\text{(number of assessment groups)}}
\]

In the following example, the calculation is

\[
\frac{2.13 + 2.86 + 3.79 + 1.43 + 2.39 + 3.7}{2} = 8.15
\]
### ServiceNow Jakarta Now Platform Capabilities

**Normalized values**

<table>
<thead>
<tr>
<th>Assessment group</th>
<th>Category</th>
<th>Weight</th>
<th>Source</th>
<th>Rating</th>
<th>Normalized value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASG0010010</td>
<td>Politeness</td>
<td>5</td>
<td>Group: NY DB</td>
<td>9.37</td>
<td>2.13</td>
</tr>
<tr>
<td>ASG0010010</td>
<td>Recommendation</td>
<td>7</td>
<td>Group: NY DB</td>
<td>9</td>
<td>2.86</td>
</tr>
<tr>
<td>ASG0010010</td>
<td>Responsiveness</td>
<td>10</td>
<td>Group: NY DB</td>
<td>8.34</td>
<td>3.79</td>
</tr>
<tr>
<td>ASG0000804</td>
<td>Politeness</td>
<td>5</td>
<td>Group: NY DB</td>
<td>6.29</td>
<td>1.43</td>
</tr>
<tr>
<td>ASG0000804</td>
<td>Recommendation</td>
<td>7</td>
<td>Group: NY DB</td>
<td>7.5</td>
<td>2.39</td>
</tr>
<tr>
<td>ASG0000804</td>
<td>Responsiveness</td>
<td>10</td>
<td>Group: NY DB</td>
<td>8.14</td>
<td>3.7</td>
</tr>
</tbody>
</table>
### Group Scorecard

<table>
<thead>
<tr>
<th>Category</th>
<th>Current</th>
<th>Diff</th>
<th>2014</th>
<th>2013</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overall Rating</strong></td>
<td>8.15</td>
<td>3.63</td>
<td>4.52</td>
<td>6.48</td>
<td>9.11</td>
</tr>
<tr>
<td><strong>Politeness</strong></td>
<td>7.83</td>
<td>3.68</td>
<td>4.15</td>
<td>5.57</td>
<td>8.86</td>
</tr>
<tr>
<td><strong>Recommendation</strong></td>
<td>8.25</td>
<td>5.00</td>
<td>3.25</td>
<td>6.00</td>
<td>9.25</td>
</tr>
<tr>
<td><strong>Responsiveness</strong></td>
<td>8.24</td>
<td>2.63</td>
<td>5.61</td>
<td>7.25</td>
<td>9.16</td>
</tr>
</tbody>
</table>

#### Overall Rating on the Group Scorecard

*Assessment scorecard history*

The History view compares the current ratings for each category with ratings from the previous three years or four quarters.

Ratings that have declined are highlighted in red and display negative numbers. Ratings that have improved are highlighted in green with positive numbers. Arrow icons beside the values in the **Diff** column indicate the trend of the current assessment against the previous assessment.

- **3 Years**: To calculate the current ratings, the system averages the ratings from the trailing twelve month (TTM) period. The **Diff** column shows the discrepancy between the current ratings and the previous calendar year's ratings.
Scorecard history - 3 years

- **4 Quarters**: Quarterly assessments compare the average rating for each category in the current quarter against the average ratings from the previous four quarters. The *Diff* column shows the discrepancy between the current ratings and the previous quarter's ratings. The column labels count backward, by quarter from the current quarter. For example, if the current quarter is the 3rd quarter of 2013, then the previous quarters appear as 2nd (2013), 1st (2013), 4th (2012), and 3rd (2012). All four of the previous quarters appear, whether or not there was any data for those quarters.

---

Scorecard history - 4 quarters

*Live feed view of assessable records*

The live feed view displays live feed conversations that apply to the assessable record. Users can view the group feed, including tagged comments, and add comments of their own.
To configure a live feed view, an assessment administrator selects the Live feed check box on the Assessable Record form. Live feed is available on the scorecard even if there are no category results for the other views.

The live feed view provides these viewing options:

- **My Feed**: Displays the user's My Feed preferences.
- **Company**: Displays the user's company feed.
- **Groups**: Displays all available groups and gives the logged in user the option to leave or join a group. Select a group to display that group's conversations.
- **Tags**: Displays all the tags found in live feed comments. Click a tag to display the conversations containing that tag.
Group Scorecard

CAB Approval -
Conversation for assessable record ‘CAB Approval’

Messages Members Pending members Hashtags

Share your thoughts

System Administrator
2m ago

Has anyone had problems getting hardware this past month? I had a Linux server approved but still haven’t gotten it.

Like · Copy Link

ITIL User
Yes, my network has not even been ordered yet. When I asked procurement about it they made some excuse that they cannot get anything until they get ok from CFO.

1m ago · Like · Reply
Assessment scorecard ratings

The scorecard ratings section displays various ratings for the assessable record.

Select one of several views that present different ratings:

- Averages
- Categories
- Category Metrics
- Head to Head Compare
- History
- Live Feed

Some views display an overall rating column, which lists categories used to evaluate the assessable record. Only categories in which the assessable record has been evaluated appear on the scorecard. If the ratings section does not display any data, the assessable record or category results associated to the assessable record have been deleted.

Click a category to view the category record. Point to a category to display a line chart that shows the rating trend for that category.

![Vendor scorecard trend chart](image)

Set up and administer quizzes

Set up and administer quizzes.

Role required: assessment_admin or admin

1. Optional: Create reusable question templates for quizzes.
2. Create the quiz using the Quiz Designer or with forms accessed from the navigation menu.
   - The quiz record includes specifics such as duration, notification preferences, a questionnaire introduction, and ending notes displayed to recipients.
3. Edit the default category or create additional categories as needed.
   - The system creates a category with the same name as the quiz.
4. Define users for each category.
   - These are the recipients who answer the questions in a category. You can define different users for each category.
5. Create the questions for each category.
6. Create the answers for each question and determine if the questions are scored.
   You can create unique answers or select preconfigured answers from a template.

Publish and distribute the quiz. You can send the quiz to a single user or all users in each category. Review the results from the submitted quizzes in reports and scorecards.

Quizzes
Quizzes are questionnaires you can assign to one or more users to assess their knowledge of any subject. The quiz functionality is built on the assessment engine and provides many of the same features as assessments and surveys.

Each question is scored, and the overall score indicates the percentage of questions the user answered correctly. A quiz may have categories of questions that are assigned only to some users. You can assign weighting values to individual questions or categories of questions that make them more or less important when calculating the overall score. Quizzes require activation by a system administrator.

- An administrator can create a quiz for any purpose and assign it to a single user or multiple users.
- A quiz can contain one or more categories of questions. Each category can be assigned to users who answer only the questions in that category.
- The system can send email notifications to these users:
  - Recipients: The recipient can receive notification of an assigned quiz, a quiz whose allowed duration is at 50%, and a quiz that is overdue.
  - Recipient's manager: The recipient's manager can receive notification when a quiz is overdue.
  - Quiz manager: The quiz manager can receive notification of an overdue quiz to which he or she is assigned.

- Quizzes can contain questions that are scored or not scored. Unscored questions assess opinions or involve dates and are not counted in the final score. Scored questions specify correct answers and are scored either as 0% or 100%. You can apply a weighting scale to scored questions to establish their relative importance. You can designate questions with these data types as scored questions:
  - Checkbox
  - Choice
  - Duration
  - Likert Scale
  - Numeric Scale
  - Template
  - Yes/No

- A quiz question can be dependent on the response to any scored question. For example, you can create a dependent question requesting additional information that appears only if a recipient answers No to a specific question.

Important terms

The quiz application involves several terms.
Terms used in quiz application

<table>
<thead>
<tr>
<th>Quizzes</th>
<th>A quiz contains information such as duration, state, and notification controls and lists the existing categories. Text fields on the quiz form allow an administrator to create introductory content and end notes that are displayed to the recipient.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Categories</td>
<td>A quiz category represents a theme for quiz questions. Each category contains one or more questions and names the recipients for the questions in that category. By default, the system creates one category with the same name as the quiz. You can create additional categories as needed. Categories can be weighted higher or lower to determine the importance of that category in the overall score.</td>
</tr>
<tr>
<td>Questions</td>
<td>A quiz question is a question configured for a category and sent only to the users for that category. Questions have a wide variety of data types and can be individually weighted higher or lower. Questions may be scored or unscored.</td>
</tr>
<tr>
<td>Category user</td>
<td>A category user is the recipient of questions for a specific category. You can select different users to answer the questions for each category.</td>
</tr>
<tr>
<td>Templates</td>
<td>A template is a question data type that provides reusable rating scales for answers to questions. For example, the answer template named Satisfaction contains a satisfaction scale ranging from Very Satisfied to Very Dissatisfied.</td>
</tr>
</tbody>
</table>

Quiz roles

The Quizzes application uses these roles. No role is required to take quizzes that are assigned to you.

**Quiz roles**

<table>
<thead>
<tr>
<th>Role Title (Name)</th>
<th>Role Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>assessment administrator (assessment_admin)</td>
<td>Can administer the Assessments application and all quiz records. Can access all the modules of the Assessments application.</td>
</tr>
</tbody>
</table>

*Note: The itil_admin role and the survey_admin role contain the assessment_admin role*

| Administrator (admin) | Can access all aspects of the assessment and survey processes. Only administrators can modify survey notifications, create survey modules, and import surveys. |
**Data types for quizzes**
You need to choose a data type for each quiz question. Various data types help you collect and analyze different kinds of data.

**Available data types**

<table>
<thead>
<tr>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachment</td>
<td>Question with a Manage Attachments icon that allows users to attach one or more files.</td>
</tr>
<tr>
<td>Boolean</td>
<td>Question with a check box or a Yes/No list for user responses.</td>
</tr>
<tr>
<td>Choice</td>
<td>List of predefined options. For more information, see the definition for Choices Create quiz questions.</td>
</tr>
<tr>
<td>Date</td>
<td>Date field.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>Time and date field.</td>
</tr>
<tr>
<td>Number</td>
<td>Number field with predefined minimum and maximum values. The default is 1-10.</td>
</tr>
<tr>
<td>Percentage</td>
<td>Percentage field with a prescribed range.</td>
</tr>
<tr>
<td>Scale</td>
<td>Predefined Likert scale. Answer options appear as radio buttons.</td>
</tr>
<tr>
<td>Numeric scale</td>
<td>Selectable number scale. The default is 1-5. Answer options appear as radio buttons.</td>
</tr>
<tr>
<td>String</td>
<td>Single or multi-line text field.</td>
</tr>
<tr>
<td>Template</td>
<td>Choice list of templates that provide a predefined scale of options. For details, see Configure a template question.</td>
</tr>
<tr>
<td>Reference</td>
<td>Choice list of fields from a specified reference table. This data type does not support reference qualifiers.</td>
</tr>
</tbody>
</table>

**Activate the quiz designer**
Administrators can activate the Quiz Designer plugin.

Role required: assessment_admin or 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.

**Quiz Overview module**
The Quiz Overview module is a homepage that displays various reports on data such as results for each category and quizzes that are complete, pending, or in progress.

Role required: assessment_admin or admin

Users with the assessment_admin role can view the overview page and refresh, add, delete, and rearrange widgets.

1. Navigate to Quizzes > Overview.
2. Click elements within reports to obtain more information. The available reports are:

<table>
<thead>
<tr>
<th>Report</th>
<th>Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quizzes by State</td>
<td>Assessment Instance (asmt_assessment_instance)</td>
</tr>
<tr>
<td>Total Questions by Quiz</td>
<td>Assessment Metric (asmt_metric)</td>
</tr>
<tr>
<td>Questions by Data Type</td>
<td>Assessment Metric (asmt_metric)</td>
</tr>
<tr>
<td>Correct Answers by Assigned User</td>
<td>Metric Results (asmt_metric_result)</td>
</tr>
<tr>
<td>Number of Correct Answers</td>
<td>Metric Results (asmt_metric_result)</td>
</tr>
<tr>
<td>Incorrect Answers by Assigned User</td>
<td>Metric Results (asmt_metric_result)</td>
</tr>
<tr>
<td>Number of Incorrect Answers</td>
<td>Metric Results (asmt_metric_result)</td>
</tr>
</tbody>
</table>

**Quiz designer**
The quiz designer provides a single interface that users with the assessment_admin role can use to create, edit, and distribute quizzes.

You can also use it to edit existing quizzes and change scoring parameters.

Alternatively, you can use the modules of the assessment engine to create and edit the records that make up a quiz. All quiz records are stored in assessment tables and displayed in Quiz views of those tables. For details, see Create quizzes with forms.

**Tools on the Quiz designer**
The quiz designer includes a design canvas, a header bar, and many controls that you can use to create quizzes.

To open the quiz designer, navigate to Quizzes > Quiz Designer.

The designer contains the following elements:
- Controls
- Header bar
- Design canvas

**Controls**
Controls for the supported question data types are available in the Controls palette. Drag and drop a control onto the designer canvas to create a question of that type.
Question controls

<table>
<thead>
<tr>
<th>Data type</th>
<th>Description</th>
<th>Scored</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachment</td>
<td>Question with a Manage Attachments icon that allows users to attach one or more files.</td>
<td>Y</td>
</tr>
<tr>
<td>Boolean</td>
<td>Question with a check box or a Yes/No list for user responses.</td>
<td></td>
</tr>
<tr>
<td>Data type</td>
<td>Description</td>
<td>Scored</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>--------</td>
</tr>
<tr>
<td>Choice</td>
<td>List of predefined options. For more information, see the definition for <strong>Choices</strong> <a href="#">Create quiz questions</a>.</td>
<td>Y</td>
</tr>
<tr>
<td>Date</td>
<td>Date field.</td>
<td>N</td>
</tr>
<tr>
<td>Date/Time</td>
<td>Date and time field.</td>
<td>N</td>
</tr>
<tr>
<td>Number</td>
<td>Number field with predefined minimum and maximum values. The default is 1-10.</td>
<td>N</td>
</tr>
<tr>
<td>Percentage</td>
<td>Percentage field with a prescribed range.</td>
<td>N</td>
</tr>
<tr>
<td>Scale</td>
<td>Predefined <a href="#">Likert scale</a>. Answer options appear as radio buttons.</td>
<td>Y</td>
</tr>
<tr>
<td>Numeric Scale</td>
<td>Selectable number scale. The default is 1-5. Answer options appear as radio buttons.</td>
<td>Y</td>
</tr>
<tr>
<td>String</td>
<td>Single or multiline text field.</td>
<td>N</td>
</tr>
<tr>
<td>Template</td>
<td>Choice list of templates that provide a predefined scale of options. For details, see <a href="#">Configure a template question</a>.</td>
<td>Y</td>
</tr>
<tr>
<td>Reference</td>
<td>Choice list of fields from a specified reference table. This data type does not support reference qualifiers.</td>
<td></td>
</tr>
</tbody>
</table>

**Header Bar**

The header bar contains tabs that display different views and a menu of various functions.

Click one of the following tabs to change the view in the canvas:

- **Design**: Add categories and questions, and configure the properties of each. This is the default view of the canvas when you open the designer.
- **Configuration**: Create introductions and end notes for quizzes, and select a [signature](#).
- **Availability**: Select the recipients for each category in the quiz.

Point to the menu icon (≡) in the in the upper right of the quiz designer to select the following options:

- **Save**: Saves the current quiz.
- **Preview**: Displays a preview of the quiz as it appears to the recipients.
- **Publish**: Distributes the quiz to the selected recipients.
- **Save and Publish**: Saves and distributes the quiz in one step.
- **New Quiz**: Opens a fresh canvas for a new quiz.
- **Load Quiz**: Opens a list of existing quizzes that you can select and edit.

The availability of each option depends on the status of the quiz that is opened in the quiz designer.

**Design Canvas**
New quizzes open in the Design view. The quiz Name field appears above first category in the canvas. A blank question field appears in the category container.

Create a quiz
When you create a quiz, you can create one or more categories and then add questions to each category.

Role required: assessment_admin or admin

Each category can be assigned to a different user or the same users. You can also customize each question and make it dependent on the response to another question.

Create a quiz using these procedures:

Create quiz categories
A category represents a theme for evaluating a specific element of the quiz topic and contains questions pertaining to that theme.

Role required: assessment_admin or admin

When you create a quiz, the system creates a default category, using the name of the quiz. You can use this category, modify it, or create additional categories as needed. To have any results, a category must contain scored questions.

1. Navigate either Quizzes > Quiz Designer or Quizzes > Quizzes and click Quiz Designer in the list header.
2. Enter the name of the quiz in the Name field. The system uses this name as the name of the quiz and the first category
3. To configure the category, click the gear icon in its title bar.

The Properties dialog box appears. You can change the name of the category, add a description for it, and enter text in the Details field that introduces or explains the category to the recipients. The system updates the category as you type.

4. Click the X icon to close the category properties dialog box and save your settings.
5. To add a new category, click the + icon in the title bar of an existing category.

Create quiz questions
You can create multiple questions for each category but each question can be associated with only one category.

Role required: assessment_admin or admin

The data type that you select for each question determines how it can be answered by quiz recipients.

You can designate questions to be scored. Only scored questions are shown in the quiz results and considered when calculating the category results. You must also specify a correct answer for scored questions.

Note:
To designate a question as scored, you must use Assessment forms. For instructions, see Configure a scored question.

1. In the Design view, drag a data type icon from the Controls palette and drop it into a category container.
2. To configure the question, click in the gear icon in its title bar. The Properties dialog box appears for the question.
3. Fill in the fields on the form, as appropriate.

**Question property fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>(Required) Name of the question. Create a concise and easily recognizable name for your question. The system uses this value to identify the question in Assessment Metric lists and in scorecard charts.</td>
</tr>
<tr>
<td>Question</td>
<td>Text to display as the question on quizzes. Enter a clear, straightforward question that is easy to understand.</td>
</tr>
<tr>
<td>Type</td>
<td>(Read-only) Data type selected for this question. See the table in controls for possible data types.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Active</td>
<td>Check box that determines whether this question is available on a quiz. If a question is marked inactive, it does not appear on quizzes generated after the question becomes inactive.</td>
</tr>
<tr>
<td>Boolean option</td>
<td>Whether a check box or a Yes/No list appears as the option for the Boolean question.</td>
</tr>
<tr>
<td>Mandatory</td>
<td>Check box for requiring users to answer the question. Users cannot submit quizzes until they answer all mandatory questions, which are denoted by a red field status indicator. This field is available when the question does not have a dependency and the question data type is not Boolean with a check box option.</td>
</tr>
<tr>
<td>String option</td>
<td>Setting for the appearance of a string field in a question. This field is available when the question type is String. The string options are:</td>
</tr>
<tr>
<td></td>
<td>· <strong>Single line</strong>: Single line text field 40 characters in length that allows strings of any length.</td>
</tr>
<tr>
<td></td>
<td>· <strong>String line wide</strong>: Full page width text field that allows a single line entry of any length.</td>
</tr>
<tr>
<td></td>
<td>· <strong>Multiline</strong>: Full page width multi-line text field that allows word wrap and returns.</td>
</tr>
<tr>
<td>Min</td>
<td>Lowest positive whole number that users can enter or select to answer the question. This field is available when the question type is Number, Percentage, or Numeric Scale.</td>
</tr>
<tr>
<td>Max</td>
<td>Highest positive whole number that users can enter or select to answer the question. This field is available when the question type is Number, Percentage, or Numeric Scale.</td>
</tr>
<tr>
<td>Allow not applicable</td>
<td>Check box for including Not Applicable as an option for this question. Users can select Not Applicable if they do not have sufficient information to respond to a question. User responses of Not Applicable are excluded from results calculations. This field is available when the question does not have a dependency and the question data type is not Boolean with a check box option.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Randomize answers</td>
<td>Check box for displaying answer options in a random order whenever the question appears in a quiz. Answer preference is sometimes influenced by the order in which options appear, which can result in biased results. Randomizing options can help prevent this bias. <strong>Note:</strong> Randomizing options for certain questions may make those questions confusing for users. In general, only randomize options that do not follow a logical order.</td>
</tr>
<tr>
<td>Details</td>
<td>Information about the question that is displayed on the quiz. Include details that help users understand how to answer the question. You can also enter HTML text in this field with the WYSIWYG editor. For example, include HTML to embed links and images.</td>
</tr>
<tr>
<td>Correct answer</td>
<td>Answer option that you want to be selected by users. When you specify a correct answer for a question, the system scores the question. This field is available for all data types except <strong>Date</strong>, <strong>Date/Time</strong>, and <strong>String</strong>.</td>
</tr>
<tr>
<td>Choices</td>
<td>Options for a question with a data type of <strong>Choice</strong> or <strong>Scale</strong>. The system automatically adds text and values that you can edit for each option. Click the + icon to add an option, or click the X icon to delete an option. By default, the system arranges options in the order established by their values. To change the order, drag and drop the options.</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>
<tbody>
<tr>
<td>Displayed when</td>
<td>Condition builder that hides or displays the question depending on the answer to another question in the same category. Select an existing question from the list with a data type of Boolean, Choice, Scale, or Template. Create the condition that must exist for recipients to see the dependent question, using the is or is one of operator. The system prevents recursive dependencies between questions. For example, if Question A depends on Question B, Question B cannot depend on Question A.</td>
</tr>
</tbody>
</table>

4. To create any special conditions that must be met for a question to appear on the quiz, click the **Dependency** tab. Fill in the fields, as appropriate.

Dependent questions appear on the quiz when a recipient selects a specific answer or combination of answers to another question in the same category.

5. Select a question in the Displayed when field. The system selects the appropriate operator and displays the possible answers for the selected question.

6. Select the answers that satisfy the condition. Selected answers are indicated by a check mark.

7. Click X to close the question properties dialog box and save your settings.

8. To add a question with the same data type as an existing question in the category, click the + in the title bar of the existing question.
9. Drag questions to change their order within a category or move them between categories.
10. To delete a question, click the X in its title bar.

Configure a quiz
You can configure an entire quiz.
Role required: assessment_admin or admin
The values you enter and select on this page are applied to the entire quiz.
In the quiz designer, click Configuration and then fill in the fields as described in the table.

**Quiz designer configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Check box for enabling the distribution of this quiz to recipients.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of this configuration or the quiz to which it is attached.</td>
</tr>
<tr>
<td>Introduction</td>
<td>Introductory content to display on quizzes. You can add a welcome message or background information about the quiz.</td>
</tr>
<tr>
<td>Signature</td>
<td>(Optional) Acknowledgement by a quiz recipient of requirements, admonitions, or expectations related to a quiz.</td>
</tr>
<tr>
<td>Return URL</td>
<td>Destination address of a web page that is presented to users after they submit a completed quiz. When a return URL is configured, the End note content does not appear.</td>
</tr>
<tr>
<td>End note</td>
<td>Content that is displayed to recipients after they submit a completed quiz. You can add a thank you message, follow-up instructions, or other applicable information. End notes are not displayed if a Return URL is specified.</td>
</tr>
<tr>
<td>Duration</td>
<td>Amount of time that recipients are given to complete this quiz, starting from the time that the quiz is generated. The default duration is 14 days.</td>
</tr>
<tr>
<td>Manager</td>
<td>Assessment manager for this quiz. These users are only responsible for managing the quiz process and not the results. The system notifies the manager when submissions for this quiz are past due.</td>
</tr>
<tr>
<td>Notify manager if overdue</td>
<td>Check box for sending email notifications to a recipient's manager when that user fails to submit an assigned quiz before the due date.</td>
</tr>
</tbody>
</table>

Select a quiz recipient
When the system distributes a quiz, it sends email notifications to the category users and their managers.
Role required: assessment_admin or admin
A category can have one or more assigned users, and the same user can be assigned to more than one category.

The system also creates a link to the quiz in the recipients' My Assessments & Surveys portal. Users can only answer questions in the categories that they are assigned to.

To select the recipients for each quiz category, click Availability and then fill in the fields as described in the table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select category</td>
<td>Category for which the selected users are recipients.</td>
</tr>
<tr>
<td>Add users</td>
<td>Users selected as recipients for this category. The choice list shows all users in the system.</td>
</tr>
</tbody>
</table>

Publish a quiz

When you publish a quiz, the system sends email notifications to the recipients and to their managers. A card in each recipient's My Assessments & Surveys portal displays a link to the quiz.

Role required: assessment_admin or admin

1. If you want to see the quiz as the recipients will see it, point to the menu icon in the upper right of the quiz designer and click Preview.
2. When you are satisfied with the quiz, click Save and Publish or Publish to distribute it.

Create quizzes with forms

As an alternative to the Quiz Designer, you can create a complete quiz using records in the Assessment application.

All the elements of a quiz, the categories, questions, and answers, are stored in tables used by the assessment engine and are displayed in quiz views of these tables. Users creating quizzes in the Assessment application must have the assessment_admin role.

Create a quiz using assessment forms by following the procedures in the order shown here:

- Create the quiz.
- Set up the categories.
- Create the questions for the quiz.
- Create the answers for the questions.
- Distribute the quizzes to recipients.

Note: The recommended method of creating and editing quizzes is to use the quiz designer, which provides a single, intuitive interface for creating and editing quizzes quickly. If you determine that you need to add specific features to your quiz not offered through the quiz designer, you can do so by using some of the specific procedures described here.

Set up a category

A category represents a theme for evaluating a specific element of the quiz topic and contains questions pertaining to that theme.

When you create a quiz, the system creates a default category with the name of the quiz. You can use this category, modify it, or create additional categories as needed. Categories are records in the Quiz view of the Metric Category table.
Categories have **weighting values** that contribute to the overall score for the quiz. By default, all categories are given a weighting value of 10. You can assign any weight to your categories. To have any results, a category must contain scored questions.

You can create a new category or edit an existing one from the **Metric Categories** related list of a quiz record.

Select a user for a category

Category users are the recipients of the questions for each category.

A category can have one or more assigned users, and the same user can be assigned to more than one category. When the system distributes a quiz, it sends an email notification, if configured, to the category users and creates a link to the appropriate questionnaire in their assessments and surveys portal. Users can only answer questions attached to their assigned categories.

To select users for a category, select the **Users** related list in a category record, and click **Edit**.
Create questions

A category can have multiple questions associated with it.

Each question can only be associated with one category. Each question has an answer data type that determines how recipients answer the question. Questions are records in the Quiz view of the Assessment Metric table.

To create questions, open a category record and create a question record from the Assessment Metrics related list. Alternatively, you can navigate to Quiz Management > Questions and create a new record (see table).

**Warning:** When you create a Choice or Likert Scale question, you must reopen the Assessment Metric form after you submit it to create answers. If you distribute a questionnaire without creating the answers for questions with these data types, recipients are unable to answer the questions. If the questions are mandatory, the recipients are unable to submit their questionnaires.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>(Required) Name of the question.</td>
</tr>
<tr>
<td>Category</td>
<td>(Required) Category the question belongs to. The system populates this category if you create a new question from the Metric Category form.</td>
</tr>
</tbody>
</table>

**Note:** You cannot change the category if the **Depends on** field is set or if another metric depends on this metric.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Method</td>
<td>Setting that determines how to use the question.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Assessment</strong>: Makes the question available on a quiz distributed to users. The <strong>Assessment</strong> method is compatible with all data types except <strong>Duration</strong>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Script</strong>: Queries the database without user participation. Scripted questions are of limited value for quizzes, because they do not assess a user’s knowledge of a topic.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: If you select a <strong>Data type</strong> that is incompatible with the selected <strong>Method</strong>, the system automatically changes the <strong>Method</strong> to the correct value.</td>
</tr>
<tr>
<td>Weight</td>
<td>Numeric value that represents the importance of this question relative to other questions in the same category. By default, the weight is 10. For weighting suggestions, see <strong>weight categories and metrics</strong>. This field is available and required unless the <strong>Data type</strong> is <strong>Date</strong>, <strong>Date/Time</strong>, or <strong>String</strong>. These data types are not included in results calculations.</td>
</tr>
<tr>
<td>Order</td>
<td>(Required) Numeric value that determines the order of the question in the category. The question with the smallest order value appears as the first question in the category’s section. By default, the order is 100.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: It does not matter which order value you use for metrics with the <strong>Script</strong> method, because they do not appear on questionnaires.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box that determines whether this question appears on quizzes. If a question is inactive, it does not appear on quizzes generated after the question becomes inactive.</td>
</tr>
<tr>
<td>Mandatory</td>
<td>Check box for requiring users to answer the question. Users cannot submit questionnaires until they provide valid responses to all mandatory questions, which are denoted by a red field status indicator. This field is available only if the <strong>Method</strong> is <strong>Assessment</strong>, the <strong>Depends</strong> on field is empty, and the <strong>Data type</strong> is not <strong>Checkbox</strong>.</td>
</tr>
<tr>
<td>Allow not applicable</td>
<td>Check box for including <strong>Not Applicable</strong> as a possible answer for this question. Users can select <strong>Not Applicable</strong> if they do not have sufficient information to respond to a question. User responses of <strong>Not Applicable</strong> are excluded from results.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Question</td>
<td>The question that is displayed in quizzes. Enter a clear, straightforward question that is easy to understand.</td>
</tr>
<tr>
<td>Details</td>
<td>Information about the question and what it evaluates. Include details that help users understand how to answer the question or when you need HTML enhanced details for your question. You can create HTML text in this field with the WYSIWYG editor, such as embedding links and images.</td>
</tr>
<tr>
<td>Depends on</td>
<td>An existing question that this question is dependent on. You can select Checkbox, Choice, Likert Scale, Template, and Yes/No questions from the same category as this question. Then use the Displayed when field to set the conditions for displaying this question. The system prevents the creation of recursive dependencies between questions. For example, if Question A depends on Question B, Question B cannot depend on Question A.</td>
</tr>
<tr>
<td>Question Type</td>
<td>(Required) Format of the expected response data. See the table of data types for details.</td>
</tr>
<tr>
<td>Data type</td>
<td>(Required) Format of the expected response data. See the table of data types for details.</td>
</tr>
<tr>
<td></td>
<td>Note: You cannot change the data type if another question depends on this question</td>
</tr>
<tr>
<td>Randomize answers</td>
<td>Check box for displaying the possible answers for this question in a random order whenever the question appears. Answer preference is sometimes influenced by the order in which answer options appear, which can result in biased results. Randomizing answer options can help prevent this bias. This check box is available only if the Data type is Choice or Likert Scale.</td>
</tr>
<tr>
<td></td>
<td>Note: Randomizing answer options for certain questions may make those questions confusing for users. In general, only randomize answer options that do not follow a logical order.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Scale definition</td>
<td>Setting that determines whether lesser or greater numerical values equate to a good score in quiz result calculations. Select Low if lesser numerical values are better. Select High if greater numerical values are better. The default value is High. This field is available and required unless the Data type is Date, Date/Time, or String. The results for these data types are not included in results calculations. When the Scored check box is selected, the scale value is set to High and the field is hidden. <strong>Note:</strong> For information about how to set the scale definition for data types that do not require you to set a numerical value, see Data types for assessments.</td>
</tr>
<tr>
<td>Min</td>
<td>Lowest numerical value that can be used as an answer option. This field is available and required only if Data type is Number, Duration, or Percentage.</td>
</tr>
<tr>
<td>Max</td>
<td>Highest numerical value that can be used as an answer option or scaled value. This field is available and required if Data type is Number, Duration, or Percentage.</td>
</tr>
</tbody>
</table>
| String option | Setting for the appearance of a string field in a question. This field is available when the question type is String. The string options are:  
  - Single line: Single line text field 40 characters in length that allows strings of any length.  
  - String line wide: Full page width text field that allows a single line entry of any length.  
  - Multiline: Full page width multiline text field that allows word wrap and returns. |
| Scored     | Check box for using answers in scoring the category results and showing them in the quiz results. Scored questions are available for these data types:  
  - Choice  
  - Likert Scale  
  - Template  
  - Checkbox  
  - Yes/No  
  Selecting this check box hides the Scale definition field and sets the value in that field to High. |
| Correct answer | (Required) Desired answer to a scored question. This field is available when the Scored check box is selected. |
Create answers for questions

Questions with Choice or Likert Scale data types must have defined answer options, called metric definitions.

When you create a question with one of these data types, the Assessment Metric Definitions related list appears. Each metric definition appears as one answer option for a question on a quiz. For example, the question *What type of men's trousers are not permitted by company policy?* might have these three answers configured as metric definitions: *Slacks*, *Jeans*, and *Casual cotton*.

To create an answer option, open the question record you want to edit and click **New** in the *Assessment Metric Definitions* related list. Be sure to give each option a **Value**. The system uses this number to establish the order in which the answers appear in the quiz.

Distribute a quiz

When you finish configuring the answers for the quiz questions, you are ready to distribute the quiz.

You can send the quiz to all the category users configured for the quiz or to a single category user.

1. Navigate to **Quiz Management > Quizzes**.
2. Open the quiz record, and click **Publish**. The quiz is placed in the Published state, and it is sent to all its category users. You can edit and resend published quizzes. See *Modifying Published Quizzes* to learn how various modifications affect the quiz contents.
3. To resend a quiz, click the appropriate button:
   - **Assign Quiz**: Send the quiz to one category user.
   - **Send Quizzes**: Send the quiz to all of its category users.

**Note:** These buttons are hidden if there are no category users defined for the quiz.
Modify a published quiz

You can edit a quiz even after it has been distributed, with these results:
• Added questions are available only on quizzes that are distributed after this change.
• Changes to existing questions are immediately available to users before the quiz is submitted or during the **retake period**. This includes changes to the answers, such as additional choices or changes to the data type.
• Deleted questions are also deleted from the distributed quizzes in users’ queues.

**Edit a quiz**
You can update a quiz after the quiz has been distributed.

Role required: assessment_admin or admin

• Questions that you add are available only on quizzes that are distributed after the update.
• Before a quiz is submitted or during the **retake period**:
  • Changes to existing questions are immediately available to users. This includes changes to the answers, such as additional choices or changes to the data type.
  • Deleted questions are deleted from distributed quizzes in users’ queues.

**Open the quiz:** Group the Service Details form with one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quizzes &gt; Quiz Designer</td>
<td>Point to the menu icon in the quiz header bar and select <strong>Load Quiz</strong>.</td>
</tr>
<tr>
<td>Quizzes &gt; Quizzes</td>
<td>Right-click a quiz in the list and select <strong>Quiz Designer</strong>.</td>
</tr>
<tr>
<td>Quizzes &gt; Quizzes</td>
<td>Open a quiz from the list and click <strong>Quiz Designer</strong> in the header of the Assessment Metric Type form.</td>
</tr>
</tbody>
</table>

**Configure a scored question**
Only **scored** questions are considered when calculating category and quiz results.

Role required: assessment_admin or admin

A question must have a correct answer specified to be scored. Only results for scored questions are displayed in the **quiz scorecard**.

1. Navigate to **Quizzes > Quizzes**.
2. Open the quiz containing the questions you want to mark as scored.
3. In the **Metric Categories** related list on the **Assessment Metric Type** form, select the category for the questions you want to mark as scored.
4. In the **Assessment Metrics** related list on the **Metric Category** form, select a question from the list.
5. In the **Question Type** section of the **Assessment Metric** form, select the **Scored** check box. This check box is not available if the question’s data type is not supported for scoring.
6. Select the **Correct answer** for the question.
7. Click **Update**.
8. Repeat the process for all the questions in the category that you want the system to score.
9. Return to the list of metric categories, select another category, and configure scoring for the appropriate questions in that category.

**Configure a template question**
You can configure template questions when designing quizzes.
Role required: assessment_admin or admin

1. Drag the **Template** data type icon into a category container.
2. Click the gear icon in the question title bar to open the template properties dialog box.
3. Select a predefined scale from the list.

Question entry fields appear for that template.

4. Enter one or more questions that are appropriate for the template.
5. Click the arrow to the right of a question to configure its properties. You must provide a name for each question.
6. Click the up or down arrow to move between questions, or click the back arrow to return to the template properties dialog box.
7. Configure the properties for the remaining questions.
8. Click the X icon to close the template properties dialog box and save your settings.

Enable a quiz retake
You can configure a quiz to allow recipients to resubmit their answers as many times as they like, until the quiz's due date.

Role required: assessment_admin or admin

Results are not calculated until the quiz's configured duration has elapsed. The card in the user's queue remains visible until the quiz's due date and displays a button to allow retakes.

1. Navigate to Assessments > Metric Definition > Types.
2. Remove the Evaluation method = Assessment filter condition so you can see all the records in the list.
3. Open the quiz.
4. In the Assessment Metric Type form, select the Allow retake check box and save the record.
View a quiz result
You can view quiz results for each question and category, or view the quiz scorecard for a detailed breakdown.

Role required: assessment_admin or admin

Quiz results are stored in the Metric Result (asmt_metric_result) table and display recipients’ answers to each question in a category.

Navigate to Quizzes > Quiz Results.

Quiz reports

Quizzes provide several global reports so that assessment administrators can view important statistics.

You can share these reports with specific users or groups and change the display options.

For detailed field information and reporting options, click the link for the chart Type. To sort a column in ascending or descending order, click the arrow in the column heading.

Quiz reports

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quizzes by State</td>
<td>State of distributed quizzes. This chart displays the percentage of distributed quizzes that are ready to take, in progress, complete, or canceled.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Type</strong>: Pie Chart</td>
</tr>
<tr>
<td></td>
<td>- <strong>Table</strong>: Assessment Instance (asmt_assessment_instance)</td>
</tr>
<tr>
<td>Total Questions by Quiz</td>
<td>Total number of questions for all categories in each quiz.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Type</strong>: Bar Chart</td>
</tr>
<tr>
<td></td>
<td>- <strong>Table</strong>: Assessment Metric (asmt_metric)</td>
</tr>
<tr>
<td>Questions by Data Type</td>
<td>Total number of questions in all quizzes by data type.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Type</strong>: Bar Chart</td>
</tr>
<tr>
<td></td>
<td>- <strong>Table</strong>: Assessment Metric (asmt_metric)</td>
</tr>
<tr>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Correct Answers by Assigned User</td>
<td>Total number of scored questions answered correctly by each assigned user.</td>
</tr>
<tr>
<td></td>
<td>• Type: Bar Chart</td>
</tr>
<tr>
<td></td>
<td>• Table: Metric Results (asmt_metric_result)</td>
</tr>
<tr>
<td>Number of Correct Answers</td>
<td>Total number of correct answers for each scored question.</td>
</tr>
<tr>
<td></td>
<td>• Type: Bar Chart</td>
</tr>
<tr>
<td></td>
<td>• Table: Metric Results (asmt_metric_result)</td>
</tr>
<tr>
<td>Incorrect Answers by Assigned User</td>
<td>Total number of scored questions answered incorrectly by each assigned user.</td>
</tr>
<tr>
<td></td>
<td>• Type: Bar Chart</td>
</tr>
<tr>
<td></td>
<td>• Table: Metric Results (asmt_metric_result)</td>
</tr>
<tr>
<td>Number of Incorrect Answers</td>
<td>Total number of incorrect answers for each scored question.</td>
</tr>
<tr>
<td></td>
<td>• Type: Bar Chart</td>
</tr>
<tr>
<td></td>
<td>• Table: Metric Results (asmt_metric_result)</td>
</tr>
</tbody>
</table>

View a quiz scorecard
You can view scorecards for a quiz record.

Role required: assessment_admin or admin

For detailed information about scorecards, see Quiz scorecards.

1. Navigate to Quizzes > Quizzes.
2. Open a quiz record.

   The scorecard link is hidden if there are no quiz results to report.

4. The scorecard contains a header that displays the name of the quiz and a section that displays results or a comparison of ratings. You can select from these principal views:
   • Category Results
   • Question Results
   • Average Ratings
   • History

Quizzes application prepares printable scorecards.

A scorecard analyzes category and question responses and compares current ratings with previous ratings. You can examine ratings over time, compare question ratings, or compare the ratings of all categories. All ratings are averages for the time range selected.

The system dynamically updates a scorecard each time you view it, so the ratings reflect recently completed quizzes.

Category results
The Category Results view is a stacked bar chart of responses to all questions in a category.
Select the category to display from the choice list above the chart. Category results are only calculated for scored questions.

This view displays responses that use the following data types:

- Checkbox
- Choice
- Likert Scale
- Number
- Template
- Yes/No

**Note:** The Checkbox and Yes/No data types are combined into the Boolean data type in the Quiz designer.
To view details about a specific response to a question, point to the colored segment representing a specific response. The chart displays the count for those responses and the percentage it represents of the total responses to that question.

**Quiz category result details**

**Question results**

The Question Results view shows the results for all questions in a quiz. Select a question by name from the choice list to display the results in a pie chart or a bar chart, based on the data type.

**Pie chart**

The pie chart shows question results for these data types:

- Checkbox
- Choice
- Likert Scale
- Number
- Template
- Yes/No

---

**Note:** The **Checkbox** and **Yes/No** data types are combined into the **Boolean** data type in the **Quiz designer**.
Quiz scorecard question results - pie chart
Bar chart

A bar chart appears when question results use this data type:

- Percentage

By default, all results for percentage questions use a report range of 20% segments. To configure a report range, navigate to Reports > Administration > Report Ranges.

Average ratings

The Average Ratings view displays a bar chart of the weighted average rating for each question in a category.

Use this view to learn how individual questions affect the overall rating for the category. Select a category from the second choice list above the chart. Ratings are only calculated for scored questions.
To view the effect of each question's ratings on the entire category's ratings, point to the colored bar. The pop-up box shows the percentage of the total ratings represented by each individual question's weighted average.
Quiz scorecard rating detail

Scorecard history

The History view compares the current ratings for the categories and their questions with ratings from the previous three years or four quarters.

Ratings that have declined are highlighted in red and display negative numbers. Ratings that have improved are highlighted in green with positive numbers. Arrow icons beside the values in the Diff column indicate the trend of the current ratings against the previous ratings. Ratings are only calculated for scored questions questions.

Point to a category to display a line chart that shows the rating trend for that category. Click a category to view the Metric Category form containing the questions.

Scorecard trend chart

- **3 Years**: To calculate the current ratings, the system averages the ratings from the trailing twelve month (TTM) period. The Diff column shows the discrepancy between the current ratings and the previous calendar year's ratings.
Scorecard history - 3 years

- **4 Quarters**: Quarterly quizzes compare the average rating for each question and category in the current quarter against the average ratings from the previous four quarters. The `Diff` column shows the discrepancy between the current ratings and the previous quarter’s ratings. The column labels count backward, by quarter from the current quarter. For example, if the current quarter is the 3rd quarter of 2013, then the previous quarters appear as 2nd (2013), 1st (2013), 4th (2012), and 3rd (2012). All four of the previous quarters appear, whether or not there was any data for those quarters.
Scorecard history - 4 quarters

View an assessment category result
Category results contain values that represent an evaluated record's performance in a specific metric category. Each category result record stores data from one assessment group. Category result values are calculated based on category and metric weights and from metric result values for the same category.

Role required: assessment_admin or admin

**Note:** The system does not include metric results from certain responses in category result calculations. To compensate, the system adjusts the weight of the other normalized metric result values within the same category.

1. Navigate to **Assessments > Results > Category Results.**
2. Click the reference icon (🔗) next to an assessment group number to open the category result record.
3. View the Assessment Category Result form.
   All fields on the form are read-only.

### Assessment Category Result form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Name of the metric category that the category result values apply to.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Rating | Rating is used on scorecards and decision matrixes. Rating is updated dynamically as users complete assessments. Rating is calculated as:  

\[(\text{Sum of all normalized values that share a particular assessment group, category, and assessable record}) / (\text{Number of assessment instances for the assessment group})\]  

For example: In the Assessment Category Results table example, the assessment group ASG0000801 with category Politeness from group NY DB (the assessable record) has a Rating value 8.86.  

On the associated Metric Results table, you can see that there are 4 instances of this group: AINST000801, AINST000802, AINST000803, and AINST000804.  

The system calculated the rating using  

\[(5.14+5.14+1.43+5.14+5.14+4.29+4.29+4.29) / 4 = 8.86\]  

© 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
--- | ---
Assessment group | Assessment group to which the category result is associated. The category result Rating and Normalized value are calculated from metric results in this assessment group only.
Normalized value | Calculated value that measures the Rating relative to the weights of categories used to assess the record evaluated.

The normalized value is calculated as follows:

\[
\text{Normalized value} = \text{Rating} \times \left( \frac{\text{Associated category weight}}{\text{Sum of weights of all categories the source record has category results for in this assessment group}} \right)
\]

Example: A source record has four associated category results in assessment group ASG0000907, one for each of these categories:
- Importance Rating (weight = 10)
- Product Reliability (weight = 9)
- Company Alignment (weight = 9)
- Compliance Score (weight = 9)

If this source record's category result for Product Reliability has a Rating of 7.81, the normalized value calculation is:

\[
7.81 \times \left( \frac{9}{10+9+9+9} \right) = 1.9
\]

Weight | Weight of the associated category. You may need to configure the form to see this field.
Source | Record evaluated as the assessment subject. You may need to configure the form to see this field.

### Create a decision matrix

The name and labels on a decision matrix are closely linked to the categories you choose for the axes. For that reason, first select the metric type and define the X and Y axes before you fill in other fields on the Decision Matrix form.

Role required: assessment_admin or admin

1. Navigate to Assessments > Admin > Decision Matrixes.
2. Click New and then select the metric Type to plot results for.
3. Right-click the form header and select Save.
   The X Axis and Y Axis related lists appear.
4. Define which metric categories the axes represent. Each axis can represent a single category or multiple categories. You must specify at least one category per axis in order for the decision matrix to render properly.

   The available categories are limited to those associated to the metric type selected. To avoid confusion, always update the text for the axis and quadrant labels after editing or adding metric categories to an axis.
Decision matrix axes

5. Fill in the remaining fields on the Decision Matrix form (see table) and save the record.
**Note:** For color fields, either HTML color names or hexadecimal (hex) values are acceptable. For hex values, the # character is optional. Values are not case-sensitive. For example, all of the following values are valid: LightGray, lightgray, #D3D3D3, d3d3d3.

### Decision Matrix form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the decision matrix, which appears as the title on the decision matrix page. It is recommended to include the axis categories in the name. For example, if you selected <strong>Importance Rating</strong> as the X-axis and <strong>User Satisfaction</strong> as the Y-axis, you might name the matrix <strong>Importance vs. User Satisfaction</strong>.</td>
</tr>
<tr>
<td>Type</td>
<td>Metric type associated with this decision matrix. Only results for assessable records of the selected metric type are plotted on the decision matrix.</td>
</tr>
<tr>
<td>Default</td>
<td>Determines whether or not this is the default decision matrix. The default decision matrix opens when you click <strong>View Matrix</strong> on a scorecard. Select the check box to set the matrix as the default decision matrix. The system prevents you from creating more than one default decision matrix per metric type. If there is already a default decision matrix for the type and you try to save a different matrix with the check box selected, an error message appears. The maximum values for the default decision matrix are controlled by the <strong>Maximum number of items to show for a decision matrix field filter</strong> property (com.snc.assessment.decision_matrix_filter_max_entries), which has a default value of 1000.</td>
</tr>
</tbody>
</table>

#### Quadrant Design Section

<table>
<thead>
<tr>
<th>Quadrant label color</th>
<th>Color of the label text for the quadrants. Each quadrant label displays in the center of the quadrant. You can enter an HTML color name or hex value for this and the other color fields.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X-Axis label</td>
<td>Label text for the X-axis of the decision matrix. It is recommended to include the metric category name in the label text. For example, for an X-axis category of <strong>Importance Rating</strong>, the X-axis label is <strong>Importance</strong>.</td>
</tr>
<tr>
<td>Plotted item color</td>
<td>Color used to display plotted items.</td>
</tr>
<tr>
<td>Top left label</td>
<td>Label text for the top left quadrant. For an X-axis labeled <strong>Importance</strong> and Y-axis labeled <strong>Support</strong>, you might label the top left quadrant <strong>Low importance, high support</strong>.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Top left color</td>
<td>Fill color for the top left quadrant.</td>
</tr>
<tr>
<td>Bottom left label</td>
<td>Label text for the bottom left quadrant.</td>
</tr>
<tr>
<td>Bottom left color</td>
<td>Fill color for the bottom left quadrant.</td>
</tr>
<tr>
<td>Bottom left label</td>
<td>Label text for the bottom left quadrant.</td>
</tr>
<tr>
<td>Bottom left color</td>
<td>Fill color for the bottom left quadrant.</td>
</tr>
<tr>
<td>Y-Axis label</td>
<td>Label text for the Y-axis of the decision matrix.</td>
</tr>
<tr>
<td>Highlight item color</td>
<td>Color of highlighted plotted items. When you view a decision matrix from an assessable record’s scorecard, the assessable record plotted item appears in the highlight color. Specify a highlight color that is different than the Plotted item color.</td>
</tr>
<tr>
<td>Top right label</td>
<td>Label text for the top right quadrant.</td>
</tr>
<tr>
<td>Top right color</td>
<td>Fill color for the top right quadrant.</td>
</tr>
<tr>
<td>Bottom right label</td>
<td>Label text for the bottom right quadrant.</td>
</tr>
<tr>
<td>Bottom right color</td>
<td>Fill color for the bottom right quadrant.</td>
</tr>
</tbody>
</table>

**Related Lists**

<table>
<thead>
<tr>
<th>X Axis</th>
<th>Lists categories that define the X-axis of the decision matrix.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y Axis</td>
<td>Lists categories that define the Y-axis of the decision matrix.</td>
</tr>
</tbody>
</table>

**Decision matrixes**

Assessment results obtained by questionnaires and scripted metrics can be mapped to decision matrixes.

Assessment administrators can view and create these dynamically updated graphs, which make it possible to compare assessable records by category. Decision matrixes display data from a trailing twelve month (TTM) period.
Note: Assessment administrators can access decision matrices through the Assessment application and vendor managers can access them through the Vendor Performance application.

Decision matrix components

The decision matrix page has these components:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Options</td>
<td></td>
</tr>
<tr>
<td>Filter</td>
<td>Select the subset of assessable records you want to view. The filter options available vary by metric type, based on the Filter field and Filter condition field settings for each type. The maximum values in the filter are controlled by the Maximum number of items to show for a decision matrix field filter property (com.snc.assessment.decision_matrix_filter_max_entries), which has a default value of 1000.</td>
</tr>
<tr>
<td>Scale</td>
<td>Select the scale for the decision matrix. The greater the scale, the larger the decision matrix appears.</td>
</tr>
<tr>
<td>Decision matrix</td>
<td>X- and Y-axes</td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Plotted items</td>
<td>The labeled points you see on a decision matrix, called plotted items, represent averages of category result data for assessable records. Point to a plotted item label to view a rating summary for that assessable record. Click a plotted item label to view the scorecard for the assessable record.</td>
</tr>
</tbody>
</table>
**Plotted item rating summaries**

If you point to a plotted item label on a decision matrix, a rating summary appears. The summary displays the assessable record's average ratings for each axis. If an axis represents one metric category, the ratings are calculated averages from results for that category. If an axis represents multiple categories, the ratings are calculated averages from weighted results for all of the categories.

The summary shows:

- Current rating
- Difference between the current rating and the rating from the previous year
- Ratings from each previous year, going back three years

**Take an assessment**

Assessments that are assigned to you appear in your assessment and survey queue as a card that displays the assessment name, state, due date, and the associated incident number. Click **Take Survey** when you are ready.

Role required: none
Overdue surveys and assessments are marked with a red icon and red due date. You must answer every required question, indicated by a red bar, before you can submit the assessment as complete. If you start to take an assessment but cannot complete it, save your responses and return to it later. When you have answered all the questions and are satisfied with the responses, submit the assessment.

By default, you cannot modify your answers to an assessment after submission. However, if the administrator has configured an assessment to allow retakes, you can edit your answers and resubmit the questionnaire. Completed assessments configured for retake remain in the queue until their due date and display the Modify Assessment button on the card.

1. Navigate to **Self-Service > My Assessments & Surveys**.

   **Note:** Users with the assessment_admin role can display other users’ assessments and surveys in addition to their own. Use the **Show all** and **Show assigned to me** related links to show and hide assessments and surveys. Click a card assigned to another user to open the associated metric type or survey definition.

2. On the assessment card, note the due date.

   **Note:** Depending on the configuration, you may receive email notifications to remind you of the due date.

3. Click **Take Assessment** to open the questionnaire.

   Assessment questionnaires are arranged in sections: first by record, then by category. Each record appears as a section title. Questions for the record appear below, grouped by category. Each category appears as a subsection below the record name. Click the collapse icon () or expand icon () to hide or show the questions in a category, or all the categories and questions for a record. Colored bars indicate the status of each question.
4. Answer each question to the best of your ability. Point to a question for more information.

If you are unsure of how to respond to a question or if a question does not apply to a particular record, select Not Applicable, if available.

5. Read any assertions present at the end of the assessment and acknowledge with a signature, if required.

A signature can require you to select a check box or authenticate your full name, which the system displays in a read-only field. You cannot submit your answers to the assessment until you provide the required signature.
6. Save or submit the assessment.
   - **Save**: Saves your responses without submitting them. You can close the questionnaire and access it later from your queue.
   - **Submit**: Submits the completed assessment when you are finished.

7. If prompted, enter your user name and password to verify your full name signature.
   If all the questions are answered with valid values, a success message appears. If the system detects an unanswered mandatory question or invalid response, the assessment is not submitted, and a message appears at the top of the questionnaire explaining the error. Questions with problems are temporarily highlighted.

8. You can modify your responses to the assessment until its due date. To update your answers and resubmit an assessment that permits retakes, click **Modify Assessment**.

**Assessment questionnaires**

In the assessment process, users complete assessment questionnaires on topics of interest to provide subjective data for future business decisions.
No special role is required to complete an assessment. You are eligible to complete assessments that are assigned to you. For example, you might be expected to evaluate vendors your organization works with, based on traits related to customer service. The system stores your responses so decision makers can compare the performance of the items you evaluate. You and your manager may receive email notifications as reminders of important assessment information.

**Metric types and assessable records**

In the Assessments application, assessment administrators create and administer metric types and assessable records.

A metric type defines a set of records an organization wants to evaluate, such as vendors, projects, or employees. For each type, the system generates unique assessable records that link the type to records that need to be evaluated, such as the individual records for the vendors Amazon and Intel. There may be multiple assessable records for the same source record if the source record meets the criteria for more than one type. For example, you might want to evaluate a record on the Company table, such as Intel, as a vendor and as a manufacturer, with different categories and metrics.

For configuration suggestions, see [Assessment Administrator tasks](#).

**Assessable records**

An assessable record links a source record you want to evaluate, such as the company record for Amazon or the user record for a sales representative, to a metric type, such as vendors or employees.

You use assessments to evaluate the assessable record. The system generates assessable records from the source records that match the table and conditions set on the Assessment Metric Type form. You evaluate the assessable records with metric categories and metrics, which define traits and values to assess. For metric types with the *On demand* schedule type, you can generate on-demand assessments from the Assessable Record form. This method of assessment generation makes it easy to create and preview short questionnaires or to quickly obtain assessment results for specific assessable records.

You can set up an assessment description that includes information from multiple fields on an assessable record and is displayed on multiple lines. This provides the user who is taking the assessment with a more detailed and understandable description of the information being requested on the assessment questionnaire. Create a multi-line description using table titles, which can be defined to use one or more fields from the selected table. See [Define a new smartphone table title](#) for more information.

**Delete an assessable record**

When you delete an assessable record, the system deletes any stakeholders for the record.

Role required: assessment_admin or admin

---

**Note:** If a source record is deleted, the system deletes the associated assessable record. To delete the source record, you must first delete all associated metric results and category results.

Delete the assessable record:

- To delete a single record, open the record and click **Delete**.
- To delete multiple records, use the Assessable Records list.
View an assessable record

View the Assessable Record form to edit preferences and perform various actions.

Role required: assessment_admin or admin

1. Navigate to Assessments > Assessable Records.
2. Open a record from the list.
   By default, the list displays only assessable records with Active metric types.
3. On the Assessable Record form, edit fields and perform other actions as necessary (see table).

Viewing Assessable Records

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>(Read-Only) Assessable record name based on the display value of the source record. The name appears on assessment questionnaires.</td>
</tr>
<tr>
<td>Source</td>
<td>(Read-Only) Source record the assessable record is linked to. The Source reflects the table name and source record display value. For example, if the Name field is the display value for the Company table, the assessable record for a company record named Amazon has the Source value Company: Amazon.</td>
</tr>
<tr>
<td>Live feed</td>
<td>Check box that, when selected, creates a live feed group for the assessable record, which appears on the scorecard. If you clear the check box after a live feed group has been created, the system deletes the live feed group and all its messages.</td>
</tr>
<tr>
<td>Type</td>
<td>(Read-Only) Metric type from which the assessable record was generated.</td>
</tr>
<tr>
<td>Decision matrix</td>
<td>Check box that, when selected, enables this assessable record's results data to appear on decision matrices of the same metric type. Decision matrices are graphs that plot the assessment results for multiple assessable records. If you clear the check box, the assessable record still appears on the default decision matrices if you click the View Matrix related link on the assessable record's scorecard.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Live feed group</td>
<td>(Read-Only) Live feed group for this assessable record. When you select the Live feed check box and save the record, the system populates this field.</td>
</tr>
<tr>
<td>Related Links</td>
<td></td>
</tr>
<tr>
<td>View Scorecard</td>
<td>Opens the scorecard for the assessable record.</td>
</tr>
<tr>
<td>Related Lists</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>All metric categories associated with the assessable record. An assessable record must be associated to a category to be evaluated. Click Edit to add or remove category associations. Note that it is often more efficient to associate assessable records to categories using the Metric Category form.</td>
</tr>
<tr>
<td>Category users</td>
<td>All stakeholders who can take assessment questionnaires about this assessable record. Click Edit to create and delete stakeholders. For more information about this and other methods of creating stakeholders, see Stakeholders. This related list is available only when the associated metric type has the Scheduled schedule type.</td>
</tr>
</tbody>
</table>

**Approvals**

Approvals can be defined for all tasks and allow users or groups to be associated with a task, for the purpose of either approving or rejecting that task. Approvals are defined by navigating to System Policy > Approvals.

The following information defines an approval:

**Approval definition information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Input value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approver</td>
<td>A reference to the user who is responsible for approving the related record. Choices are:</td>
</tr>
<tr>
<td></td>
<td>- Not Yet Requested (This state indicates that you are not yet asking your approvers to approve this request. Until you set the status to Requested they will receive no email notifications about the request.)</td>
</tr>
<tr>
<td></td>
<td>- Requested</td>
</tr>
<tr>
<td></td>
<td>- Approved</td>
</tr>
<tr>
<td></td>
<td>- Rejected</td>
</tr>
<tr>
<td>Field</td>
<td>Input value</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Approving</td>
<td>A document_id reference field to the record being approved, on any table.</td>
</tr>
<tr>
<td>Comments</td>
<td>A journal field for storing comments regarding the approval.</td>
</tr>
<tr>
<td>Approval Summarizer</td>
<td>A formatter that displays key fields relevant to the approval from the referenced document. This summarizer will not display if there is no record referenced.</td>
</tr>
</tbody>
</table>

**Approval engines**

The differences in the way that companies handle their approvals, as well as the differences between approvals for the various applications (such as Service Catalog Requests and Change Management), calls for supporting flexibility in setting up approvals within applications. This flexibility is provided through the selection of an "approval engine" that is used to manage the approvals for each of the Task tables (that is, all tables that extend the Task table).

There are three different approval engine options available for each Task table.

**Approval engine options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approval Rules</td>
<td>A simple set of rules that are evaluated until one matches for the Task table. The matching approval rule is used to create the users that are to approve the task. Set up approval rules by navigating to <strong>System Policy &gt; Approvals</strong>.</td>
</tr>
<tr>
<td>Process Guides</td>
<td>A sequence of approval steps over which you may control how approvals and rejections are handled. This option is deprecated and should not be used.</td>
</tr>
<tr>
<td>Turn off Engines</td>
<td>Turn off both approval engines for this Task table. This option should be selected and is made read-only when a workflow is used to manage the approval process for the table.</td>
</tr>
</tbody>
</table>

**Caution:** Not turning off the approval engines might have a performance or behavioral impact on your instance.

**Set up an approval engine**

To manage the approvals for each of the Task tables in the system, set up an approval engine.

1. **Navigate to System Properties > Approval Engines.**

   The following page appears with the Approval Engine option for each Task table in the system. If the Approval Engine option is greyed out and shows Turn engines off, read the Notes in the same row. The most common reason an approval engine is turned off is that a workflow is managing the approvals on the table. Having the approval engine turned off prevents conflicts with the workflow that could cause a range of issues. If you want to use an approval engine on the table, set the workflow to inactive.

© 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. Select the **approval engine option** for each Task table from the choice list.
3. Click **Save**.
   These preferences are saved as system properties that are named `glide.approval_engine.<table_name>`.  

<table>
<thead>
<tr>
<th>Table</th>
<th>Name</th>
<th>Approval Engine</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Phase</td>
<td>change_phase</td>
<td>Turn engines off</td>
<td></td>
</tr>
<tr>
<td>Change Request</td>
<td>change_request</td>
<td>Turn engines off</td>
<td>Workflows are managing approvals on this table.</td>
</tr>
<tr>
<td>IMAC</td>
<td>change_request_imac</td>
<td>Turn engines off</td>
<td></td>
</tr>
<tr>
<td>Change Task</td>
<td>change_task</td>
<td>Process Guides</td>
<td></td>
</tr>
<tr>
<td>HR Case</td>
<td>hr_case</td>
<td>Turn engines off</td>
<td>Workflows are managing approvals on this table.</td>
</tr>
<tr>
<td>HR Task</td>
<td>hr_task</td>
<td>Approval Rules</td>
<td></td>
</tr>
<tr>
<td>Incident</td>
<td>incident</td>
<td>Turn engines off</td>
<td></td>
</tr>
<tr>
<td>Incident Task</td>
<td>incident_task</td>
<td>Turn engines off</td>
<td></td>
</tr>
<tr>
<td>Request new Knowledge Base</td>
<td>kb_knowledge_base_request</td>
<td>Turn engines off</td>
<td>Workflows are managing approvals on this table.</td>
</tr>
<tr>
<td>KB Submission</td>
<td>kb_submission</td>
<td>Turn engines off</td>
<td></td>
</tr>
<tr>
<td>Problem</td>
<td>problem</td>
<td>Turn engines off</td>
<td></td>
</tr>
<tr>
<td>Problem Task</td>
<td>problem_task</td>
<td>Turn engines off</td>
<td></td>
</tr>
<tr>
<td>Reconcile Duplicate Task</td>
<td>reconcile_duplicate_task</td>
<td>Turn engines off</td>
<td></td>
</tr>
<tr>
<td>Release Phase</td>
<td>release_phase</td>
<td>Turn engines off</td>
<td></td>
</tr>
<tr>
<td>Feature Task</td>
<td>release_task</td>
<td>Turn engines off</td>
<td></td>
</tr>
</tbody>
</table>
Approval rules

Many organizations rely on an approval process to ensure that requests are reasonable and fit an organization's budget.

The service catalog can use these classes of approvals:

<table>
<thead>
<tr>
<th>Approvals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
</tr>
<tr>
<td>Gating approvals</td>
</tr>
<tr>
<td>Process approvals</td>
</tr>
</tbody>
</table>

Note: To enable approval processes to operate smoothly, make sure that the appropriate users have the correct role, and that the role grants access to the necessary tables for users in all the relevant departments and domains.

Set automatic approval rules

Approval rules can automatically set the approval state to something other than Not yet requested. As a result, an approval rule can create a set of approvers. You can also start the approval process by setting the approval state to Requested.

Prerequisites

Role required: admin

Approval rules have two new fields:

- **Run rule before**: If true, the approval rule runs before the record is inserted/updated.
- **Set State**: If this rule applies, then the task record's approval state is automatically set to this value.

Note: The Set State field only behaves as expected if the Run rule before check box is enabled.

- In the example below, this rule automatically sets the state of the task to Approved thereby auto-approving the task.
Approval Rules fields

Gating approvals

A gating approval acts as a gate through which a request must pass before it can start. Until all gating approvals are met, no notifications go out, no tasks get sent to technicians, and nobody starts working on the request in question.

Generate gating approvals with:

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approval rules</td>
<td>Can apply to the service catalog as well as any other task table.</td>
</tr>
<tr>
<td>Item-based approvals</td>
<td>Flag specific catalog items as requiring specific approvals. Any requests for these items automatically require these approvals.</td>
</tr>
</tbody>
</table>

Set up a gating approval via an approval rule

You can set up a gating approval via an approval rule.

Role required: admin

1. From the left navigation pane, select **System Policy > Approval Rules**.
2. Click **New**.
## Approval rules

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of this rule.</td>
</tr>
<tr>
<td>Table</td>
<td>Task table to which this rule applies. For most service catalog approvals, select <strong>Request</strong>.</td>
</tr>
<tr>
<td>Note:</td>
<td>The list shows only tables and database views that are in the same scope as the approval rule.</td>
</tr>
<tr>
<td>Active</td>
<td>Indicator of whether the rule is active (defaults to true).</td>
</tr>
<tr>
<td>Run Rule Before</td>
<td>Indicator of whether the rule runs before or after the request record is saved. For most approvals, select this check box.</td>
</tr>
<tr>
<td>User</td>
<td>User who must approve this request (can be empty).</td>
</tr>
<tr>
<td>Group</td>
<td>Group that must approve this request (can be empty).</td>
</tr>
<tr>
<td>Set State</td>
<td>Value of the approval field on the task in after this rule runs. In most cases, select <strong>Requested</strong>.</td>
</tr>
<tr>
<td>Condition</td>
<td>Condition under which the rule applies.</td>
</tr>
<tr>
<td>Script</td>
<td>An optional server script to programmatically specify who the approver should be. For example, for the one-line script <code>current.requested_for.manager</code>, ServiceNow checks the requested_for reference field on the current record. It then locates the manager field on the referenced record and assigns that person as the approver. For other examples, see the Script field on approval rules provided by ServiceNow.</td>
</tr>
</tbody>
</table>

### Notes and limitations:

1. You can have as many rules as you want on a given table. If more than one rule applies, you'll get more than one approver.
2. You can't get duplicate approvers, for example, if two rules both want Fred Luddy to approve a particular request, the system will only create one approval entry for him.
3. By default all requests start out in a **Not yet requested** approval state. Approval notifications will not go out until the request's approval state is set to **Requested**. You can do that manually, or you can do it in script, but the easiest way to do it is to use the **Set State** field to automatically set the request to **Requested**.

**Set up a gating approval based on the item being ordered**

In addition to adding approvals via approval rules, you can also add approvals based on what kind of item is being ordered.
In addition to adding approvals via approval rules, you can also add approvals based on what kind of item is being ordered. We can, for example, specify that all Blackberrys need to be approved by David Loo.

To do so, navigate to the item in question and scroll to the related list of required approvers. There are two lists:

- **Approved By Group**: A list of groups that have to approve requests for this item
- **Approved By**: A list of users who have to approve requests for this item

**Approve list**

In the example above, this request must be approved by all members of the Hardware group and by David Loo.

Notes and limitations:

1. As with approval rules, you are protected against duplicate entries. Thus if David Loo is a member of the hardware group, as well as being a standalone approver, he will only get one approval request.

2. Item-based approved work in addition to rather than instead of approval rules so you can (and probably will) use both.

**Process approvals**

Once a request has passed its gating approvals, any relevant execution plans are initiated. Those plans, in turn, create a sequence of required tasks. You can add an approval step to an execution plan, which is configured to occur at the appropriate point.

From the left navigation pane, select **Service Catalog > Execution Plans**, and then select the plan to which to add an approval step. Then click the **New Approval** button.
The Approval Task screen appears. Just like a regular Service Catalog execution task, an approval execution task has:

- **Name**: The name of this task
- **Order**: Sequence of this task within the plan
- **SLA**: SLA to which this task applies
- **Delivery Time**: Time allowed for the completion of this task

After you create the task, right click the title bar and select **Save**. Two related lists appear at the bottom of the screen:

- **Approved By Group**: A list of groups that must approve the request before this task is complete
- **Approved By**: A list of users who must approve the request before this task is complete
In the example above, this security approval task must be approved by Fred Luddy.

**Note:** When an in-process approval is rejected, that particular line item is canceled as well, but the request itself isn't necessarily canceled. Thus if one ordered a blackberry and a laptop, and the blackberry was rejected, the laptop request would continue being processed.

**Approve with a process guide**

Process guides work similarly to approval rules in that their execution is controlled via a condition. The default version of approval tasks allows you to specify that the approval in question be approved by:

1. One or more specific people
2. One or more groups of people
You can optionally use Process Guides instead of approval tasks. Process guides are more flexible in that they allow for:

1. "Any of" or "All of" approvals
2. Sequenced approvals

You can link a process guide to an execution task.

1. From the left navigation pane, select **System Policy > Process Guides**.
2. Create a new guide.
3. Set the table to **Catalog task**.
4. Fill in a condition under which this guide should attach.

**Example #1:** Apply to all "Capacity Review" tasks.

```plaintext
Add Condition
-  +  State is Open
-  +  and Delivery task is Capacity Review
```

**Example #2:** Apply to all "Capacity Review" tasks where the requester is in Atlanta.

```plaintext
Add Condition
-  +  State is Open
-  +  and Delivery task is Capacity Review
-  +  and Request item.Requested For Location is Atlanta
```

**Process guide tips and tricks:**

1. All catalog tasks are generated when a request is first submitted, but tasks which aren’t active yet have a state of "pending". So if you do not want to send out approval requests until a task has actually started, add "state=open" as part of your condition.

2. There is a “Default” process guide in the system for catalog tasks with a sequence number of 10,000. It behaves exactly the same way the old, pre-process guide code did in regards to approvals. Approvals are based on the execution of task-related lists.

**Schematic of a hypothetical approval process**

In the diagram below of a hypothetical approval process, the gating approval is color coded blue and an in-process approval is orange.
Approval process

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>
</tr>
</thead>
<tbody>
<tr>
<td>Affected CI</td>
<td>Sales Force Automation</td>
</tr>
<tr>
<td>Planned start date</td>
<td>2016-07-27 16:00:00</td>
</tr>
<tr>
<td>Planned end date</td>
<td>2016-07-27 18:00:00</td>
</tr>
<tr>
<td>Short description</td>
<td>Rollback Oracle Version</td>
</tr>
<tr>
<td>Description</td>
<td>Performance of the Siebel SFA software has been severely degraded since the upgrade performed this weekend. We moved to an unsupported Oracle DB version. Need to rollback the Oracle instance to a supported version.</td>
</tr>
</tbody>
</table>

**Requested by** | David Loo |
| **Type**         | Normal |
| **Risk**         | High |
| **Impact**       | 3 - Low |
Summary of a catalog request

The **Deny** 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 **Deny** 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.

**Summarizers**

Approval summarizers are stored in the Macro (sys_ui_macro) table.

From the left navigation pane, select **System UI > UI Macros**. Summarizers use a naming convention of approval_summarizer_ + `<table_name>` (for example, approval_summarizer_change_request is the summarizer for change requests, while approval_summarizer_sc_request is the summarizer for service catalog requests).

Each summarizer is written in Jelly script, which is used to define internal forms. The script is stored in the large XML field at the bottom of the UI Macro form.

**Change an approval summarizer**

You can modify existing approval summaries to include additional information.

These are advanced customizations that might not be appropriate for all implementations, and require creating a custom form.

1. Navigate to **System UI > UI Macros**.
2. Open the summarizer you want to change.
3. Copy the script to another location before editing, in case you need to revert it.
4. Modify the script.
5. Click **Update**.

Create a new custom approval summarizer

After you add a new table that has approvals to an instance, you can add a custom activity formatter by creating a new UI macro and then add it to the appropriate form.

**approval_summarizer** can only be used on approval forms in the global scope.

1. Navigate to **System UI > UI Macros**
2. Click **New**.
3. Give the macro a name that follows the summarizer naming convention: `approval_summarizer_<tablename>`
4. Complete the rest of the form and click **Submit**.
5. **Create an activity formatter** and add it to the appropriate form.

To learn more about activity formatters, see *Activity formatter*.

Approval with e-signature

Approval with e-signature allows users to approve requests by re-entering their login credentials.

Approval with e-signature supports the following authentication credentials:

- User name and password matching a user in the local database.
- User name and password matching a user authorized by an external identity provider as part of a SAML 2.0 single sign-on integration.

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**.

De-activate e-signatures

Use this procedure to de-activate e-signatures.
Although plugins cannot be removed, e-signatures can be disabled.
1. Navigate to System Definition > E-Signature Registry.
2. Set Enabled to False on any tables where e-signatures are no longer required.

Use e-signature approvals

Users can approve requests with an e-signature.

Users can approve requests with an e-signature by:

- Selecting the Approve or Reject option on a list context menu.
- Clicking the Approve or Reject button on a form.
- Changing a request record’s State to Approved in either the list-editor or form.

Selecting any of these options presents the user with an Approver Authentication window, which requests the user’s credentials again.

Installed with approval with e-signature

Installing approval with e-signature installs certain properties.

- Module - E-Signature Registry
- UI Action - Approve (on table sysapproval_approver, with no action name)
- UI Action - Approve (on table sysapproval_approver, with no action name)
- UI Action - Approve (on table sysapproval_approver, with the action name authenticated_list_approval)
- UI Page - form_login_validate_dialog
- UI Page - login_validate_dialog
- UI page: saml2_esignature_login, the re-authentication page that appears when an approver tries to approve a request.
- Properties: see E-signature SAML properties
- Client Script - Authenticate Approver
- Script Include - User
- Script Include - UserAuthentication
- Processor: eSigSaml2AssertionConsumer

Installing the plugin also disables the two out-of-the-box Approve UI Actions on the sysapproval_approver table.

Select an approval table

By default, activating the Approval with E-signature plugin enables e-signature for all tables for which a previous approval exists.

E-signature approvals can also be enabled on a table-by-table basis. To enable e-signatures for a table:

1. Navigate to System Definition > E-Signature Registry.
2. In Table name, use the drop-down list to select a specific table.

Table Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>A table drop-down to select the table that requires e-signatures.</td>
</tr>
</tbody>
</table>
### Set up an approval from a local database

To set up Approvals with e-signature using credentials from a local database:

1. Activate the **Approval with e-signatures** plugin.
2. Create user records for approval users.

### 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><strong>Assertion Consumer URL for eSignature authentication</strong></td>
<td>This property defaults to the appropriate URL. To configure this property, click the lock icon to make this field editable. After edits, click the icon to lock the field.</td>
</tr>
<tr>
<td><strong>Assertion Consumer Index for eSignature authentication</strong></td>
<td>If your Service Provider has more than one URL set for the AssertionConsumerURL, you can set the index to use for eSignature, starting with index 1 or more.</td>
</tr>
<tr>
<td><strong>AuthnRequest URL for eSignature Authentication</strong></td>
<td>You can enter the URL that points to the SAML 2.0 IdP AuthnRequest URL for eSignature authentication. If the URL is the same as the Assertion Consumer URL, you can leave this setting blank.</td>
</tr>
<tr>
<td><strong>Authentication Pop-up Dialog Width</strong></td>
<td>When a user approves a request using eSignature, a dialog opens and a user can enter credentials. This setting controls the width of that dialog box. The default is 500.</td>
</tr>
<tr>
<td><strong>Authentication Pop-up Dialog Height</strong></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.

### Set up e-signature approvals

The setup required depends on where user credentials are stored. See the section that matches the source of your user credentials:

- Setting up approvals from a local database
- E-signature SAML properties

**Note:** ADFS 2.0 does not support re-authentication requests that E-Signature requires.

### Approval status

The approval status of a change request is determined by looking at the current status of all the approvers.

If any approver has rejected the change, the approval status will be Rejected. If all approvers have approved the change, the approval status will be Approved. If all approvers are in the Not Requested status or if there are no approvers, the change status will be Not Requested, otherwise the status will be Requested.

For added flexibility when creating approvals, including the ability to set up an "one of" approval where only one person of a group of approvers needs to approve, consider using **Workflows**.

### Generate an approval using approval rules

The system can automatically generate an approval request to individuals or groups when specific criteria are met. The automatic generation of approval requests is driven using the System Policy feature.
In the sample below, a change opened in the category **network** is assigned to the System Administrator:

![Approval Rules](image)

**Approval Rules**

When an approver is automatically added based on approval rules, the status of the approval automatically defaults to "Requested".

**Generate approvals using the approvers related list**

It is possible to manually add approvers to a request.

Additional approvers can be added by clicking the **Edit** button in the Approvers section near the bottom of a request. When an approver is added manually, the status for that approver defaults to "Not Requested". When the status of the approver is changed to 'Requested', the approver will be sent an email requesting approval action.

**Generate approvals using workflows**

Workflows are a powerful and flexible method of generating approvals. Use workflows to create group approvals and user approvals.

A variety of variables are available to fine-tune the approval process, including the actions that occur when approval or rejection take place. When a workflow activity generates an approval record, the system populates the **Workflow activity** field on the approval record with a reference to the activity. Do not use this field when creating business logic. For more information, see *Approval and Rollback Activities*.

---

**Note:** Conflicts can arise when the approval process for a table is managed by both the workflow engine and the approval engine. In general, if there is a workflow that manages the approval process for a table, the *approval engine* should be turned off for that table.

---

**Multiple approvers**

With multiple approvers, all approvers must authorize the request before the status will change to "Approved".

Should any approver reject the request, the status will immediately be set to 'Rejected'.

**Receive notifications**

Individuals who are designated approvers automatically receive approval notifications, including approval status updates.
Approval notifications will be sent at the following times:

- When an individual is assigned as an approver either automatically or manually. If a group is chosen, then all members of the group will be sent an email. By default, the email an approver receives will contain a "mailto" link that will allow the approver to either approve or reject the request directly from their email system.
- When the request reaches approved status, the person assigned to the request will receive an email indicating it has been approved.

The details contained in the emails and the points at which they are sent can be tailored using System Definition > Business Rules and System Policy.

Note for Blackberry users: In order to see the "mailto" links mentioned above to approve or reject a request (i.e. 'Click here to approve CHG55555' or 'Click here to reject CHG55555'), your Blackberry device must be using version 4.5 of their software which supports HTML emails. If your Blackberry device is using an earlier version, you will not be able to view or use the "mailto" links. However, as a workaround, users can reply to the email and add the statements state: approved or state: rejected within the body of the email before sending it to force the automatic approval/rejection functionality.

If you create an appropriate Inbound Email Action, you can let approvers respond to approval email notifications with a simple "yes" or "no" answer.

Dynamic approval forms

When you are looking at an approval request, the form has a context-appropriate summary of the item to be approved.

For example, if you're looking at a Change Management approval request, you'll see details from the relevant change request. For a Service Catalog approval request, you'll get details of the request.

### Change request approval example

Performace of the Siebel SFA software has been severely degraded since the upgrade performed this weekend. We moved to an unsupported Oracle DB version. Need to rollback the Oracle Instance to a supported version.
Scripts and engines execution order

Scripts, assignment rules, business rules, workflows, escalations, and engines all take effect in relation to a database operation, such as insert or update. In many cases, the order of these events is important.

Note: Client-based code that executes in the browser, using Ajax or running as JavaScript, will always execute before the form submission to the server.

The order of execution is as follows:

1. Before business rules: Scripts configured to execute before the database operation with an order less than 1000.

2. Before engines. The following are not executed in any specific order:
   - Approval engine (for task and sys_approval_approver tables)
   - Assignment rules engine (for task tables)
   - Data policy engine
   - Escalation engine
   - Field normalization engine
   - Role engine - keeps role changes in sync with sys_user_has_role table (for sys_user, sys_user_group, sys_user_grmember, and sys_user_role tables)
   - Execution plan engine (for task tables)
   - Update version engine - creates version entry when sys_update_xml entry is written (for sys_update_xml table)
   - Workflow engine (for default workflows)

3. Before business rules: Scripts configured to execute before the database operation with an order greater than or equal to 1000.
4. The database operation (insert, update, delete).

5. *After* business rules: Scripts configured to execute after the database operation with an order less than 1000.

6. *After* engines. The following are not executed in any specific order:
   - Label engine
   - Listener engine
   - Table notifications engine
   - Role engine - keeps role changes in sync with sys_user_has_role table (for sys_user, sys_user_group, sys_user_grmember and sys_user_role tables)
   - Text indexing engine
   - Update sync engine
   - Data lookup engine inserts or updates
   - Workflow engine (for deferred workflows)

7. Email notifications. The following are executed based on the weight of the notification record:
   - Notifications sent on an insert, update, or delete
   - Event-based notifications

8. *After* business rules. Scripts configured to execute after the database operation with an order greater than or equal to 1000.

**Geolocation**

The geolocation feature uses Google Maps to track users, plan efficient routes between locations, and assist in finding accurate travel times for applications that require this information, such as Work Management.

The system locates users from latitude and longitude information provided by their mobile devices or browsers. Tracking the location of certain users can improve business processes such as the completion of work order tasks. For example, in work management geolocation, the system updates an agent’s position each time that agent updates a task record. When the system updates an agent’s location frequently, agents and dispatchers can use features like auto-routing to create efficient schedules.

Geolocation features can be configured by users with the admin role.

**Activate geolocation**

An administrator can activate the Geolocation 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 Only related link on the System Plugin form.

5. Click Activate.

Installed with geolocation

The following components are installed with Geolocation:

**Modified by Geolocation**

The Geolocation plugin adds a field called Geolocation tracked to the User [sys_user] table. This field allows the system to track individual users by their geographical coordinates.

### Business rules installed with geolocation

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GeoLocation Data updated</td>
<td>User (sys_user)</td>
<td>Populates the Latitude and Longitude fields on the GeoLocation History (geo_history) table when the Latitude and Longitude fields are updated on the User (sys_user) table.</td>
</tr>
</tbody>
</table>

### Client scripts installed with geolocation

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update Geolocation on Task</td>
<td>Task (task)</td>
<td>Populates the Latitude and Longitude fields on a user record with GPS coordinates when that user loads any record on the Task table or a table that extends Task. This occurs only when geolocation tracking is enabled for the user.</td>
</tr>
</tbody>
</table>

### Properties installed with geolocation

Geolocation provides the following configurable properties in Geolocation > Administration > Geolocation Properties.

The Google Maps plugin provides additional map properties that are used to implement and control specific geolocation features. You must have a private key for Google Maps API for Business to take advantage of the properties listed here.
## Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.geolocation.allow.toll.roads</td>
<td>Allow toll roads to be used. Allows the system to use toll roads when auto-routing an agent’s tasks.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Type</strong>: True/false  &lt;br&gt;   - <strong>Default value</strong>: True</td>
</tr>
<tr>
<td>glide.geolocation.default.start.time</td>
<td>Default start time for all agents when no schedule is set. This value sets the start time for a day other than the current day, when no scheduled task exists or is continued from the previous day. This property uses a 24 hour clock.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Type</strong>: String  &lt;br&gt;   - <strong>Default value</strong>: 08:00</td>
</tr>
<tr>
<td>glide.geolocation.evening.rush.hours</td>
<td>Evening rush hour span, formatted as 14:30-16:00. All times are expressed as a range, separated by a dash with no spaces. Times not using this format are ignored. This property must be used with the work.management.morning.rush.hours and work.management.rush.travel.buffer properties and uses a 24 hour clock.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Type</strong>: String  &lt;br&gt;   - <strong>Default</strong>: 0</td>
</tr>
<tr>
<td>glide.geolocation.history.cleanup</td>
<td>Number of days to keep history data. ServiceNow keeps agent geolocation history records for the number of days specified by this value.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Type</strong>: Integer  &lt;br&gt;   - <strong>Default value</strong>: 30</td>
</tr>
<tr>
<td>glide.geolocation.morning.rush.hours</td>
<td>Morning rush hour span, formatted as 06:30-08:00. This property uses a 24 hour clock. All times are expressed as a range, separated by a dash with no spaces. Times not using this format are ignored. This property must be used with the work.management.evening.rush.hours and work.management.rush.travel.buffer properties.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Type</strong>: String  &lt;br&gt;   - <strong>Default</strong>: 0</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>glide.geolocation.proximity</td>
<td>Minimum distance an agent must move to be considered in a new location (in meters). This setting establishes a geolocation perimeter that prevents ServiceNow from creating unnecessary history records when an agent has multiple tasks in the same vicinity. An example of this might be when an agent has several tasks in one building. The system assumes that all task activity within the specified radius is part of a single record and does not create additional records when the agent moves from task to task around the building.</td>
</tr>
<tr>
<td>glide.geolocation.proximity.location</td>
<td>Maximum distance an agent can be from a specific location and still be placed at that location (in meters). This setting defines the maximum distance that an agent can be from a specified location and still be placed at that location by the system.</td>
</tr>
<tr>
<td>glide.geolocation.rush.travel.buffer</td>
<td>Percentage to add to all rush hour travel times. The system uses this percentage to calculate schedules when auto-routing an agent. Use this property when both morning and evening rush hour times are defined. An example of a valid time buffer percentage is 15.</td>
</tr>
<tr>
<td>glide.geolocation.tracking.frequency</td>
<td>Sets the length of the recurring interval, in seconds, that the system waits between attempts to update a user’s geographic coordinates. The system updates geographic coordinates only for users who have geolocation tracking enabled. Minimum amount of time between updating the user’s location (in seconds). This setting defines how long the system waits before updating an agent’s location, regardless of task activity or travel. This prevents ServiceNow from creating unnecessary history records if an agent in one location views a task multiple times.</td>
</tr>
<tr>
<td>glide.geolocation.travel.buffer</td>
<td>Percentage to add to all travel times. An example of a valid percentage value is 15.</td>
</tr>
</tbody>
</table>
### glide.geolocation.work.spacing

Amount of time (in minutes) to add between the end of a task and the travel start of the next. An example of a valid time value is 10.

- **Type:** Integer
- **Default value:** 0

### Geolocation Google key

Geolocation requires a Google Maps API for Business license to enable the use of Google driving time estimates and to use Google Maps. Applications, such as Work Management, have functionality that requires this license.

If you are using auto-routing or auto-dispatch in Work Management, both the Google Maps API for Business private key and the client ID must be set for precise time estimates. Without these values, driving times for auto-routing and auto-dispatch are not available, and a rough estimate or fixed time is used. Use these properties, found in **System Properties > Google Maps**, to enable the geolocation feature.

- **Client ID for Google Maps API for Business:** Google client ID for your organization. This ID is from Google and starts with `gme-`, such as `gme-mycompanyname`.
- **Private key for Google Maps API for Business:** Key required to get accurate driving time estimates from Google for some features of Geolocation. An example of an encoded key is: `vNIXE0xscrmjlyV-12Nj_BvUPaw=`

### Geolocation history

The Geolocation History (geo_history) table contains the history of each tracked user's location over time. To view geolocation history, navigate to **Geolocation > Geolocation History**. The record list shows time stamped location data for all users configured for geolocation tracking.

The following system properties, located in **Geolocation > Administration > Geolocation Properties**, control the data that appears in this table.

- **Minimum distance an agent must move to be considered in a new location (in meters):** Perimeter that defines a single location in which multiple tasks are present. This property prevents the system from creating unnecessary history records when multiple tasks are in the same general location.
- **Maximum distance an agent can be from a specific location and still be placed at that location (in meters):** Distance that a user can be from a specified location and still be placed at that location when the system creates history data.
- Number of days to keep history data: Time period for which the system retains history data.
- Minimum amount of time between updating the user’s location (in seconds): Time period the system waits before updating a user’s location, regardless of how often the user accesses tasks.

**Location tracking**

Geolocation adds the **Geolocation tracked** field to the User form. In the default view of a user record, select the **Geolocation tracked** check box to enable location tracking for the user.

When a user has geolocation tracking enabled, the system updates the user’s geographic coordinates whenever the user opens, or loads, a record from the Task (task) table or from a table that extends Task. After this initial update, the system continues to update the user’s geographic coordinates at a recurring interval if the user does not close or reload the record. To edit the length of this interval, navigate to **Geolocation > Administration > Geolocation Properties** and change the setting for the **property** that regulates the update interval for the user’s location. The default setting for this property is **300** seconds (5 minutes).

**Note:** The system can update geographic coordinates only for users who have location services enabled in their browsers. Even users who have the **Geolocation tracked** check box selected may be prompted by their browsers to share or withhold their location.

**State flows**

State flows enable an administrator to customize transitions from one state to another in tables derived from the Task (task) table and configure the system to perform work during transitions to specific states.

An example of a state transition is when the **State** field in an incident changes from **Active** to **Awaiting User Info**. An administrator might want to trigger an event during this transition or make a specific field mandatory when the incident reaches the end state.

State transitions in the Field Service Management application were reimplemented to use state flows. For information about customizing Field Service Management state flows, see **State flow customization**.

**Installed with state flows**

Several types of components are installed with state flows.

**Tables installed with state flows**

**Tables**

State flows adds the following tables.

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State Flow (sf_state_flow)</td>
<td>Contains state flow definitions. This table contains all state flow definitions, including those for work orders and work order tasks.</td>
</tr>
</tbody>
</table>
### Business rules installed with state flows

### Business rules

State flows adds the following business rules.

#### Business rules for state flows

<table>
<thead>
<tr>
<th>Business rule</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assert Field Uniqueness in State Flow</td>
<td>State Flow (sf_state_flow)</td>
<td>Ensures that business rules and UI actions are not accidentally copied to new state flows.</td>
</tr>
<tr>
<td>Check Client Script</td>
<td>State Flow (sf_state_flow)</td>
<td>Adds a client script to new records.</td>
</tr>
<tr>
<td>Check Event Rule</td>
<td>State Flow (sf_state_flow)</td>
<td>Adds or deletes event rules, as the event field is updated.</td>
</tr>
<tr>
<td>Check Work Notes Rule</td>
<td>State Flow (sf_state_flow)</td>
<td>Adds or deletes work note rules, as the work notes for a state flow are updated.</td>
</tr>
<tr>
<td>Create Business Rule</td>
<td>State Flow (sf_state_flow)</td>
<td>Automatically creates a business rule when automatic conditions or script are present.</td>
</tr>
<tr>
<td>Create script for Field controls</td>
<td>State Flow (sf_state_flow)</td>
<td>Create scripts for field controls, when they are in use.</td>
</tr>
<tr>
<td>Create UI Action</td>
<td>State Flow (sf_state_flow)</td>
<td>Automatically creates a UI action when manual conditions or script are filled in.</td>
</tr>
<tr>
<td>Delete Related Elements</td>
<td>State Flow (sf_state_flow)</td>
<td>When state flows are deleted, delete all related client scripts, business rules, UI actions and overrides.</td>
</tr>
<tr>
<td>Remove script for Field controls</td>
<td>State Flow (sf_state_flow)</td>
<td>If all field controls are disabled, see if any of the client scripts should be removed.</td>
</tr>
<tr>
<td>State Change</td>
<td>State Flow (sf_state_flow)</td>
<td>Get the correct state choice value when the state is changed.</td>
</tr>
</tbody>
</table>
### Business rule | Table | Description
--- | --- | ---
Update dependent records | State Flow (sf_state_flow) | When a state flow is made active or inactive, ensure the business rule and UI actions are made active or inactive as well.

**Script includes installed with state flows**

**Script includes**

State flows adds the following script includes.

**Script includes for state flows**

<table>
<thead>
<tr>
<th>Script include</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>StateFlow</td>
<td>Implements state flows and supports creation of state flow elements, such as business rules, UI actions, dictionary overrides, and client scripts.</td>
</tr>
<tr>
<td>StateFlowAJAX</td>
<td>Allows access to state flow functionality from client scripts.</td>
</tr>
</tbody>
</table>

**Use state flows**

You can create custom state flows for any table that uses states.

Make state transitions occur in any order or skip specific states according to your business practices. State flows can manage the behavior of fields and field visibility on a task form. State flows can also trigger system events that perform work such as sending email notifications.

Administrators can configure state flows to:

- Limit the choice list for the State field to contain only those states that are valid for the flow.
- Define the behavior and visibility of specific fields using field controls on a task form when state transitions occur and for certain end states.
- Configure events that are triggered when a task changes states.
- Set up UI actions and business rules to implement certain state transitions, or while the task is in certain states.

The State Flow plugin installs records used by work management to control state transitions for work orders and work order tasks. For detailed information about using work management state flows, see State flow customization.

Creating and customizing state flows requires scripting knowledge. Users with the admin role can create state flow records.

**Dictionary overrides for state flows**

A dictionary override in a state flow defines the starting state for all new records in a specific table.

You set an override in tables that extend a base table only, so that your customizations are applied only to the extended table.
1. In a state flow record, select an **Ending state**.
   This is the override value which becomes the starting state for all new records in the table named.

2. Click **Create Default Value**.
   The system populates the Dictionary override field with a value of state, which is the field in the task table affected by the override. The Dictionary override field is read-only. After the override is created, the system hides the **Create Default Value** button on all subsequent state flow forms for that table.

**Events triggered on state changes**

You can configure a state flow to trigger a registered system event when a task transitions from a starting state to a specified end state.

For example, you can use events to trigger email notifications and create script actions. When you attach an event to a state flow, the system creates a business rule called State Flow Events for `<table name>` for the table specified in the state flow. If you specify a start and end state, the business rule executes when the record transitions from the start state to the end state. If the state flow only specifies an end state, the business rule executes whenever that end state is reached.

The system creates one business rule for all state flows containing events on a single table. When all events or all state flows on a table are deleted, the system deletes the business rule.

**Field controls**

You can define controls for individual fields that are enforced when a record transitions between states.

Settings in the Field Controls section of the State Flow form enable you to apply field controls when the system detects a specified state transition or when the end state is the current state when the form is opened. The control is applied only to existing fields on the form. State flows cannot add fields to the form.

For example, you might want the Problem field to be visible when an incident moves to the Awaiting Problem state. If the incident state changes to Awaiting User Info, you hide the Problem field and make the Caller field mandatory.

The best practice when creating field controls is to configure state flow records with an ending state only and to create the correct behavior for every ending state you want to control. This ensures that the field controls are set properly when the user selects a new state, and also when the user returns a record’s State field to the original state. Only specify a full state transition, with both a starting and ending state, when you want a particular behavior for that precise state transition.

**Note:** State flows use client scripts to enforce field controls. It is possible that your settings can be changed by existing UI policies, which execute after client scripts.

The system creates the following objects as needed to enforce field properties in state flows:
### Field Controls

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business rule</td>
<td>State Flow Notes for <code>&lt;table name&gt;</code></td>
<td>Enforces mandatory fields for the table on which that field behavior is defined.</td>
</tr>
<tr>
<td>Client script (onLoad)</td>
<td><code>&lt;table name&gt;</code> state flow</td>
<td>Sets possible states and initial mandatory, read-only, and visible properties when a record is loaded.</td>
</tr>
<tr>
<td>Client script (onChange)</td>
<td><code>&lt;table name&gt;</code> change state flow</td>
<td>Sets updated mandatory, read-only, and visible properties when a record is changed.</td>
</tr>
</tbody>
</table>

### Rebuild state flows

You can rebuild state flows when a mismatch between existing and new sys_ids occurs. When you use an XML file to import a state flow record into an instance, the system attempts to match the incoming states with existing states by comparing sys_ids. Because the sys_ids of items in a choice list can vary between instances, the system can fail to match the states, even though they are otherwise identical.

When matching fails, the start and end states of affected records are left blank or contain numeric values. To repair these records navigate to State Flows > Admin > Rebuild State Flows. This module runs a script that compares the numerical value of each item in the State field choice list until it finds a match in the imported state flow record.

### Create a state flow

Creating State Flows.

2. Fill in the fields, as appropriate.

   The system enforces the field controls with the same client script that filters the choice list for the State field.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client script</td>
<td>Client script to run for this transition. The client script controls the available states you can select by limiting the contents of the State choice list to valid states. This client script also controls specific field behavior configured for state changes in the Field Controls section of the form.</td>
</tr>
<tr>
<td>Event</td>
<td>Name of an existing event to trigger when this transition occurs. See <a href="#">triggering events on state flow changes</a> for more information.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of this record. Make sure the name is descriptive of the state transition or the processing that the record is performing. This name does not have to be unique.</td>
</tr>
<tr>
<td>Roles</td>
<td>Not used for any processing.</td>
</tr>
<tr>
<td>Active</td>
<td>Enables or disables this state flow record.</td>
</tr>
<tr>
<td>Class</td>
<td>Defines the state flow class for this record. The system selects the appropriate class from these options:</td>
</tr>
<tr>
<td></td>
<td>• State Flow: Records created for state flows in all task-based tables except those in work management.</td>
</tr>
<tr>
<td></td>
<td>• Work Order Flow: Records created for state flows in the Work Order [wm_order] table. This class is available when work management is activated.</td>
</tr>
<tr>
<td></td>
<td>• Work Task Flow: Records created for state flows in the Work Order Task [wm_task] table. This class is available when work management is activated.</td>
</tr>
<tr>
<td>Dictionary override</td>
<td>Sets the starting value for the State field on all new records for the table named in the state flow record. See <a href="#">dictionary overrides</a> for configuration procedures.</td>
</tr>
<tr>
<td>Work notes</td>
<td>Noteworthy comments about this state flow transition. For details about how these notes are used, see <a href="#">Work Notes</a>.</td>
</tr>
<tr>
<td>Comment</td>
<td>Details about the customized record.</td>
</tr>
<tr>
<td>Manual (Runs scripts from a UI action that require the user to click a button or related link.)</td>
<td></td>
</tr>
<tr>
<td>Manual condition string</td>
<td>Conditions for enabling a UI action that cannot be defined with the condition builder. For example, you can use this string to define UI actions for mobile devices. This condition has an (and) relationship with the condition in the Manual condition field.</td>
</tr>
<tr>
<td>Manual condition</td>
<td>Conditions for enabling a UI action that can be defined for fields in the target table. This condition has an (and) relationship with the condition in the Manual condition string field.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Manual script</td>
<td>Script that defines what the UI action does when the conditions are true. This script runs when the user clicks a button or a related link.</td>
</tr>
<tr>
<td>UI action</td>
<td>(Read Only) Name of the button that the system creates to enable this transition. The system creates the label using the same name as the state flow record that created it.</td>
</tr>
<tr>
<td>Automatic (Runs a business rule automatically when a task record is changed and updated.)</td>
<td></td>
</tr>
<tr>
<td>Automatic condition string</td>
<td>Conditions for running the business rule that cannot be defined with the condition builder, such as evaluating if the proposed transition is a valid flow. This condition has an (and) relationship with the condition in the Automatic condition field.</td>
</tr>
<tr>
<td>Automatic condition</td>
<td>Conditions for running the business rule that can be defined for fields in the target table. This condition has an (and) relationship with the condition in the Automatic condition string field.</td>
</tr>
<tr>
<td>Automatic script</td>
<td>Script that performs additional work when the condition is true. This script can do tasks such as update the date and time the transition occurred or notify someone using email when a specific state change occurs. Automatic state transitions occur when changes are made to the task record.</td>
</tr>
<tr>
<td>Business rule</td>
<td>Name of the business rule created for this transition. Two conditions must be satisfied before this business rule can run. The task must be on a specific starting state, and the Automatic condition must be true. If both of these conditions are satisfied, the business rule performs the transition requested, using the starting and ending states from the State Flow form.</td>
</tr>
<tr>
<td>Field Controls (Determines field properties when a record transitions between states or reaches a specific end state.)</td>
<td></td>
</tr>
<tr>
<td>Mandatory fields</td>
<td>Makes the selected fields required when this transition occurs, or when the end state is the current state.</td>
</tr>
<tr>
<td>Read only fields</td>
<td>Prevents the selected fields from being edited when this transition occurs, or when the end state is the current state.</td>
</tr>
<tr>
<td>Visible fields</td>
<td>Displays the selected fields when this transition occurs, or when the end state is the current state.</td>
</tr>
<tr>
<td>Not mandatory</td>
<td>Makes the selected fields optional when this transition occurs, or when the end state is the current state.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Not read only</td>
<td>Makes the selected fields editable when this transition occurs, or when the end state is the current state.</td>
</tr>
<tr>
<td>Not visible</td>
<td>Hides the selected fields when this transition occurs, or when the end state is the current state.</td>
</tr>
</tbody>
</table>

3. Determine if you want the state transition method to be manual or automatic and open the appropriate section on the form.
   - Manual: Click **Create UI Action** to create a button on the task form that enables users to execute the transition manually. The system uses the value in the Name field as the label for the UI action. The UI action executes the script in the Manual Script field when the conditions are true. For example, a manual transition can create an **Activate** button when an incident is in the New state that enables a user to mark the incident as active.
   - Automatic: Click **Create Business Rule** to create the business rule. The business rule executes the script in the Automatic Script field when the conditions are true. For example, a business rule created by the system can set an incident state to Assigned when the Assigned to field is populated. Business rules are automatically deleted when the state flow record is deleted. For more information, see **Business Rules**.

4. Optional: Click **Create Client Script** to create the script that limits the values offered in a task record’s State field to valid states for that transition.

5. Configure the fields in the Field Controls section to control how specific fields display when a task record changes states.

**State flow cleanup**

The business rules, client scripts, and UI actions that the system creates automatically to perform custom transitions exist only while the state flow records that use them are present.

When all the state flows on a table are deleted, the system attempts to delete any unnecessary programming elements that were created on that table, using these criteria:

<table>
<thead>
<tr>
<th>Element</th>
<th>Deleted When</th>
</tr>
</thead>
<tbody>
<tr>
<td>UI action</td>
<td>The state flow that created it is deleted.</td>
</tr>
<tr>
<td>Business rule</td>
<td></td>
</tr>
<tr>
<td>Dictionary override</td>
<td></td>
</tr>
<tr>
<td>Business rule that processes events triggered by a state flow</td>
<td>All state flows for the table specified that have events configured are deleted.</td>
</tr>
<tr>
<td>Client script (onLoad)</td>
<td>All state flows for the table are deleted.</td>
</tr>
<tr>
<td>Client script (onChange)</td>
<td>All state flows with field controls are deleted.</td>
</tr>
<tr>
<td>Work notes business rule</td>
<td>All state flows with field controls or work notes are deleted.</td>
</tr>
</tbody>
</table>

**Work notes**

Work notes are an important part of the state flow process and are used to communicate information about state transitions.

© 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 state flow adds these work notes to the Work notes field of any task making this transition. These rules apply to state flow work notes:

- For a state flow with no Starting state, the work note is added every time the task transitions to the Ending state.
- For a state flow with a Starting state and an Ending state, the work note is added only when the task transitions from that starting state to that ending state.
- If two state flows with work notes have the same Ending state, but only one has a Starting state, the system adds the work notes from the state flow with the starting state. This better matches the state flow work note to the more important transition between specific starting and ending states.

Survey Management

With the ServiceNow® Survey Management application you can create, send, and collect responses for basic surveys. If installed, you can also use the Survey widget to set up a survey within Service Portal.

Explore
- Assessments and Surveys release notes
- Upgrade to Jakarta
- Get started with Survey Management
- Key survey terms

Set up
- Survey Management roles

Administer
- Survey designer
- Survey users and groups
- Customize the appearance of a survey
- Survey definitions
- Survey trigger conditions

Use
- View the results for a survey
- View results for all surveys
- Metric result fields
- View a survey scorecard
- Survey questionnaires

Develop
- Developer training
- Developer documentation

Migrate
- Legacy survey migration

Troubleshoot and get help
- Ask or answer questions in the IT Service Management forum
- Search the HI Knowledge Base for known error articles
- Contact ServiceNow Technical Support

Get started with Survey Management

Two versions of the application are supported, Survey Management, which is the latest version, and Legacy Surveys. Survey Management improves the user interface and extends the capabilities of the Legacy Surveys application.

Survey Management does not support domain separation.
Configuring surveys

There are many options for advanced configuration in Survey Management:

- Create a survey, add questions, and choose recipients, all in one interface.
- Create conditional questions, which appear only when users answer other questions a certain way.
- Restrict a survey so only specific survey users can take it, and send invitations to those users simultaneously. Alternatively, make the survey a public survey so that any user can take the survey, even users who have not logged in to the ServiceNow system.
- Set a schedule to automatically assign a survey to users and to limit how often the same user can take a survey.
- Customize the look and feel of survey questionnaires.
- Save anonymous survey responses.
- Convert survey responses to numerical scores and view them on scorecards.
- Deactivate a survey for maintenance or to retire it without deleting it.

**Note:** Because surveys use the same tables and other back-end components as assessments, you may see assessment elements such as table and field names in certain places throughout the survey feature.

Legacy Surveys

Survey administrators can continue to use legacy survey functionality and data, however, it is recommended that you migrate legacy surveys to the Survey Management application. Concurrent use of both survey applications can cause confusion and redundancy.

Survey wizards are not impacted and cannot be migrated.

**Note:** The Legacy Surveys application is not described in the documentation that you are viewing. It is documented on the ServiceNow wiki.

Version comparison

<table>
<thead>
<tr>
<th>Capability</th>
<th>Surveys</th>
<th>Legacy Surveys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Surveys in Service Portal.</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Save new survey responses each time a user takes the same survey.</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Create question templates to reuse sets of answer options.</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Categorize survey questions and report on category results.</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Deactivate a survey without deleting it.</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Capability</td>
<td>Surveys</td>
<td>Legacy Surveys</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
</tr>
<tr>
<td>Create conditional questions.</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>Send surveys automatically based on a schedule.</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>Customize survey questionnaire color scheme.</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>Save anonymous survey responses for logged-in users.</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>View survey responses on graphical scorecards.</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>Save surveys in a draft state until they are ready to publish.</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>Create and send surveys from one page.</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>Allow only specific users to access a survey.</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>Send surveys based on conditions.</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>Send survey email notifications.</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>Limit how often a user can take the same survey.</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>Add introduction and end note text.</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>Create survey modules.</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>Public survey: Allow persons to take a survey without logging in.</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>Use update sets to track changes.</td>
<td>✅</td>
<td></td>
</tr>
</tbody>
</table>

**Survey Management roles**

The Survey Management application uses the following roles.

No role is required to take assigned survey questionnaires.
Survey Management roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
<th>Contains roles</th>
</tr>
</thead>
</table>
| Survey administrator      | Create and administer surveys. Survey administrators know what types of surveys are necessary, when to send a survey, and to whom. Survey administrators can use all modules in the Survey application menu.          | • survey_reader  
• assessment_admin |
| Survey reader             | View surveys and related information, such as survey responses, survey groups, scorecards, and reports.                                                                                                     | none                                  |

Key survey terms

These survey terms are used throughout the documentation to describe survey management functions and capabilities.

Key survey terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Survey definition</td>
<td>Root record on which a survey is built. A survey definition contains information such as the survey name, state, and distribution schedule. Each survey definition has its own categories and questions. Survey definitions are comparable to legacy survey masters.</td>
</tr>
<tr>
<td>Public survey</td>
<td>Any user can take a public survey, even users who have not logged in to the ServiceNow system. For a completed survey, the Assigned to field value is Guest.</td>
</tr>
<tr>
<td>Survey category</td>
<td>Represents a theme for survey questions. Categories contain one or more questions. The system creates one category per survey by default. Additional categories are optional.</td>
</tr>
<tr>
<td>Survey question</td>
<td>A question that appears on a survey questionnaire for the associated survey definition. Survey questions are comparable to legacy survey questions.</td>
</tr>
<tr>
<td>Survey user</td>
<td>User who is authorized to receive invitations for a restricted survey.</td>
</tr>
<tr>
<td>Survey instance</td>
<td>Represents one survey questionnaire assigned to one user. Survey instances are comparable to legacy survey instances.</td>
</tr>
</tbody>
</table>
## ServiceNow

### Jakarta

### Now Platform Capabilities

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trigger condition</td>
<td>Defines a rule that enables the system to send a survey when an action occurs on a table, such as when an incident closes. Trigger conditions are comparable to legacy survey conditions.</td>
</tr>
<tr>
<td>Scorecard</td>
<td>Visual representation of survey responses. Scorecards display a variety of data summaries for one survey definition.</td>
</tr>
</tbody>
</table>

### Survey questionnaires

All surveys that are assigned to you appear in your personal assessment and survey queue.

No special role is required to complete a survey but you must be logged in and the survey must be assigned to you. When you submit a survey, the system stores your responses.

### Survey notification

If the system is configured to send email, it sends you a notification when a survey is assigned to you. The message contains a link to the survey and instructions for viewing the assessment and survey queue.

**Take a survey**

Surveys that are assigned to you, and that are not complete, appear in your assessment and survey queue.

**Role required:** none

Each assessment or survey appears as a card in the queue. The card contains helpful information, including the survey name, state, and due date, and a button to launch the questionnaire. Overdue surveys are clearly marked with a red icon and red due date. You must answer every mandatory question, indicated by a red asterisk, before you can submit the survey. If you start to take a survey but cannot complete it, save your responses and return to it later. When you have answered all the questions and are satisfied with the responses, submit the survey.

1. Navigate to **Self-Service > My Assessments & Surveys**.
   Users with the assessment_admin role, including survey administrators, can display other users’ assessments and surveys in addition to their own. Use the **Show all** and **Show assigned to me** related links at the bottom of the queue to show and hide assessments and surveys. Click a card assigned to another user to open the associated metric type or survey definition.

2. Click **Take Survey** on a survey card to open the questionnaire.
   If there is more than one survey category, you can click the collapse or expand icon to hide or show the questions in the category.

3. Answer each question to the best of your ability.
   If you are unsure of how to respond to a question or if a question does not apply to a particular record, select **Not Applicable**, if available.

4. Complete one of the following steps.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save your responses without submitting them</td>
<td>Click Save. You can close the questionnaire and access it later from your queue. Note: The system does not save the survey if there are invalid responses, such as a letter in a date field. You must enter valid responses or remove invalid responses before you can save the survey.</td>
</tr>
<tr>
<td>Submit the survey after answering all questions</td>
<td>Click Submit. You cannot return to the questionnaire after submitting. Note: If there is an unanswered mandatory question or an invalid response, an error message appears and the problematic questions are temporarily highlighted.</td>
</tr>
</tbody>
</table>

**Survey responses and results**

There is a metric result record for each user response to each question on every survey instance. Survey results for each question and category are calculated automatically based on the metric result records.

If you use survey result calculations for results and scorecards, ensure that the positive indicator field for the question is set appropriately, based on the answer options. To have any results, a category must contain scored questions.

**Survey responses**

Survey responses are stored in the Metric Result (asmt_metric_result) table and display the recipients' answers to each question in a category. To view general results, navigate to Survey > Survey Responses. To view results for a particular criterion, use a filter on the Metric Result (asmt_metric_result) table. For example, to view results based on the assignment group, apply a filter condition for assignment group.
Survey metric results

Category results

Category results are stored in the Assessment Category Result (asmt_category_result) table and display the overall ratings for each category based on the weighted value for each scored question. To view these results, navigate to Assessments > Results > Category results and filter the results using the (Type.Evaluation method) (is) (Survey) condition.
Assessment category results

Survey scorecards

A scorecard provides a visual breakdown of survey responses, based on the way questions were answered, by category. To access a scorecard, see View a survey scorecard.

View results for all surveys

You can view the survey responses that are stored on the Metric Result (asmt_metric_result) table.

Role required: survey_admin or survey_reader

1. Navigate to Survey > Survey Responses.
   Do not confuse this module with Survey > Legacy Surveys > Survey Responses, which displays legacy survey responses.
   The Type column displays the survey definition each response is associated with.
2. Select a response to view its details.

**View the results for a survey**

You can view the responses for one survey definition. Survey results are stored on the Metric Result (asmt_metric_result) table.

Role required: survey_admin or survey_reader

1. Navigate to Survey > View Surveys
2. Open a survey definition.
3. Under Related Links, click View Responses, which is available only if there are results.
   The results are grouped by metric, which is what questions are called in assessments.
4. Open a metric result to view more detail.
   The metric result contains the user’s response and calculated values of interest to advanced survey administrators. Because the Metric Result table is also used by the assessment feature, many field names are not clear in the context of surveys.

**Metric result fields**

List of field descriptions for the Metric Result form.
# Metric Result form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment group</td>
<td>Assessment group to which the metric result belongs. An assessment group is a container for survey instances and results generated in a single occurrence. The system generates an assessment group every time at least one survey instance is created. If multiple survey instances are created at once, such as when a survey administrator sends invitations to a list of survey users, they are all stored in the same assessment group.</td>
</tr>
<tr>
<td>Metric</td>
<td>Question that the user answered.</td>
</tr>
<tr>
<td>Data type</td>
<td>Data type of the question the user answered.</td>
</tr>
<tr>
<td>Method</td>
<td>Assessment method. Always Assessment for surveys.</td>
</tr>
<tr>
<td>Updated</td>
<td>Date and time the metric result was last updated.</td>
</tr>
<tr>
<td>Source</td>
<td>Survey definition from which the associated survey instance was generated.</td>
</tr>
<tr>
<td>Assigned to</td>
<td>User who completed the survey questionnaire.</td>
</tr>
<tr>
<td>Instance</td>
<td>Survey instance completed by the Assigned to user.</td>
</tr>
<tr>
<td>Actual value</td>
<td>Value obtained from the user response to the question. The actual value is determined by the question data type:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Checkbox</strong>: The actual value is 0 if the check box is cleared and 1 if it is selected.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Choice</strong> or <strong>Likert Scale</strong>: The actual value is equal to the Value of the metric definition associated with the chosen answer option.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Date, Date/Time, or String</strong>: The actual value is -1 to indicate that these data types do not contribute to category result calculations.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Template</strong>: The actual value is equal to the Value of the template definition associated with the chosen answer option.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Yes/No</strong>: The actual value is 0 if the response is No and 1 if it is Yes.</td>
</tr>
<tr>
<td>Normalized value</td>
<td>Adjusted value that accounts for the Scale definition setting, minimum and maximum values, and other factors.</td>
</tr>
<tr>
<td></td>
<td>The equation that generates the value and an example calculation appear in Example: calculate the normalized value for a survey metric.</td>
</tr>
<tr>
<td>String value</td>
<td>Value that displays the response as it appears on a questionnaire. In some cases this is the same as the Actual value, such as when the question data type is Percentage. The string value is N/A for unanswered questions of certain data types.</td>
</tr>
</tbody>
</table>
Example: calculate the normalized value for a survey metric
The normalized value is calculated based on a linear equation and the scale definition of the metric.

Equation used to calculate the normalized value

Normalized value = (Input Value - Min value defined in metric) / (Max value defined in metric - Min value defined in metric) * current metric weight / (sum of valid metric weight) * scale_factor

Note: The normalized values are directly proportional to the scale definition of the metric. If the scale definition is low, that is, the lower scale values are better, then Normalized value = 1.0 - Normalized value.

Example
Calculate the normalized value for the Please rate the competency of the technician metric. The metric has the following values:

<table>
<thead>
<tr>
<th>Values of the metric</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Input value</td>
<td>3</td>
</tr>
<tr>
<td>Minimum value</td>
<td>1</td>
</tr>
<tr>
<td>Maximum value</td>
<td>6</td>
</tr>
<tr>
<td>Current metric weight</td>
<td>10</td>
</tr>
<tr>
<td>Number of responses</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>• 4 of type=number</td>
</tr>
<tr>
<td></td>
<td>• 1 of type=yes/no</td>
</tr>
<tr>
<td></td>
<td>• 1 of type=string (invalid data type; value cannot be calculated)</td>
</tr>
<tr>
<td>Valid metric weight of each response</td>
<td>10</td>
</tr>
<tr>
<td>Scale factor</td>
<td>10</td>
</tr>
</tbody>
</table>

Normalized value = (3 - 1) / (6 - 1) * 10 / (10 + 10 + 10 + 10 + 10) * 10 = 0.8

Several data types are ignored because the values cannot be calculated. These invalid data types include string, date, and datetime.

For reporting purposes, use the Metric Result (asmt_metric_result) table.

View a survey scorecard
A survey scorecard provides a visual breakdown of survey responses by category, based on the way questions were answered.

Role required: survey_admin or survey_reader
A scorecard displays charts for survey results, in which category and question responses are analyzed and current ratings are compared with previous ratings. Users can examine ratings over time, compare question ratings, or compare the ratings of all categories. All ratings are averages.
for the time range selected. The system dynamically updates a scorecard each time you view it, so the ratings reflect recently completed surveys.

1. Navigate to Survey > View Surveys.
2. Open a survey definition.
   The scorecard link is hidden if there are no survey results to report.

The interactive scorecard displays the name of the survey and results or comparisons of the ratings. You can display results in the following views:

- Category Results
- Question Results
- Average Ratings
- History

Survey scorecard category results
The Category Results view is a stacked bar chart showing survey results for all questions in a category by respondent count.

Select a category from the list to display the questions from that category in the chart.

This view displays responses that use the following data types:

- Checkbox
- Choice
- Likert Scale
- Number
- Template
- Yes/No

**Note:** The Checkbox and Yes/No data types are combined into the **Boolean** data type in the Survey Designer
To view details about a specific response, point to the colored bar to display the response, the number of responses, and the percentage it represents of all the responses to that question.

Survey scorecard category results detail

Survey scorecard question results
The Question Results view shows the results for each question in a category using different chart types, based on a data type.

Pie chart

The pie chart shows question results for these data types:

- Checkbox
- Choice
- Likert Scale
- Number
- Template
- Yes/No

Note: The Checkbox and Yes/No data types are combined into the Boolean data type in the Survey Designer.
Service Desk Satisfaction Survey

Survey Scorecard

How courteous and respectful was the technician who responded? (1=poor, 6=excellent)

- 2 = 2 (14.29%)
- 3 = 2 (14.29%)
- 4 = 9 (64.29%)
- 5 = 1 (7.14%)

© 2020 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.
Bar chart

A bar chart appears when question results use the Percentage data type.

By default, all results for percentage questions use a report range of 20% segments. To configure a report range, navigate to Reports > Administration > Report Ranges.

Survey scorecard average ratings

The Average Ratings view displays the weighted average rating for each survey question in a category.

Use this view to learn how individual questions affect the overall rating for the category. Select a survey category from the choice list to display the chart for that category.
Service Desk Satisfaction Survey

Survey Scorecard

Average question rating in category: Service Desk Satisfaction Survey

How courteous and...  
How satisfied are...  
How satisfied wer...  
Please rate the t...  
Was technician ab...  

Average Normalized value
To view the effect of each question's ratings on the entire category's ratings, point to the colored bar. The pop-up box shows the percentage of the total ratings represented by each individual question's weighted average.

**Average ratings detail**

**Survey scorecard history**

The History view compares the current ratings for the categories and their questions with ratings from the previous three years or four quarters.

Ratings that have declined are highlighted in red and display negative numbers. Ratings that have improved are highlighted in green with positive numbers. Arrow icons beside the values in the Diff column indicate the trend of the current survey against the previous survey.

Point to a category to display a line chart that shows the rating trend for that category. Click a category to view the Survey Category form containing the survey questions.
Survey scorecard trend chart

3 years

To calculate the current ratings, the system averages the ratings from the trailing twelve month (TTM) period. The Diff column shows the discrepancy between the current ratings and the previous calendar year’s ratings.
<table>
<thead>
<tr>
<th>Survey Scorecard</th>
<th>Overall Rating</th>
<th>Current</th>
<th>Diff</th>
<th>2013</th>
<th>2012</th>
<th>2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Desk Satisfaction Survey</td>
<td>5.40</td>
<td>0.00</td>
<td>5.40</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>How satisfied were you with the response time to your incident? (1=not at all, 6=completely)</td>
<td>0.00</td>
<td>-1.02</td>
<td>3</td>
<td>1.02</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>How courteous and respectful was the technician who responded? (1=poor, 6=excellent)</td>
<td>0.00</td>
<td>-1.21</td>
<td>3</td>
<td>1.21</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Please rate the technical competency of the technician serving you (1=poor, 6=excellent)</td>
<td>0.00</td>
<td>-1.02</td>
<td>3</td>
<td>1.02</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Was technician able to resolve your issue during the first call?</td>
<td>0.00</td>
<td>-1.00</td>
<td>4</td>
<td>1.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>How satisfied are you with your overall service experience? (1=not at all, 6=completely)</td>
<td>0.00</td>
<td>-1.14</td>
<td>3</td>
<td>1.14</td>
<td>0.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>

Survey scorecard history - 3 years

© 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.
4 quarters

Quarterly surveys compare the average rating for each question and category in the current quarter against the average ratings from the previous four quarters. The Diff column shows the discrepancy between the current ratings and the previous quarter's ratings. The column labels count backward, by quarter from the current quarter. For example, if the current quarter is the 3rd quarter of 2015, then the previous quarters appear as 2nd (2015), 1st (2015), 4th (2014), and 3rd (2014). All four of the previous quarters appear, whether or not there was any data for those quarters.
### Service Desk Satisfaction Survey

<table>
<thead>
<tr>
<th>Overall Rating</th>
<th>Current</th>
<th>Diff</th>
<th>1st</th>
<th>4th</th>
<th>3rd</th>
<th>2nd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Desk Satisfaction Survey</td>
<td>0.00</td>
<td>-5.40</td>
<td>5.40</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>How satisfied were you with the response time to your incident? (1=not at all, 6=completely)</td>
<td>0.00</td>
<td>-1.02</td>
<td>1.02</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>How courteous and respectful was the technician who responded? (1=poor, 6=excellent)</td>
<td>0.00</td>
<td>-1.21</td>
<td>1.21</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Please rate the technical competency of the technician serving you (1=poor, 6=excellent)</td>
<td>0.00</td>
<td>-1.02</td>
<td>1.02</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Was technician able to resolve your issue during the first call?</td>
<td>0.00</td>
<td>-1.14</td>
<td>1.14</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>How satisfied are you with your overall service experience? (1=not at all, 6=completely)</td>
<td>0.00</td>
<td>-1.14</td>
<td>1.14</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>

Survey scorecard history - 4 quarters
**Export a scorecard as an image**

You can export a scorecard as an image to use in presentations or other documents.

**Role required:** admin or survey_admin

1. Click the menu icon () and select **Save as PNG** or **Save as JPEG** and wait for the export to complete.

2. Click **Download** and save the scorecard image to a storage location.
Survey administration

Survey administrators—users with the survey_admin role—create and maintain surveys and configure how they are distributed and published. Surveys on Service Portal are also supported.

Survey administration includes the following procedures.

- Create, customize, and publish surveys.
- Write and maintain survey questions.
- Define trigger conditions for when surveys are sent to users, such as when an incident closes.
- Maintain surveys and survey questions as the organization’s needs change.

To set up surveys in Service Portal, you must first install Service Portal and then configure the Survey widget on the page. The base system includes the Survey widget.

Surveys in Service Portal

If Service Portal is installed, you can use the Survey widget to set up surveys, quizzes, assessments, risk assessments, and attestations in Service Portal. Surveys for users on mobile devices are fully supported in Service Portal.

To create an intuitive interface for your users, you can set up surveys in Service Portal. You must first install Service Portal and then configure the survey widget on the page. To learn more about configuring a widget, see configure widget instances.
To configure a Survey widget on a page, CTRL + right-click the widget heading and select **Instance Options**.

**Service Portal: Instance options (properties) for the Survey widget**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max records</td>
<td>Number of surveys to list on the Service Portal homepage. The user can click the <strong>View all</strong> link to view all items. Default: 5</td>
</tr>
<tr>
<td>Title of the widget</td>
<td>Text that appears in the title bar of the surveys widget. Default: <strong>My Surveys</strong></td>
</tr>
</tbody>
</table>
Each survey on the My Surveys page contains a progress bar and a description. The color in the progress bar increases as a survey is completed. In the case of a triggered record, the table title is used for the survey description.

For mobile users, the *Pagination setting for Service Portal view* survey designer property is set to one question per page by default.
Survey designer

Users with the survey_admin role can use the survey designer. The survey designer lets you create survey categories and questions, configure the details, and publish the survey to specific users or groups.

You can assign a survey to individual users or groups who receive all the questions from all the categories. You can also customize each question and make it dependent on the response to another question. The following describes the procedures you follow to create and publish a survey.

- Create survey categories.
- Create questions within each category.
- Configure survey details, such as introductory and closing remarks and time limit.
- Select recipients for the survey.
- Publish the survey to the selected users or groups.

**Note:** The survey designer replaces the survey creator in the Legacy Surveys application. If you are using Internet Explorer version 8 or earlier, the system redirects you to the survey creator.

Survey designer elements
The survey designer is accessible from Survey > Survey Designer.

The survey designer contains controls, a header bar, and the design canvas.

Controls

To create a question, drag the appropriate data type control from the Controls palette and drop it onto the designer canvas.
The assessment engine provides a built-in result calculation feature that converts responses to scored question data types to a score from 0 through 10.

### Question data types

<table>
<thead>
<tr>
<th>Data type</th>
<th>Scored</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachment</td>
<td>No</td>
<td>Question with a Manage Attachments icon that allows users to attach one or more files.</td>
</tr>
<tr>
<td>Boolean</td>
<td>Yes</td>
<td>Question with a check box or Yes and No choices for user responses.</td>
</tr>
<tr>
<td>Choice</td>
<td>Yes</td>
<td>List of predefined options. For more information, see the definition of the Choices field in Create a question in the survey designer.</td>
</tr>
<tr>
<td>Date</td>
<td>No</td>
<td>Date field.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>No</td>
<td>Date and time field.</td>
</tr>
<tr>
<td>Number</td>
<td>No</td>
<td>Number field with predefined minimum and maximum values. The default is 1-10.</td>
</tr>
<tr>
<td>Percentage</td>
<td>No</td>
<td>Percentage field with a prescribed range.</td>
</tr>
<tr>
<td>Scale</td>
<td>Yes</td>
<td>Predefined Likert scale. Answer options appear as radio buttons.</td>
</tr>
<tr>
<td>Numeric Scale</td>
<td>Yes</td>
<td>Selectable number scale. The default is 1-5. Answer options appear as radio buttons.</td>
</tr>
<tr>
<td>String</td>
<td>No</td>
<td>Single or multi-line text field.</td>
</tr>
<tr>
<td>Template</td>
<td>Yes</td>
<td>Choice list of templates that provide a predefined scale of options. For details, see Quiz scorecards.</td>
</tr>
<tr>
<td>Reference</td>
<td>No</td>
<td>Choice list of fields from a specified reference table. This data type does not support reference qualifiers. For example, a user could select a user name if you specify sys_user as the reference table.</td>
</tr>
<tr>
<td>Image Scale</td>
<td>Yes</td>
<td>Question with a choice of images that can be selected. A template can be used to apply the same images to multiple questions.</td>
</tr>
<tr>
<td>Multiple Selection</td>
<td>Yes</td>
<td>Question with multiple check boxes that can be selected.</td>
</tr>
<tr>
<td>Data type</td>
<td>Scored</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Ranking</td>
<td></td>
<td>Question with an order number to be selected for each option. One order number cannot be selected twice. This question can be mandatory and it can also be dependent on a parent question, but not vice versa.</td>
</tr>
</tbody>
</table>

**Header bar**

The tabs on the header bar display views and a menu of functions.

- **Design**: Add and configure the properties of categories and questions. This is the default view.
- **Configuration**: Create introductions and end notes for surveys and select a [signature](#).
- **Availability**: Select the recipients for each category in the survey.
- **Save**: Save the current survey.
- **Preview**: Display a preview of the survey as it appears to recipients.
- **Publish**: Distribute the survey to the selected recipients.
- **Save and Publish**: Save and distribute the survey in one step.
- **New Survey**: Open a fresh canvas for a new survey.
- **Load Survey**: View the list of existing surveys.

© 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.
Design canvas

New surveys open in the canvas of the **Design** view. The survey **Name** field appears above first category in the canvas. A blank question field appears in the category container.

![New Survey](image)

**Initial appearance of the Survey Designer canvas**

**Configure a survey in the survey designer**
Configuration settings apply to the entire survey.

Role required: admin or survey_admin

Select **Configuration** in the survey designer and complete the Survey Designer Configuration form:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Select the check box to enable the distribution of this survey to recipients.</td>
</tr>
<tr>
<td>Anonymize responses</td>
<td>Select the check box to collect survey responses anonymously. Recipients are not listed with survey results. When a user submits a survey, the system clears the Assigned to field for the associated survey instance. Also, survey responses for anonymous surveys do not contain Assigned to values. <strong>Note:</strong> The <strong>Assigned to</strong> field is cleared. However, each response record includes the <strong>Created By</strong> and <strong>Updated By</strong> fields that are accessible to users with the survey_admin role.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of this configuration or the survey to which it is attached.</td>
</tr>
<tr>
<td>Introduction</td>
<td>Introductory content to display on surveys. You can add a welcome message or background information about the survey.</td>
</tr>
<tr>
<td>Signature</td>
<td>Acknowledgement by a survey recipient of requirements, admonitions, or expectations related to a survey.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Return URL</td>
<td>Destination address of a web page that is presented to users after they submit a completed survey. When a return URL is configured, the End note content does not appear.</td>
</tr>
<tr>
<td>End note</td>
<td>Content that is displayed to recipients after they submit a completed survey. You can add a thank you message, follow-up instructions, or other applicable information. End notes are not displayed if a Return URL is specified.</td>
</tr>
</tbody>
</table>
| Pagination setting for Service Portal view | Specify how the user will see pages on the desktop or tablet view in Service Portal.  
  - **Category**: Display each category on a separate page.  
  - **Question**: Display each question on a separate page. This happens for mobile regardless of this setting.  
  - **None**: All items on a single page—no pagination  
  Default: **Category**  
  **Note**: This field appears only when Service Portal is installed. |
| Duration                          | Amount of time that recipients are given to complete this survey, starting from the time that the survey is generated. The default duration is 14 days.  
  **Note**: By default, the system runs the **Cancel Expired Assessments** script every 30 days to cancel expired survey and assessment instances that are in the **Work in progress** or **Ready to take** states. |

**Survey categories**

Survey categories provide a way to group questions of a similar theme for a given survey.

There must be at least one survey category per survey definition and every survey question must be associated with a category. When you create a survey, the system generates one category, which all the questions belong to.

For simple surveys, one category is usually enough. Consider creating additional categories if you want to accomplish any of the following tasks.

- Separate groups of questions into collapsible sections by category on the survey questionnaire.
- Report on category scores, which are calculated based on responses for all questions within each category.

**Create a category in the survey designer**

A category represents a theme for evaluating a specific element of the survey topic and contains questions pertaining to that theme.
Role required: admin or survey_admin

When you create a survey, the system creates a default category, using the name of the survey. You can use this category, modify it, and create additional categories as needed. To have any results, a category must contain scored questions.

1. Navigate to Survey > Survey Designer.
2. Enter the name of the survey in the Name field.
   The system uses this name as the name of the survey and of the first category.
3. To configure the category, click the gear icon in its title bar and complete the following steps in the Properties dialog box.
   a) Enter a new name and a description for the category.
   b) Enter text in the Details field that introduces or explains the category to recipients.
   c) Click the X icon to close the Properties dialog box and save your settings.
4. To add a new category, click the + icon in the title bar of an existing category.
   The new category appears below the category that you selected to create it. You can click the X icon in a category header to delete a category that you added in error.

Create a survey category in a survey
You can modify an existing survey to add one or more survey categories.

Role required: admin or survey_admin

Only one category is required for each survey, but you can add additional categories as needed.

1. Navigate to Survey > View Surveys.
2. Open a survey definition.
3. In the Metric Categories related list, open a category or click New.
   Each survey category is stored as a record on the Metric Category (asmt_metric_category) table with a modified view for survey use.
4. Enter the survey category name and description.
   The category name appears on questionnaires when either of the following is true.
   - There is more than one category for the survey.
   - There is only one category and its name is different from the survey definition name. If you create a survey using the survey creator, the category name is the same as the survey definition name.
5. Right-click the form header and click Save.
   The Assessment Metrics and Users related lists appear.
6. Click Update.

Create a question in the survey designer
You can create multiple questions for each category in the survey designer, but each question can only be associated with one category.

Role required: admin or survey_admin

The data type that you select for each question determines how it can be answered by survey recipients.

1. In the Design view, drag a data type icon from the Controls palette and drop it into a category container.
2. To configure the question, click the gear icon in its title bar.
   The Properties dialog box opens.
3. Complete the form.

**Question property fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Concise name of the question. The system uses this value to identify the question in Assessment Metric lists and in scorecard charts.</td>
</tr>
<tr>
<td>Question</td>
<td>Text to display as the question on surveys. Enter a clear, straightforward question that is easy to understand.</td>
</tr>
<tr>
<td>Type</td>
<td>Data type selected for this question. See the table in <a href="#">Controls</a> for the available data types.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box that determines whether this question is available on a survey. A question does not appear on surveys that are generated after the question becomes inactive.</td>
</tr>
<tr>
<td>Mandatory</td>
<td>Check box to require users to answer the question. Mandatory questions are denoted by a red field status indicator and must be answered before the survey can be submitted. This field is available when the question does not have a dependency and the question type is not Boolean with a check box option.</td>
</tr>
<tr>
<td>Boolean option</td>
<td>Whether a check box or a Yes/No list appears as the option for a Boolean question.</td>
</tr>
<tr>
<td>String option</td>
<td>Setting for the appearance of a string field in a question. This field is available when the question type is String. The string options include the following.</td>
</tr>
<tr>
<td></td>
<td>· <strong>Single line</strong>: Single-line text field 40 characters in length that allows strings of any length.</td>
</tr>
<tr>
<td></td>
<td>· <strong>String line wide</strong>: Full page width text field that allows a single-line entry of any length.</td>
</tr>
<tr>
<td></td>
<td>· <strong>Multiline</strong>: Full page width multiline text field that allows word wrap and returns</td>
</tr>
<tr>
<td>Min</td>
<td>Lowest positive whole number that users can enter or select to answer the question. This field is available when the question type is Number, Percentage, or Numeric Scale.</td>
</tr>
<tr>
<td>Max</td>
<td>Highest positive whole number that users can enter or select to answer the question. This field is available when the question type is Number, Percentage, or Numeric Scale.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allow not applicable</td>
<td>Check box for including Not Applicable as an option for this question. Users can select Not Applicable if they do not have sufficient information to respond to a question. User responses of Not Applicable are excluded from results calculations. This field is available when the question does not have a dependency and the question type is not Boolean with a check box option.</td>
</tr>
<tr>
<td>Randomize answers</td>
<td>Check box for displaying answer options in a random order. Answer preference is sometimes influenced by the order in which options appear, which can result in biased results. Randomizing options can help prevent this bias. Note: Randomizing options for certain questions may make those questions confusing for users. In general, only randomize options that do not follow a logical order.</td>
</tr>
<tr>
<td>Positive indicator</td>
<td>Setting that determines whether smaller or larger numerical values equate to a good score in result calculations. Select Low values if smaller numerical values are better, such as for a question that measures the number of incidents for a vendor. Select High values if larger numerical values are better, such as for a question that measures user satisfaction on a scale of one to five.</td>
</tr>
<tr>
<td>Details</td>
<td>Information about the question that is displayed on the survey. Include details that help users understand how to answer the question.</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
Choices | Options for a question with a data type of **Choice** or **Scale**. The system automatically adds text and values that you can edit for each option. You must have at least two options, and each option must have a unique value.

Click the + icon to add an option, or click the X icon to delete an option. By default, the system arranges options in the order established by their values. To change the order, drag and drop the options.

**Note:** Value numbers also contribute to the calculations of survey response scores, which can be used by advanced survey administrators.

4. To create any special conditions that must be met before the question appears on the survey, click the Dependency tab.

The question must have a data type of **Boolean**, **Choice**, **Scale**, or **Template**.

5. Select a question in the **Displayed when** field.

The system selects the appropriate operator and displays the possible answers for the selected question.

6. Select the answer that satisfies the condition.

You can select more than one answer. Selected answers are indicated by a check mark.

The system prevents recursive dependencies between questions. For example, if Question A depends on Question B, Question B cannot depend on Question A.

7. Click the X icon to close the question properties dialog box and save your settings.

8. To add a question with the same data type as an existing question in the category, click the + icon in the title bar of the existing question.

9. Drag and drop questions to change their order within a category or move them between categories.

10. To delete a question, click the X icon in its title bar.

**Survey question data types**

You must choose a data type for each survey question. The data type determines the format of the question and the kind of data that is collected on survey questionnaires.

The following data types are available for surveys:
**Attachment data type**

On questionnaires, users can attach one or more files to a question. Users click the Manage Attachments icon and select one or more files in the Attachments pop-up window to attach to the question. From this window, users can:

- View a list of the attached files.
- View an attached file in a separate window.
- Rename an attached file.
- Add or delete files

Once a survey has been submitted, attachments cannot be updated or deleted.

Any type of file supported by the platform can be attached to a question. One or more files can be attached a question while taking a survey or completing an assessment.

The assessment administrator can see the attachments associated with an individual question as well as those associated with the survey.

See [Administering Attachments](#) for more information.

**Boolean data type**

On questionnaires, users select a check box beside a statement or leave it cleared.

If you select **Boolean**, you must fill in the **Scale definition** field. Select **High** if it is best when users select the check box.

**Choice data type**

On questionnaires, users select a value from a list of choices.

If you select **Choice**, you must fill in the **Scale definition** field and create answer options. Select **High** for the scale definition if the answer option with the largest metric definition **Value** is best.
Note: The system sets the Min and Max fields automatically based on the Value settings for the associated metric definitions.

Date and Date/Time data types

The Date and Date/Time data types are similar.

- **Date**: On questionnaires, users select a date.

- **Date/Time**: On questionnaires, users select a date and time.
Likert Scale data type

On questionnaires, users select a multiple choice value from a custom Likert scale. Each answer option is represented by a radio button on the scale. A Likert scale question that evaluates an application's ease of use might have the answer options Easy, Average, and Difficult.

If you select Likert Scale, you must fill in the Scale definition field and create answer options. Select High for the scale definition if the answer option with the largest metric definition Value is best.

Note: The system sets the Min and Max fields automatically based on the Value settings for the associated metric definitions.

Number data type

On questionnaires, users enter a number.
If you select **Number**, you must fill in these additional fields:

- **Scale definition**: Select **High** if a larger number is better, such as for a question that measures the number of sales made in a quarter.
- **Min** and **Max**: Enter the smallest and largest numbers users can enter. State the range of acceptable answers in the question text.

**Percentage data type**

On questionnaires, users enter a number.

If you select **Percentage**, you must fill in these additional fields:

- **Scale definition**: Select **High** if a larger percentage is better, such as for a question that measures the percentage of work an agent has completed.
- **Min** and **Max**: Enter the smallest and largest numbers users can enter. Generally **0** and **100** are appropriate minimum and maximum values. If you choose values other than **0** and **100**, it is usually best to state the range of acceptable answers in the question text.

**Reference data type**

On questionnaires, users select a value from a list that is generated from a specified reference table. The response field supports auto-completion.

**Note**: Reference qualifiers are not supported.

For example, a user could select a user name in response to a question if you specify User (sys_user) as the reference table.
String data type

On questionnaires, users enter text. When you select **String**, the **String option** field appears. Select one of the following options to determine how the string field appears on questionnaires:

- **Single line**
Template data type

On questionnaires, users select a value from a predefined series of answer options. To use this data type, a question template must be defined.

If you select **Template**, you must fill in these additional fields:

- **Template**: Select a template.
- **Scale definition**: Select **High** if the answer option with the largest template definition **Value** is best.

Yes/No data type

On questionnaires, users select **Yes** or **No** from a list.

© 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 you select Yes/No, you must fill in the Scale definition field. Select High if Yes is the best answer.

**Image scale data type**

On questionnaires, users select an image from a predefined set of images as their response. Image scale questions can also be used in a template for better performance with surveys that have the same type of answer options.

Five emojis, similar to the Likert scale (very dissatisfied to very satisfied) are provided. However, you can upload additional images in JPG, PNG, or GIF format. Two images can be uploaded, one for selected case and another for unselected case. Larger size images are reduced to 64 x 64 pixels.

The result behavior depends on the presence of uploaded images. If no selected image is uploaded, then the question shows up blank.

<table>
<thead>
<tr>
<th>Selected image</th>
<th>Unselected image</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Unselected image loads. Clicking on the image changes it to the selected image.</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>Selected image loads with 50% opacity. Clicking on the image changes the opacity to 100%.</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>A blank placeholder box is displayed.</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>A blank placeholder box is displayed.</td>
</tr>
</tbody>
</table>

**Note:** N/A option is not supported for image scale type question.

**Multiple selection data type**

On questionnaires, users can select multiple check boxes indicating all answers that apply. For instance, a user can be instructed to “Select all that apply” in a multiple selection question.
Ranking data type

On questionnaires, users can select a different order number for each option to rank them. Drag-and-drop functionality is also supported, which allows a user to either fill in the number, or simply drag an option.

One order number cannot be selected twice. This question can be mandatory and it can also be dependent on a parent question, but not vice versa.

Edit a survey in the survey designer
You can modify surveys using the survey designer.

Role required: admin or survey_admin
You can edit a survey even after it has been distributed, with the following results.

- Added questions are available only on surveys that are distributed after this change.
- Changes to existing questions are immediately available to users before the survey is submitted or during the retake period. This includes changes to the answers, such as additional choices or changes to the data type.
- Deleted questions are also deleted from the distributed surveys in user queues.

1. Navigate to **Survey > Survey Designer**.
2. Point to the menu icon in the survey header bar, and select **Load Survey**.
3. Select a survey from the list and modify it as needed.
4. Point to the menu icon in the survey header bar, and select **Save** or **Save and Publish**.
   
   When you publish the edited survey, the system generates survey instances for any associated survey users.

**Configure category weights for a survey**

You can assign a weight to each category in a survey. The system calculates results from the weight that you configure.

Configure the Survey Category form to display the **Weight** field.

Role required: admin or survey_admin

Weights are set to a value of **10** by default but can be changed.

1. Navigate to **Survey > View Surveys** and select a survey from the list.
2. In the Survey Definition form, select a category from the **Metric Categories** related list.
3. Edit the default weight value.
4. Click **Update**.

**View a survey instance**

A survey instance represents one questionnaire assigned to one user. You view an instance to verify that survey instances were created, to check the state of a survey instance, or to reassign a survey instance.

Role required: admin or survey_admin

Navigate to **Survey > Survey Instances** and open a survey instance.

Each survey instance is stored as a record on the Assessment Instance (asmt_assessment_instance) table with a modified view for survey use.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Automatically generated record number.</td>
</tr>
<tr>
<td>Metric type</td>
<td>Survey definition this survey instance was created from. Survey definitions</td>
</tr>
<tr>
<td></td>
<td>are stored on the Assessment Instance table, and the field label on that</td>
</tr>
<tr>
<td></td>
<td>table is <strong>Metric type</strong>.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Due date</td>
<td>Date by which the survey instance should be completed. The system populates the due date based on the <strong>Assessment duration</strong> of the associated survey definition, which is set to 14 days by default. The survey due date is not enforced in the base system. If you want to enforce the due date, consider using a workflow or other mechanism to send survey recipients reminders when a survey is overdue.</td>
</tr>
<tr>
<td>Note:</td>
<td>By default, the system runs the <strong>Cancel Expired Assessments</strong> script every 30 days to cancel expired survey and assessment instances that are in the <strong>Work in progress</strong> or <strong>Ready to take</strong> states.</td>
</tr>
<tr>
<td>State</td>
<td>State of the survey instance. The possible states are <strong>Ready to take</strong>, <strong>In progress</strong>, <strong>Complete</strong>, and <strong>Canceled</strong>.</td>
</tr>
<tr>
<td>Assigned to</td>
<td>User this survey instance is assigned to. This field becomes read-only when the state is <strong>In progress</strong>, <strong>Complete</strong>, or <strong>Canceled</strong>.</td>
</tr>
<tr>
<td>Expiration date</td>
<td>Date on which the assigned user can receive a new instance of the same survey definition. The system automatically populates the expiration date based on the <strong>Schedule period</strong> of the associated survey definition.</td>
</tr>
<tr>
<td>Related Link</td>
<td></td>
</tr>
<tr>
<td>View User’s Response</td>
<td>Shows a read-only version of the survey responses completed by the user.</td>
</tr>
<tr>
<td>Related List</td>
<td></td>
</tr>
<tr>
<td>Assessment Instance Questions</td>
<td>All instance question records, which store user response values for each question on the survey questionnaire. The following columns are relevant to surveys:</td>
</tr>
<tr>
<td>Category:</td>
<td>Displays the survey categories the questions belong to.</td>
</tr>
<tr>
<td>Metric:</td>
<td>Displays the survey questions.</td>
</tr>
</tbody>
</table>

**Survey users and groups**

Survey users and survey user groups help survey administrators control who can take a survey. Survey administrators can restrict a survey so that only specified users can access it unless a survey administrator manually assigns the survey to a different user. Survey user groups provide a way to quickly designate multiple survey users.
Administering survey users

The list of survey users for a survey is visible on the Survey Definition and Survey Category forms. You can add or remove users from the list of survey users at any point. Note that designating a survey user does not automatically generate a survey instance for that user unless both of the following conditions are true:

- The survey definition Schedule period is set to Daily, Weekly, Monthly, or Yearly. In this case the system assigns a new survey instance to each survey user at the beginning of each schedule period.
- The user has no instances of the survey that are incomplete or that have not yet reached their expiration date.

You can designate survey users from the Survey Designer, the Survey Definition form, or the Survey Category form.

**Note:** If there are trigger conditions for a survey, do not create survey users. Instead, use the Trigger Conditions form to assign users.

Create a survey user group

Survey user groups are groups that have the Type field set to survey and that display only the information most relevant to surveys. You can assign survey groups or any user group to surveys.

Role required: admin, user_admin, or survey_admin

Though it is possible to designate members of any group as survey users, one reason to create a survey group is to view it conveniently in the survey User Groups module.

1. Navigate to Survey > Administration > User Groups.
2. Click New.
3. Complete the Group form.
4. Right-click the form header and click Save.
   The Group Members and Groups related lists appear.
5. To add group members, complete the following steps.
   a) In the Group Members related list, click Edit.
   b) Select users from the list on the left and add them to the Group Members List on the right.
   c) Click Save.

Select recipients for a survey in the Survey Designer

You can assign survey users while designing or modifying the survey.

Role required: admin or survey_admin

1. In the Survey Designer, click the Availability tab.
2. Under Accessible by:, select the Specific users option, then select users.
3. If desired, select the Survey groups only check box, then select survey user groups or other groups.
4. Click Save.

Designate a survey user

You can designate one survey user at a time from the Survey Definition form.

Role required: admin or survey_admin

1. Navigate to Survey > View Surveys.
2. Open a survey definition.
   There must be at least one category.
3. In the **Survey Users** related list, click **New**.
4. Select a **User**.
5. Click **Submit**.
   The Survey Definition form reopens.
6. Optional: To remove survey users, in the **Survey Users** related list, select the check box beside
   the user, and then select **Delete** from the action list below the list.

**Designate or remove multiple survey users at one time**
Use the Survey Category form to designate or remove multiple survey users at a time.

Role required: admin or survey_admin
1. Open a survey definition.
2. In the **Metric Categories** related list, open a category.
   You can choose any category. The system applies survey user changes to all the survey's
   categories automatically.
3. In the **Users** related list, click **Edit**.
4. Use the slushbucket to add or remove survey users.
5. Click **Save** to return to the survey category.
   The changes are also reflected in the **Survey Users** related list on the survey definition.

**Allow recipients to retake a survey**
You can configure a survey to allow recipients to resubmit their answers as many times as they like,
up to the survey's due date.

Configure the Survey Definition form to display the **Allow retake** field. For more information, see
**Configure the form layout**.

Role required: admin or survey_admin
Results are not calculated for the survey until the configured duration has elapsed. The card in
the user's queue remains visible until the due date of the survey, and a button is displayed to allow
retakes.
1. Navigate to **Surveys > View Surveys**.
2. Select a survey from the list.
3. Select the **Allow retake** check box.
4. Click **Update**.

**Publish a survey**
You must publish a survey to enable people to receive and complete survey instances.

Role required: admin or survey_admin
The **State** field on the Survey Definition form indicates whether the survey is in the **Draft** or
**Published** state.

**Note:** You cannot return a survey to the **Draft** state after it has been published. You do
have the option to deactivate a survey by clearing the **Active** check box.

1. Navigate to **SurveyView Surveys** and select a survey to publish.
2. Click **Publish**.
When you publish a survey, the system generates survey instances for any associated survey users. You can assign the survey to other users manually.

**Publish a survey in the Survey Designer**
You must save changes to a survey before you can publish it to the specified recipients or groups.

Role required: admin or survey_admin

1. In the Survey Designer, point to the menu and select **Load Survey**.
2. Select a survey to publish.
3. To preview the survey as a user, point to the menu icon and click **Preview**.
4. When you are satisfied with the survey, click either **Save and Publish** or **Publish** to distribute it.

When you publish a survey, the system sends email notifications to the recipients and to their managers. The system displays a link to the survey on a card in each recipient's My Assessments & Surveys portal.

---

**Customize the appearance of a survey**
Assessment and survey administrators can set properties to customize the color of various elements on the questionnaires.

Role required: admin or survey_admin

---

**Note:**
- For color properties, enter either an HTML color name or hexadecimal (hex) value. For hex values, the # character is required. Values are not case-sensitive.
- For example, all of the following formats are valid: LightGray, lightgray, #D3D3D3. A preview of the color appears next to the field.

---

Note that the customizations you make apply to all assessments and surveys.

1. Navigate to either of the following modules.
   - Assessments > Admin > Assessment Properties
   - Survey > Administration > Properties
2. On the properties page, edit the properties as needed.
   Refer to the screenshot below to see what parts of assessment questionnaires are controlled by the properties.
3. Click **Save**. You may need to clear the browser’s cache to see updates.

**Assessment and survey properties**

You can configure a variety of properties to customize the appearance of assessment and survey questionnaires, require authentication for user signatures, open surveys in the service portal view from emails, and limit the number of items shown in a decision matrix field filter.

**Assessment and survey properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sn_portal_surveys.sp_survey.email.redirection</td>
<td><strong>Email redirection</strong></td>
<td>When Yes is selected, a survey accessed from a link in an email opens in the Service Portal.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: This property applies only to surveys.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: No</td>
</tr>
<tr>
<td>com.snc.assessment.signature_authentication</td>
<td><strong>Signature authentication</strong></td>
<td>When Yes is selected, this property requires credentials for a full name signature.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: Yes</td>
</tr>
<tr>
<td>css.assessment.question.header.background.color</td>
<td><strong>Question header background color</strong></td>
<td>Sets the background color of question headers on assessment and survey questionnaires.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: #767676</td>
</tr>
<tr>
<td>css.assessment.caption.background.color</td>
<td><strong>Caption background color</strong></td>
<td>Sets the background color of the caption on assessment and survey questionnaires.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: #eee</td>
</tr>
</tbody>
</table>
Survey definitions

A survey definition is the root record upon which a survey is built.

The survey designer generates a survey definition automatically when you save or publish the survey. Survey administrators may want to modify the survey definition to configure additional options for the survey, or to publish the survey when it is ready for distribution.

Survey administrators and survey readers can also send survey invitations directly to users from the survey definition.

Modify a survey definition
You can configure additional options for a survey definition.

Role required: admin or survey_admin

1. Navigate to Survey > View Surveys.
   Each survey definition is stored as a record on the Assessment Metric Type [asmt_metric_type] table with a modified view for survey use.
2. Open a survey definition.
3. Modify the fields on the Survey Definition form, as appropriate.

Survey Definition form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the survey, which appears on the questionnaire.</td>
</tr>
<tr>
<td>Description</td>
<td>Helpful information about the survey.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box to activate the survey definition. When the Active check box is cleared, new survey instances cannot be generated and users cannot complete existing survey instances. Use the Active check box to deactivate or activate a published survey.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Anonymize responses</td>
<td>Check box to ensure that all responses for this survey are stored without the submitting user names. When a user submits a survey, the system clears the <strong>Assigned to</strong> field for the associated survey instance. Also, survey responses for anonymous surveys do not contain <strong>Assigned to</strong> values.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The <strong>Assigned to</strong> field is cleared. However, each response record includes the <strong>Created By</strong> and <strong>Updated By</strong> fields that are accessible to users with the survey_admin role.</td>
</tr>
<tr>
<td>Send notifications</td>
<td>Check box to send a notification that the survey has been taken.</td>
</tr>
<tr>
<td>State</td>
<td>Status of the survey: <strong>Draft</strong> or <strong>Published</strong>.</td>
</tr>
<tr>
<td>Signature</td>
<td>Acknowledgement by a survey recipient of requirements, admonitions, or policies related to the survey. The signature may require the recipient to select a check box or to type a full signature to verify having read these assertions. You can display assertions without requiring a signature. Select an existing signature from the list or click <strong>New</strong> to create a new one. The signature form contains these fields:</td>
</tr>
<tr>
<td></td>
<td>* <strong>Name:</strong> Descriptive name for this signature.</td>
</tr>
<tr>
<td></td>
<td>* <strong>Signature type:</strong> Type of signature required. The selections are <strong>Check box</strong>, <strong>Full name</strong>, or <strong>Assertion only</strong>. If <strong>Assertion only</strong> is selected, no signature is required to submit the survey.</td>
</tr>
<tr>
<td></td>
<td>* <strong>Assertion:</strong> Text you want to display to recipients.</td>
</tr>
<tr>
<td></td>
<td>By default, a property called <strong>Require authentication for user signature</strong> (<strong>com.snc.assessment.signature_authentication</strong>) requires users to authenticate when providing a full name signature.</td>
</tr>
<tr>
<td>Schedule period</td>
<td>Option that determines how often a user can take the same survey and whether the system generates survey instances on a schedule.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you use a trigger condition for a survey, ensure the schedule period is set to <strong>No Limit</strong>. Trigger conditions use a different method to regulate how often users can receive survey instances.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allow retake</td>
<td>Check box that allows users to modify their answers to a completed survey. Users can resubmit a survey as many times as they want until the due date. After that date, the system removes the survey from the user’s My Assessments &amp; Surveys page.</td>
</tr>
</tbody>
</table>
| Scheduled job            | Scheduled job the system creates for this survey definition when the schedule period is a repeating interval. The system sets the scheduled job to run according to the selected schedule period. If you change the schedule period and save the survey definition:  
  - The system deletes the old scheduled job.  
  
  If you selected a recurring schedule period:  
  - A new scheduled job is created.  
  
  For example, if you change the schedule period from Daily to Weekly and save the record:  
  - The system deletes the daily scheduled job.  
  - Creates a weekly one set to run a week from the current date.  
  This field is visible to administrators only if the schedule period is Daily, Weekly, Monthly, or Yearly.                                                                                                                                                                                                                                                                                   |
| Introduction             | Introductory content to display on survey questionnaires. Consider adding a company logo, a welcome message, background information about the survey, or instructions.                                                                                                                                                                                                                                                                                                            |
| End note                 | Content to display on the screen that appears when someone submits a survey questionnaire. Consider adding a thank you message, follow-up instructions, or other applicable information.                                                                                                                                                                                                                                                                                   |
| Pagination setting for Service Portal view | The setting on which the pagination is based for desktop or tablet view in Service Portal.  
  - Category: default  
  - Question: 1 question per page (automatic for mobile)  
  - None: no pagination  
  
  **Note:** This field is displayed only when Service Portal is installed.                                                                                                          |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment duration</td>
<td>The length of time to complete assigned survey instances, starting from the time the survey instance is generated. The assessment duration sets the Due date for each survey instance. The default duration is 14 days. Configure the form to see this field.</td>
</tr>
<tr>
<td>Send notifications</td>
<td>Select the check box to send notifications for the survey when it is published. Configure the form to see the field.</td>
</tr>
<tr>
<td>Related Links</td>
<td></td>
</tr>
<tr>
<td>Enable Public Access</td>
<td>Link that enables/disables the survey as a public survey. No login is required to take a public survey (including a survey with a trigger condition) and users or non-users can respond anonymously. For completed public surveys, the Assigned to field value is Guest.</td>
</tr>
<tr>
<td>Remove Public Access</td>
<td></td>
</tr>
<tr>
<td>View Responses</td>
<td>Link that opens the list of responses for this survey. This related link is available only if there are results for the survey.</td>
</tr>
<tr>
<td>View Scorecard</td>
<td>Link that opens the scorecard for this survey. This related link is available only if there are results for the survey.</td>
</tr>
<tr>
<td>View Survey URL</td>
<td>Link that opens a dialog box that displays a URL for this survey. The URL is useful for sharing a public survey. This related link is available only if the Active check box is selected. The URL does not work until the survey definition is published.</td>
</tr>
<tr>
<td>Related Lists</td>
<td></td>
</tr>
<tr>
<td>Metric Categories</td>
<td>All survey categories for this survey.</td>
</tr>
<tr>
<td>Survey Users</td>
<td>All survey users who are authorized to take this survey. If no users are listed, any user can take this survey.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Assessment Instances | All survey instances for this survey. Configure the form to add this related list to see it.

**Note:** If you add a related list to the form, use list control to omit the New button. The system generates survey instances to produce functional surveys.

4. Save the record.

**Schedule periods**
The available schedule periods are **Only Once**, **No Limit**, **Daily**, **Weekly**, **Monthly**, and **Yearly**.

The default schedule period is **No Limit**. When you set the schedule period to anything except **Only Once** or **No Limit**, the system creates a corresponding scheduled job. The scheduled job performs the following actions.

- Ensures that a user can take one survey instance of the same survey per schedule period.
- Generates a new survey instance for each survey user at the beginning of the new schedule period, as long as the survey user does not have an incomplete instance of that survey. A survey instance is incomplete if the state is not **Complete**.

For example, if you set the schedule period to **Monthly** and someone attempts to send survey invitations twice in the same day, the system generates survey instances for the survey users the first time only. At the beginning of the next schedule period, the system generates another survey instance for each survey user who completed the previous one.

Schedule periods are enforced by the **Expiration date** field on the survey instance. As long as the survey instance expiration date has not passed, the assigned user cannot receive a new survey instance. When the system generates a survey instance and the schedule period is anything except **No Limit**, the **Expiration date** field is automatically set to the appropriate date. For example, if the schedule period is **Weekly**, the expiration date is a week after the survey instance is generated.

If you change the schedule period, the scheduled job updates automatically to the correct schedule. However, users who have survey instances for the survey cannot receive new survey instances until their existing survey instances expire, regardless of the new schedule period.

Consider the following example: Sal Pindell receives a survey instance when the schedule period is **Weekly**. The next day, a survey administrator changes the schedule period to **No Limit**. Sal cannot receive another survey instance until one of the following actions occurs.

- Seven days pass from the time Sal’s survey instance was generated.
- A survey administrator deletes Sal’s survey instance.

After one of these actions occurs, Sal can receive a new survey instance anytime, as long as he has no incomplete instances of the survey.

**Note:** If you use a trigger condition for a survey, ensure the schedule period is set to **No Limit**. Trigger conditions use a different method to regulate how often users can receive survey instances.

---

**Create a survey designer template question**

You can create a question that uses choice lists from a template.
Role required: admin or survey_admin
1. Navigate to Survey > Survey Designer and load a survey or create a new survey.
2. Drag the Template data type icon into a category container.
3. Click the gear icon in the question title bar to open the template properties dialog box.
4. Select a predefined scale from the list.
Question entry fields appear for that template.

5. Enter one or more questions that are appropriate for the template.
6. Click the arrow to the right of a question to configure its properties. You must provide a name for each question.
7. Click the back arrow to return to the template properties dialog box.
8. Configure the properties for the remaining questions.
9. Click the X icon to close the template properties dialog box and save your settings.

Survey questions

Survey questions appear on survey questionnaires for the associated survey definition.

The survey creator generates questions and answer options automatically. However, it provides only the basic configuration options for questions, such as the question text and the data type. You may want to create additional questions or set advanced configuration options for the questions, including making a question appear conditionally or making a question mandatory. You can also use question templates to define reusable sets of answer options.

Survey questions are available from Survey > Questions. The list displays information about each question, including the associated survey definition listed in the Type column, and the data type. Survey administrators can modify these questions.

Create or modify survey questions
You can create and administer survey questions.

Role required: admin or survey_admin
Changes to a survey, such as the addition of questions or the modification of question templates, do not apply immediately to the existing survey instances. However, the changes apply immediately to any new survey instances that are created after the changes are saved.

1. Navigate to Survey > View Surveys.
2. Open a survey definition.
3. In the Metric Categories related list, open a category.
4. In the Assessment Metrics related list, open an existing question or click New.
   - Each survey question is stored as a record on the Assessment Metric (asmt_metric) table with a modified view for survey use.
5. Complete the Survey Question form.
   - The fields that appear depend on the selected Data type.

### Survey Question form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the question. When you create a survey, the question name is the same as the text in the Question field.</td>
</tr>
<tr>
<td>Question</td>
<td>Text to use for the question, which appears on survey questionnaires.</td>
</tr>
<tr>
<td>Data type</td>
<td>Data type of the question. The fields for the response depend on the data type.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If another question depends on this question, you cannot change the data type.</td>
</tr>
<tr>
<td>Template</td>
<td>Question template to use for the answer options.</td>
</tr>
<tr>
<td></td>
<td>This field is visible and required only if the data type is Template.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If another question depends on this question, you cannot change the template.</td>
</tr>
<tr>
<td>Scale definition</td>
<td>Setting that determines whether smaller or larger numerical values equate to a good score in result calculations. Select Low if smaller numerical values are better, such as for a question that measures the number of incidents for a vendor. Select High if larger numerical values are better, such as for a question that measures user satisfaction on a scale of one to five.</td>
</tr>
<tr>
<td></td>
<td>This field is visible and required only when certain data types are selected.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Randomize answers</td>
<td>Check box that determines whether to present the answer options for this question in a random order each time a user opens the survey. Answer preference is sometimes influenced by the order in which answer options appear, which can result in biased results. Randomize answer options to help prevent this bias. This field is visible only if the data type is <strong>Choice</strong> or <strong>Likert Scale</strong>.</td>
</tr>
<tr>
<td>Note: Randomizing answer options may make a question confusing. In general, only randomize answer options that do not follow a logical order.</td>
<td></td>
</tr>
<tr>
<td>Mandatory</td>
<td>Check box that makes the question mandatory (selected) or optional (cleared) on survey questionnaires. Users cannot submit questionnaires until they provide valid responses to all mandatory questions, which are denoted by a red field status indicator. This field is visible only when the <strong>Depends on</strong> field is empty and the data type is not <strong>Checkbox</strong>. Questions that depend on other questions and check box questions cannot be mandatory.</td>
</tr>
<tr>
<td>Allow not applicable</td>
<td>Check box that determines whether to include a <strong>Not Applicable</strong> answer option for this question on survey questionnaires. User responses of <strong>Not Applicable</strong> are excluded from results calculations. This field is visible only if the data type is <strong>Choice</strong>, <strong>Likert Scale</strong>, <strong>Template</strong>, or <strong>Yes/No</strong>.</td>
</tr>
<tr>
<td>Depends on</td>
<td>Setting used to make this a conditional question, meaning that it only appears when users answer another question a certain way. To make a question depend on another question, select an existing question from the list, which displays <strong>Checkbox</strong>, <strong>Choice</strong>, <strong>Template</strong>, and <strong>Yes/No</strong> questions of the same category as this question. Then, use the <strong>Displayed when</strong> field to set the conditions that cause this question to appear on surveys. The system prevents the creation of recursive dependencies between questions. For example, if Question A depends on Question B, Question B cannot depend on Question A.</td>
</tr>
<tr>
<td>Displayed when</td>
<td>Answer options for the selected <strong>Depends on</strong> question which, when chosen on surveys, display this question. This field is visible and required only when the <strong>Depends on</strong> field is set.</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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min</td>
<td>Smallest numerical value to be used as an answer option for this question. This field is visible and required only if the data type is Choice, Likert Scale, Number, or Percentage.</td>
</tr>
<tr>
<td>Max</td>
<td>Largest numerical value to be used as an answer option for this question. This field is visible and required only if the data type is Choice, Likert Scale, Number, or Percentage.</td>
</tr>
<tr>
<td>String option</td>
<td>Selection that determines what kind of response text box appears for this question on survey questionnaires. This field is visible and required only if the data type is String.</td>
</tr>
</tbody>
</table>

### Related Lists

| Assessment Metric Definitions | Answer options for this question. This related list is available only if the Data type is Choice or Likert Scale. |

6. Save the record.

Be sure to create answer options if you select the Choice or Likert Scale data type.

**Survey question data types**

You must choose a data type for each survey question. The data type determines the format of the question and the kind of data that is collected on survey questionnaires.

The following data types are available for surveys:

- **Attachment data type**

  On questionnaires, users can attach one or more files to a question.

  Users click the Manage Attachments icon and select one or more files in the Attachments pop-up window to attach to the question. From this window, users can:

  - View a list of the attached files.
  - View an attached file in a separate window.
  - Rename an attached file.
  - Add or delete files

  Once a survey has been submitted, attachments cannot be updated or deleted.

  Any type of file supported by the platform can be attached to a question. One or more files can be attached a question while taking a survey or completing an assessment.

  The assessment administrator can see the attachments associated with an individual question as well as those associated with the survey.

  See [Administering Attachments](#) for more information.

- **Boolean data type**

  On questionnaires, users select a check box beside a statement or leave it cleared.
If you select **Boolean**, you must fill in the **Scale definition** field. Select **High** if it is best when users select the check box.

**Choice data type**

On questionnaires, users select a value from a list of choices.

If you select **Choice**, you must fill in the **Scale definition** field and create answer options. Select **High** for the scale definition if the answer option with the largest metric definition **Value** is best.

**Note:** The system sets the **Min** and **Max** fields automatically based on the **Value** settings for the associated metric definitions.

**Date and Date/Time data types**

The **Date** and **Date/Time** data types are similar.

- **Date:** On questionnaires, users select a date.
- **Date/Time**: On questionnaires, users select a date and time.
Likert Scale data type

On questionnaires, users select a multiple choice value from a custom Likert scale. Each answer option is represented by a radio button on the scale. A Likert scale question that evaluates an application’s ease of use might have the answer options Easy, Average, and Difficult.

If you select Likert Scale, you must fill in the Scale definition field and create answer options. Select High for the scale definition if the answer option with the largest metric definition Value is best.

Note: The system sets the Min and Max fields automatically based on the Value settings for the associated metric definitions.

Number data type

On questionnaires, users enter a number.

If you select Number, you must fill in these additional fields:

- Scale definition: Select High if a larger number is better, such as for a question that measures the number of sales made in a quarter.
- Min and Max: Enter the smallest and largest numbers users can enter. State the range of acceptable answers in the question text.

Percentage data type

On questionnaires, users enter a number.

If you select Percentage, you must fill in these additional fields:
• **Scale definition:** Select **High** if a larger percentage is better, such as for a question that measures the percentage of work an agent has completed.

• **Min** and **Max:** Enter the smallest and largest numbers users can enter. Generally 0 and 100 are appropriate minimum and maximum values. If you choose values other than 0 and 100, it is usually best to state the range of acceptable answers in the question text.

### Reference data type

On questionnaires, users select a value from a list that is generated from a specified reference table. The response field supports auto-completion.

**Note:** Reference qualifiers are not supported.

For example, a user could select a user name in response to a question if you specify User (sys_user) as the reference table.

![Example of Reference Data Type](image)

### String data type

On questionnaires, users enter text. When you select **String**, the **String option** field appears. Select one of the following options to determine how the string field appears on questionnaires:
Template data type

On questionnaires, users select a value from a predefined series of answer options. To use this data type, a question template must be defined.

If you select **Template**, you must fill in these additional fields:

- **Template**: Select a template.
- **Scale definition**: Select **High** if the answer option with the largest template definition **Value** is best.

Yes/No data type

On questionnaires, users select **Yes** or **No** from a list.
If you select Yes/No, you must fill in the Scale definition field. Select High if Yes is the best answer.

**Image scale data type**

On questionnaires, users select an image from a predefined set of images as their response. Image scale questions can also be used in a template for better performance with surveys that have the same type of answer options.

Five emojis, similar to the Likert scale (very dissatisfied to very satisfied) are provided. However, you can upload additional images in JPG, PNG, or GIF format. Two images can be uploaded, one for selected case and another for unselected case. Larger size images are reduced to 64 x 64 pixels.

The result behavior depends on the presence of uploaded images. If no selected image is uploaded, then the question shows up blank.

<table>
<thead>
<tr>
<th>Selected Image</th>
<th>Unselected Image</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Unselected image loads. Clicking on the image changes it to the selected image.</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>Selected image loads with 50% opacity. Clicking on the image changes the opacity to 100%.</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>A blank placeholder box is displayed.</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>A blank placeholder box is displayed.</td>
</tr>
</tbody>
</table>

**Note:** N/A option is not supported for image scale type question.
**Multiple selection data type**

On questionnaires, users can select multiple check boxes indicating all answers that apply. For instance, a user can be instructed to “Select all that apply” in a multiple selection question.

<table>
<thead>
<tr>
<th>Equipment Usage Survey</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Multiple Selection</strong></td>
</tr>
<tr>
<td>What equipments do you use?</td>
</tr>
<tr>
<td>Laptop</td>
</tr>
</tbody>
</table>

**Ranking data type**

On questionnaires, users can select a different order number for each option to rank them. Drag-and-drop functionality is also supported, which allows a user to either fill in the number, or simply drag an option.

1. Please rate following device in order of Importance.

<table>
<thead>
<tr>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>MAC</td>
</tr>
</tbody>
</table>
One order number cannot be selected twice. This question can be mandatory and it can also be dependent on a parent question, but not vice versa.

**Survey question template**  
Question templates define reusable sets of answer options for survey questions.

Question templates define reusable rating scales for answering questions, where each answer option on the scale is a template definition. For example, the template named **Satisfaction** represents a satisfaction scale and contains the following template definitions: **Very Satisfied**, **Satisfied**, **Neutral**, **Dissatisfied**, and **Very Dissatisfied**.

### Template definition

Templates are available for survey questions that have **Data type** set to **Template**. The following question templates are available in the base system. You can create or update a template as described in **Create a survey question template**.

#### Default question templates

<table>
<thead>
<tr>
<th>Name</th>
<th>Template definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amount</td>
<td>None, Few or little, Average amount, Many, Quite a lot</td>
</tr>
<tr>
<td>Complexity</td>
<td>Very Complex, Complex, Moderate, Simple, Very Simple</td>
</tr>
<tr>
<td>Frequency</td>
<td>Never, Seldom, Sometimes, Most of the time, All of the time</td>
</tr>
<tr>
<td>Likert 5</td>
<td>Strongly Disagree, Disagree, Neutral, Agree, Strongly Agree</td>
</tr>
<tr>
<td>Quality</td>
<td>Very Poor, Poor, Average, Good, Very Good</td>
</tr>
<tr>
<td>Satisfaction</td>
<td>Very Dissatisfied, Dissatisfied, Neutral, Satisfied, Very Satisfied</td>
</tr>
<tr>
<td>Size</td>
<td>Very Small, Small, Average, Large, Very Large</td>
</tr>
</tbody>
</table>

**Create a survey question template**  
You can create and administer question templates.

**Role required**: admin or survey_admin

Changes to a survey, such as the modification of question templates, apply to existing survey instances immediately. Templates that you create are available for use with both surveys and assessments.

1. **Navigate to Survey > Templates**.  
   Each template is stored as a record on the Assessment Metric Template (asmt_template) table.
2. Click New.
3. Enter a Name.
4. Right-click the form header and click Save.
5. In the Assessment Template Definitions related list, click New.
   Create a template definition for each answer option you want to appear on a question.
6. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display</td>
<td>Enter the text to appear as the answer option.</td>
</tr>
<tr>
<td>Value</td>
<td>Enter a numeric value, greater than or equal to zero, to which the answer option equates. Values are used in results calculations. When you view questions that use templates, answer options appear in order from smallest to largest Value. Each template definition for a given template must have a unique Value.</td>
</tr>
</tbody>
</table>

7. Click Update.

Update min and max values to match templates
If you use survey result calculation data, ensure that the Min and Max values for a question that uses a template are equal to the smallest and largest template definition Value.
Role required: admin or survey_admin
When you create a question of the Template data type, the system sets the Min and Max fields based on the template definition values. The fields for existing questions are not updated if you add a new template definition to a template or if you update the Value of an existing template. If the new Value is less than the minimum value or greater than the maximum value of any questions that use the template, update the questions accordingly.

1. Navigate to Survey > Questions.
2. Configure the list to show the Min and Max columns.
3. Add the following list filter condition: (Template) (is) (<select the template you updated>).
4. Ensure the Min and Max values match the smallest and largest template definition Value for the selected template.
   If the values do not match, edit the Min and Max values directly from the list.

   **Note:** When the data type is Template, a UI policy prevents the editing of Min and Max from the form.

Create or modify answer options
You must create answer options, called metric definitions, for survey questions that have Data type set to Choice or Likert Scale.
Role required: admin or survey_admin
Changes to a survey, such as the addition or modification of answer options, apply to existing survey instances immediately.

1. Navigate to Survey > Questions.
2. Open a choice or Likert scale survey question.
3. In the Assessment Metric Definitions related list, open a metric definition or click New.
Each answer option is stored as a record on the Assessment Metric Definition (asmt_metric_definition) table.

4. Complete the Assessment Metric Definition form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display</td>
<td>Text to appear as the answer option.</td>
</tr>
<tr>
<td>Value</td>
<td>Numeric value, greater than or equal to zero, to which the answer option equates. Values determine the order in which answer options appear. See the example below. Values are also used to calculate survey results. Each metric definition for a given question must have a different Value.</td>
</tr>
</tbody>
</table>

5. Click Submit.

On survey questionnaires, the answer options for a question appear in order from smallest to largest Value. For example, consider the survey question How do you feel? with the answer options Good, Neutral, and Bad. The following table shows the answer option order based on the Value.

<table>
<thead>
<tr>
<th>Answer option</th>
<th>Value</th>
<th>Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>Good</td>
<td>1</td>
<td>First</td>
</tr>
<tr>
<td>Neutral</td>
<td>3</td>
<td>Second</td>
</tr>
<tr>
<td>Bad</td>
<td>5</td>
<td>Third</td>
</tr>
</tbody>
</table>

If you use survey result calculations, ensure the question Scale definition is set appropriately based on the answer options. In the previous example, if you want the answer option Good to earn the highest score, the scale definition should be Low because Good has the smallest value.

Change the order of survey questions
You can easily reorder survey questions at the category level or the question level.

Role required: admin or survey_admin

You can change the order in which the questions in one category appear relative to those in other categories for the same survey definition. If you add a new question manually after you create other questions, you may want to change the order of questions.

When you create questions using the survey creator, the system sets the Order field for the first question to 101, the second to 102, and so on. After you create a new question outside of the survey creator, the Order is set to 100 by default, which means it appears before all questions generated by the survey creator.

1. Navigate to Survey > View Surveys and open the appropriate survey definition.
2. In the Metric Categories related list, edit the values in the Order column.
3. To change the order of questions within a category, complete the following steps.
a) Open the **Assessment Metrics** related list.
b) Edit the values in the **Order** column.

4. Click **Update**.

**Survey trigger conditions**

Trigger conditions specify when to send a particular survey and the persons to send it to. Survey administrators can use trigger conditions to configure the system to generate a survey instance each time a specified action occurs on a specified table, for example, when an incident or change request closes. The system sends the survey to users that are related to the triggering record, for example, incident callers or change request assignees. You can choose to send a survey every time the condition is met, or you can set a probability for the system to send a survey at random when the condition is met.

Trigger conditions are ideal for sending transactional surveys. Transactional surveys generally measure satisfaction with a recent experience, such as closing an incident or purchasing an item.

**Note:** Trigger conditions are comparable to survey conditions in legacy surveys. If you migrate a legacy survey that has survey conditions, ensure that the survey conditions are deactivated before you recreate them as trigger conditions.

**Configure a trigger condition for a survey**

Configure trigger conditions to specify when to send a particular survey and the persons to send it to.

Role required: admin or survey_admin

1. Navigate to **Survey > Trigger Conditions**.
2. Click **New**.

**Note:** Do not specify particular users for a triggered survey because only the specified users are allowed to take the survey.

3. Complete the form.

**Trigger condition fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment</td>
<td>Survey to send.</td>
</tr>
<tr>
<td>Table</td>
<td>Table to run the trigger condition on. You can select only tables in the current application scope. For example, to send a survey whenever an incident closes, select the Incident (incident) table.</td>
</tr>
<tr>
<td>User field</td>
<td>Field that stores the users you want to send the survey. You can select any field, on the selected table or on a referenced table, that references the User (sys_user) table. Use the tree picker to select a field. <strong>Note:</strong> To avoid requiring users to log in to take a survey with a trigger condition, set the survey to Public.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Repeat interval</td>
<td>Minimum period that must pass before the trigger condition can resend the survey to the same user. For example, assume the repeat interval is set to 30 days. Even if the same user qualifies for multiple surveys from this trigger condition, the system can send only one survey every 30 days.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Ensure that the Schedule period of the selected survey definition is set to <strong>No Limit</strong>. If the schedule period is set to a different value, it prevents the trigger condition from sending surveys as expected.</td>
</tr>
<tr>
<td>Application</td>
<td>(Admin only) Application is set to Core.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box that determines whether this trigger condition is active (selected).</td>
</tr>
<tr>
<td>Business rule</td>
<td>(Admin only) Business rule the system creates to monitor the selected table. When the condition is met, the business rule sends the survey to the correct user. No configuration is necessary for this business rule.</td>
</tr>
<tr>
<td>Trigger randomly</td>
<td>Check box that determines whether to send the survey to the appropriate user every time the condition is met (cleared) or only a percentage of the time (selected).</td>
</tr>
<tr>
<td>Probability (%)</td>
<td>Approximate probability that the survey is sent each time the condition is met. For example, if the probability is set to 50, the system sends the survey approximately 50% of the time the conditions are met. There are no repeat interval restrictions is assumed. This field is visible and required only when Trigger randomly is selected.</td>
</tr>
<tr>
<td>Related Field 1- 4</td>
<td>Field that contains a value you want to store for reporting purposes. You can pick any reference field on the selected table. When the trigger condition generates a survey instance, the system stores the value from the triggering record. Specify up to four fields. For example, select the Incident table, <strong>Assigned to</strong> and <strong>Problem</strong> as related fields. The system stores the assigned user and problem associated with the incident as Related record 1 and Related record 2 in the survey instance record. To view the fields, configure the form for any survey instance.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You cannot use a related field for the ticket number because you cannot select the Number column. You can, however, use the trigger_id column of the table.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Description</td>
<td>Summary information to identify the trigger condition. Note: For a triggered record, the table title is used for the survey description.</td>
</tr>
<tr>
<td>Condition</td>
<td>Condition builder that defines the criteria that must be true to send the survey. For example, to send a survey whenever an incident closes, create the condition (State) (is) (Closed).</td>
</tr>
</tbody>
</table>

You can also create a trigger condition directly from the survey creator. If you select **Certain users can take this survey, based on conditions** in the Survey User Access section, the Trigger Condition form opens automatically when you click **Save as Draft** or **Publish**.
<table>
<thead>
<tr>
<th>Assessment</th>
<th>Service Desk Satisfaction Survey</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Incident (Incident)</td>
</tr>
<tr>
<td>User field</td>
<td>Click to select...</td>
</tr>
<tr>
<td>Repeat Interval</td>
<td>Days 30</td>
</tr>
<tr>
<td></td>
<td>Hours 00 00 00</td>
</tr>
<tr>
<td>Related Field 1</td>
<td>None</td>
</tr>
<tr>
<td>Related Field 2</td>
<td>None</td>
</tr>
<tr>
<td>Related Field 3</td>
<td>None</td>
</tr>
<tr>
<td>Related Field 4</td>
<td>None</td>
</tr>
<tr>
<td>Description</td>
<td>Send incident calls service desk satisfaction surveys when incidents are closed</td>
</tr>
<tr>
<td>Condition</td>
<td>Add Filter Condition Add &quot;OR&quot; Clause</td>
</tr>
<tr>
<td></td>
<td>Choose field value</td>
</tr>
</tbody>
</table>
Trigger condition example
You can send out auto-triggered surveys when an incident is closed or resolved.

A trigger condition is configured as follows:

- **Assessment**: Service Desk Satisfaction Survey
- **Table**: Incident (incident)
- **User field**: Caller
- **Repeat interval**: 30 days
- **Active**: true
- **Trigger randomly**: false
- **Related Field 1**: Assigned to
- **Related Field 2**: Problem
- **Condition**: (State) (is) (Closed) (or) (State) (is) (Resolved)

Fannie Steese is the caller on incident INC00004305 that is assigned to Boris Catino, a service desk technician. Boris creates PRB010101 based on Fannie’s complaint and closes the incident. The system creates a survey instance assigned to Fannie so she can rate her satisfaction with the incident experience.

Because two related fields were selected as part of the trigger condition, the survey instance stores the following information from the incident:

- **User (Related Field 1)**: Boris Catino
- **Problem (Related Field 2)**: PRB010101
- **Task (automatically created)**: INC00004305

Because the task field is automatically populated, UI-based filtering by dot-walking on incidents (or any task-based table) is supported when creating a report on survey results. For example, you can query all survey instances related to incidents assigned to a group (survey reports on all incidents assigned to networking group, for instance).

---

**Note**: Even though the trigger condition is set to be triggered each time that the conditions are met, the **Repeat interval** setting ensures that Fannie does not receive another survey for another of her incidents closes within 30 days of the first incident.

---

Survey report example based on task field

One of the most common use cases for Surveys is to send out an auto-triggered survey when an incident, request, or task is closed. Once you get the survey results back, you can filter the results by users and groups related to the ticket, such as Assignment Group, or Assignee.

Filtering the survey results provides more detail on how people and teams are performing based on ticket data. Since this information is automatically captured, you can dot-walk while filtering the data (instead of utilizing a related field on the Survey trigger condition form, as previously required).
To create a report on incident-triggered survey responses by Assignment group, set up the report on the Task Assessment Details by navigating to ReportsView/Run and clicking Create a report.

### Survey distribution

There are several ways for survey administrators to distribute surveys to users.

Surveys are distributed using any of the following methods.

- Send survey invitations to users
- Share a survey URL that opens the survey directly.
- Create a module that opens a survey.

**Send survey invitations to users**

You can send survey invitations using the Assign Survey or Send Invitations buttons on the Survey Definition form.

**Role required:** admin or survey_admin

Use the Send Invitations button to immediately assign survey instances to each survey user that is listed in the survey definition. Use the Assign Survey button to assign a survey instance to any one user at a time.

Each of the buttons generates survey instances assigned to the appropriate users. In addition, if the instance is configured to send email, the system generates survey notifications. For either button to be available, the survey definition must meet all of the following conditions.

- **Active** check box is selected.
- **State** is Published.
- Survey is associated with at least one question.

**Note:** You (or a trigger) can send more than one instance of a survey to a user at any time.

1. Navigate to **Survey > View Surveys**.
2. Select an active, published survey.
3. Complete one of the following actions.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign a survey to users listed in the Survey Users related list</td>
<td>Click <strong>Send invitations</strong>.</td>
</tr>
<tr>
<td>Assign a survey to any user</td>
<td>Click <strong>Assign Survey</strong> and select one or more users, and then click OK.</td>
</tr>
</tbody>
</table>

The system creates a survey instance assigned to the user or users, assuming the user is eligible to receive a new survey instance. When you use the **Assign Survey** button, the selected user is not saved as a survey user.

**Survey URLs**

You can distribute a survey by giving survey users a survey URL.

Survey administrators can obtain one of the following types of URLs.

- A general URL for a survey, which users can open to take the survey questionnaire. The following process occurs.
  - When someone opens the URL, the system ensures that the person is logged in. It then searches for an instance of the associated survey that is assigned to the logged-in user.
  - If a survey instance is found, the appropriate action occurs based on the **State** of the survey instance (see table). If there are multiple active survey instances (**Ready to take** or **In progress**), the instance with the earliest due date opens.
  - If no survey instance is found, the system creates a new instance for the survey, assigns it to the user, and opens the survey questionnaire.

- A URL for a specific survey instance, which the assigned user can open to take the survey questionnaire. The following process occurs.
  - When someone opens the URL, the system ensures the person is logged in as the user the survey instance is assigned to. Only the assigned user can access the survey questionnaire.
  - The appropriate action occurs, depending on the **State** of the survey instance (see table).

**Survey states**

<table>
<thead>
<tr>
<th>Survey instance state</th>
<th>Action upon opening URL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ready to take:</strong> User has not saved any responses.</td>
<td>The survey questionnaire appears for the user to begin. The user can save or submit responses.</td>
</tr>
<tr>
<td><strong>In progress:</strong> User has saved at least one response.</td>
<td>The survey questionnaire appears for the user to continue. Any previously saved responses are displayed. The user can save or submit responses.</td>
</tr>
</tbody>
</table>
Obtain and distribute a general survey URL
You can distribute a general survey URL to allow any eligible user to open a survey questionnaire.
Role required: admin or survey_admin

The general URL is available on the Survey Definition form and on the survey creator. You can also email the URL for a public survey that is published.

1. Navigate to Survey > View Surveys.
2. Open a survey definition from the Assessment Metric Types list.
3. To view or copy the URL, click the View Survey URL related link.
   This related link is visible only if the survey definition is Active.
4. To distribute the URL to users, paste the copied URL as desired, or click the Email button to send via email.
   The Email button is visible only for a public survey that is published.

When a survey user clicks the general survey URL, the system creates a survey instance for the survey user as long as the user does not have an instance in the Ready to take state. The system is configured by default to send an email notification when a survey instance is generated.

As a result, the survey user receives a second notification in addition to the notification that you sent with the general survey URL. This may confuse the survey user. To avoid this issue, you can deactivate auto-notification.

Deactivate auto-notification for surveys
When you send a survey notification with a general survey URL to a survey user, the user may receive a second system-generated notification. To avoid this issue, you can deactivate auto-notification.

Role required: admin or survey_admin

1. Navigate to System Notification > Email > Notifications.
2. Open the Survey User Invite notification.
3. Configure the form to add the Send to event creator check box to the Who will receive section.
   The Send to event creator check box is selected by default.
4. Clear the Send to event creator check box.
   The system will no longer send auto-notification messages to survey users.

Obtain a survey instance URL
You can distribute a survey instance URL to allow the assigned user to open a survey questionnaire.

Role required: admin or survey_admin
The survey instance URL is available on the survey instance record.

1. Navigate to **Survey > Survey Instances**.
2. Open the instance for the survey.
3. To view or copy the URL, click **View Instance URL** related link.
   - The related link is available only when the survey instance **State** is **Ready to take** or **In progress** and the associated survey definition is **Active**.
4. In the dialog box, select and copy the URL then click **OK** or **Cancel**.
5. Distribute the URL to the assigned user.

**Test a survey URL**

When there are survey users associated with a survey, the survey is restricted so only those users can use the survey URL. You can test the survey URL to ensure it is restricted.

Role required: admin or survey_admin

1. Navigate to **Survey > View Surveys** and open a survey for which you are not a survey user.
2. Under **Related Links**, click **View Survey URL**.
3. Copy the URL and click **OK** or **Cancel**.
4. Navigate to the URL.
   - You see a message that you are not authorized to take the survey.

**Create a survey module**

You can create a module that opens a survey.

Role required: admin or survey_admin

When a user clicks a survey module, the system performs one of the following actions, depending on the configuration options for the survey and other factors.

- Creates a new survey instance
- Opens an existing survey instance
- Displays an error message.

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

<table>
<thead>
<tr>
<th>UI16</th>
<th>UI15 or UI11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Point to the application menu that contains</td>
<td>Right-click the application menu you</td>
</tr>
<tr>
<td>the module to which you want to add the</td>
<td>want to add the module to and select</td>
</tr>
<tr>
<td>survey module and click the edit application</td>
<td><strong>Edit Application Menu</strong>.</td>
</tr>
<tr>
<td>(pencil) icon.</td>
<td></td>
</tr>
</tbody>
</table>

2. In the **Modules** related list, click **New**.
3. Complete the following fields.
   - **Link type**: Assessment
     - Do not select **Survey**, which is used for legacy surveys only.
   - **Assessment**: Select the survey you want the module to open.
4. Complete and save the form.

**Sharing surveys: export and import**

You can export a survey and then import it to a different ServiceNow instance.

---

**Note:** Update sets are available in the Helsinki release and should be used to move data from one instance to another. For information about update sets, see [System update sets](#).
The system exports a single XML file that contains a survey definition (asmt_metric_type) and the associated records, including the following.

- Assessment Metric Template (asmt_template)
- Assessment Template Definition (asmt_template_definition)
- Metric definitions (asmt_metric_definition) (survey question answer options)
- Scheduled Jobs associated with the Survey (sys_trigger)
- Survey categories (asmt_metric_category)
- Survey questions (asmt_metric)
- Survey users (asmt_m2m_category_user)
- Trigger Condition (asmt_condition)

Export a survey
You can export a survey and then import it to another instance.

Role required: admin, survey_reader, or survey_admin

For information about update sets, see System update sets.

1. Navigate to Survey > View Surveys.
2. Right-click the name of a record to show the context menu.
3. Select Export Assessment.
4. If applicable, follow the prompt in your browser to save the XML file.

Import a survey
You can import a survey that has been exported as an XML file. The exported XML file does not contain result data.

Role required: admin or survey_admin

Note: Update sets are available in the Helsinki release and should be used to move data from one instance to another. For information about update sets, see System update sets.

1. Verify that the target instance has assessments enabled.
2. Follow the steps in Import an XML file to import the assessment.

Use update sets for surveys and assessments
Use an update set to capture changes to surveys and assessments.

Role required: admin or survey_admin

When developing surveys and assessments, you can use an update set to capture the changes and move them from a development instance to a production instance. Once an update set is created and marked current, all of the updates to the following tables are recorded in the update set.

The following tables are now update set enabled and also extend the application file:

- Assessment Metric Templates (asmt_template)
- Assessment Template Definitions (asmt_template_definition)
- Assessment Metric Definitions (asmt_metric_definition): survey question answer options
- Schedule (sys_trigger): scheduled jobs associated with the survey
- Assessment Metric Categories (asmt_metric_category): survey categories
- Assessment Metrics (asmt_metric): survey questions
- Assessment Category Users (asmt_m2m_category_user): survey users
- Trigger Conditions (asmt_condition)
Legacy survey migration

Users with the survey_admin role can migrate legacy survey data to create copies of legacy surveys and their related records in assessment tables. The Survey Management application, which is built on the assessment engine, is available as an alternative to legacy surveys.

The following legacy survey components are migrated:

- Survey masters
- Supported survey questions and question choices
- Survey instances
- Survey responses

Legacy survey conditions are not migrated and must be recreated as trigger conditions.

**Note:** Survey wizards cannot be migrated.

Migrate a legacy survey

Migrate a legacy survey and its related records to take advantage of a more powerful feature set.

Role required: admin or survey_admin

To avoid timing out for very large surveys, you can disable the transaction quota. See Transaction quotas.

1. Navigate to **Survey > Legacy Surveys > Masters**.
   The list of legacy survey masters appears. By default, the list shows only survey masters that have not been migrated. To show all survey masters, remove the Assessment is empty breadcrumb.
2. Open a survey and click the Migrate to Assessment related link.
   A dialog box describes what happens when you migrate the survey. Note that certain types of survey questions cannot be migrated.
3. Click OK.
   The system generates records on assessment tables based on the survey master, eligible questions and choices, results, and other related survey components. The original survey components are unaffected.
   System messages may appear at the top of the Survey form to notify you of questions that could not be migrated and to advise you to review migrated Multiple Choice questions.
4. Optional: Click the reference icon beside the Assessment field to view the new survey definition.
5. Optional: Remove survey users from the assessment survey if you want all users to be able to take it.
   When you migrate a survey, any users who have taken it are automatically associated with the assessment survey and become survey users. When there are survey users associated with an assessment survey, only those users can take it.
6. Deactivate any survey conditions associated with the survey by completing the following steps.
   a) Navigate to **Survey > Legacy Administration > Survey Conditions**.
   b) In the Active column, ensure the value is false for any survey conditions that reference the migrated survey.
7. Navigate to **Survey > Administration > Trigger Conditions** to create new trigger conditions for the migrated survey.
The **Migrate to Assessment** related link on the legacy survey record becomes unavailable after the migration. However, if you delete the record referenced in the **Assessment** field, the related link reappears and you can migrate the legacy survey again.

**Survey question migration**

Before you migrate a legacy survey, understand that some legacy survey questions cannot be migrated due to incompatible question types.

Legacy survey questions are migrated from the Survey Question (survey_question_new) table to the Assessment Metric (asmf_metric) table. In legacy surveys, the **Type** field on the Survey Question table determines how the question renders on the survey questionnaire. In assessment surveys, the **Data type** field on the Assessment Metric table serves a similar purpose. Certain legacy survey types are not supported in assessment surveys.

The following table shows the conversion path for each legacy survey question type to an assessment data type, if there is one.

<table>
<thead>
<tr>
<th>Legacy survey type</th>
<th>Assessment data type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Break</td>
<td>Not available</td>
</tr>
<tr>
<td>CheckBox</td>
<td>Checkbox</td>
</tr>
<tr>
<td>Date</td>
<td>Date</td>
</tr>
<tr>
<td>Date/Time</td>
<td>Date/Time</td>
</tr>
<tr>
<td>HTML</td>
<td>Not available</td>
</tr>
<tr>
<td>Label</td>
<td>Not available</td>
</tr>
<tr>
<td>List Collector</td>
<td>Not available</td>
</tr>
<tr>
<td>Lookup Multiple Choice</td>
<td>Not available</td>
</tr>
<tr>
<td>Lookup Select Box</td>
<td>Not available</td>
</tr>
<tr>
<td>Macro</td>
<td>Not available</td>
</tr>
<tr>
<td>Macro with Label</td>
<td>Not available</td>
</tr>
<tr>
<td>Multi Line Text</td>
<td>String (String option set to Multiline)</td>
</tr>
<tr>
<td>Multiple Choice</td>
<td>Likert Scale</td>
</tr>
<tr>
<td>Numeric Scale</td>
<td>Number</td>
</tr>
<tr>
<td>Reference</td>
<td>Not available</td>
</tr>
<tr>
<td>Select Box</td>
<td>Choice</td>
</tr>
<tr>
<td>Single Line Text</td>
<td>String (String option set to Single line)</td>
</tr>
<tr>
<td>UI Page</td>
<td>Not available</td>
</tr>
<tr>
<td>Wide Single Line Text</td>
<td>String (String option set to Single line wide)</td>
</tr>
<tr>
<td>Yes / No</td>
<td>Yes/No</td>
</tr>
</tbody>
</table>

**Migrated components**

When you migrate a survey, the system maps records from survey tables to assessment tables.

To create a functional survey on the assessment framework, the system converts survey records to the most logical equivalent assessment survey records. This may mean multiple assessment survey records represent one legacy survey record.
Migrated components

<table>
<thead>
<tr>
<th>Survey component</th>
<th>Assessment survey components</th>
</tr>
</thead>
</table>
| Survey master (survey_master)     | • Survey definition (asmt_metric_type)  
• Assessable record (asmt_assessable_record), for system use only  
• Survey category (asmt_metric_category)                                      |
| Survey question (survey_question_new) | • Survey question (asmt_metric)                                    |
| Question choice (question_choice)    | • Assessment metric definition (asmt_metric_definition)     |
| Survey instance (survey_instance)   | • Assessment group (asmt_assessment), for system use only  
• Survey instance (asmt_assessment_instance)                                 |
| Survey response (survey_response)   | • Survey instance question (asmt_assessment_instance_question)  
• Survey response (asmt_metric_result)  
• Category result (asmt_category_result), for system use only                                        |

Migrated question review

To maintain accurate result calculations, you may need to make minor adjustments to some of the migrated survey records to ensure results are calculated correctly.

**Note:** The assessment engine provides a built-in result calculation feature that converts each survey response to a score between 0 and 10. The configuration required to maintain accurate result calculations is advanced and is not recommended for basic survey implementations. If you do not plan to use result calculation data, ignore the information in this section.

For each legacy question migrated, the system creates a survey question record on the Assessment Metric (asmt_metric) table. For legacy questions of the **Multiple Choice** and **Select Box** types, the system also creates a metric definition record, on the Assessment Metric Definition (asmt_metric_definition) table, for each legacy question choice.

**Comparable metric definitions and survey question choices**

<table>
<thead>
<tr>
<th>Survey question choice field</th>
<th>Related metric definition field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text</td>
<td>Display</td>
</tr>
<tr>
<td>Value (can be any string value)</td>
<td>Value (must be a numerical value)</td>
</tr>
<tr>
<td>Order</td>
<td>Value (metric definition with smallest Value is first)</td>
</tr>
</tbody>
</table>

When the system migrates legacy survey question choices, it uses the legacy **Order** to set each metric definition **Value**. For the legacy question choice with the smallest **Order**, the corresponding metric definition **Value** is set to **1**. For the legacy question choice with the next smallest **Order**, the metric definition **Value** is **2**, and so on.
The **Scale definition** field on the migrated Survey Question form determines whether smaller or bigger metric definition values equate to a good score in survey result calculations. By default, the scale definition is set to **High**, meaning bigger values are good. When you migrate a legacy survey, check that the default scale definition makes sense for each question.

For example, the following tables depict a sample migrated question and the metric definitions automatically created for it. Recall that the system uses the order of the legacy survey question choices to set the metric definition value. **Excellent** has the lowest **Order** value, so when the system creates a metric definition for this question choice, the **Value** is set to 1. In this case the default scale definition value, **High**, does not make sense, as the system will calculate the worst scores for responses of **Excellent**.

<table>
<thead>
<tr>
<th>Question choice text</th>
<th>Question choice value</th>
<th>Question choice order</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excellent</td>
<td>A</td>
<td>100</td>
</tr>
<tr>
<td>Good</td>
<td>B</td>
<td>200</td>
</tr>
<tr>
<td>Fair</td>
<td>C</td>
<td>300</td>
</tr>
<tr>
<td>Poor</td>
<td>D</td>
<td>400</td>
</tr>
</tbody>
</table>

Legacy question: Please rate the overall quality of your service.

<table>
<thead>
<tr>
<th>Metric definition display</th>
<th>Metric definition value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excellent</td>
<td>1</td>
</tr>
<tr>
<td>Good</td>
<td>2</td>
</tr>
<tr>
<td>Fair</td>
<td>3</td>
</tr>
<tr>
<td>Poor</td>
<td>4</td>
</tr>
</tbody>
</table>

If there are no **Order** values for the legacy survey question choices, the system sets each corresponding metric definition **Value** based on the alphanumerical order of the legacy **Text** value.

<table>
<thead>
<tr>
<th>Metric definition display</th>
<th>Metric definition value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excellent</td>
<td>1</td>
</tr>
<tr>
<td>Good</td>
<td>2</td>
</tr>
<tr>
<td>Fair</td>
<td>3</td>
</tr>
<tr>
<td>Poor</td>
<td>4</td>
</tr>
</tbody>
</table>

You may also need to change the **Scale definition** setting for other migrated questions. For details, see the scale definition recommendations for each survey question data type.

**Quizzes**

Quizzes are questionnaires you can assign to one or more users to assess their knowledge of any subject. The quiz functionality is built on the assessment engine and provides many of the same features as assessments and surveys.
Each question is scored, and the overall score indicates the percentage of questions the user answered correctly. A quiz may have categories of questions that are assigned only to some users. You can assign weighting values to individual questions or categories of questions that make them more or less important when calculating the overall score. Quizzes require activation by a system administrator.

- An administrator can create a quiz for any purpose and assign it to a single user or multiple users.
- A quiz can contain one or more categories of questions. Each category can be assigned to users who answer only the questions in that category.
- The system can send email notifications to these users:
  - Recipients: The recipient can receive notification of an assigned quiz, a quiz whose allowed duration is at 50%, and a quiz that is overdue.
  - Recipient's manager: The recipient's manager can receive notification when a quiz is overdue.
  - Quiz manager: The quiz manager can receive notification of an overdue quiz to which he or she is assigned.
- Quizzes can contain questions that are scored or not scored. Unscored questions assess opinions or involve dates and are not counted in the final score. Scored questions specify correct answers and are scored either as 0% or 100%. You can apply a weighting scale to scored questions to establish their relative importance. You can designate questions with these data types as scored questions:
  - Checkbox
  - Choice
  - Duration
  - Likert Scale
  - Numeric Scale
  - Template
  - Yes/No
- A quiz question can be dependent on the response to any scored question. For example, you can create a dependent question requesting additional information that appears only if a recipient answers No to a specific question.

Important terms

The quiz application involves several terms.

<table>
<thead>
<tr>
<th>Terms used in quiz application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quizzes</td>
</tr>
</tbody>
</table>
Categories

A quiz category represents a theme for quiz questions. Each category contains one or more questions and names the recipients for the questions in that category. By default, the system creates one category with the same name as the quiz. You can create additional categories as needed. Categories can be weighted higher or lower to determine the importance of that category in the overall score.

Questions

A quiz question is a question configured for a category and sent only to the users for that category. Questions have a wide variety of data types and can be individually weighted higher or lower. Questions may be scored or unscored.

Category user

A category user is the recipient of questions for a specific category. You can select different users to answer the questions for each category.

Templates

A template is a question data type that provides reusable rating scales for answers to questions. For example, the answer template named Satisfaction contains a satisfaction scale ranging from Very Satisfied to Very Dissatisfied.

Quiz roles

The Quizzes application uses these roles. No role is required to take quizzes that are assigned to you.

<table>
<thead>
<tr>
<th>Role Title (Name)</th>
<th>Role Description</th>
</tr>
</thead>
</table>
| assessment administrator (assessment_admin) | Can administer the Assessments application and all quiz records. Can access all the modules of the Assessments application.  
Note: The itil_admin role and the survey_admin role contain the assessment_admin role |
| Administrator (admin)              | Can access all aspects of the assessment and survey processes. Only administrators can modify survey notifications, create survey modules, and import surveys. |

Set up and administer quizzes

Set up and administer quizzes.

Role required: assessment_admin or admin

1. Optional: Create reusable question templates for quizzes.
2. Create the quiz using the Quiz Designer or with forms accessed from the navigation menu.

The quiz record includes specifics such as duration, notification preferences, a questionnaire introduction, and ending notes displayed to recipients.
3. Edit the default category or create additional categories as needed. The system creates a category with the same name as the quiz.

4. Define users for each category. These are the recipients who answer the questions in a category. You can define different users for each category.

5. Create the questions for each category.

6. Create the answers for each question and determine if the questions are scored. You can create unique answers or select preconfigured answers from a template.

Publish and distribute the quiz. You can send the quiz to a single user or all users in each category. Review the results from the submitted quizzes in reports and scorecards.

Activate the quiz designer

Administrators can activate the Quiz Designer plugin.

Role required: assessment_admin or 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.

Quiz Overview module

The Quiz Overview module is a homepage that displays various reports on data such as results for each category and quizzes that are complete, pending, or in progress.

Role required: assessment_admin or admin

Users with the assessment_admin role can view the overview page and refresh, add, delete, and rearrange widgets.

1. Navigate to Quizzes > Overview.

2. Click elements within reports to obtain more information. The available reports are:

<table>
<thead>
<tr>
<th>Report</th>
<th>Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quizzes by State</td>
<td>Assessment Instance (asmt_assessment_instance)</td>
</tr>
<tr>
<td>Total Questions by Quiz</td>
<td>Assessment Metric (asmt_metric)</td>
</tr>
</tbody>
</table>
Quiz designer

The quiz designer provides a single interface that users with the assessment_admin role can use to create, edit, and distribute quizzes.

You can also use it to edit existing quizzes and change scoring parameters.

Alternatively, you can use the modules of the assessment engine to create and edit the records that make up a quiz. All quiz records are stored in assessment tables and displayed in Quiz views of those tables. For details, see Create quizzes with forms.

Tools on the Quiz designer

The quiz designer includes a design canvas, a header bar, and many controls that you can use to create quizzes.

To open the quiz designer, navigate to Quizzes > Quiz Designer.

The designer contains the following elements:

- Controls
- Header bar
- Design canvas

Controls

Controls for the supported question data types are available in the Controls palette. Drag and drop a control onto the designer canvas to create a question of that type.
### Question controls

<table>
<thead>
<tr>
<th>Data type</th>
<th>Description</th>
<th>Scored</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachment</td>
<td>Question with a Manage Attachments icon that allows users to attach one or more files.</td>
<td>Y</td>
</tr>
<tr>
<td>Boolean</td>
<td>Question with a check box or a Yes/No list for user responses.</td>
<td></td>
</tr>
<tr>
<td>Data type</td>
<td>Description</td>
<td>Scored</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
</tbody>
</table>
| Choice     | List of predefined options. For more information, see the definition for **Choices**  
Create quiz questions.                      | Y      |
| Date       | Date field.                                                                 | N      |
| Date/Time  | Date and time field.                                                         | N      |
| Number     | Number field with predefined minimum and maximum values. The default is 1-10. | N      |
| Percentage | Percentage field with a prescribed range.                                    | N      |
| Scale      | Predefined Likert scale. Answer options appear as radio buttons.             | Y      |
| Numeric Scale | Selectable number scale. The default is 1-5. Answer options appear as radio buttons. | Y      |
| String     | Single or multiline text field.                                              | N      |
| Template   | Choice list of templates that provide a predefined scale of options. For details, see  
Configure a template question.                     | Y      |
| Reference  | Choice list of fields from a specified reference table. This data type does not support reference qualifiers. | N      |

**Header Bar**

The header bar contains tabs that display different views and a menu of various functions.

Click one of the following tabs to change the view in the canvas:

- **Design**: Add categories and questions, and configure the properties of each. This is the default view of the canvas when you open the designer.
- **Configuration**: Create introductions and end notes for quizzes, and select a signature.
- **Availability**: Select the recipients for each category in the quiz.

Point to the menu icon (≡) in the upper right of the quiz designer to select the following options:

- **Save**: Saves the current quiz.
- **Preview**: Displays a preview of the quiz as it appears to the recipients.
- **Publish**: Distributes the quiz to the selected recipients.
- **Save and Publish**: Saves and distributes the quiz in one step.
- **New Quiz**: Opens a fresh canvas for a new quiz.
- **Load Quiz**: Opens a list of existing quizzes that you can select and edit.

The availability of each option depends on the status of the quiz that is opened in the quiz designer.

**Design Canvas**
New quizzes open in the Design view. The quiz Name field appears above first category in the canvas. A blank question field appears in the category container.

Create a quiz

When you create a quiz, you can create one or more categories and then add questions to each category.

Role required: assessment_admin or admin

Each category can be assigned to a different user or the same users. You can also customize each question and make it dependent on the response to another question.

Create a quiz using these procedures:

Create quiz categories
A category represents a theme for evaluating a specific element of the quiz topic and contains questions pertaining to that theme.

Role required: assessment_admin or admin

When you create a quiz, the system creates a default category, using the name of the quiz. You can use this category, modify it, or create additional categories as needed. To have any results, a category must contain scored questions.

1. Navigate either Quizzes > Quiz Designer or Quizzes > Quizzes and click Quiz Designer in the list header.
2. Enter the name of the quiz in the Name field. The system uses this name as the name of the quiz and the first category.
3. To configure the category, click the gear icon in its title bar.
   The Properties dialog box appears. You can change the name of the category, add a description for it, and enter text in the Details field that introduces or explains the category to the recipients. The system updates the category as you type.
4. Click the X icon to close the category properties dialog box and save your settings.
5. To add a new category, click the + icon in the title bar of an existing category.

Create quiz questions
You can create multiple questions for each category but each question can be associated with only one category.

Role required: assessment_admin or admin

The data type that you select for each question determines how it can be answered by quiz recipients.

You can designate questions to be scored. Only scored questions are shown in the quiz results and considered when calculating the category results. You must also specify a correct answer for scored questions.

Note:
To designate a question as scored, you must use Assessment forms. For instructions, see Configure a scored question.

1. In the Design view, drag a data type icon from the Controls palette and drop it into a category container.
2. To configure the question, click in the gear icon in its title bar. The Properties dialog box appears for the question.
3. Fill in the fields on the form, as appropriate.

**Question property fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>(Required) Name of the question. Create a concise and easily recognizable name for your question. The system uses this value to identify the question in Assessment Metric lists and in scorecard charts.</td>
</tr>
<tr>
<td>Question</td>
<td>Text to display as the question on quizzes. Enter a clear, straightforward question that is easy to understand.</td>
</tr>
<tr>
<td>Type</td>
<td>(Read-only) Data type selected for this question. See the table in controls for possible data types.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Active</td>
<td>Check box that determines whether this question is available on a quiz. If a question is marked inactive, it does not appear on quizzes generated after the question becomes inactive.</td>
</tr>
<tr>
<td>Boolean option</td>
<td>Whether a check box or a Yes/No list appears as the option for the Boolean question.</td>
</tr>
<tr>
<td>Mandatory</td>
<td>Check box for requiring users to answer the question. Users cannot submit quizzes until they answer all mandatory questions, which are denoted by a red Introduction_to_Fields#Field_Status_Indicator field status indicator.</td>
</tr>
<tr>
<td></td>
<td>This field is available when the question does not have a dependency and the question controls is not Boolean with a check box option.</td>
</tr>
<tr>
<td>String option</td>
<td>Setting for the appearance of a string field in a question. This field is available when the question type is String. The string options are:</td>
</tr>
<tr>
<td></td>
<td>·  <strong>Single line</strong>: Single line text field 40 characters in length that allows strings of any length.</td>
</tr>
<tr>
<td></td>
<td>·  <strong>String line wide</strong>: Full page width text field that allows a single line entry of any length.</td>
</tr>
<tr>
<td></td>
<td>·  <strong>Multiline</strong>: Full page width multi-line text field that allows word wrap and returns.</td>
</tr>
<tr>
<td>Min</td>
<td>Lowest positive whole number that users can enter or select to answer the question. This field is available when the question type is Number, Percentage, or Numeric Scale.</td>
</tr>
<tr>
<td>Max</td>
<td>Highest positive whole number that users can enter or select to answer the question. This field is available when the question type is Number, Percentage, or Numeric Scale.</td>
</tr>
<tr>
<td>Allow not applicable</td>
<td>Check box for including Not Applicable as an option for this question. Users can select Not Applicable if they do not have sufficient information to respond to a question. User responses of Not Applicable are excluded from results calculations. This field is available when the question does not have a dependency and the question data type is not Boolean with a check box option.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Randomize answers</td>
<td>Check box for displaying answer options in a random order whenever the question appears in a quiz. Answer preference is sometimes influenced by the order in which options appear, which can result in biased results. Randomizing options can help prevent this bias. <strong>Note:</strong> Randomizing options for certain questions may make those questions confusing for users. In general, only randomize options that do not follow a logical order.</td>
</tr>
<tr>
<td>Details</td>
<td>Information about the question that is displayed on the quiz. Include details that help users understand how to answer the question. You can also enter HTML text in this field with the WYSIWYG editor. For example, include HTML to embed links and images.</td>
</tr>
<tr>
<td>Correct answer</td>
<td>Answer option that you want to be selected by users. When you specify a correct answer for a question, the system scores the question. This field is available for all data types except Date, Date/Time, and String.</td>
</tr>
<tr>
<td>Choices</td>
<td>Options for a question with a data type of Choice or Scale. The system automatically adds text and values that you can edit for each option. Click the + icon to add an option, or click the X icon to delete an option. By default, the system arranges options in the order established by their values. To change the order, drag and drop the options.</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>
<tbody>
<tr>
<td>Displayed when</td>
<td>Condition builder that hides or displays the question depending on the answer to another question in the same category. Select an existing question from the list with a data type of Boolean, Choice, Scale, or Template. Create the condition that must exist for recipients to see the dependent question, using the is or is one of operator. The system prevents recursive dependencies between questions. For example, if Question A depends on Question B, Question B cannot depend on Question A.</td>
</tr>
</tbody>
</table>

4. To create any special conditions that must be met for a question to appear on the quiz, click the Dependency tab. Fill in the fields, as appropriate.

Dependent questions appear on the quiz when a recipient selects a specific answer or combination of answers to another question in the same category.

5. Select a question in the Displayed when field. The system selects the appropriate operator and displays the possible answers for the selected question.

6. Select the answers that satisfy the condition. Selected answers are indicated by a check mark.

7. Click X to close the question properties dialog box and save your settings.

8. To add a question with the same data type as an existing question in the category, click the + in the title bar of the existing question.
9. Drag questions to change their order within a category or move them between categories.
10. To delete a question, click the X in its title bar.

Configure a template question
You can configure template questions when designing quizzes.

Role required: assessment_admin or admin

1. Drag the Template data type icon into a category container.
2. Click the gear icon in the question title bar to open the template properties dialog box.
3. Select a predefined scale from the list.

Question entry fields appear for that template.
4. Enter one or more questions that are appropriate for the template.
5. Click the arrow to the right of a question to configure its properties. You must provide a name for each question.
6. Click the up or down arrow to move between questions, or click the back arrow to return to the template properties dialog box.
7. Configure the properties for the remaining questions.
8. Click the X icon to close the template properties dialog box and save your settings.

Configure a scored question
Only scored questions are considered when calculating category and quiz results.
Role required: assessment_admin or admin
A question must have a correct answer specified to be scored. Only results for scored questions are displayed in the quiz scorecard.

1. Navigate to Quizzes > Quizzes.
2. Open the quiz containing the questions you want to mark as scored.
3. In the Metric Categories related list on the Assessment Metric Type form, select the category for the questions you want to mark as scored.
4. In the Assessment Metrics related list on the Metric Category form, select a question from the list.
5. In the Question Type section of the Assessment Metric form, select the Scored check box.
This check box is not available if the question’s data type is not supported for scoring.

6. Select the Correct answer for the question.
7. Click Update.
8. Repeat the process for all the questions in the category that you want the system to score.
9. Return to the list of metric categories, select another category, and configure scoring for the appropriate questions in that category.

Configure a quiz

You can configure an entire quiz.

Role required: assessment_admin or admin

The values you enter and select on this page are applied to the entire quiz.

In the quiz designer, click Configuration and then fill in the fields as described in the table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Check box for enabling the distribution of this quiz to recipients.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of this configuration or the quiz to which it is attached.</td>
</tr>
<tr>
<td>Introduction</td>
<td>Introductory content to display on quizzes. You can add a welcome message or background information about the quiz.</td>
</tr>
<tr>
<td>Signature</td>
<td>(Optional) Acknowledgement by a quiz recipient of requirements, admonitions, or expectations related to a quiz.</td>
</tr>
<tr>
<td>Return URL</td>
<td>Destination address of a web page that is presented to users after they submit a completed quiz. When a return URL is configured, the End note content does not appear.</td>
</tr>
<tr>
<td>End note</td>
<td>Content that is displayed to recipients after they submit a completed quiz. You can add a thank you message, follow-up instructions, or other applicable information. End notes are not displayed if a Return URL is specified.</td>
</tr>
<tr>
<td>Duration</td>
<td>Amount of time that recipients are given to complete this quiz, starting from the time that the quiz is generated. The default duration is 14 days.</td>
</tr>
<tr>
<td>Manager</td>
<td>Assessment manager for this quiz. These users are only responsible for managing the quiz process and not the results. The system notifies the manager when submissions for this quiz are past due.</td>
</tr>
<tr>
<td>Notify manager if overdue</td>
<td>Check box for sending email notifications to a recipient’s manager when that user fails to submit an assigned quiz before the due date.</td>
</tr>
</tbody>
</table>
Select a quiz recipient
When the system distributes a quiz, it sends email notifications to the category users and their managers.

Role required: assessment_admin or admin
A category can have one or more assigned users, and the same user can be assigned to more than one category.

The system also creates a link to the quiz in the recipients' My Assessments & Surveys portal. Users can only answer questions in the categories that they are assigned to.

To select the recipients for each quiz category, click Availability and then fill in the fields as described in the table.

Select recipients

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select category</td>
<td>Category for which the selected users are recipients.</td>
</tr>
<tr>
<td>Add users</td>
<td>Users selected as recipients for this category. The choice list shows all users in the system.</td>
</tr>
</tbody>
</table>

Publish a quiz
When you publish a quiz, the system sends email notifications to the recipients and to their managers. A card in each recipient's My Assessments & Surveys portal displays a link to the quiz.

Role required: assessment_admin or admin

1. If you want to see the quiz as the recipients will see it, point to the menu icon in the upper right of the quiz designer and click Preview.
2. When you are satisfied with the quiz, click Save and Publish or Publish to distribute it.

Edit a quiz
You can update a quiz after the quiz has been distributed.

Role required: assessment_admin or admin

- Questions that you add are available only on quizzes that are distributed after the update.
- Before a quiz is submitted or during the retake period:
  - Changes to existing questions are immediately available to users. This includes changes to the answers, such as additional choices or changes to the data type.
  - Deleted questions are deleted from distributed quizzes in users' queues.

Open the quiz: Group the Service Details form with one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quizzes &gt; Quiz Designer</td>
<td>Point to the menu icon in the quiz header bar and select Load Quiz.</td>
</tr>
<tr>
<td>Quizzes &gt; Quizzes</td>
<td>Right-click a quiz in the list and select Quiz Designer.</td>
</tr>
<tr>
<td>Quizzes &gt; Quizzes</td>
<td>Open a quiz from the list and click Quiz Designer in the header of the Assessment Metric Type form.</td>
</tr>
</tbody>
</table>
Enable a quiz retake

You can configure a quiz to allow recipients to resubmit their answers as many times as they like, until the quiz's due date.

Role required: assessment_admin or admin

Results are not calculated until the quiz's configured duration has elapsed. The card in the user's queue remains visible until the quiz's due date and displays a button to allow retakes.

1. Navigate to Assessments > Metric Definition > Types.
2. Remove the Evaluation method = Assessment filter condition so you can see all the records in the list.
3. Open the quiz.
4. In the Assessment Metric Type form, select the Allow retake check box and save the record.

View a quiz result

You can view quiz results for each question and category, or view the quiz scorecard for a detailed breakdown.

Role required: assessment_admin or admin

Quiz results are stored in the Metric Result (asmt_metric_result) table and display recipients' answers to each question in a category.

Navigate to Quizzes > Quiz Results.

View a quiz designer scorecard

The quiz scorecard opens in the Category Results view.

For detailed information about scorecards, see Quiz Scorecards.

1. Navigate to Quizzes > Quizzes.
2. Open the quiz whose results you want to view.
4. The scorecard for the selected quiz opens in the Category Results view.
4. Select a category to view from the choice list above the chart.
**View a quiz category result**

Category results are stored in the Assessment Category Result (asmt_category_result) table and display the overall ratings for each category based on the weighted value for each scored question.

1. To view category results, navigate to **Quizzes > Category Results**.

![Assessment Category Results](https://example.com/assessment-category-results.png)

2. The system calculates results from the weight configured for each category. Weights are set to a value of 10 by default but can be changed. To edit a category's weight:

3. Navigate to **Quizzes > Categories**, and select a category from the list.

4. In the Metric Category form, edit the default value in the **Weight** field.

5. Click **Update**.

**Note:** You can also edit the weight of a question in the Quiz view of the Assessment Metric form.

**Take a quiz**

All available quizzes assigned to you appear in your personal assessment and survey queue. When you submit a quiz, the system stores your responses. If a quiz allows retakes, you can resubmit it as many times as you like until its due date.

**Role required:** none

No special role is required to complete a quiz, but you must be logged in and the quiz must be assigned to you.

If configured to send email, the system sends you a notification when a quiz is assigned to you. The message contains a link to the quiz and instructions for viewing the assessment and survey queue.

Each quiz assigned to you appears in your assessment and survey queue as a card that contains information about the quiz, including a launch button. Overdue quizzes are marked with a red icon and red due date.

You must answer every required question, indicated by a red star, before you can submit the quiz. If you start to take a quiz but cannot complete it, save your responses and return to it later. When you have answered all the questions and are satisfied with the responses, submit the quiz.

By default, you cannot modify your answers to a quiz after submission. However, if the administrator has configured this quiz to allow retakes, the quiz remains in your queue after you
finish it and the card shows a Modify Quiz button. You can retake the quiz as many times as you like before the due date.

1. Navigate to **Self-Service > My Assessments & Surveys**.
2. Click **Take Quiz** on a quiz card to open the questionnaire. If there is more than one quiz category, you can click the collapse or expand icon to hide or show the questions in the category.
3. Answer each question to the best of your ability. If you are unsure of how to respond to a question or if a question does not apply to you, select Not Applicable, if that choice is available.
4. Click **Save** at any time to save your responses without submitting them. You can reopen the quiz from your queue when you are ready to work on it again.
5. When you are ready to submit the completed quiz, read any assertions that require your attention.
6. If present, select the check box to acknowledge the assertion. If your full name is displayed, you are required to provide authentication to acknowledge the assertion after you submit the quiz.
7. Click **Submit**.
8. If prompted, enter your user name and password to verify your signature. If you provided valid answers for all mandatory questions, a success message appears, displaying any end note that was configured. If the quiz allows retakes, the card remains in your queue with a Modify Quiz button after submission. If retakes are not permitted, the card disappears from your queue.
9. If the system displays an error message indicating that a question has an invalid response or must still be answered, correct the error and resubmit the quiz.
10. To edit your answers and resubmit a quiz that permits retakes, click **Modify Quiz**. You can modify your responses to the quiz until its due date.

### Quiz scorecards

The Quizzes application prepares printable scorecards.

A scorecard analyzes category and question responses and compares current ratings with previous ratings. You can examine ratings over time, compare question ratings, or compare the ratings of all categories. All ratings are averages for the time range selected.

The system dynamically updates a scorecard each time you view it, so the ratings reflect recently completed quizzes.

### Category results

The Category Results view is a stacked bar chart of responses to all questions in a category.

Select the category to display from the choice list above the chart. Category results are only calculated for scored questions.

This view displays responses that use the following data types:

- Checkbox
- Choice
- Likert Scale
- Number
- Template
- Yes/No
Note: The Checkbox and Yes/No data types are combined into the Boolean data type in the Quiz designer.
Company Policies

Quiz Scorecard

<table>
<thead>
<tr>
<th>Category</th>
<th>Dress Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mera Trousers</td>
<td>[Diagram of Mera Trousers]</td>
</tr>
<tr>
<td>Shirt</td>
<td>[Diagram of Shirt]</td>
</tr>
<tr>
<td>Shoe</td>
<td>[Diagram of Shoe]</td>
</tr>
<tr>
<td>Skirt Length</td>
<td>[Diagram of Skirt Length]</td>
</tr>
</tbody>
</table>

Legend:
- Casual cotton
- Jeans
- Muscle-T
- N/A
- No
- Polo
- Yes
To view details about a specific response to a question, point to the colored segment representing
a specific response. The chart displays the count for those responses and the percentage it
represents of the total responses to that question.

Quiz category result details

Question results
The Question Results view shows the results for all questions in a quiz.
Select a question by name from the choice list to display the results in a pie chart or a bar chart,
based on the data type.

Pie chart
The pie chart shows question results for these data types:
- Checkbox
- Choice
- Likert Scale
- Number
- Template
- Yes/No

Note: The Checkbox and Yes/No data types are combined into the Boolean data type in the Quiz designer
Quiz scorecard question results - pie chart
Bar chart

A bar chart appears when question results use this data type:

- Percentage

By default, all results for percentage questions use a report range of 20% segments. To configure a report range, navigate to Reports > Administration > Report Ranges.

Average ratings

The Average Ratings view displays a bar chart of the weighted average rating for each question in a category.

Use this view to learn how individual questions affect the overall rating for the category. Select a category from the second choice list above the chart. Ratings are only calculated for scored questions.
Average Ratings view

To view the effect of each question’s ratings on the entire category’s ratings, point to the colored bar. The pop-up box shows the percentage of the total ratings represented by each individual question’s weighted average.
Quiz reports

Quizzes provide several global reports so that assessment administrators can view important statistics.

You can share these reports with specific users or groups and change the display options.

For detailed field information and reporting options, click the link for the chart Type. To sort a column in ascending or descending order, click the arrow in the column heading.

<table>
<thead>
<tr>
<th>Quiz reports</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Quizzes by State</td>
<td>State of distributed quizzes. This chart displays the percentage of distributed quizzes that are ready to take, in progress, complete, or canceled.</td>
</tr>
</tbody>
</table>
|               | • **Type**: Pie Chart  
|               | • **Table**: Assessment Instance (asmt_assessment_instance) |
| Total Questions by Quiz | Total number of questions for all categories in each quiz. |
|               | • **Type**: Bar Chart  
|               | • **Table**: Assessment Metric (asmt_metric) |
| Questions by Data Type | Total number of questions in all quizzes by data type. |
|               | • **Type**: Bar Chart  
|               | • **Table**: Assessment Metric (asmt_metric) |
| Correct Answers by Assigned User | Total number of scored questions answered correctly by each assigned user. |
|               | • **Type**: Bar Chart  
|               | • **Table**: Metric Results (asmt_metric_result) |
| Number of Correct Answers | Total number of correct answers for each scored question. |
|               | • **Type**: Bar Chart  
<p>|               | • <strong>Table</strong>: Metric Results (asmt_metric_result) |</p>
<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorrect Answers by Assigned User</td>
<td>Total number of scored questions answered incorrectly by each assigned user.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Type</strong>: Bar Chart</td>
</tr>
<tr>
<td></td>
<td>• <strong>Table</strong>: Metric Results (asmt_metric_result)</td>
</tr>
<tr>
<td>Number of Incorrect Answers</td>
<td>Total number of incorrect answers for each scored question.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Type</strong>: Bar Chart</td>
</tr>
<tr>
<td></td>
<td>• <strong>Table</strong>: Metric Results (asmt_metric_result)</td>
</tr>
</tbody>
</table>

**Wizards**

The Wizards functionality, which enabled administrators to create wizards that provide a step-by-step sequence of dialog boxes that lead the user through a procedure, was deprecated in the Eureka release. However, some users are still able to access this functionality if they enabled its plugin in previous releases.

For more information about this functionality, see https://docs.servicenow.com/bundle/archive/page/archive/fuji-archive.html.

**Survey wizards**

The Survey Wizard plugin creates surveys using wizards. Advantages versus other survey functionality include the ability to:

- Ask different questions based on responses (dynamic surveys)
- Create multiple page surveys
- Record answers for partially completed surveys

This plugin integrates with the Best Practice - Task Survey Management plugin. Because the plugin relates to the Legacy Surveys application, the plugin is documented on the ServiceNow wiki.

**Configure the survey property**

How to configure the survey properties (apply to all survey wizards and surveys).

1. Navigate to **Survey Wizards > Survey Properties**.
2. Ensure the Enable the enhanced task survey capabilities. Survey distribution is controlled by Survey Conditions. property is enabled (select the check box).

**Create a page**

How to create the survey pages (wizard panels) and add questions.

1. Navigate to **Survey Wizards > All** and open the survey wizard.
2. In the **Survey Panels** related list, click **New**.
3. Enter the Name, Title, and Description.
4. Right-click the header and select **Save**.
5. In the **Variables** related list, click **Edit**.
6. Using the **slushbucket**, select and arrange survey questions on the panel.
7. Repeat steps 1 – 6 for each page of the survey wizard.

   **Note:** To learn more, see *Wizard Panels*.

---

### Create a dynamic effect optional

Create dynamic effects, such as hiding or showing fields on a panel based on answers.

1. Navigate to *Survey Wizards > Wizard Policy > Wizard UI Policy* or *Survey Wizards > Wizard Policy > Wizard Client Scripts*
2. Click *New*.
3. Enter the UI policy or client script details.

   **Note:** For more information, see *wizard scripts*.

---

### Define a transition

Transitions define the logic used to move between pages (wizard panels) in a survey.

Use panels and transition logic to implement multiple page surveys and dynamic effects, such as skipping pages based on answers.

Define transitions:

1. Navigate to *Survey Wizards > All* and open the survey wizard.
2. Open a survey panel.
3. In the *Wizard Panel Transitions* related list, click *New*.
4. Enter the transition details and click *Submit*.
5. Repeat steps 1 – 4 for all transitions between pages in the survey wizard.

   **Note:** To learn more, see *Wizard Transitions*.

---

### Create a survey condition

How to create a survey condition that controls when and to whom the survey wizard is sent.

Create a *survey condition* that controls when and to whom the survey wizard is sent:

1. Navigate to *Survey Wizards > Survey Conditions*.
2. Click *New*.
3. Select a *Type* of Survey Wizard. Only a survey or survey wizard is sent (determined by *Type*), even if both are defined for the condition.
4. Enter the condition details.
5. Click *Submit*.

---

### Create the email notification

Create an email notification to deliver the survey wizard.

Role required: admin or survey_admin

1. Navigate to *System Notification > Email > Notifications*.
2. Filter the list to view notifications with an *Event Name* of `task.send_survey`, which is the event that is triggered when survey conditions are met.
3. Open a survey notification in the filtered list or click *New*.
4. Enter the email notification details. If you are creating a new notification, be sure to adjust conditions and weight to avoid conflicts with existing survey notifications (Event Name of task.send_survey).
5. Click Update or Submit.

Create the survey wizard

How to create the survey wizard.

The following steps provide an overview of building a survey wizard.
1. Activate the Survey Wizard plugin, if necessary.
2. Navigate to Survey Wizards > All.
3. Click New.
4. Enter the survey wizard Name.
5. In the Roles field, add the public role.
6. Right-click the header and select Save.

Define a question

How to define survey questions (wizard variables).
1. In the Wizard Variable related list, click New.
2. Enter the variable details.
3. In the Read roles field, add the public role.
4. Configure the form to add the Read roles field, if necessary.
5. Click Submit.
6. Repeat steps 1–4 for all questions in the survey.

Note: To learn more, see Define a Wizard Variable.

Installed components

Fields, tables, a business rule, a script include, an application, a survey wizard panel, and demo data (optional).

The following tables are modified:

<table>
<thead>
<tr>
<th>Display Name (Table Name)</th>
<th>Modification</th>
</tr>
</thead>
</table>
| Survey Conditions (survey_conditions) | Add fields to determine which survey is sent when conditions are met:  
• Type - either a survey or survey wizard  
• Survey_wizard - reference to applicable survey wizard |
| Task Survey (task_survey) | Add fields to track which surveys were sent to users:  
• Type - either a survey or survey wizard  
• Survey_wizard - reference to applicable survey wizard |
The following tables are added:

### New tables

<table>
<thead>
<tr>
<th>Display Name (Table Name)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Survey Panel (expert_panel_survey)</td>
<td>Adds a survey panel to wizards. Extends the expert_panel table</td>
</tr>
<tr>
<td>Survey Wizard (expert_survey)</td>
<td>Stores survey wizards. Extends expert</td>
</tr>
</tbody>
</table>

The **SurveyUtils** script include is added to record responses during survey panel transitions.

The **Task Survey Events** business rule is modified to include logic for sending survey wizards. Customers who have modified this business rule can not install the updated version automatically.

For information about the link generated from the business rule script, see [Survey Wizard - Multiple Instances](https://community.servicenow.com) on the ServiceNow Community.

The plugin adds **Survey** as a new type of wizard panel. Survey wizards are created using survey panels.

Survey wizard responses are saved when the user navigates between survey panels (clicks **Next** or **Previous**), as opposed to saving responses only at the end (surveys). This feature allows a logged in user to resume a survey that is in progress and allows survey readers to collect response data for partially completed surveys. To support the ability to resume surveys in progress, survey wizard answers are also temporarily stored in XML in the `expert_instance` table. When the user clicks **Done** on the last panel of the survey wizard, the record in the `expert_instance` table is deleted.

For information about having more than one instance of a given Wizard in play at a time, see [Survey Wizard - Multiple Instances](https://community.servicenow.com) on the ServiceNow Community.

Demo data is available with this plugin. If you choose to install demo data, a sample survey wizard, called Customer Satisfaction Survey, is added to the database.

### Request survey wizard

Before activating this plugin, consider the installed components, dependencies, and impact.

- **Installed Components** - fields, tables, a business rule, a script include, an application, a survey wizard panel, and demo data (optional). For more details, see [Installed Components](https).
- **Dependencies** - Best Practice - Task Survey Management (active by default)
- **Impact** - adds fields to existing tables, installs the Best Practice - Task Survey Management plugin, and modifies the Task Survey Events business rule. You may choose to install a demo survey with the plugin. The plugin integrates with standard survey functionality, so there is no need to transition existing surveys to survey wizards. However, survey administrators must specify a type (survey or survey wizard) for new survey conditions.

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

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 timezone, 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 | Any information that would be helpful for the ServiceNow personnel activating the plugin such as if you need the plugin activated at a specific time instead of during one of the default activation windows. |

3. Click **Submit**.

### Test the survey wizard

How to test the survey wizard.

1. Navigate to **Survey Wizards > All** and open the survey wizard.
2. Click **Try it**.
3. Answer survey questions and verify the transition logic based on answers, if applicable.
4. At survey completion, click **Done**.
5. Navigate to **Survey Wizards > Survey Instances**.
6. Search for and open the most recent instance of the survey wizard.
7. Verify that your survey answers are properly recorded.
8. Run through several scenarios to test transition logic and data collection.

### Create a survey wizard (demo)

This example creates a survey using a survey wizard.

This example creates a survey using a survey wizard (requires the [Survey Wizard plugin](#)). The survey uses dynamic features that are available using wizards.

**Create the survey wizard demo**

Create the survey wizard.

1. [Activate the Survey Wizard plugin](#), if necessary.
2. Navigate to **Survey Wizards > All**.
3. Click **New**.
4. In the Name field, enter **Software Needs Analysis**.
5. In the Roles field, add the **public** role.
6. Right-click the header and select **Save**.
Define a survey question
How to define survey questions (wizard variables).

1. In the Wizard Variable related list, click **New**.
2. Enter the variable details as listed in the table.
3. In the Read roles field, add the **public** role.
   
   Configure the form to add the Read roles field, if necessary.
4. Click **Submit**.
5. Repeat steps 1 – 4 for all variables in the table.

**Wizard variables details table**

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Question</th>
<th>Additional configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>CheckBox</td>
<td>office</td>
<td>Microsoft Office Suite</td>
<td></td>
</tr>
<tr>
<td>CheckBox</td>
<td>creativeSuite</td>
<td>Adobe Creative Suite</td>
<td></td>
</tr>
<tr>
<td>CheckBox</td>
<td>other</td>
<td>Other</td>
<td></td>
</tr>
<tr>
<td>Label</td>
<td>needs</td>
<td>Business software you use (select all that apply):</td>
<td></td>
</tr>
<tr>
<td>Single Line Text</td>
<td>otherprod</td>
<td>Please specify:</td>
<td></td>
</tr>
<tr>
<td>Numeric Scale</td>
<td>powerpoint</td>
<td>PowerPoint</td>
<td>Scale min: 1</td>
</tr>
<tr>
<td>Numeric Scale</td>
<td>word</td>
<td>Word</td>
<td>Scale min: 1</td>
</tr>
<tr>
<td>Numeric Scale</td>
<td>excel</td>
<td>Excel</td>
<td>Scale min: 1</td>
</tr>
<tr>
<td>Numeric Scale</td>
<td>publisher</td>
<td>Publisher</td>
<td>Scale min: 1</td>
</tr>
<tr>
<td>Numeric Scale</td>
<td>access</td>
<td>Access</td>
<td>Scale min: 1</td>
</tr>
<tr>
<td>Yes/No</td>
<td>photoshop</td>
<td>Photoshop</td>
<td>Default value: No</td>
</tr>
<tr>
<td>Yes/No</td>
<td>illustrator</td>
<td>Illustrator</td>
<td>Default value: No</td>
</tr>
<tr>
<td>Yes/No</td>
<td>acrobat</td>
<td>Acrobat</td>
<td>Default value: No</td>
</tr>
<tr>
<td>Yes/No</td>
<td>dreamweaver</td>
<td>Dreamweaver</td>
<td>Default value: No</td>
</tr>
<tr>
<td>Multi Line Text</td>
<td>project_description</td>
<td>Describe projects for which you use these tools:</td>
<td>Mandatory: true</td>
</tr>
</tbody>
</table>
Create a survey page
Create the survey pages (wizard panels) and add questions.

1. Navigate to **Survey Wizards > All** and select **Software Needs Analysis**.
2. In the Survey Panels related list, click **New**.
3. Enter the Name, Title, and Description as listed in the table.
4. Right-click the header and select **Save**.
5. In the Variables related list, click **Edit...**.
6. Using the **slushbucket**, select and arrange the variables as listed in the table.
7. Repeat steps 1 – 6 for all panels in the table.

<table>
<thead>
<tr>
<th>Panel variables table</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name and Title</td>
</tr>
<tr>
<td>Describe Needs</td>
</tr>
<tr>
<td>Microsoft Office</td>
</tr>
<tr>
<td>Adobe Creative Suite</td>
</tr>
<tr>
<td>End Note</td>
</tr>
</tbody>
</table>

Create a dynamic effect
How to create a dynamic effect.

On the Describe Needs panel, if the user selects **Other**, then the Please specify field should be visible and mandatory.
1. Navigate to Survey Wizards > Wizard Policy > Wizard UI Policy.
2. Click New.
3. Enter the UI policy details.

**UI policy details**

<table>
<thead>
<tr>
<th>Name</th>
<th>Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wizard</td>
<td>Software Needs Analysis</td>
</tr>
<tr>
<td>Reverse if false</td>
<td>select the check box</td>
</tr>
<tr>
<td>On load</td>
<td>select the check box</td>
</tr>
<tr>
<td>Active</td>
<td>select the check box</td>
</tr>
<tr>
<td>Short description</td>
<td>If Other is true, show Specify</td>
</tr>
<tr>
<td>Wizard Conditions</td>
<td>other is true</td>
</tr>
</tbody>
</table>

4. Right-click the header and select Save.
5. In the Wizard UI Policy Actions related list, click New.
6. Enter the action details and click Update.
   - Variable Name: otherprod
   - Mandatory: True
   - Visible: True

**Define a transition demo**

How to define transitions.

1. Navigate to Survey Wizards > All and select Software Needs Analysis.
2. Open a survey panel as listed in the table.
3. In the Wizard Panel Transitions related list, click New.
4. Enter the transition details and click Submit.
5. Repeat steps 1 – 4 for all panel transitions in the table.
### Panel transition details table

<table>
<thead>
<tr>
<th>Panel</th>
<th>Condition</th>
<th>Order</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Describe Needs</td>
<td>office is true</td>
<td>100</td>
<td>Microsoft Office</td>
</tr>
<tr>
<td>Describe Needs</td>
<td>creativesuite is true</td>
<td>200</td>
<td>Adobe Creative Suite</td>
</tr>
<tr>
<td>Microsoft Office</td>
<td>creativesuite is true</td>
<td>100</td>
<td>Adobe Creative Suite</td>
</tr>
<tr>
<td>Microsoft Office</td>
<td></td>
<td>200</td>
<td>End Note</td>
</tr>
<tr>
<td>Adobe Creative Suite</td>
<td></td>
<td>100</td>
<td>End Note</td>
</tr>
</tbody>
</table>

**Test the survey wizard demo**

How to test the survey wizard:

1. Navigate to Survey Wizards > All and select Software Needs Analysis.
2. Click Try It.
3. In the Business software you use (select all that apply) question, select: **Microsoft Office, Other**.
4. Verify that the Please specify field appears and is mandatory when Other is selected (UI policy created in Dynamic Effects).
5. Click Next.
6. Verify that the Office panel appears.
7. Enter test values for the questions and click Next.
8. Verify that the End Note panel appears (the transition logic skips the Adobe Creative Suite panel when the Adobe Creative Suite check box is not selected on the first panel).
9. Click Done.
11. Search for and open the most recent instance of the Software Needs Analysis survey wizard.
12. Verify that your survey answers are properly recorded.
13. Run through several scenarios to test transition logic and data collection.
Configure the survey
How to configure the survey.

1. Navigate to **Survey Wizards > Survey Properties**.
2. Ensure the Enable the enhanced task survey capabilities. Survey distribution is controlled by Survey Conditions. property is enabled (select the check box).
3. Navigate to **Survey Wizards > Survey Conditions**.
4. Click **New**.
5. Enter the condition details and click **Submit**.

**Condition details**

<table>
<thead>
<tr>
<th>Name</th>
<th>Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Survey Wizard</td>
</tr>
<tr>
<td>Survey wizard</td>
<td>Software Needs Analysis</td>
</tr>
<tr>
<td>Active</td>
<td>select the check box</td>
</tr>
<tr>
<td>Table</td>
<td>Incident</td>
</tr>
<tr>
<td>User field</td>
<td>Caller</td>
</tr>
<tr>
<td>Description</td>
<td>Send software survey to all users with software questions</td>
</tr>
<tr>
<td>Condition</td>
<td>Category is Software</td>
</tr>
</tbody>
</table>

6. Navigate to **System Policy > Email > Notifications**.
7. Click **New**.
8. Enter the email notification details and click **Submit**.
Email notification details

<table>
<thead>
<tr>
<th>Name</th>
<th>Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Software Survey</td>
</tr>
<tr>
<td>Event Name</td>
<td>task.send_survey</td>
</tr>
<tr>
<td>Table</td>
<td>Incident</td>
</tr>
<tr>
<td>User field</td>
<td>event.parm1</td>
</tr>
<tr>
<td>Active</td>
<td>select the check box</td>
</tr>
<tr>
<td>Conditions</td>
<td>Category is Software</td>
</tr>
<tr>
<td>Subject</td>
<td>Please take the software survey (Incident ${number})</td>
</tr>
<tr>
<td>Message</td>
<td>Please complete this survey to help us evaluate our ongoing software needs. &lt;a href=${event.parm2}&gt;Click here to take the survey.&lt;/a&gt;</td>
</tr>
</tbody>
</table>

9. Filter the Email Notifications list using the condition: Event Name is task.send_survey and Table is Incident.

10. If any other notifications exist, increase their Weight value so that only the Software Survey is sent when the incident category is software (the Software Survey has a Weight of 0, so it has the highest priority of any notifications for the incident table).

Service Portal

Service Portal is a portal framework that allows administrators to build a mobile-friendly self service experience for users. It interacts with parts of the ServiceNow platform, so users can access specific platform features using Service Portal. It is an alternative to the Content Management System (CMS) based on more modern technologies.

Both expert developers and beginners can configure Service Portal.

Less technical users can make basic configuration changes to the UI using Branding Editor and other components of Service Portal. More advanced users can edit and extend portals, pages, and widgets. Expert users can use the Widget Editor tool to write scripts to power a portal, and even create rich web applications on the Now Platform.

Explore
- Service Portal release notes
- Upgrade to Jakarta
- Understanding Service Portal
- Service Portal training on the ServiceNow Developer Portal

Set up
- Service Portal Configuration
- Search sources
- Create a service portal and its branding

Administer
- Single sign-on, logins, and URL redirects
- Service Portal security

Use
- Widget library

Develop
- Widget developer guide
- Service Portal SCSS Primer
- Developer training
- Developer documentation

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

The Service Portal is the engine that houses all of the references to content for your site. The portal record defines the URL extension for a site, as well as things like the knowledge base, catalog, and homepage. You can also use the portal record to define the header menu and the portal branding.
Service Portal

How can we help?

Order Something
Browse the catalog for services and items you need

Knowledge Base
Browse and search for articles, rate or submit feedback

Get Help
Contact support to make a request, or report a problem

Community
Community-sourced answers to your questions

Current Status
No system is reporting an issue

Popular Questions
No questions have been asked yet

My Approvals
You have no pending approvals

More Information...

Too Rated Articles

Widget

Ask a Question

Rain is leaking on main DNS Server

My Open Incidents

© 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.
Containers

Containers are markup artifacts that are put on a page to contain the layouts that house the widgets.

You can view containers and how they make up a page in the Service Portal Designer (Service Portal > Service Portal Configuration > Designer). Open a page in the Service Portal Designer, then click anything on the page. In the top left corner, breadcrumbs appear to show you which element on the page you have selected. Use the breadcrumbs to select a container, then click the edit icon.

You can also edit a container by navigating to the Page Editor and selecting the container node in the tree view. In this view, you can:

- Change the layout of widgets on a page.
- Determine the number of columns on a page.
- Determine whether to scale with changes to the browser window.
- Add a background color to a portion of a page.
- Add an background image to a portion of a page.
• View the current layout of the widgets within the page.

**Basic concepts**

You should have a basic understanding of all the following components that make up a portal:

• Themes define the look and feel of the whole portal, but can be overridden by other style configurations.
• Pages control where and how you store portal content. Pages do not have a defined relationship to portal records, they simply exist. Pages are made up of containers, columns, rows, widgets, and widget instances. You can use the CSS defined in theme and branding as global definitions for the portal or you can configure the CSS of each component. If you do not define CSS in theme or branding, Bootstrap defaults are used.
• Components in Service Portal are called widgets.

**Note:** You can use HTML templates, CSS, client scripts, server scripts, and any JavaScript dependencies to define what a widget does. From an AngularJS standpoint, widgets are essentially a superset of an Angular directive.

• Most of the data in Service Portal is managed in different locations throughout the system. For example, if you are building a knowledge portal, the data exists in Service Portal, but the knowledge articles are authored and managed in the Knowledge application. Take time to understand which tables contain and control the data you are working with in Service Portal.

**Who configures the Service Portal?**

Several different kinds of users can configure a portal.

• Limited coding: Service Portal was designed so that even users with limited coding ability or knowledge of the platform UI could set up a portal.
• ServiceNow Experts: Users with an understanding of the ServiceNow platform can create portals, set up URL redirects, and view all the components of the portal in a table. Most portal configuration takes place in the Service Portal configuration page, but in specific circumstances, Service Portal administrators may need to do additional configuration directly within the platform.
• Developers: Advanced customizations and new widget creation should be done by a developer or someone who understands AngularJS and Twitter bootstrap.

In all cases, the user configuring a portal must have the admin or sp_admin role.

**Navigate to a portal or a page using the URL**

```
https://<instance name>/<sp url suffix>?id=<page id>&<page parameters>
```

Elements:

• **Base Instance URL:** Unique, secure web address for each instance. The default format is: https://<instance name>.service-now.com
• **sp url suffix:** Suffix established for the Service Portal
• **id:** The id of the Page to navigate to within the portal frame
• **page parameters:** Some pages require additional parameters to look up a record (table, sys_id)
For example, https://<instance name>.service-now.com/sp?id=kb_view2

Additional resources

Service Portal is built using several well known technologies. Use the following websites as resources to help you understand and configure your portal:

- Twitter Bootstrap
- CSS 3 Flexbox
- AngularJS

Activate Service Portal

You can activate the Service Portal for Enterprise Service Management plugin (com.glide.service-portal.esm) if you have the admin role. This plugin includes demo data and activates related plugins if they are not already active.

Role required: admin

Service Portal activates these related plugins if they are not already active.

- Service Portal - Knowledge Base (com.glide.service-portal.knowledge-base)
- Service Portal - Service Catalog (com.glide.service-portal.service-catalog)
- Service Portal - Service Status (com.glide.service-portal.service-status)
- Service Portal Configuration Pages (com.glide.service-portal.config)
- Service Portal Designer (com.glide.service-portal.designer)
- Service Portal Social QA (com.glide.service-portal.sqanda)
- Service Portal Surveys (com.glide.service-portal.survey)

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.

Properties for Service Portal

The Service Portal properties page provides several configuration options for Service Portal.

Administrators can access these properties by navigating to Service Portal > Properties.
### Properties for Service Portal

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| Default 404 page (page ID or sp_page sys_id) for Service Portal | The default page your users see whenever a page cannot load properly.  
  * Type: string  
  * Default value: 404  
  The string must match the name of the page exactly. |
| Enable Social Q&A in Service Portal           | Allow users to ask questions in a portal using the social Q&A widgets.  
  * Type: true | false  
  * Default value: true  
  On the properties page this appears as a check box, which is selected by default. |
| Show a message to admin users in Service Portal pages if a browser error is encountered |  
  * Type: true | false  
  * Default value: true  
  On the properties page this appears as a check box, which is selected by default. |
| Maximum number of stream entries displayed in Service Portal (activity widget, conversation widget, and so on) | Limit the number of entries users can see in the ticket conversation widget. Users only see the most recent entries and won’t be able to go further back in the history than the max allowed amount.  
  * Type: integer  
  * Default value: 100 |

If `user criteria` (com.glide.service-portal.user-criteria) is enabled, the following properties also appear in the Service Portal properties page:

#### User criteria properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable use of User Criteria records instead of Roles fields for Service Portal entitlements | Defines permissions for Service Portal widgets, widget instances, pages, and search sources.  
  * Type: true | false  
  * Default value: true  
  * More information: [User criteria for Service Portal](#) |
| List of roles (comma-separated) that bypass User Criteria validation in Service Portal | Allows users with a specific role to see any page, widget, widget instance, or search source regardless of user criteria.  
  * Type: string  
  * Default value: admin |
Service Portal Configuration

Users from any coding level can create a portal as long as they have the admin or sp_admin role. The configuration page allows you to take advantage of a real-time preview, while configuring portal settings. Use each of the tiles on the configuration homepage to assemble the different components of your portal.

Requirements

Access the configuration options by navigating to Service Portal > Service Portal Configuration.
Service Portal

Create rich, engaging and modern experiences to help your business run better

Select one of the options below to continue

- **Branding Editor**
  - Customize your portal's title, logo and theme colors.
  - Preview changes as you make them

- **Designer**
  - Create and layout pages with drag-and-drop functionality.
  - Preview pages as you make changes

- **Page Editor**
  - Configure the properties of pages, containers and widgets from a map view

- **Widget Editor**
  - Create widgets from scratch or customize an existing one. Write HTML, CSS, and Javascript with real-time preview

- **New Portal**
  - Create a new Service Portal

- **Get Help**
  - Browse guides, tutorials and videos to learn how to set up, configure and customize your portals
Role required: admin or sp_admin

**Before you begin**

Consider the following before configuring Service Portal:

- Who are you building your site for and why?
- What information do you want to include in your site?
- What do you want the mobile experience to be for users?
- Which platform applications do you plan to use in your portal?

You can use parts of the platform, such as knowledge articles and catalog items, as the content for your portal.

For example, if you are building a knowledge portal, the content displays in Service Portal, but the knowledge articles are authored and managed in the Knowledge application. The same is true for any other type of content you plan to leverage. It is important to take time to understand the table structure of data to become acquainted with content.

- How customized is your service catalog? Catalog client scripts and UI policies only work in Service Portal if they use the mobile GlideForm API, so you may need to make some changes.

**Create a service portal and its branding**

Use the Branding Editor to give your portal its own look and feel. Service Portal is designed to allow customers to have control over the behavior of their portals. One of the main navigation controls for users is the header main menu. The menu options are determined by the assignment of a main menu to the portal, but the look and behavior of the menu is defined within the theme and associated header.

Role required: admin or sp_admin role.

**Note:** If you have experience with CSS and HTML you can configure these fields in the portal form directly as accessed through the portal UI. However, the Branding Editor provides a real-time theme preview.

The changes made in the Branding Editor are recorded in the portal record. Any changes made in the Branding Editor or to specific components of the portal (such as a widget or a page container) override any customizations made to the theme.

1. Create the portal.
   a) Navigate to Service Portal > Service Portal Configuration > Branding Editor.
   b) Select the Service Portal from the drop-down list.
   c) Complete the following fields.

**Quick Setup tab options**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Portal Title</td>
<td>The name of your portal. Changing the name of the portal in the Branding Editor also changes the title on the portal form field in the platform UI.</td>
</tr>
<tr>
<td>Logo</td>
<td>The logo that appears in the header for your portal.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Logo padding</td>
<td>Where you want the logo to sit in location to the edge of the header. This information is stored in the CSS variables section on the portal form.</td>
</tr>
<tr>
<td>Tag line &amp; background</td>
<td>Fields defined by the JSON schema in the Quick start config field on the portal record in the platform UI. The sample Service Portal adds Tag Line and Background to the Branding Editor using the following schema:</td>
</tr>
<tr>
<td></td>
<td>```</td>
</tr>
<tr>
<td></td>
<td>[{</td>
</tr>
<tr>
<td></td>
<td>&quot;tagline&quot;: {</td>
</tr>
<tr>
<td></td>
<td>&quot;table&quot;: &quot;sp_instance&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;sys_id&quot;: &quot;34fe3d96cb20020000f8d856634c9cf4&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;field&quot;: &quot;title&quot;</td>
</tr>
<tr>
<td></td>
<td>},</td>
</tr>
<tr>
<td></td>
<td>&quot;hero_background&quot;: {</td>
</tr>
<tr>
<td></td>
<td>&quot;table&quot;: &quot;sp_container&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;sys_id&quot;: &quot;be98a8d2cb20020000f8d856634c9c63&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;field&quot;: &quot;background_image&quot;</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td>Tag line</td>
<td>Introduce your users to a portal page with a tag line. This text is stored in an instance of the homepage search widget.</td>
</tr>
<tr>
<td>Tag line color</td>
<td>Select a color for the tag line.</td>
</tr>
<tr>
<td>Homepage background color</td>
<td>Add a color for your background. You can type in a color name, hex color, decimal (r,g,b), or select from the color palate.</td>
</tr>
<tr>
<td>Background image</td>
<td>Upload an image to appear in the background of your homepage. This image is stored in the container for the widget on your homepage.</td>
</tr>
</tbody>
</table>

**Note:** For any colors on the theme tab, you can use the standard color name, hex code, decimal (RGB) code, or select the color from the color palate. All the color definitions are stored in the CSS variables field of the portal form. The theme preview updates in real time as you make changes.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navbar</td>
<td>Use the fields in this section to customize the colors for the header menu.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Brand</td>
<td>Use the fields in this section to customize the page colors. For example, the page background or the widget background.</td>
</tr>
<tr>
<td>Text</td>
<td>Use the fields in this section to customize the color of the text on a page.</td>
</tr>
</tbody>
</table>

2. Add a header or footer to a service portal.
   a) Navigate to the portal theme (Service Portal > Service Portal Configuration > Portal Tables > Themes) then click the theme you want to add the header or footer to.
   b) In the header or footer field, select the header or footer you want to use for your portal. If you are just getting started, you can reuse the out of box Stock Header or Sample Footer widgets.
   c) Select Fixed Header or Fixed Footer to lock the header or footer in one place so when users scroll up or down they remain in the same location on the page.
   d) To configure the appearance of the header, in the Service Portal configuration page, open the Branding Editor. Under the Theme Colors tab, use the color selectors in the Navbar section to control the colors in the header.

3. Create a portal homepage.
   The home page contains the major information and actions that your users see. When a portal is referenced by the URL suffix it lands on a home page. This homepage is often labeled index in website language.
   a) From any page in the Service Portal Designer, click Edit Portal Properties.

   ![Edit Portal Properties](image)

   b) From the Homepage list, select the page you want for your portal homepage and click Save.
4. Configure the service portal header menu.

The header menu in a portal is actually comprised of two separate widgets: a header widget, which determines the style of the header, and the menu widget, which determines the actual items that appear in the header. You need to configure both before a header menu can appear and act like a header menu in your portal.

a) In the Service Portal configuration page (Service Portal > Service Portal Configuration), navigate to Portal Tables > Instance with Menu, then click New.

b) Complete the fields in the menu form.
Menu form
### Menu fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Name of the header menu. You need to know this when you associate the menu with your portal.</td>
</tr>
<tr>
<td>Additional options, JSON format</td>
<td>Advanced configuration options. For example, use this field to enable the shopping cart in the header menu with the following code:</td>
</tr>
<tr>
<td></td>
<td>{ &quot;enable_cart&quot;: { &quot;displayValue&quot;: &quot;true&quot;, &quot;value&quot;: true } }</td>
</tr>
<tr>
<td>Application</td>
<td>The record scope. The header menu record and the source table must have the same application scope.</td>
</tr>
<tr>
<td>Widget</td>
<td>The widget that the header menu is based on. Select a menu-type widget from the list. For example, the header menu widget that is included as an out-of-box widget.</td>
</tr>
</tbody>
</table>

**c)** Save the form then click **Menu Items** from the related lists.

**d)** Click **New** and complete the menu item form.

### Menu item fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>Name that appears for the item in the menu</td>
</tr>
<tr>
<td>Parent menu</td>
<td>This field should already contain the name of the menu you are adding items to. You can change the value as needed to other menus</td>
</tr>
<tr>
<td>Parent menu item</td>
<td>Use this field to nest menu items within other menu items</td>
</tr>
<tr>
<td>Order</td>
<td>Value that determines where the item appears in the menu in relation to other menu items</td>
</tr>
<tr>
<td>Type</td>
<td>The kind of page the item links to. For example, you can link to another page in the portal, or an external URL. Form fields vary depending on the option you select from this list. Select <strong>Scripted list</strong> for more advanced options.</td>
</tr>
<tr>
<td>Page</td>
<td>Name of the portal page the item links to. This option is available if you select <strong>Page</strong> as the menu item type.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Condition</td>
<td>Determines what conditions are required for menu items to show in the header. For example, the condition <code>gs.hasRole(&quot;sp_admin&quot;)</code> restricts access to menu items to users with the sp_admin role. Hide a menu item by setting this value to <code>false</code>. For more information on what conditions to use in the <strong>Condition</strong> field, see Restricting UI actions based on conditions in <a href="#">Create a UI action</a>.</td>
</tr>
<tr>
<td>Glyph</td>
<td>Icon that appears beside the menu item</td>
</tr>
</tbody>
</table>

5. After you create a menu and menu items, add the menu to a portal.
   
   a) Navigate to **Service Portal > Portals**, then open the portal you want to add a menu to.
   
   b) From the main menu field, click the reference lookup icon, then select the appropriate menu by name. Click **Save**.
Create and edit a service portal page

Pages organize content, ensure responsive mobile optimization, and design meaningful portal user experiences for your customers. A page houses containers and rows, which then contain widgets. By manipulating the layout of the page, and the widgets within it, you can construct your desired user experience.

These steps are intended for users with little to no coding experience. The Service Portal Designer includes several layers of customization from simply adding widgets in a particular configuration on a page, to adding CSS classes.

To access the Service Portal Designer, navigate to Service Portal > Service Portal Configuration, and then click Designer.

1. Switch to the portal you want to design pages for by selecting the portal name in the header.

2. From the Service Portal Designer, select a page to customize or click Add a new page.
3. Under Layouts, select Container and drag it onto the page.
4. Drag one of the other layouts and drop it in the container.
   This layout defines the structure of your page and the space available to drop widgets. The structure of the layout aligns with the Bootstrap grid template and always adds up to 12.
5. Use the filter to search for a widget, then drag the widget to the layout.
   a) Click **Edit Page Properties**.
      The page record from the Pages table (sp_page) opens.
   b) Edit the form.

### Page fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Internal name of the page. Use the title to search for a page in the Service Portal Designer.</td>
</tr>
<tr>
<td>ID</td>
<td>A unique ID for the page. The ID is what you use to assign a page to a portal. It also determines the URL for the page, for example <code>https://instance name.service-now.com/doc_portal/?id=doc_page</code>, where doc_page is the page ID.</td>
</tr>
<tr>
<td>Application</td>
<td>The application scope.</td>
</tr>
<tr>
<td>Public</td>
<td>Enables the page to be accessed without the need for authentication. If <strong>Public</strong> is selected, all users can view the page no matter the roles listed.</td>
</tr>
<tr>
<td>Draft</td>
<td>Mark a page as draft to limit user ability to view the page while you are still creating it. Only users with the admin role can view a page in draft, all other users see a 404 page.</td>
</tr>
<tr>
<td>Roles</td>
<td>Limit user access to a page by role.</td>
</tr>
<tr>
<td>Short description</td>
<td>Describes the portal page. This field is not public facing.</td>
</tr>
<tr>
<td>Page Specific CSS</td>
<td>Unless a page has Page Specific CSS, the page inherits CSS from the Theme and Branding. If you need a page to look different, the Page Specific CSS overrides the inheritance from the Theme and Branding.</td>
</tr>
<tr>
<td>Dynamic page title</td>
<td>Create variables to generate descriptive titles depending on the content loaded into a page.</td>
</tr>
<tr>
<td>Clone Page</td>
<td>Enables you to make a copy of a page that can be modified. If you clone a base system page, a new widget instance is created for each widget on the page.</td>
</tr>
</tbody>
</table>

7. Optional: Edit container properties.
   a) Click within the container you would like to edit, or select **Container** in the breadcrumbs.
   b) Click the edit icon ().
      The container record from the Containers table (sp_container) opens.
   c) Edit the form.

### Container fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Internal name of the container.</td>
</tr>
<tr>
<td>Order</td>
<td>The order in which the containers appear on a page. To set a container to appear above all other containers, give the container the lowest number in the <strong>Order</strong> field.</td>
</tr>
<tr>
<td>Page</td>
<td>The page in which the container appears.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Screen reader title</td>
<td>The title used by a screen reader.</td>
</tr>
<tr>
<td>Application</td>
<td>The application scope.</td>
</tr>
<tr>
<td>Width</td>
<td>Width of the container. Options include:</td>
</tr>
<tr>
<td></td>
<td>· Fixed</td>
</tr>
<tr>
<td></td>
<td>· Fluid</td>
</tr>
<tr>
<td>Parent class</td>
<td>Parent CSS class for the container.</td>
</tr>
<tr>
<td>CSS class</td>
<td>The CSS classes for the container. Overwrites page-specific CSS.</td>
</tr>
<tr>
<td>Background color</td>
<td>The background color of the container.</td>
</tr>
<tr>
<td>Background image</td>
<td>Background image for the container.</td>
</tr>
<tr>
<td>Background style</td>
<td>The display style of a background image. Options include:</td>
</tr>
<tr>
<td></td>
<td>· Default</td>
</tr>
<tr>
<td></td>
<td>· Cover</td>
</tr>
<tr>
<td></td>
<td>· Contain</td>
</tr>
<tr>
<td></td>
<td>· Repeating</td>
</tr>
<tr>
<td>Bootstrap alternative</td>
<td>Selecting this field removes the standard Bootstrap grid classes and disables</td>
</tr>
<tr>
<td></td>
<td>the Bootstrap grid system in the container. If selected, the following are</td>
</tr>
<tr>
<td></td>
<td>not applied:</td>
</tr>
<tr>
<td></td>
<td>· The Width field in the container record.</td>
</tr>
<tr>
<td></td>
<td>· Standard Bootstrap class in the row record within the container.</td>
</tr>
<tr>
<td></td>
<td>· The Size - xs, Size - sm, Size - md, and Size - lg fields in column</td>
</tr>
<tr>
<td></td>
<td>records within the container.</td>
</tr>
<tr>
<td></td>
<td>Only select this field if you plan to provide custom CSS classes and CSS</td>
</tr>
<tr>
<td></td>
<td>for the container, row, and column records.</td>
</tr>
<tr>
<td>Move to header</td>
<td>If selected, the container sticks to the header and does not scroll. Use this</td>
</tr>
<tr>
<td></td>
<td>option to create a subheader.</td>
</tr>
</tbody>
</table>

8. Optional: To switch to a different page, click the Pages tab in the left pane, then select the next page you want to configure.

9. Optional: Use the Preview button in the header to view your page as you design it. You can also use Preview to view your page in mobile or tablet mode through the controls presented in the header.
Designer tablet view
Include font icons on a page

Include font icons on a page so that all the widgets on the page have access to the font-icon set.

1. In the platform UI, navigate to Service Portal > Pages and click the page you want to add font-icons to.
2. Attach the font-icon file to the page record.
3. In the Page Specific CSS field for the page, add the CSS for the font-icon definition. Use the sys_id of the attachment as the src in the CSS.

Result

You can select an icon from the icon set for any widget on this page. For example, in the HTML widget you can use the source code option to use an icon.
Create a new widget

Widgets are the power behind the portal. Widgets are customizable and can be used to provide an variety of experiences for your users. Anytime you add a widget to a page it becomes an instance of itself, which can be configured specifically for each use. Create a new widget to build a custom widget from scratch.

Role required: admin or sp_admin

You can add several Icon Link widgets to a page, configure them to link to different areas and with different icons, and none of them will be affected by the others. You can start by cloning an existing widget and making changes to your cloned version. Developers or people with an advanced understanding of AngularJS can create widgets from scratch.

1. Navigate to Service Portal > Service Portal Configuration > Widget Editor.
2. Click Create a new widget.
3. Enter a name for the new widget. The widget ID is created automatically based on the widget name. Optionally select Create test page to automatically create a page containing the widget.
Note: After completing development of a widget with a test page, delete the test page. Maintaining test pages can create clutter when managing pages.

4. Click **Submit**.

   The widget HTML template, client script, and server script display in the widget editor. Basic script templates are included as a guide.
Clone a widget

Take advantage of existing code by cloning and editing an existing widget.

Role required: admin or sp_admin

**Note:** Base system widgets are read only so you can benefit from future updates. To make changes, you can clone base system widgets. However, cloned widgets are considered custom and do not benefit from future updates to the widgets they were cloned from.

1. Open the Widget Editor in the Service Portal Configuration page, then select an existing widget from the **Select a widget** list. For example, select **Hello World 2**.
2. From the list menu in the widget header, click **Clone “Hello World 2”**.
Clone a widget

3. Enter a name for the cloned widget. The widget ID is created automatically based on the widget name.

4. Optional: Select **Create test page** to automatically create a page containing the widget.

5. Use the check boxes to show or hide the different components of the widget editor as needed. Make changes to the HTML Template, CSS, client script, server script, or the link function.
¡Hola, mundo!
6. In order to enable a preview of your widget, use **Enable Preview** from the menu. Use the eye icon that appears to show or hide a preview of your widget.

If you clone a widget that uses the Angular ng-template, you must manually clone the template and change the name of the template reference in the widget.

For example, the header menu widget uses the Angular ng-template `menuTemplate`. If you clone the header menu widget, you must also clone the `menuTemplate` and give the clone a unique name. When you open the clone of the header menu widget, you can see a reference to the `menuTemplate` in the HTML.

```
menuTemplate in header widget HTML
```

**Define a search source**

A search source is a record that describes the behavior and source of searchable data. Configure a basic search source to query data from an instance table, or configure an advanced data fetch script to pull data from anywhere on the web.

A search source defines:

- Where search data is retrieved from.
- Whether search suggestions can populate the search field based on user input.
- How a search entry displays in the search result page.

Search sources have simple and advanced configurations.

**Simple**

Define a table within your ServiceNow instance as a source of searchable data.

**Advanced**

Define a data fetch script to return data. A data fetch script executes on the server and returns a result array to the search widget. This method is more complex, but offers complete power over how a search is executed. You are not limited to records and tables within ServiceNow and can define a script that fetches data from anywhere on the web. To learn more, review the [Tutorial: set up an external knowledge base search source](#).

Typeahead returns search results in real time as a user types in the search field. You can configure typeahead settings, or disable the feature entirely, within the search source record. Typeahead return search has simple and advanced configurations.

**Simple**

Define an icon to display beside typeahead results and the target page to display typeahead selections.
Advanced
Define a template for the typeahead result. See Create an advanced typeahead template.

1. In the platform UI, navigate to Service Portal > Portals and select the portal you want to add search sources to.
2. From the Search Sources related list, click New to add a search source.
3. Define the fields on the Search Source form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The display value for the search category.</td>
</tr>
<tr>
<td>ID</td>
<td>The record ID. The value should be unique, and should not include any spaces or special characters.</td>
</tr>
<tr>
<td>Application</td>
<td>The scope of the search source.</td>
</tr>
<tr>
<td>Roles</td>
<td>If the Service Portal User Criteria Support plugin is not enabled, define user roles to access this search source.</td>
</tr>
<tr>
<td>Search page template</td>
<td>The HTML template that displays the search results. If defining a basic search source, you do not need to change the default template. For an example of a modified template, see Tutorial: set up an external knowledge base search source.</td>
</tr>
</tbody>
</table>

4. Complete the fields on the Data Source tab.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is scripted source</td>
<td>Select this option to add an advanced data fetch script. If configuring an instance table as the data source, do not check this option.</td>
</tr>
<tr>
<td>Data fetch script</td>
<td>A script defining the endpoint and API calls to fetch external data. This field is only visible when Is scripted source is selected. For an example of a data fetch script, see Tutorial: set up an external knowledge base search source.</td>
</tr>
<tr>
<td>Table</td>
<td>Select a table from the list that you want to draw your results from. You can select any table in the platform. For example, User (sys_user) or Knowledge (kb_knowledge). Note: Only indexed tables return search results. Learn more: Enable text indexing for a table.</td>
</tr>
<tr>
<td>Conditions</td>
<td>Apply a filter to the table if you don't want all the search results to display. For example, Active is True.</td>
</tr>
<tr>
<td>Primary display field</td>
<td>Select which field you want to display on the search results page. For example, Name.</td>
</tr>
<tr>
<td>Display fields</td>
<td>Select additional fields to display on the search results page. For example, User ID, Email, and City.</td>
</tr>
</tbody>
</table>
5. Configure **Typeahead** settings to allow search results to populate the search field based on user input.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable typeahead</td>
<td>Allows typeahead functionality. If you do not want to integrate typeahead into your search source, clear the check box.</td>
</tr>
<tr>
<td>Advanced typeahead</td>
<td>Optionally add an advanced typeahead script to configure the way search results display. For more information, see <em>Create an advanced typeahead template</em>.</td>
</tr>
<tr>
<td>glyph</td>
<td>Adds an icon beside each typeahead result.</td>
</tr>
<tr>
<td>Page</td>
<td>Defines a service portal page to display the selected result. For example, if <strong>form</strong> is configured, a selected typeahead result opens in a form.</td>
</tr>
</tbody>
</table>

6. Click **Submit**.

7. Configure the way typeahead results display with an advanced template.
   a) In the **Typeahead** tab of the *Search Source* record, select the **Advanced typeahead config** check box.
b) In the **Typeahead template** field, add an HTML template.

This example uses AngularJS bindings to display service catalog images in the typeahead results.

```html
<i class="ta-img" ng-if="match.model.type=='sc'" style="background-image:url('{{match.model.picture}}')"></i>
<i class="ta-img" ng-if="match.model.type=='sc_guide'" style="background-image:url('{{match.model.picture}}')"></i>
<i class="ta-icon fa fa-file-text-o" ng-if="match.model.type=='sc_content' && match.model.content_type == 'kb'"></i>
<strong ng-if="match.model.type=='sc_content' && match.model.content_type == 'external'">#</strong>
<span ng-bind-html="match.label | uibTypeaheadHighlight:query"></span>
```

c) Click **Update**.

Typeahead results display beside the image defined in the service catalog record.
User criteria for Service Portal

Administrators can control access to pages, widgets, widget instances, and search sources in a portal by creating and applying user criteria.

User criteria records define conditions that are evaluated against user records. When user criteria is defined, portal records are only visible to users who pass the defined conditions.

User criteria is a platform feature used in Service Portal.
Converting role-based permissions to user criteria records

User criteria in Service Portal replaces role-based permissions. After activating the user criteria for Service Portal plugin, you must set the user criteria for Service Portal system property to true. When the system property is set to true, any existing roles defined for a page, widget, or search source are automatically converted into user criteria records. To disable user criteria and continue using role-based permissions, set the system property to false.

User criteria checks

User criteria uses the following checks in Service Portal to verify user access.

Page access user criteria

The following diagram shows how the system decides whether a user can access a page based on user criteria.
Widget access user criteria

The following diagram shows how the system determines whether a user has access to a particular widget or widget instance.
Activate the user criteria for Service Portal plugin

You can activate the Service Portal User Criteria Support plugin (com.glide.service-portal.user-criteria) 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 the user criteria for Service Portal system property

After activating the Service Portal User Criteria Support plugin, you must set the system property to true.

Role required: admin

Setting the system property activates user criteria for Service Portal. When the system property is set to true, any existing roles defined for a page, widget, or search source are automatically converted into user criteria records. To disable user criteria and continue using role-based permissions, set the system property to false.

1. Navigate to Service Portal > Properties.
2. Click the check box to set the following property to true.
3. Click Save.

Create a user criteria record for Service Portal

Create a user criteria record to apply to items in Service Portal and control user access to pages, widgets, widget instances, and search sources.
You can apply existing user criteria to records in Service Portal through Service Portal configuration (Service Portal > Service Portal configuration). You can only create user criteria within the platform UI.

1. In the navigation filter, type Service Portal.
2. Select a page, widget, or widget instance record.
3. In the related list at the bottom of the record, select the Can View or Cannot View tab, then click New. If a user criteria record is already created, you can click Edit to apply user criteria to the page, widget, or widget instance.

User criteria records are stored in the user_criteria table.

4. Complete the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the criteria record.</td>
</tr>
<tr>
<td>Users</td>
<td>User records to match access criteria.</td>
</tr>
<tr>
<td>Groups</td>
<td>Group records to match access criteria.</td>
</tr>
<tr>
<td>Roles</td>
<td>Roles to match access criteria.</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>
<tbody>
<tr>
<td>Advanced</td>
<td>Displays or hides the <strong>Script</strong> field.</td>
</tr>
<tr>
<td>Script</td>
<td>Defines any additional criteria, and returns <strong>true</strong> or <strong>false</strong>. This field is available only if Advanced is selected.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Because scripts are evaluated dynamically, including scripts in user criteria records can decrease performance.</td>
</tr>
<tr>
<td>Application</td>
<td>Application scope for the user criteria record.</td>
</tr>
<tr>
<td>Active</td>
<td>Activate or deactivates this criteria record.</td>
</tr>
<tr>
<td>Companies</td>
<td>Companies to match access criteria.</td>
</tr>
<tr>
<td>Locations</td>
<td>Locations to match access criteria.</td>
</tr>
<tr>
<td>Departments</td>
<td>Departments to match access criteria.</td>
</tr>
<tr>
<td>Match All</td>
<td>Determines whether all elements from each populated criteria field must match. If selected, only users who match all criteria are given access. If cleared, the user must meet one or more of the set criteria to be given access. By default, this check box is cleared so that any condition met provides a match. For example, consider a user criteria record for the following: - Locations A or B - Company C or D With <strong>Match All</strong> selected, only users meeting all these conditions are matched. For example, a user with a location A and a company C. With <strong>Match All</strong> cleared, users meeting any of these conditions are matched. For example, a user with a location B.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you select <strong>Match All</strong>, ensure that you do not create contradictory conditions that can never be met. For example, if all users in location A work for company G, then the conditions in this example can never be met.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.

**Apply user criteria to a page, widget, or widget instance**

Assign user criteria to pages, widgets, or widget instances to limit user access to content in a portal.
Activate the Service Portal User Criteria Support (com.glide.service-portal.user-criteria) plugin and set the glide.service_portal.user_criteria_enabled system property to true.

Role required: admin or sp_admin

You can apply several user criteria records to a single portal item.

1. In the Service Portal Configuration page (Service Portal > Service Portal Configuration), open the Page Editor.
2. Select a page from the list.
3. Select a page, widget, or widget instance node from the page tree.
4. Under related lists, click Who Can View or Who Cannot View.
5. Click New.
6. Select a criteria from the Can View or Cannot View list.

Selecting criteria from the Can View or Cannot View list applies user criteria records created in Create a user criteria record for Service Portal to the selected page, widget, or widget instance.

7. Click Save.
Apply user criteria to a search source

Assign user criteria to search sources to limit user access to content in a portal.

Role required: admin

You can add user criteria to custom or default Search sources.

1. In the Service Portal Configuration page (Service Portal > Service Portal Configuration), navigate to Portal Tables > Search Source in the header menu.
Service Portal
Create rich, engaging and modern experiences to help your business run. Select one of the options below to continue.

- **Branding Editor**: Customize your portal's title, logo and theme colors. Preview changes as you make them.
- **Designer**: Create and layout pages with drag-and-drop functionality. Preview pages as you make changes.
- **Page Editor**: Configure the properties of pages, containers and widgets from a map view.
- **Widget Editor**: Create widgets from scratch or customize an existing one. Write HTML, CSS, and JavaScript with real-time preview.

- **Search Source**
  - Service Portal
  - Service Portal Documentation
  - Service Portal Log Entry
2. Open the search source record that you would like to modify.
3. Under related lists, click Who Can View Search Sources or Who Cannot View Search Sources.
4. Click New.
5. Select a criteria from the Can View or Cannot View list.
   Selecting criteria from the Can View or Cannot View list applies user criteria records created in Create a user criteria record for Service Portal to the selected search source.

6. Click Save.

Content Management and Service Portal

Service Portal is an alternative to the Content Management System (CMS). It does not duplicate CMS or platform UI functionality. Users transitioning from a CMS to the Service Portal, may require additional considerations especially if the CMS implementation includes complex and customized Service Catalog forms.
Service Portal compatibility with existing CMS sites

ServiceNow continues to support CMS in current and upcoming releases. If you have existing CMS sites and activate Service Portal on your instance, your CMS sites will continue to work, as CMS and Service Portal are separate applications.

Differences between Service Portal and CMS

Service Portal is an alternative to CMS based on more modern technologies. Major differences include:

Underlying technology
CMS uses Jelly, which is not a widely used technology. Service Portal instead uses AngularJS, server-side JavaScript, HTML, and CSS. Any scripts that use Jelly do not work in Service Portal. Building widgets in Service Portal requires knowledge of AngularJS.

Visual layer
CMS uses iFrames which can be difficult to work with, limited in terms of styling, and susceptible to upgrade issues. Service Portal, on the other hand, is a self-contained application that accesses data from other tables on the platform. This enables fine-tuned control over style and responsive design.

Mobile first
Unlike CMS, Service Portal is optimized for a mobile environment. For this reason, the following apply to the Service Portal environment:

- Any scripts used in Service Portal can only use APIs supported in a mobile environment. For example, some APIs used in your Service Catalog client scripts may not be supported. For a list of supported APIs, see Service Portal and client scripts.
- Service Portal forms support a maximum of two-columns. As a result, any highly customized Service Catalog forms, such as catalog items and record producers that use containers and variable sets, must be simplified to work in a two-column layout.

If transitioning to Service Portal, review the following resource: Mobile client GlideForm (g form) scripting and migration.

To understand how core CMS components are configured in Service Portal, refer to the following table.

<table>
<thead>
<tr>
<th>CMS component</th>
<th>Service Portal equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content site</td>
<td>Portal</td>
</tr>
<tr>
<td>Content page</td>
<td>Page</td>
</tr>
<tr>
<td>Content types</td>
<td>Content types link a table to a content page.</td>
</tr>
<tr>
<td></td>
<td>In Service Portal, content types are no longer required. Record data</td>
</tr>
<tr>
<td></td>
<td>is queried and displayed using base system widgets. You can add</td>
</tr>
<tr>
<td></td>
<td>widgets to any number of Service Portal pages.</td>
</tr>
<tr>
<td>Layout and dropzones</td>
<td>In Service Portal, pages are made up of containers, rows, and</td>
</tr>
<tr>
<td></td>
<td>columns.</td>
</tr>
</tbody>
</table>
### CMS and Service Catalog customizations

Service Portal comes with base system widgets to address common use cases and to display record data. Even though there is no direct migration path from CMS to Service Portal, there may be some items, such as catalog items or knowledge articles, that render as expected in Service Portal without any effort.

However, because Service Portal is supported in a mobile environment, you may need to modify any customized forms and scripts. This approach ensures that the items display well on a mobile device and present a better user experience. Before transitioning to Service Portal, you may need to:

- Refactor client scripts used in your CMS/Service Catalog to use supported mobile APIs and global objects. For a list of supported APIs, see [Service Portal and client scripts](#).
- Build widgets to replace UI Macros and other unsupported scripts. If using a UI Macro in a catalog item form and referencing values on the form, you can use the following workaround instead: [Replace a Service Catalog form script with a widget](#).
- Simplify any complex forms used in your Service Catalog to fit the Service Portal two-column form layout.
- Consider which release supports the required functionality. You may want to upgrade your instance before transitioning to ensure that you have the required base system features.

### CMS to Service Portal transition

Your CMS may include complex forms and customizations that do not render as expected in Service Portal. Use this guide to understand how best to modify your CMS and Service Catalog implementation for Service Portal adoption, and to understand how a conversion may affect your users.

If you are considering transitioning from CMS to Service Portal, make sure that you understand the impact of moving to a mobile environment. Review the [Mobile client GlideForm (g form) scripting and migration](#).
## Support level and transition actions

<table>
<thead>
<tr>
<th>CMS component</th>
<th>Service Portal support</th>
<th>Possible transition actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data lookups</td>
<td>The client-side component of a data lookup is not supported in Service Portal. However, the data lookup is applied in the platform when a record is submitted or updated in Service Portal.</td>
<td>While data lookups are not applied in the Service Portal, the record updates as expected in the platform UI when submitted or updated in the Service Portal. If your CMS is used by requesters only, this limitation may not affect your implementation.</td>
</tr>
<tr>
<td>Content blocks</td>
<td>Because Content blocks use Jelly, they are not supported in Service Portal.</td>
<td>In the Service Portal, content blocks are replaced by widgets. Widgets are highly customizable components that can query record data, display and update records, and gather user input. Base system widgets generally cover most use cases. Just as you add content blocks to a page in your CMS, you can add widgets to a page using the Service Portal Designer.</td>
</tr>
</tbody>
</table>
| UI Macros       | Because UI Macros use Jelly, they are not supported in Service Portal.                                                                                                                                                   | • In Service Portal, you can use widgets instead of UI Macros. Base system widgets generally cover most use cases, but for custom solutions, you can develop new widgets using AngularJS.  
• If your implementation includes UI Macros in Service Catalog forms that reference other fields or variables in the form, you can embed the widget inside a Service Catalog variable. Learn more: Replace a Service Catalog form script with a widget. |
| UI actions      | All server-side UI actions are supported in Service Portal, although `setRedirectURL()` operations are ignored because Service Portal forms handle redirection in a different way than the platform. The form widget ignores all UI actions marked as Client. | • Refactor any UI actions to remove `setRedirectURL()` operations.  
• Check that UI actions are not marked as client.                                                                                                     |
<table>
<thead>
<tr>
<th>CMS component</th>
<th>Service Portal support</th>
<th>Possible transition actions</th>
</tr>
</thead>
</table>
| Catalog client scripts | Only UI Type options **Mobile / Service Portal** and **All** are supported. UI type **Desktop** is not supported in Service Portal. For a list of supported APIs, see [Service Portal and client scripts](#). | • Update your scripts to remove any unsupported client APIs.  
• Check that the script UI Type is set to **Mobile / Service Portal** or **All**. |

**Note:** Synchronous JavaScript calls are not supported in Service Portal and must be replaced by asynchronous calls. For example, the `getXMLWait()` method of the GlideAjax class is not supported in Service Portal. Instead, use one of the following supported asynchronous methods:

- `getXML(Function callback)`
- `getXMLAnswer(Function callback)`

For additional information on GlideAjax, refer to [GlideAjax](#).

To understand the impact of updating your CMS to work in a mobile environment, review [Mobile client GlideForm (g form) scripting and migration](#).

<table>
<thead>
<tr>
<th>UI policies</th>
<th>Scripted UI policies can only use APIs supported in Service Portal. For a list of supported APIs, see <a href="#">Service Portal and client scripts</a>.</th>
<th>Update your scripts to remove any unsupported client APIs.</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMS component</td>
<td>Service Portal support</td>
<td>Possible transition actions</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------</td>
<td>-----------------------------</td>
</tr>
</tbody>
</table>
| Service Catalog variables | Service Catalog variables are supported in Service Portal with the following exceptions:  
- UI Macros and UI pages variable types are not supported.  
- Validation Scripts for variables are not supported. Supported validation types include:  
  - The Mandatory field on the variable form.  
  - Read-only variables.  
  - All fields in the Availability tab of the variable form.  
- Default variable size is not supported.  
- Expanding and collapsing help text is not supported. Rather, the Help text and Instructions fields defined in the Annotations tab on the variable form are always expanded. The Help tag does not display.  
- The List Collector variable displays as a choice list instead of a slushbucket in the Service Portal. | • If embedding a widget in a catalog item form, you can use the UI Macro variable type. Learn more: Replace a Service Catalog form script with a widget.  
|          |                        | • If using variable with annotations, make sure to test your catalog items in Service Portal to ensure that help text displays as expected. |
| Order guides | Order Guides in Service Portal use the Order Guide widget.  
The following are not supported in Service Portal:  
- Three-step checkout  
- Uploading attachments | Upgrade to the Kingston release for a base system order guide widget that enables three-step checkout and uploading attachments. However, keep in mind that large order guides can cause performance issues in the Service Portal. If you have large order guides, you can:  
- Break them into multiple order guides.  
- Simplify variables used in the order guides.  
- As a temporary solution, you can render the Service Catalog item using an iFrame. See Service Catalog forms in Service Portal. |
| Record producers | Record producers are used in Service Portal with the following differences:  
- The sort order for catalog items in record producers is not honored.  
- Date values do not honor time zone when the record producer submits a record. | Make sure to test all record producers used in Service Portal to make sure that they behave as expected. |
| Login scenarios and redirects | In CMS, you used the CMSEntryPage script include to define login scenarios. Instead, Service Portal uses the SPEntryPage script include and related system properties to define login scenarios. Redirects are not supported in Service Portal. | In Service Portal, define login behavior by modifying the SPEntryPage script include and setting system properties.  
For more information, see Single sign-on, logins, and URL redirects. |
<table>
<thead>
<tr>
<th>CMS component</th>
<th>Service Portal support</th>
<th>Possible transition actions</th>
</tr>
</thead>
</table>
| Service Catalog forms | Service Catalog forms such as catalog items and record producers are rendered within widgets in a two-column layout. Complex forms may not display as expected.  
  - Only the top-level container settings are honored. If there are other containers within the top-level container, they are rendered as a single column. If there are container splits or nested containers within these additional containers, they are rendered as a single column. A top-level container is not a child of any other container.  
  - There can be a maximum of two columns in Service Portal. If your implementation includes forms with more than two columns, the fields are reorganized into two-columns in Service Portal.  
  - Variable sets are treated as containers. All previously listed rules apply to variable sets as well as any containers within them.  
  - Default variable size is not supported in Service Portal. | Simplify any complex forms in your Service Catalog.  
As a temporary solution, you can render the Service Catalog item using an iFrame. See Service Catalog forms in Service Portal. |
| Shopping cart       | The Service Portal includes a base system Shopping Cart widget.                        | Use the Shopping Cart widget.                                                                |

### Service Catalog forms in Service Portal

Service Catalog forms are rendered within Service Portal widgets in a two-column layout. Complex forms may not display as expected.

### Recommendations when creating Service Catalog forms

Use the following recommendations as a guide to building scalable forms that can be used in both applications:

- Keep forms simple. Because forms with multiple containers, variable sets, and client scripts do not always display as expected in Service Portal, keep forms short to eliminate conversion and debugging issues.
- Think in mobile. Any support for Catalog Client Scripts or Catalog UI Policies is the same as in mobile. Review the following resource: Mobile client GlideForm (g form) scripting and migration.
Form rendering in Service Portal

Containers and variable sets within Service Catalog forms are translated into a two-column layout when implemented in Service Portal. Service Catalog forms are rendered in Service Portal using the following rules:

- Only the top-level container settings are honored. If there are other containers within the top-level container, they are rendered as a single column. If there are container splits or nested containers within these additional containers, they are rendered as a single column. A top-level container is not a child of any other container.
- There can be a maximum of two columns in Service Portal. If your implementation includes forms with more than two columns, the fields are reorganized into two-columns in Service Portal.
- Variable sets are treated as containers. All previously listed rules apply to variable sets as well as any containers within them.
- Default variable size is not supported in Service Portal.

For other forms in the platform, the view determines how the form displays in Service Portal. For base system tables, the form opens in the Service Portal using the Service Portal table form view.

Example layout conversions

The following examples demonstrate how Service Catalog forms display in Service Portal.

Single-column form

A Service Catalog form with:

- Two containers.
- A single-column layout.
Service Catalog form

In Service Portal, the single-column layout renders as expected.
Two-column layout with subcontainers

A Service Catalog form with:

- A container with a two-column layout.
- A subcontainer with a single-column layout.
- A subcontainer with a two-column layout.
In Service Portal, the two-column layout setting of the subcontainer is ignored. The subcontainer renders as a single column.
## Two-column layout with variable sets and subcontainers

A Service Catalog form with:

- Containers with single-column and two-column layouts.
- Variable sets with a two-column layout within containers.
Service Catalog form

In Service Portal, the two-column layout settings of the variable sets are ignored when inside a container column.
<table>
<thead>
<tr>
<th>Container1</th>
<th>Variable1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>VariableSet1</td>
<td>VariableSet2</td>
</tr>
<tr>
<td>Variable5</td>
<td>Variable7</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Variable6</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Variable2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Container2</td>
<td>VariableSet3</td>
</tr>
<tr>
<td>Variable3</td>
<td>Variable8</td>
</tr>
<tr>
<td></td>
<td>Variable10</td>
</tr>
<tr>
<td>VariableSet2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Variable4</td>
</tr>
</tbody>
</table>
Containers within variable sets

A Service Catalog form with:

- Variable sets with single-column layouts.
- A container with a single-column layout with a container split within a single-column variable set.
- A container with a two-column layout within a single-column variable set.

Service Catalog form

In Service Portal, the container split and two-column container settings are ignored when inside a single-column variable set.
<table>
<thead>
<tr>
<th>Variable</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Variable1</td>
<td></td>
</tr>
<tr>
<td>Variable2</td>
<td></td>
</tr>
<tr>
<td>Variable3</td>
<td></td>
</tr>
<tr>
<td>Variable4</td>
<td></td>
</tr>
<tr>
<td>Variable5</td>
<td></td>
</tr>
<tr>
<td>Variable6</td>
<td></td>
</tr>
<tr>
<td>Variable7</td>
<td></td>
</tr>
<tr>
<td>Variable8</td>
<td></td>
</tr>
</tbody>
</table>
**Nested containers**

A Service Catalog form with:

- Containers that contain variable sets.
- Variable sets that contain nested containers.

---

**Service Catalog form**

In Service Portal, nested container formatting is ignored and displays as a single-column.
<table>
<thead>
<tr>
<th>Container1</th>
<th>VariableSet1</th>
<th>VariableSet2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Container2</td>
<td></td>
<td>NestedContainer1</td>
</tr>
<tr>
<td></td>
<td>Variable1</td>
<td>NestedVariable5</td>
</tr>
<tr>
<td></td>
<td>Variable2</td>
<td>NestedVariable6</td>
</tr>
<tr>
<td></td>
<td>Variable3</td>
<td>NestedVariable7</td>
</tr>
<tr>
<td></td>
<td>Variable4</td>
<td>NestedContainer2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NestedVariable8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NestedVariable9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NestedVariable10</td>
</tr>
</tbody>
</table>

Service Portal result
Render a complex form in Service Portal using an iFrame

Because complex forms do not display as expected in Service Portal, you can render catalog items, record producers, and order guides in Service Portal using an iFrame. This workaround is a temporary solution to enable your Service Portal to function as expected while you simplify any complex Service Catalog forms.

When rendering items in an iFrame in Service Portal, the following limitations apply:

- On catalog items and record producers, the attachment icon is not visible. As a result, users cannot attach any files during the submission. As a workaround, you can add the attachment button to your form.
- Click-through for the hover-over icon is not available.
- Forms are not optimized for a mobile environment.

Use the attached resources and follow the instructions detailed in the Community post: Service Catalog on Service Portal.

**Note:** Be sure to make changes in a test environment before updating your production instance.

Replace a Service Catalog form script with a widget

You can use widgets in Service Portal to replace UI Macros. If your Service Catalog form includes a UI Macro that references other fields or variables on the form, you can create a widget to hold reusable code and embed it within the Service Catalog form. Use special syntax to access any variable fields on the form.

Role required: admin or sp_admin

1. Create a widget that performs the action you would like to use in catalog item forms. See step 7 for a simple example widget that accesses another variable on the form.
2. Open a catalog item that previously used a UI Macro or other reusable component not supported in Service Portal.
3. In related lists, add a new variable to the catalog item.
4. Configure the variable form to add the **Widget** field.
5. In the **Type** field, select **Macro**.
6. In the **Widget** field, select a widget that performs the desired action.
7. Optional: Use the `$scope.page.g_form()` or `$scope.page.field` syntax in the embedded widget to access the catalog item values.

This example shows how to modify the value of a single-line text variable with the name **color** associated with the catalog item.

**Widget HTML Template**

```html
<div>
  Data from catalog variable:
  <h1>{{ c.data.message }}</h1>
</div>
```

**Widget client script**

```javascript
function($scope) {
  var c = this;
  
  //Watch for changes in the color variable
  $scope.$watch(function () {
```
You can use the following to access variable or catalog item fields:

- `$scope.page.g_form()`: The g_form instance on the form. You can use all supported g_form methods described in Service Portal and client scripts. For example, `g_form.setValue('variable_name', 'new value');`.
- `$scope.page.field()`: The object that represents the variable.

When you open the catalog item in the Service Portal, the embedded widget accesses the variable fields associated with the catalog item.

### What color would you like?

Blue

### Data from catalog variable:

Content of color variable: Blue

## Unsupported features in Service Portal

Service Portal is an alternative presentation layer for the platform. As such, not all features of the platform are extended to Service Portal. Consider your full application and the abilities of Service Portal before making considerable investments. ServiceNow will continue to enhance Service Portal over time.

### Not currently supported

- Approvals with e-signature
- Domain separation at Levels 1-3. However, Service Portal does include support for domain separation at the Data only level. For more information, see Application support for domain separation.
No plans to support

- @ Mentions
- Click-through/pop-ups
- Embedded HTML outside of HTML fields
- Embedded lists
- UI macros
- Formatters
- UI actions marked as Client
- Nested container Catalog variables
- Survey wizards

Some client scripting globals are also unavailable in Service Portal. For more information, see Service Portal and client scripts.

Service Portal and client scripts

You can use client scripts and catalog client scripts in the Service Portal if the UI Type is set to Mobile/Service Portal or All. Client scripts and catalog client scripts are used with the Form widget and SC Catalog Item widget, as opposed to a widget client controller.

Before flagging a script as Mobile/Service Portal or All, make sure that you are only using the mobile APIs. Setting a client script to Mobile does not ensure that it will work, it simply flags that the script should be attempted by the mobile app or the Service Portal. Many of your existing client scripts can be set to All as long as the API calls are supported by the mobile client scripting environment.

The topics in this section require advanced coding knowledge and an understanding of Service Portal APIs.

Checking desktop vs mobile runtime

You might want to mark a client script compatible with both desktop and mobile, but still do something different depending on the runtime. You can use this script:

```javascript
if (window === null)
    // Write your mobile compatible code here
else
    // Write your desktop compatible code here
```

Unsupported client scripting globals

Widget client controllers are full Angular controllers and are not subject to the unsupported client script globals listed here. Use jQuery and Angular as needed.

The following globals and APIs are unavailable in client scripts and catalog client scripts used in the Service Portal:

- window
- document
- $
- jQuery
- $$
- $j
Embedded widgets & g_form

When using the Service Catalog variable type **Macro** and **Macro with Label** you can pick a widget to embed in a catalog item form. Within the client controller for the embedded widget you can access the field object and catalog item g_form instance using:

- $scope.page.field
- $scope.page.g_form()

Supported client side APIs

These are the supported client scripting APIs you can use in onLoad, onChange, and onSubmit client scripts.

For detailed class and method information, see the API reference.
## Class Available methods

<table>
<thead>
<tr>
<th>g_form</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• addDecoration(fieldName, icon, title)</td>
<td></td>
</tr>
<tr>
<td>• addErrorMessage(message)</td>
<td></td>
</tr>
<tr>
<td>• addInfoMessage(message)</td>
<td></td>
</tr>
<tr>
<td>• addOption(fieldName, value, label, index)</td>
<td></td>
</tr>
<tr>
<td>• clearMessages()</td>
<td></td>
</tr>
<tr>
<td>• clearOptions(fieldName)</td>
<td></td>
</tr>
<tr>
<td>• clearValue(fieldName)</td>
<td></td>
</tr>
<tr>
<td>• getActionName()</td>
<td></td>
</tr>
<tr>
<td>• getBooleanValue(fieldName)</td>
<td></td>
</tr>
<tr>
<td>• getDecimalValue(fieldName)</td>
<td></td>
</tr>
<tr>
<td>• getEncodedRecord()</td>
<td></td>
</tr>
<tr>
<td>• getFieldNames()</td>
<td></td>
</tr>
<tr>
<td>• getFieldValidation(fieldName)</td>
<td></td>
</tr>
<tr>
<td>• getFormValidation(fieldName)</td>
<td></td>
</tr>
<tr>
<td>• getLabel(fieldName)</td>
<td></td>
</tr>
<tr>
<td>• getReference(fieldName, callback)</td>
<td></td>
</tr>
<tr>
<td>• getRelatedListNames()</td>
<td></td>
</tr>
<tr>
<td>• getSectionNames()</td>
<td></td>
</tr>
<tr>
<td>• getSysId()</td>
<td></td>
</tr>
<tr>
<td>• getTableName()</td>
<td></td>
</tr>
<tr>
<td>• getValue(fieldName)</td>
<td></td>
</tr>
<tr>
<td>• hasField(fieldName)</td>
<td></td>
</tr>
<tr>
<td>• hideAllFieldMsgs(type: &quot;info</td>
<td>error&quot;)</td>
</tr>
<tr>
<td>• hideErrorBox(fieldName)</td>
<td></td>
</tr>
<tr>
<td>• hideFieldMsg(fieldName, clearAll)</td>
<td></td>
</tr>
<tr>
<td>• hideRelatedList(listTableName)</td>
<td></td>
</tr>
<tr>
<td>• hideRelatedLists()</td>
<td></td>
</tr>
<tr>
<td>• isMandatory(fieldName)</td>
<td></td>
</tr>
<tr>
<td>• isNewRecord()</td>
<td></td>
</tr>
<tr>
<td>• isReadOnly(fieldName)</td>
<td></td>
</tr>
<tr>
<td>• isVisible(fieldName)</td>
<td></td>
</tr>
<tr>
<td>• removeDecoration(fieldName, icon, title)</td>
<td></td>
</tr>
<tr>
<td>• removeOption(fieldName, value)</td>
<td></td>
</tr>
<tr>
<td>• save()</td>
<td></td>
</tr>
<tr>
<td>• serialize(onlyDirtyFields)</td>
<td></td>
</tr>
<tr>
<td>• setFieldPlaceholder(fieldName, placeholder)</td>
<td></td>
</tr>
<tr>
<td>• setLabel(fieldName, label)</td>
<td></td>
</tr>
<tr>
<td>• setMandatory(fieldName, isMandatory)</td>
<td></td>
</tr>
<tr>
<td>• setReadOnly(fieldName, isReadOnly)</td>
<td></td>
</tr>
<tr>
<td>• setSectionDisplay(sectionName, isVisible)</td>
<td></td>
</tr>
<tr>
<td>• setValue(fieldName, value, displayValue)</td>
<td></td>
</tr>
<tr>
<td>• showErrorBox(fieldName, message, scrollForm)</td>
<td></td>
</tr>
<tr>
<td>• showFieldMsg(fieldName, message, type: &quot;info</td>
<td>error&quot;, scrollForm)</td>
</tr>
<tr>
<td>• showRelatedList(listTableName)</td>
<td></td>
</tr>
<tr>
<td>• showRelatedLists()</td>
<td></td>
</tr>
<tr>
<td>• submit(submitActionName)</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Using the variables.var_name notation with the g_form API is not supported in Service Portal. g_form as a global object cannot be used in a widget client controller or in a UI script.
<table>
<thead>
<tr>
<th>Class</th>
<th>Available methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>g_list</td>
<td>• get(fieldName)</td>
</tr>
<tr>
<td></td>
<td>• addItem(value, displayValue)</td>
</tr>
<tr>
<td></td>
<td>• removeItem(value)</td>
</tr>
<tr>
<td></td>
<td>• reset()</td>
</tr>
<tr>
<td></td>
<td>• setQuery(queryString)</td>
</tr>
<tr>
<td></td>
<td>• setDefaultOperator(operator)</td>
</tr>
<tr>
<td></td>
<td>• getDefaultOperator()</td>
</tr>
<tr>
<td>g_service_catalog</td>
<td>isOrderGuide()</td>
</tr>
<tr>
<td>GlideAjax</td>
<td>new GlideAjax(scriptIncludeName)</td>
</tr>
<tr>
<td></td>
<td>• addParam (name, value)</td>
</tr>
<tr>
<td></td>
<td>• getParam (name)</td>
</tr>
<tr>
<td></td>
<td>• getXML(callback)</td>
</tr>
<tr>
<td></td>
<td>• getXMLAnswer(callback)</td>
</tr>
<tr>
<td></td>
<td>• getJSON(callback)</td>
</tr>
<tr>
<td></td>
<td>• setErrorCallback(errorCallback)</td>
</tr>
<tr>
<td></td>
<td>• getURL()</td>
</tr>
<tr>
<td></td>
<td>• getParams()</td>
</tr>
<tr>
<td></td>
<td>• execute()</td>
</tr>
<tr>
<td></td>
<td>• successCallback(data, status, xhr)</td>
</tr>
<tr>
<td></td>
<td>• errorCallback(xhr)</td>
</tr>
<tr>
<td></td>
<td>• setScope(scope)</td>
</tr>
</tbody>
</table>

**Note:** Because the mobile platform does not allow synchronous GlideAjax calls, the getXMLWait() method in a GlideAjax call will not work in the Service Portal. Instead, use one of the following:

- getXML(Function callback)
- getXMLAnswer(Function callback)
### Class: GlideRecord

<table>
<thead>
<tr>
<th>Available methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>new GlideRecord(tableName)</td>
</tr>
<tr>
<td>addQuery(encodedQuery)</td>
</tr>
<tr>
<td>addQuery(fieldName, operator, value)</td>
</tr>
<tr>
<td>getEncodedQuery()</td>
</tr>
<tr>
<td>getId()</td>
</tr>
<tr>
<td>getTableName()</td>
</tr>
<tr>
<td>hasNext()</td>
</tr>
<tr>
<td>insert(callback)</td>
</tr>
<tr>
<td>gotoTop()</td>
</tr>
<tr>
<td>next()</td>
</tr>
<tr>
<td>loadRow(rowObj)</td>
</tr>
<tr>
<td>getValue(fieldName)</td>
</tr>
<tr>
<td>setValue(fieldName, value)</td>
</tr>
<tr>
<td>isDotWalkField(fieldName)</td>
</tr>
<tr>
<td>addOrderBy(fieldName)</td>
</tr>
<tr>
<td>setDisplayFields(fieldNames)</td>
</tr>
<tr>
<td>query(callback)</td>
</tr>
<tr>
<td>setRows(rowsArray)</td>
</tr>
<tr>
<td>setTableName(tableName)</td>
</tr>
<tr>
<td>setLimit(maxInt)</td>
</tr>
<tr>
<td>getLimit()</td>
</tr>
<tr>
<td>getMessage(messageKey, callback)</td>
</tr>
</tbody>
</table>

### Usage examples

**g_list**

The `g_list` global helps you set the filter of a glide list element or a list collector variable. Use this API in place of the `g_filter` API on desktop client scripts.

```javascript
function onLoad() {
  var myListCollector = g_list.get("my_list_collector");
  myListCollector.reset();

  myListCollector.setQuery("active=true^category=8c7b22230b402200b0b2c6317673a62");
  myListCollector.addItem('3a700d39af5f4fc0aab978df90f4c692', 'Power Supply');
  myListCollector.addItem('1cb93419a3a248318da8f814140b42f6', 'Backpack');
}
```

**g_service_catalog**

`g_service_catalog` is only available in Service Portal service catalog item scripts. Use this API to know if your catalog item script is run as part of an order guide or on its own.

```javascript
function onLoad() {
  if (window) // if CMS, don't run this
    return;

  // g_service_catalog api for Service Portal and Mobile
  var isOrderGuide = g_service_catalog.isOrderGuide();
  g_form.setValue("is_order_guide", isOrder_guide ? "Yes!" : "Nope :(");
```
Unsupported form scripts for Service Portal

Because Service Portal doesn't use Jelly, not all form customizations are available.

<table>
<thead>
<tr>
<th>Form script</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client scripts</td>
<td>Service Portal uses UI type set to <strong>All</strong> or <strong>Mobile/Service Portal</strong>. Client Scripts marked as <strong>Desktop</strong> rely on legacy APIs that aren't supported by Service Portal. Before flagging a script as Mobile or All, make sure you are only using mobile APIs.</td>
</tr>
<tr>
<td>UI Actions</td>
<td>All server-side UI actions are supported in Service Portal, although setRedirectURL() operations are ignored because Service Portal forms handle redirection in a different way than the platform. Any UI Actions marked as <strong>Client</strong> are ignored by the form widget.</td>
</tr>
<tr>
<td>UI Policies</td>
<td>Supported, although you should use only declarative UI Policies. Avoid scripting unless the outcome cannot be achieved through the condition builder.</td>
</tr>
<tr>
<td>UI Macros</td>
<td>Not supported as UI macros use Jelly.</td>
</tr>
<tr>
<td>Formatters</td>
<td>Not supported as formatters use Jelly.</td>
</tr>
</tbody>
</table>

Understanding Widgets

Widgets are what define the content in your portal. You can use the base system widgets provided with Service Portal, clone and modify widgets, or develop custom widgets to fit your own needs.

Out of box widgets are read-only so you can benefit from future updates, which means you can't update their code. If you need to make major changes, clone the widget and give it another name and ID.

Widget context menu

From any rendered Service Portal page you can CTRL+right-click a widget to see more configuration options in a context menu.

For example, navigate to **Service Portal > Service Portal Home** to open a sample portal page. CTRL+right-click Knowledge Base on that page.
Note: You must have the admin or sp_admin role to see the widget context menu. When you impersonate a user without one of those roles, you can still see the menu. However, a regular user signed in without those roles cannot see the menu.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Widget performance</td>
<td>How long it takes for a widget to load</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Instance options</td>
<td>Specify an instance of a widget. Widgets instance options vary depending on the widget you select. For example, the instance options for the cool clock widget include different time zones for each instance, so you can have the same clock four times on a page, but with all different time zones.</td>
</tr>
<tr>
<td>Instance in Page Editor</td>
<td>Opens that instance of the widget in the Page Editor</td>
</tr>
<tr>
<td>Page Designer</td>
<td>Opens the widget in the Service Portal Designer, which lets you add containers, columns, and widgets. You can add styling from the Service Portal Designer to your specific widget or to the page the widget lives on.</td>
</tr>
<tr>
<td>Edit Container Background</td>
<td>Make changes to the layout in which the widget is located.</td>
</tr>
<tr>
<td>Widget Options Schema</td>
<td>Define the actual options you can select for an instance of a widget. For more information on configuring your own instance options, see Widget option schema.</td>
</tr>
<tr>
<td>Widget in Form Modal</td>
<td>Opens the widget form in a pop up window so you can make quick changes to the widget.</td>
</tr>
<tr>
<td>Widget in Editor</td>
<td>Opens the widget in the Widget Editor. You can use the Widget Editor to configure HTML templates, CSS, client scripts, service scripts, and demo data for the widget.</td>
</tr>
<tr>
<td>Log to console: $scope.data</td>
<td>The $scope.data object passes data from the server to the client side controller. Instead of adding console.log messages or alerts into the controller code, you can just log the $scope.data object to the browser console and view the data there.</td>
</tr>
<tr>
<td>Log to console: $scope</td>
<td>Similar to the $scope.data object, except it logs everything in $scope to the console.</td>
</tr>
</tbody>
</table>

**Widget library**

Widgets included with Service Portal can be customized to suit your own needs or as a basic code sample for you to refer to as you are building your own widgets.

Due to the ever-changing number of widgets that exist at any given time in Service Portal, this is not a definitive list. More widget descriptions will be added as they become available.

Depending on your configuration, widgets that do not contain any information do not appear in your Service Portal page.

To view the instance options for a widget, use the widget context menu.

**Example widgets**

- Approvals widget
- Approval Info widget
- Approval Record widget
- Breadcrumbs widget
- Breakout Game widget
- Calculator widget
- Carousel widget
- Cool Clock widget
- Header menu widget
- Hello World widgets
- HTML widget
- Icon Link widget

**Service Catalog widgets**

- SP Variable Editor widget
- Catalog Content widget
- Request Fields widget
- Requested Items widget
- SC Catalog Item widget
- SC Categories widget
- SC Category Page widget
- SC Order Guide widget
- SC Popular Items widget
- SC Save Bundles widget
- SC Saved Carts widget

**Knowledge Management widgets**

- KB also in Category widget
- KB Article Comments widget
- KB Article Page widget
- KB Categories widget
- KB Category Page widget
- KB Most Viewed widget
- KB News widget
- KB Search widget
- KB Top Rated widget
- KB View widget
- KB View 2 widget
- My Favorite Tags widget

© 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.
Example widgets

All widgets in Service Portal can be used as example code for how scripts are used in a widget. However, several out-of-box widgets have been included expressly for this purpose.

Use the example widgets to see how to use HTML, CSS, or client and server scripts in Service Portal. You can also clone and extend each widget to suit your needs.

Approvals widget

Users can approve or reject items directly within Service Portal.

Note: Service Portal does not currently support Approvals with e-signature.
Approvals widget

Instance options

Use the instance options to change the appearance of the approvals widget.
### Approvals widget instance options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bootstrap color</td>
<td>Color scheme for the widget. The default colors are defined by the portal theme, but if you want the instance to have a specific color, select the option from the list.</td>
</tr>
<tr>
<td>Glyph</td>
<td>Add an icon to display beside the widget name.</td>
</tr>
<tr>
<td>Buttons stacked side by side</td>
<td>If this check box is selected, the Approve and Reject buttons appear horizontally beside each other. If this check box is cleared, the Approve and Reject buttons appear stacked vertically.</td>
</tr>
<tr>
<td>Max number of elements shown in the list</td>
<td>Limit the number of approvals users see on a page. The default number is 10. Only enter numbers greater than 0.</td>
</tr>
<tr>
<td>Who can view instances/who cannot view instances</td>
<td>Control who can or cannot view a widget instance with user criteria. User criteria must be enabled for this option to appear.</td>
</tr>
</tbody>
</table>
Approval Info widget
The Approval Info widget works in tandem with the Approval widget to display details about the approval request.

![Approval Info widget](image)

Instance options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bootstrap color</td>
<td>Color scheme for the widget. The default colors are defined by the portal theme, but if you want the instance to have a specific color, select the option from the list.</td>
</tr>
</tbody>
</table>

Approval Record widget
The Approval Record widget shows the full record for an approval including the activity stream.
Approval Record widget

Instance options

The approval record widget does not include instance options.

Breadcrumbs widget

The breadcrumbs widget allows users to easily navigate around a portal.
Breadcrumbs widget

**Instance options**

The breadcrumbs widget does not have instance options. It displays information based on where a page is located in a portal.

**Breakout Game widget**

The Breakout Game widget is a fun 404 interaction for pages that do not exist.

Control using mouse or keyboard arrow keys.

Breakout Game widget

**Instance options**

The Breakout Game does not have instance option. You can use it as an example of how to use the Link Function as part of an Angular Directive.

**Calculator widget**

The calculator widget does simple calculations.
Use the calculator widget as an example of how to pass data between the client and server.

![Calculator widget](image)

### Instance options

The calculator widget does not include instance options.

**Carousel widget**

The carousel widget displays a scrolling list of images.

Use the carousel widget to showcase items on your portal page. For example, display items available in a service catalog at the top of the service catalog page.
Carousel widget

Add slides to the carousel widget

Use the related lists for an instance of the carousel widget to add images for the carousel widget to scroll through.

Role required: Admin or sp_admin

1. Navigate to Service Portal > Widgets > Carousel.
2. Open the Carousel widget record.
3. From the carousel form, on the Instances related list, under instances, open a carousel instance.
4. From the instance of carousel form, click New on the Carousel Slides related list.
5. Complete the form.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the carousel slide. Use the name to differentiate the slide from other slide records.</td>
</tr>
<tr>
<td>Order</td>
<td>Where the slide appears in the list of slides</td>
</tr>
<tr>
<td>HREF/URL</td>
<td>Link to the item in the slide. For example, for a slide with a catalog item, link to page for the catalog item using the HREF ?id=&lt;page name&gt;&amp;sys_id=&lt;sys_id for item&gt;. For more information on linking to a page within a portal, see Navigate by URL. You can also link to other sites using the URL.</td>
</tr>
</tbody>
</table>
Repeat this step for as many slides as you want to appear in the carousel widget.

*Cool Clock widget*

The Cool Clock widget uses instance options to show different times around the world.

Cool clocks demonstrates how to use instance options in a widget. The time zone is loaded using an instance option. If you do not select a time zone, the widget uses a default time zone.
Instance options

Cool clock widget instance options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Name of the clock, for example New York, NY. The name appears below the clock so it helps to use a name related to the time zone.</td>
</tr>
<tr>
<td>Timezone</td>
<td>The location from which the time is displayed. Use the local full name, for example, America/New York, instead of the abbreviated time zone. Using the full name allows time zones to stay consistent with daylight savings time. The default value is America/Los Angeles</td>
</tr>
<tr>
<td>Second hand color</td>
<td>Color of the second hand using the hex code, RGB, or color name. The default value is red.</td>
</tr>
</tbody>
</table>

Data table from instance definition widget
Data table from instance definition displays a table that you define using the widget instance options.

After you add the data table from instance definition widget to a page, use the instance options to configure the appearance of the table.
### Incidents

All &gt; Active = true, priority=1 critical

<table>
<thead>
<tr>
<th>Number</th>
<th>Category</th>
<th>Short description</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>INC0000001</td>
<td>Network</td>
<td>Can't read email</td>
<td>1 - Crit</td>
</tr>
<tr>
<td>INC0000004</td>
<td>Inquiry / Help</td>
<td>Forgot email password</td>
<td>1 - Crit</td>
</tr>
<tr>
<td>INC0000005</td>
<td>Hardware</td>
<td>CPU load high for over 10 minutes</td>
<td>1 - Crit</td>
</tr>
<tr>
<td>INC0000006</td>
<td>Software</td>
<td>Hang when trying to print VISIO document</td>
<td>1 - Crit</td>
</tr>
<tr>
<td>INC0000008</td>
<td>Inquiry / Help</td>
<td>Printer in my office is out of toner</td>
<td>1 - Crit</td>
</tr>
</tbody>
</table>

Data table from instance definition widget

### Instance options

#### Data table instance options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>The title of the widget. If you leave this field empty the name of the table displays as the widget name.</td>
</tr>
<tr>
<td>Table</td>
<td>The table that the widget displays records from.</td>
</tr>
<tr>
<td>Filter</td>
<td>Text field from the condition builder that you can use to limit the items returned in the table. To create a filter, use the context menu to open the widget instance in the platform. Then use the condition builder to create a filter.</td>
</tr>
<tr>
<td>Maximum entries</td>
<td>Limits the number of items displayed in the table. If there are more entries than allowed in the table, users can scroll to the next page.</td>
</tr>
<tr>
<td>Glyph</td>
<td>Icon that displays beside the widget title</td>
</tr>
<tr>
<td>Fields</td>
<td>Columns to display in the table.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Bootstrap color</td>
<td>Color scheme for the widget. The default colors are defined by the portal theme, but if you want the instance to have a specific color, select the option from the list.</td>
</tr>
<tr>
<td>Link to this page</td>
<td>Direct users to a specific page when they click a record. By default, clicking an entry in the table opens that entry in a form.</td>
</tr>
<tr>
<td>Enable Filter</td>
<td>Select this check box to allow users to create their own filter for the table. This option is currently only supported for the Data Table widgets.</td>
</tr>
</tbody>
</table>

**Data Table from URL definition widget**

The Data Table from URL definition widget displays the table you select from the list.

**Instance options**

Complete the instance options to define the table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>The title of the widget. Select the Use Instance Title check box to use this title instead of the name of the table.</td>
</tr>
<tr>
<td>Glyph</td>
<td>Icon that displays beside the widget title</td>
</tr>
<tr>
<td>Bootstrap color</td>
<td>Color scheme for the widget. The default colors are defined by the portal theme, but if you want the instance to have a specific color, select the option from the list.</td>
</tr>
<tr>
<td>Link to this page</td>
<td>Direct users to a specific page when the click a record. By default, clicking an entry in the table opens that entry in a form.</td>
</tr>
</tbody>
</table>
### ServiceNow

#### Jakarta

**Now Platform Capabilities**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fields</td>
<td>Columns to display in the table. For example, short description or priority.</td>
</tr>
<tr>
<td>Use Instance Title</td>
<td>Select to use the title in the Title field instead of the table title.</td>
</tr>
<tr>
<td>Enable Filter</td>
<td>Select this check box to allow users to create their own filter for the table</td>
</tr>
</tbody>
</table>

If **Enable filter** is enabled in the instance options, users can add custom conditions to filter the results.

---

**Data Table URL with condition builder**

For more information on using the condition builder, see [Create a filter in List v3](#).

**Note:** The condition builder is only available in the desktop view.

**Form widget**

The form widget is a platform form within the Service Portal UI with a few differences.
Form widget

**URL Parameters**

The form widget accepts the following parameters within the URL

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sys_id or sl_sys_id</td>
<td>The sys_id for the record to be displayed</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.
### Parameter and Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>table, sl_table, or t</td>
<td>The table for the record to be displayed</td>
</tr>
<tr>
<td>view or v</td>
<td>The view used to display the record</td>
</tr>
</tbody>
</table>

In the following example, the URL would display an incident with a sys_id of 1c741bd70b2322007518478d83673af3 in the portal view.

```text
https://example.service-now.com/sp?id=form&table=incident&sys_id=1c741bd70b2322007518478d83673af3&view=portal
```

### Supported and unsupported form scripts

<table>
<thead>
<tr>
<th>Form script</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client scripts</td>
<td>Service Portal uses UI type set to All or Mobile/Service Portal. Client Scripts marked as Desktop rely on legacy APIs that aren't supported by Service Portal. Before flagging a script as Mobile or All, make sure you are only using mobile APIs.</td>
</tr>
<tr>
<td>UI Actions</td>
<td>All server-side UI actions are supported in Service Portal, although selfRedirectURL() operations are ignored because Service Portal forms handle redirection in a different way than the platform. Any UI Actions marked as Client are ignored by the form widget.</td>
</tr>
<tr>
<td>UI Policies</td>
<td>Supported, although you should use only declarative UI Policies. Avoid scripting unless the outcome cannot be achieved through the condition builder.</td>
</tr>
<tr>
<td>UI Macros</td>
<td>Not supported as UI macros use Jelly.</td>
</tr>
<tr>
<td>Formatters</td>
<td>Not supported as formatters use Jelly.</td>
</tr>
</tbody>
</table>

### Header menu widget

The Header Menu widget controls which options appear in the page header.

Unlike other widgets in Service Portal, the header menu widget is not something you drag onto a page. Instead you configure the header menu by associating the header menu with a 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.
Hello World widgets

The Hello World widgets are included with Service Portal as examples of how to use and create widgets.

All three Hello World widgets display the same way. The real difference between them is in their underlying code base. Each version of the widget uses a different method of using the server and client script.

To view the Hello World widgets, navigate to Service Portal > Service Portal Configuration then click Widget Editor. In the Widget Editor, click Check out the Hello World Example.

Hello World 1 displays how the HTML template and the client script communicate. For more information on using the client script in Service Portal, see Widget client script.

Use the widget list to switch to Hello World 2 or 3.
Hello World 2 includes an example of how the server script can be used as well.
For more information on Service Portal APIs, see the GlideSPScriptable API.

**HTML widget**

Use the HTML widget to directly inject HTML, text, lists, or content in general into a page.

Because the HTML widget can contain content of any kind, any example may just appear as regular text. For example, the HTML widget appears as a box of text on the 404 page.
ServiceNow Jakarta Now Platform Capabilities

Sorry, the page you requested was not found.
This page you were trying to reach at this address doesn’t seem to exist. This is usually the result of a bad or outdated link. We apologize for any inconvenience.
While you are here, see if you can beat the "404" in a game of Breakout.

HTML widget

Instance options

HTML widget instance options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Name for the HTML text. Users do not see this information.</td>
</tr>
</tbody>
</table>
| HTML | Text box for the HTML. Use the toolbar like most word processing tool bars. For more information on using the toolbar, see Formatting in the TinyMCE editor.

Icon Link widget
Link to any other item.

Configure Icon Link widgets to link to a specific URL, page within the portal, or another widget. The related list for this widget also allow you configure accessibility by user name or role.

Order Something
Browse the catalog for services and items you need

Icon Link widget
Instance options

Instance options fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Name of the icon link. Choose something that defines what the widget is linking to.</td>
</tr>
<tr>
<td>Glyph</td>
<td>Icon for the widget.</td>
</tr>
<tr>
<td>Bootstrap class name</td>
<td>Use concurrently with page or theme level CSS.</td>
</tr>
</tbody>
</table>
| Type                   | Defines what the widget links to. The fields that appear on the form vary depending on which option you select. Choose from:  
                          - Page: Another page in the Service Portal  
                          - URL: Link to an external website.  
                          - Catalog category: Link to a specific catalog category within the service catalog.  
                          - Catalog item: Link to a specific catalog item.  
                          - KB topic: Link to a KB topic page.  
                          - KB article: Link to a KB article by number.  
                          - KB category: Link to a specific KB category within the knowledge base. |
| Page                   | Page within the portal that you want to link to. This field varies depending on the Type you choose. |
| Bootstrap color        | Color scheme for the widget. The default colors are defined by the portal theme, but if you want the instance to have a specific color, select the option from the list. |
| Template               | The appearance of the link icon widget. Choose from:  
                          - Top icon  
                          - Circle icon  
                          - Color box |

**Icon menu list widget**

A simple list with a glyph icon next to each link.

Configure the icon information using the Menu Items related list.
Icon Menu list widget

1. From the instance options for the icon menu list widget, under Related Lists, click **Menu Items**.
2. Click **New**.
3. Use the fields on the New Menu Items form to configure the icons for the icon menu list widget.

### Icon menu list widget instance options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Label</strong></td>
<td>Name or description of the icon</td>
</tr>
<tr>
<td><strong>Parent Menu</strong></td>
<td>The name of the menu that the icon appears in. This automatically populates with the name of the icon menu list widget that you created but you have the option to switch it to another menu.</td>
</tr>
<tr>
<td><strong>Order</strong></td>
<td>The order in which the icons appear in the icon menu list widget.</td>
</tr>
<tr>
<td><strong>Parent menu Item</strong></td>
<td>Nest menu items within a parent menu.</td>
</tr>
<tr>
<td><strong>Page</strong></td>
<td>The page within Service Portal that the icon links to. Select <strong>Page</strong> from the Type list to enable this option.</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Select the type of link you want the icon to have. You can link to pages within Service Portal, external URLs, KB articles, Service Catalog, or lists. Different fields will appear on the form depending on the option you select from the list.</td>
</tr>
<tr>
<td><strong>Condition</strong></td>
<td>Determines what conditions are required for menu items to show in the header. For more information on what conditions to use in the <strong>Condition</strong> field, see <a href="#">Create a UI action</a>.</td>
</tr>
<tr>
<td><strong>Glyph</strong></td>
<td>Icon that you want to display in the icon menu list widget.</td>
</tr>
</tbody>
</table>
Language Switch widget
Add the Language Switch widget to a landing or homepage to allow your users to change the language of the page.

Language Switch widget

Instance options
The Language Switch widget does not include any instance options.

Link Button widget
The Link Button widget is a button you can nest in any other widget that links to another destination.

Instance options

Instance option fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bootstrap color</td>
<td>Color scheme for the widget. The default colors are defined by the portal theme, but if you want the instance to have a specific color, select the option from the list.</td>
</tr>
<tr>
<td>Link for button</td>
<td>Page that the button links to. Use ?id=&lt;page_name&gt; to link to another page in the portal.</td>
</tr>
<tr>
<td>Contents of button</td>
<td>The button text.</td>
</tr>
</tbody>
</table>
Login widget
The login widget controls user access to your site.

![Login widget](image)

Instance options

Instance options fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show panel</td>
<td>Show or hide the panel that appears behind the login widget. The panel helps the widget stand out from the page background rather than blending in.</td>
</tr>
</tbody>
</table>

My Requests widget
The My Requests widget stores all of your open requests in one place.

The list is updated in real time so you can see your requests getting processed. The widget pulls open request information from the sc_request table.
My Requests widget

### Instance options

#### Instance options fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Name of the widget. The name you enter here appears in the header for the widget.</td>
</tr>
<tr>
<td>Bootstrap color</td>
<td>Color scheme for the widget. The default colors are defined by the portal theme, but if you want the instance to have a specific color, select the option from the list.</td>
</tr>
<tr>
<td>Maximum entries</td>
<td>The maximum number of entries allowed to appear in the widget.</td>
</tr>
</tbody>
</table>

**Organization Chart widget**

The Organization Chart widget shows employees in a tree structure relative to their manager.

**Using the widget**

In the text input field, enter or select a user to see their manager and subordinates. The widget uses information from the User (sys_user) record to display the organization hierarchy relative to the selected user.
Click a card to open the profile page for that user. To reconfigure the card link, change the URL or Page in the widget instance options.

You can drag individual cards to rearrange the chart.

You can zoom in or out of the chart view by clicking the magnifying glass icons or by scrolling.

**Instance options**

Use the instance options to configure the Organization Chart widget for a portal page.
**Note:** There are no valid values for several instance options. By default, you can set only the following instance options:

- User Background Color
- Node Background Color
- URL
- Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td></td>
</tr>
<tr>
<td>Card Fields</td>
<td>Fields from the user record that appear on each card. By default, each card displays the name, title, department, email, phone, and location of each user. There are no valid values that you can enter in this field.</td>
</tr>
</tbody>
</table>

Presentation
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Background Color</td>
<td>Color of the user card. Use color names or Hex codes. For example, you can enter red or #ff0000.</td>
</tr>
</tbody>
</table>

The user background color is **lightblue** by default.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node Background Color</td>
<td>Color of cards that extend from the user card. Use color names or Hex codes. For example, you can enter yellow or #FFFF00.</td>
</tr>
</tbody>
</table>

The node background color is **azure** by default.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Table Layout | Size and margin of the content in each card.  
There are no valid values that you can enter in this field. |
| Row Layout  | Alignment of the text in the card. The text is left-aligned by default.  
There are no valid values that you can enter in this field. |
| Line      | Color of the lines that connect cards. The lines are black by default.  
There are no valid values that you can enter in this field. |
| Tree Layout | Size, spacing, and alignment of the chart.  
There are no valid values that you can enter in this field. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Picture Layout</td>
<td>Size of image space in each card. By default, the image space is 55x65 pixels. The user image is shrunk or stretched to fit the space. <strong>There are no valid values that you can enter in this field.</strong></td>
</tr>
<tr>
<td>Behavior</td>
<td>Web address of the page that opens when you click a card. Use the part of the portal URL that references the page ID. For example, to navigate to the Service Catalog, enter ?id=sc_category. If left blank, clicking the card opens the page that is specified in the Page field. If the Page field is also blank, clicking the card opens the user profile page by default.</td>
</tr>
<tr>
<td>URL</td>
<td>Portal page that opens when you click a card. Use the page ID. If left blank, clicking the card opens the web address in the URL field. If the URL field is also blank, clicking the card opens the user profile page by default. <strong>Note:</strong> The URL field overwrites the Page field. To specify a page rather than a URL, leave the URL field blank.</td>
</tr>
</tbody>
</table>

*Simple List widget*

The Simple List widget can be used to display any list in the system within Service Portal.
My Open Incidents

InsideSales NeuralView Instance relocation from US datacenter to Hongkong dat...
INC0006789 • a day

Results not as per expectation after performing the documented steps in Oracl...
INC0006911 • a day

Performance degrade observed in Oracle Planning and Budgeting
INC0006890 • a day

Network response time is poor
INC0006800 • a day

Performance degrade observed in Eloqua Marketing Measurement
INC0006790 • a day

Fidelity Stock Plan Services upgrade to the latest version
INC0006797 • a day

Simple List widget

Instance options

Instance options fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>The platform table that the simple list is formed from.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Display field</td>
<td>Main field that displays as the ‘title’ of the list item.</td>
</tr>
<tr>
<td>Glyph</td>
<td>Icon that displays next to the widget name in the header.</td>
</tr>
<tr>
<td>Filter</td>
<td>Conditions that are applied to the list. To edit the filter, in the widget instance options context menu, select <strong>Open in platform</strong>. Use the Table &amp; Filter tab to apply conditions to the simple list. For more information, see <a href="#">Create a filter in List v3</a>.</td>
</tr>
<tr>
<td>Link to this page</td>
<td>Portal page to link to from a list item.</td>
</tr>
<tr>
<td>Bootstrap color</td>
<td>Color scheme for the widget. The default colors are defined by the portal theme, but if you want the instance to have a specific color, select the option from the list.</td>
</tr>
<tr>
<td>Bootstrap size</td>
<td>Size of the widget</td>
</tr>
<tr>
<td>Maximum entries</td>
<td>Maximum allowed number of entries that appear in the list at one time.</td>
</tr>
<tr>
<td>Show even when empty</td>
<td>Widgets are designed to hide on a page when no results meet the criteria. Select this option to make the simple list widget display on a page even when empty.</td>
</tr>
<tr>
<td>List body height</td>
<td>Actual length of the widget in pixels or EMs. A long list with a small body height includes a scroll bar option.</td>
</tr>
<tr>
<td>Image field</td>
<td>Displays an image in the list. Select a field type that includes an image. For example, Photo.</td>
</tr>
<tr>
<td>Secondary fields</td>
<td>Fields from the list item that display in addition to the main display field.</td>
</tr>
<tr>
<td>Rounded images</td>
<td>Makes any images selected in the Image field round in the list.</td>
</tr>
<tr>
<td>List page</td>
<td>The page that opens when a user selects <strong>View all</strong> in the widget footer. Select a page that correlates with the items that display in the list.</td>
</tr>
<tr>
<td>Hide footer</td>
<td>Show or hide the widget footer</td>
</tr>
<tr>
<td>View</td>
<td>The view option for when a list item links to a form. The <strong>Link to this page</strong> field must be set to a form page for this option to work.</td>
</tr>
</tbody>
</table>

**Sample Footer widget**

The Sample Footer widget is an example of a footer you can use in your portal.

Unlike other widgets in Service Portal, you add a footer to your portal by configuring it in the Theme form. For more information on adding a footer to a portal, see [Create a service portal and its branding](#).

© 2016 ServiceNow. All rights reserved.
Instance options

The Sample footer widget does not include instance options.

Stock widget
The Stock widget displays an example of how widgets communicate with data outside of the system.

The Stock widget pulls information from an online data source for stock information.

Note: As of November 2017, the Yahoo Finance API has been discontinued. As the stock widget relies on this functionality, the widget is no longer supported, and has been removed as of the London release.
Instance options

The Stock widget does not include instance options.

Ticket Attachments widget
Use the attachment widget to attach items to tickets.

Attachments should be less than 24MB. You can drag files into the Attachments widget to add them to a record.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record ID</td>
<td>The ID number of the record for the attachment.</td>
</tr>
<tr>
<td>Record table</td>
<td>Limit the records users can add an attachment to by adding a table to the attachment widget. Users can then only add attachments if they are in a record for that table.</td>
</tr>
</tbody>
</table>

Ticket Conversations widget
Record of ticket items. Users can use this to communicate back and forth with the fulfiller and the receiver.

The Ticket Conversations widget displays journal entries from the activity formatter of the target record. Journal entries are presented in chronological order, with the oldest entries appearing at the bottom of the widget. Entries made by the user that created the record appear on the right side of the center divider. Entries made by other users appear to the left.

The Ticket Conversations widget is intended only for tables that extend task.

Limit the number of journal entries that appears in the ticket conversation widget using the glide.service_portal.stream_entry_limit system property. The default number is 100. Change the number by navigating to Service Portal > Properties, and enter the new number in the Maximum number of stream entries displayed in Service Portal field.
Ticket Conversations widget

Instance options

Instance options fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use dynamic placeholder</td>
<td>Use a placeholder for journal fields. The default value is false.</td>
</tr>
<tr>
<td>No readable journal field message</td>
<td>The message that displays when there are no readable journal fields. Forms that have added journal fields may not display in the Ticket Conversation widget.</td>
</tr>
</tbody>
</table>
Ticket Location widget
Share your location in a ticket.

Instance options
The Ticket Location widget does not include any instance options.

User Profile widget
Store user profile information.
Users can use the User Preferences section to enable accessibility in a portal.

System Administrator
System Administrator at Empty

Department  Finance
Location  San Diego
Bio  Empty

User Profile widget

Instance options

The User Profile widget does not include instance options.

Weather widget
The Weather widget shows an example of how the server script interprets data from a source outside of the system.
The Weather widget does not include instance options.

Search widgets

Several search widgets are provided with Service Portal.

You can configure search in Service Portal using any of the search widgets.

Contextual Search widget
Contextual Search is an embedded widget that can be added to a record producer.

By default, the widget is included in the Create Incident record producer form to display items based on keywords entered in the description. These items can be knowledge articles, service catalog items, and social Q&A records. These search results appear as the user types the information.
Please describe your issue below

The more information you can provide here, the easier time the support organization will have in diagnosing and resolving your incident.

Search Results

Deleted Email Recovery
IT | Email > Outlook > Outlook 2010
Deleted Email Recovery By default, every email deleted from your OWA mailbox goes through the following process. The email is moved to your Deleted Items folder. If you purge or remove items from. The Dumpster only holds email message for 14 days once they’ve been removed from Deleted Items. Deleted...
Author: Ron Kettering • 0 views • ⭐⭐⭐⭐⭐

What Is Spam?
IT | Email
receives some spam, email addresses posted to web sites or in newsgroups and chat rooms attract the most spam.' Definitions The term "spam" is Internet slang that refers to unsolicited commercial email (UCE) or unsolicited bulk email (UBE). Some people refer to this kind of communication as junk email...
Author: Ron Kettering • 0 views • ⭐⭐⭐⭐⭐

Contextual Search widget

Typeahead Search widget
Predictive search feature that shows words as users type.
### Instance option fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>The name or words that appear in the search field before a user starts typing. For example, search or what are you looking for</td>
</tr>
<tr>
<td>Color</td>
<td>Whether the search button beside the search field is filled in or not</td>
</tr>
<tr>
<td>Glyph</td>
<td>The icon that appears in the search field beside the widget. The search icon is the default. To use a different icon, type the name of the icon in the field, for example search-plus. For a list of icons to choose from, open the instance options for the Icon Link widget.</td>
</tr>
<tr>
<td>Size</td>
<td>Determines the font size and height of the widget. Choose from xs, sm, md, and lg.</td>
</tr>
<tr>
<td>Limit</td>
<td>The number of typeahead search entries you want to display. The default number is 15.</td>
</tr>
<tr>
<td>Contextual Search Sources</td>
<td>Limit the results available in the typeahead search by only configuring specific search sources. For example, users searching in the Service Catalog only see results for the Service Catalog when that search sources is configure. For more information on contextual search, see Configure contextual search</td>
</tr>
</tbody>
</table>

### Home Page Search widget

Add a search bar to your homepage.

Configure your own search sources to constrain what topics appear on search, or just use the default search sources. For more information on configuring search, see Search sources.
## Home Page Search widget

### Instance options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Name that appears above the search bar. For example “How can we help?”</td>
</tr>
<tr>
<td>Short description</td>
<td>A subtitle that appears below the title.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Typeahead search</td>
<td>Controls the appearance of the search bar. Use a comma separated list inside curly braces to add style details to the search bar, for example <code>{title: 'Search', color: 'blue', size: 'lg'}</code>. For more information on which style options you can add, see the instance options for the <a href="#">Typeahead Search widget</a>.</td>
</tr>
</tbody>
</table>

**Search Page widget**

The Search Page widget displays search results.

<table>
<thead>
<tr>
<th>Search results for 'email'</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deleted</strong> Email Recovery</td>
</tr>
<tr>
<td>Deleted Email Recovery By default, every email deleted from your OWA mailbox goes through the following process: The email is moved to your Deleted Items folder. If you purge or remove items from your account, they are deleted.</td>
</tr>
<tr>
<td>Article: KB0000030 · Published: 3y ago</td>
</tr>
<tr>
<td><strong>What is Spam?</strong></td>
</tr>
<tr>
<td>What is Spam? Spam has increasingly become a problem on the Internet. While every Internet user receives some spam, email addresses posted to web sites or in newsgroups and chat rooms attract the most spam.</td>
</tr>
<tr>
<td>Article: KB0000029 · Published: 3y ago</td>
</tr>
<tr>
<td><strong>How to Deal with Spam</strong></td>
</tr>
<tr>
<td>How to Deal with Spam Spam has increasingly become a problem on the Internet. While every Internet user receives some spam, email addresses posted to web sites or in newsgroups and chat rooms attract the most spam.</td>
</tr>
<tr>
<td>Article: KB0000011 · Published: 3y ago</td>
</tr>
<tr>
<td><strong>What are phishing scams and how can I avoid them?</strong></td>
</tr>
<tr>
<td>Phishing explained Phishing is defined as the process of tricking people into giving up sensitive information. Phishing scams are typically fraudulent emails appearing to come from legitimate enterprises (e.g., your company, your Internet service provider, your bank).</td>
</tr>
<tr>
<td>Article: KB0000028 · Published: 3y ago</td>
</tr>
</tbody>
</table>
Search page instance options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show score</td>
<td>When selected, shows search results relative to ranking</td>
</tr>
<tr>
<td>Max results for All search</td>
<td>The maximum number of results that show for all of the search groups when viewed together</td>
</tr>
<tr>
<td>Max results for single search group</td>
<td>The maximum number of results that show for a single search group</td>
</tr>
</tbody>
</table>

For more information on configuring search, see [Search sources](#).

Knowledge Management widgets

Use Knowledge Management widgets to build a knowledge base for your portal.

Knowledge Management widgets are included as part of the Service Portal - knowledge base plugin (com.glide.service-portal.knowledge-base), which is activated automatically with the Service Portal for Enterprise Service Management (com.glide.service-portal.esm) plugin.

For more information on knowledge management, see [Knowledge Management](#).

KB also in Category widget

List of articles also included within a particular category.

The information that appears in the KB also in Category widget is determined by the knowledge article child categories. For more information, see [Define a knowledge article category](#).

Also in Windows

What is the Windows key?

How to set or change your default web browser

How can I restore my computer to a previous configuration?

KB also in Category widget
Instance options

Instance Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bootstrap color</td>
<td>Color scheme for the widget. The default colors are defined by the portal theme, but if you want the instance to have a specific color, select the option from the list.</td>
</tr>
</tbody>
</table>

KB Article Comments widget
Rating and comment option for knowledge base articles.

Ratings on articles in the KB Article Comments widget determine the article popularity in the KB top rated widget.

Add your comment

Rate this article ★ ★ ★ ★ ★  Submit

KB Article Comments widget

Instance Options

Instance options fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show star rating</td>
<td>Select the option to show a star rating on the KB article comments widget. Selecting the use system properties option shows the star rating option based on the glide.knowman.show_star_rating system property.</td>
</tr>
<tr>
<td>Show user comments</td>
<td>Select the option to show the comment box on the KB article comments widget. Selecting the use system properties option shows the comment box based on the glide.knowman.show_user_feedback system property.</td>
</tr>
</tbody>
</table>

KB Article Page widget
Use the Article page widget to view Knowledge Base articles within Service Portal.

Any specialized font or formatting added in the text field for the knowledge article within the platform, appears the same way in the portal.
Getting Around in Windows

Windows 8.x

Windows 8.x is designed for using touch, mouse, and keyboard together, on hardware ranging from touch-enabled tablets and laptops to PCs and all-in-one computers, including those without touch capability.

Start screen and Desktop

- 8.1: Microsoft updated the Windows 8.1 interface by returning the Start button, providing its ease of access along with the option of the Metro interface. The intent is to provide a seamless experience on desktops, laptops, tablets, and phone devices. By default, the Start screen is displayed. Move your mouse pointer to the bottom left corner of the screen to make the Start button appear. Click it to display the desktop; click it again to display the Start screen.

- 8: The Start screen has a default application display you can customize:

  1. Right-click any app and the Application bar will appear at the bottom, with options for the application you have selected.
  2. To add an app to the Start screen, click Pin to Start.

If an application is already on the Start screen, you’ll see Unpin from Start instead.

Power User menu

The Power User menu displays the most commonly used applications from the Control Panel, File Explorer, and Task Manager, as well as Restart, Run, Search, and Shutdown/Update. Access it in one of the following ways:

- Press Win + X
### Instance Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bootstrap color</td>
<td>Color scheme for the widget. The default colors are defined by the portal theme, but if you want the instance to have a specific color, select the option from the list.</td>
</tr>
<tr>
<td>Show star rating</td>
<td>Displays the star rating on the article page widget. If you select Use system properties, the appearance of the star rating is defined by the glide.knowman.show_star_rating system property.</td>
</tr>
</tbody>
</table>

**KB Categories widget**

Lists the categories for your Knowledge Base.

- **Applications**: 2
- **Devices**: 1
- **IT**: 7
- **Email**: 8
- **Suppliers**: 1
- **Operating Systems**: 12

*Categories are determined by the list of Knowledge Categories provided for the Knowledge Base. To view a list of categories for a knowledge base, in the platform navigate to Knowledge > Administration > Knowledge bases, then select the name of the knowledge base, for example IT. Categories for the knowledge base appear in the related lists. If a category does not have any associated articles, it does not appear in the portal. For more information on defining categories for a knowledge base, see Define a knowledge article category.*

The knowledge base a portal uses is determined in the portal form. On the Service Portal configuration page (Service Portal > Service Portal configuration) click Portals in the header menu. Select a portal from the list, then in the knowledge base list, select a knowledge base.
Instance options

The KB categories widget does not include instance options.

**KB Category Page widget**
Articles and article preview within a particular category. Categories are specified within the Knowledge Base module.
Applications

Excel Functionality

Excel Functionality Copying formulas without changing cell locations When you want to know how to copy a formula and keep portions of the formula from changing relative to where they are being copied, precede each portion of the cell specifications that aren't supposed to  
👤 Authored by Boris Catino • 2y ago

Managing Settings in Internet Explorer 10 for Windows 8

Summary Learn to set up a home page, connection settings, and parental control in Internet Explorer. Solution Want to set up a default home page? Want to set up your Internet connection? Need to block the types of sites that display on your computer? Learn how to do all this in  
👤 Authored by Wayne Webb • 5d ago

KB Category Page widget

Instance options

Instance options fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bootstrap color</td>
<td>Color scheme for the widget. The default colors are defined by the portal theme, but if you want the instance to have a specific color, select the option from the list.</td>
</tr>
<tr>
<td>Show star rating</td>
<td>Displays the star rating on the category page. If you select Use system properties, the appearance of the star rating is defined by the glide.knowman.show_star_rating system property.</td>
</tr>
</tbody>
</table>

KB Most Viewed widget

List of most viewed knowledge base articles, based on user feedback.
KB Most Viewed widget

Instance options

Instance options fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>The name that appears in the widget header</td>
</tr>
<tr>
<td>Bootstrap color</td>
<td>Color scheme for the widget. The default colors are defined by the portal theme, but if you want the instance to have a specific color, select the option from the list.</td>
</tr>
<tr>
<td>Max number</td>
<td>The maximum number of most viewed articles listed</td>
</tr>
<tr>
<td>KB category</td>
<td>KB category for the most viewed articles. The list is generated by the kb_category table.</td>
</tr>
</tbody>
</table>

KB News widget

The KB News widget displays information from the Knowledge Base.

You can configure the KB News widget to display specific information by selecting a category from the KB category list.
KB News widget

Instance options

Instance option fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Name of the widget that appears in the widget header</td>
</tr>
<tr>
<td>Bootstrap color</td>
<td>Color scheme for the widget. The default colors are defined by the portal theme, but if you want the instance to have a specific color, select the option from the list.</td>
</tr>
<tr>
<td>Max number</td>
<td>The maximum number of news articles appearing in the widget. The default number is 5.</td>
</tr>
<tr>
<td>KB category</td>
<td>The knowledge base category determined by the kb_category table. Only published articles display. For a news widget, select something like Announcements to show upcoming events.</td>
</tr>
</tbody>
</table>

KB Search widget
The KB Search widget is a search widget that is specifically confined to the knowledge base as a search source.
The typeahead search widget is embedded in the KB search widget.
KB Search widget

Instance options

Instance option fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Name of the widget. This field is non-public facing.</td>
</tr>
</tbody>
</table>

KB Top Rated widget
Lists Knowledge Base articles with the highest rating. Ratings are determined by user feedback.
KB Top Rated widget

*Eclipse configuration for Java development*

The KB View widget is an example of how to structure a knowledge base page. Use the search filter to find a specific topic or article.
<table>
<thead>
<tr>
<th>IT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Filter...</strong></td>
</tr>
</tbody>
</table>

- **Excel**
- **Excel Functionality**
- **IE**
- **Managing Settings in Internet Explorer 10 for Windows 8**
- **Apple**
- **How to configure VPN for Apple Devices**
- **Email**
- **How to Deal with Spam**
- **What are phishing scams and how can I avoid them?**
- **What is Spam?**
- **Outlook 2010**
- **Automatic Replies (Out Of Office)**
- **Create An Email Signature**
- **Create And Edit A Contact Group**
- **Deleted Email Recovery**
- **Importing Address Book From CSV File**
- **Android**

**Instance options**

The KB view widget does not have any included instance options.
**KB View 2 widget**

The KB View 2 provides an alternative structure to the KB View widget to show a different example of how to display knowledge articles.

### Instance options

The KB View 2 widget does not have any included instance options.

**My Favorite Tags widget**

The My Favorite Tags widget allows you to filter questions based on tags. By saving favorite tags, you only see questions that conform to that filter.
My Favorite Tags widget

Instance options

The My Favorite Tags widget does not have any included instance options.

Popular Questions widget
List of popular questions asked in the community.
### Popular Questions

<table>
<thead>
<tr>
<th>Question</th>
<th>Author</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>What’s the best way to find meeting rooms in the office?</td>
<td>Joe Employee</td>
<td>4mo ago</td>
</tr>
<tr>
<td>What is the process for getting company approved banners and images?</td>
<td>Abel Tuter</td>
<td>4mo ago</td>
</tr>
<tr>
<td>What are the pros and cons between OSX and Windows machines?</td>
<td>Joe Employee</td>
<td>4mo ago</td>
</tr>
<tr>
<td>How do you install the wireless printer on OSX?</td>
<td>Adela Cervantsz</td>
<td>4mo ago</td>
</tr>
<tr>
<td>Where is tipping expected? Is that a business expense?</td>
<td>Beth Anglin</td>
<td>4mo ago</td>
</tr>
</tbody>
</table>

**First 5 of 15 shown**

### Instance options

The Popular Questions widget does not have any included instance options.

**SQANDA Create Question widget**

Type your own question. Add a tag for better searchability.
Social Q&A Create Question widget

Instance options

The SQANDA Create Question widget does not have any included instance options.

SQANDA Question widget
Use the Social Q&A question widget to view and respond to questions.
Has anyone tried ordering accessories that are not listed on the catalog?

I want to order an ergonomic mouse but everything in the company catalog is pretty basic. Can I just order one online and expense it if it's the same price?

4mo ago • Asked by Abel Tutor

1 Answer

You can always consult with your manager and they may be already on the approved list of accessories. You can also submit a request and we'll let you know if you should order it and expense it.

4mo ago • Answered by System Administrator

Your Answer

Paragraph

Post Your Answer
Instance options

The SQANDA Question widget does not have any included instance options.

SQANDA Related Question widget
Lists stats about a question as well as recently asked questions.
The SQANDA Related Questions widget does not have any included instance options.
Subscribed Questions widget
The Subscribed Questions widget allows you to see questions you have subscribed to.
You can subscribe to questions other people have asked by selecting the star icon underneath the question.

Instance options
Instance options fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bootstrap color</td>
<td>Color scheme for the widget. The default colors are defined by the portal theme, but if you want the instance to have a specific color, select the option from the list.</td>
</tr>
</tbody>
</table>

Tagged Question List widget
List of questions sortable by tag, time it was asked, top rated, and unanswered.
The Tagged Questions List widget generates the list based on tags that users have applied to questions.
## Newest Questions

<table>
<thead>
<tr>
<th>Rank</th>
<th>Votes</th>
<th>Answers</th>
<th>Question</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>office</td>
<td>What's the best way to find meeting rooms in the office?</td>
<td>4mo ago</td>
<td>Joe Employee</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>meeting</td>
<td>How are the conference rooms named in the headquarters office? Is there an easy way to find which floor and side of the office a room is located?</td>
<td>4mo ago</td>
<td>Joe Employee</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>windows</td>
<td>What are the pros and cons between OSX and Windows machines?</td>
<td>4mo ago</td>
<td>Joe Employee</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>expenses</td>
<td>Any suggestions on using the company credit card?</td>
<td>4mo ago</td>
<td>Joe Employee</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>company card</td>
<td>I just received my company credit card in mail. Before I start expensing work related purchases, I want to know about what can be considered a &quot;company expense&quot;.</td>
<td>4mo ago</td>
<td>Joe Employee</td>
</tr>
</tbody>
</table>

**Tagged Question List widget**
Instance options

The SQANDA Tagged Question List widget does not have any included instance options.

Service Catalog widgets

Use the Service Catalog widgets to build a catalog for your portal.

The service catalog widgets are part of the Service Portal Service Catalog (com.glide.service-portal.service-catalog) plugin, which is activated automatically with the Service Portal for Enterprise Service Management (com.glide.service-portal.esm) plugin.

Most of the configuration for the Service Catalog widgets takes place in the Service Catalog application of the platform. For more information on Service Catalog, see Service Catalog.

SP Variable Editor widget

The Variable Editor widget allows you to change the specifications you chose for an item in the Service Catalog.

You can embed the variable editor widget in the shopping cart widget, to allow users to edit and make changes to their cart items. The options included in the widget are determined by the specific catalog item and the variables that have been configured for it.

For more information on the service catalog variables that are available in Service Portal, see Types of service catalog variables.
### Variables

**Allocated carrier**
- Sprint Nextel

**Monthly data allowance**
- 500MB [$1 Monthly]

**Contract duration**
- 12 Months

**Color**
- Black

**Storage**
- 64GB

---

### Instance Options

The Variable Editor widget is embedded as part of the shopping cart widget, therefore no instance options are included.

### Catalog Content widget

The Catalog Content widget is part of the Service Catalog and includes a tiled list of all the content items available in the catalog.
The items that appear on the page are grouped by category alphabetically. Catalog items and categories are defined in the Service Catalog application in the platform. For more information on creating catalog items to appear in the catalog, see [Create or edit a catalog item](#).

### Catalog Content widget

<table>
<thead>
<tr>
<th>Can We Help You?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ask a Question</strong></td>
</tr>
<tr>
<td>Get an answer</td>
</tr>
<tr>
<td><strong>Change Password</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Create Incident</strong></td>
</tr>
<tr>
<td>Create an incident record to report and</td>
</tr>
<tr>
<td>request assistance with an issue you are</td>
</tr>
<tr>
<td>having</td>
</tr>
<tr>
<td><strong>Emergency Change</strong></td>
</tr>
<tr>
<td>Open an Emergency Change</td>
</tr>
<tr>
<td><strong>International Plan Request</strong></td>
</tr>
<tr>
<td>International Plan Request</td>
</tr>
<tr>
<td><strong>New Hire</strong></td>
</tr>
<tr>
<td>New Hire Order Guide</td>
</tr>
<tr>
<td><strong>Password Reset</strong></td>
</tr>
<tr>
<td>Request a reset of a password for a service or an application.</td>
</tr>
<tr>
<td><strong>Password Reset Enrollment</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Report an Issue</strong></td>
</tr>
<tr>
<td>Simple form with Subject and Description</td>
</tr>
<tr>
<td><strong>Report Outage</strong></td>
</tr>
<tr>
<td>Report an outage of a service or an application.</td>
</tr>
<tr>
<td><strong>Report Performance Problem</strong></td>
</tr>
<tr>
<td>Request assistance with a performance issue you are having with a service or an application.</td>
</tr>
<tr>
<td><strong>Request Knowledge Base</strong></td>
</tr>
<tr>
<td>Request for a Knowledge Base</td>
</tr>
</tbody>
</table>

### Instance Options

The Catalog Content widget does not include instance options.

**Request Fields widget**

The Request Fields widget display information about any request a user has made.

Fields for the Request Fields widget are defined by the HTML template and the server.
Request Fields widget

### Instance options

#### Request fields widget instance options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pickup message</td>
<td>Information that appears at the bottom of the widget. Make sure any changes you make are within the curly braces. The default is ( \text{${Requests are picked up within &lt;br/}&gt; 4 hours (M-F 9-5)} ).</td>
</tr>
</tbody>
</table>

Requested Items widget

Describes at what stage of the order a requested item is.

You can define different workflows for items directly within the Service Catalog module. For more information on Service Catalog workflows, see Service Catalog request fulfillment.
Requested Items widget

Instance options

Requested Items instance options fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Name of the widget. The title appears in the header of the widget.</td>
</tr>
<tr>
<td>Bootstrap color</td>
<td>Color scheme for the widget. The default colors are defined by the portal theme, but if you want the instance to have a specific color, select the option from the list.</td>
</tr>
<tr>
<td>Display field</td>
<td>Determine what information displays as the title for each requested item. Short description is the default.</td>
</tr>
<tr>
<td>Filter</td>
<td>Limit what appears in the list using a filter. You can add a filter by opening the Requested Items record in the platform (From the context menu, click Open in platform) and using the condition builder.</td>
</tr>
<tr>
<td>Table</td>
<td>Table that displays the item when the user clicks an entry</td>
</tr>
<tr>
<td>Link to this page</td>
<td>Page that opens when the user clicks an item</td>
</tr>
<tr>
<td>Maximum entries</td>
<td>Max number of entries that appear in the list of requested items</td>
</tr>
</tbody>
</table>

SC Catalog Item widget
Describe catalog items and add options for users to select from.
Configure catalog items using the Service Catalog in the platform UI by navigating to Service Catalog > Catalog Definitions > Maintain items. Catalog items must have Availability set to Desktop or Desktop and Mobile.

Any specialized font or formatting added in the description field for the catalog item within the platform, appears the same way in the portal.

Catalog variables determine what information your users are allowed to pick from, for example, color, size, or price. For more information on defining the variables in the catalog item, see Create a service catalog variable.

Determine whether users can add this item to the shopping cart by selecting the Show Add Cart button check box in the widget instance options.
iPhone 6

iPhone 6s offers a multitude of features packaged within cutting edge design.

This phone will be part of the corporate mobile contract, and you will not be billed for its use. The device has the following technical specifications:

- iOS 9
- Retina display
- A9 chip
- Touch ID

What color would you like?

Black

How many gigs of storage?

16

Price: $450

Recurring Price: $50 Monthly

Submit

Add attachments
### Instance options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bootstrap color</td>
<td>Color of the widget based on the selections made in the Branding Editor.</td>
</tr>
<tr>
<td>Show Add Cart button</td>
<td>Includes the option to add the item to the shopping cart. If this check box is cleared the Add to Card button does not appear on the form.</td>
</tr>
<tr>
<td>Custom URL format</td>
<td>Enter a web page for the page to redirect to upon successful completion of an order.</td>
</tr>
<tr>
<td></td>
<td>• Enter a custom portal URL, that is relative to the root. For example, if you enter sp?id=sc_home, the page redirects to &lt;instance_name&gt;.servicenow.com/sp?id=sc_home.</td>
</tr>
<tr>
<td></td>
<td>• Append a custom portal URL such as sp?id=sc_home.</td>
</tr>
<tr>
<td></td>
<td>• You can also include a full web address such as <a href="https://google.com">https://google.com</a>.</td>
</tr>
<tr>
<td></td>
<td>• If the Auto Redirect on Successful Order is selected, the page redirects to the URL listed.</td>
</tr>
<tr>
<td></td>
<td>• If the option is cleared, clicking the click here to view in the confirmation banner redirects to that URL.</td>
</tr>
<tr>
<td></td>
<td>• Custom URL takes precedence over Page and Table selection</td>
</tr>
<tr>
<td>Successful Order Page</td>
<td>Select a page in the portal to redirect to after a successful order completion. If Auto Redirect on Successful Order is selected, the page redirects to the URL listed. If the option is cleared, clicking the click here to view in the confirmation banner redirects to that page.</td>
</tr>
<tr>
<td>Successful Order Table</td>
<td>Select a specific table on a page to direct a user to after the order is completed. The page ID and the table name are coupled to form a URL. If you set the page ID to Requests and the table name to Requested Item, the page opens with a URL similar to &lt;instance_name&gt;.servicenow.com/sp/?id=requests&amp;table=sc_req_item.</td>
</tr>
<tr>
<td>Auto Redirect on Successful Order</td>
<td>Select this option to redirect users to a new page automatically. If this option is not selected, the user stays on the catalog item page after submitting.</td>
</tr>
</tbody>
</table>

**SC Categories widget**

The SC Categories widget displays Service Catalog categories.

The system renders the categories available in this widget from the Categories table in Service Catalog (sc_category).
### Instance options

#### Categories widget instance options fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bootstrap color</td>
<td>Color scheme for the widget. The default colors are defined by the portal theme, but if you want the instance to have a specific color, select the option from the list.</td>
</tr>
<tr>
<td>Hide at XS</td>
<td>Hides the categories option on small screens, for example, on smartphones. The default is set to false.</td>
</tr>
<tr>
<td>Omit badges</td>
<td>Show or hide the number of items included in each category</td>
</tr>
<tr>
<td>Check canView per item</td>
<td>Verifies with each item that the user has the right roles to view the catalog item.</td>
</tr>
<tr>
<td>Category Layout</td>
<td>Select a flat or nested layout. A flat layout shows all of the available categories. A nested layout shows only the parent categories. Use a nested layout if you have a large number of categories to prevent an unnecessarily long list. Click to folder icon ( ) that appears next to a category with nested topics to expand the sub-categories. The widget only supports three levels of nesting. After level four, categories appear in the flat view.</td>
</tr>
<tr>
<td>Page</td>
<td>Defines what page opens when a user clicks a category. By default, this option redirects to the page for the selected category.</td>
</tr>
</tbody>
</table>
**Note:** If a category contains more than 200 items, update the following instance options on this widget for better performance:

- Category Layout: Flat
- Omit badges: True

---

**SC Category Page widget**

Lists the catalog items available within a certain category. Categories are determined within the Service Catalog module.

**Note:**

- Order Guides do not display when viewed in a browser on a mobile device.
- Catalog items are sorted in ascending order by their **Order** value. If catalog items have the same order, they are sorted by the **Name** field.

---

<table>
<thead>
<tr>
<th>Laptops</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sales Laptop</strong></td>
<td>Acer Aspire NX</td>
<td><strong>Apple MacBook Pro 15”</strong></td>
<td>Apple MacBook Pro</td>
</tr>
<tr>
<td>View Details</td>
<td>$1,100.00</td>
<td>View Details</td>
<td>$1,099.99</td>
</tr>
<tr>
<td><strong>Development Laptop (PC)</strong></td>
<td>Dell XPS 13</td>
<td><strong>Notebook Computer Loaner</strong></td>
<td>Loaner Laptop</td>
</tr>
<tr>
<td>View Details</td>
<td>$1,100.00</td>
<td>View Details</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.
Instance options

Category page widget instance options fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click event name</td>
<td>The name of the event that is emitted when a user clicks a catalog item. You can override the default behavior when clicking on a catalog item by providing a different event name. This would be in a situation where you embedded the category page in another widget. The default value is $sp.cat_item_list.click.</td>
</tr>
</tbody>
</table>

SC Order Guide widget

Standardized order guide for the catalog items. This widget compiles several commonly ordered items into an order guide for a specific purpose, for example, new hires.

New Hire

Service Overview:
The New Hire package includes all necessary tasks to enable your new employee to be productive on day one such as, hardware provisioning, software access, and account creation. Unless otherwise noted all new employees receive the standard package detailed below.

Services Include:
- Email account creation
- Lenovo Carbon x1
- One external monitor
- MS Office Suite:
  - Outlook
  - Word

SC Order Guide widget

© 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.
Instance Options

Order Guide instance options fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bootstrap color</td>
<td>Color scheme for the widget. The default colors are defined by the portal theme, but if you want the instance to have a specific color, select the option from the list.</td>
</tr>
<tr>
<td>Title</td>
<td>The name of the order guide.</td>
</tr>
</tbody>
</table>

SC Popular Items widget
List of service catalog items that users purchase often.

Popular Items

<table>
<thead>
<tr>
<th>Apple iPad 3</th>
<th>Executive Desktop</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Apple iPad 3" /></td>
<td><img src="image" alt="Dell Precision 690" /></td>
</tr>
<tr>
<td>View Details</td>
<td>View Details</td>
</tr>
<tr>
<td>$600.00</td>
<td>$1,875.00</td>
</tr>
</tbody>
</table>

SC Popular Items widget

Instance Options

Popular Item widget instance option fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limit</td>
<td>Maximum number of popular items shown. The default number is 9.</td>
</tr>
<tr>
<td>Include Record Producers</td>
<td>Includes requests made through record producers.</td>
</tr>
</tbody>
</table>

SC Save Bundles widget
The Save Bundles widget allows you to save specific catalog items together for reuse.

The Save Bundles widget is embedded within the SC Shopping Cart widget.
Create New Bundle

Here, you can save the current contents of your cart as a bundle, which can be restored at any time. To create a new bundle, provide a name for your bundle, select the items you would like to include in the bundle, and press save.

Bundle Name

<table>
<thead>
<tr>
<th>Item Description</th>
<th>Price</th>
<th>Quantity</th>
<th>Total Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple iPhone 5</td>
<td>$599.99</td>
<td>1</td>
<td>$599.99</td>
</tr>
<tr>
<td>Logitech USB Headset for PC &amp; Mac</td>
<td>$29.99</td>
<td>1</td>
<td>$29.99</td>
</tr>
<tr>
<td>Sales Laptop</td>
<td>$1,100.00</td>
<td>1</td>
<td>$1,100.00</td>
</tr>
</tbody>
</table>

SC Save Bundles widget

Instance Options

The Save Bundles widget does not have any included instance options.

SC Saved Carts widget

The Saved Carts widget shows previously created and saved bundles from the Service Catalog.
SC Saved Cart widget

When you add an existing cart bundle to a shopping cart, you have two options. You can:

- Replace the items in the shopping cart with the items in the bundle.
- Add the bundle in addition to the rest of the items in the cart.

### Add bundle items to a cart

<table>
<thead>
<tr>
<th>Items In Bundle</th>
<th>$</th>
<th>1</th>
<th>$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Nexus 7</td>
<td>$199.99</td>
<td>1</td>
<td>$199.99</td>
</tr>
<tr>
<td>Apple iPad 3</td>
<td>$600.00</td>
<td>1</td>
<td>$600.00</td>
</tr>
</tbody>
</table>

**Replace Cart** will remove the current contents of your cart and replace it with the bundle.

**Add to Cart** will add the contents of the bundle into your cart without removing its current contents.
**Instance Options**

The Saved Carts widget does not have any included instance options.

*SC Shopping Cart widget*

The shopping cart widget, used in combination with Service Catalog, stores all of your orders in one place.
Shopping cart widget

With the shopping cart widget, you can:

- Control the quantity of items going into the cart.
- Add items to a cart. This information gets stored in the sc_cart table.
- Define who the items are being requested for.
- Save specific items together as a bundle, which can be reloaded at a later time.
• Use the **Clear Cart** option to remove all the items from your cart.

If you want to add a bundle to your cart from the saved cart, you have the option of replacing all of the existing cart items with the bundle items, or including the bundle items with the cart items. The shopping cart respects most *Service Catalog properties*.

### Instance options

**Shopping cart instance options fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bootstrap color</td>
<td>Color scheme for the widget. The default colors are defined by the portal theme, but if you want the instance to have a specific color, select the option from the list.</td>
</tr>
<tr>
<td>Cart template</td>
<td>Enter the name of an ng-template you want to use to provide a different template for the shopping cart. By default, two ng-templates are provided: <code>small_shopping_cart.html</code> and <code>large_shopping_cart.html</code>.</td>
</tr>
</tbody>
</table>

**Enable the Shopping Cart widget**

The shopping cart widget is enabled automatically for instances upgrading to Istanbul, however, there are several ways to manually enable or disable the widget.

To enable the shopping cart for a catalog item:

1. Navigate to a catalog item on the Service Catalog page in Service Portal.
2. CTRL+right-click a catalog item widget to open the **widget instance options**.
3. Select or clear the **Show Add Cart Button** option to enable or disable the shopping cart for that particular catalog item.
Catalog item cart option

To enable the shopping cart in the portal header:
1. From the Service Portal configuration page, select the Portal editor.
2. Select the SP Header Menu in the portal hierarchy.
3. In the **Additional options** section, make sure the enable cart value is set to **true**.

```json
{
   "enable_cart": {
      "displayValue": "true",
      "value": true
   }
}
```
Set the value to \textbf{false} to hide the shopping cart.
Shopping cart in the header menu

```json
{
    "enable_cart": true,
    "displayValue": "true",
    "value": true
}
```
Service Portal configuration page widgets

Service Portal uses widgets for configuration. When you configure a page or a widget for a portal in the Service Portal Configuration page, you actually use Service Portal widgets to do so.

Service Portal configuration widgets are internal only and cannot be extended.

Configuration page widgets are included as part of the Service Portal Configuration Pages plugin (com.glide.service-portal.config), which is activated automatically when you activate the Service Portal for Enterprise Service Management plugin (com.glide.service-portal.esm).

Navigate to **Service Portal > Service Portal Configuration** to view these widgets in action.

*Service Portal Config Overview widget*

The Service Portal Config Overview widget is the widget that appears on the sp_config homepage. Use this widget to navigate Service Portal Configuration.
Service Portal
Create rich, engaging and modern experiences to help your business run better
Select one of the options below to continue

Branding Editor
Customize your portal's title, logo and theme colors. Preview changes as you make them

Designer
Create and layout pages with drag-and-drop functionality. Preview pages as you make changes

Page Editor
Configure the properties of pages, containers and widgets from a map view

Widget Editor
Create widgets from scratch or customize an existing one. Write HTML, CSS, and Javascript with real-time preview

Get Help
Browse guides, tutorials and videos to learn how to set up, configure and customize your portals
Portal config widget

The Portal Config widget is the left panel of the Branding Editor, which you use to configure themes for your portal.
Title and Logo

Portal title

Service Portal

Logo

![ServiceNow Logo](image-url)

Upload an image  Delete

Logo Padding

Left: [Sliding Bar]

Top: [Sliding Bar]

Use title and logo to represent your brand across all pages of a portal

Tag Line and Background

© 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.
**SP Page Map widget**
The Page Map widget works in the Page Editor to display any Service Portal page in a tree structure.

**SP Portal Map widget**
The Portal Map widget displays your portal in a tree structure.

**Theme Preview widget**
The Theme Preview widget appears in the Branding Editor and allows you to see any theme changes you make to your portal.
Theme Preview

Navbar

Title

Brand

Default  Primary  Success  Info  Warning  Danger  Link

Text Primary - Nullam id dolor id nibh ultricies vehicula ut id elit.
Text Success - Duis mollis, est non commodo luctus, nisi erat porttitor ligula.
Text Info - Maecenas sed diam eget risus varius blandit sit amet non magna.
Text Warning - Etiam porta sem malesuada magna mollis euismod.
Text Danger - Donec ullamcorper nulla non metus auctor fringilla.
**Widget Edit Panel widget**

The Widget Edit Panel appears on the main page of the Widget Editor in Service Portal Configuration.

Use the Widget Edit Panel to view widgets that have recently been updated, create a widget, or view an existing widget.

**Service Portal service status widgets**

Use the service status widgets to display current, planned, and historical outages for business services to your end users.

The service catalog widgets are part of the Service Portal Service Status (com.glide.service-portal.service-status) plugin, which is activated automatically with the Service Portal for Enterprise Service Management (com.glide.service-portal.esm) plugin.

**Business Service Status widget**

View how services are running on your system.
The Business Service Status widget pulls information from the cmdb_ci_service table. You can change where the data comes from in a cloned version of the widget by adjusting the settings in the widget server script.

<table>
<thead>
<tr>
<th>Status History</th>
<th>Jun 12</th>
<th>Jun 13</th>
<th>Jun 14</th>
<th>Jun 15</th>
<th>Jun 16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bond Trading</td>
<td>✔️</td>
<td>✔️</td>
<td>🔴</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Bond Trading - DR</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Client Services</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>E-Commerce</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Electronic Messaging</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Email</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>🔴</td>
<td>✔️</td>
</tr>
<tr>
<td>IT Services</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Outlook Web Access (OWA)</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>🔴</td>
<td>✔️</td>
</tr>
<tr>
<td>PeopleSoft Asset Lifecycle Management</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>PeopleSoft CRM</td>
<td>✔️</td>
<td>✔️</td>
<td>🔴</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>PeopleSoft Enterprise Services</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>PeopleSoft Financials</td>
<td>✔️</td>
<td>✔️</td>
<td>🔴</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

**Business Service Status widget**

**Instance options**

**Instance option fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Name of the widget. This only appears in the header for the widget instance options, it is not user-facing. To change the title for the list of services, clone and edit the widget HTML.</td>
</tr>
<tr>
<td>Glyph</td>
<td>Icon for the widget. This is not user-facing.</td>
</tr>
<tr>
<td>Number of Services</td>
<td>The number of services displayed in the widget. The default number is 250.</td>
</tr>
</tbody>
</table>
Current Status widget
The Current Status widget displays any issues reported in the system.

The Current Status widget checks the cmdb_ci_outage table to see if the system is experiencing any outages.

Current Status widget

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show outage details</td>
<td>Display details from the cmdb_ci_outage record</td>
</tr>
<tr>
<td>Standalone</td>
<td>Remove explanatory information. This also adds a link to more information.</td>
</tr>
</tbody>
</table>

Planned Maintenance widget
Describes any planned system maintenance.

The widget gathers information from the cmdb_ci_outage table. Any planned maintenance within the following five days appears in the Planned Maintenance widget.
Planned Maintenance widget

Instance options

The Planned Maintenance widget does not have any included instance options.

Service History widget
Displays the history of specific service’s status. For example, if the Bond Trading widget has a history of planned outages or degradations, the widget displays those with a varied color scheme to differentiate the outage type.
Service History widget

Instance options

The Service History widget does not include any instance options.

Service Status widget

Service Status is a visual representation of service availability. Each colored pill correlates with a type of service availability, for example, orange represents service degradation.
Service Status widget

**Instance options**

The Service Status widget does not have any included instance options.

*Service Status Legend widget*

Use concurrently with the Status History widget to show what the icons in the Status History widget mean.

```
Legend

- No issues
- Planned maintenance
- Service degradation
- Outage
- Multiple issues
```

Service Status Legend widget

**Instance options**

The Service Status Legend widget does not have any included instance options.

*Service Status Subscription widget*

Used in conjunction with the service status widget. Users subscribe to receive updates about the service status.
Instance options

The Service Status Subscription widget does not have any included instance options.

Configure widget instance options

When you add a widget to a page using the Service Portal Designer, it creates a widget instance. A widget instance is a reference to a widget that contains a location, properties, and CSS specific to that instance. Adding the same widget multiple times to the same page creates multiple instances. Each instance of the widget you configure remains unique, so you can have several instances of the same widgets on a page. For example, each instance of the cool clock widget on a page shows a different time zone. Configure a widget on a page by adjusting the instance options.

Role required: admin or sp_admin

Each time you add a widget to a page it creates a record on the sp_instance table with the following information:

- Reference to the column where the widget is located
- Reference to a widget
- Configuration for a widget in the form of pre-defined form fields and an Additional Options field in JSON format

For example, the icon link widget displays as many different versions of itself as you add to a page.
Icon link widgets

All widget instances point to a widget. If you make changes in that specific widget, all of the widget instances receive that change as well. You can also make changes specifically to a widget instance and only the widget instance will be affected.

1. On a page in the Service Portal Designer, point to the Edit icon (Edit) in a widget to open the widget instance options. You can also access widget instance options using the control + right-click menu.
2. From the Instance Options window, make the selections you want to configure your widget. Instance options vary depending on which widget you select.

Configure widget instance options

Advanced users can configure the available options for a widget. For more information, see Widget option schema.

Widget developer guide

Develop custom widgets in the Service Portal using AngularJS, Bootstrap, and the ServiceNow API.

What to know before you begin

To develop widgets, you need ServiceNow API experience to:

- Run record queries on the server.
- Create and update records.

You need AngularJS experience to:

- Bind variables to client controllers.
- Access server objects in a widget.
- Gather user input.
Parts of a widget

Like Angular directives, widgets execute a specified behavior within a Service Portal page. A widget includes:

**HTML template**

A mandatory widget component.

The HTML template requires knowledge of AngularJS to display and gather data. Use the HTML template to:
- Render the dynamic view that a user sees in the browser using information from the model and controller.
- Bind client script variables to your markup.
- Gather data from the end user.

**Client script**

A mandatory widget component.

A client script requires knowledge of both the ServiceNow API and AngularJS to create a client controller. Use the client script to:
- Map server data from JavaScript and JSON objects to client objects.
- Process data before rendering it.
- Pass data to the HTML template.
- Pass user input and data back to the server for processing.

**Server script**

A mandatory widget component.

A server script requires knowledge of the ServiceNow API to work with record data. Use the server script to:
- Set the initial state of the widget.
- Send record data to the widget client script using the `data` variable.
- Run server-side queries.

**Link function**

An optional widget component.

The link function requires knowledge of AngularJS. Use a link function to directly manipulate the DOM.

**Option schema**

An optional widget component.

Allows a Service Portal admin to configure a widget. Use the option schema to:
- Specify the parameters for a widget.
- Allow admin users to define instance options for a widget instance.
- Develop flexible, reusable widgets.

**Angular Providers**
An optional widget component.

Angular Providers require knowledge of AngularJS. Use Angular Providers to:
- Keep widgets in sync when changing records or filters.
- Share context between widgets.
- Maintain and persist state.
- Create reusable behaviors and UI components and inject them into multiple widgets.

Dependencies

An optional widget component.

A widget dependency is an external resource used by your widget such as JavaScript or CSS files.

Global objects in widgets

When a widget begins to render for the first time on a page, the server script executes first and accesses three global objects: input, options, and data. Because the input variable is a data object sent from the client script, this variable is undefined when first initialized.

When a widget is first instantiated, the server script:
1. Initializes an empty data object.
2. Initializes the input object with any data sent from the client controller, or the options object with any data used to initialize the widget.
3. Sends the **data** object to the client controller as JSON.

The client script:

1. Accesses the server **data** object using **c.data**.
   
   **Note:** By default, widgets use the **c** variable to represent the controller instance using `controller` as syntax. You can change this variable when creating or cloning widgets.

2. Uses `server.update()` to post changes to the data model. This method updates the server script using the **input** object.
   
   **Note:** After calling `server.update()`, the client script **data** object is automatically overwritten by the server script **data** object.

3. Uses **c.options** to access the values used to invoke the widget on the server. This object is read-only.

**Using the Widget Editor**

When you create a widget, a record is created in the `sp_widget` table. However, you can use the Widget Editor in Service Portal Configuration as your scripting environment. The Widget Editor is a full page application similar to an IDE. You can show the parts of the widget you want to edit and hide the rest, while previewing your changes in real time.
Recommendations for developing widgets

When developing custom widgets, keep these recommendations in mind for optimal performance, scalable development, and a good user experience.

Create a default state that provides an example to the end user

When initially added to a page, a widget does not have instance options defined. If a default state is not provided, a widget can appear empty and can cause confusion. Instead of creating a widget that defaults to an empty state, give your widget default data to display when no other options are defined to:

- Clearly demonstrate the widget functionality to the user.
- Provide data when previewing the widget in the widget editor.

Learn more: Tutorial: Build a custom widget.

Create a directive instead of embedding a complex widget

When an embedded widget is called from the server, all the scripts associated with that widget are returned. If you only need to embed a subsection of a widget, embedding the entire widget creates unnecessary overhead. Instead, use directives to share lightweight code between widgets. Use a directive instead of an embedded widget to:

- Share scope or custom scope behavior with multiple widgets.
- Share a reusable, lightweight subsection of a widget.
- Share a common UI feature, such as a list or an avatar.
- Augment widget behavior.

Learn more: Reuse components with Angular Providers.

Use a service or factory to share data and persist state

Data services and factories maintain and persist state in a widget without requiring multiple server calls enabling you to:

- Keep widgets in sync when changing records or filters.
- Share context between widgets.
- Develop more performant widgets.

Learn more: Reuse components with Angular Providers.

Handle events with a publish/subscribe service

Avoid using $broadcast in the DOM. $broadcast dispatches the event name to all child scopes notifying registered listeners, which can be an expensive call that requires the use of the $rootScope global object.

Instead, use a publish/subscribe service to handle events. When using a publish/subscribe service, a clear relationship forms between your widgets through callback handlers. In this model, you can better control the state of your events.

Use REST calls to fetch data from the server

When you call server.update(), the entire widget is returned from the server. If your widget includes divergent code paths, multiple calls to update the server can affect performance. As a rule, use your server script to set up the initial state of your widget. For subsequent updates, use scripted REST APIs that call script includes on your instance. This practice:

- Separates business logic from the display.
• Centralizes your code, allowing changes to be made in one place.

**Develop with localization, accessibility, and UI in mind**

To create the best experience for your users, follow these guidelines:

• Consider the impact of your widget in a mobile environment. For example, avoid using mouseover and other events that do not translate to a mobile device.
• Use **SCSS variables** to reuse items.
• Use variable names when using colors.
• Wrap strings for translation in localization APIs. See [Internationalize a widget](#).

**Remove unused Angular Providers from client script**

For easier maintenance, remove any unused Angular Providers that were injected into the client script function statement.

**Avoid using `<script>` tags in HTML templates**

To lessen the likelihood of production issues in Service Portal, avoid using inline templates using `<script>` tags in a widget’s HTML template. Instead, create a related Angular ng-template record for the widget.

**Service Portal debugging tips**

*Create a new widget*

Widgets are the power behind the portal. Widgets are customizable and can be used to provide a variety of experiences for your users. Anytime you add a widget to a page it becomes an instance of itself, which can be configured specifically for each use. Create a new widget to build a custom widget from scratch.

Role required: admin or sp_admin

You can add several Icon Link widgets to a page, configure them to link to different areas and with different icons, and none of them will be affected by the others. You can start by cloning an existing widget and making changes to your cloned version. Developers or people with an advanced understanding of AngularJS can create widgets from scratch.

1. Navigate to **Service Portal > Service Portal Configuration > Widget Editor**.
2. Click **Create a new widget**.
3. Enter a name for the new widget. The widget ID is created automatically based on the widget name. Optionally select **Create test page** to automatically create a page containing the widget.
4. Click **Submit**.

The widget HTML template, client script, and server script display in the widget editor. Basic script templates are included as a guide.

**Note:** After completing development of a widget with a test page, delete the test page. Maintaining test pages can create clutter when managing pages.
Clone a widget

Take advantage of existing code by cloning and editing an existing widget.

Role required: admin or sp_admin

Note: Base system widgets are read only so you can benefit from future updates. To make changes, you can clone base system widgets. However, cloned widgets are considered custom and do not benefit from future updates to the widgets they were cloned from.

1. Open the Widget Editor in the Service Portal Configuration page, then select an existing widget from the Select a widget list. For example, select Hello World 2.
2. From the list menu in the widget header, click Clone “Hello World 2”.

© 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. Enter a name for the cloned widget. The widget ID is created automatically based on the widget name.

4. Optional: Select **Create test page** to automatically create a page containing the widget.

5. Use the check boxes to show or hide the different components of the widget editor as needed. Make changes to the HTML Template, CSS, client script, server script, or the link function.
Hola, mundo!
6. In order to enable a preview of your widget, use **Enable Preview** from the menu. Use the eye icon that appears to show or hide a preview of your widget.

If you clone a widget that uses the Angular ng-template, you must manually clone the template and change the name of the template reference in the widget.

For example, the header menu widget uses the Angular ng-template `menuTemplate`. If you clone the header menu widget, you must also clone the `menuTemplate` and give the clone a unique name. When you open the clone of the header menu widget, you can see a reference to the `menuTemplate` in the HTML.

![menuTemplate in header widget HTML](image)

**Widget option schema**

Widget instances allow users to uniquely configure each widget they add to a page. Use the option schema to define the parameters for your widget.

**Storing instance options**

When developing a widget, you can edit the option schema to create parameters for your widget, or you can create a table to store instance options. If you edit the existing option schema, any instance options defined are stored in JSON format in the **Additional options, JSON format** field in the sp_instance table. The following field types are available:

- String
- Boolean
- Integer
- Reference
- Choice
- Field_list (depends on table)
- Field_name (depends on table)
- Glide_list

To use other field types not supported in the option schema, create an extension table to store your custom widget option schema. Using a table enables you to:

- Add any ServiceNow field type, including fields with advanced customization, to the option schema.
- Define a complex option schema.
- Search and filter instance options.
Note: While storing options in a table enables you to define more complex options, this method is more difficult to maintain than editing the option schema. To avoid creating unnecessary tables and adding additional server calls to your widget, edit the existing option schema when possible. Store options in a table only when complex or searchable options are required.

Using options in a widget

Access options in the widget from both the client script and the server script using the options global variable. You can access any option value in your widget client script or server script using options.optionName.

Client script

```javascript
function() {
    /* widget controller */
    var c = this;
    console.log(c.options.text_color) //Outputs the text_color option for this instance
}
```

Server script

```javascript
(function() {
    $sp.log(options.text_color) //Logs the value of the text_color option to the browser console.
})();
```

Define default options

Before an option value is set on an instance, it appears as an undefined value when you access that option variable. Use the widget server script to specify default values for your options.

```javascript
(function() {
    options.text_color=options.text_color||"blue";
    options.maximum_entry_count=options.maximum_entry_count||5;
})
```

Edit the widget option schema

Widget instances allow users to uniquely configure each widget they add to a page. Edit the option schema to define basic parameters for your widget.

Role required: admin or sp_admin

1. Navigate to Service Portal > Service Portal Configuration > Widget Editor.
2. Select the widget you want to configure the option schema for.
3. Click the menu icon (≡) and select Edit option schema. This option only appears for users that have the right to edit the widget.
4. Click + to add a widget option.
5. Define a label, name, type, and hint. More fields appear depending on the type you select. Adding flexible widget options allows you to create more reusable widgets. You can add default values to help users understand each widget option.
6. Click **Save**.
   The option schema you defined is stored in JSON format in the **Option schema** field in the sp_widget table. Based on this option schema, each instance of the widget can use individually defined instance options.

7. Test the option schema by adding the widget to a page in the Service Portal Designer.
   a) Navigate to **Service Portal > Service Portal Configuration > Service Portal Designer**.
   b) Add the widget to a page and click the edit icon on the widget instance to view the instance options.
   c) **Configure the widget instance options**.
d) View the configuration by navigating to the instance record in the sp_instance table. The instance options are stored in JSON format in the Additional options, JSON format field.

**Store instance options in a table**
Create a table to store widget instance options instead of editing the existing option schema. When using a table as your widget option schema, you can define custom fields using any ServiceNow field type, add filters to fields, and search or query instance options.

Role required: admin or sp_admin

To define a custom option schema, add fields to an sp_instance extension table, then set your widget to use the extension table as a data source. Using an extension table enables you to:

- Add any ServiceNow field type, including fields with advanced customization, to the option schema.
- Define complex widget options.
- Search and filter instance options.

**Note:** While storing options in a table enables you to define more complex options, this method is more difficult to maintain than editing the option schema. To avoid creating unnecessary tables and adding additional server calls to your widget, edit the existing option schema when possible. Store options in a table only when complex or searchable options are required.

1. Create a table that extends an sp_instance table to store your custom option schema.
   a) Navigate to **System Definition > Tables**.
   b) Click **New**.
   c) Define a label and name.
   d) In the Extends table field, select an sp_instance table that provides the necessary fields.

<table>
<thead>
<tr>
<th>Instance table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance (sp_instance)</td>
<td>Includes base instance fields.</td>
</tr>
<tr>
<td>Instance with Table (sp_instance_table)</td>
<td>Includes sp_instance fields and fields to display table data such as Table and Filter.</td>
</tr>
</tbody>
</table>

   e) Save the form.

2. Define custom fields in the extension table.
   You can define any field type to use in your option schema by adding new columns in the Columns list.

3. Update your widget to use the extension table as a data source.
   a) Navigate to **Service Portal > Widgets**.
   b) Open the widget you would like to create custom options for.
   c) In the Data table field, select your sp_instance extension table.
4. Configure the extension table form to display the desired fields. Fields configured on the form are available as instance options.
   a) Navigate to the extension table form: `<yourInstance>/<your_extension_table>.do`.
   b) Right-click the header menu and select **Configure > Form Layout**.
   c) Add the fields to the form.
   d) Click **Save**.

5. Configure the widget to display the desired fields as instance options.
   a) Navigate to **Service Portal > Widgets**.
   b) Open the widget that has the extension table set as the data source.
   c) Use the **Fields** slushbucket to select fields to display as instance options.
d) Save the form.

Test the option schema by adding the widget to a page in the Service Portal Designer. Click the edit icon on the widget instance to view the instance options. After configuring the widget instance options, view the configuration by navigating to the instance record in the sp_instance extension table.

Reuse components with Angular Providers

Angular Providers are reusable components that can be injected into multiple widgets. To ensure quick loading widgets and a high performing portal, create Angular Providers instead of overloading your client controllers with persistent data and additional logic. With Angular Providers, you can maintain data for the lifetime of your Service Portal and reuse components and data objects across multiple widgets.

Role required: admin or sp_admin

By creating an Angular Provider, you can:

- Keep widgets in sync when changing records or filters.
- Share context between widgets.
- Maintain and persist state.
- Create behaviors and inject them into multiple widgets.

To learn more, visit Angular Providers.

Tip: For easier maintenance and troubleshooting, remove any unused providers from the Angular Providers related list in the Widget (sp_widget) table.

   The Widget Angular Providers table opens.
2. Click New to create a new record.
3. Select the type of Angular Provider.
   - Directive
   - Factory
   - Service

To facilitate migration to ECMAScript 6 in the future, consider using services over factories.

4. Define a name.
   You will use the name to associate the Provider with your widget.

5. Add a script in the **Client Script** field.
   A basic factory that formats a number in US currency.

   ```javascript
   function formatterFactory()
   {
     var myVal = Number;
     return {
       format: function(myVal) {
         // Formatting function
       }
     }
   }
   ```
6. Associate the Angular Provider with a widget.
   a) Navigate to `<yourInstanceURL>/sp_config?id=widget_edit`.
   b) Open the widget you would like to associate with the Angular Provider.
   c) Under Related Lists, select Angular Providers.
   d) In the Angular Providers list, click New.
   e) In the Angular Provider field, select the appropriate Provider. Check the Widget field to ensure that you are associating the Angular Provider with the correct widget.

   ![New Angular Providers](image)

   f) Click Save.

7. Update the appropriate scripts in your widget to inject the Angular Provider into the widget.
Inject the factory into your widget client script by passing the name of the factory as an argument in your client controller function. You can then access the object defined in the factory function in your widget client script.

```javascript
function(formatterFactory) {
    /* widget controller */
    var c = this;
    console.log(formatterFactory.format(300));
}
```

If defining a directive, use the directive in the widget HTML template.

8. To edit the Angular Provider after it is registered with your widget, open the Angular Provider client script in the widget editor.
   a) Navigate to Service Portal Configuration > Widget Editor.
   b) Under Edit an existing widget, select the widget associated with your Angular Provider.
   c) In the Show menu, open the Dependencies list and select the Angular Provider.

   ![Dependencies](image)

   **Note:** Only Angular Providers associated with the widget are displayed in the Dependencies list. This list includes any external resources your widget depends on.

The Angular Provider client script displays in the widget editor. In the widget editor interface, you can edit and save your widget and Provider scripts at the same time.

To use an Angular Provider with multiple widgets, register your Provider with each widget and update the appropriate scripts.

**Embedded widgets**

Embed a widget in the HTML template, server script, or client script.

**Embed a widget in an HTML template**

Use the `<widget></widget>` element to embed a widget in an HTML template. Pass in the ID of the widget you are trying to embed as a parameter.

```html
<div>
    <widget id="widget-cool-clock"></widget>
</div>
```

If a widget has an option schema, you can define instance options in JSON format.

```html
<widget id="widget-cool-clock" options='{"zone": "America/Los_Angeles","title": "San Diego, CA"}'></widget>
```
Alternatively, you can define options in the widget server script.

**HTML template**

```html
<widget id="widget-cool-clock" options='data.clockOptions'></widget>
```

**Server script**

```javascript
(function() {
    data.clockOptions = {
        "zone": "America/Los_Angeles","title": "San Diego, CA"};
})();
```

### Embed a widget in a client script

Use `spUtil.get()` to get a widget model in the client script.

```javascript
spUtil.get("widget-sc-cat-item", {sys_id:
    "your_catalog_item_sys_id"}).then(function(response) {
    c.catalogItemWidget = response;
});
```

When using the `spUtil` class in a widget client script, you must inject the class into the client script function. The following example embeds the Cool Clock widget:

**Client script**

```javascript
function(spUtil) {
    var c = this;
    spUtil.get("widget-cool-clock").then(function(response) {
        c.myClockWidget = response;
    });
}
```

**HTML template**

```html
<sp-widget widget="c.myClockWidget"></sp-widget>
```

### Embed a widget in a server script

Use `$sp.getWidget()` to get a widget model in the server script.

```javascript
data.catalogItemWidget = $sp.getWidget("widget-sc-cat-item");
```

The following example embeds the Cool Clock widget:

**Server script**

```javascript
(function() {
    var coolClockOptions = {
        "zone": "America/Los_Angeles","title": "San Diego, CA"}
    data.coolClockWidget = $sp.getWidget('widget-cool-clock',
        coolClockOptions);
```
HTML template

```html
<sp-widget widget="data.coolClockWidget"></sp-widget>
```

**Widget model properties**

When a widget model is called from within another widget, the HTML template, client script, and link function are loaded just as they are in the sp_widget record. The data property is the result of the widget server script execution. Anything that you put on the data object on the server is available in the data object on the client.

<table>
<thead>
<tr>
<th>Property name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>client_script</td>
<td>string</td>
<td>Widget client script field.</td>
</tr>
<tr>
<td>css</td>
<td>string</td>
<td>Compiled CSS output from the SASS field for the widget.</td>
</tr>
<tr>
<td>data</td>
<td>object</td>
<td>Data object containing keys and values from the widget server script.</td>
</tr>
<tr>
<td>dependencies</td>
<td>array</td>
<td>Any third-party libraries to load before the widget executes.</td>
</tr>
<tr>
<td>options</td>
<td>object</td>
<td>Options used to initialize the widget.</td>
</tr>
<tr>
<td>template</td>
<td>string</td>
<td>HTML template field for the widget.</td>
</tr>
</tbody>
</table>

*Embed a widget multiple times with custom options*

Embed the cool clock widget multiple times using custom options.

**Role required:** admin or sp_admin

Create a widget that embeds multiple instances of the cool clock widget, each with a different time zone and title. Open the cool clock widget in the Widget Editor to see widget options referenced in the HTML template and the Client Script.
Cool Clock widget with Options highlighted

1. Clone the Cool Clock widget with the name Embedded clock.
2. Replace the code blocks with the following:
HTML Template

```html
<div class="panel panel-default">
  <div class="panel-heading">Time across the US</div>
  <div class="panel-body">
    <div class="row">
      <div class="col-sm-3" ng-repeat="myClock in c.data.clocks">
        <sp-widget widget="myClock"></sp-widget>
      </div>
    </div>
  </div>
</div>
```

CSS

```css
.panel {
  margin-top: 10px;
}
```

Client Script

```javascript
function() {
  // nothing to do here...
}
```

Server Script

```javascript
(function() {
  var options = [
    {zone: "America/Los_Angeles", title: "San Diego"},
    {zone: "America/Denver", title: "Denver"},
    {zone: "America/Chicago", title: "Chicago"},
    {zone: "America/New_York", title: "New York"}
  ];

  data.clocks = [];
  for (var i in options) {
    data.clocks.push($sp.getWidget("widget-cool-clock", options[i]));
  }
})();
```

Each instance of the clock in the embedded clock widget appears with a different time zone.
Create a widget dependency

In Service Portal, you can link JavaScript and CSS files to widgets to create dependencies between widgets and third-party libraries, external style sheets, and angular modules.

Role required: admin or sp_admin

Dependencies are loaded asynchronously from the server when needed.

Widgets can have as many or as few dependencies as needed. However, the more you add, the more content a widget must download to render on the page. Keep dependencies as small as possible for more efficient load times.

1. Create a dependency package.

   A dependency package is a collection of Javascript and CSS files that can be then connected to a widget.

   a) Navigate to **Service Portal > Dependencies**.

   b) In the dependency record, define the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of your dependency. (Useful for selecting a dependency from a dropdown list)</td>
</tr>
<tr>
<td>Application</td>
<td>Application scope for the dependency record.</td>
</tr>
<tr>
<td>Include on page load</td>
<td>Select if you want your dependency to be loaded onto the page on initial page load of Service Portal, or leave unchecked to load the dependency only when the linked widget is loaded onto a page.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Angular module name</td>
<td>Optional. Define the value if the linked JavaScript is an Angular module. Provide the name of the Angular module being loaded, so that it can be injected into the Service Portal Angular application.</td>
</tr>
</tbody>
</table>

2. Add files to the dependency package

After you save the information for your dependency package, use the related lists to add JS and CSS Include files. For each related list, include the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display name</td>
<td>Name of the script include.</td>
</tr>
<tr>
<td>Source</td>
<td>Depending on whether you add a JS Include or a CSS Include, select one of these options from the list:</td>
</tr>
<tr>
<td></td>
<td>• URL</td>
</tr>
<tr>
<td></td>
<td>• UI script (for a JS Include) or Style Sheet (for a CSS Include)</td>
</tr>
<tr>
<td></td>
<td>For a JS Include, use the UI Script field to reference a UI Script found in System UI &gt; UI Scripts.</td>
</tr>
<tr>
<td></td>
<td>For the CSS Include, use the Style Sheet field to reference a record in the sp_css table.</td>
</tr>
</tbody>
</table>

3. Add a dependency package to a widget

After you have created a dependency package and added files, create a relationship between the dependency and a widget.

a) Navigate to Service Portal > Widgets and find the widget record you want to add the dependency to.

b) From the Dependencies related list, click Edit.

c) In the slushbucket, find the dependency you created and double-click to add it to the selected items column on the right. Save the page to return to the widget record.

Include a font icon in a single widget

If you only want one widget to have access to a font icon, include the font icon in a single widget.

Role required: admin or sp_admin

Adding an icon to a specific widget keeps the icon scoped and prevents it from interfering with other CSS on the page.

1. In the platform UI, navigate to Service Portal > Widgets, then click the widget you want to add an icon to.
2. Attach the individual icon file to the widget record.
3. In the HTML template, include something like the following:

```html
<div>
  <i class='font-family'>icon_name</i> you did it!
</div>
```
Make sure the class is exactly the same as the font family called out in the CSS. For example
<i class='material-icons'> should be the same as the .material-icons included in the CSS. The icon_name should match the name of the file you attached.

4. In the CSS field for the widget, add the CSS for the font-icon definition. Most font-icon sets include a CSS file similar to the material icons one used below. Use the sys_id of the attachment as the src in the CSS.
<div><i class='material-icons'>ic_check_circle</i> you did it!</div>

```css
@font-face {
  font-family: 'Material Icons';
  font-style: normal;
  font-weight: 400;
  src: url('https://fonts.gstatic.com/s/materialicons/v89/materialicons.woff') format('woff');
}

.material-icons {
  font-family: 'Material Icons';
  font-weight: normal;
  font-style: normal;
  font-size: 24px; /* Preferred icon size */
  display: inline-block;
  line-height: 1;
  text-transform: none;
  letter-spacing: normal;
  word-wrap: normal;
  white-space: nowrap;
  direction: ltr;

  --webkit-font-smoothing: antialiased;
  font-feature-settings: 'liga';
}
```
An icon that you can select in the widget or widget instance.

To use custom font-icons across widgets, add the icon to a page or make it a widget dependency.

*Include font icons as a widget dependency*

You can include font icons wherever a widget is loaded by including them as a widget dependency.

**Role required:** admin or sp_admin

---

**Note:** CSS included as a widget dependency is not scoped and can disrupt other CSS on a page.

1. In the platform UI, navigate to **Service Portal > CSS** and create a new style sheet.
2. Attach the font-icon set to the sp_css record you created, and use the sys_id of the attachment as the src for the font icon.
3. Navigate to Service Portal > Dependencies and create a new dependency.
4. Attach the CSS record you created to the new dependency using the CSS Includes related list.
Internationalize a widget

Use the $() or gs.getMessage() syntax in widgets to tag strings for translation so you can localize your Service Portal content.

The $() or gs.getMessage() searches in the messages table (sys_ui_message) in the platform to see what the translation would be.
Use the HTML template to internationalize strings in a widget. Type the following in an HTML template.

```html
<div>
  <p>${This message will be internationalized.}</p>
  <p>However, this will NOT be.</p>
</div>
```

Writing text as `${message}` is the equivalent of writing `${gs.getMessage("message")}` in other parts of the system, but written as a more legible shorthand.

**Note:** In some cases, the translation might have quotes or double quotes on it. That could lead to JavaScript errors if you are using the ${} syntax in the client script. The safest way to fetch a translated message is to do it in the server script. Then, assign the value to a client-side Angular binding.

### Translating strings in the client script

```javascript
function() {
  var c =this;
  c.message="${This message will be internationalized}"
}
```

HTML template:

```html
<div>
  <!-- The output of this text will be internationalized. -->
  <p>{{c.message}}</p>
</div>
```

### Translating strings in the server script

Use the server script to translate schema options and other values during server-side runtime.

**Server script**

```javascript
function() {
  data.message=gs.getMessage("this message contains 'quotes'");
  //You can also translate schema options using the server script
  //For example, data.message=gs.getMessage(options.title);
}
```

**HTML template**

```html
<div>
  <p>{{c.data.message}}</p>
</div>
```

### Tutorial: Build a custom widget

Follow this tutorial to build a custom widget that displays Service Catalog items. Use this tutorial as a model to help you understand the advanced scripting power of the Service Portal.

In this tutorial, you will create the Quick Order widget. This widget:

- Displays popular items to the user prior to any search.
• Queries the Service Catalog and displays available options to the user.
• Includes an embedded SC Catalog Item widget, allowing the user to view and order items within the Quick Order widget.
• Uses an Angular Provider to display a category icon beside each queried item.

Tutorial: Create a widget
Create the Quick Order widget to query items in the Service Catalog.

Role required: admin or sp_admin
1. Navigate to Service Portal > Service Portal Configuration and click Widget Editor.
2. Click Create a new widget.

Widget Editor

Widget Editor is a development tool that allows you to view an widgets, create new widgets from scratch, and update the vari

- Check out the Hello World Example
- Create a new widget
- Edit an existing widget

Select a widget

3. Define the following values.
   • Widget Name: Quick Order
   • Widget ID: quick_order
   • Create a test page: Active
   • Page ID: quick_order
Adding a widget to a test page creates a record in each of the following tables:

- sp_page
- sp_container
- sp_row
- sp_column
- sp_instance
- sp_widget

**Note:** You can use the Page Editor in Service Portal Configuration to view the hierarchy of elements on your test page.

4. Click **Submit**.
5. From the **Widget Editor**, open the Quick Order widget.
6. Add the following simple template to the HTML field.

   ```html
   <div class="panel panel-primary">
   <div class="panel-heading">Request an item from the catalog</div>
   <div class="panel-body">
   My catalog results
   </div>
   </div>
   ```

7. Click **Save**.
8. Preview your test page in a new tab using the following URL: `<yourInstanceUrl>/sp?id=quick_order`.

   Your widget template displays on the test page.
Tutorial: Add a server script to query an instance table

After adding your widget and creating a basic template, you can define more advanced scripts that enable the user to query data from an instance table. Using client and server scripts, you can pass the data model between the client and server by querying data from the database, displaying it to the user, and sending any updates back to the server.

Role required: admin or sp_admin

1. From the **Widget Editor**, open the Quick Order widget.
2. Select **Server Script** to open the server script field.
3. Replace the default server script with the following custom script.

```javascript
(function() {
  if (input.keywords !== null & input.keywords !== '')
    data.items = getCatalogItems(input.keywords);

  function getCatalogItems(keywords) {
    var sc = new GlideRecord('sc_cat_item');
    sc.addActiveQuery();
    sc.addQuery('123TEXTQUERY321', keywords);
    sc.addQuery('sys_class_name', 'NOT IN', 'sc_cat_item_wizard,sc_cat_item_content');
    sc.addQuery('sc_catalogs', '0d08b13c3330100c8b837659bba8fb4');
    sc.setLimit(100);
    sc.orderByDesc('ir_query_score');
    sc.query();
    var results = [];
    while (sc.next()) {
      if (!$sp.canReadRecord(sc))
        continue;

      var item = {};
      $sp.getRecordDisplayValues(item, sc, 'name,price,sys_id');
      item.category = sc.getValue('category');
      results.push(item);
    }
    return results;
  }
}());
```

This script performs a keyword search on the `sc_cat_item` table using the 123TEXTQUERY321 query method.

4. Replace the HTML template with the following script:

```html
<div class="panel panel-primary">
  <div class="panel-heading">Request an item from the catalog</div>
  <div class="panel-body">
    <input class="form-control" type="search" placeholder="Start typing here to search the list of catalog items" ng-model="c.data.keywords" ng-change="c.server.update()" ng-model-options="{ debounce: 250 }" />
    <ul class="list-group result-container">
      <li class="list-group-item" ng-repeat="item in c.data.items">
        <a href>{{item.name}}</a><span class="pull-right">{{item.price}}</span>
      </li>
    </ul>
  </div>
</div>
```
This template adds a search field and displays the results of the query performed in the server script using the following Angular directives. To learn more about these directives, review the Angular API Reference.

**Angular directives used in the template**

<table>
<thead>
<tr>
<th>Angular directive</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ng-model</td>
<td>Automatically reads and writes value changes to the model variable <code>c.data.keywords</code>.</td>
</tr>
<tr>
<td>ng-model-options</td>
<td>Configures ng-model behavior. In this template, ng-model updates the model after a user has stopped typing for 250 milliseconds.</td>
</tr>
<tr>
<td>ng-change</td>
<td>Executes <code>c.server.update()</code> after the model value changes. This function posts the data object to the server script. After the script is executed, the data object is automatically updated with the new values from the server generated data object.</td>
</tr>
<tr>
<td>ng-repeat</td>
<td>Creates a template from the parent element and child elements. For each item in <code>c.data.items</code>, an instance of the template is created and the expressions <code>{{item.name}}</code> and <code>{{item.price}}</code> are replaced with the values from each item.</td>
</tr>
</tbody>
</table>

5. Add the following script to the **CSS - SCSS** field:

```
.result-container {
  margin-top: 10px;
}
```

6. Refresh your test page preview to view the changes.

As you type in the search box, matching catalog items appear. Try searching for **ipad**.

![Request an Item from the catalog](image)

**Tutorial: Manage the empty state of a widget**

Display a list of popular items to the user before any search terms are entered.

Role required: admin or sp_admin

Because no search has been executed when the widget initializes, the server input variable is undefined. This empty state may cause confusion when a user first interacts with the widget. To
solve this issue, give your widget something to display when the **input** variable is empty. This initial data can guide your users when initially interacting with your widget.

1. From the **Widget Editor**, open the Quick Order widget.
2. Replace the existing server script with the following script:

```javascript
(function() {
    if (input.keywords != null && input.keywords != '')
        data.items = getCatalogItems(input.keywords);
    else data.items = getPopularItems();

    function getCatalogItems(keywords) {
        var sc = new GlideRecord('sc_cat_item');
        sc.addActiveQuery();
        sc.addQuery('123TEXTQUERY321', keywords);
        sc.addQuery('sys_class_name', 'NOT IN', 'sc_cat_item_wizard,sc_cat_item_content');
        sc.addQuery('sc_catalogs', '0d08b13c3330100c8b837659bba8fb4');
        sc.setLimit(100);
        sc.orderByDesc("ir_query_score");
        sc.query();
        var results = [];
        while (sc.next()) {
            if (!$sp.canReadRecord(sc))
                continue;

            var item = {};
            $sp.getRecordDisplayValues(item, sc, 'name,price,sys_id');
            item.category = sc.getValue('category');
            results.push(item);
        }
        return results;
    }

    function getPopularItems() {
        var items = [];
        var count = new GlideAggregate('sc_req_item');
        count.addAggregate('COUNT','cat_item');
        count.groupBy('cat_item');
        count.addQuery('cat_item.sys_class_name', 'NOT IN', 'sc_cat_item_guide,sc_cat_item_wizard,sc_cat_item_content');
        count.addQuery('cat_item.sc_catalogs', '0d08b13c3330100c8b837659bba8fb4');
        count.orderByAggregate('COUNT', 'cat_item');
        count.query();
        while (count.next() && items.length < 9) {
            if (!$sp.canReadRecord("sc_cat_item", count.cat_item.sys_id.getDisplayValue()))
                continue; // user does not have permission to see this item

            var item = {};
            item.name = count.cat_item.name.getDisplayValue();
            item.category = count.cat_item.category.toString();
            item.price = count.cat_item.price.getDisplayValue();
            item.sys_id = count.cat_item.sys_id.getDisplayValue();
            items.push(item);
        }
        return items;
    }
}(function());
```

This script introduces a new function **getPopularItems()** to query the database and return popular items when the **input** variable is empty.
3. Replace the HTML template with the following script:

```html
<div class="panel panel-primary">
  <div class="panel-heading">Request an item from the catalog</div>
  <div class="panel-body">
    <input class="form-control" type="search" placeholder="Start typing here to search the list of catalog items" ng-model="c.data.keywords" ng-change="c.server.update()" ng-model-options="{debounce: 250}" />
    <h5 ng-if="!c.data.keywords">Showing the most popular items</h5>
    <ul class="list-group result-container">
      <li class="list-group-item" ng-repeat="item in c.data.items">
        <a href>{{item.name}}</a><span class="pull-right">{{item.price}}</span>
      </li>
    </ul>
    <div class="panel-footer" ng-if="c.data.keywords">
      <ng-pluralize count="c.data.items.length" when="{'0': 'No items found for ', '1': 'One item matching ', 'other': 'Found {} items matching '}">
        {{c.data.keywords}}
      </ng-pluralize>
    </div>
  </div>
</div>
```

This script provides a template to display the popular items returned from the server script.

4. Refresh your test page preview to view the changes.

The widget displays popular items to the user prior to any search input.

---

**Tutorial: Embed an existing widget**

Enable the user to view and purchase Service Catalog items in the Quick Order widget by embedding the SC Catalog Item widget.

Role required: admin or sp_admin

Instead of duplicating code, you can embed widgets to leverage pre-existing functionality. The SC Catalog Item widget is a base system widget that enables the user to view and purchase Service Catalog items.

1. Inspect the SC Catalog Item widget.
Before embedding the SC Catalog Item widget, inspect the widget to understand what data it needs access to. You may need to update your Quick Order widget client or server script to make sure that the correct data is passed to the embedded widget.

a) Navigate to `<yourInstanceURL>/sp_config?id=widget_edit`.

b) Open the SC Catalog Item widget.

c) Note that the widget ID is `widget-sc-cat-item`. You will use this ID to embed the widget model in the client script.

d) Examine the server script.

Notice that the `data` object includes a `sys_id` property populated by either the `input` or `options` objects. If neither `input` nor `options` include a `sys_id`, the `$sp.getParameter()` method retrieves the `sys_id` from the request query string.

```javascript
Server script
```

```javascript
if (input)
    data.sys_id = input.sys_id;
else if (options.sys_id)
    data.sys_id = options.sys_id;
else
    data.sys_id = $sp.getParameter('sys_id') || $sp.getParameter('sl_sys_id');
```

```javascript
```
To populate the input object, you can pass a catalog item sys_id from the Quick Order widget client script.

2. From the Widget Editor, open the Quick Order widget.
3. Replace the Quick Order widget client script with the following script:

```javascript
function($location, spUtil) {
    var c = this;

    c.select = function(item_id) {
        if (c.openItem == item_id) {
            c.openItem = null;
            return;
        }

        renderCatalogItemWidget(item_id);
    }

    function renderCatalogItemWidget(item_id) {
        c.catalogItemWidget = null;
        spUtil.get("widget-sc-cat-item", {sys_id: item_id}).then(function(response){
            c.catalogItemWidget = response;
            c.openItem = item_id;
        });
    }
}
```

This script uses spUtil.get() to retrieve the widget model by ID (widget-sc-cat-item) and define the {sys_id: item_id} object. This object posts to the server script as input.

4. Replace the HTML template with the following script:

```html
<div class="panel panel-primary">
    <div class="panel-heading">Request an item from the catalog</div>
    <div class="panel-body">
        <div class="form-control" type="search" placeholder="Start typing here to search the list of catalog items" ng-model="c.data.keywords" ng-change="c.server.update()" ng-model-options="{debounce: 250}" />
        <h5 ng-if="!c.data.keywords">Showing the most popular items</h5>
        <ul class="list-group result-container">
            <li class="list-group-item" ng-repeat="item in c.data.items">
                <a href ng-click="c.select(item.sys_id)">{{item.name}}</a><span class="pull-right">{{item.price}}</span>
                <div class="catalog-item" ng-if="item.sys_id == c.openItem">
                    <sp-widget ng-if="c.catalogItemWidget" widget="c.catalogItemWidget" />
                </div>
            </li>
        </ul>
        <div class="panel-footer" ng-if="c.data.keywords">
            <ng-pluralize count="c.data.items.length" when="{
                '0': 'No items found for ',
                '1': 'One item matching ',
                'other': 'Found {} items matching '}
           ">
                {{c.data.keywords}}
            </ng-pluralize>
        </div>
    </div>
</div>
```

This template:
• Adds on-click behavior using the ng-click directive.
• Displays the embedded SC Catalog Item widget using the sp-widget directive.

5. Replace the CSS with the following script:

```css
.result-container {
    margin-top: 10px;
}

.catalog-item {
    background-color: #f5f5f5;
    padding: 10px;
    @include border-top-radius($panel-border-radius);
    @include border-bottom-radius($panel-border-radius);
}
```

6. Refresh your test page preview to view the changes.

When you select a search result, the item opens in the embedded SC Catalog Item widget.

---

**Tutorial: Create a reusable directive and add it to a widget**

Angular Providers are reusable components that can be added to multiple widgets. Using the Widget Angular Providers table, create a directive that shows a category icon next to each result in the Quick Order widget.

Role required: admin or sp_admin

Angular Providers let you build angular directives and services that can be injected into your client script controller. The code in a Provider differs from a typical Angular directive or service because it must be anonymous, without being appended to a specific module.

The Widget Angular Providers table opens.

2. Click **New** to create a new record.

<table>
<thead>
<tr>
<th>Name</th>
<th>Client Script</th>
</tr>
</thead>
<tbody>
<tr>
<td>spTooltip</td>
<td>function spTooltip($compile) { return { restrict: 'A', link: function($scope, $e.target).attr('tooltips', true); $compile(element)($scope); } ]; } }</td>
</tr>
</tbody>
</table>
| spAttachmentManager| function(i18n) { return { template: '<div ng-show="attachments.length">
{{translations["Attachments"]}}</div><button class="btn btn-link ml-4">
<button ng-show="editMode && attachment.removeAttachment($event, attachment)"
class="fa fa-times ml-4", sysId: "", omitEdit: "" }, link: function(scope, elem, attr) { i18n.getAttachments(), function(msgArr) { scope.translations = msgArr; }, var attachmentHandler; function initializeAttachmentHandler() { $scope.attachmentHandler.getAttachments().then(function(response) { $scope.editMode = $scope.editMode; $scope.toggleName = function(s) { $scope.toggleTitle = function() { return ($scope.editMode) ? $scope.$parent.$parent.$parent.spAttachmentManager.removeAttachment = function(e, attachment) { e.stopPropagation(); (scope.attachments.length === 0) $scope.editMode = false: }); }; } scope.

3. Fill out the form.
   a) Add the type and name.
      - **Type**: Directive
      - **Name**: categoryIcon
   b) Add the client script.

```javascript
function() {
  return {
    template: '<span class="fa fa-stack fa-lg"><i class="fa fa-circle fa-stack-2x"></i><i class="fa fa-{{::icon}} fa-stack-1x fa-inverse"></i></span>',
    restrict: 'E',
    replace: true,
  }
```
This script associates the sys_id of the Category record with the Service Catalog item. The icon that displays is the icon defined in the Category record in the Service Catalog.
New Widget Angular Provider

Widget Angular Provider

Type

Directive

Name

categoryIcon

Client Script

```javascript
function() {
  return {
    template: '<span class="fa fa-stack fa-1x"><i class="fa fa-circle fa-stack-2x"></i><i class="fa fa-{::icon} fa-stack-1x fa-inverse"></i></span>',
    restrict: 'E',
    replace: true,
    scope: {
      category: '='
    },
    link: function(scope, element) {
      var _iconMap = {
        '080564f7337c284c63a6349bb05be58bf': 'tablet', // Tablets/
        '23796642a0b0807f21e1a3b72f2': 'question', // Can we help you?/
        'd9eb464c37003805463a35496b5e58bf': 'mobile-phone', // Mobiles/
        '39b0b1270e63714060f03791e092d1f3': 'print', // Office and Print/
        '5db435a377130805463a35496b5e58bf': 'print', // Printers/
        '2cb05987f47b2a080666ed31811871f': 'plug', // Peripherals/
        '39b0b1270e63714060f03791e092d1f3': 'desktop' // Software/
      };
      scope.icon = _iconMap[scope.category] || 'shopping-cart';
    }
  }
}
```

Application

Global
c) Click Save.

4. Associate the new Angular directive with the Quick Order Widget.
   a) Navigate to `<yourInstanceURL>/sp_config?id=widget_edit`.
   b) Open the Quick Order widget.
   c) Under **Related Lists**, select **Angular Providers**.
   d) In the Angular Providers list, click **New** to associate an existing Angular Provider with the Quick Order widget.
   e) Add the following values to the form.
      - **Angular Provider**: categoryIcon
      - **Widget**: Quick Order

   ![Angular Providers](image)

f) Click Save.

5. Add the categoryIcon directive to your Quick Order HTML template.
   a) From the **Widget Editor**, open the Quick Order widget.
   b) Replace the HTML template with the following script.

```html
<div class="panel panel-primary">
  <div class="panel-heading">Request an item from the catalog</div>
  <div class="panel-body">
    <input class="form-control" type="search" placeholder="Start typing here to search the list of catalog items" ng-model="c.data.keywords" ng-change="c.server.update()" ng-model-options="{debounce: 250}" />
    <h5 ng-if="!c.data.keywords">Showing the most popular items</h5>
    <h5 ng-if="#c.data.keywords">Showing the most popular items</h5>
    <h5 ng-if="#c.data.keywords">Showing the most popular items</h5>
  </div>
</div>
```

© 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.
6. Refresh your test page preview to view the changes.

A category icon displays beside each result.

Widget API reference

The following client and server side APIs are supported in the Service Portal.

Supported client side APIs

These are the supported Service Portal APIs that can be used in a widget client controller.

For detailed class and method information, see the API reference on the developer portal.
### Supported server side APIs

These are the supported Service Portal APIs that can be used in a widget server script.

<table>
<thead>
<tr>
<th>Class</th>
<th>Available methods</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GlideSPScriptable</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>· canReadRecord(GlideRecord gr)</td>
</tr>
<tr>
<td></td>
<td>· canReadRecord(String table, String sysId)</td>
</tr>
<tr>
<td></td>
<td>· getCatalogItem(String sysId)</td>
</tr>
<tr>
<td></td>
<td>· getCatalogItem(String sysId, Boolean isOrdering)</td>
</tr>
<tr>
<td></td>
<td>· getDisplayValue(String fieldName)</td>
</tr>
<tr>
<td></td>
<td>· getField(GlideRecord gr, String fieldName)</td>
</tr>
<tr>
<td></td>
<td>· getFields(GlideRecord gr, String fieldNames)</td>
</tr>
<tr>
<td></td>
<td>· getFieldsObject(GlideRecord gr, String fieldNames)</td>
</tr>
<tr>
<td></td>
<td>· getForm(String tableName, String sysId)</td>
</tr>
<tr>
<td></td>
<td>· getListColumns(String tableName, String view)</td>
</tr>
<tr>
<td></td>
<td>· getMenuHREF(GlideRecord page)</td>
</tr>
<tr>
<td></td>
<td>· getMenuItems(String sysId)</td>
</tr>
<tr>
<td></td>
<td>· getParameter(String name)</td>
</tr>
<tr>
<td></td>
<td>· getPortalRecord()</td>
</tr>
<tr>
<td></td>
<td>· getRecord()</td>
</tr>
<tr>
<td></td>
<td>· getRecordDisplayValues(Object data, GlideRecord from, String names)</td>
</tr>
<tr>
<td></td>
<td>· getRecordElements(Object data, GlideRecord from, String names)</td>
</tr>
<tr>
<td></td>
<td>· getRecordValues(Object data, GlideRecord from, String names)</td>
</tr>
<tr>
<td></td>
<td>· getStream(String table, String sysId)</td>
</tr>
<tr>
<td></td>
<td>· getUserInitials()</td>
</tr>
<tr>
<td></td>
<td>· getValue(String name)</td>
</tr>
<tr>
<td></td>
<td>· getValues(Object data, String names)</td>
</tr>
<tr>
<td></td>
<td>· getWidget(String sysId, Object options)</td>
</tr>
</tbody>
</table>

**Note:** `g_form` as a global object cannot be used in a widget client controller or in a UI script.

---

**Widget properties**

Global variable and functions available in widget client and server scripts.
Server script global objects

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>input</td>
<td>An object containing client-side properties set under c.data. The value is undefined until the client controller calls c.server.update().</td>
</tr>
<tr>
<td>data</td>
<td>An object containing properties set during server-side execution.</td>
</tr>
<tr>
<td>options</td>
<td>An object containing the schema option properties.</td>
</tr>
</tbody>
</table>

Client script global functions

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>this.server.get([Object])</td>
<td>Calls the server and sends custom input. Returns Promise.</td>
</tr>
<tr>
<td>this.server.update()</td>
<td>Calls the server and posts this.data to the server script. Returns Promise.</td>
</tr>
<tr>
<td>this.server.refresh()</td>
<td>Calls the server and automatically replaces the current options and data from the server response. Returns Promise.</td>
</tr>
</tbody>
</table>

A promise represents the eventual result of an asynchronous operation. For more information on promises, see [https://promisesaplus.com/](https://promisesaplus.com/) or [AngularJS documentation](https://angularjs.org/).

Search sources

A search source is a record that describes the behavior and source of searchable data.

A search source defines:

- Where search data is retrieved from.
- Whether search suggestions can populate the search field based on user input.
- How a search entry displays in the search result page.

Search sources have simple and advanced configurations.

**Simple**

Define a table within your ServiceNow instance as a source of searchable data. To learn more, see [Define a search source](https://servicenow.com).

**Advanced**

Define a data fetch script to return data. A data fetch script executes on the server and returns a result array to the search widget. This method is more complex, but offers complete power over how a search is executed. You are not limited to records and tables within ServiceNow and can define a script that fetches data from anywhere on the web. To learn more, review the [Tutorial: set up an external knowledge base search source](https://servicenow.com).
Typeahead settings

Typeahead returns search results in real time as a user types in the search field. You can configure typeahead settings, or disable the feature entirely, within the search source record.

Simple
Define an icon to display beside typeahead results and the target page to display typeahead selections.

Advanced
Define a template for the typeahead result. See Create an advanced typeahead template.

Search engine and custom settings

When a simple search source is defined, Service Portal uses the search engine settings configured on your instance. To learn more, see Search administration

Define a search source

A search source is a record that describes the behavior and source of searchable data. Configure a basic search source to query data from an instance table, or configure an advanced data fetch script to pull data from anywhere on the web.

A search source defines:

- Where search data is retrieved from.
- Whether search suggestions can populate the search field based on user input.
- How a search entry displays in the search result page.

Search sources have simple and advanced configurations.

Simple
Define a table within your ServiceNow instance as a source of searchable data.

Advanced
Define a data fetch script to return data. A data fetch script executes on the server and returns a result array to the search widget. This method is more complex, but offers complete power over how a search is executed. You are not limited to records and tables within ServiceNow and can define a script that fetches data from anywhere on the web. To learn more, review the Tutorial: set up an external knowledge base search source.

Typeahead returns search results in real time as a user types in the search field. You can configure typeahead settings, or disable the feature entirely, within the search source record. Typeahead return search has simple and advanced configurations.

Simple
Define an icon to display beside typeahead results and the target page to display typeahead selections.

Advanced
Define a template for the typeahead result. See Create an advanced typeahead template.

1. In the platform UI, navigate to Service Portal > Portals and select the portal you want to add search sources to.
2. From the **Search Sources** related list, click **New** to add a search source.
3. Define the fields on the **Search Source** form.

### Search Source form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The display value for the search category.</td>
</tr>
<tr>
<td>ID</td>
<td>The record ID. The value should be unique, and should not include any spaces or special characters.</td>
</tr>
<tr>
<td>Application</td>
<td>The scope of the search source.</td>
</tr>
<tr>
<td>Roles</td>
<td>If the Service Portal User Criteria Support plugin is not enabled, define user roles to access this search source.</td>
</tr>
<tr>
<td>Search page template</td>
<td>The HTML template that displays the search results. If defining a basic search source, you do not need to change the default template. For an example of a modified template, see Tutorial: set up an external knowledge base search source.</td>
</tr>
</tbody>
</table>

4. Complete the fields on the **Data Source** tab.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is scripted source</td>
<td>Select this option to add an advanced data fetch script. If configuring an instance table as the data source, do not check this option.</td>
</tr>
<tr>
<td>Data fetch script</td>
<td>A script defining the endpoint and API calls to fetch external data. This field is only visible when <strong>Is scripted source</strong> is selected. For an example of a data fetch script, see Tutorial: set up an external knowledge base search source.</td>
</tr>
</tbody>
</table>
| Table             | Select a table from the list that you want to draw your results from. You can select any table in the platform. For example, User (sys_user) or Knowledge (kb_knowledge).              
  **Note:** Only indexed tables return search results. Learn more: Enable text indexing for a table. |
| Conditions        | Apply a filter to the table if you don’t want all the search results to display. For example, Active is True. |
| Primary display field | Select which field you want to display on the search results page. For example, Name. |
| Display fields    | Select additional fields to display on the search results page. For example, User ID, Email, and City. |
5. Configure **Typeahead** settings to allow search results to populate the search field based on user input.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable typeahead</td>
<td>Allows typeahead functionality. If you do not want to integrate typeahead into your search source, clear the check box.</td>
</tr>
<tr>
<td>Advanced typeahead config</td>
<td>Optionally add an advanced typeahead script to configure the way search results display. For more information, see <a href="#">Create an advanced typeahead template</a>.</td>
</tr>
<tr>
<td>Typeahead glyph</td>
<td>Adds an icon beside each typeahead result.</td>
</tr>
<tr>
<td>Page</td>
<td>Defines a service portal page to display the selected result. For example, if <strong>form</strong> is configured, a selected typeahead result opens in a form.</td>
</tr>
</tbody>
</table>

6. Click **Submit**.

7. Configure the way typeahead results display with an advanced template.
   
a) In the **Typeahead** tab of the **Search Source** record, select the **Advanced typeahead config** check box.
b) In the **Typeahead template** field, add an HTML template.

This example uses AngularJS bindings to display service catalog images in the typeahead results.

```
<i class="ta-img" ng-if="match.model.type=='sc'" style="background-image:url('{{match.model.picture}}')"></i>
<i class="ta-img" ng-if="match.model.type=='sc_guide'" style="background-image:url('{{match.model.picture}}')"></i>
<i class="ta-icon fa fa-file-text-o" ng-if="match.model.type=='sc_content' && match.model.content_type == 'kb'"></i>
<br /></span>
```

This example uses AngularJS bindings to display service catalog images in the typeahead results.

```
<i class="ta-img" ng-if="match.model.type=='sc'" style="background-image:url('{{match.model.picture}}')"></i>
<i class="ta-img" ng-if="match.model.type=='sc_guide'" style="background-image:url('{{match.model.picture}}')"></i>
<i class="ta-icon fa fa-file-text-o" ng-if="match.model.type=='sc_content' && match.model.content_type == 'kb'"></i>
<br /></span>
```

C) Click **Update**.

Typeahead results display beside the image defined in the service catalog record.
Tutorial: set up an external knowledge base search source

Define an advanced search source to return data from any source on the Internet. To understand the power of search sources, follow this tutorial to set up an external knowledge base search source.

To create an advanced search source, you need an external resource that you can access via REST and basic knowledge of AngularJS.

In this integration, you will:

- Create a data fetch script that uses the ServiceNow Table API to query a knowledge base from another ServiceNow instance.
- Decode the JSON response and define the fields that the search widget expects.
• Update the search sources HTML template to open the search result in the external site.

1. In the platform UI, navigate to **Service Portal > Portals** and select the portal you want to add the search source to.
2. From the **Search Sources** related list, click **New**.
3. Create a name and ID for the search source. The ID should be unique, and should not include any spaces or special characters.
4. On the **Data Source** tab, select the **Is scripted source** check box.
5. Add content to the data fetch script field.
   a) Define the search function to be executed by the instance.
   
      This example uses a **recordless RESTMessage**, but you can modify this example to use a pre-configured **Outbound REST web service** if needed, or create a more secure authentication profile.

      ```javascript
      (function(query) {
        var results = [];
        /* Calculate your results here. */
        var url = "https://myInstance.service-now.com/api/now/table/kb_knowledge?sysparm_query=GOTO123TEXTQUERY321%3D" + encodeURI(query) + "&sysparm_fields=sys_id%2Cnumber%2Cshort_description%2Ccategory%2Ctext";
        var ws = new sn_ws.RESTMessageV2();
        ws.setBasicAuth("search_user", "search");
        ws.setHttpMethod("get");
        ws.setEndpoint(url);

        var jsonOutput = ws.execute();
        return results;
      })(query);
      }
      ```

      **Note:** In the preceding example, **ws.setBasicAuth** requires a user and password for the remote instance. For more detail, see **RESTMessageV2**.

   b) Add an if statement to the data fetch script to decode the JSON object being returned, iterate over each result, and set expected fields.

      The final data fetch script:

      ```javascript
      (function(query) {
        var results = [];
        /* Calculate your results here. */
        var url = "https://myInstance.service-now.com/api/now/table/kb_knowledge?sysparm_query=GOTO123TEXTQUERY321%3D" + encodeURI(query) + "&sysparm_fields=sys_id%2Cnumber%2Cshort_description%2Ccategory%2Ctext";
        var ws = new sn_ws.RESTMessageV2();
        ws.setBasicAuth("search_user", "search");
        ws.setHttpMethod("get");
        ws.setEndpoint(url);

        var jsonOutput = ws.execute();
        if (jsonOutput) {
          var response = new JSON().decode(jsonOutput.getBody());
          results = response.result;
          results.forEach(function(result) {
            result.url = "https://myInstance.service-now.com/kb_view.do?sysparm_article=" + result.number;
            result.target = "_blank";
          });
        }
      })(query);
      ```

© 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.
In this example, the following fields are set on the result object:

- **url**: If linking to an external site rather than opening the record in your ServiceNow instance, this defines where the link leads to.
- **target**: The target for the link. Set the target to _blank to open results in a new tab, otherwise leave it blank.
- **primary**: The primary field displayed in the search results.

6. Update the search page template to open the search results in the external site.

```html
<div>
    <a href="https://myInstance.service-now.com/kb_view.do?sysparm_article={{item.number}}" target="_blank" class="h4 text-primary m-b-sm block">
        <span ng-bind-html="highlight(item.primary, data.q)" ></span>
    </a>
    <span class="text-muted" ng-repeat="f in item.fields | limitTo: 4">
        <span class="m-l-xs m-r-xs" ng-if="!$first"> &middot; </span>
        {{f.label}}: <span ng-bind-html="highlight(f.display_value, data.q)" ></span>
    </span>
</div>
```

7. Click **Update**.

Test the external search in your portal. Results display under the name field value defined in step three.
Each search result opens in the external site defined in the search page template.
Example: set up a GitHub search source

Illustrates advanced search source functionality.

To create an advanced search source, you need an external resource that you can access via REST and basic knowledge of AngularJS.

1. In the platform UI, navigate to Service Portal > Portals and select the portal you want to add search sources to.
2. From the Search Sources related list, click **New**.
3. Create a name and ID for the search source. The ID should be unique, and should not include any spaces or special characters.
4. On the **Data Source** tab, select the **Is scripted source** check box.
5. Add content to the data fetch script field.

To set up a GitHub integration:

```javascript
(function(query) {
    var results = [];
    /* Calculate your results here. */
    var url = "https://api.github.com/search/repositories?q=" + encodeURI(query);
    var ws = new GlideHTTPRequest(url);
    ws.setBasicAuth("YOUR_USERNAME_HERE", "YOUR_PASSWORD_HERE");
    var jsonOutput = ws.get();
    if (jsonOutput) {
        var response = new JSON().decode(jsonOutput.getBody());
        results = response.items;
        results.forEach(function(result) {
            result.url = result.svn_url;
            result.target = "_blank";
            result.primary = result.full_name;
        });
    }
    return results;
})(query);
```

6. Use the Search page template to customize the way the search results display.

```html
<div>
    <div class="pull-right">
        <strong>{{item.language}}</strong>
        <a ng-href="{{item.svn_url}}/stargazers" target="_blank" class="m-l-sm"><span class="fa fa-star m-r-xs"></span>{{item.stargazers_count}}</a>
        <a ng-href="{{item.svn_url}}/network" target="_blank" class="m-l-sm"><span class="fa fa-code-fork m-r-xs"></span>{{item.forks}}</a>
    </div>
    <a ng-href="{{item.svn_url}}" target="_blank" class="h4 text-primary m-b-sm block">
        <span ng-bind-html="highlight(item.full_name, data.q)"></span>
    </a>
    <p>{{item.description}}</p>
    <p>Updated <sn-time-ago timestamp="item.updated_at"></sn-time-ago> ago</p>
</div>
```

**Create an advanced typeahead template**

Configure the way typeahead results display with an advanced template.

1. Complete the required fields in **Define a search source**.
2. In the **Typeahead** tab of the **Search Source** record, select the **Advanced typeahead config** check box.
3. In the **Typeahead template** field, add an HTML template.

This example uses AngularJS bindings to display service catalog images in the typeahead results.

```html
<i class="ta-img" ng-if="match.model.type=='sc'" style="background-image:url('{{match.model.picture}}')"></i>
<i class="ta-img" ng-if="match.model.type=='sc_guide'" style="background-image:url('{{match.model.picture}}')"></i>
<i class="ta-icon fa fa-file-text-o" ng-if="match.model.type=='sc_content' && match.model.content_type == 'kb'"></i>
<strong ng-if="match.model.type=='sc_content' && match.model.content_type == 'external'">#</strong>
<span ng-bind-html="match.label | uibTypeaheadHighlight:query"></span>
```

4. Click **Update**.

Typeahead results display beside the image defined in the service catalog record.
Set the default portal search source

Use the `glide.service_portal.default_search_sources` system property to define default search sources.

Role required: admin

If you don't define specific search sources for your portal, the system uses default search sources instead.
Default search source flow chart

1. In the Navigation filter, enter `sys_properties.list`. The entire list of properties in the System Properties (sys_properties) table appears.
2. On the list, find the system property `glide.service_portal.default_search_sources`, and then open the property record.
3. Copy the sys_ID of any search source you want to add into the Value field of the system property using a comma-separated list.

   To change the order in which the default search sources show in the Search List, change the order of the IDs in the property.

   You can remove the default search source behavior by deleting the property value or deleting the property altogether.
4. Click Update.

Configure contextual search

Use contextual search to limit search results for an instance of the typeahead search widget.

With contextual search enabled, users only see typeahead results for specific search sources. For example, searching on the Service Catalog page only shows results from the Service Catalog search source when contextual search is enabled.

1. In the Service Portal Designer (`Service Portal > Service Portal Configuration > Service Portal Designer`), find an instance of the typeahead search widget.
2. Point to the widget and click the edit icon ().
Alternatively, in any preview page containing the typeahead search widget, for example the Service Catalog homepage, control + right-click to open the widget context menu. Then click **Instance Options**.

3. In the Contextual Search Sources field, select search sources from the list.

Search sources listed for contextual search can be limited to just one, several, or all search sources.

Default search sources are defined in the `glide.service_portal.default_search_sources` property, so even if you don’t have search sources configured, typeahead search widget still shows typeahead suggestions. For more information on default search sources, see [Set the default portal search source](#).

### Service Portal security

Control user access to a portal.

Control who accesses your portal and what they can see in the following ways:

- **Authentication**: Configure login and single sign on for users
- **Limit page access by role**: Use roles to limit the users who can see a page.
- **Public pages**: Use the public check box on a page record to make the page publicly accessible.

**Note**: A number of portal pages that are installed by default are marked public. Filter your list of Service Portal pages for Public [is] true to identify these pages. Setting the Public value to false will prevent these pages from being publicly available.

- **User criteria**: For a more advanced way of limiting user access, create and apply user criteria to pages, widgets, widgets instances, and search sources.

### Single sign-on, logins, and URL redirects

Service Portal uses a combination of system properties and script includes to determine how the system handles URL redirects for users logging in to the portal.

Only users who understand SSO, URL redirects, and the ServiceNow platform should make any changes.

### Single sign-on and Service Portal

To use single sign-on with Service Portal, you must enable the `Integration - Multiple Provider Single Sign-On Installer` plugin (`com.snc.integration.sso.multi.installer`).

If you are using the system property to automatically redirect to your primary IdP, then Service Portal automatically redirects to that IdP. If you have multiple identity providers, Service Portal shows a link on the login page to **Use external login**. For more information on SSO and authentication in the platform, see [External single sign-on (SSO)](#).

### Require authentication for a Service Portal page

If you want to require authentication for a Service Portal page, ensure that the **Public** flag on the page record is not selected. For more information, see [Create and edit a service portal page](#).
a user navigates to a non-public page, they are redirected to the login page for the requested portal.

Because every page request is routed through the $sp page, this page must be public. The following values in the Public Pages sys_public table define the page as public:

- **Page**: $sp
- **Active**: true

### Configure the Service Portal login page

Administrators can configure a login page URL redirect for a portal.

1. In the sys_properties table, make sure these properties are set to the following:

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.entry.page.script</td>
<td>new SPEntryPage().getLoginURL()</td>
<td>Login page determination</td>
</tr>
</tbody>
</table>

2. It's better to leave this alone, but if you do need to customize the actual entry page, from the Script Includes table, search for SPEntryPage.

   **Note**: If you make changes to the script include, it won't be upgraded with future updates.

3. Edit the script on the SPEntryPage to change the assigned portal to the portal_suffix you want. SPEntryPage uses /sp/ as the portal path to redirect to. Enter your own portal_suffix in place of sp.

   ```javascript
   SPEntryPage.prototype = {
   initialize: function() {
      this.logVariables = false; // for debugging
      this.portal = "/sp/";       // The URL suffix specified in the sys_properties table
   },
   ```

### Redirect to Service Portal after login

Use system properties and script includes to conditionally redirect users to a page after logging in. Follow these steps to redirect a user to Service Portal after they log in.

1. In the sys_properties table, **Add a system property**:

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.entry.first.page.script</td>
<td>sp</td>
<td>new SPEntryPage().getFirstPageURL()</td>
<td>First page after authentication</td>
</tr>
</tbody>
</table>

   **getFirstPageURL** primarily does the following:
   - Redirects to login_redirect.do in order to break out of the frameset (if there is one).
   - Redirects to Service Portal if the user has no roles, or the full platform for everyone else.

2. Customize the after login behavior by navigating to the SPEntryPage script include.
Note: If you make changes to the script include, it won't be upgraded with future updates.

Note: If you are using external authentication, ensure that your IdP supports the RelayState URL parameter. This parameter retains the originally requested URL while the user authenticates, and is necessary for redirection after login.

Debug Service Portal URL redirects

Debug the URL redirects for logging in to Service Portal and redirecting to the first page.

To view debug output from SPEntryPage and see the session variables it redirects based on:

1. Make sure the system property glide.entry.first.page.script has the value: new SPEntryPage().getFirstPageURL().
2. From the SPEntryPage script include, set this.logVariables = true.
3. In a separate browser, log in.
4. From the system navigator, view the log output by navigating to System Logs > System Log > All.

Configure page security by role

Set up pages to be public or filtered by role.

Public pages won't require a user login; anyone can access them. All other options require user authentication.

To manage your page security:

1. In the Service Portal configuration page (Service Portal > Service Portal Configuration), open the Page Editor.
2. Search for the page you want to apply page security to in the Select Page list.
3. Select the highest level node in the tree view.
4. To make a page public, select the Public check box. All users will be able to access pages marked as Public.
5. To limit access to a certain role, add roles in a comma separated list. Users without the role listed will still be able to see links to the page if they appear in the portal. Trying to open the page will result in a page not found error.

Note: If you select Public and add a list of roles, the page is still accessible by any user.

6. To create a draft page that only administrators can see while the page is still in development, select Draft. Users must have the admin role to see any pages in draft. Everyone else will see a page not found error.
User criteria for Service Portal

Administrators can control access to pages, widgets, widget instances, and search sources in a portal by creating and applying user criteria.

User criteria records define conditions that are evaluated against user records. When user criteria is defined, portal records are only visible to users who pass the defined conditions.

User criteria is a platform feature used in Service Portal

Converting role-based permissions to user criteria records

User criteria in Service Portal replaces role-based permissions. After activating the user criteria for Service Portal plugin, you must Set the user criteria for Service Portal system property to true. When the system property is set to true, any existing roles defined for a page, widget, or search source
are automatically converted into user criteria records. To disable user criteria and continue using role-based permissions, set the system property to false.

**User criteria checks**

User criteria uses the following checks in Service Portal to verify user access.

**Page access user criteria**

The following diagram shows how the system decides whether a user can access a page based on user criteria.
Widget access user criteria

The following diagram shows how the system determines whether a user has access to a particular widget or widget instance.
Activate the user criteria for Service Portal plugin

You can activate the Service Portal User Criteria Support plugin (com.glide.service-portal.user-criteria) 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 the user criteria for Service Portal system property

After activating the Service Portal User Criteria Support plugin, you must set the system property to true.

Role required: admin

Setting the system property activates user criteria for Service Portal. When the system property is set to true, any existing roles defined for a page, widget, or search source are automatically converted into user criteria records. To disable user criteria and continue using role-based permissions, set the system property to false.

1. Navigate to Service Portal > Properties.
2. Click the check box to set the following property to true.

Enable use of User Criteria records instead of Roles fields for Service Portal

Defines permissions for Service Portal widgets, widget instances, search sources.

☐ Yes | No

3. Click Save.

Create a user criteria record for Service Portal

Create a user criteria record to apply to items in Service Portal and control user access to pages, widgets, widget instances, and search sources.
You can apply existing user criteria to records in Service Portal through Service Portal configuration (Service Portal > Service Portal configuration). You can only create user criteria within the platform UI.

1. In the navigation filter, type Service Portal.
2. Select a page, widget, or widget instance record.
3. In the related list at the bottom of the record, select the Can View or Cannot View tab, then click New. If a user criteria record is already created, you can click Edit to apply user criteria to the page, widget, or widget instance.

User criteria records are stored in the user_criteria table.

4. Complete the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Service Portal User Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the criteria record.</td>
</tr>
<tr>
<td>Users</td>
<td>User records to match access criteria.</td>
</tr>
<tr>
<td>Groups</td>
<td>Group records to match access criteria.</td>
</tr>
<tr>
<td>Roles</td>
<td>Roles to match access criteria.</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>
<tbody>
<tr>
<td>Advanced</td>
<td>Displays or hides the <strong>Script</strong> field.</td>
</tr>
<tr>
<td>Script</td>
<td>Defines any additional criteria, and returns <code>true</code> or <code>false</code>. This field is available only if <strong>Advanced</strong> is selected.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Because scripts are evaluated dynamically, including scripts in user criteria records can decrease performance.</td>
</tr>
<tr>
<td>Application</td>
<td>Application scope for the user criteria record.</td>
</tr>
<tr>
<td>Active</td>
<td>Activate or deactivates this criteria record.</td>
</tr>
<tr>
<td>Companies</td>
<td>Companies to match access criteria.</td>
</tr>
<tr>
<td>Locations</td>
<td>Locations to match access criteria.</td>
</tr>
<tr>
<td>Departments</td>
<td>Departments to match access criteria.</td>
</tr>
</tbody>
</table>
| Match All    | Determines whether all elements from each populated criteria field must match. If selected, only users who match all criteria are given access. If cleared, the user must meet one or more of the set criteria to be given access. By default, this check box is cleared so that any condition met provides a match. For example, consider a user criteria record for the following:  
- Locations A or B  
- Company C or D  

With **Match All** selected, only users meeting all these conditions are matched. For example, a user with a location A and a company C.  
With **Match All** cleared, users meeting any of these conditions are matched. For example, a user with a location B.  

**Note:** If you select **Match All**, ensure that you do not create contradictory conditions that can never be met. For example, if all users in location A work for company G, then the conditions in this example can never be met. |

5. Click **Submit**.

**Apply user criteria to a page, widget, or widget instance**

Assign user criteria to pages, widgets, or widget instances to limit user access to content in a portal.
Activate the Service Portal User Criteria Support (com.glide.service-portal.user-criteria) plugin and set the `glide.service_portal.user_criteria_enabled` system property to `true`.

Role required: admin or sp_admin

You can apply several user criteria records to a single portal item.

1. In the Service Portal Configuration page (Service Portal > Service Portal Configuration), open the Page Editor.
2. Select a page from the list.
3. Select a page, widget, or widget instance node from the page tree.
4. Under related lists, click Who Can View or Who Cannot View.
5. Click New.
6. Select a criteria from the Can View or Cannot View list.

Selecting criteria from the Can View or Cannot View list applies user criteria records created in Create a user criteria record for Service Portal to the selected page, widget, or widget instance.

7. Click Save.
Apply user criteria to a search source

Assign user criteria to search sources to limit user access to content in a portal.

Role required: admin

You can add user criteria to custom or default Search sources.

1. In the Service Portal Configuration page (Service Portal > Service Portal Configuration), navigate to Portal Tables > Search Source in the header menu.
Service Portal

Create rich, engaging and modern experiences to help your business run.
Select one of the options below to continue.

- **Branding Editor**
  Customize your portal’s title, logo and theme colors. Preview changes as you make them.

- **Designer**
  Create and layout pages with drag-and-drop functionality. Preview pages as you make changes.

- **Page Editor**
  Configure the properties of pages, containers and widgets from a map view.

- **Widget Editor**
  Create widgets from scratch or customize an existing one. Write HTML, CSS, and JavaScript with real-time preview.

- **Search Source**
  Service Portal
  Service Portal Documentation
  Service Portal Log Entry
2. Open the search source record that you would like to modify.
3. Under related lists, click **Who Can View Search Sources** or **Who Cannot View Search Sources**.
4. Click **New**.
5. Select a criteria from the **Can View** or **Cannot View** list.

Selecting criteria from the **Can View** or **Cannot View** list applies user criteria records created in **Create a user criteria record for Service Portal** to the selected search source.

6. Click **Save**.

**Service Portal components**

View this video to learn more about the different pieces that make up a portal.

**Service Portal SCSS Primer**

SCSS is a subset of the Syntactically Awesome StyleSheets (Sass) specification and is an extension of CSS. Every valid CSS style sheet is valid SCSS.
SCSS variables

SCSS variables are a way to store information that you want to reuse throughout your style sheet. You can store things like colors, font stacks, or any CSS value you think you want to reuse. SCSS uses the $ symbol to make something a variable.

SCSS supports the following data types:

- Numbers (including units)
- Strings (with or without quotes)
- Colors (name, or names)
- Booleans

Variables can also be arguments to or results from one of several available functions or mixins. During translation, the values of the variables are inserted into the output CSS document.

For example:

```css
$font-stack: Helvetica, sans-serif;
$primary-color: #333;

body {
  font: 100%$font-stack;
  color: $primary-color;
}
```

For more information on Sass, see the [Sass/SCSS reference](#).

SCSS functions

List of functions for Service Portal SCSS compiler.

**RGB functions**

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>rgb($red, $green, $blue)</code></td>
<td>Creates a Color from red, green, and blue values.</td>
</tr>
<tr>
<td><code>rgba($red, $green, $blue, $alpha)</code></td>
<td>Creates a Color from red, green, blue, and alpha values.</td>
</tr>
<tr>
<td><code>red($color)</code></td>
<td>Gets the red component of a color.</td>
</tr>
<tr>
<td><code>green($color)</code></td>
<td>Gets the green component of a color.</td>
</tr>
<tr>
<td><code>blue($color)</code></td>
<td>Gets the blue component of a color.</td>
</tr>
<tr>
<td><code>mix($color1, $color2, ($weight))</code></td>
<td>Mixes two colors together.</td>
</tr>
</tbody>
</table>

**HSL functions**

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>hsl($hue, $saturation, $lightness)</code></td>
<td>Creates a Color from hue, saturation, and lightness values.</td>
<td>Yes</td>
</tr>
<tr>
<td>Function</td>
<td>Description</td>
<td>Availability</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>hsla($hue, $saturation, $lightness, $alpha)</td>
<td>Creates a Color from hue, saturation, lightness, and alpha values.</td>
<td>Yes</td>
</tr>
<tr>
<td>hue($color)</td>
<td>Gets the hue component of a color.</td>
<td>Yes</td>
</tr>
<tr>
<td>saturation($color)</td>
<td>Gets the saturation component of a color.</td>
<td>Yes</td>
</tr>
<tr>
<td>lightness($color)</td>
<td>Gets the lightness component of a color.</td>
<td>Yes</td>
</tr>
<tr>
<td>adjust-hue($color, $degrees)</td>
<td>Changes the hue of a color.</td>
<td>Yes</td>
</tr>
<tr>
<td>lighten($color, $amount)</td>
<td>Makes a color lighter.</td>
<td>Yes</td>
</tr>
<tr>
<td>darken($color, $amount)</td>
<td>Makes a color darker.</td>
<td>Yes</td>
</tr>
<tr>
<td>saturate($color, $amount)</td>
<td>Makes a color more saturated.</td>
<td>Yes</td>
</tr>
<tr>
<td>desaturate($color, $amount)</td>
<td>Makes a color less saturated.</td>
<td>Yes</td>
</tr>
<tr>
<td>grayscale($color)</td>
<td>Converts a color to grayscale.</td>
<td>Yes</td>
</tr>
<tr>
<td>complement($color)</td>
<td>Returns the complement of a color.</td>
<td>No</td>
</tr>
<tr>
<td>invert($color)</td>
<td>Returns the inverse of a color.</td>
<td>No</td>
</tr>
</tbody>
</table>

### Opacity functions

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>alpha($color)</td>
<td>Gets the alpha component (opacity) of a color.</td>
<td>Yes</td>
</tr>
<tr>
<td>opacity($color)</td>
<td>Gets the alpha component (opacity) of a color.</td>
<td>Yes</td>
</tr>
<tr>
<td>rgba($color, $alpha)</td>
<td>Changes the alpha component for a color.</td>
<td>Yes</td>
</tr>
<tr>
<td>opacify($color, $amount)</td>
<td>Makes a color more opaque.</td>
<td>No</td>
</tr>
<tr>
<td>fade-in($color, $amount)</td>
<td>Makes a color more opaque.</td>
<td>No</td>
</tr>
<tr>
<td>transparentize($color, $amount)</td>
<td>Makes a color more transparent.</td>
<td>No</td>
</tr>
<tr>
<td>fade-out($color, $amount)</td>
<td>Makes a color more transparent.</td>
<td>No</td>
</tr>
</tbody>
</table>

### Other color functions

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>adjust-color()</td>
<td>Increases or decreases one or more components of a color.</td>
<td>Yes</td>
</tr>
<tr>
<td>scale-color()</td>
<td>Fluidly scales one or more properties of a color.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### String functions

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>change-color()</td>
<td>Changes one or more properties of a color.</td>
<td>No</td>
</tr>
<tr>
<td>ie-hex-str()</td>
<td>Converts a color into the format understood by IE filters.</td>
<td>No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>unquote($string)</td>
<td>Removes quotes from a string.</td>
<td>Yes</td>
</tr>
<tr>
<td>quote($string)</td>
<td>Adds quotes to a string.</td>
<td>Yes</td>
</tr>
<tr>
<td>str-length($string)</td>
<td>Returns the number of characters in a string.</td>
<td>No</td>
</tr>
<tr>
<td>str-insert($string, $insert, $index)</td>
<td>Inserts $insert into $string at $index.</td>
<td>No</td>
</tr>
<tr>
<td>str-index($string, $substring)</td>
<td>Returns the index of the first occurrence of $substring in $string.</td>
<td>No</td>
</tr>
<tr>
<td>str-slice($string, $start-at, [$end-at])</td>
<td>Extracts a substring from $string.</td>
<td>No</td>
</tr>
<tr>
<td>to-upper-case($string)</td>
<td>Converts a string to upper case.</td>
<td>No</td>
</tr>
<tr>
<td>to-lower-case($string)</td>
<td>Converts a string to lower case.</td>
<td>No</td>
</tr>
</tbody>
</table>

### Number functions

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>percentage($number)</td>
<td>Converts a unitless number to a percentage.</td>
<td>Yes</td>
</tr>
<tr>
<td>round($number)</td>
<td>Rounds a number to the nearest whole number.</td>
<td>Yes</td>
</tr>
<tr>
<td>ceil($number)</td>
<td>Rounds a number up to the next whole number.</td>
<td>Yes</td>
</tr>
<tr>
<td>floor($number)</td>
<td>Rounds a number down to the previous whole number.</td>
<td>Yes</td>
</tr>
<tr>
<td>abs($number)</td>
<td>Returns the absolute value of a number.</td>
<td>Yes</td>
</tr>
<tr>
<td>min($numbers…)</td>
<td>Finds the minimum of several numbers.</td>
<td>Yes</td>
</tr>
<tr>
<td>max($numbers…)</td>
<td>Finds the maximum of several numbers.</td>
<td>Yes</td>
</tr>
<tr>
<td>random([$limit])</td>
<td>Returns a random number.</td>
<td>No</td>
</tr>
</tbody>
</table>
List functions

Lists in SCSS are immutable. All list functions return a new list rather than updating the existing list in-place.

All list functions work for maps as well, treating them as lists of pairs.

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>length($list)</td>
<td>Returns the length of a list.</td>
</tr>
<tr>
<td>nth($list, $n)</td>
<td>Returns a specific item in a list.</td>
</tr>
<tr>
<td>set-nth($list, $n, $value)</td>
<td>Replaces the nth item in a list.</td>
</tr>
<tr>
<td>join($list1, $list2)</td>
<td>Joins two lists into one.</td>
</tr>
<tr>
<td>append($list1, $val)</td>
<td>Appends a single value onto the end of a list.</td>
</tr>
<tr>
<td>zip($lists...)</td>
<td>Combines several lists into a single multidimensional list.</td>
</tr>
<tr>
<td>index($list, $value)</td>
<td>Returns the position of a value within a list.</td>
</tr>
<tr>
<td>list-separator($list)</td>
<td>Returns the separator of a list.</td>
</tr>
</tbody>
</table>

Adding custom functions

Scss @function my-calculation-function($some-number, $another-number){ @return $some-number + $another-number }

SCSS nesting

SCSS lets you nest your CSS selectors in a way that follows the same visual hierarchy of your HTML.

For example:

```css
class nav {
    ul {
        margin: 0;
        padding: 0;
        list-style: none;
    }

    li { display: inline-block; }

    a {
        display: block;
        padding: 6px 12px;
        text-decoration: none;
    }
}
```

The **ul**, **li**, and **a** selectors are nested inside the **nav** selector, which is a great way to organize your CSS and make it more readable. When the widget is rendered, the generated CSS looks something like the following code block:

```css
class nav ul {
    margin: 0;
    padding: 0;
    list-style: none;
}
```
SCSS operators

SCSS has a handful of standard math operators like +, -, *, /, and %.

Use simple math to calculate widths for an aside & article. For example:

```css
.container { width: 100%; }
article[role="main"] {  
  float: left;  
  width: 600px / 960px * 100%;
}
aside[role="complementary"] {  
  float: right;  
  width: 300px / 960px * 100%;
}
```

The generated CSS looks like:

```css
.container {  
  width: 100%;
}
article[role="main"] {  
  float: left;  
  width: 62.5%;
}
aside[role="complementary"] {  
  float: right;  
  width: 31.25%;
}
```

For more information on Sass, see the [Sass/SCSS reference](#).

SCSS mixins

A mixin lets you make groups of CSS declarations that you want to reuse throughout your site. You can pass in values to make your mixin more flexible.

The following code block is an example for border-radius.

```scss
@mixin border-radius($radius) {  
-webkit-border-radius: $radius;  
-moz-border-radius: $radius;  
-ms-border-radius: $radius;
```
The generated CSS looks like:

```css
.box {
  -webkit-border-radius: 10px;
  -moz-border-radius: 10px;
  -ms-border-radius: 10px;
  border-radius: 10px;
}
```

For more information on Sass, see the [Sass/SCSS reference](#).

## Advanced resources for Service Portal

Advanced users with CSS and HTML understanding can configure fields in the portal form directly as accessed through the portal UI.

### Single sign-on, logins, and URL redirects

Service Portal uses a combination of system properties and script includes to determine how the system handles URL redirects for users logging in to the portal.

Only users who understand SSO, URL redirects, and the ServiceNow platform should make any changes.

### Single sign-on and Service Portal

To use single sign-on with Service Portal, you must enable the Integration - Multiple Provider Single Sign-On Installer plugin (com.snc.integration.sso.multi.installer).

If you are using the system property to automatically redirect to your primary IdP, then Service Portal automatically redirects to that IdP. If you have multiple identity providers, Service Portal shows a link on the login page to **Use external login**. For more information on SSO and authentication in the platform, see #unique_2308.

### Require authentication for a Service Portal page

If you want to require authentication for a Service Portal page, ensure that the **Public** flag on the page record is not selected. For more information, see #unique_2309. If a user navigates to a non-public page, they are redirected to the login page for the requested portal.

Because every page request is routed through the `$sp` page, this page must be public. The following values in the Public Pages `sys_public` table define the page as public:

- **Page**: `$sp`
- **Active**: `true`

### Configure the Service Portal login page

Administrators can configure a login page URL redirect for a portal.

1. In the `sys_properties` table, make sure these properties are set to the following:
2. It’s better to leave this alone, but if you do need to customize the actual entry page, from the Script Includes table, search for **SPEntryPage**.

**Note:** If you make changes to the script include, it won’t be upgraded with future updates.

3. Edit the script on the **SPEntryPage** to change the assigned portal to the portal_suffix you want. **SPEntryPage** uses `/sp/` as the portal path to redirect to. Enter your own portal_suffix in place of `sp`.

### Redirect to Service Portal after login

Use system properties and script includes to conditionally redirect users to a page after logging in. Follow these steps to redirect a user to Service Portal after they log in.

1. In the **sys_properties** table, **#unique_2312**:

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.entry.first.page.script</td>
<td>string</td>
<td><code>new SPEntryPage().getFirstPageURL()</code></td>
<td>First page after authentication</td>
</tr>
</tbody>
</table>

**getFirstPageURL** primarily does the following:

- Redirects to `login_redirect.do` in order to break out of the frameset (if there is one).
- Redirects to Service Portal if the user has no roles, or the full platform for everyone else.

2. Customize the after login behavior by navigating to the **SPEntryPage** script include.

**Note:** If you make changes to the script include, it won’t be upgraded with future updates.

**Note:** If you are using external authentication, ensure that your IdP supports the RelayState URL parameter. This parameter retains the originally requested URL while the user authenticates, and is necessary for redirection after login.

### Debug Service Portal URL redirects

Debug the URL redirects for logging in to Service Portal and redirecting to the first page.

To view debug output from **SPEntryPage** and see the session variables it redirects based on:

1. Make sure the system property `glide.entry.first.page.script` has the value: `new SPEntryPage().getFirstPageURL()`.
2. From the **SPEntryPage** script include, set `this.logVariables = true`.
3. In a separate browser, log in.
4. From the system navigator, view the log output by navigating to System Logs > System Log > All.

Create a custom portal theme

If you need more customization than Branding Editor can provide, you can create your own custom theme.

Role required: admin or sp_admin role

Only users with an understanding of CSS should create custom themes.

1. Navigate to Service Portal > Themes, then click New.
2. Complete the form, as necessary.

### Theme form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of your theme. Use this name to associate the theme with your portal. This name is not visible to users, you should know it to apply the correct theme to a portal.</td>
</tr>
<tr>
<td>Application</td>
<td>The record scope. The header menu record and the source table must have the same application scope.</td>
</tr>
<tr>
<td>Header</td>
<td>List of headers and footers from the sp_header_footer table that you can associate with a portal theme. Headers and footers are widgets and can be configured the same way.</td>
</tr>
<tr>
<td>Footer</td>
<td>List of headers and footers from the sp_header_footer table that you can associate with a portal theme.</td>
</tr>
<tr>
<td>Fixed header</td>
<td>Locks the header at the top of the page so that when a user scrolls the header remains on the screen.</td>
</tr>
<tr>
<td>Fixed footer</td>
<td>Locks the footer at the bottom of the page so that when a user scrolls the footer remains on the screen.</td>
</tr>
<tr>
<td>CSS variables</td>
<td>CSS custom properties that you can use to change the color and styles in a portal. For example, the stock theme uses some of the following variables:</td>
</tr>
</tbody>
</table>

```css
$sp-logo-margin-x: 15px !default;
$sp-tagline-color: $text-color !default;
$navbar-inverse-bg: #3a3f51 !default;
```

3. Click Save.
4. To add a style sheet to the theme, in the CSS Include related list, click New.
5. Complete the style sheet form fields, then click **Save**.

**Style sheet form fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the CSS Include. Remember this name to associate the CSS Include with the theme.</td>
</tr>
<tr>
<td>Application</td>
<td>The record scope. The header menu record and the source table must have the same application scope.</td>
</tr>
<tr>
<td>Source</td>
<td>Select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Style Sheet</strong>: Add an internal style sheet that has been uploaded to the CSS table (sp_css). For example, ng-sortable.min.css. Internal style sheets use standard CSS in the CSS field.</td>
</tr>
<tr>
<td></td>
<td>• <strong>URL</strong>: Link to an external style sheet. Use external style sheets to use the same CSS as a corporate website or other online resource.</td>
</tr>
<tr>
<td>Style sheet</td>
<td>Associate a style sheet or CSS file URL, depending on which option you select in the <strong>Source</strong> field.</td>
</tr>
</tbody>
</table>

6. Complete the style sheet form fields.
Style sheet form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display name</td>
<td>Name of the CSS Include. Remember this name to associate the CSS Include with the theme.</td>
</tr>
<tr>
<td>Application</td>
<td>The record scope. The header menu record and the source table must have the same application scope.</td>
</tr>
<tr>
<td>Source</td>
<td>Select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>- <strong>UI Script</strong>: Add an internal UI script that has been uploaded to the UI script table (sys_ui_script). UI scripts allow you to create client-side JavaScript and reuse it in multiple locations. For more information on UI scripts, see <a href="#">UI scripts</a>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>URL</strong>: Link to an external JavaScript file. Use external URLs to use the same JavaScript as a corporate website or other online resource.</td>
</tr>
<tr>
<td>UI Script or Java file URL</td>
<td>Associate an internal UI script or Java file URL, depending on which option you select in the Source field.</td>
</tr>
<tr>
<td>Updated</td>
<td>Date and time that the JS Include was last updated</td>
</tr>
<tr>
<td>Package</td>
<td>The Service Portal package that the JS include is associated with. For example, Service Portal Configuration Pages. This field is populated by default.</td>
</tr>
</tbody>
</table>

**Tutorial: set up an external knowledge base search source**

Define an advanced search source to return data from any source on the Internet. To understand the power of search sources, follow this tutorial to set up an external knowledge base search source.

To create an advanced search source, you need an external resource that you can access via REST and basic knowledge of [AngularJS](#).

In this integration, you will:

- Create a data fetch script that uses the ServiceNow **Table API** to query a knowledge base from another ServiceNow instance.
- Decode the JSON response and define the fields that the search widget expects.
- Update the search sources HTML template to open the search result in the external site.

1. In the platform UI, navigate to **Service Portal > Portals** and select the portal you want to add the search source to.
2. From the **Search Sources** related list, click **New**.
3. Create a name and ID for the search source. The ID should be unique, and should not include any spaces or special characters.
4. On the **Data Source** tab, select the **Is scripted source** check box.
5. Add content to the data fetch script field.
   a) Define the search function to be executed by the instance.
   
   This example uses a *recordless RESTMessage*, but you can modify this example to use a pre-configured *Outbound REST web service* if needed, or create a more secure authentication profile.

   ```javascript
   (function(query) {
     var results = [];
     /* Calculate your results here. */
     var url = "https://myInstance.service-now.com/api/now/table/kb_knowledge?sysparm_query=GOTO123TEXTQUERY321%3D" + encodeURI(query) + "&sysparm_fields=sys_id%2Cnumber%2Cshort_description%2Ccategory%2Ctext";
     var ws = new sn_ws.RESTMessageV2();
     ws.setBasicAuth("search_user", "search");
     ws.setHttpMethod("get");
     ws.setEndpoint(url);
     var jsonOutput = ws.execute();
     return results;
   })(query);
   
   **Note:** In the preceding example, *ws.setBasicAuth* requires a user and password for the remote instance. For more detail, see *RESTMessageV2*.

   b) Add an if statement to the data fetch script to decode the JSON object being returned, iterate over each result, and set expected fields.
   
   The final data fetch script:

   ```javascript
   (function(query) {
     var results = [];
     /* Calculate your results here. */
     var url = "https://myInstance.service-now.com/api/now/table/kb_knowledge?sysparm_query=GOTO123TEXTQUERY321%3D" + encodeURI(query) + "&sysparm_fields=sys_id%2Cnumber%2Cshort_description%2Ccategory%2Ctext";
     var ws = new sn_ws.RESTMessageV2();
     ws.setBasicAuth("search_user", "search");
     ws.setHttpMethod("get");
     ws.setEndpoint(url);
     var jsonOutput = ws.execute();
     if (jsonOutput) {
       var response = new JSON().decode(jsonOutput.getBody());
       results = response.result;
       results.forEach(function(result) {
         result.url = "https://myInstance.service-now.com/kb_view.do?sysparm_article=" + result.number;
         result.target = "_blank";
         result.primary = result.short_description;
       });
     }
     return results;
   })(query);
   
   In this example, the following fields are set on the result object:
- **url**: If linking to an external site rather than opening the record in your ServiceNow instance, this defines where the link leads to.
- **target**: The target for the link. Set the target to _blank to open results in a new tab, otherwise leave it blank.
- **primary**: The primary field displayed in the search results.

### 6. Update the search page template to open the search results in the external site.

```html
<div>
  <a href="https://myInstance.service-now.com/kb_view.do?sysparm_article={{item.number}}" target="_blank"
     class="h4 text-primary m-b-sm block">
    <span ng-bind-html="highlight(item.primary, data.q)"></span>
  </a>
  <span class="text-muted" ng-repeat="f in item.fields | limitTo: 4">
    &middot; {{f.label}}: <span ng-bind-html="highlight(f.display_value, data.q)"></span>
  </span>
</div>
```

### 7. Click Update.

Test the external search in your portal. Results display under the name field value defined in step three.
Each search result opens in the external site defined in the search page template.
Example: set up a GitHub search source

Illustrates advanced search source functionality.
To create an advanced search source, you need an external resource that you can access via REST and basic knowledge of AngularJS.

1. In the platform UI, navigate to Service Portal > Portals and select the portal you want to add search sources to.
2. From the Search Sources related list, click New.
3. Create a name and ID for the search source. The ID should be unique, and should not include any spaces or special characters.
4. On the Data Source tab, select the Is scripted source check box.
5. Add content to the data fetch script field.

To set up a GitHub integration:

```javascript
(function(query) {
    var results = [];
    /* Calculate your results here. */
    var url = "https://api.github.com/search/repositories?q=" + encodeURIComponent(query);
    var ws = new GlideHTTPRequest(url);
    ws.setBasicAuth("YOUR_USERNAME_HERE", "YOUR_PASSWORD_HERE");
    var jsonOutput = ws.get();
    if (jsonOutput) {
        var response = new JSON().decode(jsonOutput.getBody());
        results = response.items;
        results.forEach(function(result) {
            result.url = resultsvn_url;
            result.target = "_blank";
            result.primary = result.full_name;
        });
    }
    return results;
})(query);
```

6. Use the Search page template to customize the way the search results display.

```html
<div>
    <div class="pull-right">
        <strong>{{item.language}}</strong>
        <a ng-href="{{item.svn_url}}/stargazers" target="_blank" class="m-l-sm">
            <span class="fa fa-star m-r-xs"></span>{{item.stargazers_count}}</a>
        <a ng-href="{{item.svn_url}}/network" target="_blank" class="m-l-sm">
            <span class="fa fa-code-fork m-r-xs"></span>{{item.forks}}</a>
    </div>
    <a ng-href="{{item.svn_url}}" target="_blank" class="h4 text-primary m-b-sm block">
        <span ng-bind-html="highlight(item.full_name, data.q)"></span></a>
    <p>{{item.description}}</p>
    <p>Updated <sn-time-ago timestamp="item.updated_at"></sn-time-ago> ago</p>
</div>
```

Subscription Management

With the ServiceNow® Subscription Management application, review and manage how your ServiceNow subscriptions are used on your production instance.
Subscription Management setup guide

Because Subscription Management is active for all production instances by default, you do not need to activate a plugin. To set up Subscription Management, you assign the usage_admin role to the users who will administer subscriptions. The admins allocate users to appropriate subscriptions, monitor usage of applications (both by subscribed users and by users who are not subscribed), and update subscription levels as needed.

What to do

Assign the Usage Admins

Before you (the admin user) do anything else, assign the usage_admin role to the persons who will manage subscriptions for your organization.

Admin responsibilities and activities are described in Allocating users to a Per-User subscription and Monitoring how subscriptions are allocated.

View the list of your subscription applications

See View your subscription applications and allocation levels.

If your organization purchased Per-User subscriptions, the usage_admin allocates users

Note: You perform this task only for Per-User subscriptions. Your instance auto-allocates and reports on monthly usage for all other subscription types.

With a Per-User subscription, a specified number of users is entitled to use the application. You perform the following tasks:

- Build user sets.
- Allocate users to appropriate subscriptions.
- Monitor whether you have allocated the right number of users.
- Monitor and manage how users are allocated.
See [Allocating users to a Per-User subscription](#).

**What to do next**

**Day-to-day administration: Monitor and manage subscriptions**

See [Monitoring how subscriptions are allocated](#).

**Subscription Management admin guide**

You use the ServiceNow® Subscription Management application to review and manage how purchased subscriptions are used on your production instance. You can monitor usage to update subscription levels and to make informed decisions about subscription purchases.

**What is a subscription?**

In contrast to companies that sell software licenses, ServiceNow sells subscription services.

- Your organization has purchased a subscription to an application family. The subscription entitles an agreed-upon number of users or resources in your organization to use the applications.
- For Per-User type subscriptions only, you allocate users to the subscription. As a result, the user is subscribed to the family of applications. For other subscription types, the instance auto-allocates users or resources to the subscription.
- For your organization to comply with its service contract, only subscribed users or resources should use a subscription application family.
- The Subscription Management application monitors your purchased subscriptions on production instances only.

**How do you use Subscription Management?**

The usage_admin can perform the following tasks:

- Receive and view subscriptions that your organization has purchased.
- Monitor and adjust allocation levels.
- Plan for renewing subscriptions.
- Determine which users (by role, by user group, or by some other criterion) should be subscribed to which Per-User subscription applications.
- Build user sets.
- Allocate users and user sets to each of the Per-User subscriptions.
- Manage user sets as users, roles, and groups change over time.

**View your subscription applications and allocation levels**

The **Subscriptions** page lists the subscriptions that your organization has purchased and indicates how many users or resources are allocated to each subscription.

Role required: usage_admin or admin

On your production ServiceNow instance, navigate to **Subscription Management** > **Subscriptions**.

© 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 page lists all subscriptions that your organization has purchased. Some subscriptions do not appear in the list. See *Why a subscription might not appear in the list*.

A color code indicates the allocation level. You can click a subscription **Name** to open the **Subscription** form, where you can:

- View or update how users are allocated to a Per-User subscription. See **Subscription form**
- **View the applications and plugins that are included with a subscription**

<table>
<thead>
<tr>
<th>All</th>
<th>Name</th>
<th>Type</th>
<th>Category</th>
<th>Start date</th>
<th>End date</th>
<th>Purchased</th>
<th>Allocated</th>
<th>Display only</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Financial Management</td>
<td>Per-User</td>
<td>ServiceNow</td>
<td>01.09.2015</td>
<td>10.10.2015</td>
<td>12</td>
<td>0</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td>ITA Fulfiller</td>
<td>Per-User</td>
<td>ServiceNow</td>
<td>01.09.2015</td>
<td>31.01.2016</td>
<td>60</td>
<td>59</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td>Facilities Service Automation</td>
<td>Max-User</td>
<td>ServiceNow</td>
<td>01.09.2015</td>
<td>10.10.2015</td>
<td>60</td>
<td>62</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td>StoreBusiness</td>
<td>Unlimited-User</td>
<td>Store Application</td>
<td>01.08.2015</td>
<td>31.01.2016</td>
<td>12</td>
<td>N/A</td>
<td>false</td>
</tr>
</tbody>
</table>

Headings on the **Subscriptions** list are described in **Subscription form**.

**Subscription form**

Use the **Subscription** form to view the list of applications that are associated with the subscription and to view or update how resources are allocated to a subscription.

In any list of subscriptions, click a subscription **Name** to open the **Subscription** form. Some fields do not appear for ServiceNow Store apps.

**Note:** There are several reasons that a subscription might not appear in the list. See *Why a subscription might not appear in the list*.

<table>
<thead>
<tr>
<th><strong>Fields on the Subscription form</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td><strong>Type</strong></td>
</tr>
<tr>
<td><strong>Category</strong></td>
</tr>
<tr>
<td>ServiceNow Jakarta Now Platform Capabilities</td>
</tr>
<tr>
<td>---------------------------------------------</td>
</tr>
<tr>
<td><strong>Start date / End date</strong></td>
</tr>
<tr>
<td>Start and end of the subscription period as agreed in your service contract. This information appears in the General section of the service contract for the subscription.</td>
</tr>
<tr>
<td><strong>Display only</strong></td>
</tr>
<tr>
<td>A value of true indicates that user allocation or monitoring is not currently supported for the subscription.</td>
</tr>
<tr>
<td><strong>Cost</strong></td>
</tr>
<tr>
<td>Denotes whether the subscription is <strong>For-fee</strong> or <strong>Free</strong>. Some ServiceNow Store apps are free. You do not allocate resources to free subscriptions.</td>
</tr>
<tr>
<td><strong>Purchased</strong></td>
</tr>
<tr>
<td>Number of users or other resources that can be subscribed.</td>
</tr>
<tr>
<td><strong>Allocated</strong></td>
</tr>
<tr>
<td>Number of currently subscribed users or allocated resources for the subscription. The color codes indicate the percentage of the subscription that has been used. See Configure the color codes for subscription allocation levels.</td>
</tr>
<tr>
<td><strong>Limit to purchased</strong></td>
</tr>
<tr>
<td>Select the check box to ensure that you do not exceed the purchased subscription limit while attempting to allocate users. The setting affects whether you can use the <strong>Allocate selected users</strong> action for users in the Pending state. Behavior when allocation would result in exceeding the purchased subscription limit:</td>
</tr>
<tr>
<td>- <strong>Limit to purchased</strong> selected: You cannot apply the <strong>Allocate selected users</strong> action on the <strong>Pending Users</strong> related list.</td>
</tr>
<tr>
<td>- <strong>Limit to purchased</strong> not selected: You can apply the <strong>Allocate selected users</strong> action on the <strong>Pending Users</strong> related list. The color code on the <strong>Allocated</strong> field changes to red to indicate over-allocation.</td>
</tr>
<tr>
<td><strong>Auto-sync user sets</strong></td>
</tr>
<tr>
<td>Select the check box to periodically check all associated user sets for updates (added or removed users) based on the user set membership settings and then update subscription allocation accordingly.</td>
</tr>
<tr>
<td><strong>Note:</strong> If adding a user would exceed the subscription limit, then the following actions happen:</td>
</tr>
<tr>
<td>- The user is not subscribed</td>
</tr>
<tr>
<td>- The user is set to Pending status</td>
</tr>
<tr>
<td>- The user is listed on the Pending Users related list</td>
</tr>
</tbody>
</table>
Related links on the Subscription form

- Subscription histories
- Histories of subscription users
- Histories of subscription user sets

View Subscription Management history reports

Related lists on the Subscription form

<table>
<thead>
<tr>
<th>Related list</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscribed Users</td>
<td>This list of users that are subscribed to the applications is populated only for Per-User subscriptions. The users were allocated to the subscription individually and/or are members of user sets that were added to the subscription.</td>
</tr>
<tr>
<td>User Sets</td>
<td>User sets that were added to the subscription.</td>
</tr>
<tr>
<td>Excluded Users</td>
<td>Appears only if there are users with Excluded status. Excluded users cannot be allocated to the subscription. See Exclude a user from a subscription and Remove a user from the Excluded list.</td>
</tr>
<tr>
<td>Subscription Applications</td>
<td>Applications or suites that are associated with the subscription. Users that you allocate to the subscription are subscribed to the listed applications. To view the list of plugins that are associated with an application, click the application Name.</td>
</tr>
<tr>
<td>Pending Users</td>
<td>Appears only if there are users with Pending status. When you try to allocate users to a subscription but the subscription limit would be exceeded, the users are not subscribed and are set to Pending status. You can then deallocate some users and allocate other users to the subscription. See Manage users with 'Pending' status.</td>
</tr>
<tr>
<td>Subscription Line Items</td>
<td>Applications that require subscriptions.</td>
</tr>
</tbody>
</table>

Types of subscriptions

The Subscriptions module lists all subscription types that your organization has purchased.

You allocate users only to Per-User subscriptions. Because the instance auto-allocates all other subscription types, no action is required on your part.
### Capacity

Your ServiceNow instance auto-allocates resources such as users, devices, software, or nodes to Capacity subscriptions. For example, resources like each CI that Discovery finds or each password reset request.

### Max User

Your organization purchased a subscription for the anticipated maximum number of active ServiceNow users. To monitor overall usage, the instance auto-allocates each active user up to the limit of the Max User subscription.

### PA Indicator

Your organization purchased a subscription for an application suite that uses Performance Analytics capabilities (for example, PA for ITSM or PA for Service Management). The PA admin creates indicators on tables that are used by the applications in the suite.

### Per-User

Your organization purchased a subscription for the number of fulfiller users for subscription applications and capabilities. By default, the instance can monitor and report on usage of the application by both subscribed users and users who are not subscribed.

See [Allocating users to a Per-User subscription](#).

### Unlimited

ServiceNow Store apps only. Your instance auto-allocates and tracks active users to an Unlimited subscription. There is no limit to the number of users that can be allocated. An active user is any user in the sys_user table that has a user id and has the Active field set to true.

---

**View the applications and plugins that are included with a subscription**

You can activate a plugin that is associated with a for-fee subscription only if your organization has purchased the subscription.

**Role required:** usage_admin or admin

1. On your production ServiceNow instance, navigate to **Subscription Management > Subscriptions**. The page lists all subscriptions that your organization has purchased.

   **Note:** If the subscription does not appear in the list, contact your ServiceNow account representative to purchase the subscription.

2. Click a subscription name and then, on the Subscription form, click an application name in the Subscription Applications related list. (A subscription can include multiple applications.) The page lists the plugins that are associated with the application.

**View Subscription Management history reports**

History reports give the usage_admin at-a-glance status and trends on subscription activity for an organization.

**Role required:** usage_admin or admin

1. Follow the **How to** instructions in the table.
**History reports**

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>How to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscription histories</td>
<td>Concise data on subscription downloads and updates for your organization.</td>
<td>1. Navigate to Subscription Management &gt; Subscriptions and then click a subscription Name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. On the Subscription form, click the View Subscription History related link.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. The Subscription History popup lists the operations on subscriptions for this ServiceNow instance. Click an Operation to view details.</td>
</tr>
<tr>
<td>Histories of subscription users</td>
<td>For each Per-User subscription, concise historical data on changes in</td>
<td>1. Navigate to Subscription Management &gt; Subscriptions and then click the Name of a Per-User subscription.</td>
</tr>
<tr>
<td></td>
<td>subscription status for users: when users were subscribed and when they</td>
<td>2. On the Subscription form, click the View User Subscription History related link.</td>
</tr>
<tr>
<td></td>
<td>were unsubscribed, excluded, or unexcluded.</td>
<td>3. The User Subscription History popup lists the operations on user subscription status for the specified subscription. Click a User State to view details of a change in subscription status for a user.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. <strong>User State:</strong> Lists the change in the user status: subscribed/unsubscribed and excluded/unexcluded.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. <strong>Allocation Source:</strong> Lists the name of the user set that acted as the source of the user.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. <strong>Allocation Type:</strong> Lists the method for allocating the user to the subscription: user set or individual.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. <strong>Operation time and Created by:</strong> Lists the timestamp of change and the admin who made the change.</td>
</tr>
<tr>
<td>Histories of subscription user sets</td>
<td>Data on when subscription user sets were created, updated, or deleted.</td>
<td>1. Navigate to Subscription Management &gt; Subscription User Sets and then click the Name of a user set.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. On the Subscription User Set page, click the View User Set History related link.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. The User Set History popup lists the operations on user sets for the specified subscription. Click an Operation to view details.</td>
</tr>
</tbody>
</table>
Why does my subscription not appear in the Subscriptions list?

- You might not see all subscription services that you have purchased because the Subscription Management application does not yet allow management of some subscription services.
- Subscription data arrives on production instances only.
- Self-hosted instances do not receive subscription information.
- Subscriptions that are marked as **Display only** do not currently support resource allocation or monitoring.

Why is the Subscriptions list empty?

- The subscription information might not yet have arrived. The data is downloaded daily.

Allocating users to a Per-User subscription

You, the usage admin, use the Subscriptions module to allocate users to the Per-User type subscriptions that your organization has purchased.

Example: allocate users to a Per-User subscription

In this example, your organization purchased a subscription for 200 fulfiller users. You can therefore specify the 200 users—the **subscribed users**—who have the right to use the subscription application and features on your production instance. You can allocate users either individually or by adding user sets to the subscription.

**Note:** User sets are the preferred automated method for managing the pool of users who are subscribed to an application. Once you configure and allocate a user set, the system regularly updates the list of members based on the conditions that you specified. You do not need to manage individual users.
The subscription admin allocates a mix of user sets and individual users to the 200-user subscription.

The 200 users that the admin allocated to the subscription are now subscribed to the application.
Guidelines for allocating users

- You allocate users only to Per-User subscriptions. The instance automatically reports on monthly usage for all other subscription types.
- When you add a user set to a subscription, the system allocates all users in the user set, up to the purchased subscription limit.
- In the case that adding the users in a user set would exceed the subscription limit, then none of the users in the user set are subscribed. Instead, all users in the user set are set to Pending status and are listed on the Pending Users related list. Users that are currently subscribed are not affected. See Manage users with Pending status.
- You can unsubscribe any user as needed.
- You can exclude users. Excluded users cannot be allocated to a subscription individually or through a user set. At any time, you can remove a user from the list of excluded users.

Note: If you unsubscribe a user who is a member of a user set that is associated with an auto-synced subscription, the user will be resubscribed in the next synchronization cycle. To remove such a user, exclude the user. See Exclude a user from a subscription.

Methods for allocating users

- Define user sets and then add user sets to the subscription
- Allocate individual users to the subscription (as many as are required)

Overview of the procedure for allocating users

1. Allocate users to the subscription using one or both of the following methods:
   - Build one or more user sets and add the user sets to the subscription
   - Allocate individual users

2. After you have allocated users to the subscription, you can add or remove user sets and individual users as needed. In addition, you can exclude individual users as needed.

Subscription user sets

You define the criteria for a user to become a member of a user set (for example, all fulfiller users in the IT department). When you add a user set to a subscription, the system attempts to subscribe all users in the user set.

Auto-sync

The system updates the members in a user set whenever a user update causes the user to meet or fail to meet the criteria for the user set. For example, if a user loses the “fulfiller user” role, the user is removed from the user set.

To make subscriptions self-maintaining, you can auto-sync a subscription. The system then regularly subscribes or unsubscribes users based on updates to the user sets that are assigned to the subscription. The option is described in Auto-sync a subscription to user set updates.
Note: Even if you select the *Auto-sync with user sets* option, you can update, remove, or manually synchronize the user set at any time.

---

**How users are subscribed and unsubscribed**

- When you *add a user set* to a subscription, the system allocates all users in the user set to the subscription, up to the purchased subscription limit.
- You can add a user set to any number of subscriptions.
- Users that are allocated from multiple user sets are subscribed only one time.
- In the case that adding the users would exceed the subscription limit, then none of the users in the user set are subscribed. Instead, all users in the user set are set to `Pending` status and are listed in the Pending Users related list.
- When you remove a user set from a subscription, the system attempts to unsubscribe all users in the set. If a user is added from another user set, however, the user is not unsubscribed.
- Users that the usage admin has flagged as *excluded* are not allocated, even if other members of the user set are allocated. The usage admin can *unexclude* a user so that the user can be allocated.

**Why a user is not subscribed when you add a user set**

- The user set is empty (contains no users).
- The user had been excluded from the subscription.
- The user had already been directly allocated
- Another user set added the user (duplicate user)
- A user could not be allocated because adding the user would exceed the subscription limit. In this case, all users in the user set are set to Pending status. The names of the users are listed in the Pending Users related list.

**Why a user is not unsubscribed when you remove a user set**

- The user set is empty (contains no users).
- The user was already directly allocated
- The user is added from another user set

---

**Build a subscription user set**

You can create a user set using either of two methods: Configure a filter that selects particular users from the `User (sys_user)` table or specify a particular set of user groups from the `Group (sys_user_group)` table.

Role required: usage_admin or admin

1. Open the **Subscription User Sets** page: Navigate to **Subscription Management > Subscription User Sets**.
2. Click **New** and then enter a unique **Name** (for example, *Fulfiller users in the IT department*) and **Description** for the user set.
3. Use one of the following methods to specify the **Source** of the users that you will add to the user set:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User (sys_user)</td>
<td>The <strong>Conditions</strong> setting is a standard ServiceNow condition builder.</td>
</tr>
<tr>
<td></td>
<td>1. Specify the filters that determine which users to extract from the table. The extracted users make up the user set. For example, filter for (role) (is) (itil).</td>
</tr>
<tr>
<td></td>
<td>2. Click 🌐 to view the number of users that the filter generates.</td>
</tr>
<tr>
<td>Group (sys_user_group)</td>
<td>Unlock the Groups box and add appropriate groups.</td>
</tr>
</tbody>
</table>

4. When the list is correct, click **Submit** or **Update**. The user set that you created is available to add to any subscription.

**Add a user set to a subscription**
When you add a user set to a subscription, all users in the user set are allocated to the subscription.

Role required: usage_admin or admin

1. Navigate to **Subscription Management > Subscriptions**.
2. Click the **Name** of the Per-User subscription to allocate users to.
3. On the **User Sets** related list, click **Edit**.
4. The Add User Sets form displays the list of user sets that you can add. Move the desired user sets from the **Collection** list into the **User Sets** list and then click **Save**.

The users in the list are allocated to the subscription and the number of subscribed users is updated.

**Note:** In the case that adding the users would exceed the subscription limit, then none of the users in the user set are subscribed. Instead, all users in the user set are set to **Pending** status and are listed in the Pending Users related list. Currently subscribed users who were individually subscribed or in other users sets are not affected. See **Manage users with 'Pending' status**.

5. Optional: You can configure any subscription to check associated user sets for updates regularly and then update the list of subscribed users accordingly. On the Subscription form, select **Auto-sync with user sets**.

**Note:** If you do not select the **Auto-sync with user sets** option, then the user sets that you add to the subscription are never updated and the list of subscribed users does not auto-update over time.

6. On the Subscription form, click **Update**.

**Auto-sync a subscription to user set updates**
You can configure any subscription to check user sets regularly to find users who were added or removed. The system then regularly subscribes or unsubscribes users based on updates to user sets.

Role required: usage_admin or admin
If the system cannot allocate a user because adding the user would exceed the subscription limit, the user is set to Pending status and is listed in the **Pending Users** related list.

1. Navigate to **Subscription Management** > **Subscriptions**.
2. Click the **Name** of the Per-User subscription to update.
3. On the **Subscription** form, select **Auto-sync user sets**.
4. Optional: On the **Subscription** form, click **Sync Now** to synchronize and update the list of subscribed users immediately.

**Remove a user set from a subscription**

When you remove a user set from a subscription, the system attempts to unsubscribe all users in the set. User sets are removed regardless of the **Auto-sync with user sets** setting.

Role required: **usage_admin or admin**

1. Navigate to **Subscription Management** > **Subscriptions**.
2. Click the **Name** of the Per-User subscription.
3. In the **User Sets** list, select all user sets to remove.
4. In the **Actions on selected rows** list, select **Remove From Subscription**. On the Remove User Set from Subscription pop-up, click **Remove**.
   
   All users in the selected user sets are unsubscribed. If users in the user sets are pending, then the users are removed from the Pending Users list.

**Delete a subscription user set**

You can delete a subscription user set only if no subscriptions use the user set.

Role required: **usage_admin or admin**

   **Note:** Deleting a user set is a permanent action—the user set will no longer exist. In contrast, you can remove a user set from a subscription to unsubscribe all users in the user set—the user set will still exist.

1. Ensure that the user set is not used by any subscription.
2. Navigate to **Subscription Management** > **Subscription User Sets** and select the user set.
3. Click **Delete**.

**Allocate an individual user from the Subscription form**

In addition to adding user sets to a subscription, you can add individual users directly. Users that you allocate directly are subscribed immediately.

Role required: **usage_admin or admin**

   **Note:** A user set, not individual allocation, is the preferred automated method for managing the pool of users who should be subscribed to an application. Once you configure and allocate a user set, you do not need to manage individual users.

1. Navigate to **Subscription Management** > **Subscriptions**.
2. Click the **Name** of the Per-User subscription to allocate users to.

3. Optional: To ensure that you do not exceed the purchased subscription limit, click **Limit to purchased**.

4. On the **Subscribed Users** related list, click **Edit**.

5. The form displays the list of users that you can add. Move the desired users from the **Collection** list into the **Subscribed Users** list and then click **Save**.

   The selected users are allocated to the subscription and the **Allocated** value is updated. If allocating a user would exceed the subscription limit, the user is not subscribed. Instead, the user is set to Pending status and is listed in the Pending Users related list. See [Manage users with 'Pending' status](#).

6. Click **Update** on the **Subscription** form.

### Allocate an individual user from the User Record form

To simplify the process of setting up user capabilities, you can allocate or deallocate an individual user to a subscription while viewing the user data on the User form. Users that you allocate directly are subscribed immediately.

**Role required:** usage_admin or admin

**Note:** A user set, not individual allocation, is the preferred automated method for managing the pool of users who should be subscribed to an application. Once you configure and allocate a user set, you do not need to manage individual users.

1. Navigate to **User Administration > Users** and then click the **Name** of the user. The User form opens.

2. On the **Manage Subscriptions** related list, click **Edit**.

3. The Edit Members slushbucket lists the subscriptions that you can allocate the user to. To allocate the user, move a subscription from the **Collection** list into the **Manage Subscriptions** list and then click **Save**.
The user is allocated to the subscription and the **Allocated** value is updated. If allocating a user would exceed the subscription limit, the user is not allocated. Instead, the user is set to Pending status and is listed in the Pending Users related list on the Subscription form. See *Manage users with 'Pending' status*.

To deallocate the user, move a subscription from the Manage Subscriptions list into the Collection list.

4. Click **Update** on the **User** form.
   
   The **Subscriptions** related list is updated to list all subscriptions that the user is allocated to and the applications that the user is subscribed to.

---

**Manage users with 'Pending' status**

Users are set to Pending status when adding the users would exceed the subscription limit (the **Purchased** value).

**Role required:** usage_admin or admin

Users are added to the Pending Users list when you attempt to allocate users in the following situations:

- User sets: If adding the user set exceeds the subscription limit, the user set is not added and all users in the set are set to Pending status.
- Individual user: If allocating a user directly would exceed the subscription limit, the user is not subscribed and is instead set to Pending status.

1. Navigate to **Subscription Management** > **Subscriptions**.
2. Click the **Name** of the Per-User subscription.
3. In the Pending Users related list, select all users to update.
4. In the **Actions on selected rows** list, select an action.

<table>
<thead>
<tr>
<th>Action</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allocate selected users</td>
<td>Allocates the users to the subscription and removes the user from the Pending Users list.</td>
</tr>
<tr>
<td></td>
<td>• If the <strong>Limit to purchased</strong> option is selected and adding the selected users would exceed the subscription limit (the <strong>Purchased</strong> value), then the action is not allowed.</td>
</tr>
<tr>
<td></td>
<td>• If the <strong>Limit to purchased</strong> option is not selected and adding the selected users would exceed the subscription limit (the <strong>Purchased</strong> value), then the system displays a popup to notify you.</td>
</tr>
<tr>
<td>Exclude from subscription</td>
<td>Excludes the user and removes the user from the Pending Users list.</td>
</tr>
<tr>
<td></td>
<td>Excluded users cannot be allocated to the selected subscription. The auto-sync process does not add excluded users.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes the selected users from the Pending Users list and performs no other action.</td>
</tr>
</tbody>
</table>

---

**Unsubscribe a user**

When you remove a user from a subscription, the user is unsubscribed.
Role required: usage_admin or admin

1. Navigate to Subscription Management > Subscriptions.
2. Click the Name of the Per-User subscription.
3. In the Subscribed Users list, select all users to unsubscribe.
4. In the Actions on selected rows list, select Remove from subscription and then click Remove on the pop-up.

**Note:** If you unsubscribe a user who is a member of a user set that is associated with an auto-synched subscription, the user will be resubscribed in the next synchronization cycle. To remove such a user, exclude the user.

---

### Exclude a user from a subscription

You can exclude users. Excluded users cannot be allocated to a specified subscription. The auto-sync process does not add excluded users.

Role required: usage_admin or admin

1. Navigate to Subscription Management > Subscriptions.
2. Click the Name of the Per-User subscription.
3. In the Subscribed Users list, select all users to exclude.
4. In the Actions on selected rows list, select Exclude from subscription and then click Exclude on the popup.

### Remove a user from the Excluded list

You can unexclude a user so that the user can be allocated to a subscription.

Role required: usage_admin or admin

1. Navigate to Subscription Management > Subscriptions.
2. Click the Name of the Per-User subscription.
3. In the Excluded Users related list, select all users to unexclude.
4. In the Actions on selected rows list, select Delete and then click Delete on the pop-up.

The selected users are no longer excluded and are removed from the Excluded Users related list. No other action is taken.

**Note:** The users are not yet allocated to the subscription. You must manually add the users or synchronize the associated update set. On the Subscription form, click Sync Now to synchronize and update the list of subscribed users immediately.

### Monitoring how subscriptions are allocated

You, the usage admin, use the Subscriptions module to allocate users to the Per-User subscriptions that your organization has purchased.
Subscription life cycle

1. Receive and view subscriptions
   - Your instance downloads subscription information and notifies you by email. Now you can review the subscriptions to decide which actions to take.

2. Allocate users to subscriptions

3. Monitor and adjust subscribed users

4. Plan for renewing subscriptions

5. Review the subscriptions that your organization has purchased

Subscription Management tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Module to use to perform the task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive and view subscriptions</td>
<td>Your instance downloads subscription information and notifies you by email. Now you can review the subscriptions to decide which actions to take.</td>
<td>Subscriptions module: <a href="#">View your subscription applications and allocation levels</a></td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
<td>Module to use to perform the task</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Allocate users                         | You allocate fulfiller users to Per-User subscriptions. (The ServiceNow instance auto-allocates all other subscription types.) Allocation is typically a one-time task with minor maintenance.                                                                                                           | Subscriptions module:  
                      **Allocating users to a Per-User subscription**                                                                                                                                   |
| Monitor and adjust                     | You monitor usage of subscriptions: How many subscribed users, can you allocate more users, are there users who are not subscribed (out-of-policy users), and so on. As needed, reallocate users.                                                                                                                        | Subscription Overview module:  
                      **Monitor how resources are allocated to subscriptions**  
                      **Compliance Overview module:**  
                      **Monitor subscription compliance**                                                                                                                                          |
| Plan for renewing subscriptions        | Review historical activity to prepare to renew subscriptions: How have usage patterns changed over time, is there high demand for a particular application, and so on.                                                                                                                            | Subscriptions module:  
                      **View your subscription applications and allocation levels**  
                      **View Subscription Management history reports**                                                                                                                                  |
| Review the subscriptions that your organization has purchased | View the list of all types of subscriptions and check allocation levels at a glance.                                                                                                                                                                                                 | Subscriptions module:  
                      **View your subscription applications and allocation levels**                                                                                                                     |

**Monitor how resources are allocated to subscriptions**

Use the Subscription Overview module to monitor how users and resources are allocated to subscriptions.

Role required: usage_admin or admin

The system displays one chart for each subscription. You can:

- Monitor how resources (for example, discovered nodes or password reset requests) use Capacity subscriptions.
- Plan and budget for upcoming or future subscription needs.
- Assess whether you have allocated too many fulfiller users to a Per-User subscription. You might reallocate some users or purchase a subscription for more users.
- Assess whether you have allocated too few fulfiller users to a Per-User subscription. You might allocate more users.
- Determine whether users who are not subscribed are accessing a subscription application.

Navigate to **Subscription Management > Subscription Overview**. The **Expired Subscriptions** report lists all subscriptions where the service contract term has expired (the end date has passed). You should assess whether to renew any subscription that has expired.

Each **Subscription Metrics** chart displays the following data for a single subscription (at least one month of data is required):

- **Purchased**: The number of resources purchased for the subscription.
- **Allocated**: The average number of users for the month who have been allocated to the subscription.
- **Non-subscribed users**: The average number of individual users who performed fulfiller actions in the associated applications without being subscribed to the applications. Click a data point to view the application.

In the example, the organization updated the purchased subscription from 15 to 20 users in November 2015. Over the course of April 2016, the usage admin had allocated an average of about 19 users. In addition during the period, one user who was not subscribed performed fulfiller actions in an application associated with the subscription.
Monitor subscription compliance

Use the Compliance Overview module to monitor fulfiller actions by subscribed users and by users who are not subscribed to an application that your organization has purchased. In addition, a chart shows usage for applications where your organization has not yet purchased a subscription.

Role required: usage_admin or admin

Navigate to Subscription Management > Compliance Overview to view the charts:

- The Unique Application Users chart shows the number of individual subscribed users who performed fulfiller actions in the application. Each user is counted one time only, regardless of number of accesses.
- The Unique Out-of-Policy Users chart shows the number of individual users who performed fulfiller actions in the application without being subscribed to the application. Each user is counted one time only, regardless of number of accesses. This chart might alert you to users in the Pending state or users who are accessing the application without being subscribed.
- The Application Use Without a Purchased Subscription chart shows the number of users who performed fulfiller actions in an application even though your organization has not purchased a subscription for the application.

Configure the color codes for subscription allocation levels

On lists, forms, and charts, a configurable color code indicates the percentage of the subscription that has been allocated.

Role required: usage_admin or admin

In this example, you have not yet allocated users to the Financial Management application.

1. Navigate to Subscription Management > Properties.
2. Update the **Threshold for color codes** (subscription.used.thresh) property setting and then click **Save**.
   Specify a percentage value greater than 0 and less than 100. Default: 90% of the purchased subscription limit.
   - Subscription allocation levels below the specified threshold are marked with a green color code.
   - Allocation levels between the threshold and 100% are marked yellow.
   - Allocation levels above 100% are marked red.

**Survey Management**

With the ServiceNow® Survey Management application you can create, send, and collect responses for basic surveys. If installed, you can also use the Survey widget to set up a survey within Service Portal.

- **Explore**
  - Assessments and Surveys release notes
  - Upgrade to Jakarta
  - Get started with Survey Management
  - Key survey terms

- **Set up**
  - Survey Management roles

- **Administer**
  - Survey designer
  - Survey users and groups
  - Customize the appearance of a survey
  - Survey definitions
  - Survey trigger conditions

- **Use**
  - View the results for a survey
  - View results for all surveys
  - Metric result fields
  - View a survey scorecard
  - Survey questionnaires

- **Develop**
  - Developer training
  - Developer documentation

- **Migrate**
  - Legacy survey migration

**Get started with Survey Management**

Two versions of the application are supported, Survey Management, which is the latest version, and Legacy Surveys. Survey Management improves the user interface and extends the capabilities of the Legacy Surveys application.

Survey Management does not support domain separation.

**Configuring surveys**

There are many options for advanced configuration in Survey Management:
• Create a survey, add questions, and choose recipients, all in one interface.
• Create conditional questions, which appear only when users answer other questions a certain way.
• Restrict a survey so only specific survey users can take it, and send invitations to those users simultaneously. Alternatively, make the survey a public survey so that any user can take the survey, even users who have not logged in to the ServiceNow system.
• Set a schedule to automatically assign a survey to users and to limit how often the same user can take a survey.
• Customize the look and feel of survey questionnaires.
• Save anonymous survey responses.
• Convert survey responses to numerical scores and view them on scorecards.
• Deactivate a survey for maintenance or to retire it without deleting it.

**Note:** Because surveys use the same tables and other back-end components as assessments, you may see assessment elements such as table and field names in certain places throughout the survey feature.

**Legacy Surveys**

Survey administrators can continue to use legacy survey functionality and data, however, it is recommended that you migrate legacy surveys to the Survey Management application. Concurrent use of both survey applications can cause confusion and redundancy.

Survey wizards are not impacted and cannot be migrated.

**Note:** The Legacy Surveys application is not described in the documentation that you are viewing. It is documented on the ServiceNow wiki.

**Version comparison**

<table>
<thead>
<tr>
<th>Capability</th>
<th>Surveys</th>
<th>Legacy Surveys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Surveys in Service Portal.</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Save new survey responses each time a user takes the same survey.</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Create question templates to reuse sets of answer options.</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Categorize survey questions and report on category results.</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Deactivate a survey without deleting it.</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Create conditional questions.</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Send surveys automatically based on a schedule.</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Capability</td>
<td>Surveys</td>
<td>Legacy Surveys</td>
</tr>
<tr>
<td>------------</td>
<td>---------</td>
<td>----------------</td>
</tr>
<tr>
<td>Customize survey questionnaire color scheme.</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Save anonymous survey responses for logged-in users.</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>View survey responses on graphical scorecards.</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Save surveys in a draft state until they are ready to publish.</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Create and send surveys from one page.</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Allow only specific users to access a survey.</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Send surveys based on conditions.</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Send survey email notifications.</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Limit how often a user can take the same survey.</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Add introduction and end note text.</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Create survey modules.</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Public survey: Allow persons to take a survey without logging in.</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Use update sets to track changes.</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

**Survey Management roles**

The Survey Management application uses the following roles.

No role is required to take assigned survey questionnaires.
Survey Management roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
<th>Contains roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Survey administrator</td>
<td>Create and administer surveys. Survey administrators know what types of</td>
<td>• survey_reader</td>
</tr>
<tr>
<td>(survey_admin)</td>
<td>surveys are necessary, when to send a survey, and to whom. Survey administrators</td>
<td>• assessment_admin</td>
</tr>
<tr>
<td></td>
<td>can use all modules in the Survey application menu.</td>
<td></td>
</tr>
<tr>
<td>Survey reader</td>
<td>View surveys and related information, such as survey responses, survey</td>
<td>none</td>
</tr>
<tr>
<td>survey_reader</td>
<td>groups, scorecards, and reports.</td>
<td></td>
</tr>
</tbody>
</table>

Key survey terms

These survey terms are used throughout the documentation to describe survey management functions and capabilities.

Key survey terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Survey definition</td>
<td>Root record on which a survey is built. A survey definition contains information such as the survey name, state, and distribution schedule. Each survey definition has its own categories and questions. Survey definitions are comparable to legacy survey masters.</td>
</tr>
<tr>
<td>Public survey</td>
<td>Any user can take a public survey, even users who have not logged in to the ServiceNow system. For a completed survey, the Assigned to field value is Guest.</td>
</tr>
<tr>
<td>Survey category</td>
<td>Represents a theme for survey questions. Categories contain one or more questions. The system creates one category per survey by default. Additional categories are optional.</td>
</tr>
<tr>
<td>Survey question</td>
<td>A question that appears on a survey questionnaire for the associated survey definition. Survey questions are comparable to legacy survey questions.</td>
</tr>
<tr>
<td>Survey user</td>
<td>User who is authorized to receive invitations for a restricted survey.</td>
</tr>
<tr>
<td>Survey instance</td>
<td>Represents one survey questionnaire assigned to one user. Survey instances are comparable to legacy survey instances.</td>
</tr>
</tbody>
</table>
### Survey questionnaires

All surveys that are assigned to you appear in your personal assessment and survey queue. No special role is required to complete a survey but you must be logged in and the survey must be assigned to you. When you submit a survey, the system stores your responses.

### Survey notification

If the system is configured to send email, it sends you a notification when a survey is assigned to you. The message contains a link to the survey and instructions for viewing the assessment and survey queue.

### Take a survey

Surveys that are assigned to you, and that are not complete, appear in your assessment and survey queue.

Role required: none

Each assessment or survey appears as a card in the queue. The card contains helpful information, including the survey name, state, and due date, and a button to launch the questionnaire. Overdue surveys are clearly marked with a red icon and red due date. You must answer every mandatory question, indicated by a red asterisk, before you can submit the survey. If you start to take a survey but cannot complete it, save your responses and return to it later. When you have answered all the questions and are satisfied with the responses, submit the survey.

1. Navigate to **Self-Service > My Assessments & Surveys**.
   Users with the assessment_admin role, including survey administrators, can display other users' assessments and surveys in addition to their own. Use the **Show all** and **Show assigned to me** related links at the bottom of the queue to show and hide assessments and surveys. Click a card assigned to another user to open the associated metric type or survey definition.

2. Click **Take Survey** on a survey card to open the questionnaire.
   If there is more than one survey category, you can click the collapse or expand icon to hide or show the questions in the category.

3. Answer each question to the best of your ability.
   If you are unsure of how to respond to a question or if a question does not apply to a particular record, select **Not Applicable**, if available.

4. Complete one of the following steps.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save your responses without submitting them</td>
<td>Click <strong>Save</strong>. You can close the questionnaire and access it later from your queue. Note: The system does not save the survey if there are invalid responses, such as a letter in a date field. You must enter valid responses or remove invalid responses before you can save the survey.</td>
</tr>
<tr>
<td>Submit the survey after answering all questions</td>
<td>Click <strong>Submit</strong>. You cannot return to the questionnaire after submitting. Note: If there is an unanswered mandatory question or an invalid response, an error message appears and the problematic questions are temporarily highlighted.</td>
</tr>
</tbody>
</table>

**Survey responses and results**

There is a metric result record for each user response to each question on every survey instance. Survey results for each question and category are calculated automatically based on the metric result records.

If you use survey result calculations for results and scorecards, ensure that the **positive indicator** field for the question is set appropriately, based on the answer options. To have any results, a category must contain scored questions.

**Survey responses**

Survey responses are stored in the Metric Result (asmt_metric_result) table and display the recipients' answers to each question in a category. To view general results, navigate to **Survey > Survey Responses**. To view results for a particular criterion, use a filter on the Metric Result (asmt_metric_result) table. For example, to view results based on the assignment group, apply a filter condition for assignment group.
Category results are stored in the Assessment Category Result (asmt_category_result) table and display the overall ratings for each category based on the weighted value for each scored question. To view these results, navigate to Assessments > Results > Category results and filter the results using the (Type.Evaluation method) (is) (Survey) condition.
Assessment category results

Survey scorecards

A scorecard provides a visual breakdown of survey responses, based on the way questions were answered, by category. To access a scorecard, see View a survey scorecard.

View results for all surveys

You can view the survey responses that are stored on the Metric Result (asmt_metric_result) table.

Role required: survey_admin or survey_reader

1. Navigate to Survey > Survey Responses.
   Do not confuse this module with Survey > Legacy Surveys > Survey Responses, which displays legacy survey responses.

   The Type column displays the survey definition each response is associated with.
2. Select a response to view its details.

**View the results for a survey**

You can view the responses for one survey definition. Survey results are stored on the Metric Result (asmt_metric_result) table.

Role required: survey_admin or survey_reader

1. Navigate to Survey > View Surveys
2. Open a survey definition.
3. Under Related Links, click View Responses, which is available only if there are results.
   The results are grouped by metric, which is what questions are called in assessments.
4. Open a metric result to view more detail.
   The metric result contains the user's response and calculated values of interest to advanced survey administrators. Because the Metric Result table is also used by the assessment feature, many field names are not clear in the context of surveys.

**Metric result fields**

List of field descriptions for the Metric Result form.
## Metric Result form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment group</td>
<td>Assessment group to which the metric result belongs. An assessment group is a container for survey instances and results generated in a single occurrence. The system generates an assessment group every time at least one survey instance is created. If multiple survey instances are created at once, such as when a survey administrator sends invitations to a list of survey users, they are all stored in the same assessment group.</td>
</tr>
<tr>
<td>Metric</td>
<td>Question that the user answered.</td>
</tr>
<tr>
<td>Data type</td>
<td>Data type of the question the user answered.</td>
</tr>
<tr>
<td>Method</td>
<td>Assessment method. Always Assessment for surveys.</td>
</tr>
<tr>
<td>Updated</td>
<td>Date and time the metric result was last updated.</td>
</tr>
<tr>
<td>Source</td>
<td>Survey definition from which the associated survey instance was generated.</td>
</tr>
<tr>
<td>Assigned to</td>
<td>User who completed the survey questionnaire.</td>
</tr>
<tr>
<td>Instance</td>
<td>Survey instance completed by the Assigned to user.</td>
</tr>
<tr>
<td>Actual value</td>
<td>Value obtained from the user response to the question. The actual value is determined by the question data type:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Checkbox</strong>: The actual value is 0 if the checkbox is cleared and 1 if it is selected.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Choice</strong> or <strong>Likert Scale</strong>: The actual value is equal to the <strong>Value</strong> of the metric definition associated with the chosen answer option.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Date</strong>, <strong>Date/Time</strong>, or <strong>String</strong>: The actual value is -1 to indicate that these data types do not contribute to category result calculations.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Template</strong>: The actual value is equal to the <strong>Value</strong> of the template definition associated with the chosen answer option.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Yes/No</strong>: The actual value is 0 if the response is No and 1 if it is Yes.</td>
</tr>
<tr>
<td>Normalized value</td>
<td>Adjusted value that accounts for the <strong>Scale definition</strong> setting, minimum and maximum values, and other factors.</td>
</tr>
<tr>
<td></td>
<td>The equation that generates the value and an example calculation appear in <strong>Example: calculate the normalized value for a survey metric.</strong></td>
</tr>
<tr>
<td>String value</td>
<td>Value that displays the response as it appears on a questionnaire. In some cases this is the same as the <strong>Actual value</strong>, such as when the question data type is <strong>Percentage</strong>. The string value is <strong>N/A</strong> for unanswered questions of certain data types.</td>
</tr>
</tbody>
</table>
**Example: calculate the normalized value for a survey metric**

The normalized value is calculated based on a linear equation and the scale definition of the metric.

**Equation used to calculate the normalized value**

\[
\text{Normalized value} = \frac{(\text{Input Value} - \text{Min value defined in metric})}{(\text{Max value defined in metric} - \text{Min value defined in metric})} \times \frac{\text{current metric weight}}{\text{sum of valid metric weight}} \times \text{scale_factor}
\]

**Note:** The normalized values are directly proportional to the scale definition of the metric. If the scale definition is low, that is, the lower scale values are better, then Normalized value = 1.0 - Normalized value.

**Example**

Calculate the normalized value for the **Please rate the competency of the technician** metric. The metric has the following values:

<table>
<thead>
<tr>
<th>Values of the metric</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Input value</td>
<td>3</td>
</tr>
<tr>
<td>Minimum value</td>
<td>1</td>
</tr>
<tr>
<td>Maximum value</td>
<td>6</td>
</tr>
<tr>
<td>Current metric weight</td>
<td>10</td>
</tr>
<tr>
<td>Number of responses</td>
<td>6</td>
</tr>
<tr>
<td>- 4 of type=number</td>
<td></td>
</tr>
<tr>
<td>- 1 of type=yes/no</td>
<td></td>
</tr>
<tr>
<td>- 1 of type=string (invalid data type; value cannot be calculated)</td>
<td></td>
</tr>
<tr>
<td>Valid metric weight of each response</td>
<td>10</td>
</tr>
<tr>
<td>Scale factor</td>
<td>10</td>
</tr>
</tbody>
</table>

\[
\text{Normalized value} = \frac{(3 - 1)}{(6 - 1)} \times \frac{10}{(10 + 10 + 10 + 10 + 10)} \times 10 = 0.8
\]

Several data types are ignored because the values cannot be calculated. These invalid data types include string, date, and datetime.

For reporting purposes, use the Metric Result (asmt_metric_result) table.

**View a survey scorecard**

A survey scorecard provides a visual breakdown of survey responses by category, based on the way questions were answered.

Role required: survey_admin or survey_reader
A scorecard displays charts for survey results, in which category and question responses are analyzed and current ratings are compared with previous ratings. Users can examine ratings over time, compare question ratings, or compare the ratings of all categories. All ratings are averages for the time range selected. The system dynamically updates a scorecard each time you view it, so the ratings reflect recently completed surveys.

1. Navigate to Survey > View Surveys.
2. Open a survey definition.
   The scorecard link is hidden if there are no survey results to report.

The interactive scorecard displays the name of the survey and results or comparisons of the ratings. You can display results in the following views:

- Category Results
- Question Results
- Average Ratings
- History

**Survey scorecard category results**

The Category Results view is a stacked bar chart showing survey results for all questions in a category by respondent count.

Select a category from the list to display the questions from that category in the chart.

This view displays responses that use the following data types:

- Checkbox
- Choice
- Likert Scale
- Number
- Template
- Yes/No

---

**Note:** The Checkbox and Yes/No data types are combined into the Boolean data type in the Survey Designer.
To view details about a specific response, point to the colored bar to display the response, the number of responses, and the percentage it represents of all the responses to that question.

Survey scorecard category results detail

Survey scorecard question results
The Question Results view shows the results for each question in a category using different chart types, based on a data type.

Pie chart
The pie chart shows question results for these data types:

- Checkbox
- Choice
- Likert Scale
- Number
- Template
- Yes/No

**Note:** The Checkbox and Yes/No data types are combined into the **Boolean** data type in the Survey Designer.
Service Desk Satisfaction Survey

Survey Scorecard

How courteous and respectful was the technician who responded? (1=poor, 6=excellent)

2 = 2 (14.29%)  3 = 2 (14.29%)  4 = 9 (54.29%)  5 = 1 (7.14%)
Bar chart

A bar chart appears when question results use the Percentage data type. By default, all results for percentage questions use a report range of 20% segments. To configure a report range, navigate to Reports > Administration > Report Ranges.

Survey scorecard average ratings

The Average Ratings view displays the weighted average rating for each survey question in a category. Use this view to learn how individual questions affect the overall rating for the category. Select a survey category from the choice list to display the chart for that category.
Service Desk Satisfaction Survey

Survey Scorecard

Average question rating in category: Service Desk Satisfaction Survey

- How courteous and...
- How satisfied are...
- How satisfied were...
- Please rate the t...
- Was technician ab...

Average Normalized value
To view the effect of each question’s ratings on the entire category’s ratings, point to the colored bar. The pop-up box shows the percentage of the total ratings represented by each individual question’s weighted average.

**Average ratings detail**

**Survey scorecard history**

The History view compares the current ratings for the categories and their questions with ratings from the previous three years or four quarters.

Ratings that have declined are highlighted in red and display negative numbers. Ratings that have improved are highlighted in green with positive numbers. Arrow icons beside the values in the Diff column indicate the trend of the current survey against the previous survey.

Point to a category to display a line chart that shows the rating trend for that category. Click a category to view the Survey Category form containing the survey questions.
Survey scorecard trend chart

3 years

To calculate the current ratings, the system averages the ratings from the trailing twelve month (TTM) period. The Diff column shows the discrepancy between the current ratings and the previous calendar year’s ratings.
<table>
<thead>
<tr>
<th>Survey Scorecard</th>
<th>Overall Rating</th>
<th>Current</th>
<th>Diff</th>
<th>2013</th>
<th>2012</th>
<th>2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Desk Satisfaction Survey</td>
<td>5.40</td>
<td>0.00</td>
<td>5.40</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>How satisfied were you with the response time to your incident? (1=not at all, 6=completely)</td>
<td>5.40</td>
<td>-1.02</td>
<td>1.02</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>How courteous and respectful was the technician who responded? (1=poor, 6=excellent)</td>
<td>5.40</td>
<td>-1.21</td>
<td>1.21</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>Please rate the technical competency of the technician serving you (1=poor, 6=excellent)</td>
<td>5.40</td>
<td>-1.02</td>
<td>1.02</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>Was technician able to resolve your issue during the first call?</td>
<td>5.40</td>
<td>-1.00</td>
<td>1.00</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>How satisfied are you with your overall service experience? (1=not at all, 6=completely)</td>
<td>5.40</td>
<td>-1.14</td>
<td>1.14</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
</tr>
</tbody>
</table>

Survey scorecard history - 3 years
4 quarters

Quarterly surveys compare the average rating for each question and category in the current quarter against the average ratings from the previous four quarters. The **Diff** column shows the discrepancy between the current ratings and the previous quarter's ratings. The column labels count backward, by quarter from the current quarter. For example, if the current quarter is the 3rd quarter of 2015, then the previous quarters appear as 2nd (2015), 1st (2015), 4th (2014), and 3rd (2014). All four of the previous quarters appear, whether or not there was any data for those quarters.
### Service Desk Satisfaction Survey

#### Survey Scorecard

<table>
<thead>
<tr>
<th>Overall Rating</th>
<th>Current</th>
<th>Diff</th>
<th>1st</th>
<th>4th</th>
<th>3rd</th>
<th>2nd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Desk Satisfaction Survey</td>
<td>0.00</td>
<td>-5.40</td>
<td>5.40</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>How satisfied were you with the</td>
<td>0.00</td>
<td>-5.40</td>
<td>5.40</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>response time to your incident? (1=not at all, 6=completely)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>How courteous and respectful was the</td>
<td>0.00</td>
<td>-1.02</td>
<td>1.02</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>technician who responded? (1=poor, 6=excellent)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Please rate the technical competency</td>
<td>0.00</td>
<td>-1.02</td>
<td>1.02</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>of the technician serving you (1=poor,</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6=excellent)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Was technician able to resolve your</td>
<td>0.00</td>
<td>-1.02</td>
<td>1.02</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>issue during the first call?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>How satisfied are you with your</td>
<td>0.00</td>
<td>-1.14</td>
<td>1.14</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>overall service experience? (1=not at all,</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6=completely)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Survey scorecard history - 4 quarters**

---

© 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.
Export a scorecard as an image

You can export a scorecard as an image to use in presentations or other documents.

Role required: admin or survey_admin

1. Click the menu icon (⋮) and select **Save as PNG** or **Save as JPEG** and wait for the export to complete.

2. Click **Download** and save the scorecard image to a storage location.
Survey administration

Survey administrators—users with the survey_admin role—create and maintain surveys and configure how they are distributed and published. Surveys on Service Portal are also supported.

Survey administration includes the following procedures.

- Create, customize, and publish surveys.
- Write and maintain survey questions.
- Define trigger conditions for when surveys are sent to users, such as when an incident closes.
- Maintain surveys and survey questions as the organization's needs change.

To set up surveys in Service Portal, you must first install Service Portal and then configure the Survey widget on the page. The base system includes the Survey widget.

Surveys in Service Portal

If Service Portal is installed, you can use the Survey widget to set up surveys, quizzes, assessments, risk assessments, and attestations in Service Portal. Surveys for users on mobile devices are fully supported in Service Portal.

To create an intuitive interface for your users, you can set up surveys in Service Portal. You must first install Service Portal and then configure the survey widget on the page. To learn more about configuring a widget, see configure widget instances.
To configure a Survey widget on a page, CTRL + right-click the widget heading and select **Instance Options**.

**Service Portal: Instance options (properties) for the Survey widget**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max records</td>
<td>Number of surveys to list on the Service Portal homepage. The user can click the View all link to view all items. Default: 5</td>
</tr>
<tr>
<td>Title of the widget</td>
<td>Text that appears in the title bar of the surveys widget. Default: <strong>My Surveys</strong></td>
</tr>
</tbody>
</table>
Each survey on the My Surveys page contains a progress bar and a description. The color in the progress bar increases as a survey is completed. In the case of a triggered record, the table title is used for the survey description.

For mobile users, the *Pagination setting for Service Portal view* survey designer property is set to one question per page by default.
Survey designer

Users with the survey_admin role can use the survey designer. The survey designer lets you create survey categories and questions, configure the details, and publish the survey to specific users or groups.

You can assign a survey to individual users or groups who receive all the questions from all the categories. You can also customize each question and make it dependent on the response to another question. The following describes the procedures you follow to create and publish a survey.

- Create survey categories.
- Create questions within each category.
- Configure survey details, such as introductory and closing remarks and time limit.
- Select recipients for the survey.
- Publish the survey to the selected users or groups.

Note: The survey designer replaces the survey creator in the Legacy Surveys application. If you are using Internet Explorer version 8 or earlier, the system redirects you to the survey creator.

Survey designer elements

The survey designer is accessible from Survey > Survey Designer.

The survey designer contains controls, a header bar, and the design canvas.

Controls

To create a question, drag the appropriate data type control from the Controls palette and drop it onto the designer canvas.
The assessment engine provides a built-in result calculation feature that converts responses to scored question data types to a score from 0 through 10.

### Question data types

<table>
<thead>
<tr>
<th>Data type</th>
<th>Scored</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachment</td>
<td>No</td>
<td>Question with a Manage Attachments icon that allows users to attach one or more files.</td>
</tr>
<tr>
<td>Boolean</td>
<td>Yes</td>
<td>Question with a check box or Yes and No choices for user responses.</td>
</tr>
<tr>
<td>Choice</td>
<td>Yes</td>
<td>List of predefined options. For more information, see the definition of the <strong>Choices</strong> field in <a href="https://docs.servicenow.com">Create a question in the survey designer</a>.</td>
</tr>
<tr>
<td>Date</td>
<td>No</td>
<td>Date field.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>No</td>
<td>Date and time field.</td>
</tr>
<tr>
<td>Number</td>
<td>No</td>
<td>Number field with predefined minimum and maximum values. The default is 1-10.</td>
</tr>
<tr>
<td>Percentage</td>
<td>No</td>
<td>Percentage field with a prescribed range.</td>
</tr>
<tr>
<td>Scale</td>
<td>Yes</td>
<td>Predefined Likert scale. Answer options appear as radio buttons.</td>
</tr>
<tr>
<td>Numeric Scale</td>
<td>Yes</td>
<td>Selectable number scale. The default is 1-5. Answer options appear as radio buttons.</td>
</tr>
<tr>
<td>String</td>
<td>No</td>
<td>Single or multi-line text field.</td>
</tr>
<tr>
<td>Template</td>
<td>Yes</td>
<td>Choice list of templates that provide a predefined scale of options. For details, see <a href="https://docs.servicenow.com">Quiz scorecards</a>.</td>
</tr>
<tr>
<td>Reference</td>
<td>No</td>
<td>Choice list of fields from a specified reference table. This data type does not support reference qualifiers. For example, a user could select a user name if you specify sys_user as the reference table.</td>
</tr>
<tr>
<td>Image Scale</td>
<td>Yes</td>
<td>Question with a choice of images that can be selected. A template can be used to apply the same images to multiple questions.</td>
</tr>
<tr>
<td>Multiple Selection</td>
<td>Yes</td>
<td>Question with multiple check boxes that can be selected.</td>
</tr>
<tr>
<td>Data type</td>
<td>Scored</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Ranking</td>
<td></td>
<td>Question with an order number to be selected for each option. One order number cannot be selected twice. This question can be mandatory and it can also be dependent on a parent question, but not vice versa.</td>
</tr>
</tbody>
</table>

**Header bar**

The tabs on the header bar display views and a menu of functions.

<table>
<thead>
<tr>
<th>Survey Designer</th>
<th>Design</th>
<th>Configuration</th>
<th>Availability</th>
<th>More</th>
</tr>
</thead>
</table>

- **Save**: Save the current survey.
- **Preview**: Display a preview of the survey as it appears to recipients.
- **Publish**: Distribute the survey to the selected recipients.
- **Save and Publish**: Save and distribute the survey in one step.
- **New Survey**: Open a fresh canvas for a new survey.
- **Load Survey**: View the list of existing surveys.

Click a tab to change the view on the canvas:

- **Design**: Add and configure the properties of categories and questions. This is the default view.
- **Configuration**: Create introductions and end notes for surveys and select a signature.
- **Availability**: Select the recipients for each category in the survey.

Point to the menu icon ( Escorts) to select an option. The list of options depends on the currently open survey.
Design canvas

New surveys open in the canvas of the **Design** view. The survey **Name** field appears above first category in the canvas. A blank question field appears in the category container.

![Design canvas](image)

Initial appearance of the Survey Designer canvas

Configure a survey in the survey designer

Configuration settings apply to the entire survey.

Role required: admin or survey_admin

Select **Configuration** in the survey designer and complete the Survey Designer Configuration form:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Select the check box to enable the distribution of this survey to recipients.</td>
</tr>
<tr>
<td>Anonymize responses</td>
<td>Select the check box to collect survey responses anonymously. Recipients are not listed with survey results. When a user submits a survey, the system clears the Assigned to field for the associated survey instance. Also, survey responses for anonymous surveys do not contain Assigned to values.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of this configuration or the survey to which it is attached.</td>
</tr>
<tr>
<td>Introduction</td>
<td>Introductory content to display on surveys. You can add a welcome message or background information about the survey.</td>
</tr>
<tr>
<td>Signature</td>
<td>Acknowledgement by a survey recipient of requirements, admonitions, or expectations related to a survey.</td>
</tr>
</tbody>
</table>

**Note:** The **Assigned to** field is cleared. However, each response record includes the **Created By** and **Updated By** fields that are accessible to users with the survey_admin role.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Return URL</td>
<td>Destination address of a web page that is presented to users after they submit a completed survey. When a return URL is configured, the End note content does not appear.</td>
</tr>
<tr>
<td>End note</td>
<td>Content that is displayed to recipients after they submit a completed survey. You can add a thank you message, follow-up instructions, or other applicable information. End notes are not displayed if a Return URL is specified.</td>
</tr>
</tbody>
</table>
| Pagination setting for Service Portal view | Specify how the user will see pages on the desktop or tablet view in Service Portal.  
  - Category: Display each category on a separate page.  
  - Question: Display each question on a separate page. This happens for mobile regardless of this setting.  
  - None: All items on a single page—no pagination.  
  Default: Category  
  Note: This field appears only when Service Portal is installed. |
| Duration                      | Amount of time that recipients are given to complete this survey, starting from the time that the survey is generated. The default duration is 14 days.  
  Note: By default, the system runs the Cancel Expired Assessments script every 30 days to cancel expired survey and assessment instances that are in the Work in progress or Ready to take states. |

**Survey categories**

Survey categories provide a way to group questions of a similar theme for a given survey.

There must be at least one survey category per survey definition and every survey question must be associated with a category. When you create a survey, the system generates one category, which all the questions belong to.

For simple surveys, one category is usually enough. Consider creating additional categories if you want to accomplish any of the following tasks:

- Separate groups of questions into collapsible sections by category on the survey questionnaire.
- Report on category scores, which are calculated based on responses for all questions within each category.
Create a category in the survey designer
A category represents a theme for evaluating a specific element of the survey topic and contains questions pertaining to that theme.

Role required: admin or survey_admin

When you create a survey, the system creates a default category, using the name of the survey. You can use this category, modify it, and create additional categories as needed. To have any results, a category must contain scored questions.

1. Navigate to Survey > Survey Designer.
2. Enter the name of the survey in the Name field.
   The system uses this name as the name of the survey and of the first category.
3. To configure the category, click the gear icon in its title bar and complete the following steps in the Properties dialog box.
   a) Enter a new name and a description for the category.
   b) Enter text in the Details field that introduces or explains the category to recipients.
   c) Click the X icon to close the Properties dialog box and save your settings.
4. To add a new category, click the + icon in the title bar of an existing category.
   The new category appears below the category that you selected to create it. You can click the X icon in a category header to delete a category that you added in error.

Create a survey category in a survey
You can modify an existing survey to add one or more survey categories.

Role required: admin or survey_admin

Only one category is required for each survey, but you can add additional categories as needed.

1. Navigate to Survey > View Surveys.
2. Open a survey definition.
3. In the Metric Categories related list, open a category or click New.
   Each survey category is stored as a record on the Metric Category (asmt_metric_category) table with a modified view for survey use.
4. Enter the survey category name and description.
   The category name appears on questionnaires when either of the following is true.
   - There is more than one category for the survey.
   - There is only one category and its name is different from the survey definition name. If you create a survey using the survey creator, the category name is the same as the survey definition name.
5. Right-click the form header and click Save.
   The Assessment Metrics and Users related lists appear.
6. Click Update.

Create a question in the survey designer
You can create multiple questions for each category in the survey designer, but each question can only be associated with one category.

Role required: admin or survey_admin
The data type that you select for each question determines how it can be answered by survey recipients.

1. In the Design view, drag a data type icon from the Controls palette and drop it into a category container.
2. To configure the question, click the gear icon in its title bar. The Properties dialog box opens.
3. Complete the form.

**Question property fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Concise name of the question. The system uses this value to identify the question in Assessment Metric lists and in scorecard charts.</td>
</tr>
<tr>
<td>Question</td>
<td>Text to display as the question on surveys. Enter a clear, straightforward question that is easy to understand.</td>
</tr>
<tr>
<td>Type</td>
<td>Data type selected for this question. See the table in Controls for the available data types.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box that determines whether this question is available on a survey. A question does not appear on surveys that are generated after the question becomes inactive.</td>
</tr>
<tr>
<td>Mandatory</td>
<td>Check box to require users to answer the question. Mandatory questions are denoted by a red field status indicator and must be answered before the survey can be submitted.</td>
</tr>
<tr>
<td></td>
<td>This field is available when the question does not have a dependency and the question type is not <strong>Boolean</strong> with a check box option.</td>
</tr>
<tr>
<td>Boolean option</td>
<td>Whether a check box or a <strong>Yes/No</strong> list appears as the option for a Boolean question.</td>
</tr>
<tr>
<td>String option</td>
<td>Setting for the appearance of a string field in a question. This field is available when the question type is <strong>String</strong>. The string options include the following.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Single line</strong>: Single-line text field 40 characters in length that allows strings of any length.</td>
</tr>
<tr>
<td></td>
<td>- <strong>String line wide</strong>: Full page width text field that allows a single-line entry of any length.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Multiline</strong>: Full page width multiline text field that allows word wrap and returns</td>
</tr>
<tr>
<td>Min</td>
<td>Lowest positive whole number that users can enter or select to answer the question. This field is available when the question type is <strong>Number</strong>, <strong>Percentage</strong>, or <strong>Numeric Scale</strong>.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Max</td>
<td>Highest positive whole number that users can enter or select to answer the question. This field is available when the question type is Number, Percentage, or Numeric Scale.</td>
</tr>
<tr>
<td>Allow not applicable</td>
<td>Check box for including Not Applicable as an option for this question. Users can select Not Applicable if they do not have sufficient information to respond to a question. User responses of Not Applicable are excluded from results calculations. This field is available when the question does not have a dependency and the question type is not Boolean with a check box option.</td>
</tr>
<tr>
<td>Randomize answers</td>
<td>Check box for displaying answer options in a random order. Answer preference is sometimes influenced by the order in which options appear, which can result in biased results. Randomizing options can help prevent this bias. Note: Randomizing options for certain questions may make those questions confusing for users. In general, only randomize options that do not follow a logical order.</td>
</tr>
<tr>
<td>Positive indicator</td>
<td>Setting that determines whether smaller or larger numerical values equate to a good score in result calculations. Select Low values if smaller numerical values are better, such as for a question that measures the number of incidents for a vendor. Select High values if larger numerical values are better, such as for a question that measures user satisfaction on a scale of one to five.</td>
</tr>
<tr>
<td>Details</td>
<td>Information about the question that is displayed on the survey. Include details that help users understand how to answer the question.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Choices</td>
<td>Options for a question with a data type of <strong>Choice</strong> or <strong>Scale</strong>. The system automatically adds text and values that you can edit for each option. You must have at least two options, and each option must have a unique value. Click the + icon to add an option, or click the X icon to delete an option. By default, the system arranges options in the order established by their values. To change the order, drag and drop the options. <strong>Note:</strong> Value numbers also contribute to the calculations of survey response scores, which can be used by advanced survey administrators.</td>
</tr>
</tbody>
</table>

---

4. To create any special conditions that must be met before the question appears on the survey, click the Dependency tab. The question must have a data type of **Boolean**, **Choice**, **Scale**, or **Template**.

5. Select a question in the **Displayed when** field. The system selects the appropriate operator and displays the possible answers for the selected question.

6. Select the answer that satisfies the condition. You can select more than one answer. Selected answers are indicated by a check mark. The system prevents recursive dependencies between questions. For example, if Question A depends on Question B, Question B cannot depend on Question A.

7. Click the X icon to close the question properties dialog box and save your settings.

8. To add a question with the same data type as an existing question in the category, click the + icon in the title bar of the existing question.

9. Drag and drop questions to change their order within a category or move them between categories.

10. To delete a question, click the X icon in its title bar.

**Survey question data types**

You must choose a data type for each survey question. The data type determines the format of the question and the kind of data that is collected on survey questionnaires.
The following data types are available for surveys:

**Attachment data type**

On questionnaires, users can attach one or more files to a question. Users click the Manage Attachments icon and select one or more files in the Attachments pop-up window to attach to the question. From this window, users can:

- View a list of the attached files.
- View an attached file in a separate window.
- Rename an attached file.
- Add or delete files

Once a survey has been submitted, attachments cannot be updated or deleted.

Any type of file supported by the platform can be attached to a question. One or more files can be attached a question while taking a survey or completing an assessment.

The assessment administrator can see the attachments associated with an individual question as well as those associated with the survey.

See [Administering Attachments](administering-attachments) for more information.

**Boolean data type**

On questionnaires, users select a check box beside a statement or leave it cleared.

If you select **Boolean**, you must fill in the **Scale definition** field. Select **High** if it is best when users select the check box.

**Choice data type**

On questionnaires, users select a value from a list of choices.

If you select **Choice**, you must fill in the **Scale definition** field and create answer options. Select **High** for the scale definition if the answer option with the largest metric definition **Value** is best.
Note: The system sets the Min and Max fields automatically based on the Value settings for the associated metric definitions.

Date and Date/Time data types

The Date and Date/Time data types are similar.

- **Date**: On questionnaires, users select a date.

- **Date/Time**: On questionnaires, users select a date and time.
Likert Scale data type

On questionnaires, users select a multiple choice value from a custom Likert scale. Each answer option is represented by a radio button on the scale. A Likert scale question that evaluates an application’s ease of use might have the answer options Easy, Average, and Difficult.

If you select Likert Scale, you must fill in the Scale definition field and create answer options. Select High for the scale definition if the answer option with the largest metric definition Value is best.

Note: The system sets the Min and Max fields automatically based on the Value settings for the associated metric definitions.

Number data type

On questionnaires, users enter a number.
If you select **Number**, you must fill in these additional fields:

- **Scale definition**: Select *High* if a larger number is better, such as for a question that measures the number of sales made in a quarter.
- **Min** and **Max**: Enter the smallest and largest numbers users can enter. State the range of acceptable answers in the question text.

**Percentage data type**

On questionnaires, users enter a number.

If you select **Percentage**, you must fill in these additional fields:

- **Scale definition**: Select *High* if a larger percentage is better, such as for a question that measures the percentage of work an agent has completed.
- **Min** and **Max**: Enter the smallest and largest numbers users can enter. Generally 0 and 100 are appropriate minimum and maximum values. If you choose values other than 0 and 100, it is usually best to state the range of acceptable answers in the question text.

**Reference data type**

On questionnaires, users select a value from a list that is generated from a specified reference table. The response field supports auto-completion.

**Note**: Reference qualifiers are not supported.

For example, a user could select a user name in response to a question if you specify User (sys_user) as the reference table.
String data type

On questionnaires, users enter text. When you select String, the String option field appears. Select one of the following options to determine how the string field appears on questionnaires:

- Single line
Template data type

On questionnaires, users select a value from a predefined series of answer options. To use this data type, a question template must be defined.

If you select Template, you must fill in these additional fields:

- **Template**: Select a template.
- **Scale definition**: Select **High** if the answer option with the largest template definition **Value** is best.

Yes/No data type

On questionnaires, users select **Yes** or **No** from a list.
If you select Yes/No, you must fill in the Scale definition field. Select High if Yes is the best answer.

**Image scale data type**

On questionnaires, users select an image from a predefined set of images as their response. Image scale questions can also be used in a template for better performance with surveys that have the same type of answer options.

Five emojis, similar to the Likert scale (very dissatisfied to very satisfied) are provided. However, you can upload additional images in JPG, PNG, or GIF format. Two images can be uploaded, one for selected case and another for unselected case. Larger size images are reduced to 64 x 64 pixels.

The result behavior depends on the presence of uploaded images. If no selected image is uploaded, then the question shows up blank.

<table>
<thead>
<tr>
<th>Selected image</th>
<th>Unselected image</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Unselected image loads. Clicking on the image changes it to the selected image.</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>Selected image loads with 50% opacity. Clicking on the image changes the opacity to 100%.</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>A blank placeholder box is displayed.</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>A blank placeholder box is displayed.</td>
</tr>
</tbody>
</table>

**Note:** N/A option is not supported for image scale type question.

**Multiple selection data type**

On questionnaires, users can select multiple check boxes indicating all answers that apply. For instance, a user can be instructed to “Select all that apply” in a multiple selection question.
**Ranking data type**

On questionnaires, users can select a different order number for each option to rank them. Drag-and-drop functionality is also supported, which allows a user to either fill in the number, or simply drag an option.

**1. Please rate following device in order of Importance.**

One order number cannot be selected twice. This question can be mandatory and it can also be dependent on a parent question, but not vice versa.

**Edit a survey in the survey designer**

You can modify surveys using the survey designer.
Role required: admin or survey_admin

You can edit a survey even after it has been distributed, with the following results.

- Added questions are available only on surveys that are distributed after this change.
- Changes to existing questions are immediately available to users before the survey is submitted or during the retake period. This includes changes to the answers, such as additional choices or changes to the data type.
- Deleted questions are also deleted from the distributed surveys in user queues.

1. Navigate to Survey > Survey Designer.
2. Point to the menu icon in the survey header bar, and select Load Survey.
3. Select a survey from the list and modify it as needed.
4. Point to the menu icon in the survey header bar, and select Save or Save and Publish.
   When you publish the edited survey, the system generates survey instances for any associated survey users.

Configure category weights for a survey

You can assign a weight to each category in a survey. The system calculates results from the weight that you configure.

Configure the Survey Category form to display the Weight field.

Role required: admin or survey_admin

Weights are set to a value of 10 by default but can be changed.

1. Navigate to Survey > View Surveys and select a survey from the list.
2. In the Survey Definition form, select a category from the Metric Categories related list.
3. Edit the default weight value.
4. Click Update.

View a survey instance

A survey instance represents one questionnaire assigned to one user. You view an instance to verify that survey instances were created, to check the state of a survey instance, or to reassign a survey instance.

Role required: admin or survey_admin

Navigate to Survey > Survey Instances and open a survey instance.

Each survey instance is stored as a record on the Assessment Instance (asmt_assessment_instance) table with a modified view for survey use.

Survey Instance form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Automatically generated record number.</td>
</tr>
<tr>
<td>Metric type</td>
<td>Survey definition this survey instance was created from. Survey definitions are stored on the Assessment Instance table, and the field label on that table is Metric type.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Due date</td>
<td>Date by which the survey instance should be completed. The system populates the due date based on the <strong>Assessment duration</strong> of the associated survey definition, which is set to 14 days by default. The survey due date is not enforced in the base system. If you want to enforce the due date, consider using a workflow or other mechanism to send survey recipients reminders when a survey is overdue.</td>
</tr>
<tr>
<td>Note:</td>
<td>By default, the system runs the <strong>Cancel Expired Assessments</strong> script every 30 days to cancel expired survey and assessment instances that are in the <strong>Work in progress</strong> or <strong>Ready to take</strong> states.</td>
</tr>
<tr>
<td>State</td>
<td>State of the survey instance. The possible states are <strong>Ready to take</strong>, <strong>In progress</strong>, <strong>Complete</strong>, and <strong>Canceled</strong>.</td>
</tr>
<tr>
<td>Assigned to</td>
<td>User this survey instance is assigned to. This field becomes read-only when the state is <strong>In progress</strong>, <strong>Complete</strong>, or <strong>Canceled</strong>.</td>
</tr>
<tr>
<td>Expiration date</td>
<td>Date on which the assigned user can receive a new instance of the same survey definition. The system automatically populates the expiration date based on the <strong>Schedule period</strong> of the associated survey definition.</td>
</tr>
<tr>
<td>Related Link</td>
<td></td>
</tr>
<tr>
<td>View User's Response</td>
<td>Shows a read-only version of the survey responses completed by the user.</td>
</tr>
<tr>
<td>Related List</td>
<td></td>
</tr>
</tbody>
</table>
| Assessment Instance Questions | All instance question records, which store user response values for each question on the survey questionnaire. The following columns are relevant to surveys:  
  * **Category**: Displays the survey categories the questions belong to.  
  * **Metric**: Displays the survey questions.  |
Administering survey users

The list of survey users for a survey is visible on the Survey Definition and Survey Category forms. You can add or remove users from the list of survey users at any point. Note that designating a survey user does not automatically generate a survey instance for that user unless both of the following conditions are true:

- The survey definition Schedule period is set to Daily, Weekly, Monthly, or Yearly. In this case the system assigns a new survey instance to each survey user at the beginning of each schedule period.
- The user has no instances of the survey that are incomplete or that have not yet reached their expiration date.

You can designate survey users from the Survey Designer, the Survey Definition form, or the Survey Category form.

Note: If there are trigger conditions for a survey, do not create survey users. Instead, use the Trigger Conditions form to assign users.

Create a survey user group

Survey user groups are groups that have the Type field set to survey and that display only the information most relevant to surveys. You can assign survey groups or any user group to surveys.

Role required: admin, user_admin, or survey_admin

Though it is possible to designate members of any group as survey users, one reason to create a survey group is to view it conveniently in the survey User Groups module.

1. Navigate to Survey > Administration > User Groups.
2. Click New.
3. Complete the Group form.
4. Right-click the form header and click Save.
   The Group Members and Groups related lists appear.
5. To add group members, complete the following steps.
   a) In the Group Members related list, click Edit.
   b) Select users from the list on the left and add them to the Group Members List on the right.
   c) Click Save.

Select recipients for a survey in the Survey Designer

You can assign survey users while designing or modifying the survey.

Role required: admin or survey_admin

1. In the Survey Designer, click the Availability tab.
2. Under Accessible by:, select the Specific users option, then select users.
3. If desired, select the Survey groups only check box, then select survey user groups or other groups.
4. Click Save.

Designate a survey user

You can designate one survey user at a time from the Survey Definition form.
Role required: admin or survey_admin

1. Navigate to Survey > View Surveys.
2. Open a survey definition.
   There must be at least one category.
3. In the Survey Users related list, click New.
4. Select a User.
5. Click Submit.
   The Survey Definition form reopens.
6. Optional: To remove survey users, in the Survey Users related list, select the check box beside the user, and then select Delete from the action list below the list.

Designate or remove multiple survey users at one time

Use the Survey Category form to designate or remove multiple survey users at a time.

Role required: admin or survey_admin

1. Open a survey definition.
2. In the Metric Categories related list, open a category.
   You can choose any category. The system applies survey user changes to all the survey’s categories automatically.
3. In the Users related list, click Edit.
4. Use the slushbucket to add or remove survey users.
5. Click Save to return to the survey category.
   The changes are also reflected in the Survey Users related list on the survey definition.

Allow recipients to retake a survey

You can configure a survey to allow recipients to resubmit their answers as many times as they like, up to the survey’s due date.

Configure the Survey Definition form to display the Allow retake field. For more information, see Configure the form layout.

Role required: admin or survey_admin

Results are not calculated for the survey until the configured duration has elapsed. The card in the user's queue remains visible until the due date of the survey, and a button is displayed to allow retakes.

1. Navigate to Surveys > View Surveys.
2. Select a survey from the list.
3. Select the Allow retake check box.
4. Click Update.

Publish a survey

You must publish a survey to enable people to receive and complete survey instances.

Role required: admin or survey_admin

The State field on the Survey Definition form indicates whether the survey is in the Draft or Published state.
Note: You cannot return a survey to the Draft state after it has been published. You do have the option to deactivate a survey by clearing the Active check box.

1. Navigate to SurveyView Surveys and select a survey to publish.
2. Click Publish.
   When you publish a survey, the system generates survey instances for any associated survey users. You can assign the survey to other users manually.

Publish a survey in the Survey Designer

You must save changes to a survey before you can publish it to the specified recipients or groups.

Role required: admin or survey_admin

1. In the Survey Designer, point to the menu and select Load Survey.
2. Select a survey to publish.
3. To preview the survey as a user, point to the menu icon and click Preview.
4. When you are satisfied with the survey, click either Save and Publish or Publish to distribute it.
   When you publish a survey, the system sends email notifications to the recipients and to their managers. The system displays a link to the survey on a card in each recipient's My Assessments & Surveys portal.

Customize the appearance of a survey

Assessment and survey administrators can set properties to customize the color of various elements on the questionnaires.

Role required: admin or survey_admin

Note:
- For color properties, enter either an HTML color name or hexadecimal (hex) value. For hex values, the # character is required. Values are not case-sensitive.
- For example, all of the following formats are valid: LightGray, lightgray, #D3D3D3. A preview of the color appears next to the field.

Note that the customizations you make apply to all assessments and surveys.

1. Navigate to either of the following modules.
   - Assessments > Admin > Assessment Properties
   - Survey > Administration > Properties
2. On the properties page, edit the properties as needed.
   Refer to the screenshot below to see what parts of assessment questionnaires are controlled by the properties.
3. Click **Save**.
   You may need to clear the browser’s cache to see updates.

### Assessment and survey properties

You can configure a variety of properties to customize the appearance of assessment and survey questionnaires, require authentication for user signatures, open surveys in the service portal view from emails, and limit the number of items shown in a decision matrix field filter.

<table>
<thead>
<tr>
<th>Property</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
</table>
| sn_portal_surveys.sp_survey.email_redirection | Allow survey link from email to open in service portal view (applies only for surveys) | When Yes is selected, a survey accessed from a link in an email opens in the Service Portal. 

   **Note:** This property applies only to surveys.
   - Default value: No

<table>
<thead>
<tr>
<th>Property</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
</table>
| com.snc.assessment.signature_authentication | Require authentication for user signature. | When Yes is selected, this property requires credentials for a full name signature. 

   - Default value: Yes

<table>
<thead>
<tr>
<th>Property</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
</table>
| css.assessment.question.header.background.color | Assessment question header background color | Sets the background color of question headers on assessment and survey questionnaires. 

   - Default value: #767676
### Survey definitions

A survey definition is the root record upon which a survey is built.

The survey designer generates a survey definition automatically when you save or publish the survey. Survey administrators may want to modify the survey definition to configure additional options for the survey, or to publish the survey when it is ready for distribution.

Survey administrators and survey readers can also send survey invitations directly to users from the survey definition.

### Modify a survey definition

You can configure additional options for a survey definition.

Role required: admin or survey_admin

1. Navigate to Survey > View Surveys.
   
   Each survey definition is stored as a record on the Assessment Metric Type [asmt_metric_type] table with a modified view for survey use.

2. Open a survey definition.

3. Modify the fields on the Survey Definition form, as appropriate.

#### Survey Definition form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the survey, which appears on the questionnaire.</td>
</tr>
<tr>
<td>Description</td>
<td>Helpful information about the survey.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box to activate the survey definition. When the Active check box is cleared, new survey instances cannot be generated and users cannot complete existing survey instances. Use the Active check box to deactivate or activate a published survey.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Anonymize responses | Check box to ensure that all responses for this survey are stored without the submitting user names. When a user submits a survey, the system clears the **Assigned to** field for the associated survey instance. Also, survey responses for anonymous surveys do not contain **Assigned to** values.  
**Note:** The **Assigned to** field is cleared. However, each response record includes the **Created By** and **Updated By** fields that are accessible to users with the survey_admin role. |
| Send notifications  | Check box to send a notification that the survey has been taken.                                                                                                                                     |
| State               | Status of the survey: **Draft** or **Published**.                                                                                                                                                    |
| Signature           | Acknowledgement by a survey recipient of requirements, admonitions, or policies related to the survey. The signature may require the recipient to select a check box or to type a full signature to verify having read these assertions. You can display assertions without requiring a signature. Select an existing signature from the list or click **New** to create a new one. The signature form contains these fields:  
- **Name**: Descriptive name for this signature.  
- **Signature type**: Type of signature required. The selections are **Check box**, **Full name**, or **Assertion only**. If **Assertion only** is selected, no signature is required to submit the survey.  
- **Assertion**: Text you want to display to recipients.  
By default, a property called **Require authentication for user signature** *(com.snc.assessment.signature_authentication)* requires users to authenticate when providing a full name signature. |
| Schedule period     | Option that determines how often a user can take the same survey and whether the system generates survey instances on a schedule.       |

**Note:** If you use a trigger condition for a survey, ensure the schedule period is set to **No Limit**. Trigger conditions use a different method to regulate how often users can receive survey instances.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow retake</td>
<td>Check box that allows users to modify their answers to a completed survey. Users can resubmit a survey as many times as they want until the due date. After that date, the system removes the survey from the user's My Assessments &amp; Surveys page.</td>
</tr>
</tbody>
</table>
| Scheduled job                       | Scheduled job the system creates for this survey definition when the schedule period is a repeating interval. The system sets the scheduled job to run according to the selected schedule period. If you change the schedule period and save the survey definition:  
  · The system deletes the old scheduled job.  
If you selected a recurring schedule period:  
  · A new scheduled job is created.  
For example, if you change the schedule period from **Daily** to **Weekly** and save the record:  
  · The system deletes the daily scheduled job.  
  · Creates a weekly one set to run a week from the current date.  
This field is visible to administrators only if the schedule period is **Daily**, **Weekly**, **Monthly**, or **Yearly**.                                                                                                                                                                               |
| Introduction                        | Introductory content to display on survey questionnaires. Consider adding a company logo, a welcome message, background information about the survey, or instructions.                                                                                                                                                                                                 |
| End note                            | Content to display on the screen that appears when someone submits a survey questionnaire. Consider adding a thank you message, follow-up instructions, or other applicable information.                                                                                          |
| Pagination setting for Service Portal view | The setting on which the pagination is based for desktop or tablet view in Service Portal.  
  · Category: default  
  · Question: 1 question per page (automatic for mobile)  
  · None: no pagination  
**Note:** This field is displayed only when Service Portal is installed.                                                                                                                                                                                                 |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment duration</td>
<td>The length of time to complete assigned survey instances, starting from the time the survey instance is generated. The assessment duration sets the Due date for each survey instance. The default duration is 14 days. Configure the form to see this field.</td>
<td>By default, the system runs the <strong>Cancel Expired Assessments</strong> script every 30 days to cancel expired survey and assessment instances that are in the <strong>Work in progress</strong> or <strong>Ready to take</strong> states.</td>
</tr>
<tr>
<td>Send notifications</td>
<td>Select the check box to send notifications for the survey when it is published. Configure the form to see the field.</td>
<td></td>
</tr>
<tr>
<td>Related Links</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Public Access</td>
<td>Link that enables/disables the survey as a public survey. No login is required to take a public survey (including a survey with a trigger condition) and users or non-users can respond anonymously. For completed public surveys, the <strong>Assigned to</strong> field value is Guest.</td>
<td>You can use the <strong>View Survey URL</strong> related link to share the URL with users.</td>
</tr>
<tr>
<td>Remove Public Access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Responses</td>
<td>Link that opens the list of responses for this survey. This related link is available only if there are results for the survey.</td>
<td></td>
</tr>
<tr>
<td>View Scorecard</td>
<td>Link that opens the scorecard for this survey. This related link is available only if there are results for the survey.</td>
<td></td>
</tr>
<tr>
<td>View Survey URL</td>
<td>Link that opens a dialog box that displays a URL for this survey. The URL is useful for sharing a public survey.</td>
<td>This related link is available only if the <strong>Active</strong> check box is selected. The URL does not work until the survey definition is published.</td>
</tr>
<tr>
<td>Related Lists</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Metric Categories</td>
<td>All survey categories for this survey.</td>
<td></td>
</tr>
<tr>
<td>Survey Users</td>
<td>All survey users who are authorized to take this survey. If no users are listed, any user can take this survey.</td>
<td></td>
</tr>
</tbody>
</table>
### Schedule periods

The available schedule periods are **Only Once**, **No Limit**, **Daily**, **Weekly**, **Monthly**, and **Yearly**.

The default schedule period is **No Limit**. When you set the schedule period to anything except **Only Once** or **No Limit**, the system creates a corresponding scheduled job. The scheduled job performs the following actions.

- Ensures that a user can take one survey instance of the same survey per schedule period.
- Generates a new survey instance for each survey user at the beginning of the new schedule period, as long as the survey user does not have an incomplete instance of that survey. A survey instance is incomplete if the state is not **Complete**.

For example, if you set the schedule period to **Monthly** and someone attempts to send survey invitations twice in the same day, the system generates survey instances for the survey users the first time only. At the beginning of the next schedule period, the system generates another survey instance for each survey user who completed the previous one.

Schedule periods are enforced by the **Expiration date** field on the survey instance. As long as the survey instance expiration date has not passed, the assigned user cannot receive a new survey instance. When the system generates a survey instance and the schedule period is anything except **No Limit**, the **Expiration date** field is automatically set to the appropriate date. For example, if the schedule period is **Weekly**, the expiration date is a week after the survey instance is generated.

If you change the schedule period, the scheduled job updates automatically to the correct schedule. However, users who have survey instances for the survey cannot receive new survey instances until their existing survey instances expire, regardless of the new schedule period.

Consider the following example: Sal Pindell receives a survey instance when the schedule period is **Weekly**. The next day, a survey administrator changes the schedule period to **No Limit**. Sal cannot receive another survey instance until one of the following actions occurs.

- Seven days pass from the time Sal's survey instance was generated.
- A survey administrator deletes Sal’s survey instance.

After one of these actions occurs, Sal can receive a new survey instance anytime, as long as he has no incomplete instances of the survey.

---

**Note:** If you add a related list to the form, use list control to omit the **New** button. The system generates survey instances to produce functional surveys.

---

© 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 a survey designer template question

You can create a question that uses choice lists from a template.

Role required: admin or survey_admin

1. Navigate to **Survey > Survey Designer** and load a survey or create a new survey.
2. Drag the **Template** data type icon into a category container.
3. Click the gear icon in the question title bar to open the template properties dialog box.
4. Select a predefined scale from the list.
Question entry fields appear for that template.

5. Enter one or more questions that are appropriate for the template.
6. Click the arrow to the right of a question to configure its properties. You must provide a name for each question.
7. Click the back arrow to return to the template properties dialog box.
8. Configure the properties for the remaining questions.
9. Click the X icon to close the template properties dialog box and save your settings.

Survey questions

Survey questions appear on survey questionnaires for the associated survey definition.

The survey creator generates questions and answer options automatically. However, it provides only the basic configuration options for questions, such as the question text and the data type. You may want to create additional questions or set advanced configuration options for the questions, including making a question appear conditionally or making a question mandatory. You can also use question templates to define reusable sets of answer options.

Survey questions are available from Survey > Questions. The list displays information about each question, including the associated survey definition listed in the Type column, and the data type. Survey administrators can modify these questions.

Create or modify survey questions

You can create and administer survey questions.
Role required: admin or survey_admin

Changes to a survey, such as the addition of questions or the modification of question templates, do not apply immediately to the existing survey instances. However, the changes apply immediately to any new survey instances that are created after the changes are saved.

1. Navigate to Survey > View Surveys.
2. Open a survey definition.
3. In the Metric Categories related list, open a category.
4. In the Assessment Metrics related list, open an existing question or click New. Each survey question is stored as a record on the Assessment Metric (asmt_metric) table with a modified view for survey use.
5. Complete the Survey Question form.

The fields that appear depend on the selected Data type.

**Survey Question form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the question. When you create a survey, the question name is the same as the text in the Question field.</td>
</tr>
<tr>
<td>Question</td>
<td>Text to use for the question, which appears on survey questionnaires.</td>
</tr>
<tr>
<td>Data type</td>
<td>Data type of the question. The fields for the response depend on the data type.</td>
</tr>
<tr>
<td>Template</td>
<td>Question template to use for the answer options. This field is visible and required only if the data type is Template.</td>
</tr>
<tr>
<td>Scale definition</td>
<td>Setting that determines whether smaller or larger numerical values equate to a good score in result calculations. Select Low if smaller numerical values are better, such as for a question that measures the number of incidents for a vendor. Select High if larger numerical values are better, such as for a question that measures user satisfaction on a scale of one to five. This field is visible and required only when certain data types are selected.</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>
<tbody>
<tr>
<td>Randomize answers</td>
<td>Check box that determines whether to present the answer options for this question in a random order each time a user opens the survey. Answer preference is sometimes influenced by the order in which answer options appear, which can result in biased results. Randomize answer options to help prevent this bias. This field is visible only if the data type is Choice or Likert Scale.</td>
</tr>
<tr>
<td>Mandatory</td>
<td>Check box that makes the question mandatory (selected) or optional (cleared) on survey questionnaires. Users cannot submit questionnaires until they provide valid responses to all mandatory questions, which are denoted by a red field status indicator. This field is visible only when the Depends on field is empty and the data type is not Checkbox. Questions that depend on other questions and check box questions cannot be mandatory.</td>
</tr>
<tr>
<td>Allow not applicable</td>
<td>Check box that determines whether to include a Not Applicable answer option for this question on survey questionnaires. User responses of Not Applicable are excluded from results calculations. This field is visible only if the data type is Choice, Likert Scale, Template, or Yes/No.</td>
</tr>
<tr>
<td>Depends on</td>
<td>Setting used to make this a conditional question, meaning that it only appears when users answer another question a certain way. To make a question depend on another question, select an existing question from the list, which displays Checkbox, Choice, Template, and Yes/No questions of the same category as this question. Then, use the Displayed when field to set the conditions that cause this question to appear on surveys. The system prevents the creation of recursive dependencies between questions. For example, if Question A depends on Question B, Question B cannot depend on Question A.</td>
</tr>
<tr>
<td>Displayed when</td>
<td>Answer options for the selected Depends on question which, when chosen on surveys, display this question. This field is visible and required only when the Depends on field is set.</td>
</tr>
</tbody>
</table>
### Survey question data types

You must choose a data type for each survey question. The data type determines the format of the question and the kind of data that is collected on survey questionnaires.

The following data types are available for surveys:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min</td>
<td>Smallest numerical value to be used as an answer option for this question. This field is visible and required only if the data type is Choice, Likert Scale, Number, or Percentage.</td>
</tr>
<tr>
<td>Max</td>
<td>Largest numerical value to be used as an answer option for this question. This field is visible and required only if the data type is Choice, Likert Scale, Number, or Percentage.</td>
</tr>
<tr>
<td>String option</td>
<td>Selection that determines what kind of response text box appears for this question on survey questionnaires. This field is visible and required only if the data type is String.</td>
</tr>
<tr>
<td>Assessment Metric Definitions</td>
<td>Answer options for this question. This related list is available only if the Data type is Choice or Likert Scale.</td>
</tr>
</tbody>
</table>

6. Save the record.
   Be sure to create answer options if you select the **Choice** or **Likert Scale** data type.

#### Attachment data type

On questionnaires, users can attach one or more files to a question.

Users click the Manage Attachments icon and select one or more files in the Attachments pop-up window to attach to the question. From this window, users can:

- View a list of the attached files.
- View an attached file in a separate window.
- Rename an attached file.
- Add or delete files

Once a survey has been submitted, attachments cannot be updated or deleted.

Any type of file supported by the platform can be attached to a question. One or more files can be attached a question while taking a survey or completing an assessment.

The assessment administrator can see the attachments associated with an individual question as well as those associated with the survey.

See **Administering Attachments** for more information.

#### Boolean data type

On questionnaires, users select a check box beside a statement or leave it cleared.
If you select **Boolean**, you must fill in the **Scale definition** field. Select **High** if it is best when users select the check box.

**Choice data type**

On questionnaires, users select a value from a list of choices.

If you select **Choice**, you must fill in the **Scale definition** field and create answer options. Select **High** for the scale definition if the answer option with the largest metric definition **Value** is best.

---

**Note:** The system sets the **Min** and **Max** fields automatically based on the **Value** settings for the associated metric definitions.

---

**Date and Date/Time data types**

The **Date** and **Date/Time** data types are similar.

- **Date:** On questionnaires, users select a date.
- **Date/Time**: On questionnaires, users select a date and time.
Likert Scale data type

On questionnaires, users select a multiple choice value from a custom Likert scale. Each answer option is represented by a radio button on the scale. A Likert scale question that evaluates an application’s ease of use might have the answer options Easy, Average, and Difficult.

If you select Likert Scale, you must fill in the Scale definition field and create answer options. Select High for the scale definition if the answer option with the largest metric definition Value is best.

Note: The system sets the Min and Max fields automatically based on the Value settings for the associated metric definitions.

Number data type

On questionnaires, users enter a number.

If you select Number, you must fill in these additional fields:

- Scale definition: Select High if a larger number is better, such as for a question that measures the number of sales made in a quarter.
- Min and Max: Enter the smallest and largest numbers users can enter. State the range of acceptable answers in the question text.

Percentage data type

On questionnaires, users enter a number.

If you select Percentage, you must fill in these additional fields:
· **Scale definition**: Select **High** if a larger percentage is better, such as for a question that measures the percentage of work an agent has completed.

· **Min** and **Max**: Enter the smallest and largest numbers users can enter. Generally **0** and **100** are appropriate minimum and maximum values. If you choose values other than **0** and **100**, it is usually best to state the range of acceptable answers in the question text.

### Reference data type

On questionnaires, users select a value from a list that is generated from a specified reference table. The response field supports auto-completion.

**Note**: Reference qualifiers are not supported.

For example, a user could select a user name in response to a question if you specify User (sys_user) as the reference table.

![Reference data type example](image)

### String data type

On questionnaires, users enter text. When you select **String**, the **String option** field appears. Select one of the following options to determine how the string field appears on questionnaires:
Template data type

On questionnaires, users select a value from a predefined series of answer options. To use this data type, a question template must be defined.

If you select Template, you must fill in these additional fields:

- **Template**: Select a template.
- **Scale definition**: Select High if the answer option with the largest template definition Value is best.

Yes/No data type

On questionnaires, users select Yes or No from a list.
If you select Yes/No, you must fill in the Scale definition field. Select High if Yes is the best answer.

Image scale data type

On questionnaires, users select an image from a predefined set of images as their response. Image scale questions can also be used in a template for better performance with surveys that have the same type of answer options.

Five emojis, similar to the Likert scale (very dissatisfied to very satisfied) are provided. However, you can upload additional images in JPG, PNG, or GIF format. Two images can be uploaded, one for selected case and another for unselected case. Larger size images are reduced to 64 x 64 pixels.

The result behavior depends on the presence of uploaded images. If no selected image is uploaded, then the question shows up blank.

<table>
<thead>
<tr>
<th>Selected Image</th>
<th>Unselected image</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Unselected image loads. Clicking on the image changes it to the selected image.</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>Selected image loads with 50% opacity. Clicking on the image changes the opacity to 100%.</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>A blank placeholder box is displayed.</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>A blank placeholder box is displayed.</td>
</tr>
</tbody>
</table>

Note: N/A option is not supported for image scale type question.
Multiple selection data type

On questionnaires, users can select multiple check boxes indicating all answers that apply. For instance, a user can be instructed to “Select all that apply” in a multiple selection question.

```
Equipment Usage Survey

Multiple Selection

What equipments do you use?

☐ Laptop
☐ Tablet
☐ Smart Phone
```

Ranking data type

On questionnaires, users can select a different order number for each option to rank them. Drag-and-drop functionality is also supported, which allows a user to either fill in the number, or simply drag an option.

```
1. Please rate following device in order of Importance.

☐ 1
☐ 2
☐ 3
```

© 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.
One order number cannot be selected twice. This question can be mandatory and it can also be dependent on a parent question, but not vice versa.

**Survey question template**

Question templates define reusable sets of answer options for survey questions.

Question templates define reusable rating scales for answering questions, where each answer option on the scale is a template definition. For example, the template named *Satisfaction* represents a satisfaction scale and contains the following template definitions: *Very Satisfied*, *Satisfied*, *Neutral*, *Dissatisfied*, and *Very Dissatisfied*.

**Template definition**

Templates are available for survey questions that have **Data type** set to **Template**. The following question templates are available in the base system. You can create or update a template as described in [Create a survey question template](#).

### Default question templates

<table>
<thead>
<tr>
<th>Name</th>
<th>Template definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amount</td>
<td>None, Few or little, Average amount, Many, Quite a lot</td>
</tr>
<tr>
<td>Complexity</td>
<td>Very Complex, Complex, Moderate, Simple, Very Simple</td>
</tr>
<tr>
<td>Frequency</td>
<td>Never, Seldom, Sometimes, Most of the time, All of the time</td>
</tr>
<tr>
<td>Likert 5</td>
<td>Strongly Disagree, Disagree, Neutral, Agree, Strongly Agree</td>
</tr>
<tr>
<td>Quality</td>
<td>Very Poor, Poor, Average, Good, Very Good</td>
</tr>
<tr>
<td>Satisfaction</td>
<td>Very Dissatisfied, Dissatisfied, Neutral, Satisfied, Very Satisfied</td>
</tr>
<tr>
<td>Size</td>
<td>Very Small, Small, Average, Large, Very Large</td>
</tr>
</tbody>
</table>

**Create a survey question template**

You can create and administer question templates.

Role required: admin or survey_admin

Changes to a survey, such as the modification of question templates, apply to existing survey instances immediately. Templates that you create are available for use with both surveys and assessments.

1. Navigate to **Survey > Templates**.
Each template is stored as a record on the Assessment Metric Template (asmt_template) table.

2. Click **New**.
3. Enter a **Name**.
4. Right-click the form header and click **Save**.
5. In the **Assessment Template Definitions** related list, click **New**.
   Create a template definition for each answer option you want to appear on a question.
6. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display</td>
<td>Enter the text to appear as the answer option.</td>
</tr>
<tr>
<td>Value</td>
<td>Enter a numeric value, greater than or equal to zero, to which the answer option equates. Values are used in results calculations. When you view questions that use templates, answer options appear in order from smallest to largest <strong>Value</strong>. Each template definition for a given template must have a unique <strong>Value</strong>.</td>
</tr>
</tbody>
</table>

7. Click **Update**.

**Update min and max values to match templates**

If you use survey result calculation data, ensure that the **Min** and **Max** values for a question that uses a template are equal to the smallest and largest template definition **Value**.

Role required: admin or survey_admin

When you create a question of the **Template** data type, the system sets the **Min** and **Max** fields based on the template definition values. The fields for existing questions are not updated if you add a new template definition to a template or if you update the **Value** of an existing template. If the new **Value** is less than the minimum value or greater than the maximum value of any questions that use the template, update the questions accordingly.

1. Navigate to **Survey > Questions**.
2. Configure the list to show the **Min** and **Max** columns.
3. Add the following list filter condition: (Template) (is) (<select the template you updated>).
4. Ensure the **Min** and **Max** values match the smallest and largest template definition **Value** for the selected template.
   If the values do not match, edit the **Min** and **Max** values directly from the list.

**Note:** When the data type is **Template**, a UI policy prevents the editing of **Min** and **Max** from the form.

**Create or modify answer options**

You must create answer options, called metric definitions, for survey questions that have **Data type** set to **Choice** or **Likert Scale**.

Role required: admin or survey_admin

Changes to a survey, such as the addition or modification of answer options, apply to existing survey instances immediately.

1. Navigate to **Survey > Questions**.

© 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. Open a choice or Likert scale survey question.
3. In the Assessment Metric Definitions related list, open a metric definition or click New.
   Each answer option is stored as a record on the Assessment Metric Definition (asmt_metric_definition) table.
4. Complete the Assessment Metric Definition form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display</td>
<td>Text to appear as the answer option.</td>
</tr>
<tr>
<td>Value</td>
<td>Numeric value, greater than or equal to zero, to which the answer option equates. Values determine the order in which answer options appear. See the example below. Values are also used to calculate survey results. Each metric definition for a given question must have a different Value.</td>
</tr>
</tbody>
</table>

5. Click Submit.

On survey questionnaires, the answer options for a question appear in order from smallest to largest Value. For example, consider the survey question How do you feel? with the answer options Good, Neutral, and Bad. The following table shows the answer option order based on the Value.

<table>
<thead>
<tr>
<th>Answer option</th>
<th>Value</th>
<th>Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>Good</td>
<td>1</td>
<td>First</td>
</tr>
<tr>
<td>Neutral</td>
<td>3</td>
<td>Second</td>
</tr>
<tr>
<td>Bad</td>
<td>5</td>
<td>Third</td>
</tr>
</tbody>
</table>

If you use survey result calculations, ensure the question Scale definition is set appropriately based on the answer options. In the previous example, if you want the answer option Good to earn the highest score, the scale definition should be Low because Good has the smallest value.

Change the order of survey questions

You can easily reorder survey questions at the category level or the question level.

Role required: admin or survey_admin

You can change the order in which the questions in one category appear relative to those in other categories for the same survey definition. If you add a new question manually after you create other questions, you may want to change the order of questions.

When you create questions using the survey creator, the system sets the Order field for the first question to 101, the second to 102, and so on. After you create a new question outside of the survey creator, the Order is set to 100 by default, which means it appears before all questions generated by the survey creator.

1. Navigate to Survey > View Surveys and open the appropriate survey definition.
2. In the **Metric Categories** related list, edit the values in the **Order** column.
3. To change the order of questions within a category, complete the following steps.
   a) Open the **Assessment Metrics** related list.
   b) Edit the values in the **Order** column.
4. Click **Update**.

**Survey trigger conditions**

Trigger conditions specify when to send a particular survey and the persons to send it to.

Survey administrators can use trigger conditions to configure the system to generate a survey instance each time a specified action occurs on a specified table, for example, when an incident or change request closes. The system sends the survey to users that are related to the triggering record, for example, incident callers or change request assignees. You can choose to send a survey every time the condition is met, or you can set a probability for the system to send a survey at random when the condition is met.

Trigger conditions are ideal for sending transactional surveys. Transactional surveys generally measure satisfaction with a recent experience, such as closing an incident or purchasing an item.

**Note:** Trigger conditions are comparable to survey conditions in legacy surveys. If you migrate a legacy survey that has survey conditions, ensure that the survey conditions are deactivated before you recreate them as trigger conditions.

**Configure a trigger condition for a survey**

Configure trigger conditions to specify when to send a particular survey and the persons to send it to.

Role required: admin or survey_admin

1. Navigate to **Survey > Trigger Conditions**.
2. Click **New**.

**Note:** Do not specify particular users for a triggered survey because only the specified users are allowed to take the survey.

3. Complete the form.

**Trigger condition fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment</td>
<td>Survey to send.</td>
</tr>
<tr>
<td>Table</td>
<td>Table to run the trigger condition on. You can select only tables in the current application scope. For example, to send a survey whenever an incident closes, select the Incident (incident) table.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User field</td>
<td>Field that stores the users you want to send the survey. You can select any field, on the selected table or on a referenced table, that references the User (sys_user) table. Use the tree picker to select a field.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> To avoid requiring users to log in to take a survey with a trigger condition, set the survey to <strong>Public</strong>.</td>
</tr>
<tr>
<td>Repeat interval</td>
<td>Minimum period that must pass before the trigger condition can resend the survey to the same user. For example, assume the repeat interval is set to 30 days. Even if the same user qualifies for multiple surveys from this trigger condition, the system can send only one survey every 30 days.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Ensure that the Schedule period of the selected survey definition is set to <strong>No Limit</strong>. If the schedule period is set to a different value, it prevents the trigger condition from sending surveys as expected.</td>
</tr>
<tr>
<td>Application</td>
<td>(Admin only) Application is set to Core.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box that determines whether this trigger condition is active (selected).</td>
</tr>
<tr>
<td>Business rule</td>
<td>(Admin only) Business rule the system creates to monitor the selected table. When the condition is met, the business rule sends the survey to the correct user. No configuration is necessary for this business rule.</td>
</tr>
<tr>
<td>Trigger randomly</td>
<td>Check box that determines whether to send the survey to the appropriate user every time the condition is met (cleared) or only a percentage of the time (selected).</td>
</tr>
<tr>
<td>Probability (%)</td>
<td>Approximate probability that the survey is sent each time the condition is met. For example, if the probability is set to 50, the system sends the survey approximately 50% of the time the conditions are met. There are no repeat interval restrictions is assumed. This field is visible and required only when Trigger randomly is selected.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Related Field 1-4</td>
<td>Field that contains a value you want to store for reporting purposes. You can pick any reference field on the selected table. When the trigger condition generates a survey instance, the system stores the value from the triggering record. Specify up to four fields. For example, select the Incident table, <strong>Assigned to</strong> and <strong>Problem</strong> as related fields. The system stores the assigned user and problem associated with the incident as Related record 1 and Related record 2 in the survey instance record. To view the fields, configure the form for any survey instance. <strong>Note:</strong> You cannot use a related field for the ticket number because you cannot select the Number column. You can, however, use the trigger_id column of the table.</td>
</tr>
<tr>
<td>Description</td>
<td>Summary information to identify the trigger condition.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For a triggered record, the table title is used for the survey description.</td>
</tr>
<tr>
<td>Condition</td>
<td>Condition builder that defines the criteria that must be true to send the survey. For example, to send a survey whenever an incident closes, create the condition <strong>(State) (is) (Closed)</strong>.</td>
</tr>
</tbody>
</table>

You can also create a trigger condition directly from the survey creator. If you select **Certain users can take this survey, based on conditions** in the Survey User Access section, the Trigger Condition form opens automatically when you click **Save as Draft** or **Publish**.
<table>
<thead>
<tr>
<th>Assessment</th>
<th>ServiceDesk Satisfaction Survey</th>
<th>Application</th>
<th>Global</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Incident (Incident)</td>
<td>Active</td>
<td>✔️</td>
</tr>
<tr>
<td>User Field</td>
<td>Click to select...</td>
<td>Business rule</td>
<td></td>
</tr>
</tbody>
</table>

**Repeat Interval**

- **Days**: 30

**Related Field 1**
- None

**Related Field 2**
- None

**Related Field 3**
- None

**Related Field 4**
- None

**Description**
Send incident callers service desk satisfaction surveys when incidents are closed

**Conditions**
- Add Filter Condition
- Add "OR" Clause
- choose field
- oper
- value

Submit
Trigger condition example

You can send out auto-triggered surveys when an incident is closed or resolved.

A trigger condition is configured as follows:

- **Assessment**: Service Desk Satisfaction Survey
- **Table**: Incident (incident)
- **User field**: Caller
- **Repeat interval**: 30 days
- **Active**: true
- **Trigger randomly**: false
- **Related Field 1**: Assigned to
- **Related Field 2**: Problem
- **Condition**: (State) is (Closed) or (State) is (Resolved)

Fannie Steese is the caller on incident INC00004305 that is assigned to Boris Catino, a service desk technician. Boris creates PRB010101 based on Fannie's complaint and closes the incident. The system creates a survey instance assigned to Fannie so she can rate her satisfaction with the incident experience.

Because two related fields were selected as part of the trigger condition, the survey instance stores the following information from the incident:

- **User (Related Field 1)**: Boris Catino
- **Problem (Related Field 2)**: PRB010101
- **Task (automatically created)**: INC00004305

Because the task field is automatically populated, UI-based filtering by dot-walking on incidents (or any task-based table) is supported when creating a report on survey results. For example, you can query all survey instances related to incidents assigned to a group (survey reports on all incidents assigned to networking group, for instance).

**Note**: Even though the trigger condition is set to be triggered each time that the conditions are met, the **Repeat interval** setting ensures that Fannie does not receive another survey for another of her incidents closes within 30 days of the first incident.

Survey report example based on task field

One of the most common use cases for Surveys is to send out an auto-triggered survey when an incident, request, or task is closed. Once you get the survey results back, you can filter the results by users and groups related to the ticket, such as Assignment Group, or Assignee.

Filtering the survey results provides more detail on how people and teams are performing based on ticket data. Since this information is automatically captured, you can dot-walk while filtering the data (instead of utilizing a related field on the Survey trigger condition form, as previously required).
To create a report on incident-triggered survey responses by Assignment group, set up the report on the Task Assessment Details by navigating to ReportsView/Run and clicking Create a report.

Survey distribution

There are several ways for survey administrators to distribute surveys to users. Surveys are distributed using any of the following methods.

- Send survey invitations to users
- Share a survey URL that opens the survey directly.
- Create a module that opens a survey.

Send survey invitations to users

You can send survey invitations using the Assign Survey or Send Invitations buttons on the Survey Definition form.

Role required: admin or survey_admin

Use the Send Invitations button to immediately assign survey instances to each survey user that is listed in the survey definition. Use the Assign Survey button to assign a survey instance to any one user at a time.

Each of the buttons generates survey instances assigned to the appropriate users. In addition, if the instance is configured to send email, the system generates survey notifications. For either button to be available, the survey definition must meet all of the following conditions.

- Active check box is selected.
· **State** is Published.
· Survey is associated with at least one question.

**Note:** You (or a trigger) can send more than one instance of a survey to a user at any time.

1. Navigate to Survey > View Surveys.
2. Select an active, published survey.
3. Complete one of the following actions.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign a survey to users listed in the Survey Users related list</td>
<td>Click <strong>Send invitations.</strong></td>
</tr>
<tr>
<td>Assign a survey to any user</td>
<td>Click <strong>Assign Survey</strong> and select one or more users, and then click OK.</td>
</tr>
</tbody>
</table>

The system creates a survey instance assigned to the user or users, assuming the user is eligible to receive a new survey instance. When you use the **Assign Survey** button, the selected user is not saved as a survey user.

**Survey URLs**

You can distribute a survey by giving survey users a survey URL.

Survey administrators can obtain one of the following types of URLs.

- **A general URL** for a survey, which users can open to take the survey questionnaire. The following process occurs.
  
  - When someone opens the URL, the system ensures that the person is logged in. It then searches for an instance of the associated survey that is assigned to the logged-in user.
  
  - If a survey instance is found, the appropriate action occurs based on the **State** of the survey instance (see table). If there are multiple active survey instances (**Ready to take** or **In progress**), the instance with the earliest due date opens.
  
  - If no survey instance is found, the system creates a new instance for the survey, assigns it to the user, and opens the survey questionnaire.

- **A URL** for a specific survey instance, which the assigned user can open to take the survey questionnaire. The following process occurs.
  
  - When someone opens the URL, the system ensures the person is logged in as the user the survey instance is assigned to. Only the assigned user can access the survey questionnaire.
  
  - The appropriate action occurs, depending on the **State** of the survey instance (see table).

**Survey states**

<table>
<thead>
<tr>
<th>Survey instance state</th>
<th>Action upon opening URL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ready to take</strong>: User has not saved any responses.</td>
<td>The survey questionnaire appears for the user to begin. The user can save or submit responses.</td>
</tr>
<tr>
<td><strong>In progress</strong>: User has saved at least one response.</td>
<td>The survey questionnaire appears for the user to continue. Any previously saved responses are displayed. The user can save or submit responses.</td>
</tr>
<tr>
<td>Survey instance state</td>
<td>Action upon opening URL</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Complete**: User has submitted all required responses. | If the schedule period is **No Limit** or if the period restriction has expired, the survey questionnaire for a new survey instance appears for the user to begin.  
If the schedule period restricts the number of times a user can take the same survey, and the period restriction has not expired since the user last completed survey, an error message appears. |

If someone opens a URL for an unpublished or deactivated survey, an error message appears.

**Obtain and distribute a general survey URL**

You can distribute a general survey URL to allow any eligible user to open a survey questionnaire.

Role required: admin or survey_admin

The general URL is available on the Survey Definition form and on the survey creator. You can also email the URL for a public survey that is published.

1. Navigate to **Survey > View Surveys**.
2. Open a survey definition from the Assessment Metric Types list.
3. To view or copy the URL, click the **View Survey URL** related link.  
   This related link is visible only if the survey definition is **Active**.
4. To distribute the URL to users, paste the copied URL as desired, or click the **Email** button to send via email.  
   The **Email** button is visible only for a public survey that is published.

When a survey user clicks the general survey URL, the system creates a survey instance for the survey user as long as the user does not have an instance in the **Ready to take** state. The system is configured by default to send an email notification when a survey instance is generated.

As a result, the survey user receives a second notification in addition to the notification that you sent with the general survey URL. This may confuse the survey user. To avoid this issue, you can deactivate auto-notification.

**Deactivate auto-notification for surveys**

When you send a survey notification with a general survey URL to a survey user, the user may receive a second system-generated notification. To avoid this issue, you can deactivate auto-notification.

Role required: admin or survey_admin

1. Navigate to **System Notification > Email > Notifications**.
2. Open the **Survey User Invite** notification.
3. Configure the form to add the **Send to event creator** check box to the Who will receive section.  
   The **Send to event creator** check box is selected by default.
4. Clear the **Send to event creator** check box.  
   The system will no longer send auto-notification messages to survey users.

**Obtain a survey instance URL**

You can distribute a survey instance URL to allow the assigned user to open a survey questionnaire.

Role required: admin or survey_admin
The survey instance URL is available on the survey instance record.

1. Navigate to **Survey > Survey Instances**.
2. Open the instance for the survey.
3. To view or copy the URL, click **View Instance URL** related link.
   - The related link is available only when the survey instance **State** is **Ready to take** or **In progress** and the associated survey definition is **Active**.
4. In the dialog box, select and copy the URL then click **OK** or **Cancel**.
5. Distribute the URL to the assigned user.

---

**Test a survey URL**

When there are survey users associated with a survey, the survey is restricted so only those users can use the survey URL. You can test the survey URL to ensure it is restricted.

Role required: admin or survey_admin

1. Navigate to **Survey > View Surveys** and open a survey for which you are not a survey user.
2. Under **Related Links**, click **View Survey URL**.
3. Copy the URL and click **OK** or **Cancel**.
4. Navigate to the URL.
   - You see a message that you are not authorized to take the survey.

---

**Create a survey module**

You can create a module that opens a survey.

Role required: admin or survey_admin

When a user clicks a survey module, the system performs one of the following actions, depending on the configuration options for the survey and other factors.

- Creates a new survey instance
- Opens an existing survey instance
- Displays an error message.

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>UI16</td>
<td>Point to the application menu that contains the module to which you want to add the survey module and click the edit application (pencil) icon.</td>
</tr>
<tr>
<td>UI15 or UI11</td>
<td>Right-click the application menu you want to add the module to and select <strong>Edit Application Menu</strong>.</td>
</tr>
</tbody>
</table>

2. In the **Modules** related list, click **New**.
3. Complete the following fields.
   - **Link type**: Assessment
     - Do not select **Survey**, which is used for legacy surveys only.
   - **Assessment**: Select the survey you want the module to open.
4. Complete and save the form.

---

**Sharing surveys: export and import**

You can export a survey and then import it to a different ServiceNow instance.
**Note:** Update sets are available in the Helsinki release and should be used to move data from one instance to another. For information about update sets, see *System update sets*.

The system exports a single XML file that contains a survey definition (asmt_metric_type) and the associated records, including the following.

- Assessment Metric Template (asmt_template)
- Assessment Template Definition (asmt_template_definition)
- Metric definitions (asmt_metric_definition) (survey question answer options)
- Scheduled Jobs associated with the Survey (sys_trigger)
- Survey categories (asmt_metric_category)
- Survey questions (asmt_metric)
- Survey users (asmt_m2m_category_user)
- Trigger Condition (asmt_condition)

**Export a survey**
You can export a survey and then import it to another instance.
Role required: admin, survey_reader, or survey_admin
For information about update sets, see *System update sets*.

1. Navigate to Survey > View Surveys.
2. Right-click the name of a record to show the context menu.
3. Select Export Assessment.
4. If applicable, follow the prompt in your browser to save the XML file.

**Import a survey**
You can import a survey that has been exported as an XML file. The exported XML file does not contain result data.
Role required: admin or survey_admin

**Note:** Update sets are available in the Helsinki release and should be used to move data from one instance to another. For information about update sets, see *System update sets*.

1. Verify that the target instance has assessments enabled.
2. Follow the steps in *Import an XML file* to import the assessment.

**Use update sets for surveys and assessments**
Use an update set to capture changes to surveys and assessments.
Role required: admin or survey_admin
When developing surveys and assessments, you can use an update set to capture the changes and move them from a development instance to a production instance. Once an update set is created and marked current, all of the updates to the following tables are recorded in the update set.

The following tables are now update set enabled and also extend the application file:

- Assessment Metric Templates (asmt_template)
- Assessment Template Definitions (asmt_template_definition)
- Assessment Metric Definitions (asmt_metric_definition): survey question answer options
- Schedule (sys_trigger): scheduled jobs associated with the survey
- Assessment Metric Categories (asmt_metric_category): survey categories
- Assessment Metrics (asmt_metric): survey questions
• Assessment Category Users (asmt_m2m_category_user): survey users
• Trigger Conditions (asmt_condition)

Legacy survey migration

Users with the survey_admin role can migrate legacy survey data to create copies of legacy surveys and their related records in assessment tables. The Survey Management application, which is built on the assessment engine, is available as an alternative to legacy surveys.

The following legacy survey components are migrated:
• Survey masters
• Supported survey questions and question choices
• Survey instances
• Survey responses

Legacy survey conditions are not migrated and must be recreated as trigger conditions.

Note: Survey wizards cannot be migrated.

Migrate a legacy survey

Migrate a legacy survey and its related records to take advantage of a more powerful feature set.

Role required: admin or survey_admin

To avoid timing out for very large surveys, you can disable the transaction quota. See Transaction quotas.

1. Navigate to Survey > Legacy Surveys > Masters.
The list of legacy survey masters appears. By default, the list shows only survey masters that have not been migrated. To show all survey masters, remove the Assessment is empty breadcrumb.
2. Open a survey and click the Migrate to Assessment related link.
A dialog box describes what happens when you migrate the survey. Note that certain types of survey questions cannot be migrated.
3. Click OK.
The system generates records on assessment tables based on the survey master, eligible questions and choices, results, and other related survey components. The original survey components are unaffected.

System messages may appear at the top of the Survey form to notify you of questions that could not be migrated and to advise you to review migrated Multiple Choice questions.

4. Optional: Click the reference icon beside the Assessment field to view the new survey definition.
5. Optional: Remove survey users from the assessment survey if you want all users to be able to take it.
When you migrate a survey, any users who have taken it are automatically associated with the assessment survey and become survey users. When there are survey users associated with an assessment survey, only those users can take it.
6. Deactivate any survey conditions associated with the survey by completing the following steps.
   a) Navigate to Survey > Legacy Administration > Survey Conditions.
   b) In the Active column, ensure the value is false for any survey conditions that reference the migrated survey.
7. Navigate to Survey > Administration > Trigger Conditions to create new trigger conditions for the migrated survey.

The Migrate to Assessment related link on the legacy survey record becomes unavailable after the migration. However, if you delete the record referenced in the Assessment field, the related link reappears and you can migrate the legacy survey again.

Survey question migration

Before you migrate a legacy survey, understand that some legacy survey questions cannot be migrated due to incompatible question types.

Legacy survey questions are migrated from the Survey Question (survey_question_new) table to the Assessment Metric (asmt_metric) table. In legacy surveys, the Type field on the Survey Question table determines how the question renders on the survey questionnaire. In assessment surveys, the Data type field on the Assessment Metric table serves a similar purpose. Certain legacy survey types are not supported in assessment surveys.

The following table shows the conversion path for each legacy survey question type to an assessment data type, if there is one.

<table>
<thead>
<tr>
<th>Legacy survey type</th>
<th>Assessment data type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Break</td>
<td>Not available</td>
</tr>
<tr>
<td>CheckBox</td>
<td>Checkbox</td>
</tr>
<tr>
<td>Date</td>
<td>Date</td>
</tr>
<tr>
<td>Date/Time</td>
<td>Date/Time</td>
</tr>
<tr>
<td>HTML</td>
<td>Not available</td>
</tr>
<tr>
<td>Label</td>
<td>Not available</td>
</tr>
<tr>
<td>List Collector</td>
<td>Not available</td>
</tr>
<tr>
<td>Lookup Multiple Choice</td>
<td>Not available</td>
</tr>
<tr>
<td>Lookup Select Box</td>
<td>Not available</td>
</tr>
<tr>
<td>Macro</td>
<td>Not available</td>
</tr>
<tr>
<td>Macro with Label</td>
<td>Not available</td>
</tr>
<tr>
<td>Multi Line Text</td>
<td>String (String option set to Multiline)</td>
</tr>
<tr>
<td>Multiple Choice</td>
<td>Likert Scale</td>
</tr>
<tr>
<td>Numeric Scale</td>
<td>Number</td>
</tr>
<tr>
<td>Reference</td>
<td>Not available</td>
</tr>
<tr>
<td>Select Box</td>
<td>Choice</td>
</tr>
<tr>
<td>Single Line Text</td>
<td>String (String option set to Single line)</td>
</tr>
<tr>
<td>UI Page</td>
<td>Not available</td>
</tr>
<tr>
<td>Wide Single Line Text</td>
<td>String (String option set to Single line wide)</td>
</tr>
<tr>
<td>Yes / No</td>
<td>Yes/No</td>
</tr>
</tbody>
</table>

Migrated components

When you migrate a survey, the system maps records from survey tables to assessment tables.
To create a functional survey on the assessment framework, the system converts survey records to the most logical equivalent assessment survey records. This may mean multiple assessment survey records represent one legacy survey record.

**Migrated components**

<table>
<thead>
<tr>
<th>Survey component</th>
<th>Assessment survey components</th>
</tr>
</thead>
</table>
| Survey master (survey_master) | • Survey definition (asmt_metric_type)  
| | • Assessable record (asmt_assessable_record), for system use only  
| | • Survey category (asmt_metric_category)  |
| Survey question (survey_question_new) | • Survey question (asmt_metric)  |
| Question choice (question_choice) | • Assessment metric definition (asmt_metric_definition)  |
| Survey instance (survey_instance) | • Assessment group (asmt_assessment), for system use only  
| | • Survey instance (asmt_assessment_instance)  |
| Survey response (survey_response) | • Survey instance question (asmt_assessment_instance_question)  
| | • Survey response (asmt_metric_result)  
| | • Category result (asmt_category_result), for system use only  |

**Migrated question review**

To maintain accurate result calculations, you may need to make minor adjustments to some of the migrated survey records to ensure results are calculated correctly.

**Note:** The assessment engine provides a built-in result calculation feature that converts each survey response to a score between 0 and 10. The configuration required to maintain accurate result calculations is advanced and is not recommended for basic survey implementations. If you do not plan to use result calculation data, ignore the information in this section.

For each legacy question migrated, the system creates a survey question record on the Assessment Metric (asmt_metric) table. For legacy questions of the **Multiple Choice** and **Select Box** types, the system also creates a metric definition record, on the Assessment Metric Definition (asmt_metric_definition) table, for each legacy question choice.

**Comparable metric definitions and survey question choices**

<table>
<thead>
<tr>
<th>Survey question choice field</th>
<th>Related metric definition field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text</td>
<td>Display</td>
</tr>
<tr>
<td>Value (can be any string value)</td>
<td>Value (must be a numerical value)</td>
</tr>
<tr>
<td>Order</td>
<td>Value (metric definition with smallest Value is first)</td>
</tr>
</tbody>
</table>
When the system migrates legacy survey question choices, it uses the legacy Order to set each metric definition Value. For the legacy question choice with the smallest Order, the corresponding metric definition Value is set to 1. For the legacy question choice with the next smallest Order, the metric definition Value is 2, and so on.

The Scale definition field on the migrated Survey Question form determines whether smaller or bigger metric definition values equate to a good score in survey result calculations. By default, the scale definition is set to High, meaning bigger values are good. When you migrate a legacy survey, check that the default scale definition makes sense for each question.

For example, the following tables depict a sample migrated question and the metric definitions automatically created for it. Recall that the system uses the order of the legacy survey question choices to set the metric definition value. Excellent has the lowest Order value, so when the system creates a metric definition for this question choice, the Value is set to 1. In this case the default scale definition value, High, does not make sense, as the system will calculate the worst scores for responses of Excellent.

### Legacy question: Please rate the overall quality of your service.

<table>
<thead>
<tr>
<th>Question choice text</th>
<th>Question choice value</th>
<th>Question choice order</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excellent</td>
<td>A</td>
<td>100</td>
</tr>
<tr>
<td>Good</td>
<td>B</td>
<td>200</td>
</tr>
<tr>
<td>Fair</td>
<td>C</td>
<td>300</td>
</tr>
<tr>
<td>Poor</td>
<td>D</td>
<td>400</td>
</tr>
</tbody>
</table>

### Migrated question: Please rate the overall quality of your service.

<table>
<thead>
<tr>
<th>Metric definition display</th>
<th>Metric definition value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excellent</td>
<td>1</td>
</tr>
<tr>
<td>Good</td>
<td>2</td>
</tr>
<tr>
<td>Fair</td>
<td>3</td>
</tr>
<tr>
<td>Poor</td>
<td>4</td>
</tr>
</tbody>
</table>

If there are no Order values for the legacy survey question choices, the system sets each corresponding metric definition Value based on the alphanumerical order of the legacy Text value.

### Migrated question: Please rate the overall quality of your service.

<table>
<thead>
<tr>
<th>Metric definition display</th>
<th>Metric definition value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excellent</td>
<td>1</td>
</tr>
<tr>
<td>Good</td>
<td>2</td>
</tr>
<tr>
<td>Fair</td>
<td>3</td>
</tr>
<tr>
<td>Poor</td>
<td>4</td>
</tr>
</tbody>
</table>

You may also need to change the Scale definition setting for other migrated questions. For details, see the scale definition recommendations for each survey question data type.
Timeline Visualizations

A timeline visualization is a representation of an organization's activities over time.

Typically, timeline visualizations are useful for quickly assessing the impact of future strategic and operational activities such as change requests and projects. Timeline visualizations come in two varieties: a two-dimensional (2D) view where activities are grouped by month, and a three-dimensional (3D) view where activities are grouped in lanes. Both views are interactive, and the 2D view can be printed.

Timeline administrators, users with the timeline_admin role, can set up visualizations to represent ITSM-related activities, such as incidents, problems, changes, and projects. Timeline administrators or users with the timeline_user role can personalize their timeline visualizations from the Settings pane in the visualization.

Activating timeline visualizations adds the predefined CIO Roadmap timeline visualization, which shows your organization's projects grouped by portfolios. Organizational leaders can use the CIO Roadmap to monitor and evaluate the status of current and upcoming projects.

Key terms for timeline visualizations

- **Lane**: A logical grouping of items on the 3D timeline visualization. For example, one lane might show pending projects while another lane shows open projects.
- **Panel**: A block that represents an item record in a 2D timeline visualization, or a block that represents one or more item records in a 3D timeline visualization.
- **Summary view**: A pop-up window that appears when a user clicks a panel in either the 2D or 3D timeline visualization. The summary view contains additional information about the record. Timeline administrators configure the information that appears in the summary view.
- **Marker**: A bar indicating the start of a month in a 3D timeline visualization.
- **Slider**: A tool used to control the time period seen in a 3D visualization.
- **Slider track**: An alternative view of the panels displayed in both the 2D and 3D timeline visualization.
Activate Timeline Visualization

An administrator can activate the Timeline Visualization plugin to access the functionality. The Project Management plugin is activated if it is not already active.

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 Timeline Visualization

Timeline administrators set up timeline visualizations for the organization's leaders by creating a timeline that provides visual representations of the organization's operational and strategic activities.

Additionally, they create timeline visualization views to define what data appears in the summary window when a user clicks a panel on the timeline.

- To create a timeline visualization, navigate to Timeline Visualization > Create New and create a new record.
Timeline visualization configuration form
### Timeline visualization configuration form field descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for the visualization.</td>
</tr>
<tr>
<td>Panel table</td>
<td>Table that provides the records displayed as lanes and panels in the timeline.</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 visualization.</td>
</tr>
<tr>
<td>Relationship field</td>
<td>Field on the table that contains values displayed as lane titles. Typically this field is a reference field or a field that contains a limited range of values.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The CIO Roadmap timeline visualization is a ServiceNow customized visualization for the Project application that does not use the Relationship field.</td>
</tr>
<tr>
<td>Show slider</td>
<td>Check box that enables (selected) or disables (cleared) displaying the timeline slider that users move to change the dates shown.</td>
</tr>
<tr>
<td>Panel name</td>
<td>Field from the Panel table that contains the values displayed in the panel body.</td>
</tr>
<tr>
<td>Panel date</td>
<td>Field from the Panel table that contains the date values displayed in the panel head in 3D view and in the panel body in 2D view. These dates also determine placement of panels on a lane. Only date and date-time fields are available on the choice list.</td>
</tr>
<tr>
<td>Default</td>
<td>Check box that sets (selected) or removes (cleared) the default status of a visualization when you have more than one defined for a specific table. Applications that include a visualization use the default visualization.</td>
</tr>
<tr>
<td>Max items per lane</td>
<td>Maximum number of items that are displayed in a lane in 3D view. The default value is 500.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The field is not visible on the form by default. Configure the form to add this field.</td>
</tr>
</tbody>
</table>
### Timeline visualization configuration filtering and sorting form field descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lane condition</td>
<td>Condition builder used to create filters and apply sorting to values that are used as lanes in 3D view visualizations. For example, if you set <em>(Name) is not (IT)</em> as a lane condition for the CIO Roadmap, then IT no longer appears as a lane in the roadmap, nor does it appear as a lane option in the Settings pane. Removing the filter restores the IT lane to the visualization and to lane options in the Settings pane. To order the results, specify sorting based on relevant field names. For example, to order the portfolio names so that they appear in reverse alphabetical order on the CIO Roadmap, set the sort fields to <em>(Name) z to a</em>.</td>
</tr>
<tr>
<td>Panel condition</td>
<td>Condition builder used to create filters and apply sorting to values that are used as panels in 2D and 3D view visualizations. For example, if you set <em>(State) is one of (Pending, Open, Work in Progress)</em> as the panel condition for the CIO Roadmap, only projects that are in one of those states appear on the roadmap.</td>
</tr>
</tbody>
</table>

### Timeline visualization configuration color options form field descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Panel color key</td>
<td>Field from the Panel table that contains values used for color coding the information displayed. The field selected here determines the values that are available in the Label fields on the form. The CIO Roadmap uses State, which is a field in the Project table. Panels on the CIO Roadmap are color coded according to the project state, which can be Pending, Open, Work in Progress, Closed Complete, Closed Incomplete, and Skipped. Examples of other fields that are suitable for this selection include Priority, Risk, and Approval.</td>
</tr>
<tr>
<td>Label 1</td>
<td>Values to be color coded. The values available are determined by the Panel color key field. For example, the CIO Roadmap is based on the Project table and has the Panel color key set to the State field, which contains the values Pending, Open, Work in Progress, Closed Complete, Closed Incomplete, and Closed Skipped. You can set set specific colors for up to four values from the selected field. Other values are shown in the Default color.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Default color</td>
<td>Color applied to values that are not selected for labels. For example, the CIO Roadmap color codes and creates labels for the values Pending, Open, Work in Progress, and Closed Complete. The additional values, Closed Incomplete and Closed Skipped, use the default color.</td>
</tr>
<tr>
<td>Color 1</td>
<td>Colors that correspond to each of the Label field values. For example, if Label 1 is the Pending state, and Color 1 is red, then panels for projects in the pending state are red.</td>
</tr>
<tr>
<td>Color 2</td>
<td></td>
</tr>
<tr>
<td>Color 3</td>
<td></td>
</tr>
<tr>
<td>Color 4</td>
<td></td>
</tr>
</tbody>
</table>

**Create a Timeline Visualization view**

The timeline visualization view determines which record details appear in the pop-up summary window when a user clicks a panel.

You can create one timeline visualization view per table. For example, if your view shows incident records, you can create a view on the Incident table to show only certain information, such as the incident number, priority, and short description.

If no Timeline Visualization view exists, all panels use the default view that shows all the fields that currently appear on the default view of the form for that table. After you create a Timeline Visualization view for a table, all panels then use that view.

For example, to create a Timeline Visualization view using the Incident form:

1. Navigate to Incident > All.
2. Open an incident.
3. Right-click the form header and select Configure > Form Layout.
4. Under Form view and section, go to the View name field and select New.
5. Enter timeline visualization in the View name field.
6. Click Ok to create the timeline visualization view.
7. Add fields to or remove items from the timeline visualization view using the Available and Selected columns.
8. Click Save.

**Planning Your Timeline Visualization**

Before creating a timeline visualization, you should have a clear idea of the information that you want to display.

This planning process helps you identify the required table and fields, and determine filtering and sorting requirements. Since users can personalize the visualization, avoid setting restrictive filters that may prevent users from finding categories that they are accustomed to seeing. You can use the CIO Roadmap as a starting point for creating your own timeline visualizations.
Use Timeline Visualization

Timeline Visualization provides a high-level view of an organization's strategic and operational activities over time.

Organizational decision makers can use the information in visualizations for activities such as planning future projects and estimating resource requirements. Users can personalize the information displayed with the visualization Settings pane.

Activating the Timeline Visualization application also installs the CIO Roadmap, a timeline visualization that displays an organization's IT projects and portfolios. This following sections use the CIO Roadmap to demonstrate features of timeline visualizations.

Lanes, markers, and panels

Lanes, markers, and panels are the fundamental elements of a timeline visualization. appear in the 3D view only.

Note: Lanes and markers are available in the 3D view only. A panel in the 2D view always represents a single record, while panels in 3D view may represent one or more records.

Lanes

A lane is a channel in which activities are grouped. A visualization can display up to eight lanes at a time. While viewing a visualization, you can use the Settings pane to show or hide individual lanes.

Note: The number of items displayed in a lane depends on the Max items per lane setting on Timeline Visualization form.

Markers

Markers are horizontal lines that cross all lanes and identify a transition to the next month.

Panels

Panels in both 2D and 3D views are color coded according to values that the administrator selects during the initial setup.
In 2D view, panels are grouped by month and stacked in chronological order, from the earliest date to the latest date. By default, the 2D view opens with the current month displayed on the left side of the visualization. You can print visualizations from the 2D view using the browser's print option. In 3D view, panels are grouped in lanes and ordered by date, from earliest to latest. The date that appears on the panel determines its placement in 2D and 3D view. The date displayed is based on a value the timeline administrator selects during initial setup.

Panels appear in the CIO Roadmap according to the planned completion date for the project. In 3D view, projects with the same planned date of completion are consolidated into a single panel. In 2D view, projects with the same planned date of completion are displayed as individual panels.

Panel headers in the CIO Roadmap are color coded based on project state. However, in 3D view, if a panel represents more than one project, the panel header is colored black. The Settings pane contains a key showing each available project state and the corresponding color.

To view additional information about a panel:

- Click a panel for a single record while in 2D or 3D view to open a summary window that contains additional information. Click the heading in the summary window to open the full record.
- Click a panel that represents multiple records to open a list of those records. Click a record number to open the full record.

The timeline administrator can configure the information that appears in summary windows.

**Personalize Timeline Visualizations**

You can configure settings for timeline visualizations like lane and panel conditions, colors, and labels.

**Personalization**

Open the Settings pane and click **Configure**. Complete the form as appropriate (see table).
Visualization personalization

Timeline visualization personalization form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lane conditions</td>
<td>Condition builder used to create filters and apply sorting to values that are used as lanes in 3D view visualizations. For example, if you set (Name) (is not) (IT) as a lane condition for the CIO Roadmap, then IT no longer appears as a lane in the roadmap, nor does it appear as a lane option in the Settings pane. Removing the filter restores the IT lane to the visualization and to lane options in the Settings pane. To order the results, specify sorting based on relevant field names. For example, to order the portfolio names so that they appear in reverse alphabetical order on the CIO Roadmap, set the sort fields to (Name) (z to a).</td>
</tr>
<tr>
<td>Panel conditions</td>
<td>Condition builder used to create filters and apply sorting to values that are used as panels in the visualization. For example, if you set (State) (is one of) (Pending, Open, Work in Progress) as the panel condition for the CIO Roadmap, only projects that are in one of those states appear on the roadmap.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Panel color key</td>
<td>Field from the Panel table that contains values used for color coding the information displayed. The field selected here determines the values that are available in the Label fields on the form. The CIO Roadmap uses State, which is a field in the Project table. Panels on the CIO Roadmap are color coded according to the project state, which can be Pending, Open, Work in Progress, Closed Complete, Closed Incomplete, and Skipped. Examples of other fields that are suitable for this selection include Priority, Risk, and Approval.</td>
</tr>
<tr>
<td>Label 1</td>
<td>Values to be color coded. The values available are determined by the Panel color key field. For example, the CIO Roadmap is based on the Project table and has the Panel color key set to the State field, which contains the values Pending, Open, Work in Progress, Closed Complete, Closed Incomplete, and Closed Skipped. You can set specific colors for up to four values from the selected field. Other values are shown in the Default color.</td>
</tr>
<tr>
<td>Default color</td>
<td>Color applied to values that are not selected for labels. For example, the CIO Roadmap color codes and creates labels for the values Pending, Open, Work in Progress, and Closed Complete. The additional values, Closed Incomplete and Closed Skipped, use the default color.</td>
</tr>
<tr>
<td>Color 1</td>
<td>Colors that correspond to each of the Label field values. For example, if Label 1 is the Pending state, and Color 1 is red, then panels for projects in the pending state are red.</td>
</tr>
</tbody>
</table>

**Note:**

If the Max items per lane field is set to more than 1000, you may observe a delay when displaying the timeline data using Internet Explorer (IE) as the browser.

---

**The Settings pane**

Element names in the Settings pane vary based on the table and fields used to create the visualization.
The Settings pane contains the following elements:

### Settings pane elements

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>Identifies the type of information that is color coded on the timeline, such as state or priority. It also lists the color assigned to each possible value, such as pending state and open state.</td>
</tr>
<tr>
<td>Element</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Configure</td>
<td>Allows you to personalize a visualization by creating filters on lane information and panel information, specifying sort order for results, and reassigning panel colors. These changes affect your view of the visualization only.</td>
</tr>
<tr>
<td>View</td>
<td>Allows you to switch between 2D and 3D view.</td>
</tr>
<tr>
<td>View &lt;table&gt; List</td>
<td>Opens a separate browser tab showing the complete record list for the associated table.</td>
</tr>
<tr>
<td>Portfolio</td>
<td>Allows you to click lane names to add or remove them from the visualization. While the visualization is in 2D view, the Settings pane displays a Show all &lt;records&gt; button that allows you to override lane filters applied to the initial setup.</td>
</tr>
</tbody>
</table>

**Use the slider and slider track**

The slider and slider track are useful for quickly navigating to any point in time on a visualization.

For the CIO Roadmap, the slider track allows you to quickly view the distribution of projects over time and determine project states. While in 3D view, click and drag the slider to move the timeline forward or backward. In 2D view, click and drag the slider track right or left to move the timeline forward or backward.

The slider track provides an alternative view of panels on a visualization. For the CIO Roadmap, a colored dot in the slider track indicates the presence of one or more projects for a given day. The different dot colors correspond to different project states. This allows you to scan the slider track to identify projects of interest by their color, and then use the slider or slider track to quickly navigate to those projects. For example, if you are interested in projects that are in a pending state, you can use the slider to navigate to the colored dots that represent that state.

**Note:** Dots in the slider track do not correspond one-to-one with panels in a visualization. A dot represents the presence of one or more projects on a given date. In 3D view, if there is more than one project for a given day, all of the projects for that day are combined into a single panel on the roadmap. When the slider track is populated, projects in a multi project panel are analyzed for project state and then represented as appropriately colored dots in the slider track.

Similarly, you can use the slider or slider track in conjunction with the calendar to quickly navigate to any point in time. For example, if you are concerned about resource issues in April 2014 because you see a large cluster of dots during that time, dragging the slider or slider track to those dots brings those projects into view. Click the individual panels to view additional information.

**View timeline visualization**

You can view timeline visualizations from a project.

1. Navigate to **Project > Projects > All**.
2. Scroll to the bottom of the list and click the **Timeline Visualization** related link.

By default, the CIO Roadmap opens in three-dimensional (3D) view with the current date at the forefront of the timeline. You can use the Settings pane to change between two-dimensional (2D) and 3D view. As soon as you view a timeline visualization, it is considered open.
personalized. After that, you see your personalized view even if the timeline administrator makes changes to the default visualization.

Timeline administrators can create timeline visualizations on other tables. If you are not sure whether a timeline visualization exists for a certain application, use the application navigator to open the application of your choice, and click All. If a timeline visualization exists for the application’s table, a Timeline Visualization related link appears.

**Work with timeline visualizations**

There are various tools that allow you to move visualizations backward and forward in time depending on whether you are in 2D or 3D view.

The following options are available for navigating between months.

**2D views**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dragging</td>
<td>Hold down the left mouse button and drag the slider track right or left to view other months.</td>
</tr>
<tr>
<td>Left and right arrow keys</td>
<td>Press the left or right arrow keys on the keyboard to move the timeline forward or backward.</td>
</tr>
<tr>
<td>Mouse wheel button</td>
<td>Scroll the wheel to move the timeline forward or backward.</td>
</tr>
<tr>
<td>Right and left navigation arrows</td>
<td>Click the arrows to move from month to month. Arrows do not appear if there are no additional months to view.</td>
</tr>
</tbody>
</table>

The following options are available for navigating stacked panels.

**Navigating stacked panels**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dragging</td>
<td>Hold down the left mouse button and drag the stack up or down to view other panels.</td>
</tr>
<tr>
<td>Up and down navigation arrows</td>
<td>Click the arrows in a stack to view additional panels for the same month. Arrows do not appear if there are no additional panels to view.</td>
</tr>
</tbody>
</table>

The following options are available for navigating in 3D view.

**3D view**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dragging</td>
<td>Hold down the left mouse button and drag the slider along the slider track to move the timeline forward or backward.</td>
</tr>
<tr>
<td>Mouse wheel button</td>
<td>Scroll the wheel to move the timeline forward or backward.</td>
</tr>
<tr>
<td>Up and down arrow keys</td>
<td>Press the arrow keys to move the timeline forward or backward.</td>
</tr>
</tbody>
</table>
Installed with Timeline Visualizations

Several components are installed with timeline visualizations.

Tables

Timeline visualization adds the following table.

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeline Visualization (roadmap_page)</td>
<td>Stores all available timeline visualizations.</td>
</tr>
<tr>
<td>Personalize Timeline (roadmap_user_page)</td>
<td>Stores timeline personalization settings for all timeline visualizations.</td>
</tr>
</tbody>
</table>

Plugins

Timeline visualization activates the following plugin, if it is not already active.

<table>
<thead>
<tr>
<th>Plugin Name</th>
<th>Plugin ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Management</td>
<td>com.snc.project_management_v3</td>
<td>Tools that aid in planning, organizing, and managing projects by applying basic task management processes.</td>
</tr>
</tbody>
</table>

UI Policies

Timeline visualization adds the following UI policy.

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Timeline Visualization configuration Page to enable/disable certain fields</td>
<td>Timeline Visualization (roadmap_page)</td>
<td>Script that hides fields in the Timeline Visualization form when the form loads.</td>
</tr>
</tbody>
</table>

Script Includes

Timeline visualization adds the following script includes.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Roadmap2DUtil</td>
<td>Timeline Visualization - 2D API to generate data for lanes and panels.</td>
</tr>
<tr>
<td>RoadmapCommonUtil</td>
<td>Timeline visualization common utility to handle generic functions.</td>
</tr>
<tr>
<td>RoadmapConfig</td>
<td>Timeline visualization utility allowing configuration through the Timeline Visualization (roadmap_page) table.</td>
</tr>
<tr>
<td>RoadmapItems</td>
<td>Timeline visualization utility to get lane items.</td>
</tr>
</tbody>
</table>
### Name | Description
--- | ---
RoadmapUtil | API to generate data for lanes and panels.

## Client Scripts

Timeline visualization adds the following client scripts.

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Roadmap Color Choice</td>
<td>Timeline Visualization (roadmap_page)</td>
<td>Sets color values for the color choice fields in the timeline visualization configuration page.</td>
</tr>
<tr>
<td>Roadmap Item Table</td>
<td>Timeline Visualization (roadmap_page)</td>
<td>Allows changing the color fields for the item_color_key whenever there is a change to the panel table.</td>
</tr>
<tr>
<td>Roadmap On Load</td>
<td>Timeline Visualization (roadmap_page)</td>
<td>Loads the personalized version of the roadmap/visualization.</td>
</tr>
<tr>
<td>Roadmap Panel Table Change</td>
<td>Timeline Visualization (roadmap_page)</td>
<td>Allows changing the field name for item_color_key whenever there is a change to the panel/visualization table.</td>
</tr>
</tbody>
</table>

## Business Rules

Timeline visualization adds the following business rule.

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check only one default</td>
<td>Timeline Visualization (roadmap_page)</td>
<td>Checks if another visualization is already set as default when user sets a new visualization as the default.</td>
</tr>
</tbody>
</table>

## Timeline visualizations roles

Timeline visualizations provides two roles.

### Roles

<table>
<thead>
<tr>
<th>Role Title (Name)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeline administrator [timeline_admin]</td>
<td>Create and edit timeline visualization pages and view timeline visualizations.</td>
</tr>
<tr>
<td>Timeline user [timeline_user]</td>
<td>View timeline visualizations. Timeline user access is also granted to users with the project_manager and project_user roles.</td>
</tr>
</tbody>
</table>
Visual Task Boards

Visual Task Boards (VTB) transform the navigation of lists and forms into an interactive graphical experience.

With Visual Task Boards, you can view and update multiple task records, which appear as cards that can be moved between lanes. An activity stream on the board displays recent activity so you can easily track changes to tasks. You can add task cards from any table that extends Task to intuitively and easily track updates and edit records directly from the board. Any user can use task boards, regardless of role, though access control rules (ACLs) may limit which cards each user can see. The Visual Task Board interface provides a graphic-rich environment suited for managing and collaborating on records. For example, a support manager might create a board for her team to track their assigned incidents by state in real time.

This video demonstrates how Visual Task Boards work.

Note: UI16 or UI15 is required to use Visual Task Boards.

The following podcast offers additional information on the use of Visual Task Boards.

Activate Visual Task Boards

Visual Task Boards are active by default on new instances. For upgraded instances, you can activate the Visual Task Boards plugin [com.glide.ui.vtb] if you have the admin role.

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**.

### Installed with Visual Task Boards

Several types of components are installed with Visual Task Boards.

### Tables installed with Visual Task Boards

Visual Task Boards add the following tables.

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board Member (vtb_board_member)</td>
<td>Stores a record for each member of each task board.</td>
</tr>
<tr>
<td>Private Task (vtb_task)</td>
<td>Stores a record for each personal task on each freeform board.</td>
</tr>
<tr>
<td>Visual Task Board (vtb_board)</td>
<td>Stores a record for each task board.</td>
</tr>
<tr>
<td>Visual Task Board Card (vtb_card)</td>
<td>Stores a record for each task card on each task board.</td>
</tr>
<tr>
<td>Visual Task Board Card History (vtb_card_history)</td>
<td>Stores records for certain task card changes, such as lane or assignee changes. Each record indicates the previous value and the new value.</td>
</tr>
<tr>
<td>Visual Task Board Lane (vtb_lane)</td>
<td>Stores a record for each lane on each task board.</td>
</tr>
</tbody>
</table>

### Properties installed with Visual Task Boards

Visual Task Boards add the following properties.

**Note:** To open the System Property (sys_properties) table, enter `sys_properties.list` in the navigation filter.
### Property

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| vtb.board.upload_limit | Sets the maximum file size in megabytes allowed for each task card attachment.  
  - **Type**: integer  
  - **Default value**: 10  
  - **Location**: System Property (sys_properties) table |

### Script includes installed with Visual Task Boards

Visual Task Boards add the following script includes.

<table>
<thead>
<tr>
<th>Script include</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VisualTaskBoards</td>
<td>Provides general utilities for Visual Task Boards.</td>
</tr>
<tr>
<td>VTBBoardSecurity</td>
<td>Provides security utilities to control board access.</td>
</tr>
<tr>
<td>VTBGetBoardsByUser</td>
<td>Provides a method that retrieves all the boards a specified user owns or is a member of.</td>
</tr>
<tr>
<td>VTBTaskSecurity</td>
<td>Provides security utilities to control task access.</td>
</tr>
</tbody>
</table>

### Client scripts installed with Visual Task Boards

Visual Task Boards add the following client scripts.

<table>
<thead>
<tr>
<th>Client script</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Kanban Choice</td>
<td>Visual Task Board (vtb_board)</td>
<td>Adds the -- Kanban Board -- option to the Lane field field. This option indicates that the task board is a flexible board.</td>
</tr>
</tbody>
</table>

### Business rules installed with Visual Task Boards

Visual Task Boards add the following business rules.

<table>
<thead>
<tr>
<th>Business rule</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add members to live group</td>
<td>Board Member (vtb_board_member)</td>
<td>If a Connect Chat conversation is created for a task board, this business rule adds the board members as conversation members.</td>
</tr>
<tr>
<td>Remove member from live group</td>
<td>Board Member (vtb_board_member)</td>
<td>If a Connect Chat conversation exists for a task board and a user is removed from the board members, this business rule removes the user from the conversation members.</td>
</tr>
<tr>
<td>Business rule</td>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>--------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Remove member from VTB</td>
<td>Live Group Member</td>
<td>If a Connect Chat conversation exists for a task board and a user is removed from the conversation members, this business rule removes the user from the task board members.</td>
</tr>
<tr>
<td>Sync board name to Connect</td>
<td>Visual Task Board</td>
<td>If a Connect Chat conversation exists for a task board and someone updates the board name, this business rule updates the conversation name.</td>
</tr>
<tr>
<td>Sync chat name to VTB board</td>
<td>Live Group Profile</td>
<td>If a Connect Chat conversation exists for a task board and someone updates the conversation name, this business rule updates the board name.</td>
</tr>
<tr>
<td>Sync Members With VTB</td>
<td>Live Group Member</td>
<td>If a Connect Chat conversation exists for a task board and a user is added to the conversation members, this business rule adds the user as a board member.</td>
</tr>
<tr>
<td>Update Board on Card Change</td>
<td>Visual Task Board Card</td>
<td>Triggers the system to update the task board when changes occur to the cards.</td>
</tr>
<tr>
<td>Update Board on Lane Change</td>
<td>Visual Task Board Lane</td>
<td>Triggers the system to update the task board when changes occur to the lanes.</td>
</tr>
<tr>
<td>update board on lane change</td>
<td>Board Member</td>
<td>Triggers the system to update the task board when changes occur to the board members.</td>
</tr>
<tr>
<td>VTB Previous Additional Assignees</td>
<td>Private Task</td>
<td>Triggers the system to send an email notification to users when they are designated as additional assignees for cards.</td>
</tr>
</tbody>
</table>

Notifications installed with Visual Task Boards

Visual Task Boards add the following notifications.

<table>
<thead>
<tr>
<th>Notification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTB additional assignee notification</td>
<td>Sends an email notification to users when they are designated as additional assignees for tasks.</td>
</tr>
<tr>
<td>VTB assignee notification</td>
<td>Sends an email notification to users when they are designated as the primary assignees for personal tasks.</td>
</tr>
<tr>
<td>VTB lane change notification</td>
<td>Sends an email notification to a task’s assignees when the task changes lanes.</td>
</tr>
</tbody>
</table>
Supported browsers for Visual Task Boards

The system supports Visual Task Boards on most modern browsers.

Supported browsers

- The latest public release of Firefox or Firefox ESR
- The latest public release of Chrome
- Safari version 9.1 and later
- 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 11 is susceptible to memory leaks, which may impact performance, especially in Windows 7.

- Access Visual Task Boards on your mobile device using either a browser or the native mobile app. See Support for ServiceNow Classic for more information.

Scripting support

Visual task boards do not interact with client scripts. Use a UI policy or a data policy instead.

Board structure

There are different types of task boards for different kinds of task management. All types of boards share the same overall structure.

<table>
<thead>
<tr>
<th>Board type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Freeform boards</td>
<td>Display any kind of task record, including personal tasks. Members of freeform boards can add and remove task cards and lanes.</td>
</tr>
<tr>
<td>Flexible boards</td>
<td>Display tasks that match the configured filter against a particular table. Members of flexible boards can add task cards, which are removed automatically when the tasks no longer match the filter conditions. Members can define custom lanes, similar to a freeform board.</td>
</tr>
<tr>
<td>Guided boards</td>
<td>Display tasks that match the configured filter against a particular table, like flexible boards. Members of guided boards can add task cards, which are removed automatically when the tasks no longer match the filter conditions. Guided board lanes correspond to field values and cannot be edited in most cases.</td>
</tr>
</tbody>
</table>
The icon beside the board name on the Task Boards page identifies the type of board. Freeform boards appear with a grid of four squares; flexible boards appear with a vertical line beside two squares; guided boards appear with two vertical lines.

Task Boards screen

All boards have these elements:
## Board elements

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quick panel</td>
<td>Displays labels and users associated with the board. Board members can use the quick panel to filter cards or to quickly label or assign tasks. Members can also configure what appears in the quick panel.</td>
</tr>
<tr>
<td>Lanes</td>
<td>Organize cards on a board into vertical groups. These groups often represent the status of the task, such as To Do, Doing, and Done. Each board is composed of one or more lanes. When using a guided board, each lane represents a possible field value. For example, a board on the Incident table can display one lane for each State value such as New, Active, or Resolved. Users can move cards from one lane to another to update the task that card represents.</td>
</tr>
<tr>
<td>Cards</td>
<td>Represent individual tasks. Users can add comments, attachments, and labels to cards and assign users to cards. Each card is tied to a task record; updating one immediately updates the other. For freeform boards, each card represents a personal task. For flexible and guided boards, each card represents a record from the list that board was created from.</td>
</tr>
<tr>
<td>Task board tools</td>
<td>Displays board information, a board members, the board activity stream, and board labels.</td>
</tr>
</tbody>
</table>
Visual Task Board use

Any user can create, view, and edit freeform, flexible, and guided visual task boards, and add users to these boards as members.

You can create a freeform board and add cards from multiple task tables, or create a flexible or guided board from an existing list of records.

Create a freeform board

You can create freeform task boards for tracking any kind of task or project.

Role required: none

2. Next to My Task Boards, click New, or if you have never created a task board before click Create New Visual Task Board.
3. From the Create New Board window, click Freeform.
   A new task board opens with the default freeform lanes, To Do, Doing, and Done.
4. Click the board name and enter a new name.

After the board is created, board members can:

- Add and modify lanes
- Create and modify task cards
- Add and remove members
- Configure the look and feel

Create a data driven board

You can create a flexible or guided task board for any table that extends Task, such as Incident or Change.

Role required: none

2. Next to My Task Boards, click New, or if you have never created a task board before click Create New Visual Task Board.
3. From the Create New Board window, click Data Driven Board.
4. From the Task Table list, select a base table of tasks on which to base your board, for example, an incident table.
5. Optional: From the Lane Field list, select the field you want to use for the lane headers. Create a Flexible board with editable lane headers by selecting None.
   The type of board that is created and the lanes that appear on the board depend on which type of column you select. If you select a reference or choice column, the board is a guided board. Each lane in a guided board represents one possible value for that column and the cards appear in the appropriate lane. For example, if you create a guided task board for incidents using the State column, the board shows one lane for each incident state, such as New or Closed. If you select a column that is not a reference or choice, the board is a flexible board and the board shows the default lanes, To Do, Doing, and Done, with all cards in the To Do lane.
6. Optional: Create a filter to show only the records you want to work with. For example, you might filter out incidents that are not assigned to you.
Any card that no longer fits the parameters of the filter is automatically removed from the task board.

7. Optional: Click the board name and enter a new name.

Note: For guided boards created from choice fields, such as State, the system creates a lane for each possible choice value. For guided boards created from reference fields, the system creates a lane only for each value in use by a task card. Lanes are added as needed if the reference field values change.

After the board is created, board members can:
- Add and modify lanes
- Create and modify task cards
- Add and remove members
- Configure the look and feel

Delete a task board

You can delete any task board you own.

Role required: none

Deleting a board does not impact the underlying task records. However, you cannot recover a board after you delete it.

2. Under Boards you own, point to a board and click the delete icon (X).
3. In the confirmation dialog, click Delete.

Add or modify lanes

Any board member can edit board lanes.

Role required: none

When you create a freeform or flexible task board, it includes the default lanes To Do, Doing, and Done. Any board member can change the names and add new lanes to accommodate the task workflow you want to track.

Unlike guided boards, the lanes on a freeform or flexible task board do not match possible field values.

Note: You cannot remove lanes from guided boards.

1. Open a task board.
2. Perform any of the following actions.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Create a new lane   | 1. Scroll past the last lane and click **Add Lane**.  
2. Enter a title for the lane, then press the Enter key.  

The **Add Lane** option is always available for freeform and flexible boards. It is available for guided boards only if the lanes are based on a reference field, such as **Assigned to**. |
| Rearrange lanes     | Click a lane header and drag the lane to the desired drop zone. To cancel the move, press the Escape key while you drag the lane.  
You can also change the lane order from the board configuration menu. |
| Hide a lane         | 1. Click the lane menu (○) in a lane header.  
2. Select **Hide Lane**.  
You can restore hidden lanes from the board configuration menu. |
| Delete a lane       | 1. Click the lane menu in a lane header.  
2. Select **Delete Lane**.  
3. In the confirmation dialog box, click **Delete**.  
When you delete a lane on a freeform or flexible board, all the cards in the deleted lane are archived.  
The **Delete Lane** option is always available for freeform and flexible boards. It is available for guided boards only if the lanes are based on a reference field, and only for lanes that contain no cards. |

**Task cards**

A Visual Task Board task card can represent a personal task or a record on a table.  
You can add task cards, edit task card details, add labels to cards, and access the underlying task record the card represents, depending on the board type.

**Note:** Each board can display up to 2,000 cards by default. When the number of tasks exceeds the maximum, a warning appears and the system determines which cards to show by most recent update time. Administrators can configure a different maximum card limit for freeform boards and for flexible and guided boards.

**Freeform board tasks**

You can add personal task cards directly to lanes on a freeform board. You can also add other kinds of task cards to a freeform board from a list or form.
Add a personal task to a freeform board
You can add cards directly to a freeform board lane. These cards are called personal tasks and represent records on the Private Task (vtb_task) table.

Role required: none

1. In a lane header, click the lane menu ( ) and select Add Task. Alternatively, click Add Task at the bottom of a lane.
   A new task card appears in the lane.
2. Enter a short description for the new task card.
3. To save the card, click another area of the board or press Enter.

Add a task to a freeform board from a form
You can add a task card to a freeform board from any table that extends Task. These cards represent records on whichever table you add them from.

Role required: none

You can add cards from multiple task tables, such as Incident or Problem, to the same freeform board.

1. Open a task record, such as an incident.
2. Click the menu icon ( ) or right-click the form header to show the form context menu.
3. Select Add to Visual Task Board.
   A pop-up window appears with a list of freeform task boards.

4. Click the name of the board you want to add the card to.
   A confirmation message appears.
5. To view the board, click the board name in the confirmation message.
   The task appears in the first lane by default.
Add a task to a freeform board from a list

You can add a task card to a freeform board from any table that extends Task. These cards represent records on whichever table you add them from.

Role required: none

You can add cards from multiple task tables, such as Incident or Problem, to the same freeform board.

1. Navigate to a list of task records, such as Incident > Open.
2. Perform either of the following actions.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add one task</td>
<td>Right-click a record and select Add to Visual Task Board</td>
</tr>
<tr>
<td>Add multiple tasks</td>
<td>Select the check box beside each record you want to add and select Add to Visual Task Board from the actions choice list</td>
</tr>
</tbody>
</table>

A pop-up window appears with a list of freeform task boards.

3. Click the name of the board you want to add the card to. A confirmation message appears.
4. To view the board, click the board name in the confirmation message. The task appears in the first lane by default.

Add a task to a flexible or guided board

You can add cards directly to a flexible or guided board lane. These cards represent records on whichever table the board is associated with.
Role required: none

1. In a lane header, click the lane menu ( ) and select **Add Task**. Alternatively, click **Add Task** at the bottom of a lane.

   A pop-up window appears with a new record. Fields are populated based on any filter conditions for the board and, for guided boards, the lane you add the card to.

   Consider the example of a guided board that shows incidents with the **Software** category, with a lane for each assignee. If you add a card to the **ITIL User** lane, the new incident record **Category** and **Assigned to** fields are automatically set to **Software** and **ITIL User**.

2. Complete the form and click **Submit**.

   A new task card appears in the lane.

---

**Edit card details**

When you click a card on a Visual Task Board, a pop-up window appears with additional details.

Role required: none

You can edit certain values from the card details. Updating these values also updates the underlying task record.
Card details

1. Click a card.
   The details for that card appear in a pop-up window.
2. Alternatively, you can click an entry in the activity stream to view the details for the associated card.
3. From the card details you can:
- Click the card title to rename the card.
- Modify the short description.
- Add comments or work notes in the activity stream.
- Edit the assignees.
- Click one or more of the available labels to add a label to the card.
- Add or remove file attachments.
- Create a checklist.
- Archive the card (freeform boards only).
- Move the card to a different board (freeform boards only).

**Label a task card**

Labels help categorize tasks and visually distinguish them on the task board.

*Enable* labels for the board.

Role required: none

You can filter the visible tasks to show only those with certain labels. Labels appear on cards as colored dots.

---

**Task card labels**

You can add one or more labels to a task card.

Do one of the following actions.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Add a label to a card from the quick panel</strong></td>
<td>1. Drag a label from the quick panel directly to a task card.</td>
</tr>
<tr>
<td></td>
<td>2. Drop the label in the drop zone.</td>
</tr>
<tr>
<td><strong>Add a label to a card from the card details</strong></td>
<td>1. Open the card details for a task.</td>
</tr>
<tr>
<td></td>
<td>2. Click the details tab (i).</td>
</tr>
<tr>
<td></td>
<td>3. Under <strong>Labels</strong>, select one or more labels. Point to a label to display its name.</td>
</tr>
<tr>
<td></td>
<td>4. Close the card detail pop-up window.</td>
</tr>
</tbody>
</table>
You can use configuration options to *rename or disable* labels or to *hide* labels altogether.

**Assign a task to a user**

Assignees represent ownership of task cards and the associated records. Each task card can have one primary assignee and multiple additional assignees.

You can filter the visible tasks on a board to show only tasks assigned to a certain user. Assignees appear on cards as avatars.

When a card changes lanes, all the assignees receive an email notification.

For flexible and guided boards, the primary assignee corresponds to the underlying task’s **Assigned to** field. For example, on a board created from the Incident table, if you add Joe Employee as the primary assignee for a card, the associated incident is assigned to Joe. Note that assignment rules on the associated table may restrict who you can make the primary assignee of a card. If you attempt to assign a task card to a user in a way that violates an assignment rule, a notification appears and the assignment does not take place.
**Note:** Assignees are not automatically granted access to the board. Only members can access the board.

Do one of the following actions.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Add an assignee from the quick panel** | 1. Drag a user’s avatar from the quick panel directly to the task card.  
2. Drop the avatar in the **Primary** or **Additional** drop zone. |

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Add an assignee from the card details** | 1. Open the card details for a task.  
2. Click the assignees tab (👤).  
3. Click **Add Primary Assignee** or **Add Additional Assignee**. The **Add Primary Assignee** option is not available if there is already a primary assignee.  
4. Select a user.  
5. Close the card detail pop-up window. |

The system sends an email notification to inform the new assignee of the change.

**Add an attachment to a task card**

You can add an attachment to a record within a task board.  
Role required: none  
Adding an attachment to a task card also adds the attachment to the underlying task record.
Add attachment

1. Click a card.
2. Click the attachment tab ( ).

3. Click **Add Attachment** and select a file to add as an attachment.

**Visual Task Board checklists**

Checklists help you track the progress of tasks on your Visual Task Board. Checklists are available as a tab in the card details.
Sample checklist

You can add, remove, or rearrange checklist items. You can also save a checklist as a template for future use on other cards. Any user can create or edit a checklist. When the compact card view is disabled, the task card displays a progress bar to show how many items are complete.
You can also use checklists with task records in the standard interface. For more information, see Checklists.

Create a new checklist for a card
You can create a unique checklist for each Visual Task Board card.

Role required: none
1. Open the card details for a task.
2. Click the checklist tab (✓).
3. Click Add Item.
4. Enter text for the checklist item.
5. Press the Enter key to add the checklist item.
6. Create as many additional checklist items as desired.
7. To delete a checklist item, click the minus (-) icon.
8. Optional: To reorder checklist items, click the drag icon (_drag_ ) and drag a checklist item to a different position in the list.
9. Optional: Save the checklist as a template for easy reuse.
   a) Click the more icon (More) beside the Checklist formatter.
   b) Select Save as Template.
A dialog box appears.

c) Enter a descriptive template name to identify the checklist.
When a user creates a checklist from a template, all templates are listed in alphabetical order and there is no way to filter which templates appear. To provide a better user experience, consider implementing a naming system for checklist templates. For example, include the name of the table or another identifier to clarify how the checklist should be used.

d) Click **Save**.

10. Optional: To create a task from a checklist item:

   a) Point to a checklist item and click the create task icon (✓).

   b) Select the type of task you want to create.
   An administrator can configure which task types are available.
   The new task record appears in a pop-up window. The short description is automatically populated with the checklist item text.

   c) Fill in the form with additional detail as necessary.

   d) Click **Update**.

*Create a checklist from a checklist template*
In a Visual Task Board card, you can quickly create a checklist from a checklist template you previously created.

Create at least one checklist template.
Role required: none

A template saves time by creating checklist items automatically. You can add, edit, or remove checklist items without impacting the template.

1. Open a task card that does not already contain a checklist.

2. Click the checklist tab (✓).

3. Click the more icon (•).
   The more icon does not display unless you have added an item to the checklist, or if you have a pre-existing checklist template.

4. Under **Copy items from**, select a template.
The checklist items appear automatically.

*Delete a checklist from a card*
You can remove a checklist from a Visual Task Board card.

Role required: none

1. Open a task card that contains a checklist.

2. Click the checklist tab (✓).

3. Click the more icon (•).

4. Select **Remove Checklist**.
   A confirmation dialog box appears.
5. Click **Delete**.

*Configure which types of tasks can be created from checklist items*
A system property controls which types of tasks you can create from a Visual Task Board checklist item.

Role required: admin

You might want to add custom tables or remove tables you do not use.

1. Navigate to `sys_properties.list`.
2. Locate the `glide.ui.create_task_type_option_list` property.
3. Edit the **Value** to add or remove tables.

You can add any table that extends Task (task). Use the table name, not the label. For example, you would enter `change_request`, not Change Request. Ensure the tables listed are separated by commas, with no spaces.

The property value populates the task type selection list users choose from when they create a task from a checklist item. Note that users can only see task types for which they have the appropriate access roles.

---

**Archive a card**

Archiving a card is a non-destructive way to remove a card from a freeform board.

Role required: none

You can archive cards you are no longer working on to reduce visual clutter. Note that it is only possible to archive cards on a freeform board.

1. Perform one of the following actions.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Archive one card from the lane view** | 1. Point to a card and click the X icon that appears in the corner.  
2. In the confirmation dialog, click **Archive**. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive one card from the card details</td>
<td>1. Click a card and view the Details tab.</td>
</tr>
<tr>
<td></td>
<td>2. Under Tools, click Archive.</td>
</tr>
<tr>
<td></td>
<td>3. In the confirmation dialog, click Confirm.</td>
</tr>
</tbody>
</table>

| Archive all the cards in a lane             | 1. In the lane header, click the more options icon.                         |
|                                             | 2. Select Archive All Tasks.                                                |
|                                             | 3. In the confirmation dialog, click Archive.                               |

2. To see all archived cards for the current board, from the board navigation panel, open the board information menu (i) and click View Archived Tasks.

The Archived Tasks window appears.

3. To restore an archived card, point to it and click Restore.

Access a task record

You can open the form view of any task card. Viewing a task record on a form allows you to see all fields for that record, including fields that are not visible in the card details.

Role required: none

Do one of the following actions.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access the record from the task card</td>
<td>Click the record number on the task card.</td>
</tr>
<tr>
<td>Access the record from the card details</td>
<td>1. Open the card details for a task.</td>
</tr>
<tr>
<td></td>
<td>2. Click the record number in the header.</td>
</tr>
</tbody>
</table>

Move a card to a different lane

You can move a card from one lane to another.

Role required: none

When you move a card to a different lane on a guided board, the field on which the lanes are based is updated to reflect the new lane value.

1. Open a Visual Task Board.
2. Select a card and drag it to a different lane.

To cancel the move, press the Escape key while you drag the card.

**Note:** All mandatory fields on a record must be filled in to move the associated card to a new lane. For example, assume you have a guided board based on the Incident (incident) table, with a lane for each State. The Close code and Close notes fields become mandatory when the State changes to Closed. If you attempt to move an incident card from the New lane to the Closed lane, a pop-up view of the form appears and prompts you to fill in the mandatory fields.
Move a card to a different board

You can move a card from one freeform board to another.

1. Open the card details.
2. In the details tab (i), click Move Card.
3. In the pop-up window that appears, select the board and lane to move the card to.
   The board selection list displays freeform boards only.

Task board tools

The task board tools area in a Visual Task Board contains several tabs, each represented by an icon.

Click an icon to open the tab. Click the same icon again to hide the tab. The tabs you see for each conversation depend on the conversation type and other conditions.

Conversation tool tabs

<table>
<thead>
<tr>
<th>Tab icon</th>
<th>Tab name</th>
<th>Description</th>
</tr>
</thead>
</table>
| ![Info icon](image) | Info | Contains the following information about the task board:
- Name
- Board type
- Table name and a link to open the table view (visible on data driven boards only)
- Filter conditions (visible on data driven boards only)
- Lane field (visible to the board owner, on data driven boards only)
- Owner
- Number of lanes
- Number of cards
- URL |
<p>| <img src="image" alt="Members icon" /> | Members | Lists all members and assignees of the board. You can add or remove board members, promote assignees to be members, and filter the board by member or assignee. |
| <img src="image" alt="Labels icon" /> | Labels | Use labels to visually distinguish tasks on the task board. Filter board contents by toggling the label. You need to enable labels before being able to use this tab. |</p>
<table>
<thead>
<tr>
<th>Tab icon</th>
<th>Tab name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Activity Icon]</td>
<td>Activity</td>
<td>Displays all of the activity for cards on the board.</td>
</tr>
<tr>
<td>![Configuration Icon]</td>
<td>Configuration</td>
<td>Configure the settings for the task board. This setting is only available for the board owner. For more information, see <em>Configure the task board</em>.</td>
</tr>
</tbody>
</table>

**View board information**

You can display key information about any task board.

Role required: none
Board owner's view of board information

1. Open a task board.
2. Open the task board tools and click the board information icon (i).

Add a board as a favorite

Add boards you access frequently to the application navigator using the favorite option.

Role required: none
Adding a board as a favorite is only available in UI16.

1. Navigate to Self Service > Visual Task Boards.
2. From the board you want to favorite, select the information icon from the board tools. Then select the star.
3. Remove the board as a favorite by clearing the star icon.

**View a task board in a list**

You can view a task board in the list view using the board information option.

Role required: none

1. Open a task board.
2. Open the task board tools and click the board information icon (i).
3. Click View List at the bottom of the information panel.
   The cards from the board open in the list view.

*Note:* The freeform board list view only shows cards made by the board and no other tasks that might be added manually.

**Add or remove a task board member**

You can add and remove task board members using the members tab of the activity stream. You can also promote assignees to board members.

Role required: none

Only members of a task board can access the board. Any board member can add or remove other members.

1. On a Visual Task Board, open the task board tools.
2. Click the members tab.

3. Perform one of the following actions.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a member</td>
<td>1. In the Users section, click Add Members.</td>
</tr>
<tr>
<td></td>
<td>2. Enter a user's name or select a user from the drop-down menu.</td>
</tr>
<tr>
<td>Remove a member</td>
<td>1. In the Members section, point to a user.</td>
</tr>
<tr>
<td></td>
<td>2. Click the remove icon (−).</td>
</tr>
<tr>
<td>Promote an assignee to a member</td>
<td>1. In the Assignees section, point to a user.</td>
</tr>
<tr>
<td></td>
<td>2. Click the upward arrow icon.</td>
</tr>
<tr>
<td>Promote all assignees to members</td>
<td>In the Assignees section, click Promote All.</td>
</tr>
</tbody>
</table>
Visual Task Board SLA indicators

SLA (service level agreement) indicators alert board members if any cards on the board have breached SLAs.

When SLA indicators are enabled, a status bar appears on each card that has an associated SLA. If any cards have breached SLAs, an alert appears at the top of the board and a filter option appears in the quick panel. The indicator displays the elapsed percentage of the SLA. If there are multiple SLAs associated with a task card, the indicator displays the status of the SLA with the greatest elapsed percentage.
Visual Task Board with SLA indicators enabled
Any board member can enable SLA indicators from the board configuration menu. The setting applies to the current user only.

**Share a Visual Task Board in a Connect conversation**

You can share a Visual Task Board in a Connect Chat or Connect Support conversation.

Role required: none

1. Navigate to **Self-Service > Visual Task Boards**.
2. Drag a task board to a Connect mini window.
   A link to the task board appears in the conversation. The task board is also listed in the conversation tools, which are visible in the Connect workspace. Only conversation members who are members of the board can access it. If you share a task board in a record conversation, it appears as a URL in the record activity stream.

**Create a Connect conversation from a Visual Task Board**

Create a Connect Chat conversation from a Visual Task Board to collaborate with board members and keep track of activity as it happens.

Role required: none

When you create a conversation from a task board, all the board members become members of the conversation. The members are synchronized between the task board and the conversation. For example, if you remove a user from the conversation, the system automatically removes the user from the board as well.

1. Navigate to **Self-Service > Visual Task Boards**.
2. Open a task board.
3. In the board header, click the connect with board members icon. The system automatically opens a record conversation for the board. Each board member becomes a member of the conversation.

**Configure the task board**

The board configuration menu provides several options that affect the look and feel of the board.

Role required: none

1. From the task board tools, click the menu icon.
2. In the **Background Color** section, select a background color from the palette.
   The background color surrounds the lane area of a board. It also appears as the color for the board on the My Task Boards page. Changes to the background color apply to all users.
3. In the **Quick Panel** section, toggle quick panel options as necessary.

<table>
<thead>
<tr>
<th>Quick panel options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Panel</td>
<td>When enabled, the quick panel is visible.</td>
</tr>
<tr>
<td></td>
<td>This setting applies to the current user only.</td>
</tr>
</tbody>
</table>
### ServiceNow Jakarta Now Platform Capabilities

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Names</td>
<td>When enabled, user names appear by user avatars in the quick panel. This setting applies to the current user only.</td>
</tr>
<tr>
<td>Show Labels</td>
<td>When enabled, labels appear on cards and in the quick panel. This setting applies to all users.</td>
</tr>
<tr>
<td>Label Names</td>
<td>When enabled, the label name appears beside the colored icon for that label in the quick panel. This setting applies to the current user only and is available only when Show Labels is enabled.</td>
</tr>
</tbody>
</table>

When all the options are enabled, a quick panel looks like this:

![Quick panel](image)

4. In the **Configure Cards** section, toggle card options as necessary. Changes to the cards apply to the current user only.

#### View options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compact Cards</td>
<td>When enabled, the lane width is decreased and card information and thumbnails do not appear on the card.</td>
</tr>
<tr>
<td>Show Card Info</td>
<td>When enabled, card information appears on each card. Card information typically includes details like the task state, date opened, and last user to update it. This setting is available only when Compact Cards is disabled.</td>
</tr>
<tr>
<td>Show Card Thumbnail</td>
<td>When enabled, cards display the first image attached to that card as a thumbnail. This setting is available only when Compact Cards is disabled.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Show SLAs</td>
<td>When enabled, SLA status indicators appear on cards and alerts appear when one or more card has a breached SLA. SLA status indicators are hidden when Compact Cards is enabled. This setting is available only when there are SLAs associated with the tasks on the board.</td>
</tr>
</tbody>
</table>

5. In the Configure Lanes section, show or hide lanes by selecting or clearing the check box for each lane. Rearrange lanes by dragging and dropping them in the list.

**Configure Visual Task Board labels**

Labels help categorize tasks and visually distinguish them on the task board. You can disable or rename labels using the labels tab of the activity stream.

Role required: none

You can use up to five labels per board. Any board member can edit the labels on a board.

1. From the task board tools, open the activity stream.
2. Click the labels tab.
3. Toggle the Show Labels switch to the enabled position if it is not already enabled.
4. To change a label name, click the label text and enter a new value.
5. To disable or enable a specific label, toggle the switch by the label.

When a label is disabled, members cannot add that label to cards on the board. The label is hidden on cards that are already labeled.

**Modify the query or lane field for an existing board**

For flexible and guided boards, you can edit the board query or lane field. This ability enables you to change the board contents while preserving the member list, board configuration settings, and, if applicable, Connect Chat conversation history.

Inform the board members that you plan to change the board query or lane field. If you or any members have manually sorted cards within a lane, the order may be reset.

Role required: none but you must be the board owner

The board query consists of filter conditions that determine which tasks the board tracks. For example, you might edit the query so the board shows only active incidents, rather than all incidents.

The lane field is the field on the underlying table that defines the lanes. For example, you might change the lane field so the lanes represent incident states, rather than assignees. This change is called a lane field pivot. Lane field pivots also make it possible to convert a flexible board to a guided board or vice versa.

1. Open a task board.
2. Click the board information icon (i) by the board name.

3. Perform one of the following actions.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit the board query</td>
<td>1. Under Board Filter, click Edit Filter to open the condition builder.</td>
</tr>
<tr>
<td></td>
<td>2. Add and remove conditions as needed to edit the query.</td>
</tr>
<tr>
<td></td>
<td>3. Click Save.</td>
</tr>
</tbody>
</table>

**Change the lane field**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Click the Lane Field picker and select a field or the None option. Guided boards have the Lane Field set to a field, such as State. Flexible boards have the Lane Field set to None. You can change the Lane Field value accordingly to change the board type.</td>
</tr>
<tr>
<td></td>
<td>2. In the confirmation dialog, click OK.</td>
</tr>
</tbody>
</table>

The board reloads to reflect the changes.

**Configure the card limit for freeform boards**

Freeform boards can display up to 2,000 cards by default. You can change the default card limit by adding a property.

Role required: admin

1. **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>glide.vtb.freeform_max</td>
</tr>
<tr>
<td>Type</td>
<td>integer</td>
</tr>
</tbody>
</table>

2. Set the Value to the maximum number of cards allowed for each freeform board.

**Note:** Performance degradation may occur if you set the Value to a number greater than 1,000, especially on tablet devices.

**Configure the card limit for flexible and guided boards**

Flexible and guided boards can display up to 2,000 cards by default. You can change the default card limit by adding a property.

Role required: admin

1. **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>glide.vtb.board_max</td>
</tr>
<tr>
<td>Type</td>
<td>integer</td>
</tr>
</tbody>
</table>
2. Set the **Value** to the maximum number of cards allowed for each flexible or guided board.

   **Note:** Performance degradation may occur if you set the **Value** to a number greater than 1,000, especially on tablet devices.

### Configure the task board card view

Configure the fields that appear in a card on a task board.

**Role required:** admin

1. Navigate to the form you want to configure fields for.
2. Right-click the header and select **Configure > Form Layout**.
3. Under the Form View section, select the VTB view.
   
   You may need to create a VTB view for the form. For more information, see [Create and delete views](#).

4. Select the fields to appear on the card by adding or removing the fields from the **Selected** column. You can also adjust the order they appear on the form by moving the fields up or down.

### Workflow

Workflow provides a drag-and-drop interface for automating multi-step processes across the platform. Each workflow consists of a sequence of activities, such as generating records, notifying users of pending approvals, or running scripts. The graphical workflow editor represents workflows visually as a type of flowchart. It shows activities as boxes labeled with information about that activity and transitions from one activity to the next as lines connecting the boxes.

**Explore**
- Workflow release notes
- Upgrade to Jakarta
- Workflow movement with update sets
- Workflow activity pinning

**Set up**
- Getting started with workflows

**Administer**
- Workflow roles
- Administering workflow contexts

**Use**
- Workflow editor
- Create a workflow
- Workflow activities

**Develop**
- Developer training
- Developer documentation
- Using variables in a workflow

**Troubleshoot and get help**
- Ask or answer questions in the Developer Community
- Troubleshoot workflows
- Search the HI knowledge base for known error articles
- Contact ServiceNow Technical Support

### Getting started with workflows

The graphical workflow editor provides a drag-and-drop interface for automating multi-step processes across the platform.

Each workflow consists of a sequence of activities, such as generating records, notifying users of pending approvals, or running scripts.
The workflow starts when a triggering event occurs. Common triggers include a record being inserted into a specific table, or a particular field in a table being set to a specified value. For example, you might create a workflow that runs whenever a user requests approval for an item they want to order from the catalog.

When an activity completes, the workflow transitions to next activity. An activity might have several different possible transitions to various activities, depending on the outcome of the activity. Continuing the example above, if the user’s request is approved, the activity might transition to an activity that notifies someone to order the item; if the user’s request is denied, the activity might transition to notifying the user that their request has been denied.

The graphical workflow editor represents workflows visually as a type of flowchart. It shows activities as boxes labelled with information about that activity and transitions from one activity to the next as lines connecting the boxes.

At each step in a workflow:
1. An activity is processed and an action defined by that activity occurs.
2. At the completion of an action by an activity, the workflow checks the activity’s conditions.
3. For each matching condition, the workflow follows the transition to the next activity.

When the workflow runs out of activities, the workflow is complete.

**Workflow activities**

A workflow activity contains instructions that are processed by the workflow.

Activities can include running scripts, manipulating records, waiting for a set period of time, or logging an event. Workflow conditions determine whether or not the activity is performed.

Activities can be added, removed, or rearranged. Transitions can be drawn between activities.

This is an activity that triggers a notification:

![Sample activity](image)

For more information on available activities and their behaviors, see [Workflow activities](#).

**Transitions**

After the workflow condition is evaluated, the workflow transition determines which activity is performed when the workflow condition is met.

This is a transition that always leads from the `Change Approved` script to the `Change Task` activity:
After a workflow activity is performed, the workflow condition is evaluated to determine which transition is activated.

The condition determines behavior based on a change being approved or rejected:

Sample exit conditions

Workflow example

During workflow editing or while an unpublished workflow is running, only the person who checked out the workflow can view the changes.

After a workflow is published, it is available to other users. The workflow moves through the process as defined in the Workflow Editor. The entire workflow is represented in one screen. For example, this is the Standard Change workflow:
Sample change workflow

Workflow editor

The Workflow Editor is an interface for creating and modifying workflows by arranging and connecting activities to drive processes.

You can manage multiple workflows in the same screen, create custom workflow activities, and use existing activities as data sources. Users with the workflow_creator role can create workflows. Users with the workflow_admin role can create, modify, delete, and publish workflows.

To open the Workflow Editor, navigate to Workflow > Workflow Editor. For information about using the editor, see Create a workflow.
Welcome screen

The editor opens with the **Welcome** page, which displays a list of active, published workflows. From this tab, you can open existing workflows, create new workflows, and open help resources related to workflow.
### ServiceNow Jakarta Now Platform Capabilities

#### List display filters

<table>
<thead>
<tr>
<th>Service Category</th>
<th>Description</th>
<th>Created</th>
<th>Updated</th>
<th>Updated By</th>
<th>Published</th>
<th>Global</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Catalog Request</td>
<td>Requested Item [item, item]</td>
<td>2021-04-09 12:45</td>
<td>True</td>
<td>admin</td>
<td>True</td>
<td>Global</td>
</tr>
<tr>
<td>Procurement Process Flow Software Management</td>
<td>Requested Item [item, item]</td>
<td>2021-05-10 13:00</td>
<td>True</td>
<td>admin</td>
<td>True</td>
<td>Global</td>
</tr>
<tr>
<td>Change Request - Normal</td>
<td>Requested Item [item, item]</td>
<td>2021-06-09 14:00</td>
<td>True</td>
<td>admin</td>
<td>True</td>
<td>Global</td>
</tr>
<tr>
<td>Procurement Process Flow - Hardware Management</td>
<td>Requested Item [item, item]</td>
<td>2021-07-09 15:00</td>
<td>True</td>
<td>admin</td>
<td>True</td>
<td>Global</td>
</tr>
<tr>
<td>Change Request - Normal</td>
<td>Requested Item [item, item]</td>
<td>2021-08-09 16:00</td>
<td>True</td>
<td>admin</td>
<td>True</td>
<td>Global</td>
</tr>
</tbody>
</table>

#### Workflows

- Add a custom task group:
- Add a custom task flow provider group:
- Approval workflow for item:
- Assignment workflow for SH:
- Azure client:
- Azure store:
- Change Request - Emergency:
- Change Request - Emergency change tasks:
- Change Request - Potential:
- Change Request - Normal change tasks:
- Change Request - Standard:
- Change Request - Standard change tasks:
- Change Line: Quota management:
- Clear Software License Details:
- Comprehensive Change:
- Contact Approval:
- CSD Lease End Notification:
- Default SLA Repair workflow:
- Default SLA workflow:
- Delegated to group member:
- Device Client Software:
- Dispose SCCM Application:
- Discover SCCM:
- Document Management: Default:
- Emergency Change:
- Employee Profile Update:
- Employee User Request:
- File server management:
- General role: delegator starts user ingroup:
- Kit List Approval: Softline:
- Kit Integration: Coordinator:
- Kit Service Aid:
- Kit Client Line Acceptance:
- Kit Corporate Credit Card Request:
- Ultimate Release: Whirlwind notifications:
- Website: Request: Register Info: commercial:
- Item Designer - Approvals:
- Item Designer - Full-Feature:
- Item Designer - Generate Approvals for current sequence:
- Item Designer - Workflow:
Published: Click to view list of published workflows
Checked Out: Click to view list of workflows checked out to current user
Help: Click to view links to help resources for workflow

New Workflow button
Click to create a new workflow

Palette tabs

Workflows: Workflow activities and workflows you can use as subflows.
Core: Available workflow activities appropriate for the selected workflow. Contents can include activities provided by the base system and those purchased with orchestration.
Packs: Orchestration activity packs downloaded from the ServiceNow® App Store, organized by vendor and scope. Custom activities and workflows that you scope also appear as packs. Only visible if the orchestration plugin is installed.
Custom: Orchestration custom activities available. Only visible if the orchestration plugin is installed.
Data: Activities in the current workflow that output data. You can use these activities as data sources for other activities. Only visible if the orchestration plugin is installed.

Note: If your workflow welcome page does not look like this example, you may have customized the workflow welcome page before upgrading to Jakarta. You can update the workflow welcome page to the latest version by editing the _UI pages_. Navigate to System UI > UI Pages > workflow editor welcome. In the UI page record for workflow_editor_welcome, scroll to the Versions related list. Select the row for the version corresponding to the upgrade to Jakarta, right-click and select Revert to this version.

Workflow canvas

After you open or create a new workflow, the system displays the workflow canvas. On the canvas you interact with the workflow editor through several different elements: the canvas itself, the canvas tabs, the title bar, the palette, and the palette tabs.

The drawing canvas is where you add activities and configure transitions for checked out workflows. Add an activity by dragging it from the palette to the workflow in the canvas. For more information, see Create a workflow.

- Canvas tabs: Contains tabs for accessing workflows being edited or created.
- Title bar: Displays the workflow name and status. Provides a menu and controls for configuring, testing, and validating workflows.
- Canvas: Provides the working surface for creating new workflows or editing existing ones.
- Palette tabs: Contains tabs for accessing activities being edited or created.
- **Palette**: Contains all available workflow activities and existing workflows you can use as subflows. Drag activities and subflows to the canvas to create new workflows or edit existing ones.

**Workflow user interface**

**Workflow palette**

The default workflow palette contains workflow activities and existing workflows you can use as subflows.

The basic workflow palette contains these tabs:

- **Workflows**: Displays existing workflows and provides controls for creating new ones.
• **Core**: Displays baseline workflow activities available to all systems and Orchestration activities (when Orchestration is activated).

### Workflows tab

The **Workflows** tab lists existing workflows that you can edit or use as subflows in other workflows. Double-click a workflow to open it in the canvas. To add a workflow as a subflow, drag it to another workflow in the canvas. Click the + icon to create a new workflow.

![Workflows tab in the palette](image)

### Core tab

The **Core** tab contains the standard activities available by default to all workflows and any activities purchased with Orchestration, organized by category. Click the arrow icons to expand or collapse the activity lists under each category. To add an activity to a workflow, drag it to the canvas. For more information, see *Add an activity to a workflow*. 
When a workflow is opened in the canvas, the title bar displays the workflow title and the workflow status in italics. Possible states are Checked out by <name> and Published.
Workflow editor title bar

Controls on the right side of the title bar manage the workflow.

- **Workflow Properties** • OPEN: Opens the current workflow's properties form.
- **Start** • RUN: Runs the workflow. This control is only available for workflows running on the Global table that are accessible from all application scopes. To test workflows that are on other tables, insert a record into that table that meets the condition of the workflow.
- **Validate** • VALIDATE: Tests the workflow prior to publication. Validation detects potential problems that can prevent the workflow from publishing or cause the workflow to fail. For more information, see [Workflow Validation](#).
- **Help** • HELP: Opens documentation to help you create the workflow.

Workflow menu

Click the menu icon in the title bar for additional options to configure the workflow.
Accessing the workflow menu

These menu options are available:

**Workflow menu options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Workflow</td>
<td>Creates a new workflow.</td>
</tr>
<tr>
<td>Open Existing</td>
<td>Opens another existing workflow.</td>
</tr>
<tr>
<td>Copy</td>
<td>Creates a duplicate of the workflow. Give the copy a different name.</td>
</tr>
<tr>
<td>Publish</td>
<td>Makes the personal workflow version public, overwriting the current published workflow version. This option is only available for checked out workflows.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Checkout</td>
<td>Creates a personal version of the workflow for you, which you can edit. This option is only available for published workflows.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the workflow. You cannot delete workflows that have contexts associated with them.</td>
</tr>
<tr>
<td>Set Inactive</td>
<td>Inactivates the workflow so that it cannot be used.</td>
</tr>
<tr>
<td>Expand Transitions</td>
<td>Redraws the transitions so that they do not overlap when they leave the activity condition.</td>
</tr>
<tr>
<td>Start Workflow</td>
<td>Starts a test run of the current workflow.</td>
</tr>
<tr>
<td>Validate Workflow</td>
<td>Runs validation tests on your workflow prior to publication. Use this validation to detect potential problems that can prevent the workflow from publishing or cause the workflow to fail. For more information, see Work on workflows.</td>
</tr>
<tr>
<td>Collapse Transitions</td>
<td>Redraws the transitions so they overlap when they leave the activity condition.</td>
</tr>
<tr>
<td>Show Contexts</td>
<td>Displays all the contexts for the current workflow. You can use this option to troubleshoot a workflow.</td>
</tr>
<tr>
<td>Properties</td>
<td>Opens the Workflow Properties form, which defines the workflow’s attributes.</td>
</tr>
<tr>
<td>Edit Inputs</td>
<td>Opens the Workflow Inputs list of variables that the workflow can accept when used as a subflow. For more information, see Pass a variable from a workflow to a subflow.</td>
</tr>
<tr>
<td>Edit Stages</td>
<td>Opens the Workflow Stages list. For more information, see Workflow stages. For tables with a column of Type = Workflow.</td>
</tr>
</tbody>
</table>

### Managing workflows

Create, edit, validate, and publish workflows to automate multi-step processes across the platform. Understand workflow activities and variables and how to use them effectively. Take a deeper look at how workflows are constructed, validated, and used.

### Create a workflow

Automate a multi-step process by creating a workflow with the workflow editor.

- You must have the workflow_admin or workflow_creator role to use the workflow editor.
- If you are designing the workflow as part of an update set process, see Workflow movement with update sets before creating the workflow.

1. Navigate to Workflow > Workflow Editor.
   The Welcome tab of the Workflow Editor opens.
2. On the Workflows tab in the palette, click New Workflow.

© 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.
### ServiceNow Workflow Table

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Updated by</th>
<th>Updated</th>
<th>Published</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Catalog Item</td>
<td>Requested Item</td>
<td>gdsu.maint</td>
<td>2009-11-14 08:56:31</td>
<td>true</td>
<td>Global</td>
</tr>
<tr>
<td>Knowledge - Instant</td>
<td>Knowledge</td>
<td>admin</td>
<td>2014-11-05 01:02:23</td>
<td>true</td>
<td>Global</td>
</tr>
<tr>
<td>Grant role_delegator</td>
<td>role_to_user in group</td>
<td>jane.capsico</td>
<td>2010-02-25 10:32:49</td>
<td>true</td>
<td>Global</td>
</tr>
<tr>
<td>Item Designer</td>
<td>Approvals</td>
<td>regan.bald</td>
<td>2014-02-24 16:03:13</td>
<td>true</td>
<td>Global</td>
</tr>
<tr>
<td>Password - Master</td>
<td>Global</td>
<td>changela</td>
<td>2013-09-23 08:56:24</td>
<td>true</td>
<td>Global</td>
</tr>
<tr>
<td>Change Request -</td>
<td>Emergency</td>
<td>admin</td>
<td>2013-08-21 07:37:46</td>
<td>true</td>
<td>Global</td>
</tr>
<tr>
<td>Default SLA workflow</td>
<td>Task SLA</td>
<td>admin</td>
<td>2013-09-07 01:06:31</td>
<td>true</td>
<td>Global</td>
</tr>
<tr>
<td>Change Request -</td>
<td>Normal</td>
<td>admin</td>
<td>2013-08-21 07:37:38</td>
<td>true</td>
<td>Global</td>
</tr>
<tr>
<td>Item Designer</td>
<td>Requested Item</td>
<td>admin</td>
<td>2014-10-24</td>
<td>true</td>
<td>Global</td>
</tr>
</tbody>
</table>

### Workflow Diagram

- Create a new workflow
- View workflows
- Filter workflows
- Add new workflow

- Change Request - Emergency
- Change Request - Emergency/change tasks
- Change Request - Normal
- Change Request - Normal/change tasks
- Change Request - Standard
- Change Request - Standard/change tasks
- Comprehensive Change
- Contract Approval
- Default SLA Repair workflow
- Default SLA workflow
- Delegate roles to group member
- Emergency Change
- Grant role_delegator role to user in group
- Item Designer - Approvals
- Item Designer - Fulfillment
- Item Designer - generate approvals for current sequence
- Item Designer Workflow
- Knowledge - Approvals Publish
- Knowledge - Approvals Retire
A simplified version of the New Workflow form opens.

3. Fill in the Name and Table fields.
4. (Optional) Add a Description.
5. (Optional) Do one of the following:
   a) If the Conditions UI section is displayed, specify a Condition if needed and edit the fields. (The Conditions UI section shows only if the selected table supports conditions for launching workflows. For example, if you select the sc_req_item table, conditions are not applicable and the Conditions UI section is not displayed.)
   b) If the Stages UI section is displayed, check that the State rendering and Stage order fields contain the correct information. (The Stages UI section shows only if the selected table supports stages. For example, if you select the sc_req_item table, the Stages UI section is displayed.)

6. Click Submit.

The new workflow is created with the Begin and End activities connected by a single transition.

7. Finish creating the workflow by adding activities, validating, and publishing so the workflow is available to other users.

   For more information, see Work on workflows.

8. To change advanced settings for the workflow, click the Properties icon. If you make changes, click Update.

Workflow properties

In the properties of a workflow, you can configure settings such as its application scope, start conditions, schedule, inputs, stages, and run time metrics. You can also view information such as the workflow author, version, and history.

When you create a new workflow, the following fields are available in the dialog box:

- Name
- Table
- Description
- If condition matches
- Condition
If you click Diagrammer view in Related Lists, the following UI sections are available in the dialog box:

- General
- Conditions
- Inputs
- Activities
- Application
- Schedule
- Stages
- Estimated Runtime

### General

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name to identify the workflow.</td>
</tr>
<tr>
<td>Table</td>
<td>The table for the workflow to run on. Workflows that run on specific tables can still interact with other tables. Select Global (global) to run the workflow on all tables.</td>
</tr>
<tr>
<td>Checked out</td>
<td>(Read-only) When the workflow was checked out. Automatically set by the Checkout action in the workflow menu.</td>
</tr>
<tr>
<td>Checked out by</td>
<td>(Read-only) The user who has this workflow checked out. This value is automatically set by the Checkout action in the workflow menu.</td>
</tr>
<tr>
<td>Published</td>
<td>(Read-only) Check box to indicate whether the workflow has been published. Automatically set by the Publish action in the workflow menu.</td>
</tr>
<tr>
<td>Description</td>
<td>The purpose of the workflow.</td>
</tr>
</tbody>
</table>

**Note:** The list shows only tables and database views that are in the same scope as the workflow. Also, all users who edit the workflow must have access to the necessary tables and domains.

### Conditions

Create conditions to trigger the workflow. The Conditions section does not appear if you select a table, such as sc_req_item, that does not require a condition.
### If condition matches

When the condition evaluates to true, the workflow launches an active context:

- **None**: The workflow is not automatically started by the workflow engine. To run this workflow, write a script to start the workflow.
- **Run the Workflow**: The default value. The workflow engine starts the workflow if the information in the **Condition** field matches a record that is inserting into the table.
- **Run if no other workflows match yet (deprecated)**: The workflow only runs if no other workflows are running on the execution thread that started this workflow. Avoid using.
- **Run if no other workflows matched**: The workflow only runs if no other workflows are running on a specific record. For example, there are four workflows inserted into the incident table, which have a condition such as `short_desc` contains `test`. A new workflow, which has **If condition matches** is set to **Run if no other workflows match yet**, only runs if none of the four workflows have started running on the incident record.

### Condition

A condition builder for specifying workflow conditions that trigger the behavior selected from the **If condition matches** list.

### Order

Numeric value that determines the order of the workflow, relative to other workflows. Workflows are evaluated in order from the lowest order number to the highest. A workflow runs if it is the first to match conditions.

## Inputs

The Inputs section lists all the activities in the current workflow that input data, the data type, and the default value. The Inputs section is only available after a workflow has been created. To create a variable, click **New**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>Displayed column label. Localized depending on user locale.</td>
</tr>
<tr>
<td>Reference</td>
<td>Input field from another table.</td>
</tr>
<tr>
<td>Type</td>
<td>Data type. For example, integer or string.</td>
</tr>
<tr>
<td>Default value</td>
<td>Value used if you do not provide a value.</td>
</tr>
</tbody>
</table>

## Activities

The Activities section enables you to set activity pinning and maximum activity count.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity pinning</td>
<td>List of options that control updates to custom activities at the workflow level. Pinning protects custom activities from being updated automatically when downloaded from the ServiceNow Store. For more information, see Workflow activity pinning. The possible options are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Set by activity</strong>: Allows all activities in the workflow to use their own pinning settings. This is the default pinning option.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Pin all activities</strong>: Pins all activities in the workflow to their current version.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unpin all activities</strong>: Allows all activities in the workflow to be updated.</td>
</tr>
<tr>
<td>Max activity count</td>
<td>The maximum number of activities performed by the workflow. This value is used to prevent infinite loops and is set to 100 by default. When the stated maximum count is reached, the workflow is canceled. If this field is blank, the maximum count is set to -1, and the workflow is canceled.</td>
</tr>
</tbody>
</table>

**Application**

The Application section enables you to see application scope and scope restrictions.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>(Read-only) Scope of this activity. For more information, see Application Scope.</td>
</tr>
<tr>
<td>Accessible from</td>
<td>Scope restrictions for this workflow. Possible settings are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>All application scopes</strong>: Workflow is accessible to all application scopes.</td>
</tr>
<tr>
<td></td>
<td>• <strong>This application scope only</strong>: Workflow access is limited to the scope named in the Application field.</td>
</tr>
<tr>
<td></td>
<td>For more information see Workflow scope.</td>
</tr>
</tbody>
</table>

**Schedule**

Use the Schedule section to create a schedule for this workflow using the schedule builder.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Delivery based on   | The schedule type for this workflow. Possible types are:  
  - **User-specified duration**: Duration based on a user-specified value. This is the default schedule type.  
  - **Relative duration**: Duration calculated from a preconfigured schedule, such as 8-5 weekdays. |
| Expected time       | User-defined interval. This field is visible when the schedule type is **User-specified duration**.                                             |
| Schedule            | Preconfigured schedule that determines when this workflow runs.                                                                                |
| Timezone            | Time zone for this instance.                                                                                                                  |

### Stages

The Stages section appears if you select a table with **Type = Workflow**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stage</td>
<td>Displays the workflow stage progress on the selected table. Optionally, select <strong>Stage rendering</strong> and <strong>Stage order</strong> schemes to customize the appearance of the stage field. The default values cover typical scenarios.</td>
</tr>
<tr>
<td>Stage rendering</td>
<td>The renderer to use when displaying stage icons on a form or list view. For more information about renderers, see <em>Workflow stage renderers</em>.</td>
</tr>
<tr>
<td>Stage order</td>
<td>The order of workflow stages when you view a workflow field in a list. Select <strong>Computed</strong> to let the workflow engine compute the stage order from the order of execution in the workflow. Select <strong>User Specified</strong> to use the <strong>Order</strong> field from that Workflow stages.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the stage as it appears in workflow fields.</td>
</tr>
<tr>
<td>Duration</td>
<td>Time allocated for the specific stage.</td>
</tr>
<tr>
<td>Order</td>
<td>The order of workflow stages when you view a workflow field in a list. Select <strong>Computed</strong> to let the workflow engine compute the stage order from the order of execution in the workflow. Select <strong>User Specified</strong> to use the <strong>Order</strong> field from that Workflow stages.</td>
</tr>
<tr>
<td>Value</td>
<td>The value of the stage when it is referenced from elsewhere in the system, such as in a script.</td>
</tr>
</tbody>
</table>
Estimated Runtime

The **Estimated Runtime** section opens the controls for configuring the **ERT** for the workflow. Core workflows included in the base system are not configured for estimated run time by default. All new workflows are configured with default ERT values automatically. You can edit existing run time estimates or configure new ones for any existing workflow. For details about how estimated run times are configured and calculated, see [Workflow run time metrics](#).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requires ERT</td>
<td>Check box to indicate that this workflow requires an estimated runtime configuration. You can use the ERT calculations to determine if workflows are running longer or shorter than expected and to identify errors in workflow processing. By default, new workflows require an ERT.</td>
</tr>
<tr>
<td>Estimated Run Time</td>
<td>The initial estimate for the workflow’s run time.</td>
</tr>
<tr>
<td>Number of data points</td>
<td>(Read only) The number of times the system has compared the estimated run time to an actual run time result.</td>
</tr>
<tr>
<td>Outlier Percentage Threshold for ERT</td>
<td>(Required) The percentage deviation from the estimated run time that identifies an outlier workflow run time. The system uses a default value of 20. For more information, see <a href="#">Outlying workflow run times</a>.</td>
</tr>
</tbody>
</table>

Create a workflow from a table

Automate a multi-step process by creating a workflow from the list view of any table that supports workflows.

- If you are designing the workflow as part of an update set process, see [Workflow movement with update sets](#) before creating the workflow.

1. Open a table, such as Incident or Problem, in list view. For example, navigate to **Incident > Open**.
2. Right-click in the column header and select **Configure > Workflows**.
The **Workflow Versions** on that table appear in a list.

3. Click **New**.
   The **Workflow Version** opens in **New Workflow** view. The **Table** field is filled in with the table you selected in step 1 and is read-only.

4. Enter **Name**.
5. (Optional) Enter **Description**.
6. (Optional) Edit conditions fields as necessary.
7. Click **Submit**.
   The new workflow is added to the **Workflow Versions** list.
8. Click the workflow **Name**.
   The new workflow is created with the **Begin** and **End** activities connected by a single transition.
9. Finish creating the workflow by adding activities, validating, and publishing so the workflow is available to other users. For more information, see Work on workflows.

10. (Optional) To change advanced settings for the workflow, click the Properties icon. If you make changes, click Update.

Create a workflow for a new service catalog item

When you create a new service catalog item, you can create a new corresponding workflow at the same time.

- If you are designing the workflow as part of an update set process, see Workflow movement with update sets before creating the workflow.

1. Navigate to Service Catalog > Catalog Definitions > Maintain Items.
2. At the top of the form, next to Catalog Items, click New.

   The Catalog Item form opens.

3. Add a Name.
4. Next to the Workflow field, click the lookup icon.
5. Next to Workflow at the top, click New.
The Workflow version dialog opens in the New Workflow View. The **Table** field is set to **Requested Item (sc_req_item)** and is read-only.

6. Add a **Name**.

7. (Optional) Add a **Description**.

8. (Optional) Change the stage information as necessary.

9. Click **Submit**.
The new workflow is created with the **Begin** and **End** activities connected by a single transition.

10. Finish creating the workflow by adding activities, validating, and publishing so the workflow is available to other users.
   For more information, see *Work on workflows*.
11. To change advanced settings for the workflow, click the **Properties** icon.
12. Click **Update**.
   If you close the workflow editor, you can see the Catalog Item record. Note that the workflow is added to the Workflow field. The Show Workflow and Information icons appear next to the **Workflow** field. Hover over the information icon to view a read-only summary of the workflow.

**Create a workflow for an SLA Definition**

Automate a multi-step process by creating a workflow from an SLA definition.

- If you are designing the workflow as part of an update set process, see *Workflow movement with update sets* before creating the workflow.

1. Open a list of SLA definitions. For example **Facilities > SLA Definitions** or **Service Level Management > SLA Definitions**.
2. At the top of the form, next to **SLA Definitions**, click **New**.
3. Select **Contract SLA** or **Service Offering SLA**.
   The SLA Definition or Service Offering SLA form opens.
4. Next to the **Workflow** field, click the lookup icon.
5. Next to **Workflow** at the top, click **New**.
The Workflow Version dialog shows in the New Workflow view. The Table field is set to SLA Definition (contract_sla) or Service Offering SLA (service_offering_sla) and is read-only.

6. Enter Name.
7. (Optional) Enter Description
8. (Optional) Edit conditions fields as necessary.
9. Click Submit.
   The new workflow is created with the Begin and End activities connected by a single transition.
10. Finish creating the workflow by adding activities, validating, and publishing so the workflow is available to other users.
   For more information, see Work on workflows.

11. (Optional) To change advanced settings for the workflow, click the Properties icon. If you make changes, click Update.

Ending workflows with multiple branches

A workflow is complete when it reaches the End activity, even if there are still active branches of the workflow in progress. To ensure that both branches are completed, add a Join activity to resolve the branches.

For example, the following figure shows a workflow with two branches that execute independently. When Task 1 and Task 2 of Branch B are completed, the workflow is marked complete even if the Branch A tasks are not completed.

For both branches to complete, add a Join activity to resolve the branches. When one branch reaches the join, the workflow waits for the other branch. When both branches are complete, the workflow reaches the end. The Incomplete condition of the a Join activity is met only if one of the branches cannot be completed.
Workflow with completed branches

Work on workflows

To complete a workflow, you add workflow activities, validate the workflow, and publish it.

Add a workflow activity

Activities determine the functionality of the workflow. When they are created, all workflows contain Start and End activities.

For more information, see Workflow activities.

1. Open a workflow.
2. Check out the workflow.
3. Drag a workflow activity from the Activities menu into the workflow body.
4. Populate the Workflow Activity form that appears.

Validate a workflow

You can manually validate a workflow from the Workflow Editor. You can generate a workflow validation report from the Workflow Version form.

Role required: workflow_admin, workflow_creator, or admin

Running a workflow on a new node automatically attempts to validate the workflow. If validation is successful, the system updates the workflow version record to indicate the workflow has been validated and marks the record as updated by the user who ran the workflow.

1. Open the workflow to validate in the workflow editor.
   When the workflow is loaded, the workflow validator icon appears in the toolbar.
   2. Click the validator icon to run a series of validation tests on the current workflow version and generate a report.
3. Complete the following steps to generate a workflow validation report from the Workflow Version form
   a) Navigate to Workflow > Administration > Workflow Versions, and select a workflow to validate.
   b) Under Related Links, click Validate Workflow.

Publish a workflow

When a workflow is complete, publish the workflow so that it is available to all users.

Before you publish a workflow, validate it to test it for issues that might cause it to fail, such as missing subflows or disconnected transitions. For more information, see Workflow validation.
To publish a workflow:

1. Navigate to Workflow > Workflow Editor.
2. Open the workflow that you want to publish.
3. In the title bar, click the menu icon and select Publish.

If you published a new version of workflow, the changes are not applied to running workflow contexts. Any currently running workflow context continues using the workflow version that was available when the workflow started. The next time the workflow runs, it uses the new version.

**Determine whether a workflow can run**

A workflow can run only if a checked out version is available to the user who has it checked out, and a valid, published version is available for all users with permission to run it.

Role required: workflow_admin, workflow_creator, or admin

1. In the navigation filter, enter wf_workflow.list, and then open one of the workflows.
2. In the Versions related list, check for all of the following conditions:
   a) There is only one workflow version in a state of Checked out and Checked out by.
   b) There is only one version and it is not checked out. This version must be both Active and Published.
      You may need to personalize the list and add the Active column.
   c) If there are multiple versions, only one is Published.

These checks determine the only two conditions under which a workflow can run:

- A checked out version of a workflow is available for the user who has it checked out.
- A valid, published version of a workflow is available for all users who have permission to run the workflow.

Main flows containing subflows that do not meet one of these two conditions are not permitted to execute against a current record transaction. Instead, a critical log entry detailing the subflow state is added to the Workflow Context record. To enable the workflow to execute on the next appropriate transaction, remove the subflow from the main flow or modify the published and active states of the subflow.

**Edit a published workflow**

You can edit a published workflow after you check it out.

*Note:* You cannot check out or delete workflows that are associated with a read-only application file.

To check out a workflow:

1. Navigate to Workflow > Workflow Editor.
2. Open the workflow that you want to edit.
3. In the title bar, click the menu icon and select Checkout.

   A new version of the workflow is created and assigned to you.

   If you are in a different domain than the published workflow, the new workflow version is created in your domain.

After you finish editing the workflow, validate and publish the workflow to make the new version available to other users.
Workflows used as subflows

A workflow can launch another workflow as an activity.

The parent workflow triggers the subflow and then waits for the subflow to complete before continuing. Run the workflow validation tool prior to publishing to detect missing subflows and other dependency problems, such as those involving update sets.

The Workflows tab in the Workflow Editor contains a list of the workflows available for use as subflows.

Workflows available to use as subflows

Make sure that the selected subflow is active. If the subflow is inactive, the main workflow will hang with a Loading message. If you place an inactive subflow into a workflow, the subflow appears with a red banner, indicating that it cannot run. An active subflow is highlighted in blue when selected.
Subflows and the Create Task activity

If a workflow contains a Create Task activity that has executed on the current record, additional task activities in the workflow might not execute as expected.

This can happen when the same subflow containing a Create Task activity runs more than once in a parent flow. When the subflow reruns and attempts to execute the Create Task activity again, the system reopen the first task activity instead and does not create an additional task.

Note: An alternative to creating duplicate subflows that use the Create Task activity is to add a Run Script activity to the workflow that creates a task with a script.
The same create task activity runs twice in a workflow

In this configuration, the workflow does not run the same subflow containing a Create Task activity more than once. This allows the workflow to create additional tasks.
Running different subflows containing the Create Task activity

Pass a variable from a workflow to a subflow

Use this process to pass variables from a parent workflow to a subflow.

**Note:** You can also use the **Return Value** activity in the subflow to return values to the parent workflow. Make sure to have a **Return Value** on every ending transition path.

1. Prepare the subflow to accept variables from the parent workflow by defining the inputs.
2. Include the subflow in the parent workflow and connect the inputs to the parent workflow variables.

**Note:** Subflows on the Requested Item (sc_req_item) table in the Service Catalog cannot accept variables from parent workflows.

Define inputs for a subflow

Define the input variables for a workflow to request from parent workflows when it is launched as a subflow.

All inputs are stored in the Variables (var_dictionary) table.

1. In the editor, open and check out the workflow.
2. In the title bar, click the menu icon and select **Edit Inputs**.
3. In the Workflow Inputs window, click **New**.
4. Populate the record with the definition of the variable, including the column name, the label that is displayed to the user, and the type of field.
5. Click Submit.

Invoke a subflow in a workflow
Use this procedure to add a subflow to a workflow.

1. In the Workflow Editor, open and check out the parent workflow.
2. Drag the subflow from the Workflows tab to the parent workflow.
3. In the New Activity dialog box, define the variables defined by the subflow's Inputs.
   These fields can accept both static values or variables in the following format:
   `${variable_name}`
4. Click Submit.

   The workflow triggers the subflow at the appropriate time and passes the variables as indicated by the Inputs definition.

Prepare a subflow
Review the process of preparing a subflow for use in a parent workflow, and for preparing the parent workflow to use a subflow.

1. In the editor, open and check out the workflow that you want to use as a subflow.
2. In the title bar, click the menu icon and select Edit Inputs.

3. In the Workflow Inputs window, click New in the Variables list.
4. Add a new variable depending on the type of values that it is going to store. The following example sets up a string value.

```
Workflows Inputs
```

- **Column name**: u_bluesubvariable
- **Label**: Blue Sub Variable
- **Type**: String

```
current.description = workflow.inputs.bluesubvariable;
```

5. Click Submit.
6. Close the Workflows Inputs dialog.
7. Create a Run Script activity on the subflow.
   - Set the value from the parameter to a field on the current form. This is important because the Notification activity can only pull values from the current variable and not from the newly added variable. The following example sets the value in the Description field.

```
current.description = workflow.inputs.bluesubvariable;
```
   - Create a new field on the request form but do not display the field. This serves as temporary storage.
8. Create a Notification activity on the subflow. Use `{description}` in the subject to return the value from the field.
New Activity: Notification

Name: Blue Notification

Stage:

To: Beth Anglin

Subject: This is for $description 12345ABC

Message:
- Test notification
- Blue Sub Variable $description
- Request for: $requested_for

Advanced:

This is what the subflow would look like:
Prepare a workflow to use a subflow
After you create a subflow, use this procedure to prepare the parent workflow.

1. On the parent workflow, create a variable similar to what you did on the subflow, but name it something different.

   In the following example, the variable is named **Blue Main Variable**.

   ![Variable creation screenshot]

2. Click **Submit**.

3. Insert a **Run Script** activity to return the value from a field to the newly created variable.

   In this example, the value of the **Short Description** field is returned and given to the newly created variable.

   ```javascript
   workflow.scratchpad.bluemainvariable = current.short_description;
   ```
4. Click Submit.
5. In the subflow activity, set the Blue Sub Variable to pass the bluemainvariable to the bluesubvariable.

$$\text{workflow.scratchpad.bluemainvariable} = \text{current.short_description};$$

This is what the main workflow looks like:
Using variables in a workflow

Within workflow there are several different types of variables that are available.

Some variables define, describe, or compose the pieces of the workflow (such as workflow activities). Some variables are available specifically to facilitate the execution of a workflow (such as scratchpad variables). Some variables define, describe, or compose the data records being manipulated by the workflow process (for example, the elements of a Glide Record that are defined in a dictionary.xml file describing a record, such as an incident).

Activity variables

Activity variables are properties specifically associated with a workflow activity.

These are the inputs that appear on the activity definition when a specific activity is dragged onto the workflow canvas. These variables are properties that define, compose or describe the workflow activity, or the work it is designed to perform.

Activity variables are declared in a related list within the Workflow Activity Definition.

To add, view, or modify a variable:

1. Navigate to Workflow > Activity Definitions.
2. Select a workflow activity, such as Approval - User.
3. In the Activity Variables section or tab, add, view, or modify the variables. Activity variables are defined using the same fields as Dictionary records.

Note: If defining a new activity variable that is dependent on another activity variable, put the prefix “vars.” before the name of the parent activity variable. For example, if the child field is dependent on a field named parent, put the value vars.parent in the Dependent field.

To control the visibility of an activity variable on the workflow canvas after the activity has been dragged to the canvas, use a UI policy on the wf_activity table.

To access the variables or assign values to these variables within the workflow activity, use the vars variable of the workflow activity.

activity.vars.variable_name = new_variable_value

Workflow input variables

Workflow variables are external values that are passed into and referenced by a workflow during its execution.

Workflow variables can be declared externally in a script and passed into a main workflow or they can be declared within a main workflow and passed as inputs to a subflow.

Note: There is a specific kind of input variable for any workflow that is declared against the table Requested Item (sc_request_item). To understand the use of these variables see Workflow catalog variables.

Workflow variables are declared in a form available from the Workflow Editor gear menu.

To add, view, or modify a variable:

1. Navigate to Workflow > Workflow Editor.
2. Edit and checkout a workflow.
3. Select the Workflow Activities menu and select Edit Inputs.
4. Select an existing variable or click New.
Note the **Column name** field. Use this value when accessing the variable from a script. Workflow variables do not appear on the workflow canvas, they are only available for view from the Workflow Activity menu.

The input variables are available to use in scripts. To access an input variable from a script:

```
var input  = workflow. variables. variableName // get the workflow variable identified by column name.
```

### Assigning values to variables from outside of workflow

After being declared in a workflow, values can be assigned to the variables from where the workflow is kicked off.

The following example demonstrates how a workflow variable’s value can be set in a script include, business rule, or UI action:

```
// Declare an instance of workflow.js
var wf  = new Workflow ( ) // Get the workflow id
var  wfId  = wf. getWorkflowFromName ( "Workflow Name" ) ;
// Start workflow, passing along name : value pair(s) for mapping to variable
// where input_var_name is the name of the variable declared in gear menu
// and input_var_value is whatever that value should be for this execution of workflow
wf. startFlow (wfId , null , "Workflow Name" , {input_var_name : input_var_value } ) ;
```

Another example that demonstrates a more readable way of passing multiple variables involves declaring an object, adding the names/values to the object, and passing it:

```
// Declare an instance of workflow.js
var wf  = new Workflow ( )
// Get the workflow id
var  wfId  = wf. getWorkflowFromName ( "Workflow Name" ) ;
// Start workflow, passing along object containing name/value pairs mapping to inputs expected by the workflow
var vars  = { } ;
vars. input_var_name1 = input_var_value1 ;
vars. input_var_name2 = input_var_value2 ;
// add as many variables as your workflow is expecting, then pass the object
wf. startFlow (wfId , null , "Workflow Name" , vars ) ;
```

### Assigning Values for Subflow Inputs from inside of a Main Workflow

If a workflow that accepts inputs is called from within another workflow, those input values can be set from the workflow canvas within the UI of the workflow activity. Each input variable declared for a subflow will have a text box input area displayed on the activity. Within these text boxes, the variables can be set with any value either from the scratchpad or from within the current record.

For more information, see [Workflows used as subflows](#).
Reading the Value of a Workflow Input Variable

The value of a Workflow input variable is accessible anywhere within the workflow that accepts javascript by dot walking the current workflow object:

```javascript
var readValue = workflow.inputs.variable_name;
```

Workflow scratchpad variables

The scratchpad in workflow is a space in the workflow context to store and share string based variables (as name:value pairs) between instances of activities within an executing instance of a workflow.

The scratchpad is global to the instance of the running workflow and as such, is available equally to all activities.

Declaration

The scratchpad itself is automatically available to an executing workflow and requires no specific declaration. Variables are declared and stored in the scratchpad simultaneously by referencing it. For example:

```javascript
workflow.scratchpad.variableName = variableValue;
```

Display

There is no way to view the contents of the scratchpad.

Access and Assignment

As stated in the Declaration section:

```javascript
workflow.scratchpad.variableName = variableValue;
```

or:

```javascript
var myValue = workflow.scratchpad.variableName;
```

Current variables

Current is the database GlideRecord that kicked off the workflow, either by association to the table in the Workflow properties table or by being associated with a catalog item.

Declaration

Variables in current are the columns that are defined in the dictionary.xml file that support the database record. There is no way at runtime to add variables to the current record.
Display

Variables of a current record are displayed on the Glide Forms and Lists throughout the applications that use them.

Access and Assignment

To access the variables or assign values to the variables within the workflow activity, get the value from the current record by referencing the Glide Element.

\[
\text{var myVarValue} = \text{current.getElementById(nameOfTheField)};
\]

or

\[
\text{var myVarValue} = \text{current.fieldName};
\]

or

\[
\text{current.variableName.setValue( "A Variable Value")};
\]

Workflow catalog variables

Workflows that are associated with the Requested Item (sc_req_item) table have a specific type of workflow input.

The inputs into this workflow are essentially question:answer pairings that, when associated with a specific catalog task, become options on the task form. These options are generated by that catalog task activity within a workflow.

Scope

For the purposes of Service Catalog and workflow, a variable’s scope determines its availability to a catalog task activity within a workflow. You can define variables as global or catalog item-specific. When a variable is associated to a catalog item and the workflow generating the catalog task is associated to the catalog item, the variable scope determines which variables are available for mapping within the catalog task activity in a workflow. If a workflow is associated with Requested Item (sc_request_item), and is not specifically associated with a catalog item, any catalog variable with a blank Cat Item field value is available to all catalog task activities within the workflow.

Declaration

You can declare requested item catalog variables at the catalog item level or at a global level.

You can declare global catalog variables using the workflow editor context menu.

Also see, Global variable declaration option 2.

1. Navigate to Workflow > Workflow Editor.
2. Open and check out a workflow that runs against the Requested Item (sc_req_item) table.
3. Click the menu icon and select Edit Catalog Variables.
4. Click New to create a new variable or select an existing variable.
5. Select the Global check box.
6. Click Submit.
Global variable declaration option 2
You can declare global catalog variables using the Service Catalog.

1. Navigate to Service Catalog > Item Variables.
2. The list of variables that appears in the workspace has a default filter of Cat Item != <blank>. Change the filter to Cat Item = <blank> and run the query.
   The catalog variables that appear are available to any catalog task that is initiated from within a workflow.
3. Click New to create a new variable.
4. Leave the Cat Item field blank.
5. Select the Global check box.
6. Click Submit.
   Also see, Global variable declaration option 1.

Catalog item specific variable declaration option 1
You can declare a catalog item-specific variable.

These variables are only available to the catalog item referenced in the Cat Item field on the variable record.

1. Navigate to Service Catalog > Catalog Variables > Item Variables.
   Note the list of variables that appears in the workspace has a default filter of Cat Item != <blank>.
2. Enter or select a catalog item in the Cat Item reference field.
   Selecting a Cat Item restricts the scope and availability of the catalog variable to that specific catalog item.
3. Click Submit.
   Also see, Catalog item specific variable declaration option 2.

Catalog item specific variable declaration option 2
You can declare a catalog item-specific variable directly from a catalog item record.

Creating a catalog variable in this way automatically sets the Cat Item reference to the catalog item selected.

1. Navigate to Service Catalog > Catalog Definitions > Maintain Items.
2. Select or create an a catalog item.
   Note the Variables related list. All variables declared using this related list have a Cat Item reference value of the current catalog item.
3. From the Variables related list, click New.
4. Ensure that the Cat Item field correctly references the catalog item previously selected or created.
5. Go to or open the Question section or tab.
6. Add a Question.
7. Add a Name.
   Variable names should not include white space and cannot begin with a number.
8. Click Submit.
   Also see, Catalog item specific variable declaration option 1.

Display
Catalog specific item variables are visible in several places depending on where in the process the variable is viewed.
Declaration can happen and variables can be seen from within the menu, inside both the **Maintain Items** module and in the **Item Variable** modules of the Service Catalog.

Within a workflow, the Catalog Specific Item variables are available to the **Catalog Task** activity in the form of a slushbucket at the bottom of the **Catalog Task** activity. Item variables that are selected, are the question and answer pairs that will appear on the task that is generated by that instance of **Catalog Task** when executing that workflow.

If a workflow is associated with a specific catalog item, the association acts as a filter for item variables that appear in the slushbucket of the **Catalog Task** activity.

The last place the variables are seen is in the task form that is generated by the Catalog Task Item. The variables selected in the slushbucket are the question and answer pairs that appear to the user on the task form.

**Access and assignment**

The Catalog Item Variables are available and assigned to a specific **Catalog Task** activity (thereby to a specific task) using the slushbucket entry of a catalog task.

The user working the task enters the values of the variables.

To access the values of a Catalog Item Variable inside a script:

```javascript
var gr = current; // or create and query a new GlideRecord
var itemVariable = gr. variables [ variableName ]; //access the service catalog variable identified by the variable name.
var itemValue = itemVariable. getGlideObject (). getValue ();
var itemQuestion = itemVariable. getGlideObject (). getQuestion (). getLabel ();
```

**Workflow events**

The system employs two types of events: registered platform events and workflow events.

**Registered platform events**

Registered events are created in business rules and are used for such tasks as sending email notifications when records are inserted into the database. Workflow events are registered within workflows only and are not used anywhere else in the platform. Registered platform events can be triggered by a workflow for external use, but cannot be used within a workflow.

**Workflow events**

Workflow events follow different rules than platform events that are registered using the event registry. Platform events are entered into the Event Registration (sysevent_register) table and are available for platform processes to use. Workflow events are triggered exclusively for the workflow engine and are used only to direct the work of executing workflow contexts. When an event is registered in a workflow, it is attached to a currently executing activity in the **registered_events** column of the Workflow Executing Activity (wf_executing) table.

Workflow events also can be broadcast to a workflow from any scripting source that has access to the workflow context, such as a script include or a **Run Script** activity. In this case, the event, such as `cancel`, is passed to all records in the Workflow Executing (wf_executing) table for a specific context.

Whether by registry or by broadcast, an event is handled by the activity definition associated with the currently executing activity. Each activity definition comes with a set of handlers. For example,
most activities come with `onExecute`, `onCancel`, and `onUpdate` event handlers. As an example of a more specific event, the Approval - User activity also comes with `onDetermineApprovalState`, which is specific to the work of the approval activity.

Multiple parallel events

A single workflow can have multiple event threads running concurrently, such as when a workflow has timers that overlap on separate workflow branches. If any additional thread completes before the first thread, the system stores event information from the additional thread on the Workflow Queued Commands (wf_command) table. After the first thread completes, the system retrieves the information stored by the additional thread and proceeds through the workflow with the event information from each thread.

Workflow events in the base system

Several workflow events are available in the base system.

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
<th>Purpose</th>
<th>To use</th>
<th>Source</th>
<th>Thread</th>
<th>Listeners</th>
</tr>
</thead>
<tbody>
<tr>
<td>activityComplete</td>
<td>String value used by activity definitions to respond to the <code>onActivityComplete</code> event.</td>
<td>Informs records in the Workflow Executing Activity (wf_executing) table about the completion of other activities in the same workflow context.</td>
<td>If the activity is allowed to set the boolean value for <code>wf_executing.notify_termination = true</code> during the <code>onExecute</code> event.</td>
<td>Workflow Engine, Process Terminations</td>
<td>Current thread, current mutex</td>
<td>Join activity</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event</td>
<td>Description</td>
<td>Purpose</td>
<td>To use</td>
<td>Source</td>
<td>Thread</td>
<td>Listeners</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>--------------</td>
<td>-----------------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>otherEvent</td>
<td>String value used by the <strong>Join</strong> activity to respond to an otherEvent.</td>
<td>Informs records in the Workflow Executing Activity (wf_executing) table about an otherEvent that has completed.</td>
<td>The <strong>Join</strong> activity transitions from $n$ number of preceding activities. These preceding activities all create a wf_executing record, which causes a check to see if the record already exists. If the <strong>Join</strong> already exists, then the <strong>Join</strong> created by the executing transition sets the wf_executing record for deletion.</td>
<td><strong>Join</strong> activity</td>
<td>Current thread, current mutex</td>
<td><strong>Join</strong> activity, onOtherEvent event handler</td>
</tr>
<tr>
<td>timer</td>
<td>String value used by workflow activities to respond to a <strong>Timer</strong> activity that has expired.</td>
<td>Allows wf_executing records to be informed about a timer activity that has completed and has fired the timer event.</td>
<td>The <strong>Timer</strong> activity schedules a job that calls a script. The script calls fireEvent (wf_executing, timer).</td>
<td><strong>Timer</strong> activity via a scheduled job</td>
<td>Worker thread, private mutex</td>
<td><strong>Timer</strong> activity, onTimer event handler</td>
</tr>
<tr>
<td>Event</td>
<td>Description</td>
<td>Purpose</td>
<td>To use</td>
<td>Source</td>
<td>Thread</td>
<td>Listeners</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>------------------------------------------------</td>
<td>----------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>execute</td>
<td>String value used by workflow activities to respond to a Timer activity that has expired.</td>
<td>Informs a record in the wf_executing table with the initial state of Executing to proceed with its primary work.</td>
<td>The workflow engine, for each transition executed, creates an executing record with a state of Executing. Once created, the executing record is put in a queue for processing. For each item in the queue, the Rhino globals are established, the activity definition that drives the executing record is instantiated, and the run() function is called. When the state of a record is Executing, this function always calls onExecute.</td>
<td>Workflow engine, via the WFActivity Handler</td>
<td>Current thread, current mutex</td>
<td>All activities, onExecute event handler</td>
</tr>
<tr>
<td>Event</td>
<td>Description</td>
<td>Purpose</td>
<td>To use</td>
<td>Source</td>
<td>Thread</td>
<td>Listeners</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>--------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>execute</td>
<td>String value used by the Lock activity to respond to a waiting lock that is ready to make another attempt to obtain a specific lock. This execute is different than the previous execute because it is called on a separate thread, at specified intervals, and is treated as an outside event.</td>
<td>Informs a wf_executing record waiting to execute that the specified wait interval has passed and that it should attempt to get the lock again.</td>
<td>Lock activity schedules a job with a script that uses the workflow script include's fireEvent( 'execute') method.</td>
<td>Lock activity via a scheduled job</td>
<td>Worker thread, private mutex</td>
<td>Lock activity, onExecute event handler</td>
</tr>
<tr>
<td>determineApprovalState</td>
<td>String value used by approval activities to respond to a change in the overall approval status of the current record.</td>
<td>Informs wf_executing records for approval activities about an approval that completed and triggered the timer event.</td>
<td>Approval Coordinator both registers for the event and triggers the event. The child approvals have listeners that determine their approval state.</td>
<td>Approval Coordinator triggers the event during its onExecute</td>
<td>Current thread, current mutex</td>
<td>Approval Coordinator, Approval - User, and Approval - Group all have onDetermineApprovalState event handlers. If the state is anything but Requested, the activity is considered finished, and the approval state (Approved, Rejected, Cancelled) is set to the wf_executing.result column</td>
</tr>
<tr>
<td>Event</td>
<td>Description</td>
<td>Purpose</td>
<td>To use</td>
<td>Source</td>
<td>Thread</td>
<td>Listeners</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>---------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>-----------</td>
</tr>
<tr>
<td>cancel (from within activity definitions)</td>
<td>String value used by workflow activities to respond to a request for cancellation.</td>
<td>Informs all workflow executing records in a context that the workflow is being canceled.</td>
<td>The <strong>End</strong> activity uses the global <code>workflow.broadcastEvent('cancel')</code> to interrupt the currently running workflow executing records. This changes the state of those records to <strong>Cancelled</strong>.</td>
<td><strong>End</strong> activity</td>
<td>Current thread, current mutex</td>
<td>All activities, <strong>onCancel</strong> event handler</td>
</tr>
<tr>
<td>Event</td>
<td>Description</td>
<td>Purpose</td>
<td>To use</td>
<td>Source</td>
<td>Thread</td>
<td>Listeners</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>---------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>-----------</td>
</tr>
<tr>
<td>cancel (outside current context)</td>
<td>String value used by workflow activities to respond to a request for cancellation.</td>
<td>This event is the same as the cancel event above and handled the same. However, the management of this event is subtly different. This event informs all wf_executing records in a context that the workflow is being canceled. The event is managed via the <code>onCancel</code> event handler of each executing activity definition, but the event is called differently. In particular, the call to cancel from outside an activity definition is blocked by the current mutex. This is a significant difference in that the event does not interrupt a currently executing activity that is still operating within the parameters of the current mutex.</td>
<td>Any script can call cancel on a known executing context via the workflow script include. For example, var w = new Workflow(); w.cancel(context); //where context is a GlideRecord of the context to be canceled.</td>
<td>Any script include, scheduled job, UI action, or other source</td>
<td>Current thread, private mutex</td>
<td>All activities, <code>onCancel</code> event handler</td>
</tr>
<tr>
<td>Event</td>
<td>Description</td>
<td>Purpose</td>
<td>To use</td>
<td>Source</td>
<td>Thread</td>
<td>Listeners</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>-----------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>stop (see End activity)</td>
<td>The <strong>End</strong> activity checks for this event.</td>
<td>If the stop event is the current event, then the cancel operation of the <strong>End</strong> activity is bypassed.</td>
<td>Only in the <strong>End</strong> activity.</td>
<td>Any script can trigger or broadcast the stop event via a script include or workflow Run Script activity</td>
<td>Current thread, current mutex</td>
<td>This event is used by the <strong>End</strong> activity to exclude the <strong>Cancel</strong> activity and allow a workflow to end, even if canceled.</td>
</tr>
<tr>
<td>listener</td>
<td>String value that the workflow (subflow) activity triggers as an event.</td>
<td>When a main workflow calls a subflow, the workflow keeps the ID of the subflow's context in the scratchpad. When the subflow is complete, it triggers the listener event via a business rule.</td>
<td>The listener event is passed to the parent context on completion of a subflow and is managed by the onListener action of the workflow activity.</td>
<td>Business rule that is triggered by the update of a workflow that has a parent</td>
<td>Current thread, current mutex</td>
<td>This event is used by a subflow to inform its parent flow that it is complete. The parent workflow will react to this event and continue.</td>
</tr>
<tr>
<td>probe_complete</td>
<td>String value triggered in the workflow by an Orchestration activity indicating that the MID Server has completed a task.</td>
<td>The <strong>probe_complete</strong> event is triggered from Orchestration sensor processors via the workflow helper function handleEventById.</td>
<td>Event used to restate a workflow that is waiting for the MID Server to process a task or activity</td>
<td>Worker thread, private mutex</td>
<td>Orchestration activities</td>
<td></td>
</tr>
<tr>
<td>pause</td>
<td>String value sent to a workflow from an SLA to pause the <strong>Timer</strong> activity.</td>
<td>When an SLA is paused, the SLA workflows must be paused if there is a timer running.</td>
<td>Use is exclusive to the SLA timer</td>
<td>SLA</td>
<td>Business rule thread, private mutex</td>
<td><strong>Timer</strong> activity</td>
</tr>
<tr>
<td>Event</td>
<td>Description</td>
<td>Purpose</td>
<td>To use</td>
<td>Source</td>
<td>Thread</td>
<td>Listeners</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>---------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>-----------</td>
</tr>
<tr>
<td>resume</td>
<td>String value used by the Timer activity to resume a paused timer (see pause).</td>
<td>When an SLA is resumed, the SLA workflows must be resumed as well.</td>
<td>Use is exclusive to the SLA timer.</td>
<td>SLA</td>
<td>Business rule thread, private mutex</td>
<td>Timer activity</td>
</tr>
</tbody>
</table>

**Glide events relative to workflows**

Workflow uses several Glide events.

**Workflow Glide events**

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
<th>Purpose</th>
<th>To Use</th>
<th>Source</th>
<th>Thread</th>
<th>Listeners</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insert</td>
<td>Global event set upon the insert of a GlideRecord that causes the script engine, and through that the workflow engine, to wake up.</td>
<td>Starts workflows that are associated with the current GlideRecord either by reference, as in request items and SLA timers, or by conditions associated with the GlideRecord's table.</td>
<td>There is no explicit customer-facing use for this in a workflow. It is part of the Glide engine, and with this event, the only thing workflows can do is start. Workflows can also be started manually using a script.</td>
<td>Workflow Engine, RunEngine</td>
<td>Current thread, current mutex</td>
<td>User action of insert</td>
</tr>
<tr>
<td>Update</td>
<td>Global event set upon the update of a GlideRecord that causes the script engine, and through that the workflow engine, to wake up.</td>
<td>Looks to the Workflow Context (wf_context) table to find running workflows that are associated with the current GlideRecord by document ID.</td>
<td>There is no explicit customer-facing use for this in a workflow. It is part of the Glide engine, and with this event, the only thing workflows can do is advance through the next set of transitions.</td>
<td>Workflow Engine, RunEngine</td>
<td>Current thread, current mutex</td>
<td>User action of update of a GlideRecord</td>
</tr>
<tr>
<td>Event</td>
<td>Description</td>
<td>Purpose</td>
<td>To Use</td>
<td>Source</td>
<td>Thread</td>
<td>Listeners</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>---------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>-----------</td>
</tr>
<tr>
<td>Delete</td>
<td>Global event set upon the delete of a GlideRecord that causes the script engine, and through that the workflow engine, to wake up.</td>
<td>Looks to the Workflow Context (wf_context) table to find running workflows that are associated with the current GlideRecord by document ID.</td>
<td>There is no explicit customer-facing use for this in a workflow. It is part of the Glide engine, and with this event, the only thing workflows can do is advance through the next set of transitions.</td>
<td>Workflow Engine, RunEngine</td>
<td>Current thread, current mutex</td>
<td>User action of delete of a GlideRecord</td>
</tr>
<tr>
<td>Query</td>
<td>Global event set upon the query of the Glide database that causes the script engine, and through that the workflow engine, to wake up.</td>
<td>Looks to the Workflow Context (wf_context) table to find running workflows that are associated with the current GlideRecord by document ID.</td>
<td>There is no explicit customer-facing use for this in a workflow. It is part of the Glide engine, and with this event, the only thing workflows can do is advance through the next set of transitions.</td>
<td>Workflow Engine, RunEngine</td>
<td>Current thread, current mutex</td>
<td>User action of query of a GlideRecord</td>
</tr>
</tbody>
</table>

Workflow event-specific functions
There are several functions that relate specifically to workflow events.
## Workflow event-specific functions

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Purpose</th>
<th>Use</th>
<th>Thread</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>registerForEvent</td>
<td>Function in the workflow environment that writes events represented as strings to the wf_executing.registered_events field.</td>
<td>The workflow events are just strings. When an activity that has registered for an event executes, a comma delimited set of events is stored with the Workflow Executing Activity (wf_executing) record. When the event is triggered in the workflow context, the wf_executing table looks for all executing records that contain the string that represents the event in the wf_executing.registered_events field.</td>
<td>The global variable workflow that is available to all Workflow Activity (wf_activity) records is the source of the call. For example, from inside a Run Script activity, a designer can write: workflow.registerForEvent('myEventName');</td>
<td>Current thread, current mutex</td>
<td>Global variable workflow</td>
</tr>
<tr>
<td>unRegisterForEvent</td>
<td>Function in the workflow environment that removes a string value representing an event that has been written to the wf_executing.registered_events field.</td>
<td>The workflow events are just strings that are written to the wf_executing.registered_events field. When an activity unRegisters for an event, the comma delimited set of events stored with the Workflow Executing Activity (wf_executing) record is searched, and if that string is found, it is removed.</td>
<td>The global variable workflow that is available to all Workflow Activity (wf_activity) records is the source of the call. For example, from inside a Run Script activity, a designer can write: workflow.unRegisterForEvent('myEventName');</td>
<td>Current thread, current mutex</td>
<td>Global variable workflow</td>
</tr>
<tr>
<td>Function</td>
<td>Description</td>
<td>Purpose</td>
<td>Use</td>
<td>Thread</td>
<td>Source</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>fireEvent</td>
<td>Function in the workflow environment that examines the contents of the wf_executing field, comparing its contents to the eventName passed in.</td>
<td>The workflow events are just strings that are written to the wf_executing field. When fireEvent(eventName) is called by a workflow activity, the workflow engine queues up any executing records that contain the string in the registered field.</td>
<td>The global variable workflow script include contains the call for this. For example, from inside a Run Script activity, a designer can write: workflow.fireEvent('myEventName');</td>
<td>Current thread, current mutex</td>
<td>Global variable workflow script include</td>
</tr>
<tr>
<td>fireEvent</td>
<td>Function in the workflow environment that sends an event to a specific Workflow Executing Activity (wf_executing) record. The eventRecord is a GlideRecord of the type wf_executing.</td>
<td>This event call expects an onMyEvent event handler in the activity represented in the event record (Workflow Executing Activity (wf_executing) table). When fireEvent(eventRecord, eventName) is called by a workflow activity, the workflow engine queues up the specific executing record with that event and passes the event into the activity definition for the on&lt;eventName&gt; handler to manage. This event is queued up in its own mutex, so the current queue completes before this event is processed.</td>
<td>The workflow script include contains the call for this. For example, from inside a Run Script activity, a designer can write: var w = new Workflow(); w.fireEvent(executing, eventName);</td>
<td>Current thread, current mutex</td>
<td>Workflow script include</td>
</tr>
<tr>
<td>Function</td>
<td>Description</td>
<td>Purpose</td>
<td>Use</td>
<td>Thread</td>
<td>Source</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>---------</td>
<td>-----</td>
<td>--------</td>
<td>--------</td>
</tr>
<tr>
<td>fireEvent ((\text{eventRecordSysId}, \text{eventName}))</td>
<td>Function in the workflow environment that sends an event to a specific Workflow Executing Activity ((\text{wf_executing})) record. The \text{eventRecordSysId} is the \text{sys_id} of a GlideRecord of the type \text{wf_executing}.</td>
<td>This is the same as the \text{fireEvent} above, except that it accepts an ID and returns the Workflow Executing Activity ((\text{wf_executing})) record.</td>
<td>The Workflow script include contains the call for this. For example, from inside a \texttt{Run Script} activity, a designer can write: \begin{verbatim} var w = new Workflow(); w.fireEvent(executing, eventName); \end{verbatim}</td>
<td>Current thread, current mutex</td>
<td>Workflow script include</td>
</tr>
<tr>
<td>fireEvent ((\text{eventRecordSysId, eventName, optionalJSONObject}))</td>
<td>Function in the workflow environment that sends an event to a specific Workflow Executing Activity ((\text{wf_executing})) record. The \text{eventRecordSysId} is the \text{sys_id} of a GlideRecord of the type \text{wf_executing}.</td>
<td>This is the same as the \text{fireEvent} above, except that it accepts a JSON object as a third parameter. This object can specify any data expressible as JSON. You can also specify additional functionality when creating a workflow activity.</td>
<td>The Workflow script include contains the call for this. For example, from inside a \texttt{Run Script} activity, a designer can write: \begin{verbatim} var w = new Workflow(); w.fireEvent(executing, eventName, JSONObject); \end{verbatim}</td>
<td>Current thread, current mutex</td>
<td>Workflow script include</td>
</tr>
<tr>
<td>broadcastEvent ((\text{contextId, eventName}))</td>
<td>Function in the workflow environment that sends an event to all currently running Workflow Executing Activity ((\text{wf_executing})) records in a specified context, regardless of their state.</td>
<td>This is the same as the \text{fireEvent} above, except that it accepts an ID and returns the Workflow Executing Activity ((\text{wf_executing})) record.</td>
<td>The Workflow script include contains the call for this. For example, from inside a \texttt{Run Script} activity, a designer can write: \begin{verbatim} var w = new Workflow(); w.broadcastEvent(contextId, eventName); \end{verbatim}</td>
<td>Current thread, current mutex</td>
<td>Workflow script include</td>
</tr>
</tbody>
</table>
## Event-specific workflow activities

The following workflow activities trigger events.

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Purpose</th>
<th>Use</th>
<th>Thread</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>broadcastEvent(eventName)</td>
<td>Function in the workflow environment that sends an event to all currently running Workflow Executing Activity (wf_executing) records in the current context, regardless of their state.</td>
<td>This should not be confused with broadcastEvent above. This event is only available to current Workflow Executing Activity (wf_executing) records.</td>
<td>This is available only through the global workflow variable of the current context. The following is an example of its use from within an activity definition's script: <code>workflow.broadcastEvent(eventName)</code></td>
<td>Current thread, current mutex</td>
<td>Global variable workflow</td>
</tr>
</tbody>
</table>
### Event-specific workflow activities

<table>
<thead>
<tr>
<th>Activity Name</th>
<th>Description</th>
<th>Purpose</th>
<th>To Use</th>
<th>Source</th>
<th>Thread</th>
<th>Listeners</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Event</td>
<td>Requires an event from the event registry rather than a workflow event. This activity is located in the Notification category of the workflow tree.</td>
<td>Fires the notification event specified in the Workflow Activity (wf_activity) table.</td>
<td>1. Navigate to System Policy &gt; Events &gt; Registry</td>
<td>Event Registry</td>
<td>Triggered in the current thread and handled on the worker thread in notifications. Never processed by a workflow</td>
<td>On the notification thread, outside of workflow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. Create an event.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3. Navigate to System Policy &gt; Templates and create an email template</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4. Navigate to System Policy &gt; Email &gt; Notifications.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5. Create a new notification that is triggered by the event you created and sends the template you created.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6. On the workflow canvas, drag the Create Event activity onto the canvas and associate it with the newly registered</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activity Name</td>
<td>Description</td>
<td>Purpose</td>
<td>To Use</td>
<td>Source</td>
<td>Thread</td>
<td>Listeners</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------</td>
<td>--------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Wait for WF Event</strong></td>
<td>Listens for workflow events, as described in the <em>Workflow Events in the Base System</em> table, and only within the current context. This activity is located in the <em>Conditions</em> category of the workflow tree.</td>
<td>Waits for another transition branch of the current context to trigger an event.</td>
<td>Takes an event name as input. When the activity is executed, the specified event name is added to a string array stored in the <code>registered_events</code> column. The values in this column are in a list of all events the activity waits for when it is executing.</td>
<td><em>The Wait for WF Event activity has a generic onUnhandledEvent that tests the current event against the value that was passed to the variable. If they match, the Wait for WF Event moves the workflow forward.</em></td>
<td></td>
<td>The <code>onUnhandledEvent</code> of the <em>Wait for WF Event</em> activity</td>
</tr>
</tbody>
</table>

**Workflow stages**

Workflows can indicate workflow progress by updating any field designated as a stage field. For example, the Incident (incident) table has an **Incident state** field that indicates progress, but the service catalog uses the **Stage** field.

To indicate the workflow's progress through the possible stage values, the interface updates the **Stage field** selected in the workflow properties. Available fields depend on the table used by the workflow. If the field provides a choice list, then the choices are available as stage values for the workflow. If the field is a workflow field, it displays an icon to indicate the workflow's progress, as with the Service Catalog's **Stage** field.

---

© 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.
After stages are added to the workflow, they can be assigned to each workflow activity. If an activity with an assigned stage is encountered when the workflow runs, the workflow engine assigns the stage to the record associated with the workflow context.

For workflows that use the Requested Item (sc_req_item) table, the stage field is automatically set to the **Stage** field of the table and cannot be changed. The stage state displayed for a workflow running on the Requested Item table is based on the state of the workflow activities.

- If an activity is active, then the stage is shown with the state of **In progress**.
- If an activity is in the **Pending** or **Completed** state, the stage reflects this state.
- If an activity is cancelled, **Request Cancelled** appears in the **Stage** field. The "Cancelled" label set in the wf_stage table is a reserved word, and does not display in the **Stage** field.

### How stage values are derived

Stage values are derived from various sources in the interface.

**Note:** An updated method for managing workflow stages as a set is also available. For information about grouping and reusing stages, see [Workflow stage sets](#).

Stage values are derived from the following sources:

- **Choices for Stage column:** Choices defined for the column selected as the **Stage** column for the workflow.
- **Default stages for table:** Stages defined in the Stage Default (wf_stage_default) table for the table selected.
- **Workflow-specific stages:** Applied only to the workflow for which they were defined in the Workflow Stage (wf_stage) table.
- **Stage values in existing records:** Values from the designated **Stage** column in the table assigned to the workflow are inherited from existing records.

If the stage field for a workflow is the table column named **Stage**, then the progress of the workflow appears in any list view containing the **Stage** column.
Stages in a list

Stage values shown in the list views are accompanied by the state, based on the workflow activities being executed. If an activity has a stage specified for it, and the activity is currently active in the workflow, then the stage is shown with a state of *in progress*. Similarly, if the activity is in the *Pending* or *Completed* state, the stage reflects this state.

Example

If the workflow table is Request Item (sc_req_item), then the stage field is automatically set to the *Stage* column of that table and cannot be changed. The following stage values for the request item are displayed in a choice list from the Dictionary Entry (sys_dictionary) table:

- Waiting for Approval
- Fulfillment
- Delivery

In addition, the Request Item table has the following default stages:

- Request Cancelled
- Completed

© 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: If an activity is cancelled, Request Cancelled appears in the Stage field. The "Cancelled" label set in the wf_stage table is a reserved word, and does not display in the Stage field.

When you edit available activity stages in the Workflow Editor, the list displays the following stage values:

- Waiting for Approval
- Fulfillment
- Delivery
- Request Cancelled
- Completed

The following diagram depicts the process used to gather stage values from the Request Item table to populate the Stages list in workflow activities.
Note: If you are creating a workflow with a table other than Request Item (sc_req_item), you must select a **Stage field** in the workflow properties for the workflow to have stages.

**Use workflow stages**

You can add or modify workflow stages.

1. Navigate to **Workflow > Workflow Editor**.
2. Create a new workflow by clicking **New** or open an existing workflow.
3. In the Workflow Properties form, if the table is not the Requested Item (sc_req_item) table, select a field to display stages in the Stage field property. *Available fields* depend on the table selected for the workflow.

4. After assigning a list of stages to the workflow, you can set a stage value in any of the workflow activities that provide a Stage field in their dialog box.

Setting a stage value in a workflow activity tells the workflow engine to assign that stage to the record associated with the workflow context when the activity is encountered during a run.

When an activity starts with a specified stage, the platform updates the Stage field with the current value. In workflows run against the Requested Item (sc_req_item) table, the sc_req_item.stage field is defined as a workflow type field.

When displaying the stages for a workflow on the Requested Item (sc_req_item) table, the stage state is based on the state of the workflow activities. If an activity has a stage specified for it, and the activity is currently active in the workflow, then the stage is shown with an In progress state. Similarly, if the activity is in the Pending or Completed state, the stage reflects this state.

5. To edit the workflow-specific stages for an existing workflow, click the gear icon in the header bar and select Edit Stages. Again, these stage values are combined with the choices, defaults, and existing values.
Workflow stages

To optimize the use of stages, you can assign a stage to multiple activities in a workflow. For example, if your workflow uses the following activities to create tasks:

1. Get approval
2. Order equipment
3. Receive equipment
4. Add equipment to CMDB
5. Set up equipment
6. Install software
7. Configure software
8. Deliver to user

The following stages might be used:

- Approval
- Order
- Configure
- Deliver

A good practice is to assign stages to the activities as follows:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Assigned stage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get approval</td>
<td>Approval</td>
</tr>
<tr>
<td>Order equipment</td>
<td>Order</td>
</tr>
<tr>
<td>Receive equipment</td>
<td>Order</td>
</tr>
<tr>
<td>Add equipment to CMDB</td>
<td>Order</td>
</tr>
<tr>
<td>Set up equipment</td>
<td>Configure</td>
</tr>
<tr>
<td>Install software</td>
<td>Configure</td>
</tr>
<tr>
<td>Configure software</td>
<td>Configure</td>
</tr>
<tr>
<td>Deliver to user</td>
<td>Deliver</td>
</tr>
</tbody>
</table>

When the **Order equipment**, **Receive equipment**, or **Add equipment to CMDB** activity is active, the **Stage** display shows that the **Order** stage is **In progress**.

Add and translate stages

You can add default stages to use for a table, and stages to existing workflow **Add default stages for a table**

You can assign a stage set as a default set to any number of tables.

The stages in the assigned stage set pre-fill the workflow version stages when you create a new workflow for the associated table.

1. Navigate to **Workflow > Default Stages (by table)**.
2. Click **New**.
3. Select a stage Set.
   You can create a new set by clicking New, typing a name, and clicking Submit.

4. Select a corresponding Table.

5. Click Submit.
   The stages in the selected stage set are automatically added to any new workflows that use the corresponding table.

**Add a stage to an existing workflow**
If a stage required for a workflow has not been imported or is not in the stage set assigned to the workflow table, you can add it to the workflow manually.

1. Navigate to Workflow > Workflow Editor.
2. Open and check out the workflow.
3. In the title bar, click the menu icon and select Edit Stages.
4. In the Workflow Stages list, click New.
5. On the Workflow Stage form, fill in the fields as appropriate.
   Do not use a Name or Value field value that already exists in the base system.

---

**Workflow stage fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the stage as it appears in workflow fields.</td>
</tr>
<tr>
<td>Value</td>
<td>The value of the stage when it is referenced from elsewhere in the system, such as in a script.</td>
</tr>
<tr>
<td>Duration</td>
<td>The default duration for the stage. Currently not used.</td>
</tr>
</tbody>
</table>

6. Click Submit.
7. Publish the workflow.

**Add a stage to a workflow activity**
After stages are added to a workflow, you can assign them to the workflow activities.

1. Navigate to Workflow > Workflow Editor.
2. Open and check out the workflow.
3. Double-click the activity.
4. In the Stage field on the Activity Properties form, find and select the stage to display when the workflow reaches the activity.
5. Click Update.

**Translate workflow stages**
You can provide translations for workflow stage names so the names appear in the language selected for the instance.

The instance must already have internationalization support installed.

Language-specific text appears in workflow fields displayed in a list, workflow stage sets, and the workflow editor for users with that language selected. Language-specific text does not automatically appear when displaying stages on a form. To translate stages on a form, add translated text to the workflow field choices.
You can add translated text for any language enabled on the instance. For example, to translate workflow stages into French:

1. Set the interface language to French.
2. Navigate to Workflow > Workflow Editor.
3. Open and check out a workflow.
4. In the title bar, click the menu icon and select Edit Stages.
5. Edit the Name field for each stage and enter the text to display to French users.
   Do not change the Value field.
6. Confirm that the workflow stages display the French text.

Alternatively, to translate stages for multiple workflows at once, you can directly edit the Workflow Stages (wf_stage) table. For example, to translate workflow stages from multiple workflows into French:

1. Set the interface language to French.
2. In the application navigation filter, enter wf_stage.list.
3. Edit the Name field for each stage and enter the text to display to French users. Do not change the Value field.

**Workflow stage sets**

Stage sets are named groups of workflow stages commonly used together. Create a stage set and assign it as a default set to any number of tables. You can import the choice list values of a workflow field as stages for a workflow, and export a stage set to create a new one.

A single stage set usually represents a process, such as the stages required to display the progress of a service catalog request. You can also assign a stage set as the default set for workflows on specific tables.

In an active context, workflow stages provide summary-level feedback about the progress of a workflow. Stage icons display the status of each activity as it is being driven by a workflow. The system updates a Stage field, defined in the workflow properties, to indicate the progress of the workflow through the possible stage values.

**Updates to workflow stage values**

During an upgrade, the system makes changes to the Value field of records in the Workflow Stage (wf_stage) table.

- All entries are made lowercase.
- All spaces and special characters are replaced with underscores.

These changes support Localization settings and enable workflows to display translated text in the Stage field.

*Create a new stage set*

You can create a new stage set by creating a stage set record and adding stage set entries manually.

Create a stage set record only when you want additional stages that are not available on the table by default.

1. Navigate to Workflow > Stage Sets.
2. Click New.
3. Enter a **Name** that indicates the purpose of the stage set. For example, you can create a Requested Item stage set to hold the stages commonly used by inventory tracking workflows or service catalog fulfillment workflows.

4. Click **Submit**.

5. Open the new stage set record.

6. In the **Stage Set Entries** related list, click **New**.
   - Each stage set entry can be used as the **Stage** for an activity in a workflow that uses this stage set.

7. Enter a **Name** that indicates the stage name to appear in workflow fields.

8. Enter a **Value** to use when referencing the entry, such as in a script.

9. Click **Submit**.

10. In the **Stage Set Entries** related list, ensure that each entry has a unique **Order** value.
    - Enter a low value for stages that should appear early in the workflow and a higher value for later stages.

The stage set can be added to a workflow or assigned as the default stage set for workflows that are created for a specific table.

**Import stages from a choice list**

You can import the choice list values of a workflow field as stages for a workflow.

Create a choice list as follows:
• Add a custom field of Type **Workflow** to the table.
• Configure the custom field to use a choice list.
• If you are creating a new field, set the **Choice List type** to **Display without --None--** and create the choices for the newly created field.

For more information, see [Create a workflow stage field](#).

1. Navigate to **Workflow > Workflow Editor**.
2. Open and check out the workflow.
3. In the title bar, click the menu icon and select **Properties**
4. In the Workflow Properties dialog box, click the **Stages** tab.
5. From the **Stage field** list, verify that the correct workflow field is selected.
6. In the Related Links section, click **Import Stages from Choice List**.
7. In the dialog box asking you to confirm that you want to import the choice list, click **OK**.
8. Click **Update**.

The stage set can be added to a workflow or assigned as the default set for workflows that are created for a specific table.

**Export a stage set from a workflow**
You can create a new stage set by exporting the stages from an existing workflow as a set, instead of manually adding stage set entries to a stage set record.

1. Navigate to **Workflow > Workflow Editor**.
2. Open and check out the workflow containing stages that you want to export as a new stage set.
3. In the title bar, click the menu icon and select **Edit Stages** to open the Workflow Stages dialog box.
4. In the Related Links section, click **Export to Stage Set**.
5. Enter a unique **Name** for the new stage set.
6. Click **OK**.

The stage set can be added to a workflow or assigned as the default set for workflows that are created for a specific table.

**Add a stage set to a workflow**
You can add any number of stage sets to an existing workflow.

When multiple stage sets have stage set entries with the same **Value**, the stage appears on the workflow only once.

1. Navigate to **Workflow > Workflow Editor**.
2. Open and check out the workflow.
3. In the title bar, click the menu icon and select **Edit Stages** to open the Workflow Stages dialog box.
4. In the Related Links section, click **Import from Stage Set**.
5. Select the stage set.
6. Click **Ok**.
7. Import additional stage sets as needed for the workflow.

After you add all necessary stage sets to the workflow, you can add them to the workflow activities. For more information, see [Add a stage to a workflow activity](#).

**Use a default stage set**
You can assign a stage set as a default set to any number of tables.
The stages in the assigned stage set pre-fill the workflow version stages when you create a new workflow for the associated table.

1. Navigate to Workflow > Default Stages (by table).
2. Click New.
3. Select a Table.
4. Select the Set you want to assign to the selected table.
5. Click Submit.

Create a workflow stage field

Workflows can provide a summary of workflow progress by updating any field of the Workflow type. If the field is a workflow field, it displays an icon to indicate the workflow stage progress.

Role required: admin

In a form, the workflow field displays the current stage as a choice list value.

In a list, the workflow field displays stage icons that represent the series of states, stages, phases, or tasks within a workflow. The stage icons are populated using the activity stages from the associated workflow. For more information, see Workflow stages.

To create a workflow stage field:

1. Navigate to Workflow > Default Stages (by table).
2. Right-click near a column header and select Configure > List Layout.
3. Create a new field in lower right.
4. On the form view of the table used by the workflow, create a field with the Type set to Workflow.
   For detailed steps, see Add and customize a field in a table.
5. Click Save.
6. Right-click the field label and select Configure Dictionary.
7. Open a dictionary entry.
8. In the Choice List Specification section of the Dictionary Entries form, select Dropdown with --None-- from the Choice list.
9. Click Update.
10. To ensure that the workflow field properly displays stages on the form, define a choice for each workflow stage.

© 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 create workflow stages using a choice list that already has choices, you can import the stages from the choice list. A stage is created for each choice defined for the Stage field selected in the workflow properties. For detailed steps about importing a choice list, see Import stages from a choice list.

- The Value of each choice must match the Value of the corresponding workflow stage.
- Do not use spaces in the Value field for either choices or stages. Use underscores in place of spaces.
- Make the choice list read-only. If a user changes the stage value for a record from the choice list rather than allowing the workflow to control the value, the workflow-driven, legacy, and linear renders may not work as intended. You can also use business rules or events to ensure the workflow progresses accordingly.

For detailed steps on defining choice lists, see Define an option for a choice list.

11. To see workflow stages as icons, add the field to the list layout of the workflow table.
For detailed steps, see Configure the list layout.

After you create or update the workflow field:

- Unless the workflow uses the Requested Item (sc_req_item) table, ensure that the workflow field is selected from the Stage field list in the workflow properties. For detailed steps, see Select a stage field. If a workflow uses the Requested Item table, the stage field is automatically set to the Stage field of the table and cannot be changed.
- Work through the workflow. Any other updates made to the workflow field, such as updates from business rules or other scripts, can interfere with displaying workflow stages.

Select a stage field
A Stage field allows the workflow context to show additional workflow information, such as the stage name and the estimated completion time for an activity.

Ensure that the workflow field you want to use as the stage field is configured to properly display stages. For detailed steps, see Create a workflow stage field.

Unless the workflow uses the Requested Item (sc_req_item) table, you can specify which field from the workflow table is the stage field. For workflows that use the Requested Item (sc_req_item) table, the stage field is automatically set to the Stage field of the table and cannot be changed.

To add or edit a workflow stage field:

1. Navigate to Workflow > Workflow Editor.
2. Create or check out the workflow.
3. In the title bar, click the menu icon and select Properties.
4. In the Workflow Properties dialog box, click the General tab.
5. In the Table list, verify that the table containing the workflow field is selected.
6. Click the Stages tab.
7. From the Stage field list, select the workflow field.
8. Click Update.

Workflow stage field icons and tooltips
A workflow stage field displays icons to indicate the workflow stage.

Based on the stage renderer selected for the workflow, these icons may display a tooltip with additional information.
## Workflow field icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Workflow stage</th>
</tr>
</thead>
<tbody>
<tr>
<td>![current active step icon]</td>
<td>Current active step</td>
</tr>
<tr>
<td>![approval pending icon]</td>
<td>Approval pending</td>
</tr>
<tr>
<td>![approval rejected icon]</td>
<td>Approval rejected</td>
</tr>
<tr>
<td>![complete icon]</td>
<td>Complete</td>
</tr>
<tr>
<td>![late or canceled icon]</td>
<td>Late (Change/Request) or Canceled (Catalog)</td>
</tr>
<tr>
<td>![skipped icon]</td>
<td>Skipped (Catalog only)</td>
</tr>
</tbody>
</table>

### Stage tooltips

Based on the stage renderer selected for a workflow, workflow stage icons may display tooltips with detailed information about a stage.
### Stage renderers and tooltip behavior

<table>
<thead>
<tr>
<th>Renderer</th>
<th>Tooltip behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legacy</td>
<td>When a user points to a stage, the tooltip displays the name of the stage. In the expanded view, the activity status appears in parentheses next to the stage.</td>
</tr>
</tbody>
</table>

![Waiting for Approval](image-url)
When a user points to a stage, the tooltip displays the name of the stage. If the stage is a gated approval, the tooltip also shows the name of the approver. In the expanded view, the activity status appears in parentheses next to the stage.

If you do not want the approver’s name included in the tooltip, navigate to System Properties > Service Catalog and clear the Show the current pending approver’s name in the stage widget mouseover check box.

Property for displaying pending approver’s name

Workflow stage renderers
Workflow stage renderers determine how a workflow displays stages in a workflow field.

There are multiple renderers available.

Note: Most workflows should use the workflow-driven renderer. This renderer is used by default for all workflows. Use a different stage renderer only after careful consideration and to satisfy specific requirements for how the stages appear.
Workflow-driven

Use the workflow-driven renderer as much as possible. This renderer displays icons for stages using the stage state controlled by the workflow. Icons are displayed in a way that is meaningful for many situations. This renderer can display stages from a main workflow and subflows. The order of the icons is determined by the expected path of the executing workflow. As the workflow progresses, stages on paths that the workflow did not take are removed from the display. Stages from paths other than the expected path are not included unless the workflow follows that path.

The **Stage order** field on the **Stages** tab has two options:

- Computed uses the actual workflow path in order
- User-specified uses the order specified in the **Order** column on the Workflow Stages record

Main flow

The main flow renderer displays icons for stages defined in the main workflow only. Use this renderer when you do not want to expose the details of the subflows. For example, a single main workflow may run several subflows to handle implementation details. The stages in these subflows do not provide useful information for the user who starts the workflow, but are useful when editing the subflow. In this scenario, using the main flow renderer leads to the best user experience. The stage field displays the high-level process of the workflow without exposing unnecessary details.

The **Stage order** field on the **Stages** tab has two options:

- Computed uses the actual workflow path in order
- User-specified uses the order specified in the **Order** column on the Workflow Stages record

**Note:** If the workflow context for a request item has been deleted, the stages for that request item can no longer be rendered. This stage history is stored on the workflow context.

Linear

Linear rendering displays all stage icons from the main workflow and all subflows within a single workflow field on a list or form. It displays icons in a linear sequence regardless of the paths the workflow follows as it executes. This renderer uses stages defined in both the main workflow and any subflows that the main flow launches. The icons appear in the user-specified order. Skipped stages do not appear.

Use this renderer when the workflow stages must display in a consistent order and the actual details of how the workflow runs are less important. For example, a workflow may revisit or revert to previous stages based on one or more Condition Workflow activities. Displaying these loops in the stage field does not provide useful information to the user. In this scenario, using the linear renderer leads to the best user experience. The stage field displays the predefined process, including stages from subflows, in a consistent order.

For example, you can create a service catalog workflow that uses a subflow to complete delivery of the requested item. The following images illustrate the main flow and subflow for ordering corporate-branded supplies.
The linear renderer displays all these stages in one workflow field. The parent workflow specifies the Waiting for approval, Fulfillment, and Completed stages. The subflow specifies the Delivery and Waiting for Task, and Delivery OK stages.

**Progress bar**

The progress bar renderer displays a single progress bar instead of a sequence of stage icons. This renderer is particularly useful when you want to display the general progress of the workflow as a percent. Each stage in the workflow controls an equal percentage of the progress bar. For example, if a workflow has 10 stages, reaching each stage causes the workflow field to display an additional 10% of the progress bar. Stage names do not appear in the progress bar.
The progress bar renderer provides a way to display the status of a workflow that has a large number of stages. Other rendering options may provide a better user experience when rendering fewer than four stages in a single workflow.

The **Stage order** field on the **Stages** tab has two options:

- Computed uses the actual workflow path in order
- User-specified uses the order specified in the **Order** column on the Workflow Stages record

### Legacy

The legacy renderer displays stages in the same way as releases prior to Dublin. When an instance is upgraded from a release prior to Dublin, all existing workflows are set to use the legacy renderer. Whenever possible, use a different stage renderer instead. If you want your workflow to maintain pre-Dublin behavior, use the Legacy option. The legacy renderer sometimes assigns incorrect data to and/or reports incorrect data from the workflow stage field. If possible, we recommend all workflows use the Workflow-driven renderer.

With the legacy renderer, you can create and reference a custom workflow field icon set by setting the icons attribute to a new script include. For example, to use the `WorkflowIconsSCR` script include to define which icons to use, add the attribute `icons=WorkflowIconsSCR` to the **Attributes** field of the dictionary entry for the workflow field. To use the default icon display behavior, use the attribute `icons=WorkflowIconsStages`.

The legacy renderer works with all tables except the Requested item (sc_req_item) table. In this case, use the requested item renderer instead.

### Requested item

The requested item renderer functions the same way as the legacy renderer, but is for use with the Requested item (sc_req_item) table.

Select a stage renderer

In most cases, the default workflow-driven renderer should be used. If you have specific requirements for displaying stages, you can select a different stage renderer.

Consider the following when selecting a stage renderer:

- Use the workflow-driven renderer if possible. This is the default renderer that should be used in most cases.
- Use the legacy renderer only if your instance was upgraded from a release prior to Dublin and you want your workflow to maintain pre-Dublin behavior.

To use linear, main flow, or progress bar rendering, satisfy the following requirements.
### Linear and progress bar renderer requirements

<table>
<thead>
<tr>
<th>Renderer</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| Linear      | • The parent workflow and all subflows must modify the same current record.  
• In the properties for all subflows, the **Stage field** value for all subflows must match that of the parent workflow.  
• The parent flow and all subflows must contain the same stages. Use a stage set to ensure the parent flow and all subflows have the same stages.  
• On the workflow canvas, each workflow needs only the stages used directly by that workflow. It is not necessary to add stages from subflows to activities on the parent flow, or stages from the parent flow to activities on the subflows. |
| Main flow   | • The workflow contains subflows.  
• You do not want or need to reveal the details about the subflows. |
| Progress bar| • The workflow properties must have a **Stage ordering** value of **User-defined**  
• There must be workflow stages within the workflow.  
• Because stage names do not appear in a workflow field when using the progress bar renderer, you can simplify stage names to represent a percentage of the workflow. For example, if a process has four main steps, name the workflow stages as 25%, 50%, 75%, and 100%. Enter the numerical value of each stage, such as 25, in the **Value** and **Order** fields. |

To select a stage renderer:

1. Navigate to **Workflow > Workflow Editor**.
2. Open and check out the workflow.
3. In the title bar, click the menu icon and select **Properties**.
4. In the Workflow Properties dialog box, click the **Stages** tab.
5. From the **Stage rendering** list, select a stage renderer.
   - If you are using two workflows to update two unique workflow fields on a single record, both workflows must use a non-legacy renderer. You can select a different stage renderer for each workflow but do not select **Legacy** for either one.
   - If you want to use the linear renderer, make sure you select **Linear** in the properties for the parent workflow and all subflows.
6. Click **Update**.
**Workflow fields with deleted records**

Workflow fields may indicate when a record required by the workflow is deleted.

After a referenced record is deleted, the reference in the primary record is no longer valid. If the stage renderer detects a reference that is no longer valid, the stage field displays a message about the deleted record.

Administrators can restore deleted records. For more information, see [Restore a deleted record and reference](#).

**Workflows with missing records**

The image shows a list with two workflows. The top request does not have an associated request item. The bottom request has an associated request item, but the item does not have an associated workflow context.

**Workflow validation**

Workflow validation examines different characteristics of a workflow to locate issues that might prevent the workflow from being published or cause it to fail. The validation report summarizes the results of each separate workflow validation.

Validation prevents workflows with critical flaws from executing and resulting in an unstable or incomplete state. There are a number of validators in the base system that notify workflow designers of potential problems. For example, multiple End activities, disconnected transitions, incorrect table references, missing subflows, and dependencies affected by update sets. A workflow validation report displays the results from each validator, including a message explaining what was found. The system automatically validates a workflow when you publish it. You can also run validation on a workflow directly from controls in the Workflow Editor.

**Highlighting critical errors**

The graphical Workflow Editor highlights critical errors when a workflow is loaded. In this example, a subflow is missing and is not available to the parent workflow for the current user. The graphical Workflow Editor indicates the error when the parent workflow loads by highlighting (in red) the activity that calls the subflow. To correct the error in the parent workflow, click the validate icon in the header bar and inspect the error description in the validation report.
Validate missing subflow

Validations at publishing

If you attempt to publish an invalid workflow or a workflow with potential problems, the system displays an error message and blocks the operation, if necessary. When validation error messages appear, click the validate icon in the graphical Workflow Editor to see the error report.

Validation warning

A validation warning notifies you that a potential problem exists in a workflow but permits you to publish the workflow. Validation warnings appear when:

- You edit and then attempt to publish a workflow that is included as a subflow in another workflow. The system cannot determine how your changes will affect the parent workflow and alerts you of the relationship.
- A workflow activity uses a different table than the table assigned to the workflow. The system alerts you of the potential conflict.

Publish Confirmation

Validation warning. Click the validation button in the toolbar to get details:

Validate Summary - Workflow version contains Warnings - Total checks performed:15 (Info:13 Warn:2, Critical:0)

Publish this workflow with warnings?

validation warning

Validation failure
A validation failure notifies you that a critical error has occurred in the workflow that prevents you from publishing the workflow. An example of a critical error is a missing subflow.

**Validation failure**

**Workflow validation report**

Validators display three notification levels: CRITICAL, WARN, and INFO. The designer can publish a workflow that returns WARN or INFO level validation, but not a workflow that returns an overall validation level of CRITICAL.
Workflow validation report

Header summary

The header of the validation report summarizes the entire validation run against the specified workflow.

- **Validate Summary**: The overall score reflects the most severe notification level encountered during the validation.
- **Total checks performed**: The total number of validations run is also broken down to show the number at each notification level.

Report columns
The body of the report displays the results of each individual validation check that was performed. The columns are **Type**, **Level**, and **Message**. You can sort and filter these columns as you would any list.

### Workflow termination and external dependencies levels

<table>
<thead>
<tr>
<th>Name</th>
<th>Implication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Info</td>
<td>Provides information about the current workflow version. An example of an information level message is one that names the lowest common table in the workflow. Workflows at this validation level are considered valid and publishable.</td>
</tr>
<tr>
<td>Warning</td>
<td>Alerts the user that the validator detected anomalies in the workflow that might compromise its ability to execute. An example of a warning level message is one that alerts you to a missing activity input transition. Workflows at this validation level are considered valid and publishable.</td>
</tr>
<tr>
<td>Critical</td>
<td>Names a workflow element containing a critical error that prevents the workflow from executing successfully. Examples of this are missing or invalid subflows and missing transitions. Workflows at this validation level cannot be published or run in production.</td>
</tr>
</tbody>
</table>

### Message

The validation message provides a detailed description of the results, including table names, update sets, and other specifics.

For the procedure to validate a workflow and generate a validation report, see [Validate a workflow](#).

### Workflow validator

ServiceNow offers several workflow validators for workflow designers to test their workflows.

This page lists all available workflow validators. See [Workflow validation](#) for information on using workflow validators and the workflow validation report to see the type of information that is returned.

### Hanging workflows and update sets

<table>
<thead>
<tr>
<th>Hanging Workflows</th>
<th>Update Sets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify workflow design decisions that can result in a hanging workflow</td>
<td>Identify related artifacts being moved in different update sets</td>
</tr>
<tr>
<td>ValidateTransitionOut</td>
<td>ValidateUpdateSetDependencies</td>
</tr>
<tr>
<td>ValidateTransitionIn</td>
<td>ValidateUpdateSetParentDependencies</td>
</tr>
<tr>
<td>ValidateDanglingTransition</td>
<td>ValidateInputVarUpdateSetDependencies</td>
</tr>
<tr>
<td>ValidateSubflows</td>
<td></td>
</tr>
<tr>
<td>ValidateScriptForCurrentDotUpdate</td>
<td></td>
</tr>
</tbody>
</table>
Workflow termination and external dependencies

<table>
<thead>
<tr>
<th>Unexpected Workflow Termination</th>
<th>External Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify workflows that can end unexpectedly</td>
<td>Identify external artifacts that have potential workflow dependencies</td>
</tr>
<tr>
<td>ValidateSingleEnd</td>
<td>ValidateParentFlow</td>
</tr>
</tbody>
</table>

Workflow conflicts

<table>
<thead>
<tr>
<th>Workflow Properties Conflicts</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify workflow design decisions that conflict with workflow properties</td>
<td></td>
</tr>
<tr>
<td>ValidateLowestCommonTable</td>
<td>ValidateTableChange</td>
</tr>
</tbody>
</table>

**ValidateTransitionOut**

The **ValidateTransitionOut** validator finds activity conditions with no exit transitions.

**Validation summary**

- **Risk**: Activity conditions might not transition to the next activity, which could cause the workflow to hang.
- **Severity Level**: Warning
- **Valid Result**: Valid
- **Valid Message**: All conditions have transitions.
- **Invalid Result**: Invalid
- **Invalid Message**: This workflow contains <condition count> activity conditions without an output transition.
- **Suggested Action**: If this is a conscious design decision, there is no corrective action. Otherwise, find the condition cited in the validator and add an appropriate transition to the next activity.
- **Publishable**: Yes
- **Runnable**: Yes
- **Related Information**: None

**Troubleshooting**

Design choices made when creating a workflow on the canvas might legitimately use an activity without an exit condition. In the first example, the **Notification** and **Timer** activities both execute at the start of the workflow. The **Timer** is the entity that decides when the workflow ends. In this situation, executing the **Notification**, but not transitioning away, keeps the design simple and adds no risk. The validator finds and reports the missing transition from the **Notification** activity as a **Warning** that the designer can ignore.
Condition with no valid transition

In the second example, the Notification activity has no exit transition. The designer missed this because of the layout. The transition from the Timer activity passes behind the Notification activity and appears to connect the exit from the Notification activity to the End. In workflows with more than 10 or 15 activities, it might be difficult to see all the transitions clearly. This workflow’s designer intended for the Notification activity to transition to the End.

No condition out

This validator directs the designer to the specific activity and condition that does not have an exit transition. The designer then makes the decision whether or not to respond to the warning.

ValidateTransitionIn
The ValidateTransitionIn validator finds activities that do not have inbound transitions and cannot execute in the workflow.

Validation summary

- **Risk**: Activities that do not have inbound transitions have no means of being executed in the workflow. If other logic builds from these activities, the workflow could hang, with no means of moving forward.
- **Purpose**: Find activities that do not have inbound transitions.
- **Severity Level**: Warning.
- **Valid Result**: Valid.
- **Valid Message**: All activities in this workflow have at least one inbound transition.
- **Invalid Result**: Invalid.
- **Invalid Message**: This workflow contains <activity count> activity conditions without an input transition.
- **Suggested Action**: Either remove the activities to reduce confusion and make the workflow easier to understand or provide the appropriate inbound transition.

### Troubleshooting

Although the activities detected in this validator do no harm to the execution of the workflow, the designer needs to know that there are activities on the canvas that cannot execute and serve no purpose, particularly in a production system. This error is typically caused by a visual misinterpretation of the drawing.

This example workflow appears to be perfectly valid. Under closer inspection, however, we see that the transition from **Set Values** does not stop at **Approval - User** (there is no arrow end). Instead, that transition goes directly to **End**. As a result, **Approval - User** cannot execute. Because there is an activity in the workflow based on the approval's condition routing, it appears that the designer intended for the approval to execute and that a correction is needed.

```
<table>
<thead>
<tr>
<th>Begin</th>
<th>X= Set Values</th>
<th>Approval - User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always</td>
<td></td>
<td>Approved</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rejected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Approval Action</td>
</tr>
</tbody>
</table>
```

### TransitionIn invalid

This validator directs the designer to the specific activity and condition that has no inbound transition. The designer should establish a transition or remove the activity.
ValidateDanglingTransition
The **ValidateDanglingTransition** validator finds and reports any transitions that do not terminate on an activity.

**Note:** These transitions are not drawn on the workflow canvas, but are still present in the database.

**Warning:** This is a critical error that prevents a workflow from running.

**Validation summary**
- **Risk:** A workflow with dangling transitions will silently hang a workflow with no recovery options.
- **Severity Level:** Critical
- **Valid Result:** Valid
- **Valid Message:** Valid
- **Invalid Result:** Invalid
- **Invalid Message:** Invalid
- **Suggested Action:** Remove or connect the offending transition. Get the source activity name from the validation report details and resolve the issue. Then, run the validation again to test your changes.
- **Publishable:** No
- **Runnable:** No
- **Related Information:** None

**Troubleshooting**

On rare occasions, the destination of a workflow transition becomes null. The workflow canvas shows no evidence of the transition, but at run time, the workflow hangs when it encounters one of these dangling transitions. If the **ValidateDanglingTransition** validator reports this condition at publishing time, it blocks the publication action until the issue is resolved. If this condition is detected on a runtime check, the workflow is not allowed to execute against a current record’s transaction. Instead, the system adds a critical log entry detailing the activity with the faulted transition to the current record’s workflow context. To enable the workflow to execute on the next appropriate transaction, remove the faulted transition from the workflow model.

To find and remove the faulted transition:

1. Make note of the workflow version and activity that contains the faulted transition as indicated in the validator details.
2. Navigate to **Workflow > Administration > Workflow Version**.
3. In the list of workflow versions, select the workflow that has the faulted transition.
4. On Workflow Version form, add the workflow activities related list. Click the menu icon, select **Configure > Related Lists**, move Workflow Activity-->Workflow Version from the **Available** list to the **Selected** list, and click **Save**.
5. In the **Workflow Activities** related list, select the activity cited in the validator.
6. In the Workflow Activity form, view the **Workflow Transitions** section or tab and identify the transition in that list that has no value or a null value in the To column.
7. Delete this transition.

© 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.
8. Return to the workflow version and re-run the validation check.

The Critical warning should disappear. The workflow should execute as expected on the next appropriate transaction.

**ValidateSubflows**

The ValidateSubflows validator detects any workflows included as subflows that are either inactive, deleted, or not available as a published workflow for the current user.

Any of these conditions cause the workflow to hang when the workflow activity in the main flow is encountered.

**Warning:** This is a critical error that prevents a workflow from running.

**Validation summary**

- **Risk:** A parent workflow that transitions to a deleted subflow hangs indefinitely, with no recovery options.
- **Severity Level:** Critical
- **Valid Result:** Valid
- **Valid Message:** This workflow contains `<count>` valid subflows.
- **Invalid Result:** Invalid
- **Invalid Message:** This workflow contains `<invalid count>` invalid subflow(s) of `<total subflow count>` total subflows.
- **Suggested Action:** Remove the link in the parent workflow to the questionable subflow, examine the subflow to ensure that it is valid and published, or that it is checked out to the current user. After making the correction to the state of the subflow, run the validation again to test your changes.
- **Publishable:** No
- **Runnable:** No
- **Related Information:** Workflows used as subflows

**Troubleshooting**

When a workflow runs, regardless of whether it is a subflow or a main flow, the script engine determines which version of a workflow should execute, given the current user and workflow conditions. When a workflow is checked out by the same user who is running the workflow, the checked out version is the version that executes. If the user is not the same person who has the workflow checked out, the published version of the workflow executes. If there is no published workflow, no workflow runs.

One scenario addressed by the ValidateSubflows validator is when a workflow:

- Is checked out to User A.
- Is a subflow in a parent workflow being run by User B.
- Has no published alternative to the subflow being run by User B.

When this occurs, the parent workflow runs to the execution of the unpublished subflow and then hangs at that activity, with no means to transition forward. Main flows that encounter this condition in a subflow are not permitted to execute against a current record's transaction. Instead, a critical log entry detailing the subflow's state is added to the current workflow's Workflow Context record. To correct the problem, remove the subflow from the main flow, or...
publish the subflow so it is available to User B. This allows the workflow to execute on the next appropriate transaction.

Another scenario addressed by the **ValidateSubflow** validator is when a workflow:

- Is a subflow in a parent workflow being run by any user.
- Has no published alternative to the subflow, because the workflow has been deleted or all versions of the workflow are unpublished or inactive.

**Note:** You cannot delete a from a list or form workflow that is a subflow. However, you can create one of these unstable conditions with advanced scripting, SQL options, or incomplete update sets that contain main flows, but not the referenced subflows. When troubleshooting a workflow that triggered this validator, consider the history of the subflow while assessing the error condition.

**Validation summary**

- **Risk:** At best, a workflow that uses `current.update()` in scripts experiences degraded performance. In the worst case, the workflow enters an infinite, recursive loop that crashes the server.
- **Severity Level:** Warning
- **Valid Result:** Valid
- **Valid Message:** The JavaScript in this workflow has no instances of `current.update()`.
- **Invalid Result:** Invalid
- **Invalid Message:** This workflow uses `current.update()` in <count of current.update references> JavaScript statements.
- **Suggested Action:** Remove `current.update()` from the activity scripts cited by this validator. Workflows execute within a transaction, and current is updated, or possibly inserted, at the end of the transaction, as appropriate. There is no need to explicitly update the record during the transaction.
- **Publishable:** Yes
- **Runnable:** Yes

**Problems with `current.update()` in workflow scripts**

A workflow initiates execution in one of these ways:

- **Script Engine:** If a workflow is assigned to a specific table, and given a run condition, the workflow runs on INSERT.
- **Script:** Any business rule, script include, background script, or client script can initiate a workflow using the workflow script include and calling `startFlow()`.

The workflow engine initiates a workflow based on the matched criteria of the current record being inserted. The transaction for current is managed by the script engine and not the workflow. Workflows that progress on the `update()` of the current record are not invoked via the workflow engine, but as a call from either a client script or business rule. In either case, the script engine is
invoked, and the current record is put in memory. Edits and modifications to any current fields are made and are available to other activities and scripts that are executed in the same transaction.

When appropriate, other engines that run in sequence with the workflow engine, such as the business rule engine or field normalization, are invoked against the same current record transaction. Any changes made to current through these scripts and activities modify the record in memory. These changing values are available for reference in any other transactions called from activities and scripts in the same INSERT transaction. When all expected changes are executed, the current record is inserted.

When one of these scripts calls `current.update()` on a record that has yet to be inserted, the action forces an unnecessary and error-prone database transaction. If a record is not yet in the database, it cannot be updated. Business rules that trigger on `update()` on a record that is in the process of being inserted can cause a very unstable and potentially infinite looping condition.

**Troubleshooting**

This validator detects the use of `current.update()` in any of the editable script fields. Do not call `current.update()` from within a workflow script. In the event of an INSERT or UPDATE of current, the changes made to current are available to all scripts executing in the same transaction, and the script engine stores all changes in the database. Leave the update of current to the engine. Use the scripts only for setting and referencing the current field values.

**ValidateLowestCommonTable**
The **ValidateLowestCommonTable** validator reports the lowest table in the Glide hierarchy that the workflow uses.

For example, the Requested Item (sc_req_item) table is the lowest table in a workflow containing a **Catalog Task** activity. This information is significant to a designer who wants to change the table against which an existing workflow runs after adding activities to the canvas.

**Note:** This validator provides information only. It does not indicate an error or warning condition.

**Validation summary**

- **Risk:** This validator informs only and has no risk associated with it.
- **Severity Level:** Data/Information
- **Valid Result:** Valid
- **Invalid Message:** The lowest common table in this workflow is <<table_name>>.
- **Invalid Result:** N/A (informational only)
- **Invalid Message:** N/A (informational only)
- **Suggested Action:** None
- **Publishable:** Yes
- **Runnable:** Yes
- **Related Information:** *Tables and classes, Workflow activities*

**ValidateTableChange**
The **ValidateTableChange** validator reports any activities in the workflow that are invalid given the table associated with the workflow version.

For example, a workflow version that is associated with the Change Request (change_request) table but has a **Catalog Request** activity on the canvas is invalid, since the activity is not compatible with the selected table.
Validation summary

- **Risk:** If the current record at runtime does not originate from the table specified by the lowest common table, the activities for the lowest common table cannot set specific values.
- **Severity Level:** Warning if the table that is associated with a workflow is higher in the table hierarchy than the lowest common table required for the workflow activities.
- **Valid Result:** Valid
- **Valid Message:** All activities are valid for the newly selected table
- **Invalid Result:** Invalid Activity
- **Invalid Message:** This workflow contains <count of invalid activities> invalid activities for the newly selected table.
- **Suggested Action:** Make one of these changes:
  - Change the workflow to not require the activities associated with the lowest table reported.
  - Modify the workflow to use a table that contains the lowest common table in its hierarchy.
  - Ensure that the current record meets the requirements of the at-risk activities.

- **Publishable:** Yes
- **Runnable:** Yes
- **Related Information:** Workflow activities

Troubleshooting

Navigate to Workflow > Administration > Activity Definitions. Note the Table column in the list. Each activity that is not global is associated with a table.

When you select a table in the Workflow Properties form, the activity menu presents only activities that are compatible with the selected table. Associating a table with a workflow activity enables the system to make certain decisions about the activity that affect value comparison, condition routing, or the setting and getting of field values in the current record.

When a workflow is set to the Global (global) table, it is possible that the process executing the workflow ensures that the current record meets the requirements of the activities identified by this validator. In that case, the activity still works as expected. If that assurance cannot be guaranteed by the user process, do not use the activity identified by the validator without assigning a table that meets the requirements of all the activities on the canvas.

This validation check ensures that the table specified by all the activities in a particular workflow is included in the hierarchy of the table selected for the workflow.

ValidateParentFlow

The ValidateParentFlow validator reports any workflows that use the workflow as a subflow.

Validation summary

- **Risk:** There is no risk in a workflow being a subflow. This is only a warning that other workflows are at risk from dramatic changes to a subflow.
- **Severity Level:** Warning
- **Valid Result:** Valid
- **Valid Message:** Currently <workflow version name> is not a subflow.
- **Invalid Result:** None
- **Warning Message:** This workflow version (<workflow version name>) is required as a subflow in <workflow version count> other workflows.
**Suggested Action:** Exercise caution when modifying things like input parameters and return values to assure that parent workflows are not adversely affected.

**Publishable:** Yes

**Runnable:** Yes

**Related Information:** Workflows used as subflows

### Troubleshooting

The system warns the workflow designer at publishing time and during validation that a workflow is a subflow. This warning reminds the designer that changes to the current workflow have the potential to affect workflows cited in the validation report or other workflows already running in production. Regardless of how simple the change to a workflow that is a subflow, thoroughly test all parent flows cited in this validation report before publication.

When a workflow is a subflow, changes that can cause it to become invalid include:

- Changing the data types of **input variables**. Verify that all parent workflows cited in this validation report can pass the correct value type.
- Adding input variables. Verify that all parent workflows cited in this validation report are able to pass all variable values into the subflow.
- Changing or removing the return value of a workflow. Verify that any changes to the return value of a workflow are compatible with the requirements of all the parent flows.
- Changing the table on which the workflow runs. Verify that the table selection is compatible with all parent flows.

**Note:** To delete a workflow that is a subflow, first remove the dependency by removing the subflow from all parent flows cited in this validation report. After the dependencies are cleared, a user with the proper role can delete the subflow.

**ValidateSingleEnd**

The **ValidateSingleEnd** validator finds and identifies multiple **End** activities in a single workflow.

Multiple **End** activities in a workflow might be intentional and have no affect on the workflow, or might be a mistake that the designer needs to correct.

### Validation summary

- **Risk:** If the execution paths to the **End** activities are not mutually exclusive, then the first **End** encountered completes the workflow and cancels all other executing activities.
- **Severity Level:** Warning
- **Valid Result:** Valid
- **Valid Message:** This workflow contains 1 **End** activity.
- **Invalid Result:** Invalid Activity
- **Invalid Message:** This workflow contains <count of ends> **End** activities.
- **Suggested Action:** Remove extraneous **End** activities that are not intended as part of the design.
- **Publishable:** Yes
- **Runnable:** Yes
- **Related Information:** None
Troubleshooting

As soon as an **End** activity is encountered in the workflow, the workflow completes even if there are other viable execution paths leading to a second **End** activity that is still executing. Those executing activities are canceled as part of the **End** activity’s clean up actions. Therefore, the results of designing workflows with multiple **Ends** must be carefully considered.

In the case of large workflows, it is often more intuitive to read the workflow when there are multiple **End** activities. In the following example, the paths to the two **Ends** are mutually exclusive execution paths. If this was a large workflow, with many activities between **Branch** and the second **End**, the value of the multiple ends becomes apparent. Tracing a **No** response from **User** is invalid to a single **End** behind 33 other activities would be significantly more difficult. There is no risk in this workflow design because there is no reason for other activities to execute if the **End** after the **Notification** activity terminates the workflow.

The next example has multiple **End** activities in execution paths that are not mutually exclusive. A **Yes** response from **User is valid** causes the **Set Values** activity to finish immediately. By reaching its **End** activity first, this execution path cancels the **Approval for Apps** and the **DB Task** activities, which might not be the desired outcome. If the paths are all expected to complete before **End**, the activities should come to a **Join** (as in the previous example) that transitions to a single **End**.
Mutually inexclusive execution paths

**Note:** To add the second End, right-click to copy the original End activity and paste it onto the canvas. In most cases, a single End is the best and most reliable way to ensure that all activities expected to execute prior to workflow completion, do so successfully.

**ValidateUpdateSetDependencies**

The ValidateUpdateSetDependencies validator identifies all the subflows called in the current workflow and determines if any of those subflows are being edited in a different (in progress) update set.

This warning informs the user that this workflow and one or more of its dependencies are being actively modified in a way that will not deploy concurrently to another instance without additional effort.

For information about update sets, see [Create and select an update set](#).

**Validation summary**

- **Risk:** If a parent workflow is edited in one update set and its dependent subflow is edited in another, the two workflows might not be compatible when moved to a different instance. Making independent changes, such as to common or expected values, can make the two workflows incompatible.
- **Severity Level:** Warning
- **Valid Result:** Valid
- **Valid Message:** There were no Update Set dependency issues found.
- **Invalid Result:** Invalid
- **Invalid Message:** This workflow has dependent workflows that are in a different update set.
- **Suggested Action:** Modify and deploy both workflows in the same update set. If you must modify dependencies in separate update sets, use one of these methods:
  - Ensure that all update sets migrate concurrently.
  - Prior to deploying the main flow update set, merge the dependencies into one update set before completing that update set.

- **Publishable:** Yes
- **Runnable:** Yes
- **Related Information:** Workflow movement with update sets

**Troubleshooting**

A workflow is added to an update set only when the workflow is published. This validator issues a warning when either of the following conditions exist:

- A published subflow is in a different update set than the parent workflow and that update set is In progress.
- A subflow is checked out by another user, who is working in a different update set than the current user.

**Note:** This validator does not look for update sets that have been closed. It looks only at update sets that are In progress or at the update sets of all subflows being used by the current workflow that are checked out to users who are working in a different update set.

**Example**

Following is an example of an at-risk development scenario in which two users create dependencies between workflows in different update sets.

**User A:**
1. Sets Update Set A to the current update set.
2. Checks out Workflow A.
3. Changes the return value of the **String** type in Workflow A to a **Reference/User** type.
4. Publishes Workflow A, causing an entry into Update Set A.

**User B:**
1. Sets Update Set B to the current update set.
2. Checks out Workflow B.
3. Includes Workflow A as a subflow.
4. Uses the user reference return value from Workflow A as an approval assignment.
5. Publishes Workflow B, causing an entry into Update Set B.
Risks

- User B moves Update Set B to a different instance that has an older version of Workflow A. The return value is not a user reference, which causes the outcome of Workflow B to be different than it was when tested in development.
- User B moves Update Set B to a new instance that does not have a version of Workflow A. Workflow B experiences a validation failure at runtime and cannot execute. A log entry is added to the workflow log of the current record.

Possible solutions

Solution 1
Migrate the parent workflow and all dependent workflows to a new instance together using the same update set.

1. Set the update set to the one you want to migrate to new instances.
2. Check out and republish the workflows that need to be included.
   - This action forces an entry into the current update set.
3. Complete the update set with all dependencies.
4. Follow standard procedures for migrating update sets to local instances.

Solution 2
Move dependent workflows between update sets.

1. Identify the update set containing the main workflow to be migrated.
2. Navigate to System Update Sets > Local Update Sets.
3. Find and select the update set that contains the dependencies to the main workflow.
4. In the Customer Updates related list, select the workflow version of the subflow you want to move.
5. Select the update set containing the parent workflow in the Update set field.
   - If this field is not on the Customer Update form, configure the form and add the field.
6. Click Update.
   - The base system moves the dependent subflow to the update set selected.
7. Repeat steps 4-6 to add additional dependent subflows to the parent flow update set.

ValidateUpdateSetParentDependencies
The ValidateUpdateSetParentDependencies validator identifies all the workflows that call the current workflow as a subflow and determines if any of those parent workflows are being edited in a different update set that is in progress.

This warning informs the user that this workflow and one or more workflows that depend on this workflow are being actively modified in a way that will not deploy concurrently to another instance without additional effort.
Validation summary

- **Risk:** If a parent workflow is edited in one update set and its dependent subflow is edited in another, the two workflows might not be compatible when moved to a different instance. Making independent changes, such as editing common or expected values, can make the two workflows incompatible.
- **Severity Level:** Warning
- **Valid Result:** Valid
- **Valid Message:** There were no Update Set dependency issues found.
- **Invalid Result:** Invalid
- **Invalid Message:** This workflow has dependent workflows that are in a different update set.
- **Suggested Action:** Modify and deploy both workflows in the same update set. If you must modify dependencies in separate update sets, use one of these methods:
  - Ensure that all update sets migrate concurrently.
  - Prior to deploying the main flow update set, merge the dependencies into one update set before setting that update set to complete.
- **Publishable:** Yes
- **Runnable:** Yes
- **Related Information:** Workflow movement with update sets

Troubleshooting

A workflow is added to an update set only when the workflow is published. This validator issues a warning when either of the following conditions exist:

- A published subflow is in a different update set than the parent workflow and that update set is In progress.
- A subflow is checked out by another user, who is working in a different update set than the current user.

**Note:** This validator does not look for update sets that have been closed. It looks only at update sets that are In progress or at the update sets of all parent workflows that call the current workflow and are checked out to users who are working in a different update set.

Example

Following is an example of an at-risk development scenario in which two users create dependencies between workflows in different update sets.

**User A:**
1. Sets Update Set A to the current update set.
2. Checks out Workflow A.
3. Changes the return value of the **String** type in Workflow A to a **Reference/User** type.
4. Publishes Workflow A, causing an entry into Update Set A.

**User B:**
1. Sets Update Set B to the current update set.
2. Checks out Workflow B.
3. Includes Workflow A as a subflow.
4. Uses the user reference return value from Workflow A as an approval assignment.
5. Publishes Workflow B, causing an entry into Update Set B.

Risks

- User B moves Update Set B to a different instance that has an older version of Workflow A. The return value is not a user reference, which causes the outcome of Workflow B to be different than it was when tested in development.
- User B moves Update Set B to a new instance that does not have a version of Workflow A. Workflow B experiences a validation failure at runtime and cannot execute. A log entry is added to the workflow log of the current record.

Possible solutions

Solution 1
Migrate the parent workflow and all dependent workflows to a new instance together using the same update set.
1. Set the update set to the one you want to migrate to new instances.
2. Check out and republish the workflows that need to be included.
   - This action forces an entry into the current update set.
3. Complete the update set with all dependencies.
4. Follow standard procedures for migrating update sets to local instances. For information about update sets, see System update sets.

Solution 2
Move dependent workflows between update sets.
1. Identify the update set containing the main workflow to be migrated.
2. Navigate to System Update Sets > Local Update Sets.
3. Find and select the update set that contains the dependencies to the main workflow.
4. In the Customer Updates related list, select the workflow version of the subflow you want to move.
5. Select the update set containing the parent workflow in the Update set field.
   - If this field is not on the Customer Update form, configure the form and add the field.
6. Click Update.
   - The base system moves the dependent subflow to the update set selected.
7. Repeat steps 4-6 to add additional dependent subflows to the parent flow update set.
**ValidateInputVarUpdateSetDependencies**

The **ValidateInputVarUpdateSetDependencies** validator examines update sets to ensure that workflow input variables for a given workflow have not been deleted in different update sets than those currently **In progress**.

**Validation summary**

- **Risk**: Workflows and their input variables are not moved together in a single update set. The deletion of input variables is captured in a different update entry. If these two entries are not in the same update set, the workflow execution can be unstable.
- **Purpose**: Determine whether input variables that belonged to this workflow were deleted in a different update set.
- **Severity Level**: Warning
- **Valid Result**: Valid
- **Valid Message**: There were no Input Variable Update Set dependency issues found.
- **Invalid Result**: Invalid
- **Invalid Message**: There are input variables that have been deleted and logged in a different update set.
- **Suggested Action**: If the deletion is not intended to be separate from the workflow, ensure that both update sets are committed concurrently to the new instance, or merge both payloads into a single update set.
- **Publishable**: Yes
- **Runnable**: Yes
- **Related Information**: Workflow movement with update sets

**Troubleshooting**

Workflow input variables get individual entries in the **Customer Update** related list in the current user's update set. This validator reports to the user when workflow input deletions have happened in an update set other than the current user's update set.

Follow the instructions for **Input variable removal** when the validator issues this warning.

**ValidateWorkflowEndStages**

The **ValidateWorkflowEndStages** validator checks that in workflows with stages, the end activity of the workflow has a stage named Complete or Completed.

If the workflow has stages associated with it, but does not have the completed stage on the end activity, then the stage indicator will not show that the workflow completed.

**Validation summary**

- **Risk**: The stage indicator will not show the workflow is completed.
- **Severity Level**: Warning
- **Valid Result**: Valid
- **Valid Message**: Workflow end stages are valid.
- **Invalid Result**: Invalid
- **Invalid Message**: End activity A found with invalid stage 'S.'
- **Suggested Action**: If this is not by design, make the appropriate changes.
- **Publishable**: Yes
- **Runnable**: Yes

© 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.
Troubleshooting

Check the workflow for an end activity. Ensure that this activity assigns a stage named Complete or Completed.

**ValidateWorkflowStageColumn**
The **ValidateWorkflowStageColumn** validator detects and reports when the stage field (stage column) for a workflow is not correct or is unusable.

Validation summary

- **Risk:** The stage indicators may not display appropriate information.
- **Severity Level:** Warning
- **Valid Result:** Valid
- **Valid Message:** Workflow stage values are valid.
- **Invalid Result:** Warning
- **Info Summary:** Stage warnings found.
- **Invalid Messages:**
  - Table T does not have a column named C.
  - Workflow for table T has stages, but no stage column.
  - Table T has a stage column `C`, but no stages are set by activities.
  - Workflow on table T has stage column `C` that is not type=workflow.

- **Suggested Action:** If this is not by design, make the appropriate changes.
- **Publishable:** Yes
- **Runnable:** Yes
- **Related Information:** Workflow activities, Workflow stages

Troubleshooting

To check the stage column:

1. Open and check out a workflow.
2. Open the workflow version properties dialog by clicking the menu icon and selecting **Properties**.
3. View the **Stages** tab or section.
4. Check that the assigned stage column is actually a column in the table to which the workflow is associated.
5. Check that the column is type=workflow.

**Tip:** Stage columns should not be choice lists. If they are, the list appears read-only in form views, since changing that column value outside the workflow engine does not ensure safe tracking of stage states.

**ValidateWorkflowStateValues**
The **ValidateWorkflowStateValues** validator checks a number of stage aspects in workflow activities for correctness.
This validator has multiple possible error messages.

**Validation summary**

- **Risk:** The stage indicators may not display appropriate information.
- **Severity Level:** Warning
- **Valid Result:** Valid
- **Valid Message:** Workflow stage values are valid.
- **Invalid Result:** invalid
- **Warning summary:** Stage warnings found.
- **Invalid Messages:**
  - Stage with empty name is not allowed.
  - Stage with empty value is not allowed.
  - Cannot have more than one stage with the same name: x.
  - Cannot have more than one stage with the same value: y
- **Suggested Action:** If this is not by design, make the appropriate changes.
- **Publishable:** Yes
- **Runnable:** Yes
- **Related Information:** Workflow activities

**Troubleshooting**

Use the following procedure to troubleshoot this validator:

1. Open and check out a workflow.
2. Open the list of stages for the workflow by clicking the menu icon and selecting **Edit Stages**.
3. Check the names and values.
   
   Ensure that the names and values are unique and are not empty.

4. If the same stage name or value appears more than once, remove one of the rows. It is then very important to go through the workflow and reassign stages in the activities that used the removed stage.
Validate Workflow State Values

Tip: Make a list of which activities assign which stages.

Workflow concepts

You can do many things using the workflow editor.

- Modify core activities and exit conditions.
- Create custom activities and reuse the data for other workflows.
  See Orchestration activity designer.
- Download activity packs from the ServiceNow Store and create packs for upload.
- **Edit workflows** graphically.
- **Define transitions** between workflow activities.
- For the table that corresponds to the workflow, customize business rules.
- Summarize workflow progress through **stages**.
- **Validate workflows** to identify potential problems.
- **Publish workflows** for other users.
- **Edit multiple tables** without needing to directly modify them.

**Workflow versions**

To prevent users from making changes to a workflow that affect other users of the system, workflows must be checked out before they can be edited.

Only one user can check out a workflow at a time. When a workflow is checked out, changes apply only to the user who has the workflow checked out. Other users can continue to use the published workflow. After the changes are complete, the workflow can be published so that it is available to all users.

**Note:** Because each workflow has a unique sys_id, different workflows can have the same name. This is typically expected in a domain-separated environment where users in different companies cannot see each other’s workflows because they are in different domains. However, this can lead to confusion in other environments. In general, give each workflow a unique name to prevent workflow designers from making changes to the wrong workflow.

When a new version of an existing workflow is published, the changes are not applied to running workflow contexts. Any currently running workflow context continues using the workflow version that was available when the workflow started. The next time the workflow runs, it uses the updated, published version.

**Workflow scope**

Workflow application scope determines the access that an application has to the information in a workflow, specifically to the data contained in the activities in that workflow.

When a workflow is created, it inherits the application scope from the gear menu for the logged in user. This scope cannot be changed in the workflow editor. When the workflow executes, it runs in this scope and can only be called from a different application if the workflow’s accessibility setting permits access to all scopes (public). Otherwise, the workflow’s application scope is private to the application.

**Note:** Any script that is created in the workflow editor, such as an advanced script in an If activity, runs in the scope of the workflow. All core activities provided in the base system or for Orchestration run in the scope of the workflow.

Custom activities run in their own scope, even if it is different from that of the workflow. The scope of a custom activity can be private or public. Any script that runs inside a custom activity with a scope can only access outside artifacts that are within the scope of that activity or artifacts that are configured to run in any scope. Conversely, an outside artifact can only access the script inside that private activity if the outside artifact is running in the same scope. Activities with public scopes can interact with outside artifacts in any application scope.

You can use private activities as part of a workflow that has a public application scope. These activities are protected from reaching outside of the workflow or from being reached from outside the workflow. For details about setting application scoping for custom activities, see the field description table for the appropriate activity template.
**Workflow scope restrictions**

There are some restrictions to public and private application scopes.

During runtime, publicly scoped workflows can access other application resources, as long as these resources are set to be accessible to all application scopes. Privately scoped workflows in a private application scope can only access resources private to its scope. Due to scope access boundaries, any privately scoped workflows that make calls out to other scoped resources fail with either an exception or a hung activity while waiting for returned results. This occurs when making calls to these common global resources:

- ECC queues
- Tasks
- Approvals
- Events
- SLA timers
- Timers
- Script includes
- Business rules
- Workflow APIs

As you design workflows, validate the visibility and accessibility of all resources prior to deployment.

See [Application scope](#).

For information on how to configure the scope for a workflow, see [Workflow properties](#).

**Workflows and domain separation**

When domain separation is enabled, workflows and workflow activities inherit the domain of the user who publishes or creates them.

While workflows are managed by multiple tables, only the following tables are used for domain separation features:

- **Workflow (wf_workflow)**: used for delegated administration or process separation.
- **Workflow Version (wf_workflow_version)**: used for delegated administration or process separation.
- **Workflow Context (wf_context)**: used for data separation.

**Note:** The Workflow Version table (wf_workflow_version) table does not contain a domain field; Workflow Version records inherit their domain from the parent Workflow record.

The workflow editor displays a workflow's domain in the title bar after the workflow name.
Workflow editor domain

**Workflows and delegated administration**

Delegated administration allows child domains to inherit workflows from higher up the domain hierarchy and to override them with domain-specific versions if necessary.
Workflow and delegated administration

Workflow records in the Workflow (wf_workflow) and Workflow Version (wf_workflow_version) tables are considered processes. A user in a child domain may check out but not copy a workflow from a parent domain. When a user in a child domain checks out a workflow from a parent domain, the system creates a version of the workflow in that user's domain. This new version is a unique record in the Workflow (wf_workflow) table. After the user publishes this new workflow, other users...
in the child domain use the new workflow, which overrides the workflow from the parent domain. The original workflow in the parent domain is no longer visible to users in the child domain.

For example, a managed service provider (MSP) hosts ITSM services for several companies, including ACME and Initech, on a single instance. As administrators, the MSP creates a Change Request - Emergency workflow that applies to all domains because it was created in the TOP domain, which is the highest domain in the domain hierarchy. This workflow overrides the global Change Request - Emergency workflow and specifies that emergency change requests require approval from the CAB approval group. Because of delegated administration, every domain in the hierarchy sees and uses this workflow. Now suppose the ACME domain requires a different approval policy where emergency change requests require approval from the emergency CAB approval group. The MSP creates another version of the Change Request - Emergency workflow in the ACME domain. This workflow overrides the version in the TOP domain and only applies to users in the ACME domain.

**Workflow permissions**

When a user starts a new workflow, the workflow runs with that user's domain and credentials. The workflow preserves a user's domain and credentials until an activity causes the workflow to wait, such as an approval activity waiting for approval or rejection. When the stopped workflow resumes, such as when a user approves a request, the workflow uses the credentials of the approving user, but continues to run within the domain of the original user.

**Workflows and data separation**

Data separation restricts workflow contexts to users who are either in the same domain of the workflow or are members of a parent domain.
Workflow and data separation

Workflow records in the Workflow Contexts (wf_contexts) table are considered data. Data separation restricts workflow contexts to users who are either in the same domain of the workflow or are members of a parent domain. While a user in a parent domain can see running workflows...
in a child domain, a user in a child domain cannot see running workflows in a parent domain. If necessary, administrators can use visibility or contains domain to expand who can see domain-specific data.

For example, when an ACME user requests something from the service catalog, a Service Catalog Request workflow context is created in the ACME domain. Similarly, a service catalog request from an Initech user creates a workflow context in the Initech domain. An MSP user in the TOP domain can see both workflow contexts because it is the parent domain for both the ACME and Initech domains. However when an ACME or Initech user logs in, data separation prevents them from seeing each other's service catalog requests. This is expected behavior because each workflow context contains data specific to that domain, such as the item requested and the request's approval history.

**Workflow engine operation order**

The workflow engine runs in a predefined order relative to business rules and database operations. It caches commonly-used published workflows to improve performance.

The Run after bus. rules run workflow property defines if a workflow is Default or Deferred.

The diagram below shows the workflow engine order of operations and when Default and Deferred flows are executed. For a more general overview of engine operation order, see Execution order of scripts and engines.
**Before** business rules (order < 1000)
Do not use `current.update()` here

Default workflows
Do not use `current.update()`

**Before** business rules (order >= 1000)
Do not use `current.update()`

Database operation
(insert, update, delete)

The current record is inserted or updated at the end of the database operation.

**After** business rules (order < 1000)
Use `current.update()` if there is no deferred workflow

Deferred workflows
Do not use `current.update()`

**Always use** `current.update()`
Workflow caching

The workflow engine caches commonly-used published workflows to improve performance. Caching significantly reduces the number of database queries per workflow. By default, the engine caches up to 300 unique workflow versions. Caching very large workflows may reduce this number as the cache size cannot exceed the Java Virtual Machine (JVM) heap size.

To change the maximum number of cached workflow versions, navigate to Workflow > Administration > Properties and modify the value of the The max number of models that will be concurrently held in the LRU cache (glide.workflow.model.cache.max) property. You must restart the instance to apply this change.

Workflow tables

For full flexibility, workflows store information over a number of different tables.

Usually tables containing workflow information are not edited one-by-one. Instead, use the Workflow Editor to edit workflows. The following lists are provided for reference purposes.

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workflows</td>
<td></td>
</tr>
<tr>
<td>Column Renderer (column_renderer)</td>
<td>A renderer widget for a stage column. Stage renderers are written in Jelly as a UI Macro. The default is Workflow-Driven; it covers most workflow related stage scenarios.</td>
</tr>
<tr>
<td>Version (wf_versionable)</td>
<td>Tracks different versions of element definitions (wf_element_activity).</td>
</tr>
<tr>
<td>Workflow (wf_workflow)</td>
<td>The master records of workflows.</td>
</tr>
<tr>
<td>Workflow Context (wf_context)</td>
<td>Individual instances of a workflow being used.</td>
</tr>
<tr>
<td>Workflow Execution (wf_workflow_execution)</td>
<td>Synthetic &quot;current&quot; records for workflows that run on Global.</td>
</tr>
<tr>
<td>Workflow Instance (wf_workflow_instance)</td>
<td>Connections of workflows to subflows.</td>
</tr>
<tr>
<td>Workflow Version (wf_workflow_version)</td>
<td>Particular versions of a workflow, either published versions or versions that have been checked out.</td>
</tr>
<tr>
<td>Activities</td>
<td></td>
</tr>
<tr>
<td>Activity Designer (wf_element_activity)</td>
<td>Custom activity definitions.</td>
</tr>
<tr>
<td>Activity Variables (wf_activity_variable)</td>
<td>Variables for activities.</td>
</tr>
<tr>
<td>Workflow Activity (wf_activity)</td>
<td>Activities as they are being used in workflows.</td>
</tr>
<tr>
<td>Workflow Activity Definition (wf_activity_definition)</td>
<td>Definitions of activities that can be used in a workflow.</td>
</tr>
<tr>
<td>Workflow Executing Activity (wf_executing)</td>
<td>Individual instances of activities being performed in active contexts.</td>
</tr>
<tr>
<td>Workflow components</td>
<td></td>
</tr>
<tr>
<td>Element Provider (wf_element_provider)</td>
<td>Template definitions for custom activities.</td>
</tr>
<tr>
<td>Group approval (sysapproval_group)</td>
<td>Group-level approvals.</td>
</tr>
<tr>
<td>Variable (item_option_new)</td>
<td></td>
</tr>
</tbody>
</table>
### Table

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workflow Condition (wf_condition)</td>
<td>All of the defined conditions in workflows.</td>
</tr>
<tr>
<td>Workflow Element Definition (wf_element_definition)</td>
<td>Parent table for activity definitions.</td>
</tr>
<tr>
<td>Workflow Estimated Runtime Configuration (wf_estimated_runtime_config)</td>
<td>Runtime performance data for completed workflows.</td>
</tr>
<tr>
<td>Workflow Queued Command (wf_command)</td>
<td>Temporary internal storage for workflows that are currently executing.</td>
</tr>
<tr>
<td>Workflow SC Variable (wf_variable)</td>
<td>The Service Catalog variables for a workflow.</td>
</tr>
<tr>
<td>Workflow Schedule (wf_workflow_schedule)</td>
<td>Definitions of the times to run specific workflows.</td>
</tr>
<tr>
<td>Workflow Transition (wf_transition)</td>
<td>All of the defined transitions in workflows.</td>
</tr>
<tr>
<td>History</td>
<td></td>
</tr>
<tr>
<td>Workflow Activity History (wf_history)</td>
<td>The history of executed activities.</td>
</tr>
<tr>
<td>Workflow Log Entry (wf_log)</td>
<td>All of the events and history of the workflow.</td>
</tr>
<tr>
<td>Workflow Transition History (wf_transition_history)</td>
<td>The history of executed transitions.</td>
</tr>
<tr>
<td>Stages</td>
<td></td>
</tr>
<tr>
<td>Stage Default (wf_stage_default)</td>
<td>Definitions of default stage fields for tables to use.</td>
</tr>
<tr>
<td>Stage Set (stage_set)</td>
<td>A named set of stages that can be used to populate workflow stages for multiple workflows.</td>
</tr>
<tr>
<td>Stage Set Entry (stage_set_entry)</td>
<td>The stages that belong to a named stage set.</td>
</tr>
<tr>
<td>Stage Set for Table (stage_set_table)</td>
<td>Defines a relationship of a stage set to a table so that the stage set can be used as the default stages when a new workflow is created for the table. This replaces the wf_default_stage table and is the view that shows when you click Default Stages (by table) in the menu.</td>
</tr>
<tr>
<td>Workflow Stage (wf_stage)</td>
<td>Definitions of stages used by workflows.</td>
</tr>
</tbody>
</table>

### Workflow administration

Tailor workflows exactly the way you want them.

### Workflow roles

Certain roles are required to use workflows.

#### Workflow roles

<table>
<thead>
<tr>
<th>Role title (name)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity creator (activity_creator)</td>
<td>Creates and edits custom workflow activities, reuses custom activity data, and manages activity packs downloaded from the ServiceNow Store.</td>
</tr>
<tr>
<td>Role title (name)</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Web service administrator</td>
<td>Accesses and uses REST and SOAP messages in the Orchestration activity designer. Creates and edits custom activities that use the REST web service and SOAP web service templates.</td>
</tr>
<tr>
<td>(web_service_admin)</td>
<td></td>
</tr>
<tr>
<td>Workflow administrator</td>
<td>Creates, edits, publishes, and deletes graphical workflows.</td>
</tr>
<tr>
<td>(workflow_admin)</td>
<td></td>
</tr>
<tr>
<td>Workflow creator</td>
<td>Creates new graphical workflows.</td>
</tr>
<tr>
<td>(workflow_creator)</td>
<td></td>
</tr>
<tr>
<td>Workflow publisher</td>
<td>Publishes graphical workflows.</td>
</tr>
<tr>
<td>(workflow_publisher)</td>
<td></td>
</tr>
</tbody>
</table>

**Administering workflow contexts**

The workflow context performs the activities and transitions defined in the workflow with the new record as current.

Workflow in ServiceNow names a running workflow a Workflow Context. The Workflow Context maintains the state of the overall process in the Workflow Context record. The Workflow Context maintains the state of the individual activities as they execute in a series of related lists. These lists maintain the state of currently executing activities, the result of finished activities, and the execution path the workflow took through the process model.

The Workflow Context canvas provides a visual representation of the execution path the workflow took through the process model. The state of each activity (finished, executing, cancelled, error) is represented using the color palette. The executed paths are represented in the color blue; the non-executed paths are represented in grey. Active and historic workflow contexts, as well as the activities within them, can be viewed using the Live Workflows section of the Workflow application menu.

**Viewing a workflow context**

Workflow contexts can be found in two places:
- From the Workflow Context related link on the form of the task being powered by the workflow.
- By navigating to Workflow > All Contexts and selecting an active context.

**Displaying workflow progress**

Two related links on the Workflow Context form allow you to view the progress of a workflow in different formats.
- Show Timeline displays the workflow context as a timeline.
- Show Workflow displays the workflow context in the graphical workflow editor.
Graphical interface

To view the workflow context in the graphical workflow editor interface, click the Show Workflow link from either the workflow context record or the current record.

Show workflow

In the top right hand corner are two controls:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Refresh" /></td>
<td>Refreshes the workflow context.</td>
</tr>
<tr>
<td><img src="image" alt="Color Key" /></td>
<td>Displays a key of the colors used in the workflow to denote the state of activities and transitions:</td>
</tr>
</tbody>
</table>
Execution order

View tooltip text in the workflow context graphical view to see the execution order of individual activities.

In **Workflow > Live Workflows > Active Contexts** or **All Contexts**, Open the context you want to examine. Click **Show Workflow**, and point to a finished or executing activity. The tooltip shows error data, execution time, and the order in which the activity executed in the workflow. Use this data to help troubleshoot activities in an error state.
Cancel a workflow

Canceling a workflow stops the workflow from executing and sets the workflow context State to Canceled. To cancel an executing workflow, you can use the `cancelContext(context)` script. You can define an on Cancel script to clean up unresolved workflow activities.

Canceling a workflow attempts to stop the workflow gracefully by injecting a cancel command into the workflow engine.

1. Navigate to Workflow > Active Contexts.
2. Select a workflow context record.
3. Select the Cancel related link.
   A confirmation window appears.
4. Click OK. The Wait for Cancel window appears. The workflow engine attempts to cancel the workflow gracefully.

If the workflow does not respond to the cancel command, the Force Cancel window appears.
5. Click **Force cancel** to interrupt the thread the workflow is actively executing or click **Continue waiting** to continue waiting for the workflow to cancel gracefully.

**Warning:** Whenever possible, allow a workflow to cancel gracefully. Forcing a workflow to cancel can leave related workflows and scripts in an unresolved state. You can use an on-cancel script to clean up unresolved artifacts from a cancelled workflow.

---

**Cancel a workflow with the `cancelContext(context)` script**

To cancel an executing workflow, you can use the `cancelContext(context)` script. This script can be useful in cases where a workflow must be canceled in response to an event or where a user must manually cancel a workflow.

For more information, see the [API reference](#).

**Define an on-cancel script**

Canceling a workflow can leave records or scripts in an unresolved state. For example, canceling a service catalog workflow may leave catalog items in the requesting user's cart. An administrator can specify an On-cancel script that runs when the workflow transitions to the Canceled state. This script can notify users, log information, or resolve the state of any scripts run within a workflow activity. The sys_id of the workflow context is available in this script using the `context_sys_id` variable.

To define this script:

1. Navigate to **Workflow > Workflow Versions**.
2. Select a workflow version that you have checked out. Workflow versions that are not checked out are not editable.
3. Edit the **On-cancel script** field.
   - You may need to [configure the form](#) to add this field.
4. Click **Update**.

This example script adds a comment to a Requested Item (sc_req_item) record indicating the workflow for that request has been canceled.

```javascript
var grContext = new GlideRecord("wf_context");
grContext.get(context_sys_id);
var grReq = new GlideRecord("sc_req_item");
```
Scheduling a workflow

In addition to being run based on conditions, workflows can also be scheduled to perform at a particular time, similar to a scheduled job.

Scheduled workflows do not have a defined current record and do not run on specific records within a table. Due to this behavior, certain activities that depend on a current record, such as Create Task or Catalog Task are unavailable on scheduled workflows. If your workflow requires one of these activities, consider using a scheduled job that inserts a record to start the workflow instead of using a scheduled workflow.

To schedule a workflow, navigate to Workflow > Scheduled Workflows and click New. Populate the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for the scheduled workflow.</td>
</tr>
<tr>
<td>Workflow</td>
<td>Select an existing published workflow to be triggered at the specified date, time, or interval.</td>
</tr>
<tr>
<td>Active</td>
<td>If selected, the scheduled workflow will be triggered at the appropriate time.</td>
</tr>
<tr>
<td>Application</td>
<td>Specifies the type of application, such as Global.</td>
</tr>
</tbody>
</table>
| Run        | A choice list to determine when the workflow should be triggered. Options are:  

  - **Daily**: At a particular hour every day.  
  - **Weekly**: On a particular day of the week.  
  - **Monthly**: On a particular day of the month  
  - **Periodically**: After every set duration.  
  - **Once**: At one specific date and time. |
| Time       | For daily/weekly/monthly scheduled workflows, the time of day to run the workflow. |
| Day        | For weekly scheduled workflow, the day of the week to run the workflow. For monthly scheduled workflows, the day of the month to run the workflow. |
| Repeat Interval | For periodical workflows, the interval between workflows, beginning from the Starting date and time. |
| Starting   | For periodical workflows, the first date and time to run the workflow. For scheduled workflows run once, the date and time to run the workflow. |
Workflow movement with update sets

The system tracks workflows in update sets differently than other records because workflow information is stored across multiple tables.

Changes made to a workflow version are not added to the update set until the workflow is published, at which point the entire workflow is added into the update set. Update sets store workflows as a single Workflow (wf_workflow) record and only retain the latest version with the update type of Workflow.

For information about update sets, see System update sets.

Workflow update set migration use case - simple

Create a new workflow with no dependencies and then migrate the workflow in an update set.

1. User A selects Update Set A.
2. User A creates a new workflow called Workflow A.
3. User A publishes Workflow A.
   A customer update set record is added to Update Set A containing an XML payload, including the published Workflow A and all activity dependencies. The XML payload also contains the workflow input variables associated with the workflow.
4. User A completes Update Set A and migrates it to the production instance.
5. Update Set A commits successfully.
6. Workflow A works as expected.

Workflow update set migration use case - subflow dependency (success)

Successfully edit and migrate an existing workflow and its dependent subflow.

1. User A selects Update Set B.
2. User A checks out Workflow A.
3. User A adds a subflow called Workflow B to Workflow A.
   Assume that Workflow B was previously published and migrated to the production instance.
4. User A publishes Workflow A.
   A customer update set record is added to Update Set B containing an XML payload, including the published Workflow A and all activity dependencies. The XML payload also contains the workflow input variables associated with the workflow.
5. User A completes Update Set B and migrates it to the production instance.
6. Update Set B commits successfully.
7. Workflow A works as expected with Workflow B as a subflow.

Workflow update set migration use case - subflow dependency (failure)

Edit and migrate an existing workflow from a test instance to a production instance that fails to run on the production instance because of a missing dependent subflow.

1. User A selects Update Set C.
2. User A checks out Workflow A.
3. User A adds a subflow called Workflow B to Workflow A.
   Assume that Workflow B was previously published, but has not been migrated to the production instance.
4. User A publishes Workflow A.
   A customer update set record is added to Update Set C containing an XML payload, including the published Workflow A and all activity dependencies. The XML payload also contains the workflow input variables associated with the workflow.
   Notably absent from Update Set C is the subflow called Workflow B. Workflow B was published before User A selected Update Set C.
5. User A completes Update Set C and migrates it to the production instance.
6. Update Set C commits with warnings.
7. Workflow A is invoked on the production instance with the following results:
   Workflow A fails the runtime validation check and is prevented from running on the production system. The system adds to the workflow context a workflow log entry detailing the cause of the failure, notably the absence of a dependent workflow.
   To learn more about the validation checks on workflow dependencies and update sets see ValidateUpdateSetDependencies.

Workflow update set migration use case - subflow dependency (risk)

Multiple users migrate a workflow from a test instance to a production instance without proper coordination. This use case can succeed, but only when each user understands the dependencies and properly migrates the dependent parts of the workflow to the new instance.

This example does not represent an update set failure, although update sets are most often blamed in this use case. Validation increases the visibility of workflow dependencies across multiple update sets and provides designers with better information. In most cases, the warnings do not prevent an action, but only identify risk. The designer is responsible for taking action on advice given in the validation checks.

1. User A selects Update Set C.
2. User A checks out Workflow A.
3. User A adds a subflow called Workflow B that returns a User ID.

   Note: Assume that Workflow B was previously published and migrated to the production instance.
4. User A uses the return value of Workflow B to generate approvals.
5. User B selects Update Set D.
6. User B checks out Workflow B (the subflow in Workflow A).
7. User B modifies the return value of the workflow by changing it from a User ID to a String Message.
8. User A publishes Workflow A.

   Note: A dialog box displays warnings associated with Workflow A and encourages User A to validate the workflow before publishing.
9. User A cancels publishing and validates Workflow A.
10. User A is warned that Workflow B was modified by a user in a different update set.
11. User A ignores this warning and publishes Workflow A.

**Note:** A customer update set record is added to Update Set C containing an XML payload, including the published Workflow A and all activity dependencies. The XML payload also contains the workflow input variables associated with the workflow.

12. User A completes Update Set C and migrates it to the production instance.

13. Workflow A is invoked on the production instance and runs successfully using the older version of Workflow B already on the system.

14. User B publishes Workflow B.

**Note:** User B is not warned of the Update Set C dependency, because the update set is no longer In progress. However, User B is informed via a dialog box that there are warnings associated with the workflow version and is instructed to validate Workflow B. If User B cancels publication and validates the workflow, User B is warned that there are workflows that use Workflow B as a subflow. Knowing the return value was changed, User B should test those workflows as well. See [ValidateUpdateSetDependencies](#) to understand the parameters of update set warnings.

15. User B finally publishes Workflow B.

**Note:** A customer update set record is added to Update Set D containing an XML payload, including the published Workflow B and all activity dependencies.

16. User B completes Update Set D and migrates it to the production instance.

17. Update Set D commits without warnings.

18. Workflow A is invoked on the production instance and fails to run successfully, because the return value of Workflow B no longer generates a User ID.

### Input variable movement

You can add input variables to existing workflows and add them to update sets.

When you submit the new variables, an entry is made into the current update set that reflects the addition of a variable to the Variables (var_dictionary) table. Unlike the workflow version that only writes to the update set when the workflow is published, the variables write individual update entries into the currently selected update set immediately upon submission.

### Input variable movement use case - two input variables

An existing workflow already contains two input variables.

1. User A checks out the workflow.
2. User A adds two input variables.

   ServiceNow adds to the current update set one customer update record for each new variable.

   The current workflow now has 4 input variables: the two that were present prior to check out and the two new ones.
3. User A publishes the workflow.

   There are now three related customer update records: two for new variables, and one for the published workflow. The XML payload of the new workflow version now includes all input variable database entries. So while the two original input variables do not have individual
customer update records, all four variables are migrated to the local instance with the payload of the newly published workflow version.

4. Verify variables included in a specific workflow.
5. User A completes the update set.
6. Adding Input Variables - Success

User A migrates and commits the update set to a local instance where the original workflow version had previously been committed.

- The two existing input variables are already present because of the earlier version.
- The system adds the two new input variables when the user commits the update set.
- The system preserves the two legacy input variables on the instance receiving the update set. The update set does not overwrite these variables.
- The new published workflow version uses all four variables.
- The user tests the new workflow version and it runs as expected.

Verify variables included in a specific workflow
Follow the steps in this page to verify the variables that are included in a specific workflow.

1. Navigate to System Update Sets > Local Update Sets.
2. Select the active update set.
3. Select the customer update entry for the workflow.
4. View the XML Payload.
5. Search for the name of one of the columns or search for var_dictionary.

There is one var_dictionary entry for each input variable.

Input variable removal
Deleting workflow input variables, like insert and update actions, creates a customer update record in a user's current update set.

These deletions migrate to a new instance with the update set, regardless of whether the workflow that owns the input variables is published in the same update set. Plan carefully and use caution when editing a workflow and selecting update sets.

Input variable removal risk
An existing workflow already contains two input variables.

1. The workflow was migrated to a production instance with the two variables.
2. On a development instance, User A selects Update Set A and checks out the workflow.
3. User A removes one input variable and all references to it in the workflow.

   The system enters into Update Set A one customer update record reflecting the deletion of the input variable. No record is added for the new workflow version which no longer depends on the input. This does not happen until the workflow is published.
4. User A continues working on other features in Update Set A that need to be moved to production.
5. User A completes Update Set A and migrates it to the production instance without publishing the workflow.

   The update set entry that deletes the workflow input variable now applies to the production instance. The prior version of the workflow is running on this instance and still references the missing variable.
Input variable removal solution
When editing workflows, particularly when deleting input variables, be sure to use a single update set for all variable editing and workflow publishing.

If necessary, merge the update set into a more general set targeted for deployment after the workflow is published. For information about update sets, see System update sets.

**Note:** If a workflow version is already running on a production system and input variables are deleted from a newer version, those deletions could affect transactions already running against the earlier version. Use extreme caution when deleting workflow input variables and plan the migration carefully.

Input variable removal prevention
Prior to publishing a workflow version, the system validates the workflow model to assist the designer in planning for deployment.

This validation warns of critical errors that can prevent a workflow from running successfully, but also warns of dependencies and conflicts in update sets. See ValidateUpdateSetDependencies for more details.

Avoiding duplicate workflows
Update sets manage the published state of all versions of a workflow prior to committing the workflow version on a local instance.

The last version of a workflow committed as an Insert or Update using an update set becomes the currently published version, regardless of the publishing sequence for the workflow versions.

Commit a workflow in an update set
Follow the steps in this page to commit a workflow in an update set.

1. Workflow A - Version 1 is created and published in Update Set A.
2. Update Set A is completed and migrated to a local instance.
3. When the update set is committed, the system sets all prior versions of Workflow A to published = false.
   In the first migration, there are no prior versions.
4. Workflow A - Version 1 becomes the only published version of the workflow.

Update set migration example
It is not possible to have multiple published versions as a result of update set commits. However, this does not eliminate risk, and care should be taken when migrating update sets.

Consider this example:

1. Workflow A - Version 1 is migrated and committed to the production instance.
2. Update Set B is created.
3. Update Set C is created.
4. Workflow A - Version 2 is published in Update Set B.
   A customer update record is added to Update Set B with the Version 2 payload.
   A customer update record is added to Update Set B with the Version 1 workflow left unpublished.
5. Update Set B is completed.
6. Workflow A - Version 3 is published in Update Set C.
   A customer update record is added to Update Set C with the Version 3 payload.
A customer update record is added to Update Set C with the Version 2 workflow left unpublished.

7. Update Set C is completed.

8. Update Set C is migrated and committed to the production instance.
   Workflow A - Version 1 is set to unpublished.
   Workflow A - Version 2 update is skipped since Update Set B, which contains Version 2, was never migrated.
   Workflow A - Version 3 is committed and becomes the only published version of the workflow.

**Update set migration risk**

Update Set B is migrated and committed to the production instance.

1. Workflow A - Version 3 is set to unpublished.
3. Workflow A - Version 2 is committed and becomes the only published version of the workflow.
   The workflow has gone back a version, perhaps unintentionally. The regressed version becomes the currently published version.

**Workflow timelines**

The system provides a timeline view of history activities associated with a workflow context.

Timelines display a linear calendar of activities, such as tasks and approvals, defined by their start and end dates. Each activity on the timeline is represented by a span, which is displayed as a horizontal, colored bar. Each span has a label and a tooltip that contains additional information about the activity. The left pane displays all the activities in the context (or contexts) in an expandable hierarchy. You can change the timeline’s perspective for a more granular view of the data.

---

**Note:** Workflow timelines reflect context history only and are not real-time gauges of workflow activity.

---

**Use a timeline**

By default, the timeline displays all activities and transitions requested when first opened.

Collapse any part of the hierarchy in the activity pane and the timeline adjusts automatically. Date/time and duration controls enable you to scale the timeline to view all the elements at once. To display a timeline, click a UI action within a Workflow Context record.

1. Navigate to **Workflow > Live Workflows > Active Contexts.**
2. Select a context.
3. In **Related Links**, click **Show Timeline** to display the timeline for the entire context.
   The timeline opens with all activities expanded and the view set to **Max**, which displays the entire timeline at the width of the pane. The title of the timeline is in the form Workflow context: <context name>, Requested Item: <requested item number>. 
4. 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.

5. 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.

6. Use the pink slider at the bottom of the timeline to change the perspective.
1. Move the slider from right to left to view all the spans on a long timeline.

2. Adjust the end points of the slider to make arbitrary changes to the magnification.
   
   A narrow slider zooms in on the spans and provides a more detailed view of complex timelines. A wide slider pulls the view out and makes more of the timeline visible on the screen.

7. To focus the timeline view on selected activities, expand or collapse the activity tree.
   
   Spans not visible in the activity tree are not shown in the timeline pane.

8. Hover over an activity span to display a tooltip with information about the activity.
   
   This action highlights the activity in the activity pane.
9. Hover over the transition between two activities to highlight the activity and the predecessor activity in the activity pane.

10. Double-click a span to display a history record for that activity.
    History records shows information such as the State and the starting and ending times.
Timeline for a selected activity

You can display a partial workflow timeline.

1. Navigate to Workflow > Live Workflows > Active Contexts.
2. Open a Workflow Context record.
3. On the Workflow Activity History related list, select one or more individual activities.
4. Click Show Timeline from the action menu.
   The resulting view is a snapshot of the timeline, showing only the selected activities and their transitions, if any.
5. Collapse the tree to confine the view even further.
6. To view a timeline displaying activities from different contexts:
   You might use this feature to display a subflow's context with the parent workflow context.
   1. Navigate to Workflow > Live Workflows > History.
   2. Select individual history items from the list.
   3. Select the Show Timeline option from the actions menu.

   History items are arranged in a hierarchy in the activities pane under their contexts. The timeline title is Multiple Contexts. The timeline draws only the activities and relationships of the history items selected.

View subflows in a workflow timeline

In a workflow timeline, subflow spans appear as a different color than the activities of the main workflow.
Workflow context: iPhone4, Requested Item: RITM0010025

Workflow timeline subflow

Workflow error handling

The personalized JavaScript that users create in workflow activity variables is vulnerable to run-time syntax errors. Available error information is available in a tooltip when you point to a workflow activity in an error state.

In the base system, workflow activities do not provide condition routing on the error state. As a result, the workflow progresses based on the state of the current record. For example, a workflow contains an Approval - User activity that uses an advanced script to add additional approvers. A syntax error in the script results in no approvers being added. Because a state of no approvers is a valid return, even without the syntax error, the approval activity is skipped and the workflow progresses along a positive path. However, this might not be a valid response for the workflow designer who does not want the workflow to progress along the positive path without approvers.

Workflow error handling detects and logs syntax errors and provides a state that the workflow designer can use to add error conditions to the workflow. Use error handling to locate syntax errors in advanced script fields for these workflow activities:

- Approval - User
- Approval - Group
- Catalog Task
- Create Task
- If
- Run Script
- Notification
Available error information

This table shows which activities support error exits.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Workflow log</th>
<th>Red error indicator</th>
<th>Activity state</th>
<th>Activity result</th>
<th>Fault description</th>
<th>Reroute on error</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approval - User</td>
<td>Yes</td>
<td>Yes</td>
<td>Error</td>
<td>Skipped</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Approval - Group</td>
<td>Yes</td>
<td>Yes</td>
<td>Error</td>
<td>Skipped</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Catalog Task</td>
<td>Yes</td>
<td>No</td>
<td>Finished</td>
<td>none</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Create Task</td>
<td>Yes</td>
<td>Yes</td>
<td>Finished</td>
<td>none</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>If</td>
<td>Yes</td>
<td>Yes</td>
<td>Error</td>
<td>none</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Run Script</td>
<td>Yes</td>
<td>Yes</td>
<td>Error</td>
<td>error</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Notification</td>
<td>Yes</td>
<td>Yes</td>
<td>Error</td>
<td>error</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Workflow error tracking features

Error handling provides visual cues within the workflow, such as error descriptions for activities in pop-ups, and detailed log records.

Banners

Look for an activity with a red banner, indicating that a syntax error has occurred in a script field. All activities that provide error handling, with the exception of Catalog Task and Create Task, display a red banner for this error.

![Switch](image)

Check assignment group

Always

Tooltips

Point to the activity displaying a red banner to view information about the error. A tooltip shows the State and Result of the activity and provides a brief Fault Description (except for task activities). Note that this approval continued as skipped despite the error given in the fault description. See Workflow error handling for the information available to each activity.
Execution order

Tooltip text in the Workflow Context graphical view displays the execution order of individual activities, which assists in troubleshooting.

To view the order in which a workflow activity was executed:

1. Navigate to **Workflow > Live Workflows > Active Contexts** or **All Contexts**.
2. Open the context you want to examine.
3. Click **Show Workflow**.
4. Hover the cursor over a finished or executing activity.

A tooltip appears showing error data, execution time, and the order in which that activity executed in the workflow. You can use this data to help troubleshoot activities in an error state.
Workflow log

View the log in the Workflow Context form for more information about the syntax error in the activity. Since task activities do not display a red banner when a syntax error has occurred, you must view the log if you suspect the workflow has not run properly. Examine the error description in the log, and then inspect the script in the activity named in the log.

To view the activity by name, navigate to Workflow > Administration > Properties and enable the Log workflow debug messages property.
In this example, an SSH activity named File Read specifies an invalid MID Server.

Error handling log

If the credentials used by an activity in the workflow fail, and the activity cannot authenticate on the target, a message describing the failure appears in the Workflow Log related list. The message displays the target IP address and the credential details.
Credential debugging in the workflow log

Create an error condition exit

An administrator can reroute the workflow when a script error occurs by creating an error condition exit for specific activities within the workflow. This allows the workflow to process script errors in a predictable way and not create undesirable results.

1. Open and check out a workflow.
2. Right-click in the top portion of the activity for which you want to create an error exit.
3. Select Add condition from the context menu.
4. Add a condition exit with the following values:
   - Name: Error
   - Condition: activity.state=='faulted'
5. Click Submit.
The **Error** exit appears on the activity.

6. Connect the **Error** exit to another activity for handling the error state, such as **Notification** or **Log Message**.

---

**Reconfigure an approval condition**

Approval activities react differently to script errors than the other activities.

Approval activity script errors can prevent an approval from being processed successfully. This, in turn, can cause the approval to complete as **Skipped**, which can appear to be an **Approved** state. To prevent this from happening, reconfigure the **Approved** exit as follows:

1. Open an approval workflow and make sure it is checked out.
2. On an approval activity, double-click the **Approved** exit.
3. Add the following script to the **Condition** field:
   ```java
   && activity.state != 'faulted'
   ```
   This prevents the activity from continuing down the normal path in an error state and ensures that **Skipped** or **Approved** is the desired state.
4. Click **Update**.

---

**Workflow run time metrics**

You can enable the collection of workflow run time metrics to determine whether workflows are performing as expected or consuming additional resources.

Outlying run times for a workflow are identified by comparing actual run times to an outlier range calculated with the outlier threshold and estimated run time defined in the workflow properties.

You can monitor the results of these metrics on the Workflow Operations Dashboard and custom homepages with workflow gauges.

**Enable workflow run time metrics**

Provide an estimated run time that can be compared to actual workflow run times.
For baseline workflows, you must also manually enable the collection of run time metrics. The system automatically enables the collection of run time metrics for new workflows.

1. Navigate to **Workflow > Workflow Editor**.
2. Open and check out the workflow.
3. In the title bar, click the menu icon and select **Properties**.
4. In the Workflow Properties dialog box, click the **Estimated Runtime** tab.
5. To enable the collection of run time metrics, check that the **Requires ERT** option is selected.
6. Open a configuration from the **Estimated Run Time** column.
7. In **Estimated Run Time**, enter an initial estimate for the workflow’s run time.
   - The system compares this initial estimate to actual run time results to create outlier reports. The system can automatically update this field in certain circumstances. Workflow designers can also manually update this field.
8. In the **Outlier Percentage Threshold for ERT** field, enter the percentage deviation from the estimated run time that identifies an outlier workflow run time.
   - The system uses a default value of **20**.
9. Click **Update**.

### Outlying workflow run times

Workflow run times are identified as outliers when they are longer or shorter than the outlier range that is computed for the workflow.

The outlier range is automatically computed with the **Estimated Run Time** and **Outlier Percentage Threshold for ERT** values in the workflow properties. These values are used in the following formulas.

#### Formulas for computing workflow outlier ranges

<table>
<thead>
<tr>
<th>Value computed</th>
<th>Computation used</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outlier Value</td>
<td>Estimated Run Time * (Outlier Percentage Threshold for ERT / 100)</td>
<td>10 seconds * (20 / 100) = 10 seconds * 0.2 = 2 seconds</td>
</tr>
<tr>
<td>Outlier Range</td>
<td>(Estimated Run Time - Outlier Value) to (Estimated Run Time + Outlier Value)</td>
<td>(10 seconds - 2 seconds) to (10 seconds + 2 seconds) = 8 to 12 seconds</td>
</tr>
</tbody>
</table>

When a workflow runs within the outlier range, its estimated run time is automatically updated.

If a workflow has an outlying run time, it appears in any outlier workflow gauges on the Workflow Operations Dashboard and custom home pages.

### Workflow estimated run time updates

When a workflow runs within the outlier range, its estimated run time is automatically updated.

The estimated run time is updated with the **cumulative moving average** of the latest run time value in relation to previous run times. The computed value is rounded to the nearest second and stored as a **GlideDateTime**.

For example:

<table>
<thead>
<tr>
<th>Data point</th>
<th>Latest value</th>
<th>Cumulative running average (CRA)</th>
<th>CRA after rounding to the nearest second</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10 seconds</td>
<td>10 seconds</td>
<td>10 seconds</td>
</tr>
<tr>
<td>2</td>
<td>12 seconds</td>
<td>11 seconds</td>
<td>11 seconds</td>
</tr>
</tbody>
</table>
You can also manually update the estimated run time in the workflow properties.

**Troubleshoot workflows**

Troubleshooting tools for workflows enable administrators to isolate execution paths, compare contexts, and track incomplete activities.

The workflow timeline provides a visual representation of the workflow, including transitions and the elapsed time for each activity. A troubleshooting tool for highlighting execution paths helps users perform forensics on a workflow. The highlighting feature can group multiple execution paths in various colors and can isolate rollback processing. Use the workflow highlighter to isolate incomplete tasks and approvals. You can also enable a workflow performance timing feature to troubleshoot slow workflows.

**Execution path troubleshooting in timelines**

Use the controls in a workflow timeline to isolate specific execution paths or compare multiple execution paths over time.

Timelines show how the activities in the workflow progressed in relation to one another over time. Isolate execution paths and follow transition lines between subflows and the main flow. Processing times provide a view of the workflow that you cannot get from the workflow diagram. Tooltips give precise information about each activity, such as duration.
Workflow timeline troubleshooting

Execution history table
Highlight execution paths and rollbacks to locate activities that may have been left in an unresolved state.

Rollbacks, cancels, and deletions during the execution of a workflow can prevent some activities from fully completing. Use highlighting in the execution history table to determine which activities in the workflow were left in an unresolved state.

1. Run the workflow.
2. Navigate to Workflow > All Contexts.
3. Select a context to troubleshoot.
4. In the Workflow Context form, select the Workflow Activity History related list.
5. Right-click an activity and select Workflow Debug > Toggle Execution Path Highlighting from the context menu.

All activities in that execution path are highlighted in a color selected by the platform. The debug path shows all activities that completed successfully during the workflow.
6. Right-click a rollback activity and select **Workflow Debug > Toggle Rollback Highlighting** from the context menu.

The platform highlights the rollback path (restarted activities) in a different color. Each color represents a group of activities that were part of the same rollback execution. The highlighting includes the activity that initiated the rollback. If you right-click an activity that was not part of a rollback, no rows are highlighted.

**Note:** The rollback activity itself appears in both execution path and rollback highlighting.
7. To remove highlighting, right-click in the list and select an option to clear execution path or rollback highlighting.

You can clear individual rollback paths or all rollback highlighting.

Use the Workflow Operations Dashboard

On the Workflow Operations Dashboard, view and add widgets to help you monitor workflows. Review the performance of workflows and determine which workflows must be improved.

Role required: workflow_admin

The different levels of access are:

- **View**: View the dashboard and refresh report widgets.
- **Customize**: Refresh, add, delete, and rearrange widgets.

On the Workflow Operations Dashboard, you can click widget elements to view the records they represent. You can also add new report widgets that are not displayed by default.

1. To view the Workflow Operations Dashboard, navigate to **Workflow > Operations > Workflow Operations Dashboard**.

The default reports on the dashboard include:

- Workflow contexts providing run time metrics
- Active workflows started during a specified time period
- Workflows run between yesterday and today
- Workflows by state for the current month
• Aged workflow contexts for the past month

2.

To find and add more widgets, click the Add Content icon ( ) in the upper left corner of the dashboard.

If a workflow consistently appears as an outlier and there is no error causing the run time values, you can use its historical run time values to calculate a new estimated run time value. Then update the estimated run time in the workflow properties.

**Workflow gauges**

Multiple gauges are available to help you review the performance of workflows. You can add these gauges to the Workflow Operations Dashboard or custom homepages.

**Workflow gauges**

<table>
<thead>
<tr>
<th>Content</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ERT Dashboard Controls &gt;</strong></td>
<td></td>
</tr>
<tr>
<td>Outlier Finished Workflows for ERT (Percentage Outlier)</td>
<td>Identifies workflows that finished, but did not finish within estimated runtime (ERT) values. Enter an outlier percentage to see workflows that ran outside the specified runtime range.</td>
</tr>
<tr>
<td>Outlier Long Running Workflows for ERT (Percentage Outlier)</td>
<td>Displays workflows running longer than the configured runtime threshold.</td>
</tr>
<tr>
<td><strong>Workflow Dashboard &gt;</strong></td>
<td></td>
</tr>
<tr>
<td>Workflows Without Current Record</td>
<td>Displays workflow contexts that do not have an associated current record.</td>
</tr>
<tr>
<td><strong>Gauges &gt; Workflow Context</strong></td>
<td></td>
</tr>
<tr>
<td>Number of Active Workflows Started Hourly Over Time (Yesterday)</td>
<td>Displays the total number of running workflows per hour over a given time period. By default, it displays the number of workflows that ran per hour over the previous day (yesterday).</td>
</tr>
<tr>
<td>Outlier Finished Workflows Not Cumulated to ERT</td>
<td>Displays workflow contexts that are finished outside the estimated runtime outlier value and not cumulated to estimated run time value.</td>
</tr>
<tr>
<td>Running Workflow Contexts</td>
<td>Displays the total number of running workflows.</td>
</tr>
<tr>
<td>Successfully Finished Workflows Cumulated to ERT</td>
<td>Displays the total number of successfully completed workflows whose running duration is cumulated to the estimated run time value.</td>
</tr>
<tr>
<td>Workflows by State (This Month)</td>
<td>Displays the total number of workflows run in a month grouped by the current state.</td>
</tr>
<tr>
<td>Aged Workflow Contexts (Running Since Last Month)</td>
<td>Displays the total number of workflow contexts running for a given period of time by workflow name. By default, it displays the total number of workflow contexts running over the last month.</td>
</tr>
<tr>
<td>Workflows Run Between Yesterday and Today (by Table)</td>
<td>Displays workflows that have run in the last day grouped by table name.</td>
</tr>
</tbody>
</table>
Workflow performance timing

The workflow engine can generate detailed performance timing data that is useful for troubleshooting slow workflows.

An administrator must enable this functionality.

When workflow performance timing is enabled, the workflow engine tracks key performance data, including various execution speed metrics. The Workflow Timing (wf_workflow_timing) table stores the data, with a record for each workflow context. The workflow timing record is updated when the workflow engine completes the workflow, waits for an activity to complete, or otherwise exits the workflow execution.

Workflow estimated run time properties

Administrators can enable the collection of workflow run time metrics by setting Estimated Run Time (ERT) properties.

Administrators can use ERT metrics to determine if workflows are running longer or shorter than expected and to identify errors in workflow processing. The system displays run time metrics on the Workflow Operations Dashboard.

Enable workflow performance timing

Workflow performance timing is disabled by default. You can create a system property to enable it.

Role required: admin

Add a system property with the following specifications.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>glide.workflow.show_timing</td>
</tr>
<tr>
<td>Type</td>
<td>true</td>
</tr>
<tr>
<td>Value</td>
<td>true</td>
</tr>
</tbody>
</table>

Workflow activities

Workflow activity properties reference

Each activity performs a different task, such as running a script, sending notifications, or requesting approvals. Activities can succeed or fail, which can result in actions performed by other activities.

For information about configuring different types of activities, click an activity name in the list below or see Workflow activities reference.

Core activities provided in the base system

- Approval and rollback workflow activities
- Condition Workflow activities
- Notification workflow activity
- Notify workflow activities
- Subflow activities
Activities provided with Orchestration

The following activities are included with Orchestration.

- Active Directory activity pack
- Orchestration activities
- PowerShell activities
- Puppet activities

Templates provided for creating custom activities

If Orchestration is active on your system, users with the proper roles can create custom activities using the ServiceNow Orchestration activity designer. For information about the templates Orchestration provides for creating custom activities that you can upload to the ServiceNow Store, see Orchestration custom activity templates.

Workflow activities reference

Workflow activity reference, organized by category.

Each activity performs a different task, such as running a script, sending notifications, or requesting approvals.

Approval and rollback activities

Approval and rollback activities generate and manage approvals. Not all workflows can include approval activities. For more information, read Approval and rollback workflow activities.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approval Action workflow activity</td>
<td>The Approval Action activity performs an approval action on the current task.</td>
</tr>
<tr>
<td>Approval Coordinator workflow activity</td>
<td>The Approval Coordinator activity creates an approval whose outcome depends on the outcome of one or more child activities, including one or more Approval - User, Approval - Group, and/or Manual Approval activities,</td>
</tr>
<tr>
<td>Approval - Group workflow activity</td>
<td>The Approval - Group activity creates approval records for each member of a specified group.</td>
</tr>
<tr>
<td>Approval - User workflow activity</td>
<td>The Approval - User activity creates one or more individual user approvals.</td>
</tr>
<tr>
<td>Generate workflow activity</td>
<td>The Generate activity immediately creates task or approval records from any task or approval activities placed after the Generate activity in the workflow path.</td>
</tr>
<tr>
<td>Manual Approvals workflow activity</td>
<td>The Manual Approvals activity watches and manages any approvals that users add manually outside of the workflow process. This activity only selects approvals that are in the Not requested state.</td>
</tr>
<tr>
<td>Activity</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Rollback To workflow activity</td>
<td>The Rollback To activity transitions directly to the activity specified by the outgoing transition line arrow.</td>
</tr>
</tbody>
</table>

**Condition activities**

Condition activities provide conditional branching and logical operation functionality for workflows.

**Condition activities**

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If workflow activity</td>
<td>The If activity checks a condition or script to determine if a Yes or No transition should be taken.</td>
</tr>
<tr>
<td>Switch workflow activity</td>
<td>The Switch activity checks if the value of a passed field or variable is equivalent to one of several case values.</td>
</tr>
<tr>
<td>Wait for condition workflow activity</td>
<td>The Wait for condition activity causes the workflow to wait at this activity until the current record matches the specified condition.</td>
</tr>
<tr>
<td>Wait for WF Event workflow activity</td>
<td>The Wait for WF Event activity causes the workflow to wait at this activity until the specified event is fired.</td>
</tr>
</tbody>
</table>

**Notify activities**

Notify activities manage calls and SMS messages in Notify.

**Notify activities**

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forward call workflow activity</td>
<td>The Forward Call activity forwards a Notify call to an E.164-compliant phone number.</td>
</tr>
<tr>
<td>Input workflow activity</td>
<td>The Input activity creates a phone menu by presenting a list of options on a Notify call.</td>
</tr>
<tr>
<td>Hangup workflow activity</td>
<td>The Hangup activity disconnects an active Notify phone call.</td>
</tr>
<tr>
<td>Play workflow activity</td>
<td>The Play activity plays a sound file on a Notify call.</td>
</tr>
<tr>
<td>Record workflow activity</td>
<td>The Record workflow activity records audio from a user on a Notify call.</td>
</tr>
<tr>
<td>Reject workflow</td>
<td>The Reject workflow activity rejects an incoming Notify call.</td>
</tr>
<tr>
<td>Say workflow activity</td>
<td>The say workflow activity allows you to play a message, using text to speech, on a Notify call.</td>
</tr>
<tr>
<td>Forward to notify client workflow activity</td>
<td>The forward to notify client workflow activity connects a phone call to a Notify WebRTC client.</td>
</tr>
<tr>
<td>Call workflow activity</td>
<td>The Call activity makes outbound phone calls using a Notify workflow.</td>
</tr>
<tr>
<td>Join conference call workflow activity</td>
<td>The Join Conference Call connects an incoming or outgoing call to a Notify conference call.</td>
</tr>
</tbody>
</table>
### Send SMS workflow activity
The **Send SMS workflow activity** to send short text messages using Notify to users’ phones.

### Queue workflow activity
The **Queue** activity places an active Notify call in a queue.

### Notification activities
Notification workflow activities notify users of events that occur during the workflow.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Create Event workflow activity</strong></td>
<td>The <strong>Create Event</strong> activity adds an event to the event queue, but does not immediately fire the event.</td>
</tr>
<tr>
<td><strong>Notification workflow activity</strong></td>
<td>The <strong>Notification</strong> activity sends an email or SMS message to specified users or groups.</td>
</tr>
</tbody>
</table>

### Timer activities
Timer activities pause workflows for set periods of time.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SLA Percentage Timer workflow activity</strong></td>
<td>The <strong>SLA Percentage Timer</strong> activity pauses the workflow for a duration equal to a percentage of an SLA.</td>
</tr>
<tr>
<td><strong>Timer workflow activity</strong></td>
<td>The <strong>Timer</strong> activity pauses the workflow for a specified period of time.</td>
</tr>
</tbody>
</table>

### Task activities
Task activities create and modify workflow tasks.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Add Worknote workflow activity</strong></td>
<td>The <strong>Add Worknote</strong> activity adds text to the Worknotes field of the current incident record.</td>
</tr>
<tr>
<td><strong>Attachment Note workflow activity</strong></td>
<td>The <strong>Attachment Note</strong> activity adds an attachment to the current record.</td>
</tr>
<tr>
<td><strong>Catalog Task workflow activity</strong></td>
<td>The <strong>Catalog Task</strong> activity creates a service catalog task record.</td>
</tr>
<tr>
<td><strong>Create Task workflow activity</strong></td>
<td>The <strong>Create Task</strong> activity generates a record on any of the tables that extend Task (task).</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.
Utility activities

Utility activities provide controls over the path of the workflow, and other useful tools.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch workflow activity</td>
<td>The <strong>Branch</strong> activity splits the workflow into multiple transition paths from a single activity.</td>
</tr>
<tr>
<td>Join workflow activity</td>
<td>The <strong>Join</strong> activity unites multiple execution paths into one transition.</td>
</tr>
<tr>
<td>Lock workflow activity</td>
<td>The <strong>Lock</strong> activity prevents other instances of this workflow from continuing past this activity until the lock is released.</td>
</tr>
<tr>
<td>Log Message workflow activity</td>
<td>The <strong>Log Message</strong> activity writes a message to the workflow log.</td>
</tr>
<tr>
<td>Log Trace Message workflow activity</td>
<td>The <strong>Log Trace Message</strong> activity writes a trace message to the workflow log.</td>
</tr>
<tr>
<td>REST Message legacy workflow activity</td>
<td>The legacy <strong>REST Message</strong> activity enables an administrator to override the REST endpoint or supply the variables configured in the REST Message module.</td>
</tr>
<tr>
<td>Return Value workflow activity</td>
<td>The <strong>Return Value</strong> activity returns a value to a parent workflow, when run from a subflow.</td>
</tr>
<tr>
<td>Run Script workflow activity</td>
<td>The <strong>Run Script</strong> activity runs the specified script in the scope of the workflow version.</td>
</tr>
<tr>
<td>Set Values workflow activity</td>
<td>The <strong>Set Values</strong> activity sets values on the current record when the workflow quiesces or ends.</td>
</tr>
<tr>
<td>SOAP Message legacy workflow activity</td>
<td>The legacy <strong>SOAP Message</strong> activity uses SOAP messages defined in the System Web Services plugin and can call the messages using a MID Server.</td>
</tr>
<tr>
<td>Turnstile workflow activity</td>
<td>The <strong>Turnstile</strong> activity limits how many times a workflow can pass through the same point.</td>
</tr>
<tr>
<td>Unlock workflow activity</td>
<td>The <strong>Unlock</strong> activity releases a lock that was previously placed by the <strong>Lock</strong> activity.</td>
</tr>
</tbody>
</table>

Subflow activities

Subflow activities run and manage workflows from a parent workflow.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parallel Flow Launcher workflow activity</td>
<td>The <strong>Parallel Flow Launcher</strong> activity launches multiple subflows in parallel.</td>
</tr>
</tbody>
</table>

Activities provided with Orchestration

The following activities are included with Orchestration.

- Active Directory activity pack
Orchestration activities
- PowerShell activities
- Puppet activities

Templates provided for creating custom activities

If Orchestration is active on your system, users with the proper roles can create custom activities using the Orchestration activity designer. For information about the templates Orchestration provides for creating custom activities that you can upload to the ServiceNow Store, see Orchestration custom activity templates.

Approval and rollback workflow activities

Approval and rollback activities generate and manage approvals. Approval and rollback activities are not available in some workflows.

- With two exceptions, approval and rollback activities are only available when the workflow runs on a table that extends Task. The exceptions are the Approval - User and Approval Action activities, which are available globally.
- Approval and rollback activities are available only if approval engines are turned off for the table on which the workflow runs. If approval engines are enabled for the table, approval activities appear greyed out and cannot be selected. To learn more about how workflow and approval engines interact, read Approval workflow activities and approval engines.

Approval Action workflow activity

The Approval Action activity performs an approval action on the current task. Use this activity to mark the current task record as approved or rejected.

Note: When an Approval Action activity is used to mark a task approved, the activity marks all pending approvals as No Longer Required. This activity behaves differently from Set Values or Run Script when used to set the Approval field's value.

Results

The result value of the activity is the final approval disposition selected by the approver. The result value can be Approved or Rejected. A workflow designer can assign a result value using the activity.result variable from within a script field of the activity.

Input variables

Input variables determine the initial behavior of the activity.
Approval Action activity input variables

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Action | The action to perform on the task. Options are:  
• Mark task approved  
• Mark task rejected  
• Mark task requested  
• Disregard pending approvals: the system sets approval records to **no longer required** and marks the activity as **approved**. |

Conditions

The conditions determine which transition runs after this activity.

Approval Action activity conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always</td>
<td>The event or condition that causes the approval to move to the next workflow step.</td>
</tr>
<tr>
<td>Error</td>
<td>The event or condition that generates an error.</td>
</tr>
<tr>
<td>Skipped</td>
<td>The event or condition that allows a skipped approval.</td>
</tr>
</tbody>
</table>

States

The activity state tells the workflow engine what to do with the activity.

Approval Action activity states

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executing</td>
<td>The workflow engine starts the <code>execute</code> function of the activity.</td>
</tr>
<tr>
<td>Waiting</td>
<td>The workflow engine ignores the activity until a specific event to restart the activity is fired.</td>
</tr>
<tr>
<td>Finished</td>
<td>The activity finished running. See the result value for the outcome of the activity.</td>
</tr>
<tr>
<td>Cancelled</td>
<td>This activity, or the workflow that contains this activity, was canceled.</td>
</tr>
<tr>
<td>Error</td>
<td>A JavaScript error occurred. Review the logs for error details.</td>
</tr>
</tbody>
</table>

Approval Coordinator workflow activity

The **Approval Coordinator** activity creates an approval whose outcome depends on the outcome of one or more child activities, including one or more **Approval - User**, **Approval - Group**, and/or **Manual Approval** activities.
Note: This activity is only available when the workflow runs on a table that extends Task.

To create an Approval Coordinator activity, first drag the activity onto the workflow canvas, causing the activity form to display. On the activity form, fill in the appropriate fields, then click Submit.

After you click Submit, the activity appears on the workflow canvas. From there, specify the child activities by clicking the links that appear on the body of the activity.

When the Approval Coordinator activity completes, all pending approvals that were created by any of the Approval Coordinator approval activities are immediately set to No Longer Required. If a single user is called as an approver twice by the same workflow, such as when a single user is both a product approver and an executive approver, any approvals for that user after the first are skipped.

Results

The result value of the Approval Coordinator activity depends on the approval actions taken by the approvers and the approval conditions specified in the Wait for field. Possible result values are:

- Approved
- Rejected
- Deleted
- Cancelled

Input variables

Input variables determine the initial behavior of the activity.

Approval Coordinator activity input variables

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wait for</td>
<td>Indicate what to wait for to indicate that the approval activity is approved or rejected. Options are:</td>
</tr>
<tr>
<td></td>
<td>- Any child activity to be approved: Any child activity (User, Group, or Manual Approval) that completes with a result of approved causes the Approval Coordinator activity to complete with a result of approved.</td>
</tr>
<tr>
<td></td>
<td>- All child activities to be approved: All child activities of the Approval Coordinator activity must complete with a result of approved to cause the Approval Coordinator activity to complete with a result of approved.</td>
</tr>
<tr>
<td></td>
<td>- The first approval or rejection from any child activity: The first child activity that completes with a result of approved or rejected causes the Approval Coordinator activity to complete with the same result.</td>
</tr>
<tr>
<td></td>
<td>- Condition based on script: Call a script to determine how to manage an approval or rejection.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>When a rejection occurs</td>
<td>Specify what the coordinator should do when it sees a rejection from any one of the child activities. Options are:</td>
</tr>
<tr>
<td>Only appears if Wait for is set to All child activities to be approved or Any child activity to be approved.</td>
<td>- <strong>Reject the approval</strong>: Immediately complete the Approval Coordinator activity with a result of rejected.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Wait for other responses before deciding</strong>: Wait until we get other responses from other child activities before making an approval or rejection decision.</td>
</tr>
<tr>
<td></td>
<td>This allows users to change their minds until a decision is made.</td>
</tr>
<tr>
<td></td>
<td>In addition, if Wait for is set to Any child activity to approve then a single child activity completion with a result of approved will cause the Approval Coordinator activity to complete with a result of approved even if other child activities have completed with a result of rejected.</td>
</tr>
<tr>
<td>Approval script</td>
<td>If the Wait for variable is set to Condition based on script this script is called to determine how to handle an approval or rejection. The script needs to set the variable answer to , approved or rejected to indicate the overall approval status for this approval. When called, the following variable is available to the script:</td>
</tr>
</tbody>
</table>
| Only appears if Wait for is set to Condition based on script. | counts.total = total number of child approval activities that are part of this approval  
counts.approved = # of child approval activities that approved so far  
counts.rejected = # of child approval activities that rejected so far  
counts.requested = # of child approval activities that are pending approval |

### Conditions

The conditions determine which transition runs after this activity.

**Approval Coordinator activity conditions**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved</td>
<td>The users from the groups have approved the request based on the Wait for rules.</td>
</tr>
<tr>
<td>Rejected</td>
<td>The users from the groups have rejected the request based on the Wait for rules.</td>
</tr>
</tbody>
</table>
States

The activity state tells the workflow engine what to do with the activity.

Approval Coordinator activity states

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executing</td>
<td>The workflow engine starts the execute function of the activity.</td>
</tr>
<tr>
<td>Waiting</td>
<td>The workflow engine ignores the activity until a specific event to restart the activity is fired.</td>
</tr>
<tr>
<td>Finished</td>
<td>The activity finished running. See the result value for the outcome of the activity.</td>
</tr>
<tr>
<td>Cancelled</td>
<td>This activity, or the workflow that contains this activity, was canceled.</td>
</tr>
<tr>
<td>Error</td>
<td>A JavaScript error occurred. Review the logs for error details.</td>
</tr>
</tbody>
</table>

Approval - Group workflow activity

The Approval - Group activity creates approval records for each member of a specified group.

Note: This activity is only available when the workflow runs on a table that extends Task.

The group approval is approved or rejected based on the user approvals, according to the logic specified in the Wait For field.

Results

The workflow designer can assign a result value using activity.result from within a script field of the activity. By default, the result value is the final approval disposition. This disposition depends on the approval actions take by the approvers and the approval conditions specified in the Wait for or When Anyone Rejects fields. Possible result values are:

- Approved
- Rejected
- Deleted
- Cancelled

Input variables

Input variables determine the initial behavior of the activity.

Approval - Group activity input variables

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approval - Group When</td>
<td>Specify when this activity generates a group approval record.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Condition</td>
<td>Conditions which, if met, cause the group approval to be generated. If the conditions are not met, the approval is skipped.</td>
</tr>
<tr>
<td>Approval - Group Approvers</td>
<td>Specify the groups whose approval will be requested.</td>
</tr>
<tr>
<td>Groups</td>
<td>The groups whose approval will be requested.</td>
</tr>
<tr>
<td></td>
<td>To edit this field, click the lock icon. To select specific groups by name, use the lookup list. To select groups from field values on the current record at runtime, click the tree icon.</td>
</tr>
<tr>
<td></td>
<td>Each member of the group will be assigned an individual approval record.</td>
</tr>
<tr>
<td></td>
<td>If no group is selected, the activity automatically sets the approval to <strong>Approved</strong>.</td>
</tr>
<tr>
<td>Approval - Group Condition</td>
<td>Specify how the activity decides to approve or reject the group approval, based on the responses from individual members of the group.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Wait for</td>
<td>A choice between different approval logics to determine which individual approvals or rejections result in approval or rejection of the activity's approval. Options are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>An approval from each group:</strong> Any user from each group can approve and the first approval from each group causes the activity to complete with a result of <em>approved</em> (see below for how a rejection is handled).</td>
</tr>
<tr>
<td></td>
<td>• <strong>An approval from any group:</strong> Any user from any group can approve and the first approval from any group causes the activity to complete with a result of <em>approved</em>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>An approval from everyone from all groups:</strong> All users from all groups must approve to cause the activity to complete with a result of <em>approved</em> (see below for how a rejection is handled).</td>
</tr>
<tr>
<td></td>
<td>• <strong>First response from each group:</strong> The first approval or rejection from any user in each group is used to indicate the state of the group approval (see below for how a rejection is handled).</td>
</tr>
<tr>
<td></td>
<td>Indicate what happens when any user rejects their approval request. Options are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Reject the approval:</strong> Immediately complete the activity with a result of <em>rejected</em>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>First response from any group:</strong> The first approval or rejection from any user in any group causes the activity to complete with a result of <em>approved</em> or <em>rejected</em>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Condition based on script:</strong> Each time a user approves or rejects, the <em>Approval script</em> is called to determine if the activity should complete.</td>
</tr>
</tbody>
</table>
Approval script

Only appears when Wait for is set to Condition based on script.

If the Wait for variable is set to **Condition based on script** this script is called to determine how to handle an approval or rejection. The script needs to set the variable answer to approved or rejected to indicate the overall status for this approval.

This script is responsible for setting the approval state for each group that is part of this approval activity before returning the overall approval state for all of the groups.

When called, the following variables are available to the script for all the groups that are part of this approval activity:

```plaintext
# Script variables

counts.total = total number of groups that are part of this approval

counts.approved = # of groups that approved so far

counts.rejected = # of groups that rejected so far

counts.requested = # of groups that are pending approval

counts.not_required = # of groups that approval is not required

And for each group:

groups[group_id].total = total number of users that are part of this group's approval

groups[group_id].approved = # of users that approved so far

groups[group_id].rejected = # of users that rejected so far

groups[group_id].requested = # of users that are pending approval

groups[group_id].not_required = # of users that approval is not required

groups[group_id].approvalIDs[state] = array of user ids that are at the specified approval state
```

```
# Note: Iterate the groups using:
for (var id in groups) {
    var group = groups[id];
    ...
}
```

```javascript
function fncGetGroupObj(group_id) {
    var objGroupApproval = new GlideRecord('sysapproval_group');
    objGroupApproval.get(group_id);
    var objGroup = new GlideRecord('sys_user_group');
    objGroup.get(objGroupApproval.assignment_group.sys_id);
    return objGroup;
}
```

Approval scripts also allow computations. For example, if only half of the approvals are required:

```javascript
if (counts.approved/counts.total > .49) {
    answer = 'approved';
} else if (counts.rejected/counts.total > .50) {
    answer = 'rejected';
}
```
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>When anyone rejects</td>
<td>A choice between different approval logics to determine which individual rejections result in rejection of the activity's approval. Options are:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Reject the approval</strong>: Immediately complete the activity with a result of rejected.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Wait for other responses before deciding</strong>: Wait until we get other responses before making an approval or rejection decision. This allows users to change their mind until a decision is made.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: If <strong>Wait for</strong> is set to <strong>Anyone to approve</strong>, then a single approval causes the activity to complete with a result of approved, even if one or more users reject.</td>
</tr>
</tbody>
</table>

**Approval - Group Schedule**

Specify how workflow calculates the approval record's expected start date and due date. Once you've made a selection for 'Due date based on', and 'Schedule based on', the appropriate fields will display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Due date based on</td>
<td>Select how workflow determines the task's duration, due date, and schedule.</td>
</tr>
<tr>
<td></td>
<td>- <strong>A user specified duration</strong>: The duration is based on a user specified value.</td>
</tr>
<tr>
<td></td>
<td>- <strong>A relative duration</strong>: The duration is calculated from a relative duration (such as End of Next Business Day).</td>
</tr>
<tr>
<td></td>
<td>- <strong>A date/time or duration field</strong>: The duration is based on the value of a field on the current record.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Script</strong>: The duration is returned by a script.</td>
</tr>
</tbody>
</table>

| Duration                       | The specific number of days and hours.                                                                                      |
| Only appears when Due date based on is set to A user specified duration |                                                                                                                            |

| Relative duration              | The general number and length of business days.                                                                            |
| Only appears when Due date based on is set to A relative duration |                                                                                                                            |

| Due date field                 | The date/time or duration field.                                                                                            |
| Only appears when Due date based on is set to A date/time or duration field |                                                                                                                            |

<p>| Due date script                | The script that sets 'answer' to the number of seconds for the duration.                                                      |
| Only appears when Due date based on is set to Script |                                                                                                                            |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Schedule based on             | The basic schedule the timer uses to count working hours. If a schedule is specified, the duration will only be considered for times that are specified on the schedule. For example, if the duration is 2 hours and the workflow begins at 4:00pm on a schedule that is 8am - 5pm, then it ends at 9:00am the next day. The options are:  
  - This workflow’s schedule: The schedule uses workflow context date, time, and an optional Time zone based on value.  
  - A specific schedule: The schedule uses a pre-defined Schedule and an optional Time zone based on value.  
  - A schedule field: The schedule uses a value from a table and an optional Time zone based on value. |
| Schedule                      | The predefined Schedule from a list.                                                                                                                                                                   |
| Schedule field                | A date and time or duration field for the schedule, that is associated with the table. Valid fields appear in blue on the Select the element from a tree dialog.                                               |
| Time zone based on            | The time zone for calculating the duration. The time zone may be based on:  
  - No time zone: Default. Workflow uses the GMT time zone.  
  - A specific time zone: A specific Time zone that you choose from a choice list.  
  - A time zone field: A Time zone field to track time duration from a field on the form. |
| Time zone                     | Select the time zone you want from the choice list.                                                                                                                                                   |
| Time zone field               | A date and time or duration field for the schedule, that is associated with the table. Valid fields appear in blue on the Select the element from a tree dialog.                                               |
| Approval - Advanced           | If desired, write a script for determining additional users to request approvals from.                                                                                                                |
| Advanced                      | Select this check box to write a script for determining additional users to request approvals from. Use the Additional groups script to customize group approvals. |
### Field

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional groups script</td>
<td>If the <strong>Advanced</strong> check box is selected, this script is called to determine any additional group approvals to be created. The script needs to set the variable <code>answer</code> to a comma-separated list of group ids or an array of group ids to add as approver groups. For example:</td>
</tr>
</tbody>
</table>
|                     | `answer = [];
|                     | answer.push('id1');
|                     | answer.push('id2');` |

### Conditions

The following conditions determine which transition runs after this activity.

**Approval - Group activity conditions**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved</td>
<td>The users from the groups have approved the request based on the <strong>Wait for</strong> rules.</td>
</tr>
<tr>
<td>Rejected</td>
<td>The users from the groups have rejected the request based on the <strong>Wait for</strong> rules.</td>
</tr>
<tr>
<td>Error</td>
<td>The event or condition that generates an error.</td>
</tr>
<tr>
<td>Skipped</td>
<td>The event or condition that allows a skipped approval.</td>
</tr>
</tbody>
</table>

### States

The activity state tells the workflow engine what to do with the activity.

**Approval - Group activity states**

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executing</td>
<td>The workflow engine starts the <code>execute</code> function of the activity.</td>
</tr>
<tr>
<td>Waiting</td>
<td>The workflow engine ignores the activity until a specific event to restart the activity is fired.</td>
</tr>
<tr>
<td>Finished</td>
<td>The activity finished running. See the result value for the outcome of the activity.</td>
</tr>
<tr>
<td>Cancelled</td>
<td>This activity, or the workflow that contains this activity, was canceled.</td>
</tr>
<tr>
<td>Error</td>
<td>A JavaScript error occurred. Review the logs for error details.</td>
</tr>
</tbody>
</table>

**Approval - User workflow activity**

The **Approval - User** activity creates one or more individual user approvals.
Results

The result value is the final approval disposition. This disposition depends on the approval actions take by the approvers and the approval conditions specified in the Wait for or When Anyone Rejects fields. Possible result values are:

- Approved
- Rejected
- Deleted
- Cancelled

Input variables

Approval - User activity input variables

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approval - User When</td>
<td>Specify when this activity generates a user approval record.</td>
</tr>
<tr>
<td>Condition</td>
<td>Conditions which, if met, cause the individual approval to be generated. If the conditions are not met, the approval is skipped.</td>
</tr>
<tr>
<td>Approval - User Approvers</td>
<td>Specify the users whose approval will be requested.</td>
</tr>
<tr>
<td>Users</td>
<td>The users for the approval. Use the tree icon to select user reference fields from the current record to create approvals, such as ${assigned_to}. If no user is selected, the activity automatically sets the approval to Approved.</td>
</tr>
<tr>
<td>Groups</td>
<td>Groups whose members should also receive approvals. Note that this is different than the Approval - Group activity, which creates a group approval in addition to the individual approvals. The tree icon can be used to select group reference fields from the current record to create approvals, such as ${assignment_group}.</td>
</tr>
<tr>
<td>Approval - User Condition</td>
<td>Specify how the activity decides to approve or reject the approval, based on the responses from individual approvers.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Wait for</td>
<td>A choice between different approval logics to determine which individual approvals result in approval of the activity's approval. Options are:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Anyone to approve</strong>: Any user can approve and the first approval causes the activity to complete with a result of <strong>approved</strong>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Everyone to approve</strong>: All users must approve (see below for how a rejection is handled).</td>
</tr>
<tr>
<td></td>
<td>- <strong>First response from anyone</strong>: The first approval or rejection from any user causes the activity to complete.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Condition based on script</strong>: Each time a user approves or rejects, the Approval script is called to determine if the activity should complete.</td>
</tr>
<tr>
<td>When anyone rejects</td>
<td>A choice between different approval logics to determine which individual rejections result in rejection of the activity's approval. Options are:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Reject the approval</strong>: Immediately complete the activity with a result of <strong>rejected</strong>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Wait for other responses before deciding</strong>: Wait until we get other responses before making an approval or rejection decision. This allows users to change their mind until a decision is made.</td>
</tr>
<tr>
<td><strong>Note</strong>: Note that if <strong>Wait for</strong> is set to <strong>Anyone to approve</strong> then a single approval will cause the activity to complete with a result of <strong>approved</strong> even if one or more users reject.</td>
<td></td>
</tr>
<tr>
<td>Approval Column</td>
<td>A string field for the name of the approval field on the table the workflow is running on. The default value is <strong>approval</strong>, which is the field on the Task table.</td>
</tr>
<tr>
<td><strong>Note</strong>: Use the field’s name, not its label.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong>: If using any custom approval column fields and approval column journals, use Set Value activities in the workflow to set the custom Approval column fields.</td>
<td></td>
</tr>
<tr>
<td>Approval Journal Column</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Approval Script</td>
<td>If the <strong>Wait for</strong> variable is set to <strong>Condition based on script</strong> this script is called to determine how to handle an approval or rejection. The script needs to set the variable <strong>answer</strong> to approved or rejected to indicate the approval status for this approval. When called, the following information is available:</td>
</tr>
<tr>
<td></td>
<td>counts.total = total number of users that are part of this approval</td>
</tr>
<tr>
<td></td>
<td>counts.approved = # of users that approved so far</td>
</tr>
<tr>
<td></td>
<td>counts.rejected = # of users that rejected so far</td>
</tr>
<tr>
<td></td>
<td>counts.requested = # of users that are pending approval</td>
</tr>
<tr>
<td></td>
<td>counts.not_requested = # of users that are not pending approval</td>
</tr>
<tr>
<td></td>
<td>counts.not_required = # of users that approval is not required</td>
</tr>
</tbody>
</table>

### Approval - User Schedule

Specify how workflow calculates the approval record’s expected start date and due date. Once you’ve made a selection for ‘Due date based on’, and ‘Schedule based on’, the appropriate fields will display.

<table>
<thead>
<tr>
<th>Due date based on</th>
<th>Select how workflow determines the task’s duration, due date, and schedule.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>A user specified duration:</strong> The duration is based on a user specified value.</td>
</tr>
<tr>
<td></td>
<td><strong>A relative duration:</strong> The duration is calculated from a relative duration (such as End of Next Business Day).</td>
</tr>
<tr>
<td></td>
<td><strong>A date/time or duration field:</strong> The duration is based on the value of a field on the current record.</td>
</tr>
<tr>
<td></td>
<td><strong>Script:</strong> The duration is returned by a script.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Duration</th>
<th>The specific number of days and hours.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only appears when <strong>Due date based on</strong> is set to <strong>A user specified duration</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Relative duration</th>
<th>The general number and length of business days.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only appears when <strong>Due date based on</strong> is set to <strong>A relative duration</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Due date field</th>
<th>The date/time or duration field.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only appears when <strong>Due date based on</strong> is set to <strong>A date/time or duration field</strong></td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Due date script</td>
<td>The script that sets 'answer' to the number of seconds for the duration.</td>
</tr>
<tr>
<td>Schedule based on</td>
<td>The basic schedule the timer uses to count working hours. If a schedule is specified, the duration will only be considered for times that are specified on the schedule. For example, if the duration is 2 hours and the workflow begins at 4:00pm on a schedule that is 8am - 5pm, then it ends at 9:00am the next day. The options are:</td>
</tr>
<tr>
<td></td>
<td>• This workflow’s schedule: The schedule uses workflow context date, time, and an optional Time zone based on value.</td>
</tr>
<tr>
<td></td>
<td>• A specific schedule: The schedule uses a pre-defined Schedule and an optional Time zone based on value.</td>
</tr>
<tr>
<td></td>
<td>• A schedule field: The schedule uses a value from a table and an optional Time zone based on value.</td>
</tr>
<tr>
<td>Schedule</td>
<td>The predefined Schedule from a list.</td>
</tr>
<tr>
<td>Schedule field</td>
<td>A date and time or duration field for the schedule, that is associated with the table. Valid fields appear in blue on the Select the element from a tree dialog.</td>
</tr>
<tr>
<td>Time zone based on</td>
<td>The time zone for calculating the duration. The time zone may be based on:</td>
</tr>
<tr>
<td></td>
<td>• No time zone: Default. Workflow uses the GMT time zone.</td>
</tr>
<tr>
<td></td>
<td>• A specific time zone: A specific Time zone that you choose from a choice list.</td>
</tr>
<tr>
<td></td>
<td>• A time zone field: A Time zone field to track time duration from a field on the form.</td>
</tr>
<tr>
<td>Time zone</td>
<td>Select the time zone you want from the choice list.</td>
</tr>
<tr>
<td>Time zone field</td>
<td>A date and time or duration field for the schedule, that is associated with the table. Valid fields appear in blue on the Select the element from a tree dialog.</td>
</tr>
<tr>
<td>Approval - Advanced</td>
<td>If desired, write a script for determining additional users to request approvals from.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Select this check box to write a script for determining additional users to request approvals from.</td>
</tr>
</tbody>
</table>
### Field

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Additional approvers script  | If the Advanced check box is selected, this script is called to determine any additional user approvals to be created. The script needs to set the variable answer to a comma-separated list of user ids and group ids or an array of user and group ids to add as approvers. For example:  
  ```javascript
  answer = [];
  answer.push('id1');
  answer.push('id2');
  ``` |

### Conditions

The following conditions determine which transition runs after this activity.

**Approval - User activity conditions**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved</td>
<td>The users approved the request based on the Wait for rules.</td>
</tr>
<tr>
<td>Rejected</td>
<td>The users rejected the request based on the Wait for rules.</td>
</tr>
<tr>
<td>Error</td>
<td>The event or condition that generates an error.</td>
</tr>
<tr>
<td>Skipped</td>
<td>The event or condition that allows a skipped approval.</td>
</tr>
</tbody>
</table>

### States

The activity state tells the workflow engine what to do with the activity.

**Approval - User activity states**

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executing</td>
<td>The workflow engine starts the execute function of the activity.</td>
</tr>
<tr>
<td>Waiting</td>
<td>The workflow engine ignores the activity until a specific event to restart the activity is fired.</td>
</tr>
<tr>
<td>Finished</td>
<td>The activity finished running. See the result value for the outcome of the activity.</td>
</tr>
<tr>
<td>Cancelled</td>
<td>This activity, or the workflow that contains this activity, was canceled.</td>
</tr>
<tr>
<td>Error</td>
<td>A JavaScript error occurred. Review the logs for error details.</td>
</tr>
</tbody>
</table>
Generate workflow activity
The Generate activity immediately creates task or approval records from any task or approval activities placed after the Generate activity in the workflow path.

Note: This activity is only available when the workflow runs on a table that extends Task.

By default, the workflow does not create any tasks or approvals until it reaches them in the workflow.

The Generate activity follows all transitions through the workflow to each activity. For each activity:

- If it is a task activity, creates the task and sets:
  - The State to Pending
  - The Expected Start Date
  - The Due Date

- If it is an approval activity, creates the approvals and sets:
  - The approval State to Not Requested
  - The Expected Start Date
  - The Due Date

Expected start dates and due dates are calculated based on the Expected Duration of all of the tasks and approvals between the Generate activity and the activity being updated. In the case of a branched path (between a Branch and Join activity), the longer duration will be used for any post-branch activities.

The Generate activity can be used more than once, and any tasks or approvals will be refreshed with updated information. This is useful in situations where the list of approvers or other important information is still editable while the workflow is in process and it may be necessary to update or correct the generated approvals or tasks.

To exclude a set of activities from the Generate activity, select the Skip during generate check box on any condition and its transitions will not be followed during the generate process. By default, the following conditions have the Skip during generate check box selected:

- Rejected (for any of the approval activities)
- No condition of If activity
- Continue condition of Turnstile activity
- Incomplete condition of Join activity

Input variables
Input variables determine the initial behavior of the activity.

Generate activity input variables

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate approvals</td>
<td>If selected, approvals are created when running the Generate activity. If cleared, the approvals are used to compute their estimated duration, but no approvals are created.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Generate tasks</td>
<td>If selected, tasks are created when running the Generate activity. If cleared, the tasks are used to compute their estimated duration, but no tasks are created.</td>
</tr>
</tbody>
</table>

**States**

The activity state tells the workflow engine what to do with the activity.

**Generate activity states**

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executing</td>
<td>The activity is executing.</td>
</tr>
<tr>
<td>Finished</td>
<td>The activity finished running. See the result value for the outcome of the activity.</td>
</tr>
<tr>
<td>Cancelled</td>
<td>This activity, or the workflow that contains this activity, was canceled.</td>
</tr>
</tbody>
</table>
Example

Generate workflow

In this example, the following approvals are generated:

- Approval-2
- Approval-3

Approval-4 is skipped since the \textbf{Rejected} condition of Approval-3 has \textit{Skip during generate} selected.

Here is an example of using the \textbf{Generate} activity that describes the expected start and due dates:
Generate workflow start and due date

In this example, if the **Generate** activity is run on Jan 1, 2016, the following expected start dates and due dates would be set for the generated tasks.

<table>
<thead>
<tr>
<th>Task</th>
<th>Expected Start Date</th>
<th>Reason</th>
<th>Due Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task 2 (1 day)</td>
<td>Jan. 2, 2016</td>
<td>Task 1 is 1 day</td>
<td>Jan. 3, 2016</td>
</tr>
<tr>
<td>Task 4 (1 day)</td>
<td>Jan. 3, 2016</td>
<td>Task 3 is 2 days</td>
<td>Jan. 4, 2016</td>
</tr>
<tr>
<td>Task 5 (1 day)</td>
<td>Jan. 4, 2016</td>
<td>Task 4 ends the latest before the Join</td>
<td>Jan. 5, 2016</td>
</tr>
</tbody>
</table>

Notice that Task 5 starts on Jan. 4, 2016 since the longest path (based on due dates) to the **Join** is Task 3/Task 4.

**Manual Approvals workflow activity**

The **Manual Approvals** activity watches and manages any approvals that users add manually outside of the workflow process. This activity only selects approvals that are in the Not requested state.

*Note:* This activity is only available when the workflow runs on a table that extends Task.

If there are no pending manual approvals when this activity executes, the activity immediately completes with a result of **approved**. This activity does not create approval records. Use this activity to pause the workflow when a user adds a manual approval to a record with an associated workflow, and it is in the Not requested state. The workflow waits for the approval to be closed before proceeding.

**Results**

The workflow designer can assign a result value using `activity.result` from within a script field of the activity. By default, the result value of the activity is the final approval disposition determined by the approval actions take by the approvers. Possible result values are:

- Approved
Input variables

Input variables determine the initial behavior of the activity.

**Manual Approvals activity input variables**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Wait for</strong></td>
<td>Indicate what to wait for to indicate that the approval activity is approved or rejected. Options are:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Any manual user or group approval</strong>: Any user can approve and the first approval causes the activity to complete with a result of <strong>approved</strong>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>All manual user or group approvals</strong>: All users must approve (see below for how a rejection is handled).</td>
</tr>
<tr>
<td></td>
<td>- <strong>The first response from any manual approval</strong>: The first approval or rejection from any user causes the activity to complete.</td>
</tr>
<tr>
<td><strong>When anyone rejects</strong></td>
<td>Indicate what happens when any user rejects their approval request. Options are:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Reject the approval</strong>: Immediately complete the activity with a result of <strong>rejected</strong>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Wait for other responses before deciding</strong>: Wait until we get other responses before making an approval or rejection decision. This allows users to change their mind until a decision is made.</td>
</tr>
<tr>
<td></td>
<td>In addition, if <strong>Wait for</strong> is set to <strong>Anyone to approve</strong> then a single approval will cause the activity to complete with a result of <strong>approved</strong> even if one or more users reject.</td>
</tr>
</tbody>
</table>

**Conditions**

The conditions determine which transition runs after this activity.

**Manual Approvals activity conditions**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved</td>
<td>The users from the groups have approved the request based on the <strong>Wait for</strong> rules.</td>
</tr>
<tr>
<td>Rejected</td>
<td>The users from the groups have rejected the request based on the <strong>Wait for</strong> rules.</td>
</tr>
</tbody>
</table>
States

The activity state tells the workflow engine what to do with the activity.

**Manual Approvals activity states**

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executing</td>
<td>The workflow engine starts the <code>execute</code> function of the activity.</td>
</tr>
<tr>
<td>Waiting</td>
<td>The workflow engine ignores the activity until a specific event to restart the activity is fired.</td>
</tr>
<tr>
<td>Finished</td>
<td>The activity finished running. See the result value for the outcome of the activity.</td>
</tr>
<tr>
<td>Cancelled</td>
<td>This activity, or the workflow that contains this activity, was canceled.</td>
</tr>
<tr>
<td>Error</td>
<td>A JavaScript error occurred. Review the logs for error details.</td>
</tr>
</tbody>
</table>

**Rollback To workflow activity**

The **Rollback To** activity transitions directly to the activity specified by the outgoing transition line arrow.

*Note:* This activity is only available when the workflow runs on a table that extends Task.

**Rollback To** determines which activities to reset based on the actual workflow sequence (transition line attachments) of activities between itself and the transitioned to activity, not the execution order. **Rollback To** then marks all the approvals that have transitioned between the rollback and the transitioned to activity as **Not Yet Requested** and the tasks as either **Open** or **Pending**.

Use the **Rollback To** activity for all workflows in which multiple rollbacks are required. **Rollback To** has no variables.

**Conditions**

The conditions determine which transition runs after this activity.

**Rollback To activity conditions**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always</td>
<td>The event or condition that causes the approval to revert to the previous workflow step.</td>
</tr>
<tr>
<td>Error</td>
<td>The event or condition that generates an error.</td>
</tr>
<tr>
<td>Skipped</td>
<td>The event or condition that allows a skipped approval.</td>
</tr>
</tbody>
</table>

**States**

The activity state tells the workflow engine what to do with the activity.
### Rollback To activity states

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executing</td>
<td>The workflow engine starts the <code>execute</code> function of the activity.</td>
</tr>
<tr>
<td>Waiting</td>
<td>The workflow engine ignores the activity until a specific event to restart the activity is fired.</td>
</tr>
<tr>
<td>Finished</td>
<td>The activity finished running. See the result value for the outcome of the activity.</td>
</tr>
<tr>
<td>Cancelled</td>
<td>This activity, or the workflow that contains this activity, was canceled.</td>
</tr>
<tr>
<td>Error</td>
<td>A JavaScript error occurred. Review the logs for error details.</td>
</tr>
</tbody>
</table>

### Rollback To behavior

The **Rollback To** activity transitions directly to the activity specified by the transition line arrow. Use the **Rollback To** activity for all workflows that use multiple or nested rollbacks. **Rollback To** resets the targeted task (the direct transition) to **Open**. All tasks that have executed between the **Rollback To** activity and the targeted task (rolled back task) are set to **Pending**.

```
(0) Begin
(1) Log Message
(2) Task 1
(3) Task 3
(4) Task 2
(5) Timer
(6) Approval 1
(7) Roll back to first task
(8) Task 1
(9) Task 2
(10) Approval 1
(11) Log approval
(12) Join
(13) Send email
(14) End
```
Transition history

The state of (3) Task 3 does not change, since this activity does not directly transition from the rollback target activity. To see what activities were rolled back, select the Workflow Transition History related list and look at the Rolled back column.

The Rollback To activity (7) updates the following activities:

(8) Task 1: reset to Open
(9) Task 2: reset to Pending
(10) Approval 1: reset to Not Yet Requested
Rollback To workflow transition

Rollback To activity
When conditions in a workflow trigger a Rollback To activity, the workflow moves processing backward to a specified activity in the workflow and resets certain activities that have already executed back to their original state. This is useful when handling an unexpected failure or as part of a programmed logical flow.

When an activity is reset during a workflow rollback, the following happens:

- Approvals are reset to Not Requested.
- Tasks are reset to either Open or Pending. A rollback workflow path cannot create new tasks.

Activities that perform external system operations, such as deleting a file or sending an email, are not rolled back. Only approval and task activity states are reset.

A workflow can contain a single rollback, multiple rollbacks, or nested rollbacks in more complex workflows. The Rollback To activity resets activities based on the actual workflow sequence.
Condition Workflow activities

Condition activities provide conditional branching and logical operation functionality for workflows.

If workflow activity
The If activity checks a condition or script to determine if a Yes or No transition should be taken.

If the workflow creator specifies both the Condition and the Advanced script, both must evaluate successfully for activity to take the Yes transition.

Results

The workflow designer can assign a result value using activity.result from within the Script field on the activity record. By default, the result value of the activity is the final result of the condition or script specified. Possible result values are:

- Yes
- No

Input variables

The following variables determine the behavior of the activity.

If activity input variables

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition</td>
<td>If specified and the current record matches the condition, the Yes transition is taken.</td>
</tr>
<tr>
<td>Advanced and Script</td>
<td>To specify a script, select the Advanced check box. You may then enter a script that is evaluated. If your script sets the variable answer to yes, then the Yes transition is taken. Otherwise, the No transition is taken.</td>
</tr>
</tbody>
</table>

Conditions

The following conditions determine which transition comes after the activity.

If activity conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Taken when the condition, if specified, matches and the Advanced script, if specified, returns yes.</td>
</tr>
<tr>
<td>No</td>
<td>Taken when either the condition does not match or the Advanced script, if specified, returns no.</td>
</tr>
</tbody>
</table>
States

The activity state tells the workflow engine what to do with the activity.

If activity states

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executing</td>
<td>The workflow engine knows to start the onExecute function of the activity.</td>
</tr>
<tr>
<td>Waiting</td>
<td>The workflow engine ignores the activity until a specific event to restart the activity is fired.</td>
</tr>
<tr>
<td>Finished</td>
<td>The activity finished running. See the result value for the outcome of the activity.</td>
</tr>
<tr>
<td>Cancelled</td>
<td>This activity, or the workflow that contains this activity, was canceled.</td>
</tr>
<tr>
<td>Error</td>
<td>A JavaScript error occurred. Review the logs for error details.</td>
</tr>
</tbody>
</table>

Switch workflow activity

The Switch activity checks if the value of a passed field or variable is equivalent to one of several case values.

The switch activity behavior is similar to a switch statement in Java.

When creating a switch activity, select a Variable or Field to check against activity conditions for a matching field value. When the value passed in this variable or field matches the value defined in the Condition field of the activity condition, the workflow progresses through that activity condition.

Results

The variable or field selected in the Variable or Field activity variable determines the possible result values.

Input variables

The following variables determine the behavior of the activity.

Switch activity input variables

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select Variable or Field as the type of value to check against available conditions. This selection sets the label and available options for the other field.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Variable or Field | Select the source of the value compared against the switch activity conditions. The field label and available options depend on the Type selection.  
- Variable: select any service catalog variable.  
- Field: select any field from the Table defined in the workflow properties. |

**States**

The activity state tells the workflow engine what to do with the activity.

**Switch activity states**

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executing</td>
<td>The workflow engine knows to start the onExecute function of the activity.</td>
</tr>
<tr>
<td>Waiting</td>
<td>The workflow engine ignores the activity until a specific event to restart the activity is fired.</td>
</tr>
<tr>
<td>Finished</td>
<td>The activity finished running. See the result value for the outcome of the activity.</td>
</tr>
<tr>
<td>Cancelled</td>
<td>This activity, or the workflow that contains this activity, was canceled.</td>
</tr>
<tr>
<td>Error</td>
<td>A JavaScript error occurred. Review the logs for error details.</td>
</tr>
</tbody>
</table>

**Example**

You can create a switch activity that sets different field values on an incident based on the Assignment group of the incident record.
Switch activity example

The **Field** selected is the incident **Assigned to** field.
If the value of the **Assigned to** field of the workflow-triggering incident is **Service Desk** or **Field Services**, the workflow populates values on the incident record before continuing. If the **Assigned to** value is **Hardware**, the workflow continues without populating any field values.

Condition type (Standard, Else, or Error) is used. For more information, see *Manage workflow activity conditions*.

### Condition Properties

#### Hardware group condition

**Wait for condition workflow activity**

The **Wait for condition** activity causes the workflow to wait at this activity until the current record matches the specified condition.

The workflow evaluates the **Wait for condition** activity each time the current record is updated. Use this activity to pause a workflow indefinitely until a particular criteria is met by a record update. To pause a workflow for a timed duration see *Timer workflow activities*. 
For workflow to consider the condition met, all conditions specified – whether in the builder or in a script – must be true.

**Note:** A Wait for condition activity should only be used to wait for an external event such as a record update, and not one from a workflow setting a value. If you have a workflow setting a value and want to wait for that same field to be seen as 'changed,' try inserting a one-second timer.

**Results**

The workflow designer can assign a result value using `activity.result` from within a script field of the activity. The activity transitions when the result value is true.

**Input variables**

The following variables determine the behavior of the activity.

**Wait for condition activity input variables**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition</td>
<td>The workflow is paused at this activity until this condition matches the current record.</td>
</tr>
<tr>
<td>Condition script</td>
<td>If specified, the workflow is paused at this activity until this script sets the answer variable to true.</td>
</tr>
</tbody>
</table>

**States**

The activity state tells the workflow engine what to do with the activity.

**Wait for condition activity states**

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executing</td>
<td>The workflow engine knows to start the <code>onExecute</code> function of the activity.</td>
</tr>
<tr>
<td>Waiting</td>
<td>The workflow engine ignores the activity until a specific event to restart the activity is fired.</td>
</tr>
<tr>
<td>Finished</td>
<td>The activity finished running. See the result value for the outcome of the activity.</td>
</tr>
<tr>
<td>Cancelled</td>
<td>This activity, or the workflow that contains this activity, was canceled.</td>
</tr>
<tr>
<td>Error</td>
<td>A JavaScript error occurred. Review the logs for error details.</td>
</tr>
</tbody>
</table>

**Wait for WF Event workflow activity**

The **Wait for WF Event** activity causes the workflow to wait at this activity until the specified event is fired.

Use this activity to wait for another activity to fire an event. Events from other activities are fired in a script using the workflow.fireEvent('eventName') API call.
Results

The workflow designer can assign a result value using `activity.result` from within a script field of the activity. This activity transitions when the specified event fires.

Input variables

The following variables determine the behavior of the activity.

**Wait For WF Event activity input variables**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wait for Event</td>
<td>An event name to trigger the workflow.</td>
</tr>
</tbody>
</table>

States

The activity state tells the workflow engine what to do with the activity.

**Wait For WF Event activity states**

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executing</td>
<td>The workflow engine knows to start the <code>onExecute</code> function of the activity.</td>
</tr>
<tr>
<td>Waiting</td>
<td>The workflow engine ignores the activity until a specific event to restart the activity is fired.</td>
</tr>
<tr>
<td>Finished</td>
<td>The activity finished running. See the result value for the outcome of the activity.</td>
</tr>
<tr>
<td>Cancelled</td>
<td>This activity, or the workflow that contains this activity, was canceled.</td>
</tr>
<tr>
<td>Error</td>
<td>A JavaScript error occurred. Review the logs for error details.</td>
</tr>
</tbody>
</table>

Notify workflow activities

Notify activities manage calls and SMS messages in Notify.

All Notify workflows that manage a phone call must run on the `notify_call` table. Call-related Notify activities can be added only to workflows where the `Table` field value is `Notify Call (notify_call)`.

You can identify if an outbound call was answered by a human or by an answering machine from within a Notify workflow by evaluating the `current.is_human` variable, such as with an `If` workflow activity. This variable is set by the telephony provider when an outbound call is answered. This variable is always true for inbound calls.

**Note:** Do not add a `Timer` activity between multiple Notify activities that interact with active phone calls.

**Important:** When creating a Notify workflow, set the workflow `If condition matches` field to `-- None --`. Notify controls which workflow to run based on the configured number groups.
Forward call workflow activity
The **Forward Call** activity forwards a Notify call to an E.164-compliant phone number.

If the person receiving a forwarded call hangs up, the **forward call** activity completes and transitions to the next activity. Any further Notify activities in the workflow run for the caller only.

### Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone number to call</td>
<td>Enter the phone number to forward the call to.</td>
</tr>
<tr>
<td>Timeout (in seconds)</td>
<td>Enter the amount of time to wait for the call to be answered before hanging up.</td>
</tr>
<tr>
<td>Record</td>
<td>Select this check box to record the conversation.</td>
</tr>
</tbody>
</table>

### Conditions

The conditions determine which transition comes after this activity. The **forward call** activity does not specify any conditions by default.

You can add an error condition to this activity. The activity transitions through the error condition if the phone number to call is invalid.

**Input workflow activity**
The **Input** activity creates a phone menu by presenting a list of options on a Notify call.

### Input Variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of digits</td>
<td>Specify the maximum number of digits the caller can enter. A caller can enter fewer digits than the maximum and press the <strong>Finish key</strong> to complete the entry.</td>
</tr>
<tr>
<td>Finish key</td>
<td>Specify the key a caller can press on their phone when finished selecting a menu option.</td>
</tr>
<tr>
<td>Timeout (in seconds)</td>
<td>Specify the amount of time to wait before closing the menu automatically when the caller does not select a menu option.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Select this check box to use a script to build the phone menu, instead of using the activity conditions.</td>
</tr>
</tbody>
</table>
Variable | Description
---|---
Script | Define the script to build the phone menu. The script must specify an *answer* variable as a JavaScript object with the following format:
```
answer = {
  1: {
    "say": "https://some_url.com/options/one.mp3",
    "myCustomData": "some data here"
  },
  2: {
    "say": "type 2 to speak to a representative",
    "language": "en-US",
    "myCustomData": "some more data here"
  }
};
```
The script may specify either a text-to-speech string and language code or the URL of a prerecorded message for each entry. You can also add optional attributes to store related information, such as `myCustomData` in the example above.

### Conditions

The conditions determine the transition that comes after this activity.

The *input* activity does not specify any conditions by default. You must define conditions to build the phone menu. Each condition is one option on the phone menu. Notify reads the text from each condition *Name* to the caller, up to 100 characters per condition.

You can specify a language for each condition by prefixing the message with the language code, in the format `xx-XX:<Message>`. For example, add `fr-CA:` for Canadian French. Available languages are stored on the Notify Language (notify_language) table.

The condition that the activity transitions through depends on the digits entered by the caller. Set the condition *Condition* value to `parseInt(workflow.scratchpad.digits) == <expected digits>`. For example, to transition through a condition when the caller presses the number 3, set the *Condition* to `parseInt(workflow.scratchpad.digits) == 3`.

You can add an error condition to this activity. The activity transitions through the error condition if the advanced script returns an invalid value, or if the text to say for a condition is empty.

### Scratchpad Entries

The activity uses the workflow scratchpad to write persistent values.

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>workflow.scratchpad.digits</td>
<td>The digits entered by the caller, as a string.</td>
</tr>
</tbody>
</table>
### Workflow Activity: workflow.scratchpad.menu<activity name>

The entire **answer** variable, if using the advanced script option. You can access this menu from other activities after this activity successfully executes.

For example, if the activity name is *choices*, you can access values from the menu using:

```javascript
var previousActivity = "choices";
var choicesMenu = workflow.scratchpad.menu[previousActivity];
var menuItem = choicesMenu[workflow.scratchpad.digits];
// Selects the menu item based on the caller's input.
var selectedValue = menuItem.myCustomData; // get the custom data for the selected menu item.
```

### Hangup workflow activity

The **Hangup** activity disconnects an active Notify phone call.

You can use the **hangup** activity to disconnect only calls that have been answered. Use the **reject** activity to disconnect calls that have not been answered.

### Play workflow activity

The **Play** activity plays a sound file on a Notify call.

### Input Variables

Input variables determine the initial behavior of the activity.

#### Input Variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>URL</strong></td>
<td>Enter the URL of a sound file to play. If the URL is inaccessible, or if the audio file mime type is not supported by the telephony provider, the <strong>play</strong> activity is skipped.</td>
</tr>
<tr>
<td><strong>Loop</strong></td>
<td>Enter the number of times the sound file should play.</td>
</tr>
</tbody>
</table>

### Conditions

The conditions determine which transition comes after this activity. The **play** activity does not specify any conditions by default.

You can create an error condition to handle errors with the sound file. The activity transitions through the error condition if the specified sound file is not available, or has an unsupported mime type. Supported mime types are listed on the Notify Audio MIME Types **[notify_mime_type]** table.

### Record workflow activity

The **Record** workflow activity records audio from a user on a Notify call.
Input Variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max duration (in seconds)</td>
<td>Enter the maximum duration, in seconds, allowed for a recording.</td>
</tr>
<tr>
<td>Timeout (in seconds)</td>
<td>Enter the amount of time to wait before ending a recording automatically when the caller is silent.</td>
</tr>
<tr>
<td>Finish Key</td>
<td>Specify the key a caller can press on their phone to end the recording.</td>
</tr>
</tbody>
</table>

Scratchpad Entries

The activity uses the workflow scratchpad to store persistent values.

The `record` activity adds the `recording` variable to the workflow scratchpad. This variable stores metadata about the recording, such as URI, ID, and duration. You can access the following values from this variable.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>recording.recordingDuration</td>
<td>The duration of the recording, in seconds.</td>
</tr>
<tr>
<td>recording.from_number</td>
<td>The caller's phone number, including country code.</td>
</tr>
<tr>
<td>recording.notify_number</td>
<td>The Notify phone number used to respond to the call, including country code.</td>
</tr>
<tr>
<td>recording.recordingID</td>
<td>The ID used by the telephony provider to identify the recording.</td>
</tr>
<tr>
<td>recording.recordingURL</td>
<td>The URL from the telephony provider to access the recording.</td>
</tr>
</tbody>
</table>

Reject workflow

The `Reject` workflow activity rejects an incoming Notify call.

You can use the `reject` activity to disconnect only calls that have not yet been answered. Use the `hang up` activity to disconnect calls that have been answered.

Input variables

Input variables determine the initial behavior of the activity.
Input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reason</td>
<td>Select a reason for rejecting the call, such as busy.</td>
</tr>
</tbody>
</table>

Say workflow activity

The `say` workflow activity allows you to play a message, using text to speech, on a Notify call.

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text to say</td>
<td>Specify the text to read.</td>
</tr>
<tr>
<td>Language</td>
<td>Select the language and locale to use when reading text.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Select this check box to use a script to define the language and message, instead of using the <code>Text to say</code> and <code>Language</code> values.</td>
</tr>
<tr>
<td>Script</td>
<td>Define a script to set what text is read on the call. The script must return a string that defines the language and the text to read. For example, to play an English-language message, return <code>{language: 'en-US', text: 'Text to read'}</code>.</td>
</tr>
</tbody>
</table>

Forward to notify client workflow activity

The `forward to notify client` workflow activity connects a phone call to a Notify WebRTC client.

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Select the user to connect the call to.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Select this check box to use a script to determine which client to connect to, instead of using the <code>User</code> variable.</td>
</tr>
<tr>
<td>Script</td>
<td>Define a script that controls which client to connect to. This script should return a GlideRecord for a single User (sys_user) record.</td>
</tr>
<tr>
<td>Timeout (in seconds)</td>
<td>Enter the amount of time to wait for the call to be connected before hanging up.</td>
</tr>
<tr>
<td>Record</td>
<td>Select this check box to record the call.</td>
</tr>
</tbody>
</table>
Conditions

The conditions determine which transition comes after this activity. The **Forward to Notify Client** activity does not specify any conditions by default.

You can add an error condition to this activity. The activity transitions through the error condition if there is an issue with the Notify client.

Call workflow activity

The **Call** activity makes outbound phone calls using a Notify workflow.

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify Number</td>
<td>The Notify phone number to make the call from. When you initiate a call, the outgoing call workflow for the number group associated with this number runs.</td>
</tr>
<tr>
<td>Phone number to call</td>
<td>The E.164-compliant phone number to call.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Select this check box to use a script to determine number to call, and the Notify number to call from instead of using the <em>Phone number to call</em> and <em>Notify Number</em> variables.</td>
</tr>
<tr>
<td>Script</td>
<td>Define a script that controls which number to call. This script should return a string listing the Notify number sys_id, as well as the phone number to call, such as <code>{notify_number: ‘sys_id’, phone_number: ‘+316...’} </code></td>
</tr>
</tbody>
</table>

Conditions

The conditions determine which transition comes after this activity. The **call** activity does not specify any conditions by default.

You can add an error condition to this activity. The activity transitions through the error condition if the call could not be set up due to invalid data returned by the advanced script.

Join conference call workflow activity

The **Join Conference Call** connects an incoming or outgoing call to a Notify conference call.

Notify includes the workflows Notify: (Re)join Conference Call and Notify: Join Conference Call Via SMS to demonstrate how to use the **join conference call** activity to connect inbound and outbound calls, and inbound SMS messages to a conference call.

Input variables

Input variables determine the initial behavior of the activity.
### Input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced</td>
<td>Select this check box to display advanced configuration options.</td>
</tr>
<tr>
<td>Script</td>
<td>Specify advanced configuration options using JavaScript, such as if the new participant should be muted upon joining the conference call. You can access values from the workflow scratchpad.</td>
</tr>
</tbody>
</table>

### Conditions

The conditions determine which transition comes after this activity. The `join conference call` activity does not specify any conditions by default.

You can add an error condition to this activity. The activity transitions through the error condition if the `conference_call` scratchpad variable is not set.

### Scratchpad entries

The activity uses the workflow scratchpad to read persistent values.

<table>
<thead>
<tr>
<th>Scratchpad variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>workflow.scratchpad.conference_call</td>
<td>A GlideRecord for a single conference call record. A call processed by this activity is added to this conference call. If this value is not specified, the <code>join conference call</code> activity will log an error.</td>
</tr>
<tr>
<td></td>
<td>When initiating an outgoing call workflow using the Notify API <code>call(String notifyPhoneNumber, String toPhoneNumber, GlideRecord conferenceCall)</code> method, this scratchpad value is set automatically to the conference call GlideRecord. For incoming call workflows, or workflows initiated using a different mechanism, you must explicitly set this scratchpad value.</td>
</tr>
</tbody>
</table>

---

**Send SMS workflow activity**

The **send SMS** workflow activity to send short text messages using Notify to users’ phones.

### Input variables

Input variables determine the initial behavior of the activity.
### Input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From</td>
<td>Select the Notify phone number to use to send the SMS message.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Select this check box to use JavaScript to determine which numbers to send the message to, and the Notify number to use to send the message.</td>
</tr>
<tr>
<td>To</td>
<td>Select any number of users to send the message to. The user record must have a E.164-compliant phone number or notification device configured for SMS messages.</td>
</tr>
<tr>
<td>To (groups)</td>
<td>Select any number of groups to send the message to. All members of that group with an E.164-compliant phone number or SMS notification device receive the message.</td>
</tr>
<tr>
<td>Message</td>
<td>Enter the message to send. You can add field values from the current record by using the Select variables box. You can also add values from the workflow scratchpad. If a field and a scratchpad variable have the same name, the field value is used. Because you can use variables in this message, it is not possible to determine the length of the message at design time. If the activity sends a message that is longer than supported by the telephony provider, the message is truncated and the instance logs a warning.</td>
</tr>
<tr>
<td>To (script)</td>
<td>Enter a script to determine which numbers to send the message to, and the Notify number to use to send the message. The script should return a JavaScript object with the format <code>{notify_number: \'...sys_id...', users: [...], groups: [...], numbers: [...]}</code>. Specify the users or groups to send the message to as an array of sys_id values. Specify other numbers as an array of E.164-compliant phone numbers. This field appears only if Advanced is selected.</td>
</tr>
</tbody>
</table>

### Conditions

The conditions determine which transition comes after this activity. This activity does not specify any conditions by default.

You can add an error condition to this activity. The activity transitions through the error condition if the Notify number used to make the call is not configured correctly or unable to send SMS messages, or if an error occurs while sending the SMS.

**Queue workflow activity**

The Queue activity places an active Notify call in a queue.
Add the **Queue** activity to a workflow on the Notify Call (notify_call) table to put the current call on hold. This activity does not specify any input variables. The queue that the call is added to is given a random ID.

**Workflow notification activities**

Notification workflow activities notify users of events that occur during the workflow.

**Create Event workflow activity**

The **Create Event** activity adds an event to the event queue, but does not immediately fire the event.

The event processor typically processes the event within one minute. This activity triggers any business rules or email notifications that would normally be triggered by the event.

**Results**

**Finished:** the activity added the event to the event queue.

**Input variables**

**Create Event activity input variables**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event name</td>
<td>The name of the event to create. From the Event Name lookup list, select the event to add to the queue. If the event requires parameters, specify them in the Parameter script field.</td>
</tr>
<tr>
<td>Parameter 1</td>
<td>The first parameter of the event.</td>
</tr>
<tr>
<td>Parameter 2</td>
<td>The second event parameter.</td>
</tr>
</tbody>
</table>

**Note:** If this parameter is a string value, it must be within quotes (" ").

**Notification workflow activity**

The **Notification** activity sends an email or SMS message to specified users or groups.

**Input variables**

**Notification activity input variables**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Addressees</td>
<td>The users who will be recipients of the email.</td>
</tr>
</tbody>
</table>
### States

The activity state tells the workflow engine what to do with the activity.

**Notification activity states**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executing</td>
<td>The workflow engine knows to start the <code>run</code> function of the activity.</td>
</tr>
<tr>
<td>Finished</td>
<td>The activity finished running. See the result value for the outcome of the activity.</td>
</tr>
<tr>
<td>Cancelled</td>
<td>This activity, or the workflow that contains this activity, was canceled.</td>
</tr>
</tbody>
</table>

**Timer workflow activities**

Timer activities pause workflows for set periods of time.

**SLA Percentage Timer workflow activity**

The **SLA Percentage Timer** activity pauses the workflow for a duration equal to a percentage of an SLA.

A workflow must run on the Task SLA table to use this activity.

### Results

**SLA Percentage Timer activity results**

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete</td>
<td>The activity successfully reached the specified duration</td>
</tr>
</tbody>
</table>
### Input variables

Input variables determine the initial behavior of the activity.

**SLA Percentage Timer activity input variables**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percentage</td>
<td>The duration to pause the workflow for, as a percentage of the current SLA</td>
</tr>
</tbody>
</table>

### States

The activity state tells the workflow engine what to do with the activity.

**SLA Percentage Timer states**

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executing</td>
<td>The activity is in this state very briefly while initializing, after which it immediately changes to Waiting.</td>
</tr>
<tr>
<td>Waiting</td>
<td>The workflow engine waits until the SLA reaches the specified percentage. The engine then transitions the workflow to the next activity.</td>
</tr>
<tr>
<td>Finished</td>
<td>The activity finished running. See the result value for the outcome of the activity.</td>
</tr>
<tr>
<td>Cancelled</td>
<td>This activity, or the workflow that contains this activity, was canceled.</td>
</tr>
<tr>
<td>Error</td>
<td>A JavaScript error occurred. Review the logs for error details.</td>
</tr>
</tbody>
</table>

**Timer workflow activity**

The Timer activity pauses the workflow for a specified period of time.

This duration can be an absolute time value or a relative value based on a defined schedule. It is best to adjust the Duration so the workflow can progress in a timely manner. To pause a workflow indefinitely until a condition is met, see wait for condition.
Results

Timer activity results

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete</td>
<td>The activity successfully reached the specified duration.</td>
</tr>
<tr>
<td>Cancelled</td>
<td>The activity or workflow was canceled before the timer reached the specified duration.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.

Timer activity input variables

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timer Information</td>
<td>How the timer duration is computed. The options are:</td>
</tr>
<tr>
<td>Timer based on</td>
<td>• A user specified duration: The duration is based on the Duration fields, such as days and hours.</td>
</tr>
<tr>
<td></td>
<td>• A relative duration: The duration is based on the Relative duration (such as End of Next Business Day) and Wait fields.</td>
</tr>
<tr>
<td></td>
<td>• A date/time or duration field: The duration is based on the Field value and the Wait field.</td>
</tr>
<tr>
<td></td>
<td>• Script: The duration is based on a script that returns the number of seconds.</td>
</tr>
<tr>
<td>Duration</td>
<td>The specific number of days and hours to wait before proceeding to the next activity in the workflow.</td>
</tr>
<tr>
<td>Relative duration</td>
<td>The general number and length of business days to wait before progressing to the next workflow activity.</td>
</tr>
<tr>
<td>Wait</td>
<td>An additional timer adjustment when Timer based on is A relative duration or A date/time or duration field. The options are:</td>
</tr>
<tr>
<td></td>
<td>• The full duration: No modification of the calculated duration.</td>
</tr>
<tr>
<td></td>
<td>• A % of the duration: The duration is adjusted by multiplying the number of seconds by the (Percentage / 100).</td>
</tr>
<tr>
<td></td>
<td>• Some time before: The duration is shortened by the Time before days and hours.</td>
</tr>
<tr>
<td></td>
<td>• Some time after: The duration is lengthened by the Time after days and hours.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Percentage</td>
<td>The Wait percentage value when Timer based on is A relative duration or A date/time or duration field.</td>
</tr>
<tr>
<td>Time before</td>
<td>The modifier time value when Wait is Some time before.</td>
</tr>
<tr>
<td>Time after</td>
<td>The modifier time value when Wait is Some time after.</td>
</tr>
<tr>
<td>Field</td>
<td>The date/time or duration field that contains the elapsed wait-time before moving to the next workflow activity.</td>
</tr>
<tr>
<td>Script</td>
<td>The script that sets 'answer' to the number of seconds for the duration.</td>
</tr>
</tbody>
</table>
| Timer Schedule                    | The basic schedule the timer uses to count working hours. If a schedule is specified, the duration will only be considered for times that are specified on the schedule. For example, if the duration is 2 hours and the workflow begins at 4:00pm on a schedule that is 8am - 5pm, then it ends at 9:00am the next day. The options are:  
  - This workflow's schedule: The schedule uses workflow context date, time, and an optional Time zone based on value.  
  - A specific schedule: The schedule uses a pre-defined Schedule and an optional Time zone based on value.  
  - A schedule field: The schedule uses a value from a table and an optional Time zone based on value. |
| Schedule                          | The pre-defined Schedule from a list.                                                                                                       |
| Schedule field                    | A date and time or duration field for the schedule, that is associated with the table. Valid fields appear in blue on the Select the element from a tree dialog. |
### States

The activity state tells the workflow engine what to do with the activity.

#### Timer activity states

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executing</td>
<td>The Timer activity is in this state very briefly while initializing, after which it immediately changes to Waiting.</td>
</tr>
<tr>
<td>Waiting</td>
<td>The workflow engine waits until the timer reaches the specified duration. The engine then transitions the workflow to the next activity.</td>
</tr>
<tr>
<td>Finished</td>
<td>The activity finished running. See the result value for the outcome of the activity.</td>
</tr>
<tr>
<td>Cancelled</td>
<td>This activity, or the workflow that contains this activity, was canceled.</td>
</tr>
<tr>
<td>Error</td>
<td>A JavaScript error occurred. Review the logs for error details.</td>
</tr>
</tbody>
</table>

### Example

You can use a Timer activity to pause the workflow until the end of the business day.
Timer example

In this example, the script evaluates the time between the `now` variable and the `eod` variable. The `eod` variable is defined, in 24 hour time, as 4:00 PM. The script then sets the `answer` variable to the difference between these variables, in seconds, and logs a message.

```javascript
// get now and calc end of day (4:00pm)
var now = new Date();
var eod = new Date();
eod.setHours(16);
eod.setMinutes(0);
eod.setSeconds(0);
answer = (eod.getTime() - now.getTime())/1000;
```
Task workflow activities

Task activities create and modify workflow tasks. Task activities are only available when the workflow runs on a table that extends Task.

Add Worknote workflow activity

The Add Worknote activity adds text to the Worknotes field of the current incident record. A workflow must run on the Incident table to use this activity.

Input variables

Add Worknote activity input variables

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work Note</td>
<td>The text to add to the incident record.</td>
</tr>
</tbody>
</table>

Attachment Note workflow activity

The Attachment Note activity adds an attachment to the current record.

Note: This activity is only available when the workflow runs on a table that extends Task.

This activity allows the use of irregular HTML tags to reference attachments, specifically the [code] tag. Entries in a journal field that use irregular HTML do not work if the glide.ui.allow_deep_html_validation property is true. This property is set to false by default.

Results

- **Finished**: the activity added the attachment to the record.

Input variables

The following variables determine the behavior of the activity.

Attachment Note activity input variables

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>When this activity runs, it makes a note on the current record that a file has been attached. Specify the field on the current record in which you want this note to appear. The options are:</td>
</tr>
<tr>
<td>Field</td>
<td></td>
</tr>
<tr>
<td>none</td>
<td>(defaults to Work Notes)</td>
</tr>
<tr>
<td>Additional Comments</td>
<td></td>
</tr>
<tr>
<td>Work notes</td>
<td></td>
</tr>
</tbody>
</table>
### Attachment Name

When this activity runs, it creates a .txt file with the name you specify in this field.

### Attachment Data

The content of the .txt file attachment. It can be in plain text or use variables to extract specific data from a table.

---

**Catalog Task workflow activity**

The **Catalog Task** activity creates a service catalog task record.

**Note:** This activity is only available when the workflow runs on a table that extends Task.

A user must complete the catalog task. This activity is available only for workflows running on the Catalog Request Item (sc_req_item) table.

### Results

You can assign a result value using `activity.result` from within a script field of the activity. The final **State** value of the catalog task record determines the result value for the **Create Task** activity. Possible result values are:

- Closed complete
- Closed incomplete
- Closed skipped
- Deleted
- Cancelled

### Input fields

The values you enter in the following fields determine the behavior of the activity.

**Catalog task activity information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalog Task Activity Settings</td>
<td>The following fields specify the behavior of the Catalog Task Activity.</td>
</tr>
<tr>
<td>Task Table</td>
<td>The table on which this activity runs. In most cases, leave set to the default value: (sc_req_item).</td>
</tr>
<tr>
<td>Priority</td>
<td>The value you want assigned to the <strong>Priority</strong> field for the new task.</td>
</tr>
<tr>
<td>Wait for completion</td>
<td>If selected, the workflow activity waits for the task to complete before continuing. If cleared, the task is created but the workflow proceeds.</td>
</tr>
</tbody>
</table>

Catalog Task Record Settings

The following fields specify the field values that this activity sets for the catalog task it creates.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task value from</td>
<td>Specify how you want to populate fields on the new task.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Fields</strong>: a predefined set of fields including Fulfillment group, Assigned to, Short description and Instructions.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Template</strong>: an existing template for the selected task table.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Values</strong>: values that you specify using a Set Values widget.</td>
</tr>
<tr>
<td></td>
<td>After you select a value for Task value from, additional fields specific to that value appear on the form.</td>
</tr>
<tr>
<td>Fulfillment group</td>
<td>The group that is responsible for completing the task. Populates the Assignment group field on the new task.</td>
</tr>
<tr>
<td>Only appears when Task value from is set to Fields</td>
<td></td>
</tr>
<tr>
<td>Assigned to</td>
<td>The user who is responsible for completing the task. Populates the Assignment to field on the new task.</td>
</tr>
<tr>
<td>Only appears when Task value from is set to Fields</td>
<td></td>
</tr>
<tr>
<td>Short description</td>
<td>A short description for the task. Populates the Short description field on the new task.</td>
</tr>
<tr>
<td>Only appears when Task value from is set to Fields</td>
<td></td>
</tr>
<tr>
<td>Instructions</td>
<td>The task instructions for the user to complete prior to closing the task. Populates the Description field on the new task.</td>
</tr>
<tr>
<td>Only appears when Task value from is set to Fields</td>
<td></td>
</tr>
<tr>
<td>Template</td>
<td>The values in the task will be populated from the values in the template you select.</td>
</tr>
<tr>
<td>Only appears when Task value from is set to Template</td>
<td></td>
</tr>
<tr>
<td>SetValues</td>
<td>Select any field on the task record to a value you specify here.</td>
</tr>
<tr>
<td>Only appears when Task value from is set to Values</td>
<td></td>
</tr>
<tr>
<td>Advanced</td>
<td>Check Advanced if you want to use a script to assign values on the catalog task. When you check Advanced, a text box appears where you can enter your script.</td>
</tr>
<tr>
<td>Advanced Script</td>
<td>Set additional values for the task in this script. This script is run after the task values are set using the Fields, Template or Values you have specified.</td>
</tr>
<tr>
<td>Only appears when the Advanced field is checked</td>
<td></td>
</tr>
<tr>
<td>Catalog Task Variables</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Variables on Task Form</td>
<td>Specify optional catalog variables to include on the Catalog task form. The variables you select here will be displayed in a field called [Variable Editor](https:// servicenow.com). If you select no variables here, the Variable Editor field in the Catalog Task form will not be visible.</td>
</tr>
<tr>
<td><strong>Catalog Task Schedule</strong></td>
<td></td>
</tr>
<tr>
<td>Due date based on</td>
<td>Select how workflow determines the task's duration, due date, and schedule.</td>
</tr>
<tr>
<td>· A user specified duration</td>
<td>The duration is based on a user specified value.</td>
</tr>
<tr>
<td>· A relative duration</td>
<td>The duration is calculated from a relative duration (such as End of Next Business Day).</td>
</tr>
<tr>
<td>· A date/time or duration field</td>
<td>The duration is based on the value of a field on the current record.</td>
</tr>
<tr>
<td>· Script</td>
<td>The duration is returned by a script.</td>
</tr>
<tr>
<td>Duration</td>
<td>The specific number of days and hours.</td>
</tr>
<tr>
<td>Only appears when <strong>Due date based on</strong> is set to A user specified duration</td>
<td></td>
</tr>
<tr>
<td>Relative duration</td>
<td>The general number and length of business days.</td>
</tr>
<tr>
<td>Only appears when <strong>Due date based on</strong> is set to A relative duration</td>
<td></td>
</tr>
<tr>
<td>Due date field</td>
<td>The date/time or duration field.</td>
</tr>
<tr>
<td>Only appears when <strong>Due date based on</strong> is set to A date/time or duration field</td>
<td></td>
</tr>
<tr>
<td>Due date script</td>
<td>The script that sets 'answer' to the number of seconds for the duration.</td>
</tr>
<tr>
<td>Only appears when <strong>Due date based on</strong> is set to Script</td>
<td></td>
</tr>
<tr>
<td>Schedule based on</td>
<td>The basic schedule the timer uses to count working hours. If a schedule is specified, the duration will only be considered for times that are specified on the schedule. For example, if the duration is 2 hours and the workflow begins at 4:00pm on a schedule that is 8am - 5pm, then it ends at 9:00am the next day. The options are:</td>
</tr>
<tr>
<td>· This workflow's schedule</td>
<td>The schedule uses workflow context date, time, and an optional <a href="https://servicenow.com">Time zone based on value</a>.</td>
</tr>
<tr>
<td>· A specific schedule</td>
<td>The schedule uses a pre-defined <a href="https://servicenow.com">Schedule</a> and an optional <a href="https://servicenow.com">Time zone based on value</a>.</td>
</tr>
<tr>
<td>· A schedule field</td>
<td>The schedule uses a value from a table and an optional <a href="https://servicenow.com">Time zone based on value</a>.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Schedule</td>
<td>The predefined Schedule from a list.</td>
</tr>
<tr>
<td>Schedule field</td>
<td>A date and time or duration field for the schedule, that is associated with the table. Valid fields appear in blue on the Select the element from a tree dialog.</td>
</tr>
<tr>
<td>Time zone based on</td>
<td>The time zone for calculating the duration. The time zone may be based on:</td>
</tr>
<tr>
<td></td>
<td>· No time zone: Default. Workflow uses the GMT time zone.</td>
</tr>
<tr>
<td></td>
<td>· A specific time zone: A specific Time zone that you choose from a choice list.</td>
</tr>
<tr>
<td></td>
<td>· A time zone field: A Time zone field to track time duration from a field on the form.</td>
</tr>
<tr>
<td>Time zone</td>
<td>Select the time zone you want from the choice list.</td>
</tr>
<tr>
<td>Time zone field</td>
<td>A date and time or duration field for the schedule, that is associated with the table. Valid fields appear in blue on the Select the element from a tree dialog.</td>
</tr>
</tbody>
</table>

**States**

The activity state tells the workflow engine what to do with the activity.

**Catalog Task activity states**

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executing</td>
<td>The workflow engine knows to start the onExecute function of the activity.</td>
</tr>
<tr>
<td>Waiting</td>
<td>The workflow engine ignores the activity until a specific event to restart the activity is fired.</td>
</tr>
<tr>
<td>Finished</td>
<td>The activity finished running. See the result value for the outcome of the activity.</td>
</tr>
<tr>
<td>Cancelled</td>
<td>This activity, or the workflow that contains this activity, was canceled.</td>
</tr>
<tr>
<td>Error</td>
<td>A JavaScript error occurred. Review the logs for error details.</td>
</tr>
</tbody>
</table>

**Create Task workflow activity**

The Create Task activity generates a record on any of the tables that extend Task (task).

**Note:** This activity is only available when the workflow runs on a table that extends Task.
If the **Wait for completion** check box is selected, the workflow context waits for a user action on the task, such as Complete or Incomplete, and then progresses based on the user action.

**Results**

You can assign a result value using `activity.result` from within a script field of the activity. By default, the final **State** value of the task record determines the result value for the **Create Task** activity. Possible result values are:

- Closed complete
- Closed incomplete
- Closed skipped
- Deleted
- Cancelled

**Input variables**

The following variables determine the behavior of the activity.

**Create Task activity input variables**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Task Activity Settings</td>
<td>The following fields specify the behavior of the Create Task Activity.</td>
</tr>
<tr>
<td>Task type</td>
<td>The type of task to create. Select from the corresponding task table for the workflow.</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority that is assigned to the task.</td>
</tr>
<tr>
<td>Wait for completion</td>
<td>If selected, the workflow activity waits for the task to complete before continuing. If cleared, the task is created but the workflow proceeds.</td>
</tr>
<tr>
<td>Create Task Record Settings</td>
<td>The following fields specify the field values that this activity sets for the task it creates.</td>
</tr>
<tr>
<td>Task values from</td>
<td>The values used to create the task may either come from:</td>
</tr>
<tr>
<td>Fulfillment group</td>
<td>The group that is responsible for completing the task. Populates the Assignment group field on the new task.</td>
</tr>
<tr>
<td>Assigned to</td>
<td>The user who is responsible for completing the task. Populates the Assignment to field on the new task.</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>
<tbody>
<tr>
<td>Short description</td>
<td>A short description for the task. Populates the Short description field on the new task.</td>
</tr>
<tr>
<td>Instructions</td>
<td>The task instructions for the user to complete prior to closing the task. Populates the Description field on the new task.</td>
</tr>
<tr>
<td>Task template</td>
<td>A template that is used to fill in values for the task.</td>
</tr>
<tr>
<td>Set values</td>
<td>A widget that is used to specify values for any fields of the task.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Check Advanced if you want to use a script to assign values on the catalog task. When you check Advanced, a text box appears where you can enter your script.</td>
</tr>
<tr>
<td>Advanced Script</td>
<td>Set additional values for the task in this script. This script is run after the task values are set using the Fields, Template or Values you have specified. Use the variable task when setting additional values, for example:</td>
</tr>
<tr>
<td>Task Schedule</td>
<td>Select how workflow determines the task's duration, due date, and schedule.</td>
</tr>
<tr>
<td>Due date based on</td>
<td>• A user specified duration: The duration is based on a user specified value.</td>
</tr>
<tr>
<td></td>
<td>• A relative duration: The duration is calculated from a relative duration (such as End of Next Business Day).</td>
</tr>
<tr>
<td></td>
<td>• A date/time or duration field: The duration is based on the value of a field on the current record.</td>
</tr>
<tr>
<td></td>
<td>• Script: The duration is returned by a script.</td>
</tr>
<tr>
<td>Duration</td>
<td>The specific number of days and hours.</td>
</tr>
<tr>
<td>Relative duration</td>
<td>The general number and length of business days.</td>
</tr>
<tr>
<td>Due date field</td>
<td>The date/time or duration field.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Due date script</td>
<td>The script that sets 'answer' to the number of seconds for the duration.</td>
</tr>
<tr>
<td>Schedule based on</td>
<td>The basic schedule the timer uses to count working hours. If a schedule is specified, the duration will only be considered for times that are specified on the schedule. For example, if the duration is 2 hours and the workflow begins at 4:00pm on a schedule that is 8am - 5pm, then it ends at 9:00am the next day. The options are:</td>
</tr>
<tr>
<td>Schedule</td>
<td>The predefined Schedule from a list.</td>
</tr>
<tr>
<td>Schedule field</td>
<td>A date and time or duration field for the schedule, that is associated with the table. Valid fields appear in blue on the Select the element from a tree dialog.</td>
</tr>
<tr>
<td>Time zone based on</td>
<td>The time zone for calculating the duration. The time zone may be based on:</td>
</tr>
<tr>
<td>Time zone</td>
<td>Select the time zone you want from the choice list.</td>
</tr>
<tr>
<td>Time zone field</td>
<td>A date and time or duration field for the schedule, that is associated with the table. Valid fields appear in blue on the Select the element from a tree dialog.</td>
</tr>
</tbody>
</table>

**States**

The activity state tells the workflow engine what to do with the activity.
Create Task activity states

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executing</td>
<td>The workflow engine knows to start the <code>onExecute</code> function of the activity.</td>
</tr>
<tr>
<td>Waiting</td>
<td>The workflow engine ignores the activity until a specific event to restart the activity is fired.</td>
</tr>
<tr>
<td>Finished</td>
<td>The activity finished running. See the result value for the outcome of the activity.</td>
</tr>
<tr>
<td>Cancelled</td>
<td>This activity, or the workflow that contains this activity, was canceled.</td>
</tr>
<tr>
<td>Error</td>
<td>A JavaScript error occurred. Review the logs for error details.</td>
</tr>
</tbody>
</table>

Utility workflow activities

Utility activities provide controls over the path of the workflow, and other useful tools.

**Branch workflow activity**

The *Branch* activity splits the workflow into multiple transition paths from a single activity.

To add a transition path, drag the *Branch* activity onto the canvas. When the Branch activity properties form displays, click `Submit` to add the activity to the canvas. Once the activity is on the canvas, right click in the activity body, then click `Add Condition`.

All transitions from this activity execute concurrently. This activity provides a single *Always* condition. You can draw any number of transitions from this condition. Using this activity is equivalent to drawing multiple transitions from a single condition of another activity.

Branching can affect the behavior of rollback activities. See *Rollback To activity* for more information.

**Join workflow activity**

The *Join* activity unites multiple execution paths into one transition.

Use this activity to cause a workflow to wait for all activities in multiple paths to finish before continuing. If multiple concurrent workflow paths meet without a *Join* activity, any subsequent activities execute twice.

To add Join to the canvas, click `Submit`. On the canvas, connect incoming transitions from each activity you want to act as a predecessor to the Join activity. Then connect outgoing transitions to the two exit conditions: Complete and Incomplete.

Results

Provide an Incomplete transition out of a *Join* whenever it is possible for any predecessor activities to follow a transition path that does not lead to the *Join* activity.

**Join activity results**

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete</td>
<td><em>Join</em> exits along the Complete path when the system has determined that all predecessor activities have completed and transitioned to the <em>Join</em>.</td>
</tr>
<tr>
<td>Result</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Incomplete</td>
<td>Join exits along the Incomplete path when the system determines that at least one predecessor activity completed but transitioned along a path that bypassed the Join activity.</td>
</tr>
</tbody>
</table>

**Lock workflow activity**

The **Lock** activity prevents other instances of this workflow from continuing past this activity until the lock is released.

Several instances of the same workflow may run concurrently. For example, if a workflow is triggered when a record is added to a particular table and multiple records are added one after the other, that workflow will be triggered multiple times: once by each record insertion. In such cases, you can use the lock activity to ensure that this instance of the workflow has completely finished one or more activities before any other instance of the workflow can proceed.

A workflow can explicitly release a lock with the **Unlock** activity. The lock may also be released when the **Max duration** is reached.

When an instance of the workflow reaches the **Lock** activity, it attempts to obtain a lock using the key specified in the lock activity. If another instance has already obtained the lock and has not yet released it, this lock attempt fails. The instance continues trying to obtain the lock until **Max attempts** has been reached.

---

**Note:**

We recommend placing a one-second timer activity before the lock activity. This helps prevent a rare condition in which the lock activity may not be able to distinguish one workflow instance from another. This condition can occur because the entity owning the lock is not the specific workflow instance, but rather the code-execution thread in which that instance is running. In most cases, each workflow instance runs on a different thread, but adding a timer activity ensures that this is the case.
Example of Lock Activity Preceded by Timer Activity

Since a **Lock** activity can only temporarily prevent processing of other workflow instances, do not add activities that cause the workflow to wait between a **Lock** and **Unlock** activity block. This
may cause the **Unlock** activity to be unable to acquire the lock to release it and instead take 60 seconds to complete. Restricted wait activities include:

- Approval activities
- Task activities
- Timer activities
- Wait for condition activity
- Wait for WF Event activity

**Results**

**Lock activity results**

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The activity successfully obtained a lock. This instance of the workflow can proceed past this point, but other instances cannot until the lock is released.</td>
</tr>
<tr>
<td>Failure</td>
<td>After attempting to obtain the lock <strong>Max attempts</strong> times, the activity could not obtain the lock.</td>
</tr>
</tbody>
</table>

**Input variables**

Input variables determine the initial behavior of the activity.

**Lock activity input variables**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>A unique mutex key. The <strong>Unlock activity</strong> activity uses this key to release the lock.</td>
</tr>
<tr>
<td>Duration</td>
<td>The maximum time the lock persists. The lock is released after it reaches this duration. Releasing a lock this way is equivalent to running the <strong>Unlock activity</strong>.</td>
</tr>
<tr>
<td>Max. duration</td>
<td>The maximum time the lock persists. The lock is released after it reaches this duration. Releasing a lock this way is equivalent to running the <strong>Unlock activity</strong>.</td>
</tr>
<tr>
<td>Lock attempts</td>
<td>Specify how the activity behaves if the lock attempt is denied. If the final lock attempt fails, the activity state will be set to 'timeout' and the activity result will be set to 'failed'.</td>
</tr>
<tr>
<td>Max. attempts</td>
<td>Specify the maximum number of times the activity may attempt to obtain the lock.</td>
</tr>
<tr>
<td>Delay between attempts</td>
<td>The amount of time required after a failed lock attempt before another lock attempt is allowed.</td>
</tr>
</tbody>
</table>

**States**

The activity state tells the workflow engine what to do with the activity.
Lock activity states

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Waiting</td>
<td>The workflow engine is waiting to obtain a lock.</td>
</tr>
<tr>
<td>Finished</td>
<td>The activity successfully obtained the lock.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The activity could not obtain a lock within the number of attempts specified by the Max. attempts input variable.</td>
</tr>
</tbody>
</table>

Log Message workflow activity
The Log Message activity writes a message to the workflow log.

Use this activity to add entries to the workflow’s log for debugging or tracing purposes.

Input variables

Input variables determine the initial behavior of the activity.

Log Message activity input variables

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message</td>
<td>The message to log. This variable can be a string or a JavaScript expression that evaluates to a string.</td>
</tr>
</tbody>
</table>

Log Trace Message workflow activity
The Log Trace Message activity writes a trace message to the workflow log.

The trace message includes the activity name, the event that invoked the workflow, and the table of the current record. There are no variables or conditions. To log other data, use the Log Message workflow activity activity.

REST Message legacy workflow activity
The legacy REST Message activity enables an administrator to override the REST endpoint or supply the variables configured in the REST Message module.

This activity is deprecated in the Jakarta release and no longer shows up in the Workflow canvas for new workflow development. New workflows should use the Orchestration REST Activity templates instead.

Existing workflows using it will continue to work as designed. To edit this activity in an existing workflow, you must re-activate the activity.

The REST Message activity executes a dead link REST function (POST, PUT, GET, or DELETE) on an endpoint using values defined in the function record.

**Note:** If you want to use a MID Server to send the REST message, the MID Server must be accessible by the instance and configured to use SSH.
## Input variables

**REST Message activity input variables**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rest Message</td>
<td>Name of the <em>REST message</em> to run. This is a reference field to the REST Message (sys_rest_message) table (<em>System Web Services</em> &gt; <em>Outbound</em> &gt; <em>REST Message</em>).</td>
</tr>
<tr>
<td>REST Message Function</td>
<td>Function to call that is defined in a REST message function. This is a reference field to the HTTP Method (sys_rest_message_fn) table (<em>System Web Services</em> &gt; <em>Outbound</em> &gt; <em>REST Message</em>). You can edit functions in the <em>HTTP Methods</em> related list in each REST Message record.</td>
</tr>
<tr>
<td>REST Endpoint</td>
<td>REST endpoint to use instead of the <em>Endpoint</em> defined in the HTTP Method record. Leave this field blank to use the defined endpoint in the REST Message Function record.</td>
</tr>
</tbody>
</table>
| Rest Message Variables        | Values to use for *variables* defined in the HTTP Method record. Use the following format for the string: \n
```
name1=value1, name2=value2, ...
```

For example, use `name=${nameValue}, id=${idValue}` where name and id are function variables. If either the variable name or value contains a comma or equal sign, escape those characters with a backslash. |
| Use MID Server                | Check this box if you want to use a MID Server to send the REST message. A MID Server might be necessary to reach an endpoint within a firewall or a subnetwork that is not visible from the instance. If this check box is selected, but no MID Server is defined in the *MID Server* field, the workflow automatically attempts to find a MID Server based on IP range and the REST capability. |
| MID Server                    | Name of the MID Server to use. This field is available when *Use MID Server* is selected. The workflow ignores this parameter if the *use_midserver* parameter is disabled.                                                                                                                       |
| Rest Message Script           | The script to execute after the request has been made and a response has been received. You can access the full response body from the *activity.output* variable.                                                                                                                               |
Return Value workflow activity
The **Return Value** activity returns a value to a parent workflow, when run from a subflow.
This activity has no variables or conditions. For more information, see [Workflows used as subflows](https://servicenow.com). Use this activity within a subflow to store data that the parent flow can access. The **Return Value** activity adds the data from the subflow's `value` variable to the parent workflow's scratchpad.

**Scratchpad entries**

The activity uses the workflow scratchpad to read and write persistent values.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>The activity writes the value from the subflow <code>value</code> variable to the parent scratchpad. The parent workflow activity that runs the subflow includes a Map return value to variable that defines where the parent workflow stores the returned data. This data can be scalar, a stringifiable JavaScript object, or an expression that evaluates to a stringifiable JavaScript object.</td>
</tr>
</tbody>
</table>

---

Run Script workflow activity
The **Run Script** activity runs the specified script in the scope of the workflow version.

**Note:** All changes to `current` are automatically updated. There is no need to call `current.update()`

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Script</td>
<td>Script to execute.</td>
</tr>
</tbody>
</table>

Set Values workflow activity
The **Set Values** activity sets values on the current record when the workflow quiesces or ends.

**Input Fields**

The values you enter in the following fields determine the behavior of the activity.
Set Values Activity Input Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set these values</td>
<td>From the list on the left, select the field on the current record whose value you want to set when the workflow quiesces or ends. In the user-input field to the right, select or enter the value to which you want that field set.</td>
</tr>
</tbody>
</table>

**Note:** Avoid setting the same fields from different Set Value activities. The workflow only sets the value specified by the last Set Values activity run before quiescing or ending.

**Note:** Using the Set Values activity to set the Approval field on a task does not cancel pending approvals. To approve a task in a workflow, use the Approval Action activity instead.

**SOAP Message legacy workflow activity**

The legacy SOAP Message activity uses SOAP messages defined in the System Web Services plugin and can call the messages using a MID Server. This activity is deprecated in the Jakarta release and no longer shows up in the Workflow canvas for new workflow development. New workflows should use the Orchestration SOAP Activity templates instead.

Existing workflows using it will continue to work as designed. To edit this activity in an existing workflow, you must re-activate the activity.

**Input variables**

**SOAP Message activity input variables**

<table>
<thead>
<tr>
<th>Field</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOAP Message</td>
<td>soap_message</td>
<td>The SOAP Message defined under the System Web Services plugin's Outbound SOAP Message (sys_soap_message) table. (<a href="#">System Web Services &gt; Outbound &gt; SOAP Message</a>)</td>
</tr>
<tr>
<td>SOAP Message Function</td>
<td>soap_message_function</td>
<td>The function to call that is defined in the SOAP Message. Functions are listed in the SOAP Message Functions related list in each SOAP Message record.</td>
</tr>
<tr>
<td>SOAP Endpoint</td>
<td>soap_endpoint</td>
<td>Endpoint to use instead of the SOAP endpoint value in the SOAP Message Function record. Leave this field blank to use the defined endpoint in the SOAP Message Function record.</td>
</tr>
<tr>
<td>Field</td>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Variables</td>
<td>variables</td>
<td>Variables to substitute into the SOAP Envelope defined in the SOAP Message Function record. Use this format for the string: name1=value1, name2=value2, ... If either the name or value contains a comma or equal sign, escape these characters with a backslash.</td>
</tr>
<tr>
<td>Use MID Server</td>
<td>use_midserver</td>
<td>Check box for using a MID Server to send the SOAP message. A MID Server might be necessary to reach an endpoint within a firewall or a sub-network that is not visible from the instance. If this check box is selected (true), but no MID Server is defined in the MID Server field, Workflow automatically attempts to find a MID Server.</td>
</tr>
<tr>
<td>MID Server</td>
<td>midserver</td>
<td>Name of the MID Server to use. This field appears when you select the Use MID Server check box. The workflow ignores this parameter if the use_midserver parameter is disabled.</td>
</tr>
<tr>
<td>Sensor Script</td>
<td>sensor_script</td>
<td>The script to execute after the request has been made and a response has been received. You can access the full XML response body from the activity.output object.</td>
</tr>
</tbody>
</table>

**Turnstile workflow activity**

The **Turnstile** activity limits how many times a workflow can pass through the same point. Use this activity to prevent infinite loops. This activity is useful alongside the **Rollback To workflow activity**.

**Results**

You can assign a result value using the activity.result variable from within a script field of the activity. By default, the activity script evaluates if the activity should continue to iterate or stop.

**Turnstile activity results**

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continue</td>
<td>The <strong>Allowed iterations</strong> value is greater than the number of times the workflow accessed this activity.</td>
</tr>
</tbody>
</table>
### Result

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cancel</td>
</tr>
</tbody>
</table>

### Input variables

Input variables determine the initial behavior of the activity.

**Turnstile activity input variables**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allowed iterations</td>
<td>Number of times the workflow can pass through this activity before the turnstile ends the loop.</td>
</tr>
</tbody>
</table>

### Conditions

The conditions determine which transition comes after this activity.

**Turnstile activity conditions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continue</td>
<td>If the workflow has returned to this point an amount of times less than the allowed iteration.</td>
</tr>
<tr>
<td>Cancel</td>
<td>If the workflow has returned to this point an amount of times more than the allowed iteration.</td>
</tr>
</tbody>
</table>

### States

The activity state tells the workflow engine what to do with the activity.

**Turnstile activity states**

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executing</td>
<td>The workflow engine knows to start the <code>onExecute</code> function of the activity.</td>
</tr>
<tr>
<td>Waiting</td>
<td>The workflow engine ignores the activity until a specific event to restart the activity is triggered.</td>
</tr>
<tr>
<td>Finished</td>
<td>The activity finished running. See the result value for the outcome of the activity.</td>
</tr>
<tr>
<td>Cancelled</td>
<td>This activity, or the workflow that contains this activity, was canceled.</td>
</tr>
<tr>
<td>Error</td>
<td>A JavaScript error occurred. Review the logs for error details.</td>
</tr>
</tbody>
</table>

**Unlock workflow activity**

The **Unlock** activity releases a lock that was previously placed by the **Lock** activity.
To release a lock, specify the same lock key that was specified in the **Lock** activity. If the **Lock** activity had a **Duration** specified, and that duration has already passed, the lock will already be released.

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th><strong>Unlock activity input variables</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>Lock key</td>
</tr>
</tbody>
</table>

**States**

The activity state tells the workflow engine what to do with the activity.

<table>
<thead>
<tr>
<th><strong>Unlock activity states</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>State</strong></td>
</tr>
<tr>
<td>Finished</td>
</tr>
</tbody>
</table>

**Subflow activities in workflow**

Subflow activities run and manage workflows from a parent workflow.

The **Parallel Flow Launcher** subflow activity is available.

*Parallel Flow Launcher workflow activity*

The **Parallel Flow Launcher** activity launches multiple subflows in parallel.

Workflows running in parallel execute simultaneously and may complete in any order. The activity can launch a single subflow or multiple subflows as needed. You can manage the input values and values returned for each subflow.

**Note:** The Parallel Flow Launcher activity waits until all subflows are completed before proceeding. If any subflow does not finish, the activity waits indefinitely.

**Note:** Do not launch a large number of subflows with the Parallel Flow Launcher activity. If overused, this activity can overburden the instance. For launching very large numbers of subflows, consider putting the Parallel Flow Launcher inside a loop controlled by a turnstile or other conditional activity and having it do batches of no more than 500 at a time.

**Activity variables**

Activity variables determine the initial behavior of the activity.
Parallel Flow Launcher activity input variables

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parallel Flow Launcher configuration</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A unique name for the activity.</td>
</tr>
<tr>
<td>Stage</td>
<td>The stage to display when the workflow reaches the activity.</td>
</tr>
<tr>
<td>Inputs</td>
<td>Inputs to the subflows to run. Specify an array of name: value pairs for each input defined in the workflow being launched. The name and data type of each input variable entered must match those used by the subflow that this activity launches. For a detailed example, see <a href="#">Parallel Flow Launcher Example</a>.</td>
</tr>
<tr>
<td>Parallel Flow Launcher selection</td>
<td></td>
</tr>
<tr>
<td>Workflow</td>
<td>The workflow to run.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Check Advanced, to enter a script that uses a WorkflowCoordinator object to manage the subflows. When you check Advanced, a text box appears where you can enter a script that specifies a unique workflow for each set of input variables. See <a href="#">WorkflowCoordinator object</a> for more information.</td>
</tr>
<tr>
<td>Parallel Flow Launcher iteration</td>
<td>Specify parameters to tune the performance of batched workflows.</td>
</tr>
<tr>
<td>Count</td>
<td>If not specified by an input set, Count determines the number of subflows executed in parallel from this activity. If the Advanced option is not selected, ensure that this field is populated with a valid number.</td>
</tr>
<tr>
<td>Max flows</td>
<td>The maximum number of workflows this activity can launch. If this value is a positive integer, it overrides the max parameter used in the WorkflowCoordinator constructor.</td>
</tr>
<tr>
<td>Max simultaneous</td>
<td>The maximum number of parallel workflows this activity can run at one time. If this value is a positive integer, it overrides the poolsize parameter used in the WorkflowCoordinator constructor.</td>
</tr>
<tr>
<td>Parallel Flow Launcher Process</td>
<td></td>
</tr>
<tr>
<td>Process flow complete</td>
<td>To specify a script that runs after each subflow completes, check Process flow complete. If you check this field, a text box labelled Flow complete appears, where you can enter the script to run.</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>
<tbody>
<tr>
<td>Flow complete</td>
<td>The script that runs each time a subflow finishes. This field is available when the Process flow complete option is selected.</td>
</tr>
<tr>
<td></td>
<td>The same script functions and variables available in other workflow scripts, such as those in the Run Script activity, are available here. For more information, see Completed subflow values in scripts.</td>
</tr>
<tr>
<td></td>
<td>The variable “flow” is available to this script. It is an object that contains the following information about the flow that is finishing:</td>
</tr>
<tr>
<td></td>
<td><code>flow.output (String)</code>: The value that the subflow returns to the parent if it executed a Return Value activity before ending.</td>
</tr>
<tr>
<td></td>
<td><code>flow.index (Number)</code>: The zero-relative index of the subflow that finished.</td>
</tr>
<tr>
<td></td>
<td><code>flow.contextId (String)</code>: The sys_id of the workflow context for the completed subflow.</td>
</tr>
<tr>
<td></td>
<td><code>flow.inputs (Object)</code>: The inputs that were passed to the subflow when its context was created and started.</td>
</tr>
<tr>
<td></td>
<td><code>flow.status (String)</code>: The final state of the context. This corresponds to the state column in the subflow context record, which has possible values of executing, finished, cancelled, or faulted. (Since the flow is completed, it cannot be executing at this point.)</td>
</tr>
<tr>
<td>Parallel Flow Launcher Split</td>
<td></td>
</tr>
<tr>
<td>Process finished</td>
<td>To specify a script that runs after all subflows have finished, check Process finished. If you check this field, a text box labelled Finished Script appears where you can enter the script to run. The <code>coordinator</code> variable is made available to this script and is an object that allows access to any of the finished subflows using the getFlow(index) method. For example:</td>
</tr>
<tr>
<td></td>
<td>for (var i = 0; i &lt; coordinator.getNumFlows(); i++)</td>
</tr>
<tr>
<td></td>
<td>writeFlowResultsToTable( i, coordinator.getFlow(i) );</td>
</tr>
</tbody>
</table>
Finished script

The script that runs after all subflows launched by the activity are complete. You can use variables that contain completed flow information in this script.

The 'coordinator' variable is made available to this script and is an object that allows access to any of the finished subflows using the getFlow(index) method. For example:

```javascript
for (var i = 0; i < coordinator.getNumFlows(); i++)
    writeFlowResultsToTable( i, coordinator.getFlow(i) );
```

This field is available when Process finished is selected.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finished script</td>
<td>The script that runs after all subflows launched by the activity are complete. You can use variables that contain completed flow information in this script. The 'coordinator' variable is made available to this script and is an object that allows access to any of the finished subflows using the getFlow(index) method. For example:</td>
</tr>
</tbody>
</table>

### States

The activity state tells the workflow engine what to do with the activity. To view an activity’s state, point to the activity. A pop-up window shows the State and Result of the activity. If the activity is in an error state, the pop-up window provides a brief Fault Description.

#### Parallel Flow Launcher activity states

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Waiting</td>
<td>The activity is waiting for all subflows to finish. All subflows have started and some may have finished.</td>
</tr>
<tr>
<td>Finished</td>
<td>The activity successfully completed all of the subflows.</td>
</tr>
<tr>
<td>Error</td>
<td>The activity encountered an error.</td>
</tr>
</tbody>
</table>

### WorkflowCoordinator object

A WorkflowCoordinator object specifies which subflows to run and the input variables to pass to those subflows.

When using a WorkflowCoordinator object, you can create a Parallel Flow Launcher activity that launches multiple subflows. When using the activity without a WorkflowCoordinator object, you can only launch a single subflow multiple times. Use one of the following methods to specify a WorkflowCoordinator object for the activity when the Advanced activity input variable is selected.

- Reference a workflow scratchpad variable that contains an existing WorkflowCoordinator object. To save a WorkflowCoordinator object to the scratchpad, call the `save(variableName)` function on the WorkflowCoordinator object. You can reference the object using the value passed in the `variableName` parameter. For example, you can create a workflow scratchpad variable that contains an existing WorkflowCoordinator object in a Run Script activity, save the object using `<object>.save('coord')`, and then call this object by entering `coord` in the Workflow activity variable of a subsequent Parallel Flow Launcher activity.
- Define the WorkflowCoordinator within the Workflow activity variable. Add the `javascript:` identifier at the beginning of the script. The Parallel Flow Launcher example shows how to use a WorkflowCoordinator object in this way.
- Create a factory class to define the WorkflowCoordinator object. The system does not provide a factory class for WorkflowCoordinator by default.

Completed subflow values in scripts

The Parallel Flow Launcher activity exposes additional variables you can use in scripts.

Additional variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>coordinator</td>
<td>The WorkflowCoordinator used when running the subflows. You can use this variable in the Finished script to perform any final operations. Additionally, you can use the WorkflowCoordinator in a later workflow activity by passing the activity name or sys_id to the WorkflowCoordinator.load('&lt;Activity&gt;') function. For example, to load the WorkflowCoordinator object from a Parallel Flow Launcher activity called Launch Subflows, enter <code>var coord = WorkflowCoordinator.load('Launch Subflows');</code> in a later activity.</td>
</tr>
</tbody>
</table>
| flow | The subflow launched by the activity that completed most recently. You can use this variable in the Flow complete script to perform any post-processing operations on each subflow. To get a complete subflow from a coordinator object, use `var flow = coord.getFlow(I);` where `I` is the numeric index of the subflow based on the order it was launched. These values are available from the completed subflow:  
  - **index**: the numerical index of this subflow based on the order it was launched  
  - **workflow**: the sys_id or name, depending on which you passed to the WorkflowCoordinator constructor, of the workflow used for this subflow  
  - **inputs**: any input values provided to the launched subflow  
  - **status**: status of the subflow context  
  - **output**: the value returned by the subflow  
  - **contextId**: the sys_id of the workflow context for the subflow |

Parallel Flow Launcher example

This example shows how to use the Parallel Flow Launcher activity with an array of input values and with a WorkflowCoordinator object.
**Sample workflow**

This example shows a SQL-based web server with four application nodes. A single subflow runs to provision the database, and multiple parallel subflows each configure an application node. Finally, a separate set of parallel subflows configures the nodes to use a load balancer and sets up the server DNS.

**Parallel flow launcher business case**

**Provision the application nodes**

The first *Parallel Flow Launcher* activity launches the *Provision Node* subflow four times. The activity passes a unique IP address to each subflow from an array in the *Inputs* variable. The scripts defined in the *Flow complete* and *Finished script* variables write log messages regarding the status of the subflows.
Activity Properties: Parallel Flow Launcher

- **Name**: Provision application nodes
- **Stage**: 
- **Inputs**: 
  - [{u_host: '192.168.0.10'},
   {u_host: '192.168.0.20'},
   {u_host: '192.168.0.30'},
   ...
  ]
- **Workflow**: Provision Node
- **Count**: 
- **Max flows**: 25
- **Max simultaneous**: 5
- **Process flow complete**: ✔
- **Flow complete**:
  ```
  // To access the flow that completed, use the 'flow' variable.
  //
  // var flowOutput = flow.output;
  //
  workflow.debug("Provision Node Finished. Context: " + flow.contextId);
  ```
- **Process finished**: ✔
- **Finished script**:
  ```
  // To access the set of completed workflows use the 'coordinator' variable.
  //
  // var flowResult = coordinator.getFlow(1).output;
  //
  workflow.debug("All Nodes Provisioned");
  ```
Add nodes to the load balancer

The second **Parallel Flow Launcher** activity uses WorkflowCoordinator objects to specify which subflows to run. The `coordinator` variable stores the completed flow information from the previous **Provision Nodes** activity. The script then retrieves the IP address and port for each node that was provisioned. The `coord2` WorkflowCoordinator object runs the Add Node to Load Balancer subflow once for each node, using the retrieved IP address and port information as input variables. Finally, the `coord2` WorkflowCoordinator object runs the **SetupDNS** subflow once to configure the load balancer.

```javascript
var coordinator = WorkflowCoordinator.load("Provision Nodes");
var coord2 = new WorkflowCoordinator({
  workflow: 'Add Node to Load Balancer'
});
for (i = 0; i < coordinator.getNumFlows(); i++) {
  var ip = coordinator.getInput(i).ip;
  var port = coordinator.getInput(i).port;
  coord2.add({
    ip: ip,
    port: port
  });
}
var loadBalancerIP = '10.0.20.10';
coord2.add({
  ip: loadBalancerIP, hostname: 'www.snow1.net',
  'SetupDNS':
});
coord2;
```

Specifying which subflows to run

**Workflows used as subflows**

A workflow can launch another workflow as an activity.

The parent workflow triggers the subflow and then waits for the subflow to complete before continuing. Run the workflow validation tool prior to publishing to detect missing subflows and other dependency problems, such as those involving update sets.

The **Workflows** tab in the Workflow Editor contains a list of the workflows available for use as subflows.
Workflows available to use as subflows

Make sure that the selected subflow is active. If the subflow is inactive, the main workflow will hang with a **Loading** message. If you place an inactive subflow into a workflow, the subflow appears with a red banner, indicating that it cannot run. An active subflow is highlighted in blue when selected.
Subflows and the Create Task activity

If a workflow contains a `Create Task` activity that has executed on the current record, additional task activities in the workflow might not execute as expected.

This can happen when the same subflow containing a Create Task activity runs more than once in a parent flow. When the subflow reruns and attempts to execute the `Create Task` activity again, the system reopens the first task activity instead and does not create an additional task.

Note: An alternative to creating duplicate subflows that use the `Create Task` activity is to add a `Run Script` activity to the workflow that creates a task with a script.
The same create task activity runs twice in a workflow

In this configuration, the workflow does not run the same subflow containing a Create Task activity more than once. This allows the workflow to create additional tasks.
Running different subflows containing the Create Task activity

View workflow activity descriptions

Tooltips are available for workflow activities to help you understand how to use each activity.

1. To view an activity description in the workflow editor, point to the icon for the activity in the palette.
2. To modify activity descriptions, navigate to Workflow > Administration > Activity Definitions and edit the Description field.

**Note:** To view more information about an activity, double-click the activity on the canvas and then click the help icon in the title bar of the Activity Properties window.

**Elements in workflow activity definitions**

Each activity can specify a number of elements that control the behavior of the activity or are controlled by the activity.

Not all activities specify all possible elements. See Workflow activities for links to the activities provided by default. Each activity description includes a detailed explanation of the specific elements offered by that activity.
Workflow activity elements

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Results</td>
<td>The possible activity.results value. The activity result usually determines which condition the activity transitions through.</td>
</tr>
<tr>
<td>Scratchpad entries</td>
<td>Scratchpad variables the activity depends on to run, or variables the activity writes to the scratchpad.</td>
</tr>
<tr>
<td>Input variables</td>
<td>Values that control the behavior of the activity. Fields to set these values appear on the Activity Properties form when a new activity is added to a workflow. See Activity variables for more information.</td>
</tr>
<tr>
<td>Conditions</td>
<td>Determines which transition the activity follows after completing. See Manage workflow activity conditions for more information.</td>
</tr>
<tr>
<td>States</td>
<td>Determines how the workflow handles the record being executed.</td>
</tr>
</tbody>
</table>

Add an activity to a workflow

Available activities are displayed in the Core, Packs, and Custom tabs in the Workflow Editor palette.

1. In the Workflow Editor, check out a workflow.
2. To add a workflow activity, drag it from the Core, Packs, or Custom tab to the canvas and drop it on a transition line in the workflow body.

   The transition turns blue when it is connected to the new activity. The designer adds the activity to the flow at that point and displays the property form for the new activity.

   If an activity is greyed out, approval engines are enabled for the table on which the workflow runs. To use the activity, turn approval engines off for the table.
Unavailable activities and approval engines

3. Create any additional conditions needed for the activity and ensure that all exits are connected.
4. Run the workflow validation tool prior to publishing to detect missing or disconnected transitions that can cause a workflow to hang.

**Note:** All activity descriptions have a Table value. If this value is Global, the activity is available for use with any workflow regardless of the table selected in the workflow properties. Activities that identify a specific table appear in the palette only if the table configured for the workflow matches or extends the table identified in the activity.
Adding an activity to a workflow

**Duplicate a workflow activity**

You can duplicate an activity used in a workflow, including all the configured properties.

1. Right-click the activity and select **Copy Activity** from the context menu.
   
   The system automatically duplicates the activity, but does not create transitions.

2. Double-click the copy and configure the properties appropriately.

3. Drag the activity to a location in the workflow.

4. Add **transitions**.
Manage transitions between workflow activities

Transitions define the processing path of the workflow, depending on conditions defined in each activity.

All conditions in an activity must have a transition and all transitions must have a connection to another activity or to the End activity.

---

Note:

Run the workflow validation tool prior to publishing to detect missing or disconnected transitions that could cause a workflow to hang.

1. Add transitions to the workflow using either of these methods:
   - Drag and drop an activity directly onto a transition line to connect it to the adjacent activities. The transition line turns blue when the connection is made. The system updates the transitions automatically to reflect the new sequence.
- Drag the activity to an open area in the canvas and create the transitions manually. Click the yellow square on the right side of the activity condition and drag a connector to the next task.
2. You can draw multiple transitions from the same activity condition if the activity executes concurrently.
3. To remove a transition, click to highlight it, and then press Delete.

Custom activity transitions

Controls on the Approval - User activity enable an administrator to add additional workflow transitions to the activity other than the default transitions of Approved or Rejected.

Transitions defined using this method do not become a permanent feature of the Approval - User activity. After a new transition is configured, that transition must be applied manually to subsequent instances of the activity, where desired.

Manage workflow activity conditions

Activities contain default conditions that determine which transitions are followed.

For example, the Approval - User activity has two conditions, Approved and Rejected.

Example of activity conditions
You can use a JavaScript condition check to create custom conditions on Core workflow activities. (Custom activities do not support this feature.)

1. Right-click the activity and select **Add Condition** from the context menu.
2. In the **New Workflow Condition** dialog box, fill in the fields as appropriate (see table).

### New Workflow Conditions form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The label that is displayed on the workflow.</td>
</tr>
<tr>
<td>Activity</td>
<td>Name of the activity for which this condition is submitted. This value is populated automatically by the system.</td>
</tr>
<tr>
<td>Short description</td>
<td>Brief description of this condition.</td>
</tr>
</tbody>
</table>
| Condition           | A JavaScript condition check. The following variables are available:  
  - `current`: Current record that the workflow is running against.  
  - `activity.result`: Result value set by the activity upon completion.  
  - `activity.vars`: Variables associated with the Workflow Executing Activity record. Used for advanced condition checks. |
| Skip during generate | If selected, the **Generate activity** does not follow this transition to generate approvals or tasks. |

3. Click **Submit**.
4. To change the order in which conditions appear on the workflow activity, right-click the activity and select **Reorder Conditions**.

A dialog box appears, with a list of the available conditions.
List of conditions in the current activity

5. Drag the conditions to a new position in the list.
6. Click OK.

Activity result value

The result value specified by an activity controls the condition through which the activity transitions.

Use the result value as part of the Condition field in the activity. For example, if the Condition field of an Approval - User activity contains activity.result == 'rejected', the activity transitions through that condition when a rejection is received from the approver. Result values are set in the Script field of the activity definition.

Edit the workflow activity properties form

Customize which workflow variables appear on an activity properties form and how the variables are arranged on the form.

1. Navigate to Workflow > Administration > Activity Definitions.
2. Scroll to the activity that you want to work with and click the activity name.
3. On the Workflow Activity Definition form, click the Edit Variables Layout related link.
4. On the Form Design page for the Activity Properties form, add and remove activity variables. The activity variables appear as separate items that you can rearrange on the form.

For more details on using the form design interface, see Using the form designer.
Using workflow approval activities and rolling back workflows

When you work with approvals, you need to understand how approval activities interact with approval engines, how to correct a skipped approval workflow activity, and how rollbacks work.

Approval workflow activities and approval engines

Approvals can be managed by approval activities or approval engines, but not both. Approval activities can be used if approval engines are not turned on for the table associated with the workflow.

Approvals can be managed by approval activities or approval engines, but not both. Trying to use both can cause a range of issues. Approval activities are not available (greyed out) in the palette if approval engines are used on the specified table. If you hover over a greyed out approval activity in the palette, a comment with more information is provided. For more information about approvals and approval engines, see Approvals.

Unavailable approval activities

To turn approval engines off for the table, navigate to the System Properties > Approval Engines and change the setting for the table to Turn engines off.
Turn off approval engines

Correct a skipped workflow approval activity

While a workflow is in an active context, an approval activity can skip to the next activity.
An approval activity might skip for the following reasons:

- The approval user or group is missing or invalid (for example, sys_id).
- The approval user or group became inactive after the approval record was created.
- The activity is a dot-walked field, such as current.opened_by.department.manager, and it has a missing or invalid approval user or group.
- The business rule on the table that is associated with the workflow is invalid.

To correct a missed approval activity:

1. Navigate to Workflow > Live Workflows > All Contexts.
2. Click the date and time in the Started column for the workflow that is incorrectly processing approval activities.
3. In Related Links, click Show Workflow.
4. Review the portion of the workflow that executed, and then do one or more of the following:
   - Verify that after approval, the workflow progressed to the next activity. If a workflow failed to progress, check the business rules. For more information, see Debugging business rules.
   - Point to each processed approval activity to find activities where the State is Finished and Result is Skipped.
5. Navigate to Workflow > Workflow Editor and open the workflow.
6. Double-click the skipped approval activity.
7. Click Users or Groups.
8. Assign an active user or group for the approval activity. For more information, see Workflow error handling.

Rollback To activity

When conditions in a workflow trigger a Rollback To activity, the workflow moves processing backward to a specified activity in the workflow and resets certain activities that have already executed back to their original state. This is useful when handling an unexpected failure or as part of a programmed logical flow.

When an activity is reset during a workflow rollback, the following happens:

- Approvals are reset to Not Requested.
- Tasks are reset to either Open or Pending. A rollback workflow path cannot create new tasks.

Activities that perform external system operations, such as deleting a file or sending an email, are not rolled back. Only approval and task activity states are reset.

A workflow can contain a single rollback, multiple rollbacks, or nested rollbacks in more complex workflows. The Rollback To activity resets activities based on the actual workflow sequence (transition line attachments) of activities between itself and the transitioned to activity, rather than using the execution order to determine where processing should restart.

Rollback To behavior

The Rollback To activity transitions directly to the activity specified by the transition line arrow.

Use the Rollback To activity for all workflows that use multiple or nested rollbacks. Rollback To resets the targeted task (the direct transition) to Open. All tasks that have executed between the Rollback To activity and the targeted task (rolled back task) are set to Pending.

(0) Begin
(1) Log Message
(2) Task 1
(3) Task 3
(4) Task 2
(5) Timer
(6) Approval 1
(7) Roll back to first task
(8) Task 1
(9) Task 2
(10) Approval 1
(11) Log approval
(12) Join
(13) Send email
(15) End
Rollback to workflow

Transition history

The state of (3) Task 3 does not change, since this activity does not directly transition from the rollback target activity. To see what activities were rolled back, select the Workflow Transition History related list and look at the Rolled back column.

The Rollback To activity (7) updates the following activities:

(8) Task 1: reset to Open
(9) Task 2: reset to Pending
(10) Approval 1: reset to Not Yet Requested
Rollback To workflow transition

**Using variables in Notify workflow activities**

Certain Notify workflow activities support variable substitution for reading text to callers.

Certain Notify workflow activities allow you to use variables, such as those from the workflow scratchpad, to determine the activity behavior. Each activity supports a maximum of 20 variables. The following activities allow variable substitution:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Say</td>
<td>Supports variable substitution in the <strong>Text</strong> field only.</td>
</tr>
<tr>
<td>Input</td>
<td>Supports variable substitution in the <strong>Text</strong> field only.</td>
</tr>
<tr>
<td>Play</td>
<td>Supports variable substitution in the <strong>URL</strong> field only.</td>
</tr>
</tbody>
</table>
### Scratchpad variables

You can call variables from the workflow scratchpad or the activity scratchpad using the syntax `${variable_name}`. You do not need to include either workflow.scratchpad or activity.scratchpad before the variable name. For example, to use the variable `activity.scratchpad.langCode = 'en-US'`, call `${langCode}` within the activity. If the scratchpad does not contain the specified variable, the variable evaluates to an empty value.

You can get values from objects on the scratchpad using the format `${object.value}`. For example, you can get the name of a user object, such as `workflow.scratchpad.user = {name: 'john.smith'}` by calling `${user.name}`.

### The digit variable

The **Input** activity exposes the `${digit}` variable. Use this variable in each condition presented by the activity. The number read to the user is determined automatically by each condition. The caller can press that number to cause the activity to transition through that condition.

### Use multiple timer activities in one workflow

Workflow timer activities store data independently of each other in an activity-specific scratchpad.

Previously, all timer activities in a workflow accessed a single, shared scratchpad, which could lead to conflicts when adding multiple timer activities to one workflow.

Timer scratchpads entries hold these values:

- `workflow.scratchpad.endTime`
- `workflow.scratchpad.realStartTime`
- `workflow.scratchpad.retroactiveSecsLeft`

### Publish a custom workflow activity

When a user creates a custom activity and saves or submits it, that activity appears in the **Custom** and **Packs** tabs of the designer palette, but is only visible to the user who created it.

When configuration is complete, the user clicks **Publish**, which makes the activity accessible to other users on the instance with the `workflow_admin` or `activity_creator` role. Published activities are available for upload to the ServiceNow Store, can be added to workflows, and can be edited by any user with the proper roles.

To edit a published activity, click **Checkout**. When an activity is checked out by a user, only that user can modify it. The fields of a checked out activity are read-only for all other users. When the checked out activity has been modified successfully, the user publishes it again. The system adds a new version of this activity to the Custom tab in the workflow editor palette.

**Note:** Activities you create and publish are only visible in the Packs tab if they were created in the current application scope.
Locked versions

Problems can arise if an activity version is checked out by a user and not checked back in, for example, when the user is sick or leaves the company. An activity in this state cannot be checked out for update.

A user with the admin role can return a locked activity to a published state. The administrator opens the locked activity from the Custom tab of the workflow editor, selects the checked-out version, and selects Force Checkout, and then Publish.

Workflow activity pinning

Workflow administrators can pin a custom activity to prevent the system from automatically updating that activity when a new version is downloaded from the ServiceNow Store.

You can pin or unpin individual activities or set pinning within workflow properties that controls the versions used for all the activities in that workflow. This can result in two workflows using different versions of the same activity.

Note: Activity pinning and unpinning applies to the custom activities downloaded from the ServiceNow Store only, and does not apply to newly published activity definitions made locally on your instance. To make use of these locally updated custom activities, you must check out your workflow and manually add the activities.
Index

A
account
  Twilio
    associating 355
activate Service Portal user criteria 2169, 2169, 2367, 2367
Active Directory
  Orchestration activity pack 1486
  Orchestration example 1478
activities
  Active Directory activity pack 1486
  activity packs
    requesting activation of 1336
  Add F5 Pool Member 1529
  Add F5 Profile to Virtual Server 1533
  Add F5 Virtual Server 1535
  Add User to Group 1487
  Add User to Group Azure AD 1500
  Assign User License 1501
  Azure AD 1500
  Change AD User Password 1488
  Change Service State 1580
  Check F5 Pool 1532
  Copy File 1603
  Create AD Object 1489
  Create Directory 1604
  Create User 1502
  Delete F5 Pool 1537
  Delete F5 Pool Member 1536
  Delete F5 Virtual Server 1531
  Delete User 1504
  Disable AD User Account 1491
  Enable AD User Account 1492
  F5 load balancer 1529
  File Copy 1615
  File Read 1612
  Files Compare 1611
  Get F5 Pool Member 1530
  Get File List 1605
  Get User Info 1505
  Global activities 1618
  Infoblox DDI 1539
  Install Windows App 1579
  Is AD Account Locked 1493
  Join Domain 1578
  Modify F5 Virtual Server 1534
  PowerShell activity pack 1564
  PowerShell HResult codes 1345
  Probe activity pack 1583
  Query AD 1494
  Remove AD Object 1495, 1538
  Remove File or Directory 1606
  Remove User from Group 1496, 1507
  Remove User License 1508
  Rename File or Directory 1608
  Reset AD User Password 1497
  Reset User Password 1509
  Restart Windows Server 1581
  Secure Copy 1610
  Set File Attributes 1609
  SFTP File Transfer 1598
  SSH activity pack 1610
  Uninstall Windows App 1582
  Unlock AD Account 1498
  Update AD Object 1499
activity designer
  activity packs 1485
  activity scoping 1721
  auto-mapping JDBC output variables 1637, 1659
  auto-mapping REST output variables 1688
  auto-mapping SOAP output variables 1666
  copying activities 1723
  creating custom activities 1623
  introduction to 1620
  JavaScript probe activity, creating 1676
  JavaScript Probe execution command 1679
  JavaScript probe execution parameter 1677
  JavaScript probe template post-processing parameters 1678
  JDBC activity, creating 1654
  JDBC connections 1657
  JMS activity system setup 1718
  JMS activity, creating 1717
  JMS execution parameters 1719
  JMS template post-processing parameters 1720
  mapping output variables 1640
  output variables 1637
  parsing rules example 1646
  parsing rules, creating 1641
  parsing sources 1645
  PowerShell 1564
  PowerShell activity, creating 1681
  PowerShell execution command 1629
  PowerShell execution parameters 1682
  PowerShell template post-processing parameters 1684
  Pre-processing fields 1634
  Probe activity, creating 1706
  Probe execution command 1708
  Probe execution parameter 1706
  Probe template post-processing parameters 1707
  REST activity, creating 1686
  REST execution command 1691
  REST execution parameters 1689
  REST execution parameters, JavaScript array in 1690
  REST template post-processing parameters 1691
  reusing data 1725
  run script activity, creating 1716
  Run Script processing script 1717
  SFTP activity, creating 1695
  SFTP execution command 1701
  SFTP template post-processing parameters 1700
  SOAP activity, creating 1665
  SOAP execution command 1670

© 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.
SOAP execution parameters 1673
SOAP execution parameters, JavaScript array in 1675
SOAP input variables 1627
SOAP template post-processing parameters 1675
SSH activity, creating 1710
SSH execution command 1714
SSH execution parameters 1711
SSH template post-processing parameters 1712
Template conditions 1653
Template outputs 1639
Template post-processing fields 1635
templates 1654
testing input fields 1631
testing JDBC input fields 1661
variables, mapping 1628

add actions
  chat window menu 408
add blank line
  email template 173
administering context
  workflow 2662
Legacy Notify 354
workflow context 2662
AES 128
  configure 947
  encryption key 947
AES 256
  configure 950
  encryption key 950
agent0.log.0 1294
allocate users
  to subscriptions 2396
allocate users to subscriptions 2401, 2402
Amazon EC2
  instance 1812, 1813, 1815
Amazon Web Services
  external credential storage
    configure AWS credentials on a CyberArk vault 910, 924
    configure the credential identifier for AWS 916
Amazon Web Services (AWS)
  credentials for 871
Angular directives 2338
Angular providers 2338
Approval Action
  Input Variables 2698
  Results 2698
  States 2698
Approval and Rollback Activities 2698
Approval Coordinator
  Conditions 2699
  Input Variables 2699
  Result Values 2699
  States 2699
approval engines
  set up 1974
Approval Group
  Conditions 2702
metric values, updating 1877
script method 1839
Assessment notification
workflow 1894
assessment properties 2055, 2458
assessment questionnaires 1970
assessment trigger condition
creating 1899
example 1892
assessments
categories, create 1851
category users 1877
category users, creating 1878
change the order of an answer 1862
clean up data 1887
create metrics 1864
create quizzes with forms 1934
creating quizzes with forms 1922, 1934, 1935, 1942
customize appearance 2054, 2457
export 1872
generate 1849
generate assessable records 1864
generate on-demand assessments 1884
generate with on-demand API 1885
import 1872
installed components 1825
instances 1888
metric categories 1850
notifications 1894
on-demand assessments 1884
on-demand for multiple assessable records 1885
on-demand for one assessable record 1884
process 1839
publish metric types 1886
results 1899, 1902
roles 1839
schedule types 1886
scheduled
configure for 1886
generate manually 1887
vendor type, generating 1887
scheduled assessments 1886, 1887
signatures 1873
stakeholders 1877
stakeholders, creating 1878
terms 1839
view instances 1888
assessments overview
reports 1899
roles 1899
assessments overview module 1899
associating
account
Twilio 355
Twilio
account 355
audio files
connect 34
auto-upgrade 979
auto-upgrader 979
automatic approval rules
set 1976
automation status sets 1233
Azure AD activity pack
Add User to Group 1500
Assign User License 1501
Create User 1502
Delete User 1504
Get User Info 1505
Remove User from Group 1507
Remove User License 1508
Reset User Password 1509

B
Baseline
creating 509
differences
displaying 509
Baseline CMDB 509
Basic Auth credentials 872
basic search source
table search source 2160, 2346
bubble chart
components 1904, 1907
bubble charts
create 1902
view 1902
business rules
installed with live feed 438
Business rules
Notify 300
business service management
maps 646
Business Service Management Map
next generation version 650

C
Calculator widget 2208
call
conference
viewing 352
canceling
workflow 2666
Capacity subscriptions 2393
Catalog Content widget 2266
categories
survey management 2037, 2440
categories for assessments 1851
category results 1957
category users 1877
category users, creating 1878
certificate
configure 947
https 947
Certification
filters 710, 712, 714, 714, 714, 716, 717
certification audit results
compliance view, viewing 705
deleting 703
viewing 700
Certification Audits 693, 693, 698, 707, 707, 709
Certification Follow On Tasks 718, 718, 722
certification templates 724
audit types 724
clones 734
creation 724
deletion 736
management 730
record lists 728
change verification rule 512
chat 382
Chat
installed components
fields 384
script includes 386
chat action details 410
chat actions 407
chat room access rights
define 405
chat room message read access
change 406
chat window menu
adding
actions 408
check in a document 1142
check out a document 1142
checklists
using with visual task boards
configuring checklists 2535
creating checklists from templates 2534
creating new checklists 2533
deleting checklists 2534
choice
Legacy Notify
creating 350
response 350
CI
proposed changes
add 511
displaying 511
CI class
reclassify 538
CI relation rollups
create 530
CI relations formatter
CI relationship builder 528
flat layout 521
tree layout 522
CI relationship editor 522
CI relationships
security 530
CI type
create 537
ClassName
methodName() 333, 334
Client
call(Object identifier) 340
Client(Object) 340
forwardCall(Object argument) 342
hangupCall() 341
mute(Boolean muted) 342
Notify WebRTC Client 339
pickupCall() 341
client software distribution (CSD)
activating 1366
configuration
retrieving SCCM data for 1380
SCCM server Discovery 1381
configuring providers 1395
creating catalog items for SCCM applications 1386
creating software models for SCCM 1382
dashboard 1393
deploying software from SCCM 1376
extension keys 1396
extension points 1394, 1396
installed components 1367
introduction 1365
lease extensions 1374
licenses and counters for 1371
ordering software from the service catalog 1372
plugins installed with 1368
properties for 1369
providing Windows credentials for SCCM 1379
revoking software not installed by SCCM 1391
roles installed with 1368
SCCM configuration 1382
SCCM deployment workflow 1389
SCCM software revocation
revoking software installed by SCCM 1390
SCCM software revocation workflow 1392
script includes installed with 1369
tables installed with 1367
validating software installations 1390
workflows installed with 1371
cloning issues 1300
cloud management
credentials for 875
CMDB
Extended 629
CMDB Classifications 531
CMS gauge
on a page, putting 821
what happens on a click, controlling 822
CMS gauge support 821
CMS to Service Portal transition 2177, 2181
CMS translation
viewing 866
color codes
Subscription Management 2408
com.glide.service-portal.user-criteria 2169, 2367
Common Information Model (CIM)
credentials for 874
compliance
filter 711
Compliance
desired state reporting 690
installed with 676
scripted audits 747, 748, 756
compliance overview
module 681
Compliance Overview module 2408
condition
parameters 673
condition activities
if 2723
switch 2724
wait for condition 2727
wait for WF event 2728
conference
call
viewing 352
configuration
CMBD 531
CMDB 535
Related Lists of CI components 536
Configuration Management
CI forms 629
related lists 629
configuring
endpoints
Twilio 357
Legacy notify 355
Twilio
endpoints 357
Legacy notify 355
configuring email
alternate
POP3 68
SMTP 66
SMTP and POP3 72
connect
administering 31
audio notifications
customizing 34
chat mini windows
drag files 30
connect actions 35
connect interface 17
connect overlay
disabling 34
close sidebar 19
connect workspace
conversation pane 25
conversation tools 25, 2537
installed components
business rules 12
notifications 9
properties 10
tables 10
mentioning users 30
mini windows 21
notifications 26, 27
polling interval 34
properties 31
record conversations
 disabling for all tables 42
 disabling for specific tables 43
 supported browsers 8
 uploading a profile picture 29
 visual task boards
 sharing 30, 41, 2545, 2545
 Connect 8
 connect chat
 administering 41
connect workspace
 adding and removing conversation members 40
 editing conversation details 40
 conversation members
 adding and removing 40
 email notification interval 40
 following a record 39
 record conversations
 enabling 42
 starting conversations 38
 using 38
Connect chat
 browser notifications 27
disable 43
Connect Chat
 activate 9
 record cards 37
 Connect chat notifications
 browser support 27
 Connect record card 37
connect support
 activating 13
 additional plugins 16
 administering 53
 administering queues 55
 creating an incident from a conversation 50
 dashboards for 57, 58
 escalating a conversation 50
 homepage for 57, 58
 installed components
 business rules 15
 properties 14
 tables 14
 making a queue accessible to end users 56
 metrics for 57, 58
 monitoring incoming conversations 44
 sharing knowledge 46
 transferring a conversation 47
Connect Support
 add users to conversation 49
 add users to support conversations 57
 administration 57
 chat states 51
Connect Support and Service Portal 59
Connect Support migration 53
Connect Support Service Portal 59
Connect Support Service Portal widget instance
 options 60
 containment service rule metadata 584
 content blocks
 create header block 825
 dynamic block 840
 static html block 842
 types 825
Content Blocks
 add an image 843
 catalog cart block 840
 CMS block tag 824
 configure 823
 content management 846
 detailed content block 847
Flash movie block 844
iFrame 845
Live Feed 846
static html block 843
content management
corporate style guide 799
design 796
organize content 797
prepare data 799
prototypes 801
rapid web design 801
team members 798
Content Management
Apache Jelly engine 848
business rules 805
client script 805
configure a new site 807
configure list definitions 842
configure menu items 829
content block types 825
content blocks
catalog card block 840
detailed content blocks 847
dynamic blocks 840
Flash movie block 844
header block 825
iFrame 845
static HTML block 842, 843
content links 844
content pages 812
content site 806
content types 820
Content Types 820, 822
copy a page to create a template 819
copy a site 810
create a navigation menu block 826
create menu sections 828
customize the menu style 832
DIV-based layouts 856
element link examples 858
frame 854
global search 865
installed with 804
integration points 857
integration points example 863
Jelly
Examples 851
list block 841
login rules 811
master template 819
menu types 830
navigation 801
navigation menu example 839
roles 805
script includes 805
security 811, 812, 816, 854
set up site 806
single sign on 812
source view 859
style
design themes 853
frame 854, 854
frame UI macro 855
themes 853
style sheets 853
tables 804
testing 865
translation 866
URLs 811
Content Management integration points
example 837
static methods 860
Content Management Integration Points
dynamic methods 862
iFrame method examples 847
manage system content 801
Content Management meta tags
hierarchy 856
page level 855
site level 856
content management system 795
Content Management System
activate 803
Content Management templates 817
content pack 59, 645, 1089
content pages
add content 814
application 816
assign to a site 816
copy 815
create 812
Content types
configure 820
Content Types
view 822
context
workflow
administering 2662
contextual search
Service Portal 2359
Controls
managing 738, 740, 741, 745, 746
conversation
Legacy notify
viewing 351
create
bubble charts 1902
Create a Survey Wizard
configure the survey 2130
create a dynamic effect 2127, 2128
create a survey page 2127
define a survey question 2126
test the survey wizard demo 2129
create a widget 2155, 2304
Create a widget 2329, 2330, 2332, 2333, 2335, 2338
create knowledge
access an external knowledge article 1086
creating
Legacy Notify
choice 350
question 349
response 350
creating quizzes with forms
available data types 1922

© 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 a published quiz 1942
select a user for a category 1935
set up a category 1934
credential issues after cloning 1300
credential tagging 1571
credential tagging for Orchestration activities 903, 1622
credentials
affinity 902
Amazon Web Services (AWS) 871
applicative credentials 870
basic authentication 872
checking IP service affinity 904
CIM 874
cloud management 875
creating 869
CyberArk integration
configuration tasks 920
CyberArk storage
configuring credential identifier 923
configuring SNMPv2 credentials 923
configuring the MID Server 921
configuring the vault 920
import the JAR file 921
installing the AIM API 920
data
debug 925
event storage
activation of 907
configuration of 910
configuring identifier of 915
importing a JAR file for resolution of 914
external storage architecture for 908
external storage for 907
introduction to 867
JAR file 910
JDBC 878
JMS 880
Linux
commands requiring root privileges 889
MID Servers from credentials table 899
MID Servers from service account 899
NetApp storage devices 875
privileged commands 891
resolving 910
SAP JCo 881
SNMP 882
SNMPv3 884
SSH 885
SSH private key 886
testing 899
UNIX
commands requiring root privileges 889
VMware 895
Windows 896
Windows domain requirements 898
Windows permission requirements 897
Windows requirements for 898
Ctrl-Alt-Del 1475, 1809
Ctrl+Alt+Del 1408, 1741
CyberArk
configuration tasks 920
configuring credential identifier 923
configuring SNMPv2 credentials 923
configuring the MID Server 921
configuring the vault 920
import the JAR file 921
installing the AIM API 920
introduction to 917
dashboards
connect support 57
data archiving
activate push retention plugin 259
email archiving 215
email messages 212
manually archive push notifications 259
push notification retention 257
data certification
activating 757
certification audit definition 770
certification audit instances 769
certification element 768
certification instances 769
certification schedules 764
certification tasks 766
data Certification
installed 758
perform data certification 786, 786, 787, 788, 789, 790, 790, 791, 792, 792, 793, 793, 793, 794, 794, 795, 795, 795
data certification overview module
using 773
data encryption
Orchestration activities 1634
data fetch script 2351, 2355, 2356, 2383, 2387
data table from URL definition widget 2215
data types
survey questions 2041, 2067, 2444, 2470
databus 1724, 1725
decision matrix
creating 1960
decision matrixes
administering 1964
defining
on-cancel script 2667
on-cancel 2667
delete
assessable record 1875, 1971
demand management
assessment category
creating 1850
Dependency Views
menus 651
Independent identification rule 562
desired state 687
Desired State Overview module
access 690
use 688
develop widgets in the Service Portal 2298
Discovery
  credentials
testing 899
credentials for
  activating external storage 907
  affinity 902
Amazon Web Services (AWS) 871
applicative credentials 870
basic authentication 872
checking IP service affinity 904
CIM 874
configuring external storage 910
configuring identifier of 915
creating 869
CyberArk integration 917
external storage 907
external storage architecture 908
importing a JAR file for resolution of 914
JDBC 878
JMS 880
Linux 888
MID Server from credentials table 899
MID Server from service account 899
NetApp storage devices 875
SAP JCo 881
SNMP 882
SNMP community 882
SNMPv3 884
SSH 885
SSH private key 886
UNIX 888
VMware 895
Windows 896
Windows domain requirements 898
Windows permission requirements 897
Windows requirements 898
domain separation setup 1272
long running commands with sudo 894
document feeds
  configure 421
  configure security 421
disable 422
installed components 422
live feed UI action 421
document publication
  approval 1153
draft review 1156, 1158
electronic signature 1156
  publish 1157
Documents
  parameters 1145, 1146, 1146, 1146, 1147, 1148, 1149
domain separation
  live feed 433
  MID Server 1272
domain separation setup
  Discovery 1272
dynamic approval forms 1991
E
  e-signature approval
  approval tables, selecting 1987
de-activate 1986
local database, setting up 1988
plugin, installed with 1987
SAML 2.0 authentication, setting up 1988
setting up 1989
ECC queue
  accessing 1292
  retry policy 1288
ECC queue message
  create 1293
Edge Encryption
  adding proxies 965
  attachment decryption job 988
  attachment encryption 987
  attachment encryption job 988
  attachment key rotation job 983
  attachments 987
  configuration 982
  configure 1025, 1025
database recovery job 992
deactivate encryption 985
decryption job 986
dictionary attributes 1019
digital signature 956
encryption application 930
encryption change 989
encryption deactivation 985
encryption job 985
encryption key management 931
encryption patterns
  advanced 990
  basic 990
  predefined 991
encryption proxy 930
encryption rule actions 996
encryption rule conditions 995
encryption rules 992, 995
encryption type
  change 989
  deactivate 985
  encryption types 932
  field encryption 984
  file store 960
  getting started 935
  installation 942
  installed components
    tables 933
installer 943, 944, 947, 947, 947, 950, 950, 951, 953
instance configuration 984
Java Cryptography Extension (JCE) installation 958
Java KeyStore 959
key management 931, 961
key rotation 981, 982
key store management 931
keytool utility 959
limitations 939
Linux installation 955
Linux uninstall 966
Linux update 981
logging 1021
mass encryption jobs 991
mass key rotation job 983
inbound email actions
  creating 193
  example: creating a change request 206
  example: handling email replies 204
  example: logging a problem 205
  examples 204

next steps 111

notifications
  baseline 150
  creating a notification filter 286
  forcing delivery 286
  subscription-based
    accessing 278
    adding notifications 279
    creating a service provider 281
    filtering notifications with a schedule 288
    making mandatory 285

OAuth 2.0 76

quick messages 226

removing the email icon 228

service availability 62

setting the from address 224

size limits 104

size restrictions 62

standard configuration 63

system mailboxes \ 218

templates
  applying to a notification 164
  calendar integration 173
  convert to HTML 164
  creating 161
  the client 218

Email
  additional properties 94
  diagnostics 108
  inbound mail configuration properties 87
  outgoing mail configuration properties 84
  properties 82

Email API 229

email layout
  creating 180
  email layouts 178

email message
  construct 168

email notification
  specifying HTML content of 180

email notifications
  applying a template 164
  assignment groups 201
  calendar integration
    creating invitations for custom tables 175
    mapping date fields to variables 175
  content pages links 142
  converting to Rich HTML 123
  creating 112
  creating categories 111
  creating custom watermark 216
  document attachments 129
  editing HTML in notifications 128
  enabling record links 140
  

monitor 1020

NAE key store 960

order token repair job 991

overview 927

password encryption 965

patterns 932

prohibited keywords 1015

properties 962

proxy download 942

proxy properties 959

proxy system requirements 936

proxy update rollback 982

proxy upgrade 977

secure SSL connection 957

set up encryption key 958

set up keystore 958

single key rotation job 982

start the proxy 951, 953, 964,

stop the proxy 966

user account 942

web proxy configuration properties 962

Windows installation 955

Windows uninstall 967

Windows update 981

Edge Encryption environment
  memory 938
  Number of proxy servers 938
  redundancy 938

editing
  Legacy notify
    properties 359
  properties
    Legacy notify 359

e-mail
  accounts
    creating 78, 79
    testing 79
  alternate configurations 65
  attachment limit properties 106
  client
    display additional information 222
    phone 225
  client interface 219
  configuration 62
  configuring email client auto-complete 221
  controlling access to the client 222
  creating an email client template 223
  customizing the client 220
  displaying an editable form field 225
  displaying the Reply To field 225
  existing users, matching 199
  filters
    activating 211
    creating 211
  inbound actions
    importing users 199
  inbound email
    action criteria 189
  inbound email action processing order
    configuring 207
    managing multiple filters in an inbound email action 210
examples
assignment notification 158
priority 1 incident update 159
hiding watermarks 218
line breaks with rich HTML 130
omitting watermarks 217
specifying alternative outbound email 133
specifying outbound email address for a language 134
subscription-based
advanced scripting for SMS 283
selecting a service provider 283
time zone 133
used by live feed 440
watermarks 215
email objects
accessing with variables 197
e-mail retention plugin
activating 214
Email Service 229
e-mail template 180
e-mail variables 134
embed widgets example 2319
embedding widgets 2335
employee self-service 1812
enable email
basic 65
basic e-mail 65
enable Service Portal shopping cart widget 2281
encryption proxy
adding proxies 965
digital signature 956
download 942
encryption key management 931
file store 980
installer 943, 944, 947, 947, 947, 950, 950, 951, 953
Java Cryptography Extension (JCE) installation 958
Java KeyStore 959
key management 931
keytool utility 959
Linux installation 955
Linux uninstall 966
Linux update 981
NAE key store 960
password encryption 965
properties 969
scheduled upgrade 977
secure SSL connection 957
start the proxy 951, 953, 964
stop the proxy 966
system requirements 936
update rollback 982
web proxy configuration properties 962
Windows installation 955
Windows uninstall 967
Windows update 981
endpoints
Twilio
configuring 357
example
menu items and content links 837
exclude
users from subscriptions 2404
existing notification message filter
edit 288
existing notification message schedule
edit 288
existing users
email, matching 199
export
assessments 1872
export scorecard
image 2028, 2431
external credential storage
architecture for 908
CyberArk
configuration tasks 920
configuring credential identifier 923
configuring SNMPv2 credentials 923
configuring the MID Server 921
configuring the vault 920
import the JAR file 921
installing the AIM API 920
JAR file for 910
F
filter
compliance 711
filters
Notification conditions 267, 267
Form widget 2216
formatter
approval summarizer 1983
G
g_chat
available methods 410
General Scripting
execution order of scripts and engines 1992
Generate
Example 2714
Input Variables 2714
States 2714
gEOLOCATION
activate 1993
googLe key 1997
history 1997
tracking 1998
Geolocation
glide.service_portal.user_criteria_enabled 2169, 2367
global
print(String message) 1014
guided setup
MID Server 1181
H
hashtags
security 436
header menu widget 2218
Hello World widgets 2219
help the help desk
  login script
  install 634
  use 634
Help the Help Desk
detect software on 64-bit systems 641
determine values for the Assigned to field 639
Error message 640
run script 636, 637, 640
SOAP authentication 631, 631, 633, 633
view scan results 640
Help the Help Desk password
encode 635
help the help desk status
access 637
homepages
  connect support 57, 58
  customize 1820, 1821
delte 1821

I
I18N 1076, 1076
  Identification 561
  Identification and Reconciliation 561
  Identification types
    custom 1443, 1776
import
  assessments 1872
inbound email
  setting field values 202
inbound email actions
  locked out user 201
  triggering 201
inbound event
  integrate 202
inbound JSON request
  create notification 202
Incident Alert
  Notify number groups 313
incoming email
  values 207
Independent identification rule 562
Infoblox DDI activity pack
  Create Network 1558
  Delete Network 1561
  DHCP activities 1544
  DHCP Delete IP Reservation 1545
  DHCP List IP Reservations 1546
  DHCP Reserve IP v4 Address Range 1544
  DNS activities 1547
  DNS Delete 1552
  Get Network Details 1559
  IPAM activities 1554
  IPAM Delete 1557
  IPAM List IP Reservations 1556
  IPAM Register IP Address 1554
  IPAM Reserve IP Address 1555
  List DNS C-records 1547
  List DNS Record 1551
  List Registered Networks 1562
  network activities 1558
  Register DNS A-record 1548
  Register DNS C-Record 1550
  REST credential for 1539
  roles and permissions needed 1541
  workflows included with 1540
input variables
  parallel flow launcher 2763
install edge encryption 955
Installation 1178, 1191, 1202, 1210, 1210, 1280
installed with
  Content Management business rules 805
  Content Management client script 805
  Content Management roles 805
  Content Management script includes 805
  Content Management tables 804
Instant Messaging 411, 412, 412
integration 1021
ITIL
  service design 504
  service transition 505
ITIL configuration management 506
ITIL Configuration Management integration 503

J
J2SSH
  long running commands 894
JAR files
  synchronizing to MID Servers 1286
JDBC credentials 878
JMS credentials 880
JSON API 1009
JsonNode
  encodedQueryFor(String tableName) 1013
  getAsString() 1012
  getAsString(String propertyName) 1012
  getIterator(String xPath) 1011
  getName() 1013
  iterator() 1012
  nameFor(String tableName, String fieldName) 1013
JsonNode API 1011
JsonNodeIterator
  hasNext() 1014
  next() 1014
JsonNodeIterator API 1014

K
knowledge
  mobile access 1080
  view on mobile 1081
Knowledge
  Administration 1061
  Approve knowledge submission 1046
  Article view properties 1069
  Assign a manager 1060
  Category 1044
  create knowledge 1040
  Define a category 1059
  featured content 1049
feedback 1039
Import a document 1047
Knowledge base form 1061
Knowledge homepage properties 1071
Knowledge search properties 1067
Manager 1048
migrating access controls 1087
mobile search 1082
Move an article 1044
Other knowledge properties 1071
pin an article 1049
portal properties 1064
properties 1064
Publish and retire workflows 1063
Retired knowledge articles 1045
search changes 1085
searching knowledge 1032
Supported import elements 1047
user criteria 1050
user criteria for an article 1056
Workflows 1063
Knowledge document
installed with 1151
knowledge settings fields 1152
View linked knowledge 1152
Knowledge management
Request a knowledge base 1040
Service catalog 1040
Knowledge Management
article versioning
activate plugin 1090, 1101, 1133
approve article being reviewed 1097
compare versions 1099
configuration properties 1074, 1096
create new article version 1097
disable article versioning 1099
feedback on versions 1094
manually update customized files 1091
overview 1090, 1095, 1096
recall article being reviewed 1098, 1099
revert previous version to published 1098
version information 1096
versioning changes 1092
view all article versions 1098
duplicate article numbers 1077
homepage 1030
internationalization 1076, 1076
Knowledge Advanced plugin 1090, 1101, 1133
Knowledge Management Service Portal 1123
Knowledge Service Portal
homepage 1102, 1103
overview 1100
search results page 1106
knowledge subscription
configuration properties 1074
knowledge subscriptions 1133, 1134, 1135, 1135, 1136, 1136, 1137, 1137
roles 1030
Service Portal
configuration properties 1101
set up 1026
Social Q&A Properties 1073
submissions 1087
Knowledge Management Service Portal
widgets 1112, 1113, 1114, 1115, 1115, 1116
Knowledge submissions 1087
Knowledge subscriptions
email notification templates 1135
knowledge subscription notifications 1137
knowledge subscription properties 1134
manage knowledge subscriptions 1137
subscribe to knowledge article 1135
subscribe to knowledge base 1135
unsubscribe from knowledge article 1136
unsubscribe from knowledge base 1136
Knowledge v3
after migration 1084
default knowledge base 1084
knowledge article view 1085
knowledge portal changes 1086
migrate knowledge content 1089
migrating functionality 1087
migration guide 1083
publish and retire workflows 1089, 1089
replace modules 1087
security changes 1085
using legacy knowledge 1084
L
layouts
email 178
legacy chat
installed components
business rules 387
properties 384
tables 386
use legacy chat 387
legacy chat migration 53
Legacy notify
conversation
viewing 351
properties
editing 359
viewing 359
public conference calls 354
Twilio
configuring 355
viewing
conversation 351
Legacy Notify
account status messages 361
administering 354
call
conference 352
conference
call 352
Conference call participants 361
legacy survey
migrate 2088, 2491
legacy surveys
migrate 2088, 2491
Linux
commands requiring root privileges 889

© 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.
Linux credentials

live feed
  access from CMS pages
  administer
  bookmarking feeds
  bookmarking hashtags
  disable record feed
  document feeds
  domain separation
  hashtag security
  installed with
  limit access by role
  managing message content
  table access rules
  table notification
  related feeds
  workaround posted
  table notifications
  non-task example
  problem resolved example
  task table notifications
  team security

live Feed

Live Feed
  activating
  added to your homepage
  browser support
  following feeds
  following other users
  messages
  multiple records
  post a message
  post content in live feed
  post a message
  records
  selecting feeds
  UI usage
  update profile
  using
  using social IT
  post content in live feed
  using with UI
  viewing another user

live feed teams
  security

load balancers
  F5 custom Orchestration activities
  locked out user
  inbound email actions

M

managed document record
  create

managed documents

Managed Documents
  cancel a document
  check in a document
  check out a document
  concepts
  copy a document
  create a document

create a document collection
create or request a new document
deactivate a document
defects
install plugin
plug in
reopen a deactivated document
roll back a document
specify an approver
upload a document

Manager notifications
  enabling

Manual Approvals
  Conditions
  Input Variables
  Result Values
  States

manually install
  proxy server

Max User subscriptions

message
  Legacy Notify
  viewing

metric result
  field names
metric types
create

Metric Types
Microsoft Exchange
  activity pack

  configuring MID Server for
  Create Address List
  Create Mailbox
  Delete Address List
  Delete Mailbox
  Disable Mailbox
  Enable Mailbox
  Get Address List
  Get Mailbox
  introduction to
  Move Address List
  Move Mailbox
  passing multivalued properties
  Set Address List
  Set Mailbox
  Update Address List

MID server
  variables

MID Server
  adding privileged commands
  authentication failure
  authorization failure
  auto-assign to subnets
  auto-assignment
  automation status sets
  capabilities
configuration
  capabilities
  IP address range
configure
configure the ALL application
configuring for SCCM
configuring privileged commands for 892, 1275
credentials for 867
dashboard 1219
debug 925
domain separation 1272
guided setup 1181
heartbeat 1173
installation 1180, 1186
installing on Linux 1192
installing on multiple machines 1207
installing on Windows 1197
integrate Edge Encryption 1025, 1025
keypairs used for encryption
rekey the MID Server 1280
logs 1294
mapping IP addresses to DNS names 1277
monitoring 1212
network connectivity testing 1203
pause 1271
pausing 1271
PowerShell authentication failure errors
troubleshooting an Active Directory activity 1574
troubleshooting an Exchange activity 1575
PowerShell troubleshooting 1574
privileged commands for
pbrun special configuration 894, 1274
product overview 1169, 1170
properties 1267
role validation 1188
selection criteria 1223
selection criteria for 1729
set version 1217
setting up role 1186
setup and testing 1211
SNMP OIDs for IP range auto-assignment 1231
specify MID Server applications 1226
starting 1211
statistics 1294
stopping 1211, 1212
troubleshooting RCP server 1576
upgrades 1213
upgrading manually 1218
user compatibility 1299
user connectivity 1306
user connectivity debugging 1313
validation of 1203
version compatibility 1177
MID Server active issues table 1299
MID Server alerts 1301
MID Server cloning issue 1300
MID Server clusters 1296
MID Server Clusters 1295
MID Server configuration
memory size and allocation 1287
MID Server credentials
credential table 899
service account 899
mid server login credentials
encrypting 1279
MID Server requirements
system 1174
MID Server resource thresholds 1301
MID Server signed script file 1283
MID Server upgrade check 1214
MID Server upgrade error messages 1213
MID Servers
and JAR files 1286
deploying 1205
multiple 1205
MIDSSystem
methods 1286
Migrate Knowledge
after migration 1084
default knowledge base 1084
guide 1083
knowledge article view 1085
knowledge portal changes 1086
migrate knowledge content 1089
migrating functionality 1087
publish and retire workflows 1089, 1089
replace modules 1087
security changes 1085
using legacy knowledge 1084
migrate surveys 2088, 2491
migrated survey components 2089, 2492
migrated survey questions
review 2090, 2493
multiple approvers 1990
multiple assessable records
multiple category users, associating 1880, 1882
stakeholders, deleting 1881
Multiple provider ISO 967

N
NetApp storage devices
credentials for 875
NG CI relations formatter 517
notification
calendar integration 173
Notification Activities
Create Event 2738
Notification Activity 2738
notification channels 266
notification message
subscribe 276
notifications
deactivate for surveys 2085, 2488
editing devices 276
email client
configuring email client auto-complete 221
controlling access to 222
creating an email client template 223
customizing 220
displaying an editable form field 225
displaying the Reply To field 225
interface 219
quick messages 226
removing the email icon 228
setting the from address 224
SMS 225
image filtering properties 93
message body limit properties 105
Languages 311
migration 347
mute a participant 298
Notify on task 312
Notify with incident alert 312, 312
Notify with on-call scheduling 317, 317
Number groups 313
On-call: assign by acknowledgement workflow 318
outbound requirements 296
Play activity 307, 2732
Properties 299
queueCall(GlideRecord callRecord) 326
Record activity 308, 2732
Reject activity 308, 2733
Say activity 309, 2734
sendSMS(NotifyPhoneNumber notifyPhoneNumber, String toPhoneNumber, String messageBody, GlideRecord source) 322
sendSMS(NotifyPhoneNumber notifyPhoneNumber, String toPhoneNumber, String messageBody) 322
Tables 299
Twilio service 292
Using SMS 298
variable substitution 2789
WebRTC Client event handlers 343
workflow activities 301, 2729
Notify on task
Conference call from task 312
SMS from task 312
Notify with Incident Alert Management
Conference call 313
conference call information 315
launching 313
sending 317
SMS Notifications 317
viewing 315
Notify with on-call scheduling
NotifyNow key differences 319
Set up 317
NotifyAction
addConference() 335
addDial() 329
addGather() 329
addHangUp() 330
addPlay() 331
addQueue() 330
addReject() 331
addSay() 332
fromJson(String json) 333
NotifyClient
SendDtmf(String digits) 343
NotifyNow
addConferenceCallParticipant(String conferenceCall, String participant) 377
convertLocalPhoneNumberToE164(String userlID, String phoneNumber) 378
getConferenceCallParticipants(String conferenceCallId, Boolean isCallable) 379
getFrequentlyCalledUsers(Number limit) 380
getPreferredE164SMSNumber(GlideRecord user) 381
Languages 311
migration 347
mute a participant 298
Notify on task 312
Notify with incident alert 312, 312
Notify with on-call scheduling 317, 317
Number groups 313
On-call: assign by acknowledgement workflow 318
outbound requirements 296
Play activity 307, 2732
Properties 299
queueCall(GlideRecord callRecord) 326
Record activity 308, 2732
Reject activity 308, 2733
Say activity 309, 2734
sendSMS(NotifyPhoneNumber notifyPhoneNumber, String toPhoneNumber, String messageBody, GlideRecord source) 322
sendSMS(NotifyPhoneNumber notifyPhoneNumber, String toPhoneNumber, String messageBody) 322
Tables 299
Twilio service 292
Using SMS 298
variable substitution 2789
WebRTC Client event handlers 343
workflow activities 301, 2729
Notify on task
Conference call from task 312
SMS from task 312
Notify with Incident Alert Management
Conference call 313
conference call information 315
launching 313
sending 317
SMS Notifications 317
viewing 315
Notify with on-call scheduling
NotifyNow key differences 319
Set up 317
NotifyAction
addConference() 335
addDial() 329
addGather() 329
addHangUp() 330
addPlay() 331
addQueue() 330
addReject() 331
addSay() 332
fromJson(String json) 333
NotifyClient
SendDtmf(String digits) 343
NotifyNow
addConferenceCallParticipant(String conferenceCall, String participant) 377
convertLocalPhoneNumberToE164(String userlID, String phoneNumber) 378
getConferenceCallParticipants(String conferenceCallId, Boolean isCallable) 379
getFrequentlyCalledUsers(Number limit) 380
getPreferredE164SMSNumber(GlideRecord user) 381
getPreferredE164VoiceNumber(GlideRecord user) 380
getPreferredEmailAddress(GlideRecord user) 381
getReadyState() 366
getStatus() 366
initiateConferenceCall(String, String, GlideRecord, Boolean) 368
isCallable(String participant) 369
isSMSCapable() 370
isSMSCapable(String userID) 370
isVoiceCapable() 371
isVoiceCapable(String userID) 371
kick(GlideRecord participant) 372
mute(GlideRecord participant) 372
sendEmailQuestion(String emailAddress, String question, GlideRecord sourceRecord, String emailSubject) 374
sendSMS(String phoneNumber, String smsBody, GlideRecord source) 375
sendSMS(String phoneNumber, String smsBody) 375
sendSMSQuestion(String phoneNumber, String question, GlideRecord sourceRecord) 376
SMS codes 1428, 1761
umute(GlideRecord participant) 373

NotifyPhoneNumber
getDialCode() 336
getID() 336
getNumber() 336
getOwner() 337
getTerritory() 337
supportsConferenceCall() 337
supportIncomingPhoneCall() 338
supportIncomingSMS() 338
supportOutgoingPhoneCall() 338
supportOutgoingSMS() 339
supportsRecording() 339
supportsWebRTC() 339

Now Platform 8

O

ODBC Driver 1021, 1023
ODBC truststore 1023
On-call scheduling with Notify
   Force communication channel 318
on-cancel
   script defining 2667
one assessable record
   one category user, associating 1882
Orchestration
   activating 1326
Active Directory
   example 1478
Active Directory activity pack
   Add User to Group 1487
   Change AD User Password 1488
   Create AD Object 1489
   Disable AD User Account 1491
   Enable AD User Account 1492
   introduction 1486
   Is AD Account Locked 1493
Query AD 1494
Remove AD Object 1495
Remove User from Group 1496
Reset AD User Password 1497
Unlock AD Account 1498

Active directory user management 1478
activities for workflows reactivating deprecated activities 1338
activity designer
   activity scoping 1721
   auto-mapping JDBC output variables 1637, 1659
   auto-mapping REST output variables 1688
   auto-mapping SOAP output variables 1666
   creating custom activities 1623
   JavaScript probe activity, creating 1676
   JavaScript Probe execution command 1679
   JavaScript probe execution parameters 1677
   JavaScript probe template post-processing parameters 1678
   JDBC activity, creating 1654
   JDBC connections 1657
   JMS activity system setup 1718
   JMS activity, creating 1717
   JMS execution parameters 1719
   JMS template post-processing parameters 1720
   mapping output variables 1640
   output variables 1637
   parsing rules example 1646
   parsing rules, creating 1641
   parsing sources 1645
   PowerShell 1564
   PowerShell activity, creating 1681
   Powershell execution command 1629
   Powershell execution parameters 1682
   Powershell template post-processing parameters 1684
   Pre-processing fields 1634
   Probe activity, creating 1706
   Probe execution command 1708
   Probe execution parameters 1706
   Probe template post-processing parameters 1707
   REST activity, creating 1686
   REST execution command 1691
   REST execution parameters 1689
   REST execution parameters, JavaScript array in 1690
   REST template post-processing parameters 1691
   reusing data 1725
   run script activity, creating 1716
   Run Script processing script 1717
   SFTP activity, creating 1695
   SFTP execution command 1701
   SFTP template post-processing parameters 1700
   SOAP activity, creating 1665
   SOAP execution command 1670
   SOAP execution parameters 1673
SOAP execution parameters, JavaScript array in 1675
SOAP input variables 1627
SOAP template post-processing parameters 1675
SSH activity, creating 1710
SSH execution command 1714
SSH execution parameters 1711
SSH template post-processing parameters 1712
Template outputs 1639
Template post-processing fields 1635
templates 1654
testing input fields 1631
testing JDBC input fields 1661
variables, mapping 1628
activity packs requesting activation 1336
applications included with 1346
Azure AD activity pack
Add User to Group 1500
Assign User License 1501
Create User 1502
Delete User 1504
Get User Info 1505
Remove User from Group 1507
Remove User License 1508
Reset User Password 1509
basic activities 1337
client software distribution
SCCM deployment workflow 1389
client software distribution (CSD)
activating 1366
components installed with 1367
configuring providers 1395
creating catalog items for SCCM applications 1386
creating software models for SCCM 1382
dashboard 1393
deploying software from SCCM 1376
extension keys 1396
extension points 1394, 1396
introduction to 1365
lease extensions 1374
licenses and counters for 1371
ordering software from the service catalog 1372
plugins installed with 1368
properties for 1369
providing Windows credentials for SCCM 1379
retrieving SCCM data for 1380
roles installed with 1368
SCCM configuration 1382
SCCM server Discovery 1381
SCCM software revocation workflow 1392
script includes installed with 1369
tables installed with 1367
validating installations 1390
workflows installed with 1371
configuring client software distribution
revoking software not installed by SCCM 1391
credentials testing 899
credentials for
activating external storage 907
affinity 902
Amazon Web Services (AWS) 871
basic authentication 872
checking IP service affinity 904
CIM 874, 884, 885
cloud management 875
configuring external storage 910
configuring identifier of 915
creating 869
CyberArk integration 917
external storage 907
external storage architecture 908
importing a JAR file for resolution of 914
JDBC 878
JMS 880
Linux 888
MID Server from credentials table 899
MID Server from service account 899
NetApp storage devices 875
SAP JCo 881
SNMP 882
SNMP community 882
SSH private key 886
UNIX 888
VMware 895
Windows 896
Windows domain requirements 898
Windows permission requirements 897
Windows requirements 898
data encryption 1634
databus 1724
documentation links for 1323
example 1478
eamples 1478
Exchange activity pack
configuring MID Server for 1511
Create Address List 1512
Create Mailbox 1520
Delete Address List 1513
Delete Mailbox 1522
Disable Mailbox 1523
Enable Mailbox 1525
Get Address List 1515
Get Mailbox 1526
introduction to 1510
Move Address List 1516
passing multivalued properties 1512
Set Address List 1517
Set Mailbox 1527
Update Address List 1519
F5 custom activities 1529
F5 Network Management activity pack
Add F5 Pool 1538
Add F5 Pool Member 1529
Add F5 Profile to Virtual Server 1533
Add F5 Virtual Server 1535
Check F5 Pool 1532
Delete F5 Pool 1537
Delete F5 Pool Member 1536
Delete F5 Virtual Server 1531
Get F5 Pool Member 1530
Modify F5 Virtual Server 1534

Global activities
introduction 1618
how probes work 1340

Infoblox activity pack
Create Network 1558
Delete Network 1561
DHCP activities 1544
DHCP Delete IP Reservation 1545
DHCP List IP Reservations 1546
DHCP Reserve IP v4 Address Range 1544
DNS activities 1547
DNS Delete 1552
Get Network Details 1559
IPAM activities 1554
IPAM Delete 1557
IPAM List IP Reservations 1556
IPAM Register IP Address 1554
IPAM Reserve IP Address 1555
List DNS C-records 1547
List DNS Record 1551
List Registered Networks 1562
network activities 1558
Register DNS A-record 1548
Register DNS C-Record 1550
REST credential for 1539
roles and permissions needed 1541
workflows included with 1540
introduction to 1323
list of activities 1330
list of plugins 1327
MID Server autofinder
mapping IP addresses to DNS names 1277
MID servers 1726
PowerShell
credential tagging 1571
PowerShell activities
enable WMI Windows Installer Provider 1580
PowerShell activities
basic 1342
Run PowerShell 1342
PowerShell activity pack
Change Service State 1580
Install Windows App 1579
Join Domain 1578
Restart Windows Server 1581
Uninstall Windows App 1582
PowerShell activity pack
HResult codes 1345
introduction 1564
PowerShell protocols
introduction to 1564
MID Server PowerShell files 1565
probe activities
Resolve DNS Name 1583
SNMP Query 1584
Test Server Alive 1619
Probe activity pack 1583
publishing custom activities 1722
returning locked activity to published state 1722
runtime plugin 1329

SCCM activity pack
activating 1586
Add to Device Collection 1587
Add to User Collection 1588
configuring MID Server for 1379, 1586
Get Applications 1589
Get Deployments 1590
Get Device Collections 1592
Get User Collections 1593
introduction to 1585
Remove from Device Collection 1596
Remove from User Collection 1597

SCCM software revocation
revoking software installed by SCCM 1390

SFTP File Transfer activity pack
Copy File 1603
Create Directory 1604
Get File List 1605
Remove File or Directory 1606
Rename File or Directory 1608
Set File Attributes 1609
workflow included with 1598

SSH activity pack
File Copy 1615
File Read 1612
Files Compare 1611
Secure Copy 1610

SSH legacy activities
File Replace String 1615
File Write 1613
introduction to 1345
Reset Linux User Password 1617
Run Command 1345
Run SCP 1346

Update AD Object custom activity 1499

Orchestration ROI
automation entry record 1347
correlated task rules 1349
installed components
business rules 1353
client scripts 1352
plugins 1351
roles 1351
script includes 1352
tables 1350
UI actions 1351
introduction 1346
labor rate card 1347
premium reports
scheduled job for 1365
reports
activating premium plugin 1364
introduction to 1353
premium 1362
standard 1353
standard reports
properties for 1361
scheduled job for 1361
time range for calculations 1350

Order-preserving database 950
Order-preserving encryption 939

© 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.
Password Reset CMS Integration

password reset
Password Change
  - design the process
  - reports
  - password reset
    - activate
    - enroll
    - enroll SMS
    - password reset orchestration add-on
    - SMS codes
  - Password Reset
    - Active Directory
    - advanced configuration
    - CAPTCHA
    - credential store connections
    - credential stores
    - custom credential stores
    - custom identifications
    - custom verifications
    - customize
    - data confirmation
    - design the process
    - Details tab
    - enrollment
    - example scripts
    - extension scripts
    - installed with
    - NotifyNow SMS verification
    - overview
    - personal data
    - plan the process
    - properties
    - reports
    - script includes
    - Security Questions
    - service desk-assisted
    - SMS verification
    - SOAP credentials
    - unblock users
    - user lockout
    - user requests
    - verification types
    - verifications
    - Windows Application

Pending
  - allocation to subscriptions
  - Per-User subscriptions
  - Perform Data Certification
    - cancel a certification instance
    - cancel all tasks in an instance
    - cancel an individual task
    - cancel certification tasks
    - certification task form
    - certification task list
    - certify an element
    - escalate a certification task
    - export the certification list
    - fulfill certification tasks
    - mark certification task as closed incomplete
    - reassign a certification task
    - reset certifications
    - send certification task reminders
    - send email reminder
    - track a certification task
    - track task with certification instance
    - view an audit result

Performance analytics
  - dashboards
  - connect support
  - pfexec commands
  - pinning
    - in workflows
  - Planning Data Certification
    - 775, 775, 780, 783, 784, 785, 786
  - platform
    - plugins, subscription
    - populate CMDB
    - computer information
    - post content in live feed
      - add @mentions
      - add a knowledge article link
      - add a link
      - add a poll
      - attach files
      - attach images
      - attach knowledge articles
      - attach links
      - clipboard
      - copy an image
      - delete a message
      - like a message
      - message
      - messages
      - post
      - reply
      - reply to a message

Powershell
  - Change Service State activity
  - Install Windows App activity
  - Join Domain activity
  - Restart Windows Server activity
  - Uninstall Windows App activity

PowerShell
  - HResult codes
  - Orchestration activity pack
protocols
   introduction to 1564
   MID Server PowerShell files 1565, 1571
troubleshoot authentication failure
   Active Directory activity 1574
troubleshooting 1574
troubleshooting authentication failure
   Exchange activity 1575
troubleshooting RCP server 1576
privileged commands
   adding for MID Server 892, 1274
   configuring for MID Server 892, 1275
MID Server
   pbrun special configuration 894, 1274
probe activities
   Resolve DNS Name 1583
   SNMP Query 1584
   Test Server Alive 1619
Probe activity pack
   introduction 1583
problem management
   creating knowledge 1086
properties
   Legacy Notify
      editing 359
      viewing 359
   MID Server 1267
Properties
   Notify 299
proposed changes
   create validation script 514
   edit validation script 514
   verify 513
proxy database 950
Proxy database
   size 939
proxy server
   set initial memory 963
   set memory 963
   set upper bound memory 963
proxy server installation 955
publish a document
   managed documents 1143

quizzes
   activate 1922, 2094
   administer 1919, 2093
   categories 1920, 2091
   category user 1920, 2091
   create 1926, 2098
   process 1919, 2093
   questions 1920, 2091
   roles 1920, 2091
   set up 1919, 2093
   templates 1920, 2091

R
   Reconciliation 561
   record feed 465, 466
   record feeds
      add live feed 424, 425
      configure 424
      configure security 425
      context menu 425
      disable 422, 425
      form header 424
   relationship editor
      filter list of CI relationships 524
      select a CI relationship type 524
      select targets 524
   relationship filter
      create 520
      edit 520
   report lowest table
      Glide hierarchy 2639
   reports
      Orchestration ROI
         premium 1362
         standard 1353
      premium for Orchestration ROI
         activating plugin 1364
      subscriptions 2406, 2408
   request
      getAsJsonContent() 997, 1001
      getAsXmlContent() 998, 1001
      XMLContains(String path) 998
   request API 997
   reset your password 1475, 1809
response
   Legacy Notify
      choice 350
      creating 350
   REST API 229
   ROI for Orchestration
      automation entry records 1347
      correlated task rules 1349
      installed components
         business rules 1353
         client scripts 1352
         plugins 1351
         roles 1351
         script includes 1352
         tables 1350
         UI actions 1351
      introduction to 1346
labor rate cards 1347
premium reports
  scheduled job for 1365
properties for 1361
standard reports
  scheduled job for 1361
time range for calculations 1350
roles
desired state 688
MID Server 1186
rollback to
  behavior 2720, 2786
Rollback To
  States 2719
rollback to activity 2722, 2786
RSA key pair 947

S

SAP credentials 881
SCCM
  configuring collections for 1382
  creating catalog items for 1386
  creating software models for 1382
  deploying software with client software distribution (CSD) 1376
  deployment workflow 1389
  discovering SCCM server 1381
  lease extensions 1374
  ordering software from the service catalog 1372
  retrieving data for client software distribution 1380
  revoking software installed by 1390
  revoking software installed by another process 1391
  revoking software with 1390
  software revocation workflow 1392
validating deployments 1390
Windows credentials for 1379
SCCM activity pack
  activating 1586
  Add to Device Collection 1587
  Add to User Collection 1588
  configuring MID Server for 1379, 1586
  Get Applications 1589
  Get Deployments 1590
  Get Device Collections 1592
  Get User Collections 1593
  introduction to 1585
  Remove from Device Collection 1596
  Remove from User Collection 1597
SCCM cmdlet libraries 1378
SCCM configuration 1376
SCCM roles 1376
schedules
  Notification conditions 267, 267
scorecard
  view 2016, 2419
scorecards
  averages 1909
categories 1910
category metrics 1911
  head to head compare 1912
history 1915
links
  create 1907
  live feed 1916
surveys
  average ratings 2021, 2424
category results 2017, 2420
history 2023, 2426
question results 2019, 2422
  view 1907
Scorecards
  ratings 1919
script
  on-cancel
    defining 2667
    parameters 673
script includes
  installed with live feed 438
Scripted Audits
  scripting methods 756
search
  Service Portal 2160, 2345, 2346, 2351, 2355, 2356, 2383, 2387
Security
  Orchestration Runtime plugin 1329
Security Questions
  Password Reset 1433, 1442, 1767, 1775
self-service password reset 1416, 1749
self-signed certificate 1023
send document out
  approval 1144
  review 1144
Server scripting
  email notifications 145
Server Scripting
  email notifications
    changing link text 141
    enabling links 140
    example scripts 147
    linking to related records 141
    mail script API 146
    using JavaScript 145
  mail script API 146
  using JavaScript 145
service administration 1825
Service Catalog
  UI Macro 2193
Service Catalog forms 2181
Service Catalog requests
  add new request items 1812
  create incident
    create change request 1818
  delete request items 1815
  place a request 1816
  view request status 1819
service delegation 1822, 1823
Service Desk 411, 412
Service Mapping
  credentials for
    applicative credentials 870
    MID Server 1174
service portal 2155, 2304
Service Portal

advanced search source 2351, 2355, 2356, 2383, 2387
before you begin 2132
carousel widget slides 2210
CMS 2175
Config Overview widget 2285
contextual search 2359
create user criteria 2169, 2367
debug URL redirects 2362, 2380
edit widget option schema 2310
KB News Widget 2251
KB search widget 2252
KB View 2 2256
KB View widget 2254
Language Switch widget 2225
Link button widget 2226
login page configuration 2361, 2379
login widget 2226
My Favorite Tags widget 2256
My Requests widget 2226
nested widgets 2317
page create 2149
Page Map widget 2289
portal 2140
Portal Config widget 2287
Portal Map widget 2289
properties 2136
public pages 2362
redirect after login 2361, 2380
role-based pages 2362
Sample Footer widget 2234
Save Bundles widget 2276
Saved Carts widget 2277
search 2345
Search Page widget 2244
search source 2160, 2346
shopping cart widget 2279
Simple List widget 2232
sp_instance extension table 2312
Stock widget 2235
Subscribed Questions widget 2263
Theme Preview widget 2289
URL redirects 2360, 2379
user criteria 2165, 2363
Variable Editor widget 2265
Weather widget 2239
widget 2157, 2306
widget dependencies 2322
Widget Edit Panel widget 2291
widget instance options 2297, 2309
widget localization 2328
widget option schema 2312
widget user criteria 2171, 2369
Service Portal and Connect Support 59
Service Portal approvals widget 2203
Service Portal breakout game widget 2208
Service portal business service status widget 2291
Service Portal carousel widget 2209
Service Portal configuration page widgets 2285
Service Portal Connect Support 59
Service Portal Contextual Search widget 2240
Service Portal Cool Clock widget 2212
Service Portal current status widget 2293
Service Portal data table widget 2213
Service Portal default search sources 2358
Service Portal example widgets 2203
Service Portal font icon in a widget 2323
Service Portal font-icons in a widget dependency 2326
Service Portal home page search widget 2242
Service Portal HTML widget 2221
Service Portal Icon Link widget 2222
Service Portal icon menu list widget 2223
Service Portal KB also in Category widget 2245
Service Portal KB article page widget 2246
Service Portal KB categories widget 2248
Service Portal KB category page widget 2249
Service Portal KB most viewed widget 2250
Service Portal KB Top Rated widget 2253
Service Portal knowledge management widgets 2245
Service Portal list of widgets 2202
Service Portal Planned Maintenance widget 2293
Service Portal Popular Questions widget 2257
Service Portal Request Fields widget 2267
Service Portal Requested Items widget 2268
Service Portal SC Catalog Item widget 2269
Service Portal SC Category Page widget 2274
Service Portal SC Order Guide widget 2275
Service Portal SC Popular Items widget 2276
Service Portal SCSS 2373
Service Portal SCSS mixins 2378
Service Portal SCSS nesting 2377
Service Portal SCSS operators 2378
Service Portal SCSS variables 2374
Service Portal search widgets 2240
Service Portal security 2360
Service Portal service catalog widgets 2265
Service Portal Service History 2294
Service Portal Service Status legend widget 2296
Service Portal Service Status Subscription widget 2296
Service Portal Service Status widget 2295
Service Portal service status widgets 2291
Service Portal setup 2138
Service Portal SQANDA Create Question widget 2258
Service Portal SQandA Question widget 2259
Service Portal SQandA Related Question widget 2261
Service Portal supported and unsupported scripts 2200
Service Portal supported client scripts 2195
Service Portal Tagged Question List widget 2263
Service Portal Ticket Attachments widget 2236
Service Portal Ticket Conversations widget 2236
Service Portal Ticket Location widget 2238
Service Portal Typeahead Search widget 2241
Service Portal unsupported client scripts 2195
Service Portal unsupported features 2194
Service Portal User Profile widget 2238
Service Portal video configuration 2373
Service Portal widget showcase 2202
Service Portal widgets 2200, 2298, 2329, 2330, 2332, 2333, 2335, 2338
Service Release Automation Orchestration Runtime plugin 1329

© 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.
Setting Up Chat Queues for Help Desk Chat
  add custom link 417
  assign service desk staff 415
  chat queue 415
  define a chat queue 414
  end user 416
  ess portal 417
  help desk chat 416
  link syntax 417
  monitor chat queues 418
  monitor help desk chat tasks 418

SSH activity pack
  File Copy 1615
  File Read 1612
  Files Compare 1611
  introduction 1610
  Secure Copy 1610

SSH credentials 885
SSH legacy activities
  introduction 1345
  Reset Linux User Password 1617
  Run Command 1345
  Run SCP 1346

SSH private key credentials 886
state flows
  installed components
    business rules 1999
    script includes 2000
    tables 1998
  rebuilding 2000

State Flows
dictionary overrides 2000
field controls 2000
triggered events 2000

Strong identification rule 562
design theme 853
design themes 853
frame 854
frame UI macro 855

Style in Content Management
style sheets 853

subflow activities
  parallel flow launcher example 2767
  parallel flow launcher for 2763
  parallel flow launcher input variables 2763
  script values in 2767
  WorkflowCoordinator object in 2766

subflows
  inputs for 2581
  invoking in a parent workflow 2582
  preparing for use in a parent workflow 2582
  variables passed from parent workflow 2581

subscription
  sync to user sets 2400
  subscription allocation
    color codes 2408
  Subscription form 2391
  subscription histories 2394

Subscription Management
  allocate users 2401, 2402, 2403
  color codes 2408
  exclude users 2404
  pending users 2403
  unexclude users 2404
  user sets 2398

Subscription Management admin guide 2390
Subscription Management setup guide 2389
Subscription Overview page 2406
subscription plugins 2394
subscription reports 2406, 2408

© 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.
subscription types 2393
subscription user sets 2398
subscriptions
allocate users to 2396
monitoring 2404
not in list 2395
Subscriptions list 2390
sudo commands
for SSH 891
long running 894
suggested CI relationship
add 517
survey
create groups 2052, 2455
groups 2052, 2053, 2455, 2456
module 2086, 2489
send invitations 2083, 2486
users 2052, 2053, 2455, 2456
view instances 2050, 2453
Survey
groups 2051, 2454
users 2051, 2454
survey administration
survey definition 2056, 2459
survey category
create in survey 2038, 2441
survey definitions
modify 2056, 2459
schedule periods 2060, 2463
survey designer
configuring a survey in 2036, 2439
elements 2032, 2435
template questions 2060, 2464
survey management
categories 2037, 2440
category create 2038, 2441
category weights
survey designer 2050, 2453
key terms 2009, 2412
questions 2064, 2467
roles 2008, 2411
scorecards
average ratings 2021, 2424
category results 2017, 2420
history 2023, 2426
question results 2019, 2422
survey designer
allow retakes 2053, 2456
categories 2037, 2441
category weights 2050, 2453
edit survey 2049, 2452
publishing a survey in 2054, 2457
questions 2038, 2441
select survey recipients 2052, 2455
survey results 2011, 2414
Survey Management 2006, 2409
survey properties 2065, 2458
survey question migration 2089, 2492
survey questionnaires 2010, 2413
survey questions
change answer options 2076, 2479
changing order 2077, 2480
create or update 2064, 2467
create template 2075, 2478
min max values 2076, 2479
template 2075, 2478
survey results
view 2014, 2417
view all 2013, 2416
surveys
auto-notification 2085, 2488
customize appearance 2054, 2457
designing 2032, 2435
distribute 2083, 2486
distribute URL 2085, 2488
export 2086, 2087, 2489, 2490
import 2086, 2489
instance URL 2085, 2488
question data types 2041, 2067, 2444, 2470
Service Portal 2029, 2432
survey definitions 2056, 2459
survey designer elements 2032, 2435
take 2010, 2413
test survey URL 2086, 2489
update sets 1872, 2087, 2490
URLs 2084, 2487
sync subscription 2400
T
table access
live feed 433
table notifications
live feed examples 429
setting up for non-task tables 428
Tables
Notify 299
tables installed with live feed 437
Task Activities 2745, 2745, 2745, 2746, 2749, 2784
task table notifications
live feed 426
tasks
delegate 1823
technical best practices 2303
Tests
managing 738, 740, 741, 745, 746
Time
view system logs 102
Timeline Visualization
create 2498
create view 2502
use Timeline Visualization 2503
timeline visualizations
installed components 2510
Timeline Visualizations
lanes, markers, and panels 2503
personalize Timeline Visualizations 2504
slider and slider track 2508
view timeline visualizations 2508
work with timeline visualizations 2509
Tokenization 939
transitions that do not terminate on an activity
reporting 2636
trigger condition
create 2078, 2481
for assessments 1889
trigger conditions 2078, 2481
Twilio
  account associating 355
  endpoints configuring 357
  Legacy notify configuring 355

U
UI Macro
  Service Portal 2193
unexclude
  users from subscriptions 2404
UNIX
  commands requiring root privileges 889
  credentials 888
Unlimited subscriptions 2393
unsubscribe
  users from subscriptions 2403
update sets
  use with assessments 1872, 2087, 2490
  use with surveys 1872, 2087, 2490
upgrade
  proxy server 979
Upgrade test 1214
upgrading
  MID Server version 1217
upload document
  attachment 1144
usage
  subscriptions 2404
Use Chat
  add a favorite room 404
  add favorite user 393
  change the display 403
  chat window 400
  create a chat room 395, 397
  delete a chat room 405
  invite a user 404
  join chat room 399, 399, 400
  join one-to-one chat 399
  message 402
  remove a favorite room 404
  remove favorite user 393
  send emoticons 402
  send message 401
  set chat preferences 404
  start a one-to-one chat 395
  task 397, 399
  task record 400
  update profile 388
  update status 389
  use favorites list 391
  view a room 394
  view online user 393

use feeds in live feed
  activity stream 469
  create a group feed 468
  create record feeds 469
  delete a feed 476
  group feed 473
  invite a new member 473, 473
  leave a feed 476
  live feed 469, 476
  mark a feed as a favorite 472
  navigate 476
  other modules 476
  participate in a feed 471
  record feed 473
  record feeds 469
  records 469
  remove a member from a feed 474
  subscribe to a feed 475
  view a feed 473
  view a feed member 473

use hashtags in live feed
  add an image to a hashtag 446
  bookmark a hashtag 448
  change a hashtag 445
  follow a hashtag 447
  merge a hashtag 445
  posted message 449
  remove a hashtag 449
  tag messages 443
  unfollow a hashtag 447
  view available hashtags 444

use knowledge
  mobile 1080

use teams in live feed
  automatic team creation 453
  create a team 450
  delete a team 458
  email 456
  email notification 455
  feed notification 456
  invite a new member 453
  join a team 453
  leave a team 456
  manage 456
  membership request 456
  modify a team 456
  remove a member 454
  reply to notifications 456
  subscribe 455, 456
  team 456
  team notification 455
  view a team feed 453
  view a team member 453

useful attachment scripts 148
user creation
  enabling automatic creation 199
user criteria
  Service Portal 2165, 2363
user notification preferences
  channels 260
  conditions 260
  global switch 260
notification channels 266
User notification preferences
create channels 264
user notification preferences UI15 274
user notification preferences UI16 260
user roles
installed with live feed 438
user set 2399, 2401
user sets 2398
users
allocate to subscriptions 2401, 2402
exclude from subscriptions 2404
pending allocation 2403
unexclude from subscriptions 2404
unsubscribe 2403
using approval rules
generate approvals 1989
using approvers related list
generate approvals 1990
using social IT
post content in live feed 490, 492, 492, 494, 496, 497, 497, 499, 500, 501
post content in Live Feed 489
record feeds 422, 423, 424, 424, 425, 425
use feeds in live feed 468, 469, 469, 469, 471, 472, 473, 473, 473, 474, 475, 476, 476, 476
use feeds in Live Feed 468
use hashtags in live feed 443, 444, 445, 446, 447, 448, 449
use hashtags in Live Feed 443
use teams in Live Feed 450
Using Social IT
use chat 388, 389, 391, 393, 393, 393, 394, 395, 395, 397, 399, 399, 399, 400, 400, 401, 402, 403, 404, 404, 404, 405
using workflows
generate approvals 1990
Using Workflows
workflow concepts 2651, 2652, 2652, 2653, 2653, 2654, 2656, 2656, 2658, 2660, 2660
utility activities
branch activity 2753
join activity 2753
lock activity 2754
log message activity 2757
log trace message 2757
REST message activity 2757
Return value activity 2759
Run script activity 2759
set values activity 2759
SOAP message activity 1338, 2760
turnstile activity 2761
unlock activity 2762
workflow 2753
Utility Activities
join activity 2574
V
Verifications configuring 1428, 1761
view
bubble charts 1902
survey results 2014, 2417
view legacy chat messages
journal field 406
View System Logs
e-mail logs 102
viewing
calls
conference 352
call 352
Legacy notify
conversation 351
properties 359
Legacy Notify
message 351
question 348
properties
Legacy Notify 359
visual task boards
activate 2512
attachments 2529
board structure 2516
browser support 2516
card details 2525
checklists
configuring 2535
creating from templates 2534
creating new 2533
deleting 2534
client script 2516
configuring 2545
connect
sharing visual task boards in 30, 41, 2545, 2545
deleting 2521
favorite 2539
flexible boards
adding tasks to 2524
configuring card limit 2548
creating 2520
freeform boards
adding personal tasks to 2523
adding tasks to 2523, 2524
configuring card limit 2548
creating 2520
moving cards between boards 2537
tasks 2522
guided boards
adding tasks to 2524
configuring card limit 2548
creating 2520
installed components
business rules 2514
client scripts 2514
notifications 2515
properties 2513
tables 2513

card details 2525
checklists
configuring 2535
creating from templates 2534
creating new 2533
deleting 2534
client script 2516
configuring 2545
connect
sharing visual task boards in 30, 41, 2545, 2545
deleting 2521
favorite 2539
flexible boards
adding tasks to 2524
configuring card limit 2548
creating 2520
freeform boards
adding personal tasks to 2523
adding tasks to 2523, 2524
configuring card limit 2548
creating 2520
moving cards between boards 2537
tasks 2522
guided boards
adding tasks to 2524
configuring card limit 2548
creating 2520
installed components
business rules 2514
client scripts 2514
notifications 2515
properties 2513
tables 2513

card details 2525
checklists
configuring 2535
creating from templates 2534
creating new 2533
deleting 2534
client script 2516
configuring 2545
connect
sharing visual task boards in 30, 41, 2545, 2545
deleting 2521
favorite 2539
flexible boards
adding tasks to 2524
configuring card limit 2548
creating 2520
freeform boards
adding personal tasks to 2523
adding tasks to 2523, 2524
configuring card limit 2548
creating 2520
moving cards between boards 2537
tasks 2522
guided boards
adding tasks to 2524
configuring card limit 2548
creating 2520
installed components
business rules 2514
client scripts 2514
notifications 2515
properties 2513
tables 2513

card details 2525
checklists
configuring 2535
creating from templates 2534
creating new 2533
deleting 2534
client script 2516
configuring 2545
connect
sharing visual task boards in 30, 41, 2545, 2545
deleting 2521
favorite 2539
flexible boards
adding tasks to 2524
configuring card limit 2548
creating 2520
freeform boards
adding personal tasks to 2523
adding tasks to 2523, 2524
configuring card limit 2548
creating 2520
moving cards between boards 2537
tasks 2522
guided boards
adding tasks to 2524
configuring card limit 2548
creating 2520
installed components
business rules 2514
client scripts 2514
notifications 2515
properties 2513
tables 2513

card details 2525
checklists
configuring 2535
creating from templates 2534
creating new 2533
deleting 2534
client script 2516
configuring 2545
connect
sharing visual task boards in 30, 41, 2545, 2545
deleting 2521
favorite 2539
flexible boards
adding tasks to 2524
configuring card limit 2548
creating 2520
freeform boards
adding personal tasks to 2523
adding tasks to 2523, 2524
configuring card limit 2548
creating 2520
moving cards between boards 2537
tasks 2522
guided boards
adding tasks to 2524
configuring card limit 2548
creating 2520
installed components
business rules 2514
client scripts 2514
notifications 2515
properties 2513
tables 2513

card details 2525
checklists
configuring 2535
creating from templates 2534
creating new 2533
deleting 2534
client script 2516
configuring 2545
connect
sharing visual task boards in 30, 41, 2545, 2545
deleting 2521
favorite 2539
flexible boards
adding tasks to 2524
configuring card limit 2548
creating 2520
freeform boards
adding personal tasks to 2523
adding tasks to 2523, 2524
configuring card limit 2548
creating 2520
moving cards between boards 2537
tasks 2522
guided boards
adding tasks to 2524
configuring card limit 2548
creating 2520
installed components
business rules 2514
client scripts 2514
notifications 2515
properties 2513
tables 2513

© 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.

2817
<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>2547</td>
<td>labels</td>
</tr>
<tr>
<td>2521</td>
<td>lanes</td>
</tr>
<tr>
<td>2521</td>
<td>adding</td>
</tr>
<tr>
<td>2521</td>
<td>deleting</td>
</tr>
<tr>
<td>2521</td>
<td>modifying</td>
</tr>
<tr>
<td>2522</td>
<td>members</td>
</tr>
<tr>
<td>2542</td>
<td>adding</td>
</tr>
<tr>
<td>2542</td>
<td>removing</td>
</tr>
<tr>
<td>2516</td>
<td>script</td>
</tr>
<tr>
<td>2516</td>
<td>scripting support</td>
</tr>
<tr>
<td>2543</td>
<td>SLA indicators</td>
</tr>
<tr>
<td>2535</td>
<td>archiving</td>
</tr>
<tr>
<td>2528</td>
<td>assigning</td>
</tr>
<tr>
<td>2527</td>
<td>labels</td>
</tr>
<tr>
<td>2537</td>
<td>moving between boards</td>
</tr>
<tr>
<td>2536</td>
<td>moving between lanes</td>
</tr>
<tr>
<td>2536</td>
<td>opening form view of</td>
</tr>
<tr>
<td>2516</td>
<td>types</td>
</tr>
<tr>
<td>2520</td>
<td>using</td>
</tr>
<tr>
<td>2538</td>
<td>viewing board information</td>
</tr>
<tr>
<td>2514</td>
<td>installed components script includes</td>
</tr>
<tr>
<td>2563</td>
<td>Visual Task Boards list view</td>
</tr>
<tr>
<td>895</td>
<td>VMware credentials</td>
</tr>
<tr>
<td>2549</td>
<td>VTB card view configuration</td>
</tr>
</tbody>
</table>

**Workflow**

- Documentation tab 2563
- estimated run time 2686
- estimated run time updates 2687
- Estimated Runtime tab 2563
- execution history table 2689
- execution path timelines 2688
- gauges 2692
- General tab 2563
- History (Past Contexts) tab 2563
- Inputs tab 2563
- monitor 1729, 2691
- Orchestration Usage Dashboard 1729
- outlying run times 2687
- overview 2549, 2549, 2661
- properties 2563
- run time metrics, enable 2686
- run time metrics, overview 2686
- Schedule tab 2563
- Stages tab 2563
- troubleshoot 2688
- variables 2588, 2588, 2588, 2589, 2590, 2590, 2591, 2591, 2592, 2592, 2592, 2593
- Version tab 2563
- Workflow Operations Dashboard 2691

**Workflow activities**

- activity designer 2693
- activity result value 2783
- adding to a workflow 2776
- core 2693
- correcting skipped activities 2785
- creating custom transitions 2781
- duplicating in a workflow 2778
- elements listed 2775
- locked versions 2790
- managing conditions 2781
- managing transitions between 2779
- Orchestration 2693
- pinning introduction 2791
- publishing a custom activity 2790
- utility activities 1338, 2753, 2753, 2753, 2754, 2757, 2757, 2757, 2759, 2759, 2759, 2760, 2761, 2762
- viewing descriptions of 2774

**Workflow activities overview**

Multiple timer activities in one workflow 2790