



## **Cisco Catalyst Center ITSM Integration Guide, Release 2.3.7.x**

**First Published:** 2023-12-20

**Last Modified:** 2025-06-24

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023–2025 Cisco Systems, Inc. All rights reserved.



# CONTENTS

<b>CHAPTER 1</b>	<b>New and Changed Information 1</b>
	New and changed information 1
<b>CHAPTER 2</b>	<b>About Catalyst Center ITSM Integration 3</b>
	Catalyst Center integration use cases 3
	Catalyst Center ITSM support 3
<b>CHAPTER 3</b>	<b>Catalyst Center ITSM Integration Workflows 5</b>
	Catalyst Center integration supported workflows 5
	Catalyst Center integration with a generic REST endpoint 5
	Configure network events 6
	Configure event settings 8
	Catalyst Center integration with ServiceNow without the Cisco Catalyst app 9
	Configure the network issue monitor and enrichment for ITSM (ServiceNow) bundle 10
	Configure event settings 14
	Configure the automation events for ITSM (ServiceNow) bundle 15
	Catalyst Center integration with ServiceNow using the Cisco Catalyst app 20
	Requirements 22
	Configure the basic ITSM (ServiceNow) CMDB synchronization bundle 23
	Configure the network issue monitor and enrichment for ITSM (ServiceNow) bundle 33
	Configure event settings 36
	Configure the automation events for ITSM (ServiceNow) bundle 38
	Configure the Cisco SD-Access integration with ITSM (ServiceNow) 42
	Catalyst Center endpoint attribute retrieval with ServiceNow 46
	Requirements 47
	Configure the Endpoint Attribute Retrieval Bundle with ITSM (ServiceNow) 48

---

**CHAPTER 4****SWIM Closed Loop Automation 55**

About SWIM closed loop automation 55

SWIM closed loop automation requirements 56

SWIM closed loop automation workflow 56

---

**CHAPTER 5****Catalyst Center-to-PagerDuty Integration 63**

About Catalyst Center-to-PagerDuty integration 63

Subscribe Catalyst Center event notifications to PagerDuty 64

---

**CHAPTER 6****Catalyst Center-to-Cisco Webex Integration 67**

About Catalyst Center-to-Cisco Webex integration 67

Subscribe Catalyst Center event notifications to Cisco Webex 68



# CHAPTER 1

## New and Changed Information

- [New and changed information, on page 1](#)

### New and changed information

This table summarizes the new and changed features for this release.

**Table 1: New and changed features**

Feature	Description
Independent ITSM Integration for AutomationWorkflows	<p>With this release, you can choose to enable or disable ITSM integration for Group Based Policy, Network Provisioning or SWIM automation workflows, independent of each other, while configuring the automation bundle.</p> <p>See <a href="#">Configure the automation events for ITSM (ServiceNow) bundle, on page 15</a>.</p>
Closed Loop Automation for Assurance Events	<p>This release supports closed loop automation for assurance events between Catalyst Center and ServiceNow.</p> <p>When an assurance event or issue is ignored or resolved in Catalyst Center, an update is sent to ServiceNow irrespective of the endpoint (Event Management/REST API Endpoint/Generic REST API Endpoint) configured in the Network Issue Monitor and Enrichment for ITSM bundle.</p> <p>See <a href="#">Configure the network issue monitor and enrichment for ITSM (ServiceNow) bundle, on page 10</a>.</p>
Name Change to Catalyst Center	<p>As part of our vision to converge our products around an integrated platform, we are changing the name of Cisco DNA Center to Catalyst Center in this release. The capability and functionality of Catalyst Center remains the same as Cisco DNA Center.</p>
Name Change to Cisco Catalyst App	<p>The Cisco DNA app on the ServiceNow Store is rebranded as Cisco Catalyst from app version 2.3.1 onwards.</p> <p>The previous versions of the app are still called Cisco DNA, and you can continue using them with the corresponding release versions of Catalyst Center.</p>

Feature	Description
ITSM Integration API	<p>This release supports a new <b>ITSM Integration</b> API to retrieve the ITSM integration status.</p> <p>For more information, see <b>ITSM Integration API</b> in the <a href="#">Cisco Catalyst Center Release Notes</a>.</p>



## CHAPTER 2

# About Catalyst Center ITSM Integration

---

- [Catalyst Center integration use cases, on page 3](#)
- [Catalyst Center ITSM support, on page 3](#)

## Catalyst Center integration use cases

Catalyst Center supports these kinds of integration use cases with other third-party applications:

- Network management integrations:
  - Bidirectional IP grid synchronization
  - Integration with third-party IP Address Management (IPAM) systems
- Operation integrations:
  - ITSM event, problem, and incident management
  - Approvals and schedule window information
  - Assistance in issue triage and association
  - Data exports for building custom dashboards and reports



---

**Note** See the "Deploy Catalyst Center platform" chapter in the [Cisco Catalyst Center Platform User Guide](#) for detailed information about configuring integration settings.

---

## Catalyst Center ITSM support

Catalyst Center supports these capabilities:

- Integrating Catalyst Center into ITSM processes of incident, event, change, and problem management.
- Integrating Catalyst Center into ITSM approval and preapproval chains.
- Integrating Catalyst Center with formal change and maintenance window schedules.

The scope of the integration is to retrieve events relating to software image updates, changes to configuration of network devices and group-based policy updates that are required for compliance, security, or any other operational triggers from Catalyst Center, and then publish the event data on a recurring schedule to an ITSM (Service Now) system.

Catalyst Center bundles are prebuilt solutions that enable integration between Catalyst Center capabilities and specific IT domains. You can configure and use these bundles:

- **Basic ITSM (ServiceNow) CMDB Synchronization**
- **REST API**
- **Endpoint Attribute Retrieval with ITSM (ServiceNow)**
- **Network Issue Monitor and Enrichment for ITSM (ServiceNow)**
- **Rogue and aWIPS**
- **Automation Events for ITSM (ServiceNow)**





## CHAPTER 3

# Catalyst Center ITSM Integration Workflows

- [Catalyst Center integration supported workflows, on page 5](#)
- [Catalyst Center integration with a generic REST endpoint, on page 5](#)
- [Catalyst Center integration with ServiceNow without the Cisco Catalyst app, on page 9](#)
- [Catalyst Center integration with ServiceNow using the Cisco Catalyst app, on page 20](#)
- [Catalyst Center endpoint attribute retrieval with ServiceNow, on page 46](#)

## Catalyst Center integration supported workflows

These Catalyst Center ITSM integration workflows are supported:

- Catalyst Center ITSM integration with a generic REST endpoint: See [Catalyst Center integration with a generic REST endpoint, on page 5](#).
- Catalyst Center ITSM integration with ServiceNow without using the Cisco Catalyst application for ServiceNow: See [Catalyst Center integration with ServiceNow without the Cisco Catalyst app, on page 9](#).
- Catalyst Center ITSM integration with ServiceNow using the Cisco Catalyst application for ServiceNow: See [Catalyst Center integration with ServiceNow using the Cisco Catalyst app, on page 20](#).
- Catalyst Center ITSM endpoint attribute retrieval with ServiceNow using the Cisco Catalyst application for ServiceNow: See [Catalyst Center endpoint attribute retrieval with ServiceNow, on page 46](#).

## Catalyst Center integration with a generic REST endpoint

This table describes the procedure for configuring Catalyst Center integration with a generic REST endpoint. You may wish to publish Network and Automation events to a generic REST endpoint, outside of a configuration management database, for performance, security, event response, or other reasons.

**Table 2: Catalyst Center to generic REST endpoint integration procedure**

Step	Description
Step 1	Install or upgrade to the latest Catalyst Center release. For information about installing Catalyst Center, see the <a href="#">Cisco Catalyst Center Installation Guide</a> .

Step	Description
Step 2	Enable and configure bundles using the <b>Bundles</b> window in the Catalyst Center GUI. For more information about configuring bundles, see <a href="#">Cisco Catalyst Center Platform User Guide</a> .
Step 3	In the configuration slide-in pane, click <b>Destination to receive events</b> .
Step 4	To send the data to a different staging table in ServiceNow, select <b>Generic REST Endpoint in ServiceNow</b> as the destination to receive events.  Determine the generic REST endpoint (destination URI) for the publication of the Network and Automation events.
Step 5	Configure network event settings in <b>Event Settings</b> .  The Catalyst Center platform and ITSM integration allows the user to select from a list of events specific to the configured bundles, to create and modify the severity of events, incidents, or problems to match business priorities.  For information, see <a href="#">Configure event settings, on page 8</a> .
Step 6	Configure the integration settings. From the main menu, choose <b>System &gt; Settings &gt; System Configuration &gt; Integration Settings</b> . Enter your callback URL hostname or IP address.
Step 7	Access the generic REST endpoint in ITSM and review the network event data that has been posted using the REST APIs in this procedure. Begin to review and manipulate this data according to your business or network needs.

## Configure network events

You can subscribe to specific events that may occur in your network. After you subscribe, you receive a notification whenever the network event occurs. You subscribe to an event using the **Event Notifications** window in the Catalyst Center platform GUI.

**Figure 1: Catalyst Center platform Events window**

APIs

Integration Flows

Event Notifications

Notifications

Event Catalog

Q

Search Table

Event ID	Name	Type	Category	Severity
INTEGRATIONS-ITSM-842	Publish CMDB sync failure	INTEGRATIONS	INFO	3
LICMGMT-DEV-DEREG-FAILURE	Device de-registration failed	APP	TASK_FAILURE	3
LICMGMT-DEV-DEREG-SUCCESS	Device de-registration succeeded	APP	TASK_COMPLETE	4
LICMGMT-DEV-REG-FAILURE	Device registration failed	APP	TASK_FAILURE	3
LICMGMT-DEV-REG-	Device registration			

### Before you begin

- For subscribing to network events, you must have configured the required destination to deliver event notifications from the Catalyst Center platform. To access the **Destinations** window, click the menu icon and choose **System > Settings > External Services > Destinations**.
- You must have the appropriate permissions to perform the tasks described in this procedure. For information about role-based access control for the Catalyst Center platform, see the [Cisco Catalyst Center Platform User Guide](#).

### Procedure

- 
- Step 1** From the main menu, choose **Platform > Developer Toolkit > Event Notifications**.  
The **Event Notifications** window opens.
- Step 2** Click the **Notifications** tab to view the notification tiles.  
Each notification is represented by a tile and contains link to view notification details. From the CHANNELS area in the left pane, click the radio button next to the notification channels to view the existing tiles with the selected channel.
- Step 3** Follow the steps in the **Create a New Notification** wizard to create a new notification.  
Click **Let's Do It** to go directly to the workflow.
- Step 4** In the **Select Site and Events** window, select a site from the drop-down list and select the Network event or events that support the required notification channel.
- Step 5** Click **Next**.  
The **Select Channels** window opens.
- Step 6** In the **Select Channels** window, select the notification channel.  
Click **Next** to configure the values in the corresponding **Settings** window.
- Step 7** Click **Next**.  
The **Name and Description** window opens.
- Step 8** Click **Next**.  
The **Summary** window opens.
- Step 9** In the **Summary** window, review the configuration settings.  
To make any changes, click **Edit**.
- Step 10** Click **Finish**.  
The **Done! Your new notification is complete** window appears.  
For more information, see **Work with Event Notifications** in the [Cisco Catalyst Center Platform User Guide](#) and **Create an Event Notification** in the [Cisco Catalyst Center User Guide](#).
-

## Configure event settings

The Catalyst Center platform and ITSM integration lets you select from a list of possible issues to create and modify the severity of events, incidents, or problems in ServiceNow to match your business priorities. You perform these tasks in the **Events Settings** window.

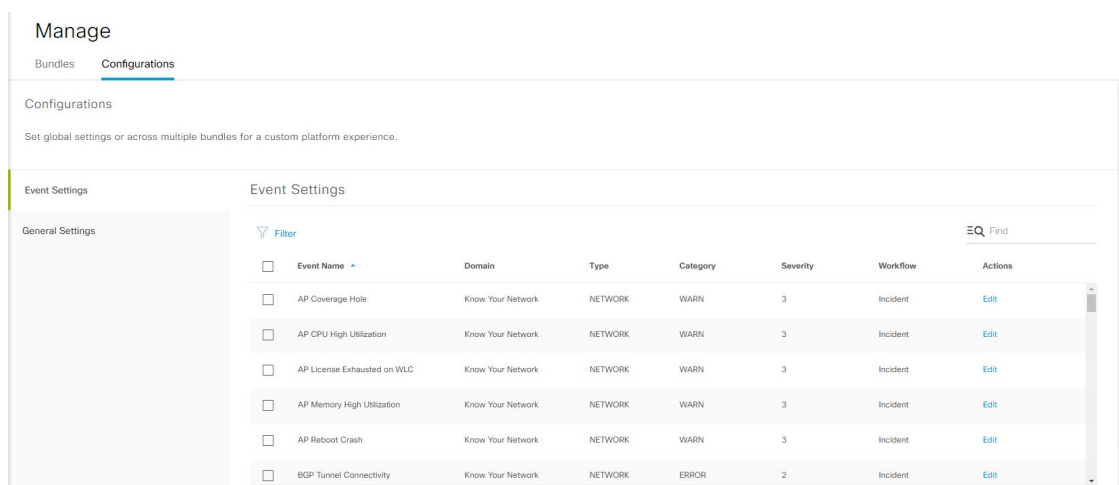


**Note** For this release, there are no SWIM events to configure in **Event Settings**. You only configure network assurance events.



**Important** The **Event Settings** window and its functionality are applicable only to configure events for an ITSM integration and not for events that are configured to other destinations. To configure events to a webhook or other destination, click the link above the columns. Use the **Event Notifications** window to configure events for an email, webhook, or SNMP trap.

**Figure 2: Events Settings window**



### Before you begin

You must have the appropriate permissions to do the tasks as described in this procedure. For information about role-based access control for the Catalyst Center platform, see the [Cisco Catalyst Center Platform User Guide](#).

### Procedure

- Step 1** From the main menu, choose **Platform > Manage > Configurations**.  
A **Configurations** window that contains an **Events Settings** section opens.
- Step 2** Review the information presented in the **Event Settings** section:
- **Event Name:** Name of the Catalyst Center event.

- **Domain:** Domain of the Catalyst Center event.
- **Type:** Network, App, System, Security, or Integrations.
- **Category:** Error, Warn, Info, Alert, Task Progress, or Task Complete.
- **Severity:** 1 to 5.

**Note**

Severity 1 is the most important or critical priority. You can edit the severity level of the event.

- **Workflow:** Incident, Problem, Event, or RFC (Request for Change).
- **Actions:** Edit.

To change what is displayed in the table, click the **Filter** icon or enter a keyword in the **Find** field. For example, to view all network notifications, enter **Network** in the **Find** field. To view all severity1 notifications, enter **1** in the **Find** field.

**Step 3** To edit an event, click **Edit** in the **Actions** column.

To change any setting, click the down-arrow and select a value from the available options.

**Step 4** Click the box next to the event name to enable notifications.

You must select the events in the **Event Settings** section to configure events for an ITSM integration. This enables notifications through Catalyst Center when the event occurs in the future.

**Step 5** Click **Save**.

## Catalyst Center integration with ServiceNow without the Cisco Catalyst app

This table describes the procedure for configuring Catalyst Center integration with ServiceNow without using the Cisco Catalyst app. Follow the procedure to configure integration for network events, SWIM events, or both event types depending on the functionality that you require.

**Note**

You can also use the **Basic ITSM (ServiceNow) CMDB synchronization** bundle with this workflow. If you use this bundle, be sure to select **Post device inventory details to a staging table** as the destination type. The other destination type (**Synchronize device inventory directly with CMDB**) requires the Cisco Catalyst app. Additionally, the **Post device inventory details to a staging table** destination type only sends data to the REST API endpoint. You will need to create a script to do any further action on the data.

**Table 3: Catalyst Center-to-ServiceNow integration without the Cisco Catalyst App procedure**

Step	Description
Step 1	Install or upgrade to the latest Catalyst Center release. For information about <i>installing</i> Catalyst Center, see the <a href="#">Cisco Catalyst Center Installation Guide</a> .

Step	Description
Step 2	<p>Click this link to access the ServiceNow Store website:</p> <p><a href="https://store.servicenow.com/sn_appstore_store.do#!/store/application/03eb0f4ddbf6ba00f27978b5ae96197b">https://store.servicenow.com/sn_appstore_store.do#!/store/application/03eb0f4ddbf6ba00f27978b5ae96197b</a></p> <p>For information about configuring user profiles and setting up the MID Server, see the "Scope Certified Application (Cisco Catalyst) - Installation and Configuration" guide available on the ServiceNow Store website.</p>
Step 3	<p>Configure the <b>Network Issue Monitor and Enrichment for ITSM (ServiceNow)</b> bundle. For information, see <a href="#">Configure the network issue monitor and enrichment for ITSM (ServiceNow) bundle, on page 10</a>.</p> <p>This bundle enables Change Management between the two systems (Catalyst Center and ServiceNow). Change Management and Incident/Problem Management workflows should be enabled based on the automation or assurance use cases that you want to log tickets to in ServiceNow.</p>
Step 4	<p>Configure network event settings in <b>Event Settings</b>.</p> <p>For information, see <a href="#">Configure event settings, on page 14</a>.</p> <p><b>Note</b></p> <p>The Catalyst Center platform and ITSM integration allows the user to select from a list of possible issues to create and modify the severity of events, incidents, or problems in ServiceNow to match business priorities.</p>
Step 5	<p>Configure the Automation events for ITSM (ServiceNow) bundle.</p> <p>For information, see <a href="#">Configure the automation events for ITSM (ServiceNow) bundle, on page 15</a>.</p> <p>The Automation Events for ITSM (ServiceNow) bundle retrieves events relating to software image updates required for compliance, security or any other operational triggers from Catalyst Center. SWIM event notifications are sent from Catalyst Center to ServiceNow when they occur, not on a polling and notify schedule.</p> <p>For information, see <a href="#">About SWIM closed loop automation, on page 55</a>.</p>
Step 6	<p>Access your ServiceNow instance and review the network and SWIM event data that has been posted using the REST APIs in this procedure. Begin to review and manipulate this data in ServiceNow per your business or network needs.</p>

## Configure the network issue monitor and enrichment for ITSM (ServiceNow) bundle

Follow this procedure to set up monitoring for network for assurance and maintenance issues, as well as publishing event details to a ServiceNow system.

**Note**

- Closed loop automation is supported for assurance events between Catalyst Center and ServiceNow. Closed loop automation is not supported for other event types.
- The closed loop automation support is extended only to the REST API endpoint configured in the Network Issue Monitor and Enrichment for ITSM (ServiceNow) bundle. The Event Management and Generic REST API endpoints configured in this bundle do not support automatic ticket creation and auto resolution of tickets for closed loop automation of assurance events. However, an update regarding an assurance event being resolved/ignored is sent to the Event Management and Generic REST API endpoints.
- When an assurance event or issue is ignored or resolved in Catalyst Center, an update is sent to ServiceNow irrespective of the endpoint (Event Management/REST API Endpoint or Generic REST API Endpoint) configured in the Automation Events for ITSM (ServiceNow) Bundle.
- Event data can be published to the **Event** table in ServiceNow. This requires that you have the Event Management plug-in in your ServiceNow instance. If you do not have the Event Management plug-in in your ServiceNow instance, the bundle can be configured to send the data to a REST API endpoint in the Cisco Catalyst app.

**Before you begin**

You must have the appropriate permissions to do the tasks as described in this procedure. For information about role-based access control for the Catalyst Center platform, see the [Cisco Catalyst Center Platform User Guide](#).

**Procedure**

- 
- Step 1** From the main menu, choose **Platform > Manage > Bundles**.
- Review the displayed bundles and their current status.
- Step 2** Click the **Network Issue Monitor and Enrichment for ITSM (ServiceNow)** bundle link or icon (colored square with initial) for additional information about the bundle.
- Additional information provided may include:
- **General information:** Vendor, version, platform, tags displayed under the square icon.
  - **Information:** Tab that displays general information (purpose of bundle and how bundle works in the network), sample schemas, configuration notes, and other data about the bundle.
  - **Contents:** Tab that accesses the APIs and integration flows that make up the bundle, or provides information about the integration flows that make up the bundle.
  - **Release Notes:** Tab that displays latest release information about the bundle, including its version.
- Step 3** Click each of the above tabs and review the information about the bundle.
- Step 4** Click the **Enable** button to enable the bundle.
- An **Information** field appears in the window.
- Step 5** In the **Information** field, click the **Enable** button to confirm enabling the bundle.

After clicking the **Enable** button to confirm, a success message appears.

**Step 6** Click **OK** in the success message.

**Step 7** Click the **Configure** button to configure at the bundle level.

A configuration slide-in pane appears.

**Step 8** In the configuration slide-in pane, click **ServiceNow Access Settings** to configure a ServiceNow Connection instance.

**Step 9** Click the radio button to configure either an existing ServiceNow Connection instance or configure a new instance.

**Figure 3: Example of ServiceNow instance configuration fields**

For configuring an existing ServiceNow Connection instance, select it from the drop-down menu in the window and click **Activate**.

**Step 10** For configuring a new ServiceNow Connection instance, this additional information must be entered:

- **Instance Name:** Name of the instance.
- **Description:** Descriptive text of the instance.
- **Host name:** Hostname for the ServiceNow system.
- **Username:** Username required to access the ServiceNow system.
- **Password:** Password required to access the ServiceNow system.

**Step 11** Click **Check Connectivity** to test whether you can connect to the server where the endpoint is located.



After a successful test of connectivity to the server, configure **Destination to receive events**.

**Step 12** In the configuration slide-in pane, click **Destination to receive events** to configure a Destination Connection instance.

**Step 13** Click the radio button to configure either an existing Destination Connection instance or configure a new instance.

**Figure 4: Example of Destination to receive events configuration fields**

Configure Network Issue Monitor and Enrichment for ITSM (ServiceNow)

Configure your bundle

> ServiceNow Access Settings

▼ Destination to receive events

INFORMATION

Instance Name \*

Description

DESTINATION TO RECEIVE EVENTS

Destination to receive events \* ▼

Destination Uri

Enter a custom endpoint

Cancel Activate

For configuring an existing Destination Connection instance, select it from the drop-down menu in the window and click **Activate**.

**Step 14** For configuring a new Destination instance, this additional information must be entered:

- **Instance Name:** Name of the instance.
- **Description:** Descriptive text of the instance.
- **Destination to receive events:** Select one of these options:
  - **Event Management:** When setting up Catalyst Center integration with ServiceNow without using the Cisco Catalyst app, select the **Event Management** option. The **Event Management** option also requires that you have the Event Management plug-in configured within the ServiceNow instance.
  - **REST API Endpoint:** The **REST API Endpoint** option can be used with the Cisco Catalyst app. With this option, data is sent to a REST API endpoint within the Cisco Catalyst app.

**Note**

When a network event or issue is ignored or resolved in Catalyst Center, an event status update is sent to the Cisco Catalyst app in ServiceNow, and the ticket created for the event in ServiceNow is closed automatically.

- **Generic REST Endpoint in ServiceNow:** With this option, you can send the data to a different staging table in ServiceNow.
- **Destination URI:** Enter a destination URI (Uniform Resource Indicator) for the **Generic REST Endpoint in ServiceNow** option. This field is mandatory for this option.

After entering this information, proceed to the next step.

**Step 15** Click **Activate** to save your changes and activate the bundle or click **Cancel** to cancel the configuration and close the slide-in pane.

The changes made to the bundle begin to take effect immediately. Additionally, the bundle status changes from **ENABLED** to **ACTIVE**.

## Configure event settings

The Catalyst Center platform and ITSM integration lets you select from a list of possible issues to create and modify the severity of events, incidents, or problems in ServiceNow to match your business priorities. You do these tasks in the **Events Settings** window.



**Note** For this release, there are no SWIM events to configure in **Event Settings**. You only configure network assurance events.



**Important** The **Event Settings** window and its functionality is only applicable to events for an ITSM (ServiceNow) integration and not for events configured to other destinations. For events being configured to a webhook or other destination, click the link above the columns to access the **Events** window. Use the **Events** window to configure events for an email, webhook, or SNMP trap.

**Figure 5: Events Settings window**

The screenshot shows the 'Manage' section with 'Configurations' selected. Under 'Event Settings', there is a table with columns: Event Name, Domain, Type, Category, Severity, Workflow, and Actions. The table lists several network assurance events, all with a 'Know Your Network' domain and 'Incident' workflow.

Event Name	Domain	Type	Category	Severity	Workflow	Actions
AP Coverage Hole	Know Your Network	NETWORK	WARN	3	Incident	Edit
AP CPU High Utilization	Know Your Network	NETWORK	WARN	3	Incident	Edit
AP License Exhausted on WLC	Know Your Network	NETWORK	WARN	3	Incident	Edit
AP Memory High Utilization	Know Your Network	NETWORK	WARN	3	Incident	Edit
AP Reboot Crash	Know Your Network	NETWORK	WARN	3	Incident	Edit
BGP Tunnel Connectivity	Know Your Network	NETWORK	ERROR	2	Incident	Edit

### Before you begin

You must have the appropriate permissions to do the tasks as described in this procedure. For information about role-based access control for the Catalyst Center platform, see the [Cisco Catalyst Center Platform User Guide](#).

## Procedure

**Step 1** From the main menu, choose **Platform > Manage > Configurations**.  
A **Configurations** window opens that contains an **Events Settings** section.

**Step 2** Review the **Event Settings** section, which contains this information:

- **Event Name:** Name of the Catalyst Center event.
- **Domain:** Domain of the Catalyst Center event.
- **Type:** Network, App, System, Security, Integrations type.
- **Category:** Error, Warn, Info, Alert, Task Progress, Task Complete.
- **Severity:** P1 (Severity 1) through P5 (Severity 5).

**Note**

Severity 1 is the most important or critical priority and should be assigned as such.

- **Workflow:** Incident, Problem, Event, or RFC (Request for Change).
- **Actions:** Edit.

You can adjust what is displayed in the table by clicking the **Filter** icon and using the filter, or by typing a keyword in the **Find** field. For example, to display all access point notifications, type **AP** in the **Find** field. To view all network notifications, type **Network** in the **Find** field. To view all severity notifications, type **1** in the **Find** field.

**Step 3** Click **Edit** in the **Actions** column to edit an event.  
Select a setting by clicking on the downward pointing angle and adjust the value. For example, click **Network** and adjust to **App**. This changes the event type from a network type to an application type. Click **Severity** and adjust to **1** from **5**. This raises the severity level from 5 to 1.

**Step 4** Click the box next to the Event name to enable notifications.  
This enables notifications through Catalyst Center when the event occurs in the future.

**Step 5** Click **Save**.

## Configure the automation events for ITSM (ServiceNow) bundle

Follow this procedure to set up monitoring and publishing events requiring device provisioning activities, software image updates for compliance, security, or other operational triggers to a ServiceNow system.



**Note** You can publish the event data to the **Event** table in ServiceNow if you have the Event Management plug-in in your ServiceNow instance. If not, you can configure the bundle to send the data to a REST API endpoint in the Cisco Catalyst app.

Enabling ITSM in Catalyst Center enforces a ServiceNow approval process for better control of Catalyst Center device provisioning activities and group-based policy changes. However, enabling ITSM for software image updates is not necessary as SWIM does not honor the Visibility and Control of Configurations settings. See the Configure System Settings chapter in the [Cisco Catalyst Center Administrator Guide](#) for information about enabling ITSM approval.

### Before you begin

You must have the appropriate permissions to do the tasks as described in this procedure. For information about role-based access control for the Catalyst Center platform, see the [Cisco Catalyst Center Platform User Guide](#).

## Procedure

- 
- Step 1** From the main menu, choose **Platform > Manage > Bundles**.  
Review the displayed bundles and their status.
- Step 2** Click the Automation Events for ITSM (ServiceNow) bundle link or icon (colored square with initial) for additional information about the bundle.  
Additional information that is provided may include:
- **General information:** Vendor, version, platform, tags displayed under the square icon.
  - **Information:** Tab that displays general information (purpose of bundle and how bundle works in the network), sample schemas, configuration notes, and other data about the bundle.
  - **Contents:** Tab that accesses the APIs and integration flows that make up the bundle, or provides information about the integration flows that make up the bundle.
  - **Release Notes:** Tab that displays latest release information about the bundle, including its version.
- Step 3** Click each of the preceding tabs and review the information about the bundle.
- Step 4** Click **Enable** to enable the bundle.  
An **Information** field appears in the window.
- Step 5** Click **Enable** in the **Information** field to confirm enabling the bundle.  
After clicking **Enable** to confirm, a success message appears.
- Step 6** Click **OK** in the success message.
- Step 7** Click **Configure** to configure at the bundle level.  
A configuration slide-in pane appears.

**Step 8** In the configuration slide-in pane, click **Automation Events Workflow Selection** to select events relating to software image updates, changes to configuration of network devices and group based policy update that need to be enabled for ITSM integration. This selection could be one or more, or all the events.

**Step 9** Click the radio button to configure either an existing ServiceNow Connection instance or configure a new instance.

**Figure 6: Example of Automation Events Workflow Selection configuration fields**

Configure Catalyst Center Automation events for ITSM (ServiceNow)

Configure your bundle

Automation Events Workflow Selection

This is used to select what events (events relating to software image updates, changes to configuration of network devices and group based policy updates) need to be enabled for ITSM integration. This selection could be one or more or all the events.

☐ Select an existing instance ☒ Create a new instance

AUTOMATION EVENTS WORKFLOW SELECTION

Software Image Management \*

Network Provisioning \*

Group Based Policies \*

> Destination to receive events

Cancel Activate

To configure an existing ServiceNow Connection instance, select it from the drop-down list in the window and click **Activate**.

**Step 10** To configure a new ServiceNow Connection instance, you must enter this additional information:

- **Instance Name:** Name of the instance.
- **Description:** Descriptive text of the instance.
- **Software Image Management:** Select **true** from the drop-down list to enable ITSM integration of events relating to software image updates.
- **Network Provisioning:** Select **true** from the drop-down list to enable ITSM integration of events relating to configuration changes of network devices.
- **Group Based Policies:** Select **true** from the drop-down list to enable ITSM integration of events relating to group based policy updates.

**Step 11** In the configuration slide-in pane, click **ServiceNow Access Settings** to configure a ServiceNow Connection instance.

**Step 12** Click the radio button to configure either an existing ServiceNow Connection instance or configure a new instance.

**Figure 7: Example of ServiceNow instance configuration fields**

Configure SWIM Events for ITSM (ServiceNow)

Configure your bundle

ServiceNow Access Settings

>> Back to Select Instance

INFORMATION

Instance Name \*

Description

SERVICENOW ACCESS SETTINGS

Host Name \*

https://<servicenow-host-name>

Username \*

<username-for-servicenow-host>

Password \*

SHOW

HINT

Check connectivity

> Destination to receive events

Cancel Activate

To configure an existing ServiceNow Connection instance, select it from the drop-down list in the window and click **Activate**.

**Step 13** To configure a new ServiceNow Connection instance, you must enter this additional information:

- **Instance Name:** Name of the instance.
- **Description:** Descriptive text of the instance.
- **Host name:** Hostname for the ServiceNow system.
- **Username:** Username required to access the ServiceNow system.
- **Password:** Password required to access the ServiceNow system.

**Step 14** Click **Check Connectivity** to test whether you can connect to the server where the endpoint is located.

After a successful test of connectivity to the server, activate the bundle.

**Step 15** In the configuration slide-in pane, click **Destination to receive events** to configure a Destination Connection instance.

**Step 16** Click the radio button to configure either an existing Destination Connection instance or configure a new instance.

**Figure 8: Example of Destination to receive events configuration fields**

Configure SWIM Events for ITSM (ServiceNow)

Configure your bundle

> ServiceNow Access Settings

▼ Destination to receive events

INFORMATION

Instance Name \*

Description

DESTINATION TO RECEIVE EVENTS

Destination to receive events \* ▼

Destination Uri

Enter a custom endpoint

Cancel Activate

To configure an existing Destination Connection instance, select it from the drop-down menu in the window and click **Activate**.

**Step 17**

To configure a new Destination instance, you must enter this additional information:

- **Instance Name:** Name of the instance.
- **Description:** Descriptive text of the instance.
- **Destination to receive events:** Select one of these options:
  - **Event Management:** When setting up Catalyst Center integration with ServiceNow without using the Cisco Catalyst app, select the **Event Management** option. The **Event Management** option requires that you have the Event Management plug-in that is configured within the ServiceNow instance.
  - **REST API Endpoint:** You can use the **REST API Endpoint** option with the Cisco Catalyst app. Data is sent to a REST API endpoint within the Cisco Catalyst app with the **REST API Endpoint** option.
  - **Generic REST Endpoint in ServiceNow:** For the **Generic REST Endpoint in ServiceNow** option, you can send the data to a different staging table in ServiceNow.
- **Destination URI:** Enter a destination Uniform Resource Indicator (URI) for the **Generic REST Endpoint in ServiceNow** option. This field is mandatory for this option.

After entering this information, proceed to the next step.

**Step 18** Click **Activate** to save your changes and activate the bundle or click **Cancel** to cancel the configuration and close the slide-in pane.

**Note**

By clicking **Activate**, you enable the changes that are made to the bundle and the changes take effect immediately. The bundle's status changes from **ENABLED** to **ACTIVE**.

## Catalyst Center integration with ServiceNow using the Cisco Catalyst app

Catalyst Center supports an application (Catalyst Center) that facilitates integration with ServiceNow. This application (app) is designed to work with ServiceNow without its Event Management plug-in.

Install the Cisco Catalyst app (version 2.3.1) within the ServiceNow instance. Ensure that the app does these tasks:

- Schedules the basic one-way synchronization of Catalyst Center discovered devices into the ServiceNow Configuration Management Database (CMDB) using Catalyst Center inventory as a source of truth. The Cisco Catalyst app supports CMDB synchronization from Catalyst Center to ServiceNow.
- Automatically triggers problem, incident, and change workflows for network events published by Catalyst Center.
- Enriches Incident tickets with network details from Catalyst Center The Cisco Catalyst app makes REST API calls into Catalyst Center. This API call helps in fetching client or user enrichment information based on either the client MAC address or the network user ID.
- Supports integration of the Catalyst Center platform with ServiceNow for an automated way to create change request (CR) tickets in ServiceNow for network events.

This table describes the procedure for configuring Catalyst Center integration with ServiceNow using the Cisco Catalyst app. Follow the procedure to configure integration for network events, SWIM events, or both event types depending upon the functionality that you require.

**Table 4: Catalyst Center-to-ServiceNow integration with Cisco Catalyst app procedure**

Step	Description
Step 1	Install or upgrade to the latest Catalyst Center release. For information about installing Catalyst Center, see the <a href="#">Cisco Catalyst Center Installation Guide</a> .



Step	Description
Step 2	<p>Install or upgrade to a compatible version of ServiceNow mentioned on the ServiceNow Store website.</p> <p>Click this link to access the ServiceNow Store website:</p> <p><a href="https://store.servicenow.com/sn_appstore_store.do#!/store/application/03eb0f4ddbf6ba00f27978b5ae96197b/2.3.1">https://store.servicenow.com/sn_appstore_store.do#!/store/application/03eb0f4ddbf6ba00f27978b5ae96197b/2.3.1</a></p> <p>See your ServiceNow documentation for the installation and upgrade procedures.</p> <p><b>Note</b> Only a ServiceNow administrator can do this procedure.</p>
Step 3	<p>Click the link to access the ServiceNow Store website containing the Cisco Catalyst app:</p> <p><a href="https://store.servicenow.com/sn_appstore_store.do#!/store/application/03eb0f4ddbf6ba00f27978b5ae96197b/2.3.1">https://store.servicenow.com/sn_appstore_store.do#!/store/application/03eb0f4ddbf6ba00f27978b5ae96197b/2.3.1</a></p> <p>Download and install the Cisco Catalyst app (version 2.3.1) into ServiceNow by following the documentation available at the website.</p> <p><b>Note</b> This procedure is to be done by a ServiceNow administrator.</p>
Step 4	<p>Review and ensure that the requirements are met for the Catalyst Center-to-ServiceNow integration.</p> <p>For information, see <a href="#">Requirements, on page 22</a>.</p>
Step 5	<p>Access the Catalyst Center platform GUI and configure the <b>Basic ITSM (ServiceNow) CMDB Synchronization</b> bundle.</p> <p>For information, see <a href="#">Configure the basic ITSM (ServiceNow) CMDB synchronization bundle, on page 23</a>.</p> <p><b>Note</b> Synchronizing the network device inventory with the ServiceNow CMDB is a prerequisite to enable the auto-generation of ITSM tickets. Therefore, the CMDB Sync must be enabled first (if it is not already done outside of Catalyst Center). Check with your ServiceNow administrator to see whether the CMDB Sync is being done elsewhere.</p>
Step 6	<p>Configure the <b>Network Issue Monitor and Enrichment for ITSM (ServiceNow)</b> bundle. For information, see <a href="#">Configure the network issue monitor and enrichment for ITSM (ServiceNow) bundle, on page 10</a>.</p> <p>This bundle enables data to be sent from Catalyst Center to create any type of workflow in ServiceNow. Change Management and Incident/Problem Management workflows should be enabled based on the automation or assurance use cases that you want to log tickets to in ServiceNow.</p>
Step 7	<p>Configure network event settings in <b>Event Settings</b>.</p> <p>For more information, see <a href="#">Configure event settings, on page 36</a>.</p> <p><b>Note</b> The Catalyst Center platform and ITSM integration allows the user to select from a list of possible issues to create and modify the severity of events, incidents, or problems in ServiceNow to match business priorities.</p>

Step	Description
Step 8	Configure the Automation Events for ITSM (ServiceNow) bundle. For information, see <a href="#">Configure the automation events for ITSM (ServiceNow) bundle, on page 15</a> .
Step 9	Access your ServiceNow instance and review the network and SWIM event data that has been posted using the Catalyst Center REST APIs in this procedure. Begin to review and use this data per your business or network needs.

## Requirements

Review and ensure that this networking and systems requirements are met for the Catalyst Center-to-ServiceNow integration:

- Networking:
  - The Cisco Catalyst app is configured with the IP address and access information of the Catalyst Center installation that it is being integrated with.



### Note

Contact your Catalyst Center administrator to obtain this information.

- HTTPS network access between Catalyst Center and ServiceNow.



### Note

Contact and work with your network administrator to establish this.

- Management, Instrumentation, and Discovery (MID) Server:
  - The MID server is up and running, as well as accessible from the ServiceNow instance.
  - The Catalyst Center platform is accessible from the MID server.
  - The Catalyst Center platform REST APIs are allowed from the MID server.



### Note

The MID server is used to proxy the REST requests from the ServiceNow instance.

See the *Scope Certified Application Installation and Configuration Guide* on the ServiceNow Store website for MID server configuration information: [https://store.servicenow.com/sn\\_appstore\\_store.do#!/store/application/03eb0f4ddb6ba00f27978b5ae96197b](https://store.servicenow.com/sn_appstore_store.do#!/store/application/03eb0f4ddb6ba00f27978b5ae96197b)

- Catalyst Center Platform:
  - The Catalyst Center platform is enabled in Catalyst Center.
  - The requisite bundle or bundles in the Catalyst Center platform are configured and activated (as described in the next procedures).



**Note** These bundles have the required APIs that integrate with the Cisco Catalyst app in ServiceNow.

## Configure the basic ITSM (ServiceNow) CMDB synchronization bundle

Perform this procedure to either trigger or schedule a synchronization between the Catalyst Center devices and your ServiceNow CMDB system. If devices have not been synchronized between Catalyst Center and the ServiceNow CMDB system, this bundle must be activated as a prerequisite, before activating any other bundles.



**Note** The Catalyst Center CMDB synchronization cannot detect multiple instances of Catalyst Center:

- To identify the attributes that were synchronized from a particular Catalyst Center instance, each attribute is tagged with a Catalyst Center IP address.
- ServiceNow can now identify which Catalyst Center instance the attribute came from. An extra attribute for the Configuration Item (CI) has been added to retain the Catalyst Center IP address or hostname information.

### Before you begin

- Ensure that you have ServiceNow running on a system that you will integrate with Catalyst Center platform.
- Run a successful **Discovery** job in Catalyst Center. You can check whether a **Discovery** job is successful in **Device Inventory**. From the main menu, choose **Provision** > **Inventory** to view the results.
- You must have the appropriate permissions to perform the tasks as described in this procedure. For information about role-based access control for the Catalyst Center platform, see the [Cisco Catalyst Center Platform User Guide](#).

### Procedure

**Step 1** From the main menu, choose **Platform** > **Manage** > **Bundles**.

Review the displayed bundles and their current status.

**Step 2** Click the **Basic ITSM (ServiceNow) CMDB synchronization** bundle link or icon (colored square with initial) for additional information about the bundle.

Additional information provided may include:

- **General information:** Vendor, version, platform, tags displayed under the square icon.
- **Information:** Tab that displays general information (purpose of bundle and how bundle works in the network), sample schemas, configuration notes, and other data about the bundle.

- **Contents:** Tab that accesses the integration flows and APIs that make up the bundle.
- **Release Notes:** Tab that displays latest release information about the bundle, including its version.

**Step 3** Click the **Contents** tab.

**Step 4** Click the **Integration Flows** header.

An integration flow or list of integration flows appear underneath the header.

**Step 5** Click **Enable** to activate the integration flow links.

An **Information** field appears in the window.

**Step 6** In the **Information** field, click **Enable** to confirm enabling the bundle.

After clicking **Enable** to confirm, a success message appears.

**Step 7** Click **Okay** in the success message.

**Step 8** Click the integration flow link to do these tasks:

- Review the **Description**, **Tags**, **How to Use this Flow**, and scheduler.
- Click **Run Now** (to run the scheduler now), **Run Later** (to schedule for a later time), or **Recurring** (to set up a recurring schedule).  
For **Run Later**, you need to select a date, time, and time zone. For **Recurring**, you need to set a repeating interval (daily or weekly), an interval duration (minutes or hours), and a start and end date.
- Click **Schedule** to enable the scheduler.

**Important**

Only configure and enable an integration flow schedule, after you have finished configuring the bundle itself as described in this procedure. You configure and enable an integration flow schedule by returning to this view and clicking **Schedule**. Or, click the **View Flows** link in the **Configure Basic ITSM (ServiceNow) CMDB synchronization** slide-in pane (see the next steps). Or, click the menu icon and choose **Platform > Developer Toolkit > Integration Flows > Schedule to Publish Inventory Details-ServiceNow Connector**.

**Step 9** Click the **X** icon to return to the previous bundle window.

**Step 10** Click the **Configure** button to configure at the bundle level.


A configuration slide-in pane appears. Review the CMDB synchronization information.

**Step 11** Click the radio button to configure either existing or new ServiceNow access settings for the CMDB synchronization.

**Figure 9: ServiceNow Access Settings**

Configure Basic ITSM (ServiceNow) CMDB synchronization

Configure your bundle ×

 This bundle has additional configurations for its Schedule-Based Integration Flows. [View Flows](#)

- Schedule to Publish Inventory Details - ServiceNow Connector - Recurring daily in intervals of 24 hours


ServiceNow Access Settings

This is used to specify the connection settings to a ServiceNow instance

☐ Select an existing instance ☒ Create a new instance

Instance Name \*

Description

 Exit Next

For configuring an existing setting, select it from the drop-down menu in the window and click **Next**.

**Step 12**

For configuring a new access setting, this instance information must be entered.

- **Instance Name:** Name of the instance.
- **Description:** Descriptive text of the instance.

Click **Next**.

**Step 13**

For configuring a new access setting, these additional settings information must be entered.

**Figure 10: ServiceNow Access Settings**

Configure Basic ITSM (ServiceNow) CMDB synchronization

Configure your bundle

---

### ServiceNow Access Settings

Host Name \*  
https://<servicenow-host-name>

Username \*  
<username-for-servicenow-host>

Password \*  
\*\*\*\*\* [SHOW](#)

[Check connectivity](#)

[Exit](#) [Back](#) [Next](#)

- **Hostname:** Hostname or IP address of the ServiceNow server.
- **Username:** Username for access to the ServiceNow server.
- **Password:** Password for access to the ServiceNow server.

Click **Check Connectivity** to check access to the ServiceNow server.

Click **Next**.

**Step 14** Click the radio button to configure either an existing instance or configure a new instance for the CMDB inventory settings.

**Figure 11: CMDB Inventory Settings**

Configure Basic ITSM (ServiceNow) CMDB synchronization

Configure your bundle ✕

---

i This bundle has additional configurations for its Schedule-Based Integration Flows. [View Flows](#)

- Schedule to Publish Inventory Details - ServiceNow Connector - Recurring daily in intervals of 24 hours

CMDB Inventory Settings

This is used to specify the CMDB Configuration details for ServiceNow, which includes the list of device attributes(mandatory/optional) that needs to be synced, type of destination within ServiceNow to receive the CMDB details, connection settings to the ServiceNow instance, transformation mapping between Cisco DNA Center device families and ServiceNow CI classes, maximum number of devices that can be synced in a single API call and the discovery source details.

☐ Select an existing instance ☒ Create a new instance

Instance Name \*

Description

Exit Back Next

For configuring an existing instance, select it from the drop-down menu in the window and click **Configure**.

**Step 15** For configuring a new instance, this additional information must be entered.

- **Instance Name:** Name of the instance.
- **Description:** Descriptive text of the instance.

Click **Next**.

**Step 16** In the **Select Destination** window, enter this information:

- **Destination Type:** There are two destination type options to select from:
  - **Synchronize device inventory directly with CMDB**
  - **Post device inventory details to a staging table**

**Note**

Use the **Synchronize device inventory directly with CMDB** destination type to send data to a REST API endpoint within the Cisco Catalyst app. You should use this destination type, if you are using the Cisco Catalyst app and do not have your own customized ServiceNow instance. Use the other destination type (**Post device inventory details to a staging table**) to send data to a REST API endpoint outside of the Cisco Catalyst app. Ensure that the created staging table has a field called `u_inventory_details`. The inventory details from the Cisco Catalyst app are mapped to this field. With the **Post device inventory details to a staging table** destination type, after data transfer you must write custom code to take the data from the staging table and map it to the ServiceNow CMDB.

- **Destination URI:** Uniform Resource Indicator of the ServiceNow server (CMDB) or staging table.

**Figure 12: Select Destination window**

Configure Basic ITSM (ServiceNow) CMDB synchronization

Configure your bundle

### Select Destination

Destination Type \*

Synchronize device inventory directl... ▾

Destination Uri \*

/api/now/import/x\_caci\_cisco\_dna\_cisr

[Enter a Custom Endpoint](#)

Exit Back Next

Click **Next**.

**Step 17** In the **Select Inventory Data Fields** window, select the data fields to be synchronized.

**Note**

Inventory data fields are Cisco created data types that can be designated as an attribute or reference to be synchronized into a CMDB or staging table.

Clicking the top check box in the **Select Inventory Data Fields** window will select all of the inventory data fields for synchronization. Click this top check box if you want to sync all of the inventory data fields. Otherwise, review and click one check box at a time to create a smaller subset of inventory data fields for synchronization.



**Figure 13: Select Inventory Data Fields window**

Configure Basic ITSM (ServiceNow) CMDB synchronization

Configure your bundle

### Select Inventory Data Fields

<input type="checkbox"/>	Name	Description	Is Attribute / Is Reference	
<input checked="" type="checkbox"/>	Host Name	Hostname of the device	<input checked="" type="radio"/> Attribute	<input type="radio"/> Reference
<input checked="" type="checkbox"/>	MAC Address	MAC Address of the Device	<input checked="" type="radio"/> Attribute	<input type="radio"/> Reference
<input checked="" type="checkbox"/>	Device Id	Id of the Device	<input checked="" type="radio"/> Attribute	<input type="radio"/> Reference
<input checked="" type="checkbox"/>	IP Address	Management IP Address of the device	<input checked="" type="radio"/> Attribute	<input type="radio"/> Reference
<input checked="" type="checkbox"/>	Serial Number	Serial Number of the device	<input checked="" type="radio"/> Attribute	<input type="radio"/> Reference
<input type="checkbox"/>	Upgrade Failure Reason	Upgrade Failure Reason	<input checked="" type="radio"/> Attribute	<input type="radio"/> Reference
<input type="checkbox"/>	CurrentSMU Upgrade Date	CurrentSMU Upgrade Date	<input checked="" type="radio"/> Attribute	<input type="radio"/> Reference
<input type="checkbox"/>	CurrentSMU	CurrentSMU	<input checked="" type="radio"/> Attribute	<input type="radio"/> Reference
<input type="checkbox"/>	Prior Upgrade Date	Prior Upgrade Date	<input checked="" type="radio"/> Attribute	<input type="radio"/> Reference
<input type="checkbox"/>	Code Upgrade Date	Code Upgrade Date	<input checked="" type="radio"/> Attribute	<input type="radio"/> Reference

[Exit](#) [Back](#) [Next](#)

The **Select Inventory Data Fields** window consists of these columns:

- **Name:** Name of the inventory data field.
- **Description:** Brief description of the inventory data field.
- **Is Attribute/Is Reference:** Whether the inventory data field is an attribute or a reference. A reference data field is used to create a relationship between two tables in a database. This is used for querying purposes. An attribute data field is used to add more data to a table in a database.

**Step 18** For the data fields selected to be synchronized in the preceding step, review their designation as either attribute or reference.

To change a data field's default designation, just click the desired data field designation (**Attribute** or **Reference**).

The integration supports only 'location', 'building', and 'part number' as reference fields.

After selecting the data fields to be synchronized and whether the data field is an attribute or reference, click **Next**.

**Step 19** In the **Update Transforms** window, either accept or update the ServiceNow transformation mapping between Catalyst Center device families and ServiceNow CI classes.

**Figure 14: Update Transforms window**

Configure Basic ITSM (ServiceNow) CMDB synchronization

Configure your bundle

### Update Transforms

Device Family	CI Class
Routers	cmdb_ci_ip_router
Switches and Hubs	cmdb_ci_ip_switch

Exit Back Next

Device families are the Catalyst Center device classifications (for example, Unified AP, Routers, Wireless Controller, Switches, and Hubs), where the inventory attributes/references mapping to ServiceNow is already available in the existing Cisco Catalyst application in ServiceNow. The type and number of device families can vary depending upon the different Cisco devices in the user's network.

**Note**

Catalyst Center platform is able to automatically retrieve all of the device families in the user's Catalyst Center network and display them in this GUI window.

CI classes are the database tables for ServiceNow (for example, cmdb\_ci\_wap\_network, cmdb\_ci\_ip\_router, and cmdb\_ci\_ip\_switch). The **CI Class** column in the GUI window is used to map the CI classes to their respective device families.

This table displays the Catalyst Center default CI classes for each device family. The default CI classes can be modified by the user. In case of other device families not listed below, Cisco will not have any default values specified in the **CI Class** column. The ServiceNow application user needs to either manually create the corresponding CI Classes and attributes/references mapping or use a pre-existing CI class a 'parent' CI class. Ensure the pre-existing or newly created class is inherited from Network Gear (cmdb\_ci\_netgear) class.

**Table 5: Default Device Family to CI Class Mapping List**

Device Family	Corresponding CI Class
Unified AP	cmdb_ci_wap_network
Wireless Controller	x_caci_cisco_dna_wireless_lan_controller

Device Family	Corresponding CI Class
Routers	cmdb_ci_ip_router
Switches and Hubs	cmdb_ci_ip_switch
Meraki Access Point	cmdb_ci_wap_network
Meraki Cameras	cmdb_ci_netgear
Meraki Dashboard	cmdb_ci_netgear
Meraki Security Appliances	cmdb_ci_netgear
Meraki Switches	cmdb_ci_ip_switch

After accepting or updating the information in this window, click **Next**.

**Note**

After configuring the bundle and setting up the schedule, if a new device (device family) is discovered and it lacks a CI class mapping in the **Update Transform** window, you must reconfigure the bundle to include a CI class mapping. This ensures that all devices are properly synced to the CMDB CI tables as expected.

**Step 20**

In the **Set Source Identifier and Operational Limit** window, configure the data source and maximum limit.

*Figure 15: Set Source Identifier and Operational Limit window*

## Set Source Identifier and Operational Limit

Source Identifier(Exact Match)\*

Other Automated



Inventory Items Per Iteration\*

100

Configure these values:

- **Source Identifier (Exact Match):** Enter the same value as previously selected or keep the value at its default, **Other Automated**.
  - Synchronize device inventory directly with CMDB
  - Post device inventory details to a staging table

**Note**

**Other Automated** is a preconfigured value for the discovery source attribute in an OOB ServiceNow instance. This is the value that indicates the data source from where the ServiceNow CI was discovered. As a default, Cisco uses one of the existing preconfigured values for the integration.

We recommend that the user creates their own discovery source, so as to uniquely identify the source from where the devices were fetched to sync into the ServiceNow instance. The steps to create a new discovery source are described in the ServiceNow App 'Installation and Configuration guide'.

- **Inventory Items Per Iteration:** Maximum number of devices that can be synchronized in an iteration (single API call). We recommend that you set the limit to 100 devices.

After entering the information, click **Next**.

## Step 21

In the **Summary** window, review the configuration summary.

**Figure 16: Summary window**

Configure Basic ITSM (ServiceNow) CMDB synchronization

Configure your bundle

---

### Summary

Review your configuration and make any changes.

- Destination and Instance** [Edit](#)

Destination: ServiceNow    Domain: https://ven02562.service-now.com    Uri: /api/x\_caci\_cisco\_dna/dna\_utils/CreateReferencesForCIs    Username:   
 Password: \*\*\*\*\*
- Inventory Data Fields** [Edit](#)

Send To Destination: Host Name (A), MAC Address (A), Device Id (A), IP Address (RF), Serial Number (A), Upgrade Failure Reason (A), CurrentSMU Upgrade Date (A), CurrentSMU (A), Prior Upgrade Date (A), Code Upgrade Date (A), Building (RF), Location (RF), Time Since Code Upgrade (A), Ports (A), Number of Users (A), Role (A), Uptime (A), Reachability status (A), Part Number (RF), Type (A), Software Version (A)
- Data Transforms** [Edit](#)

Transformations: Routers: cmdb\_ci\_ip\_router, Switches and Hubs: cmdb\_ci\_ip\_switch
- Limit and source** [Edit](#)

Discovery Source: Other Automated    Max Limit: 1000

After reviewing the information, click **Configure**.

For a successful configuration, you will receive a **Done! Bundle Configured** message.

## What to do next

Configure the Integration Flow for this bundle (**Schedule to Publish Inventory Details - ServiceNow Connector**), using one of the methods described in Step 8.

You can also test the CMDB synchronization by doing these tasks:

- From the main menu, choose **Platform > Runtime Dashboard > CMDB Synchronization Summary**. Click **Refresh** to refresh the GUI view. Review the inventory device synchronization status to ServiceNow.
- From the main menu, choose **Platform > Runtime Dashboard > Event Summary**. Click **Refresh** to refresh the GUI view. Click the individual events in the window to view the event data and access links to ServiceNow.
- Go to ServiceNow and search for a synchronized device. Check the **Configuration** and **Other Attributes** tabs for synchronized data in that device's record.

# Configure the network issue monitor and enrichment for ITSM (ServiceNow) bundle

Follow this procedure to set up monitoring for network for assurance and maintenance issues, as well as publishing event details to a ServiceNow system.

**Note**

- Closed loop automation is supported for assurance events between Catalyst Center and ServiceNow. Closed loop automation is not supported for other event types.
- The closed loop automation support is extended only to the REST API endpoint configured in the Network Issue Monitor and Enrichment for ITSM (ServiceNow) bundle. The Event Management and Generic REST API endpoints configured in this bundle do not support automatic ticket creation and auto resolution of tickets for closed loop automation of assurance events. However, an update regarding an assurance event being resolved/ignored is sent to the Event Management and Generic REST API endpoints.
- When an assurance event or issue is ignored or resolved in Catalyst Center, an update is sent to ServiceNow irrespective of the endpoint (Event Management/REST API Endpoint or Generic REST API Endpoint) configured in the Automation Events for ITSM (ServiceNow) Bundle.
- Event data can be published to the **Event** table in ServiceNow. This requires that you have the Event Management plug-in in your ServiceNow instance. If you do not have the Event Management plug-in in your ServiceNow instance, the bundle can be configured to send the data to a REST API endpoint in the Cisco Catalyst app.

**Before you begin**

You must have the appropriate permissions to do the tasks as described in this procedure. For information about role-based access control for the Catalyst Center platform, see the [Cisco Catalyst Center Platform User Guide](#).

**Procedure**

**Step 1** From the main menu, choose **Platform > Manage > Bundles**.

Review the displayed bundles and their current status.

**Step 2** Click the **Network Issue Monitor and Enrichment for ITSM (ServiceNow)** bundle link or icon (colored square with initial) for additional information about the bundle.

Additional information provided may include:

- **General information:** Vendor, version, platform, tags displayed under the square icon.
- **Information:** Tab that displays general information (purpose of bundle and how bundle works in the network), sample schemas, configuration notes, and other data about the bundle.
- **Contents:** Tab that accesses the APIs and integration flows that make up the bundle, or provides information about the integration flows that make up the bundle.
- **Release Notes:** Tab that displays latest release information about the bundle, including its version.

**Step 3** Click each of the above tabs and review the information about the bundle.

**Step 4** Click the **Enable** button to enable the bundle.

An **Information** field appears in the window.

**Step 5** In the **Information** field, click the **Enable** button to confirm enabling the bundle.

After clicking the **Enable** button to confirm, a success message appears.

**Step 6** Click **OK** in the success message.

**Step 7** Click the **Configure** button to configure at the bundle level.

A configuration slide-in pane appears.

**Step 8** In the configuration slide-in pane, click **ServiceNow Access Settings** to configure a ServiceNow Connection instance.

**Step 9** Click the radio button to configure either an existing ServiceNow Connection instance or configure a new instance.

**Figure 17: Example of ServiceNow instance configuration fields**

Configure Network Issue Monitor and Enrichment for ITSM (ServiceNow)

Configure your bundle

ServiceNow Access Settings

>> Back to Select Instance

INFORMATION

Instance Name \*

Description

SERVICENOW ACCESS SETTINGS

Host Name \*

https://<servicenow-host-name>

Username \*

<username-for-servicenow-host>

Password \*

SHOW

Hint

Check connectivity

Destination to receive events

Cancel Activate

For configuring an existing ServiceNow Connection instance, select it from the drop-down menu in the window and click **Activate**.

**Step 10** For configuring a new ServiceNow Connection instance, this additional information must be entered:

- **Instance Name:** Name of the instance.
- **Description:** Descriptive text of the instance.
- **Host name:** Hostname for the ServiceNow system.

- **Username:** Username required to access the ServiceNow system.
- **Password:** Password required to access the ServiceNow system.

**Step 11** Click **Check Connectivity** to test whether you can connect to the server where the endpoint is located.

After a successful test of connectivity to the server, configure **Destination to receive events**.

**Step 12** In the configuration slide-in pane, click **Destination to receive events** to configure a Destination Connection instance.

**Step 13** Click the radio button to configure either an existing Destination Connection instance or configure a new instance.

**Figure 18: Example of Destination to receive events configuration fields**

Configure Network Issue Monitor and Enrichment for ITSM (ServiceNow)

Configure your bundle

> ServiceNow Access Settings

▼ Destination to receive events

INFORMATION

Instance Name \*

Description

DESTINATION TO RECEIVE EVENTS

Destination to receive events \* ▼

Destination Uri

Enter a custom endpoint

Cancel Activate

For configuring an existing Destination Connection instance, select it from the drop-down menu in the window and click **Activate**.

**Step 14** For configuring a new Destination instance, this additional information must be entered:

- **Instance Name:** Name of the instance.
- **Description:** Descriptive text of the instance.
- **Destination to receive events:** Select one of these options:
  - **Event Management:** When setting up Catalyst Center integration with ServiceNow without using the Cisco Catalyst app, select the **Event Management** option. The **Event Management** option also requires that you have the Event Management plug-in configured within the ServiceNow instance.

- **REST API Endpoint:** The **REST API Endpoint** option can be used with the Cisco Catalyst app. With this option, data is sent to a REST API endpoint within the Cisco Catalyst app.

**Note**

When a network event or issue is ignored or resolved in Catalyst Center, an event status update is sent to the Cisco Catalyst app in ServiceNow, and the ticket created for the event in ServiceNow is closed automatically.

- **Generic REST Endpoint in ServiceNow:** With this option, you can send the data to a different staging table in ServiceNow.
- **Destination URI:** Enter a destination URI (Uniform Resource Indicator) for the **Generic REST Endpoint in ServiceNow** option. This field is mandatory for this option.

After entering this information, proceed to the next step.

**Step 15**

Click **Activate** to save your changes and activate the bundle or click **Cancel** to cancel the configuration and close the slide-in pane.

The changes made to the bundle begin to take effect immediately. Additionally, the bundle status changes from **ENABLED** to **ACTIVE**.

## Configure event settings

The Catalyst Center platform and ITSM integration lets you select from a list of possible issues to create and modify the severity of events, incidents, or problems in ServiceNow to match your business priorities. You do these tasks in the **Events Settings** window.

**Note**

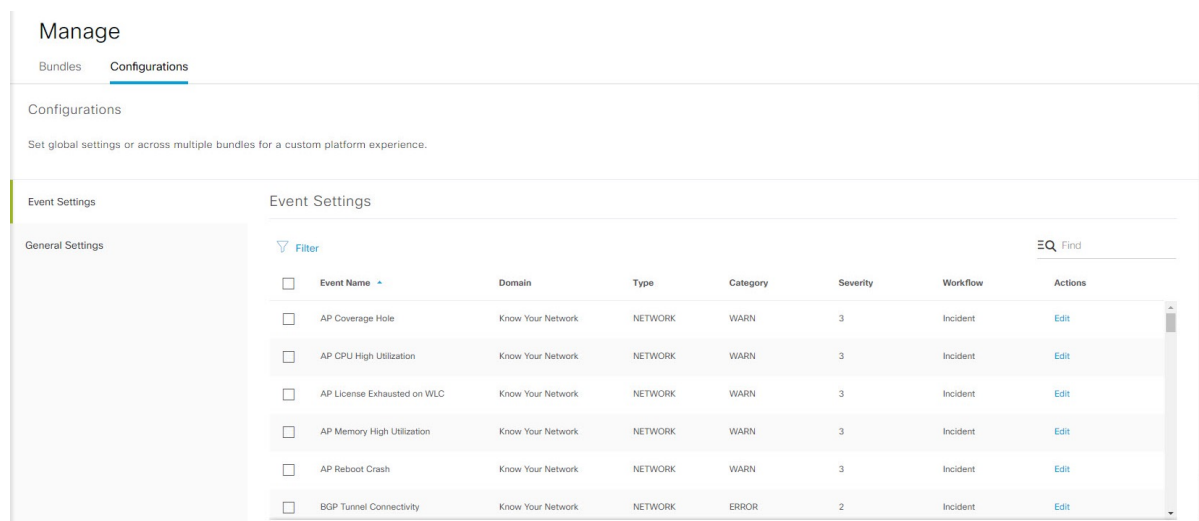
For this release, there are no SWIM event to configure in **Event Settings**. You only configure network assurance events.

**Important**

The **Event Settings** window and its functionality is only applicable to events for an ITSM (ServiceNow) integration and not for events configured to other destinations. For events being configured to a webhook or other destination, click the link above the columns to access the **Events** window. Use the **Events** window to configure events for an email, webhook, or SNMP trap.



Figure 19: Events Settings window



### Before you begin

You must have the appropriate permissions to do the tasks as described in this procedure. For information about role-based access control for the Catalyst Center platform, see the [Cisco Catalyst Center Platform User Guide](#).

## Procedure

- Step 1** From the main menu, choose **Platform > Manage > Configurations**.  
A **Configurations** window opens that contains an **Events Settings** section.
- Step 2** Review the **Event Settings** section that appears.

This **Event Settings** information appears:

- **Event Name:** Name of the Catalyst Center event.
- **Domain:** Domain of the Catalyst Center event.
- **Type:** Network, App, System, Security, Integrations type.
- **Category:** Error, Warn, Info, Alert, Task Progress, Task Complete.
- **Severity:** P1 (Severity 1) through P5 (Severity 5).

#### Note

Severity 1 is the most important or critical priority and should be assigned as such.

- **Workflow:** Incident, Problem, Event, or RFC (Request for Change).
- **Actions:** Edit.

You can adjust what is displayed in the table by clicking the **Filter** icon and using the filter, or by typing a keyword in the **Find** field. For example, to display all access point notifications, type **AP** in the **Find** field. To view all network notifications, type **Network** in the **Find** field. To view all severity notifications, type **1** in the **Find** field.

**Step 3** Click **Edit** in the **Actions** column to edit an event.

Select a setting by clicking the downward pointing angle and adjust the value. For example, click **Network** and adjust to **App**. This changes the event type from a network type to an application type. Click **Severity** and adjust to **1** from **5**. This raises the severity level from 5 to 1.

**Step 4** Click the box next to the event name to enable notifications.

This enables notifications through Catalyst Center when the event occurs in the future.

**Step 5** Click **Save**.

## Configure the automation events for ITSM (ServiceNow) bundle

Follow this procedure to set up monitoring and publishing events requiring device provisioning activities, software image updates for compliance, security, or other operational triggers to a ServiceNow system.



**Note** You can publish the event data to the **Event** table in ServiceNow if you have the Event Management plug-in in your ServiceNow instance. If not, you can configure the bundle to send the data to a REST API endpoint in the Cisco Catalyst app.

Enabling ITSM in Catalyst Center enforces a ServiceNow approval process for better control of Catalyst Center device provisioning activities and group-based policy changes. However, enabling ITSM for software image updates is not necessary as SWIM does not honor the Visibility and Control of Configurations settings. See the Configure System Settings chapter in the [Cisco Catalyst Center Administrator Guide](#) for information about enabling ITSM approval.

### Before you begin

You must have the appropriate permissions to do the tasks as described in this procedure. For information about role-based access control for the Catalyst Center platform, see the [Cisco Catalyst Center Platform User Guide](#).

### Procedure

**Step 1** From the main menu, choose **Platform > Manage > Bundles**.

Review the displayed bundles and their status.

**Step 2** Click the Automation Events for ITSM (ServiceNow) bundle link or icon (colored square with initial) for additional information about the bundle.

Additional information that is provided may include:

- **General information:** Vendor, version, platform, tags displayed under the square icon.

- **Information:** Tab that displays general information (purpose of bundle and how bundle works in the network), sample schemas, configuration notes, and other data about the bundle.
- **Contents:** Tab that accesses the APIs and integration flows that make up the bundle, or provides information about the integration flows that make up the bundle.
- **Release Notes:** Tab that displays latest release information about the bundle, including its version.

**Step 3** Click each of the preceding tabs and review the information about the bundle.

**Step 4** Click **Enable** to enable the bundle.

An **Information** field appears in the window.

**Step 5** Click **Enable** in the **Information** field to confirm enabling the bundle.

After clicking **Enable** to confirm, a success message appears.

**Step 6** Click **OK** in the success message.

**Step 7** Click **Configure** to configure at the bundle level.

A configuration slide-in pane appears.

**Step 8** In the configuration slide-in pane, click **Automation Events Workflow Selection** to select events relating to software image updates, changes to configuration of network devices and group based policy update that need to be enabled for ITSM integration. This selection could be one or more, or all the events.

**Step 9** Click the radio button to configure either an existing ServiceNow Connection instance or configure a new instance.

**Figure 20: Example of Automation Events Workflow Selection configuration fields**

Configure Catalyst Center Automation events for ITSM (ServiceNow)

Configure your bundle

Automation Events Workflow Selection

This is used to select what events (events relating to software image updates, changes to configuration of network devices and group based policy updates) need to be enabled for ITSM integration. This selection could be one or more or all the events.

☐ Select an existing instance ☒ Create a new instance

AUTOMATION EVENTS WORKFLOW SELECTION

Software Image Management \*

Network Provisioning \*

Group Based Policies \*

Destination to receive events

Cancel Activate

To configure an existing ServiceNow Connection instance, select it from the drop-down list in the window and click **Activate**.

**Step 10** To configure a new ServiceNow Connection instance, you must enter this additional information:

- **Instance Name:** Name of the instance.
- **Description:** Descriptive text of the instance.
- **Software Image Management:** Select **true** from the drop-down list to enable ITSM integration of events relating to software image updates.
- **Network Provisioning:** Select **true** from the drop-down list to enable ITSM integration of events relating to configuration changes of network devices.
- **Group Based Policies:** Select **true** from the drop-down list to enable ITSM integration of events relating to group based policy updates.

**Step 11** In the configuration slide-in pane, click **ServiceNow Access Settings** to configure a ServiceNow Connection instance.

**Step 12** Click the radio button to configure either an existing ServiceNow Connection instance or configure a new instance.

**Figure 21: Example of ServiceNow instance configuration fields**

Configure SWIM Events for ITSM (ServiceNow)

Configure your bundle

ServiceNow Access Settings

>> Back to Select Instance

INFORMATION

Instance Name \*

Description

SERVICENOW ACCESS SETTINGS

Host Name \*

https://<servicenow-host-name>

Username \*

<username-for-servicenow-host>

Password \*

SHOW

Hint

Check connectivity

Destination to receive events

Cancel Activate

To configure an existing ServiceNow Connection instance, select it from the drop-down list in the window and click **Activate**.

**Step 13** To configure a new ServiceNow Connection instance, you must enter this additional information:

- **Instance Name:** Name of the instance.
- **Description:** Descriptive text of the instance.
- **Host name:** Hostname for the ServiceNow system.
- **Username:** Username required to access the ServiceNow system.
- **Password:** Password required to access the ServiceNow system.

**Step 14** Click **Check Connectivity** to test whether you can connect to the server where the endpoint is located. After a successful test of connectivity to the server, activate the bundle.

**Step 15** In the configuration slide-in pane, click **Destination to receive events** to configure a Destination Connection instance.

**Step 16** Click the radio button to configure either an existing Destination Connection instance or configure a new instance.

**Figure 22: Example of Destination to receive events configuration fields**

Configure SWIM Events for ITSM (ServiceNow)

Configure your bundle

> ServiceNow Access Settings

✓ Destination to receive events

INFORMATION

Instance Name \*

Description

DESTINATION TO RECEIVE EVENTS

Destination to receive events \* ▾

Destination Uri

Enter a custom endpoint

Cancel Activate

To configure an existing Destination Connection instance, select it from the drop-down menu in the window and click **Activate**.

**Step 17** To configure a new Destination instance, you must enter this additional information:

- **Instance Name:** Name of the instance.
- **Description:** Descriptive text of the instance.

- **Destination to receive events:** Select one of these options:
  - **Event Management:** When setting up Catalyst Center integration with ServiceNow without using the Cisco Catalyst app, select the **Event Management** option. The **Event Management** option requires that you have the Event Management plug-in that is configured within the ServiceNow instance.
  - **REST API Endpoint:** You can use the **REST API Endpoint** option with the Cisco Catalyst app. Data is sent to a REST API endpoint within the Cisco Catalyst app with the **REST API Endpoint** option.
  - **Generic REST Endpoint in ServiceNow:** For the **Generic REST Endpoint in ServiceNow** option, you can send the data to a different staging table in ServiceNow.
- **Destination URI:** Enter a destination Uniform Resource Indicator (URI) for the **Generic REST Endpoint in ServiceNow** option. This field is mandatory for this option.

After entering this information, proceed to the next step.

**Step 18** Click **Activate** to save your changes and activate the bundle or click **Cancel** to cancel the configuration and close the slide-in pane.

**Note**

By clicking **Activate**, you enable the changes that are made to the bundle and the changes take effect immediately. The bundle's status changes from **ENABLED** to **ACTIVE**.

## Configure the Cisco SD-Access integration with ITSM (ServiceNow)

The Cisco SD-Access integration with ServiceNow monitors and publishes fabric events that require fabric role updates for security or other operational triggers to an ITSM (ServiceNow) system. It also allows you to trigger or schedule a synchronization between Catalyst Center devices and the ServiceNow CMDB system.

### Before you begin

Ensure that you have ServiceNow running on a system that you will integrate with Catalyst Center platform.

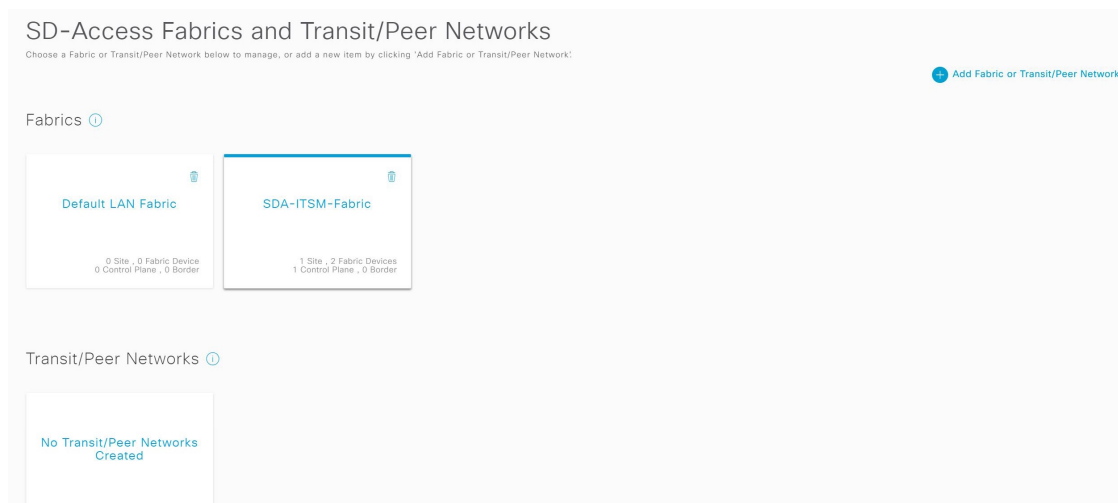
- Run a successful **Discovery** job in Catalyst Center. You can check whether a **Discovery** job is successful in **Device Inventory**. From the main menu, choose **Provision** > **Inventory** to view the results.
- You must have the appropriate permissions to perform the tasks as described in this procedure. For information about role-based access control for the Catalyst Center platform, see the [Cisco Catalyst Center Platform User Guide](#).

### Procedure

- Step 1** From the main menu, choose **Platform** > **Manage** > **Bundles**.  
Review the displayed bundles and their status.
- Step 2** Enable and configure the **Basic ITSM (ServiceNow) CMDB Synchronization** bundle to configure data synchronization. For more information, see [Configure the Basic ITSM \(ServiceNow\) CMDB Synchronization Bundle](#).

- Step 3** Enable and configure the Automation Events for ITSM (ServiceNow) bundle to monitor and publish a fabric event. For more information, see [Configure the automation events for ITSM \(ServiceNow\) bundle, on page 15](#).
- Step 4** Configure access settings to ServiceNow for the Cisco SD-Access-ServiceNow instance. From the main menu, choose **System > Settings > External Services**.
- Step 5** In the left pane, click **Destination** and select **ITSM** to add or edit a ServiceNow instance. For more information, see **Configure ITSM Integration** in the [Cisco Catalyst Center Platform User Guide](#).
- Step 6** Add a device to the fabric and assign a role based on your requirement. The role can be control plane, border, or edge. From the main menu, choose **Provision > Fabric**.
- The window displays all the provisioned fabric domains.
- Step 7** From the list of fabric domains, select **SDA-ITSM-Fabric**.

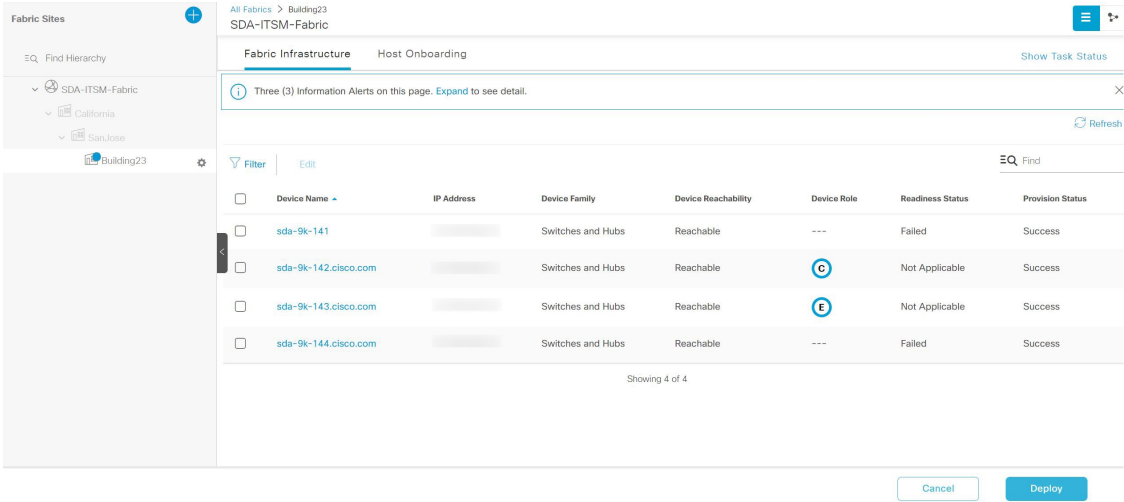
**Figure 23: Catalyst Center Platform fabrics**



The resulting screen displays all the fabric sites in the fabric domain.

- Step 8** Select a fabric site.
- The **Fabric Infrastructure** table lists all devices in the network that have been inventoried.
- Note**  
Any device that is added to the fabric is shown with a blue circle in the **Device Role** column.

Figure 24: List of devices in Fabric Infrastructure



**Step 9** In the list view, click a device. The device details window slides in with these **Fabric** options:

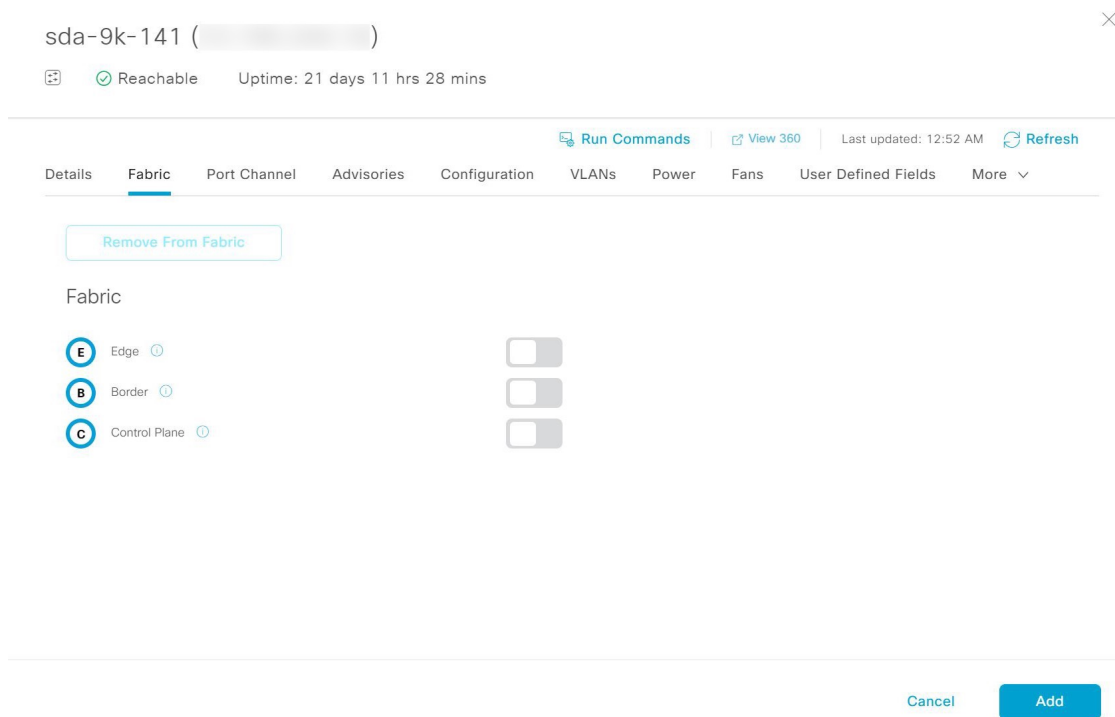
Option	Description
Edge	Click the toggle button next to this option to enable the selected device as an edge node.
Border	Click the toggle button next to this option to enable the selected device as a border node.
Control Plane	Click the toggle button next to this option to enable the selected device as a control plane node.

- Note**
- To configure a device as a fabric-in-a-box, select the **Control Plane**, **Border**, and **Edge** options.
  - To configure the device as a control plane and a border node, select both **Control Plane** and **Border**.

**Step 10** Click **Add**.

**Step 11** (Optional) To remove a device from the fabric, select the device and in the device slide-in pane, click **Remove From Fabric**.



**Figure 25: Device Roles of a Fabric**

**Step 12** Click **Deploy** to deploy the device role.

**Step 13** In the **Modify Fabric Domain** window, click **Now** to create a ticket immediately or click **Later** to schedule the ticket creation at a specific time.

**Step 14** Click **Apply**.

**Note**

If you select **Later** to schedule a ticket creation at a specific time, the request goes to the Catalyst Center scheduler.

**Step 15** From the main menu, choose **Activities > Tasks** to view upcoming, in-progress, successful, and failed fabric tasks.

**Step 16** In the **Tasks** window, the ticket status summary displays this information:

- Status of the fabric ticket request: Ticket Approved, Ticket Rejected, or Failed.
- Timestamp of the fabric ticket.

Figure 26: Status of fabric ticket requests

Audit Logs			Tasks	Work Items
<div>FILTERS: TYPE All</div>			<div>STATUS All Upcoming In Progress Success Failed</div>	<div>Last updated: 12:31:10 AM Refresh</div>
1	PROVISION	Modifying Fabric at sjc23	Starts: Dec 22, 2020 12:32 AM Status: Ticket Pending	Edit Cancel
2	PROVISION	Modifying Fabric at sjc23 Remove CP	Starts: Dec 22, 2020 12:28 AM Status: Ticket Pending Failed	
3	PROVISION	Modifying Fabric at sjc23 remove cp	Starts: Dec 22, 2020 12:15 AM Status: Ticket Rejected Failed	
4	PROVISION	Modifying Fabric at sjc23	Starts: Dec 21, 2020 11:44 PM Status: Success	
5	DISCOVERY	sda-itsm-discovery-2	Starts: Dec 21, 2020 11:36 PM Status: Success	
6	PROVISION	Modifying Fabric at sjc23		

- Step 17

To view the event summary of the Cisco SD-Access provision creation request, click the menu icon and choose **Platform > Runtime Dashboard > SDA Provision Creation Request**.

The **SDA Provision Creation Request** slide-in pane displays the Event ID, Source, Destination, ITSM Workflow, ITSM Status, ITSM ID, ITSM Link, ITSM Last Updated Time, ITSM Entity Severity/Priority, and Event Severity of an individual fabric event. For more information, see **Review the Event Summary** in the [Cisco Catalyst Center Platform User Guide](#).

# Catalyst Center endpoint attribute retrieval with ServiceNow

With this Catalyst Center release, you can configure Catalyst Center endpoint attribute retrieval with ServiceNow using the Cisco Catalyst app (version 2.3.1) that allows you to schedule a synchronization or trigger an update between the endpoint inventory and your ITSM (ServiceNow) configuration management database (CMDB). Endpoint attribute information from ServiceNow can be used to help profile endpoints in your network. ServiceNow appears in the endpoint profiling workspace as an additional probe. You may create custom profiling rules leveraging the attributes sent by ServiceNow.

Mapping between the ServiceNow CMDB fields and endpoint attributes occur at the platform level and is accomplished using the **Endpoint Attribute Retrieval with ITSM (ServiceNow)** bundle. This bundle supports the **Scheduler for ServiceNow Asset Sync** integration flow, which can be configured to run on a set schedule to invoke an internal Cisco API to retrieve the endpoint attribute information from ServiceNow.

This table describes the procedure for configuring Catalyst Center endpoint attribute retrieval with ServiceNow.



Note

This procedure does not modify or delete any CIs on the existing ITSM (ServiceNow) tool.

Table 6: Catalyst Center endpoint attribute retrieval with ServiceNow

Step	Description
Step 1	<p>Install or upgrade to the latest Catalyst Center release.</p> <p>For information about installing Catalyst Center, see the <a href="#">Cisco Catalyst Center Installation Guide</a>.</p>
Step 2	<p>Install or upgrade to a compatible version of ServiceNow mentioned on the ServiceNow Store website.</p> <p>Click this link to access the ServiceNow Store website:</p> <p><a href="https://store.servicenow.com/sn_appstore_store.do#!/store/application/03eb0f4ddb6ba00f27978b5ae96197b/2.3.1">https://store.servicenow.com/sn_appstore_store.do#!/store/application/03eb0f4ddb6ba00f27978b5ae96197b/2.3.1</a></p> <p>See your ServiceNow documentation for the installation and upgrade procedures.</p> <p><b>Note</b> This procedure must be done by a ServiceNow administrator.</p>
Step 3	<p>Download and install the Cisco Catalyst app (version 2.3.1) into ServiceNow by following the documentation available at the ServiceNow website.</p> <p><b>Note</b> Catalyst Center supports an application (Catalyst Center) that facilitates endpoint attribute retrieval with an ITSM (ServiceNow). This application or app is designed to work with ServiceNow <i>without</i> its Event Management plug-in.</p> <p>Click this link to access the ServiceNow Store website where the Cisco Catalyst app is located:</p> <p><a href="https://store.servicenow.com/sn_appstore_store.do#!/store/application/03eb0f4ddb6ba00f27978b5ae96197b/2.3.1">https://store.servicenow.com/sn_appstore_store.do#!/store/application/03eb0f4ddb6ba00f27978b5ae96197b/2.3.1</a></p> <p><b>Note</b> This procedure must be done by a ServiceNow administrator.</p>
Step 4	<p>Review and ensure that the requirements are met for the Catalyst Center-to-ServiceNow integration.</p> <p>For information, see <a href="#">Requirements, on page 22</a>.</p>
Step 5	<p>Configure the <b>Endpoint Attribute Retrieval with ITSM (ServiceNow)</b> bundle.</p> <p>For information, see <a href="#">Configure the Endpoint Attribute Retrieval Bundle with ITSM (ServiceNow), on page 48</a>.</p>

## Requirements

Review and ensure that this networking and systems requirements are met for the Catalyst Center-to-ServiceNow integration:

- Networking:
  - The Cisco Catalyst app is configured with the IP address and access information of the Catalyst Center installation that it is being integrated with.




---

**Note** Contact your Catalyst Center administrator to obtain this information.

---

- HTTPS network access between Catalyst Center and ServiceNow.




---

**Note** Contact and work with your network administrator to establish this.

---

- Management, Instrumentation, and Discovery (MID) Server:
  - The MID server is up and running, as well as accessible from the ServiceNow instance.
  - The Catalyst Center platform is accessible from the MID server.
  - The Catalyst Center platform REST APIs are allowed from the MID server.




---

**Note** The MID server is used to proxy the REST requests from the ServiceNow instance.

---

See the *Scope Certified Application Installation and Configuration Guide* on the ServiceNow Store website for MID server configuration information: [https://store.servicenow.com/sn\\_appstore\\_store.do#!/store/application/03eb0f4ddbfb6ba00f27978b5ae96197b](https://store.servicenow.com/sn_appstore_store.do#!/store/application/03eb0f4ddbfb6ba00f27978b5ae96197b)

- Catalyst Center Platform:
  - The Catalyst Center platform is enabled in Catalyst Center.
  - The requisite bundle or bundles in the Catalyst Center platform are configured and activated (as described in the next procedures).




---

**Note** These bundles have the required APIs that integrate with the Cisco Catalyst app in ServiceNow.

---

## Configure the Endpoint Attribute Retrieval Bundle with ITSM (ServiceNow)

Perform this procedure to configure Catalyst Center endpoint attribute retrieval from the ServiceNow CMDB.

### Before you begin

- Ensure that you have ServiceNow running on a system that you will integrate with Catalyst Center platform.
- You must have the appropriate permissions to perform the tasks as described in this procedure. For information about role-based access control for the Catalyst Center platform, see the [Cisco Catalyst Center Platform User Guide](#).

- Ensure that you have installed or upgraded the latest Catalyst Center release with Cisco ISE version 3.1 or later.

**Note**

While configuring the **ISE Configuration** in the Cisco AI Endpoint Analytics configuration window, it is recommended to check the **Enhanced Authorization Integration** check box to avoid duplicate data being sent to Cisco ISE. For more information, see **Publish Authorization Attributes to Cisco ISE** in the [Cisco Catalyst Center User Guide](#).

## Procedure

**Step 1** From the main menu, choose **Platform > Manage > Bundles**.

Review the displayed bundles and their current status.

**Step 2** Click the **Endpoint Attribute Retrieval with ITSM (ServiceNow)** bundle link or icon (colored square with initial) for additional information about the bundle.

Additional information provided may include these details:

- **General information:** Vendor, version, platform, tags displayed under the square icon.
- **Information:** Tab that displays general information (purpose of bundle and how bundle works in the network), sample schemas, configuration notes, and other data about the bundle.

**Note**

The specific endpoint attribute data that is retrieved is displayed in the **Information** tab. This endpoint attribute data will be retrieved from ServiceNow (with the display name in Catalyst Center within the parenthesis):

- Asset Tag (CMDB asset tag)
  - Model Category (CMDB model category)
  - Model (CMDB model)
  - Managed by (CMDB managed by)
  - Serial Number (CMDB serial number)
  - Location (CMDB location)
  - Department (CMDB department)
  - MAC Address (CMDB MAC address)
  - Display Name (CMDB display name)
- **Contents:** Tab that accesses the APIs and integration flows that make up the bundle, or provides information about the integration flows that make up the bundle.
  - **Release Notes:** Tab that displays the latest release information about the bundle, including its version.

**Step 3** Click the **Contents** tab.

**Step 4** Click the **Integration Flows** header.

The integration flows appear underneath the header.

**Step 5** Click the **Enable** button to activate the integration flow links.

An **Information** field appears in the window.

**Step 6** In the **Information** field, click the **Enable** button to confirm enabling the bundle.

After clicking the **Enable** button to confirm, a success message appears.

**Step 7** Click **Okay** in the success message.

**Step 8** Click the link for the individual integration flow to do these tasks.

For the schedule-based integration flow (**Scheduler for ServiceNow Asset Sync**), do these tasks:

- Review the **Description**, **Tags**, **How to Use this Flow**, and scheduler.
- Click **Run Now** (to run the scheduler now), **Run Later** (to schedule for a later time), or **Recurring** (to set up a recurring schedule).

For **Run Later**, you need to select a date, time, and time zone. For **Recurring**, you need to set a repeating interval (hourly, daily or weekly), an interval duration (minutes or hours), and a start and end date.

- Click **Schedule** to enable the scheduler.

**Important**

- Only configure and enable an integration flow schedule after you have finished configuring the bundle itself as described in this procedure. You can configure and enable an integration flow schedule by returning to this view and clicking **Schedule**. Or, click the **View Flows** link in the **Endpoint Attribute Retrieval with ITSM (ServiceNow)** slide-in pane (see these steps). Or, click the menu icon and choose **Platform > Developer Toolkit > Integration Flows > Scheduler for ServiceNow Asset Sync**.
- When you perform the synchronization once, it is always a full sync.
- The incremental sync is performed only on the scheduled synchronization.
- The **Recurring** synchronization is scheduled synchronization, while the **Run Later** synchronization is a one-time sync.
- The first occurrence of recurring synchronization is also a full sync. You must configure a minimum of two occurrences for the recurring synchronization.
- To complete the first full synchronization, you must configure the synchronization schedule with an hourly difference of at least two hours.

**Figure 27: Scheduler for ServiceNow Asset Sync**

Scheduler for ServiceNow Asset Sync

Not Scheduled

---

**DESCRIPTION**

This BAPI runs on defined schedule to invoke an other BAPI-Get CI Data from SNow

**TAGS**

CMDB Asset ITSM Integration

**HOW TO USE THIS FLOW**

The integration flows can be scheduled to run periodically at a specified date/time. Configure scheduling the integration flow with the form provided.

\* Schedule window cannot be lower than 1 hour with a concurrency of 1

☒ Run Now  
☐ Run Later  
☐ Recurring

Schedule

**Step 9** Click the **X** icon to return to the previous bundle window.

**Step 10** Click the **Configure** button to configure at the bundle level.

A configuration slide-in pane appears. Review the **Configure Endpoint Attribute Retrieval with ITSM (ServiceNow)** information.

**Step 11** Click the **Configure** button to configure at the bundle level.

A configuration slide-in pane appears.

**Step 12** In the configuration slide-in pane, click **ServiceNow Access Settings** to configure a ServiceNow Connection instance.

**Step 13** Click the radio button to configure either an existing ServiceNow Connection instance or configure a new instance.

**Figure 28: Example of ServiceNow Instance Configuration Fields**

Configure Endpoint Attribute Retrieval with ITSM (ServiceNow)

Configure your bundle ✕

*i* This bundle has additional configurations for its Schedule-Based Integration Flows. [View Flows](#)

- Scheduler for ServiceNow Asset Sync - Unscheduled

✓ ServiceNow Access Settings

This is used to specify the connection settings to a ServiceNow instance

☐ Select an existing instance ☒ Create a new instance

INFORMATION

Instance Name \*

Description

SERVICENOW ACCESS SETTINGS

Cancel Activate

To configure an existing ServiceNow Connection instance, select it from the drop-down menu in the window and click **Activate**.

**Step 14** To configure a new ServiceNow Connection instance, you must enter this additional information:

- **Instance Name:** Name of the instance.
- **Description:** Descriptive text of the instance.
- **Host name:** Hostname for the ServiceNow system.
- **Username:** Username required to access the ServiceNow system.
- **Password:** Password required to access the ServiceNow system.

**Step 15** Click **Check Connectivity** to test whether you can connect to the server where the endpoint is located.

**Step 16** Expand the **Synchronization Options** to define the incremental sync of endpoints and do these steps:

- Click the **Create a new instance** radio button and configure a new ServiceNow connection instance:
  - In the **INFORMATION** area, enter the instance name and description.
  - In the **SYNCHRONIZATION OPTIONS** area, check the **Incremental Sync** check box to select the incremental sync of endpoints and specify the maximum limit for incremental sync records to pull in each cycle.



We recommend that you use **Incremental Sync**, which allows you to first retrieve all the data from ServiceNow and later retrieve only the modified data from the subsequent iterations.

**Note**

- You can specify a maximum of 100 incremental sync records.
- When you set up the synchronization for the first time, it is performed in full sync, even if it is an incremental sync.
- When you edit the synchronization settings, it is done in full sync, even if it is an incremental sync.

**Step 17**

Click **Save** to save the bundle.

---

**What to do next**

Configure the integration flow (**Scheduler for ServiceNow Asset Sync**) for this bundle, using one of the methods described previously.





## CHAPTER 4

# SWIM Closed Loop Automation

- [About SWIM closed loop automation, on page 55](#)
- [SWIM closed loop automation requirements, on page 56](#)
- [SWIM closed loop automation workflow, on page 56](#)

## About SWIM closed loop automation

This release supports closed loop automation for software image management (SWIM) between Catalyst Center and ServiceNow. Closed-loop automation consists of a user configuring the provisioning of software device images in Catalyst Center. This configuration information is then communicated directly from Catalyst Center to ServiceNow as an immediate or scheduled change request. The ServiceNow administrator reviews the change request and either approves or rejects it in ServiceNow. The change request acceptance or rejection is then communicated back to Catalyst Center.

After receipt of an approved change request from ServiceNow, Catalyst Center does the software update at that time (immediately) or at its scheduled future time.

After Catalyst Center successfully does the software update, a notification (task completed) is sent back to ServiceNow. If the software update fails, then this is also communicated back to ServiceNow (task fail), so that the user can then manually do the software update in Catalyst Center.



---

**Note** If the SWIM provisioning is stopped by the user in Catalyst Center during this process, a task termination notification is sent to ServiceNow.

---

Ensure that the Cisco Catalyst app (version 2.2.0) is installed within the ServiceNow instance and do these procedures to enable SWIM closed loop automation between Catalyst Center and ServiceNow:

1. Review the requirements to ensure that the prerequisites for this feature have been met. See [SWIM closed loop automation requirements, on page 56](#).
2. Review the SWIM closed loop automation workflow to ensure that the required Catalyst Center admin and ServiceNow admin tasks are done for this feature. See [SWIM closed loop automation workflow, on page 56](#).

# SWIM closed loop automation requirements

This table lists the requirements for SWIM closed loop automation.

**Table 7: SWIM closed loop automation requirements**

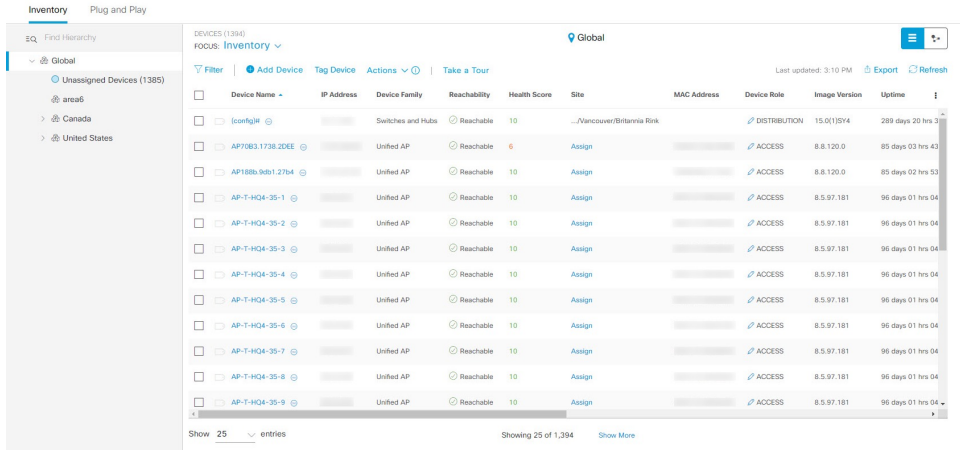
Software product, app, or procedure	Requirement
Catalyst Center	The latest Catalyst Center release.
Service Now	Any compatible version of ServiceNow mentioned on the ServiceNow Store website. Click this link to access the ServiceNow Store website: <a href="https://store.servicenow.com/sn_appstore_store.do#!/store/application/03eb0f4ddbf6ba00f27978b5ae96197b/2.2.0">https://store.servicenow.com/sn_appstore_store.do#!/store/application/03eb0f4ddbf6ba00f27978b5ae96197b/2.2.0</a>
Cisco Catalyst app	Cisco Catalyst app (version 2.2.0) This app is available through the ServiceNow website: <a href="https://store.servicenow.com/sn_appstore_store.do#!/store/application/03eb0f4ddbf6ba00f27978b5ae96197b/2.2.0">https://store.servicenow.com/sn_appstore_store.do#!/store/application/03eb0f4ddbf6ba00f27978b5ae96197b/2.2.0</a> The Cisco Catalyst app must be installed in your ServiceNow instance by a ServiceNow administrator. The Cisco Catalyst app versions 2.1.1 and 2.0.1 are compatible with the Tokyo and Utah releases of ServiceNow. If you want to use the Vancouver release of ServiceNow, you must first upgrade the Cisco Catalyst app to the latest version, 2.2.0.
Catalyst Center-to-ServiceNow ITSM integration	See <a href="#">Catalyst Center integration with ServiceNow using the Cisco Catalyst app, on page 20</a> .

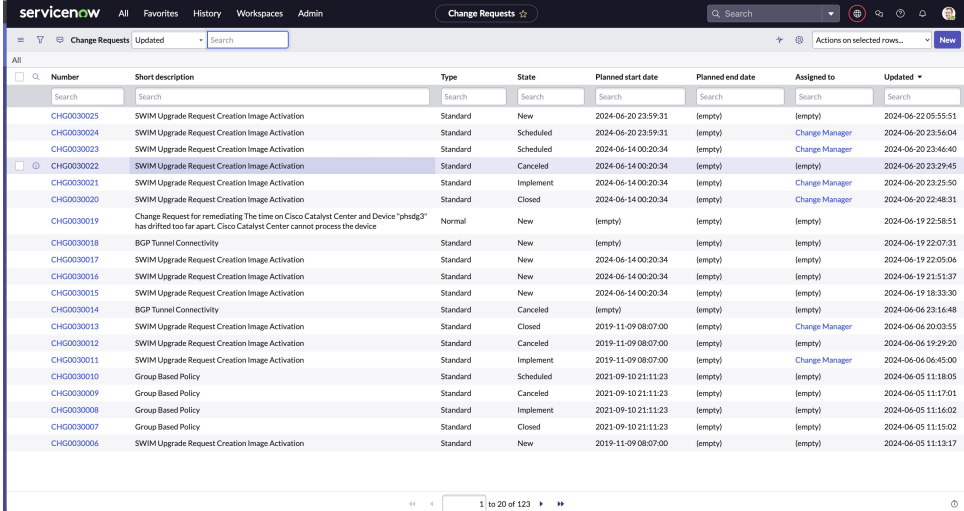
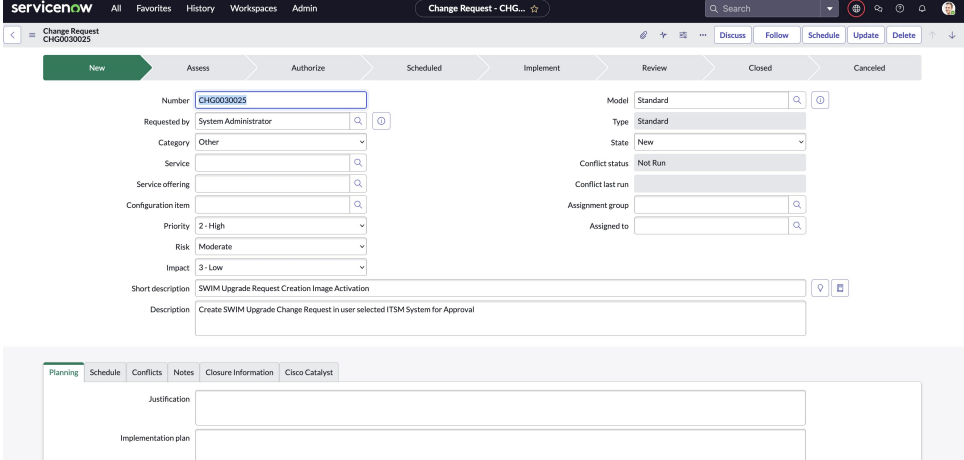
# SWIM closed loop automation workflow

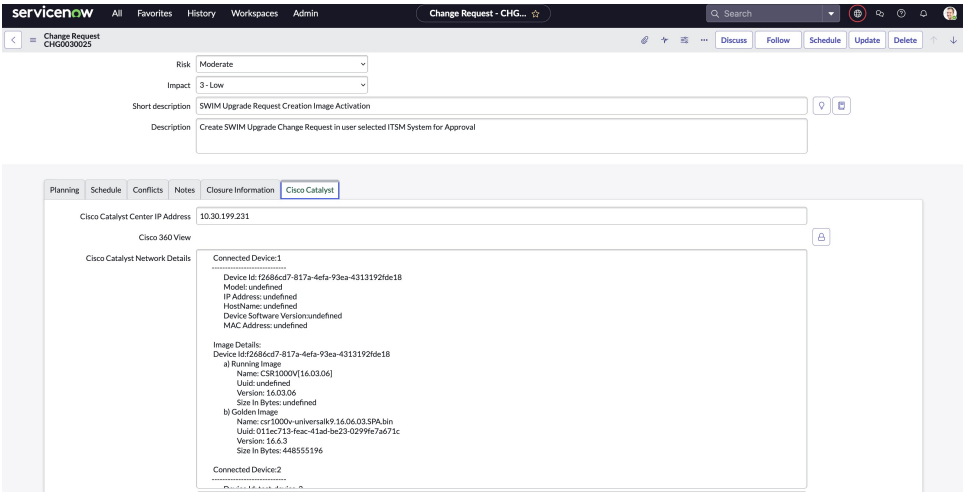
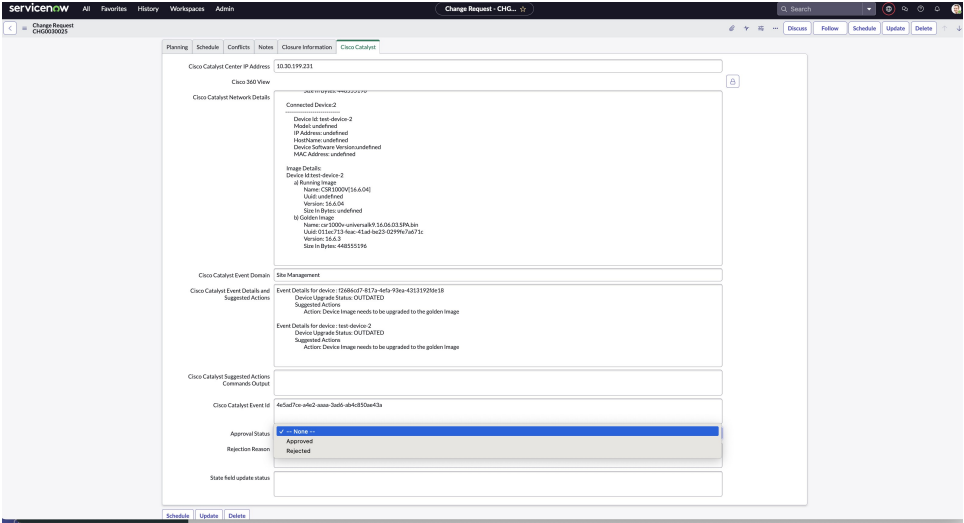
This table describes the SWIM closed loop automation workflow between Catalyst Center and ServiceNow.

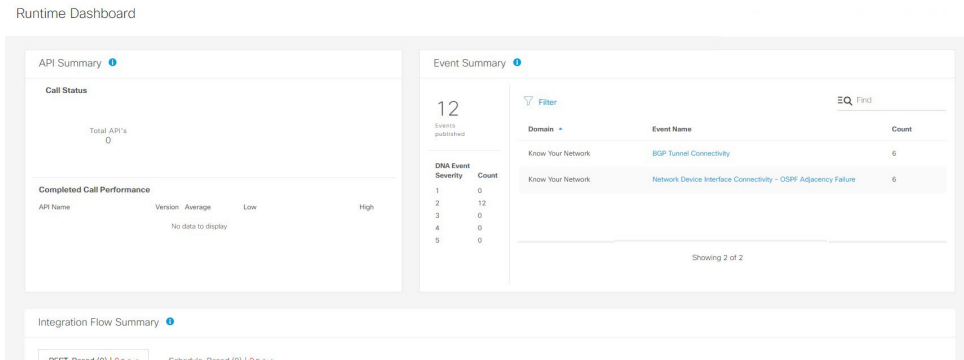
**Table 8: SWIM closed loop automation workflow**

Step	Description
Step 1	The Catalyst Center admin configures the Image Repository to prepare for the provisioning of devices in the network.  <b>Note</b> See the Manage Software Images chapter in the <a href="#">Cisco Catalyst Center User Guide</a> for information about setting up the Image Repository, as well as to review the software image provisioning process.

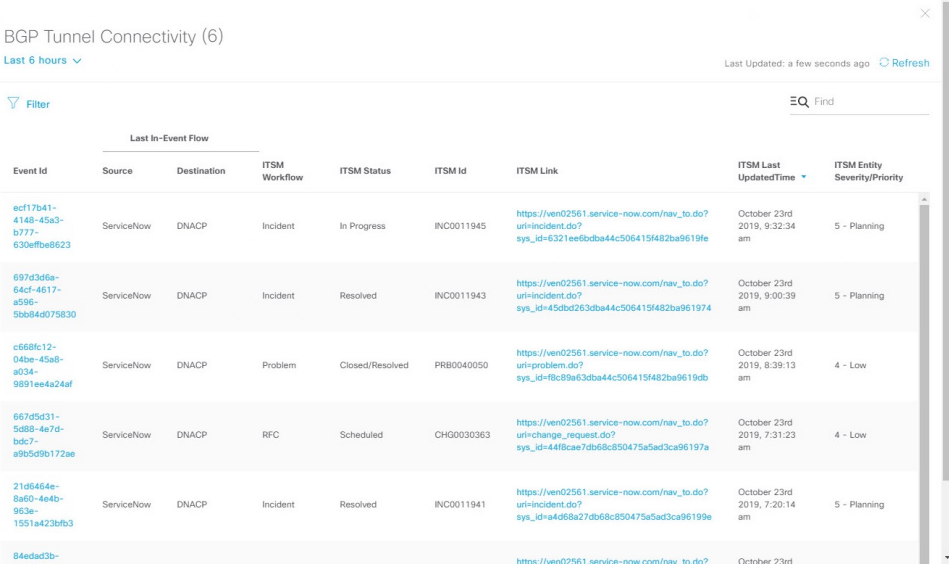
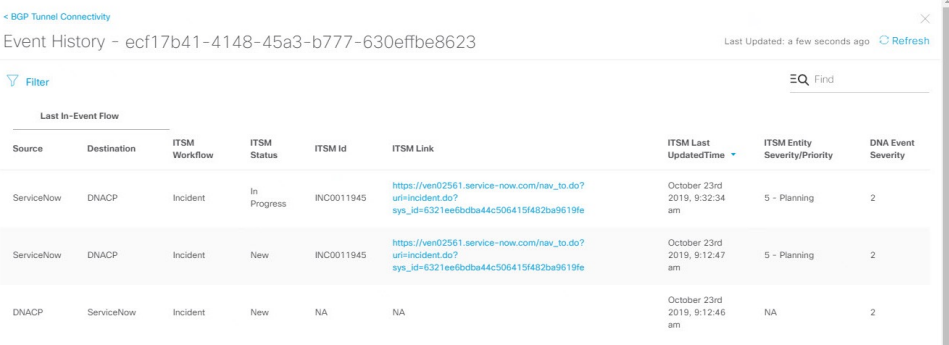
Step	Description
Step 2	<p>The Catalyst Center admin distributes the software image to a device or devices at the present time or schedules this activity for a later time.</p> <p><b>Note</b> Before this step is done, ensure that the Automation Events for ITSM (ServiceNow) bundle is configured and activated.</p> <ul style="list-style-type: none"> <li>From the Catalyst Center home page, the admin clicks <b>Provision</b>&gt; <b>Inventory</b>.</li> <li>From the <b>Focus</b> drop-down list, the admin selects <b>Software Images</b> and selects the device with the image to upgrade.</li> <li>From the <b>Actions</b> drop-down list, the admin chooses <b>Software Images</b> &gt; <b>Update Image</b> and does these tasks: <ul style="list-style-type: none"> <li><b>Distribute</b>: Clicks <b>Now</b> to start the distribution immediately or clicks <b>Later</b> to schedule the distribution at a specific time.</li> <li>Clicks <b>Next</b>.</li> <li><b>Activate</b>: Clicks <b>Now</b> to start the activation immediately or clicks <b>Later</b> to schedule the activation at a specific time.</li> <li><b>Confirm</b>: Clicks <b>Confirm</b> to confirm the update.</li> </ul> </li> </ul> <p><b>Figure 29: Cisco Catalyst Assurance provision</b></p>  <p><b>Note</b> See the "Manage Software Images" chapter in the <a href="#">Cisco Catalyst Center User Guide</a> for detailed information about this step.</p>

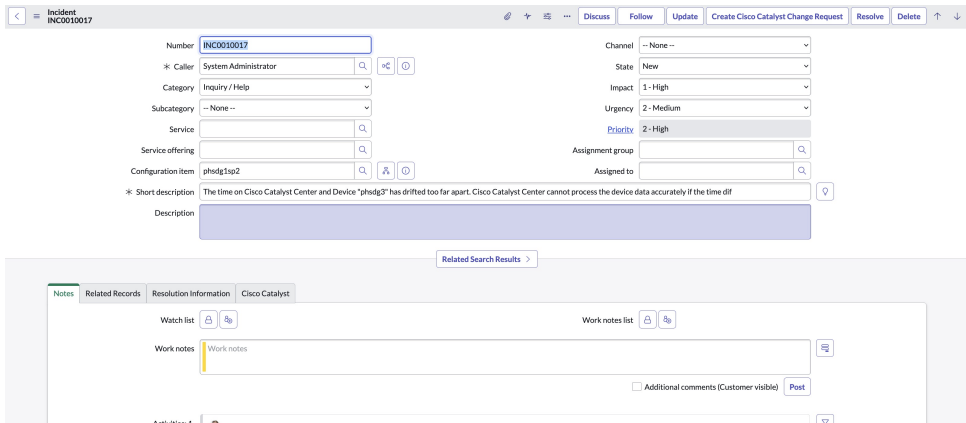
Step	Description
Step 3	<p>After a software image distribution is created in Catalyst Center (software image update to be activated immediately or later), a SWIM event is created and communicated directly to the ServiceNow ITSM as a change request ticket. This is done through the use of APIs from the Cisco Catalyst app. The change request ticket status is new.</p> <p>The SWIM event appears in the ServiceNow GUI in the ServiceNow <b>Change Requests</b> table.</p> <p><b>Figure 30: ServiceNow Change Requests</b></p> 
Step 4	<p>In the <b>Change Requests</b> table, the ServiceNow admin clicks the change request number (identifier) to open and review its status and data. In the ServiceNow GUI, the ServiceNow admin can edit the change request. For example, the admin can change the <b>State</b> from 'New' to 'Scheduled' and enter 'Change Management' for the <b>Assignment group</b>. The ServiceNow admin can also identify the SWIM change request with information in the <b>Short Description</b> field.</p> <p><b>Figure 31: Change Request</b></p> 

Step	Description
Step 5	<p>The ServiceNow admin now clicks the <b>Cisco Catalyst</b> tab in the change request. Important additional data synchronized from Catalyst Center to ServiceNow can be viewed in this tab.</p> <p><b>Figure 32: Cisco Catalyst tab</b></p> 
Step 6	<p>The ServiceNow admin now either approves or rejects the change request ticket in the ServiceNow GUI.</p> <p>In the <b>Cisco Catalyst</b> tab, the ServiceNow admin clicks the <b>Approval Status</b> field and clicks either <b>Approved</b> to approve the request or <b>Rejected</b> to reject the request.</p> <p><b>Note</b> Before the change request is executed, it must be approved in ServiceNow. Only after an approval in ServiceNow will the change request be executed in Catalyst Center.</p> <p><b>Figure 33: Cisco Catalyst Approval Status field</b></p> 

Step	Description
Step 7	After the ServiceNow admin approves the ticket and the status of the change request is changed to Implement, a notification is sent to Catalyst Center. In case the ticket is rejected, the update is sent to Catalyst Center in Scheduled state itself and the ServiceNow ticket is automatically canceled.
Step 8	<p>After a successful software image update in Catalyst Center, a notification (task completed) is sent back to ServiceNow. ServiceNow then closes the change request ticket. The change request ticket closure is done through the use of APIs from the Cisco Catalyst app.</p> <p><b>Note</b></p> <p>For a failed software update, ServiceNow reports the failure so that the ServiceNow admin can manually take action on the change request ticket. For a terminated software update, the change request ticket is canceled in ServiceNow. The reporting of both a failed software image update and a terminated software image update are also done through the use of APIs from the Cisco Catalyst app.</p>
Step 9	<p>The Catalyst Center admin can review the SWIM event by choosing <b>Runtime Dashboard &gt; Event Summary</b>.</p> <p><b>Note</b></p> <p>By clicking the individual events in the GUI window, the admin accesses additional GUI windows that permit direct access to the event in ServiceNow.</p> <p><b>Figure 34: Event Summary</b></p> <div><p>Runtime Dashboard</p></div>



Step	Description																																																															
Step 10	<p>The Catalyst Center admin clicks an event name (link) to view additional detailed data.</p> <p><b>Figure 35: Event history</b></p>  <table><thead><tr><th>Event Id</th><th>Source</th><th>Destination</th><th>ITSM Workflow</th><th>ITSM Status</th><th>ITSM Id</th><th>ITSM Link</th><th>ITSM Last UpdatedTime</th><th>ITSM Entity Severity/Priority</th></tr></thead><tbody><tr><td>ecf17b41-4148-45a3-b777-630effbe8623</td><td>ServiceNow</td><td>DNACP</td><td>Incident</td><td>In Progress</td><td>INC0011945</td><td>https://ven02561.service-now.com/nav_to.do?uri=incident.do?sys_id=6321ee6bdba44c506415f482ba9619fe</td><td>October 23rd 2019, 9:32:34 am</td><td>5 - Planning</td></tr><tr><td>697d3d6a-64cf-4617-a596-50b84d075830</td><td>ServiceNow</td><td>DNACP</td><td>Incident</td><td>Resolved</td><td>INC0011943</td><td>https://ven02561.service-now.com/nav_to.do?uri=incident.do?sys_id=450bd263dba44c506415f482ba961974</td><td>October 23rd 2019, 9:00:39 am</td><td>5 - Planning</td></tr><tr><td>c668fc12-04be-45a8-a034-9891ee4a24af</td><td>ServiceNow</td><td>DNACP</td><td>Problem</td><td>Closed/Resolved</td><td>PRB0040050</td><td>https://ven02561.service-now.com/nav_to.do?uri=problem.do?sys_id=fbc89a63dba44c506415f482ba9619db</td><td>October 23rd 2019, 8:39:13 am</td><td>4 - Low</td></tr><tr><td>667d5d31-5d88-4e7d-bdc7-a9b5d9b172ae</td><td>ServiceNow</td><td>DNACP</td><td>RFC</td><td>Scheduled</td><td>CHG0030363</td><td>https://ven02561.service-now.com/nav_to.do?uri=change_request.do?sys_id=44f8cae7db68c850475a5ad3ca96197a</td><td>October 23rd 2019, 7:31:23 am</td><td>4 - Low</td></tr><tr><td>21d6464e-8a60-4e4b-963e-1551a423bf93</td><td>ServiceNow</td><td>DNACP</td><td>Incident</td><td>Resolved</td><td>INC0011941</td><td>https://ven02561.service-now.com/nav_to.do?uri=incident.do?sys_id=a4d68a27db68c850475a5ad3ca96199e</td><td>October 23rd 2019, 7:20:14 am</td><td>5 - Planning</td></tr><tr><td>84edad3b-</td><td></td><td></td><td></td><td></td><td></td><td>https://ven02561.service-now.com/nav_to.do?uri=incident.do?sys_id=6321ee6bdba44c506415f482ba9619fe</td><td>October 23rd 2019, 9:32:34 am</td><td>5 - Planning</td></tr></tbody></table>	Event Id	Source	Destination	ITSM Workflow	ITSM Status	ITSM Id	ITSM Link	ITSM Last UpdatedTime	ITSM Entity Severity/Priority	ecf17b41-4148-45a3-b777-630effbe8623	ServiceNow	DNACP	Incident	In Progress	INC0011945	https://ven02561.service-now.com/nav_to.do?uri=incident.do?sys_id=6321ee6bdba44c506415f482ba9619fe	October 23rd 2019, 9:32:34 am	5 - Planning	697d3d6a-64cf-4617-a596-50b84d075830	ServiceNow	DNACP	Incident	Resolved	INC0011943	https://ven02561.service-now.com/nav_to.do?uri=incident.do?sys_id=450bd263dba44c506415f482ba961974	October 23rd 2019, 9:00:39 am	5 - Planning	c668fc12-04be-45a8-a034-9891ee4a24af	ServiceNow	DNACP	Problem	Closed/Resolved	PRB0040050	https://ven02561.service-now.com/nav_to.do?uri=problem.do?sys_id=fbc89a63dba44c506415f482ba9619db	October 23rd 2019, 8:39:13 am	4 - Low	667d5d31-5d88-4e7d-bdc7-a9b5d9b172ae	ServiceNow	DNACP	RFC	Scheduled	CHG0030363	https://ven02561.service-now.com/nav_to.do?uri=change_request.do?sys_id=44f8cae7db68c850475a5ad3ca96197a	October 23rd 2019, 7:31:23 am	4 - Low	21d6464e-8a60-4e4b-963e-1551a423bf93	ServiceNow	DNACP	Incident	Resolved	INC0011941	https://ven02561.service-now.com/nav_to.do?uri=incident.do?sys_id=a4d68a27db68c850475a5ad3ca96199e	October 23rd 2019, 7:20:14 am	5 - Planning	84edad3b-						https://ven02561.service-now.com/nav_to.do?uri=incident.do?sys_id=6321ee6bdba44c506415f482ba9619fe	October 23rd 2019, 9:32:34 am	5 - Planning
Event Id	Source	Destination	ITSM Workflow	ITSM Status	ITSM Id	ITSM Link	ITSM Last UpdatedTime	ITSM Entity Severity/Priority																																																								
ecf17b41-4148-45a3-b777-630effbe8623	ServiceNow	DNACP	Incident	In Progress	INC0011945	https://ven02561.service-now.com/nav_to.do?uri=incident.do?sys_id=6321ee6bdba44c506415f482ba9619fe	October 23rd 2019, 9:32:34 am	5 - Planning																																																								
697d3d6a-64cf-4617-a596-50b84d075830	ServiceNow	DNACP	Incident	Resolved	INC0011943	https://ven02561.service-now.com/nav_to.do?uri=incident.do?sys_id=450bd263dba44c506415f482ba961974	October 23rd 2019, 9:00:39 am	5 - Planning																																																								
c668fc12-04be-45a8-a034-9891ee4a24af	ServiceNow	DNACP	Problem	Closed/Resolved	PRB0040050	https://ven02561.service-now.com/nav_to.do?uri=problem.do?sys_id=fbc89a63dba44c506415f482ba9619db	October 23rd 2019, 8:39:13 am	4 - Low																																																								
667d5d31-5d88-4e7d-bdc7-a9b5d9b172ae	ServiceNow	DNACP	RFC	Scheduled	CHG0030363	https://ven02561.service-now.com/nav_to.do?uri=change_request.do?sys_id=44f8cae7db68c850475a5ad3ca96197a	October 23rd 2019, 7:31:23 am	4 - Low																																																								
21d6464e-8a60-4e4b-963e-1551a423bf93	ServiceNow	DNACP	Incident	Resolved	INC0011941	https://ven02561.service-now.com/nav_to.do?uri=incident.do?sys_id=a4d68a27db68c850475a5ad3ca96199e	October 23rd 2019, 7:20:14 am	5 - Planning																																																								
84edad3b-						https://ven02561.service-now.com/nav_to.do?uri=incident.do?sys_id=6321ee6bdba44c506415f482ba9619fe	October 23rd 2019, 9:32:34 am	5 - Planning																																																								
Step 11	<p>The Catalyst Center admin clicks an event ID number (link) to view only data associated with that specific event.</p> <p><b>Figure 36: Event ID data</b></p>  <table><thead><tr><th>Source</th><th>Destination</th><th>ITSM Workflow</th><th>ITSM Status</th><th>ITSM Id</th><th>ITSM Link</th><th>ITSM Last UpdatedTime</th><th>ITSM Entity Severity/Priority</th><th>DNA Event Severity</th></tr></thead><tbody><tr><td>ServiceNow</td><td>DNACP</td><td>Incident</td><td>In Progress</td><td>INC0011945</td><td>https://ven02561.service-now.com/nav_to.do?uri=incident.do?sys_id=6321ee6bdba44c506415f482ba9619fe</td><td>October 23rd 2019, 9:32:34 am</td><td>5 - Planning</td><td>2</td></tr><tr><td>ServiceNow</td><td>DNACP</td><td>Incident</td><td>New</td><td>INC0011945</td><td>https://ven02561.service-now.com/nav_to.do?uri=incident.do?sys_id=6321ee6bdba44c506415f482ba9619fe</td><td>October 23rd 2019, 9:12:47 am</td><td>5 - Planning</td><td>2</td></tr><tr><td>DNACP</td><td>ServiceNow</td><td>Incident</td><td>New</td><td>NA</td><td>NA</td><td>October 23rd 2019, 9:12:46 am</td><td>NA</td><td>2</td></tr></tbody></table>	Source	Destination	ITSM Workflow	ITSM Status	ITSM Id	ITSM Link	ITSM Last UpdatedTime	ITSM Entity Severity/Priority	DNA Event Severity	ServiceNow	DNACP	Incident	In Progress	INC0011945	https://ven02561.service-now.com/nav_to.do?uri=incident.do?sys_id=6321ee6bdba44c506415f482ba9619fe	October 23rd 2019, 9:32:34 am	5 - Planning	2	ServiceNow	DNACP	Incident	New	INC0011945	https://ven02561.service-now.com/nav_to.do?uri=incident.do?sys_id=6321ee6bdba44c506415f482ba9619fe	October 23rd 2019, 9:12:47 am	5 - Planning	2	DNACP	ServiceNow	Incident	New	NA	NA	October 23rd 2019, 9:12:46 am	NA	2																											
Source	Destination	ITSM Workflow	ITSM Status	ITSM Id	ITSM Link	ITSM Last UpdatedTime	ITSM Entity Severity/Priority	DNA Event Severity																																																								
ServiceNow	DNACP	Incident	In Progress	INC0011945	https://ven02561.service-now.com/nav_to.do?uri=incident.do?sys_id=6321ee6bdba44c506415f482ba9619fe	October 23rd 2019, 9:32:34 am	5 - Planning	2																																																								
ServiceNow	DNACP	Incident	New	INC0011945	https://ven02561.service-now.com/nav_to.do?uri=incident.do?sys_id=6321ee6bdba44c506415f482ba9619fe	October 23rd 2019, 9:12:47 am	5 - Planning	2																																																								
DNACP	ServiceNow	Incident	New	NA	NA	October 23rd 2019, 9:12:46 am	NA	2																																																								

Step	Description
Step 12	<p>The Catalyst Center admin clicks the ITSM Link to return to the ServiceNow Service Management GUI and specific incident.</p> <p><b>Figure 37: ServiceNow Incident</b></p> 



## CHAPTER 5

# Catalyst Center-to-PagerDuty Integration

- [About Catalyst Center-to-PagerDuty integration, on page 63](#)
- [Subscribe Catalyst Center event notifications to PagerDuty, on page 64](#)

## About Catalyst Center-to-PagerDuty integration

You can integrate Catalyst Center with PagerDuty.



**Note** PagerDuty is an incident management platform that provides reliable notifications to detect and correct infrastructure problems. For information about PagerDuty, see <https://www.pagerduty.com/>.

This table displays the supported Catalyst Center-to-PagerDuty integration workflow.

**Table 9: Catalyst Center-to-PagerDuty integration workflow**

Step	Description
Step 1	<p>Review these Catalyst Center-to-PagerDuty integration requirements:</p> <ul style="list-style-type: none"><li>• The latest Catalyst Center release.</li><li>• PagerDuty</li></ul> <p><b>Note</b> PagerDuty integration with Catalyst Center is accomplished using the PagerDuty Events REST APIs and the Catalyst Center Events framework.</p>
Step 2	<p>Configure the integration settings. From the main menu, choose <b>System &gt; Settings &gt; System Configuration &gt; Integration Settings</b>. Enter your callback URL hostname or IP address.</p>
Step 3	<p>Select and subscribe one or more events to forward notifications from Catalyst Center to PagerDuty.</p> <p>To access an event in Catalyst Center, click the menu icon and choose <b>Platform &gt; Developer Toolkit &gt; Event Notifications &gt; Event Catalog</b>. <b>Event Catalog</b> displays all the events.</p> <p>Click the <b>Notification</b> tab to subscribe to an event.</p>

Step	Description
Step 4	<p>In the <b>Notifications</b> tab, create a new notification for the event.</p> <p>Follow the steps in the <b>Create a New Notification</b> wizard and select PagerDuty as the notification channel.</p> <p>This data must be entered in the Catalyst Center platform GUI for the selected event:</p> <ul style="list-style-type: none"> <li>• PagerDuty Events API URL</li> <li>• PagerDuty Integration key (routing key)</li> </ul> <p>For detailed information about this event configuration procedure, see <a href="#">Subscribe Catalyst Center event notifications to PagerDuty, on page 64</a>.</p>
Step 5	<p>Notifications for the selected event are now forwarded to PagerDuty from Catalyst Center.</p> <p>These are the supported workflow connections between Catalyst Center issues and PagerDuty events:</p> <ul style="list-style-type: none"> <li>• Open Catalyst Center to trigger PagerDuty.</li> </ul>
Step 6	<p>PagerDuty responds to Catalyst Center with one of these REST API responses:</p> <ul style="list-style-type: none"> <li>• 202: The event has been accepted by PagerDuty.</li> <li>• 400: Bad Request - Check that the JSON is valid.</li> <li>• 429: Too many API calls at a time.</li> <li>• 500 or other 5xx: Internal Server Error - the PagerDuty server experienced an error while processing the event.</li> <li>• Networking Error: Error while trying to communicate with PagerDuty servers.</li> </ul>
Step 7	<p>Review and change (if necessary) the incident status in PagerDuty.</p> <p><b>Note</b> See your PagerDuty documentation for information about doing this step.</p>
Step 8	<p>Close the incident in PagerDuty.</p> <p><b>Note</b> See your PagerDuty documentation for information about doing this step.</p>
Step 9	<p>PagerDuty integration is a one-way notification from Catalyst Center to PagerDuty. Catalyst Center is not dependent on PagerDuty status to close an issue.</p>

## Subscribe Catalyst Center event notifications to PagerDuty

You can configure a Catalyst Center platform event notification to appear in PagerDuty as an alert. Follow the steps described in this procedure to configure a Catalyst Center event notification so that it appears in PagerDuty.

### Before you begin

Ensure that you have PagerDuty running on a system that you will integrate with Catalyst Center platform. See your PagerDuty documentation for instructions on setting up PagerDuty.

You must have the appropriate permissions to do the tasks as described in this procedure. For information about role-based access control (RBAC) for the Catalyst Center platform, see the [Cisco Catalyst Center Platform User Guide](#).

## Procedure

- 
- Step 1** From the main menu, choose **Platform > Developer Toolkit > Event Notifications**.  
The **Event Notifications** window opens.
- Step 2** Click the **Notifications** tab to view the notification tiles.  
Each notification is represented by a tile and contains link to view notification details. From the CHANNELS area in the left pane, click the radio button next to the notification channels to view the existing tiles with the selected channel.
- Step 3** Follow the steps in the **Create a New Notification** wizard to create a new notification.  
Click **Let's Do It** to go directly to the workflow.
- Step 4** In the **Select Site and Events** window, select a site from the drop-down list and select an event or events that support the required notification channel.
- Step 5** Click **Next**.  
The **Select Channels** window opens.
- Step 6** In the **Select Channels** window, select **PAGERDUTY** as the notification channel.  
Click **Next** to configure these values in the **PAGERDUTY Settings** window:
- In the SERVICE CONFIGURATION area, click either **Select Existing Instance** to use the existing PagerDuty instance or **Create New Instance** to create a new PagerDuty instance.
  - From the **Select Instance** drop-down list, select a PagerDuty instance.
  - In the **PagerDuty Events API URL** field, enter a PagerDuty event API URL.
  - In the **PagerDuty Integration Key** field, enter a PagerDuty integration key.
  - In the **PagerDuty Events API Version** field, select an events API version from the drop-down list.
- Step 7** Click **Next**.  
The **Name and Description** window opens.
- Step 8** Click **Next**.  
The **Summary** window opens.
- Step 9** In the **Summary** window, review the configuration settings.  
To make any changes, click **Edit**.
- Step 10** Click **Finish**.

The **Done! Your new notification is complete** window appears.

For more information, see **Work with Event Notifications** in the [Cisco Catalyst Center Platform User Guide](#) and **Create an Event Notification** in the [Cisco Catalyst Center User Guide](#).

---

### What to do next

Access PagerDuty to review the events.

The Catalyst Center events will appear in PagerDuty as alerts within the PagerDuty **INCIDENTS** window. You can review and mark the alert as **Resolved** in this window.



## CHAPTER 6

# Catalyst Center-to-Cisco Webex Integration

- [About Catalyst Center-to-Cisco Webex integration, on page 67](#)
- [Subscribe Catalyst Center event notifications to Cisco Webex, on page 68](#)

## About Catalyst Center-to-Cisco Webex integration

You can integrate Catalyst Center with Cisco Webex.

This table provides the supported Catalyst Center-to-Cisco Webex integration workflow.

**Table 10: Catalyst Center-to-Cisco Webex integration workflow**

Step	Description
Step 1	<p>Review these Catalyst Center-to-Cisco Webex integration requirements:</p> <ul style="list-style-type: none"><li>• The latest Catalyst Center release.</li><li>• Cisco Webex</li></ul> <p><b>Note</b> Catalyst Center integration with Cisco Webex is accomplished by using a Cisco Webex Bot, as well as using REST APIs.</p>
Step 2	<p>Create a Cisco Webex Bot for use in the integration.</p> <p>For information about creating a Cisco Webex Bot, see <a href="#">Webex Teams - Integrations &amp; Bots</a>.</p>
Step 3	<p>Configure the integration settings. From the main menu, choose <b>System &gt; Settings &gt; System Configuration &gt; Integration Settings</b>. Enter your callback URL hostname or IP address.</p>
Step 4	<p>Select and subscribe one or more events to forward notifications from Catalyst Center to Cisco Webex.</p> <p>To access an event in Catalyst Center, click the menu icon and choose <b>Platform &gt; Developer Toolkit &gt; Event Notifications &gt; Event Catalog</b>. <b>Event Catalog</b> displays all the events. Review the events and click the <b>Notifications</b> tab to subscribe to an event.</p>

Step	Description
Step 5	<p>In the <b>Notifications</b> tab, create a new notification for the event.</p> <p>Follow the steps in the <b>Create a New Notification</b> wizard and select Cisco Webex as the notification channel.</p> <p>This required data must be entered in the Catalyst Center platform GUI:</p> <ul style="list-style-type: none"> <li>• Authentication (bot access token)</li> <li>• Space name (or room ID)</li> </ul> <p>For detailed information about this procedure, see <a href="#">Subscribe Catalyst Center event notifications to Cisco Webex, on page 68</a>.</p>
Step 6	Any notifications for the selected event are now forwarded to Cisco Webex from Catalyst Center and published as a new message in Cisco Webex.
Step 7	<p>Cisco Webex responds to Catalyst Center with one of these API messages:</p> <ul style="list-style-type: none"> <li>• 202: The event has been accepted by Cisco Webex.</li> <li>• 400: Bad Request - Check that the JSON is valid.</li> <li>• 429: Too many API calls at a time.</li> <li>• 500 or other 5xx: Internal Server Error - the Cisco Webex server experienced an error while processing the event.</li> <li>• Networking Error: Error while trying to communicate with Cisco Webex servers.</li> </ul>
Step 8	Review the issue in Cisco Webex.
Step 9	Close the issue in Cisco Webex.
Step 10	Catalyst Center receives the status from Cisco Webex and then closes the issue.

## Subscribe Catalyst Center event notifications to Cisco Webex

Complete these steps to subscribe Catalyst Center platform event notifications to Cisco Webex.

### Before you begin

Ensure that you have Cisco Webex running on the network that you integrate with the Catalyst Center platform.

Ensure that you have **Webex Teams Room Id** and **Webex Teams Bot Access Token**. For more information, see [About Catalyst Center-to-Cisco Webex integration, on page 67](#).

You must have the appropriate permissions to do the tasks as described in this procedure. For information about role-based access control (RBAC) for the Catalyst Center platform, see the [Cisco Catalyst Center Platform User Guide](#).



## Procedure

- 
- Step 1** From the main menu, choose **Platform > Developer Toolkit > Event Notifications**.  
The **Event Notifications** window opens.
- Step 2** Click the **Notifications** tab to view the notification tiles.  
Each tile represents a notification and contains link to view notification details. From the CHANNELS area in the left pane, click the radio button next to the notification channels to view the existing tiles with the selected channel.
- Step 3** Follow the steps in the **Create a New Notification** wizard to create a new notification.  
Click **Let's Do It** to go directly to the workflow.
- Step 4** In the **Select Site and Events** window, select a site from the drop-down list and select an event or events that support the Webex notification channel.
- Step 5** Click **Next**.  
The **Select Channels** window opens.
- Step 6** In the **Select Channels** window, select WEBEX as the notification channel.  
Click **Next** to configure the values in the **WEBEX Settings** window.
- From the **Select Existing Instance** drop-down list, select an existing Webex instance or **Create New Instance**.
  - In the **Webex URL** field, enter the Webex URL.
  - In the **Webex Room ID** field, enter the Webex room ID, which is the space for receiving the event notifications.
  - In the **Webex Bot Access Token** field, enter the Webex bot access token.
- Step 7** Click **Next**.
- Step 8** In the **Name and Description** window, do these tasks:
- In the **Name** field, enter a unique name for the notification.
  - In the **Description** box, enter a description for the notification.
- Step 9** Click **Next**.  
The **Summary** window opens.
- Step 10** In the **Summary** window, review the configuration settings.  
To make any changes, click **Edit**.
- Step 11** Click **Finish**.  
The **Done! Your new notification is complete** window appears.  
For more information, see **Work with Event Notifications** in the [Cisco Catalyst Center Platform User Guide](#) and **Create an Event Notification** in the [Cisco Catalyst Center User Guide](#).
-

**What to do next**

Access Cisco Webex to review the events.