



Cisco DNA Center ITSM Integration Guide, Release 2.3.7.0 and 2.3.7.3

First Published: 2023-08-11

Last Modified: 2024-03-21

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 Cisco Systems, Inc. All rights reserved.



CONTENTS

| | | |
|------------------|------------------------------------|----------|
| CHAPTER 1 | New and Changed Information | 1 |
| | New and Changed Information | 1 |

| | | |
|------------------|--|----------|
| CHAPTER 2 | About Cisco DNA Center ITSM Integration | 3 |
| | Cisco DNA Center Integration Use Cases | 3 |
| | Cisco DNA Center ITSM Support | 3 |

| | | |
|------------------|---|----------|
| CHAPTER 3 | Cisco DNA Center ITSM Integration Workflows | 5 |
| | Cisco DNA Center Integration Supported Workflows | 5 |
| | Cisco DNA Center Integration with a Generic REST Endpoint | 5 |
| | Configure Network Events | 6 |
| | Configure Event Settings | 8 |
| | Cisco DNA Center Integration with ServiceNow Without the Cisco DNA App | 9 |
| | Configure the Network Issue Monitor and Enrichment for ITSM (ServiceNow) Bundle | 10 |
| | Configure Event Settings | 14 |
| | Configure the Cisco DNA Center Automation Events for ITSM (ServiceNow) Bundle | 15 |
| | Cisco DNA Center Integration with ServiceNow Using the Cisco DNA App | 19 |
| | Requirements | 21 |
| | Configure the Basic ITSM (ServiceNow) CMDB Synchronization Bundle | 22 |
| | Configure the Network Issue Monitor and Enrichment for ITSM (ServiceNow) Bundle | 32 |
| | Configure Event Settings | 35 |
| | Configure the Cisco DNA Center Automation Events for ITSM (ServiceNow) Bundle | 37 |
| | Configure the Cisco SD-Access Integration with ITSM (ServiceNow) | 40 |
| | Cisco DNA Center Endpoint Attribute Retrieval with ServiceNow | 44 |
| | Requirements | 45 |
| | Configure the Endpoint Attribute Retrieval Bundle with ITSM (ServiceNow) | 46 |

| | | |
|------------------|--|-----------|
| CHAPTER 4 | SWIM Closed Loop Automation | 53 |
| | About SWIM Closed Loop Automation | 53 |
| | SWIM Closed Loop Automation Requirements | 54 |
| | SWIM Closed Loop Automation Workflow | 54 |

| | | |
|------------------|---|-----------|
| CHAPTER 5 | Cisco DNA Center-to-PagerDuty Integration | 61 |
| | About Cisco DNA Center-to-PagerDuty Integration | 61 |
| | Subscribe Cisco DNA Center Event Notifications to PagerDuty | 63 |

| | | |
|------------------|---|-----------|
| CHAPTER 6 | Cisco DNA Center-to-Cisco Webex Integration | 65 |
| | About Cisco DNA Center-to-Cisco Webex Integration | 65 |
| | Subscribe Cisco DNA Center Event Notifications to Cisco Webex | 66 |



CHAPTER 1

New and Changed Information

- [New and Changed Information](#), on page 1

New and Changed Information

The following table summarizes the new and changed features for this release.

Table 1: New and Changed Features

| Feature | Description | Where Documented |
|--|--|---|
| Support for Visibility and Control of configurations | This Cisco DNA Center platform release supports an ITSM approval process for better control over device provisioning activities in Cisco DNA Center. | See Configure the Cisco DNA Center Automation Events for ITSM (ServiceNow) Bundle , on page 15. |



CHAPTER 2

About Cisco DNA Center ITSM Integration

- [Cisco DNA Center Integration Use Cases, on page 3](#)
- [Cisco DNA Center ITSM Support, on page 3](#)

Cisco DNA Center Integration Use Cases

Cisco DNA Center supports the following 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 Cisco DNA Center Platform chapter in the [Cisco DNA Center Platform User Guide](#) for detailed information about configuring integration settings.

Cisco DNA Center ITSM Support

Cisco DNA Center supports the following capabilities:

- Integrating Cisco DNA Center into ITSM processes of incident, event, change, and problem management.
- Integrating Cisco DNA Center into ITSM approval and preapproval chains.
- Integrating Cisco DNA 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 Cisco DNA Center, and then publish the event data on a recurring schedule to an ITSM (Service Now) system.

Cisco DNA Center bundles are prebuilt solutions that enable integration between Cisco DNA capabilities and specific IT domains. You can configure and use the following bundles:

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



CHAPTER 3

Cisco DNA Center ITSM Integration Workflows

- [Cisco DNA Center Integration Supported Workflows, on page 5](#)
- [Cisco DNA Center Integration with a Generic REST Endpoint, on page 5](#)
- [Cisco DNA Center Integration with ServiceNow Without the Cisco DNA App, on page 9](#)
- [Cisco DNA Center Integration with ServiceNow Using the Cisco DNA App, on page 19](#)
- [Cisco DNA Center Endpoint Attribute Retrieval with ServiceNow, on page 44](#)

Cisco DNA Center Integration Supported Workflows

The following Cisco DNA Center ITSM integration workflows are supported:

- Cisco DNA Center ITSM integration with a generic REST endpoint: See [Cisco DNA Center Integration with a Generic REST Endpoint, on page 5](#).
- Cisco DNA Center ITSM integration with ServiceNow without using the Cisco DNA application for ServiceNow: See [Cisco DNA Center Integration with ServiceNow Without the Cisco DNA App, on page 9](#).
- Cisco DNA Center ITSM integration with ServiceNow using the Cisco DNA application for ServiceNow: See [Cisco DNA Center Integration with ServiceNow Using the Cisco DNA App, on page 19](#).
- Cisco DNA Center ITSM endpoint attribute retrieval with ServiceNow using the Cisco DNA application for ServiceNow: See [Cisco DNA Center Endpoint Attribute Retrieval with ServiceNow, on page 44](#).

Cisco DNA Center Integration with a Generic REST Endpoint

The following table describes the procedure for configuring Cisco DNA 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: Cisco DNA Center to Generic REST Endpoint Integration Procedure

| Step | Description |
|--------|--|
| Step 1 | Install or upgrade to the latest Cisco DNA Center release. For information about installing Cisco DNA Center, see the Cisco DNA Center Installation Guide . |

| Step | Description |
|--------|---|
| Step 2 | Enable and configure bundles using the Bundles window in the Cisco DNA Center GUI. For more information about configuring bundles, see Cisco DNA Center Platform User Guide . |
| Step 3 | In the configuration slide-in pane, click Destination to receive events . |
| Step 4 | To send the data to a different staging table in ServiceNow, choose Generic REST Endpoint in ServiceNow 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 Event Settings . The Cisco DNA Center platform and ITSM integration allows the user to choose 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 Configure Event Settings, on page 8 . |
| Step 6 | Configure the integration settings. From the top-left corner, click the menu icon and choose System > Settings > System Configuration > Integration Settings . 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 Cisco DNA Center platform GUI.

Figure 1: Cisco DNA Center Platform Events Window

The screenshot shows the 'Event Notifications' window in the Cisco DNA Center GUI. The 'Event Catalog' tab is active, displaying a table of events. The table has columns for Event ID, Name, Type, Category, and Severity. The events listed are:

| 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 Cisco DNA 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 Cisco DNA Center platform, see the [Cisco DNA Center Platform User Guide](#).

-
- Step 1** From the top-left corner, click the menu icon and 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 DNA Center Platform User Guide](#) and **Create an Event Notification** in the [Cisco DNA Center User Guide](#).
-

Configure Event Settings

The Cisco DNA Center platform and ITSM integration allows you choose 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. The **Events Settings** window is accessible from the **Configurations** menu option in the Cisco DNA Center platform.



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

| 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 perform the tasks as described in this procedure. For information about role-based access control for the Cisco DNA Center platform, see the [Cisco DNA Center Platform User Guide](#).

Step 1 From the top-left corner, click the menu icon and 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 Cisco DNA Center event.
- **Domain:** Domain of the Cisco DNA 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 choose a value from the available options.

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

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

Step 5 Click **Save**.

Cisco DNA Center Integration with ServiceNow Without the Cisco DNA App

The following table describes the procedure for configuring Cisco DNA Center integration with ServiceNow without using the Cisco DNA 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 choose **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 DNA 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 perform any further action on the data.

Table 3: Cisco DNA Center-to-ServiceNow Integration Without the Cisco DNA App Procedure

| Step | Description |
|--------|---|
| Step 1 | Install or upgrade to the latest Cisco DNA Center release. For information about <i>installing</i> Cisco DNA Center, see the Cisco DNA Center Installation Guide . |

| Step | Description |
|--------|---|
| Step 2 | <p>Install or upgrade to a compatible version of ServiceNow mentioned on the ServiceNow Store website.</p> <p>Click the following link to access the ServiceNow Store website:</p> <p>https://store.servicenow.com/sn_appstore_store.do#!/store/application/03eb0f4ddb6ba00f27978b5ae96197b</p> <p>Refer to your ServiceNow documentation for its installation and upgrade procedures.</p> <p>Note This procedure must be performed by a ServiceNow administrator.</p> |
| Step 3 | <p>Configure the Network Issue Monitor and Enrichment for ITSM (ServiceNow) bundle. For information, see Configure the Network Issue Monitor and Enrichment for ITSM (ServiceNow) Bundle, on page 10.</p> <p>This bundle enables Change Management between the two systems (Cisco DNA 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 Event Settings.</p> <p>For information, see Configure Event Settings, on page 14.</p> <p>Note The Cisco DNA Center platform and ITSM integration allows the user to choose 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 Cisco DNA Center Automation events for ITSM (ServiceNow) bundle.</p> <p>For information, see Configure the Cisco DNA Center Automation Events for ITSM (ServiceNow) Bundle, on page 15.</p> <p>The Cisco DNA Center Automation events for ITSM (ServiceNow) bundle retrieves events relating to software image updates required for compliance, security or any other operational triggers from Cisco DNA Center. SWIM event notifications are sent from Cisco DNA Center to ServiceNow when they occur, not on a polling and notify schedule.</p> <p>For information, see About SWIM Closed Loop Automation, on page 53</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

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

**Note**

- 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 DNA app.
- The Event Management and Generic REST API Endpoint options do not support automatic ticket creation and auto resolution of tickets for closed loop integration.

Before you begin

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

-
- Step 1** From the top-left corner, click the menu icon and 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 the following:
- **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

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, choose it from the drop-down menu in the window and click **Activate**.

Step 10 For configuring a new ServiceNow Connection instance, the following 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, choose it from the drop-down menu in the window and click **Activate**.

Step 14

For configuring a new Destination instance, the following additional information must be entered:

- **Instance Name:** Name of the instance.
- **Description:** Descriptive text of the instance.
- **Destination to receive events:** Choose one of the following:
 - **Event Management:** When setting up Cisco DNA Center integration with ServiceNow without using the Cisco DNA app, choose 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 DNA app. With this option, data is sent to a REST API endpoint within the Cisco DNA app.
 - **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 Cisco DNA Center platform and ITSM integration permits you to choose 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. The **Events Settings** window is accessible from the **Configurations** menu option in the Cisco DNA Center platform.



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

| 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 perform the tasks as described in this procedure. For information about role-based access control for the Cisco DNA Center platform, see the [Cisco DNA Center Platform User Guide](#).

-
- Step 1** From the top-left corner, click the menu icon and choose **Platform > Manage > Configurations**.
A **Configurations** window opens that contains an **Events Settings** section.
- Step 2** Review the **Event Settings** section, which contains the following information:
- **Event Name:** Name of the Cisco DNA Center event.
 - **Domain:** Domain of the Cisco DNA 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.
Choose 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 Cisco DNA Center when the event occurs in the future.
- Step 5** Click **Save**.
-

Configure the Cisco DNA Center Automation Events for ITSM (ServiceNow) Bundle

Perform 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.

Enabling ITSM in Cisco DNA Center enforces a ServiceNow approval process for better control of Cisco DNA Center software image updates and other device provisioning activities. For example, see [SWIM Closed Loop Automation Workflow, on page 54](#) for information about the approval process in ServiceNow.

See the Configure System Settings chapter in the [Cisco DNA Center Administrator Guide](#) for information about enabling ITSM approval for device configuration changes.

**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 DNA app.
- The Event Management and Generic REST API Endpoint options do not support automatic ticket creation, approval/rejection workflow and auto resolution of tickets for closed loop integration.

Before you begin

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

-
- Step 1** From the top-left corner, click the menu icon and choose **Platform > Manage > Bundles**.
Review the displayed bundles and their status.
- Step 2** Click the **Cisco DNA Center 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 the following:
- **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 the **Enable** button to enable the bundle.
An **Information** field appears in the window.
- Step 5** Click the **Enable** button in the **Information** field 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 6: 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

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

Step 10 For configuring a new ServiceNow Connection instance, you must enter the following 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 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, activate the bundle.

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

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

Figure 7: 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

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

Step 14 For configuring a new Destination instance, you must enter the following additional information:

- **Instance Name:** Name of the instance.
- **Description:** Descriptive text of the instance.
- **Destination to receive events:** Choose one of the following:
 - **Event Management:** When setting up Cisco DNA Center integration with ServiceNow without using the Cisco DNA app, choose 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 DNA app. Data is sent to a REST API endpoint within the Cisco DNA 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 15 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. Additionally, the bundle's status changes from **ENABLED** to **ACTIVE**.

Cisco DNA Center Integration with ServiceNow Using the Cisco DNA App

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

Ensure that the Cisco DNA app (version 2.2.0) is installed within the ServiceNow instance and performs the following tasks:

- Schedules the basic one-way synchronization of Cisco DNA Center discovered devices into the ServiceNow Configuration Management Database (CMDB) using Cisco DNA Center inventory as a source of truth. The Cisco DNA app supports CMDB synchronization from Cisco DNA Center to ServiceNow.
- Automatically triggers problem, incident, and change workflows for network events published by Cisco DNA Center.
- Enriches ITSM tickets with network details from Cisco DNA Center. The Cisco DNA app makes REST API calls into Cisco DNA Center. These API calls help in fetching enrichment information of various types such as device, issue, user, and client for a user created ticket.
- Supports integration of the Cisco DNA Center platform with ServiceNow for an automated way to create change request (CR) tickets in ServiceNow for network events.

The following table describes the procedure for configuring Cisco DNA Center integration with ServiceNow using the Cisco DNA 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: Cisco DNA Center-to-ServiceNow Integration with Cisco DNA App Procedure

| Step | Description |
|--------|---|
| Step 1 | Install or upgrade to the latest Cisco DNA Center release. For information about <i>installing</i> Cisco DNA Center, see the Cisco DNA Center Installation Guide . |

| Step | Description |
|--------|---|
| Step 2 | <p>Install or upgrade to a compatible version of ServiceNow mentioned on the ServiceNow Store website.</p> <p>Click the following link to access the ServiceNow Store website:</p> <p>https://store.servicenow.com/sn_appstore_store.do#!/store/application/03eb0f4ddb6ba00f27978b5ae96197b/2.2.0</p> <p>Refer to your ServiceNow documentation for its installation and upgrade procedures.</p> <p>Note This procedure must be performed by a ServiceNow administrator.</p> |
| Step 3 | <p>Click the following link to access the ServiceNow Store website where the Cisco DNA app is located:</p> <p>https://store.servicenow.com/sn_appstore_store.do#!/store/application/03eb0f4ddb6ba00f27978b5ae96197b/2.2.0</p> <p>Download and install the Cisco DNA app (version 2.2.0) into ServiceNow by following the documentation available at the website.</p> <p>Note This procedure is to be performed by a ServiceNow administrator. The Cisco DNA 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 DNA app to the latest version, 2.2.0.</p> |
| Step 4 | <p>Review and ensure that the requirements are met for the Cisco DNA Center-to-ServiceNow integration.</p> <p>For information, see Requirements, on page 21.</p> |
| Step 5 | <p>Access the Cisco DNA Center platform GUI and configure the Basic ITSM (ServiceNow) CMDB Synchronization bundle.</p> <p>For information, see Configure the Basic ITSM (ServiceNow) CMDB Synchronization Bundle, on page 22.</p> <p>Note 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 Cisco DNA Center). Check with your ServiceNow administrator to see whether the CMDB Sync is being done elsewhere.</p> |
| Step 6 | <p>Configure the Network Issue Monitor and Enrichment for ITSM (ServiceNow) bundle. For information, see Configure the Network Issue Monitor and Enrichment for ITSM (ServiceNow) Bundle, on page 10.</p> <p>This bundle enables data to be sent from Cisco DNA 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 Event Settings.</p> <p>For more information, see Configure Event Settings, on page 35.</p> <p>Note The Cisco DNA Center platform and ITSM integration allows the user to choose 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 Cisco DNA Center Automation events for ITSM (ServiceNow) bundle. For information, see Configure the Cisco DNA Center Automation Events for ITSM (ServiceNow) Bundle, on page 15 . |
| Step 9 | Access your ServiceNow instance and review the network and SWIM event data that has been posted using the Cisco DNA Center REST APIs in this procedure. Begin to review and utilize this data per your business or network needs. |

Requirements

Review and ensure that the following networking and systems requirements are met for the Cisco DNA Center-to-ServiceNow integration:

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



Note Contact your Cisco DNA Center administrator to obtain this information.

- HTTPS network access between Cisco DNA 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 Cisco DNA Center platform is accessible from the MID server.
 - The Cisco DNA 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

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



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

Configure the Basic ITSM (ServiceNow) CMDB Synchronization Bundle

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



Note The Cisco DNA Center CMDB synchronization cannot detect multiple instances of Cisco DNA Center:

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

Before you begin

- Ensure that you have ServiceNow running on a system that you will integrate with Cisco DNA Center platform.
- Run a successful **Discovery** job in Cisco DNA Center. You can check whether a **Discovery** job is successful in **Device Inventory**. From the top-left corner, click the menu icon and 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 Cisco DNA Center platform, see the [Cisco DNA Center Platform User Guide](#).

Step 1 From the top-left corner, click the menu icon and 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 the following:

- **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 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 integration flow link to perform the tasks listed below:

- 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 by clicking the **View Flows** link in the **Configure Basic ITSM (ServiceNow) CMDB synchronization** slide-in pane (see following steps), or by clicking the menu icon (☰) > **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 8: ServiceNow Access 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 - Unscheduled

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, choose it from the drop-down menu in the window and click **Next**.

Step 12 For configuring a new access setting, the following 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, the following additional settings information must be entered.

Figure 9: 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 *

<password-to-connect-to-servicenow-host>

[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 10: 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 - Unscheduled

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, choose it from the drop-down menu in the window and click **Configure**.

Step 15

For configuring a new instance, the following 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 the following information:

- **Destination Type:** There are two destination type options to choose 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 DNA app. You should use this destination type, if you are using the Cisco DNA 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 DNA app. Ensure that the created staging table has a field called `u_inventory_details`. The inventory details from the Cisco DNA 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 11: Select Destination Window

The screenshot shows a configuration window titled "Configure Basic ITSM (ServiceNow) CMDB synchronization" with a subtitle "Configure your bundle". The main heading is "Select Destination". There are two input fields: "Destination Type *" with a dropdown arrow, and "Destination Uri *" with a placeholder text "Enter a Custom Endpoint". At the bottom left is an "Exit" button with a back arrow icon. At the bottom right are "Back" and "Next" buttons.

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 12: 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 the following 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**).

Currently, the integration only supports '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 Cisco DNA Center device families and ServiceNow CI classes.

Figure 13: 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 |

Device families are the Cisco DNA 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 DNA Center application in ServiceNow. The type and number of device families can vary depending upon the different Cisco devices in the user's network.

Note Cisco DNA Center platform is able to automatically retrieve all of the device families in the user's Cisco DNA 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, cmdb_ci_ip_switch, and x_caci_cisco_dna_wireless_lan_controller). The **CI Class** column in the GUI window is used to map the CI classes to their respective device families.

The following table displays the Cisco DNA 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 the 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**.

Step 20

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

Figure 14: Set Source Identifier and Operational Limit Window

Configure Basic ITSM (ServiceNow) CMDB synchronization
Configure your bundle

Set Source Identifier and Operational Limit

Enter Discovery Source *

Other Automated

Enter Max Limit *

1000

Configure the following values:

- **Enter Destination Type:** 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.

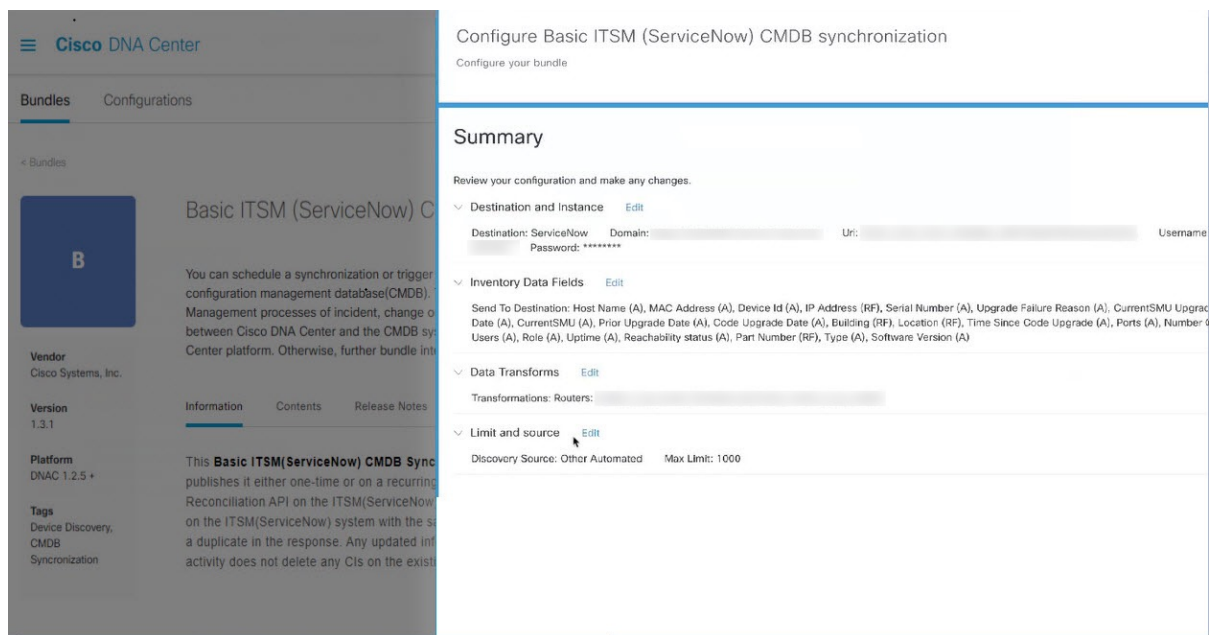
We recommend that the user creates their own discovery source, so as to uniquely identify the source from where the devices were fetched to sync into the ServiceNow instance. The steps to create a new discovery source are described in the ServiceNow App 'Installation and Configuration guide'.

- **Enter the Max Limit:** Maximum number of devices that can be synchronized in an iteration (single API call).

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

Step 21 In the **Summary** window, review the configuration summary.

Figure 15: Summary Window



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 performing the following tasks:

- From the top-left corner, click the menu icon and choose **Platform > Runtime Dashboard > CMDB Synchronization Summary**. Click **Refresh** to refresh the GUI view. Review the inventory device synchronization status to ServiceNow.

- From the top-left corner, click the menu icon and 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

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



Note

- 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 DNA app.
- The Event Management and Generic REST API Endpoint options do not support automatic ticket creation and auto resolution of tickets for closed loop integration.

Before you begin

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

-
- Step 1** From the top-left corner, click the menu icon and 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 the following:
- **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 16: 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, choose it from the drop-down menu in the window and click **Activate**.

Step 10 For configuring a new ServiceNow Connection instance, the following 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 17: Example of Destination to Receive Events Configuration Fields

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

Step 14 For configuring a new Destination instance, the following additional information must be entered:

- **Instance Name:** Name of the instance.
- **Description:** Descriptive text of the instance.
- **Destination to receive events:** Choose one of the following:
 - **Event Management:** When setting up Cisco DNA Center integration with ServiceNow without using the Cisco DNA app, choose 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 DNA app. With this option, data is sent to a REST API endpoint within the Cisco DNA app.

- **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 Cisco DNA Center platform and ITSM integration lets you choose 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. The **Events Settings** window is accessible from the **Configurations** menu option in the Cisco DNA Center platform.

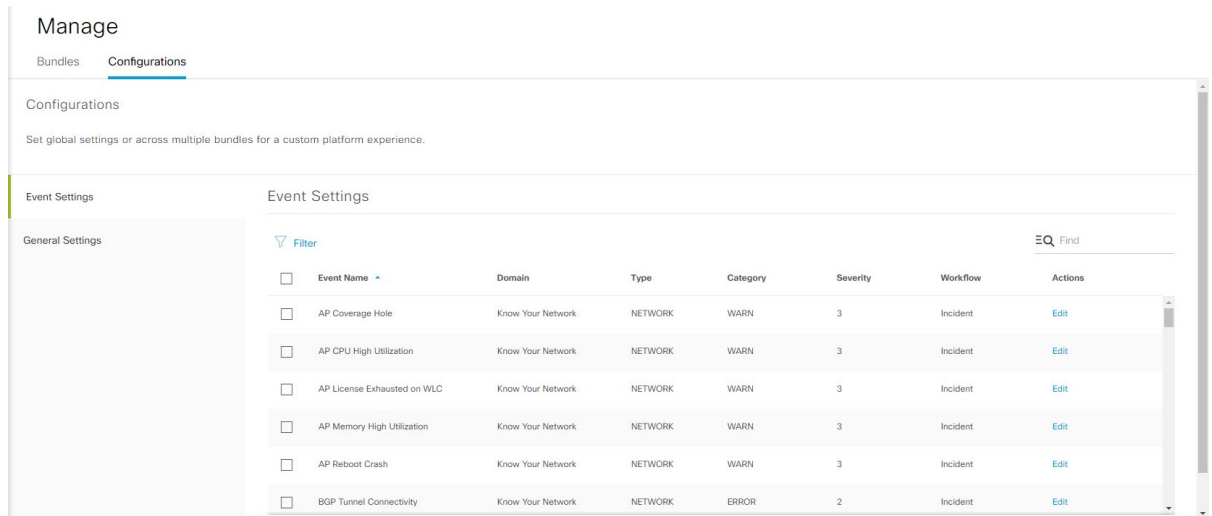


Note For this release, there are no SWIM event to configure in **Event Settings**, you only configure network assurance events.



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 18: Events Settings Window



Before you begin

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

Step 1 From the top-left corner, click the menu icon and choose **Platform > Manage > Configurations**.

A **Configurations** window opens that contains an **Events Settings** section.

Step 2 Review the **Event Settings** section that appears.

The following **Event Settings** information is displayed:

- **Event Name:** Name of the Cisco DNA Center event.
- **Domain:** Domain of the Cisco DNA 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.

Choose 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 Cisco DNA Center when the event occurs in the future.

Step 5 Click **Save**.

Configure the Cisco DNA Center Automation Events for ITSM (ServiceNow) Bundle

Perform 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.

Enabling ITSM in Cisco DNA Center enforces a ServiceNow approval process for better control of Cisco DNA Center software image updates and other device provisioning activities. For example, see [SWIM Closed Loop Automation Workflow, on page 54](#) for information about the approval process in ServiceNow.

See the Configure System Settings chapter in the [Cisco DNA Center Administrator Guide](#) for information about enabling ITSM approval for device configuration changes.



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 DNA app.
 - The Event Management and Generic REST API Endpoint options do not support automatic ticket creation, approval/rejection workflow and auto resolution of tickets for closed loop integration.
-

Before you begin

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

Step 1 From the top-left corner, click the menu icon and choose **Platform > Manage > Bundles**.

Review the displayed bundles and their status.

Step 2 Click the **Cisco DNA Center 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 the following:

- **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 the **Enable** button to enable the bundle.

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

Step 5 Click the **Enable** button in the **Information** field 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 19: 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

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

Step 10 For configuring a new ServiceNow Connection instance, you must enter the following 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 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, activate the bundle.

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

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

Figure 20: 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

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

Step 14 For configuring a new Destination instance, you must enter the following additional information:

- **Instance Name:** Name of the instance.

- **Description:** Descriptive text of the instance.
- **Destination to receive events:** Choose one of the following:
 - **Event Management:** When setting up Cisco DNA Center integration with ServiceNow without using the Cisco DNA app, choose 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 DNA app. Data is sent to a REST API endpoint within the Cisco DNA 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 15 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. Additionally, 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 Cisco DNA Center devices and the ServiceNow CMDB system.

Before you begin

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

- Run a successful **Discovery** job in Cisco DNA Center. You can check whether a **Discovery** job is successful in **Device Inventory**. From the top-left corner, click the menu icon and 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 Cisco DNA Center platform, see the [Cisco DNA Center Platform User Guide](#).

Step 1 From the top-left corner, click the menu icon and choose **Platform > Manage > Bundles**.

Review the displayed bundles and their status.

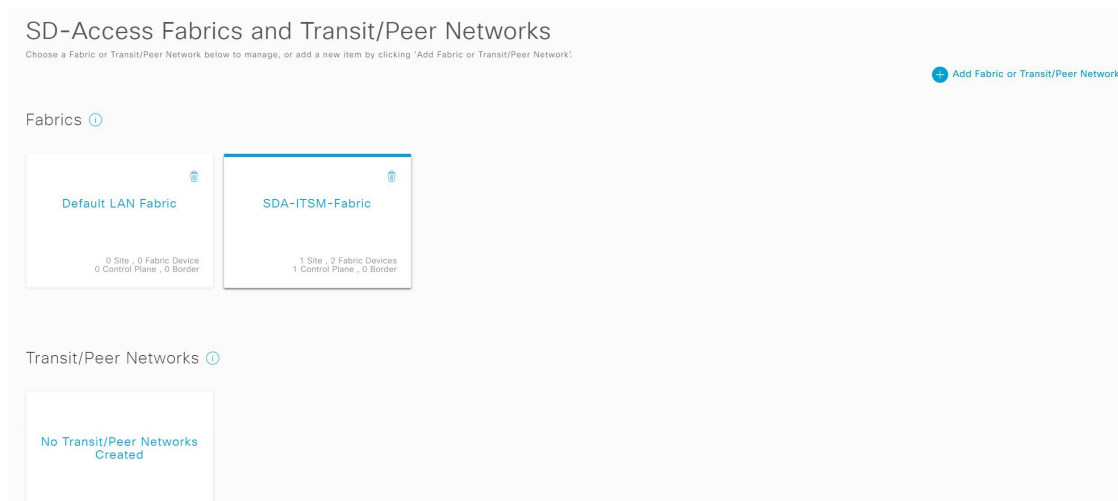
Step 2 Enable and configure the **Basic ITSM (ServiceNow) CMDB Synchronization** bundle to configure data synchronization. For more information, see [Configure the Basic ITSM \(ServiceNow\) CMDB Synchronization Bundle](#).

- Step 3** Enable and configure the **Cisco DNAC Automation events for ITSM (ServiceNow)** bundle to monitor and publish a fabric event. For more information, see [Configure the Cisco DNA Center 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 top-left corner, click the menu icon and choose **System > Settings > External Services**.
- Step 5** In the left pane, click **Destination** and choose **ITSM** to add or edit a ServiceNow instance. For more information, see **Configure ITSM Integration** in the [Cisco DNA 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 top-left corner, click the menu icon and choose **Provision > Fabric**.

The window displays all the provisioned fabric domains.

- Step 7** From the list of fabric domains, choose **SDA-ITSM-Fabric**.

Figure 21: Cisco DNA Center Platform Fabrics



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

- Step 8** Choose 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 22: List of Devices in Fabric Infrastructure

The screenshot shows the Cisco DNA Center interface for managing Fabric Infrastructure. The main content area displays a table of devices with the following columns: Device Name, IP Address, Device Family, Device Reachability, Device Role, Readiness Status, and Provision Status. The table lists four devices, all of which are 'Switches and Hubs' and 'Reachable'. The 'Readiness Status' for the three devices with IP addresses is 'Not Applicable', and for the device without an IP address, it is 'Failed'. The 'Provision Status' for all devices is 'Success'.

| Device Name | IP Address | Device Family | Device Reachability | Device Role | Readiness Status | Provision Status |
|----------------------|------------|-------------------|---------------------|-------------|------------------|------------------|
| sda-9k-141 | | Switches and Hubs | Reachable | --- | Failed | Success |
| sda-9k-142.cisco.com | | Switches and Hubs | Reachable | C | Not Applicable | Success |
| sda-9k-143.cisco.com | | Switches and Hubs | Reachable | E | Not Applicable | Success |
| sda-9k-144.cisco.com | | Switches and Hubs | Reachable | --- | Failed | Success |

Showing 4 of 4

Buttons: Cancel, Deploy

Step 9

In the list view, click a device. The device details window slides in with the following **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, choose the **Control Plane**, **Border**, and **Edge** options.
- To configure the device as a control plane and a border node, choose both **Control Plane** and **Border**.

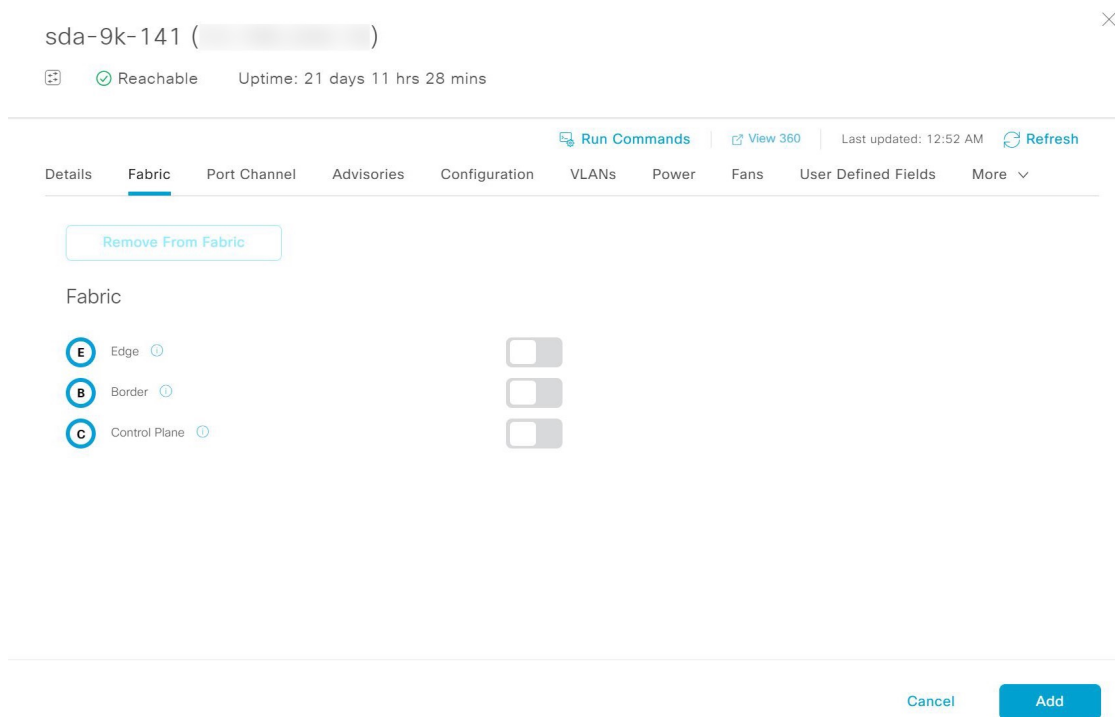
Step 10

Click **Add**.

Step 11

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

Figure 23: 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 choose **Later** to schedule a ticket creation at a specific time, the request goes to the Cisco DNA Center scheduler.

Step 15 From the top-left corner, click the menu icon and choose **Activity > Tasks** to view upcoming, in progress, success, and failed fabric tasks.

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

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

Figure 24: Status of Fabric Ticket Requests

| Task ID | Type | Task Name | Starts | Status | Additional Info |
|---------|-----------|-------------------------------------|-----------------------|-----------------|-----------------|
| 1 | PROVISION | Modifying Fabric at sjc23 | Dec 22, 2020 12:32 AM | Ticket Pending | |
| 2 | PROVISION | Modifying Fabric at sjc23 Remove CP | Dec 22, 2020 12:28 AM | Ticket Pending | Failed |
| 3 | PROVISION | Modifying Fabric at sjc23 remove cp | Dec 22, 2020 12:15 AM | Ticket Rejected | Failed |
| 4 | PROVISION | Modifying Fabric at sjc23 | Dec 21, 2020 11:44 PM | Success | |
| 5 | DISCOVERY | sda-itsm-discovery-2 | Dec 21, 2020 11:36 PM | 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 DNA Center Platform User Guide](#).

Cisco DNA Center Endpoint Attribute Retrieval with ServiceNow

With this Cisco DNA Center release, you can configure Cisco DNA Center endpoint attribute retrieval with ServiceNow using the Cisco DNA app (**version 2.1.1**) 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.

The following table describes the procedure for configuring Cisco DNA Center endpoint attribute retrieval with ServiceNow.



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

Table 6: Cisco DNA Center Endpoint Attribute Retrieval with ServiceNow

| Step | Description |
|--------|--|
| Step 1 | <p>Install or upgrade to the latest Cisco DNA Center release.</p> <p>For information about installing Cisco DNA Center, see the Cisco DNA Center Installation Guide.</p> |
| Step 2 | <p>Install or upgrade to a compatible version of ServiceNow mentioned on the ServiceNow Store website.</p> <p>Click the following link to access the ServiceNow Store website:</p> <p>https://store.servicenow.com/sn_appstore_store.do#!/store/application/03eb0f4ddb6ba00f27978b5ae96197b/2.1.1</p> <p>Refer to your ServiceNow documentation for its installation and upgrade procedures.</p> <p>Note This procedure must be performed by a ServiceNow administrator.</p> |
| Step 3 | <p>Download and install the Cisco DNA app (version 2.1.1) into ServiceNow by following the documentation available at the ServiceNow website.</p> <p>Note Cisco DNA Center supports an application (Cisco DNA) 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 DNA app is located:</p> <p>https://store.servicenow.com/sn_appstore_store.do#!/store/application/03eb0f4ddb6ba00f27978b5ae96197b/2.1.1</p> <p>Note This procedure must be performed by a ServiceNow administrator. The Cisco DNA 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 DNA app to the latest version, 2.2.0.</p> |
| Step 4 | <p>Review and ensure that the requirements are met for the Cisco DNA Center-to-ServiceNow integration.</p> <p>For information, see Requirements, on page 21.</p> |
| Step 5 | <p>Configure the Endpoint Attribute Retrieval with ITSM (ServiceNow) bundle.</p> <p>For information, see Configure the Endpoint Attribute Retrieval Bundle with ITSM (ServiceNow), on page 46.</p> |

Requirements

Review and ensure that the following networking and systems requirements are met for the Cisco DNA Center-to-ServiceNow integration:

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



Note Contact your Cisco DNA Center administrator to obtain this information.

- HTTPS network access between Cisco DNA 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 Cisco DNA Center platform is accessible from the MID server.
 - The Cisco DNA 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

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



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

Configure the Endpoint Attribute Retrieval Bundle with ITSM (ServiceNow)

Perform this procedure to configure Cisco DNA 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 Cisco DNA 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 Cisco DNA Center platform, see the *Cisco DNA Center Platform User Guide*.

- Ensure that you have installed or upgraded the latest Cisco DNA 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 ISE. For more information, see **Publish Authorization Attributes to Cisco ISE** in the [Cisco DNA Center User Guide](#).

Step 1 From the top-left corner, click the menu icon and 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 the following:

- **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. The following endpoint attribute data will be retrieved from ServiceNow (with the display name in Cisco DNA 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 perform the following tasks.

For the schedule-based integration flow (**Scheduler for ServiceNow Asset Sync**), perform the following 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 the following 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 25: 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 26: 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

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

Step 14 For configuring a new ServiceNow Connection instance, the following 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 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 the following:

- a. Click the Create a new instance radio button and do the following to configure a new ServiceNow connection instance:
 1. In the **INFORMATION** area enter the instance name and description.

2. 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 record to pull in each cycle.

It is recommended to use the **Incremental Sync** that allows you to first retrieve all the data from the service now 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 performed 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 53](#)
- [SWIM Closed Loop Automation Requirements, on page 54](#)
- [SWIM Closed Loop Automation Workflow, on page 54](#)

About SWIM Closed Loop Automation

This release supports closed loop automation for software image management (SWIM) between Cisco DNA Center and ServiceNow. Closed-loop automation consists of a user configuring the provisioning of software device images in Cisco DNA Center. This configuration information is then communicated directly from Cisco DNA 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 Cisco DNA Center.

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

After Cisco DNA Center successfully performs 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 perform the software update in Cisco DNA Center.



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

Ensure that the Cisco DNA app (version 2.2.0) is installed within the ServiceNow instance and perform the following procedures to enable SWIM closed loop automation between Cisco DNA 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 54](#).
2. Review the SWIM closed loop automation workflow to ensure that the required Cisco DNA Center admin and ServiceNow admin tasks are performed for this feature. See [SWIM Closed Loop Automation Workflow, on page 54](#).

SWIM Closed Loop Automation Requirements

The following table lists the requirements for SWIM closed loop automation.

Table 7: SWIM Closed Loop Automation Requirements

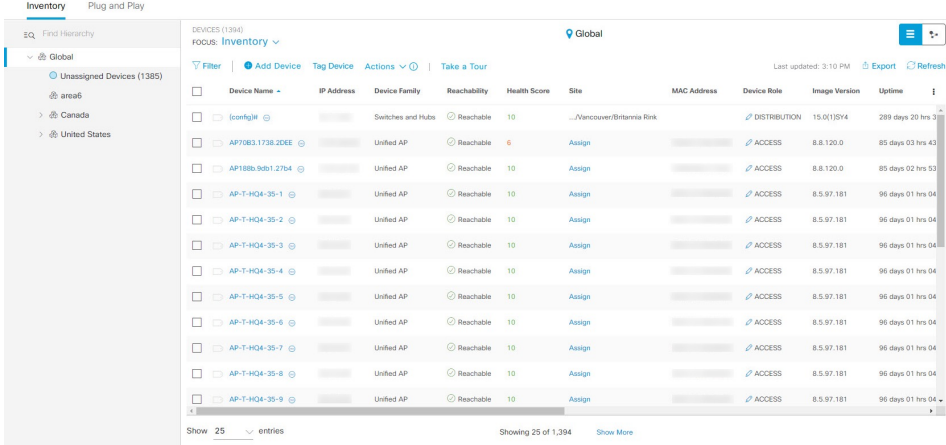
| Software Product, App, or Procedure | Requirement |
|---|---|
| Cisco DNA Center | The latest Cisco DNA Center release. |
| Service Now | Any compatible version of ServiceNow mentioned on the ServiceNow Store website. Click the following link to access the ServiceNow Store website: https://store.servicenow.com/sn_appstore_store.do#!/store/application/03eb0f4ddb6ba00f27978b5ae96197b/2.2.0 |
| Cisco DNA Center app | Cisco DNA app (version 2.2.0) This app is available through the ServiceNow website located at: https://store.servicenow.com/sn_appstore_store.do#!/store/application/03eb0f4ddb6ba00f27978b5ae96197b/2.2.0 The Cisco DNA app must be installed in your ServiceNow instance by a ServiceNow administrator. The Cisco DNA 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 DNA app to the latest version, 2.2.0. |
| Cisco DNA Center-to-ServiceNow ITSM integration | See Cisco DNA Center Integration with ServiceNow Using the Cisco DNA App , on page 19. |

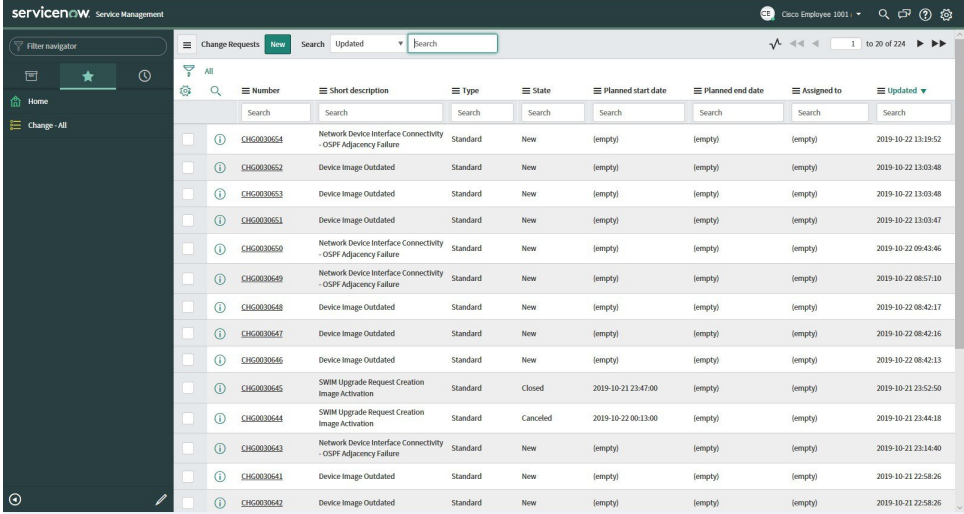
SWIM Closed Loop Automation Workflow

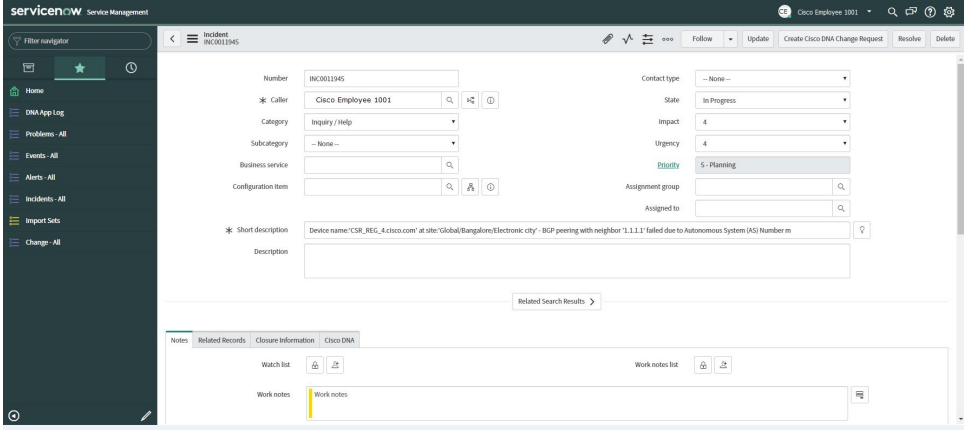
The following table describes the SWIM closed loop automation workflow between Cisco DNA Center and ServiceNow.

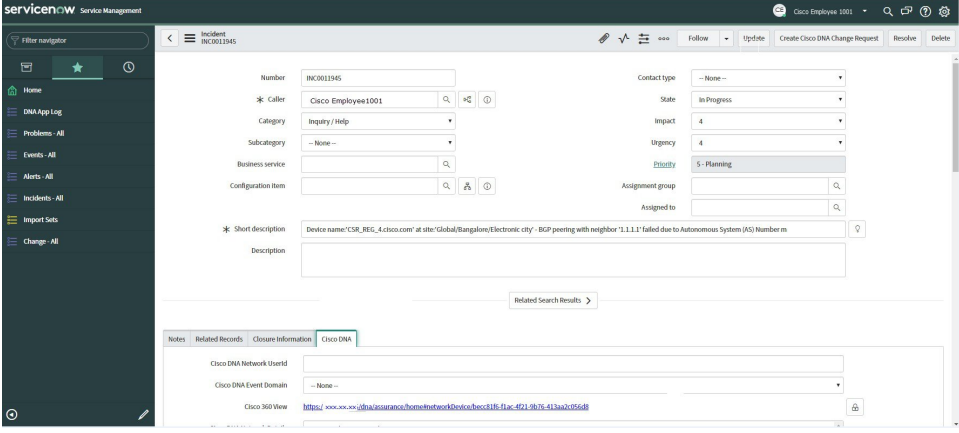
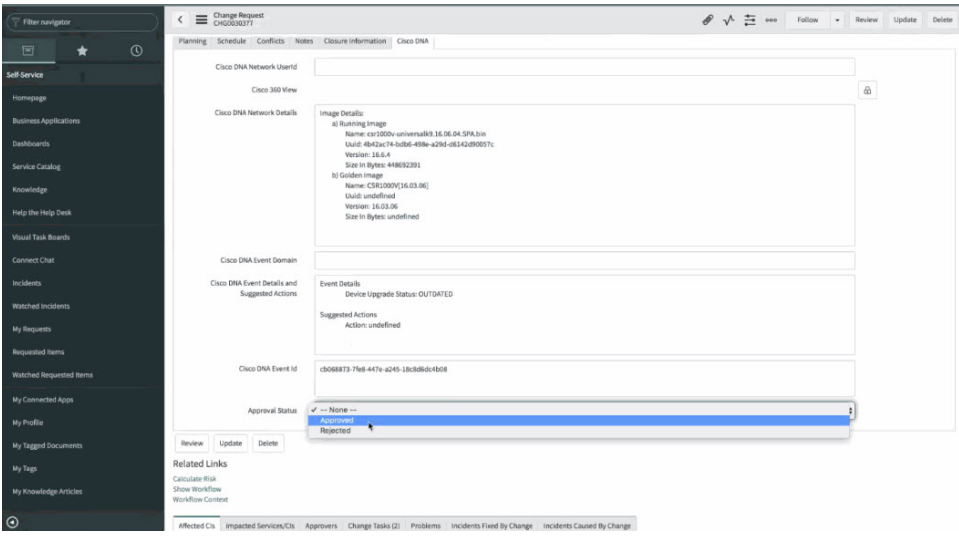
Table 8: SWIM Closed Loop Automation Workflow

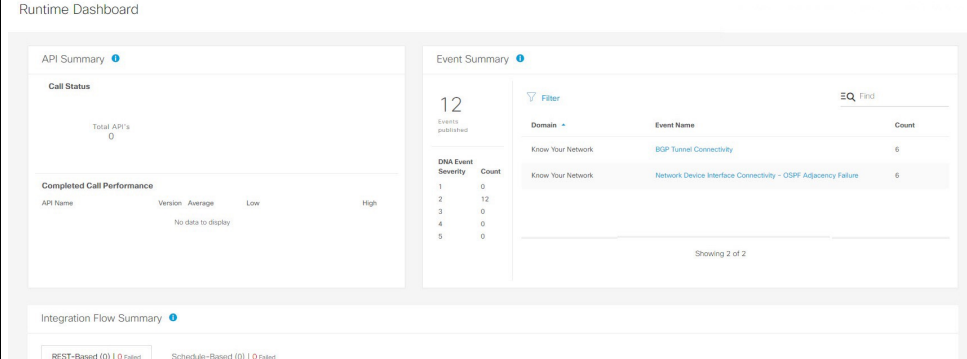
| Step | Description |
|--------|---|
| Step 1 | The Cisco DNA Center admin configures the Image Repository to prepare for the provisioning of devices in the network. Note See the Manage Software Images chapter in the Cisco DNA Center User Guide for information about setting up the Image Repository, as well as to review the software image provisioning process. |

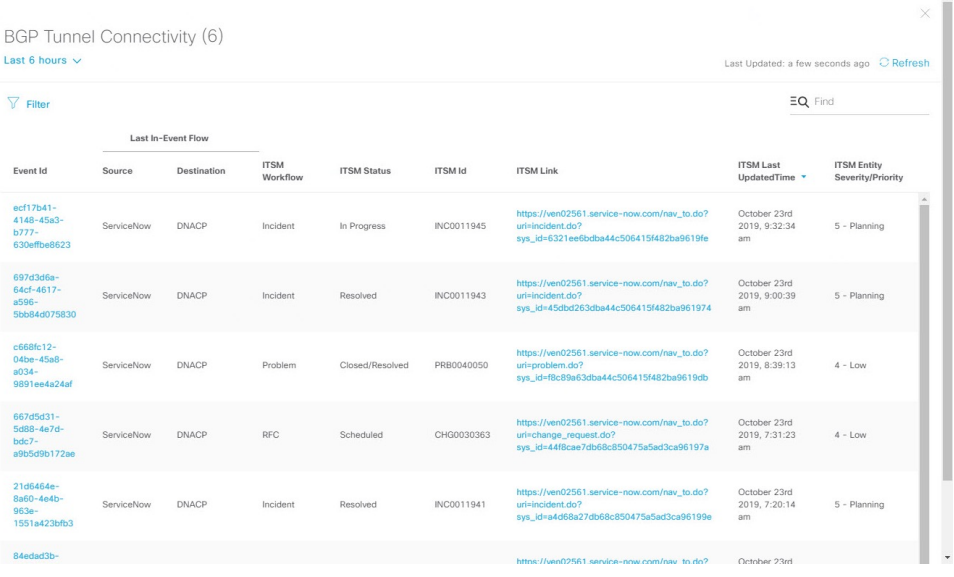
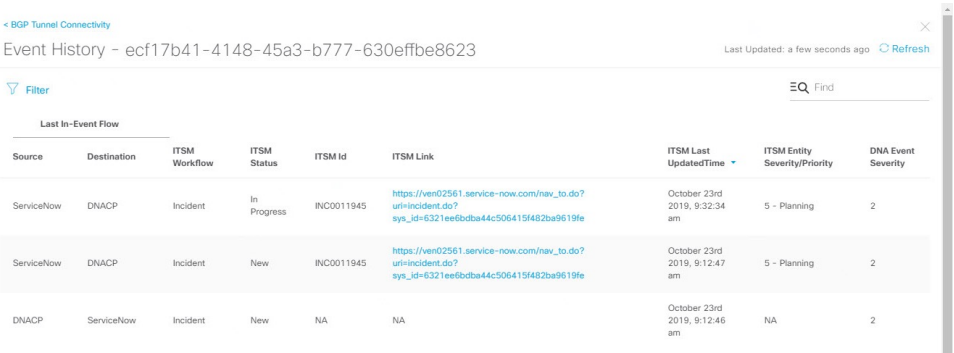
| Step | Description |
|--------|---|
| Step 2 | <p>The Cisco DNA Center admin distributes the software image to a device or devices at the present time or schedules this activity for a later time.</p> <p>Note Before this step is done, ensure that the Cisco DNA Center Automation events for ITSM (ServiceNow) bundle is configured and activated.</p> <ul style="list-style-type: none"> • From the Cisco DNA Center home page, the admin clicks Provision > Inventory. • From the Focus drop-down list, the admin chooses Software Images and selects the device with the image to upgrade. • From the Actions drop-down list, the admin chooses Software Images > Update Image and does the following: <ul style="list-style-type: none"> • Distribute: Clicks Now to start the distribution immediately or clicks Later to schedule the distribution at a specific time. • Clicks Next. • Activate: Clicks Now to start the activation immediately or clicks Later to schedule the activation at a specific time. • Confirm: Clicks Confirm to confirm the update. <p>Figure 27: Cisco DNA Assurance Provision</p>  <p>Note See the Manage Software Images chapter in the <i>Cisco DNA Center User Guide</i> for detailed information about this step.</p> |

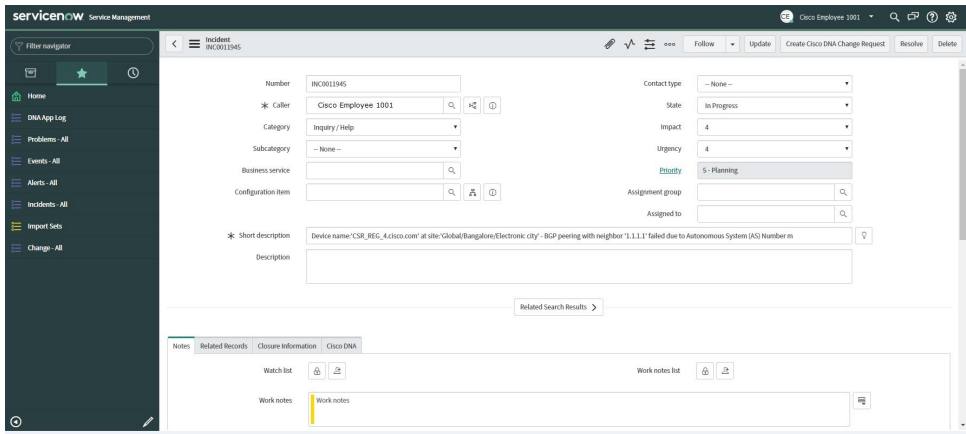
| Step | Description | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|------------|---|----------|-------------------|---------------------|------------------|--------------------|---------------------|-------------|---------|------------|--|----------|-----|---------|---------|---------|---------------------|------------|-----------------------|----------|-----|---------|---------|---------|---------------------|------------|-----------------------|----------|-----|---------|---------|---------|---------------------|------------|-----------------------|----------|-----|---------|---------|---------|---------------------|------------|--|----------|-----|---------|---------|---------|---------------------|------------|--|----------|-----|---------|---------|---------|---------------------|------------|-----------------------|----------|-----|---------|---------|---------|---------------------|------------|-----------------------|----------|-----|---------|---------|---------|---------------------|------------|-----------------------|----------|-----|---------|---------|---------|---------------------|------------|--|----------|--------|---------------------|---------|---------|---------------------|------------|--|----------|----------|---------------------|---------|---------|---------------------|------------|--|----------|-----|---------|---------|---------|---------------------|------------|-----------------------|----------|-----|---------|---------|---------|---------------------|------------|-----------------------|----------|-----|---------|---------|---------|---------------------|
| Step 3 | <p>After a software image distribution is created in Cisco DNA 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 DNA app. The change request ticket status is new.</p> <p>The SWIM event appears in the ServiceNow GUI in the ServiceNow Change Requests table.</p> <p>Figure 28: ServiceNow Change Requests</p>  <table border="1" data-bbox="380 531 1338 1041"> <thead> <tr> <th>Number</th> <th>Short description</th> <th>Type</th> <th>State</th> <th>Planned start date</th> <th>Planned end date</th> <th>Assigned to</th> <th>Updated</th> </tr> </thead> <tbody> <tr> <td>CHG0030654</td> <td>Network Device Interface Connectivity - OSPF Adjacency Failure</td> <td>Standard</td> <td>New</td> <td>(empty)</td> <td>(empty)</td> <td>(empty)</td> <td>2019-10-22 13:19:52</td> </tr> <tr> <td>CHG0030652</td> <td>Device Image Outdated</td> <td>Standard</td> <td>New</td> <td>(empty)</td> <td>(empty)</td> <td>(empty)</td> <td>2019-10-22 13:03:48</td> </tr> <tr> <td>CHG0030653</td> <td>Device Image Outdated</td> <td>Standard</td> <td>New</td> <td>(empty)</td> <td>(empty)</td> <td>(empty)</td> <td>2019-10-22 13:03:48</td> </tr> <tr> <td>CHG0030651</td> <td>Device Image Outdated</td> <td>Standard</td> <td>New</td> <td>(empty)</td> <td>(empty)</td> <td>(empty)</td> <td>2019-10-22 13:03:47</td> </tr> <tr> <td>CHG0030650</td> <td>Network Device Interface Connectivity - OSPF Adjacency Failure</td> <td>Standard</td> <td>New</td> <td>(empty)</td> <td>(empty)</td> <td>(empty)</td> <td>2019-10-22 09:43:46</td> </tr> <tr> <td>CHG0030649</td> <td>Network Device Interface Connectivity - OSPF Adjacency Failure</td> <td>Standard</td> <td>New</td> <td>(empty)</td> <td>(empty)</td> <td>(empty)</td> <td>2019-10-22 08:57:10</td> </tr> <tr> <td>CHG0030648</td> <td>Device Image Outdated</td> <td>Standard</td> <td>New</td> <td>(empty)</td> <td>(empty)</td> <td>(empty)</td> <td>2019-10-22 08:42:17</td> </tr> <tr> <td>CHG0030647</td> <td>Device Image Outdated</td> <td>Standard</td> <td>New</td> <td>(empty)</td> <td>(empty)</td> <td>(empty)</td> <td>2019-10-22 08:42:16</td> </tr> <tr> <td>CHG0030646</td> <td>Device Image Outdated</td> <td>Standard</td> <td>New</td> <td>(empty)</td> <td>(empty)</td> <td>(empty)</td> <td>2019-10-22 08:42:13</td> </tr> <tr> <td>CHG0030645</td> <td>SWIM Upgrade Request Creation Image Activation</td> <td>Standard</td> <td>Closed</td> <td>2019-10-21 23:47:00</td> <td>(empty)</td> <td>(empty)</td> <td>2019-10-21 23:52:50</td> </tr> <tr> <td>CHG0030644</td> <td>SWIM Upgrade Request Creation Image Activation</td> <td>Standard</td> <td>Canceled</td> <td>2019-10-22 00:13:00</td> <td>(empty)</td> <td>(empty)</td> <td>2019-10-21 23:44:18</td> </tr> <tr> <td>CHG0030643</td> <td>Network Device Interface Connectivity - OSPF Adjacency Failure</td> <td>Standard</td> <td>New</td> <td>(empty)</td> <td>(empty)</td> <td>(empty)</td> <td>2019-10-21 23:14:40</td> </tr> <tr> <td>CHG0030641</td> <td>Device Image Outdated</td> <td>Standard</td> <td>New</td> <td>(empty)</td> <td>(empty)</td> <td>(empty)</td> <td>2019-10-21 22:58:26</td> </tr> <tr> <td>CHG0030642</td> <td>Device Image Outdated</td> <td>Standard</td> <td>New</td> <td>(empty)</td> <td>(empty)</td> <td>(empty)</td> <td>2019-10-21 22:58:26</td> </tr> </tbody> </table> | Number | Short description | Type | State | Planned start date | Planned end date | Assigned to | Updated | CHG0030654 | Network Device Interface Connectivity - OSPF Adjacency Failure | Standard | New | (empty) | (empty) | (empty) | 2019-10-22 13:19:52 | CHG0030652 | Device Image Outdated | Standard | New | (empty) | (empty) | (empty) | 2019-10-22 13:03:48 | CHG0030653 | Device Image Outdated | Standard | New | (empty) | (empty) | (empty) | 2019-10-22 13:03:48 | CHG0030651 | Device Image Outdated | Standard | New | (empty) | (empty) | (empty) | 2019-10-22 13:03:47 | CHG0030650 | Network Device Interface Connectivity - OSPF Adjacency Failure | Standard | New | (empty) | (empty) | (empty) | 2019-10-22 09:43:46 | CHG0030649 | Network Device Interface Connectivity - OSPF Adjacency Failure | Standard | New | (empty) | (empty) | (empty) | 2019-10-22 08:57:10 | CHG0030648 | Device Image Outdated | Standard | New | (empty) | (empty) | (empty) | 2019-10-22 08:42:17 | CHG0030647 | Device Image Outdated | Standard | New | (empty) | (empty) | (empty) | 2019-10-22 08:42:16 | CHG0030646 | Device Image Outdated | Standard | New | (empty) | (empty) | (empty) | 2019-10-22 08:42:13 | CHG0030645 | SWIM Upgrade Request Creation Image Activation | Standard | Closed | 2019-10-21 23:47:00 | (empty) | (empty) | 2019-10-21 23:52:50 | CHG0030644 | SWIM Upgrade Request Creation Image Activation | Standard | Canceled | 2019-10-22 00:13:00 | (empty) | (empty) | 2019-10-21 23:44:18 | CHG0030643 | Network Device Interface Connectivity - OSPF Adjacency Failure | Standard | New | (empty) | (empty) | (empty) | 2019-10-21 23:14:40 | CHG0030641 | Device Image Outdated | Standard | New | (empty) | (empty) | (empty) | 2019-10-21 22:58:26 | CHG0030642 | Device Image Outdated | Standard | New | (empty) | (empty) | (empty) | 2019-10-21 22:58:26 |
| Number | Short description | Type | State | Planned start date | Planned end date | Assigned to | Updated | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CHG0030654 | Network Device Interface Connectivity - OSPF Adjacency Failure | Standard | New | (empty) | (empty) | (empty) | 2019-10-22 13:19:52 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CHG0030652 | Device Image Outdated | Standard | New | (empty) | (empty) | (empty) | 2019-10-22 13:03:48 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CHG0030653 | Device Image Outdated | Standard | New | (empty) | (empty) | (empty) | 2019-10-22 13:03:48 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CHG0030651 | Device Image Outdated | Standard | New | (empty) | (empty) | (empty) | 2019-10-22 13:03:47 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CHG0030650 | Network Device Interface Connectivity - OSPF Adjacency Failure | Standard | New | (empty) | (empty) | (empty) | 2019-10-22 09:43:46 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CHG0030649 | Network Device Interface Connectivity - OSPF Adjacency Failure | Standard | New | (empty) | (empty) | (empty) | 2019-10-22 08:57:10 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CHG0030648 | Device Image Outdated | Standard | New | (empty) | (empty) | (empty) | 2019-10-22 08:42:17 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CHG0030647 | Device Image Outdated | Standard | New | (empty) | (empty) | (empty) | 2019-10-22 08:42:16 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CHG0030646 | Device Image Outdated | Standard | New | (empty) | (empty) | (empty) | 2019-10-22 08:42:13 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CHG0030645 | SWIM Upgrade Request Creation Image Activation | Standard | Closed | 2019-10-21 23:47:00 | (empty) | (empty) | 2019-10-21 23:52:50 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CHG0030644 | SWIM Upgrade Request Creation Image Activation | Standard | Canceled | 2019-10-22 00:13:00 | (empty) | (empty) | 2019-10-21 23:44:18 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CHG0030643 | Network Device Interface Connectivity - OSPF Adjacency Failure | Standard | New | (empty) | (empty) | (empty) | 2019-10-21 23:14:40 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CHG0030641 | Device Image Outdated | Standard | New | (empty) | (empty) | (empty) | 2019-10-21 22:58:26 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CHG0030642 | Device Image Outdated | Standard | New | (empty) | (empty) | (empty) | 2019-10-21 22:58:26 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| | |
|--------|--|
| Step 4 | <p>In the Change Requests 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 State from 'New' to 'Scheduled' and enter 'Change Management' for the Assignment group. The ServiceNow admin can also identify the SWIM change request with information in the Short Description field.</p> <p>Figure 29: Change Request</p>  <p>Number: INC001945</p> <p>Caller: Cisco Employee 1001</p> <p>Category: Inquiry / Help</p> <p>Subcategory: --None--</p> <p>Business service: [empty]</p> <p>Configuration item: [empty]</p> <p>Short description: Device name: CSR_REC_4cisco.com at site: Global/Bangalore/Electronic city - BGP peering with neighbor 1.1.1.1 failed due to Autonomous System (AS) Number m</p> <p>State: In Progress</p> <p>Impact: 4</p> <p>Urgency: 4</p> <p>Priority: S - Planning</p> <p>Assignment group: [empty]</p> <p>Assigned to: [empty]</p> |
|--------|--|

| Step | Description |
|---------------|---|
| <p>Step 5</p> | <p>The ServiceNow admin now clicks the Cisco DNA tab in the change request. Important additional data synchronized from Cisco DNA Center to ServiceNow can be viewed in this tab.</p> <p>Figure 30: Cisco DNA Tab</p>  |
| <p>Step 6</p> | <p>The ServiceNow admin now either approves or rejects the change request ticket in the ServiceNow GUI. In the Cisco DNA tab, the ServiceNow admin clicks the Approval Status field and clicks either Approved to approve the request or Rejected to reject the request.</p> <p>Note 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 Cisco DNA Center.</p> <p>Figure 31: Cisco DNA Approval Status Field</p>  |
| <p>Step 7</p> | <p>After the ServiceNow admin approves the ticket and the status of the change request is changed to Implement, a notification is sent to Cisco DNA Center. In case the ticket is rejected, the update is sent to Cisco DNA Center in Scheduled state itself and the ServiceNow ticket is automatically canceled.</p> |

| Step | Description | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--------------------|--|----------|---------|---------|-----|------|--------------------|--|--|--|--|--------|------------|-------|-------------------|-------------------------|---|-------------------|--|---|----------|-------|---|---|---|----|---|---|---|---|---|---|
| Step 8 | <p>After a successful software image update in Cisco DNA 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 DNA app.</p> <p>Note 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 DNA app.</p> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Step 9 | <p>The Cisco DNA Center admin can review the SWIM event by choosing Runtime Dashboard > Event Summary.</p> <p>Note 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>Figure 32: Event Summary</p>  <p>Runtime Dashboard</p> <p>API Summary</p> <p>Call Status</p> <p>Total API's 0</p> <p>Completed Call Performance</p> <table border="1"> <thead> <tr> <th>API Name</th> <th>Version</th> <th>Average</th> <th>Low</th> <th>High</th> </tr> </thead> <tbody> <tr> <td colspan="5">No data to display</td> </tr> </tbody> </table> <p>Event Summary</p> <p>12 Events published</p> <table border="1"> <thead> <tr> <th>Domain</th> <th>Event Name</th> <th>Count</th> </tr> </thead> <tbody> <tr> <td>Know Your Network</td> <td>BGP Tunnel Connectivity</td> <td>6</td> </tr> <tr> <td>Know Your Network</td> <td>Network Device Interface Connectivity - OSPF Adjacency Failure</td> <td>6</td> </tr> </tbody> </table> <p>DNA Event Severity</p> <table border="1"> <thead> <tr> <th>Severity</th> <th>Count</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>0</td> </tr> <tr> <td>2</td> <td>12</td> </tr> <tr> <td>3</td> <td>0</td> </tr> <tr> <td>4</td> <td>0</td> </tr> <tr> <td>5</td> <td>0</td> </tr> </tbody> </table> <p>Showing 2 of 2</p> <p>Integration Flow Summary</p> <p>REST-Based (0) 0 failed Schedule-Based (0) 0 failed</p> | API Name | Version | Average | Low | High | No data to display | | | | | Domain | Event Name | Count | Know Your Network | BGP Tunnel Connectivity | 6 | Know Your Network | Network Device Interface Connectivity - OSPF Adjacency Failure | 6 | Severity | Count | 1 | 0 | 2 | 12 | 3 | 0 | 4 | 0 | 5 | 0 |
| API Name | Version | Average | Low | High | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| No data to display | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Domain | Event Name | Count | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Know Your Network | BGP Tunnel Connectivity | 6 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Know Your Network | Network Device Interface Connectivity - OSPF Adjacency Failure | 6 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Severity | Count | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | 12 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5 | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| Step | Description | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|--|--------------------|---------------|-----------------|---|---|-------------------------------|-------------------------------|--|----------|-------------|---------------|---------------|-------------|-----------|-----------------------|-------------------------------|-------------------------------|--|------------|----------|-------------|-------------|---|---|-------------------------------|--------------|--|------------|----------|----------|------------|---|---|-------------------------------|--------------|---|------------|----------|---------|-----------------|------------|---|-------------------------------|---------|--|------------|-------|-----|-----------|------------|---|-------------------------------|---------|--|------------|-------|----------|----------|------------|---|-------------------------------|--------------|---------------------------|--|--|--|--|--|---|--------------|--|
| <p>Step 10</p> | <p>The Cisco DNA Center admin clicks an event name (link) to view additional detailed data.</p> <p>Figure 33: Event History</p>  <p>BGP Tunnel Connectivity (6) Last Updated: a few seconds ago Refresh</p> <p>Filter EQ Find</p> <table border="1"> <thead> <tr> <th colspan="8">Last In-Event Flow</th> </tr> <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-a59e-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>c568e12-04be-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=fbc9ae3dba44c506415f482ba9619db</td> <td>October 23rd 2019, 8:39:13 am</td> <td>4 - Low</td> </tr> <tr> <td>667d5d31-5d89-4e7d-bdc7-a9e5d9b172ae</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=44fbc8e7db68c850475a5ad3ca96197a</td> <td>October 23rd 2019, 7:31:23 am</td> <td>4 - Low</td> </tr> <tr> <td>21d6464e-8a60-4e4b-963e-1551a423bfb3</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=e4d68a27db68c850475a5ad3ca96199e</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?</td> <td>October 23rd</td> <td></td> </tr> </tbody> </table> | Last In-Event Flow | | | | | | | | 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-a59e-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 | c568e12-04be-45a8-a034-9891ee4a24af | ServiceNow | DNACP | Problem | Closed/Resolved | PRB0040050 | https://ven02561.service-now.com/nav_to.do?uri=problem.do?sys_id=fbc9ae3dba44c506415f482ba9619db | October 23rd 2019, 8:39:13 am | 4 - Low | 667d5d31-5d89-4e7d-bdc7-a9e5d9b172ae | ServiceNow | DNACP | RFC | Scheduled | CHG0030363 | https://ven02561.service-now.com/nav_to.do?uri=change_request.do?sys_id=44fbc8e7db68c850475a5ad3ca96197a | October 23rd 2019, 7:31:23 am | 4 - Low | 21d6464e-8a60-4e4b-963e-1551a423bfb3 | ServiceNow | DNACP | Incident | Resolved | INC0011941 | https://ven02561.service-now.com/nav_to.do?uri=incident.do?sys_id=e4d68a27db68c850475a5ad3ca96199e | October 23rd 2019, 7:20:14 am | 5 - Planning | 84edad3b- | | | | | | https://ven02561.service-now.com/nav_to.do? | October 23rd | |
| Last In-Event Flow | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 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-a59e-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 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| c568e12-04be-45a8-a034-9891ee4a24af | ServiceNow | DNACP | Problem | Closed/Resolved | PRB0040050 | https://ven02561.service-now.com/nav_to.do?uri=problem.do?sys_id=fbc9ae3dba44c506415f482ba9619db | October 23rd 2019, 8:39:13 am | 4 - Low | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 667d5d31-5d89-4e7d-bdc7-a9e5d9b172ae | ServiceNow | DNACP | RFC | Scheduled | CHG0030363 | https://ven02561.service-now.com/nav_to.do?uri=change_request.do?sys_id=44fbc8e7db68c850475a5ad3ca96197a | October 23rd 2019, 7:31:23 am | 4 - Low | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 21d6464e-8a60-4e4b-963e-1551a423bfb3 | ServiceNow | DNACP | Incident | Resolved | INC0011941 | https://ven02561.service-now.com/nav_to.do?uri=incident.do?sys_id=e4d68a27db68c850475a5ad3ca96199e | October 23rd 2019, 7:20:14 am | 5 - Planning | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 84edad3b- | | | | | | https://ven02561.service-now.com/nav_to.do? | October 23rd | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <p>Step 11</p> | <p>The Cisco DNA Center admin clicks an event ID number (link) to view only data associated with that specific event.</p> <p>Figure 34: Event ID Data</p>  <p>< BGP Tunnel Connectivity Event History - ecf17b41-4148-45a3-b777-630effbe8623 Last Updated: a few seconds ago Refresh</p> <p>Filter EQ Find</p> <table border="1"> <thead> <tr> <th colspan="8">Last In-Event Flow</th> </tr> <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> | Last In-Event Flow | | | | | | | | 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 | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Last In-Event Flow | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 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 Cisco DNA Center admin clicks the ITSM Link to return to the ServiceNow Service Management GUI and specific incident.</p> <p>Figure 35: ServiceNow Incident</p>  |



CHAPTER 5

Cisco DNA Center-to-PagerDuty Integration

- [About Cisco DNA Center-to-PagerDuty Integration, on page 61](#)
- [Subscribe Cisco DNA Center Event Notifications to PagerDuty, on page 63](#)

About Cisco DNA Center-to-PagerDuty Integration

You can integrate Cisco DNA 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/>.

The following table displays the supported Cisco DNA Center-to-PagerDuty integration workflow.

Table 9: Cisco DNA Center-to-PagerDuty Integration Workflow

| Step | Description |
|--------|--|
| Step 1 | <p>Review the following Cisco DNA Center-to-PagerDuty integration requirements:</p> <ul style="list-style-type: none">• The latest Cisco DNA Center release.• PagerDuty <p>Note PagerDuty integration with Cisco DNA Center is accomplished using the PagerDuty Events REST APIs and the Cisco DNA Center Events framework.</p> <p>For information about the PagerDuty Events APIs, see https://developer.pagerduty.com/docs/events-api-v2/overview/.</p> |
| Step 2 | <p>Configure the integration settings. From the top-left corner, click the menu icon and choose System > Settings > System Configuration > Integration Settings. Enter your callback URL hostname or IP address.</p> |

| Step | Description |
|--------|---|
| Step 3 | <p>Select and subscribe one or more events to forward notifications from Cisco DNA Center to PagerDuty.</p> <p>To access an event in Cisco DNA Center, click the menu icon and choose Platform > Developer Toolkit > Event Notifications > Event Catalog. Event Catalog displays all the events.</p> <p>Click the Notification tab to subscribe to an event.</p> |
| Step 4 | <p>In the Notifications tab, create a new notification for the event.</p> <p>Follow the steps in the Create a New Notification wizard and select PagerDuty as the notification channel.</p> <p>The following data must be entered in the Cisco DNA Center platform GUI for the selected event:</p> <ul style="list-style-type: none"> • PagerDuty Events API URL • PagerDuty Integration key (routing key) <p>For detailed information about this event configuration procedure, see Subscribe Cisco DNA Center Event Notifications to PagerDuty, on page 63.</p> |
| Step 5 | <p>Notifications for the selected event are now forwarded to PagerDuty from Cisco DNA Center.</p> <p>The following are the supported workflow connections between Cisco DNA Center issues and PagerDuty events:</p> <ul style="list-style-type: none"> • Open Cisco DNA Center to trigger PagerDuty. |
| Step 6 | <p>PagerDuty responds to Cisco DNA Center with one of the following REST API responses:</p> <ul style="list-style-type: none"> • 202: The event has been accepted by PagerDuty. • 400: Bad Request - Check that the JSON is valid. • 429: Too many API calls at a time. • 500 or other 5xx: Internal Server Error - the PagerDuty server experienced an error while processing the event. • Networking Error: Error while trying to communicate with PagerDuty servers. |
| Step 7 | <p>Review and change (if necessary) the incident status in PagerDuty.</p> <p>Note Refer to your PagerDuty documentation for information about performing this step.</p> |
| Step 8 | <p>Close the incident in PagerDuty.</p> <p>Note Refer to your PagerDuty documentation for information about performing this step.</p> |
| Step 9 | <p>PagerDuty integration is a one-way notification from Cisco DNA Center to PagerDuty. Cisco DNA Center is not dependent on PagerDuty status to close an issue.</p> |

Subscribe Cisco DNA Center Event Notifications to PagerDuty

You can configure a Cisco DNA Center platform event notification to appear in PagerDuty as an alert. Follow the steps described in this procedure to configure a Cisco DNA 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 Cisco DNA Center platform. Refer to your PagerDuty documentation for instructions on setting up PagerDuty.

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

-
- Step 1** From the top-left corner, click the menu icon and 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, choose PAGERDUTY as the notification channel.
Click **Next** to configure the following 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, choose 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, choose an events API version from the dropdown 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 DNA Center Platform User Guide](#) and **Create an Event Notification** in the [Cisco DNA Center User Guide](#).

What to do next

Access PagerDuty to review the events.

The Cisco DNA 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

Cisco DNA Center-to-Cisco Webex Integration

- [About Cisco DNA Center-to-Cisco Webex Integration, on page 65](#)
- [Subscribe Cisco DNA Center Event Notifications to Cisco Webex, on page 66](#)

About Cisco DNA Center-to-Cisco Webex Integration

You can integrate Cisco DNA Center with Cisco Webex.

The following table displays the supported Cisco DNA Center-to-Cisco Webex integration workflow.

Table 10: Cisco DNA Center-to-Cisco Webex Integration Workflow

| Step | Description |
|--------|--|
| Step 1 | <p>Review the following Cisco DNA Center-to-Cisco Webex integration requirements:</p> <ul style="list-style-type: none"> • The latest Cisco DNA Center release. • Cisco Webex <p>Note Cisco DNA 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 Webex Teams - Integrations & Bots.</p> |
| Step 3 | <p>Configure the integration settings. From the top-left corner, click the menu icon and choose System > Settings > System Configuration > Integration Settings. Enter your callback URL hostname or IP address.</p> |
| Step 4 | <p>Select and subscribe one or more events to forward notifications from Cisco DNA Center to Cisco Webex.</p> <p>To access an event in Cisco DNA Center, click the menu icon and choose Platform > Developer Toolkit > Event Notifications > Event Catalog. Event Catalog displays all the events. Review the events and click the Notifications tab to subscribe to an event.</p> |

| Step | Description |
|---------|--|
| Step 5 | <p>In the Notifications tab, create a new notification for the event.</p> <p>Follow the steps in the Create a New Notification wizard and select Cisco Webex as the notification channel.</p> <p>The following required data must be entered in the Cisco DNA Center platform GUI:</p> <ul style="list-style-type: none"> • Authentication (bot access token) • Space name (or room ID) <p>For detailed information about this procedure, see Subscribe Cisco DNA Center Event Notifications to Cisco Webex, on page 66.</p> |
| Step 6 | Any notifications for the selected event are now forwarded to Cisco Webex from Cisco DNA Center and published as a new message in Cisco Webex. |
| Step 7 | <p>Cisco Webex responds to Cisco DNA Center with one of the following API messages:</p> <ul style="list-style-type: none"> • 202: The event has been accepted by Cisco Webex. • 400: Bad Request - Check that the JSON is valid. • 429: Too many API calls at a time. • 500 or other 5xx: Internal Server Error - the Cisco Webex server experienced an error while processing the event. • Networking Error: Error while trying to communicate with Cisco Webex servers. |
| Step 8 | Review the issue in Cisco Webex. |
| Step 9 | Close the issue in Cisco Webex. |
| Step 10 | Cisco DNA Center receives the status from Cisco Webex and then closes the issue. |

Subscribe Cisco DNA Center Event Notifications to Cisco Webex

Complete the following steps to subscribe Cisco DNA 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 Cisco DNA Center platform.

Ensure that you have **Webex Teams Room Id** and **Webex Teams Bot Access Token**. For more information, see [About Cisco DNA Center-to-Cisco Webex Integration, on page 65](#).

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

-
- Step 1** From the top-left corner, click the menu icon and 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 following values in the **WEBEX Settings** window.
- From the **Select Existing Instance** drop-down list, choose 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**.
The **Name and Description** window opens.
- Step 8** In the **Name and Description** window, do the following:
- 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 DNA Center Platform User Guide](#) and **Create an Event Notification** in the [Cisco DNA Center User Guide](#).
-

What to do next

Access Cisco Webex to review the events.