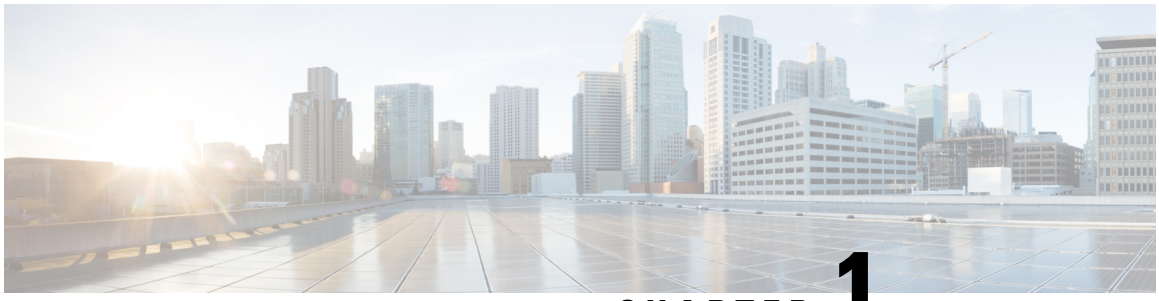
Cisco DNA Center User Guide, Release 2.2.2

First Published: 2021-08-09

Last Modified: 2023-04-07

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

CONTENTS



CHAPTER 1

New and Changed Information

The following table summarizes the new and changed features and tells you where they are documented.

Table 1: New and Changed Features for Cisco DNA Center, Release 2.2.2

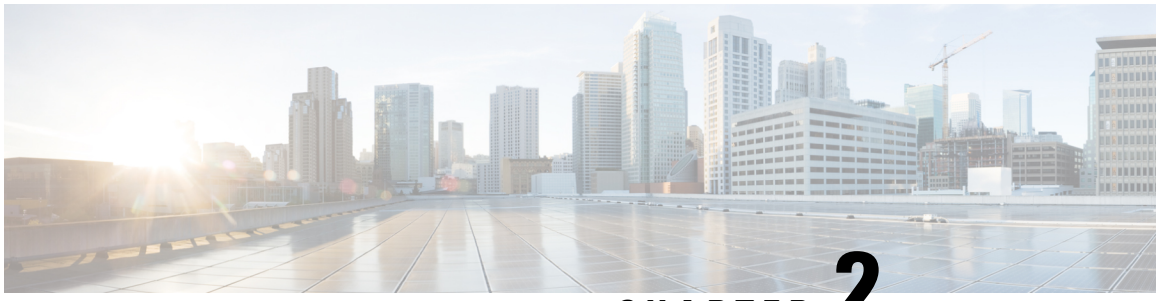
Feature	Description	Where Documented
Deregister faulty device from CSSM	The RMA workflow deregisters the faulty device from CSSM and registers the replacement device with CSSM.	Limitations of the RMA Workflow in Cisco DNA Center Replace a Faulty Device, on page 83
Automatic download option for ThousandEyes Enterprise Agent application	Within a few minutes of starting the Application Hosting Service, the ThousandEyes Enterprise Agent application is automatically downloaded. In the absence of an internet connection, you can set a proxy connection from the console to download the application.	Automatic Download of ThousandEyes Enterprise Agent Application, on page 473
Firepower Management Center	Cisco DNA Center supports the integration of Firepower Management Center (FMC). FMC provides complete and unified management over Firepower Threat Defense (FTD) devices for managing Cisco network security solutions.	Integrate Firepower Management Center, on page 69
Create Network Profiles for Firewall	Cisco DNA Center allows you to create network profiles for firewalls. You can create custom configurations to set up security devices like the Cisco Adaptive Security Appliance (ASA) family of devices and create FTD configurations to configure FTD devices.	Create Network Profiles for Firewall, on page 167
Retry option in RMA workflow	Cisco DNA Center allows you to retry the RMA workflow with the click of a single button.	Replace a Faulty Device
Preview Device 2.0	The **Preview Devices 2.0** toggle button is new in the top-right corner of the **Provision** > **Inventory** page. Click the **Preview Devices 2.0** toggle button to view the devices, site profiles, software images, topology, RMA, PnP, templates, and PSIRTs in a new 2.0 framework.	—

Feature	Description	Where Documented
Explore menu	The following features are moved from the Cisco DNA Center home page to the **Explore** menu: • Design • Policy • Provision • Assurance • Platform	—
Topology support for new devices	Topology support is provided for the following devices: • Cisco Catalyst IR8100 Heavy Duty Series Routers (IR8140H-K9 and IR8140H-P-K9) • Cisco Catalyst 9124AX Access Point (C9124AXI and C9124AXD)	—
Cisco Umbrella configuration support for new devices	Cisco Umbrella configuration support is available for the following devices: • Cisco Catalyst 9200 Access Switch with Cisco IOS-XE software version 17.3.1 or later • Cisco Catalyst 9300 Access Switch with Cisco IOS-XE software version 17.3.1 or later	About Cisco Umbrella, on page 484 Provision Cisco Umbrella on Network Devices, on page 487
Cisco Umbrella - Review Internal Domains	You can add and delete the list of internal domains from Cisco Umbrella.	Provision Cisco Umbrella on Network Devices, on page 487
Configuration Drift Visibility	The **Config Drift** page displays configuration changes and allows you to pick any two versions of the same device and compare their running configuration data. **Note** With this release, the information under **Previous Running vs Current Running** has been moved to the **Config Drift** page.	Display Information About Your Inventory, on page 49
Cisco Group-Based Policy Analytics	The **Access Contracts** can now be created and modified directly from the **Analytics** tab.	Access Contracts, on page 274
Group-Based Access Control	You can now view the policy enforcement statistics data in the Policies listing window. The total numbers of policy permits and denies are displayed for the selected time period. Group-based access control policies can be created or updated based on the traffic flows for a given source and destination group pair. You can also create custom views of the policy matrix to focus only on the policies that you are interested.	Create Group-Based Access Control Policy, on page 253

Feature	Description	Where Documented
Plug and Play support for Cisco DNA Traffic Telemetry Appliance	You can claim a Cisco DNA Traffic Telemetry Appliance from the Plug and Play Devices list.	Provision a Cisco DNA Traffic Telemetry Appliance, on page 371
IPv6 search	Cisco DNA Center allows you search for devices using their IPv6 addresses. You can search for a device using its full IPv6 address, any abbreviated form, or double column in the IPv6 address with prefix and postfix combinations.	Use Global Search, on page 15
User-defined fields	User-defined fields are custom labels that you can create and assign to any device in Cisco DNA Center. By assigning these labels to a device and adding values to them, you can show more details about the device in the device details page.	Manage User-Defined Fields, on page 54
Inventory Insights	Cisco DNA Center provides insights about the devices in your network if there are any inconsistencies in the device configuration of two connected devices.	Inventory Insights, on page 75
Persistence across inventory views	The device selection and the number of devices shown in the inventory table persist across inventory views in Cisco DNA Center.	Display Information About Your Inventory, on page 49
Separation of golden tagging and download	From this release, you can separate download and golden tagging of software images. Cisco DNA Center allows you to download the software images by not marking them as golden.	Specify a Golden Software Image, on page 93
Cisco sensor provisioning SSID	Cisco DNA Center sensors use the Cisco sensor provisioning Service Set Identifier (SSID) to communicate with the Plug and Play (PnP) server and obtain day-0 configurations for running tests.	Provision a Cisco Sensor SSID for Nonfabric Deployment, on page 156
Interface/VLAN groups	Cisco DNA Center allows you to configure networks to have multiple broadcast domains through different VLANs. The Cisco DNA Center interface groups are logical groups of interfaces that facilitate user configuration, where the same interface group can be configured on multiple WLANs or while overriding a WLAN interface per AP group.	Design and Provision Interface/VLAN Groups to Nonfabric Deployments, on page 153
Troubleshoot network connectivity	You can now troubleshoot network connectivity using Cisco DNA Center.	Troubleshoot Network Connectivity, on page 240
Migration support for Cisco SD-Access	Cisco DNA Center provides Machine Reasoning Engine (MRE) workflows to assist you in planning your network migration to Cisco SD-Access.	Validate Cisco SD-Access Migration Using the MRE Workflow, on page 235

Feature	Description	Where Documented
Security Advisory Knowledge Bundle (KB)	You can enable notifications for new security advisory KBs. After notification is enabled, Cisco DNA Center provides visual notification and actionable alerts for any new security advisory KBs that are available from the cloud.	Add Notification for a New Security Advisory KB, on page 231
Security Advisories view in Inventory	The Cisco DNA Center security focus view allows you to view the list of security advisories for your devices, based on the data retrieved from the previous security scan. The device data that you retrieve from the Security Advisories tool is now displayed in the Inventory page.	View Security Advisories in Inventory Page, on page 232
Authentication check using security option	Cisco DNA Center security focus allows you to view the results of trustworthy checks on your devices.	Perform an Integrity Verification Check, on page 64
Cisco AI Endpoint Analytics	• **AI Endpoint Spoofing Detection**: Cisco AI Endpoint Analytics analyzes NetFlow telemetry data to detect spoofed endpoints. If an endpoint's behavior is not in line with its profile, Cisco AI Endpoint Analytics flags the anomaly, assigns a Trust Score to the endpoint, and lists it as a spoofed endpoint. You then review the details of the flagged endpoints and apply Adaptive Network Control (ANC) policies (created in Cisco ISE) from the Cisco AI Endpoint Analytics window. • **Automatic Profiling Rule Updates**: Cisco provides automatic system rule updates to enhance endpoint profiling accuracy. These updates help you profile endpoints more granularly and help profile previously unknown endpoints. Review the profiling changes suggested in an update. Then, you can either apply these changes or ignore the update. Major and minor profiling changes to existing endpoint profiles are displayed for your review. • **Cisco ISE MDM Attributes Support**: Cisco AI Endpoint Analytics receives MDM attributes from Cisco ISE if Cisco ISE is integrated with an MDM server. These MDM attributes are available for creating endpoint profiles using custom rules. • **Global Search Support**: In the Cisco DNA Center global search, when you search for endpoints by their IP address or MAC address, a link to AI Endpoint Analytics is displayed along with available profiling details for the endpoint. The profiling details and other information about the endpoint are displayed in the search result.	Introduction to Cisco AI Endpoint Analytics
Network Bug Identifier	The Cisco DNA Center network bug identifier tool allows you to scan the network for a selected set of defects or bugs that have been identified previously and are known to Cisco.	Enable Network Bug Identifier, on page 241
System Bug Identifier	The System Bug Identifier tool provides an option to identify bugs in Cisco DNA Center.	Enable System Bug Identifier, on page 243

Feature	Description	Where Documented
View IP Address Pools	• In the **IPv4** and **IPv6** columns, an **i** icon appears next to the corresponding used percentage of **IPv4** and **IPv6** for a given IP address pool. The tooltip displays the percentage of **Free**, **Unassignable**, **Assigned**, and **Default Assigned** IP addresses. • In the IP address pool slide-in pane, the **Used** area displays **Assigned** and **Unassigned** IP addresses to a network device. • Global and site IP address pools can have blocklisted IP addresses. • Subpools cannot have blocklisted IP addresses. • Cisco DNA Center rejects the IP address pool creation request of a CIDR address pool if it contains blocklisted IP addresses. • In the next free IP address pool request, Cisco DNA Center skips the blocklisted IP addresses to find the next free IP address pool.	View IP Address Pools, on page 187



CHAPTER 2

Get Started with Cisco DNA Center

About Cisco DNA Center

Cisco Digital Network Architecture offers centralized, intuitive management that makes it fast and easy to design, provision, and apply policies across your network environment. The Cisco DNA Center GUI provides end-to-end network visibility and uses network insights to optimize network performance and deliver the best user and application experience.

Log In

Access Cisco DNA Center by entering its network IP address in your browser. For compatible browsers, see the Cisco DNA Center Release Notes. This IP address connects to the external network and is configured during the Cisco DNA Center installation. For more information about installing and configuring Cisco DNA Center, see the Cisco DNA Center Installation Guide.

You should continuously use Cisco DNA Center to remain logged in. If you are inactive for too long, Cisco DNA Center logs you out of your session automatically.

Step 1 Enter an address in your web browser's address bar in the following format. Here, *server-ip* is the IP address (or the hostname) of the server on which you have installed Cisco DNA Center:

https://*server-ip*

Example: https://192.0.2.1

Depending on your network configuration, you might have to update your browser to trust the Cisco DNA Center server security certificate. Doing so will help ensure the security of the connection between your client and Cisco DNA Center.

Step 2 Enter the Cisco DNA Center username and password assigned to you by the system administrator. Cisco DNA Center displays its home page.

If your user ID has the SUPER-ADMIN-ROLE and no other user with the same role has logged in before, you will see a first-time setup wizard instead of the home page.

Step 3 To log out, click the **Menu** icon (☰) and choose **Sign Out**.

Complete the Quick Start Workflow

After you have installed and configured the Cisco DNA Center appliance, you can log in to its GUI. Use a compatible, HTTPS-enabled browser when accessing Cisco DNA Center.

When you log in for the first time as the admin superuser (with the username `admin` and the SUPER-ADMIN-ROLE assigned), the Quick Start workflow automatically starts. Complete this workflow to discover the devices that Cisco DNA Center will manage and enable the collection of telemetry from those devices.

Before you begin

To log in to Cisco DNA Center and complete the Quick Start workflow, you will need:

- The *admin* superuser username and password that you specified while completing one of the following procedures in the Cisco DNA Center Second-Generation Appliance Installation Guide:
  - Configure the Primary Node Using the Maglev Wizard
  - Configure the Primary Node Using the Expert Configuration Wizard (44- or 56-core appliance)
  - Configure the Primary Node Using the Expert Configuration Wizard (112-core appliance)
- The information described in the installation guide's Required First-Time Setup Information topic.

Step 1 After the Cisco DNA Center appliance reboot is completed, launch your browser.

Step 2 Enter the host IP address to access the Cisco DNA Center GUI, using **`HTTPS://`** and the IP address of the Cisco DNA Center GUI that was displayed at the end of the configuration process.

After entering the IP address, one of the following messages appears (depending on the browser you are using):

- Google Chrome: `Your connection is not private`
- Mozilla Firefox: `Warning: Potential Security Risk Ahead`

Step 3 Ignore the message and click **Advanced**.

One of the following messages appears:

- Google Chrome:

```
This server could not prove that it is GUI-IP-address; its security certificate is not trusted
by your computer's
 operating system. This may be caused by a misconfiguration or an attacker intercepting your
connection.
```

- Mozilla Firefox:

```
Someone could be trying to impersonate the site and you should not continue.

Websites prove their identity via certificates. Firefox does not trust GUI-IP-address because
its certificate issuer is unknown,
the certificate is self-signed, or the server is not sending the correct intermediate certificates.
```

These messages appear because the controller uses a self-signed certificate. For information on how Cisco DNA Center uses certificates, see the "Certificate and Private Key Support" section in the Cisco DNA Center Administrator Guide.

Step 4 Ignore the message and do one of the following:

- Google Chrome: Click the **Proceed to** *GUI-IP-address* **(unsafe)** link.
- Mozilla Firefox: Click **Accept the Risk and Continue**.

The Cisco DNA Center login screen appears.

Step 5 Enter the admin's username (admin) and password that you set when you configured Cisco DNA Center, then click **Log In**.

In the resulting screen, you are prompted to specify a new admin password (as a security measure).

Step 6 Do the following, then click **Next**:

a) Enter the same admin password you specified in Step 5.
b) Enter and confirm a new admin password.

Step 7 In the resulting screen, enter your cisco.com username and password and then click **Next**.

These credentials are used to register software downloads and receive system communications.

The **Terms & Conditions** screen opens, providing links to the software End User License Agreement (EULA) and any supplemental terms that are currently available.

Step 8 After reviewing these documents, click **Next** to accept the EULA.

The **Quick Start Overview** slider opens. Click > to view a description of the tasks that the Quick Start workflow will help you complete in order to start using Cisco DNA Center.

Step 9 Complete the Quick Start workflow:

a) Click **Let's Do it**.
b) In the **Discover Devices: Provide IP Ranges** screen, enter the following information and then click **Next**:
   - The name for the device discovery job.
   - The IP address ranges of the devices you want to discover. Click + to enter additional ranges.
   - Specify whether you want to designate your appliance's loopback address as its preferred management IP address. For more information, see the "Preferred Management IP Address" topic in the Cisco DNA Center User Guide.
c) In the **Discover Devices: Provide Credentials** screen, enter the information described in the following table for the type of credentials you want to configure and then click **Next**:

Field	Description
CLI (SSH) Credentials	

Field	Description
Username	Username used to log in to the CLI of the devices in your network.
Password	Password used to log in to the CLI of the devices in your network.
Name/Description	Name or description of the CLI credentials.
Enable Password	Password used to enable a higher privilege level in the CLI. Configure this password only if your network devices require it.
SNMP Credentials: SNMPv2c Read tab	
Name/Description	Name or description of the SNMPv2c read community string.
Community String	Read-only community string password used only to view SNMP information on the device.
SNMP Credentials: SNMPv2c Write tab	
Name/Description	Name or description of the SNMPv2c write community string.
Community String	Write community string used to make changes to the SNMP information on the device.
SNMP Credentials: SNMPv3	
Name/Description	Name or description of the SNMPv3 credentials.
Username	Username associated with the SNMPv3 credentials.
Mode	Security level that SNMP messages require: • **No Authentication, No Privacy** (noAuthnoPriv): Does not provide authentication or encryption. • **Authentication, No Privacy** (authNoPriv): Provides authentication, but does not provide encryption. • **Authentication and Privacy** (authPriv): Provides both authentication and encryption.
Authentication Password	Password required to gain access to information from devices that use SNMPv3. The password must be at least eight characters in length. Note the following points: • Some wireless controllers require that passwords be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

Field	Description
Authentication Type	Hash-based Message Authentication Code (HMAC) type used when either **Authentication and Privacy** or **Authentication, No Privacy** is set as the authentication mode: • **SHA**: HMAC-SHA authentication. • **MD5**: HMAC-MD5 authentication.
Privacy Type	Privacy type used when **Authentication and Privacy** is set as the authentication mode: • **AES128**: 128-bit AES encryption. • **None**: No privacy.
Privacy Password	Password used to generate the secret key for encrypting messages that are exchanged with devices that support AES128 encryption. Passwords must be at least eight characters long. Note the following points: • Some wireless controllers require that passwords be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
NETCONF	
Port	The NETCONF port that Cisco DNA Center should use in order to discover wireless controllers that run Cisco IOS-XE.

d) In the **Create Site** screen, group the devices you are going to discover into one site in order to facilitate telemetry and then click **Next**.

You can enter the site's information manually or click the location you want to use in the provided map.

e) In the **Enable Telemetry** screen, check the network components that you want Cisco DNA Center to collect telemetry for and then click **Next**.

To open a pop-up window that lists the commands Cisco DNA Center will send to enable telemetry on a particular component, click its **View Sample Commands** link.

f) In the **Summary** screen, review the settings that you have entered and then do one of the following:

- If you want to make changes, click the appropriate **Edit** link to open the relevant screen.
- If you're happy with the settings, click **Start Discovery and Telemetry**. Cisco DNA Center validates your settings to ensure that they will not result in any issues. After validation is complete, the screen updates.

  Cisco DNA Center begins the process of discovering your network's devices and enabling telemetry for the network components you selected. The process will take a minimum of 30 minutes (more for larger networks).

g) Click **Launch Homepage** to open the Cisco DNA Center homepage.

While Cisco DNA Center discovers your network's devices and enables telemetry, you can familiarize yourself with the functionality that the product provides. Begin by clicking **Launch Homepage**. Then click the **Explore** link to open a page that provides pointers to product documentation and videos.

A message appears at the top of the homepage to indicate when the Quick Start workflow has completed.

Default Home Page

After you log in, Cisco DNA Center displays its home page. The home page has the following main areas: **Assurance Summary**, **Network Snapshot**, **Network Configuration**, and **Tools**.

The **Assurance Summary** area includes:

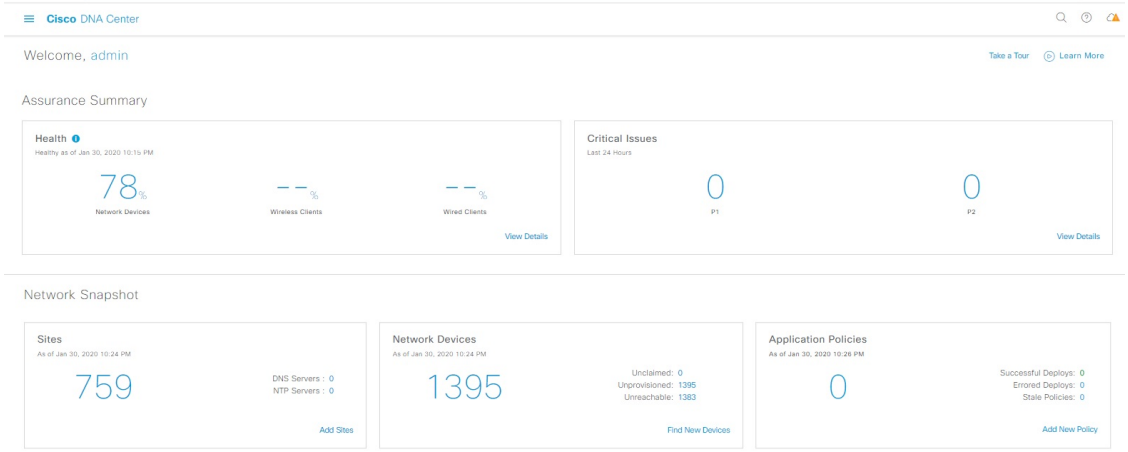
- **Health**: Provides the health score of your overall enterprise, which includes network devices, wired clients, and wireless clients. Clicking **View Details** takes you to the **Overall Health** window.
- **Critical Issues**: Provides the count of P1 and P2 issues. Clicking **View Details** takes you to the **Open Issues** window.
  - **P1**: Critical issues that need immediate attention before they cause a wider impact on network operations.
  - **P2**: Major issues that can potentially impact multiple devices or clients.
- **Trends and Insights**: Provides insights about the performance of your network. Clicking **View Details** takes you to the **Network Insights** window.

The **Network Snapshot** area includes:

- **Sites**: Provides the number of sites discovered on your network along with the number of DNS and NTP servers. Clicking **Add Sites** takes you to the **Add Site** window.
- **Network Devices**: Provides the number of network devices discovered on your network along with the number of unclaimed, unprovisioned, and unreachable devices. Clicking **Find New Devices** takes you to the **New Discovery** window.
- **Application Policies**: Provides the number of application policies discovered on your network along with the number of successful and errored deployments. Clicking **Add New Policy** takes you to the **Application Policies** window.
- **Network Profiles**: Provides the number of profiles discovered on your network. Clicking **Manage Profiles** takes you to the **Network Profiles** window.
- **Images**: Provides the number of images discovered on your network along with the number of untagged and unverified images. Clicking **Import Images/SMUs** takes you to the **Image Repository** window.
- **Licensed Devices**: Provides the number of devices that have a Cisco DNA Center license along with the number of switches, routers, and access points. Clicking **Manage Licenses** takes you to the **License Management** window.

Tools: Use the **Tools** area to configure and manage your network.

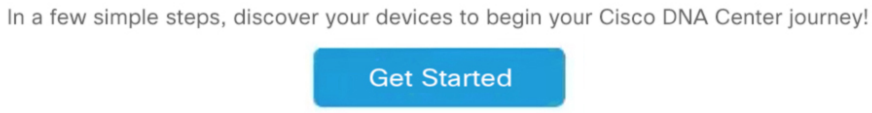
Figure 1: Cisco DNA Center Home Page



Different Views of Home Page:

Getting Started

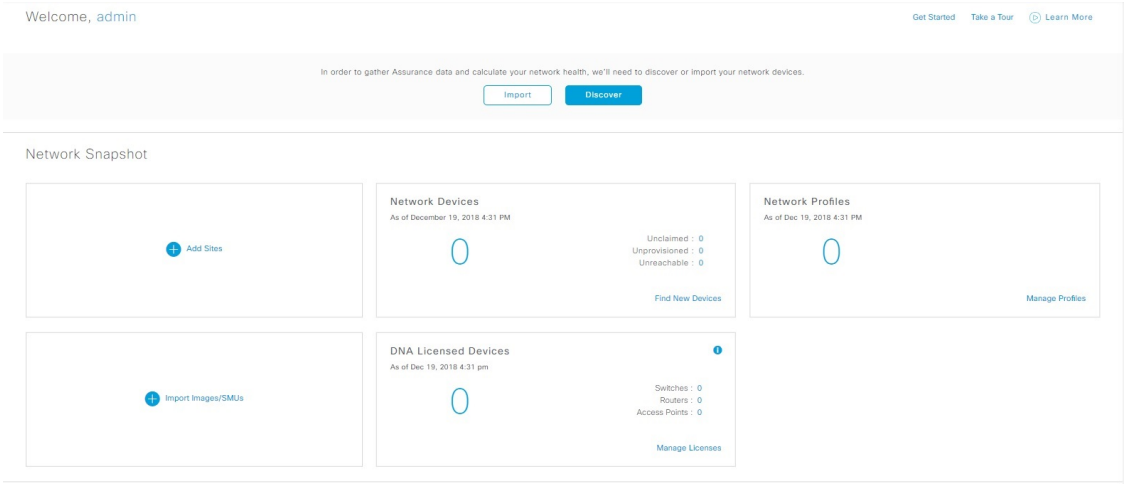
When you log in to Cisco DNA Center for the first time as a Network Administrator or System Administrator, or when there are no devices in the system, you see the following dashlet. Click **Get Started** and complete the getting started workflow to discover new devices in your network.



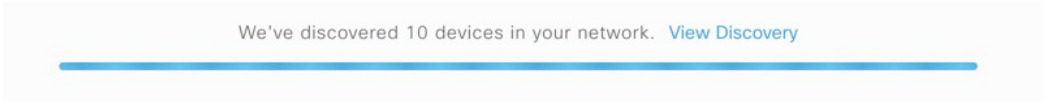
When you log in to Cisco DNA Center for the first time as an Observer, you see the following message:

Day 0 Home Page

If you skipped getting started, or when there are no devices in the system, you see the following home page.



When discovery is in progress, you see a progress message with a link to the **Discovery** window.



When there are devices in the system, you see a network snapshot of discovered devices.

Click the **Menu** icon (☰) at the top-left corner of the home page to access the following menus:

- Design
- Policy
- Provision
- Assurance
- Workflows
- Tools
- Platform
- Activity
- Reports
- System
- Explore

Click the icons at the top- and bottom-right corner of the home page to perform common tasks:

Icon	Description
🔍	**Search**: Search for devices, users, hosts, menus, and other items that are stored anywhere in the Cisco DNA Center database.

Icon	Description
	**Help** • **About**: Display the current Cisco DNA Center software version. Click **Release Notes** to launch the release notes in a separate browser tab. Click **Packages** to view the system and application package versions. Click **Serial number** to view the serial number of the Cisco DNA Center appliance. • **API Reference**: Open the Cisco DNA Center platform API documentation in Cisco DevNet. • **Developer Resources**: Open Cisco DevNet, where you can access developer tools. • **Help**: Launch context-sensitive online help in a separate browser tab. • **Contact Support**: Open a support case with the Cisco Technical Assistance Center (TAC). • **Make a Wish**: Submit your comments and suggestions to the Cisco DNA Center product team.
	**Software Updates**: See a list of available software updates. Click the **Go to Software Updates** link to view system and application updates.
	**Notifications**: Displays event notifications and sets notification preferences. A red circle by the notification icon indicates that there are new notifications.
	**Interactive Help**: Opens a menu of interactive help flows that help you complete specific tasks from the GUI.

Note By default, the login name you provided is displayed in the Welcome text. To change the name, click the name link; for example, **admin**. You are taken to the **User Management** window, where you can edit the display name.

Use Global Search

Use the global Search function to find items in the following categories anywhere in Cisco DNA Center:

- **Activities**: Search for Cisco DNA Center menu items, workflows, and features by name.
- **Applications**: Search for them by name.
- **Application Groups**: Search for them by name.
- **Authentication template**: Search for them by name or type.

- **Devices**: Search for them by collection status, reachability status, location, or tag.
- **Fabric**: Search by fabric name.
- **Hosts and Endpoints**: Search for them by name, IP address, or MAC address.
- **IP Pools**: Search for them by name or IP address.
- **Network Devices**: Search for them by name, IP address, serial number, software version, platform, product family, or MAC address.
- **Network Profiles**: Search by profile name.
- **Network Settings**
  - **Device Credentials**: Search by name.
  - **IP Address Pools**: Search for them by group name or pool CIDR.
  - **Service Provider Profiles**: Search for them by profile name, WAN provider, or model.
- **Policy**: Search for them by name or description.
- **Sites**: Search for them by name.
- **Traffic copy**: Search for them by name and description.
- **Transits**: Search by transit name.
- **Users**: Search for the system settings and users by username. Case-insensitivity and substring search are not supported for usernames.
- Other items, as new versions of Cisco DNA Center are released.

To start a global Search, click the icon in the top-right corner of any Cisco DNA Center page. Cisco DNA Center displays a pop-up global search window, with a Search field where you can begin entering identifying information about an item.

You can enter all or part of the target item's name, address, serial number, or other identifying information. The Search field is case-insensitive and can contain any character or combination of characters.

As you begin entering your search string, Cisco DNA Center displays a list of possible search targets that match your entry. If more than one category of item matches your search string, Cisco DNA Center sorts them by category, with a maximum of five items in each category. The first item in the first category is selected automatically, and summary information for that item appears in the summary panel on the right.

You can scroll the list as needed, and click any of the suggested search targets to see information for that item in the summary panel. If there are more than five items in a category, click **View All** next to the category name. To return to the categorized list from the complete list of search targets, click **Go Back**.

As you add more characters to the search string, global Search automatically narrows the displayed list.

Cisco DNA Center allows you to search for a device using its entire IPv6 address or any abbreviated form of the IPv6 address.

For example, to search for *2001:0db8:85a3:0000:0000:8a2e:0370:7334*, you can use the following search entries:

- `2001:0db8:85a3:0000:0000:8a2e:0370:7334` (using the full IPv6 address)

- **2001:db8:85a3:0:0:8a2e:0:7334** (truncating leading zeros)
- **2001:db8:85a3::8a2e:0:7334** (compressing consecutive zeros with a double colon)
- **2001:db8:85a3** (using a portion of the IPv6 address)

Cisco DNA Center allows you to search for an IPv6 address by using the double colon in the IPv6 address with prefix, postfix, or any combination.

For example, to search for *2001:db8:85a3::8a2e:0:7334*, you can use the following search entries:

- **::** (using double colon alone)
- **85a3::8a2e** (using prefix and postfix with double colon)
- **85a3::** (using prefix with double colon)
- **::8a2e** (using postfix with double colon)

You can search for devices in Cisco DNA Center by entering their MAC addresses in any format (with a hyphen or colon).

When you are finished, click ✖ to close the window.

Global search can display five results per category at a time.

View Event Notifications

Cisco DNA Center logs both system-generated and user-generated events. You can view these events at any time. When new events are logged, a red dot appears next to the **Notification** icon at the top right of the page.

You can also configure Cisco DNA Center to log and notify you of specific events. For more information, see Set Event Notification Preferences.

In the Cisco DNA Center GUI, click the **Notification** icon at the top-right corner of the page.

The notifications are displayed in a list with the most recent messages at the top.

Set Event Notification Preferences

Cisco DNA Center allows you to configure the types of events that you want to know about and how you want to be notified. Based on your notification preferences, when you receive a notification, a small dot appears next to the **Notification** icon at the top-right corner of the page.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰), hover your cursor over **admin**, and choose **My Profile and Settings** > **Notification Preferences**.

Note (Optional) You can also navigate to the **Notification Preferences** page from the Cisco DNA Center home page by clicking the notification icon at the top-right corner of the page. From the bottom of the **Notifications** pane, click the gear icon.

The **Notification Preferences** page displays a list of notification categories. You can expand a notification category to view more specific notifications underneath. The descriptions help you understand the types of activities that trigger a notification. You can choose to receive specific notifications or all notifications within a category.

Step 2 In the **In Notification Center** column, check the check boxes for the respective notification types that you want to receive.

Enable Localization

You can view the Cisco DNA Center GUI screens in English (the default), Chinese, Japanese, or Korean.

To change the default language, perform the following task:

Step 1 In your browser, change the locale to one of the supported languages: Chinese, Japanese, or Korean.

- From Google Chrome, do the following:
  1. **a.** Click the icon in the top-right corner, and then choose **Settings**.
  2. **b.** Scroll down and click **Advanced**.
  3. **c.** From the **Languages** > **Language** drop-down list, choose **Add languages**.

     The **Add languages** pop-up window appears.
  4. **d.** Choose **Chinese**, **Japanese**, or **Korean**, and then click **Add**.
- From Mozilla Firefox, do the following:
  1. **a.** Click the icon in the top-right corner, and then choose **Options**.
  2. **b.** From the **Language and Appearance** > **Language** area, choose **Search for more languages**.

     The **Firefox Language Settings** pop-up window appears.
  3. **c.** From the **Select a language to add** drop-down list, choose **Chinese**, **Japanese**, or **Korean**.
  4. **d.** Click **Ok**.

Step 2 Log in to Cisco DNA Center.

The GUI screens are shown in the selected language.

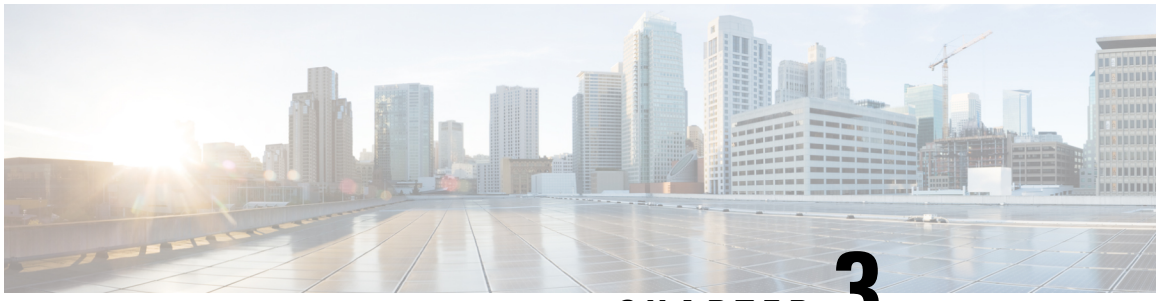
Figure 2: Example Localized Login Screen

Where to Start

To start using Cisco DNA Center, you must first configure the Cisco DNA Center settings so that the server can communicate outside the network.

After you configure the settings, your current environment determines how you start using Cisco DNA Center:

- Existing infrastructure: If you have an existing infrastructure (brownfield deployment), start by running Discovery. After you run Discovery, all your devices are displayed on the **Inventory** window.
- New or nonexisting infrastructure: If you have no existing infrastructure and are starting from scratch (greenfield deployment), create a network hierarchy.



CHAPTER 3

Discover Your Network

About Discovery

The Discovery feature scans the devices in your network and sends the list of discovered devices to Inventory.

The Discovery feature also can work with the Device Controllability feature to configure the required network settings on devices, if these settings are not already present on the device.

There are three ways for you to discover devices:

- Use Cisco Discovery Protocol (CDP) and provide a seed IP address.
- Specify a range of IP addresses. (A maximum range of 4096 devices is supported.)
- Use Link Layer Discovery Protocol (LLDP) and provide a seed IP address.

When configuring the Discovery criteria, remember that there are settings that you can use to help reduce the amount of time it takes to discover your network:

- **CDP Level** and **LLDP Level**: If you use CDP or LLDP as the Discovery method, you can set the CDP or LLDP level to indicate the number of hops from the seed device that you want to scan. The default, level 16, might take a long time on a large network. So, if fewer devices have to be discovered, you can set the level to a lower value.
- **Subnet Filters**: If you use an IP address range, you can specify devices in specific IP subnets for Discovery to ignore.
- **Preferred Management IP**: Whether you use CDP, LLDP, or an IP address range, you can specify whether you want Cisco DNA Center to add any of the device's IP addresses or only the device's loopback address.

Note For Cisco SD-Access Fabric and Cisco DNA Assurance, we recommend that you specify the device's loopback address.

Regardless of the method you use, you must be able to reach the device from Cisco DNA Center and configure specific credentials and protocols in Cisco DNA Center to discover your devices. These credentials can be configured and saved in the **Design** > **Network Settings** > **Device Credentials** window or on a per-job basis in the **Discovery** window.

Note If a device uses a first hop resolution protocol like Hot Standby Router Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP), the device might be discovered and added to the inventory with its floating IP address. Later, if HSRP or VRRP fails, the IP address might be reassigned to a different device. This situation can cause issues with the data that Cisco DNA Center retrieves for analysis.

Discovery Dashboard

In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Discovery** to view the **Discovery Dashboard**. The **Discovery Dashboard** shows the inventory overview, latest discovery, discovery type, discovery status, and recent discoveries.

Discovery Prerequisites

Before you run Discovery, complete the following minimum prerequisites:

- Understand what devices will be discovered by Cisco DNA Center by viewing the Supported Devices List.
- Understand that the preferred network latency between Cisco DNA Center and devices is 100 ms round-trip time (RTT). (The maximum latency is 200 ms RTT.)
- Ensure at least one SNMP credential is configured on your devices for use by Cisco DNA Center. At a minimum, this can be an SNMPv2C read credential. For more information, see Discovery Credentials, on page 23.
- Configure SSH credentials on the devices you want Cisco DNA Center to discover and manage. Cisco DNA Center discovers and adds a device to its inventory if at least one of the following criteria is met:
  - The account that is being used by Cisco DNA Center to SSH into your devices has privileged EXEC mode (level 15).
  - You configure the device's enable password as part of the CLI credentials configured in the Discovery job. For more information, see Discovery Configuration Guidelines and Limitations, on page 25.

Discovery Credentials

Discovery credentials are the CLI, SNMPv2c, SNMPv3, HTTP(S), and NETCONF configuration values for the devices that you want to discover. You must specify the credentials based on the types of devices you are trying to discover:

- Network devices: CLI and SNMP credentials.

Note For NETCONF-enabled devices such as embedded wireless controllers, you must specify SSH credentials with admin privilege and select the NETCONF port.

- Compute devices (NFVIS): CLI, SNMP, and HTTP(S) credentials.

Because the various devices in a network can have different sets of credentials, you can configure multiple sets of credentials in Cisco DNA Center. The Discovery process iterates through all sets of credentials that are configured for the Discovery job until it finds a set that works for the device.

If you use the same credential values for the majority of devices in your network, you can configure and save them to reuse in multiple Discovery jobs. To discover devices with unique credentials, you can add job-specific Discovery credentials when you run Discovery jobs. You can configure up to 10 global credentials for each credential type and define any five of them. If you need to define job-specific credential, you can define four global credentials and one job-specific credential for each credential type.

Discovery Credentials and Cisco ISE

If you are using Cisco ISE as an authentication server, the Discovery feature authenticates devices using Cisco ISE as part of the discovery process. To make sure that your devices are discovered properly, follow these guidelines:

- Do not use Discovery credentials that have fewer than 4 alphanumeric characters. Although devices may have credentials with fewer than 4 alphanumeric characters, Cisco ISE allows 4 alphanumeric characters as the minimum username and password length. If the device credentials have fewer than 4 characters, Cisco DNA Center cannot collect the device's inventory data, and the device will go into a partial collection state.
- Do not use credentials that have the same username, but different passwords (cisco/cisco123 and cisco/pw123). While Cisco DNA Center allows the discovery of devices with the same username but different passwords, Cisco ISE does not allow this. If a duplicate username is used, Cisco DNA Center cannot authenticate the device and collect its inventory data, and the device will go into a partial collection state.

For information on how to define Cisco ISE as a AAA server, see Add Cisco ISE or Other AAA Servers, on page 190.

Guidelines and Limitations for Discovery Credentials

The following are the guidelines and limitations for the Cisco DNA Center Discovery credentials:

- To change the device credentials used in a Discovery job, you need to edit the Discovery job and deselect the credentials that you no longer want to use. Then, you need to add the new credentials and start the discovery. For more information, see Change Credentials in a Discovery Job, on page 42.
- If you change a device's credential after successfully discovering the device, subsequent polling cycles for that device fail. To correct this situation, use one of the following options:
  - Use the Discovery tool to:
    - Run a new Discovery job with job-specific credentials that match the device's new credential.
    - Edit the existing Discovery job and re-run the Discovery job.
  - Use the Design tool to:
    - Create a new global credential and run a new Discovery job using the correct global credential.
    - Edit an existing global credential and use Copy & Edit to recreate the Discovery job. Alternately, create a new Discovery job.
- If an ongoing Discovery polling cycle fails because of a device authentication failure, you can correct the situation using one of following options:
  - Use the Discovery tool to:
    - Stop or delete the current Discovery job and run a new Discovery job with job-specific credentials that match the device's credential.
    - Stop or delete the current Discovery job, edit the existing Discovery job, and re-run the Discovery job.
  - Use the Design tool to:
    - Create a new global credential and run a new Discovery job using the correct global credential.
    - Edit an existing global credential and use Copy & Edit to recreate the Discovery job. Alternately, create a new Discovery job.
- Deleting a global credential does not affect previously discovered devices. The status of the previously discovered devices does not indicate an authentication failure. However, the next Discovery job that tries to use the deleted credential will fail. The Discovery job will fail **before** it tries to contact any devices.

Discovery Credentials Example

The devices that form a typical network can have widely varying Discovery requirements. Cisco DNA Center lets you create multiple Discovery jobs to support these varying requirements. For example, assume that a network of 200 devices form a Cisco Discovery Protocol (CDP) neighborhood. In this network, 190 devices share a global credential (Credential 0) and the remaining devices each have their own unique credential (Credential-1 through Credential-10).

To discover all the devices in this network using Cisco DNA Center, perform the following task:

Step 1 Configure the CLI global credentials as Credential-0.

Step 2 Configure the SNMP (v2c or v3) global credentials.

Step 3 Run a Discovery job using one of the 190 device IP addresses (190 devices that share the global credentials) and the global Credential-0.

Step 4 Run 10 separate Discovery jobs for each of the remaining 10 devices using the appropriate job-specific credentials, for example, Credential-1, Credential-2, Credential-3, and so on.

Step 5 Review the results in the **Inventory** window.

Preferred Management IP Address

When Cisco DNA Center discovers a device, it uses one of the device's IP addresses as the preferred management IP address. The IP address can be that of a built-in management interface of the device, another physical interface, or a logical interface such as Loopback0. You can configure Cisco DNA Center to use the device's loopback IP address as the preferred management IP address, provided the IP address is reachable from Cisco DNA Center.

When you choose **Use Loopback IP** as the preferred management IP address, Cisco DNA Center determines the preferred management IP address as follows:

- If the device has one loopback interface, Cisco DNA Center uses that loopback interface IP address.
- If the device has multiple loopback interfaces, Cisco DNA Center uses the loopback interface with the highest IP address.
- If there are no loopback interfaces, Cisco DNA Center uses the Ethernet interface with the highest IP address. (Subinterface IP addresses are not considered.)
- If there are no Ethernet interfaces, Cisco DNA Center uses the serial interface with the highest IP address.

After a device is discovered, you can update the management IP address from the **Inventory** window. For more information, see Update a Device's Management IP Address, on page 77.

Discovery Configuration Guidelines and Limitations

The following are the guidelines and limitations for Cisco DNA Center to discover your Cisco Catalyst 3000 Series Switches and Catalyst 6000 Series Switches:

- Configure the CLI username and password with privileged EXEC mode (level 15). This is the same CLI username and password that you configure in Cisco DNA Center for the Discovery function. Cisco DNA Center requires the highest access level to the device.
- Explicitly specify the transport protocols allowed on individual interfaces for both incoming and outgoing connections. Use the **transport input** and **transport output** commands for this configuration. For information about these commands, see the command reference document for the specific device type.
- Do not change the default login method for a device's console port and the VTY lines. If a device is already configured with a AAA (TACACS) login, make sure that the CLI credential defined in the Cisco DNA Center is the same as the TACACS credential defined in the TACACS server.
- Cisco Wireless Controllers must be discovered using the Management IP address instead of the Service Port IP address. If not, the related wireless controller 360 and AP 360 pages will not display any data.

Perform Discovery

Discover Your Network Using CDP

You can discover devices using Cisco Discovery Protocol (CDP), an IP address range, or LLDP. This procedure shows you how to discover devices and hosts using CDP. For more information about the other discovery methods, see Discover Your Network Using an IP Address Range, on page 31 and Discover Your Network Using LLDP, on page 36.

Note

- The Discovery function requires the correct SNMP Read Only (RO) community string. If an SNMP RO community string is not provided, as a *best effort*, the Discovery function uses the default SNMP RO community string, public.
- CLI credentials are not required to discover hosts; hosts are discovered through the network devices to which they are connected.

Before you begin

- Enable CDP on your network devices.
- Configure your network devices, as described in Discovery Prerequisites, on page 22.
- Configure your network device's host IP address as the client IP address. (A host is an end-user device, such as a laptop computer or mobile device.)

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Discovery**.
The **Discovery** window appears with dashlets.

Step 2 Click **Add Discovery**.
The **New Discovery** window appears.

Step 3 In the **Discovery Name** field, enter a name.

Step 4 Expand the **IP Address/Range** area if it is not already visible, and configure the following fields:

a) For **Discovery Type**, click **CDP**.

b) In the **IP Address** field, enter a seed IP address for Cisco DNA Center to start the Discovery scan.

c) (Optional) In the **Subnet Filter** field, enter an IP address or subnet to exclude from the Discovery scan.

You can enter addresses either as an individual IP address (*x.x.x.x*) or as a classless inter-domain routing (CIDR) address (*x.x.x.x/y*), where *x.x.x.x* refers to the IP address and *y* refers to the subnet mask. The subnet mask can be a value from 0 to 32.

d) Click +.

Repeat Step c and Step d to exclude multiple subnets from the Discovery job.

e) (Optional) In the **CDP Level** field, enter the number of hops from the seed device that you want to scan.

Valid values are from 1 to 16. The default value is 16. For example, CDP level 3 means that CDP will scan up to three hops from the seed device.

f) For **Preferred Management IP**, choose one of the following options:

- **None**: Allows the device to use any of its IP addresses.
- **Use Loopback IP**: Specify the device's loopback interface IP address.

Note If you choose **Use Loopback IP** and the device does not have a loopback interface, Cisco DNA Center chooses a management IP address using the logic described in Preferred Management IP Address, on page 25.

Note To use the loopback interface IP address as the preferred management IP address, make sure that the CDP neighbor's IP address is reachable from Cisco DNA Center.

Step 5 Expand the **Credentials** area and configure the credentials that you want to use for the Discovery job.

Choose any of the global credentials that have already been created or configure your own Discovery credentials. If you configure your own credentials, you can save them only for the current job by clicking **Save** or you can save them for the current and future jobs by checking the **Save as global settings** check box and then clicking **Save**.

a) Make sure that the global credentials that you want to use are selected. If you do not want to use a credential, deselect it.
b) To add additional credentials, click **Add Credentials**.
c) To configure CLI credentials, configure the following fields:

Table 2: CLI Credentials

Field	Description
Name/Description	Name or phrase that describes the CLI credentials.
Username	Name that is used to log in to the CLI of the devices in your network.
Password	Password that is used to log in to the CLI of the devices in your network. For security reasons, re-enter the password as confirmation. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Enable Password	Password used to move to a higher privilege level in the CLI. Configure this password only if your network devices require it. For security reasons, re-enter the enable password. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

d) Click **SNMP v2c** and configure the following fields:

Table 3: SNMPv2c Credentials

Field	Description
Read	• **Name/Description**: Name or description of the SNMPv2c settings that you are adding. • **Read Community**: Read-only community string password used only to view SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Write	• **Name/Description**: Name or description of the SNMPv2c settings that you are adding. • **Write Community**: Write community string used to make changes to the SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

e) (Optional) Click **SNMP v3** and configure the following fields:

Table 4: SNMPv3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Choose one of the following modes: • **noAuthNoPriv**: Does not provide authentication or encryption. • **AuthNoPriv**: Provides authentication, but does not provide encryption. • **AuthPriv**: Provides both authentication and encryption.
Auth Type	Authentication type to be used. (Enabled if you select **AuthPriv** or **AuthNoPriv** as the authentication mode.) Choose one of the following authentication types: • **SHA**: Authentication based on HMAC-SHA. • **MD5**: Authentication based on HMAC-MD5.

Field	Description
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	Privacy type. (Enabled if you select **AuthPriv** as the authentication mode.) Choose one of the following privacy types: • **AES128**: CBC mode AES for encryption. • **None**: No privacy.
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support AES128 encryption. Passwords (or passphrases) must be at least eight characters long. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

f) (Optional) Click **SNMP PROPERTIES** and configure the following fields:

Table 5: SNMP Properties

Field	Description
Retries	Number of times Cisco DNA Center tries to communicate with network devices using SNMP.
Timeout	Number of seconds between retries.

g) (Optional) Click **HTTP(S)** and configure the following fields:

Table 6: HTTP(S) Credentials

Field	Description
Type	Specifies the kind of HTTPS credentials you are configuring. Valid types are **Read** or **Write**.

Field	Description
Read	You can configure up to 10 HTTPS read credentials: • **Name/Description**: Name or description of the HTTPS credentials that you are adding. • **Username**: Name used to authenticate the HTTPS connection. • **Password**: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). The password must contain from 7 to 128 characters, including at least one: • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 9) • Special character: # _ * ? – The password cannot contain spaces or angle brackets (< >). Note that some Cisco IOS XE devices do not allow a question mark (?).
Write	You can configure up to 10 HTTPS write credentials: • **Name/Description**: Name or description of the HTTPS credentials that you are adding. • **Username**: Name used to authenticate the HTTPS connection. • **Password**: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). The password must contain from 7 to 128 characters, including at least one: • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 9) • Special character: # _ * ? – The password cannot contain spaces or angle brackets (< >). Note that some Cisco IOS XE devices do not allow a question mark (?).

h) (Optional) If you have network devices with NETCONF enabled, click **NETCONF** and enter a port number in the **Port** field.

Note You must enable NETCONF and set the port to 830 to discover Cisco Catalyst 9800 Series Wireless Controller devices. NETCONF provides a mechanism to install, manipulate, and delete configurations of network devices. NETCONF will be disabled if you select Telnet in the **Advanced** area.

Step 6 To configure the protocols to be used to connect with devices, expand the **Advanced** area and do the following tasks:

a) Click the names of the protocols that you want to use. A green check mark indicates that the protocol is selected.

Valid protocols are **SSH** (default) and **Telnet**.

b) Drag and drop the protocols in the order that you want them to be used.

Step 7 Click **Discover** and select whether to run the discovery now or schedule the discovery for a later time.

- To run the discovery now, click the **Now** radio button and click **Start**.
- To schedule the discovery for a later time, click the **Later** radio button, define the date and time, and click **Start**.

Click the notifications icon to view the scheduled discovery tasks. Click **Edit** to edit the discovery task before the discovery starts. Click **Cancel** to cancel the scheduled discovery job before it starts.

The **Discoveries** window displays the results of your scan.

The **Discovery Details** pane shows the status (active or inactive) and the Discovery configuration. The **Discovery Devices** pane displays the host names, IP addresses, and status of the discovered devices.

Discover Your Network Using an IP Address Range

You can discover devices using an IP address range, CDP, or LLDP. This procedure shows you how to discover devices and hosts using an IP address range. For more information about the other Discovery methods, see Discover Your Network Using CDP, on page 26 and Discover Your Network Using LLDP, on page 36.

Before you begin

Your devices must have the required device configurations, as described in Discovery Prerequisites, on page 22.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Discovery**.
The **Discovery** window appears with dashlets.

Step 2 Click **Add Discovery**.
The **New Discovery** window appears.

Step 3 In the **Discovery Name** field, enter a name.

Step 4 Expand the **IP Address/Ranges** area, if it is not already visible, and configure the following fields:

a) For **Discovery Type**, click **IP Address/Range**.

b) In the **From** and **To** fields, enter the beginning and ending IP addresses (IP address range) for Cisco DNA Center to scan, and click **+**.

You can enter a single IP address range or multiple IP addresses for the discovery scan.

Note Cisco Wireless Controllers must be discovered using the management IP address instead of the service port IP address. If not, the related wireless controller 360 and AP 360 pages will not display any data.

c) (Optional) Repeat Step b to enter additional IP address ranges.

d) (Optional) In the **Subnet Filter** field, enter an IP address/range or subnet to exclude from the Discovery scan. You can enter addresses either as an individual IP address (*x.x.x.x*) or as a classless inter-domain routing (CIDR) address

(*x.x.x.x/y*), where *x.x.x.x* refers to the IP address and *y* refers to the subnet mask. The subnet mask can be a value from 0 to 32.

e) For **Preferred Management IP Address**, choose one of the following options:

- **None**: Allows the device to use any of its IP addresses.
- **Use Loopback IP**: Specify the device's loopback interface IP address.

Note If you choose **Use Loopback IP** and the device does not have a loopback interface, Cisco DNA Center chooses a management IP address using the logic described in Preferred Management IP Address, on page 25.

Step 5 Expand the **Credentials** area and configure the credentials that you want to use for the Discovery job.

Choose any of the global credentials that have already been created or configure your own Discovery credentials. If you configure your own credentials, you can save them for only the current job by clicking **Save**, or you can save them for the current and future jobs by checking the **Save as global settings** check box and then clicking **Save**.

a) Make sure that the global credentials that you want to use are selected. If you do not want to use a credential, deselect it.

b) To add additional credentials, click **Add Credentials**.

c) To configure CLI credentials, configure the following fields:

Table 7: CLI Credentials

Field	Description
Name/Description	Name or phrase that describes the CLI credentials.
Username	Name that is used to log in to the CLI of the devices in your network.
Password	Password that is used to log in to the CLI of the devices in your network. For security reasons, re-enter the password as confirmation. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Enable Password	Password used to move to a higher privilege level in the CLI. Configure this password only if your network devices require it. For security reasons, re-enter the enable password. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

d) Click **SNMP v2c** and configure the following fields:

Table 8: SNMPv2c Credentials

Field	Description
Read	• **Name/Description**: Name or description of the SNMPv2c settings that you are adding. • **Read Community**: Read-only community string password used only to view SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Write	• **Name/Description**: Name or description of the SNMPv2c settings that you are adding. • **Write Community**: Write community string used to make changes to the SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

e) (Optional) Click **SNMP v3** and configure the following fields:

Table 9: SNMPv3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Choose one of the following modes: • **noAuthNoPriv**: Does not provide authentication or encryption. • **AuthNoPriv**: Provides authentication, but does not provide encryption. • **AuthPriv**: Provides both authentication and encryption.
Auth Type	Authentication type to be used. (Enabled if you select **AuthPriv** or **AuthNoPriv** as the authentication mode.) Choose one of the following authentication types: • **SHA**: Authentication based on HMAC-SHA. • **MD5**: Authentication based on HMAC-MD5.

Field	Description
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	Privacy type. (Enabled if you select **AuthPriv** as the authentication mode.) Choose one of the following privacy types: • **AES128**: CBC mode AES for encryption. • **None**: No privacy.
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support AES128 encryption. Passwords (or passphrases) must be at least eight characters long. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

f) (Optional) Click **SNMP PROPERTIES** and configure the following fields:

Table 10: SNMP Properties

Field	Description
Retries	Number of times Cisco DNA Center tries to communicate with network devices using SNMP.
Timeout	Number of seconds between retries.

g) (Optional) Click **HTTP(S)** and configure the following fields:

Table 11: HTTP(S) Credentials

Field	Description
Type	Specifies the kind of HTTPS credentials you are configuring. Valid types are **Read** or **Write**.

Field	Description
Read	You can configure up to 10 HTTPS read credentials: • **Name/Description**: Name or description of the HTTPS credentials that you are adding. • **Username**: Name used to authenticate the HTTPS connection. • **Password**: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). The password must contain from 7 to 128 characters, including at least one: • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 9) • Special character: # _ * ? – The password cannot contain spaces or angle brackets (< >). Note that some Cisco IOS XE devices do not allow a question mark (?).
Write	You can configure up to 10 HTTPS write credentials: • **Name/Description**: Name or description of the HTTPS credentials that you are adding. • **Username**: Name used to authenticate the HTTPS connection. • **Password**: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). The password must contain from 7 to 128 characters, including at least one: • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 9) • Special character: # _ * ? – The password cannot contain spaces or angle brackets (< >). Note that some Cisco IOS XE devices do not allow a question mark (?).

h) (Optional) If you have network devices with NETCONF enabled, click **NETCONF** and enter a port number in the **Port** field.

Note You must enable NETCONF and set the port to 830 to discover Cisco Catalyst 9800 Series Wireless Controller devices. NETCONF provides a mechanism to install, manipulate, and delete configurations of network devices.

Step 6 (Optional) To configure the protocols that are to be used to connect with devices, expand the **Advanced** area and do the following tasks:

a) Click the protocols that you want to use. A green check mark indicates that the protocol is selected.

Valid protocols are **SSH** (default) and **Telnet**.

b) Drag and drop the protocols in the order that you want them to be used.

Step 7 Click **Discover** and select whether to run the discovery now or schedule the discovery for a later time.

- To run the discovery now, click the **Now** radio button and click **Start**.
- To schedule the discovery for a later time, click the **Later** radio button, define the date and time, and click **Start**.

Click the notifications icon to view the scheduled discovery tasks. Click **Edit** to edit the discovery task before the discovery starts. Click **Cancel** if you want to cancel the scheduled discovery job before it starts.

The **Discoveries** window displays the results of your scan.

The **Discovery Details** pane shows the status (active or inactive) and the Discovery configuration. The **Discovery Devices** pane displays the host names, IP addresses, and status of the discovered devices.

Discover Your Network Using LLDP

You can discover devices using Link Layer Discovery Protocol (LLDP), CDP, or an IP address range. This procedure shows you how to discover devices and hosts using LLDP. For more information about the other discovery methods, see Discover Your Network Using CDP, on page 26 and Discover Your Network Using an IP Address Range, on page 31.

Note

- The Discovery function requires the correct SNMP Read Only (RO) community string. If an SNMP RO community string is not provided, as a *best effort*, the Discovery function uses the default SNMP RO community string, public.
- CLI credentials are not required to discover hosts; hosts are discovered through the network devices to which they are connected.

Before you begin

- Enable LLDP on your network devices.
- Configure your network devices, as described in Discovery Prerequisites, on page 22.
- Configure your network device's host IP address as the client IP address. (A host is an end-user device, such as a laptop computer or mobile device.)

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Discovery**.
The **Discovery** window appears with dashlets.

Step 2 Click **Add Discovery**.
The **New Discovery** window appears.

Step 3 In the **Discovery Name** field, enter a name.

Step 4 Expand the **IP Address/Range** area and configure the following fields:

a) For **Discovery Type**, click **LLDP**.

b) In the **IP Address** field, enter a seed IP address for Cisco DNA Center to start the Discovery scan.

c) (Optional) In the **Subnet Filter** field, enter an IP address or subnet to exclude from the Discovery scan.

You can enter addresses either as an individual IP address (*x.x.x.x*) or as a classless inter-domain routing (CIDR) address (*x.x.x.x/y*), where *x.x.x.x* refers to the IP address and *y* refers to the subnet mask. The subnet mask can be a value from 0 to 32.

d) Click +.

Repeat Step c and Step d to exclude multiple subnets from the Discovery job.

e) (Optional) In the **LLDP Level** field, enter the number of hops from the seed device that you want to scan.

Valid values are from 1 to 16. The default value is 16. For example, LLDP level 3 means that LLDP will scan up to three hops from the seed device.

f) For **Preferred Management IP**, choose one of the following options:

- **None**: Allows the device use any of its IP addresses.
- **Use Loopback IP**: Specify the device's loopback interface IP address.

Note If you choose this option and the device does not have a loopback interface, Cisco DNA Center chooses a management IP address using the logic described in Preferred Management IP Address, on page 25.

Note To use the loopback interface IP address as the preferred management IP address, make sure that the LLDP neighbor's IP address is reachable from Cisco DNA Center.

Step 5 Expand the **Credentials** area and configure the credentials that you want to use for the Discovery job.

Choose any of the global credentials that have already been created, or configure your own Discovery credentials. If you configure the credentials, you can choose to save them for future jobs by checking the **Save as global settings** check box.

a) Make sure that the global credentials that you want to use are selected. If you do not want to use a credential, deselect it.

b) To add additional credentials, click **Add Credentials**.

c) For CLI credentials, configure the following fields:

Table 12: CLI Credentials

Field	Description
Name/Description	Name or phrase that describes the CLI credentials.
Username	Name that is used to log in to the CLI of the devices in your network.
Password	Password that is used to log in to the CLI of the devices in your network. For security reasons, re-enter the password as confirmation. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

Field	Description
Enable Password	Password used to move to a higher privilege level in the CLI. Configure this password only if your network devices require it. For security reasons, re-enter the enable password. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

d) Click **SNMP v2c** and configure the following fields:

Table 13: SNMPv2c Credentials

Field	Description
Read	• **Name/Description**: Name or description of the SNMPv2c settings that you are adding. • **Read Community**: Read-only community string password used only to view SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Write	• **Name/Description**: Name or description of the SNMPv2c settings that you are adding. • **Write Community**: Write community string used to make changes to the SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

e) (Optional) Click **SNMP v3** and configure the following fields:

Table 14: SNMPv3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Choose one of the following modes: • **noAuthNoPriv**: Does not provide authentication or encryption. • **AuthNoPriv**: Provides authentication, but does not provide encryption. • **AuthPriv**: Provides both authentication and encryption.

Field	Description
Auth Type	Authentication type to be used. (Enabled if you select **AuthPriv** or **AuthNoPriv** as the authentication mode.) Choose one of the following authentication types: • **SHA**: Authentication based on HMAC-SHA. • **MD5**: Authentication based on HMAC-MD5.
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	Privacy type. (Enabled if you select **AuthPriv** as the authentication mode.) Choose one of the following privacy types: • **AES128**: CBC mode AES for encryption. • **None**: No privacy.
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support AES128 encryption. Passwords (or passphrases) must be at least eight characters long. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

f) (Optional) Click **SNMP PROPERTIES** and configure the following fields:

Table 15: SNMP Properties

Field	Description
Retries	Number of times Cisco DNA Center tries to communicate with network devices using SNMP.
Timeout	Number of seconds between retries.

g) (Optional) Click **HTTP(S)** and configure the following fields:

Table 16: HTTP(S) Credentials

Field	Description
Type	Specifies the kind of HTTPS credentials you are configuring. Valid types are **Read** or **Write**.
Read	You can configure up to 10 HTTPS read credentials: • **Name/Description**: Name or description of the HTTPS credentials that you are adding. • **Username**: Name used to authenticate the HTTPS connection. • **Password**: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). The password must contain from 7 to 128 characters, including at least one: • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 9) • Special character: # _ * ? – The password cannot contain spaces or angle brackets (< >). Note that some Cisco IOS XE devices do not allow a question mark (?).
Write	You can configure up to 10 HTTPS write credentials: • **Name/Description**: Name or description of the HTTPS credentials that you are adding. • **Username**: Name used to authenticate the HTTPS connection. • **Password**: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). The password must contain from 7 to 128 characters, including at least one: • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 9) • Special character: # _ * ? – The password cannot contain spaces or angle brackets (< >). Note that some Cisco IOS XE devices do not allow a question mark (?).

Step 6 (Optional) To configure the protocols to be used to connect with devices, expand the **Advanced** area and do the following tasks:

a) Click the names of the protocols that you want to use. A green check mark indicates that the protocol is selected. Valid protocols are **SSH** (default) and **Telnet**.
b) Drag and drop the protocols in the order that you want them to be used.

Step 7 Click **Discover** and select whether to run the discovery now or schedule the discovery for a later time.

- To run the discovery now, click the **Now** radio button and click **Start**.
- To schedule the discovery for a later time, click the **Later** radio button, define the date and time, and click **Start**.

Click the notifications icon to view the scheduled discovery tasks. Click **Edit** to edit the discovery task before the discovery starts. Click **Cancel** if you want to cancel the scheduled discovery job before it starts.

The **Discoveries** window displays the results of your scan.

The **Discovery Details** pane shows the status (active or inactive) and the Discovery configuration. The **Discovery Devices** pane displays the host names, IP addresses, and status of the discovered devices.

Manage Discovery Jobs

Stop and Start a Discovery Job

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Discovery**. The **Discovery** window appears with dashlets.

Step 2 Click **View All Discoveries**.

Step 3 To stop an active Discovery job, perform these steps:

a) From the **Discoveries** pane, select the corresponding job.
b) Click **Stop**.

Step 4 To restart an inactive Discovery job, perform these steps:

a) From the **Discoveries** pane, select the corresponding job.
b) Click **Re-discover** to restart the selected job.

Edit a Discovery Job

You can edit an existing Discovery job and then rerun the Discovery job.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Discovery**. The **Discovery** window appears with dashlets.

Step 2 Click **View All Discoveries**.

Step 3 From the **Discoveries** pane, select the Discovery job.

Step 4 Click **Edit**.

Step 5 Depending on the Discovery type, you can change the type of job, except for the following fields:

- **CDP**: Discovery name, Discovery type, IP address. For more information about the fields you can change, see Discover Your Network Using CDP, on page 26.
- **IP Range**: Discovery name, type, IP address range (although you can add additional IP address ranges). For more information about the fields you can change, see Discover Your Network Using an IP Address Range, on page 31.
- **LLDP**: Discovery name, type, IP address. For more information about the fields you can change, see Discover Your Network Using LLDP, on page 36.

Step 6 Click **Start**.

Change Credentials in a Discovery Job

You can change the credentials used in a Discovery job and then re-run the Discovery job.

Before you begin

You should have created at least one Discovery job.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Discovery**.
The **Discovery** window appears with dashlets.

Step 2 Click **View All Discoveries**.

Step 3 From the **Discoveries** pane, select the Discovery job.

Step 4 Click **Edit**.

Step 5 Expand the **Credentials** area.

Step 6 Deselect the credentials that you do not want to use.

Step 7 Configure the credentials that you want to use:

a) Click **Add Credentials**.

b) To configure CLI credentials, configure the following fields:

Table 17: CLI Credentials

Field	Description
Name/Description	Name or phrase that describes the CLI credentials.
Username	Name that is used to log in to the CLI of the devices in your network.
Password	Password that is used to log in to the CLI of the devices in your network. For security reasons, re-enter the password as confirmation. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

Field	Description
Enable Password	Password used to move to a higher privilege level in the CLI. Configure this password only if your network devices require it. For security reasons, re-enter the enable password. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

c) Click **SNMP v2c** and configure the following fields:

Table 18: SNMPv2c Credentials

Field	Description
Read	• **Name/Description**: Name or description of the SNMPv2c settings that you are adding. • **Read Community**: Read-only community string password used only to view SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Write	• **Name/Description**: Name or description of the SNMPv2c settings that you are adding. • **Write Community**: Write community string used to make changes to the SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

d) (Optional) Click **SNMP v3** and configure the following fields:

Table 19: SNMPv3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Choose one of the following modes: • **noAuthNoPriv**: Does not provide authentication or encryption. • **AuthNoPriv**: Provides authentication, but does not provide encryption. • **AuthPriv**: Provides both authentication and encryption.

Field	Description
Auth Type	Authentication type to be used. (Enabled if you select **AuthPriv** or **AuthNoPriv** as the authentication mode.) Choose one of the following authentication types: • **SHA**: Authentication based on HMAC-SHA. • **MD5**: Authentication based on HMAC-MD5.
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	Privacy type. (Enabled if you select **AuthPriv** as the authentication mode.) Choose one of the following privacy types: • **AES128**: CBC mode AES for encryption. • **None**: No privacy.
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support AES128 encryption. Passwords (or passphrases) must be at least eight characters long. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 8 Click **Start**.

Clone a Discovery Job

You can clone a Discovery job and retain all of the information defined for that job.

Before you begin

You should have run at least one Discovery job.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Discovery**. The **Discovery** window appears with dashlets.

Step 2 Click **View All Discoveries**.

Step 3 From the **Discoveries** pane, select the Discovery job.

Step 4 Click **Copy & Edit**.

Cisco DNA Center creates a copy of the Discovery job, named Copy of *Discovery_Job*.

Step 5 (Optional) Change the name of the Discovery job.

Step 6 Define or update the parameters for the new Discovery job.

Delete a Discovery Job

You can delete a Discovery job whether it is active or inactive.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Discovery**. The **Discovery** window appears with dashlets.

Step 2 Click **View All Discoveries**.

Step 3 From the **Discoveries** pane, select the Discovery job that you want to delete.

Step 4 Click **Delete**.

Step 5 Click **OK** to confirm.

View Discovery Job Information

You can view information about a Discovery job, such as the settings and credentials that were used. You also can view the historical information about each Discovery job that was run, including information about the specific devices that were discovered or that failed to be discovered.

Before you begin

Run at least one Discovery job.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Discovery**. The **Discovery** window appears with dashlets.

Step 2 Click **View All Discoveries**.

Step 3 From the **Discoveries** pane, select the Discovery job. Alternatively, use the **Search** function to find a Discovery job by device IP address or name.

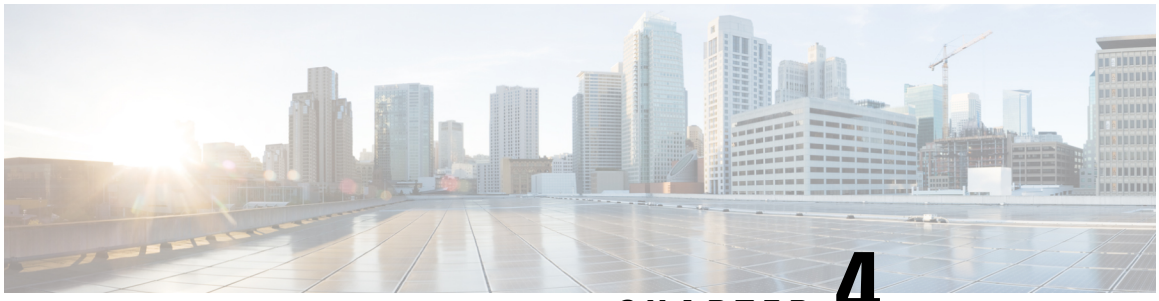
Step 4 Click the down arrow next to one of the following areas for more information:

- **Discovery Details**: Displays the parameters that were used to run the Discovery job. Parameters include attributes such as the CDP or LLDP level, IP address range, and protocol order.
- **Credentials**: Provides the names of the credentials that were used.

- **History**: Lists each Discovery job that was run, including the time when the job started, and whether any devices were discovered.

  To successfully discover embedded wireless controllers, the NETCONF port must be configured. If the NETCONF port is not configured, wireless data is not collected.

  Use the **Filter** function to display devices by any combination of IP addresses or ICMP, CLI, HTTPS, or NETCONF values.



CHAPTER 4

Manage Your Inventory

About Inventory

The Inventory function retrieves and saves details, such as host IP addresses, MAC addresses, and network attachment points about devices in its database.

The Inventory feature can also work with the Device Controllability feature to configure the required network settings on devices, if these settings are not already present on the device.

Inventory uses the following protocols, as required:

- Link Layer Discovery Protocol (LLDP).
- IP Device Tracking (IPDT) or Switch Integrated Security Features (SISF). (IPDT or SISF must be enabled on the device.)

- LLDP Media End-point Discovery. (This protocol is used to discover IP phones and some servers.)
- Network Configuration Protocol (NETCONF). For a list of devices, see Discovery Prerequisites, on page 22.

After the initial discovery, Cisco DNA Center maintains the inventory by polling the devices at regular intervals. The default interval is every 24 hours. However, you can change this interval as required for your network environment. For more information, see Update the Device Polling Interval, on page 77. Also, a configuration change in the device triggers an SNMP trap, which in turn triggers device resynchronization. Polling occurs for each device, link, host, and interface. Only the devices that have been active for less than one day are displayed. This prevents stale device data, if any, from being displayed. On average, polling 500 devices takes approximately 20 minutes.

Inventory and Cisco ISE Authentication

Cisco ISE has two different use cases in Cisco DNA Center:

- If your network uses Cisco ISE for device authentication, you need to configure the Cisco ISE settings in Cisco DNA Center. As a result, when provisioning devices, Cisco DNA Center configures the devices with the Cisco ISE server information that you defined. In addition, Cisco DNA Center configures the devices on the Cisco ISE server and propagates subsequent updates to the devices. For information about configuring Cisco ISE settings in Cisco DNA Center, see Configure Global Network Servers, on page 189.

Note If you are using Cisco ISE for authenticating Cisco Catalyst 9800 series devices, you must configure Cisco ISE to provide privilege for NETCONF users.

If a device is not configured or updated on the Cisco ISE server as expected due to a network failure or the Cisco ISE server being down, Cisco DNA Center automatically retries the operation after a certain wait period. However, Cisco DNA Center does not retry the operation if the failure is due to a rejection from Cisco ISE, as an input validation error.

When Cisco DNA Center configures and updates devices in the Cisco ISE server, the transactions are captured in the Cisco DNA Center audit logs. You can use the audit logs to help troubleshoot issues related to the Cisco DNA Center and Cisco ISE inventories.

After you provision a device, Cisco DNA Center authenticates the device with Cisco ISE. If Cisco ISE is not reachable (no RADIUS response), the device uses the local login credentials. If Cisco ISE is reachable, but the device does not exist in Cisco ISE or its credentials do not match the credentials configured in Cisco DNA Center, the device does not fall back to use the local login credentials. Instead, it goes into a partial collection state.

To avoid this situation, make sure that before you provision devices using Cisco DNA Center, you have configured the devices in Cisco ISE with the same device credentials that you are using in Cisco DNA Center. Also, make sure that you configured valid discovery credentials. For more information, see Discovery Credentials, on page 23.

- If required, you can use Cisco ISE to enforce access control to groups of devices.

Display Information About Your Inventory

The **Inventory** table displays information for each discovered device. Click the column header to sort the rows in ascending order. Click the column header again to sort the rows in descending order.

To select which columns to show or hide in the table, click . Note that the column selection does not persist across sessions.

The device selection persists across views. When devices are selected and you choose a different view from the **Focus** drop-down list, the selection persists in the new view.

By default, 25 entries are shown in the **Inventory** table. Click **Show More** to view more entries. You can view up to 200 entries in the **Inventory** table.

The number of entries that are shown in the **Inventory** table persists across views. If there are more than 25 entries in the **Inventory** table and you choose a different view from the **Focus** drop-down list, the same number of entries persists in the new view.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Provision** > **Inventory**.

The **Inventory** window displays the device information gathered during the discovery process. The following table describes the information that is available.

Table 20: Inventory

Column	Description
Device Name	

Column	Description
	Name of the device. Click the device name to view the following device details: **Details**: Displays details such as device name, reachability status, manageability status, IP address, device model, role, uptime, site, and so on. • **View Assurance 360**: Displays the Assurance 360 window. For 360 to open, you must have installed the Assurance application. • **Interfaces** • **Ethernet Ports** (For all devices): Displays the operational status and administrative status of the Ethernet ports. For Cisco Catalyst 4000 Series, 6000 Series, and 9000 Series Switches and Aggregation Services Routers (ASR) 1000 Series Routers, the ports view displays the details of line cards and supervisor cards if they are available. The line card includes the details of platform, address, serial number, role, and stack member number. The supervisor card includes the details of part number, serial number, switch number, and slot number. The Ports table displays the operational status, admin status, type, MAC address, PoE status, speed, and MTU. The table also displays the ID of the following types of VLANs: • VLAN ID of the manufacturing-supplied default VLAN • VLAN ID of the configured default VLAN • VLAN ID of the configured VLAN For Cisco Catalyst 2000, 3000, and 9000 Series Switches, click either a port in the ports view or click the port name in the Ports table to view the maximum allocated power, allocated power, and power drawn details of the port. • **VLANs** (Only for switches and hubs): The VLAN table displays the operational status, admin status, VLAN type, and IP address. The table also displays the ID of the following types of VLANs: • VLAN ID of the manufacturing-supplied default VLAN • VLAN ID of the configured default VLAN • VLAN ID of the configured VLAN You can click the Search or Filter option to view the details of the desired VLAN. • **Virtual Ports** (Only for wireless devices, controllers, and routers): The ports table displays the operational status, admin status, type, MAC address, PoE status, speed, and MTU. You can click the Search or Filter option to view the details of the desired ports. • **Hardware and Software**: Displays the hardware and software details of the device. • **Configuration**: Displays detailed configuration information, similar to what is

Column	Description
	displayed in the output of the **show running-config** command. This feature is not supported for access points (APs) and wireless controllers. Therefore, configuration data is not returned for these device types. • **Power**: Displays details about the power budgeted for, power consumed by, and power remaining for the device. The Power Supplies table shows the operational status, serial number, and vendor equipment type details. • **Fans**: Displays the operational status, serial number, and vendor equipment type of fans. • **User Defined Fields**: Displays the user-defined fields associated with the device. • **Config Drift**: Displays the configuration changes and allows you to pick any two versions of the same device and compare their running configuration data. **Note** Running configuration data is not supported for devices such as wireless or legacy controllers. • **Wireless Info**: Displays the primary and secondary managed locations. • **Mobility**: Displays the mobility group name, RF group name, virtual IP, and mobility MAC address. **Note** A device name that is displayed in red means that inventory has not polled the device and updated its information for more than 30 minutes.
IP Address	IP address of the device.
Support Type	Shows the device support level as follows: • **Supported**: The device pack is tested for all applications on Cisco DNA Center. You can open a service request if any of the Cisco DNA Center functionalities for these devices do not work. • **Unsupported**: All remaining Cisco and third-party devices that are not tested and certified on Cisco DNA Center. You may try out various functionalities on Cisco DNA Center for these devices, as a best effort. However, we do not expect you to raise a service request or a bug if Cisco DNA Center features do not work as expected. • **Third Party**: Device pack is built by customers or business partners and goes through the certification process. Third party devices will support base automation capabilities such as Discovery, Inventory, Topology, and so on. Cisco TAC provides an initial level of support for these devices. However, if there is a problem with the device pack, you need to contact the business partner.

Column	Description
Reachability	The following is a list of the various statuses: • **Reachable**: The device is reachable by Cisco DNA Center using SNMP, HTTP(S), and NETCONF poll mechanisms. • **Ping Reachable**: The device is reachable by Cisco DNA Center using ICMP polling mechanism and not reachable using SNMP, HTTP(S), and Netconf poll mechanisms. • **Unreachable**: The device is not reachable using SNMP, HTTP(S), Netconf, and ICMP poll mechanisms.
Manageability	Shows the device status as follows: • **Managed with green tick icon**: Device is reachable and is fully managed. • **Managed with orange error icon**: Device is managed with some error such as unreachable, authentication failure, missing Netconf ports, internal error, and so on. You can hover the cursor over the error message to view more details about the error and the impacted applications. • **Unmanaged**: Device cannot be reached and no inventory information was collected due to device connectivity issues.
MAC Address	MAC address of the device.
Image Version	Cisco IOS software that is currently running on the device.
Platform	Cisco product part number.
Serial Number	Cisco device serial number.
Uptime	Period of time that the device has been up and running.
Device Role	Role assigned to each discovered device during the scan process. The device role is used to identify and group devices according to their responsibilities and placement within the network. If Cisco DNA Center is unable to determine a device role, it sets the device role to Unknown. **Note** If you manually change the device role, the assignment remains static. Cisco DNA Center does not update the device role even if it detects a change during a subsequent device resynchronization. If required, you can use the drop-down list in this column to change the assigned device role. The following device roles are available: • **Unknown** • **Access** • **Core** • **Distribution** • **Border Router**

Column	Description
Site	The site to which the device is assigned. Click **Assign** if the device is not assigned to any site. Click **Choose a Site**, select a site from the hierarchy, and click **Save**. For more information, see About Network Hierarchy, on page 110.
Last Updated	Most recent date and time that Cisco DNA Center scanned the device and updated the database with new information about the device.
Device Family	Group of related devices, such as routers, switches, hubs, or wireless controllers.
Device Series	Series number of the device; for example, Cisco Catalyst 4500 Series Switches.
Resync Interval	The polling interval for the device. This interval can be set globally in Settings or for a specific device in Inventory. For more information, see Cisco DNA Center Administrator Guide.
Last Sync Status	Status of the last Discovery scan for the device: • **Managed**: Device is in a fully managed state. • **Partial Collection Failure**: Device is in a partial collected state and not all the inventory information has been collected. Hover the cursor over the **Information (i)** icon to display additional information about the failure. • **Unreachable**: Device cannot be reached and no inventory information was collected due to device connectivity issues. This condition occurs when periodic collection takes place. • **Wrong Credentials**: If device credentials are changed after adding the device to the inventory, this condition is noted. • **In Progress**: Inventory collection is occurring.

Manage User-Defined Fields

User-defined fields are custom labels that you can create and assign to any device in Cisco DNA Center. These labels allow you to display more details about the device in the device details page. For a user-defined field to be displayed, you must assign it to a device and add a value to it.

Create User-Defined Fields

Cisco DNA Center allows you to create user-defined fields and assign them to any device.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The **Inventory** page displays the device information that is gathered during the discovery process.

Step 2 From the **Actions** drop-down list, choose **Provision** > **Inventory** > **Manage User Defined Fields**.

Step 3 In the **Manage User Defined Fields** dialog box, click **Create New Field**.

Step 4 In the **Create New Field** dialog box, enter a name and description for user-defined field in the **Field Name** and **Field Description** fields.

Note You can add device details that are not already present in the device details page, such as customer IP address and customer device name, in user-defined fields.

Step 5 Click **Save**.

Similarly, you can create more user-defined fields. The user-defined fields appear in a table.

Step 6 If you want to edit a user-defined field, click the corresponding edit icon, make the required changes, and click **Save**.

Step 7 If you want to delete a user-defined field, click the corresponding delete icon and click **Yes** in the subsequent warning message.

Add User-Defined Fields to a Device

Before you begin

You must have created at least one user-defined field in the **Manage User Defined Fields** page. See Create User-Defined Fields, on page 54

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The **Inventory** page displays the device information that is gathered during the discovery process.

Step 2 Click the name of a device for which you want to add user-defined fields.

Step 3 In the left pane, click **User Defined Fields**.

Step 4 Click **Add**.

Step 5 Choose a user-defined filed in the **Field Name** drop-down list and enter its value in the **Value** Field.

For example, if you have created user-defined field for customer IP address, choose it in the **Field Name** drop-down list, and enter the customer IP address in the **Value** filed.

Step 6 If you want to remove a user-defined field from the device, click the corresponding delete icon.

Step 7 Click **Save**.

Launch Topology Map from Inventory

You can launch the Topology map for the discovered devices from the Inventory window.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provisioning** > **Inventory**.

Step 2 Use the Toggle button  to switch between the Topology map view and the Inventory view. The Topology map view displays the topology and the provisioning status of the device. Click on each node to view the device details. See About Topology for more information on Topology map.

Note Click **Collapse All** or **Expand All** to collapse and expand the Topology map view.

Types of Devices in the Cisco DNA Center Inventory

Devices show up in inventory one of two ways: by being discovered or by being added manually. Cisco DNA Center Inventory supports the following types of devices:

- **Network Devices**: Supported network devices include Cisco routers, switches, and wireless devices such as wireless controllers (WLCs) and access points (APs).
- **Compute Devices**: Supported compute devices include the Cisco Unified Computing System (UCS), devices running Cisco Enterprise Network Functions Virtualization Infrastructure Software (NFVIS), and other data center devices.
- **Meraki Dashboard**: Dashboard to the Cisco cloud management platform for managing Cisco Meraki products.
- **Firepower Management Center (FMC)**: Provides complete and unified management over Firepower Threat Defense (FTD) devices for managing Cisco network security solutions.

For a complete list of supported devices, see Cisco DNA Center Supported Devices.

Manage Network Devices

Add a Network Device

You can add a network device to your inventory manually.

Before you begin

Make sure you configure your network device. For more information, see Discovery Prerequisites, on page 22.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The Inventory page displays the device information that is gathered during the Discovery process.

Step 2 Click **Add Device**.

Step 3 From the **Type** drop-down list, choose **Network Device**.

Step 4 In the **Device IP / DNS Name** field, enter the IP address or name of the device.

Note If the device uses HSRP protocol, you must enter the primary IP address and not the virtual IP address.

Step 5 Expand the **CLI** area, if it is not already expanded, and do one of the following:

a) Click the **Select global credential** radio button if you want to use the global CLI credentials that have been already created.

Note If no CLI global credentials are available, create the global CLI credentials in the **Network Settings > Device Credentials** page. See Configure Global CLI Credentials.

b) Click the **Add device specific credential** radio button and configure the following fields:

Table 21: CLI Credentials

Field	Description
Username	Name that is used to log in to the CLI of the devices in your network.
Password	Password that is used to log in to the CLI of the devices in your network. For security reasons, re-enter the password as confirmation. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Enable Password	Password used to move to a higher privilege level in the CLI. For security reasons, re-enter the enable password. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 6 Expand the **SNMP** area, if it is not already visible and do one of the following:

a) Click the **Select global credential** radio button if you want to use the global SNMP credentials that have been already created.

Note If no SNMP global credentials are available, create the global SNMP credentials in the **Network Settings > Device Credentials** page. See Configure Global SNMPv2c Credentials and Configure Global SNMPv3 Credentials.

b) Click the **Add device specific credential** radio button and do the following:

Step 7 From the **Version** drop-down list, choose **V2C** (SNMP Version 2c) or **V3** (SNMP Version 3).

If you chose **V2C**, configure the following fields:

Table 22: SNMPv2c Credentials

Field	Description
Read	• **Name/Description**: Name or description of the SNMPv2c settings that you are adding. • **Read Community**: Read-only community string password used only to view SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

Field	Description
Write	• **Name/Description**: Name or description of the SNMPv2c settings that you are adding. • **Write Community**: Write community string used to make changes to the SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

If you chose **V3**, configure the following fields:

Table 23: SNMPv3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Choose one of the following modes: • **noAuthNoPriv**: Does not provide authentication or encryption. • **AuthNoPriv**: Provides authentication, but does not provide encryption. • **AuthPriv**: Provides both authentication and encryption.
Auth Type	Authentication type to be used. (Enabled if you select **AuthPriv** or **AuthNoPriv** as the authentication mode.) Choose one of the following authentication types: • **SHA**: Authentication based on HMAC-SHA. • **MD5**: Authentication based on HMAC-MD5.
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	Privacy type. (Enabled if you select **AuthPriv** as the authentication mode.) Choose one of the following privacy types: • **AES128**: CBC mode AES for encryption. • **None**: No privacy.

Field	Description
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support AES128 encryption. Passwords (or passphrases) must be at least eight characters long. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 8 Expand the **SNMP RETRIES AND TIMEOUT** area, if it is not already expanded, and configure the following fields.

Table 24: SNMP Properties

Field	Description
Retries	Number of attempts allowed to connect to the device. Valid values are from 1 to 3. The default is 3.
Timeout	Number of seconds Cisco DNA Center waits when trying to establish a connection with a device before timing out. Valid values are from 1 to 300 seconds in intervals of 5 seconds. The default is 5 seconds.

Step 9 Expand the **HTTP(S)** area, if it is not already visible, and do one of the following:

a) Click the **Select global credential** radio button if you want to use the global HTTP(S) credentials that have been already created.

Note If no HTTP(S) global credentials are available, create the global HTTP(S) credentials in the **Network Settings > Device Credentials** page. See Configure Global HTTPS Credentials.

b) Click the **Add device specific credential** radio button and configure the following fields:

Table 25: HTTP(S)

Field	Description
Username	Name that is used to log in to the HTTP(S) of the devices in your network.
Password	Password that is used to log in to the HTTP(S) of the devices in your network. For security reasons, re-enter the password as confirmation. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Port	Specify the required http(s) port number.

Step 10 Expand the **NETCONF** area, if it is not already expanded, and configure the **Port** field.

NETCONF requires that you configure SSH as the CLI protocol and define the SSH credentials.

Step 11 Select one of the network **Protocol** radio button that enables Cisco DNA Center to communicate with remote devices. Valid values are **SSH2** or **Telnet**.

Step 12 (Optional) Click **Validate** next to **Credentials**. Cisco DNA Center validates the device credentials and shows valid credentials with a green tick mark and invalid credentials with a red cross mark.

All the credentials will be validated except the SNMP Write credentials.

Step 13 Click **Add**.

Update Network Device Credentials

You can update the discovery credentials of selected network devices. The updated settings override the global and job-specific settings for the selected devices.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The Inventory page displays the device information gathered during the Discovery process.

Step 2 Select the network devices that you want to update.

Step 3 From the **Actions** drop-down list, choose **Inventory** > **Edit Device**.

Step 4 In the **Edit Device** dialog box, choose **Network Device** from the **Type** drop-down field, if it is not already selected.

Step 5 Expand the **CLI** area, if it is not already expanded, and do one of the following:

a) If you want to use the global CLI credentials that have been already created, click the **Select global credential** radio button.

Note If no CLI global credentials are available, create them in the **Network Settings** > **Device Credentials** page. See Configure Global CLI Credentials.

b) Click the **Edit device specific credential** radio button and configure the following fields:

Table 26: CLI Credentials

Field	Description
Username	Name that is used to log in to the CLI of the devices in your network.
Password	Password that is used to log in to the CLI of the devices in your network. For security reasons, re-enter the password as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.

Field	Description
Enable Password	Password that is used to move to a higher privilege level in the CLI. For security reasons, re-enter the enable password. Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 6 Expand the **SNMP** area, if it is not already expanded, and do one of the following:

a) If you want to use the global SNMP credentials that have been already created, click the **Select global credential** radio button.

Note If no SNMP global credentials are available, create them in the **Network Settings** > **Device Credentials** page. See Configure Global SNMPv2c Credentials and Configure Global SNMPv3 Credentials.

b) Click the **Edit device specific credential** radio button and do the following:

Step 7 From the **Version** drop-down list, choose **V2C** (SNMP Version 2c) or **V3** (SNMP Version 3).

If you chose **V2C**, configure the following fields:

Table 27: SNMPv2c Credentials

Field	Description
Read	• **Name/Description**: Name or description of the SNMPv2c settings that you are adding. • **Read Community**: Read-only community string password used only to view SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Write	• **Name/Description**: Name or description of the SNMPv2c settings that you are adding. • **Write Community**: Write community string used to make changes to the SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

If you chose **V3**, configure the following fields:

Table 28: SNMPv3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.

Field	Description
Mode	Security level that an SNMP message requires. Choose one of the following modes: • **noAuthNoPriv**: Does not provide authentication or encryption. • **AuthNoPriv**: Provides authentication, but does not provide encryption. • **AuthPriv**: Provides both authentication and encryption.
Auth Type	Authentication type to be used. (Enabled if you select **AuthPriv** or **AuthNoPriv** as the authentication mode.) Choose one of the following authentication types: • **SHA**: Authentication based on HMAC-SHA. • **MD5**: Authentication based on HMAC-MD5.
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	Privacy type. (Enabled if you select **AuthPriv** as the authentication mode.) Choose one of the following privacy types: • **AES128**: CBC mode AES for encryption. • **None**: No privacy.
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support AES128 encryption. Passwords (or passphrases) must be at least eight characters long. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 8 Expand the **SNMP RETRIES AND TIMEOUT** area, if it is not already expanded, and configure the following fields.

Table 29: SNMP Properties

Field	Description
Retries	Number of attempts allowed to connect to the device. Valid values are from 1 to 3. The default is 3.
Timeout	Number of seconds Cisco DNA Center waits when trying to establish a connection with a device before timing out. Valid values are from 1 to 300 seconds in intervals of 5 seconds. The default is 5 seconds.

Step 9 Expand the **HTTP(S)** area, if it is not already expanded, and do one of the following:

a) If you want to use the global HTTP(S) credentials that have been already created, click the **Select global credential** radio button.

Note If no HTTP(S) global credentials are available, create them in the **Network Settings** > **Device Credentials** page. See Configure Global HTTPS Credentials.

b) Click the **Edit device specific credential** radio button and configure the following fields:

Table 30: HTTP(S)

Field	Description
Username	Name that is used to log in to the HTTP(S) of the devices in your network.
Password	Password that is used to log in to the HTTP(S) of the devices in your network. For security reasons, re-enter the password as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.
Port	Specify the required HTTP(s) port number.

Step 10 Expand the **NETCONF** area, if it is not already expanded, and configure the **Port** field.

NETCONF requires that you configure SSH as the CLI protocol and define the SSH credentials.

Step 11 Select one of the network **Protocol** radio buttons that enables Cisco DNA Center to communicate with remote devices. Valid values are **SSH2** or **Telnet**.

Step 12 (Optional) Click **Validate** next to **Credentials**. Cisco DNA Center validates the device credentials and shows the valid credentials with green tick mark and invalid credentials with red cross mark.

If you have chosen more than one device for updating the credentials, the **Validation** button will be disabled.

Step 13 Click **Update**.

Security Focus for Network Devices

The Cisco DNA Center security focus allows you to view the results of the trustworthy checks on your devices.

Few security checks are performed to ensure that your Cisco devices are authentic and are not compromised or altered physically.

As a part of device identity verification, following checks are performed:

- Verification of Secure Unique Device Identifier (SUDI) certificate chain.
- Signature verification of SUDI certificate response of the device.
- Product ID verification with the SUDI certificate.
- Serial number verification with the SUDI certificate.

These checks are triggered under the following circumstances:

- Every time Inventory gets collected in the Cisco DNA Center.
- When you make any configuration changes on your devices.
- When you make any image upgrades in your devices.

The following CLI command is used to perform device identity verification check:

```
show platform sudi certificate sign nonce ${randomNonceValue}
```

Perform an Integrity Verification Check

This procedure explains how to view the status of the integrity verification check:

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The Inventory page displays the device information that is gathered during the Discovery process.

Step 2 From the **Inventory** drop-down menu, select **Security**.

Step 3 View the device details listed in the table.

Step 4 To customize the table, click the three vertical dots at the end of the table to choose either **Add** or **Delete**.
The **Integrity Verification** column displays the results.

Step 5 If the **Integrity Verification** column for your device displays **Failed** as the status, click the Information icon to display the reason.

The following integrity verification statuses are possible:

- **Passed**: Device identity verification passed.
- **Failed**: Device identity verification failed.
- **Unverified**: Unable to perform verification.
- **Not Available**: The device or software image version does not support verification.

Manage Compute Devices

Add a Compute Device

You can add a compute device to your inventory manually. A compute device includes devices such as the Cisco Unified Computing System (UCS), devices running Cisco Enterprise Network Functions Virtualization Infrastructure Software (NFVIS), and other data center devices.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Provision** > **Inventory**.

The Inventory page displays the device information gathered during the Discovery process.

Step 2 Click **Add Device**.

Step 3 From the **Type** drop-down list, choose **Compute Device**.

Step 4 In the **Device IP / DNS Name** field, enter the IP address or name of the device.

Step 5 Expand the **HTTP(S)** area, if it is not already expanded, and do one of the following:

a) If you want to use the global HTTP(S) credentials that have been already created, click the **Select global credential** radio button.

Note If no HTTP(S) global credentials are available, create them in the **Network Settings** > **Device Credentials** page. See Configure Global HTTPS Credentials.

b) Click the **Add device specific credential** radio button and configure the following fields:

Table 31: HTTP(S)

Field	Description
Username	Name used to authenticate the HTTPS connection.
Password	Password used to authenticate the HTTPS connection.
Port	Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).

Step 6 Expand the **CLI** area, if it is not already expanded, and do one of the following:

a) If you want to use the global CLI credentials that have been already created, click the **Select global credential** radio button.

Note If no CLI global credentials are available, create them in the **Network Settings** > **Device Credentials** page. See Configure Global CLI Credentials.

b) Click the **Add device specific credential** radio button and configure the following fields:

Table 32: CLI Credentials

Field	Description
Username	Name that is used to log in to the CLI of the devices in your network.

Field	Description
Password	Password that is used to log in to the CLI of the devices in your network. For security reasons, re-enter the password as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.
Enable Password	Password that is used to move to a higher privilege level in the CLI. For security reasons, re-enter the enable password. Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 7 Expand the **SNMP** area, if it is not already expanded, and do one of the following:

a) If you want to use the global SNMP credentials that have been already created, click the **Select global credential** radio button.

Note If no SNMP global credentials are available, create them in the **Network Settings** > **Device Credentials** page. See Configure Global SNMPv2c Credentials and Configure Global SNMPv3 Credentials.

b) Click the **Add device specific credential** radio button and do the following:

Step 8 From the **Version** drop-down list, choose **V2C** (SNMP Version 2c) or **V3** (SNMP Version 3).

If you chose **V2C**, configure the following fields:

Table 33: SNMPv2c Credentials

Field	Description
Read	• **Name/Description**: Name or description of the SNMPv2c settings that you are adding. • **Read Community**: Read-only community string password used only to view SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Write	• **Name/Description**: Name or description of the SNMPv2c settings that you are adding. • **Write Community**: Write community string used to make changes to the SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

If you chose **V3**, configure the following fields:

Table 34: SNMPv3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.

Field	Description
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Choose one of the following modes: • **noAuthNoPriv**: Does not provide authentication or encryption. • **AuthNoPriv**: Provides authentication, but does not provide encryption. • **AuthPriv**: Provides both authentication and encryption.
Auth Type	Authentication type to be used. (Enabled if you select **AuthPriv** or **AuthNoPriv** as the authentication mode.) Choose one of the following authentication types: • **SHA**: Authentication based on HMAC-SHA. • **MD5**: Authentication based on HMAC-MD5.
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	Privacy type. (Enabled if you select **AuthPriv** as the authentication mode.) Choose one of the following privacy types: • **AES128**: CBC mode AES for encryption. • **None**: No privacy.
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support AES128 encryption. Passwords (or passphrases) must be at least eight characters long. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 9 (Optional) Click **Validate** next to **Credentials**. Cisco DNA Center validates the device credentials and shows the valid credentials with green tick mark and invalid credentials with red cross mark.

All the credentials will be validated except the SNMP Write credentials.

Step 10 Click **Add**.

Update Compute Device Credentials

You can update the discovery credentials of selected compute devices. The updated settings override the global and job-specific settings for the selected devices.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The Inventory page displays the device information that is gathered during the Discovery process.

Step 2 Select the devices that you want to update.

Step 3 From the **Actions** drop-down list, choose **Inventory** > **Edit Device**.

Step 4 In the **Edit Device** dialog box, from the **Type** drop-down list, choose **Compute Device**.

Step 5 Expand the **HTTP(S)** area, if it is not already expanded.

Step 6 In the **Username** and **Password** fields, enter the username and password.

Step 7 In the **Port** field, enter the port number.

Step 8 (Optional) Click **Validate** next to **Credentials**. Cisco DNA Center validates the device credentials and shows valid credentials with a green tick mark and invalid credentials with a red cross mark.

If you have chosen more than one device for updating the credentials, the **Validation** button is disabled.

Step 9 Click **Update**.

Manage Meraki Dashboards

Integrate the Meraki Dashboard

You can integrate your Meraki dashboard with Cisco DNA Center.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The Inventory page displays the device information that is gathered during the Discovery process.

Step 2 Click **Add Device**.

Step 3 In the **Add Device** dialog box, from the **Type** drop-down list, choose **Meraki Dashboard**.

Step 4 Expand the **HTTP(S)** area, if it is not already expanded.

Step 5 In the **API Key/Password** field, enter the API key and password credentials and click the **Get Organization details** link.

Step 6 From the **Organization** drop-down list, select the organization options, or search for an organization name.

Step 7 (Optional) Click **Validate** next to **Credentials**. Cisco DNA Center validates the device credentials and shows valid credentials with a green tick mark and invalid credentials with a red cross mark.

Step 8 Click **Add**.

Only the selected organizations start collecting for the Meraki dashboard and devices.

Update Meraki Dashboard Credentials

You can update the Meraki dashboard credentials of selected devices. The updated settings override the global and job-specific settings for the selected devices.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The Inventory page displays the device information that is gathered during the Discovery process.

Step 2 Select the devices that you want to update.

Step 3 From the **Actions** drop-down list, choose **Inventory** > **Edit Device**.

Step 4 In the **Edit Device** dialog box, from the **Type** drop-down list, choose **Meraki Dashboard**.

Step 5 Expand the **HTTP(S)** area, if it is not already expanded.

Step 6 In the **API Key / Password** field, enter the API key and password credentials used to access the Meraki dashboard.

Step 7 In the **Port** field, enter the port number.

Step 8 (Optional) Click **Validate** next to **Credentials**. Cisco DNA Center validates the device credentials and shows valid credentials with a green tick mark and invalid credentials with a red cross mark.

If you have chosen more than one device for updating the credentials, the **Validation** button is disabled.

Step 9 Click **Update**.

Manage Firepower Management Center

Integrate Firepower Management Center

You can integrate your Firepower Management Center (FMC) with Cisco DNA Center.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The Inventory page displays the device information that is gathered during the discovery process.

Step 2 Click **Add Device**.

Step 3 In the **Add Device** dialog box, from the **Type** drop-down list, choose **Firepower Management Center**.

Step 4 In the **Device IP / DNS Name** field, enter the IP address or name of the device.

Step 5 Expand the HTTP(S) area if it is not already expanded.

The **Add device specific credential** radio button is chosen by default.

Step 6 Enter the following information:

a) **Username**: Name used to authenticate the HTTPS connection.

b) **Password**: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration.

c) **Port**: The number of the TCP/UDP port used for HTTPS traffic. The default port number is 443.

Step 7 Click **Add**.

Note When you add FMC to inventory, the Firepower Threat Defense (FTD) devices managed by FMC are also added to inventory automatically.

Update Firepower Management Center Credentials

Cisco DNA Center allows you to update the Firepower Management Center (FMC) credentials. The updated settings override the global and job-specific settings for the selected devices.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The Inventory page displays the device information that is gathered during the discovery process.

Step 2 Choose the FMC device that you want to update.

Note You cannot update, edit, or delete the Firepower Threat Defense (FTD) devices that are managed by FMC. You must manage FTD devices via FMC in inventory.

Step 3 From the **Actions** drop-down list, choose **Inventory** > **Edit Device**.

The **Edit Device** dialog box appears.

Step 4 Click **Credentials**.

Step 5 Expand the HTTP(S) area if it is not already expanded.

The **Add device specific credential** radio button is chosen by default.

Step 6 Enter the following information:

a) **Username**: Name used to authenticate the HTTPS connection.

b) **Password**: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration.

c) **Port**: The number of the TCP/UDP port used for HTTPS traffic. The default port number is 443.

Step 7 Click **Management IP** and enter the IP address or name of the device in the **Device IP / DNS Name** field.

Step 8 Click **Resync Interval** and choose a resync interval type:

- **Custom**: You can enter the resync interval in minutes. The valid ranges are from 25 to 1440 minutes (24 hours).
- **Global**: By default, resync interval is set to 1440 minutes (24 hours).
- **Disable**: Resync interval is disabled or set to zero.

Step 9 Click **Role** and choose a role in the **Device Role** drop-down list.

Step 10 Click **Update**.

Filter Devices

Note To remove or change the filters, click **Reset**.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The Inventory page displays the device information that is gathered during the Discovery process.

Step 2 Click **Filter**.

The following types of filters are available:

- Quick Filter
- Advanced Filter
- Recent Filters

Quick Filter: This filter allows you to retrieve the device details based on:

- **Device Family**
- **Device Role**
- **Last Sync Status**
- **Provision Status**
- **Credential Status**
- **OS Updated Status**
- **Image Needs Update**
- **Image Pre Check Status**
- **Support Type**

Advanced Filters: This filter allows you to set the filtering criteria using operators such as Contains, Starts With, Ends With, Equals, Does not contains and Regex (Regular Expression), to narrow down the device details. For example, you can choose the filter pattern by table column names and the operator from the drop-down list. In addition, you must enter filter criteria value based on the available data.

Recent Filters: This filter shows the recently used filters. To save the filter criteria, drag and drop the filters from the RECENT to the SAVED filters.

Step 3 Enter the appropriate value in the selected filter field. For example, for the **Device Name** filter, enter the name of a device.

Cisco DNA Center presents you with autocomplete values as you enter values in the other fields. Choose one of the suggested values or finish entering the desired value.

You also can use a wildcard (asterisk) with these filters. For example, you can enter values with an asterisk at the beginning, end, or in the middle of a string value. Then, press **Enter**.

Step 4 Click **Apply** to filter the information.

The data displayed in the **Devices** table updates automatically according to your filter selection.

Note You can use several filter types and more than one value per filter.

Step 5 (Optional) If needed, add more filters.

To remove a filter, click the **x** next to the corresponding filter value.

Manage Devices in Inventory

The following sections provide information about how to assign devices to sites and manage device tags by using the Inventory window.

Add a Device to a Site

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Provision** > **Inventory**.
The **Inventory** window displays the device information gathered during the **Discovery** process.

Step 2 Check the check box for the devices that you want to assign to a site.

Step 3 From the **Actions** menu, choose **Provision** > **Assign Device to Site**.
The **Assign Device to Site** slide-in pane appears.

Step 4 In the **Assign Device to Site** slide-in pane, click the link next to the  icon for the device.
The **Choose a floor** slide-in pane appears.

Step 5 In the **Choose a floor** slide-in pane, select the floor to assign to the device.

Step 6 Click **Save**.

Step 7 (Optional) If you selected multiple devices to add to the same location, you can check the **Apply to All** check box for the first device to assign its location to the rest of the devices.

Step 8 Click **Assign**.

Step 9 When assigning devices to a site, if Device Controllability is enabled, a workflow is automatically triggered to push the device configuration from the site to the devices.
From the **Focus** drop-down list, choose **Provision** and click **See Details** in the **Provision Status** column. The configuration that is pushed to the device is shown in a separate window if you enabled Device Controllability.

Tag Devices

A device tag allows you to group devices based on an attribute or a rule. A single device can have multiple tags; similarly, a single tag can be applied to multiple devices.

You can add tags to or remove tags from devices in the Provision window.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision**. The Device Inventory page displays device information gathered during the discovery process.

Step 2 Check the check box next to the device(s) for which you want to apply a tag, and then click **Tag Device**.

Step 3 Enter a tag name in the **Tag Name** field.

- If you are creating a new tag, click **Create New Tag**. You also can create a new tag with a rule. See Tag Devices Using Rules, on page 73 for more information.
- If you are using an existing tag, select the tag from the list, and then click **Apply**.

A tag icon and the tag name(s) appear under the device name(s) for which you applied the tag(s).

Step 4 To remove a tag from a device, do one of the following:

- Click **Create New Tag**, unselect all tags, and then click **Apply**.
- Hover the cursor over the tag icon or tag name, and then click **X** to disassociate the tag from the device.

Tag Devices Using Rules

You can group devices based on tags in which you define a rule. When you define a rule, Cisco DNA Center automatically applies the tag to all devices that match the specified rule. Rules can be based on device name, device family, device series, IP address, location, or version.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision**. The Device Inventory page displays device information gathered during the discovery process.

Step 2 Check the check box next to the device(s) for which you want to apply a tag, then click **Tag Device**.

Step 3 Enter a tag name in the **Tag Name** field, then click **Create New Tag with Rule**.

The Create New Tag window appears.

The **Manually Added** field under **Total Devices Tagged Count** indicates the number of devices you selected in Step 2.

Step 4 Click **Add Condition**, then complete the required fields for the rule.

The **Matching Devices** number automatically changes to indicate how many devices match this condition.

You can have two options to create additional conditions:

- *And* conditions—Click the **Add Condition** link. **And** appears above the condition.
- *Or* conditions—Click the add icon (+) next to an existing condition. **Or** appears next to the condition.

You can add as many conditions as needed. As you make changes to the rule, the Matching Devices count changes to reflect how many devices in the inventory match the rule you specified. You can click on the device number to view the devices that match the rule.

Step 5 Click **Save** to save your tag with the defined rule.

A tag icon and the tag name(s) appear under the device name(s) for which you applied the tag(s).

As devices are added to the inventory, if they match the rules you defined, the tag is automatically applied to the devices.

Edit Device Tags

You can edit device tags that you previously created.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Provision**. The Device Inventory page displays device information gathered during the discovery process.

In the **Device Name** column, you can see any previously created device tags listed under the device names.

Step 2 Without selecting any devices, click **Tag Device**.

The previously created tags are listed.

Step 3 Hover your cursor over the tag you want to edit, then click the pencil icon next to the tag name.

Alternatively, you can select **Tag Device** > **View All Tags**, then click the pencil icon next to the tag that you want to edit.

Step 4 Make changes to the tag, then click **Save** to save your changes.

Delete Tags

You can delete a device tag or template tag only if it is not associated with a device or template.

Before you begin

Remove the tag that is associated statically or dynamically (using rules) with the device.

Remove the tag that is associated with a template.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Provision**.

The Device Inventory page displays device information gathered during the discovery process.

Step 2 Without selecting any devices, choose **Tag Device** > **Manage Tags**.

Step 3 Hover your cursor over the tag that you want to delete, then click the delete icon next to the tag name.

Step 4 In the warning message, click **Yes**.

An error message is generated if the tag is associated with a device or template. Remove the tag associated with the device or template and delete the tag.

Inventory Insights

The **Inventory Insights** window displays devices that have configuration inconsistencies with other directly-connected devices. It also displays devices that are misconfigured, as compared with the Cisco DNA Center best-practice recommendations. Cisco DNA Center provides the following insights with suggested actions:

- Speed/Duplex settings mismatch
- VLAN mismatch

Speed/Duplex Settings Mismatch

Cisco DNA Center displays the devices that are connected with each other but configured with different speed and duplex values at the two ends of the device link.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The **Inventory** page displays the device information that is gathered during the discovery process.

Step 2 From the **Focus** drop-down list, choose **Inventory Insights**.

The **Inventory Insights** window appears.

Step 3 Click **Speed/Duplex settings mismatch** to see the suggested actions that can be performed on devices.

The suggested actions appear in the right pane.

Step 4 Click the number of instances to see the mismatches.

The **Speed/Duplex settings mismatch** window highlights the mismatches of speed and duplex.

Step 5 Make the required changes in the device configuration by following the suggested actions.

VLAN Mismatch

Cisco DNA Center displays the devices that are connected with each other but configured with different VLANs at the two ends of device link.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The **Inventory** page displays the device information that is gathered during the discovery process.

Step 2 From the **Focus** drop-down list, choose **Inventory Insights**.

The **Inventory Insights** window appears.

Step 3 Click **VLAN Mismatch** to see the suggested actions that can be performed on devices.

The suggested actions appear in the right pane.

Step 4 Click the number of instances to see the mismatches.

The **VLAN Mismatch** window highlights the mismatches of Allowed VLAN and Native VLAN.

Step 5 Make the required changes in the device configuration by following the suggested actions.

Change the Device Role (Inventory)

During the Discovery process, Cisco DNA Center assigns a role to each of the discovered devices. Device roles are used to identify and group devices and to determine a device's placement on the network topology map in the Topology tool. The top tier is the internet. The devices underneath are assigned one of the following roles:

Table 35: Device Roles and Topology Positions

Topology Position	Device Role
Tier 1	Internet (not configurable)
Tier 2	Border Router
Tier 3	Core
Tier 4	Distribution
Tier 5	Access
Tier 6	Unknown

Note When you assign the **Access** role to a device, IP Device Tracking (IPDT) is either configured or removed from the device based on the IPDT settings of the Site.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The Inventory page displays the device information gathered during the Discovery process.

Step 2 Locate the device whose role you want to change, click the pencil icon under the **Device Role** column, and choose a role from the **Update Device Role** dialog box. Valid choices are **Unknown**, **Access**, **Core**, **Distribution**, or **Border Router**.

Alternatively, you can update the device role in the **Edit Device** dialog box:

- Select the device whose role you want to change.
- Choose **Actions** > **Inventory** > **Edit Device**.
- Click the **Role** tab and choose an appropriate role from the **Device Role** drop-down list.

Note If you manually change the device role, the assignment remains static. Cisco DNA Center does not update the device role even if it detects a change during a subsequent device resynchronization.

Update a Device's Management IP Address

You can update the management IP address of a device.

Note You cannot update more than one device at a time. Also, you cannot update a Meraki device's management IP address.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The Inventory page displays the device information that is gathered during the Discovery process.

Step 2 Select the device that you want to update.

Step 3 From the **Actions** drop-down list, choose **Inventory** > **Edit Device**.

The **Edit Device** dialog box is displayed.

Step 4 Click the **Management IP** tab, and enter the new management IP address in the **Device IP/ DNS Name** field.

Note Make sure that the new management IP address is reachable from Cisco DNA Center and that the device credentials are correct. Otherwise, the device might enter an unmanaged state.

What to do next

Reprovision the device to update the source-interface configuration.

Update the Device Polling Interval

You can update the polling interval at the global level for all devices by choosing **System** > **Settings** > **Network Resync Interval** or at the device level for a specific device by choosing **Device Inventory**. When you set the

polling interval using the **Network Resync Interval**, that value takes precedence over the **Device Inventory** polling interval value.

If you do not want a device to be polled, you can disable polling.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

Step 2 Select the devices that you want to update.

Step 3 Click **Update Polling Interval**.

Step 4 From the **Update Resync Interval** dialog box, in the **Status** field, click **Enabled** to turn on polling or click **Disabled** to turn off polling.

Step 5 In the **Polling Time** field, enter the time interval (in minutes) between successive polling cycles. Valid values are from 25 to 1440 minutes (24 hours).

Note The device-specific polling time supersedes the global polling time. If you set the device-specific polling time and then change the global polling time, Cisco DNA Center continues to use the device-specific polling time.

Step 6 Click **Update**.

Resynchronize Device Information

You can immediately resynchronize device information for selected devices, regardless of their resynchronization interval configuration. A maximum of 40 devices can be resynchronized at the same time.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The Inventory page displays the device information gathered during the Discovery process.

Step 2 Select the devices about which you want to gather information.

Step 3 From the **Actions** drop-down list, choose **Inventory** > **Resync Device**.

Step 4 Click **OK**.

Delete a Network Device

You can delete devices from the Cisco DNA Center database, as long as they have not already been added to a site.

When you remove a wireless sensor from the inventory, the sensor is reset to the factory defaults so that when it rejoins, it gets the current configuration.

Before you begin

You must have administrator (ROLE_ADMIN) permissions and access to all devices (RBAC Scope set to ALL) to perform this procedure.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Inventory**.
The **Inventory** window displays the device information gathered during the **Discovery** process.

Step 2 Check the check box next to the device or devices that you want to delete.

Note You can select multiple devices by checking additional check boxes, or you can select all the devices by checking the check box at the top of the list.

Step 3 From the **Actions** drop-down list, choose **Inventory** > **Delete Device**.

Step 4 In the **Warning** window, check the **Config Clean-Up** check box to remove the network settings and telemetry configuration from the selected device.

Step 5 Confirm the action by clicking **OK**.

Launch Command Runner (Inventory)

You can launch the Command Runner application for selected devices from within the **Inventory** window.

Before you begin

Install the Command Runner application. For more information, see the Cisco DNA Center Administrator Guide.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The Inventory page displays the device information that is gathered during the Discovery process.

Step 2 Select the devices on which you want to run commands.

Step 3 From the **Actions** drop-down list, choose **Others** > **Launch Command Runner**.

For information about the commands that you can run and how to run them, see Run Diagnostic Commands on Devices, on page 191.

Troubleshoot Device Reachability Issues Using Run Commands

You can launch the **Run Commands** window from the **Inventory** window and run platform commands such as ping, traceroute, and snmpget to troubleshoot device reachability issues.

Note If you want to execute the platform commands directly on a Cisco DNA Center cluster, do not select any device before launching **Run Commands**. Otherwise, the execution of commands will be for that device and not the platform.

Before you begin

Install the Command Runner application. For more information, see the Cisco DNA Center Administrator Guide.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

Step 2 From the **Actions** drop-down list, choose **Others** > **Run Commands**.

You can enter **`man`** anytime to retrieve a list of currently supported commands and shortcuts.

Use a CSV File to Import and Export Device Configurations

CSV File Import

You can use a CSV file to import your device configurations or sites from another source into Cisco DNA Center. If you want to download a sample template, go to the Provision Devices page and choose **Actions** > **Inventory** > **Import Inventory**. Click **Download Template** to download a sample CSV file template.

When you use a CSV file to import device or site configurations, the extent to which Cisco DNA Center can manage your devices depends on the information you provide in the CSV file. If you do not provide values for CLI username, password, and enable password, Cisco DNA Center will have limited functionality and cannot modify device configurations, update device software images, or perform any other valuable functions.

You can specify the credential profile in the CSV file to apply the corresponding credentials to a set of devices. If you specify the credential profile and also enter the values manually in the CSV file, the manually entered credentials take higher priority and the device is managed based on a combination of manually entered credentials and credential profile. For example, if the CSV file contains a credential profile with SNMP and SSH or Telnet credentials in addition to manually entered SNMP credentials, the device is managed based on the manually entered SNMP credentials and the SSH or Telnet credentials in the credential profile. Telnet is not recommended.

Note You also must provide values for the fields that correspond to the protocol you specify. For example, if you specify SNMPv3, you must specify values for the SNMPv3 fields in the sample CSV file such as the SNMPv3 username and authorization password.

For partial inventory collection in Cisco DNA Center, you must provide the following values in the CSV file:

- Device IP address
- SNMP version

- SNMP read-only community strings
- SNMP write community strings
- SNMP retry value
- SNMP timeout value

For full inventory collection in Cisco DNA Center, you must provide the following values in the CSV file:

- Device IP address
- SNMP version
- SNMP read-only community strings
- SNMP write community strings
- SNMP retry value
- SNMP timeout value
- Protocol
- CLI username
- CLI password
- CLI enable password
- CLI timeout value

CSV File Export

Cisco DNA Center enables you to create a CSV file that contains all or selected devices in the inventory. When you create this file, you must enter a password to protect the configuration data that the file will contain.

Import Device Configurations from a CSV File

You can import device configurations from a CSV file.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The Inventory page displays the device information gathered during the Discovery process.

Step 2 From the **Actions** drop-down list, choose **Inventory** > **Import Inventory** to import the device credentials.

Step 3 Drag and drop the CSV file into the boxed area in the **Bulk Import** dialog box or click the dotted-line boxed area and browse to the CSV file.

Step 4 Click **Import**.

Export Device Data

You can export specific data pertaining to selected devices to a CSV file. The CSV file is compressed. Click **Export** to export the data of filtered devices or all devices.

Caution Handle the CSV file with care because it contains sensitive information about the exported devices. Ensure that only users with special privileges perform a device export.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The Inventory page displays the device information gathered during the Discovery process.

Step 2 To export configuration information for only certain devices, check the check box next to the devices that you want to include. To include all devices, check the check box at the top of the device list.

Step 3 From the **Actions** drop-down list, choose **Inventory** > **Export Inventory** to export the device configurations.

The **Export Inventory** dialog box appears.

Step 4 In the **Password** field, enter a password that will be used to encrypt the exported CSV file.

Note The password is required to open the exported file.

Step 5 Confirm the encryption password.

Step 6 Check the **Include SSH key information** check box to include information such as initial SSH key, initial SSH key algorithm, current SSH key, and current SSH key algorithm in the exported CSV file.

Step 7 Click **Export**.

Note Depending on your browser configuration, you can save or open the compressed file.

Export Device Credentials

You can export device credentials to a CSV file. You are required to configure a password to protect the file from unwanted access. You need to supply the password to the recipient so that the file can be opened.

Caution Handle the CSV file with care because it lists all of the credentials for the exported devices. Ensure that only users with special privileges perform a device export.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The Inventory page displays the device information that is gathered during the Discovery process.

Step 2 Check the check box next to the devices that you want to include in the CSV file. To include all the devices, select the check box at the top of the list.

Step 3 From the **Actions** drop-down list, choose **Inventory** > **Export Inventory**.

The **Export** dialog box appears.

Step 4 In **Select Export Type**, click the **Credentials** radio button.

Step 5 Check the **Include SSH key information** check box to include information such as initial SSH key, initial SSH key algorithm, current SSH key, and current SSH key algorithm in the exported CSV file.

Step 6 In the **Password** field, enter a password that will be used to encrypt the exported CSV file.

Note The password is required to open the exported file.

Step 7 Confirm the encryption password and click **Export**.

Note Depending on your browser configuration, you can save or open the compressed file.

Replace a Faulty Device

Replacing devices that fail in the network is a critical part of device lifecycle management. The Return Material Authorization (RMA) workflow in Cisco DNA Center provides you with the ease of automation to replace failed devices quickly, thus improving productivity and reducing operational expense. RMA provides a common workflow to replace routers, switches, and APs.

When using the RMA workflow with routers and switches, the software image, configuration, and license are restored from the failed device to the replacement device. For wireless APs, the replacement device is assigned to the same site, provisioned with primary wireless LAN controller, RF profile, and AP group settings, and placed on the same floor map location in Cisco DNA Center as the failed AP.

Before you begin

- The software image version of the faulty device must be imported in the image repository before marking the device for replacement.
- The faulty device must be in an unreachable state.
- The faulty device must be assigned to a user-defined site, if the replacement device onboards Cisco DNA Center through Plug and Play (PnP).
- The replacement device must not be in a provisioning state while triggering the RMA workflow.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The **Inventory** window displays the device information that is gathered during the Discovery process.

Step 2 Select the faulty device that you want to replace.

Note RMA supports replacement of faulty SMUs and packages.

Step 3 From the **Actions** drop-down list, choose **Inventory** > **Device Replacement** > **Mark Device for Replacement**.

Step 4 In the **Mark for Replacement** window, click **Mark**.

Note To achieve seamless replacement of fabric devices, a DHCP server is configured on the neighbor device. This is required to assign an IP address, and is removed after successful replacement of the faulty device.

The latest configuration changes from the faulty device are pushed to the replaced device during the RMA workflow.

Step 5 From the **Inventory** drop-down list, choose **Marked for Replacement**.

A list of devices marked for replacement is displayed.

Step 6 (Optional) If you do not want to replace the device, select the device and choose **Actions** > **Unmark for Replacement**.

Step 7 Select the device that you want to replace and choose **Actions** > **Replace Device**.

Step 8 In the **Replace Device** window, click **Start**.

Step 9 In the **Replace Device** window, select a device under the **Available Replacement Devices** area.

Step 10 Click **Next**.

Step 11 Review the **Replacement Summary** and then click **Next**.

Step 12 Select whether to replace the device now, or schedule the replacement for a later time, and then click **Submit**.

The RMA workflow begins.

Step 13 Click **Monitor Replacement Status** to go to the **Provision** page.

Step 14 Click **Replace Status** for the replacement device to view the status of the RMA workflow progress, as follows:

- Distribute the software image to the replacement device.
- Activate the software image on the device.
- Deploy licenses.
- Create the DHCP server on the neighbor device.
- Provision VLAN and startup configurations.
- Reload the device.
- Check for reachability.
- Deploy SNMPv3 credentials to the replacement device.
- Authenticate through Cisco ISE.
- Revoke the PKI certificate.
- Delete the faulty device.
- Synchronize the replacement device.
- Remove the DHCP server from the neighbor device.
- RMA workflow deregisters the faulty device from CSSM.
- RMA workflow registers the replacement device with CSSM.

After the workflow is complete, the **Replace Status** is updated to **Replaced**.

Step 15 If an error message appears, click the error link.

Step 16 Click **Retry** to retrigger the workflow with the same set of faulty and replacement devices.

Note The main inventory window displays the details of the new replacement device that has replaced the faulty device.

Replace a Faulty Access Point

Using the AP RMA feature, you can replace a faulty AP with a replacement AP available in the device inventory.

Before you begin

- The AP Return Material Authorization (RMA) feature supports only like-to-like replacement. The replacement AP must have the same model number and PID as the faulty AP.
- The replacement AP must have joined the same Cisco Wireless Controller as the faulty AP.
- A Cisco Mobility Express AP that acts as the wireless controller is not a candidate for the replacement AP.
- The software image version of the faulty AP must be imported in the image repository before marking the device for replacement.
- The faulty device must be assigned to a user-defined site if the replacement device onboards Cisco DNA Center through Plug and Play (PnP).
- The replacement AP must not be in provisioning state while triggering the RMA workflow.
- The faulty device must be in an unreachable state.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The **Inventory** page displays the device information that is gathered during the Discovery process.

Step 2 Check the check box of the faulty AP that you want to replace.

Step 3 From the **Actions** drop-down list, choose **Device Replacement** > **Mark Device for Replacement**.

Step 4 In the **Mark for Replacement** window, click the radio button next to the faulty device name.

Step 5 From the **Actions** drop-down list, choose **Replace Device**.

Step 6 In the **Replace Device** window, click **Start**.

Step 7 In the **Available Replacement Devices** table, click the radio button next to the replacement device name.

Step 8 Click **Next**.

Step 9 Review the **Replacement Summary** and then click **Next**.

Step 10 In the **Schedule Replacement** window, select whether to replace the device now, or schedule the replacement for a later time, and then click **Submit**.

The RMA workflow begins.

Step 11 To monitor the replacement status, under **What's Next**, click **Monitor Replacement Status**.

The **Mark For Replacement** window lists the devices that are marked for replacement.

Check the status of the replacement in the **Replace Status** column, which initially shows **In-Progress**.

Step 12 Click **In-Progress** in the **Replace Status** column.

The **Replace Status** tab shows the various steps that Cisco DNA Center performs as part of the device replacement.

Step 13 In the **Marked for Replacement** window, click **Refresh** and click **Replace Status** to view the replacement status.

If the faulty AP replacement fails, then the **Replace Status** column shows the reason for failure with an error message.

You can either replace the faulty AP with another new AP or retry the failed replacement using the AP RMA Retry feature.

Step 14 To retry the failed replacement, click the error message in the **Replace Status** column against the device name.

Step 15 Click **Retry**.

Step 16 In the **Marked for Replacement** window, click **In-Progress** against the **Replace Status** column.

The **Replace Status** tab shows success after successful replacement of the faulty AP.

Step 17 The **Replace Status** in the **Replacement History** window shows **Replaced** after the faulty device is replaced successfully.

Step 18 (Optional) If you do not want to replace the device, select the device and choose **Actions** > **Unmark for Replacement**.

Limitations of the RMA Workflow in Cisco DNA Center

- RMA supports replacement of similar devices only. For example, a Cisco Catalyst 3650 switch can be replaced only with another Cisco Catalyst 3650 switch. Also, the platform IDs of the faulty and replacement devices must be the same.
- RMA supports replacement of all switches, routers, and Cisco SD-Access devices, *except for the following*:
  - Devices with embedded wireless controllers
  - Wireless Controllers (WLC)
  - Fabric in a Box
  - Classic- and policy-extended nodes
  - Devices that are discovered and configured using LAN automation, including the seed devices (LAN automation primary and peer devices)
  - Chassis-based switches, including the Catalyst 9400, Catalyst 9600, Catalyst 4500e, Catalyst 6500, Catalyst 6800, and Nexus 7700 Series Switches
  - Switch stacks (hardware and SVL stacking)
  - Devices with single and dual supervisor engines
  - Devices that have third-party certificates
  - Devices that have external SCEP broker PKI certificates
- The RMA workflow supports device replacement only if:
  - Both faulty and replacement devices have the same extension cards.

- The number of ports in both devices does not vary because of the extension cards.
- The faulty device is managed by Cisco DNA Center with a static IP. (RMA is not supported for devices that are managed by Cisco DNA Center with a DHCP IP.)

- Make sure that the replacement device is connected to the same port to which the faulty device was connected.
- Cisco DNA Center does not support legacy license deployment.

  RMA workflow deregisters the faulty device from CSSM and registers the replacement device with CSSM.

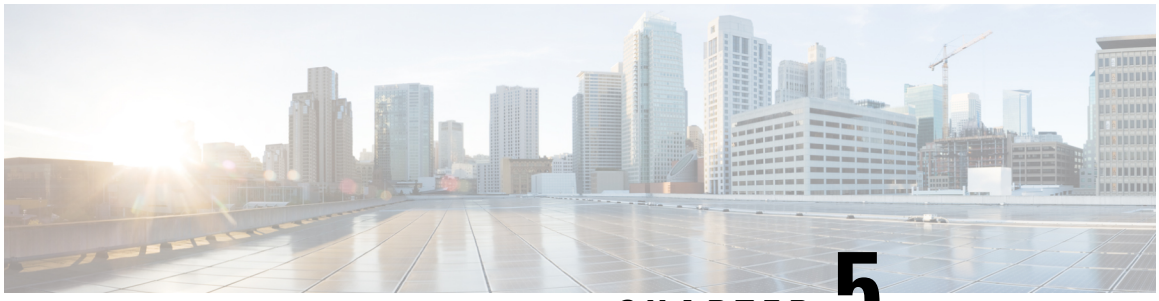
  - If the software image installed on the faulty device is earlier than Cisco IOS XE 16.8, the **License Details** window does not display the Network and Feature License details and no warning message is displayed. Therefore, you should be aware of the legacy network license configured on the faulty device and manually apply the same legacy network license on the replacement device.
  - If the software image installed on the faulty device is Cisco IOS XE 16.8 or later, the **License Details** window displays details of the network license (for example, **Legacy** or **Network**) and the feature license (for example, IP Base, IP Service, or LAN Base). The following warning message is displayed while marking the faulty device for replacement:

    ```
    Some of the faulty devices don't have a Cisco DNA license. Please
    ensure your replacement device has the same Legacy license of the
    faulty device enabled.
    ```

  - If the legacy network licenses of the replacement and faulty devices do not match, the following error message is displayed during the license deployment:

    ```
    Cisco DNA Center doesn't support legacy license deployment. So
    manually update the faulty device license on the replacement device
    and resync before proceeding.
    ```

- Cisco DNA Center provisions the replacement device with the running and VLAN configurations of the faulty device that are available in the archive. If any configuration changes were made to the faulty device after the latest archive, the replacement device might not have the latest configuration.
- If the replacement device onboards through PnP-DHCP functionality, make sure that the device gets the same IP address after every reload and the lease timeout of DHCP is longer than two hours.



CHAPTER 5

Manage Software Images

About Image Repository

Cisco DNA Center stores all of the software images, software maintenance updates (SMUs), subpackages, ROMMON images, and so on for the devices in your network. Image Repository provides the following functions:

- Image Repository: Cisco DNA Center stores all the unique software images according to image type and version. You can view, import, and delete software images.
- Provision: You can push software images to the devices in your network.

Before using Image Repository features, you must enable Transport Layer Security protocol (TLS) on older devices such as Cisco Catalyst 3000, 4000, and 6000. After any system upgrades, you must re-enable TLS. For more information, see “Configure Security for Cisco DNA Center” in the Cisco DNA Center Administrator Guide.

Integrity Verification of Software Images

The Integrity Verification application monitors software images that are stored in Cisco DNA Center for unexpected changes or invalid values that could indicate your devices are compromised. During the import process, the system determines image integrity by comparing the software and hardware platform checksum

value of the image that you are importing to the checksum value identified for the platform in the Known Good Values (KGV) file to ensure that the two values match.

On the **Image Repository** window, a message displays if the Integrity Verification application cannot verify the selected software image using the current KGV file. For more information about the Integrity Verification application and importing KGV files, see the *Cisco Digital Network Architecture Center Administrator Guide*.

View Software Images

After you run Discovery or manually add devices, Cisco DNA Center automatically stores information about the software images, SMUs, and subpackages for the devices.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Image Repository**.

The software images are organized and displayed based on the device type. By default, software images for physical devices are displayed. Toggle to the **Virtual** tab to view software images for virtual devices.

Note When cisco.com credentials are not set, a warning alert is displayed.

Step 2 In the **Family** column, click the downward arrow to view all the software images for the specified device type family. The **Device(s)** column indicates how many devices are using the specific image shown in the **Image Name** field. Click the number of devices to view the devices that are using the image.

Step 3 In the **Version** column, click the **Add On** link to view the applicable **SMUs**, **Subpackages**, **ROMMON**, **APSP**, and **APDP** upgrades for the base image.

Subpackages are the additional features that can be added to the existing base image. The subpackage version that matches the image family and the base image version is displayed here.

AP Service Pack (APSP) and AP Device Pack (APDP) are images for upgrading APs associated with wireless controllers.

- When a new AP hardware model is introduced, APDP is used to connect to the existing wireless network.
- For associated APs, critical AP bug fixes are applied through APSP.

Note If you tag any SMU as golden, it is automatically activated when the base image is installed.

You cannot tag a subpackage as golden.

For ROMMON upgrades, the cisco.com configuration is mandatory. When a device is added, the latest ROMMON details are retrieved from cisco.com for applicable devices. Also, when the base image is imported or tagged, the ROMMON image is automatically downloaded from cisco.com.

Step 4 In the **Device Role** column, select a device role for which you want to indicate that this is a "golden" software image. For more information, see About Golden Software Images, on page 93 and Specify a Golden Software Image, on page 93.

Use a Recommended Software Image

Cisco DNA Center displays and allows you to select Cisco-recommended software images for the devices that it manages.

Note Only the latest Cisco-recommended software images are available for download.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Settings** > **Cisco.com Credentials**.

Step 2 Verify that you have entered the correct credentials to connect to cisco.com.

Step 3 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Image Repository**.

Cisco DNA Center displays the Cisco-recommended software images according to device type.

Step 4 Designate the recommended image as golden. See Specify a Golden Software Image, on page 93 for more information.

Step 5 Push the recommended software image to the devices in your network. See Provision a Software Image, on page 95 for more information.

Import a Software Image

You can import software images and software image updates from your local computer or from a URL.

Imported images are categorized based on different supervisors that are present in a specific device family. Categorization under different supervisors supports only the Cisco Catalyst 9400 series family.

If you use FTP to import an image from an FTP server, use the FTP standard:

```
ftp://username:password@ip_or_hostname/path
```

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Image Repository**.

Step 2 Click **Import**.

Step 3 Click **Choose File** to navigate to a software image or software image update stored locally. Alternately, enter the image URL to specify an HTTP or FTP source from which to import the software image or software image update.

Step 4 If the image you are importing is for a third-party (non-Cisco) vendor, select **Third Party** under **Source**. Choose an **Application Type**, describe the device **Family**, and identify the **Vendor**.

Step 5 Click **Import**.

A window displays the progress of the import.

Step 6 Click **Show Tasks** to verify that the image was imported successfully.

If you imported a SMU, Cisco DNA Center automatically applies the SMU to the correct software image, and an **Add-On** link appears below the corresponding software image.

Step 7 Click the **Add-On** link to view the SMU.

Step 8 In the **Device Role** field, select the role for which you want to mark this SMU as golden. See Specify a Golden Software Image, on page 93.

You can only mark a SMU as golden if you previously marked the corresponding software image as golden.

Note Cisco DNA Center does not allow you to import software images for the FTD devices that are managed by FMC. When you add FMC to inventory and it goes to the 'Managed' state, the software images present in FMC are shown in Image Repository and are categorized based on device family.

Assign a Software Image to a Device Family

After importing a software image, you can assign or unassign it to available device families. The imported image can be assigned to multiple devices at any time.

To assign an imported software image to a device family:

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Image Repository**.

Step 2 Click **Imported Images**.

Step 3 Click **Assign** in the corresponding image name row.

Step 4 In the **Assign Device Family** window, choose the **Device Series from Cisco.com** or **All Device Series** and click **Assign** link to which you want to map the image.

Note: If cisco.com credentials are not set, specify the credentials in **System** > **Settings** > **Cisco.com Credentials**.

Step 5 Select appropriate site from the Global hierarchy and click **Assign** and then click **Save**.

Step 6 To unassign an image, choose a site from the Global hierarchy and click **Unassign** link in the **Action** column.

The software image is assigned to the device family and the number of devices using that image are shown in the **Device(s)** column. After assigning the image, you can mark it as a golden image. See Specify a Golden Software Image.

If the device family is marked as a golden image, you cannot delete that image from the device family.

Note For PnP devices, you can import a software image and assign it to a device family even before the device is available. You can also mark the image as a golden image. When the device is made available in the inventory, the image that is assigned to the device family is automatically assigned to the newly added devices of that device family.

When the image is imported and Cisco DNA Center has cisco.com credentials added, Cisco DNA Center provides the list of device families that are applicable for the image. You can select the required device family from the list.

When the image is not available in cisco.com or when credentials are not added in Cisco DNA Center, you must design the right device family for the image.

Upload Software Images for Devices in Install Mode

The Image Repository page might show a software image as being in Install Mode. When a device is in Install Mode, Cisco DNA Center is unable to upload its software image directly from the device. When a device is in Install Mode, you must first manually upload the software image to the Cisco DNA Center repository before marking the image as golden, as shown in the following steps.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Image Repository**.

Step 2 In the **Image Name** column, find the software image of the device that is running in **Install Mode**.

Step 3 Click **Import** to upload the binary software image file for the image that is in Install Mode.

Step 4 Click **Choose File** to navigate to a software image stored locally or **Enter image URL** to specify an HTTP or FTP source from which to import the software image.

Step 5 Click **Import**.

A window displays the progress of the import.

Step 6 Click **Show Tasks** and verify that the software image you imported is green, indicating it has been successfully imported and added to the Cisco DNA Center repository.

Step 7 Click **Refresh**.

The Image Repository window refreshes. Cisco DNA Center displays the software image, and the Golden Image and Device Role columns are no longer dimmed.

About Golden Software Images

Cisco DNA Center allows you to designate software images and SMUs as *golden*. A golden software image or SMU is a validated image that meets the compliance requirements for the particular device type. Designating a software image or SMU as golden saves you time by eliminating the need to make repetitive configuration changes and ensures consistency across your devices. You can designate an image and a corresponding SMU as golden to create a standardized image. You can also specify a golden image for a specific device role. For example, if you have an image for the Cisco 4431 Integrated Service Routers device family, you can further specify a golden image for those Cisco 4431 devices that have the Access role only.

You cannot mark a SMU as golden unless the image to which it corresponds is also marked golden.

Specify a Golden Software Image

You can specify a golden software image for a device family or for a particular device role. The device role is used for identifying and grouping devices according to their responsibilities and placement within the network.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Image Repository**.

The software images are displayed according to device type.

Step 2 From the **Family** column, select a device family for which you want to specify a golden image.

Step 3 From the **Image Name** column, select the software image that you want to specify as golden.

Step 4 If the software image that you specify as golden is already uploaded into the Cisco DNA Center repository, click the star icon in the **Golden Image** column.

The software image is marked as golden.

Step 5 If the software image that you specify as golden is not already uploaded into the Cisco DNA Center repository, click the download icon in the **Golden Image** column.

This process might take some time.

Note Importing software images from devices is not allowed.

Step 6 From the **Download Image** dialog box, do one of the following:

- Keep the **Mark the image as golden after download** check box checked by default and click **Download**. The software image is downloaded and marked as golden.

  Note If Cisco.com credentials are not set, you are prompted to specify them.

  The in-progress software image download is shown in the **Device Role** column.

  If the software image is downloaded and successfully marked as golden, the color of the star icon turns gold. If the software image download fails, the color of the star icon turns red and a **Please Retry** status is displayed.

- Uncheck the **Mark the image as golden after download** check box and click **Download**. The software image is downloaded to the repository but is not marked as golden.

Step 7 In the **Device Role** column, select a device role for which you want to specify a golden software image. Even if you have devices from the same device family, you can specify a different golden software image for each device role. Note that you can select a device role for physical images only, not virtual images.

Configure an Image Distribution Server

You can configure an external image distribution server to distribute software images.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Settings** > **Device Settings** > **Image Distribution Servers**.

Step 2 Click **Add** to add a new image distribution server.

Step 3 Configure the server settings:

- **Host**: Hostname or IP address of the image distribution server.
- **Root Location**: Working root directory for file transfers.

  Note For Cisco AireOS Controllers, the image distribution fails if the configured path is more than 16 characters.

- **Username**: Name that is used to log in to the image distribution server. The username must have read/write privileges on the working root directory on the server.
- **Password**: Password that is used to log in to the image distribution server.
- **Port Number**: Port number on which the image distribution server is running.

Step 4 Click **Save**.

Step 5 To edit the image distribution server settings, do the following:

a) Click the **Edit** icon for the image distribution server where you want to change the configuration.
b) Make the required changes in the **Edit** window.
c) Click **Save**.

Add Image Distribution Servers to Sites

You can associate SFTP servers located in different geographical regions to sites, buildings, and floors. All the devices under the network hierarchy use the associated image distribution server during a network upgrade.

Before you begin

You must configure an image distribution server. See Configure an Image Distribution Server, on page 94.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings**.

Step 2 In the left pane, choose the desired site to which you want to associate the image distribution server.

Step 3 Click **Add Servers**.

Step 4 In the **Add Servers** window, check the **Image Distribution** check box.

Step 5 Click **OK**.

Step 6 Click the **Primary** drop-down list and choose the image distribution server that you want to configure as primary.

Step 7 Click the **Secondary** drop-down list and choose the image distribution server that you want to configure as secondary.

Step 8 Click **Save**.

Provision a Software Image

You can push software images to the devices in your network. Before pushing a software image to a device, Cisco DNA Center performs upgrade readiness prechecks on the device, such as checking the device management status, disk space, and so on. If any prechecks fail, you cannot perform the software image update. After the software image of the device is upgraded, Cisco DNA Center checks for the CPU usage, route summary, and so on, to ensure that the state of the network remains unchanged after the image upgrade.

Note You can perform prechecks on multiple devices.

Cisco DNA Center compares each device's software image with the image that you have designated as golden for that specific device type. If there is a difference between the software image of the device and the golden image, Cisco DNA Center specifies the software image of the device as outdated. The upgrade readiness prechecks are triggered for those devices. If all the prechecks are cleared, you can distribute (copy) the new image to the device and activate it (that is, make the new image the running image). The activation of the new image requires a reboot of the device. Because a reboot might interrupt the current network activity, you can schedule the process for a later time.

If you have not designated a golden image for the device type, the device's image cannot be updated. See Specify a Golden Software Image, on page 93.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

Step 2 From the **Focus** drop-down list, choose **Software Images**. Select the device whose image you want to upgrade.

Note If the prechecks succeed for a device, the **Outdated** link in the Software Image column has a green tick mark. If any of the upgrade readiness prechecks fail for a device, the **Outdated** link has a red mark, and you cannot update the software image for that device. Click the **Outdated** link and correct the errors before proceeding. See List of Device Upgrade Readiness Prechecks.

Step 3 From the **Actions** drop-down list, choose **Software Images** > **Update Image**.

The **Image Upgrade** window appears.

Step 4 **Analyze Selection**: Choose the devices that you want to upgrade and click **Next**.

Step 5 **Distribute**: Click **Now** to start the distribution immediately or click **Later** to schedule the distribution at a specific time.

To choose the validators you want to run for the current workflow and add new custom checks, do the following:

a) Hover your mouse over the Info icon to view the validation criteria and the CLI commands that are used for validation.
b) Click the on or off toggle button to uncheck the validators that you do not want to run for the current workflow.
c) (Optional) To add new custom pre checks and post checks, do the following:

- Click **add a new check** link to launch the **Add a New Custom Check** window.
- Enter the **Name** for the custom check.
- Click the **When** drop-down arrow and choose pre, post, or both as required.
- Click **Select a Test Device** drop-down arrow and choose a device for which you want to run these custom checks.
- Click **Open Command Runner** and enter the CLI commands.
- Expand the **Additional Criteria** area.
- Click the **Operation** drop-down arrow and choose **Distribution**.
- Click the **Device Series** drop-down arrow and choose the device series for which you want to run these custom checks.
- Click **Save**.
- If you want to edit a custom check, click the corresponding More icon, choose **Edit**, make the required changes, and click **Save**.
- If you want to delete a custom check, click the corresponding More icon, choose **Delete**, and click **Delete** in the **Confirm Delete** message.

Note

- If you have associated external image distribution server to a network hierarchy, the image distribution to all the devices under the network hierarchy happens from the image distribution server. See Add Image Distribution Servers to Sites, on page 95.
- If the image is already distributed for the selected device, click **Next**.
- If the **SWIM Events for ITSM (ServiceNow)** bundle is enabled, you need to update the image (distribute and activate) at a later time. Do not click **Now** to update the image. If you must update the image now, then the bundle and its integration workflow (image update schedule approval in ServiceNow) must first be disabled. To access the bundle, choose **Platform** > **Manage** > **Bundles** > **SWIM Events for ITSM (ServiceNow)**. Click the **Disable** button in the **SWIM Events for ITSM (ServiceNow)** window. Wait a few seconds before proceeding to update the image, because the process to disable the bundle and workflow takes a few seconds.

Step 6 Click **Next**.

Step 7 **Activate**: Click **Now** to start the activation immediately or click **Later** to schedule the activation at a specific time.

To choose the validators you want to run for the current workflow and add new custom checks, do the following:

a) Hover your mouse over the Info icon to view the validation criteria and the CLI commands that are used for validation.
b) Click the on or off toggle button to uncheck the validators that you do not want to run for the current workflow.
c) (Optional) To add new custom pre checks and post checks, do the following:

- Click **add a new check** link to launch the **Add a New Custom Check** window.
- Enter the **Name** for the custom check.
- Click the **When** drop-down arrow and choose pre or post or both as required.
- Click **Select a Test Device** drop-down arrow and choose a device for which you want to run these custom checks.
- Click **Open Command Runner** and enter the CLI commands.
- Expand the **Additional Criteria** area.
- Click the **Operation** drop-down arrow and choose **Activation**.
- Click the **Device Series** drop-down arrow and choose the device series for which you want to run these custom checks.
- Click **Save**.
- If you want to edit a custom check, click the corresponding More icon, choose **Edit**, make the required changes, and click **Save**.
- If you want to delete a custom check, click the corresponding More icon, choose **Delete**, and click **Delete** in the **Confirm Delete** message.

Step 8 Click **Next**.

Step 9 **Summary**: Review the Image upgrade settings. Click **Back** if you want to make any changes otherwise click **Submit**.

From the **Actions** drop-down list, choose **Software Images** > **Image Update Status** to check the status of the update.

Import ISSU Compatibility Matrix

In-Service Software Upgrade (ISSU) is a process that upgrades the image on a device without rebooting or with minimal interruption of service. For an example of the Cisco IOS XE ISSU compatibilty matrix for Catalyst Switches, see https://software.cisco.com/download/home/286315874/type/286326638/release/17.4.1.

You can download and import the ISSU compatibility matrix in Cisco DNA Center when you want to upgrade devices with ISSU.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Image Repository**.

Step 2 Click **Import**.

The **Import Image/Add-On** window appears.

Step 3 To import the ISSU compatibility matrix with a software image, do the following:

a) Click **Choose File** and browse to a software image or enter the URL of an HTTP or FTP source from which to import a software image.

b) If the image you are importing is for a third-party (non-Cisco) vendor, select **Third Party** under **Source**. Choose an **Application Type**, describe the device **Family**, and identify the **Vendor**.

c) Under **Select ISSU compatibility matrix**, click **Choose File** and browse to the ISSU compatibility matrix file.

d) Click **Import**.

Step 4 (Optional) To import the ISSU compatibility matrix for software images that are already imported, do the following:

a) Under **Select ISSU compatibility matrix**, click **Choose File** and browse to the ISSU compatibility matrix file.

b) Click **Import**.

Step 5 Click **Show Tasks** to view the ISSU compatibility matrix file **Import** status.

Upgrade a Software Image with ISSU

Upgrading devices using the In-Service Software Upgrade (ISSU) eliminates the need to reboot and reduces service interruption.

Before you begin

Before you upgrade a device using the ISSU, you must import the ISSU compatibility matrix file. See Import ISSU Compatibility Matrix, on page 97.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

Step 2 From the **Focus** drop-down list, choose **Software Images**. Select the device whose image you want to upgrade.

Step 3 From the **Actions** drop-down list, choose **Software Images** > **Update Image**.

The **Image Upgrade** window appears.

Step 4 In the **Analyze Selection** page, enable the ISSU upgrade:

a) Choose the device that you want to upgrade with ISSU.

Note See the **To Image** column to know the ISSU validation status.

- **ISSU shown in amber**: ISSU validation has failed because the selected image is not ISSU compatible.
- **ISSU shown in gray**: ISSU validation is success and the device supports ISSU.

b) From the ISSU drop-down list, choose **Enable ISSU Upgrade**.
c) Click **Next**.

Step 5 From the **Distribute** page, click **Now** to start the image distribution immediately or **Later** to schedule the distribution at a specific time.

To choose the validators you want to run for the current workflow and add new custom checks, do the following:

a) Hover your cursor over the Info icon to view the validation criteria and the CLI commands that are used for validation.
b) Click the toggle button to uncheck the validators that you do not want to run for the current workflow.
c) (Optional) To add new custom prechecks and postchecks, do the following:

- Click **add a new check** link to launch the **Add a New Custom Check** window.
- Enter the **Name** for the custom check.
- Click the **When** drop-down list and choose **pre**, **post**, or **both** as required.
- Click **Select a Test Device** drop-down list and choose a device for which you want to run these custom checks.
- Click **Open Command Runner** and enter the CLI commands.
- Expand the **Additional Criteria** area.
- Click the **Operation** drop-down arrow and choose **Distribution**.
- Click the **Device Series** drop-down arrow and choose the device series for which you want to run these custom checks.
- Click **Save**.
- If you want to edit a custom check, click the corresponding More icon, choose **Edit**, make the required changes, and click **Save**.
- If you want to delete a custom check, click the corresponding More icon, choose **Delete**, and click **Delete** in the **Confirm Delete** message.

Note

- If associated with a network hierarchy, an external image distribution server dispenses the image to all devices in the network hierarchy. See Add Image Distribution Servers to Sites, on page 95.
- If the image is already distributed for the selected device, click **Next**.
- If the **SWIM Events for ITSM (ServiceNow)** bundle is enabled, you need to update the image (distribute and activate) at a later time. Do not click **Now** to update the image.

  If you must update the image now, the bundle and its integration workflow (image update schedule approval in ServiceNow) must first be disabled. To access the bundle, choose **Platform** > **Manage** > **Bundles** > **SWIM Events for ITSM (ServiceNow)**. Click the **Disable** button in the **SWIM Events for ITSM (ServiceNow)** window. Wait a few seconds before proceeding to update the image, because the process to disable the bundle and workflow takes a few seconds.

Step 6 Click **Next**.

Step 7 From the **Activate** page, click **Now** to start the activation immediately or click **Later** to schedule the activation at a specific time.

To choose the validators you want to run for the current workflow and add new custom checks, do the following:

a) Hover your cursor over the Info icon to view the validation criteria and the CLI commands that are used for validation.
b) Click the toggle button to uncheck the validators that you do not want to run for the current workflow.
c) (Optional) To add new custom prechecks and postchecks, do the following:
   - Click **add a new check** link to launch the **Add a New Custom Check** window.
   - Enter the **Name** for the custom check.
   - Click the **When** drop-down list and choose **pre**, **post**, or **both** as required.
   - Click **Select a Test Device** drop-down list and choose a device for which you want to run these custom checks.
   - Click **Open Command Runner** and enter the CLI commands.
   - Expand the **Additional Criteria** area.
   - Click the **Operation** drop-down list and choose **Activation**.
   - Click the **Device Series** drop-down list and choose the device series for which you want to run these custom checks.
   - Click **Save**.
   - If you want to edit a custom check, click the corresponding More icon, choose **Edit**, make the required changes, and click **Save**.
   - If you want to delete a custom check, click the corresponding More icon, choose **Delete**, and click **Delete** in the **Confirm Delete** message.

Step 8 Click **Next**.

Step 9 From the **Summary** page, review the image upgrade settings. Click **Back** if you want to make any changes; otherwise click **Submit**.

From the **Actions** drop-down list, choose **Software Images** > **Image Update Status** to check the status of the update.

List of Device Upgrade Readiness Prechecks

Precheck	Description
File transfer check	Checks if the device is reachable through HTTPS and SCP. The default order of protocols is HTTPS first and then SCP.
NTP clock check	Compares device time and Cisco DNA Center time to ensure successful Cisco DNA Center certificate installation.
Flash check	Verifies if there is enough disk space for the update. If there is not enough disk space, a warning or error message is returned. For information about the supported devices for Auto Flash cleanup and how files are deleted, see Auto Flash Cleanup.
Config register check	Verifies the config registry value.
Crypto RSA check	Checks whether an RSA certificate is installed.

Precheck	Description
Crypto TLS check	Checks whether the device supports TLS 1.2.
IP Domain name check	Checks whether the domain name is configured.
Startup config check	Checks whether the startup configuration exists for the device.
NFVIS Flash check	Checks if the golden image is ready to be upgraded in the NFVIS device.
Service Entitlement check	Checks if the device has valid license.

View Image Update Status

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

Step 2 From the **Focus** drop-down list, choose **Software Images**.

Step 3 From the **Actions** drop-down list, choose **Software Images** > **Image Update Status**.

By default, the **Image Update Status** window shows all the recent image update tasks. You can click the down arrow and choose **Failed**, **In-progress**, or **Success** tasks.

Step 4 Click the down arrow corresponding to each task and do the following to view details of the task:

a) Click **Show Scripts** to view the precheck and postcheck status.
b) Click **View** to view the precheck and postcheck details.
c) Click **View Diff** to view the precheck and postcheck difference.

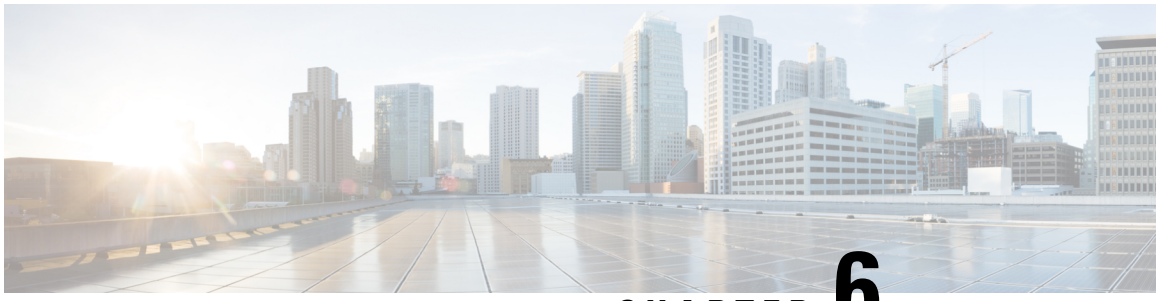
Auto Flash Cleanup

During the device upgrade readiness precheck, the flash check verifies whether there is enough space on the device to copy the new image. If there is insufficient space:

- **For devices that support auto flash cleanup**, the flash check fails with a warning message. For these devices, the auto cleanup process is attempted during the image distribution process to create the sufficient space. As a part of the auto flash cleanup, Cisco DNA Center identifies unused .bin, .pkg, and .conf files and delete them iteratively until enough free space is created on the device. Image distribution is attempted after the flash cleanup. You can view these deleted files in **Sytem** > **Audit Logs**.

Note Auto flash cleanup is supported on all devices except Nexus switches and Wireless controllers.

- **For devices that do not support auto flash cleanup**, the flash check fails with an error message. You can delete files from device flash to create required space before starting the image upgrade.



CHAPTER 6

Display Your Network Topology

About Topology

The **Topology** window displays a graphical view of your network. Using the Discovery settings that you have configured, Cisco DNA Center discovers the devices in your network and assigns a device role to them. Based on the device role assigned during discovery (or changed in Device Inventory), Cisco DNA Center creates a physical topology map with detailed device-level data.

Using the topology map, you can do the following:

- Display the topology of a selected area, site, building, or floor.
- Display detailed device information.
- Display detailed link information.
- Filter devices based on a specific Layer 2 VLAN.
- Filter devices based on a Layer 3 protocol (such as Intermediate System - Intermediate System [IS-IS], Open Shortest Path First [OSPF], Enhanced Interior Gateway Routing Protocol [EIGRP], or static routing).
- Filter devices with Virtual Routing and Forwarding (VRF) capability.
- Pin devices to the topology map.
- Save a topology map layout.
- Open a topology map layout.

- Export screen shots of the complete topology layout in PNG format.

Display the Topology of Areas, Sites, Buildings, and Floors

You can display the topology of an area, site, building, or floor.

Before you begin

- Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.
- You must have defined a network hierarchy and provisioned devices to the buildings or floors within it.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Tools** > **Topology**.

Step 2 In the left tree view menu, select the area, site, building, or floor that you are interested in.

Step 3 Use the Toggle button  to switch between the Geographical map view and the Layer 2 map view.

The Geographical map view displays the sites. The nearer sites are grouped together and indicated with the number of sites in the group. The device health is indicated in different colors. Hover over the site to view the detailed device health.

Use the Search field in the top right corner to find a building in the Geographical map view, and a device in the Layer 2 map view.

Note

- Click the icon in the lower-right corner to open a legend that shows the available shortcut keys for the topology maps.
- Click the **Toggle Annotate** icon to draw annotations in the Layer 2 map. You can click the export icon to export the topology map along with the annotations.

Step 4 Click **Take a Tour** to know the details of various options available in the Topology page.

Filter Devices on the Topology Map

You can filter devices based on one of the following attributes:

- VLAN
- Routing
- VRF
- Tagging

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Topology**.

Step 2 Click **Filter**.

Note If you are not able to view the **Filter**, click a site in the left tree view menu.

Step 3 Do one of the following:

- From the **VLAN** drop-down list, choose the VLAN that you want to view.
- From the **Routing** drop-down list, choose the protocol that interests you.
- From the **VRF** drop-down list, choose the VRF that you want to view.
- Click **View All Tags** and choose the tags you want to view. The devices associated with the selected tags will be highlighted. If you want to create a new tag, do the following:

a) Click **Create New Tag**.
b) Enter the **Tag Name**.
c) Click **Save**.

You can also associate a device with the tag by doing the following:

a) Click the device.
b) Click **Tag Device**.
c) Select the tag to which you want to associate the device.
d) Click **Apply**.

Display Device Information

Cisco DNA Center allows you to display the device name, IP address, and software version of devices.

Note The device information that is accessible in the **Topology** window is also accessible in the **Device Inventory** window.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Topology**.

Step 2 In the tree view menu, select the area, site, building, or floor that you are interested in.

Step 3 In the topology area, hover your mouse over the device or device group that interests you.

Note A device group is labeled with the number and types of devices it contains. A blue arrow under a switch indicates that switch has a host. Click the blue arrow to view the host.

Step 4 Click **Display** and enable the following items to view additional device details. For more information, hover your mouse over the ⓘ icon next to the items.

- **Device Health**: Displays the health of the devices.
- **Link Health**: Displays the health of the links between the devices.
- **License status**: Displays the license status of the device. Cisco DNA Center highlights a device if its license is about to expire and a warning icon appear next to it. Click the highlighted device to view its license details.
- **Device IP**: Displays device IP address under device label.
- **Device Suffixes**: Displays full name of the device, with its suffix.

Note Topology uses Link Layer Discovery Protocol (LLDP) to determine the neighbor devices when network devices are not configured with Cisco Discovery Protocol (CDP) in Cisco DNA Center.

Display Link Information

Cisco DNA Center allows you to display information about the links in the topology map. For simple links, the display shows information for the single link. For aggregated links, the display shows a listing of all the underlying links. The information includes the interface name, its speed, and its IP address.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Topology**.

Step 2 In the tree view menu, select the area, site, building, or floor that you are interested in.

Step 3 Hover your cursor over the link that interests you.

Step 4 Click **Display** and enable **Link Health**.

A down link is shown in red. If you want to delete the link, select it and click **Delete**. You can bring the link up by doing the following:

a) Log in to the device.
b) Enable the interface.
c) Resynchronize the device on the Inventory page.

Note Topology uses Link Layer Discovery Protocol (LLDP) to determine the links for devices that are discovered using LLDP in Cisco DNA Center.

Pin Devices to the Topology Map

Devices can be grouped or aggregated so that they take up less room on the map. However, at times, you might want to separate a device from its group. You can do this by pinning a device to the map.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Topology**.

Step 2 Do one of the following:

- To pin a device, click the device group, and in the dialog box, click the pin icon to the left of the device name.
- To pin all the devices, click the device group, and, in the dialog box, click **Pin All**.

Note Double click the group to unpin the devices in the group.

Assign Devices to Sites

Devices can be assigned to specific sites using the topology map.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Topology**.

Step 2 Click **Unassigned Devices** in the left pane. All the unassigned devices are displayed in the topology area.

Step 3 Click the device for which you want to assign a site. Device details are displayed in a pop-up window. In the **Assign devices to:** section, click the **choose the location** drop-down list to select a location.

Step 4 (Optional) To assign the site only for the selected device and not for the connected (downstream) devices, uncheck the **Auto-assign unclaimed downstream devices** check box.

Step 5 Click **Assign**.

Save a Topology Map Layout

Cisco DNA Center has a Cisco recommended topology layout that is displayed by default when you open the topology tool. You can customize multiple layouts and save them to view later. You can also set one of the layouts as the default to be displayed when you open the topology map.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Tools** > **Topology**.

Step 2 Click **Custom View**.

Step 3 In the **Enter View Title** field, enter a name for your customized map.

Step 4 Click **Save**.

Step 5 (Optional) To set your customized map as the default, click **Make Default**.

Open a Topology Map Layout

You can open previously saved topology maps.

Before you begin

You should have saved topology map layouts.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Tools** > **Topology**.

Step 2 Click **Custom View**.

Step 3 Click the name of the map that you want to display.

Export the Topology Layout

You can export a snapshot of the full topology layout. The snapshot is downloaded as a SVG, PDF, PNG file to your local machine.

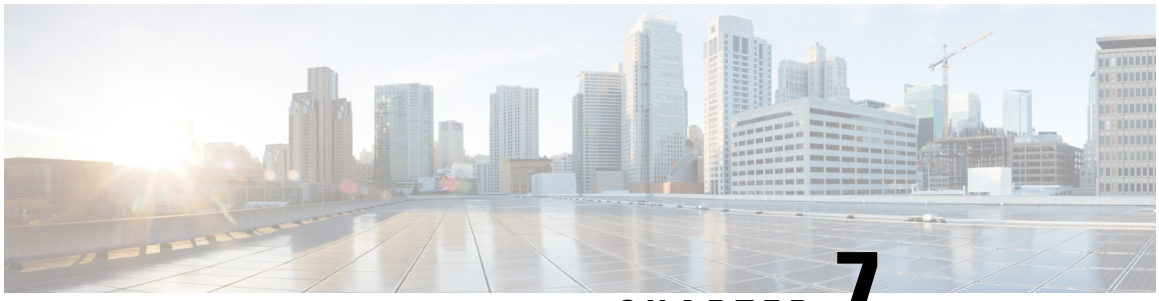
Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Tools** > **Topology**.

Step 2 Click (this icon represents **Export Topology**).

Step 3 Select a file format and click **Export**.



CHAPTER 7

Design Network Hierarchy and Settings

Design a New Network Infrastructure

The **Design** area is where you create the structure and framework of your network, including the physical topology, network settings, and device type profiles that you can apply to devices throughout your network.

Use the **Design** workflow if you do not already have an existing infrastructure. If you have an existing infrastructure, use the **Discovery** feature. For more information, see About Discovery, on page 21.

You can perform these tasks in the **Design** area:

Step 1 Create your network hierarchy. For more information, see Create a Site in a Network Hierarchy, on page 111.

Step 2 Define global network settings. For more information, see About Global Network Settings, on page 173.

Step 3 Define network profiles.

About Network Hierarchy

You can create a network hierarchy that represents your network's geographical locations. Your network hierarchy can contain sites, which in turn contain buildings and areas. You can create site and building IDs to easily identify where to apply design settings or configurations later. By default, there is one site called **Global**.

The network hierarchy has a predetermined hierarchy:

- **Areas** or **Sites** do not have a physical address, such as the United States. You can think of areas as the largest element. Areas can contain buildings and subareas. For example, an area called United States can contain a subarea called California, and the subarea California can contain a subarea called San Jose.
- **Buildings** have a physical address and contain floors and floor plans. When you create a building, you must specify a physical address and latitude and longitude coordinates. Buildings cannot contain areas. By creating buildings, you can apply settings to a specific area.
- **Floors** are within buildings and consist of cubicles, walled offices, wiring closets, and so on. You can add floors only to buildings.

You can change the site hierarchy for unprovisioned devices while preserving AP locations on sitemaps. Note, however, that you cannot move an existing floor to a different building.

The following is a list of tasks that you can perform:

- Create a new network hierarchy. For more information, see Create a Site in a Network Hierarchy, on page 111.
- Upload an existing network hierarchy from Cisco Prime Infrastructure. For more information, see Upload an Existing Site Hierarchy, on page 113.

Guidelines for Image Files to Use in Maps

- Use a graphical application that can save the map image files to any of these formats: .jpg, .gif, .png, .dxf, and .dwg.
- Ensure that the dimension of an image is larger than the combined dimension of all the buildings and outside areas that you plan to add to the campus map.
- Map image files can be of any size. Cisco DNA Center imports the original image to its database at a full definition, but during display, it automatically resizes them to fit the workspace.

- Obtain the horizontal and vertical dimensions of the site in feet or meters before importing. This helps you to specify these dimensions during map import.

Create a Site in a Network Hierarchy

Cisco DNA Center allows you to easily define physical sites and then specify common resources for those sites. The **Design** area uses a hierarchical format for intuitive use, while eliminating the need to redefine the same resource in multiple places when provisioning devices. By default, there is one site called **Global**. You can add more sites, buildings, and areas to your network hierarchy. You must create at least one site before you can use the provision features.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

A world map is displayed in the right pane.

Step 2 In the **Network Hierarchy** window, click **+ Add Site** > **Add Area** or click the gear icon ⚙ next to the parent site in the left pane, and then click **Add Area**.

Step 3 Enter a name for the site in the **Area Name** field.

Step 4 From the **Parent** drop-down list, choose a parent node.

By default, **Global** is the parent node.

Step 5 Click **Add**.

The site is created under the parent node in the left pane.

You can also upload an existing hierarchy.

Export a Site Hierarchy from Cisco Prime Infrastructure and Import into Cisco DNA Center

A network hierarchy is a representation of your network's geographical locations. You create site and building IDs so that later you can easily identify where to apply design settings or configurations. If you have an existing network hierarchy on Cisco Prime Infrastructure, you can import it into Cisco DNA Center, saving time and effort spent in creating a new network hierarchy.

This is a simple process that requires you to export two files from Cisco Prime Infrastructure as a CSV file that contains location groups or site information, and a map archive file that contains various floor maps in your network hierarchy.

This procedure describes how to export an existing site hierarchy from Cisco Prime Infrastructure to Cisco DNA Center. You can export a site hierarchy from Cisco Prime Infrastructure Release 3.2 and later.

Before you begin

- Make sure that you have Cisco Wireless Controllers and Access Points in your inventory. If not, discover them using the **Discovery** feature.
- Add and position APs on a floor map.
- If you manually created any sites in Cisco DNA Center that are present in Cisco Prime Infrastructure, you must remove those sites manually before importing them into Cisco DNA Center.

Step 1 Export the location groups from Cisco Prime Infrastructure as a CSV file to your workstation. In Cisco Prime Infrastructure, choose **Inventory** > **Group Management** > **Network Device Groups**.

Step 2 In the **Device Groups** window, click **Export Groups**.

Step 3 In the **Export Groups** dialog box, click the **APIC-EM** radio button to download the CSV file, and click **OK**.

Wait for the CSV file to download. The CSV file contains information about the geographic locations of various sites, buildings, and floors and their hierarchy in the network.

Step 4 Export maps from Cisco Prime Infrastructure. This downloads map information, such as floor dimension, and calibration information, such as the Radio Frequency (RF) attenuation model that has been applied to each floor in Cisco Prime Infrastructure.

To export maps, choose **Maps** > **Wireless Maps** > **Site Maps (New)**.

Step 5 From the **Export** drop-down list, choose **Map Archive**.

The **Export Map Archive** window appears, and the **Select Sites** window appears by default.

Step 6 Check the check box of a specific site, campus, building, or floor that you want to export. Alternately, check the **Select All** check box to export all the maps.

Step 7 Check if the **Map Information** and **Calibration Information** are selected. Selecting one option is mandatory. If not, click the **On** button for **Map Information** or **Calibration Information**.

- Selecting **Map Information** exports floor dimensions such as length, width, and height. It also exports details about the APs that have been placed on the floor maps, and the obstacles and areas overlayed on the floor maps within Cisco Prime Infrastructure.
- Selecting **Calibration Information** exports the RF attenuation model that has been applied to each floor in Cisco Prime Infrastructure. It is a good practice to export the existing calibration data from Cisco Prime Infrastructure. Otherwise, you must enter the calibration details manually in Cisco DNA Center.

Step 8 Click **Generate Map Archive**.

A tar file that contains the various floor maps in your network hierarchy is created and saved on your workstation.

Step 9 To import the site hierarchy to Cisco DNA Center, in the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**, and then choose **Import** > **Import Sites**.

A world map is displayed in the right pane.

Step 10 In the **Import Sites** window, drag and drop the Cisco Prime Infrastructure location groups CSV file. Alternately click **Select CSV from your computer** to navigate to where the file is located, and click **Import** to import the Cisco Prime Infrastructure location groups CSV file.

Step 11 Import the map archive file that contains floor maps and related map information. Choose **Design** > **Network Hierarchy**, and then choose **Import** > **Import Prime Maps**.

Step 12 In the **Import Prime Maps Archive** window, drag and drop the map archive file, or click **click to select** to select the file from your workstation.

Step 13 Click **Save**.

Upload an Existing Site Hierarchy

You can upload a CSV file or a map archive file that contains an existing network hierarchy. For example, you can upload a CSV file with location information that you exported from Cisco Prime Infrastructure. (For information about exporting maps from Cisco Prime Infrastructure, see Export Maps Archive, on page 113.)

Note Before importing a map archive file into Cisco DNA Center, make sure that the devices such as Cisco Wireless Controllers and the associated APs are discovered and listed on the Cisco DNA Center inventory page.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy** and then choose **Import** > **Import Sites**.

A world map is displayed in the right pane.

Step 2 Drag and drop your CSV file, or navigate to where your CSV file is located, then click **Import**.

If you do not have an existing CSV file, click **Download Template** to download a CSV file that you can edit and upload.

Step 3 To import the Cisco Prime Infrastructure maps tar.gz archive file, choose **Import** > **Map Import**.

Step 4 Drag and drop the map archive file into the boxed area in the **Import Site Hierarchy Archive** dialog box, or click the **click to select** link and browse to the archive file.

Step 5 Click **Save** to upload the file.

The **Import Preview** window appears, which shows the imported file.

Export Maps Archive

You can export maps archive files from Cisco Prime Infrastructure and import them into Cisco DNA Center.

Step 1 From the Cisco Prime Infrastructure user interface, choose **Maps** > **Wireless Maps** > **Site Maps (New)**.

Step 2 From the **Export** drop-down list, choose **Map Archive**.

Step 3 On the **Select Sites** window, configure the following. You can either select map information or calibration information to be included in the maps archive.

- **Map Information**: Click the **On or Off** button to include map information in the archive.
- **Calibration Information**: To export calibration information, click the **On or Off** button. Click the **Calibration Information for selected maps** or the **All Calibration Information** radio button. If you select **Calibration Information for selected maps**, the calibration information for the selected site maps is exported. If you select **All Calibration Information**, the calibration information for the selected map, along with additional calibration information that is available in the system, is also exported.
- In the **Sites** left pane, check one or more check boxes of the site, campus, building floor, or outdoor area that you want to export. Check the **Select All** check box to export all the maps.

Step 4 Click **Generate Map Archive**. A message `Exporting data is in progress` is displayed.
A tar file is created and is saved to your local machine.

Step 5 Click **Done**.

Export a Global Maps Archive

You can export a complete network global hierarchy map, or choose the hierarchy of a site, a building, or a floor that the hierarchy map downloads to an archive file. The map archive file contains data such as date and time, number of floors, and APs.

Note You can export up to 500 floors.

Before you begin

To perform the following task, you must be a **Super Admin** or **Network Admin**.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 To export the complete network map, choose **Export** > **Export Maps**. Alternatively, click the gear icon next to the desired site, building, or floor in the left pane and choose **Export Maps**.

- If you choose a site and click **Export Maps**, the site map containing all the subsites, buildings, and floors is exported.
- If you choose a building and click **Export Maps**, the building map containing all the floors is exported.
- If you choose a floor and click **Export Maps**, only the chosen floor map is exported.

Step 3 In the Export Maps Archive window, do one of the following:

- In the **File Name** field, enter a filename, click **Export**, and click **OK**.

  A new tar file containing the selected maps archive file is created and saved on your computer.

- In the **File Name** field, enter an existing filename and click the **Click to select** link to choose the existing file from your computer. Click **OK**.

  The maps are archived in the chosen file and saved in your computer.

Export Site Hierarchy

You can export the complete hierarchy of a site that downloads to a CSV format file. The site hierarchy file contains details such as site names, parent hierarchy, number of floors, location, and site address.

The following procedure explains how to export a site hierarchy:

Before you begin

To perform the following task, you must be a **Super Admin** or **Network Admin**.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 To export the complete site hierarchy, choose **Export** > **Export Sites**. Alternatively, click more icon next to **Global** and choose **Export Sites**.

Step 3 In the **Export Sites** dialog box, click **OK**.
The complete site hierarchy file containing site names, parent hierarchy, number of floors, location, and address is exported in CSV format and saved in your computer.

Search the Network Hierarchy

You can search the network hierarchy to quickly find a site, building, or area. This is particularly helpful after you have added many sites, areas, or buildings.

To search the tree hierarchy, in the **Find Hierarchy** search field in the left pane and enter either the partial or full name of the site, building, or floor name that you are searching. The tree hierarchy is filtered based on the text you enter in the search field.

Edit Sites

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, navigate to the corresponding site that you want to edit.

Step 3 Click the gear icon ⚙ next to the site and select **Edit Site**.

Step 4 Make the necessary changes, and click **Update**.

Delete Sites

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, navigate to the site that you want to delete.

Step 3 Click the gear icon ⚙ next to the corresponding site and select **Delete Site**.

Step 4 Confirm the deletion.

Add Buildings

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

A world map is displayed in the right pane.

Step 2 In the **Network Hierarchy** window, click **+Add Site** > **Add Building**, or click the gear icon ⚙ next to the parent site in the left pane and select **Add Building**.

You can also upload an existing hierarchy.

Step 3 In the **Building Name** field, enter a name for the building.

The building name can contain all special characters except for " & ? ' / < > are allowed.

Step 4 From the **Parent** drop-down list, choose a parent node.

By default, **Global** is the parent node.

Step 5 In the **Address** field, enter an address. If you are connected to the Internet, as you enter the address, the Design Application narrows down the known addresses to the one you enter. The user can move the marker to change the position on the map. When you see that the correct address appears in the window, select it. When you select a known address, the **Longitude** and **Latitude** coordinates fields are automatically populated.

Step 6 Click **Add**.

The building that you created is added under the parent site in the left menu.

Step 7 To add another area or building, in the hierarchy frame, click the gear icon next to an existing area or building that you want to be the parent node.

Edit a Building

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Design** > **Network Hierarchy**.

Step 2 In the left tree pane, navigate to the building that you want to edit.

Step 3 Click the gear icon next to the building and select **Edit Building**.

Step 4 Make the necessary changes in the **Edit Building** window, and click **Update**.

Delete a Building

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, navigate to the building that you want to delete.

Step 3 Click the gear icon next to the building and select **Delete Building**.

Step 4 Confirm the deletion.

Note Deleting a building deletes all its container maps. APs from the deleted maps are moved to Unassigned state.

Add a Floor to a Building

After you add a building, create floors and upload a floor map.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Design** > **Network Hierarchy**.

Step 2 Expand the **Global** site and the previously created area to see all the previously created buildings.

Step 3 Click the gear icon next to the building to which you want to add a floor, and then click **Add Floor**.

Step 4 Enter a name for the floor. The floor name contain upto 21 characters. has a 21.

The floor name can contain all special characters except for & > < ? ' / [ ] are not allowed.

The floor name can start with a letter or a hyphen (-) and the string following the first character can include one or more of the following:

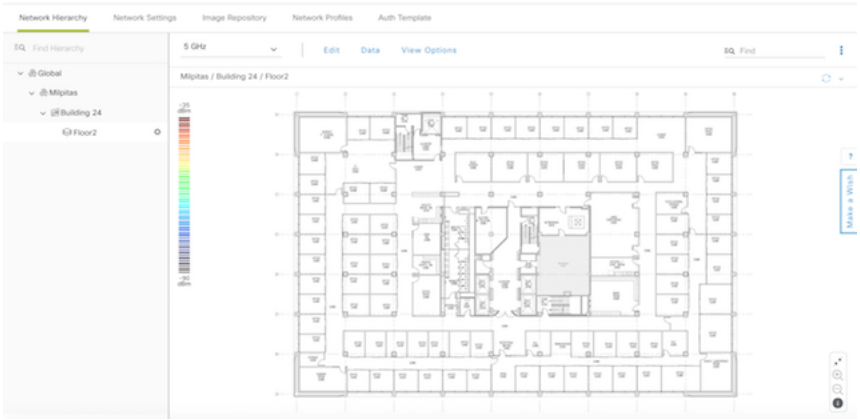
- Upper or lower case letters or both
- Numbers
- Underscores (_)
- Hyphens (-)
- Periods (.)
- Spaces ( )

Step 5 Define the type of floor by choosing the Radio Frequency (RF) model from the **Type (RF Model)** drop-down list: **Indoor High Ceiling**, **Outdoor Open Space**, **Drywall Office Only**, and **Cubes And Walled Offices**. This defines if the floor is an open space or a drywall office, and so on. Based on the RF model selected, the wireless signal strength and the distribution of heatmap is calculated.

Step 6 You can drag a floor plan on to the map or upload a file. Cisco DNA Center supports the following file types: .jpg, .gif, .png, .dxf, and .dwg.

After you import a map, make sure that you mark the Overlay Visibility as **On** (**Floor** > **View Option** > **Overlays**). By default, overlays are not displayed after you import a map.

Figure 3: Example of a Floor Plan



Step 7 Click **Add**.

Edit a Floor

After you add a floor, you can edit the floor map so that it contains obstacles, areas, and APs on the floor.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Design** > **Network Hierarchy**.

Step 2 Expand the network hierarchy to find the floor that you want to edit, or enter the floor name in the **Search Hierarchy** text field in the left pane.

Step 3 Make the necessary changes in the **Edit Floor** dialog window, and click **Update**.

Monitor a Floor Map

The floor view navigation pane provides access to multiple map functions like:

- Use the **Find** feature located at the top-right corner of the floor map window to find specific floor elements such as APs, sensors, clients, and so on. The elements that match the search criteria are displayed on the floor map along with a table in the right pane. When you hover your mouse over the table, it points to the search element on the floor map with a connecting line.
- Click the icon at the top-right corner of the floor map window to:
  - Export a floor plan as a PDF.
  - Measure the distance on the floor map.
  - Set the scale to modify the floor dimensions.
- Click the icon at the bottom-right of the floor map window to zoom in on a location. The zooming levels depend upon the resolution of an image. A high-resolution image might provide more zoom levels. Each zoom level comprises of a different style map shown at different scales, each one showing the corresponding details. Some maps are of the same style, but at a smaller or larger scale.
- Click the icon to see a map with fewer details.
- Click the icon to view the map icon legend.

Edit Floor Elements and Overlays

Using the **Edit** option available on the floor area, you can:

- Add, position, and delete the following floor elements:
  - Access Points
  - Sensors
- Add, edit, and delete the following overlay objects:
  - Coverage Areas
  - Obstacles
  - Location Regions

- Rails
- Markers
- GPS Markers

Guidelines for Placing Access Points

Follow these guidelines while placing APs on the floor map:

- Place APs along the periphery of coverage areas to keep devices close to the exterior of rooms and buildings. APs placed in the center of these coverage areas provide good data on devices that would otherwise appear equidistant from all other APs.
- Location accuracy can be improved by increasing overall AP density and moving APs close to the perimeter of the coverage area.
- In long and narrow coverage areas, avoid placing APs in a straight line. Stagger them so that each AP is more likely to provide a unique snapshot of the device location.
- Although the design provides enough AP density for high-bandwidth applications, location suffers because each AP view of a single device is not varied enough. Therefore, location is difficult to determine. Move the APs to the perimeter of the coverage area and stagger them. Each has a greater likelihood of offering a distinctly different view of the device, resulting in higher location accuracy.
- For optimal heatmap visibility on floor maps, configure the AP height to approximately 10 feet (3 meters) or lower.

Add, Position, and Delete APs

Cisco DNA Center computes heatmaps for the entire map that show the relative intensity of the Radio Frequency (RF) signals in the coverage area. The heatmap is only an approximation of the actual RF signal intensity because it does not consider the attenuation of various building materials, such as drywall or metal objects, nor does it display the effects of RF signals bouncing off obstructions.

Make sure that you have Cisco APs in your inventory. If not, discover APs using the Discovery feature. See About Discovery, on page 21.

Cisco DNA Center supports the following 802.11ax APs:

- Cisco Catalyst 9120 Access Points
- Cisco Catalyst 9117 Access Points
- Cisco Catalyst 9115 Access Points
- Cisco Catalyst 9100 Access Points

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, select the floor.

Step 3 Click **Edit**, which is located above the floor plan in the middle pane.

Step 4 In the **Floor Elements** panel, next to **Access Points**, click **Add**.

Access points that are not assigned to any floors appear in the list.

Step 5 On the **Add APs** window, check the check boxes of the access points to select the APs in bulk, and click **Add Selected**. Alternatively click **Add** next to an access point.

Note You can search for access points using the search option available. Use the **Filter** field to search for access points using the AP name, MAC address, model, or Cisco Wireless Controller. The search is case-insensitive. The search result appear in a table. Click **Add** to add one or more of these APs to the floor area.

Step 6 Close the **Add APs** window after assigning APs to the floor area.

Step 7 Newly added APs appear on the top-right corner of the floor map.

Step 8 In the **Floor Elements** pane, next to Access Points, click **Position** to position the APs correctly on the map.

- To position the APs, click an AP and drag and drop it to the appropriate location on the floor map. Alternatively you can update the x and y coordinates and AP Height in the **Selected AP Details** window. When you drag an access point on the map, its horizontal (x) and vertical (y) position appears in the text field. When selected, the access point details are displayed in the right pane. The **Selected AP Details** window displays the following:
  - **Position by 3 points**: You can draw three points on the floor map and position APs using the points created. To do this:
    a. Click **Position by 3 points**.
    b. To define the points, click anywhere on the floor map to start drawing the first point. Click again to finish drawing a point. A dialog box appears to set the distance to first point. Enter the distance, in meters, and click **Set Distance**.
    c. Define the second and third points similarly, and click **Save**.
  - **Position by 2 Walls**: You can define two walls on the floor map and position APs between the defined walls. This helps you to know the position of APs between the two walls. This helps you to understand the AP position between the walls.
    a. Click **Position by 2 walls**.
    b. To define the first wall, click anywhere on the floor map to start drawing the line. Click again to finish drawing a line. A dialog box appears to set the distance to the first wall. Enter the distance in meters and click **Set Distance**.
    c. Define the second wall similarly and click **Save**.

       The AP is placed automatically as per the defined distance between the walls.
  - **AP Name**: Shows the AP name.
  - **AP Model**: Indicates the AP model for the selected access point.
  - **MAC Address**: Displays the MAC address.
  - **x**: Indicates the horizontal span of the map, in the selected unit of measurement (either feet or meters).
  - **y**: Indicates the vertical span of the map, in the selected unit of measurement (either feet or meters).
  - **AP Height**: Indicates the height of the access point, in the selected unit of measurement (either feet or meters).

For each of the access point's radios:

- **Protocol**: Protocol for a radio: 802.11a/n/ac, 802.11b/g/n, or 802.11a/b/g/n.
- **Antenna**: Antenna type for a radio.

  Note While internal radios have only one antenna type, there may be several external antenna types to choose from.

- **Antenna Image**: Shows the antenna image (or AP image for an internal antenna).
- **Antenna Orientation**: Indicates the Azimuth and the Elevation orientations, in degrees.
- **Azimuth**: Horizontal angle of the antenna, measured clockwise relative to the x axis (so 0 azimuth indicates that the antenna is pointing right). The azimuth range is from 0 to 360.

  Note While most directional antennas reach maximum gain facing the azimuth, some antennas attain it by facing 90 degrees away from the azimuth. In those cases, if you configure an AP's azimuth to 0 (pointing right), the highest gain of the generated heatmap will point down. And if you configure the azimuth to 270 (pointing up), the highest gain of the generated heatmap will point right.

- **Elevation**: Vertical angle of the antenna. In wall-mounted antennas, elevation is measured relative to the horizontal axis. So, 45 degrees indicates that the antenna is pointing 45 degrees up, and -45 degrees means that the antenna is pointing 45 degrees down. In ceiling-mounted antennas, elevation is measured relative to the vertical axis. So, 45 degrees indicates that the antenna is pointing 45 degrees towards the azimuth, and -45 degrees means that the antenna is pointing 45 degrees in the opposite direction. The elevation range is -90 to 90 degrees.

Step 9 After you have completed placing and adjusting access points, click **Save**.

The heatmap is generated based on the new position of the AP.

If a Cisco Connected Mobile Experiences (CMX) is synchronized with Cisco DNA Center, you can view the location of clients on the heatmap. See Create Cisco CMX Settings, on page 159.

Step 10 In the **Floor Elements** panel, next to **Access Points**, click **Delete**.
The **Delete APs** window appears, listing all the assigned and placed access points.

Step 11 Check the check boxes next to the access points that you want to delete, and click **Delete Selected**.

- To delete all the access points, click **Select All** and then **Delete Selected**.
- To delete an access point from the floor, click the **Delete** icon.
- Use **Quick Filter** and search using the AP name, MAC address, model, or controller. The search is case-insensitive. The search result appears in the table. Click the **Delete** icon to delete the APs from the floor area.

Export Bulk APs from Prime Infrastructure and Import into Cisco DNA Center

Cisco DNA Center allows you to import, assign and position a collection of access points to the floor map. If you have an existing collection of access points on Cisco Prime Infrastructure, you can import it into Cisco DNA Center, saving time and effort spent in importing, assigning, and positioning access points to the floor map.

This procedure describes how to export an existing collection of access points from Cisco Prime Infrastructure, and import into Cisco DNA Center.

Before you begin

- To perform the following task, you must be a **Super Admin** or **Network Admin**.
- Make sure that you have APs in your inventory. If not, discover them using the **Discovery** feature.
- Add and position APs on a floor map.
- The site, building, and floor must be present in the site hierarchy.

Step 1 Export the bulk AP positions from Cisco Prime Infrastructure as a CSV file to your workstation.

Step 2 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

A world map is displayed in the right pane.

Step 3 You can either import the bulk APs by selecting the desired site in the left pane and from the **Import** drop-down list, choose **Import Bulk AP**, or click the gear icon next to the desired site in the left pane and choose **Import Bulk AP**.

Step 4 In the **Import Bulk AP** window, drag and drop the AP file, or click **Choose a file** to select the file from your workstation.

Note
- To manually create the **AP Positions** CSV file with Prime Template, export a Prime Template to your workstation by clicking **Download Prime Template**. Prime Template does not support nested files.
- To manually create the **AP Positions** CSV file with Cisco DNA Template, export a Cisco DNA Template to your workstation by clicking **Download Template**. Cisco DNA Template supports nested files.

Wait for the CSV file to download. The CSV file contains information about AP positions of various sites in the network.

Step 5 Click **Import**.

The **Import Summary** window appears.

- The **Information** tab shows the list of successfully imported APs.
- Click the **Warning** tab to see the list of warnings.
- Click the **Error** tab to see the list of errors.

Quick View of APs

Hover your cursor over the AP icon on the floor map to view AP details, Rx neighbor information, client information, and Device 360 information.

- Click **Info** to view the following AP details:
  - **Associated**: Indicates whether an AP is associated or not.
  - **Name**: AP name.
  - **MAC Address**: MAC address of the AP.

- **Model**: AP model number.
- **Admin/Mode**: Administration status of the AP mode.
- **Type**: Radio type.
- **OP/Admin**: Operational status and AP mode.
- **Channel**: Channel number of the AP.
- **Antenna**: Antenna name.
- **Azimuth**: Direction of the antenna.

- Click the **Rx Neighbors** radio button to view the immediate Rx neighbors for the selected AP on the map with a connecting line. The floor map also shows whether the AP is associated or not along with the AP name.
- Click **Device 360** to get a 360° view of a specific network element (router, switch, AP, or Cisco wireless controller).

Note For Device 360 to open, you must have the Assurance application installed.

Add, Position, and Delete Sensors

Note Make sure you have the Cisco AP 1800S sensor in your inventory. The Cisco Aironet 1800s Active Sensor must be provisioned using Plug and Play for it to show up in the Inventory.

A *sensor device* is a dedicated AP 1800s sensor. The Cisco Aironet 1800s Active Sensor gets bootstrapped using PnP. After it obtains the Assurance server reachability details, it directly communicates with the Assurance server.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, select the floor.

Step 3 Click **Edit**, which is located above the floor plan.

Step 4 In the **Floor Elements** panel, next to **Sensors**, click **Add**.

Step 5 On the **Add Sensors** window, check the check boxes of the sensors that you want to add. Alternatively, click **Add** next to the sensor row to add sensors.

Note You can search for specific sensors using the search option. Use the **Filter** field and search using the name, MAC address, or model of a sensor. The search is case-insensitive. The search results are displayed in the table. Click **Add** to add one or more these sensors to the floor area.

Step 6 Close the **Add Sensors** window after assigning sensors to the floor map.
Newly added sensors appear on the top-right corner of the floor map.

Step 7 To position the sensors correctly, in the **Floor Elements** pane, next to **Sensors**, click **Position** to place them correctly on the map.

Step 8 After you have completed placing and adjusting sensors, click **Save**.

Step 9 To delete a sensor, in the **Floor Elements** pane, next to **Sensors**, click **Delete**.
The **Delete Sensors** window lists all the assigned and placed sensors.

Step 10 Check the check boxes of the sensors that you want to delete, and click **Delete Selected**.

- To delete all the sensors, click **Select All**, and click **Delete Selected**.
- To delete a sensor from the floor, click the **Delete** icon next to that sensor.
- Use **Quick Filter** and search using the name, MAC address, or model. The search is case-insensitive. The search results are displayed in a table. Click the **Delete** icon to delete one or more sensors from the floor area.

Add Coverage Areas

By default, any floor area or outside area defined as part of a building map is considered as a wireless coverage area.

If you have a building that is nonrectangular or you want to mark a nonrectangular area within a floor, you can use the map editor to draw a coverage area or a polygon-shaped area.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, select the floor.

Step 3 Click **Edit**, which is located above the floor plan in the middle pane.

Step 4 In the **Overlays** panel, next to **Coverage Areas**, click **Add**.
The **Coverage creation** dialog-box appears.

Step 5 To draw a coverage area, from the **Type** drop-down list, choose **Coverage Area**.

a. Enter the name of the area you are defining, and click **Add Coverage**. The coverage area must be a polygon with at least 3 vertices.

b. Move the drawing tool to the area you want to outline.

c. Click the tool to start and stop a line.

d. After you have outlined the area, double-click the area, which results in the area getting highlighted.

Note The outlined area must be a closed object for it to be highlighted on the map.

Step 6 To draw a polygon-shaped area, from the **Type** drop-down list, choose **Perimeter**.

a. Enter the name of the area you are defining, and click **Ok**.

b. Move the drawing tool to the area you want to outline.

- Click the tool to start and stop a line.
- After you have outlined the area, double-click the area, which results in area getting highlighted on the page.

Step 7 To edit a coverage area, in the **Overlays** panel, next to **Coverage Areas**, click **Edit**.

The available coverage areas are highlighted on the map.

Step 8 Make the changes and click **Save** after the changes.

Step 9 To delete a coverage area, in the **Overlays** panel, next to **Coverage Areas**, click **Delete**.

The available coverage areas are highlighted on the map.

Step 10 Hover your cursor over the coverage area and, click delete.

Step 11 Click **Save** after the deletion.

Create Obstacles

You can create obstacles so that they can be considered while computing Radio Frequency (RF) prediction heatmaps for access points.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, select the floor.

Step 3 Click **Edit**, which is located above the floor plan in the middle pane.

Step 4 In the **Overlays** panel, next to **Obstacles**, click **Add**.

Step 5 In the **Obstacle Creation** dialog box, choose an obstacle type from the **Obstacle Type** drop-down list. The type of obstacles that you can create are **Thick Wall**, **Light Wall**, **Heavy Door**, **Light Door**, **Cubicle**, and **Glass**.
The estimated signal loss for the obstacle type you selected is automatically populated. The signal loss is used to calculate RF signal strength near these objects.

Step 6 Click **Add Obstacle**.

Step 7 Move the drawing tool to the area where you want to create an obstacle.

Step 8 Click the drawing tool to start and stop a line.

Step 9 After you have outlined the area, double-click the area to highlight it.

Step 10 In the **Obstacle Creation** window, click **Done**.

Step 11 Click **Save** to save the obstacle on the floor map.

Step 12 To edit an obstacle, in the **Overlays** panel, next to **Obstacles**, click **Edit**.

All the available obstacles are highlighted on the map.

Step 13 Click **Save** after the changes.

Step 14 To delete an obstacle, in the **Overlays** panel, next to **Obstacles**, click **Delete**.

All the available obstacles are highlighted on the map.

Step 15 Hover your cursor over the obstacle and click to delete.

Step 16 Click **Save**.

Location Region Creation

You can create inclusion and exclusion areas to further refine location calculations on a floor. You can define the areas that are included (inclusion areas) in the calculations and those areas that are not included (exclusion areas). For example, you might want to exclude areas such as an atrium or stairwell within a building, but include a work area, such as cubicles, labs, or manufacturing floors.

Guidelines for Placing Inclusion and Exclusion Areas on a Floor Map

- Inclusion and exclusion areas can be any polygon-shaped area and must have at least 3 points.
- You can only define 1 inclusion region on a floor. By default, an inclusion region is defined for each floor area when it is created. The inclusion region is indicated by a solid aqua line, and generally outlines the entire floor area.
- You can define multiple exclusion regions on a floor area.

Define an Inclusion Region on a Floor

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, select the floor.

Step 3 In the **Overlays** panel, next to **Location Regions**, click **Add**.

Step 4 In the **Location Region Creation** dialog window, from the **Inclusion Type** drop-down list, choose an option.

Step 5 Click **Add Location Region**.

A drawing icon appears to outline the inclusion area.

Step 6 To begin defining the inclusion area, move the drawing tool to a starting point on the map and click once.

Step 7 Move the cursor along the boundary of the area you want to include and click to end a border line.

Click again to define the next boundary line.

Step 8 Repeat Step 7 until the area is outlined and then double-click the drawing icon.

A solid aqua line defines the inclusion area.

Step 9 Click **Save**.

Define an Exclusion Region on a Floor

To further refine location calculations on a floor, you can define areas that are excluded (exclusion areas) in the calculations. For example, you might want to exclude areas such as an atrium or stairwell within a building. As a rule, exclusion areas are defined within the borders of an inclusion area.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, select the floor.

Step 3 Click **Edit**, which is located above the floor plan in the middle pane.

Step 4 In the **Overlays** panel, next to **Location Regions**, click **Add**.

Step 5 In the **Location Region Creation** window, from the **Exclusion Type** drop-down list, choose a value.

Step 6 Click **Location Region**.

A drawing icon appears to outline the exclusion area.

Step 7 To begin defining the exclusion area, move the drawing icon to a starting point on the map and click once.

Step 8 Move the drawing icon along the boundary of the area that you want to exclude.

Click once to start a boundary line, and click again to end the boundary line.

Step 9 Repeat the preceding step until the area is outlined and then double-click the drawing icon. The defined exclusion area is shaded in purple when the area is fully defined.

Step 10 To define more exclusion regions, repeat Step 5 to Step 9.

Step 11 When all the exclusion areas are defined, click **Save**.

Edit Location Regions

Step 1 In the **Overlays** panel, next to **Location Regions**, click **Edit**.
The available location regions are highlighted on the map.

Step 2 Make the necessary changes, and click **Save**.

Delete Location Regions

Step 1 In the **Overlays** panel, next to **Location Regions**, click **Delete**.
The available location regions are highlighted on the map.

Step 2 Hover your cursor over the region that you want to delete, and click **Delete**.

Step 3 Click **Save**.

Create a Rail

You can define a rail line on a floor that represents a conveyor belt. Also, you can define an area around the rail area known as the snap-width to further assist location calculations. This represents the area in which you expect clients to appear. Any client located within the snap-width area is plotted on the rail line (majority) or outside of the snap-width area (minority).

The snap-width area is defined in feet or meters (user-defined) and represents the distance that is monitored on either side (east and west or north and south) of the rail.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, select the floor.

Step 3 Click **Edit**, which is located above the floor plan in the middle pane.

Step 4 In the **Overlays** panel, next to **Rails**, click **Add**.

Step 5 Enter a snap-width (feet or meters) for the rail, and click **Add Rail**.

A drawing icon appears.

Step 6 Click the drawing icon at the starting point of the rail line. Click again when you want to stop drawing the line or change the direction of the line.

Step 7 Click the drawing icon twice when the rail line is drawn on the floor map. The rail line appears on the map and is bordered on either side by the defined snap-width region.

Step 8 Click **Save**.

Step 9 In the **Overlays** panel, next to **Rails**, click **Edit**.

The available rails are highlighted on the map.

Step 10 Make changes, and click **Save**.

Step 11 In the **Overlays** panel, next to **Rails**, click **Delete**.

All the available rail lines are highlighted on the map.

Step 12 Hover your cursor over the rail line that you want to delete, and click **Delete**.

Step 13 Click **Save**.

Place Markers

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, select the floor.

Step 3 Click **Edit**, which is located above the floor plan in the middle pane.

Step 4 In the **Overlays** panel, next to **Markers**, click **Add**.

A drawing icon appears.

Step 5 Enter the name for the markers, and then click **Add Marker**.

Step 6 Click the drawing icon and place the marker on the map.

Step 7 Click **Save**.

Step 8 In the **Overlays** panel, next to Markers, click **Edit**.

The available markers are highlighted on the map.

Step 9 Make changes, and click **Save**.

Step 10 In the **Overlays** panel, next to **Markers**, click **Delete**.

All the available markers are highlighted on the map.

Step 11 Hover your cursor on the marker that you want to delete, and click delete.

Step 12 Click **Save**.

Add GPS Markers

To increase the accuracy of a client's position, Cisco DNA Center GPS markers enable you to find the actual position of a building space on the world map.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, select the floor.

Step 3 Click **Edit**, which is located above the floor plan in the middle pane.

Step 4 In the **Overlays** panel, next to **GPS Markers**, click **Add**.

A location icon appears.

Step 5 Locate the location icon on the floor map

Note
- You must locate the GPS markers a minimum threshold distance of 25 feet from each other.
- You must not locate the GPS markers in a straight line.

A **Place Marker** dialog box appears to specify a physical address, latitude, and longitude coordinates of GPS marker on the floor map.

Step 6 Click **Add GPS Marker**.

Note You must add a minimum of three GPS markers to the floor map in a polygon-shape.

Step 7 Click **Save**.

Note The GPS marker is an attribute of the building and can be applied to all the floors of the building.

Edit GPS Markers

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, select the floor.

Step 3 Click **Edit**, which is located above the floor plan in the middle pane.

Step 4 In the **Overlays** panel, next to **GPS Markers**, click **Edit**.

Step 5 Click the GPS marker on the map that you want to edit.

A **Place Marker** dialog box appears to modify the physical address, latitude, and longitude coordinates of GPS marker on the floor map.

Step 6 Click **Edit GPS Marker**.

Step 7 Click **Save**.

Delete GPS Markers

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, select the floor.

Step 3 Click **Edit**, which is located above the floor plan in the middle pane.

Step 4 In the **Overlays** panel, next to **GPS Markers**, click **Delete**.

Step 5 Click the GPS marker on the map that you want to delete.

Step 6 Click **Save**.

Floor View Options

Click the **View Options**, which is located above the floor plan in the middle pane. The floor map along with these panels appear in the right pane: **Access Points**, **Sensor**, **Overlay Objects**, **Map Properties**, and **Global Map Properties**.

You can modify the appearance of the floor map by selecting or unselecting various parameters. For example, if you want to view only the access point information on the floor map, check the **Access Point** check box. You can expand each panel to configure various settings available for each floor element.

View Options for Access Points

To view access points on a map, click the **On/Off** button next to **Access Points**. Expand the **Access Points** panel to configure these settings:

- **Display Label**: From the drop-down list, choose a text label that you want to view on the floor map for the AP. The available display labels are:
  - **None**: No labels are displayed for the selected access point.
  - **Name**: AP name.
  - **AP MAC Address**: AP MAC address.
  - **Controller IP**: IP address of Cisco Wireless Controller to which the access point is connected.
  - **Radio MAC Address**: Radio MAC address.
  - **IP Address**
  - **Channel**: Cisco Radio channel number or **Unavailable** (if the access point is not connected).
  - **Coverage Holes**: Percentage of clients whose signal has become weaker until the client lost its connection. It shows **Unavailable** for access points that are not connected and **MonitorOnly** for access points that are in monitor-only mode.
  - **TX Power**: Current Cisco Radio transmit power level (with 1 being high) or **Unavailable** (if the access point is not connected). If you change the radio band, the information on the map changes accordingly.

The power levels differ depending on the type of access point. The Cisco Aironet 1000 Series Lightweight Access Point accepts a value between **1** and **5**; the Cisco Aironet 1230AG Series Access Point accepts a value between **1** and **7**; and the Cisco Aironet 1240AG Series Access Point and Cisco Aironet 1100 Series Access Point accept a value between **1** and **8**.

- **Channel and Tx Power**: Channel and transmit power level (or **Unavailable** if the access point is not connected).
- **Utilization**: Percentage of bandwidth used by the associated client devices (including receiving, transmitting, and channel utilization). Displays **Unavailable** for disassociated access points and **MonitorOnly** for access points in monitor-only mode.
- **Tx Utilization**: Transmitted (Tx) utilization for the specified interface.
- **Rx Utilization**: Received (Rx) utilization for the specified interface.
- **Ch Utilization**: Channel utilization for the specified access point.
- **Assoc. Clients**: Total number of clients associated.
- **Dual-Band Radios**: Identifies and marks the XOR dual-band radios on the Cisco Aironet 2800 and 3800 Series Access Points.
- **Health Score**: AP health score.
- **Issue Count**
- **Coverage Issues**
- **AP Down Issues**

- **Heatmap Type**: Heatmap is a graphical representation of Radio Frequency (RF) wireless data where the values taken by variable are represented in maps as colors. The current heatmap is computed based on the RSSI prediction model, antenna orientation, and AP transmit power. From the **Heatmap Type** drop-down list, select the heatmap type:
  - **None**
  - **AP RSSI**: Coverage heatmap, which identifies the strength of wireless signal in the specific band.
    - **RSSI Cut off (dBm)**: Drag the slider to set the RSSI cutoff level. The RSSI cutoff ranges from -60 dBm to -90 dBm.
    - **Heatmap Opacity (%)**: Drag the slider between 0 to 100 to set the heatmap opacity.
    - **Heatmap Color Scheme**: The color green indicates good heatmap coverage, and the color red indicates poor heatmap coverage.
  - **Client Density**: Density of associated clients.
    - **Map Opacity (%)**: Drag the slider to set the map opacity.
  - **IDS**: Heatmap that shows the monitor mode access point coverage provided to the wireless clients on a floor map.
  - **Planned Heatmap**: A planned heatmap is a hypothetical heatmap that shows the possible coverage of planned access points on a floor map.

- **Coverage**: Heatmap that excludes monitor-mode access points. (Available only if monitor-mode access points are on the floor plan.)

The AP details are reflected on the map immediately. Hover your cursor over the AP icon on the map to view AP details, RX neighbors details, client details, and switch information.

View Options for Sensors

Click the **Sensors** button to view sensors on the map. Expand the **Sensors** panel to configure these settings:

- **Display Label**: From the drop-down list, choose a text label that you want to view on the floor map for the selected access point. The available display labels are:
  - **None**
  - **Name**: Sensor name.
  - **Sensor MAC Address**: Sensor MAC address.

View Options for Overlay Objects

Expand the **Overlay Objects** panel to configure these settings. Use the **On/Off** buttons to view these overlay objects on the map.

- **Coverage Areas**
- **Location Regions**
- **Obstacles**
- **Rails**
- **Markers**

View Options for Switches

Click the **On/Off** button next to **Switch** to view the list of APs available for that particular switch on the map.

Expand the **Switch** panel to configure the display label setting.

- Display Label: From the drop-down list, choose a text label that you want to view on the floor map for the selected switch. The available display labels are:
  - None
  - Name
  - Switch MAC Address
  - APs Count
  - Clients Count
  - SSIDs Count

The AP details for the selected switch are reflected on the map immediately. Hover your cursor over the switch icon on the map to view switch details.

Click the switch name to view the following details:

- Switch MAS Address
- APs count
- Clients count
- SSIDs count
- Heatmap: You can view heatmap for all the APs, APs which belong to a particular switch, or APs which belong to other switches by clicking the respective radio buttons.
- APs owned: Shows the list of APs which belongs to this particular switch.

Configure Map Properties

Expand the **Map Properties** panel to configure:

- **Auto Refresh**—Provides an interval drop-down list to set how often you want to refresh maps data from the database. From the **Auto Refresh** drop-down list, set the time intervals: **None**, **1 min**, **2 mins**, **5 mins**, or **15 mins**.

Configure Global Map Properties

Expand the **Global Map Properties** panel to configure:

- **Unit of Measure**—From the drop-down list, set the dimension measurements for maps to either **Feet** or **Meters**.

Identify Wireless Interferers on the Floor Map

Cisco DNA Center detects interference and disables the interference source for a specific band on a floor map. Any interference in the 2.4-GHz band disrupts the network traffic of the 802.11 wireless network.

Cisco DNA Center identifies the position, area of impact, and intensity of the interferer.

This procedure shows how to identify network interferers on a floor map.

Before you begin

Ensure that either Cisco Connected Mobile Experiences (CMX) or Cisco DNA Spaces is synchronized with Cisco DNA Center.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

A world map is displayed in the right pane.

In the left pane, navigate to the floor on which you want to identify the interferer.

Step 2 In the site hierarchy pane, click the gear icon next to the floor and choose **Sync: DNA Spaces/CMX** to synchronize **DNA Spaces** or **CMX** with the floor.

Note (Optional) In the world map, hover your cursor over the floor and choose **Sync: DNA Spaces/CMX** to synchronize **DNA Spaces** or **CMX** with the floor.

Step 3 In the **Network Hierarchy** window, click **View Options**.

Step 4 In the **View Options** window, scroll down and click the **On/Off** toggle button next to **Interferers** to view interferers on the floor map.

Step 5 Expand **Interferers** and click the **On/Off** toggle button next to **Show Zone of Impact** to view the zone of impact of interferers on the floor map.

Note By default, **Zone of Impact** is turned off.

Step 6 In the world map, hover your cursor over the interferer and click the impacted channel to view the interferer device details.

The **Interferer** window shows the following attributes of the identified interferer:

- Type
- State
- Name
- Interferer reported by either CMX or Cisco DNA Spaces
- MAC address
- Detecting AP(s)
- Duty cycle
- Affected channels
- Zone of impact
- First detected
- Last reported

Data Filtering

Filter Access Point Data

Click **Access Point** under the **Filters** panel in the right pane.

- Choose the radio type from the drop-down list, located above the floor map in the middle pane: **2.4 GHz**, **5 GHz**, or **2.4 GHz & 5 GHz**.
- Click **+ Add Rule** to add a query:
  - Choose the access point identifier you want to view on the map.

- Choose the parameter by which you want to filter access points.
- Enter the specific filter criteria in the text box for the applicable parameters, and click **Go**. The search results appear in a tabular format.
- Click **Apply Filters to List** to view the filter results on the map. To view a particular access point on the map, check the check box of the access point in the table that is displayed, and click **Show Selected on Maps**.

When you hover your mouse cursor over the search result in the table, the location of the AP is marked by a line on the map.

Filter Sensor Data

Click **Sensor** under the **Filters** panel in the right pane.

- Choose the radio type from the drop-down list, located above the floor map in the middle pane: **2.4 GHz**, **5 GHz**, or **2.4 GHz & 5 GHz**.
- Click **+ Add Rule** to add a query:
  - Choose the sensor identifier you want to view on the map: **Name** and **MAC Address**.
  - Choose the parameter by which you want to filter sensors.
  - Enter the specific filter criteria in the text box for the applicable parameters, and click **Go**. The search results appear in a tabular format.
  - Click **Apply Filters to List** to view the filter results on the map. To view a particular sensor on the map, check the check box of the sensor in the table that is displayed, and click **Show Selected on Maps**.

When you hover your mouse cursor over the search result in the table, the location of the sensor is marked by a line on the map.

Filter Client Data

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 In the left pane, select a floor.

Step 3 Click **Data**, which is located above the floor plan in the middle pane.

Step 4 In the **Filters** panel, click **Clients**.

Step 5 Click + icon to add a rule.

Step 6 From the filtering criteria drop-down list, choose the client identifier you want to view on the map.

Step 7 Choose the respective parameter for the chosen client identifier.

Step 8 Enter the specific filter criteria in the text box for the applicable parameters.

Step 9 Click **Apply Filters to List** to narrow down the clients list based on the following filter results on the map: **User Name**, **Average Health Score**, **Issues Count**, **IP Address**, **MAC Address**, **Status**, **Band**, **SSID**, **Vendor**, **AP Name**, **Operating System**, **Average RSSI (dBm)**, **Average SNR (dB)**, and **Average Data Rate**.

The search results appear in a tabular format.

Step 10 To view a particular client on the map, check the check box next to the client in the table, and click **Show Selected on Maps**.

Note When you hover your mouse over the search result in the table, a solid line and a dotted line appears,

- Solid line indicates the location of the client on the map.
- Dotted line indicates the association of the access point and the client on the map.

Create a Floor Map Using an Ekahau Project File

Before you begin

The Ekahau Pro tool allows you to create the complete network plan for your enterprise, including floor layout, AP locations, and obstacles. After creating the floor layout, you can export the simulated network plan and the real-world site survey data into a format that Cisco DNA Center can use. You can import the Ekahau project file into Cisco DNA Center for further planning.

The Ekahau Pro tool allows you to automatically create the site hierarchy, save it as a project file, and import it into Cisco DNA Center.

Note Ekahau projects are supported only for predictive mode, not for design mode.

Step 1 Plan the floor layout in the Ekahau Pro tool.

- Create buildings and floors.

  It is not mandatory to create buildings in the Ekahau Pro tool.
- Import the floor plan.
- Add the planned APs or hypothetical APs.
- Add building coordinates.
- Define the site name.

  The AP name that you provide here will be used to update the AP name on the Cisco Wireless Controller during the wireless controller configuration.
- Add obstacles.
- Export the project as a PDF.

Step 2 Deploy the planned APs at locations designed on the floor layout.

- The physical AP is mounted at the designed location that is specified on the floor layout. The MAC address of the planned AP is updated with the MAC address of the physical AP.
- The physical AP is connected to the VLAN of the intended wireless controller.

Step 3 Configure the Cisco Wireless Controller.

- Discover the Cisco Wireless Controller and APs in your network by running the **Discovery** job, so that the discovered wireless controllers and APs are listed on the **Inventory** window.
- Update the AP name on the wireless controller with the AP name given in the Ekahau Pro project during the floor planning.

Step 4 Import the Ekahau project into Cisco DNA Center.

Step 5 Map the planned APs to real APs in Cisco DNA Center.

Import the Ekahau Project to Cisco DNA Center

Step 1 Design your network hierarchy by adding sites, buildings, and floors.

For more information, see Create a Site in a Network Hierarchy, on page 111, Add Buildings, on page 115, and Add a Floor to a Building, on page 116.

While adding floors, make sure that you create floors with the same name given in the Ekahau project.

Step 2 In the left pane, navigate to the site where you want to import the Ekahau project.

Step 3 Click the gear icon next to the site, and click **Import Ekahau Project**.

The **Import Ekahau Project** dialog box appears.

Step 4 Drag and drop the .esx file into the boxed area in the **Import Ekahau Project** dialog box, or click the **click to select** link and browse to the .esx file.

Once the import is successful, each planned AP is mapped to an existing real AP in the inventory using the AP name. The planned AP is displayed with an icon **P** on the floor map. For example, if the name of the planned AP is SJC01-02-AP-B-1, the import process searches for real AP with the same name.

Step 5 If an AP is not found in the inventory and remains unmapped, then the planned AP is retained on the floor.

To view reason for mismatch, hover your cursor over the planned AP icon on the floor map, and click **Import History**.

The following attempts are made to map the planned APs to real APs:

- If the newly discovered APs match with the planned AP, then the planned AP is replaced with the discovered real AP.
- If a planned AP remains unmapped, then you can manually replace the planned AP with real AP, providing reasons for failure.

Step 6 To manually assign the planned AP to a real AP, hover your cursor over the planned AP icon on the floor map, and click **Assign** > **Assign**.

The **Assign Planned APs** panel appears.

Step 7 In the **Assign Planned APs** panel, map the planned AP to a real AP by AP name, AP type, or All APs.

Step 8 Select the radio button next to the AP Name, and click **Assign** to manually assign the planned AP.

Step 9 Click **Save**.

Export the Ekahau Project from Cisco DNA Center

To augment the preconfigured working floors, the Cisco DNA Center allows you to export the working floors from Cisco DNA Center as an Ekahau project and import the project into the Ekahau Pro Tool.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

A world map appears in the right pane.

Step 2 In the left pane, select the desired site, building, or floor.

Step 3 To export an Ekahau project of a site or building, from the **Export** drop-down list, choose **Export Maps**, or from the left pane, click the gear icon next to the desired site or building and choose **Export Maps**.

To export an Ekahau project of a floor map, from the left pane, click the gear icon next to the desired floor and choose **Export Maps**.

The **Information** dialog box appears.

Step 4 In the **Information** dialog box, select the **Ekahau Project** export format.

Step 5 Click **Yes**.

An ESX file is created and saved to your local machine.

Step 6 Import the ESX file into the Ekahau Pro tool, augment the floor, and save the file.

Step 7 Import the Ekahau project into the Cisco DNA Center under the site. For more information, see Import the Ekahau Project to Cisco DNA Center.

About Interactive Floor Planning

Interactive planning helps you plan a floor layout by drawing planned APs or hypothetical APs and obstacles with a raster image or a CAD floor plan as the backdrop. You can export the floor map as a PDF and share it with the technicians who are mounting the APs. The floor drawing helps the technicians to visualize the floor layout and the exact AP mount locations.

With interactive floor planning, you can:

- Create a floor layout with a raster or CAD floor plan as the canvas.
- Place the planned APs or hypothetical APs on the floor map based on the signal coverage requirement. These hypothetical APs or planned APs are not yet installed or discovered by Cisco DNA Center.
- Assign the antenna type and orientation.
- Draw obstacles on the floor.

- Plan all APs in sequence.
- Export the floor map as a PDF.

Interactive Floor Planning

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 Design your network hierarchy by adding sites, buildings, and floors.

Step 3 In the left menu, select the floor.

You can draw the planned APs and obstacles on the selected floor.

Step 4 Click **Edit**, which is located above the floor plan in the middle pane.

Step 5 In the **Floor Elements** panel, next to **Planned Access Points**, click **Add**.

The **Add Planned AP** window appears.

Step 6 In the **AP Name** text box, enter a name for the planned AP.

Step 7 (Optional) In the **MAC Address** text box, enter the MAC address of the planned AP.

Step 8 From the **AP Model** drop-down list, choose an AP model.

Step 9 In the **x** and **y** text boxes, enter the horizontal and vertical span of the map, in feet.

Step 10 In the **AP Height** text box, enter the height of the AP.

Step 11 Click the radio band tabs to configure the antenna type, azimuth, and elevation orientation.

Step 12 From the **Antenna** drop-down list, choose the appropriate antenna type for this AP.

The antenna image reflects the antenna selected.

Step 13 Depending on the antenna type, enter the **Azimuth** and **Elevation** orientation, in degrees.

Step 14 Click **Save**.

The newly added planned AP appears on the floor map.

Step 15 If you have not specified the horizontal and vertical span (that is, the x and y coordinates), the planned AP appears on the top-right corner of the floor map.

Step 16 Position the planned AP correctly on the map by dragging and dropping to the appropriate location on the map.

Step 17 Click **Save**.

Step 18 The next AP that you can plan appears on the top-right corner of the floor map.

Step 19 Repeat Step 6 through Step 14 to plan the next AP.

Step 20 To draw obstacles, in the **Overlays** panel, next to **Obstacles**, click **Add**.

For more information, see Create Obstacles, on page 125.

Step 21 To export the floor plan as a PDF, click the ⋮ icon at the top-right corner of the **Network Hierarchy** window, and choose **Export**.

Step 22 In the **Export** window, check the **PDF** check box to export as a PDF.

Step 23 Click **Export**.

The PDF is created and downloaded to your local machine. The PDF contains the floor map along with the planned AP details that you configured. The planned APs are listed based on the AP model.

Place Planned Access Points on a Floor Map Using AP Model Catalog

Using the AP Model Catalog feature, you can configure one AP on the floor with the AP model, antenna type, azimuth, and elevation orientation, and then replicate that configuration on rest of the APs that belong to the same model type.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 Design your network hierarchy by adding sites, buildings, and floors.

Step 3 In the left menu, select the floor.

You can draw the planned APs and obstacles on the selected floor.

Step 4 Click the **Unlock Floor** icon ( ), which is located above the floor plan in the middle pane.

The list of AP models that are available on a particular floor appears on the left side of the floor map.

Step 5 To add a new AP model to the floor, click **Add model**.

The **Select AP models to add** dialog box appears.

Step 6 From the **Select AP models to add** drop-down list, choose the AP models, and then click **Add AP models**.

The new AP models are added to the floor.

Step 7 To remove an AP model, click the **X** above the AP model name.

You can only remove an AP model if no APs of that model type are added to the floor map.

Step 8 To add the planned APs to the floor map, click the AP model to select it, move your cursor to the appropriate location on the floor map, and then click again.

A planned AP of the selected model is added to the floor map and the **Edit Planned AP** pane appears on the right, with an AP name added to it by default.

Step 9 From the **Edit Planned AP** pane, click the gear icon, which is located next to the **AP Name** field.

The **Name pattern** dialog box appears.

Step 10 When you add the first AP to the floor, make sure that you enter a valid name pattern, for example SJC-BLD21-FL2-AP####, and then click **Set name pattern**.

Note The planned APs must be unique within Cisco DNA Center, so make sure that the name pattern identifies the floor.

The #### in the name pattern is replaced by numbers in the **AP Name**, for example SJC-BLD21-FL2-AP0001, SJC-BLD21-FL2-AP0002, and so on.

Step 11 From the **Antenna** drop-down list in the **Edit Planned AP** pane, choose the appropriate antenna type for each of the radio slots of the AP.

The antenna image reflects the antenna selected.

Step 12 Depending on the antenna type, enter the **Azimuth** and **Elevation** orientation, in degrees.

Step 13 To add another AP with the same AP properties as that of the AP that you just created, click a location in the floor map where you want to position the new AP.

A new AP appears on the map with all of the properties inherited and the AP name appended, for example BLD1-AP0002-TX.

Step 14 To add more APs with the same properties and appended AP Name, click the floor map.

Step 15 To stop adding APs to the floor map, press **Esc** or right-click the floor map.

Step 16 To reposition the APs, drag and drop them to the appropriate location in the floor map.

Step 17 Click **Save** to save your changes or click **X** to discard them.

Step 18 To delete a planned AP, right-click the AP name on the floor map, and click **Delete**.

Step 19 To edit a planned AP, right-click the AP name on the floor map, and click **Edit**.

The **Edit Planned AP** window appears. Make your changes in the **Edit Planned AP** window, and then click **Save**.

Step 20 To view details, right-click the AP name on the floor map, and click **View Details**.

Configure Global Wireless Settings

Global wireless network settings include settings for Service Set Identifier (SSID), wireless interfaces, wireless radio frequency (RF), and sensors.

Note Creating a wireless sensor device profile applies only to Cisco Aironet 1800s Active Sensor devices.

Create SSIDs for an Enterprise Wireless Network

The following procedure describes how to configure SSIDs for an enterprise wireless network.

Note The SSIDs are created at the Global level. The site, building, and floor inherit settings from the Global level.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** and then click the **Wireless** tab.

Step 2 From the **SSID** table, hover over Add and choose **Enterprise**.

The **Wireless SSID** workflow appears.

Step 3 Complete the **Basic Settings** step:

a) In the **Wireless Network Name (SSID)** field, enter a unique name for the wireless network or the SSID that you are creating.

Note The SSID name can contain up to 32 alphanumeric characters with leading spaces. All special characters except for < /.* and trailing spaces are allowed.

The following combination of substring is not allowed: .*

b) For **Wireless Option**, choose the wireless band preference:

- **Dual band operation (2.4 GHz and 5 GHz)**: The WLAN is created for both 2.4 GHz and 5 GHz. The band select is disabled by default.
- **Dual band operation with band select**: The WLAN is created for 2.4 GHz and 5 GHz and band select is enabled.
- **5 GHz only**: The WLAN is created for 5 GHz and band select is disabled.
- **2.4 GHz only**: The WLAN is created for 2.4 GHz and band select is disabled.

c) For **Type of Enterprise Network**, choose how the quality of service is provisioned on the wireless network:

- **Voice and Data**: The quality of service is optimized for voice and data traffic.
- **Data Only**: The quality of service is optimized for wireless data traffic only.

d) For **SSID STATE**, customize the following settings:

- **Admin Status**: Use this toggle to enable or disable admin status.
- **Broadcast SSID**: Use this toggle to enable or disable the visibility of the SSID to all wireless clients within range.

e) Click **Next**.

Step 4 Complete the **Security Settings** step:

a) For **Level of Security**, choose the encryption and authentication type for the network:

- **Enterprise**: You can configure both **WPA2** and **WPA3** security authentication type by checking the respective check boxes. By default, the **WPA2** check box is enabled.

  Note Wi-Fi Protected Access (WPA2) uses the stronger Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP).

  WPA3 is the latest version of WPA, which is a suite of protocols and technologies that provide authentication and encryption for Wi-Fi networks. WPA3-Enterprise provides higher-grade security protocols for sensitive data networks.

- **Personal**: You can configure **WPA2** and **WPA3** security authentication types by checking the respective check boxes. If you choose **Personal**, enter the passphrase key in the **Pass Phrase** field. This key is used as the pairwise master key (PMK) between clients and the authentication server.

  Note WPA3-Personal brings better protection to individual users by providing more robust password-based authentication making the brute-force dictionary attack much more difficult and time-consuming.

  For WPA2 personal, you can override a preshared key (PSK) at the site, building, or floor level. If you override a PSK at the building level, the subsequent floors inherit the new settings. For information, see Preshared Key Override, on page 145.

- **Open Secured**: From the **Assign Open SSID** drop-down list, select an open SSID to redirect the clients to open secured SSID. The open secured policy provides least security.
- **Open**: Provides no security. It allows any device to connect to the wireless network without any authentication.

b) For **Authentication, Authorization, and Accounting Configuration**, configure the AAA-related settings:

- For **Configure AAA**, click to add and configure the AAA servers for enterprise wireless network SSID. For more information, see Configure AAA Server for an Enterprise Wireless Network.
- **Fast Lane**: Check this check box to enable fastlane capabilities on the network.

  Note By enabling fastlane, you can set the IOS devices to receive an optimized level of wireless connectivity and enhanced Quality of Service (QoS).

- **Identity PSK**: Check this check box to enable unique pre-shared keys that can be created for individuals or groups of users in the SSID.
- **Deny LLA Clients**: Check this check box to deny clients with random MAC addresses.

c) Click **Next**.

Step 5 Complete the **Advance Settings** step:

a) For **Fast Transition (802.11r)**:

- Choose **Adaptive**, **Enable**, or **Disable** mode.

  Note 802.11r allows wireless clients to quickly roam from one AP to another AP. Fast transition ensures less disrupted connectivity when a wireless client roams from one AP to another AP.

- Check the **Over the DS** check box to enable fast transition over a distributed system.

b) For **MFP Client Protection**, choose a setting: **Optional**, **Required**, or **Disabled**.

Note Management Frame Protection (MFP) increases the security of management frames. It provides security for the otherwise unprotected and unencrypted 802.11 management messages that are passed between access points and clients. MFP provides both infrastructure and client support.

By default, the **Optional** radio button is selected. If you click the **Required** radio button, then the clients are allowed to associate only if the MFP is negotiated (that is, if WPA2 is configured on the wireless controller and the client supports CCXv5 MFP and is also configured for WPA2).

c) For **11K**:

- **Neighbor List**: Check this check box to all the 11k capable clients to request a neighbor report about the known neighboring APs that are candidates for roaming.

  Note To facilitate roaming, a 11k capable client that is associated with an AP sends a request to a list of neighboring APs. The request is sent in the form of an 802.11 management frame, which is known as an action frame. The AP responds with a list of neighbor APs on the same WLAN with their Wi-Fi channel numbers. The response is also an action frame. The client identifies the AP candidates for next roam from the response frame.

- **Session Timeout**: Check this check box to set the maximum time for a client session to remain active before reauthorization.

Note By default, the **Session Timeout** is enabled with a timeout of 1800 seconds. The session timeout range is from 300 to 86400 seconds.

- **Client Exclusion**: Check this check box to set the client exclusion timer.

  Note When a user fails to authenticate, the wireless controller excludes the client from connecting. The client is not allowed to connect to the network until the exclusion timer expires. By default, the **Client Exclusion** is enabled with a timeout of 180 seconds. The range is from 0 to 2147483647 seconds.

d) For **11v BSS Transition Support**:

- **BSS Max Idle Service**: Check this check box to set the idle period timer value. The idle period timer value is transmitted using the association and reassociation response frame from APs to the client.

  Note The BSS Max idle period is the timeframe during which an AP does not disassociate a client due to nonreceipt of frames from the connected client.

- **Client User Idle Timeout**: Check this check box to set the user idle timeout for a WLAN.

  Note If the data sent by the client is more than the threshold quota specified within the user idle timeout, the client is considered to be active and the wireless controller refreshes for another timeout period.

  By default, **Client User Idle Timeout** is enabled with a user idle timeout of 300 seconds.

- **Directed Multicast Service**: Check this check box to enable directed multicast service.

  Note By default, the **Directed Multicast Service** is enabled. Using the Directed Multicast Service (DMS), the client requests APs to transmit the required multicast packets as unicast frames. This allows clients to sleep for a longer time and saves the battery power.

e) Click **Next**.

Step 6 Complete the **Associate SSID to Profile** step:

a) Click **Add Profile** and then configure the profile settings:

- **Profile Name**: Enter a name for the wireless profile.
- **Fabric**: Specify whether the SSID is fabric or non fabric.

  Note A fabric SSID is a wireless network, which is part of Software Defined-Access (SD-Access). With fabric SSID, it is mandatory to have SD-Access. Non fabric is a traditional wireless network that does not require SD-Access.

  For a non fabric SSID, choose the following:

  - **Interface**: Click the **Interface Management** drop-down list and choose an interface or click the plus icon to add a new wireless interface.

    Note This is the VLAN ID that is associated with the wireless interface.

  - **VLAN Group**: Click the **VLAN Group Name** drop-down list and choose a VLAN group or click the plus icon to add a VLAN group.

- **Do you need Anchor for this SSID?**: Choose whether the SSID will be an anchor or not.
- **Flex Connect Local Switching**: Check this check box to enable local switching for the WLAN. When you enable local switching, any FlexConnect access point that advertises this WLAN is able to locally switch data packets.

  Note If you have enabled **Flex Connect Local Switching** for an SSID, then all APs on that particular floor where the network profile is mapped will switch to FlexConnect mode.

b) Click **Associate Profile** to choose the profile.
c) Click **Next**.

Step 7 Review the **Summary** step and if necessary, click **Edit** for a step to go back to the step to make changes.

Step 8 If you are satisfied with the SSID settings, click **Save**.

The SSID is created.

Preshared Key Override

SSIDs are created at the Global hierarchy. The sites, buildings, and floors inherit settings from the Global hierarchy. You can override a preshared key (PSK) at the site, building, or floor level. If you override a PSK at the building level, the subsequent floor inherits the new setting.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **Wireless**.

Step 2 In the left menu, select the site, building, or floor to edit the PSK.

Step 3 Under **Enterprise Wireless**, click the **Passphrase** field, and enter a new passphrase for the PSK SSID.

Step 4 Click **Save**.

A success message saying `Passphrase for the SSID(s) updated successfully` is displayed.

Hover your cursor over the inherit icon next to the SSID to view the origin of this setting.

Step 5 To reset the PSK override, check the check box of the PSK SSID on the site, building, or floor and click **Delete**. The PSK is reset to the global passphrase value.

Configure AAA Server for an Enterprise Wireless Network

Before you begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **Wireless**.

Step 2 Under **Enterprise Wireless** area, in the **Action** column click **Configure AAA** of SSID for which you want to configure the AAA server.

The **Configure AAA Server** for SSID window appears.

Step 3 From the **Server** drop-down list, you can either search for a server IP address by entering its name in the **Search** field or choose AAA IP address.

Note The **Configure AAA** feature is not supported for Mobility Express (ME) and Evolved Converged Access (ECA) devices.

Step 4 Click+ to add an **Additional Server**.

Note You can configure a maximum of six AAA servers for an SSID of guest wireless network.

Step 5 From the **Additional Server** drop-down list, choose the server IP address.

Step 6 (Optional) To delete a server or an additional server, click the delete icon next to each server.

Step 7 Click **Configure**.

The Cisco DNA Center allows you to override the set of AAA server configuration for SSID on the site level. For each set of overridden AAA settings per SSID, the Cisco DNA Center creates a new WLAN profile with the corresponding AAA servers mapped to it. If an SSID is overridden for different floors, and you make changes in the AAA servers, the Cisco DNA Center creates the new WLAN profiles equals to the number of floors.

You must reprovision the device to override the AAA servers on the site level. See Provision Devices.

Create SSIDs for a Guest Wireless Network

This procedure explains how to create SSIDs for a guest wireless network.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Design** > **Network Settings** > **Wireless**.

Step 2 Under + Create , click **Guest** to create a new SSID.

The **Guest Wireless Network** window appears.

Step 3 In the **Wireless Network Name (SSID)** field, enter a unique name for the guest SSID that you are creating.

The SSID name can contain up to 32 alphanumeric characters with leading spaces. All special characters except for < /.* and trailing spaces are allowed.

The following combination of substring is not allowed: .*

Step 4 Under **Type of Enterprise Network**, click **Voice and Data** or **Data Only**. The selection type defines the quality of service that is provisioned on the wireless network.

If you select **Voice and Data**, the quality of service is optimized for voice and data traffic.

If you select **Data Only** option, the quality of service is optimized for wireless data traffic only.

Step 5 Configure wireless band preferences by selecting one of the **Wireless Options**:

- **Dual band operation (2.4 GHz and 5 GHz)**: The WLAN is created for both 2.4 GHz and 5 GHz. The band select is disabled by default.
- **Dual band operation with band select**: The WLAN is created for 2.4 GHz and 5 GHz and band select is enabled.
- **5 GHz only**: The WLAN is created for 5 GHz and band select is disabled.
- **2.4 GHz only**: The WLAN is created for 2.4 GHz and band select is disabled.

Step 6 Under **SSID STATE**, configure the following:

- Click the **Admin Status** button off, to disable the admin status.
- Click the **BROADCAST SSID** button off, if you do not want the SSID to be visible to all wireless clients within the range. Turning off the **Broadcast SSID** hides the SSID from clients attempting to connect to this SSID, reducing unnecessary load on the wireless infrastructure.

Step 7 Under **Level Of Security**, configure the layer 2 and layer 3 security policies.

Step 8 Under **L2 Security**, set the encryption and authentication type for this network.

Step 9 Click the **Enterprise**, **Personal**, **Open Secured**, or **Open** radio button to configure the respective security authentication.

- **Enterprise**: You can configure either **WPA2** or **WPA3** security authentication type by checking the respective check boxes. By default, the **WPA2** check box is enabled.

  Wi-Fi Protected Access (WPA2) uses the stronger Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). Fast transition is applicable for enterprise WPA2 SSID.

  WPA3 security authentication is the latest version of WPA which is a suite of protocols and technologies that provide authentication and encryption for Wi-Fi networks. WPA3-Enterprise provides higher grade security protocols for sensitive data networks.

- **Personal**: You can configure both **WPA2** and **WPA3** or configure **WPA2** and **WPA3** individually by checking the respective check boxes.

  WPA3 personal security authentication brings better protection to individual users by providing more robust password-based authentication. This makes the brute-force dictionary attack much more difficult and time-consuming.

  Enter the passphrase key in the **Pass Phrase** field. This key is used as the pairwise master key (PMK) between the clients and the authentication server.

- **Open Secured**: From the **Assign Open SSID** drop-down list, choose an open SSID to associate with the open SSID. Associating secures the open SSID. You must have an open SSID created before associating it with the open secured SSID.

  Note Fast Transition is not applicable for open-secured SSID.

- **Open**: The open policy provides no security. It allows any device to connect to the wireless network without any authentication.

Step 10 Under **L3 Security**, set the encryption and authentication type for this guest network: **Web Policy** or **Open**.

Step 11 The **Open** policy type provides no security. It allows any device to connect to the wireless network without any authentication.

Step 12 If you choose **Web Policy**, you need to configure one of the authentication servers: **ISE Authentication**, **Web Authentication**, or **Web Passthrough**.

The **Web Policy** encryption and authentication type provides a higher level of Layer 3 security.

- For an External Web Authentication (EWA), click the **Web Policy** radio button as the level of security under **L3 Security** and **Web Authentication External** as the authentication server from the **Authentication** drop-down list.
- For a Central Web Authentication (CWA), click the **Web Policy** as the level of security under **L3 Security** and **ISE Authentication** as the authentication server from the **Authentication** drop-down list.

Step 13 Under **Authentication Server**, you can configure the authentication server for the SSID.

Step 14 If you choose **ISE Authentication**, choose the type of portal you want to create from the **WHAT KIND OF PORTAL ARE YOU CREATING TODAY ?** drop-down list:

- **Self Registered**: The guests are redirected to the Self-Registered Guest portal to register by providing information to automatically create an account.
- **HotSpot**: The guests can access the network without providing any credentials.

Choose where you want to redirect the guests after successful authentication from the **WHERE WILL YOUR GUESTS REDIRECT AFTER SUCCESSFUL AUTHENTICATION ?** drop-down list:

- **Success Page**: The guests are redirected to an **Authentication Success** window.
- **Original URL**: The guests are redirected to the URL they had originally requested.
- **Custom URL**: The guests are redirected to the custom URL that is specified here. Enter a redirect URL in the **Redirect URL** field.

  Now that you have created an SSID, you must associate it with a wireless profile. This profile helps you to construct a topology, which is used to deploy devices on a site.

Step 15 If you choose **Web Authentication** or **Web Passthrough**, configure **Internal** or **External** authentication type.

Web authentication or Web Auth is a layer 3 security method that allows a client to pass Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) traffic only until they have passed some form of authentication.

Web passthrough is a solution that is used for guest access and requires no authentication credentials. In web passthrough authentication, wireless users are redirected to the usage policy page while trying to use the Internet for the first time. After accepting the policy, users are allowed to browse the Internet.

- If you choose **Web Authentication Internal** or **Web Passthrough Internal** from the **Authentication Server** drop-down list, then the page is reconstructed by the Cisco Wireless Controller.
- If you choose **Web Authentication External** or **Web Passthrough External** from the **Authentication Server** drop-down list, then the client is redirected to the specified URL. You need to enter a redirect URL in the **Web Auth Url** field.

Step 16 Under **TIMEOUT SETTINGS FOR SLEEPING CLIENTS**, configure authentication for sleeping clients: **Always authenticate** or **Authenticate after**.

The clients with guest access that have had successful web authentication are allowed to sleep and wake up without having to go through another authentication process through the login page. You can configure the duration for which the sleeping clients are to be remembered for before reauthentication becomes necessary. The valid range is 10 minutes to 43200 minutes, with the default being 720 minutes. You can configure the duration on a WLAN and on a user group

policy that is mapped to the WLAN. The sleeping timer becomes effective after the idle timeout. If the client timeout is lesser than the time configured on the sleeping timer of the WLAN, then the lifetime of the client is used as the sleeping time.

- Click the **Always authenticate** radio button to enable authentication for sleeping clients.
- Click the **Authenticate after** radio button and enter the duration for which the sleeping clients are to be remembered before reauthentication becomes necessary. The valid range is 10 minutes to 43200 minutes and the default duration is 720 minutes.

Step 17 Click **Show Advanced Settings** to configure the following.

Step 18 Set **Fast Transition (802.11r)** to **Enable**, **Adaptive**, or **Disable** mode.

By default, **Fast Transition (802.11r)** is in **Adaptive** mode.

The 802.11r allows wireless clients to quickly roam from one AP to another AP. Fast transition ensures less disrupted connectivity when a wireless client roams from one AP to another AP.

Step 19 Check the **Over the DS** check box to enable fast transition over a distributed system. This option is available only if the **Fast Transition (802.11r)** is in **Adaptive** or **Enable** mode.

By default, the **Over the DS** check box is enabled.

Step 20 Under **11k**, check the **Neighbor List** check box to allow the 11k capable clients to request a neighbor report about the known neighboring APs that are candidates for roaming.

To facilitate roaming, a 11k capable client that is associated with an AP sends a request to a list of neighboring APs. The request is sent in the form of an 802.11 management frame, which is known as an action frame. The AP responds with a list of neighbor APs on the same WLAN with their Wi-Fi channel numbers. The response is also an action frame. The client identifies the AP candidates for next roam from the response frame.

Step 21 Check the **Client Exclusion** check box, and enter a value to set the client exclusion timer in the **in (secs)** field.

When a user fails to authenticate, the wireless controller excludes the client from connecting and is not allowed to connect to the network until the exclusion timer expires. By default, the **Client Exclusion** is enabled with a timeout of 180 seconds. The range is 0 to 2147483647 seconds.

Step 22 Check the **Session Timeout** check box, and enter a value in seconds.

The session timeout is the maximum time for a client session to remain active before reauthorization. By default, the **Session Timeout** is enabled with a timeout of 1800 seconds. The range is 300 to 86400 seconds.

Step 23 Under **MFP Client Protection**, click one of the radio buttons: **Optional**, **Required**, and **Disabled**.

Management Frame Protection (MFP) increases the security of management frames. It provides security for the otherwise unprotected and unencrypted 802.11 management messages that are passed between access points and clients. MFP provides both infrastructure and client support.

By default, the **Optional** is selected. If you choose **Required**, the clients are allowed to associate only if the MFP is negotiated (that is, if WPA2 is configured on the wireless controller and the client supports CCXv5 MFP and is also configured for WPA2).

Step 24 Under **11k**, check the **Neighbor List** check box to allow the 11k capable clients to request a neighbor report about the known neighboring APs that are candidates for roaming.

To facilitate roaming, a 11k capable client that is associated with an AP sends request to a list of neighboring APs. The request is sent in the form of an 802.11 management frame, which is known as an action frame. The AP responds with

a list of neighbor APs on the same WLAN with their Wi-Fi channel numbers. The response is also an action frame. The client identifies the AP candidates for the next roam from the response frame.

Step 25 Under **11v BSS Transition Support**, configure the following.

Step 26 Check the **BSS Max Idle Service** check box to set the idle period timer value. The idle period timer value is transmitted using the association and reassociation response frame from APs to the client.

The BSS Max idle period is the timeframe during which an AP does not disassociate a client due to nonreceipt of frames from the connected client.

Step 27 Check the **Client User Idle Timeout** check box and enter a value to configure the user idle timeout for a WLAN in the **Client User Idle Timeout** field.

If the data sent by the client is more than the threshold quota specified within the user idle timeout, then the client is considered to be active and the wireless controller refreshes for another timeout period.

By default, the **Client User Idle Timeout** is enabled with a user idle timeout of 300 seconds.

Step 28 Check the **Directed Multicast Service** check box to enable the directed multicast service.

By default, the **Directed Multicast Service** is enabled. Using the Directed Multicast Service (DMS), the client requests APs to transmit the required multicast packets as unicast frames. This allows clients to sleep for a longer time and save the battery power.

Step 29 Click **Configure AAA** to add and configure the AAA servers for guest wireless network SSID. For more information, see Configure AAA Server for a Guest Wireless Network.

Step 30 Click **Next**.

The **Wireless Profiles** window is displayed.

Step 31 If you do not have an existing wireless profile, in the **Wireless Profiles** window, click **Add** to create a new wireless profile.

Step 32 Enter a profile name in the **Wireless Profile Name** field.

Step 33 Specify whether the SSID is fabric or not by clicking the **Yes** or **No** radio button next to **Fabric**.

Fabric SSID is a wireless network, which is part of Software Defined-Access (SD-Access). SD-Access is a solution that automates and simplifies configuration, policy, and troubleshooting of wired and wireless networks. With fabric SSID, it is mandatory to have SDA. Nonfabric is a traditional wireless network that does not require SD-Access.

Step 34 If you want the guest SSID to be a guest anchor, click the **Yes** or **No** radio button next to **Do you need a Guest Anchor for this guest SSID**.

If you want your guest SSID to be a guest anchor, click **Yes**.

Step 35 From the **Select Interface** drop-down list, choose the interface or click **+** to create a new wireless interface.

This is the VLAN ID that is associated with the wireless interface.

Step 36 If you click **No**, enable the FlexConnect mode by checking the **Flex Connect Local Switching** check box. The selection of FlexConnect mode switches the traffic locally. Based on your configuration, the profile is applied to a site and a flex group is created internally.

If you have enabled **Flex Connect Local Switching** for an SSID, then all APs on that particular floor where the network profile is mapped will switch to FlexConnect mode.

Step 37 In the **Local to VLAN** field, enter a value for the VLAN ID.

Step 38 To assign this profile to a site, click **Sites**.

Step 39 In the **Sites** window, check the check box next to the site to associate this profile and click **OK**.

You can either select a parent site or the individual sites. If you select a parent site, all children inherit their settings from the parent site. You can uncheck the check box to deselect a site.

Step 40 Click + Add Model Config to attach a model config design to the wireless profile.

The **Add Model Config** window appears.

Step 41 From the **Device Type(s)** drop-down list, choose the device type.

You can either search for a device name by entering its name in the **Search...** field or expand **Wireless Controller** and select the device type.

Step 42 Under **APPLICABILITY**, from the **Tags** drop-down list, choose the applicable tags.

Step 43 Click **Add**.

Step 44 Click **Save**.

The created profile appears in the **Wireless Profiles** window.

Step 45 To associate the SSID to a wireless profile, in the **Wireless Profiles** window, check the **Profile Name** check box to associate the SSID; then, click **Next**.
The **Portal Customization** window appears, where you can assign the SSID to a guest portal.

Step 46 In the **Portal Customization** window, click **Add** to create the guest portal.

The **Portal Builder** window appears.

Step 47 Expand **Page Content** in the left menu to include various variables.

Step 48 Drag and drop variables into the portal template window and edit them.

- The variables for the **Login** page are:
  - **Access Code**
  - **Header Text**
  - **AUP**
  - **Text Fields**
- The variables for the **Registration** page are:
  - **First Name**
  - **Last Name**
  - **Phone Number**
  - **Company**
  - **SMS Provider**
  - **Person being visited**
  - **Reason for a visit**
  - **Header text**
  - **User Name**

- **Email Address**
- **AUP**

- The variables for the **Registration Success** page are:
  - **Account Created**
  - **Header texts**
- The variable for the **Success** page is: **Text fields**.

Step 49 To customize the default color scheme in the portal, expand **Color** in the left menu and change the color.

Step 50 To customize the font, expand **Font** in the left menu and change the font.

Step 51 Click **Save**.

The created portal appears in the **Portal Customization** window.

Step 52 Under **Portals**, click the radio button next to the **Portal Name** to assign the SSID to that guest portal.

Step 53 Click **Finish**.

Configure AAA Server for a Guest Wireless Network

Before you begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **Wireless**.

Step 2 Under **Guest Wireless** area, in the **Action** column click **Configure AAA** of SSID for which you want to configure the AAA server.

The **Configure AAA Server** for SSID window appears.

Step 3 From the **Server** drop-down list, you can either search for a AAA IP address by entering its name in the **Search** field or choose AAA IP address.

Note
- You must configure at least one Policy Service Node (PSN) server for Central Web Authentication (CWA) SSIDs of guest wireless network.
- Cisco DNA Center allows you to map AAA server in any combination of identity services engine PSNs and third-party AAA IPs.
- In the **Server** drop-down list, the **AAA** IP addresses, and the PSN IP addresses are grouped in the corresponding sections.
- The **Configure AAA** feature is not supported for Mobility Express (ME) and Evolved Converged Access (ECA) devices.

Step 4 Click+ to add an **Additional Server**.

Note You can configure a maximum of six AAA servers for an SSID of guest wireless network.

Step 5 From the **Additional Server** drop-down list, choose the server IP address.

Step 6 (Optional) To delete a server or an additional server, click the delete icon next to each server.

Step 7 Click **Configure**.

The Cisco DNA Center allows you to override the set of AAA server configuration for SSID on the site level. For each set of overridden AAA settings per SSID, the Cisco DNA Center creates a new WLAN profile with the corresponding AAA servers mapped to it. If an SSID is overridden for different floors, and you make changes in the AAA servers, the Cisco DNA Center creates the new WLAN profiles equals to the number of floors.

You must reprovision the device to override the AAA servers on the site level. See Provision Devices.

Create a Wireless Interface

You can create wireless interfaces only in nonfabric deployments.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **Wireless**.

Step 2 Under **Wireless Interfaces**, click **+Add**.

The **New Interfaces** window appears.

Step 3 In the **Interfaces Name** text box, enter the dynamic interface name.

Step 4 (Optional) In the **VLAN ID** text box, enter the VLAN ID for the interface. The valid range is from 0 to 4094.

Step 5 Click **Ok**.

The new interface appears under **Wireless Interfaces**.

Design and Provision Interface/VLAN Groups to Nonfabric Deployments

Cisco DNA Center allows you to configure networks with multiple broadcast domains through different VLANs. When the same set of APs broadcast the same WLAN, the broadcast domains are controlled through multiple VLANs on the same WLAN through interface groups.

Cisco DNA Center interface groups are logical groups of interfaces that facilitate user configuration, where the same interface group can be configured on multiple WLANs or while overriding a WLAN interface per AP group. An interface can be part of multiple interface groups. A WLAN can be associated with an interface or interface group.

Note The interface group name and the interface name cannot be the same.

The Cisco DNA Center VLAN group feature maps a WLAN to a single VLAN or multiple VLANs using VLAN groups. VLAN groups can be associated to policy profiles.

The following procedure explains how to design and provision the interface or VLAN groups for nonfabric deployments.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **Wireless**.

Step 2 In **VLAN Group**, you can view the **VLAN Group Name** and **VLAN ID** columns.

Step 3 Click **Add**.
The **Add VLAN Group** dialog box opens.

Step 4 Enter a valid **VLAN Group Name**, select single or multiple interfaces from the list, and click **Save**.

Note If you select more than 15 interfaces, the selected interfaces might not be displayed correctly onscreen.

Step 5 In the **Edit Network Profile** page, the VLAN group is associated with the SSID. For information on how to create an SSID, see Create SSIDs for an Enterprise Wireless Network.

Step 6 To add more SSIDs to the VLAN group, click **Add SSID**.

Step 7 Choose **Interface** or **VLAN** group.

Step 8 Click the add icon to create a new interface or VLAN group.

Note Interface or VLAN group is not applicable for FlexConnect local switching.

Step 9 Click **Save**.

Step 10 In **Configure Interface and VLAN**, you can view the list of interface names, interface groups names, and other parameters required to configure the interface and VLAN.

Note An interface group cannot contain more than 64 interfaces.

Step 11 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Network Devices** > **Inventory**.

Step 12 Select the device.

Step 13 From the **Actions** drop-down menu, choose **Provision** > **Provision Device**.

Step 14 Review the details in the **Assign Site**, **Configuration**, **Model Configuration**, **Advanced Configuration**, and **Summary** screens. From each a screen, click **Next** to advance to the next screen.

Step 15 Click **Deploy**.
The **Provision Device** dialog box is displayed.

Step 16 Choose **Now** and click **Apply**.
The message **Task Scheduled view status in Tasks** appears at the bottom-right corner.

Create a Wireless Radio Frequency Profile

You can either use the default radio frequency profiles (LOW, TYPICAL, HIGH), or create custom radio frequency profiles.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **Wireless**.

Step 2 Under **Wireless Radio Frequency Profile**, click **+Add RF**.

The **Wireless Radio Frequency** window appears.

Step 3 In the **Profile Name** text box, enter the RF profile name.

Step 4 Use the **On/Off** button to select the radio band: **2.4 GHz** or **5 GHz**. If you have disabled one of the radios, the base radio of the AP that you are going to configure this AP profile into will be disabled.

Step 5 Configure the following for the **2.4 GHz** radio type:

- Under **Parent Profile**, select **High**, **Medium (Typical)**, **Low**, or **Custom**. (The **Data Rate** and **Tx Configuration** fields change depending on the parent profile selected. For example, if you select **High**, it populates the profile configurations available in the device for 2.4 GHz. If you change any settings in the populated **Data Rate** and **Tx Configuration**, the **Parent Profile** automatically changes to **Custom**.) Note that a new RF profile is created only for the select custom profiles.

  Note Low, Medium (Typical), and High are the pre-canned RF profiles. If you select any of the pre-canned RF profiles, the respective RF profiles which are there in the device is used and the new RF profile is not be created on Cisco DNA Center.

- **DCA** dynamically manages channel assignment for an RF group and evaluates the assignments on a per-AP radio basis.
  - Check the **Select All** check box to select DCA channels **1**, **6**, and **11**. Alternatively, check the individual check boxes next to the channel numbers.
  - Click **Show Advanced** to select the channel numbers under the **Advanced Options**. Check the **Select All** check box to select DCA channels that are under **Advanced Options**, or check the check box next to the individual channel numbers. The channel numbers that are available for B profile are **2**, **3**, **4**, **5**, **7**, **8**, **9**, **10**, **12**, **13**, and **14**.

    Note You need to configure these channels globally on Cisco Wireless Controller.

- Use the **Supported Data Rate** slider to set the rates at which data can be transmitted between an access point and a client. The available data rates are **1**, **2**, **5.5**, **6**, **9**, **11**, **12**, **18**, **24**, **36**, **48**, and **54**.
- Under **Tx Power Configuration**, you can set the power level and power threshold for an AP.
  - **Power Level**—To determine whether the power of an AP needs to be reduced or not. Reducing the power of an AP helps mitigate co-channel interference with another AP on the same channel or in close proximity. Use the **Power Level** slider to set the minimum and maximum power level. The range is -10 to 30 dBm and the default is -10 dBM.
  - **Power Threshold**—It is the cutoff signal level used by Radio Resource Management (RRM) to determine whether to reduce the power of an AP or not. Use the **Power Threshold** slider to increase and decrease the power value which causes the AP to operate at higher or lower transmit power rates. The range is -50 dBM to 80 dBM and the default threshold is -70 dBM.
  - **RX SOP**—Receiver Start of Packet Detection Threshold (RX SOP) determines the Wi-Fi signal level in dBm at which an APs radio demodulates and decodes a packet. From the RX SOP drop-down list, choose **High**, **Medium**, **Low**, or **Auto** threshold values for each 802.11 band.

Step 6 Configure the following for the **5 GHz** radio type:

- From the **Parent Profile** drop-down list, choose **High**, **Medium (Typical)**, **Low**, or **Custom**. (The **Data Rate** and **Tx Configuration** fields change depending on the parent profile selected. For example, if you select **High**, it populates the configurations available in the device for 2.4 GHz. If you change any settings in the populated **Data Rate** and **Tx Configuration** fields, the **Parent Profile** automatically changes to **Custom**.) Note that a new RF profile is created only for select custom profiles.

Note **Low**, **Medium (Typical)**, and **High** are the pre-canned RF profiles. If you select any of the pre-canned RF profiles, the respective RF profiles which are already there in the device is used and the new RF profile is not be created on the Cisco DNA Center.

- From the **Channel Width** drop-down list, choose one of the channel bandwidth options: **Best**, **20 MHz**, **40 MHz**, **80 MHz**, or **160 MHz**, or **Best**.
- Set the **DCA Channel** to manage channel assignments:

  Note You must configure the channels globally on Cisco Wireless Controller.

  - **UNNI-1 36-48**—The channels available for UNII-1 band are: **36**, **40**, **44**, and **48**. Check the **UNII-1 36-48** check box to include all channels or check the check box of the channels to select them individually.
  - **UNII-2 52-144**—The channels available for UNII-2 band are: **52**, **56**, **60**, **64**, **100**, **104**, **108**, **112**, **116**, **120**, **124**, **128**, **132**, **136**, **140**, and **144**. Check the **UNII-2 52-144** check box to include all channels or check the check box of the channels to select them individually.
  - **UNII-3 149-165**—The channels available for UNII-3 band are: **149**, **153**, **157**, **161**, and **165**. Check the **UNII-3 149-165** check box to include all channels or check the check box of the channels to select them individually.
- Use the **Data Rate** slider to set the rates at which data can be transmitted between an access point and a client. The available data rates are **6**, **9**, **12**, **18**, **24**, **36**, **48**, and **54**.
- Under **Tx Power Configuration**, you can set the power level and power threshold for an AP.
  - **Power Level**—To determine whether the power of an AP needs to be reduced or not. Reducing the power of an AP helps mitigate co-channel interference with another AP on the same channel or in close proximity. Use the **Power Level** slider to set the minimum and maximum power level. The range is -10 to 30 dBm and the default is -10 dBM.
  - **Power Threshold**—It is the cutoff signal level used by Radio Resource Management (RRM) to determine whether to reduce the power of an AP or not. Use the **Power Threshold** slider to increase and decrease the power value which causes the AP to operate at higher or lower transmit power rates. The range is -50 dBM to 80 dBM and the default threshold is -70 dBM.
  - **RX SOP**—Receiver Start of Packet Detection Threshold (RX SOP) determines the Wi-Fi signal level in dBm at which an APs radio demodulates and decodes a packet. From the RX SOP drop-down list, choose **High**, **Medium**, **Low**, or **Auto** threshold values for each 802.11 band.

Step 7 Click **Save**.

Step 8 To mark a profile as a default RF profile, check the **Profile Name** check box and click **Mark Default**.

Step 9 In the **Warning** window, click **OK**.

Provision a Cisco Sensor SSID for Nonfabric Deployment

- The Cisco DNA Center sensor uses the Cisco sensor provisioning Service Set Identifier (SSID) to communicate with the Plug and Play (PnP) server and obtain day-0 configurations for running tests.

Note The Cisco sensor provisioning SSID is not applicable for APs working as sensors.

- For fabric deployments, the Cisco sensor provisioning SSID is mapped to an Infrastructure Virtual Network Access Point (INFRA VN–AP) pool to communicate with Cisco DNA Center.
- The following platforms support the Cisco sensor provisioning SSID:
  - Cisco AireOS Controller
  - Cisco Catalyst 9800 Series Wireless Controller (both fabric and nonfabric deployments)
- The Cisco sensor provisioning SSID supports the following network controllers:
  - Cisco Catalyst 9800 Wireless Controllers for Cloud
  - Cisco Catalyst 9800 Series Wireless Controller
  - Cisco AireOS Controller

The following procedure enables you to configure the Cisco sensor provisioning SSID for nonfabric deployments.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Design** > **Network Settings** > **Wireless**.

Step 2 Click **Add Create** and choose **Enterprise**.

Step 3 Toggle the **Sensor** field and click **Next**.

Note The parameters for the SSID are automatically populated and cannot be edited.

Step 4 Click **Next**.

Step 5 In the **Wireless Profiles** screen, check a profile from the **Profiles** table.
The **Edit Wireless Profile** dialog box opens.

Step 6 In Fabric, select **Yes** and click **Save**.
The **Success Profile sensorProfile selected** message appears.

Step 7 Click **Finish**.

Step 8 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Provision** > **Network Devices** > **Inventory**.

Step 9 Check a device and from the **Actions** drop-down menu, choose **Provision** > **Provision Device**.

Step 10 Review the details under **Assign Site**, **Configuration**, **Model Configuration**, **Advanced Configuration**, and **Summary**.
Click **Next** after each screen.

Step 11 Click **Deploy**.
The **Provision Device** dialog box is displayed.

Step 12 Choose **Now** and click **Apply**.
The message **Task Scheduled view status in Tasks** appears at the bottom-right corner.

Manage Backhaul Settings

Use this procedure to view, create, and manage backhaul configurations for wireless sensors. A wireless sensor requires a backhaul SSID to communicate with Cisco DNA Center.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Manage** > **Sensors**.

The **Sensor List** window appears.

Step 2 Click on **Settings** > **Backhaul Settings** tab.

The **Backhaul Settings** window appears.

Step 3 You can add and manage backhaul SSIDs by doing the following:

a) Click **+ Add Backhaul**.

The **Create Sensor Backhaul SSID Assignment** window appears with two areas: **Wired Backhaul** and **Wireless Backhaul**.

b) In the **Settings Name** field, enter a name for the backhaul SSID.

c) In the **Wired Backhaul** area, configure the following:

- **Level of Security**: Displays the encryption and authentication type used by the selected SSID. The available security options are:
  - **802.1x EAP**: Standard used for passing Extensible Authentication Protocol (EAP) over wired LAN.
  - **Open**: No security or authentication is used.
- **EAP Method**: If you choose **802.1x EAP**, you must choose one of the following EAP methods for user authentication from the drop-down list:
  - **EAP-FAST**: Enter the user name and password in the fields provided.
  - **PEAP-MSCHAPv2**: Enter the user name and password in the fields provided.
  - **EAP-TLS**: Choose **Enroll Using Certificate Bundle** or **Enroll Using SCEP**.

    If you choose **Enroll Using Certificate Bundle**, click the drop-down arrow under **Certificate Bundle**, click **+ Add New Certificate Bundle**, and enter the user name and certificate bundle password.
  - **PEAP-TLS**: Choose **Enroll Using Certificate Bundle** or **Enroll Using SCEP**.

    If you choose **Enroll Using Certificate Bundle**, click the drop-down arrow under **Certificate Bundle**, click **+ Add New Certificate Bundle**, and enter the user name and certificate bundle password.

d) In the **Wireless Network Name (SSID)** area, select the wireless network (SSID) and configure the following.

- **Level of Security**: Displays the encryption and authentication type used by the selected SSID. The available security options are:
  - **WPA2 Enterprise**: Provides a higher level of security using Extensible Authentication Protocol (EAP) (802.1x) to authenticate and authorize network users with a remote RADIUS server.
  - **WPA2-Personal**: Provides a good security using a passphrase or a pre-shared key (PSK). This allows anyone with the passkey to access the wireless network.

If you select **WPA2 Personal**, enter the passphrase in the **Passphrase** text box.

- **PSK Format**:The available pre-shared key formats are:
  - **ASCII**: Supports ASCII PSK passphrase.
  - **HEX**: Supports 64-character HEX key PSK password.
- **Open**: No security or authentication is used.

e) Click **Save**.

Step 4 You can edit the existing backhaul configurations by doing the following:

a) Check the check box of the backhaul configuration.
b) Hover your cursor over the **Actions** drop-down list and choose **Edit**.

Step 5 You can delete a backhaul configuration by doing the following:

a) Check the check box of the backhaul configuration.
b) Hover your cursor over the **Actions** drop-down list and choose **Delete**.

About Cisco Connected Mobile Experiences Integration

Cisco DNA Center supports the integration of Connected Mobile Experiences (CMX) for wireless maps. With the CMX integration, you can get the exact location of your wireless clients, rogue access points and interferers on the floor map within the Cisco DNA Center user interface.

Depending on your requirements, you can create CMX settings either at the global level or at the site, building, or floor level. For a small enterprise, you can assign CMX at the global level, which is the parent node. All children inherit their settings from the parent node. For a medium enterprise, you can assign CMX at the building level and for a small enterprise, you can assign CMX at the floor level.

Note CMX should be anonymized for security purposes.

Create Cisco CMX Settings

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Settings** > **External Services** > **CMX Servers**.

The **CMX Servers** window appears.

Step 2 Click **Add**.

The **Add CMX Server** window appears.

Step 3 In the **IP Address** field, enter the valid IP address of the CMX web GUI.

Step 4 In the **User Name** and **Password** fields, enter the CMX web GUI username and password credentials.

Step 5 In the **SSH User Name** and **SSH Password** fields, enter the CMX admin username and password credentials.

Note Make sure that CMX is reachable.

Step 6 Click **Add**.

The CMX server is added successfully.

Step 7 To assign a CMX server to a site, building, or a floor, click the **Menu** icon and choose **Design** > **Network Settings** > **Wireless**.

Step 8 In the left tree view menu, select either Global or the area, building, or floor that you are interested in.

Step 9 Under **CMX Servers**, from the **CMX Servers** drop-down list, select the CMX server.

Step 10 Click **Save**.

The **Create CMX Settings** page appears.

After the CMX is added, if you make any changes to the floor on the **Network Hierarchy** page, the changes are synchronized automatically with the CMX.

When the CMX is synced, Cisco DNA Center starts querying the CMX for the client location and displays the location on the floor map.

From the floor map, you can do the following:

- View the location of the client, which is shown as a blue dot.
- Hover your cursor over an AP. A dialog box is displayed with **Info**, **Rx Neighbor**, and **Clients** tabs. Click each tab for more information. Click **Device 360** to open the Device 360 window and view issues. Click an issue to see the location of the issue and the location of the client device.
- Click an AP to open a side bar with details about the AP.
- Perform real-time client tracking when Intelligent Capture and CMX are integrated.

Step 11 If the CMX was down when you made changes, you must synchronize manually. To do so, on the **Network Hierarchy** page, click the gear icon next to the building or floor on which you made the changes in the left tree pane, and then choose **Sync with CMX** to push the changes manually.

Step 12 To edit the CMX server details or delete a CMX server, do the following:

a) In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Settings** > **External Services** > **CMX Servers**.
b) Select the CMX server that you want to edit, make any changes, and click **Update**.
c) Select the CMX server that you want to delete and click **Delete**.
d) Click **OK** to confirm the deletion.

For CMX Authentication Failure

- Check if you are able to log in to the CMX web GUI with the credentials that you provided at the time of CMX settings creation on Cisco DNA Center.
- Check if you are able to log in to the CMX console using SSH.
- Check if you are able to exercise CMX REST APIs using the API Documentation link on the CMX GUI.

If Clients Do Not Appear on the Cisco DNA Center Floor Map

- Check if the Cisco wireless controller on the particular floor is configured with CMX and is active.

- Check if the CMX GUI shows clients on the floor map.
- Use the Cisco DNA Center Maps API to list the clients on the floor: `curl -k -u <user>:<password> -X GET /api/v1/dna-maps-service/domains/<floor group id>/clients?associated=true`

About Cisco DNA Spaces Integration

Enterprises operating in the physical world have limited to no visibility into the behavior of people and connected assets within their buildings. Cisco DNA Spaces solves this physical blind-spot problem using location-sensing intelligence from all underlying Cisco wireless networks and translating the data into business-ready insights.

Cisco DNA Center supports the integration of Cisco DNA Spaces. With the Cisco DNA Spaces integration, you can get the exact location of your wireless clients, rogue APs, and interferers on the floor map in the Cisco DNA Center GUI. Depending on your requirements, you can create Cisco DNA Spaces settings either at the global level or at the site, building, or floor level.

Note The Cisco DNA Center and Cisco DNA Spaces integration is currently limited to only automatic map exports and synchronization for the location hierarchy. The integration does not support captive portal-based authentication features.

Integrate Cisco DNA Spaces with Cisco DNA Center

Use this procedure to integrate Cisco DNA Spaces with Cisco DNA Center.

Step 1 Onboard the Cisco DNA Spaces client:

a) Log in to Cisco DNA Spaces using your email ID, and click **Continue**.

The **Select Customer** dialog box is displayed.

b) From the **Select Customer** drop-down list, choose the Spaces tenant for the Cisco DNA Center instance (for example, dna-center-dev-US), and then click **Proceed**.

c) In the Cisco DNA Spaces GUI, click the **Menu** icon and choose **Setup** > **Wireless Networks**.

The **Connect your wireless network** window is displayed.

d) In the **Connect your wireless network** window, complete Steps 1 to 3 as documented in the *Cisco DNS Configuration Guide* to onboard the Cisco DNA Spaces client.

You can access the *Cisco DNS Configuration Guide* from the right pane under **Need Help?**. Choose **View Configuration Steps**.

Step 2 Deploy the **DNA Spaces Enabler Package** software on Cisco DNA Center:

a) Contact your Cisco account representative to obtain the **DNA Spaces Enabler Package** software.

b) Log in to Cisco DNA Center.

c) From the Cisco DNA Center GUI, click the **?** icon to verify that Cisco DNA Center is running the current release.

d) In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Software Updates**.

The **Software Updates** page opens and the **DNA Spaces Enabler Package** is displayed in the list of **Application Updates**.

e) Click **Install All**.

The **Select Any Package To Continue** dialog box is displayed.

f) Select the **DNA Spaces Enabler Package** and click **Continue**.

The **System Readiness Check** dialog box is displayed.

g) Click **Continue**.

The **Success** dialog box states that the package will soon be installed.

Step 3 Register Cisco DNA Center with Cisco DNA Spaces:

a) Log in to Cisco DNA Spaces using your email ID, and click **Continue**.

The **Select Customer** dialog box is displayed.

b) From the **Select Customer** drop-down list, choose the Spaces tenant for the Cisco DNA Center instance (for example, dna-center-dev-US), and then click **Proceed**.

c) In the Cisco DNA Spaces GUI, click the **Menu** icon and choose **Integrations** > **DNA Center**.

The **DNAC Integration** window is displayed.

d) In the **DNAC Integration** window, click **Create Token**.

The **Create new token** dialog box is displayed.

e) In the **Instance Name** field, enter a unique name for the instance, and then click **Create Token**.

A new token for the instance opens.

f) Scroll to the right of the token and choose **Copy Token**.

g) To paste the token in to the Cisco DNA Center GUI, log in to Cisco DNA Center.

h) In the Cisco DNA Center GUI, click the **Menu** icon and choose **System** > **Settings**.

i) In the left navigation pane, scroll down and choose **DNA Spaces/CMX Servers**.

The **DNA Spaces/CMX Servers** window is displayed.

j) From the **DNA Spaces** area, choose **Activate**.

The **Integrate DNA Spaces** dialog box is displayed.

k) In the **Tenant Token** text box, press **Ctrl V** to paste the token that you copied from Cisco DNA Spaces, then click **Connect**.

The **Success** dialog box is displayed with the following information:

```
This cluster is integrated with Cisco DNA Spaces successfully.
```

The DNA Spaces/CMX Servers window displays a green ✓ **Activated** status, and the tenant that you selected in Cisco DNA Spaces (for example, dna-center-dev-US) is displayed in the **Tenant** field.

Step 4 Assign Cisco DNA Spaces to sites in Cisco DNA Center:

a) In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **Wireless**.

b) In the left tree view menu, select either **Global** or the area, building, or floor to which you want to assign Cisco DNA Spaces.

c) Under **DNA Spaces/CMX Servers**, from the **Location Services** drop-down list, select a site (for example, DNA Spaces - dna-center-dev-US).
d) Click **Save**.

Step 5 Monitor sites in Cisco DNA Center using Cisco DNA Spaces:

a) In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Hierarchy**.
b) In the left tree view menu, select either **Global** or the area, building, or floor that you want Cisco DNA Spaces to monitor.

Cisco DNA Center deploys the site information to Cisco DNA Spaces automatically.

c) To confirm that the Cisco DNA Spaces is operational, verify that the Cisco DNA Spaces/CMX status icon displays on the floor that you want to monitor, as shown in the following figure.

Figure 4: Cisco DNA Spaces Status Icon

Configure Native VLAN for a Flex Group

Native VLAN carries the management traffic between APs and Cisco Wireless Controllers. With this feature, you can configure VLAN for a site through the Cisco DNA Center user interface. You can configure native VLAN at the global level and override at the site, building, or floor level.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **Wireless**.

Step 2 In the left pane, choose **Global** if you are configuring native VLAN at the global level.

Step 3 Under **Native VLAN**, enter a value for the VLAN ID in the VLAN text box. The valid range is from 1 to 4094.

Step 4 Click **Save**.

Step 5 Configure the SSID and create a wireless network profile. Make sure that the **FlexConnect Local Switching** check box on the **Design** > **Network Settings** > **Wireless** page is enabled. For more information, see the Create SSIDs for an Enterprise Wireless Network, on page 141 and Create SSIDs for a Guest Wireless Network, on page 146.

Step 6 For the saved VLAN ID to get configured on the wireless controller, you must provision the wireless controller on the **Provision** page. For more information, see Provision a Cisco AireOS Controller, on page 375.

Step 7 After provisioning the wireless controller, you must provision the AP that is associated with the controller. For more information, see Provision a Cisco AP—Day 1 AP Provisioning, on page 385.

Step 8 To override the native VLAN at the site, building, or floor level, in the left tree view menu, select the site, building, or floor.

Step 9 Under **Native VLAN**, enter a value for the VLAN ID.

Step 10 Reprovision the wireless controllers and the associated access point.

Create Network Profiles

In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Profiles**, and click **Add Profile** to create network profiles for:

- Routing and NFV
- Firewall
- Switching
- Wireless

Create Network Profiles for NFVIS

This workflow shows how to:

1. Configure the router WAN.
2. Configure the ENCS integrated switch.

Note This option is available only on ENCS 5400 devices.

3. Create custom configurations.
4. View the profile summary.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Profiles**.

Step 2 Click **+Add Profile** and choose **NFVIS**.

Step 3 The **Router WAN Configuration** window appears.

- Enter the profile name in the **Name** text box.
- Select the number of **Service Providers** and **Devices** from the drop-down list. Up to three service providers and two devices are supported per profile.

- Select the **Service Provider Profile** from the drop-down list. For more information, see Configure Service Provider Profiles, on page 189.
- Select the **Device Type** from the drop-down list.
- Enter a unique string in the **Device Tag** to identify the different devices, or select an existing tag from the drop-down list. Select the appropriate tag, because your selection is used as part of the matching criteria for Day-0 and Day-N templates applied to the network profile.
- To enable at least one line link for each device to proceed, click **O** and check the check box next to **Connect**. Select the **Line Type** from the drop-down list. Click **OK**.
- Click **+Add Services** to add services to the profile. The **Add Services** window appears. Click on a **Router**, **Firewall**, or **Application** icon and drag it onto the diagram. Based on your selection, the default network connections are automatically created. You can also select **Custom- Net** to add custom services or networks to the profile.

  To configure the router, click on the router and select **Configuration**. Select the **Type**, **Image** and **Profile** from the drop-down list. For more information, see Import a Software Image, on page 91. Set the **vNIC Mapping** fields as required.

  To configure the firewall, click on the firewall and select **Configuration**. Select the **Type**, **Image** and **Profile** from the drop-down list. The drop-down list for **Type** is populated based on the firewall plugins installed on the system. Set the **vNIC Mapping** fields as required.

  To configure the application, click on the application and select **Configuration**. Select the **Type**, **Image** and **Profile** from the drop-down list. The drop-down list for **Type** is populated based on the application plugins installed on the system. Set the **vNIC Mapping** fields as required.

  To configure custom networks, click on custom-net interface. Select **Connect from** and click on the node you want to add the custom network to and select **Connect to**. Click on custom-net and select **Add Configuration**. Select the **Network Mode** and enter the VLAN ID in **VLAN**.

  Click **Save**.
- Click **Next**.

Step 4 If you have selected an ENCS device, the **ENCS Integrated Switch Configuration** page appears.

- Click **+Add Row**. Select **Type** from the drop-down list and enter the **VLAN ID/Allowed VLAN** and the **Description**.
- Click **Next**.

Step 5 The **Custom Configuration** page appears.

The custom configurations are optional. You may skip this step and apply the configurations at any time in the Network Profiles page.

If you choose to add the custom configurations:

- Select the **Onboarding Template(s)** or **Day-N Templates** tab, as required.
- Select the Template from the drop-down list. The templates are filtered by the **Device Type** and **Tag Name**.
- Click **Next**.

Step 6 The **Summary** page appears.

This page summarizes the router configurations. Based on the devices and services selected, the hardware recommendation is provided in this page.

- Click **Save**.

Step 7 The **Network Profiles** page appears.

Click **Assign Sites** to assign a site to the network profile. For more information, see Create a Site in a Network Hierarchy, on page 111.

Create Network Profiles for Routing

This workflow shows how to:

1. Configure the router WAN.
2. Configure the router LAN.
3. Configure the integrated switch configuration.
4. Create custom configurations.
5. View the profile summary.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Profiles**.

Step 2 Click **+Add Profile** and choose **Routing**.

Step 3 The **Router WAN Configuration** window appears.

- Enter the profile name in the **Name** text box.
- Select the number of **Service Providers** and **Devices** from the drop-down list. Up to three service providers and ten devices are supported per profile.
- Select the **Service Provider Profile** from the drop-down list. For more information, see Configure Service Provider Profiles, on page 189.
- Select the **Device Type** from the drop-down list.
- Enter a unique string in the **Device Tag** to identify the different devices, or select an existing tag from the drop-down list. Use the device tag if two or more devices are of the same type. If all the devices are of a different type, the device tag is optional. Select the appropriate tag, because your selection is used as part of the matching criteria for Day-0 and Day-N templates applied to the network profile.
- To enable at least one line link for each device to proceed, click **O** and check the check box next to **Connect**. Select the **Line Type** from the drop-down list. Click **OK**.

  If you select multiple service providers, you can select the primary interface as gigabit Ethernet and the secondary as cellular, or both the interfaces as gigabit Ethernet. You can also select the primary interface as cellular and the secondary interface as gigabit Ethernet.

  Note Only Cisco 1100 Series Integrated Services Routers, Cisco 4200 Series Integrated Services Routers, Cisco 4300 Series Integrated Services Routers, and Cisco 4400 Series Integrated Services Routers support the cellular interface.

- Click **Next**.

Step 4 The **Router LAN Configuration** page appears.

- Click the **Configure Connection** radio button and choose L2, L3, or both.
- If you choose **L2**, select the **Type** from the drop-down list and enter the **VLAN ID/Allowed VLAN** and the **Description**.
- If you choose **L3**, select the **Protocol Routing** from the drop-down list and enter the **Protocol Qualifier**.

You can click **Skip** to skip the configuration.

- Click **Next**.

Step 5 The **Integrated Switch Configuration** page appears.

The integrated switch configuration allows you to add new VLANs or retain the previous configuration selected in the router LAN configuration.

- To add one or more new VLANs, click **+**.
- To delete a VLAN, click **x**.
- Click **Next**.

Note Switchport Interface support is available only for Cisco 1100 Series and Cisco 4000 series Integrated Services Routers.

Step 6 The **Custom Configuration** page appears.

The custom configurations are optional. You can skip this step and apply the configurations at any time in the Network Profiles page.

If you choose to add custom configurations:

- Click the **Onboarding Template(s)** or **Day-N Templates** tab, as required.
- Choose a template from the drop-down list. The templates are filtered by **Device Type** and **Tag Name**.
- Click **Next**.

Step 7 On the **Summary** page, click **Save**.

This page summarizes the router configurations. Based on the devices and services selected, the hardware recommendation is provided.

Step 8 The **Network Profiles** page appears.

Click **Assign Sites** to assign a site to the network profile. For more information, see Create a Site in a Network Hierarchy, on page 111.

Create Network Profiles for Firewall

This workflow shows how to:

1. Create custom configurations.

2. Create Firepower Threat Defense (FTD) configurations.
3. View the profile summary.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Profiles**.

Step 2 Click +**Add Profile** and choose **Firewall**.

The **Firewall Type** page appears.

Step 3 To create custom configurations for regular firewalls like Adaptive Security Appliance (ASA) firewalls, do the following:

a) In the **Name** field, enter the profile name.

b) Choose the number of devices from the **Devices** drop-down list.

Note You can choose up to 10 devices per profile.

c) Choose the type of device from the **Device Type** drop-down list.

d) (Optional) From the **Device Tag** drop-down list, choose the device tags.

e) Click **Next**.

The **Custom Configuration** page appears.

f) From the **Template** drop-down list, choose a template.

Note If there are no templates, you must create at least one template in **Tools** > **Template Editor**. For information, see Create Templates, on page 194.

g) Click **Next**.

The **Summary** page appears. This page summarizes the custom configurations. Based on the selected device type, a hardware recommendation is provided.

h) Click **Save**.

The **Network Profiles** page appears.

i) To assign a site to the network profile, click **Assign Sites**. For more information, see Create a Site in a Network Hierarchy, on page 111.

Step 4 To create FTD configurations to configure the FTD devices, do the following:

a) In the **Name** field, enter the profile name.

b) From the **Devices** drop-down list, choose the number of devices.

Note You can choose up to 10 devices per profile.

c) To provision an FTD firewall, check the **FTD** check box.

d) From the **Device Type** drop-down list, choose the type of device.

e) (Optional) Choose the device tags from the **Device Tag** drop-down list.

f) Click **Next**.

The **FTD Configuration** page appears.

g) Click the **Routed Mode** or **Transparent Mode** radio button.

h) Click **Next**.

The **Summary** page appears. This page summarizes the FTD configurations. Based on the selected device type, hardware recommendation is provided on this page.

i) Click **Save**.

The **Network Profiles** page appears.

j) To assign a site to the network profile, click **Assign Sites**. For information, see Create a Site in a Network Hierarchy, on page 111.

Create Network Profiles for Switching

You can apply two types of configuration templates to a switching profile:

- Onboarding template
- Day N template

Before you begin

Define the **Onboarding Configuration** template that you want to apply to the devices. Such templates contain basic network configuration commands to onboard a device so that it can be managed on the network. See Create Templates to Automate Device Configuration Changes, on page 193.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Profiles**.

Step 2 Click **+Add Profile** and choose **Switching**.

Step 3 In the Switching profile window, enter the profile name in the **Profile Name** text box.

Depending on the type of template that you want to create, click **OnBoarding Template(s)** or **Day-N Template(s)**.

- Click **+Add**.
- Select **Switches and Hubs** from the **Device Type** drop-down list.
- Select the **Tag Name** from the drop-down list. This step is optional. If the tag that you selected has already been associated with a template, only that template is available in the Template drop-down list.
- Select the **Device Type** from the drop-down list.
- Select a **Template** from the drop-down list. You can select the Onboarding Configuration template that you have already created.

Step 4 Click **Save**.

The profile that is configured on the switch is applied when the switch is provisioned. Note that you must add the network profile to a site for it to be effective.

Create Network Profiles for Wireless

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Profiles**.

Step 2 Click **+Add Profile** and choose **Wireless**.

Before assigning a wireless network profile, make sure that you have created wireless SSIDs under **Design** > **Network Settings** > **Wireless** tab.

Step 3 In the **Add a Network Profile** window, enter a valid profile name in the **Profile Name** text box.

Step 4 Click **+ Add SSID**.

The SSIDs that were created are populated.

Step 5 From the **SSID** drop-down list, choose the SSID.

The SSID type is displayed.

Step 6 Specify whether the SSID is fabric or nonfabric by selecting **Yes** or **No**.

Step 7 If you are creating a nonfabric SSID, select **No**, and configure the following parameters.

Step 8 From the **Interface Name** drop-down list, choose an interface name for the SSID, or click **+ create a new wireless interface** to create a new wireless interface.

Step 9 Check the **Flex Connect Local Switching** check box to enable local switching for the WLAN.

If you have enabled **Flex Connect Local Switching** for an SSID, then all APs on that particular floor where the network profile is mapped will switch to FlexConnect mode.

When you enable local switching, any FlexConnect AP that advertises this WLAN is able to locally switch data packets.

Step 10 The VLAN ID that is associated with the wireless interface is autopopulated based on the interface name selected.

If you want to change the VLAN ID, in the **Local to VLAN** text box, enter a new value for the VLAN ID.

Step 11 Click **+ Add Model Config** to add model config designs to a network profile.

The **Add Model Config** window appears.

Step 12 From the **Device Type(s)** drop-down list, select the device type.

You can either search for a device name by entering its name in the **Search** field or expand **Wireless Controller** and select the device type.

Step 13 Expand **Wireless** and select the model config design that you are attaching to this wireless profile.

Step 14 From the **Tags** drop-down list under **APPLICABILITY**, select the applicable tags.

Step 15 Click **Add**.

The attached model config appears under the **Attach Model Config** area in the **Add a Network Profile** window.

Step 16 To associate a template with the network profile, click **Add** under the **Attach Template(s)** area.

Step 17 From the **Device Type(s)** drop-down list, choose the device type.

You can either search for a device name by entering its name in the **Search** field or expand **Wireless Controller** and select the device type.

Step 18 You can choose the device tag and template from the **Device Tag** and **Template** drop-down lists.

You can use tags on templates only when you have to push different templates for the same device type based on the device tag.

Step 19 Click **Add**.

The created profile appears in the **Wireless Profiles** window.

Step 20 Click **Save** to add a network profile.

The newly added network profile appears on the **Design** > **Network Profiles** page.

Step 21 To assign this profile to a site, click **Assign Sites**.

Step 22 In the **Add Sites to Profile** window, check the check box next to the site to associate to this profile.

You can select a parent node or the individual sites. If you select a parent site, all the children under the parent node are also selected. You can uncheck the check box to deselect a site.

Step 23 Click **Save**.

Preprovision the AP Group, Flex Group, and Site Tag in a Network Profile

Cisco DNA Center allows you to preprovision the AP group, flex group, and site tag in a network profile. Preprovisioning saves time during AP provisioning by eliminating the need to make repetitive configuration changes and ensures consistency across your devices.

- AP group configuration is applicable to Wireless LAN controllers running an AireOS image.
- Flex group configuration is applicable to Wireless LAN controllers running an AireOS image.
- Site tag configuration is applicable to Catalyst 9800 series wireless controllers.

Before you begin

You must create a network profile and assign a site (floor) to the network profile to enable AP group, flex group, and site tag creation.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Profiles**.

Step 2 Click **Edit**.

Step 3 Click **Show Advanced Settings**.

Step 4 To create an AP group in the network profile, expand **AP Group** and click **+ Create an AP Group**.

The **Create an AP Group** window appears.

Step 5 In the **AP Group Name** field, enter the AP group name.

Step 6 From the **RF Profile** drop-down list, choose the RF profile.

The options are **High**, **Typical**, **Low**, **custom_rf_profile2**, and **rf_prof1_custom**.

Step 7 In the **Select Sites** field, you can either search for a site by entering its name or expand **Global** to select the site.

Step 8 (Optional) Click **Save & Add another** to add another AP group.

Step 9 Click **Save**.

The AP group is created based on the selected RF profile under the **AP Group** area in the **Edit Network Profile** window.

Step 10 To enable the flex group in the network profile, check the **Flex Connect Local Switching** check box and define the VLAN ID in the **Local to VLAN** text box to mark the nonfabric SSID as a flex-based SSID.

If you have enabled **Flex Connect Local Switching** for an SSID, then all APs on that particular floor where the network profile is mapped will switch to FlexConnect mode.

The **Flex Group** option is enabled under **View Advanced Settings**.

Step 11 To create a flex group in the network profile, expand **Flex Group** and click **+ Create Flex Group**.

The **Create Flex Group** window appears.

Step 12 In the **Flex Group** field, enter the flex group name.

Step 13 In the **Select Sites** field, you can either search for a site by entering its name or expand **Global** to select the site.

Step 14 (Optional) Click **Save & Add another** to add another flex group.

Step 15 Click **Save**.

The flex group is created under the **Flex Group** area in the **Edit Network Profile** window.

Step 16 To create a site tag in the network profile, expand **Site Tag** and click **+ Create a Site Tag**.

The **Create a Site Tag** window appears.

Step 17 In the **Site Tag** field, enter the site tag name.

Step 18 In the **Flex Profile Name** name field, enter the flex profile name.

Note To enable the **Flex Profile Name** name field, check the **Flex Connect Local Switching** check box in the **Edit Network Profile** window.

Step 19 In the **Select Sites** field, you can either search for a site by entering its name or expand **Global** to select the site.

Step 20 (Optional) Click **Save & Add another** to add another site tag.

Step 21 Click **Save**.

The site tag is created under the **Site Tag** area in the **Edit Network Profile** window.

Create Network Profile for Cisco DNA Traffic Telemetry Appliance

Before you begin

Define the template that you want to apply to the telemetry appliances. See Create Templates to Automate Device Configuration Changes, on page 193.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Profiles**.

Step 2 Click **+Add Profile** and choose **Telemetry Appliance**.

Step 3 In the **Telemetry Appliance Type** window, complete the following:

a) Enter the profile name in the **Name** text box.

b) From the **Devices** drop-down list, choose the number of devices.
c) From the **Device Tag** drop-down list, choose an existing device tag defined in Cisco DNA Center or enter a new tag. This step is optional. If the tag that you selected has already been associated with a template, only that template is available in the Template drop-down list.
d) Click **Next**.

Step 4 In the **Custom Configuration** window, choose the template. The chosen template will be applied to the device once it is managed in Cisco DNA Center inventory.

Step 5 Click **Next**.

Step 6 In the **Summary** window, click **Save.**

About Global Network Settings

You can create network settings that become the default for your entire network. There are two primary areas from which you can define the settings within your network:

- **Global settings**: Settings defined here affect your entire network and include settings for servers such as DHCP, DNS, AAA, NTP, and so on; IP address pools; Device Credential profiles; Telemetry settings such as Syslog, Traps, and Netflow.
- **Site settings**: Settings define here override global settings and can include settings for servers, IP address pools, and device credential profiles.

Note Changes in network settings that are being used by the active fabric are not supported. These network settings include site hierarchy, renaming IP pools, and several other features.

Note Certain network settings can be configured on devices automatically using the Device Controllability feature. When Cisco DNA Center configures or updates devices, the transactions are captured in the Cisco DNA Center audit logs. You can use the audit logs to help you track changes and troubleshoot issues.

You can define the following global network settings by choosing **Design** > **Network Settings** and clicking the appropriate tab.

- Network servers, such as AAA, DHCP, and DNS—For more information, see Configure Global Network Servers, on page 189.
- Device credentials, such as CLI, SNMP, and HTTP(S)—For more information, see Configure Global CLI Credentials, on page 176, Configure Global SNMPv2c Credentials, on page 177, Configure Global SNMPv3 Credentials, on page 178, and Configure Global HTTPS Credentials, on page 180.
- IP address pools—For more information, see Configure IP Address Pools, on page 184.
- Wireless settings as SSIDs, wireless interfaces, and wireless radio frequency profiles—For more information, see Configure Global Wireless Settings, on page 141.
- Configure global telemetry settings, such as syslog, SNMP, and NetFlow Collector servers using telemetry.

About Device Credentials

Device credentials refer to the CLI, SNMP, and HTTPS credentials that are configured on network devices. Cisco DNA Center uses these credentials to discover and collect information about the devices in your network. In Cisco DNA Center, you can specify the credentials that most of the devices use so that you do not have to enter them each time you run a discovery job. After you set up these credentials, they are available for use in the **Discovery** tool.

CLI Credentials

You need to configure the CLI credentials of your network devices in Cisco DNA Center before you can run a Discovery job.

These credentials are used by Cisco DNA Center to log in to the CLI of a network device. Cisco DNA Center uses these credentials to discover and gather information about network devices. During the discovery process, Cisco DNA Center logs in to the network devices using their CLI usernames and passwords and runs **show** commands to gather device status and configuration information, and **clear** commands and other commands to perform actions that are not saved in a device's configuration.

Note In Cisco DNA Center's implementation, only the username is provided in cleartext.

SNMPv2c Credentials

Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language to monitor and manage network devices.

SNMPv2c is the community string-based administrative framework for SNMPv2. SNMPv2c does not provide authentication or encryption (noAuthNoPriv level of security). Instead, it uses a community string as a type of password that is typically provided in cleartext.

Note In Cisco DNA Center's implementation, SNMP community strings are not provided in cleartext for security reasons.

You must configure the SNMPv2c community string values before you can discover your network devices using the Discovery function. The SNMPv2c community string values that you configure must match the SNMPv2c values that have been configured on your network devices. You can configure up to 10 read community strings and 10 write community strings in Cisco DNA Center.

If you are using SNMPv2 in your network, specify both the Read Only (RO) and Read Write (RW) community string values to achieve the best outcome. If you cannot specify both, we recommend that you specify the RO value. If you do not specify the RO value, Cisco DNA Center attempts to discover devices using the default RO community string, *public*. If you specify only the RW value, Discovery uses the RW value as the RO value.

For Plug and Play, both SNMPv2c Read Only and Read Write credentials must be provided.

SNMPv3 Credentials

The SNMPv3 values that you configure to use Discovery must match the SNMPv3 values that have been configured on your network devices. You can configure up to 10 SNMPv3 values.

The security features provided in SNMPv3 are as follows:

- Message integrity: Ensures that a packet has not been tampered with in transit.
- Authentication: Determines if a message is from a valid source.
- Encryption: Scrambles a packet's contents to prevent it from being seen by unauthorized sources.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and a user's role. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

The security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The various security levels that exist within a security model are as follows:

- noAuthNoPriv: Security level that does not provide authentication or encryption
- AuthNoPriv: Security level that provides authentication, but does not provide encryption
- AuthPriv: Security level that provides both authentication and encryption

The following table describes the security model and level combinations:

Table 36: SNMPv3 Security Models and Levels

Level	Authentication	Encryption	What Happens
noAuthNoPriv	User Name	No	Uses a username match for authentication.
AuthNoPriv	Either: • HMAC-MD5 • HMAC-SHA	No	Provides authentication based on the Hashed Message Authentication Code-Secure Hash Algorithm (HMAC-SHA).
AuthPriv	Either: • HMAC-MD5 • HMAC-SHA	Either: • CBC-DES • CBC-AES-128	Provides authentication based on HMAC-MD5 or HMAC-SHA. Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard or CBC-mode AES for encryption.

The security level must be the same for the SNMPv3 user and the SNMPv3 groups to which that user belongs. If the SNMPv3 user and that user's SNMPv3 groups have different security levels, when Cisco DNA Center configures the SNMPv3 trap host, device SNMP reachability could become impaired.

HTTPS Credentials

HTTPS is a secure version of HTTP that is based on a special PKI certificate store.

About Global Device Credentials

"Global device credentials" refers to the common CLI, SNMP, and HTTPS credentials that Cisco DNA Center uses to discover and collect information about the devices in your network. Cisco DNA Center uses global credentials to authenticate and access the devices in a network that share these configured device credentials. You can add, edit, and delete global device credentials. You can also associate credentials to the Global site or a specific site.

Configure Global CLI Credentials

You can configure and save up to 10 global CLI credentials.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **Device Credentials**.

Step 2 With the Global site selected, in the **CLI Credentials** area, click **Add**.

Step 3 Enter information in the following fields:

Table 37: CLI Credentials

Field	Description
Name/Description	Name or phrase that describes the CLI credentials.
Username	Name that is used to log in to the CLI of the devices in your network.
Password	Password that is used to log in to the CLI of the devices in your network. For security reasons, re-enter the password as confirmation. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Enable Password	Password used to move to a higher privilege level in the CLI. Configure this password only if your network devices require it. For security reasons, re-enter the enable password. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 4 Click **Save**.

To apply the credential to a site, click on the site in the hierarchy on the left, select the button next to the credential, then click **Save**.

Step 5 If you are changing existing credentials, you are prompted to update the new credentials on devices now or schedule the update for a later time.

- To update the new credentials now, click the **Now** radio button and click **Apply**.
- To schedule the update for a later time, click the **Later** radio button, define the date and time of the update and click **Apply**.

Note Use the **Time Zone** check box to indicate whether you want the update to happen according to the site time zone or according to a specified time zone.

Configure Global SNMPv2c Credentials

You can configure global SNMPv2c credentials to monitor and manage your network devices.

Note For Plug and Play, both SNMPv2c Read Only and Read Write credentials must be provided.

Before you begin

You must have your network's SNMP information.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **Device Credentials**.

Step 2 With the Global site selected, in the **SNMP Credentials** area, click **Add**.

Step 3 For the Type, click **SNMP v2c** and enter the following information:

Table 38: SNMPv2c Credentials

Field	Description
Read	• **Name/Description**: Name or description of the SNMPv2c settings that you are adding. • **Read Community**: Read-only community string password used only to view SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Write	• **Name/Description**: Name or description of the SNMPv2c settings that you are adding. • **Write Community**: Write community string used to make changes to the SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 4 Click **Save**.

Step 5 If you are changing existing credentials, you are prompted to update the new credentials on devices now or schedule the update for a later time.

- To update the new credentials now, click the **Now** radio button and click **Apply**.
- To schedule the update for a later time, click the **Later** radio button, define the date and time of the update and click **Apply**.

Note Use the **Time Zone** check box to indicate whether you want the update to happen according to the site time zone or according to a specified time zone.

Configure Global SNMPv3 Credentials

You can configure global SNMPv3 credentials to monitor and manage your network devices.

Before you begin

You must have your network's SNMP information.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **Device Credentials**.

Step 2 With the Global site selected, in the **SNMP Credentials** area, click **Add**.

Step 3 For the Type, click **SNMP v3** and enter the following information:

Table 39: SNMPv3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Choose one of the following modes: • **noAuthNoPriv**: Does not provide authentication or encryption. • **AuthNoPriv**: Provides authentication, but does not provide encryption. • **AuthPriv**: Provides both authentication and encryption.
Auth Type	Authentication type to be used. (Enabled if you select **AuthPriv** or **AuthNoPriv** as the authentication mode.) Choose one of the following authentication types: • **SHA**: Authentication based on HMAC-SHA. • **MD5**: Authentication based on HMAC-MD5.

Field	Description
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	Privacy type. (Enabled if you select **AuthPriv** as the authentication mode.) Choose one of the following privacy types: • **AES128**: CBC mode AES for encryption. • **None**: No privacy.
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support AES128 encryption. Passwords (or passphrases) must be at least eight characters long. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 4 Click **Save**.

Step 5 If you are changing existing credentials, you are prompted to update the new credentials on devices now or schedule the update for a later time.

- To update the new credentials now, click the **Now** radio button and click **Apply**.
- To schedule the update for a later time, click the **Later** radio button, define the date and time of the update and click **Apply**.

Note Use the **Time Zone** check box to indicate whether you want the update to happen according to the site time zone or according to a specified time zone.

Configure Global HTTPS Credentials

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **Device Credentials**.

Step 2 With the Global site selected, in the **HTTPS Credentials** area, click **Add**.

Step 3 Enter the following information:

Table 40: HTTP(S) Credentials

Field	Description
Type	Specifies the kind of HTTPS credentials you are configuring. Valid types are **Read** or **Write**.
Read	You can configure up to 10 HTTPS read credentials: • **Name/Description**: Name or description of the HTTPS credentials that you are adding. • **Username**: Name used to authenticate the HTTPS connection. • **Password**: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). The password must contain from 7 to 128 characters, including at least one: • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 9) • Special character: # _ * ? – The password cannot contain spaces or angle brackets (< >). Note that some Cisco IOS XE devices do not allow a question mark (?).

Field	Description
Write	You can configure up to 10 HTTPS write credentials: • **Name/Description**: Name or description of the HTTPS credentials that you are adding. • **Username**: Name used to authenticate the HTTPS connection. • **Password**: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). The password must contain from 7 to 128 characters, including at least one: • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 9) • Special character: # _ * ? – The password cannot contain spaces or angle brackets (< >). Note that some Cisco IOS XE devices do not allow a question mark (?).

Step 4 Click **Save**.

Step 5 If you are changing existing credentials, you are prompted to update the new credentials on devices now or schedule the update for a later time.

- To update the new credentials now, click the **Now** radio button and click **Apply**.
- To schedule the update for a later time, click the **Later** radio button, define the date and time of the update, and click **Apply**.

Note Use the **Time Zone** check box to indicate whether you want the update to happen according to the site time zone or according to a specified time zone.

Guidelines for Editing Global Device Credentials

The following are guidelines and limitations for editing existing global device credentials:

- Cisco DNA Center uses the following process when you edit, save, and then apply a global device credential:

  1. Cisco DNA Center pushes the credential to the device that has local authentication. With local authentication, credential changes are applied and Cisco DNA Center manages the devices using these credentials.

     (Cisco DNA Center does not push CLI credential changes to a device that is under a site with an inherited or configured AAA server. With AAA authentication, credential changes are not applied.

Cisco DNA Center manages the devices using these credentials only if the same credentials exist on the AAA server.)

2. After successfully pushing the credential to the device, Cisco DNA Center confirms it can reach the device using the new credential.

Note If this step fails, Inventory uses the old credentials to manage the device even though Cisco DNA Center pushed the new credentials to the device. In this case, the **Provision** > **Inventory** window might indicate that the device is Unmanaged if you updated an existing credential.

3. After successfully reaching the device using the new credential, the Cisco DNA Center Inventory starts managing the device using the new credential.

- Sites can contain devices that use SNMPv2c and SNMPv3 credentials. When you edit and save global SNMPv2c or SNMPv3 credentials, Cisco DNA Center pushes those changes to devices and enables that credential. For example, if you have a device that uses SNMPv2c, but you edit and save the SNMPv3 global credential, Cisco DNA Center pushes the new SNMPv3 credential to all devices in the associated site and enables it, meaning that all devices will be managed using SNMPv3, even the devices that previously had SNMPv2c enabled.
- To avoid any possible disruptions, modify the **User Name** when you edit CLI credentials. This creates a new CLI credential and leaves any existing CLI credentials unchanged.

Edit Global Device Credentials

When you edit global device credentials, the changes impact all devices that are associated to the sites under the global site. After you edit and save a global device credential, Cisco DNA Center searches all sites that reference the device credential you changed and pushes the change to all the devices.

You can update or create new global device credentials, but Cisco DNA Center never removes any credentials from devices.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **Device Credentials**.

Step 2 With the Global site selected, select the device credential you want to change, and under the **Actions** column on the right, click **Edit**.

Step 3 In the **Edit CLI Credentials** dialog box, click **Save**.

Step 4 In the **Apply CLI Credentials** dialog box, click **Cancel**.

Step 5 At the bottom of the **Device Credentials** window, click **Save**.

The following message is displayed:

```
Created Common Settings successfully.
```

Step 6 Return to the **Device Credentials** window and click **Edit** for the desired device credential.

Step 7 In the **Edit CLI Credentials** dialog box, make any changes, and click **Save**.

Note The CLI password credentials support only *ASCII-printable characters* (character code 32-127; see https://en.wikipedia.org/wiki/ASCII#Printable_characters).

Step 8 Select whether to update the new credentials on devices now or schedule the update for a later time.

- To update the new credentials now, click the **Now** radio button and click **Apply**.
- To schedule the update for a later time, click the **Later** radio button, define the date and time of the update and click **Apply**.

Note Use the **Time Zone** check box to indicate whether you want the update to happen according to the site time zone or according to a specified time zone.

A status message indicates whether the device credential change succeeded or failed.

Step 9 To view the status of the credential change, in the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The **Credential Status** column displays one of the following statuses:

- Success: Cisco DNA Center successfully applied the credential change.
- Failed: Cisco DNA Center was unable to apply the credential change. Hover over the icon to display additional information about which credential change failed and why.
- Not Applicable: The credential is not applicable to the device type.

If you edited and saved more than one credential (for example, CLI, SNMP, and HTTPS), the **Credential Status** column displays **Failed** if Cisco DNA Center was unable to apply *any* of the credentials. Hover over the icon to display additional information about which credential change failed.

Associate Device Credentials to Sites

The sites you create under the Global site can inherit the global device credentials, or you can create different device credentials specific for a site.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **Device Credentials**.

Step 2 Select a site from the hierarchy in the left pane.

Step 3 Select the credential you want to associate with the selected site, then click **Save**.

A success message appears at the bottom of the screen indicating the device credential was successfully associated with the site.

Step 4 Click **Reset** to clear the entries on the screen.

Configure IP Address Pools

Cisco DNA Center supports IPv4 and IPv6 dual-stack IP pools.

You can manually create IPv4 and IPv6 address pools.

You can also configure Cisco DNA Center to communicate with an external IP address manager. For more information, see the Cisco DNA Center Administrator Guide.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 Click **Add** and complete the required fields in the **Add IP Pool** window.

If you have configured Cisco DNA Center to communicate with an external IP address manager, you cannot create an IP pool that overlaps an existing IP address pool in the external IP address manager.

Step 3 Click **Save**.

The newly added pool appears in the IP Address Pools table. You can click the **IPv4** or **IPv6** option in the **SUBNET TYPE** area if you prefer to view only the IPv4 or IPv6 address pools.

Note When you edit an IP address pool and make DHCP changes, you do not need to reprovision devices using that IP address pool.

Import IP Address Pools from an IP Address Manager

You can import IP address pools from Bluecat or Infoblox.

Note The IP address pools cannot have subpools and cannot have any assigned IP addresses from the IP address pool.

You must configure Cisco DNA Center to communicate with an external IP Address Manager (IPAM). For more information, see the Cisco DNA Center Administrator Guide.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 From the **Actions** drop-down list, choose **Import from IPAM Server** and complete the required fields.

Step 3 Enter a CIDR and then click **Retrieve** to get the list of IP pools available to import.

Step 4 Click **Select All** or choose the IP address pools to import, then click **Import**.

Import IP Address Pools from a CSV File

You can import IP address pools from a CSV file.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 From the **Actions** drop-down list, choose **Import from CSV File**.

Step 3 Click **Download Template** to download the latest sample file.

Step 4 Add the IP address pools to the file and save the file.

Step 5 Upload the CSV file by doing one of the following actions:

a) Drag and drop the file to the drag and drop area.

b) Click where it says "**click** to select" and select the file.

Step 6 Click **Import**.

Reserve an IP Pool

Before you begin

Ensure that one or more IP address pools have been created.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 Expand the hierarchy pane and choose a site.

Step 3 Click **Reserve** and complete the following fields to reserve all or part of an available global IP address pool for the specific site:

- **IP Address Pool Name**: Unique name for the reserved IP address pool.
- **Type**: Type of IP address pool. For LAN automation, choose **LAN**. Options are:
  - **LAN**: Assigns IP addresses to LAN interfaces for applicable VNFs and underlays.
  - **Management**: Assigns IP addresses to management interfaces. A management network is a dedicated network that is connected to VNFs for VNF management.
  - **Service**: Assigns IP addresses to service interfaces. Service networks are used for communication within VNFs.
  - **WAN**: Assigns IP addresses to NFVIS for UCS-E provisioning.
  - **Generic**: Used for all other network types.
- **IP Address Space**: IPv4 and IPv6 address pool from which you want to reserve all or part of the IP addresses.
- **CIDR Prefix/Number of IP Addresses**: IP subnet and mask address used to reserve all or part of the global IP address pool or the number of IP addresses you want to reserve. If you choose \64 as the **CIDR Prefix** for an IPv6 IP pool, the **SLAAC** option is checked. (When **SLAAC** is selected, the devices automatically acquire IP addresses without the need for DHCP servers.)
- **Gateway**: Gateway IP address.
- **DHCP Servers**: DHCP server IP address(es).
- **DNS Servers**: DNS server address(es).

Step 4 Click **Reserve**.

If you reserve both IPv4 and IPv6 address pools, which means the fabric is provisioned with a dual-stack IP pool, you cannot switch back to a single-stack IP pool if the IPv6 pool is already attached to a VN.

However, if the IPv6 pool is not attached to a VN, you can downgrade it from a dual-stack IPv6 to a single-stack IPv4 pool. To downgrade to a single stack, in the IP Address Pools window, click **Edit** for the dual-stack IP pool. In the **Edit IP Pool** window, uncheck the **IPv6** check box and click **Save**.

Edit IP Pools

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 Choose the Global site or expand the hierarchy tree and choose the desired site.

Step 3 To edit all the IP pools in bulk, do the following:

a) From the **Actions** drop-down list, choose **Edit All**.

b) Click **Yes** in the **Warning** message.

c) In the **Edit IP Pool** window make the desired changes and click **Save**.

Step 4 To edit only the desired IP pools, do the following:

a) Choose the desired IP pools and from the **Actions** drop-down list, click **Edit Selected**.

You can also click **Edit** corresponding to the chosen IP pools.

b) In the **Edit IP Pool** window make the desired changes and click **Save**.

Delete IP Pools

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 Choose the Global site or expand the hierarchy tree and choose the desired site.

Step 3 To delete all the IP pools in bulk, do the following:

a) From the **Actions** drop-down list, choose **Delete All**.

b) Click **Yes** in the **Warning** message.

Step 4 To delete only the desired IP pools, do the following:

a) Choose the desired IP pools and from the **Actions** drop-down list, click **Delete Selected**.

You can also click **Delete** corresponding to the chosen IP pools.

b) Click **Yes** in the **Warning** message.

Clone an IP Pool

You can clone an existing IP pool at the site level. When you clone an IP pool, the DHCP server and DNS server IP addresses are automatically filled.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 Expand the hierarchy tree, and then choose a site.

Step 3 Locate the desired IP pool and, in the **Actions** area, click **Clone**.

Step 4 In the **Clone IP Pool** window, do the following:

a) Optionally, edit the pool name. (You cannot edit the Type, IP Address Space, or Global Pool values, which are inherited from the pool from which you are cloning.)

b) Edit the CIRD prefix values as necessary.

c) Click **Clone**.

Release IP Pools

You can release single-stack and dual-stack pools that are reserved at the site level.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 Choose the Global site or expand the hierarchy tree and choose the desired site.

Step 3 To release all the IP pools in bulk, do the following:

a) From the **Actions** drop-down list, choose **Release All**.

b) Click **Yes** in the **Warning** message.

c) At the prompt, click **Release**.

Step 4 To release only the desired IP pools, do the following:

a) Choose the desired IP pools and from the **Actions** drop-down list, click **Release Selected**.

b) At the prompt, click **Release**.

View IP Address Pools

This procedure shows how to view 10 or more IP address pools in table view and tree view.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **IP Address Pools**.

Step 2 Select a site from the hierarchy in the left pane.

Step 3 Use the Toggle button to switch between the Table view and Tree view.

- When the view contains 10 or more IP pools, by default the GUI displays the pools in table view.
- When the view contains fewer than 10 IP pools, by default the GUI displays the pools in tree view.

Note Toggling between the table and tree map view is based on the pool count not on the user selection on the UI.

Tree view applies to the Global pool as well as to the site pool.

Step 4 The **IP Address Pools** table view displays list of IP address pools based on **Name**, **Type**, **IPv4 Subnet**, **IPv4 Used**, **IPv6 Subnet**, **IPv6 Used**, and **Actions**.

Note
- Hover your cursor over the **i** icon next to the **IPv4 Used** and **IPv6 Used**. A tooltip appears that displays more information about **IPv4 Used**, **IPv6 Used**, **Free**, **Unassignable**, **Assigned**, and **Default Assigned** IP address pool.
- In the **IPv4** and **IPv6** columns, hover your cursor over the **i** icon next to the corresponding used percentage of **IPv4** and **IPv6** for a given IP address pool. A tooltip displays the percentage of **Free**, **Unassignable**, **Assigned**, and **Default Assigned** IP addresses.

Step 5 In the Table view, click the **IPv4 only** or **Dual-Stack** option in the **Subnet Type** area if you prefer to view only the **IPv4** or **Dual-Stack** address pools.

Step 6 In the Tree view, hover your cursor over the IP address pool that you are interested in, and click to view the slide-in pane which contains the following information:

- Subnet type of an IP address pool.
- Percentage of available IP addresses along with **Pool CIDR**, **Gateway**, **DHCP Server(s)**, and **DNS Server(s)** under the respective pool.
- Percentage of used IP addresses under the respective pool.

Step 7 In the **Used** area, click **Assigned** to view the list of assigned IP addresses to a device filtered based on **Device Name**, **IP Address**, and **Site**.

Step 8 Click **Unassignable** to view the list of unassigned IP addresses which cannot be assigned to a device filtered based on **Device Name**, **IP Address**, and **Site**.

Step 9 Click **Edit** to edit an IP address pool.

Step 10 Click **Release** to release an IP address pool.

Note
- In the side bar for a global pool, you can view the usage of a given pool across all the child pool.
- Global and site IP address pool can have blocklisted IP addresses.
- Subpools cannot have blocklisted IP addresses.
  - Cisco DNA Center rejects the IP address pool creation request of a CIDR address pool if it contains blocklisted IP addresses.
  - In the next free IP address pools request, Cisco DNA Center skips the blocklisted IP addresses to find the next IP address free pool.

Step 11 (Optional) In the side bar click **Export** to export the table data.

Configure Service Provider Profiles

You can create a service provider (SP) profile that defines the class of service for a particular WAN provider. You can define 4-class, 5-class, 6-class, and 8-class service models. After you create an SP profile, you can assign it to an application policy and to the WAN interfaces in the application policy scope, including setting the subline rate on the interface, if needed.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **SP Profiles**.

Step 2 In the **QoS** area, click **Add**.

Step 3 In the **Profile Name** field, enter a name for the SP profile.

Step 4 From the **WAN Provider** drop-down list, enter a new service provider, or choose an existing one.

Step 5 From the **Model** drop-down list, choose a class model: **4 class**, **5 class**, **6 class**, and **8 class**.

For a description of these classes, see Service Provider Profiles, on page 296.

Configure Global Network Servers

You can define global network servers that become the default for your entire network.

Note You can override global network settings on a site by defining site-specific settings.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **Network**.

Step 2 In the **DHCP Server** field, enter the IP address of a DHCP server.

Note You can click the plus icon and enter both IPv4 and IPv6 addresses.

You must define at least one DHCP server in order to create IP address pools.

Step 3 In the **DNS Server** field, enter the domain name of a DNS server.

Note You can click the plus icon and enter both IPv4 and IPv6 addresses.

You must define at least one DNS server in order to create IP address pools.

Step 4 Click **Save**.

Add Cisco ISE or Other AAA Servers

You can define Cisco Identity Services Engine (ISE) servers or other, similar AAA servers for network, client, and endpoint authentication at the site or global level. For network authentication, RADIUS and TACACS protocols are supported. For client and endpoint authentication, only RADIUS is supported. Only one Cisco ISE is supported per Cisco DNA Center.

You can configure the source interface under the RADIUS or TACACS server group to support multi-ISE configuration, wherein each Cisco ISE cluster has its own server group. The source interface used for RADIUS and TACACS servers is determined in the following way:

- If the device has a Loopback0 interface configured, Loopback0 is configured as the source interface.
- Otherwise, the interface that Cisco DNA Center uses as the management IP is configured as the source interface.

After you configure a Cisco ISE server for a site, the devices that are assigned to the site are automatically updated on the corresponding Cisco ISE server with a /32 mask. Subsequently, any changes to those devices in Cisco ISE are sent automatically to Cisco DNA Center.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **Network**.

Step 2 Click **Add Servers** to add a AAA server.

Step 3 In the **Add Servers** window, check the **AAA** check box, and click **OK**.

Step 4 Set the AAA server for network users, client/endpoint users, or both.

Step 5 Check the **Network** and/or **Client/Endpoint** check boxes and configure servers and protocols for the AAA server.

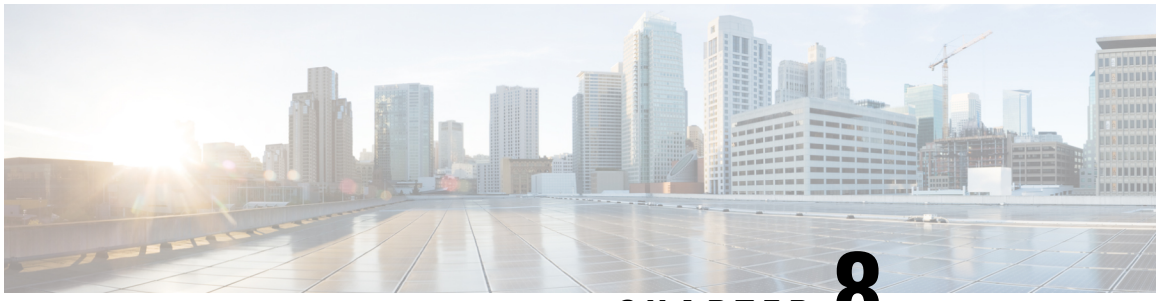
Step 6 Choose the **Servers** for authentication and authorization: **ISE** or **AAA**.

- If you choose **ISE**, configure the following:
  - From the **Network** drop-down list, choose the IP address of the Cisco ISE server. The **Network** drop-down list contains all the IP addresses of the Cisco ISE servers that are registered in **System Settings** on the Cisco DNA Center home page. Selecting a Cisco ISE IP populates the primary and additional IP address drop-down lists with Policy Service Nodes (PSN) IP addresses for the selected Cisco ISE. You can either enter an IP address for the AAA server or choose the PSN IP address from the **IP Address (Primary)** and **IP Address (Additional)** drop-down lists.
  - Choose the **Protocol**: **RADIUS** or **TACACS**.

    Note AAA settings for a physical and managed site for a particular WLC must match, or provisioning fails.

- If you choose **AAA**, configure the following:
  - Enter an IP address for the AAA server or choose the IP addresses from the **IP Address (Primary)** and **IP Address (Additional)** drop-down lists. These drop-down lists contain the non-Cisco ISE AAA servers registered in the **System Settings**.

Step 7 Click **Save**.



CHAPTER 8

Run Diagnostic Commands on Devices

About Command Runner

The Command Runner tool allows you to send diagnostic CLI commands to selected devices. Currently, **show** and other read-only commands are permitted.

Run Diagnostic Commands on Devices

Command Runner lets you run diagnostic CLI commands on selected devices and view the resulting command output. Command Runner supports only a subset of the shortcuts that are available as part of a standalone terminal.

Before you begin

Begin using Command Runner, do the following:

1. In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Software Updates** > **Installed Apps**.
2. Find the **Command Runner** application and click **Install**.
3. After installation, run a Discovery job to populate Cisco DNA Center with devices. You are presented with a list of devices from which to run diagnostic CLI commands.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Command Runner**.

The **Command Runner** window appears.

Step 2 In the **Search** field, click the drop-down arrow to search by **Device IP** or **Device Name**.

Step 3 Choose a device or devices on which to run diagnostic CLI commands.

A **Device List** with your selection appears.

Step 4 (Optional) Select another device to add to the list. You can select up to 20 reachable devices.

Note Although the device list displays everything available in inventory, Command Runner is not supported for wireless access points and Cisco Meraki devices. If you choose an access point device or Cisco Meraki device, a warning message appears, stating that no commands will be executed on them.

Step 5 In the **Select/Enter commands** field, enter a CLI command and click **Add**.

Command Runner supports type ahead. As you begin typing, Command Runner displays the commands available for you to choose. You can also type a new, valid command.

Step 6 Click **Run Command(s)**.

If successful, a `Command(s) executed successfully` message appears.

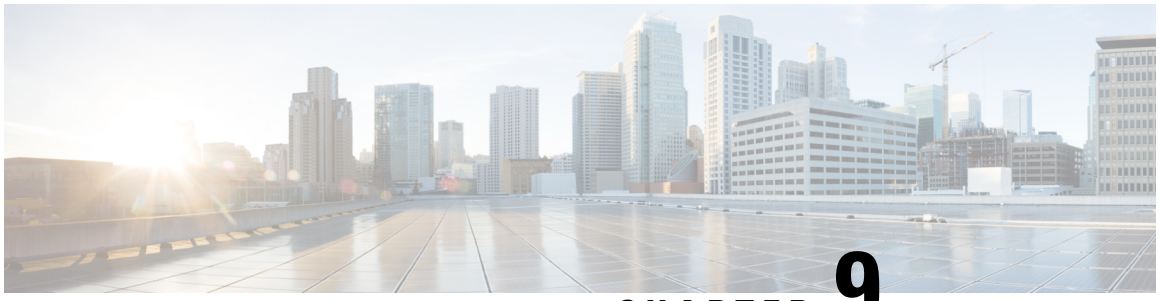
Step 7 Click the command displayed underneath the device to view the command output.

Note The complete command output is displayed in the **Command Runner** window. Any sensitive information, such as passwords, is masked in the command output.

Step 8 (Optional) Click **Export all CLI Output** to export the command output to a text file that you can save locally.

Step 9 Click **Go Back** to return to the previous window.

Note If necessary, click the **x** next to a device name to remove the device from the device list. Similarly, click the **x** next to a command to remove the command from the list.



CHAPTER 9

Create Templates to Automate Device Configuration Changes

About Template Editor

Cisco DNA Center provides an interactive editor called Template Editor to author CLI templates. You can design templates easily with a predefined configuration by using parameterized elements or variables. After creating a template, you can reuse the template to deploy your devices in one or more sites that are configured anywhere in your network.

With Template Editor, you can:

- Create, edit, and delete a template
- Add interactive commands
- Validate errors in template
- Version control the templates for tracking purposes
- Simulate templates

Note Be careful that your template does not overwrite a network-intent configuration pushed by Cisco DNA Center.

Create Projects

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Tools** > **Template Editor**.

Step 2 In the left pane, click > **Create Project**.

The **Add New Project** slide-in pane appears.

Step 3 In the **Name** field, enter a name for the project.

Step 4 (Optional) In the **Description** field, enter a description for the project.

Step 5 Click **Add**.

The project is created and appears in the left pane.

Create Templates

Cisco DNA Center provides regular and composite configuration templates. CLI templates allow you choose the elements in the configuration. Cisco DNA Center provides variables that you can replace with the actual values and logic statements.

Create a Regular Template

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Tools** > **Template Editor**.

Note By default, the **Onboarding Configuration** project is available for creating day-0 templates. You can create your own custom projects. Templates created in custom projects are categorized as day-N templates.

Step 2 In the left pane, select the project under which you are creating templates.

Step 3 Click the gear icon and choose **Add Template** in the left pane.

Note The template that you create for day-0 can also be applied for day-N.

Step 4 Configure the settings for the regular template:

a) For **Template Type**, leave the option set to **Regular Template**.

b) For **Template Language**, choose either the **Velocity** or **Jinja** language to be used for the template content.

c) In the **Name** field, enter a unique name for the template.

d) (Optional) In the **Description** field, enter a description for the template.

e) In the **Tags** field, click the drop-down list and choose tags for your template.

Note Tags are like keywords that help you locate your template more easily.

If you use tags to filter the templates, you must apply the same tags to the device to which you want to apply the templates. Otherwise, you get the following error during provisioning: `Cannot select the device. Not compatible with template.`

f) For **Device Type (s)**, click **Edit** to choose the device types that you want this template to apply to.

The **Select Device Type(s)** slide-in pane appears. By default, all device types are displayed.

- Use the **Find** feature to quickly search for the device by entering the device name or expand the device type and check the check boxes next to the device types that you want to apply to the template.

  To view the devices that are selected, choose **Selected** from the **Show** drop-down list.

There are different granularity levels for selecting the device type from the hierarchical structure. The device type is used during deployment to ensure that templates deploy devices that match the specified device type criteria. This lets you create specialized templates for specific device models.

Template Editor does not show device product IDs (PIDs); instead, it shows the device series and model description. You can use cisco.com to look up the device data sheet based on the PID, find the device series and model description, and choose the device type appropriately.

g) After selecting device types, click **Back to Add New Template**.

h) For **Software Type**, click the drop-down list and choose the software type.

Note For more information on the Cisco Wireless Controller supported software versions and the minimum supported version, see Cisco DNA Center Supported Devices.

For example, if you select IOS as the software type, the commands apply to all software types, including IOS-XE and IOS-XR. This value is used during provisioning to check whether the selected device conforms to the selection in the template.

i) In the **Software Version** field, enter the software version.

Note During provisioning, Cisco DNA Center checks to see if the selected device has the software version listed in the template. If there is a mismatch, the provision skips the template.

Step 5 Click **Add**.

The template is created and appears under the project you selected in the left pane.

Step 6 You can edit the template content by selecting the template that you created in the left pane. For more information about editing the template content, see Edit Templates, on page 197.

Blocked List Commands

Blocked list commands are commands that cannot be added to a template or provisioned through a template. If you use blocked list commands in your templates, it shows a warning in the template that it may potentially conflict with some of the Cisco DNA Center provisioning applications.

The following commands are blocked in this release:

- **router lisp**
- **hostname**

Sample Templates

Refer to these sample templates while creating variables for your template.

Configure Hostname

```
hostname$name
```

Configure Interface

```
interface $interfaceName
description $description
```

Configure NTP on Cisco Wireless Controllers

```
config time ntp interval $interval
```

Create a Composite Template

Two or more regular templates are grouped into a composite sequence template. You can create a composite sequential template for a set of templates, which are applied collectively to devices. For example, when you deploy a branch, you must specify the minimum configurations for the branch router. The templates that you create can be added to a single composite template, which aggregates all the individual templates that you need for the branch router. You must specify the order in which templates that are in the composite template are deployed to devices.

Note You can add only a committed template to a composite template.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Tools** > **Template Editor**.

Step 2 In the left pane, select the project under which you are creating templates.

Step 3 Click the gear icon > **Add Templates** in the left pane.

The **Add New Template** slide-in pane appears.

Step 4 Configure the settings for the composite template:

a) For **Template Type**, choose **Composite Sequence** for a composite template.

b) For **Template Language**, choose either the **Velocity** or **Jinja** language to be used for the template content.

c) In the **Name** field, enter a unique name for the template.

d) (Optional) In the **Description** field, enter a description for the template.

e) In the **Tags** field, click the drop-down list and choose tags for your template.

Note Tags are like keywords that help you locate your template more easily.

f you use tags to filter the templates, you must apply the same tags to the device to which you want to apply the templates. Otherwise, you get the following error during provisioning: `Cannot select the device. Not compatible with template.`

f) For **Device Type (s)**, click **Edit** to choose the device types that you want this template to apply to.

The **Select Device Type(s)** slide-in pane appears. By default, all device types are displayed.

- Use the **Find** feature to quickly search for the device by entering the device name or expand the device type and check the check boxes next to the device types that you want to apply to the template.

  To view the devices that are selected, choose **Selected** from the **Show** drop-down list.

g) After selecting device types, click **Back to Add New Template**.

h) For **Software Type**, click the drop-down list and choose the software type.

Note You can select the specific software type (such as IOS-XE or IOS-XR) if there are commands specific to these software types. If you select IOS as the software type, the commands apply to all software types, including IOS-XE and IOS-XR. This value is used during provisioning to check whether the selected device confirms to the selection in the template.

i) In the **Software Version** field, enter the software version.

Note During provisioning, Cisco DNA Center checks to see if the selected device has the similar software version listed in the template. If there is a mismatch, the provision skips the template.

Step 5 Click **Add**.

The composite template is created and appears under the project you selected in the left pane.

Step 6 Click the composite template that you created in the left view pane.

Step 7 In the **Template Editor** window, drag and drop templates from the left pane to order or sequence the templates.

The templates are deployed based on the order in which they are sequenced. You can change the order of templates in the **Template Editor** window.

Note By default, the **Applicable** option is chosen in the **View** filter. Only the applicable templates that can be added to the composite template are shown in the **Template Editor** window. You can choose the **All** option in the **View** filter to view all the templates in the **Template Editor** window. In the **All** option view, the templates that match the chosen device types and software version are marked by a plus icon.

You can drag and drop templates that have the same device type, software type, and software version as that of the composite template.

Step 8 To cancel the deployment process upon failure of the first template, select the first template in the **Template Editor** window and check the **Abort sequence on targets if deployment fails** check box.

Step 9 From the **Actions** drop-down list, choose **Commit** to commit the template content.

Edit Templates

After creating a template, you can edit the template to include content.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Template Editor**.

Step 2 In the left pane, choose the template that you want to edit.

The **Template Editor** window appears.

Step 3 In the **Template Editor** window, enter the template content. You can have a template with a single-line configuration or a multi-select configuration.

Step 4 From **Template Language**, choose the language with which to write the content:

- **Velocity**: Use the Velocity Template Language (VTL). For information, see http://velocity.apache.org/engine/devel/vtl-reference.html.

  The Velocity template framework restricts the use of variables that start with a number. Make sure that the variable name starts with a letter and not with a number.

- **Jinja**: Use the Jinja language. For information, see https://www.palletsprojects.com/p/jinja/.

Step 5 From the **Actions** drop-down list, choose **Check for errors** to validate the template.

Cisco DNA Center checks for these errors and reports them:

- Language syntax errors.
- Conflicts with blocked list commands. For more information, see Blocked List Commands, on page 195.

Step 6 From the **Actions** drop-down list, choose **Save**.

After saving the template, Cisco DNA Center checks for any errors in the template. If there are any syntax errors, the template content is not saved and all input variables that are defined in the template are automatically identified during the save process. The local variables (variables that are used in **for** loops, assigned though a set, and so on) are ignored.

Step 7 From the **Actions** drop-down list, choose **Commit**.

Note You can associate only a committed template to a network profile.

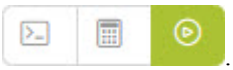
Template Simulation

The interactive template simulation lets you simulate the CLI generation of templates by specifying test data for variables before sending them to devices. You can save the test simulation results and use them later, if required.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Template Editor**.

Step 2 From the left pane, expand a project and click a template to run a simulation for.

The template appears.

Step 3 In the top-right corner, click the **Simulator Editor** toggle  .

Step 4 Click the **Actions** drop-down list and choose **Create Simulation**.

The **Simulation Input** form appears.

Step 5 In the **Simulation Name** field, enter a name for the simulation.

Note If there are implicit variables in your template then click **edit** link to select a device or site in the **Simulation Input** form to run the simulation against real devices based on your bindings.

Step 6 In the **Simulation Input** form, complete the required fields, and click **Run**.

The results are displayed in the **Template Preview** window.

Export Template(s)

You can export a template or multiple templates to a single file, in JSON format.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Template Editor**.

Step 2 In the left pane, select the template that you want to export. Choose ⚙ > **Export**.

- To export multiple templates under a project, select a project in the left pane and choose ⚙ > **Export Template(s)**.

  Select the templates from the **Export Template(s)** window and, click **Export**.

- To export multiple templates under different projects, click ⊕ > **Export Project(s)**, in the left pane.

  Select the templates to be exported, from the **Export Project(s)** window, and click **Export**.

Step 3 Click **Save**, if prompted.

The latest version of the template is exported.

To export an earlier version of the template, open the template from **Actions** > **Show History** > **View**.

Click **Actions** > **Export**.

Import Template(s)

You can import a template or multiple templates under a project.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Template Editor**.

Step 2 In the left pane, select a project to which you want to import the template(s). Choose ⚙ > **Import Template(s)**.

Step 3 Click **Select a File from your computer** on the **Import Template(s)** window and browse to the location of your JSON template file.

Step 4 Select the JSON file and click **Open**.

The template is imported under the selected project. If a template with the same name exists, Cisco DNA Center displays an error message and does not import the template.

Note To import a template with the same name as an existing one, check the **Create new version of imported template/project when template/project with the same name already exists in the hierarchy** check box on the **Import Template(s)** window.

Selecting this option creates a new version of the existing template.

Clone a Template

You can make a copy of a template to reuse portions of it.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Tools** > **Template Editor**.

Step 2 In the left pane, select the template that you want to export. Choose > **Clone**.

Step 3 Enter the name of the cloned template in the **Name** field of the **Clone Template** window.

Step 4 Choose a project from the **Project Name** drop-down list.

Step 5 Click **Clone**.

Step 6 To commit the cloned template, select the template from the left pane of the window and click **Actions** > **Commit**.

The latest version of the template is cloned.

To clone an earlier version of the template, open the template from **Actions** > **Show History** > **View**.

Click **Actions** > **Clone**.

Export Project(s)

You can export a project or multiple projects, including their templates, to a single file in JSON format.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Tools** > **Template Editor**.

Step 2 In the left pane, select the project that you want to export. Choose > **Export Project**.

To export projects in bulk, click > **Export Project(s)** in the left pane.

Select the projects to be exported and click **Export**.

Step 3 Click **Save**, if prompted.

Import Project(s)

You can import a project or multiple projects with their templates, into the Cisco DNA Center Template Editor.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Tools** > **Template Editor**.

Step 2 In the left pane, click > **Import Project(s)**.

Step 3 Click **Select a File from your computer** on the **Import Project(s)** window and browse to the location of your JSON project file.

Step 4 Select the JSON file and click **Open**.

The project and its templates are imported. If a project with the same name exists, Cisco DNA Center displays an error message and does not import the project.

Note To import a project with the same name as an existing one, check the **Create new version of imported template/project when template/project with the same name already exists in the hierarchy** check box on the **Import Project(s)** window.

Selecting this option creates a new version of the existing project.

Template Form Editor

The Template form editor is used for adding additional metadata information to the template variables in the template. You can also use the form editor to provide validations for variables such as maximum length, range, and so on.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Template Editor**.

Step 2 From the left pane, expand a project and click a template.

The template appears.

Step 3 Click the **Form Editor** toggle  .

The Form Editor enables you to add meta data to the template variables. All the variables that are identified in the template are displayed. You can configure the following metadata:

- Choose the variable and check the **Not a Variable** check box if you do not want the string to be considered as a variable.
- Enter the field name in the **Field Name** text box. This is the label that is used for the UI widget of each variable during provisioning.
- Enter the tooltip text that is displayed for each variable in the **Tooltip** text box.
- Enter the default value in the **Default Value** text box. This value appears during provisioning as the default value.
- Enter any instructional text in the **Instructional Text** text box. Instructional text appears within the UI widget (for example, **Enter the hostname here**). The text within the widget is cleared when you click the widget to enter any text.
- Choose the data type from the **Data Type** drop-down list: **String**, **Integer**, **IP Address**, or **Mac Address**.
- Check the **Required** check box if this is a required variable during the provisioning. All the variables by default are marked as Required, which means you must enter the value for this variable at the time of provisioning. If the parameter is not marked as **Required** and if you do not pass any value to the parameter, it substitutes an empty string at run time. A lack of a variable can lead to command failure, which may not be syntactically correct. If you want to make an entire command optional based on a variable not marked as **Required**, use the **if-else** block in the template.
- Choose the type of UI widget you want to create at the time of provisioning from the **Display Type** drop-down list: **Text Field**, **Single Select**, or **Multi Select**.

- Enter the number of characters that are allowed in the **Maximum Characters** text box. This is applicable only for the string data type.

Step 4 After configuring metadata information, from the **Actions** drop-down list, choose **Save**.

Step 5 After saving the template, you must version it. You must version the template every time you make changes to it. From the **Actions** drop-down list, choose **Commit**. The **Commit** window appears. You can enter a commit note in the **Commit Note** text box. The version numbers are automatically generated by the system.

Step 6 To view the history, from the **Actions** drop-down list, select **Show History** to view previously created and versioned templates.

A pop-up window appears.

- Click **View** in the pop-up window to see the content of the old version.
- Click **Edit** in the pop-up window to edit the template.

Variable Binding

While creating a template, you can specify variables that are contextually substituted. Many of these variables are available in the Template Editor drop-down list.

Template Editor provides an option to bind or use variables in the template with the source object values while editing or through the input form enhancements; for example, DHCP server, DNS server, and syslog server.

Some variables are always bound to their corresponding source and their behavior cannot be changed. You can view the list of implicit variables by clicking the ⓘ icon next to the name of the template in the **Code Editor** or the **Form Editor** window.

The predefined object values can be one of the following:

- Inventory
  - Device object
  - Interface object
- **Common Settings**: Settings available under **Design** > **Network Settings** > **Network**. The common settings variable binding resolves values that are based on the site to which the device belongs.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Template Editor**.

Step 2 Choose the template and click the **Input Form** icon to bind variables in the template to network settings.

Step 3 Select the variables in the **Input Form** pane and check the **Required** check box to bind variables to the network settings.

Step 4 From the **Display** drop-down list, choose the type of UI widget to create at the time of provisioning: **Text Field**, **Single Select**, or **Multi Select**.

Step 5 To bind variables to network settings, select each variable in **Input Form**, and check the **Bind to Source** check box under **Content**.

- Choose the **Source**, **Entity**, and **Attributes** from the respective drop-down lists.

- For the source type **CommonSettings**, choose one of these entities: **dhcp.server**, **syslog.server**, **snmp.trap.receiver**, **ntp.server**, **timezone.site**, **device.banner**, **dns.server**, **netflow.collector**.

  You can apply a filter on the **dns.server** or **netflow.collector** attributes to display only the relevant list of **bind** variables during provisioning of devices. To apply a filter on an attribute, select an attribute from the **Filter by** drop-down list. From the **Condition** drop-down list, select a condition to match the **Value**.

- For the source type **NetworkProfile**, choose **SSID** as the entity type. The SSID entity that is populated is defined under **Design** > **Network Profile**. The binding generates a user-friendly SSID name, which is a combination of SSID name, site, and SSID category. From the **Attributes** drop-down list, choose **wlanid**. This attribute is used during the advanced CLI configurations at the time of template provisioning.

- For the source type **Inventory**, choose one of these entities: **Device**, **Interface**, **AP Group**, **Flex Group**, **Wlan**, **Policy Profile**, **Flex Profile**. For the entity type **Device** and **Interface**, the **Attribute** drop-down list shows the device or interface attributes. The variable resolves to the AP Group and Flex Group name that is configured on the device to which the template is applied.

  You can apply filter on the **Device**, **Interface**, or **Wlan** attributes to display only the relevant list of **bind** variables during provisioning of devices. To apply a filter on an attribute, select an attribute from the **Filter by** drop-down list. From the **Condition** drop-down list, select a condition to match the **Value**.

After binding variables to a common setting, when you assign templates to a wireless profile and provision the template, the network settings that you defined under **Network Settings** > **Network** appear in the drop-down list. You must define these attributes under **Network Settings** > **Network** at the time of designing your network.

Special Keywords

All commands executed through templates are always in the **config t** mode. Therefore, you do not have to specify the **enable or config t** commands explicitly in the template.

Day-0 templates do not support special keywords.

Enable Mode Commands

Specify the **#MODE_ENABLE** command if you want to execute any commands outside of the **config t** command.

Use this syntax to add **enable mode** commands to your CLI templates:

```
#MODE_ENABLE
<<commands>>
#MODE_END_ENABLE
```

Interactive Commands

Specify **#INTERACTIVE** if you want to execute a command where a user input is required.

An interactive command contains the input that you must enter following the execution of a command. To enter an interactive command in the CLI Content area, use the following syntax:

```
CLI Command<IQ>interactive question 1 <R> command response 1 <IQ>interactive question
2<R>command response 2
```

Where **<IQ>** and **<R>** tags evaluate the text provided against what is seen on the device.

The Interactive question uses regular expressions to validate if the text received from the device is similar to the text entered. If the regular expressions entered in the **<IQ><R>** tags are found, then the interactive question passes and a part of the output text appears. This means that you need to enter a part of the question and not the entire question. Entering Yes or No between the **<IQ>** and **<R>** tags is sufficient but you must make sure that the text Yes or No appears in the question output from the device. The best way to do this is by running the command on the device and observing the output. In addition, you need to ensure that any regular expression metacharacters or newlines entered are used appropriately or avoided completely. The common regular expression metacharacters are **. ( ) [ ] { } | * + ? \ $ ^ : &**.

For example, the following command has output that includes metacharacters and newlines.

```
Switch(config)# no crypto pki trustpoint DNAC-CA
% Removing an enrolled trustpoint will destroy all certificates received from the related
Certificate Authority
Are you sure you want to do this? [yes/no]:
```

To enter this in a template, you need to select a portion that does not have any metacharacters or newlines. Here are a few examples of what could be used.

```
#INTERACTIVE
no crypto pki trustpoint DNAC-CA<IQ>yes/no<R>yes
#ENDS_INTERACTIVE


#INTERACTIVE
no crypto pki trustpoint DNAC-CA<IQ>Removing an enrolled<R>yes
#ENDS_INTERACTIVE


#INTERACTIVE
no crypto pki trustpoint DNAC-CA<IQ>Are you sure you want to do this<R>yes
#ENDS_INTERACTIVE


#INTERACTIVE
crypto key generate rsa general-keys <IQ>yes/no<R> no
#ENDS_INTERACTIVE
```

Where **<IQ>** and **<R>** tags are case-sensitive and must be entered in uppercase.

Note In response to the interactive question after providing a response, if the newline character is not required, you must enter the **<SF>** tag. Include one space before the **<SF>** tag. When you enter the **<SF>** tag, the **</SF>** tag pops up automatically. You can delete the **</SF>** tag because it is not needed.

For example:

```
#INTERACTIVE
config advanced timers ap-fast-heartbeat local enable 20 <SF><IQ>Apply(y/n)?<R>y
#ENDS_INTERACTIVE
```

Combining Interactive Enable Mode Commands

Use this syntax to combine interactive **Enable Mode** commands:

```
#MODE_ENABLE
#INTERACTIVE
commands<IQ>interactive question<R> response
```

```
#ENDS_INTERACTIVE
#ENDS_END_ENABLE

#MODE_ENABLE
#INTERACTIVE
mkdir <IQ>Create directory<R>xyz
#ENDS_INTERACTIVE
#MODE_END_ENABLE
```

Multiline Commands

If you want multiple lines in the CLI template to wrap, use the **MLTCMD** tags. Otherwise, the command is sent line by line to the device. To enter multiline commands in the CLI Content area, use the following syntax:

```
<MLTCMD>first line of multiline command
second line of multiline command
...
...
last line of multiline command</MLTCMD>
```

- Where **<MLTCMD>** and **</MLTCMD>** are case-sensitive and must be in uppercase.
- The multiline commands must be inserted between the **<MLTCMD>** and **</MLTCMD>** tags.
- The tags cannot start with a space.
- The **<MLTCMD>** and **</MLTCMD>** tags cannot be used in a single line.

Associate Templates to Network Profiles

Before you begin

Before provisioning the template, ensure that the templates are associated with a network profile and the profile is assigned to a site.

During provisioning, when the devices are assigned to the specific sites, the templates associated with the site through the network profile appear in the advanced configuration.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Profiles**, and click **Add Profile**.

The following types of profiles are available:

- **Routing & NFV**: Select this to create a routing and NFV profile.
- **Switching**: Select this to create a switching profile.
  - Click the **Onboarding Templates** or **Day-N Templates** as required.
  - Enter the **Profile Name**.
  - Click **+Add** and select the device type, tag, and template from the **Device Type**, **Tag Name**, and **Template** drop-down lists.

    If you do not see the template that you need, create a new template in Template Editor as described in Create a Regular Template, on page 194.
  - Click **Save**.

- **Wireless**: Select this to create a wireless profile. Before assigning a wireless network profile to a template, ensure that you have created wireless SSIDs.
  - Enter the **Profile Name**.
  - Click **+ Add SSID**. Those SSIDs that were created under **Network Settings** > **Wireless** are populated.
  - Under **Attach Template(s)**, select the template that you want to provision from the **Template** drop-down list.
  - Click **Save**.

Step 2 The **Network Profiles** page lists the following:

- **Profile Name**
- **Type**
- **Version**
- **Created By**
- **Sites**: Click **Assign Site** to add sites to the selected profile.

Step 3 For Day-N provisioning, choose **Provision** > **Devices**. The **Device Inventory** window appears.

- Check one or more check boxes next to the device name that you want to provision.
- From the **Action** drop-down list, choose **Provision**.
- In the **Assign Site** window, assign a site to which the profiles are attached. In the **Choose a Site** field, enter the name of the site to which you want to associate the controller or select from the **Choose a Site** drop-down list.
- Click **Next**.

  The **Configuration** window appears. In the **Managed AP Locations** field, enter the AP locations managed by the controller. Here you can change, remove, or reassign the site. This is applicable only for wireless profiles.

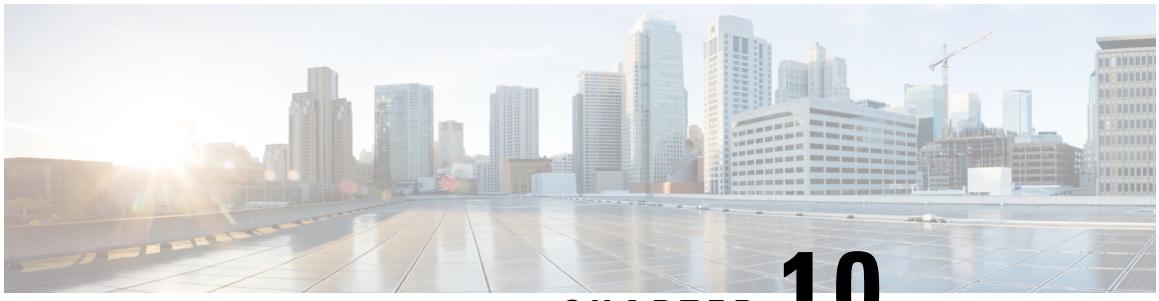
- Click **Next**.
- The **Advanced Configuration** window appears. The templates associated with the site through the network profile appear in the advanced configuration.
  - Use the **Find** feature to quickly search for the device by entering the device name, or expand the templates folder and select the template in the left pane. In the right pane, select values for those attributes that are bound to the source.
  - To export the template variables into a CSV file while deploying the template, click **Export** in the right pane. You can use the CSV file to make necessary changes in the variable configuration and import it into Cisco DNA Center at a later time by clicking **Import** in the right pane.
- Click **Next** to deploy the template. You are prompted to deploy the template now or to schedule it to a later time.
- To deploy the template now, click the **Now** radio button and click **Apply**. To schedule the template deployment for a later date and time, click the **Later** radio button and define the date and time of the deployment.

  The **Status** column in the **Device Inventory** window shows SUCCESS after a successful deployment.

Step 4 For Day-0 provisioning, choose **Provision** > **Devices** > **Plug and Play**. The **Plug and Play** window appears.

- Choose a device and click **Claim** from the **Actions** drop-down list.
- Click **Next**, and in the **Site Assignment** window, choose a site from the **Site** drop-down list.
- Click **Next**, and in the **Configuration** window, choose the image and the Day-0 template.
- Click **Next**, and in the **Advanced Configuration** window, enter the location.

- Click **Next** to view the **Device Details**, **Image Details**, **Day-0 Configuration Preview**, and **Template CLI Preview**.



CHAPTER 10

Design Model Configuration

Introduction to Model Config Editor

Model Config allows you to define advanced customizations of the Cisco Validated Designs (CVD) that are encapsulated within the provisioning applications. Model Configs are a set of model-based, discoverable, and customizable configuration capabilities, which you can deploy on your network devices with high-level service intent and device-specific CLI templates.

The Model Configs feature simplifies network provision by extracting complex device configurations and facilitating customizable network configurations using an intuitive GUI instead of device-specific CLIs. A common design is deployed to various device hardware platforms and software types in a uniform way. During deployments, the Cisco DNA Center infrastructure automatically validates and translates extracted designs to device-specific CLI commands.

To provision model config design, do the following:

1. Create a new model config design using the **Model Config Editor** window (**Menu** icon (☰) **Tools** > **Model Config Editor**).
2. Apply the model config design to different network profiles.
3. Using the provision workflow, apply the model config design that is specified in network profiles to a network device.

Supported Model Config Design Types

Cisco DNA Center supports the following wireless Model Config design types:

- CleanAir configuration

- Multicast configuration
- Advanced SSID configuration
- Global IPv6 configuration

Create a Design for Cisco CleanAir

CleanAir is a spectrum intelligence solution designed to proactively manage the challenges of a shared wireless spectrum. It allows you to see all the users of the shared spectrum (both native devices and foreign interferers). It also enables you or your network to act on this information. For example, you can manually remove the interfering device, or the system can automatically steer the channel away from the interference. CleanAir provides spectrum management and Radio Frequency (RF) visibility.

Before you begin

You should have discovered the devices in your network using the **Discovery** functionality so that the discovered devices are listed in the **Inventory** window.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Model Config Editor**.

Step 2 In the left pane, you can either search for a model config capability by entering its name in the **Search Capability** field, or by expanding the **Wireless** Model Configs and choosing **CleanAir Configuration**.

Step 3 In the **Design Instances** pane, check the **Default CleanAir 802.11a Design** or **Default CleanAir 802.11b Design** check box to use the default CleanAir design.

Note You cannot edit and delete the **Default CleanAir 802.11a Design** or **Default CleanAir 802.11b Design**.

Step 4 In the **Design Instances** window, click **Add**.

The **Add CleanAir Configuration** window is displayed.

Step 5 In the **Design Name** field, enter a name for the design.

Step 6 From the **Radio Band** drop-down list, choose **2.4 GHz** or **5 GHz**.

Step 7 Click the **CleanAir Enable** toggle button to enable the CleanAir functionality on the 2.4-GHz or 5-GHz radio band.

If the **CleanAir Enable** toggle button is enabled, click it to prevent the Cisco Wireless Controller from detecting spectrum interference.

Step 8 Click the **CleanAir Device Reporting Enable** toggle button to enable the CleanAir system to report detected sources of interference, if any.

If the **CleanAir Device Reporting Enable** toggle button is enabled, click it to prevent the Cisco Wireless Controller from reporting interferers.

Step 9 Click the **Persistent Device Propagation** toggle button to enable propagation of information about persistent devices that can be detected by CleanAir.

Persistent device propagation enables you to propagate information about persistent devices to the neighboring APs that are connected to the same Cisco Wireless Controller. Persistent interferers are present at the location, and interfere with WLAN operations even if they are not detectable at all times.

Step 10 Expand **Enable Interferers Features** and check the check box next to the source of interference that needs to be detected and reported by the CleanAir system:

- Ble Beacon
- Bluetooth Paging Inquiry
- Bluetooth SCO ACL
- Generic Dect
- Generic TDD
- Generic Waveform
- Jammer
- Microwave Oven
- Motorola Canopy
- SI FHSs
- Spectrum 802.11 FH
- Spectrum 802.11 Non STD Channel
- Spectrum 802.11 Spec Inverted
- Spectrum 802.11 Super AG SuperAG
- Spectrum 802.15.4
- Video
- Wimax Fixed
- Wimax Mobile
- Xbox

Step 11 In the **CleanAir Description** field, enter a description.

Step 12 Click **Apply**.
The created design instance appears in the **Design Instances** window under the **CleanAir Configuration - Model Configs** area.

Step 13 To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

Step 14 Attach the created config design to a network profile so that it can be deployed on the wireless controller. In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Profiles**.

For more information, see Create Network Profiles for Wireless, on page 170.

Step 15 Provision the model config design specified in the network profile to network devices. In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

For more information, see Provision a Cisco AireOS Controller, on page 375.

Create a Model Config Design for Dot11ax Configuration

The Cisco DNA Center Dot11ax model config feature configures Dot11ax parameters on devices.

Dot11ax configuration involves the 802.11ax wireless specifications standard, also known as High Efficiency (HE) Wireless. Dot11ax is a dual-band 2.4-GHz and 5-GHz technology. You can configure Dot11ax configuration parameters only on Wi-Fi 6-supported Cisco Catalyst 9100 series Access Points.

Note BSS color is used to identify an overlapping basic service set (OBSS). BSS configs are pushed on Wi-Fi 6-supported access points only. The Cisco Catalyst 9100 series Access Points are the next-generation Wi-Fi 802.11ax access point, and ideal for high-density, high-definition applications.

Before you begin

You must discover the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Model Config Editor**.

Step 2 In the left pane, you can either search for a model config by entering its name in the **Search Capability** field, or by expanding **Wireless** and choosing **Dot11ax Configuration**.

Step 3 In the **Design Instances** pane, check the **Default Dot11ax Design** check box to use the default dot11ax design.

Note You cannot edit and delete the **Default dot11ax Design**.

Step 4 In the **Design Instances** window, click **Add Design**.

The **Add Dot11ax Configuration** window appears.

Step 5 In the **Design Name** field, enter a name for the model config design.

Step 6 Click the **BSS Color** toggle button to enable the BSS color functionality on the 2.4-GHz or 5-GHz radio band. The default value is disabled.

Step 7 Click the **Target Wakeup Time** toggle button to enable the target wakeup time. The default value is disabled.

Step 8 From the **Radio Band** drop-down list, choose a 2.4-GHz or 5-GHz radio band.

Note To lock all the properties in the design, click **Lock all**. To lock a specific property, click the lock symbol that is next to each property.

Step 9 Click **Save**.

The created design instance appears in the Design Instances window under the **Dot11ax Configuration – Model Configs** area.

Step 10 To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

Step 11 Attach the created config design to a network profile so that it can be deployed on the access points. In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Profiles**. For more information, see Create Network Profiles for Wireless.

Step 12 Provision the model config design specified in the network profile to network devices. In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**. For more information, see Provision a Cisco AireOS Controller, on page 375.

Create a Model Config Design for Multicast

Use the multicast model config feature to configure multicast parameters on devices.

If your network supports packet multicasting, you can configure the multicast method that the Cisco Wireless Controller uses. The wireless controller performs multicasting in one of these modes:

- Unicast mode: In this mode, the wireless controller unicasts every multicast packet to every access point associated to the wireless controller. This mode is not very efficient, but is required on networks that do not support multicasting.
- Multicast mode: In this mode, the wireless controller sends multicast packets to a CAPWAP multicast group. This method reduces the overhead on the wireless controller processor and shifts the work of packet replication to your network. This method is more efficient than the unicast method.

Before you begin

You should have discovered the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Model Config Editor**.

Step 2 In the left pane, you can either search for a model config by entering its name in the **Search Capability** field, or by expanding **Wireless** and choosing **Multicast Configuration**.

Step 3 In the **Design Instances** pane, check the **Default Multicast Design** check box to use the default multicast design.

Note You cannot edit or delete the **Default Multicast Design**.

Step 4 In the **Design Instances** window, click **Add Design**.

The **Add Multicast Configuration** window appears.

Step 5 In the **Design Name** field, enter a name for the model config design.

Step 6 Click the **Enable Global Multicast Mode** toggle button to configure sending multicast packets. The default value is disabled.

Step 7 From the **AP Multicast Mode** drop-down list, choose **UNICAST** or **MULTICAST**.

- Choose **UNICAST** to configure the wireless controller to use the unicast method to broadcast packets.
- Choose **MULTICAST** to configure the wireless controller to use the multicast method to broadcast packets to a CAPWAP multicast group.

Step 8 Expand **IPV4 Multicast Group Address** and enter the IPv4 multicast address in the **IP Address** field.

Step 9 Expand **IPV6 Multicast Group Address** and enter the IPv6 multicast address in the **IP Address** field.

Step 10 Click **Apply**.

The created design instance appears in the **Design Instances** window under the **Multicast - Model Config** area.

Step 11 To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

Step 12 Attach the created config design to a network profile so that it can be deployed on the wireless controller. In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Profiles**.

For more information, see Create Network Profiles for Wireless, on page 170.

Step 13 Provision the model config design specified in the network profile to network devices. In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

For more information, see Provision a Cisco AireOS Controller, on page 375.

Create a Model Config Design for Advanced SSID

A WLAN associates an SSID to an interface or an interface group. The WLAN is configured with security, quality of service (QoS), radio policies, and other wireless network parameters. You can configure up to 512 WLANs for each wireless controller.

Use the advanced service set identifier (SSID) model config to configure the advanced SSID parameters on devices.

Before you begin

You should have discovered the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Model Config Editor**.

Step 2 In the left pane, you can either search for a model config by entering its name in the **Search** field, or expand **Wireless** and choose **Advanced SSID Configuration**.

Step 3 In the **Design Instances** pane, check the **Default Advanced SSID Design** check box to use the default advanced SSID design.

Note You cannot edit or delete the Default Advanced SSID Design.

Step 4 In the **Design Instances** pane, click **Add Design**.

The **Add Advanced SSID Configuration** window appears.

Step 5 In the **Design Name** field, enter a name for the model config.

Step 6 In the General tab, click the **Peer-to-Peer Blocking** drop-down list and choose an option for peer-to-peer blocking.

Peer-to-peer blocking is applied to individual WLANs. Each client inherits the peer-to-peer blocking setting of the WLAN to which it is associated. Peer-to-peer blocking enables you to have more control over how traffic is directed.

- **DISABLE**: Disables peer-to-peer blocking and forwards traffic locally within the wireless controller whenever possible.
- **DROP**: Causes the wireless controller to discard the client packets.

- **FORWARD UP**: Causes the client packets to be forwarded on an upstream VLAN. The device above the wireless controller decides what action to take regarding the packets. The device can either be a router or a Layer 3 switch.
- **ALLOW PVT GROUP**: Applicable to preshared key (PSK) clients only. Traffic is forwarded based on the associated identity PSK (IPSK) tags for the source and destination client devices.

Step 7 Click the **Passive Client Enable** toggle button to enable the Passive Client feature.

Passive clients are wireless devices, such as scales and printers, that are configured with a static IP address. These clients do not transmit any IP information (such as IP address, subnet mask, and gateway information) when they associate with an access point. As a result, when passive clients are used, the wireless controller never knows the IP address unless they use DHCP.

Step 8 Click the **Assisted Roaming Prediction Optimization** toggle button to configure an assisted roaming prediction list for a WLAN.

Step 9 Click the **Neighbor List Dual Band** toggle button to configure a neighbor list on a dual radio band.

Step 10 Click the **Network Admission Control (NAC-SNMP)** toggle button to enable SNMP NAC support on the WLAN.

Step 11 Click the **Network Admission Control (NAC-Radius)** toggle button to enable RADIUS NAC support on the WLAN.

Step 12 From the **DHCP Required** drop-down list, choose **Yes** or **No** to pass the DHCP request before going into the RUN state (a state where the client can pass traffic through the wireless controller).

Step 13 Expand **DHCP Server** and enter the IP address of the DHCP server in the **IP Address** field.

Step 14 Click the **FlexConnect Local Authentication** toggle button to enable FlexConnect local authentication.

Step 15 In the **NAS ID** field, enter the network access server identifier.

Step 16 Click **Client Data Rates** to configure the following client data rate limits per client by entering values in the respective fields:

- Average Downstream Data Rate Per Client (kbps)
- Burst Downstream Data Rate Per Client (kbps)
- Average Downstream Real-Time Rate Per Client (kbps)
- Burst Downstream Real-Time Rate Per Client (kbps)
- Average Upstream Data Rate Per Client (kbps)
- Burst Upstream Data Rate Per Client (kbps)
- Average Upstream Real-Time Rate Per Client (kbps)
- Burst Upstream Real-Time Rate Per Client (kbps)

Step 17 Click the **SSID Data Rates** to configure the following SSID data rate limits per SSID by entering values in the respective fields:

- Average Upstream Data Rate Per SSID (kbps)
- Burst Upstream Data Rate Per SSID (kbps)
- Average Upstream Real-Time Rate Per SSID (kbps)
- Burst Upstream Real-Time Rate Per SSID (kbps)
- Average Downstream Data Rate Per SSID (kbps)

- Burst Downstream Data Rate Per SSID (kbps)
- Average Downstream Real-Time Rate Per SSID (kbps)
- Burst Downstream Real-Time Rate Per SSID (kbps)

Note To lock all the properties in the design, click **Lock all**. To lock a specific property, click the lock symbol next to that property.

Step 18 Click **802.11ax Configuration** to configure the 802.11ax BSS Configuration parameters. You can use the toggle button to enable or disable the following configuration parameters:

- BSS Target Wake Up Time
- Downlink OFDMA
- Uplink OFDMA
- Downlink MU-MIMO
- Uplink MU-MIMO

Note To lock all the properties in the design, click **Lock all**. To lock a specific property, click the lock symbol next to that property.

Step 19 Click **Save**.

The created design instance appears in the **Design Instances** window under the **Advanced SSID Configuration - Model Config** area.

Step 20 To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

Step 21 Attach the created config design to a network profile so that it can be deployed on the wireless controller. In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Profiles**.

For more information, see Create Network Profiles for Wireless, on page 170.

Step 22 Provision the model config design specified in the network profile to network devices. In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

For more information, see Provision a Cisco AireOS Controller, on page 375.

Create a Design for Global IPv6

Before you begin

You should have discovered the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Model Config Editor**.

Step 2 In the left pane, you can either search for a model config by entering its name in the **Search Capability** field, or expand **Wireless** and choose **Global IPV6 Configuration**.

Step 3 In the **Design Instances** pane, check the **Default Global IPv6 Design** check box to use the default global IPV6 design.

Note You cannot edit or delete the **Default Global IPv6 Design**.

Step 4 In the **Design Instances** window, click **Add Design**.

The **Add Global IPV6 Configuration** window appears.

Step 5 In the **Design Name** field, enter a name for the model config.

Step 6 Click the **Global IPV6 Config** toggle button to enable IPv6 globally on devices.

Step 7 Click **Apply**.

The created design instance appears in the **Design Instances** window under the **Global IPV6 Configuration - Model Config** area.

Step 8 To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

Step 9 Attach the created config design to a network profile so that it can be deployed on the wireless controller. In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Profiles**.

For more information, see Create Network Profiles for Wireless, on page 170.

Step 10 Provision the model config design specified in the network profile to network devices. In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

For more information, see Provision a Cisco AireOS Controller, on page 375.

Discover and Create Designs from a Legacy Device

Instead of manually creating designs using the Model Config Editor, you can use the Discover Model Configs feature to discover the existing model config designs available on legacy devices and use them as a template to create new designs.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Model Config Editor**.

Step 2 Click the **Discovery** tab.

A list of discovered devices that are available in the **Inventory** window appears.

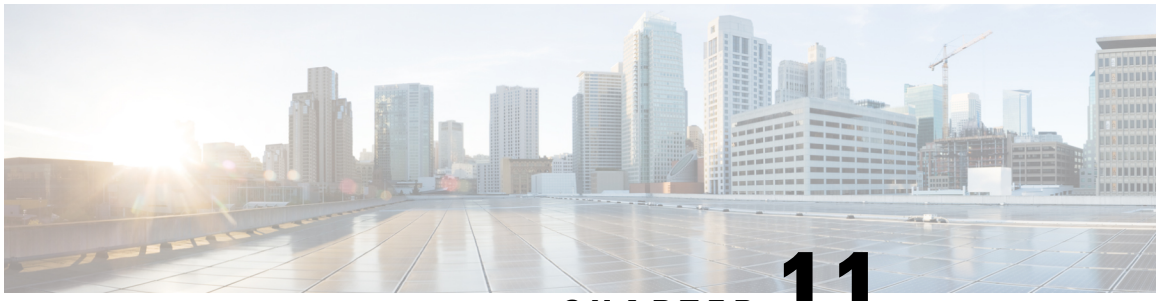
Step 3 Click the radio button next to the device name and click **Discover Model Configs**.

Step 4 In the right pane, expand **Wireless** and choose a model config design type.

The configuration available for the selected model config type appears. For example, if you choose **CleanAir Configuration** under **Wireless**, the available configuration for the CleanAir appears.

Step 5 Click the radio button next to the configuration that you want to use as a template to create a new design, and click **Create Design**.

Step 6 In the window that appears, make the necessary changes and click **Save**.



CHAPTER 11

Configure Telemetry

About Application Telemetry

Application telemetry allows you to configure global network settings on devices for monitoring and assessing their health.

Configure Syslog, SNMP Traps, NetFlow Collector Servers, and Wired Client Data Collection Using Telemetry

With Cisco DNA Center, you can configure global network settings when devices are assigned to a specific site. Telemetry polls network devices and collects telemetry data according to the settings in the SNMP server, the syslog server, the NetFlow Collector, or the wired client.

Before you begin

Create a site and assign a device to the site. See Create a Site in a Network Hierarchy, on page 111.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **Telemetry**.

Step 2 Expand the **SNMP Traps** area if it is not visible and do one of the following:

a) Check the **Cisco DNA Center as SNMP trap server** check box.

b) Check the **Add an external SNMP trap server** check box and enter the IP address of the external SNMP trap server.

The selected server collects SNMP traps and messages from the network devices.

Step 3 Expand the **Syslogs** area if it is not visible and do one of the following:

a) Check the **Use Cisco DNA Center as syslog server** check box.
b) Check the **Add an external syslog server** check box and enter the IP address of the external syslog server.

Step 4 Expand the **NetFlow** area if it is not visible and do one of the following:

a) Check the **Use Cisco DNA Center as NetFlow collector server** check box.

The NetFlow configuration on the device interfaces is completed only when you enable application telemetry on the device. Select the NetFlow collector at the site level to configure the NetFlow destination server to the device.

b) Check the **Add an external NetFlow collector server** check box and enter the IP address and port number of the NetFlow Collector server.

The selected server is the destination server for NetFlow export from the network devices. If the NetFlow Collector is not selected, the application telemetry enablement will not work.

Step 5 Expand the **Wired Client Data Collection** area and check the **Monitor wired clients** check box.

This selection turns on IP Device Tracking (IPDT) on the access devices of the site.

By default, IPDT is disabled for the site.

Step 6 Expand the **Wireless Controller, Access Point and Wireless Clients Health** area and check the **Enable Wireless Telemetry** check box.

When selected, you can monitor the health of your network's wireless controller, access points, and wireless clients.

Step 7 Click **Save**.

Criteria for Enabling Application Telemetry on Devices

Cisco DNA Center automatically enables application telemetry on all applicable interfaces or WLANs that are selected based on the new automatic interfaces or WLAN selection algorithm.

Application telemetry is pushed to WLANs that are provisioned through Cisco DNA Center.

Note

- The conventional tagging-based algorithm is supported and has precedence over the newer automatic interfaces or WLAN selection algorithm.
- If you want to switch over from automatic selection algorithm to tagging-based algorithm, you must disable telemetry before provisioning the tagged SSIDs to the devices.

The following table provides the criteria for selecting interfaces and WLANs based on the conventional tagging-based algorithm (with **lan** keyword) and the new automatic selection algorithm for all the supported platforms:

Platform	Conventional Tagging-Based Algorithm	Automatic Selection Algorithm

Router	• Interface description has the **lan** keyword.[1][2]
	• Interface is a physical interface.
	• Interface has an IP address other than the management IP address.
		• Interface has an IP address other than the management IP address.
		• Interface is not any of the following:
		  • WAN
		  Note An interface is treated as a WAN-facing interface if it has a public IP address, and if there is a route rule with a public IP address that routes through the interface.
		  In this context, a public IP address is not in a private range (for example, not in 192.168.x.x, 172.16.y.y, 10.z.z.z), or is an IP address that is not in the system's IP pools.
		  Route rules can be dynamically learned. In this context, the **show ip route** command does not show a route to a public IP address that goes through this interface.
		  • Loopback.
		  • Management interface: IGABITETHERNET0, GIGABITETHERNET0/0, MGMT0, FASTETHERNET0, or FASTETHERNET1.

Switch	• Interface description has the **lan** keyword.[1, 2]
	• Switch port is configured as an access port.
	• Switch port is configured with the **switch-mode access** command.
		• Interface is a physical interface.
		• Access port does not have neighbors.
		• Interface is not any of the following:
		  • Management interface: FASTETHERNET0, FASTETHERNET1, GIGABITETHERNET0/0, or MGMT0
		  • LOOPBACK0, Bluetooth, App Gigabit, WPAN, Cellular, or Async
		  • VSL interface.

Platform	Conventional Tagging-Based Algorithm	Automatic Selection Algorithm

Cisco AireOS Controller	• WLAN profile name is tagged with the **lan** keyword.[1, 2]	• Not a Guest SSID:
		  • WLAN is not configured as a guest type.
		  • Name of the SSID does not contain the **guest** keyword.
		• SSID is configured in Local mode.

Cisco Catalyst 9800 Series Wireless Controller with Optimized Application Performance Monitoring (APM) profile and IOS release 16.12.1 and later.	• WLAN profile name is tagged with the **lan** keyword.[1, 2]
	• WLAN is configured in Local mode.
		• Not a Guest SSID:
		  • WLAN is not configured as a guest type.
		  • Name of the SSID does not contain the **guest** keyword.
		• If the SSIDs are mixed, that is Local mode, Flex mode, and Fabric mode, the Cisco Application Visibility and Control (AVC) basic record is configured. If all the SSIDs are in Local mode, the Optimized APM record is configured.

	Note If you want to update the telemetry configuration, you must disable telemetry and then enable it after making the configuration changes.	
Cisco DNA Traffic Telemetry Appliance with Optimized APM profile and IOS release 17.3 and later.	• Interface description has the **lan** keyword.[1, 2] • Interface is a physical interface.	• Interface is a physical interface. • Interface is not a management interface: GIGABITETHERNET0, GIGABITETHERNET0/0, MGMT0, FASTETHERNET0, and FASTETHERNET1.

[1] The **lan** keyword is case insensitive and can be separated by a space, hyphen, or underscore.
[2] Resynchronize the network device to read the **lan** interface description.

Provision Application Telemetry Settings

Configure global telemetry settings as described in Configure Syslog, SNMP Traps, NetFlow Collector Servers, and Wired Client Data Collection Using Telemetry, on page 219.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Inventory**.

The Inventory page displays the device information gathered during the Discovery process. To view devices available in a particular site, expand the Global site in the left pane, and select the site, building, or floor.

Step 2 Choose the devices that you want to provision.

Step 3 From the **Actions** drop-down list, choose **Telemetry** and do one of the following:

Note The application telemetry option is enabled only if the device supports application telemetry enablement from Cisco DNA Center.

a) **Enable Application Telemetry**: To configure application telemetry for the selected devices.
b) **Disable Application Telemetry**: To remove the application telemetry configuration from the chosen devices.

Step 4 Click **Apply**.

The **Application Telemetry** column shows the telemetry configuration status. If you don't see the Application Telemetry column in the default column setting, click the **More** icon (⋮) at the right end of the column headings and check the **Application Telemetry** check box.

Update Telemetry Settings to Use a New Cluster Virtual IP Address

If you are using the Cisco DNA Center application telemetry to monitor device data, and you need to change the Cisco DNA Center cluster virtual IP address (VIP), complete the following steps to change the VIP and to ensure that node telemetry data is sent to the new VIP.

Before you begin

- Determine the version of Cisco DNA Center that you are using. You can check this by logging in to the Cisco DNA Center GUI and using the **About** option to view the Cisco DNA Center version number.
- Obtain SSH client software.
- Identify the VIP address that was configured for the 10-GB interface facing the enterprise network on the Cisco DNA Center primary node. Log in to the appliance using this address, on port 2222. To identify this port, see the rear-panel figure in the "Front and Rear Panels" section in the Cisco DNA Center Installation Guide.
- Obtain the Linux username (**`maglev`**) and password configured on the primary node.
- Identify the cluster VIP that you want to assign. The cluster VIP must conform to the requirements explained in the "Required IP Addresses and Subnets" section in the Cisco DNA Center Installation Guide.

Step 1 Access the Cisco DNA Center GUI and **Disable Application Telemetry** at all the sites, as follows:

a) In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Inventory** > **Provision**.

The Inventory page displays the device information gathered during the Discovery process. To view devices available in a particular site, expand the Global site in the left pane, and select the site, building, or floor.

b) Choose all the sites and devices currently being monitored.
c) From the **Actions** drop-down list, choose **Telemetry** > **Disable Application Telemetry**.
d) Wait for the sites and devices to show that telemetry has been disabled.

Step 2 Use the appliance Configuration wizard to change the cluster VIP, as follows:

a) Using an SSH client, log in to the VIP address that was configured for the 10-GB interface facing the enterprise network on the Cisco DNA Center primary node. Be sure to log in on port 2222.
b) When prompted, enter the Linux username and password.
c) Enter the following command to access the Configuration wizard on the primary node:

```
$ sudo maglev-config update
```

If you are prompted for the Linux password, enter it again.

d) Click **[Next]** until the screen prompting you for the cluster virtual IP appears. Enter the new cluster VIP, then click **[Next]** to proceed through the remaining screens of the wizard.

You must configure one virtual IP per configured interface. We recommend that you enter the **sudo maglev-config update** command so that the wizard prompts you to provide one VIP per configured interface.

When you reach the final screen, a message appears, stating that the wizard is ready to apply your changes.

e) Click **[proceed]** to apply the cluster VIP change.

At the end of the configuration process, a success message appears and the SSH prompt reappears.

Step 3 Restart the necessary Cisco DNA Center services by entering the following series of commands at the SSH prompt:

```
magctl service restart -d collector-netflow
magctl service restart -d collector-syslog
magctl service restart -d collector-trap
magctl service restart -d wirelesscollector
```

Step 4 Wait for all the services to restart. You can monitor the progress of the restarts by entering the following command, substituting service names as needed for the release train appropriate for your Cisco DNA Center version.

```
magctl appstack status | grep -i -e collector-netflow -e collector-syslog -e collector-trap -e
wirelesscollector
```

When all the necessary services are running, you see command output similar to the following, with a Running status for each service that has restarted successfully:

```
assurance-backend  wirelesscollector-123-bc99s  1/1   Running   0   25d   <IP>   <IP>
ndp   collector-netflow-456-lxvlx   1/1   Running   0   1d   <IP>   <IP>
ndp   collector-syslog-789-r0rr1    1/1   Running   0   25d   <IP>   <IP>
ndp   collector-trap-101112-3ppllm  1/1   Running   0   25d   <IP>   <IP>
```

Step 5 Access the Cisco DNA Center GUI and **Enable Application Telemetry** to all nodes as follows:

a) In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Inventory** > **Provision**.
b) Choose all the sites and devices that you want to monitor.
c) From the **Actions** drop-down list, choose **Telemetry** > **Enable Application Telemetry**.
d) Wait for the sites and devices to show that telemetry has been enabled.

Update Device Configuration Using Telemetry

You can push the configuration changes to a device irrespective of whether the device controllability is enabled or disabled.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Inventory**.

The Inventory page displays the device information gathered during the Discovery process. To view devices available in a particular site, expand the **Global** site in the left pane, and select the site, building, or floor.

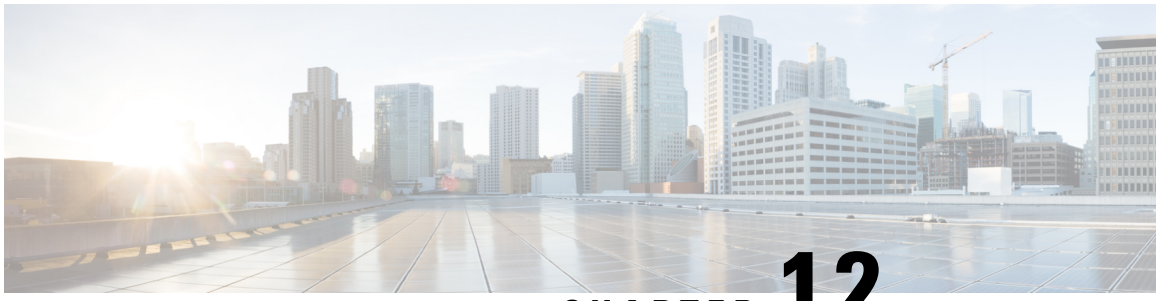
Step 2 Choose the devices that you want to update the configuration changes.

Step 3 From the **Actions** drop-down list, choose **Telemetry** > **Update Telemetry Settings**.

Step 4 In the **Update Telemetry Settings** window, do the following:

- (Optional) Check the **Force Configuration Push** check box to push the configuration changes to the device. If there is no change in the configuration settings, the existing configuration is pushed again to the device.
- Click **Next**.
- Click the **Now** radio button or click the **Later** radio button and specify the date and time to update the telemetry settings.

Step 5 Click **Apply**.



CHAPTER 12

Identify Network Security Advisories

Security Advisories Overview

The Cisco Product Security Incident Response Team (PSIRT) responds to Cisco product security incidents, regulates the Security Vulnerability Policy, and recommends Cisco Security Advisories and Alerts.

The Security Advisories tool uses these recommended advisories, scans the inventory within Cisco DNA Center, and finds the devices with known vulnerabilities.

Prerequisites

To use the Security Advisories tool, you must install the Machine Reasoning package. See *Download and Install Packages and Updates* in the Cisco DNA Center Administrator Guide.

If you log in to Cisco DNA Center as an Observer, you cannot view the **Security Advisories** tool in the home page.

View Security Advisories

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Security Advisories**.

Step 2 If you are launching the **Security Advisories** page for the first time, click **Scan Network**.

Cisco DNA Center uses the knowledge base to identify security issues and improve automated analysis. We recommend that you update the knowledge base on a regular basis to view the latest security advisories.

a) In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Settings** > **Machine Reasoning Knowledge Base**.
b) Click **Import**, or click **Download** to download the latest available knowledge base, and then click **Import**.
c) Click the **AUTO UPDATE** toggle button to subscribe to automatic updates.

Note
- The security advisories dashboard shows security advisories published by Cisco that may affect devices on your network based on the software image currently installed. A further analysis of the configuration, platform details, or other criteria is required to determine if a vulnerability is actually present.
- The **Overview** tab with its security advisories graphic displays the distribution percentage of impact on the network, such as **Critical**, **High**, **Medium**, **Low**, or **Informational**.
- Security advisories scanning is only available for routers and switches that are running the minimum supported software version. For more information, see Cisco DNA Center Supported Devices.
- The security advisories displayed are subject to the Cisco Security Vulnerability Policy.

The following table describes the information that is available.

Column	Description
Advisory ID	ID of the security advisories found in the network. Click the ID to go to the respective advisory web page.
Advisory title	Name of the security vulnerability advisory applicable to the network devices.
CVSS score	Score evaluated based on the Common Vulnerability Scoring System (CVSS) model.
Impact	Impact of the vulnerability on the network.
CVE	Common Vulnerabilities and Exposures (CVE) identifier for the vulnerability.
Devices	The number of devices impacted by the vulnerability. Click the number to view the devices that may be vulnerable based on this specific advisory, and upgrade the devices as needed.
Match Type	Indicates whether the vulnerability was detected based on **Image Version** match or **Configuration** match.
Known since (days)	The number of days since the vulnerability was discovered.
Last updated	The date when the advisory was last updated.

Step 3 Click the **Devices** tab to view the number of advisories applicable to each device.

a) Click the number of advisories to view all that match the device.

b) Click the topology icon in the top-right corner to view the device topology. You can click a device in the topology to view all advisories that match the device.

A lock icon next to the device indicates that there are one or more advisories applicable to the device.

Step 4 Click **Scan Network** at any time to refresh the results displayed.

Schedule a Security Advisories Scan

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Security Advisories**.

Step 2 Click **Scan Network**.

The **Scan Network** window appears.

Step 3 To scan the security advisories immediately, click the **Now** radio button and click **Start**.

Step 4 To schedule the scan for a later date and time, click the **Later** radio button and specify the date and time.

Step 5 Use the **Time Zone** drop-down list to schedule the scan according to a specific time zone.

Step 6 Choose the recurrence option: **None** (the default), **Daily**, or **Weekly**.

Step 7 In the **Run at Interval** field, enter the number of days or weeks for the recurrence of the scan.

Step 8 (Optional) Check the **Set Schedule End** check box to schedule an end date and number of occurrences.

a) To schedule a scan end date, click the **End Date** radio button and define the date and time.

b) To define the number of scan occurrences, click the **End After** radio button.

Step 9 Click **Schedule**.

Step 10 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Activity** > **Tasks** and confirm the schedule and recurrence of the scan.

Note In Cisco DNA Center releases earlier than 2.1.1.x, you have the ability to opt in or out of telemetry that Cisco collects. When you opt in, we collect your cisco.com ID, system telemetry, feature usage telemetry, network device inventory, and license entitlement. Telemetry is not application or feature specific; the disclosure of telemetry is for all of Cisco DNA Center. In Cisco DNA Center 2.1.1.x and later, telemetry collection is mandatory. The telemetry is designed to help the development of features that you use. See the *Cisco DNA Center Data Sheet* for a more expansive list of data that we collect.

When a security advisory scan runs, the following telemetry data is collected:

- Whether automatic update of knowledge packages has been set up.
- Whether recurring scanning and recurring reports have been set up.
- The number of reports that have been run.
- The number of devices with a security advisory match based on software version and configuration.
- The number of thumbs up/thumbs down votes, per scan.
- The manual configurations entered as a search, and the associated advisory.
- The number of advisory matches by software version and configuration, including product family.
- The number of devices based on other categories (zero advisories, unknown, and unsupported).
- The number of successful, failed, and terminated scans.
- The average scan time.

Hide and Unhide Devices from an Advisory

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Security Advisories**.

Step 2 If you are launching the **Security Advisories** page for the first time, click **Scan Network**.

Step 3 In the **Scan Network** window, choose **Now**, and then click **Start**.

Step 4 To hide the devices from an advisory, do the following:

a) From the **Focus** drop-down list, choose **Advisories**.

b) In the **Devices** column, click the devices count that corresponds to the advisory for which you want to hide the devices.

The **Active** tab shows the number of devices for which these advisories are issued.

c) Choose the devices that you want to hide and click **Suppress Device**.

The hidden devices can be viewed in the **Suppressed** tab.

d) Close the advisory window and view the change in the device count for this advisory.

Step 5 To restore the devices to an advisory, do the following:

a) From the **Focus** drop-down list, choose **Advisories**.

b) In the **Devices** column, click the devices count that corresponds to the advisory for which you want to unhide the devices.

c) Click the **Suppressed** tab to view the hidden devices.
d) Choose the devices that you want to unhide and click **Mark as Active**.

The restored devices can be viewed in the **Active** tab.

e) Close the advisory window and view the change in the device count for this advisory.

Hide and Unhide Advisories from a Device

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Security Advisories**.

Step 2 If you are launching the **Security Advisories** page for the first time, click **Scan Network**.

Step 3 In the **Scan Network** window, choose **Now**, and then click **Start**.

Step 4 To hide the advisories for a device, do the following:

a) From the **Focus** drop-down list, choose **Devices**.
b) In the **Advisories** column, click the advisories count that corresponds to device for which you want to hide the advisories.

The **Active** tab shows the number of advisories issued for this device.

c) Choose the advisories that you want to hide and click **Suppress Advisory**.

The hidden advisories can be viewed in the **Suppressed** tab.

d) Close the device window and view the change in the advisory count for this device.

Step 5 To restore the advisories for a device, do the following:

a) From the **Focus** drop-down list, choose **Devices**.
b) In the **Advisories** column, click the advisories count that corresponds to the device for which you want to unhide the advisories.
c) Click the **Suppressed** tab to view the hidden advisories.
d) Choose the advisories that you want to unhide and click **Mark as Active**.

The restored advisories can be viewed in the **Active** tab.

e) Close the device window and view the change in the advisories count for this device.

Add Notification for a New Security Advisory KB

A security advisory Knowledge Bundle (KB) uses a Machine Reasoning Engine (MRE) to scan the network. You can configure Cisco DNA Center to notify you when a new security advisory Knowledge Bundle (KB) is available. After you enable notifications, Cisco DNA Center displays a visual notification and actionable alert whenever a new security advisory Knowledge Bundle (KB) is available.

The following procedure explains how to add notifications for a new security advisory knowledge bundles:

Before you begin

- You must install the Cisco DNA Center core package. See Download and Install Packages and Updates in the *Cisco DNA Center Administrator Guide*.
- You must install the Machine Reasoning (MRE) package. See Download and Install Packages and Updates in the *Cisco DNA Center Administrator Guide*.
- The following containers must be present in your system:
  - cnsr-reasoner
  - cloud connectivity/download

Step 1 In the Cisco DNA Center GUI, click the notification icon located at the top-right corner. From the drop-down menu, select the gear icon to view the notification preferences.

Step 2 In the **My Profile and Settings** window, enable the security advisory notification by choosing the **Security Advisories** option.

Step 3 Click **Save**.

Step 4 In the **Machine Reasoning Engine** window, click the **Download Latest** link to download the latest knowledge bundle.

Step 5 Review and update the Knowledge Base settings.

Step 6 In the **Security Advisory Settings** section, choose the recurrence option: **None** (default), **Daily**, or **Weekly**.

Step 7 In the Cisco DNA Center GUI, choose **Notification Center** > **Go to Security Advisories** to view the Security Advisories tool page directly.

Step 8 Rescan the network with the newly downloaded security advisories. For more information, see Schedule a Security Advisories Scan, on page 229.

View Security Advisories in Inventory Page

The Cisco DNA Center security focus view allows you to view the list of security advisories for your devices, based on the data retrieved from the previous security scan. The device data that you retrieve from the Security Advisories tool is now displayed in the inventory page.

Use the following procedure to view the security advisories column in the inventory page:

Before you begin

- You must install the Cisco DNA Center core package. See Download and Install Packages and Updates in the *Cisco DNA Center Administrator Guide*.
- You must install the Machine Reasoning package. See Download and Install Packages and Updates in the *Cisco DNA Center Administrator Guide*.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Security Advisories**.

Step 2 Click **Scan Network**.

The **Scan Network** window appears.

Step 3 To scan the security advisories immediately, click the **Now** radio button and click **Start**. For more details, refer Schedule a Security Advisories Scan.

Step 4 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

Step 5 From the **FOCUS: Inventory** drop-down menu, select **Security**.
The **Advisories** column is displayed in the **Inventory**table.

Step 6 In the **Device Details** page, select a device and view the advisories data.

Step 7 Click **Manage All** to navigate to **Security Advisories** tool.

Add a Match Pattern

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Security Advisories**.

Step 2 If you are launching the **Security Advisories** page for the first time, click **Scan Network**.

Step 3 In the **Scan Network** window, choose **Now**, and then click **Start**.

Step 4 Choose an advisory and in the **Match Type** column, click **Add match pattern**.

Step 5 In the **Add Configuration Match Pattern** window, enter the condition to match with devices in the **CONDITIONS** text box.

Step 6 Click **Save**.

The match pattern is added to the advisory.

Step 7 Click **Scan Network** to check the number of devices that match with the match pattern.

Define AND/OR for the Match Pattern

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Security Advisories**.

Step 2 If you are launching the **Security Advisories** page for the first time, click **Scan Network**.

Step 3 In the **Scan Network** window, choose **Now**, and then click **Start**.

Step 4 Choose an advisory and in the **Match Type** column, click **Add match pattern**.

Step 5 In the **Add Configuration Match Pattern** window, do the following:

a) In the **CONDITIONS** text box, enter a condition and then click the **Add** icon.
b) From the drop-down list, choose **AND** or **OR** and then enter the next condition.
c) If you want to delete a condition, click the **Remove** icon.
d) Click **Save**.
The match pattern is added to the advisory.

Step 6 Click **Scan Network** to check the number of devices that match the match pattern.

Edit the Match Pattern

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Security Advisories**.

Step 2 If you are launching the **Security Advisories** page for the first time, click **Scan Network**.

Step 3 In the **Scan Network** window, choose **Now**, and then click **Start**.

Step 4 Choose an advisory that already has a match pattern and in the **Match Type** column, click **Edit match pattern**.

Step 5 In the **Edit Configuration Match Pattern** window, enter the condition to match with devices in the **CONDITIONS** text box.

Step 6 Click **Save**.

The match pattern is changed.

Step 7 Click **Scan Network** to check the number of devices that match the match pattern.

Delete the Match Pattern

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Security Advisories**.

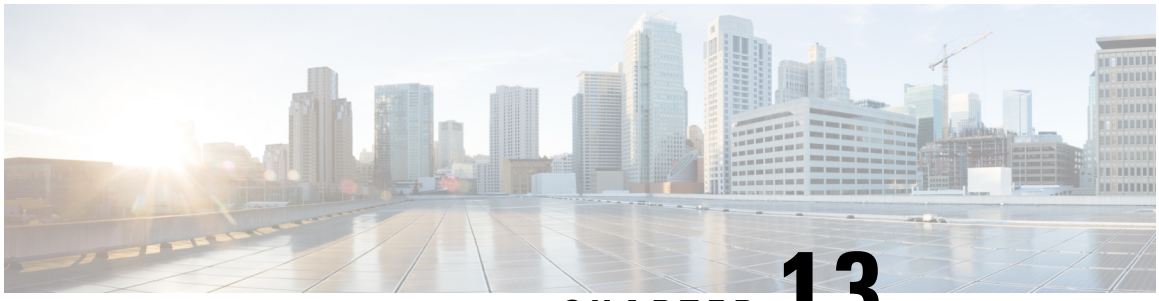
Step 2 If you are launching the **Security Advisories** page for the first time, click **Scan Network**.

Step 3 In the **Scan Network** window, choose **Now**, and then click **Start**.

Step 4 Choose an advisory that already has a match pattern and in the **Match Type** column, click **Edit match pattern**.

Step 5 In the **Edit Configuration Match Pattern** window, click **Delete**.

The match pattern is deleted.



CHAPTER 13

Troubleshoot Network Devices Using Network Reasoner

About Network Reasoner

The Network Reasoner tool allows you to troubleshoot various issues on your network quickly. In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Network Reasoner** to launch the Network Reasoner Dashboard. The Network Reasoner dashboard hosts separate workflows using which you can proactively troubleshoot the network issues. The dashboard provides a brief description about the workflows, the number of affected devices in the last 24 hours, and impact of running a workflow on a network.

Note You must install the Machine Reasoning package to view the Network Reasoner feature under the Tools menu. For more information, see the Cisco DNA Center Administrator Guide.

Validate Cisco SD-Access Migration Using the MRE Workflow

The following MRE workflows assist in planning your migration to Cisco SD-Access:

- SDA Hardware Readiness Check
- SDA Software Readiness Check
- Redundant Link Check

- L3 Access Check
- MTU Link Check
- SDA Health Check
- SDA Scale Limits Check

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Network Reasoner**.

Step 2 In the **Network Reasoner** dashboard, click the following workflows as required:

Workflow	Description	Action
SDA Hardware Readiness Check	Checks whether the hardware is ready for Cisco SD-Access migration.	**a.** Click **SDA Hardware Readiness Check**. **b.** Click **Run Machine Reasoning**.
SDA Software Readiness Check	Checks whether the software is ready for Cisco SD-Access migration.	**a.** Click **SDA Software Readiness Check**. **b.** Click **Run Machine Reasoning**.
Redundant Link Check	Checks whether any redundant uplinks are present in your device and if there are ways to increase availability by configuring redundant uplinks on the access switches.	**a.** Click **Redundant Link Check**. **b.** Select an appropriate device. **c.** Click **Troubleshoot**.
L3 Access Check	Checks whether your network has access switches that are running Layer 3 routing protocols to move to Cisco SD-Access with minimal design changes.	**a.** Click **L3 Access Check**. **b.** Select an appropriate device. **c.** Click **Troubleshoot**.
MTU Link Check	Checks whether the links between the main network devices and the access, core, and other switches are configured with the correct MTU.	**a.** Click **MTU Link Check**. **b.** Select an appropriate device. **c.** Click **Troubleshoot**.
SDA Health Check: Fabric Count	Checks the health of the Cisco DNA Center cluster to determine whether it is reaching any scale limit thresholds due to managing fabrics.	**a.** Click **Fabric Count**. **b.** Click **Run Machine Reasoning**.
SDA Health Check: SDA Scale Limits Check	Checks whether the number of client endpoints, network devices, and configured fabrics in Cisco DNA Center are within the published SDA limits.	**a.** Click **SDA Scale Limits Check**. **b.** Click **Run Machine Reasoning**.

Workflow	Description	Action
SDA Health Check: Client Count	Checks the health of the Cisco DNA Center cluster to determine whether it is reaching any scale limit thresholds due to managing clients.	**a.** Click **Client Count**. **b.** Click **Run Machine Reasoning**.
SDA Health Check: Device Count	Checks the health of the Cisco DNA Center cluster to determine whether it is reaching any scale limit thresholds due to managing network devices.	**a.** Click **Device Count**. **b.** Click **Run Machine Reasoning**.

Troubleshoot High CPU Utilization

CPU utilization troubleshooting support is available only for the following network devices with software version 16.9.3 and later:

- Cisco Catalyst 9400 Series Switches
- Cisco Catalyst 9300 Series Switches
- Cisco Catalyst 3850 Series Switches
- Cisco Catalyst 3650 Series Switches

Before you begin

- Install the Machine Reasoning package. See Download and Install Packages and Updates in the Cisco DNA Center Administrator Guide.
- Create a user role with write permissions for Machine Reasoning under the **System** function. For more information, see Configure Role-Based Access Control in the Cisco DNA Center Administrator Guide.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Network Reasoner**.

Step 2 Click the **CPU Utilization** tab.

The **CPU Utilization** page displays the filtered list of devices with high CPU utilization in the past 24 hours.

Click **All** to see the list of all devices from the inventory, and you can choose any device to run the workflow.

Step 3 Choose the device that you want to troubleshoot.

Click **Filter** and enter the devices by entering **Tag**, **Device Name**, **IP Address**, **Device Type**, **Site**, or **Reachability**.

Step 4 Click **Troubleshoot**.

Step 5 In the **Reasoner Input** window, enter the **CPU Utilization Threshold** percentage that you want to check against.

Step 6 Click **Run Machine Reasoning**.

Note The following processes, if observed, are considered for detailed analysis:

- **MATM Process Group**: MATM RP Shim, NGWC Learning, and VMATM Callback
- **IOSXE Process Group**: IP Input, ARP Input, IOSXE-RP Punt Se, SISF Main Thread, DAI Packet, and ARP Snoop

The **CPU Utilization** window appears, where you can see the **Root Cause Analysis** of the high CPU utilization for the chosen device.

The **Reasoning Activity** tab shows the various parameters that are checked as part of the troubleshooting process.

Step 7 (Optional) Click **Stop** to stop the ongoing reasoning activity.

Step 8 Click the **Conclusion** tab to see the processes that consume more CPU and the utilization percentage.

Step 9 Click **View Relevant Activities** for each process to view the **Activity Details** in the right pane.

Step 10 (Optional) Click **Run Again** to rerun the troubleshooting process for the same device.

Note The Machine Reasoning Engine (MRE) implements a system-terminate algorithm that detects and terminates network reasoner workflows when thresholds exceed a specified level, or when no events are received from the timeout request for inactivity.

Troubleshoot a Power Supply Failure

Power supply troubleshooting workflow support is available only for the following network devices with software version 16.6.1 and later:

- Cisco Catalyst 3650 Series Switches
- Cisco Catalyst 3850 Series Switches
- Cisco Catalyst 9300 Series Switches
- Cisco Catalyst 9400 Series Switches
- Cisco Catalyst 9500 Series Switches

Before you begin

- Install the Machine Reasoning package. See Download and Install Packages and Updates in the Cisco DNA Center Administrator Guide.
- Create a user role with write permissions for Machine Reasoning under the **System** function. For more information, see Configure Role-Based Access Control in the Cisco DNA Center Administrator Guide.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Network Reasoner**.

Step 2 Click the **Power Supply** tab.

The **Power Supply** page displays the filtered list of devices with power supply failures in the past 24 hours.

Click **All** to see the list of all devices in the inventory. You can choose any device to run the workflow.

Step 3 Choose the device that you want to troubleshoot.

Click **Filter** and filter the devices by entering **Tag**, **Device Name**, **IP Address**, **Device Type**, **Site**, or **Reachability**.

Step 4 Click **Troubleshoot**.

The **Power Supply** window appears, where you can see the **Root Cause Analysis** of the power supply failure for the chosen device.

The **Reasoning Activity** tab shows the various parameters that are checked as part of the troubleshooting process.

Step 5 (Optional) Click **Stop** to stop the ongoing reasoning activity.

Step 6 Click the **Conclusion** tab to see the **Stack Identifier**, **Product ID**, **Serial Number**, and **Status** of the power supply for the chosen device and the suggested action.

Step 7 Click **View Relevant Activities** for each stack identifier to view the **Activity Details** in the right pane.

Step 8 (Optional) Click **Run Again** to rerun the troubleshooting process for the same device.

Note The MRE implements a system-terminate algorithm that detects and terminates network reasoner workflows when thresholds exceed a specified level, or when no events are received from the timeout request for inactivity.

Troubleshoot a Downed Interface

Interface down troubleshooting workflow support is available only for the following network devices with software version 16.9.3, and later:

- Cisco Catalyst 3650 Series Switches
- Cisco Catalyst 3850 Series Switches
- Cisco Catalyst 9300 Series Switches
- Cisco Catalyst 9400 Series Switches
- Cisco Catalyst 9500 Series Switches

Before you begin

- Install the Machine Reasoning package. See Download and Install Packages and Updates in the Cisco DNA Center Administrator Guide.
- Create a user role with write permissions for Machine Reasoning under the **System** function. For more information, see Configure Role-Based Access Control in the Cisco DNA Center Administrator Guide.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Network Reasoner**.

Step 2 Click the **Interface Down** tab.

The **Interface Down** page displays the filtered list of devices with an interface that went down in the past 24 hours.

Click **All** to see the list of all devices from the inventory, and you can choose any device to run the workflow.

Step 3 Choose the device that you want to troubleshoot.

Click **Filter** and enter the devices by entering **Tag**, **Device Name**, **IP Address**, **Device Type**, **Site**, or **Reachability**.

Step 4 Click **Troubleshoot**.

Step 5 In the **Reasoner Input** window, enter the interface name that you suspect has issues.

Step 6 Click **Run Machine Reasoning**.

The **Interface Down** window appears, where you can see the **Root Cause Analysis** of the downed interface for the chosen device.

The **Reasoning Activity** tab shows the various parameters that are checked as part of the troubleshooting process.

Step 7 (Optional) Click **Stop** to stop the ongoing reasoning activity.

Step 8 Click the **Conclusion** tab to see the potential root causes for the interface down issue and the suggested action.

Step 9 Click **View Relevant Activities** for each root cause analysis to view the **Activity Details** in the right pane.

Step 10 (Optional) Click **Run Again** to rerun the troubleshooting process for the same device.

Note The MRE implements a system-terminate algorithm that detects and terminates network reasoner workflows when thresholds exceed a specified level, or when no events are received from the timeout request for inactivity.

Troubleshoot Network Connectivity

Only the following network devices running Cisco IOS-XE software version 16.9.3 or later support the network connectivity troubleshooting :

- Cisco Catalyst 9200 Series Switches
- Cisco Catalyst 9300 Series Switches
- Cisco Catalyst 9400 Series Switches
- Cisco Catalyst 9500 Series Switches
- Cisco Catalyst 9600 Series Switches

Use the following procedure to check the reachability of an end point from a device using IP address:

Before you begin

- Install the Machine Reasoning package. See Download and Install Packages and Updates in the Cisco DNA Center Administrator Guide.
- Create a user role with write permissions for Machine Reasoning under the **System** function. For more information, see Configure Role-Based Access Control in the Cisco DNA Center Administrator Guide.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Network Reasoner**.

Step 2 Click the **Network Connectivity** tab.

Step 3 You can view the device table with details, such as **Device Name**, **IP Address**, **Device Type**, **Site**, **Reachability**, **Role**, and **Platform**.

Step 4 Select a device and click **Troubleshoot**.
The **Reasoner Inputs** dialog box is displayed.

Step 5 In the **Destination IP address** field, enter a valid IP address and click **Run Machine Reasoning**.

Note Provide the Virtual Routing and Forwarding (VRF) name, if applicable.

Step 6 In the **Root Cause Analysis** window, under **Reasoning Activity**, you can view various workflows that are validated as a part of the troubleshooting process.

Step 7 In the **Conclusions** tab, you can view the status of the validation check and the suggested action.

Troubleshoot IP Connectivity of a Device

As ping is a simple command, IP connectivity troubleshooting support is available for all the network devices.

Before you begin

- Install the Machine Reasoning package. See Download and Install Packages and Updates in the Cisco DNA Center Administrator Guide.
- Create a user role with write permissions for Machine Reasoning under the **System** function. For more information, see Configure Role-Based Access Control in the Cisco DNA Center Administrator Guide.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Network Reasoner**.

Step 2 In the **Network Reasoner** dashboard, click **Ping Device**.

Step 3 In the **Devices** window, choose a device and click **Troubleshoot**.

Step 4 In the **Reasoner Inputs** window, enter **Target IP Address** and click **Run Machine Reasoning**.

Step 5 Click **View Details** to view the ping status.

Enable Network Bug Identifier

Cisco DNA Center network bug identifier tool allows you to scan the network for a selected set of defects or bugs that have been identified previously and are known to Cisco.

The Cisco DNA Center network bug identifier helps in identifying specific patterns in the device configuration or in the operational data of the device and matches them with known defects based on those patterns. This tool provides the following views:

- Bugs focused
- Device focused

The following procedure explains how to identify bugs using the network bug identifier tool:

Before you begin

- Install the Cisco DNA Center core package. See Download and Install Packages and Updates in the *Cisco DNA Center Administrator Guide*.
- Install the Machine Reasoning package. See Download and Install Packages and Updates in the *Cisco DNA Center Administrator Guide*.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Network Reasoner**.

Step 2 Select **Network Bug Identifier**.

Step 3 Click **Scan Network**.

Step 4 In the **Scan Network** window, do any one of the following:

- To scan your system for bugs immediately, click the **Now** radio button and click **Submit**.
- To schedule the scan for a later date and time, click the **Later** radio button and specify date and time.

The dashboard progress indicator shows the list of devices scanned in batches of 10.

Step 5 In the **Network Bug Identifier** page, click **Bugs on Devices** to view the following details:

- **Bug ID**
- **Affected Devices**
- **Severity**
- **Affected Versions**
- **Workaround**

Step 6 Click on the number of **Affected Devices** against a specific **Bug ID** to view the complete details of that devices affected by the bugs.

Step 7 In the **Network Bug Identifier** window, click **Affected Devices** to view the following details:

- **Device Name**
- **IP Address**
- **Device Type**
- **Site**
- **Reachability**
- **Bugs**
- **Image Version**

Step 8 Click the **Bugs** value against a specific **Device Name** to view the complete details about the bugs associated with the devices.

Step 9 Click the Information icon against **BUG SUMMARY** and then click **View All** to view the full subset of bugs supported by Cisco Machine Reasoning Engine (MRE).

Note The current capability of this tool is limited to switches and routers running **IOS-** or **IOS-XE**-based images.

Enable System Bug Identifier

The **System Bug Identifier** tool provides an option to identify bugs in the Cisco DNA Center. The following procedure explains how to enable the **System Bug Identifier** tool:

Before you begin

- Install the Cisco DNA Center core package. See Download and Install Packages and Updates in the *Cisco DNA Center Administrator Guide*.
- Install the Machine Reasoning package. See Download and Install Packages and Updates in the *Cisco DNA Center Administrator Guide*.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Tools** > **Network Reasoner**.

Step 2 Select **System Bug Identifier**.

Step 3 Click **Scan System**.

Step 4 In the **Scan System** window, do any on the following:

a. To scan your system for bugs immediately, click the **Now** radio button and click **Submit**

b. To schedule the scan for a later date and time, click the **Later** radio button and specify date and time.

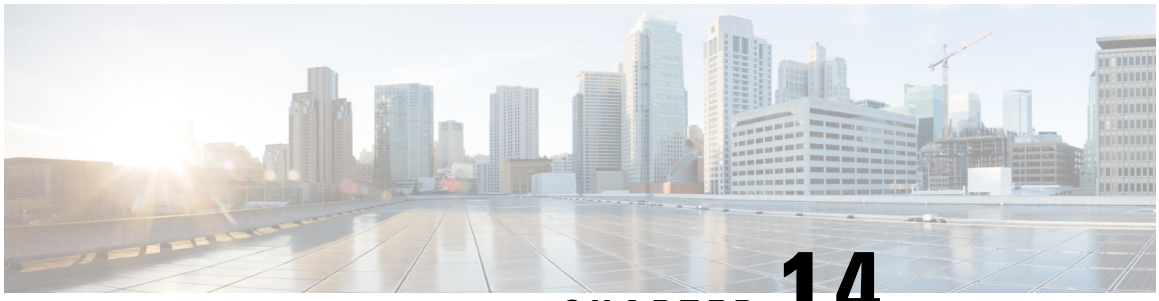
Step 5 The **System Bug Identifier** page shows the **BUG SUMMARY** and the **Bugs Identified on Your System** table.

You can view the following details in the **Bugs Identified on Your System** table:

- **Bug ID**
- **Name**
- **Severity**
- **First identified**
- **Last identified**
- **Identified frequency**
- **Workaround**
- **Affected Versions**

Step 6 Click the **Bug ID**.
The **Bug Details** dialog box appears and displays the details of the bug.

Step 7 Click the arrow next to **Bug ID** and to go to the **Bug Search Tools** page, which shows more details about the bugs.



CHAPTER 14

Configure Policies

Policy Overview

Cisco DNA Center enables you to create policies that reflect your organization's business intent for a particular aspect of the network, such as network access. Cisco DNA Center takes the information collected in a policy and translates it into network-specific and device-specific configurations required by the different types, makes, models, operating systems, roles, and resource constraints of your network devices.

Using Cisco DNA Center, you can create virtual networks, access control policies, traffic copy policies, and application policies.

Group-Based Access Control Policies

Cisco DNA Center implements Software-Defined Access in two ways:

- Virtual networks (VNs) provide macro-level segmentation, such as to separate IoT devices from the corporate network.
- Group-based policies provide micro-level segmentation, such as to control what types of network traffic to permit or deny between engineering and HR groups.

The Group-Based Access Control Policy menu allows you to monitor and manage your scalable group access policies. These policies provide the following benefits:

- Rich identity-based access control functionality with network automation and assurance benefits.
- Granular access control.
- Scalable groups apply to all virtual networks, which simplifies policy management.

- Policy views help you to understand the overall policy structure, and create or update required access control policies.
- Eliminates the need to switch between different applications to manage scalable groups and define protected assets.
- Provides enhanced features for deploying enterprise-wide access control policies.
- Restricts lateral movement of threats like ransom ware before you have identity or Network Admission Control (NAC) applications in place.
- Provides an easy migration path to Cisco Identity Services Engine (Cisco ISE) for users who are using third-party identity applications, but want to move to Cisco ISE.

For information about creating IP pools, sites, and virtual networks in Cisco DNA Center, see the Cisco DNA Center User Guide.

For information about configuring Cisco DNA Center for Cisco ISE, see the Cisco DNA Center Installation Guide.

For information about configuring Cisco ISE for Cisco DNA Center, see the Cisco Identity Services Engine Administrator Guide.

Define the scalable groups and contracts first, then create access control policies. The access control policies define which network traffic can pass from a source scalable group to a destination scalable group.

- **Scalable Group**: A classification category, to which you can assign users, network devices, or resources. Scalable groups are used in access control policies. You can associate scalable groups with virtual networks based on your organization's network configuration, access requirements, and restrictions.
- **Contract**: An access contract is a set of rules that controls the type of network traffic that is allowed to pass between the source and destination scalable groups. In other words, a contract is a traffic filter definition. Access contracts define the actions (permit or deny) performed when the traffic matches a network application, protocol, and port. The default action is to use the Catch All rule when no other rules match.
- **Group-Based Access Control Policies**: A group-based access control policy identifies a specific source and destination group pair and associates an access contract. The access contract specifies what types of traffic are permitted or denied between the source group and the destination group. These policies are unidirectional.

  Scalable groups and access contracts are the basic building blocks of access control policy. While creating the access control policy, you can use the scalable groups and contracts that you have created before or create new scalable groups and contracts while creating the policy. If you want to specify the network resources that can be accessed from a specific source group, you can create an access control policy with a single source and multiple destination groups. On the other hand, if you want to specify the source groups that are permitted to access a particular network resource, you can create an access control policy with a single destination and multiple source groups. For example, if you want to specify the network resources that can be accessed by the users associated with the "contractors" source scalable group, you can create an access control policy with a single source and multiple destination groups. If you want to specify the source groups that are permitted to access the "Finance Servers" destination scalable group, you can create an access control policy with single destination and multiple source groups.

  You can specify the default policy to use when no contract is specified for a source and destination scalable group combination. The default policy is **Permit**. You can change this policy to **Deny**, **Permit_IP_Log**, or **Deny_IP_Log**, if necessary. You can set the default policy based on your network type, an open or closed network.

Note We recommend that you change the default policy from "Permit" to "Deny" only if you have created explicit policies to permit necessary network traffic for all your network infrastructure devices. Failure to do so can result in loss of network connectivity.

List View

Click the **List** icon at the top right of the **Group-Based Access Control** window to launch the **List** view.

- **Source View**: Displays a list of existing policies organized based on the source groups. You can expand each row to view the specific source-destination policy details.
- **Destination View**: Displays a list of existing policies organized based on the destination groups. You can expand each row to view the specific source-destination policy details.

To see which destination groups are available from a specific source group, use the **Source** view. To see which source groups are permitted to access a particular destination group, use the **Destination** view. For example, to see which destination groups are available to users who are part of the "Contractors" source scalable group, use the **Source** view. To see which source groups can access the "Finance servers" destination scalable group, use the **Destination** view.

You can also view the policy enforcement statistics data in the policies listing table. The total number of policy permits and denies are displayed for the selected time period.

The policy enforcement statistics are collected from the network devices that are provisioned for group-based policy and telemetry data language (TDL) subscription. These configurations are normally provisioned automatically for network devices that are part of a fabric. Manual configuration can be done for nonfabric network devices.

Note the following points while using the policy enforcement statistics data:

- Policy enforcement statistics data is available only when Group-Based Policy Analytics package is deployed.
- Telemetry subscription is added as part of base provisioning for both fabric and nonfabric network devices. TrustSec enforcement command is pushed when a new network device is added to DNAC and assigned to a site.
- Software-Defined Access (SDA) adds TrustSec enforcement for the network devices that are added to a fabric. TrustSec telemetry data is collected only when this enforcement is enabled on a network device. If it is not enabled, the telemetry subscriptions used for policy monitoring are used to collect the TDL data for TrustSec.
- Cisco IOS XE 16.12 and later support TDL streaming data.
- NETCONF must be enabled on the network devices.
- The following configuration must be added manually for the nonfabric network devices:

```
cts role-based enforcement vlan-list <VLAN of the endpoints>
```

- After upgrading to Cisco DNA Center 2.2.2, you might see the following message in the **Provision > Network Devices > Inventory** window:

```
We detected IOS-XE devices in your network where new telemetry subscription for assurance
data needs to be enabled and some of the existing subscription needs to be optimized
for performance. Please note that you will have to enable netconf and configure the
netconf port in the Inventory credentials for these devices. Also note that these devices
will receive a new subscription for group based policy monitoring telemetry. Do you
want to take an action to provision these subscriptions?
```

Click **Apply Fix** to push the configuration to all network devices with site assigned.

Click **Deploy** to deploy the updated policies to the network devices. When you click **Deploy**, Cisco DNA Center requests the Cisco Identity Services Engine (Cisco ISE) to send notifications about the policy changes to the network devices.

Matrix View

Click the **Grid** icon at the top right of the **Group-Based Access Control** window to launch the Matrix view. The Matrix view is a core policy view, which provides an overview of all policies for all scalable groups (whether explicit or default). You can use the Matrix view to view all source and destination policies and understand the overall policy structure. You can view, create, and update access control policies from the Matrix view.

The Matrix view contains two axes:

- Source Axis: The vertical axis lists all the source scalable groups.
- Destination Axis: The horizontal axis lists all the destination scalable groups.

Place the cursor on a cell to view the policy for a given source scalable group and a destination scalable group. The color of a cell is based on the policy that applies to that cell. The following colors indicate which policies are applied to each cell:

- **Permit**: Green
- **Deny**: Red
- **Custom**: Gold
- **Default**: Gray

Place the cursor on the **Permit**, **Deny**, **Custom**, or **Default** icon that is displayed at the top of the matrix to view the cells to which that policy is applied.

Click a cell to open the **Create Policy** or **Edit Policy** slide-in pane that allows you to create or edit the policies for the selected cell. The **Create Policy** slide-in pane shows the source and destination scalable groups as read-only fields. You can update the policy status and access contract.

You can create custom views of the policy matrix to focus only on the policies that you are interested. To do this, click the **View** drop-down list and choose **Create View**. While creating the custom view, you can specify the subset of scalable groups that you want to include in the custom view. You can save the custom views and edit them later, if required. Click the **View** drop-down list and choose **Manage Views** to create, edit, duplicate, or delete the custom views. The **Default View** shows all the source and destination scalable groups.

You can navigate through the matrix by dragging the matrix content area with the cursor or by using horizontal and vertical scroll bars. You can also use the mini-map to navigate through the matrix. The mini-map helps you to easily navigate through the matrix when the matrix size is large and it extends beyond the screen size. You can move and place the mini-map anywhere on your screen. The mini-map provides the whole matrix

view. The light gray portion in the mini-map represents the portion of the matrix that is currently displayed on your screen. You can drag that area to scroll through the matrix.

Note The mini-map is closed by default. Click the **Expand** icon to expand and view the mini-map.

The Matrix view highlights the cell and the corresponding row (source scalable group) and column (destination scalable group) when a cell is selected. The coordinates (source and destination scalable groups) of the selected cell are displayed near the matrix content area.

Click **Deploy** to deploy the updated policies on the network devices. When you click **Deploy**, Cisco DNA Center requests Cisco ISE to send notifications about the policy changes to the network devices.

You can use the **Filter** option to view a subset of the policy matrix, for a selected set of source and destination groups. You can create a filter to focus only on the policies that you are interested. To create the filter, select the source and destination groups that you want to include.

Cisco DNA Center integrates with Cisco ISE. Cisco ISE provides the runtime policy platform for providing policy download to the network devices on behalf of Cisco DNA Center. The TrustSec Workcenter user interface screens for Security Groups, Security Group Access Control Lists (SGACLs), and Egress Policy are displayed in Read-Only mode in Cisco ISE to prevent policy synchronization issues.

Policy Creation Overview

1. Define categorizations for your organization, or the portion of your organization that you plan to start with.
2. Create scalable groups for the categorizations that you identified.
3. Create access contracts for the types of network traffic you wish to control. There are predefined sample access contracts to Permit or Deny all traffic, and also some example contracts showing more specific traffic filtering. You can create additional, more granular access contracts based on specific application definitions.
4. Decide which categories of network users require access to particular network resources, such as application servers and connections to other networks.
5. Create access policies, associate a source group, a destination group, and an access contract, to define how traffic is allowed to flow from the source to the destination.

Create Scalable Groups

Before you begin

To perform the following task, you must be a Super Admin or Network Admin.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Group-Based Access Control** > **Scalable Groups**.

Step 2 Click **Create Scalable Group**.
The **Create Scalable Group** slide-in pane appears.

Step 3 In the **Create Scalable Group** slide-in pane, enter a name and description (optional) for the scalable group.

Note The following characters are supported for the **Name** field:

- alphanumeric characters
- underscore (_)

The scalable group name must start with an alphabetic character.

Cisco DNA Center generates the tag value. You can update this value, if necessary. An error message is displayed if the value that you specify is already used by an existing scalable group. The valid range is from 2 to 65519.

Step 4 Choose the **Virtual Networks** to be associated with this scalable group from the drop-down list. By default, the default virtual network (`DEFAULT_VN`) is selected.

Step 5 Check the **Propagate to ACI** check box if you want the scalable group to be propagated to Cisco Application Centric Infrastructure (ACI).

Step 6 Click **Save**.

The **Scalable Groups** window displays the scalable group name, tag value, assigned virtual networks, and associated policies. You can also view the sample scalable groups in this window. You can use or delete those scalable groups.

You can edit or delete the scalable groups from the **Scalable Groups** window. Click the **Scalable Group Name** link to view the details of a scalable group. Click **Edit** in the **View Scalable Group** window to update the scalable group details. When you click **Deploy**, Cisco DNA Center requests Cisco ISE to send notifications about the changes to the network devices.

Click the link in the **Policies** column of a scalable group to view the access control rules that use that scalable group and the policy to which it belongs. You cannot delete a scalable group if it is used in any access policy.

An orange triangle icon is displayed next to a scalable group if synchronization with Cisco ISE is not completed.

Cisco ISE supports packets coming from ACI to the TrustSec domain by synchronizing the Internal Endpoint Groups (IEPGs) and creating correlating read-only scalable groups in Cisco ISE. These scalable groups are displayed in the **Scalable Groups** window with the value `ACI` in the **Created In** column. You cannot edit or delete the scalable groups that are learned from ACI, but you can use them in the policies.

The **Associated Contracts** column shows the associated ACI-learned contracts for the scalable groups that are learned from ACI. Click the link displayed in the **Associated Contracts** column to view the details about the associated contracts.

When an IEPG is updated in ACI, the corresponding scalable group configuration is updated in Cisco ISE. A new EEPG is created in ACI, when a scalable group is created in Cisco ISE.

Note You cannot create a scalable group with the name "ANY" or tag value 0xFFFF/65535. Scalable Group ANY/65535 is a reserved internal scalable group that is used for the Cisco DNA Center default policy.

While synchronizing the scalable groups in Cisco DNA Center with Cisco ISE:

- If a scalable group is present in Cisco DNA Center and is not present in Cisco ISE, it is created in Cisco ISE.

- If a scalable group is present in Cisco ISE and is not present in Cisco DNA Center, it is created in Cisco DNA Center.
- If the scalable group name is same in both Cisco DNA Center and Cisco ISE, but the description and ACI data are different, Cisco DNA Center is updated with the data specified in Cisco ISE.
- If the scalable group name is same in Cisco DNA Center and Cisco ISE, but the tag values are different, a new scalable group with the tag value specified in Cisco ISE is created in Cisco DNA Center. The name of the existing scalable group in Cisco DNA Center is updated with the suffix `_DNAC`.
- If the tag value is same but the scalable group name is different, the scalable group name in Cisco DNA Center is updated with the name specified in Cisco ISE.

Create Access Contracts

An access contract is a set of rules that controls the type of network traffic that is allowed to pass between the source and destination scalable groups. Access contracts define the actions (permit or deny) performed when the traffic matches a network application, protocol, and port.

Note Security Group Access Control List (SGACL) in Cisco ISE is called `Access Contract` in Cisco DNA Center.

Before you begin

To perform the following task, you must be a Super Admin or Network Admin.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Group-Based Access Control** > **Access Contracts**.

Step 2 Click **Create Access Contract**.

Step 3 In the **Create Access Contract** slide-in pane, enter a name and description for the contract.

Step 4 Create the traffic filter rules:

- From the **Action** drop-down list, choose **Deny** or **Permit**.
- From the **Application** drop-down list, choose the application for which you want to apply that action. The port and protocol are automatically selected based on the application that you select.

  If you want to specify the transport protocol, source port, and destination port, choose the **Advanced** option from the **Application** drop-down list.

You can create multiple rules. To create multiple rules for a contract, click the + symbol and choose the settings for the **Action** and **Application** columns. The rules are checked in the order in which they are listed in the contract. Use the handle icon at the left end of a rule to drag and change the order of the rule.

You can enable or disable logging for any traffic filter rule (including the default action) by using the **Logging** toggle. Logging is disabled by default. When logging is enabled, the network device sends a syslog message when the traffic filter rule is hit. This might be helpful in troubleshooting and initial testing of a policy. However, we recommend that you use this option sparingly, because it might have a resource and performance impact on the network devices.

Step 5 From the **Default Action** drop-down list, choose **Deny** or **Permit**.

You can enable logging for the default action, if required.

Step 6 Click **Save**.

You can view, create, duplicate, update, and delete contracts from the **Access Contracts** listing window.

You can also view the sample contracts in the **Access Contracts** window. You can use or delete those sample contracts. However, you cannot delete the default contracts (Permit IP, Deny IP, Permit_IP_Log, and Deny_IP_Log).

Click the **Contract Name** link in the **Access Contracts** window to view the details of a contract. Click **Edit** in the **View Contract** window to edit the contract details.

An orange triangle icon is displayed next to a contract if synchronization with Cisco ISE is incomplete.

The contracts that are learned from ACI are displayed in the **Access Contracts** window with the value `ACI` in the **Created In** column. You cannot edit or delete the contracts that are learned from ACI, but you can use them in the policies while using the ACI-learned scalable groups. While creating or updating a policy from the Matrix view, if you select an ACI-learned scalable group as the destination group, the associated contracts are displayed in the **Preferred Contracts** tab. You can view all the contracts in the **All Contracts** tab.

You can view the number of rules used in each contract in the **Rules Count** column.

Click the link in the **Policies** column of a contract to view the policies that use that contract.

You cannot delete a contract if it is used in a policy. You must delete the contract from that policy before you delete the contract.

When you update the scalable groups, contracts, or policies, you must deploy the changes on the network devices. If you update the policies and do not deploy the updated policies, notifications about the policy changes are not sent to the network devices and the policies that are currently active in the network may not be consistent with the policy information displayed in Cisco DNA Center. To resolve this situation, you must deploy the updated policies on the network devices.

You can duplicate an existing contract and create a new contract by editing the required details. When you duplicate a contract, all information in the existing contract is copied and the copied contract has the existing contract name with the string `Copy` appended at the end.

You can use the **Filter** option to search for the contracts that you look for.

While synchronizing the access contracts in Cisco DNA Center with Cisco ISE:

- If a contract is present in Cisco DNA Center and is not present in Cisco ISE, it is created in Cisco ISE.
- If a contract is present in Cisco ISE and is not present in Cisco DNA Center, it is created in Cisco DNA Center.
- If the contract name is the same in Cisco DNA Center and Cisco ISE, but the description and traffic rule content are different, Cisco DNA Center is updated with the data specified in Cisco ISE.
- If the contract name and rule are the same, but the description is different, Cisco DNA Center is updated with the description specified in Cisco ISE.
- Text SGACL command lines in Cisco ISE are migrated as content that cannot be parsed. You can edit these contracts, but Cisco DNA Center does not parse them or check syntax. The changes that you make in Cisco DNA Center are reflected in Cisco ISE.

- If a policy has multiple SGACLs in Cisco ISE, those contracts are migrated as default policies in Cisco DNA Center.

Create Group-Based Access Control Policy

Scalable groups and access contracts are the basic building blocks of an access control policy. While creating an access control policy, you can use the scalable groups and contracts that you have created before, or create new scalable groups and contracts while creating the policy.

If you want to specify the network resources that can be accessed from a specific source group, you can create an access control policy with a single source and multiple destination groups. On the other hand, if you want to specify the source groups that are permitted to access a particular network resource, you can create an access control policy with a single destination and multiple source groups.

For example, if you want to specify the network resources that can be accessed by the users associated with the *Contractors* source scalable group, you can create an access control policy with a single source and multiple destination groups. If you want to specify the source groups that are permitted to access the *Finance Servers* destination scalable group, you can create an access control policy with a single destination and multiple source groups.

Group-based access control policies can also be created or updated based on the traffic flows for a given source and destination group pair.

To create a group-based access control policy, use the following procedure.

Step 1 From the **Policy List** or **Matrix** view, click **Create Policies**.

Step 2 To create an access control policy with a single source and multiple destination groups, click **Source to Destination(s)** and complete these steps:

a) Click the radio button next to the source scalable group that you want to select. If the scalable group that you need does not exist, click **Create Scalable Group** to create a new scalable group. For more information, see Create Scalable Groups, on page 249.

b) Click **Next**.

c) Choose the destination scalable groups to map to the selected source scalable group.

You can view the scalable group details and edit the scalable groups, if necessary.

If a policy already exists between the source and destination, an orange triangle icon is displayed near a scalable group.

d) Click **Next**.

e) Click the radio button next to the contract that you want to select. If the contract that you need does not exist, click **Create Contract** to create a new contract. For more information, see Create Access Contracts, on page 251.

You can view and edit the contract details, if necessary.

Note You can choose only one contract for a policy.

f) Click **Next**.

The **Summary** window lists the policies that are created based on the selected scalable groups and contract.

g) Click **Save**.

Step 3 To create an access control policy with a single destination and multiple source groups, click **Destination to Source(s)** and complete the following steps:

a) Click the radio button next to the destination scalable group that you want to select. If the scalable group that you need does not exist, click **Create Scalable Group**.

b) Click **Next**.

c) Choose the source scalable groups to map to the selected destination scalable group.

You can view the scalable group details and edit the scalable groups, if necessary.

If a policy already exists between the source and destination, an orange triangle icon is displayed near a scalable group.

d) Click **Next**.

e) Click the radio button next to the contract that you want to select. If the contract that you need does not exist, click **Create Contract**.

You can view and edit the contract details, if necessary.

Note You can choose only one contract for a policy.

f) Click **Next**.

The **Summary** window lists the policies that are created based on the selected scalable groups and contract.

g) Click **Save**.

Note You can toggle between the **List** view and the **Drag and Drop** view using the **Toggle** button in the top-right corner of the Scalable Group listing area. The **Drag and Drop** view allows you to drag and drop the scalable groups to the **Source** and **Destination** fields while creating the access control policy. However, only the first 50 scalable groups are listed in the **Drag and Drop** view. You can use the **Drag and Drop** view if you have a smaller number of scalable groups (up to 50). If you have more than 50 scalable groups, use the **List** view to view them all.

To create or modify a group-based access control policy based on the traffic flows:

1. From the policy matrix view, click the cell for which you want to create or modify the group-based access control policy.
2. In the **Policy Details** slide-in pane, click **View Traffic Flows**.

   In the **View Traffic Flows** slide-in pane, you can see the rules for the selected contract or the default policy in the left pane. You can view the traffic flows that match any selected rule in the right pane.
3. Click **View Traffic** in the Default Action rule to see the list of flows that match that rule. While modifying an existing policy using access contracts with additional rules, you can use the **View Traffic** option for any rule to see the list of flows matching that rule.
4. For policies that are using the Default Action rule (with no explicitly selected access contract), you can select an access contract or create a new access contract to be used by that policy.

   For policies with access contract PERMIT or DENY, you can select an access contract or create a new access contract to be used by that policy.

   For policies with custom access contract, you can edit the selected access contract.

   While saving a newly created or edited contract, you have the following options:

- Save the changes to the existing contract. Changes affect all policies that reference the contract.
- Save the changes as a new contract. Changes are applied only to the current policy.
- Save the changes as a new contract. Changes are not applied to any policy.

While synchronizing the policies in Cisco DNA Center with Cisco ISE:

- If a policy is present in Cisco DNA Center and is not present in Cisco ISE, it is created in Cisco ISE.
- If a policy is present in Cisco ISE and is not present in Cisco DNA Center, it is created in Cisco DNA Center.
- If a policy contract is different in Cisco ISE, Cisco DNA Center is updated with the contract specified in Cisco ISE.
- Policy mode information (Enabled, Disabled, or Monitor) is also imported from Cisco ISE.

Cisco ISE has an option to allow multiple SGACLs for a single policy (this option is not enabled by default in Cisco ISE). Cisco DNA Center does not support the use of multiple access contracts for a single policy. During policy synchronization, if a policy in Cisco ISE has multiple SGACLs, the Cisco DNA Center administrator is given the option to change that policy to have no contract selected (to use the default policy). The administrator can select a new or existing access contract for that policy after the policy synchronization is complete.

Cisco Group-Based Policy Analytics

The following sections provide detailed information about Cisco Group-Based Policy Analytics.

Overview

Group-Based Policy Analytics enables you with insights, to create group-based policies by visualizing communications between assets, to assess the impact of introducing new access controls, and understand exactly which protocols you need to allow in the policies.

Cisco Group-Based Policy Analytics aggregates information on groups of assets on your network, and their communication to answer the following questions:

- Which groups are communicating with each other?
- What kind of communication is this?
- Which group does a given asset belong to?

Installation

You can purchase one of following types of licenses for Cisco DNA Center:

- Cisco DNA Essentials
- Cisco DNA Advantage
- Cisco DNA Premier

Cisco DNA Advantage and Cisco DNA Premier contain the Group-Based Policy Analytics package. This package consists of the following archives (.tar.gz files):

- Backend
- User Interface
- Summarizer Pipeline
- Aggregation definitions

Cisco Group-Based Policy Analytics is a part of Cisco DNA Center but, is not installed by default. In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Software Updates** > **Installed Apps**. Scroll down to **Group-Based Policy Analytics** under **Policy Applications**. Click **Install** to install the application.

Hardware and Software Compatibility

Platform Support

Cisco Group-Based Policy Analytics is supported on the following hardware platforms:

- 44 cores, single node or three-node cluster
- 56 cores, single node or three-node cluster
- 112 cores, single node or three-node cluster

These platforms must meet the performance and scalability requirements mentioned here.

For details about the supported hardware, see Cisco UCS M4 appliances or Cisco UCS M5 appliances.

The following table lists the performance metrics that Cisco DNA Center and Cisco Group-Based Policy Analytics support on each of the core platforms. The NetFlow metrics were introduced by Cisco Group-Based Policy Analytics.

Table 41: Performance Metrics

Metric	44 cores, three nodes	56 cores	112 cores
Devices (NADs)	5000 1000 switches or 1000 routers or a combination of both; 4000 APs	8000 2000 switches or 2000 routers or a combination of both; 6000 APs	18,000 5000 switches or 5000 routers or a combination of both; 12,000 APs
Clients (endpoints)	25,000 20,000 wireless; 5,000 wired	40,000 30,000 wireless; 10,000 wired	100,000 60,000 wireless; 40,000 wired
NetFlows per sec	30,000	48,000	120,000

Device Support

You must enable NetFlow to use Cisco Group-Based Policy Analytics. The following table shows the various ways in which NetFlow can be enabled on different network devices.

Table 42: Device Support

Network Devices	Series	NetFlow Configurable in telemetry section of Network Settings in Cisco DNA Center UI (Flexible NetFlow or Application Visibility and Control Based NetFlow)	NetFlow Configurable using the template editor tool in the Cisco DNA Center UI (Flexible NetFlow or Application Visibility and Control Based NetFlow)	NetFlow Collection in Fabric Deployment	NetFlow Collection in Nonfabric Deployment
Routers	Cisco 1000 Series Integrated Services Routers (ISR1K)	Yes	Yes	Yes	Yes
	Cisco 4000 Series Integrated Services Routers (ISR4K)	Yes	Yes	Yes	Yes
	Cisco Cloud Services Router 1000v Series (CSR 1000v)	Yes	Yes	Yes	Yes
	Cisco 1000 Series Aggregation Services Routers (ASR1K)	Yes	Yes	Yes	Yes
Switches	Cisco Catalyst 9200 series	Yes	Yes	Yes	Yes
	Cisco Catalyst 9300 Series	Yes	Yes	Yes	Yes
	Cisco Catalyst 9400 Series	Yes	Yes	Yes	Yes
	Cisco Catalyst 9500 Series	No	Yes	Yes	Yes
	Cisco Catalyst 9600 Series	No	Yes	Yes	Yes
	Cisco Catalyst 2k series	No	Yes	NA	Yes
	Cisco Catalyst 3560 series	No	Yes	NA	Yes
	Cisco Catalyst 3650 series	No	Yes	Yes	Yes
	Cisco Catalyst 3850 series	No	Yes	Yes	Yes
	Cisco Catalyst 4k series	No	Yes	Yes	Yes
	Cisco Catalyst 6500 Series Switches	No	Yes	Yes	Yes
	Cisco Catalyst 6800 Series Switches	No	Yes	Yes	Yes

Network Devices	Series	NetFlow Configurable in telemetry section of Network Settings in Cisco DNA Center UI (Flexible NetFlow or Application Visibility and Control Based NetFlow)	NetFlow Configurable using the template editor tool in the Cisco DNA Center UI (Flexible NetFlow or Application Visibility and Control Based NetFlow)	NetFlow Collection in Fabric Deployment	NetFlow Collection in Nonfabric Deployment
Wireless Controllers	Cisco 3504 Wireless Controller (AireOS-Based)	Yes	Yes	No	Yes, only central switching SSID
	Cisco 5520 Wireless Controller (AireOS-Based)	Yes	Yes	No	Yes, only central switching SSID
	Cisco 8540 Wireless Controller (AireOS-Based)	Yes	Yes	No	Yes, only central switching SSID
	Cisco Catalyst 9800 based controller	Yes	Yes	Yes	Yes

Cisco ISE

Cisco ISE 2.4 Patch 7 and later, Cisco ISE 2.6 Patch 1 and later, and Cisco ISE 2.7 and later are supported.

Cisco Stealthwatch

Cisco Stealthwatch 7.x or later is supported.

Browser Support

Cisco Group-Based Policy Analytics is compatible with 64-bit Windows, Macintosh, and Linux systems with the following web browsers:

- Google Chrome: Version 73.0 or later
- Mozilla Firefox: Version 65.0 or later

Navigate the Cisco Group-Based Policy Analytics Home Page

In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Group-Based Access Control** > **Analytics**.

The **View Traffic for** numbers for Scalable Groups, Cisco ISE Profiles, and Stealthwatch Host Groups indicate the number of groups that consist of at least one endpoint that initiated traffic in the past 14 days.

Note The **View Traffic for** numbers are not the numbers of configured groups. These numbers do not include the groups in which all the endpoints are simply responding to requests (for example, acting solely as a server).

Figure 5: Group-Based Policy Analytics Home Page

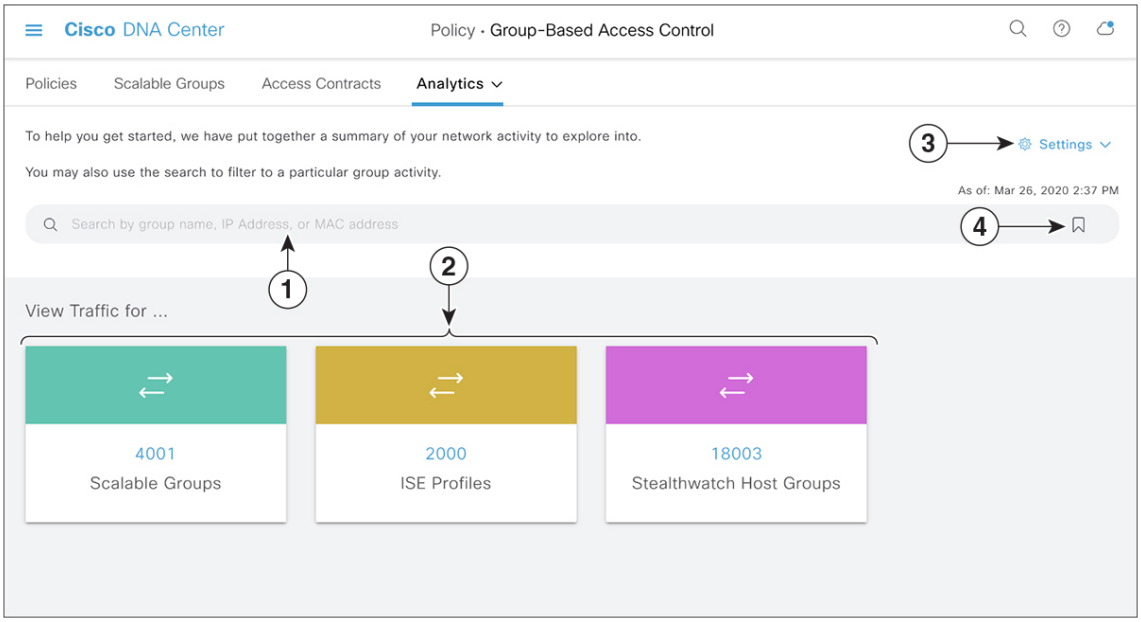
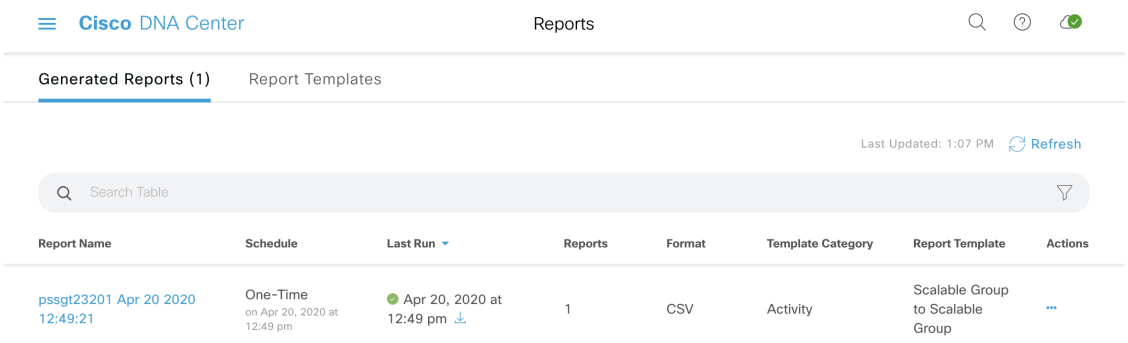


Figure 1 shows the main elements in the Cisco Group-Based Policy Analytics home page.

1. Use the **Search** field to search for various groups, IP addresses, and MAC addresses. Click Use Search to know more about the Search field.
2. When you click a number displayed in any of the boxes, it takes you to the Multiple Groups to Multiple Groups window with the selected box group as the source, and Scalable Groups as the destination.
3. You have the following options:
   - **Configuration**: Click this link to configure or edit collectors such as Cisco ISE, Cisco Stealthwatch, or NetFlow.
   - **Data and Reports**: Clicking this link, opens the **Reports** window in Cisco DNA Center, as shown in the following image. You can view the status of reports here. You can also edit, duplicate, run, or download the reports.



4. Click the  icon to load a saved filter or save the current search.

Understand Connectors

Cisco Group-Based Policy Analytics gathers telemetry from the following sources, which are also known as connectors. You can configure the connectors either by following the Initial Configuration of Cisco Group-Based Policy Analytics, on page 261 workflow, or by choosing **Policy** > **Group-Based Access Control** > **Analytics** > **Settings** > **Configuration**.

Group Data Connectors

The group data connectors collect information about groups that assets are classified into. Cisco ISE and Cisco Stealthwatch are group data connectors.

- **Cisco ISE**

  Cisco ISE is a next-generation identity and access control policy platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations. Cisco ISE is installed on a virtual machine, a physical machine or a combination of both. Cisco ISE uses the Cisco Platform Exchange Grid (pxGrid) service as the publisher-subscriber module for sharing SessionDirectory, Scalable Groups, and other information. PxGrid uses a query interface and supports bulk download. Users on the network are authenticated, authorized, and accounted for, and a session directory is maintained. User events are published to the connectors that are subscribed to the SessionDirectory service. Other services like scalable group notifications can also be subscribed to.

  User identity and device information obtained during authentication is used to classify the packets, as they enter the network. This packet classification is maintained by tagging packets when they enter the network so that they can be properly identified for applying security and other policy criteria along the data path. The tag, also called the Scalable Group Tag (SGT), allows Cisco ISE to enforce access control policies by enabling the network device to act upon the SGT to filter traffic.

  In addition, Cisco ISE collects information about endpoints connected to your network, such as the type of device, OS, OS version, IP address and other attributes. These are called ISE profiles.

  The Cisco ISE connector provides Cisco Group-Based Policy Analytics with SGT definitions and profiles from Cisco ISE.

- **Cisco Stealthwatch**

  Cisco Stealthwatch is a network-based anomaly detection system which provides advanced threat detection, accelerated threat response and network traffic security analysis. The Cisco Stealthwatch connector obtains the host groups that are configured on Cisco Stealthwatch. A host group is essentially a virtual container containing multiple host IP addresses or IP address ranges that have similar attributes, such as location, function, or topology.

Communication Connector

The communication connector helps gather information on traffic seen between groups, that could be leveraged in Group-Based Policy decisions. This is done using NetFlow from network devices managed by Cisco DNA Center. NetFlow is collected and aggregated natively by Cisco DNA Center.

Initial Configuration of Cisco Group-Based Policy Analytics

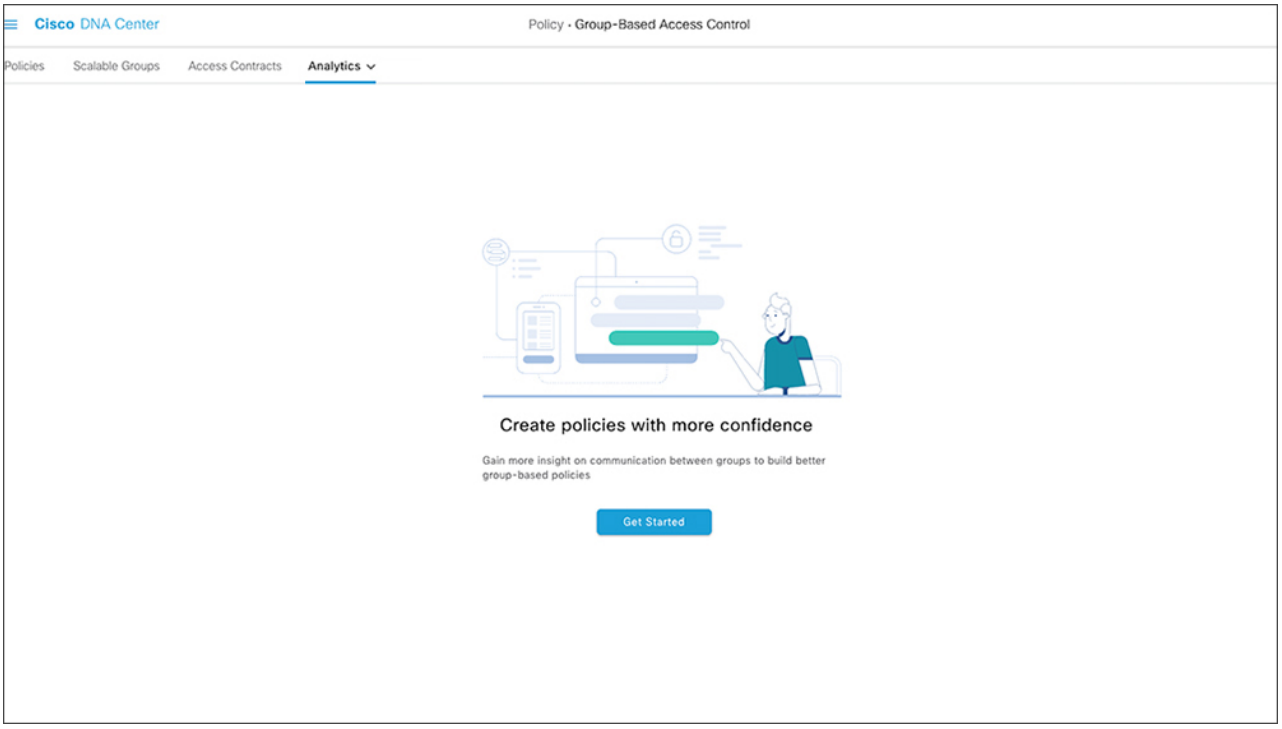
This workflow helps you configure the data connectors that are required to collect telemetry data related to network activity, and endpoints from specific sources such as Cisco ISE, Cisco Stealthwatch, and NetFlow. This task is useful when you are configuring data connectors for the first time.

Before you begin

Cisco DNA Center must have Cisco Group-Based Policy Analytics installed.

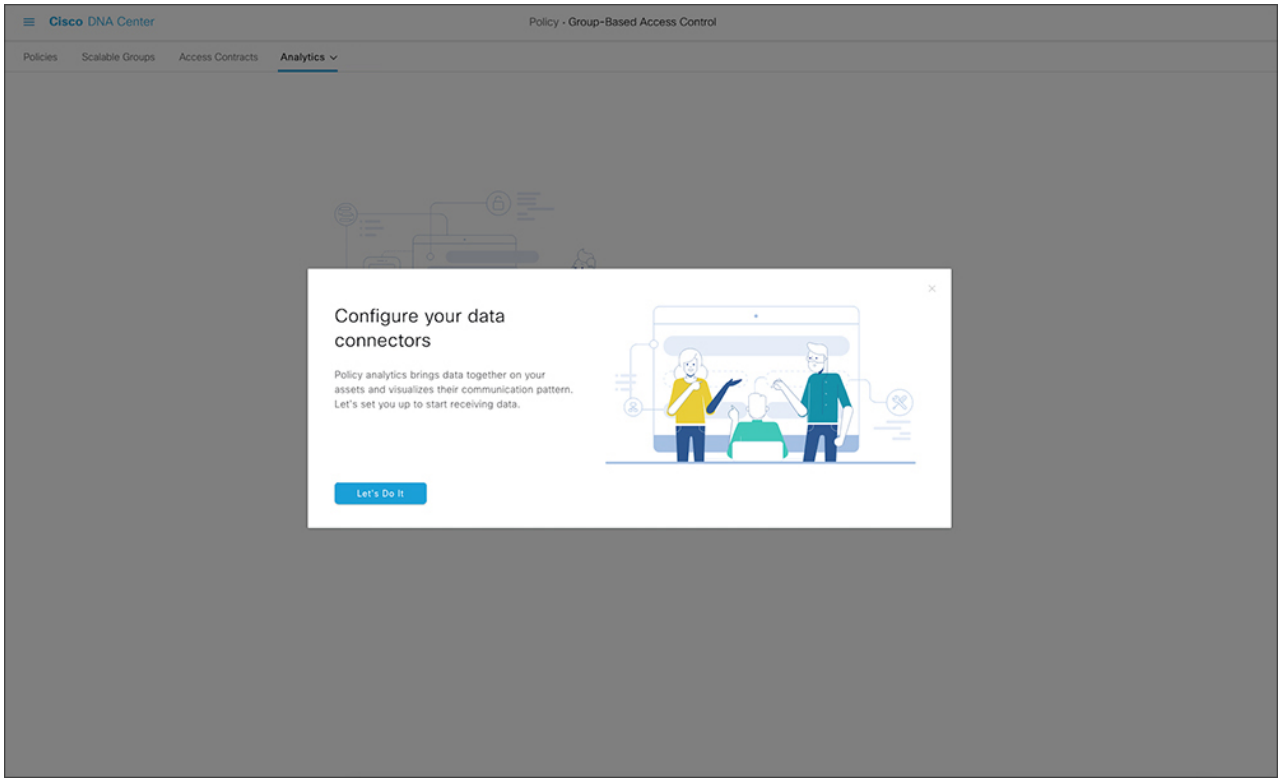
Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Group-Based Access Control** > **Analytics**. The **Create policies with more confidence** window appears:

Figure 6: Create policies with more confidence



Step 2 Click **Get Started**.
The **Configure your data connectors** window opens.

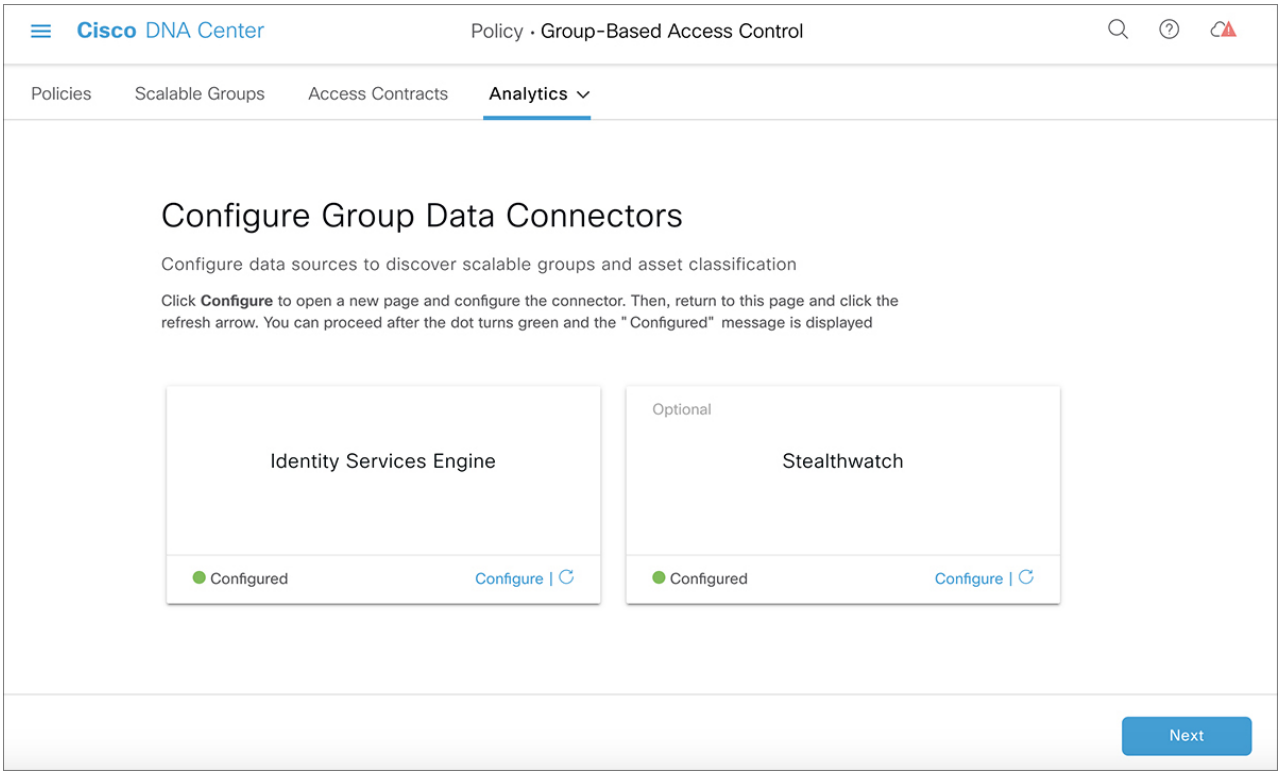
Figure 7: Configure Your Data Connectors



Step 3 Click **Let's Do It**.

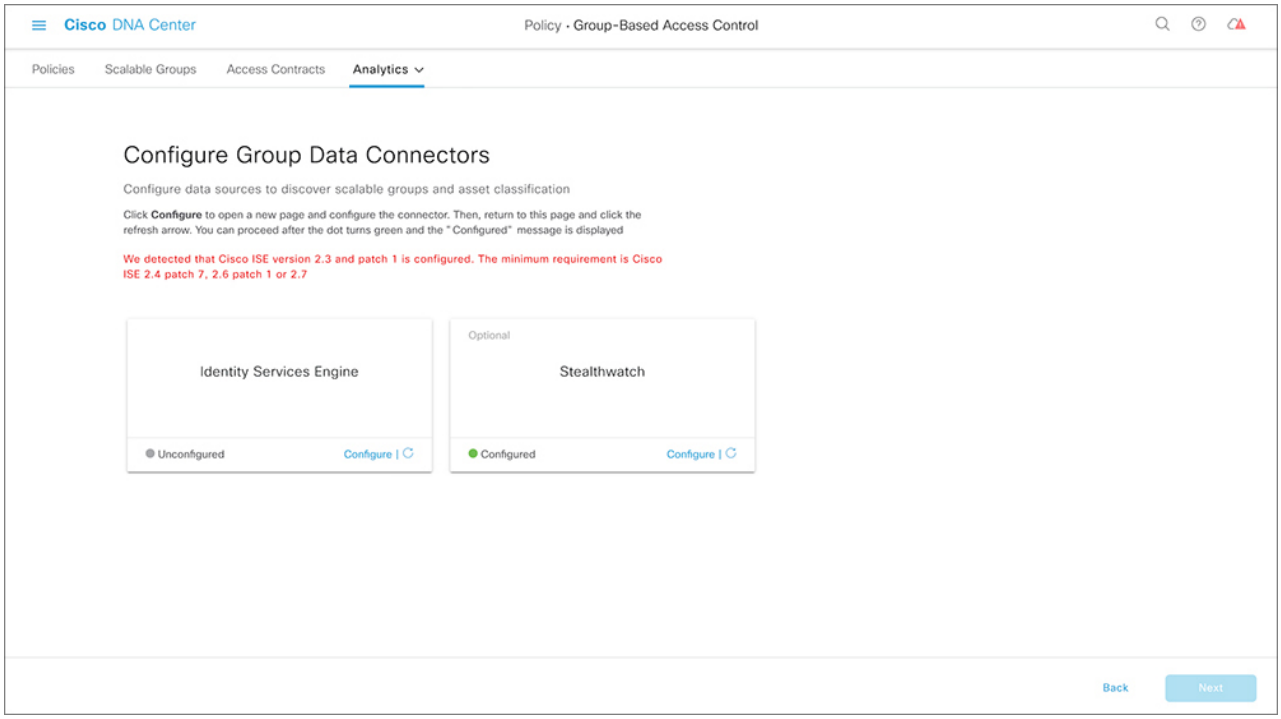
The **Configure Group Data Connectors** window opens.

Figure 8: Configure Group Data Connectors



If the Cisco ISE version installed on Cisco DNA Center is earlier than the version required for running Cisco Group-Based Policy Analytics, an error is displayed:

Figure 9: Cisco ISE Version Requirement

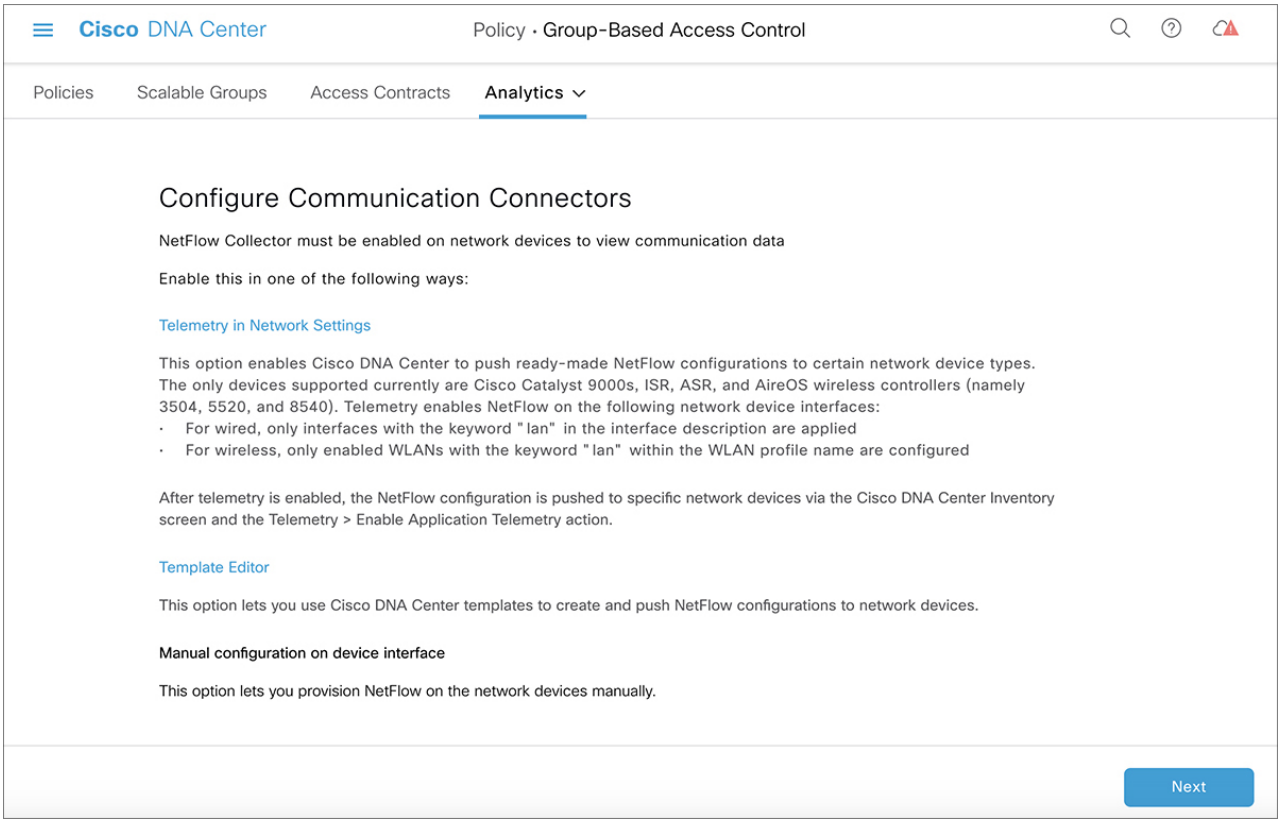


Step 4 Click **Configure** at the bottom of the connector you want to configure.
A new window opens, redirecting you to the Cisco DNA Center **Settings** window, where you can configure the required connectors. You must configure the Cisco ISE connector. Configuring the Cisco Stealthwatch connector is optional. (Both the Cisco ISE connector and the Cisco Stealthwatch connector configuration windows are part of the Cisco DNA Center GUI.)

Step 5 Close the **Settings** window. You will see a green dot next to the **Configure** option for the successfully configured connectors in the **Configure Group Data connectors** window.

Step 6 Click **Next**.

Figure 10: Configure Communication Connectors

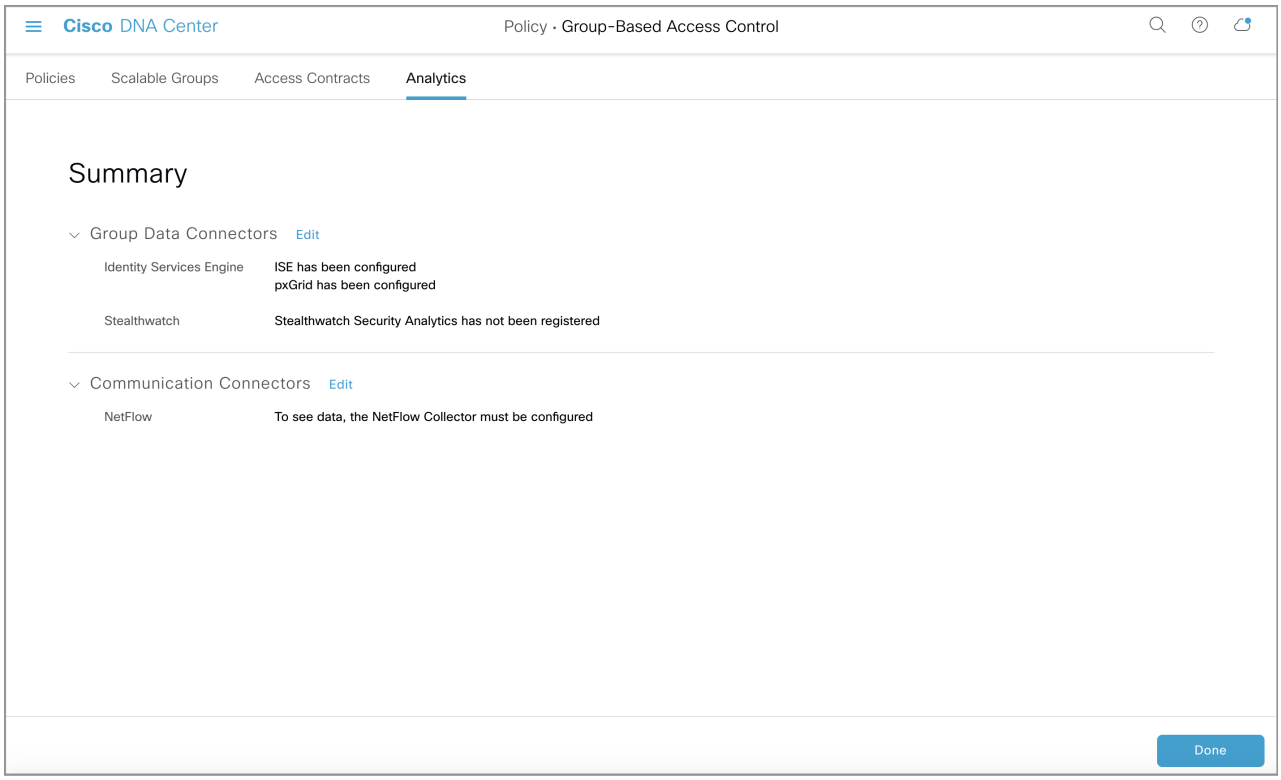


The **Configure Communication Connectors** window opens.

Step 7 There are three ways to configure the communication connector (NetFlow).You can provision NetFlow on the Cisco DNA Center device interface manually, click **Template Editor** to configure NetFlow using the **Template Editor Tool** in Cisco DNA Center, or click **Telemetry in Network Settings** to configure NetFlow in the telemetry section of network settings. To know more, see the Device Support section in Hardware and Software Compatibility, on page 256.

Step 8 Click **Next**.

Figure 11: Summary



The **Summary** window, which shows the configuration details of the connectors, is displayed.

Step 9 Click **Done** to start discovering your groups and endpoints.

Explore Groups and Endpoints

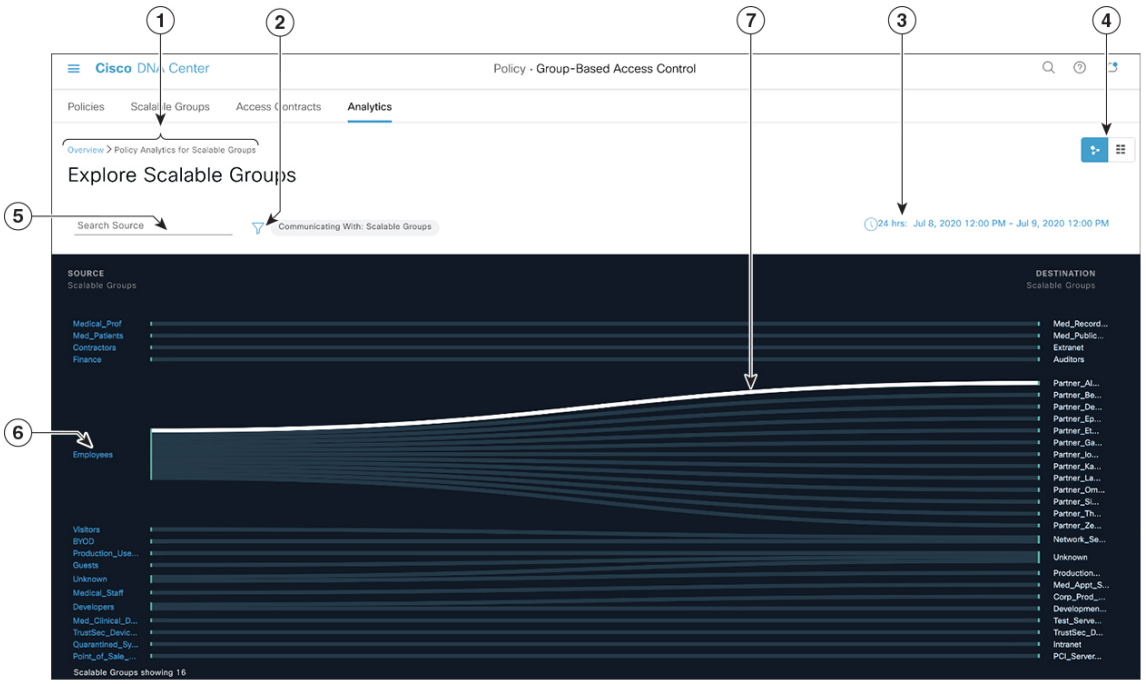
The following section provides information about the different ways to visualize traffic between different groups.

Multiple Groups to Multiple Groups

Scalable Groups to Scalable Groups: Chart View

When you click the number displayed in the **Scalable Groups** box, from the home page, the **Explore Scalable Groups** window is displayed. In this window, you can see a summary of all the group-to-group communication among Scalable Groups. By default, the time range for this visual is the last available 24 hours of data. Note that this is different from the time range mentioned in the home page, where it is set to the last 14 days. The chart shows the top 25 source Scalable Groups and their corresponding interactions, starting with the source Scalable Group with the highest number of unique flows within the given time period and so on. The following section describes the main elements in this view:

Figure 12: Scalable Groups to Scalable Groups: Chart View

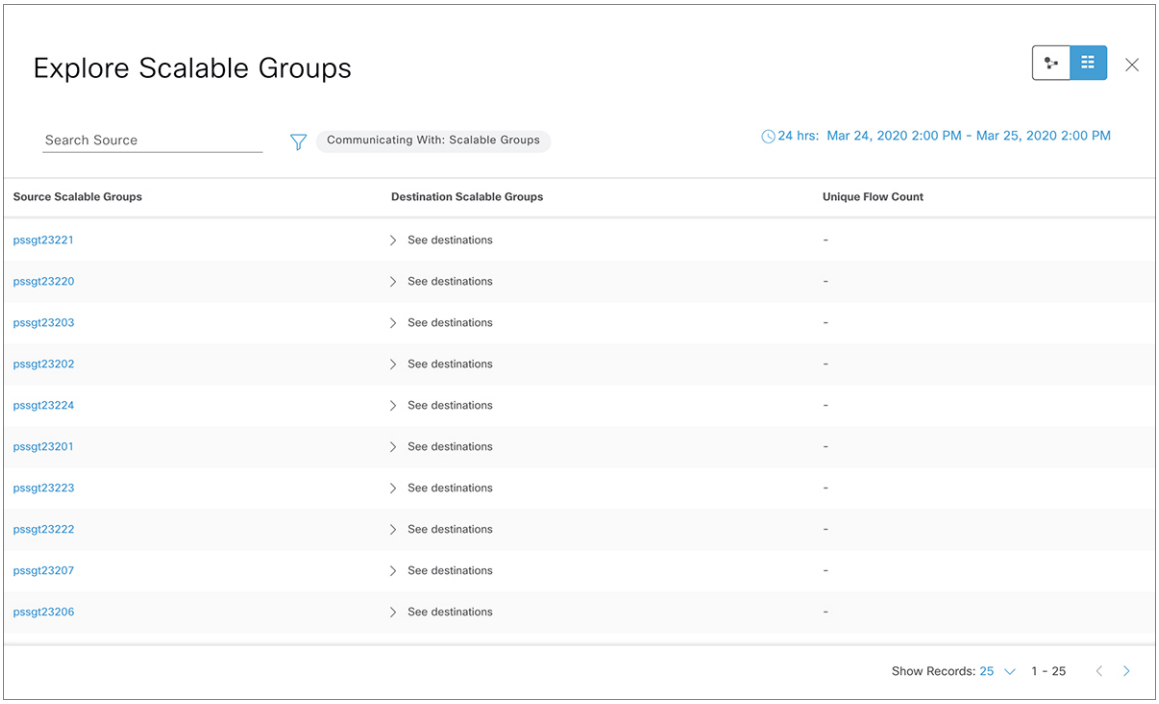


1. Follow the breadcrumb, to go back to the Navigate the Cisco Group-Based Policy Analytics Home Page.
2. Click the icon to choose the destination category other than Scalable Groups.
3. Set the date and time using the Date and Time Selector.
4. Click the icon to display the chart view, or to display the table view.
5. Click and type a search term here to narrow down the source Scalable Group list. If a Scalable Group contains your search term, it will be displayed.
6. Click a source group to view the Single Group to Multiple Groups window.
7. When you hover your cursor over a link, the link is highlighted and a tooltip shows the number of unique traffic flows. Clicking the link takes you to the Single Group to Single Group window.

Scalable Groups to Scalable Groups: Table View

The following window is displayed when you click the icon:

Figure 13: Scalable Groups to Scalable Groups: Table View

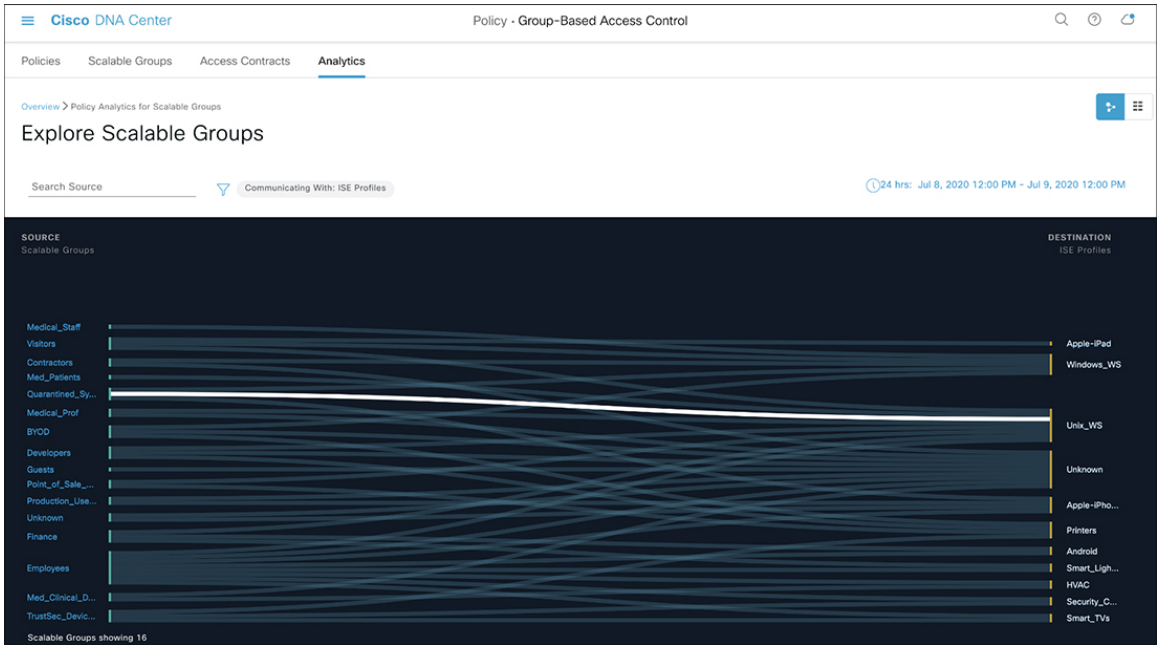


If you click the **See destinations** link on a particular row, it opens a window showing all the destination Scalable Groups for the selected source Scalable Group, and the unique flow count for each destination Scalable Group. The rest of the elements on this window are the same as that displayed in the chart view.

ISE Profiles to Scalable Groups

When you click the number displayed in the **ISE Profiles** box, from the home page, the **Explore ISE Profiles** window is displayed. In this window, you can see a summary of all the communication from ISE Profiles as the source and Scalable Groups as the destination.

Figure 14: ISE Profiles to Scalable Groups: Chart View

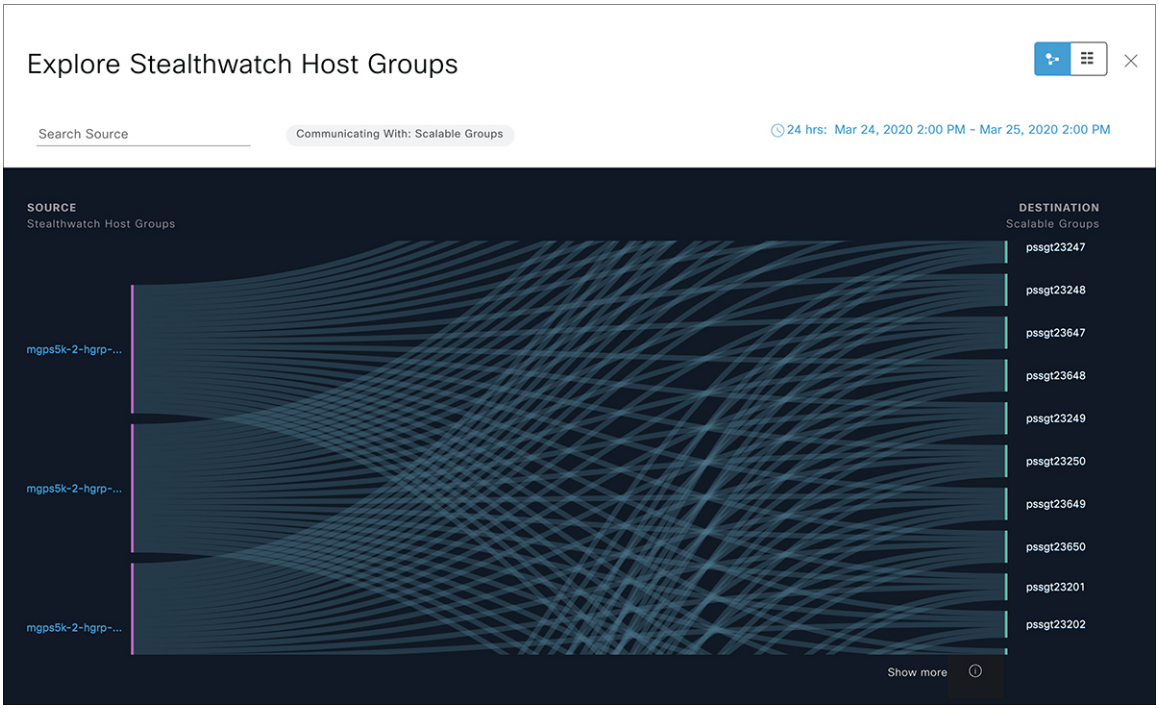


In order to focus on group-based policy decisions, either the source or destination category must be Scalable Groups in this view. In the above chart, since the source was chosen as ISE Profiles, the destination category must be Scalable Groups. Hence there is no need for the icon in this view.

Stealthwatch Host Groups to Scalable Groups

When you click the number displayed in the **Stealthwatch Host Groups** box from the home page, the **Explore Stealthwatch Host Groups** window is displayed. In this window, you can see a summary of all the communication, with Stealthwatch Host Groups as the source and the Scalable Groups as the destination.

Figure 15: Stealthwatch Host Groups to Scalable Groups: Chart View



In order to focus on group-based policy decisions, either the source or destination category must be Scalable Groups in this view. In the above chart, since the source was chosen as Stealthwatch Host Groups, the destination category must be Scalable Groups. Hence there is no need for the icon in this view.

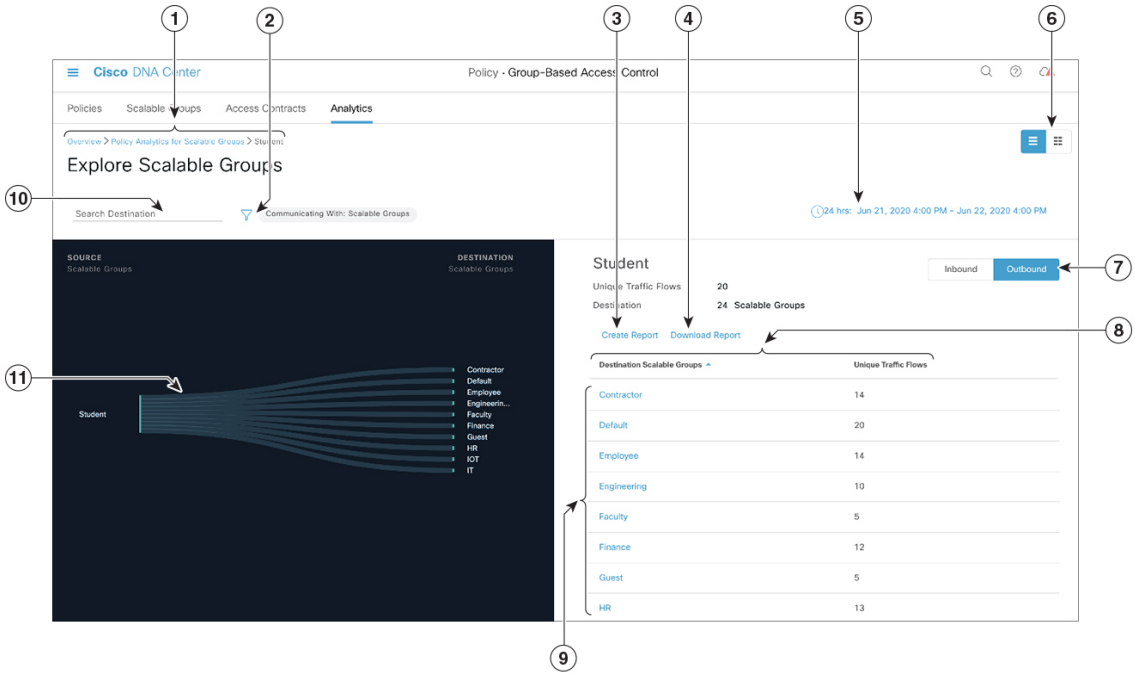
Single Group to Multiple Groups

Single Group to Multiple Groups: Outbound

This section explains the elements of the window, displayed to view the activity between a single source group and multiple destination groups. The source or the destination or both must be a Scalable Group. By default, the time range for this visual is the last available 24 hrs of data and the default number of links or records shown is 10.

The following example shows the Single Group to Multiple Groups window with both source and destination as **Scalable Groups**.

Figure 16: Single Group to Multiple Groups: Outbound

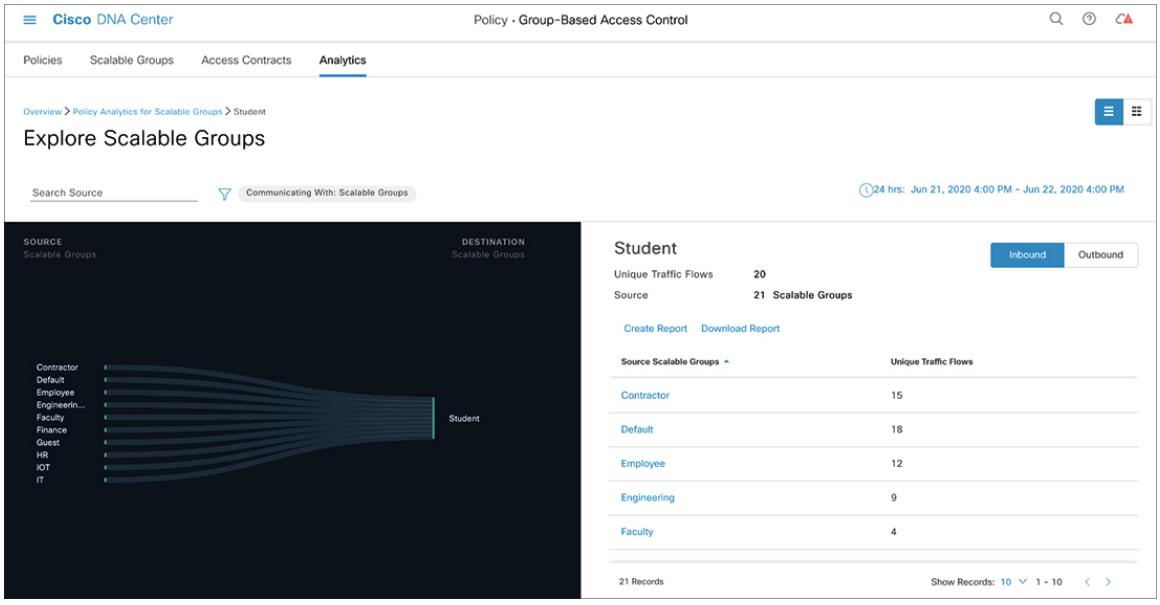


1. Follow the breadcrumb, to go back to the Multiple Groups to Multiple Groups.
2. Click the icon to choose the destination Scalable Group, ISE Profile, or Stealthwatch Host Group.
3. Click **Create Report** to generate a new report in CSV format with the information in this view. The **Reports** window opens where you can see the generated report. This window also provides you access to previously generated reports and allows you to download the reports.
4. Click **Download Report** to view the generated reports. The **Reports** window opens, where you can click the *download* icon under the **Last Run** column to download a report.
5. Set the date and time using the Date and Time Selector.
6. Click the icon to display the chart view or to view the table view.
7. **Outbound** displays the connections initiated by the selected scalable group. **Inbound** displays the connections initiated by another group to this scalable group.
8. Click any column to sort in ascending or descending order.
9. Click a group to view the Single Group to Single Group window with the corresponding destination as the selected group. The source group does not change.
10. Enter a search term here to narrow down the destination Scalable Group list. If a Scalable Group from this view contains your search term, it will be displayed.
11. When you hover your cursor over a link, it is highlighted, and a tooltip shows the number of unique traffic flows. If you click this link, it takes you to the Single Group to Single Group window.

Single Group to Multiple Groups: Inbound

If you click **Inbound**, it shows all the connections initiated by any group as the source and the selected Scalable Group as destination, as shown in the following image:

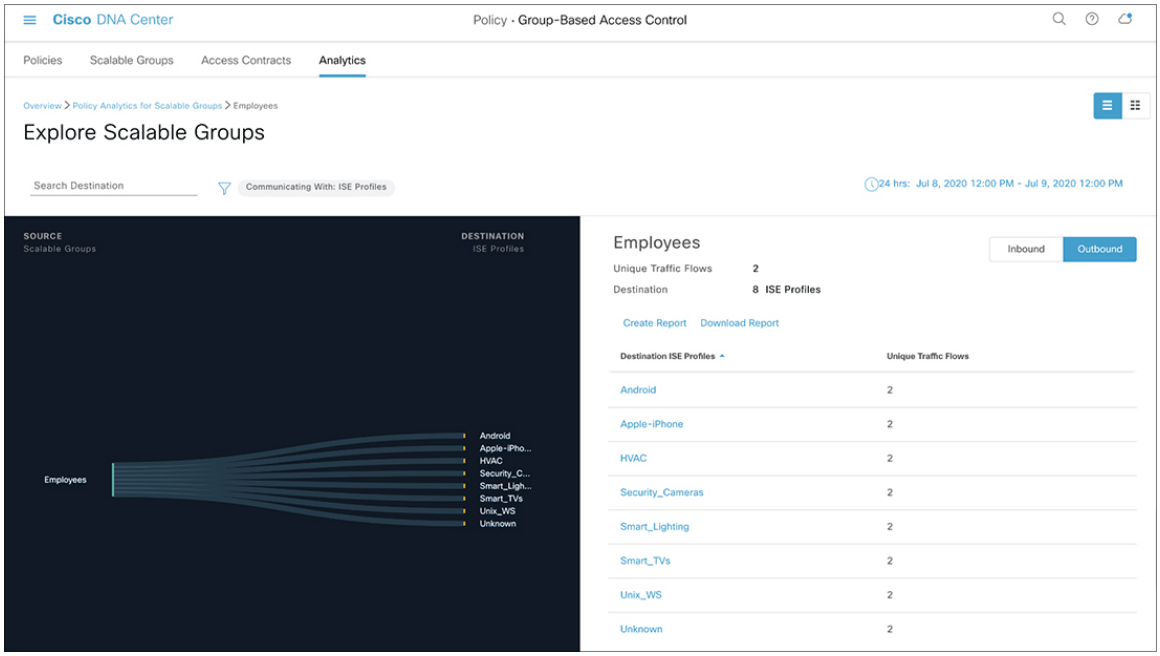
Figure 17: Single Group to Multiple Groups: Inbound



Single ISE Profile to Multiple Scalable Groups: Chart View

The following window is displayed when an ISE Profile is selected as the source and Scalable Groups is chosen as the destination in the outbound direction.

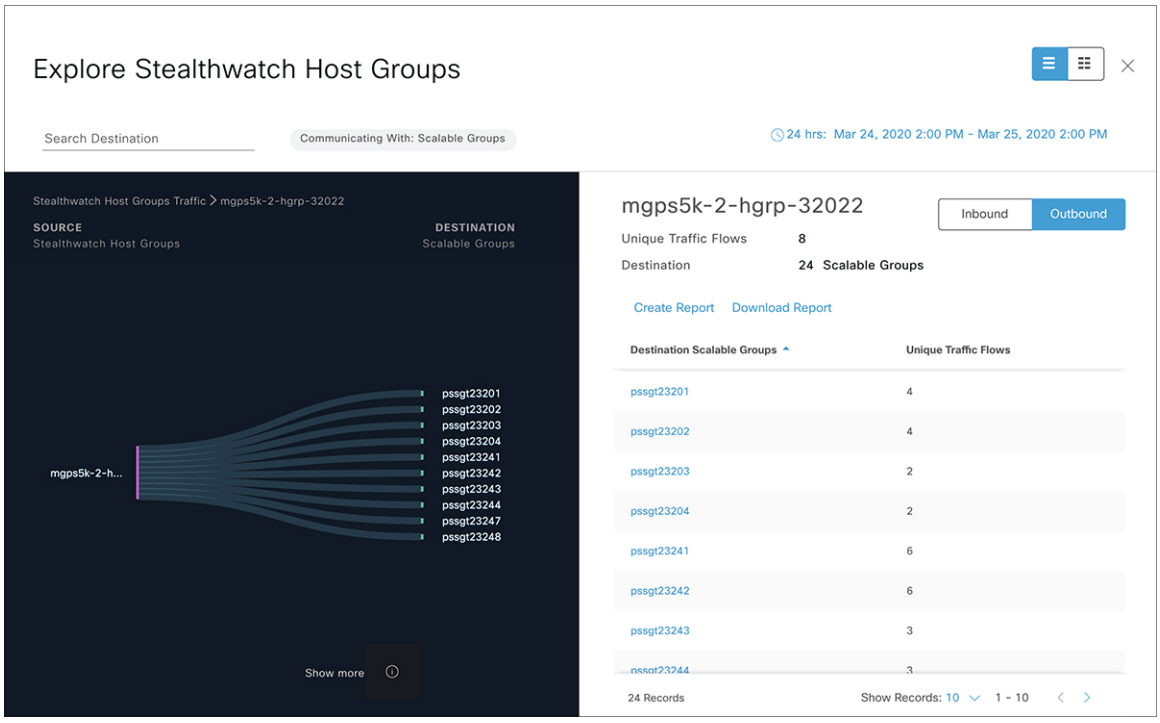
Figure 18: Single ISE profile to Multiple Scalable Groups: Chart View



Single Stealthwatch Host Group to Multiple Scalable Groups: Chart View

The following window is displayed when a Stealthwatch Host Group is selected as the source and Scalable Groups is chosen as the destination in the outbound direction.

Figure 19: Single Stealthwatch Host Group to Multiple Scalable Groups: Chart View



Single Group to Single Group

This **Explore Scalable Groups** window shows the activity between a single source group and a single destination group. The source group or the destination group or both must be a scalable group. By default, the time range for this visual is the last available 24 hours of data and the default number of links or records shown is 10.

When you hover your cursor over a link, it is highlighted and a tooltip shows the number of unique traffic flows.

When you click the directional arrow displayed between the source and destination groups, the source and destination groups are interchanged in this view.

Click **Create Report** to generate a new report in CSV format with the information in this view. The **Reports** window opens, where you can see the generated report. This window also provides you access to previously generated reports and allows you to download the reports.

Click **Download Report** to view the generated reports. The **Reports** window opens, where you can click the *download* icon under the **Last Run** column to download a report.

Click **View Contract** to launch the **View Contract** window. The left pane in the **View Contract** window displays the rules for permitted and denied traffic between the source and destination groups. You can view the traffic flows that match any selected rule in the right pane. You can also view the port and protocol details in the right pane. For more information about contracts, see Access Contracts.

Click the  icon to display the chart view or  to display the table view.

You can set the date and time using the Date and Time Selector.

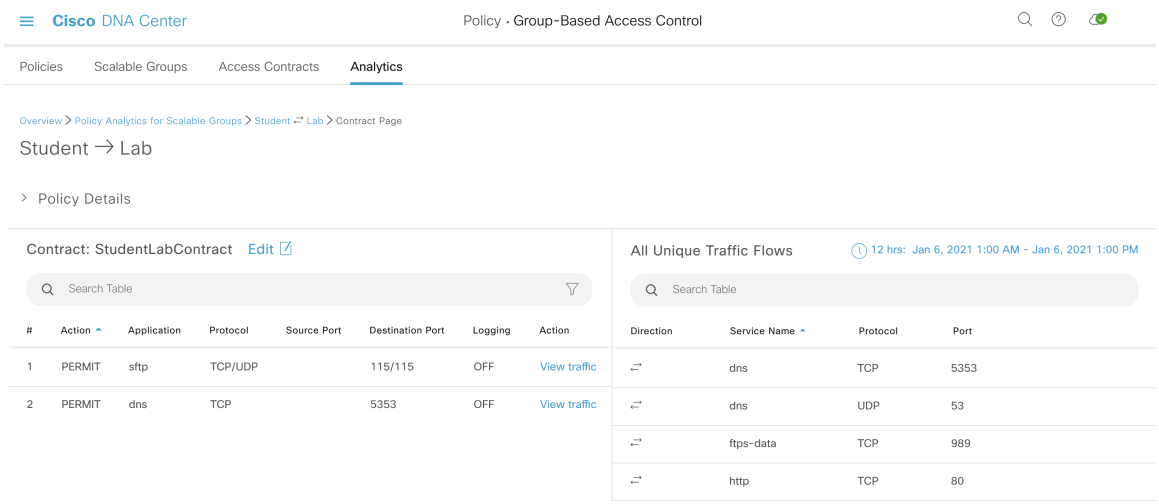
Access Contracts

Access Contracts can now be created and modified directly from the **Analytics** tab.

View Contract

To launch the **View Contract** window, from the **Explore Scalable Groups** window, click **View Contract**. The left pane in the **View Contract** window displays the rules for permitted and denied traffic between the source and destination groups. You can view the traffic flows that match any selected rule in the right pane.

Figure 20: View Contract



This table can also be accessed from the **Policies** window. In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Policy** > **Group-Based Access Control** > **Policies**

From the policy matrix view, click the cell for which you want to create or modify contracts. In the **Policy Details** slide-in pane, click **View Traffic Flows**.

If there is currently no contract assigned between the source and destination groups, no data is displayed. You can use the **Change Contract** or **Create Access Contract** option to create or modify the contract.

Click **View traffic** in the **Action** column to see the list of flows that match that rule.

Create Access Contract

To launch the **Contract Content** window, from the **Policy Details** pane, click **Create Access Contract**. To create the traffic filter rules:

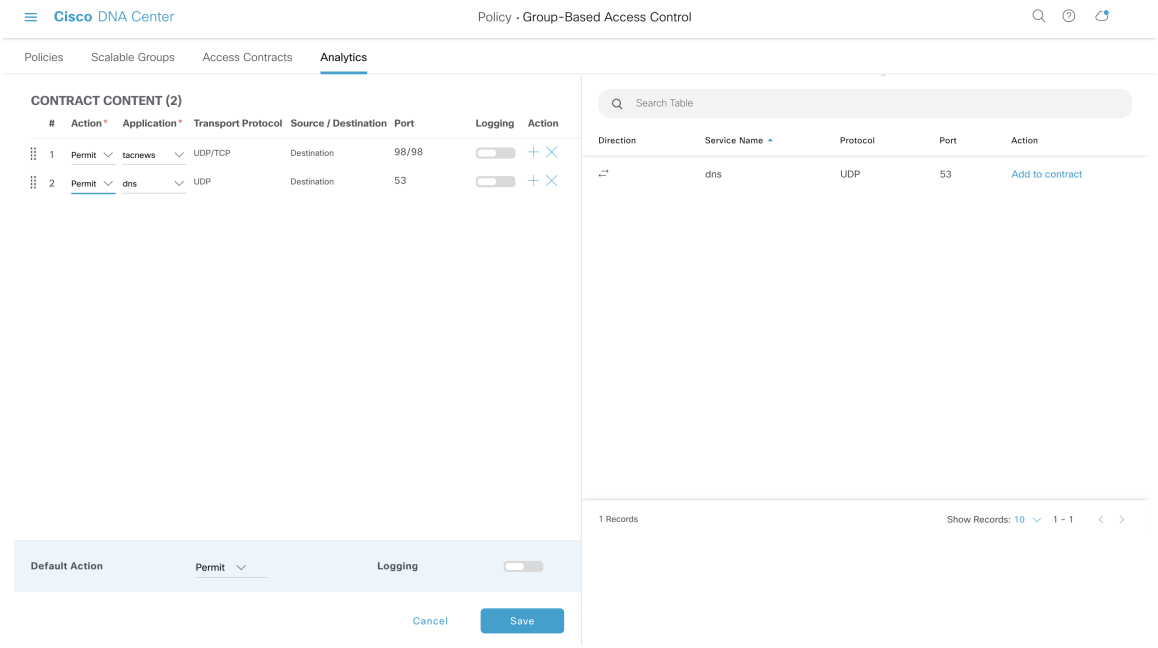
- From the **Action** drop-down list, choose **Deny** or **Permit**.
- From the **Application** drop-down list, choose the application for which you want to apply that action. The port and protocol are automatically selected based on the application that you select.

  If you want to specify the transport protocol, source port, and destination port, choose the **Advanced** option in the **Application** drop-down list.

You can create multiple rules. To create multiple rules for a contract, click the Plus icon and choose the settings for the **Action** and **Application** columns. The rules are checked in the order in which they are listed in the contract. Use the Handle icon at the left end of a rule to drag and change the order of the rule.

You can use the **Add to Contract** option within the **All Unique Traffic Flows** pane to add an entry to the contract.

Figure 21: Create Access Contract



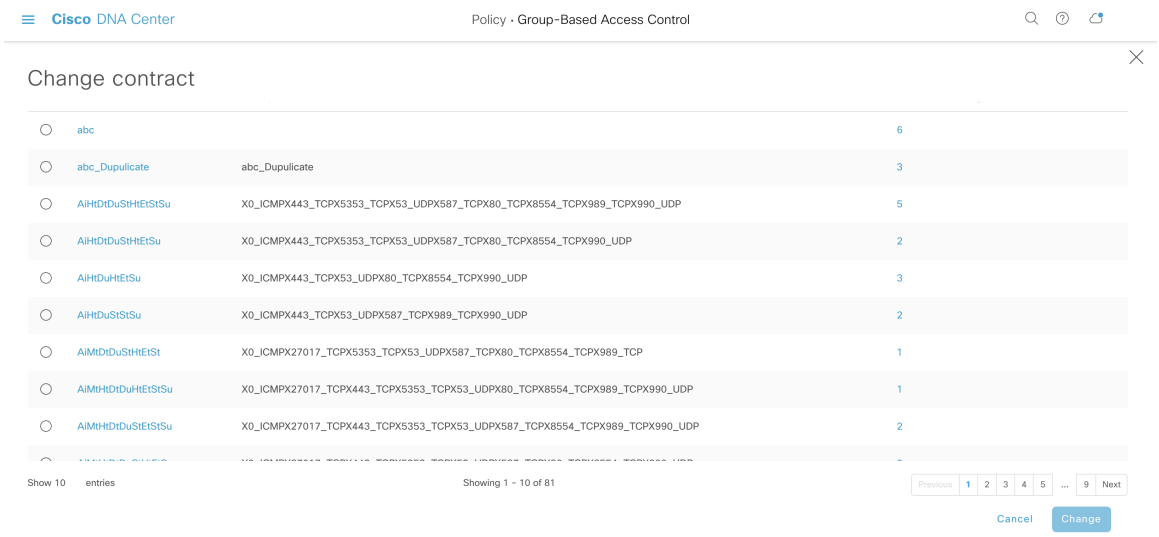
While saving a newly created or edited contract, you have the following options:

- **Update current policy only**: A duplicate of the contract is created and applied to the current policy. Other policies that reference this contract are not affected.
- **Update contract for all referenced policies**: The contract is updated and applied to the current policy and other policies that reference this contract.
- **Create a new contract with no policies affected**: A duplicate of the contract is created but not applied to any policy.

Change Contract

To launch the **Change Contract** window, from the **Policy Details** pane, click **Change Contract**. All available contracts are displayed. You can select the required contract and click **Change** to add that contract to the policy.

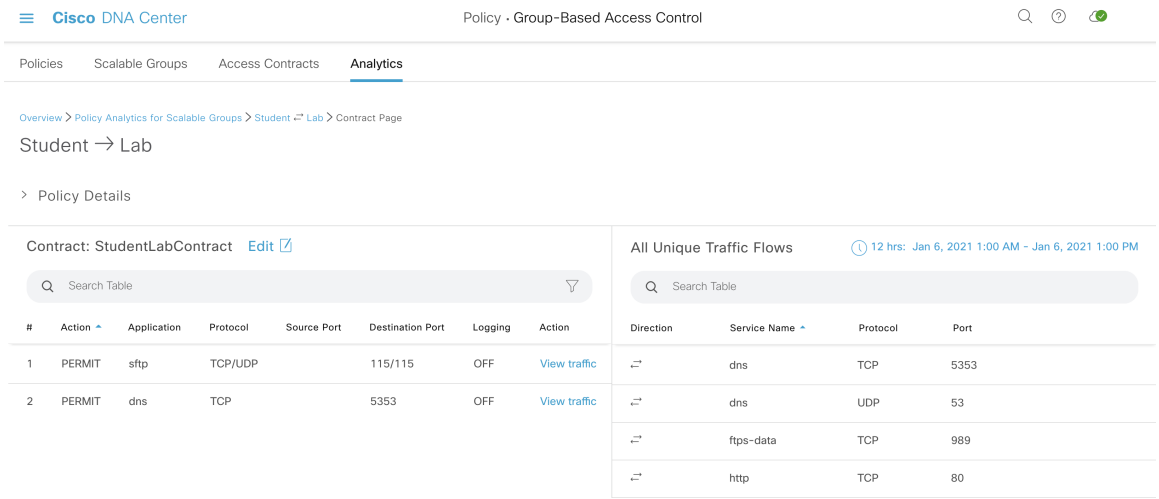
Figure 22: Change Contract



Edit Contract

The **Edit** option is displayed only when a contract has already been added to the policy. If you want to edit the contract details, click **Edit** displayed after the name of the contract.

Figure 23: Edit Contract



After updating the contract, click **Save**. The following options are available:

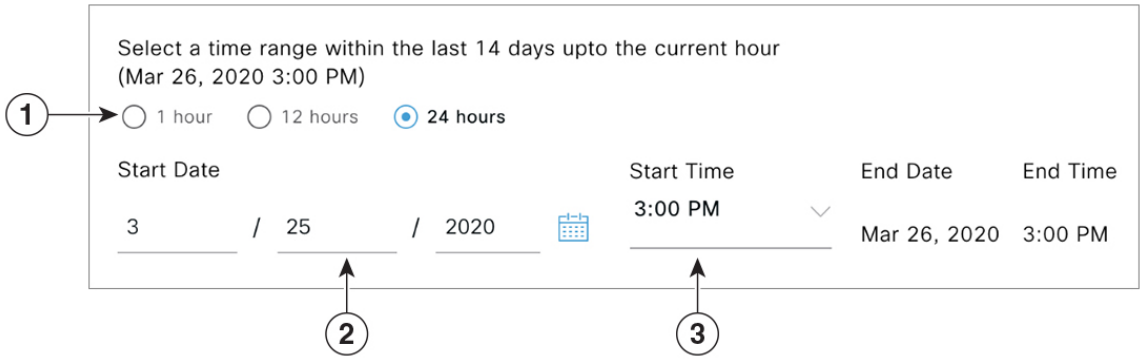
- **Update current policy only**: A duplicate of the contract is created and applied to the current policy. Other policies that reference this contract are not affected.
- **Update contract for all referenced policies**: The contract is updated and applied to the current policy and other policies that reference this contract.
- **Create a new contract with no policies affected**: A duplicate of the contract is created but not applied to any policy.

After choosing the appropriate option, enter a name and description (if you select the first or third option), and then click **Confirm**.

Date and Time Selector

You can select the time period for which you want to see the connection summary. You can select a time range between the last 14 days up to the current hour.

Figure 24: Date and Time Selector

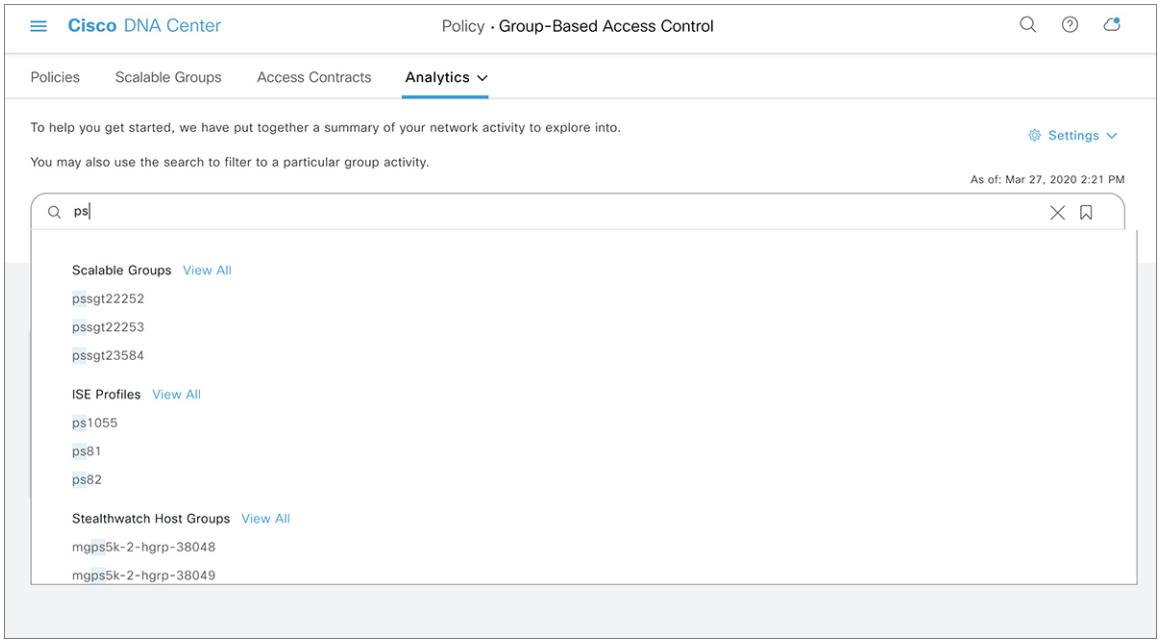


1. Select one of the three fixed time ranges. The **End Time** will be adjusted automatically.
2. Specify the **Start Date** by entering the month, day, and year manually or by using the calendar icon.
3. Choose the **Start Time** from the dropdown menu.

Use Search

The Cisco Group-Based Policy Analytics home page has a **Search** field that can search across the data for scalable groups, ISE profiles, Stealthwatch host groups, IP addresses, or MAC addresses.

Figure 25: Search Field



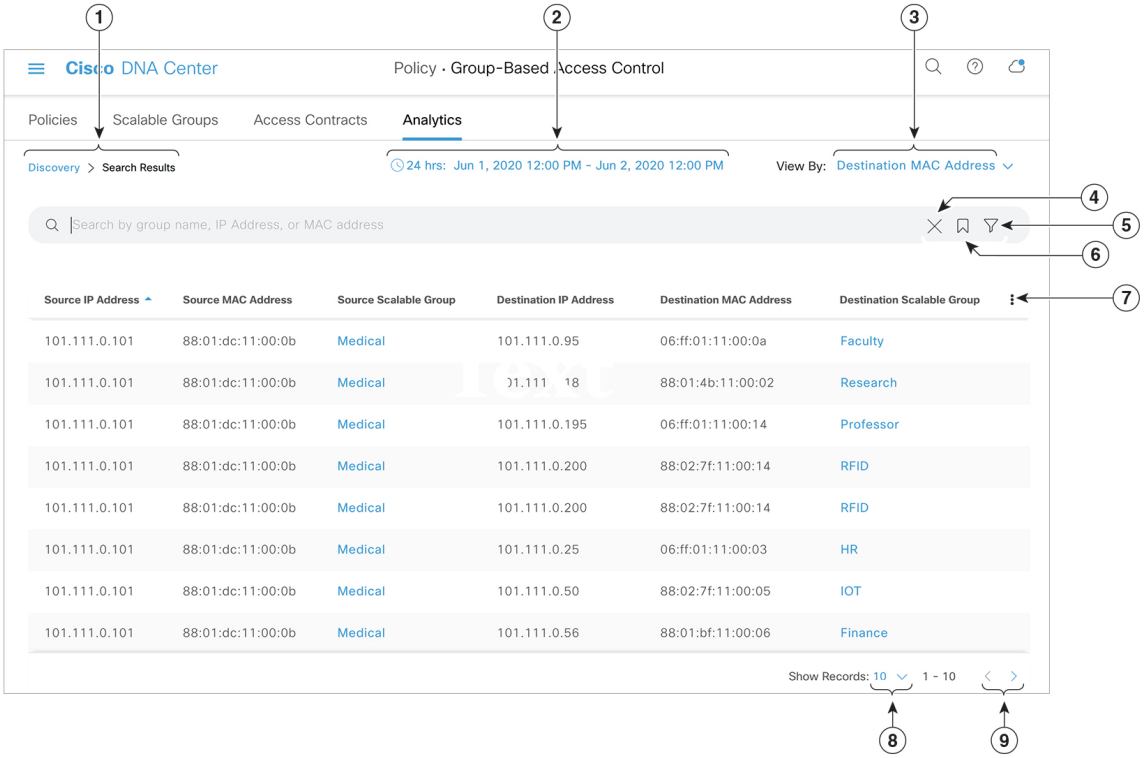
As you start entering the characters in the search field, an automatic search is performed for scalable groups, ISE profiles, and Stealthwatch host groups, and up to three results are displayed for each group type. The **View All** link to the search results appears only when relevant characters are identified in the search field. For IP addresses, the relevant characters are whole numbers and period. For MAC addresses, the relevant characters are hexadecimal and colon.

Note

- The **Search Results** window does not open until you click the **View All** link.
- A read-only user cannot search for an IP address or a MAC address. See Role-Based Access Control for more information.

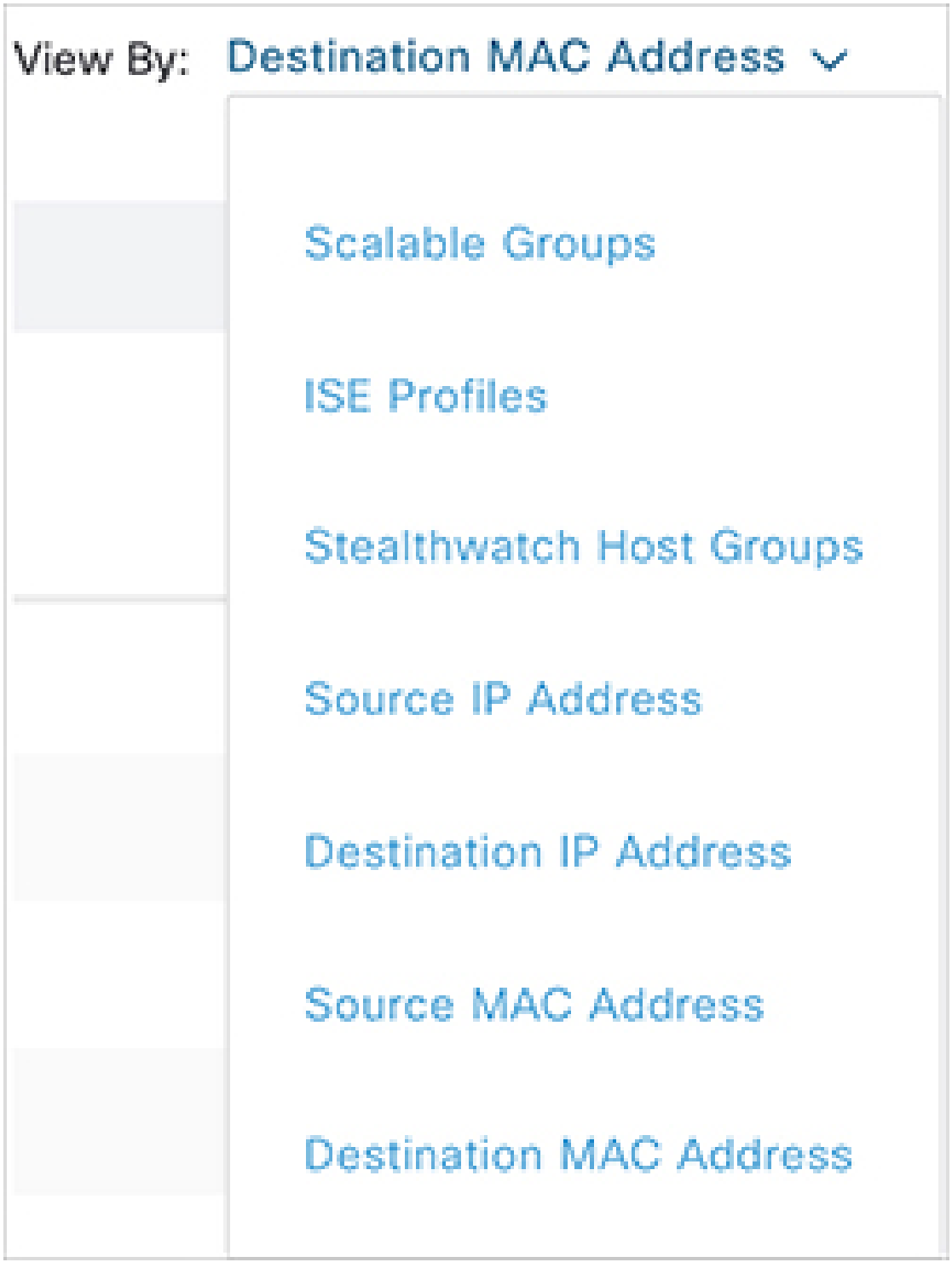
The following section describes the main elements in the **Search Results** window.

Figure 26: Search Results



1. Follow the breadcrumb to go back to the home page.
2. Set the date and time using the Date and Time Selector.
3. From the **View By** drop-down list, choose the required option to change your search criteria. The following options are available.

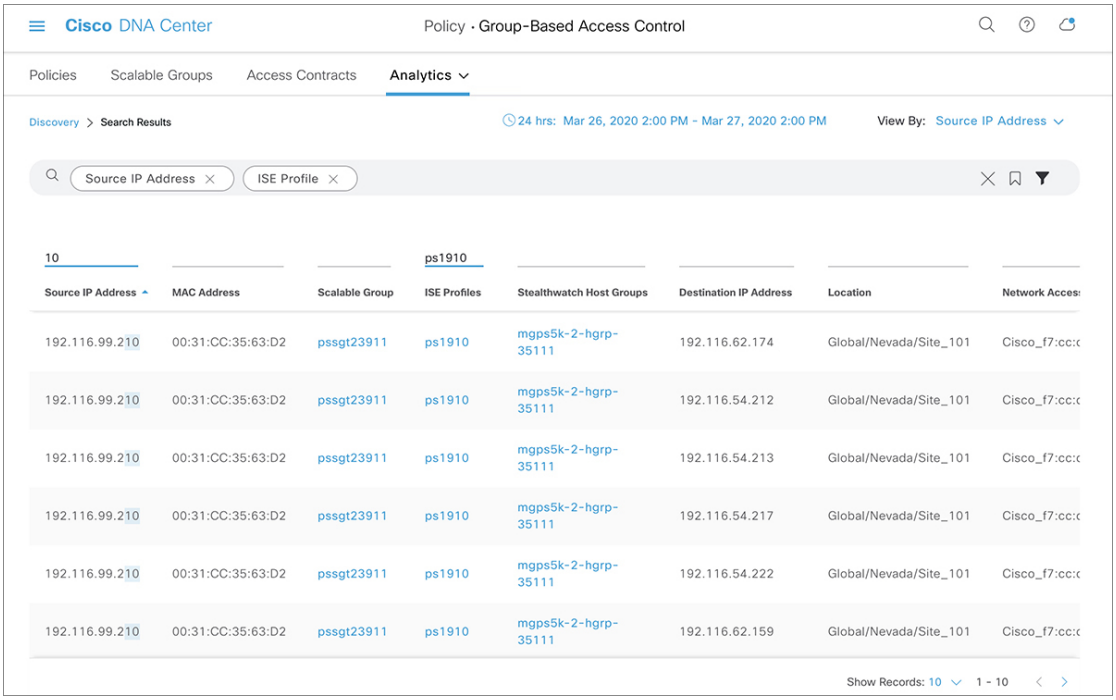
Figure 27: View By



4. Use the icon to close the search results.

5. The filter icon ( ) is used in advanced filtering, and is available only when you search for a MAC address or an IP address. When you click the icon, each column is provided with a search field on top of the column name.

Figure 28: Multiple Search Criteria

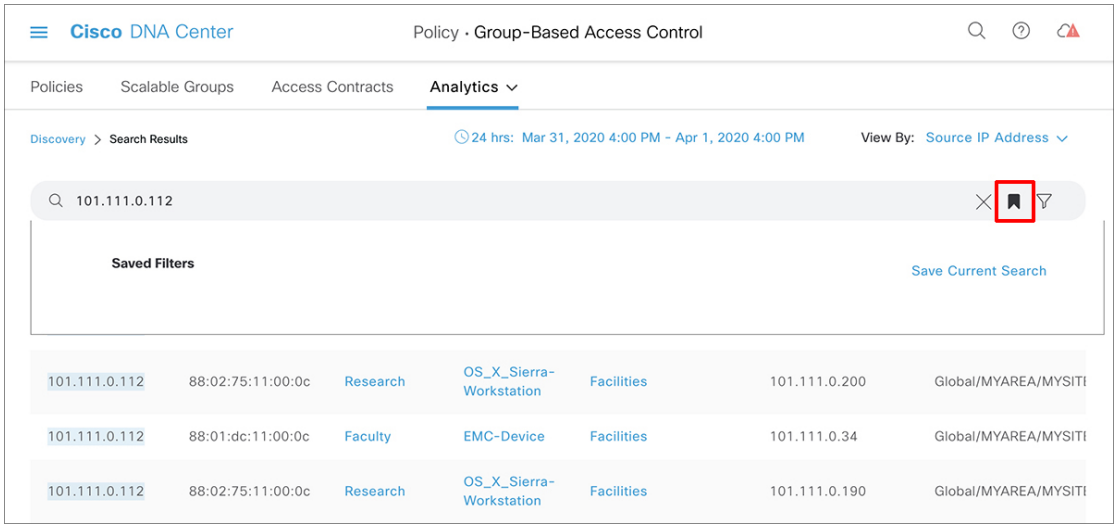


For each column, you can enter up to three search criteria. When entering more than one criterion per column, you can specify an OR operation or an AND operation. The resultant query performs an AND operation across the columns. In the preceding figure, the query matches the entries where the IP address contains *10* and ISE profiles contain *ps1910*.

6. Use the bookmark ( ) icon to load a saved filter or save the current search.

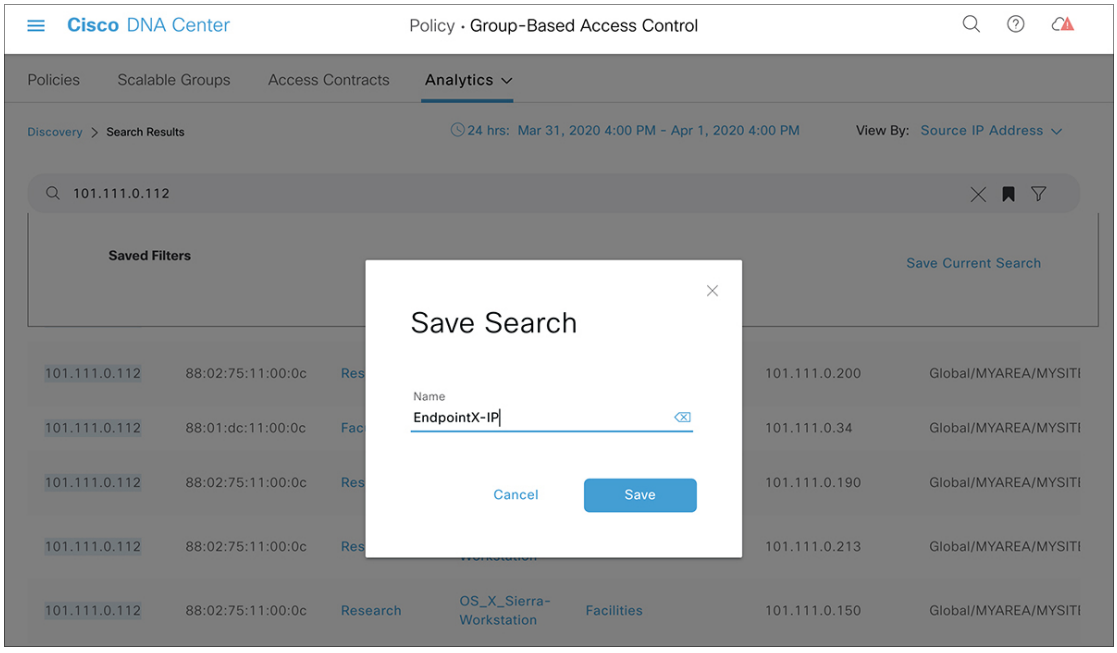
   Click the icon and use the **Save Current Search** option to save the current displayed search.

Figure 29: Save Filter



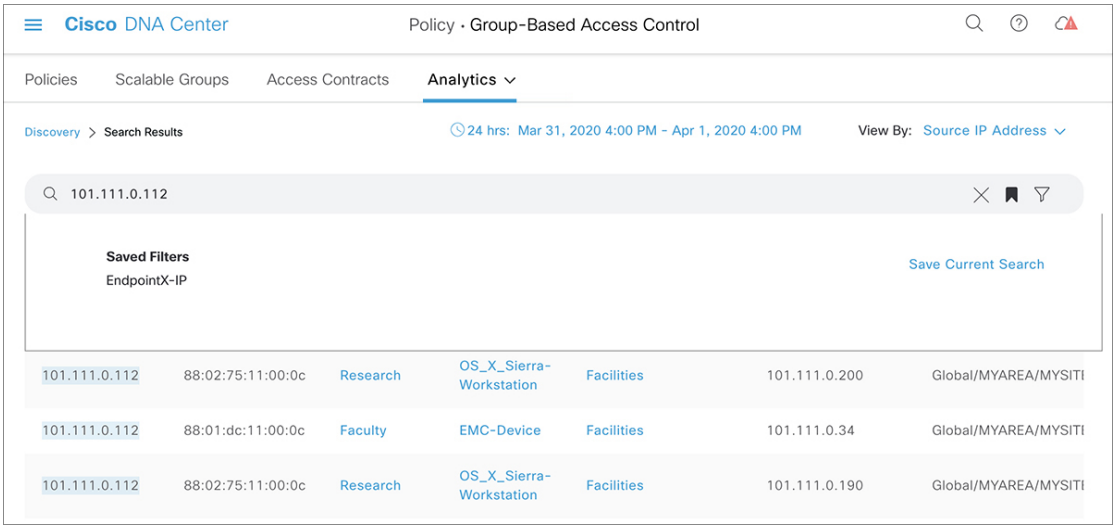
After you click this option, enter a name for the search and save it.

Figure 30: Save Search



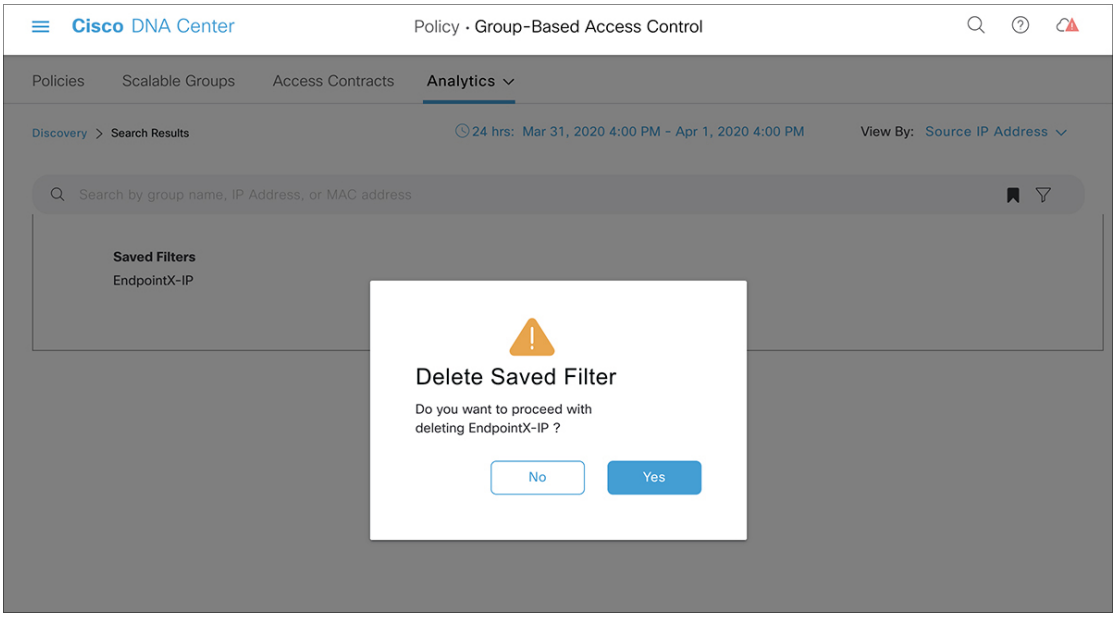
When you click the  icon again, you can see the name of the saved search.

Figure 31: View Saved Filter



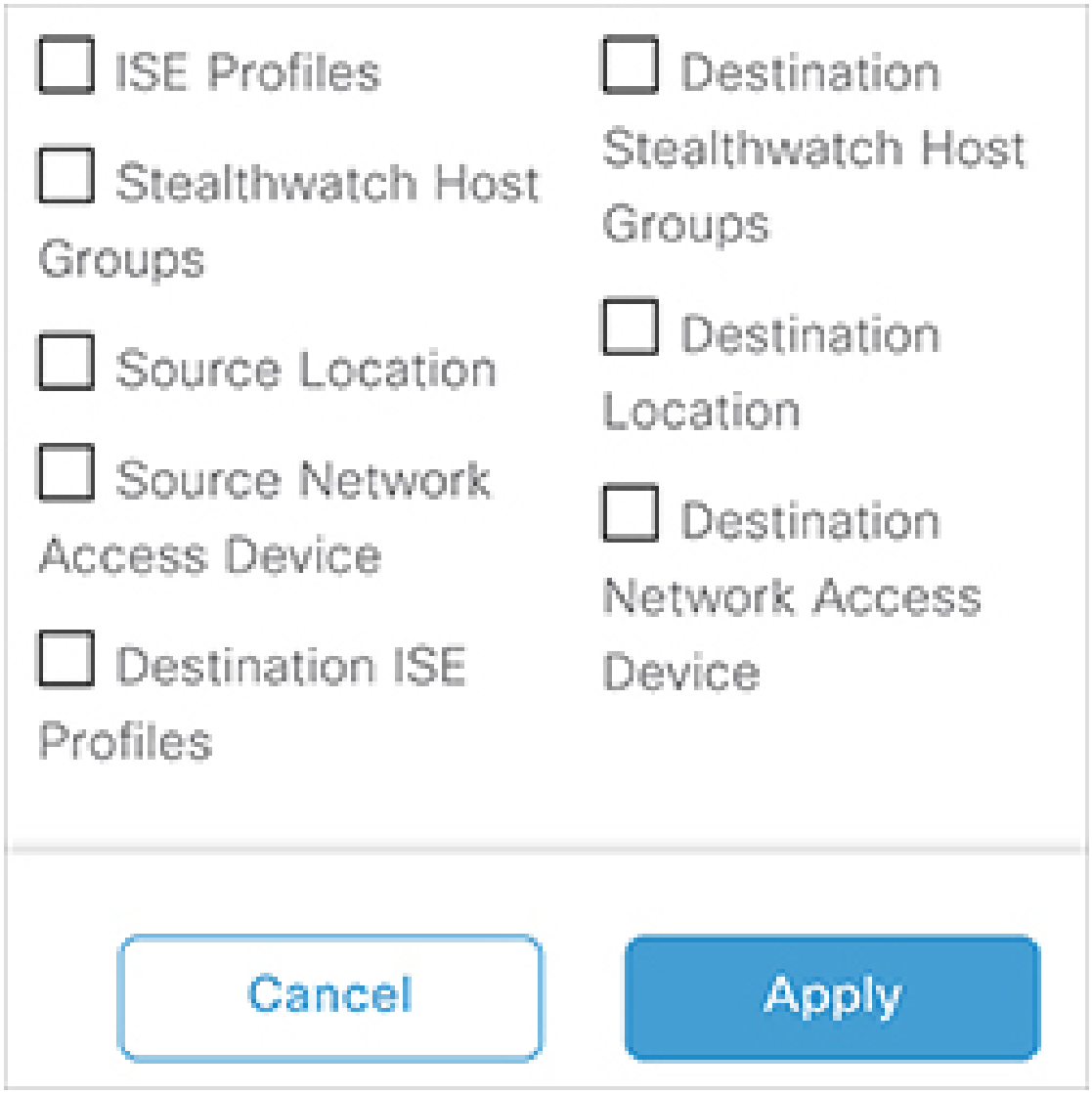
To delete a saved search, click the  icon. Hover your cursor over the name of the saved search and click the  icon. Click **Yes** in the **Delete Saved Filter** dialog box to permanently delete the filter.

Figure 32: Delete Saved Filter



7. Click this icon to open the column selector and customize your search view. You can select only the required columns for viewing to avoid focusing on the other data on the screen.

Figure 33: Column Selector



8. Choose to show 1, 25, 50, or 100 records per page.
9. The < and > links are enabled if there is a previous page or next page, respectively.

Role-Based Access Control

Cisco Group-Based Policy Analytics supports Role-Based Access Control. It differentiates between a read-write user and a read-only user. However, because Cisco Group-Based Policy Analytics Release 1.0, is primarily based on visibility, which does not make any changes to the system, there are only a few limitations for a read-only user:

- A read-only user cannot save search queries.
- A read-only user cannot makes changes in the Initial Configuration of Cisco Group-Based Policy Analytics, on page 261 window.

- A read-only user cannot export data because exporting data is an HTTPS POST operation.
- A read-only user can only perform search by group and is restricted from other search functions as they involve HTTPS POST operations.

IP-Based Access Control Policies

An IP-based access control policy controls the traffic going into and coming out of a Cisco device in the same way that an Access Control List (ACL) does. As with an ACL, an IP-based access control policy contains lists of permit and deny conditions that are applied to traffic flows based on various criteria, including protocol type, source IP address, destination IP address, or destination port number.

IP-based access control policies can be used to filter traffic for various purposes, including security, monitoring, route selection, and network address translation.

An IP-based access control policy has two main components:

- **IP Network Groups**: IP network groups comprise IP subnets that share the same access control requirements. These groups can be defined only in Cisco DNA Center. An IP network group may have as few as one IP subnet in it.
- **Access Contract**: An access contract is a common building block that is used in both IP-based and group-based access control policies. It defines the rules that make up the access control policies. These rules specify the actions (permit or deny) performed when traffic matches a specific port or protocol and the implicit actions (permit or deny) performed when no other rules match.

Workflow to Configure an IP-Based Access Control Policy

Before you begin

- Cisco ISE is not mandatory if you are adding groups within the **Policy** > **IP Based Access Control** > **IP Network Groups** window while creating a new IP-based access control policy.
- Make sure that you have defined the following global network settings and provision the device:
  - Network servers, such as AAA, DHCP, and DNS servers: See Configure Global Network Servers, on page 189.
  - Device credentials, such as CLI, SNMP, HTTP, and HTTPS: See About Global Device Credentials, on page 176.
  - IP address pools: See Configure IP Address Pools, on page 184.
  - Wireless settings as SSIDs, wireless interfaces, and wireless radio frequency profiles: See Configure Global Wireless Settings, on page 141.
  - Provision devices: See Provisioning, on page 353.

Step 1 Create IP network groups.

For more information, see Create an IP Network Group, on page 287.

Step 2 Create an IP-based access control contract.

An IP-based access control contract defines a set of rules between the source and destination. These rules dictate the action (allow or deny) that network devices perform based on the traffic that matches the specified protocols or ports. For more information, see Create an IP-Based Access Control Contract, on page 288.

Step 3 Create an IP-based access control policy. The access control policy defines the access control contract that governs traffic between the source and destination IP network groups.

For more information, see Create an IP-Based Access Control Policy, on page 289.

Configure Global Network Servers

You can define global network servers that become the default for your entire network.

Note You can override global network settings on a site by defining site-specific settings.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **Network**.

Step 2 In the **DHCP Server** field, enter the IP address of a DHCP server.

Note You can click the plus icon and enter both IPv4 and IPv6 addresses.

You must define at least one DHCP server in order to create IP address pools.

Step 3 In the **DNS Server** field, enter the domain name of a DNS server.

Note You can click the plus icon and enter both IPv4 and IPv6 addresses.

You must define at least one DNS server in order to create IP address pools.

Step 4 Click **Save**.

Create an IP Network Group

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **IP Based Access Control** > **IP Network Groups**.

Step 2 Click **Add Groups**.

Step 3 In the **Name** field, enter a name for the IP network group.

Step 4 In the **Description** field, enter a word or phrase that describes the IP network group.

Step 5 In the **IP Address or IP/CIDR** field, enter the IP addresses that make up the IP network group.

Step 6 Click **Save**.

Edit or Delete an IP Network Group

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **IP Based Access Control** > **IP Network Groups**.

Step 2 In the **IP Network Groups** table, check the check box next to the group that you want to edit or delete.

Step 3 Do one of the following tasks:

- To make changes to the group, click **Edit**. For field definitions, see Create an IP Network Group, on page 287. Make the desired changes and click **Save**.
- To delete the group, click **Delete** and then click **Yes** to confirm.

Create an IP-Based Access Control Contract

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **IP Based Access Control** > **Access Contract**.

Step 2 Click **Add Contract**.

Step 3 Enter a name and description for the contract.

Step 4 From the **Implicit Action** drop-down list, choose either **Deny** or **Permit**.

Step 5 From the **Action** drop-down list in the table, choose either **Deny** or **Permit**.

Step 6 From the **Port/Protocol** drop-down list, choose a port or protocol.

a) If Cisco DNA Center does not have the port or protocol that you need, click **Add Port/Protocol** to create your own.
b) In the **Name** field, enter a name for the port or protocol.
c) From the **Protocol** drop-down list, choose **UDP**, **TDP**, or **TCP/UDP**.
d) In the **Port Range** field, enter the port range.
e) If you want Cisco DNA Center to configure the port or protocol as defined, and not report any conflicts, check the **Ignore Conflict** check box.
f) Click **Save**.

Step 7 (Optional) To include more rules in your contract, click **Add** and repeat Step 5 and Step 6.

Step 8 Click **Save**.

Edit or Delete an IP-Based Access Control Contract

If you edit a contract that is used in a policy, the policy's state changes to **MODIFIED** in the **IP Based Access Control Policies** window. A modified policy is considered to be stale because it is inconsistent with the policy that is deployed in the network. To resolve this situation, you need to redeploy the policy to the network.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **IP Based Access Control** > **Access Contract**.

Step 2 Check the check box next to the contract that you want to edit or delete and do one of the following tasks:

- To make changes to the contract, click **Edit**, make the changes, and, click **Save**. For field definitions, see Create an IP-Based Access Control Contract, on page 288.

  Note If you make changes to a contract that is used in a policy, you need to deploy the modified policy by choosing **Policy** > **IP Based Access Control** > **IP Based Access Control Policies**, checking the check box next to the policy name, and clicking **Deploy**.

- To delete the contract, click **Delete**.

Create an IP-Based Access Control Policy

Create an IP-based access control policy to limit traffic between IP network groups.

- Multiple rules can be added to a single policy with different configurations.
- For a given combination of IP groups and contract classifiers, rules are created and pushed to the devices. This count cannot exceed 64 rules as Cisco WLC limits an ACL to have a maximum of 64 rules.
- If a custom contract or the IP group that is used in a **Deployed** policy is modified, the policy is flagged with status as **Modified**, indicating that it is Stale and requires a redeployment for the new configurations to be pushed to the device.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **IP Based Access Control** > **IP Based Access Control Policies**.

Step 2 Click **Add Policy**.

Step 3 Complete the following fields:

Field	Description
Policy Name	Name of the policy.
Description	Word or phrase that identifies the policy.
SSID	Lists FlexConnect SSIDs and non-FlexConnect SSIDs that were created during the design of SSIDs. If the selected SSID is configured in a FlexConnect mode, then the access policy is configured in FlexConnect mode. Otherwise, it will be configured in a regular way. **Note** If an SSID is part of one policy, that SSID will not be available for another policy. A valid site-SSID combination is required for policy deployment. You will not be able to deploy a policy if the selected SSID is not provisioned under any devices.
Site Scope	Sites to which a policy is applied. If you configure a wired policy, the policy is applied to all wired devices in the site scope. Likewise, if you configure a wireless policy for a selected service set identifier (SSID), the policy is applied to all of the wireless devices with the SSID defined in the scope. For more information, see Site Scope, on page 292.

Field	Description
Source	Origin of the traffic that is affected by the contract. From the **Source** drop-down list, choose an IP network group. If the IP network that you want is not available, click **+Group** to create one.
Contract	Rules that govern the network interaction between the source and destination in an ACL. Click **Add Contract** to define the contract for the policy. In the dialog box, click the radio button next to the contract that you want to use. Alternatively, you can select the permit (permit all traffic) or deny (deny all traffic) contract.
Destination	Target of the traffic that is affected by the contract. Click the **Destination** drop-down list, choose an IP network group. If the IP network that you want is not available, click **+Create IP Network Group** to create one.
Direction	Configures the relationship of the traffic flow between the source and destination. To enable the contract for traffic flowing from the source to the destination, select **One-Way**. To enable the contract for traffic flowing in both directions (from the source to the destination and from the destination to the source), select **Bi-directional**.

Step 4 (Optional) To create an IP network group, click **Create IP Network Group**.

Step 5 (Optional) To add another rule, click the plus sign.

Note To delete a rule, click **x**.

Step 6 (Optional) To reorder the sequence of the rules, drag and drop a rule in the order you want.

Step 7 Click **Deploy**.

The success message `IP-Based Access Control Policy has been created and deployed successfully` is displayed. Depending on the SSID selected, either a FlexConnect policy or a standard policy is created with different levels of mapping information and deployed. The **Status** of the policy is shown as **DEPLOYED**. A wireless icon next to the **Policy Name** shows that the deployed access policy is a wireless policy.

Edit or Delete an IP-Based Access Control Policy

If you need to, you can change or delete an IP-based access control policy.

Note If you edit a policy, the policy's state changes to **MODIFIED** on the **IP Based Access Control Policies** window. A modified policy is considered to be stale because it is inconsistent with the policy that was deployed in the network. To resolve this situation, you need to redeploy the policy to the network.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **IP Based Access Control** > **IP Based Access Control Policies**.

Step 2 Check the check box next to the policy that you want to edit or delete and do one of the following tasks:

- To make changes, click **Edit**. When you are done, click **Save**. For field definitions, see Create an IP-Based Access Control Policy, on page 289.
- To delete the policy, click **Delete**.

Step 3 If you make changes to the policy, deploy the modified policy by checking the check box next to the policy name and clicking **Deploy**.

Deploy an IP-Based Access Control Policy

If you make changes that affect a policy's configuration, you need to redeploy the policy to implement these changes.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **IP Based Access Control** > **IP Based Access Control Policies**.

Step 2 Locate the policy that you want to deploy.

Step 3 Check the check box next to the policy.

Step 4 Click **Deploy**.
You are prompted to deploy your policy immediately or to schedule it for a later time.

Step 5 Do one of the following:

- To deploy the policy immediately, click the **Run Now** radio button and click **Apply**.
- To schedule the policy deployment for a later date and time, click the **Schedule Later** radio button and define the date and time of the deployment.

Note The site time zone setting is not supported for scheduling application policy deployments.

Application Policies

Quality of Service (QoS) refers to the ability of a network to provide preferential or deferential service to selected network traffic. By configuring QoS, you can ensure that network traffic is handled in such a way that makes the most efficient use of network resources while still adhering to the objectives of the business, such as guaranteeing that voice quality meets enterprise standards, or ensuring a high Quality of Experience (QoE) for video.

You can configure QoS in your network using application policies in Cisco DNA Center. Application policies comprise these basic parameters:

- **Application Sets**: Sets of applications with similar network traffic needs. Each application set is assigned a business relevance group (business relevant, default, or business irrelevant) that defines the priority of its traffic. QoS parameters in each of the three groups are defined based on Cisco Validated Design (CVD). You can modify some of these parameters to more closely align with your objectives.
- **Site Scope**: Sites to which an application policy is applied. If you configure a wired policy, the policy is applied to all the wired devices in the site scope. Likewise, if you configure a wireless policy for a

selected service set identifier (SSID), the policy is applied to all of the wireless devices with the SSID defined in the scope.

Cisco DNA Center takes all of these parameters and translates them into the proper device CLI commands. When you deploy the policy, Cisco DNA Center configures these commands on the devices defined in the site scope.

Note Cisco DNA Center configures QoS policies on devices based on the QoS feature set available on the device. For more information about a device's QoS implementation, see the corresponding device's product documentation.

CVD-Based Settings in Application Policies

The default QoS trust and queuing settings in application policies are based on the Cisco Validated Design (CVD) for Enterprise Medianet Quality of Service Design. CVDs provide the foundation for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Each one has been comprehensively tested and documented by Cisco engineers to ensure faster, more reliable, and fully predictable deployment.

The latest validated designs relating to QoS are published in the Cisco Press book, *End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks*, 2nd Edition, available at: http://www.ciscopress.com/store/end-to-end-qos-network-design-quality-of-service-for-9781587143694. For additional information, see the following Cisco documentation:

- Cisco Validated Designs
- Enterprise Medianet Quality of Service Design 4.0
- Medianet Campus QoS Design 4.0
- Medianet WAN Aggregation QoS Design 4.0

Site Scope

A site scope defines the sites to which an application policy is applied. When defining a policy, you configure whether a policy is for wired or wireless devices. You also configure a site scope. If you configure a wired policy, the policy is applied to all the wired devices in the site scope. Likewise, if you configure a wireless policy for a selected service set identifier (SSID), the policy is applied to all of the wireless devices in the site scope with the SSID defined in the scope.

This allows you to make tradeoffs as necessary to compensate for differences in the behaviors between wired and wireless network segments. For example, wireless networks typically have lower bandwidth, lower speed, and increased packet loss in comparison to wired networks. Individual wireless segments may exhibit further variation due to local conditions of RF interference, congestion, and other factors, such as the varying capabilities of network devices. The ability to apply per-segment policies to individual wireless segments enables the adjustment of traffic-handling rules to ensure that the highest-priority traffic is least affected by degradation of the wireless network.

Business-Relevance Groups

A business-relevance group classifies a given application set according to how relevant it is to your business and operations.

Business-relevance groups are Business Relevant, Default, and Business Irrelevant, and they essentially map to three types of traffic: high priority, neutral, and low priority.

- **Business Relevant**: (High-priority traffic) The applications in this group directly contribute to organizational objectives, and as such, may include a variety of applications, including voice, video, streaming, and collaborative multimedia applications, database applications, enterprise resource applications, email, file transfers, content distribution, and so on. Applications designated as business relevant are treated according to industry best-practice recommendations, as prescribed in Internet Engineering Task Force (IETF) RFC 4594.
- **Default**: (Neutral traffic) This group is intended for applications that may or may not be business relevant, for example, generic HTTP or HTTPS traffic may contribute to organizational objectives at times, while at other times, such traffic may not. You may not have insight into the purpose of some applications, for instance, legacy applications or even newly deployed applications. Therefore, the traffic flows for these applications should be treated with the Default Forwarding service, as described in IETF RFC 2747 and 4594.
- **Business Irrelevant**: (Low-priority traffic) This group is intended for applications that have been identified as having no contribution towards achieving organizational objectives. They are primarily consumer-oriented or entertainment-oriented or both in nature. We recommend that this type of traffic be treated as a *Scavenger* service, as described in IETF RFCs 3662 and 4594.

Applications are grouped into application sets and sorted into business-relevance groups. You can include an application set in a policy as-is, or you can modify it to meet the needs of your business objectives and your network configuration.

For example, YouTube is member of the consumer-media application set, which is business-irrelevant (by default), because most customers typically classify this application this way. However, this classification may not be the true for all companies, for example, some businesses may be using YouTube for training purposes. In such cases, an administrator can move the YouTube application into the streaming-video application set, which is business relevant by default.

Consumers and Producers

You can configure relationships between applications such that when traffic from one application is sent to another application (thus creating a specific a-to-b traffic flow), the traffic is handled in a specific way. The applications in this relationship are called producers and consumers, and are defined as follows:

- **Producer**: Sender of the application traffic. For example, in a client/server architecture, the application server is considered the producer because the traffic primarily flows in the server-to-client direction. In the case of a peer-to-peer application, the remote peer is considered the producer.
- **Consumer**: Receiver of the application traffic. The consumer may be a client end point in a client/server architecture or it may be the local device in a peer-to-peer application. Consumers may be end-point devices, but may, at times, be specific users of such devices (typically identified by IP addresses or specific subnets). There may also be times when an application is the consumer of another application's traffic flows.

Setting up this relationship allows you to configure specific service levels for traffic matching this scenario.

Marking, Queuing, and Dropping Treatments

Cisco DNA Center bases its marking, queuing, and dropping treatments on IETF RFC 4594 and the business relevance category that you have assigned to the application. Cisco DNA Center assigns all of the applications in the Default category to the Default Forwarding application class and all of the applications in the Irrelevant Business category to the Scavenger application class. For applications in the Relevant Business category, Cisco DNA Center assigns traffic classes to applications based on the type of application. The following table lists the application classes and their treatments.

Table 43: Marking, Queuing, and Dropping Treatments

Business Relevance	Application Class	Per-Hop Behavior	Queuing and Dropping	Application Description
Relevant	VoIP[3]	Expedited Forwarding (EF)	Priority Queuing (PQ)	VoIP telephony (bearer-only) traffic; for example, Cisco IP phones.
	Broadcast Video	Class Selector (CS) 5	PQ	Broadcast TV, live events, video surveillance flows, and similar inelastic streaming media flows; for example, Cisco IP Video Surveillance and Cisco Enterprise TV. (Inelastic flows refer to flows that are highly drop sensitive and have no retransmission or flow-control capabilities or both.)
	Real-time Interactive	CS4	PQ	Inelastic high-definition interactive video applications and audio and video components of these applications; for example, Cisco TelePresence.
	Multimedia Conferencing	Assured Forwarding (AF) 41	Bandwidth (BW) Queue and Differentiated Services Code Point (DSCP) Weighted Random Early Detect (WRED)	Desktop software multimedia collaboration applications and audio and video components of these applications; for example, Cisco Jabber and Cisco WebEx.
	Multimedia Streaming	AF31	BW Queue and DSCP WRED	Video-on-Demand (VoD) streaming video flows and desktop virtualization applications,such as Cisco Digital Media System.
	Network Control	CS6	BW Queue only[4]	Network control-plane traffic, which is required for reliable operation of the enterprise network, such as EIGRP, OSPF, BGP, HSRP, IKE, and so on.
	Signaling	CS3	BW Queue and DSCP	Control-plane traffic for the IP voice and video telephony infrastructure.
	Operations, Administration, and Management (OAM)	CS2	BW Queue and DSCP[5]	Network operations, administration, and management traffic, such as SSH, SNMP, syslog, and so on.
	Transactional Data (Low-Latency Data)	AF21	BW Queue and DSCP WRED	Interactive (foreground) data applications, such as enterprise resource planning (ERP), customer relationship management (CRM), and other database applications.
	Bulk Data (High-Throughput Data)	AF11	BW Queue and DSCP WRED	Noninteractive (background) data applications, such as email, file transfer protocol (FTP), and backup applications.

Business Relevance	Application Class	Per-Hop Behavior	Queuing and Dropping	Application Description
Default	Default Forwarding (Best Effort)	DF	Default Queue and RED	Default applications and applications assigned to the default business-relevant group. Because only a small number of applications are assigned to priority, guaranteed bandwidth, or even to differential service classes, the vast majority of applications continue to default to this best-effort service.
Irrelevant	Scavenger	CS1	Minimum BW Queue (Deferential) and DSCP	Nonbusiness related traffic flows and applications assigned to the business-irrelevant group, such as data or media applications that are entertainment-oriented. Examples include YouTube, Netflix, iTunes, and Xbox Live.

[3] VoIP signaling traffic is assigned to the Call Signaling class.
[4] WRED is not be enabled on this class because network control traffic should not be dropped.
[5] WRED is not enabled on this class because OAM traffic should not be dropped.

Service Provider Profiles

Service provider (SP) profiles define the class of service for a particular WAN provider. You can define 4-class, 5-class, 6-class, and 8-class models.

When application policies are deployed on the devices, each SP profile is assigned a certain service-level agreement (SLA) that maps each SP class to a DSCP value and a percentage of bandwidth allocation.

You can customize the DSCP values and the percentage of bandwidth allocation in a SP profile when configuring an application policy.

After you create the SP profile, you need to configure it on the WAN interfaces.

Table 44: Default SLA Attributes for SP Profiles with 4 Classes

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Voice	EF	Yes	10	—
Class 1 Data	AF31	—	—	44
Class 2 Data	AF21	—	—	25
Default	0	—	—	31

Table 45: Default SLA Attributes for SP Profiles with 5 Classes

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Voice	EF	Yes	10	—
Class 1 Data	AF31	—	—	44
Class 2 Data	AF21	—	—	25
Class 3 Data	AF11	—	—	1
Default	Best Effort	—	—	30

Table 46: Default SLA Attributes for SP Profiles with 6 Classes

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Class 1 Data	AF31	—	—	10
Class 3 Data	AF11	—	—	1
Video	AF41	—	—	34
Voice	EF	Yes	10	—
Default	0	—	—	30
Class 2 Data	AF21	—	—	25

Table 47: Default SLA Attributes for SP Profiles with 8 Classes

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Network-Control Management	CS6	—	—	5
Streaming Video	AF31	—	—	10
Call Signalling	CS3	—	—	4
Scavenger	CS1	—	—	1
Interactive Video	AF41	—	—	30
Voice	EF	Yes	10	—

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Default	0	—	—	25
Critical Data	AF21	—	—	25

Queuing Profiles

Queuing profiles allow you to define an interface's bandwidth allocation based on the interface speed and the traffic class.

Note Queuing profiles do not apply to WAN-facing interfaces that are connected to a service provider profile.

The following interface speeds are supported:

- 100 Gbps
- 10/40 Gbps
- 1 Gbps
- 100 Mbps
- 10 Mbps
- 1 Mbps

If the speed of an interface falls between two interface speeds, Cisco DNA Center treats the interface at the lower interface speed.

Note Cisco DNA Center attempts to detect the operational speed of the interface in order to apply the correct policy. However, if a switch port is administratively down, Cisco DNA Center cannot detect the speed. In this case, Cisco DNA Center uses the interface's supported speed.

You define a queuing policy as part of an application policy. When you deploy the application policy, the devices in the sites that are selected in the site scope are configured with the assigned LAN queuing policy. If no LAN queuing policy is assigned, the application policy uses the default CVD queuing policy.

If you change the queuing policy in an application policy that has already been deployed, the policy becomes stale, and you need to redeploy the policy for the changes to be configured on the devices.

Note the following additional guidelines and limitations of queuing policies:

- You cannot delete a LAN queuing profile if it is used in a policy.
- If you update a queuing profile that is associated with a policy, the policy is marked as stale. You need to redeploy the policy to provision the latest changes.

- Traffic class queuing customization does not affect interfaces on Cisco service provider switches and routers. You should continue to configure these interfaces without using Cisco DNA Center.

Table 48: Default CVD LAN Queuing Policy

Traffic Class	Default Bandwidth (Total = 100%)[6]
Business Relevant Voice	10%
Business Relevant Broadcast Video	10%
Business Relevant Real-Time Interactive	13%
Business Relevant Multimedia Conferencing	10%
Business Relevant Multimedia Streaming	10%
Business Relevant Network control	3%
Business Relevant Signaling	2%
Business Relevant OAM	2%
Business Relevant Transactional Data	10%
Business Relevant Bulk Data	4%
Business Relevant Scavenger	1%
Business Relevant Best Effort	25%

[6] We recommend that the total bandwidth for Voice, Broadcast Video, and Real-Time Interactive traffic classes equals no more than 33%.

Processing Order for Devices with Limited Resources

Some network devices have a limited memory (called TCAM) for storing network ACLs and access control entries (ACEs). So, because ACLs and ACEs for applications are configured on these devices, the available TCAM space is used. When the TCAM space is depleted, QoS settings for additional applications cannot be configured on that device.

To ensure that QoS policies for the most important applications get configured on these devices, Cisco DNA Center allocates TCAM space in the following order:

1. **Rank**: Number assigned to custom and favorite applications, but not to existing, default NBAR applications. The lower the rank number, the higher the priority. For example, an application with rank 1 has a higher priority than an application with rank 2, and so on. Having no rank is the lowest priority.

Note

- Custom applications are assigned rank 1 by default.
- If we mark the NBAR application as favorite, the rank is set to 1000.

2. **Traffic Class**: Priority based on the following order: Signaling, Bulk Data, Network Control, Operations Administration Management (Ops Admin Mgmt), Transactional Data, Scavenger, Multimedia Streaming, Multimedia Conferencing, Real Time Interactive, Broadcast Video, and VoIP Telephony.
3. **Popularity**: Number (1–10) that is based on CVD criteria. The popularity number cannot be changed. An application with a popularity of 10 has a higher priority than an application with a popularity of 9, and so on.

Note
- Custom applications are assigned popularity 0.
- Default NBAR applications are assigned a popularity number (1–10) that is based on CVD criteria. When you mark an application as a favorite, this does not change the popularity number; only the rank is changed.

4. **Alphabetization**: If two or more applications have the same rank and popularity number, they are sorted alphabetically by the application's name, and assigned a priority accordingly.

For example, let us assume that you define a policy that has the following applications:

- Custom application, custom_realtime, which has been assigned rank 1 and popularity 10 by default.
- Custom application, custom_salesforce, which has been assigned rank 1 and popularity 10 by default.
- Application named corba-iiop, which is in the transactional data traffic class, and you have designated as a favorite, giving that application a ranking of 10,000 and popularity of 9 (based on CVD).
- Application named gss-http, which is in the Ops Admin Mgmt traffic class, and you have designated as a favorite, giving that application a ranking of 10,000 and popularity of 10 (based on CVD).
- All other, default NBAR applications, which have no rank, but will be processed according to their traffic class and default popularity (based on CVD).

According to the prioritization rules, the applications are configured on the device in this order:

Application Configuration Order	Reason
1. Custom application, custom_realtime	Custom applications are given highest priority. Given that the custom_salesforce and custom_realtime applications have the same rank and popularity, they are sorted alphabetically, custom_realtime before custom_salesforce.
2. Custom application, custom_salesforce	
3. Favorite application, gss-http	Because both of these applications have been designated as favorites, they have the same application ranking. So, Cisco DNA Center evaluates them according to their traffic class. Because gss-http is in the Ops Admin Mgmt traffic class, it is processed first, followed by the corba-iiop application, which is in the Trasactional Data traffic class. Their popularity does not come into play because the processing order has been determined by their traffic class.
4. Favorite application, corba-iiop	

Application Configuration Order	Reason
5. All other, default NBAR applications	All other applications are next and are prioritized according to traffic class and then popularity, with the applications having the same popularity being alphabetized according to the application's name.

Policy Drafts

When you create a policy, you can save it as a draft without having to deploy it. Saving it as a draft allows you to open the policy later and make changes to it. You can also make changes to a deployed policy, and save it as a draft.

Note After you save or deploy a policy, you cannot change its name.

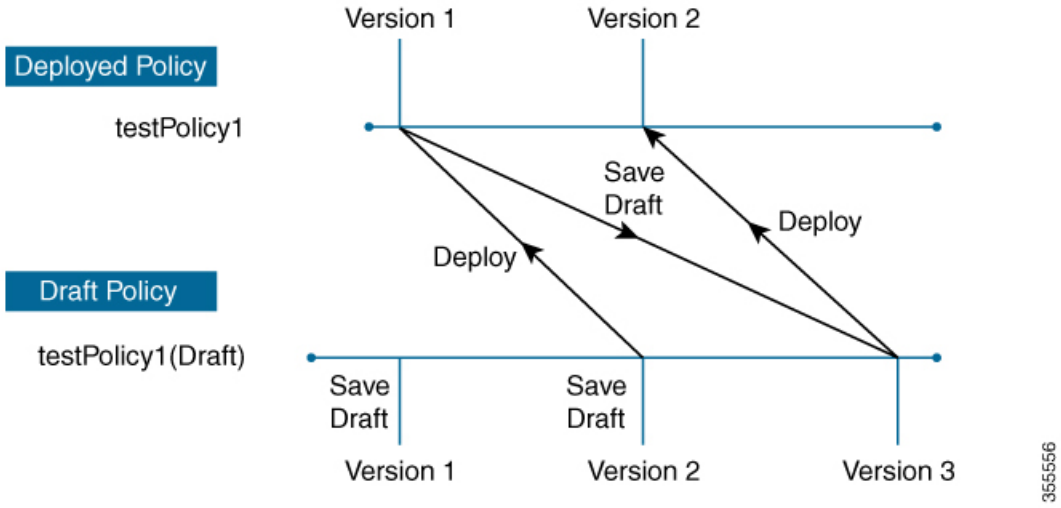
Draft policies and deployed policies are related to one another, but they have their own versioning.

When you save a policy as a draft, Cisco DNA Center appends the policy name with (Draft), and increments the version number. When you deploy a policy, Cisco DNA Center increments the version number of the deployed policy.

For example, as shown in the following figure, you create a policy named testPolicy1 and save it as a draft. The policy is saved as testPolicy1 (Draft), version number 1. You make a change to the draft and save it again. The policy has the same name, testPolicy1 (Draft), but its version number is incremented to 2.

You decide you like the policy, and you deploy it to the network. The policy is deployed with the name testPolicy1 and its version number is 1. You make a change to the deployed policy and save it as a draft. The draft policy, testPolicy1 (Draft), is incremented to version number 3. When you ultimately deploy that version, testPolicy1 is incremented to version 2.

Figure 34: Deployed Policy and Draft Policy Versioning



Any time you modify and save either a draft policy or a deployed policy, the draft policy version number is incremented. Similarly, any time you deploy either a draft policy or a modified deployed policy, the deployed policy version is incremented.

Just as with deployed policies, you can display the history of draft policies and roll them back to previous versions.

For more information about viewing the history of policy versions and rolling back to a previous version, see Policy Versioning, on page 302.

Policy Preview

Before you deploy a policy, you can generate the CLI that will be applied to a device.

The Preview operation generates the CLI commands for a policy, compares them with the CLI commands in the running configuration on the device, and returns only the remaining CLI commands that are required to configure the policy on the device.

After reviewing the preview output, you can deploy the policy to all of the devices in the scope, or you can continue to make changes to the policy.

Policy Precheck

When you create an application policy, you can verify if it will be supported on the devices in the site scope before you deploy it. The precheck function verifies if the device type, model, line cards, and software images support the application policy that you created. If any of these components are not supported, Cisco DNA Center reports a failure for the device. Cisco DNA Center also provides possible ways to correct the failures. If these remedies do not fix the failure, you can remove the device from the site scope.

If you deploy the application policy as-is, the policy will fail to deploy on the devices that reported a failure during the precheck process. To avoid the failure, you can remove the device from the site scope or update the device components to a level that the application policy supports. For a list of supported devices, see the Cisco DNA Center Supported Devices document.

Policy Scheduling

After you create or change a policy, you can deploy or redeploy the policy to the devices associated with it. You can deploy or redeploy a policy immediately or at a specific date and time, for example, on a weekend during off-peak hours. You can schedule a policy deployment for wired or wireless devices.

After you have scheduled a policy to be deployed, the policy and site scope are locked. You can view the policy, but you cannot edit it. If you change your mind about deploying the policy, you can cancel it.

Note When the scheduled event occurs, the policy is validated against the various policy components, for example, applications, application sets, and queuing profiles. If this validation fails, the policy changes are lost.

Policy Versioning

Policy versioning allows you to do the following tasks:

- Compare a previous version to the current (latest) one to see the differences.
- Display previous versions of a policy and select a version to reapply to the devices in a site scope.

Editing one version of a policy does not affect other versions of that policy or the components of the policy, such as the application sets that the policy manages. For example, deleting an application set from a policy does not delete the application set from Cisco DNA Center, other versions of that policy, or even other policies. Because policies and application sets exist independent of each other, it is possible to have a policy version that contains application sets that no longer exist. If you attempt to deploy or roll back to an older version of a policy that references an application set that no longer exists, an error occurs.

Note Policy versioning does not capture changes to applications (such as rank, port, and protocol), application set members, LAN queuing profiles, and sites.

Original Policy Restore

The first time that you deploy a policy to devices, Cisco DNA Center detaches the device's original Cisco Modular QoS CLI policy configurations, but leaves them on the device. Cisco DNA Center stores the device's original NBAR configurations in Cisco DNA Center. This allows you to restore the original Modular QoS CLI policies and NBAR configuration onto the devices later, if needed.

Note Because the Modular QoS CLI policies are not deleted from the device, if you remove these policies, you will not be able to restore them using the Cisco DNA Center original policy restore feature.

When you restore the original policy configuration onto a device, Cisco DNA Center removes the existing policy configuration that you deployed and reverts to the original configuration that was on the device.

Any Modular QoS CLI policy configurations that existed before you deployed application policies are reattached to the interfaces. However, queuing policies, such as multilayer switching (MLS) configurations, are not restored; instead, the devices retain the MLS configurations that were last applied through Cisco DNA Center.

After you restore the original policy configuration to the device, the policy that is stored in Cisco DNA Center is deleted.

Note the following additional guidelines and limitations for this feature:

- If the first attempt to deploy a policy to a device fails, Cisco DNA Center automatically attempts to restore the original policy configurations onto the devices.
- If a device is removed from an application policy after that policy has been applied to the device, the policy remains on the device. Cisco DNA Center does not automatically delete the policy or restore the QoS configuration on the device to its original (pre-Cisco DNA Center) configuration.

Stale Application Policies

An application policy can become stale if you change the configuration of something that is referenced in the policy. If an application policy becomes stale, you need to redeploy it for the changes to take affect.

An application policy can become stale for any of the following reasons:

- Change to applications referenced in an application set.
- Change to interfaces, such as SP Profile assignment, WAN subline rate, or WAN or LAN marking.
- Change to the queuing profile.
- New site added under a parent site in the policy.
- Device added to a site that is referenced by the policy.
- Devices moved between sites in the same policy.
- Change in interfaces exclusion/inclusion.
- Change in device Controller-Based Application Recognition (CBAR) status.

Application Policy Guidelines and Limitations

- Cisco DNA Center cannot learn multiple WLANs with the same SSID name on a wireless controller. At any point, Cisco DNA Center has only one entry for a WLAN with a unique name, although it is possible for the WLC to contain multiple entries with the same name and different WLAN profile names.

  You might have duplicate SSID names per WLC by design, or you might have inadvertently added a WLC with a duplicate SSID name using Cisco DNA Center. In either case, having duplicate SSID names per WLC is problematic for several features:

  - **Learn Config**: Cisco DNA Center learns only one randomly chosen SSID name per WLC and discards any remaining duplicate SSID names. (**Learn Config** is typically used in a brownfield scenario.)
  - **Application Policy**: When deploying an application policy, Cisco DNA Center randomly applies the policy to only one of the duplicate SSID names and not the others. In addition, policy restore, CLI preview, EasyQoS Fastlane, and PSK override features either fail or have unexpected outcomes.
  - **Multiscale Network**: In a multiscale network, multiple duplicate SSID names on multiple devices can cause issues. For example, one device has a WLAN configured as a nonfabric SSID, and a second device has the same WLAN, but it is configured as a fabric SSID. When you perform a **Learn Config**, only one SSID name is learned. The other SSID name from the other device is discarded. This behavior can cause conflicts, especially if the second device supports only fabric SSID names, but Cisco DNA Center is trying to perform operations on the device with nonfabric SSID names.
  - **IPACL Policy**: When deploying an IPACL policy, Cisco DNA Center randomly applies the policy to only one of the duplicate SSIDs. In addition, scenarios involving Flex Connect are also impacted.

- Cisco DNA Center does not recommend out-of-band (OOB) changes to device configurations. If you make OOB changes, the policy in Cisco DNA Center and the one configured on the device become inconsistent. The two policies remain inconsistent until you deploy the policy from Cisco DNA Center to the device again.
- The QoS trust functionality cannot be changed.
- Custom applications are not supported on the wireless controller. Therefore, custom applications are not selected while creating a wireless application policy.

- Make sure you delete the corresponding wireless application policy before deleting an SSID from design and reprovisioning the wireless controller.
- Wireless application for eWLC is not supported on SSID provisioned through learned configuration.
- Cisco DNA Center provides ACL-based Application Policy support for Cisco Catalyst IE 3300 Rugged Series switches and Cisco Catalyst IE 3400 Heavy Duty Series switches. You can deploy a maximum of eight port-based custom applications. However, there is no restriction for DSCP-based applications.

Note Cisco DNA Center does not support FlexConnect Local Switching mode for AireOS and eWLC platforms.

Manage Application Policies

The following sections provide information about how to manage application policies.

Prerequisites

To configure Application policies, make sure that you address the following requirements:

- Cisco DNA Center supports most of the Cisco LAN, WAN, WLAN devices. To verify whether the devices and software versions in your network are supported, see *Cisco DNA Center Supported Devices*.
- Make sure that your Cisco network devices, such as the ISR-G2, the ASR 1000, and Wireless LAN Controller, have the AVC (Application Visibility and Control) feature license installed. For information, see the *NBAR2 (Next Generation NBAR) Protocol Pack FAQ*.
- AVC support is available for switches running IOS-XE version 16.9 only if auto-QoS is not configured on the switches. You must upgrade the switches with auto-QOS configuration to IOS-XE version 16.11 or later to get AVC support.
- For Cisco DNA Center to identify the WAN interfaces that need policies, you must specify the interface type (WAN), and optionally, its subline rate and service-provider Class-of-Service model. For more information, see Assign a Service Provider Profile to a WAN Interface, on page 317.
- Verify that the device roles that were assigned to devices during the Discovery process are appropriate for your network. If necessary, change the device roles that are not appropriate. For more information, see Change the Device Role (Inventory), on page 76.

Create an Application Policy

This section provides information about how to create an application policy.

Before you begin

- Define your business objectives. For example, your business objective might be to improve user productivity by minimizing network response times or to identify and deprioritize nonbusiness applications. Based on these objectives, decide which business relevance category your applications fall into.
- Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

- Verify that the device roles that were assigned to devices during the Discovery process are appropriate for your network. If necessary, change the device roles that are not appropriate. For more information, see Change the Device Role (Inventory), on page 76.
- Add devices to sites. For more information, see Add a Device to a Site, on page 72.
- If you plan to configure this policy with an SP profile for traffic that is destined for an SP, make sure that you have configured an SP profile. After creating the application policy, you can return to the SP profile and customize its SLA attributes and assign the SP profile to WAN interfaces. For more information, see Configure Service Provider Profiles, on page 189.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Policy** > **Application** > **Application Policies**.

Step 2 Click **Add Policy**.

Step 3 In the **Application Policy Name** field, enter a name for the policy.

Step 4 Click either the **Wired** or **Wireless** radio button.

Step 5 For wireless networks, select an SSID that is provisioned from the **SSID** drop-down list.

Step 6 Click **Site Scope** and check the check box next to the sites where you want to deploy the policy.

Note For policies of wired devices, you cannot select a site that is already assigned to another policy. For policies of wireless devices, you cannot select a site that is already assigned to another policy with the same SSID.

Step 7 For policies of wired devices, you can exclude devices or specific interfaces from being configured with the policy:

a) From the **Site Scope** pane, click next to the site you are interested in.

A list of devices in the selected scope is displayed.

b) Locate the device that you want to exclude and click the toggle button in the corresponding **Policy Exclusions** column.

c) To exclude specific interfaces, click **Exclude Interfaces**.

d) From the list of **Applicable Interfaces**, click the toggle button next to the interfaces that you want to exclude.

By default, only the **Applicable Interfaces** are shown. You can choose **All** from the **Show** drop-down list to view all the interfaces.

e) Click **< Back to Devices in *Site-Name***.

f) Click **< Back to Site Scope**.

Step 8 For WAN devices, you can configure specific interfaces:

a) From the **Site Scope** pane, click next to the desired site.

b) From the list of devices in the site, click **Configure** in the **SP Profile Settings** column next to the desired device.

Note This option is only available for routers.

c) In the **WAN Interface** column, from the **Select Interface** drop-down list, choose an interface.

d) In the **Role** column, from the **Select Role** drop-down list, choose a role according to the type of interface you are configuring:

- Physical interface: Choose **WAN**. This role is the only valid role for a physical interface.
- Tunnel interface: Choose either **DMVPN Branch** or **DMVPN Hub**. If you choose **DMVPN Hub**, you can also define the bandwidth to its corresponding branches.

Note Make sure that the tunnel interfaces have been created on the devices before deploying these policy settings.

e) In the **Service Provider Profile** column, from the **Select Profile** drop-down list, choose an SP profile.
f) (Optional) If necessary, in the **Sub-Line Rate (Mbps)** column, enter the upstream bandwidth that the interface requires.
g) (Optional) To configure additional WAN interfaces, click **+** and repeat Step c through Step f.
h) Click **Save**.
i) Click **< Back to Site Scope**.

Step 9 From the **Site Scope** pane, click **OK**.

Step 10 (Optional) If the CVD queuing profile (CVD_QUEUING_PROFILE) does not meet your needs, create a custom queuing profile.

a) Click **Queuing Profiles**.
b) Select a queuing profile from the list in the left pane.
c) Click **Select**.

Step 11 (Optional) If this policy is for traffic that is destined for an SP, customize the SP profile SLA attributes:

a) Click **SP Profile**.
b) Choose an SP profile.
c) Customize the SLA attributes (**DSCP**, **SP Bandwidth %**, and **Queuing Bandwidth %**).

Step 12 (Optional) Configure the business relevance of the application sets used in your network.

Cisco DNA Center comes with application sets that are preconfigured into business-relevancy groups. You can keep this configuration or modify it by dragging and dropping an application set from one business-relevancy group to another.

Applications marked as a favorites are listed at the top of the application set. To change favorites, go to the Applications registry.

Step 13 (Optional) Customize applications by creating consumers and assigning them to applications, or by marking an application as bidirectional:

a) Expand the application group.
b) Click the gear icon next to the desired application.
c) From the **Traffic Direction** area, click the **Unidirectional** or **Bi-directional** radio button.
d) To choose an existing consumer, from the **Consumer** drop-down list, choose the consumer that you want to configure. To create a new consumer, click **+ Add Consumer** and define the **Consumer Name**, **IP/Subnet**, **Protocol**, and **Port/Range**.
e) Click **OK**.

Step 14 Configure host tracking. Click the **Host Tracking** toggle button to turn host tracking on or off.

When deploying an application policy, Cisco DNA Center automatically applies ACL entries to the switches to which collaboration endpoints (such as Telepresence units or Cisco phones) are connected.

The ACE matches the voice and video traffic generated by the collaboration endpoint, ensuring that the voice and video traffic are correctly marked.

When host tracking is turned on, Cisco DNA Center tracks the connectivity of the collaboration endpoints within the site scope and to automatically reconfigure the ACL entries when the collaboration endpoints connect to the network or move from one interface to another.

When host tracking is turned off, Cisco DNA Center does not automatically deploy policies to the devices when a collaboration endpoint moves or connects to a new interface. Instead, you need to redeploy the policy for the ACLs to be configured correctly for the collaboration endpoints.

Step 15 (Optional) Preview the CLI commands that will be sent to devices. For more information, see Preview an Application Policy, on page 313.

Step 16 (Optional) Precheck the devices on which you plan to deploy the policy. For more information, see Precheck an Application Policy, on page 313.

Step 17 Do one of the following tasks:

- Save the policy as a draft by clicking **Save Draft**. For more information, see Policy Drafts, on page 301.
- Deploy the policy by clicking **Deploy**. You can deploy the policy now or schedule it for a later time.

  To deploy the policy now, click the **Now** radio button and click **Apply**.

  To schedule the policy deployment for a later date and time, click the **Later** radio button and define the date and time of the deployment. For more information, see Policy Scheduling, on page 302.

  Note Site time zone setting is not supported for scheduling application policy deployments.

View Application Policy Information

You can display various information about the application policies that you have created and deployed.

Before you begin

You must have at least one deployed application policy.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Application** > **Application Policies**.

Step 2 Sort the policies by name, or filter them by name, status, or queuing profile.

Step 3 View the list of policies and the following information about each:

- **Policy Name**: Name of the policy.
- **Version**: Iteration of the policy. Each time a policy is deployed or saved as a draft, it is incremented by one version. For example, when you create a policy and deploy it, the policy is at version 1. If you change the policy and deploy it again, the version of the policy is incremented to version 2. For more information, see Policy Drafts, on page 301 and Policy Versioning, on page 302.
- **Policy Status**: State of the policy. If the policy applied on Cisco Catalyst 3850, Catalyst 4500, and Catalyst 9000 devices and is impacted by the port channel update (create/modify/delete), an alert is shown in the policy status.
- **Deployment Status**: State of the last deployment (per device). Presents a summary of the following
  - Devices that were successfully provisioned.
  - Devices that failed to be provisioned.
  - Devices that were not provisioned due to the deployment being terminated.

Clicking the state of the last deployment displays the Policy Deployment window, which provides a filterable list of devices on which the policy is deployed. For each device, the following information is displayed:

- Device details (name, site, type, role, and IP address)
- Success deployment status. Clicking the gear icon next to the status launches the **Effective Marking Policy** window that shows the **Business Relevant** and **Business Irrelevant** applications and the traffic class queue in which they end up. For devices that have limited TCAM resources or an old NBAR protocol pack, only a subset of the applications that are included in the policy can be provisioned, and they are shown in the view.
- Failure status shows the reason for the failure.

- **Scope**: Number of sites (not devices) that are assigned to the policy. For policies of wireless devices, the name of the SSID to which the policy applies is included.
- **LAN Queuing Profile**: Name of the LAN queuing profile that is assigned to the policy.

Edit an Application Policy

You can edit an application policy.

Before you begin

You must have created at least one policy.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Application** > **Application Policies**.

Step 2 Use the **Filter** field to locate the policy that you want to edit.

Step 3 Click the radio button next to corresponding policy.

Step 4 From the **Actions** drop-down list, choose **Edit**.

Step 5 Make changes to the application policy, as needed.

Step 6 You can change the business relevance of an application by moving application set between business relevant, business irrelevant, and default groups.

For information about the application policy settings, see Create an Application Policy, on page 305.

Step 7 To update the queuing profile, click **Queuing Profiles**, and select a queuing profile from the list in the left pane.

Step 8 Click **Select**.

Step 9 Do one of the following tasks:

- Save the policy as a draft by clicking **Save Draft**. For more information, see Policy Drafts, on page 301.
- Deploy the policy by clicking **Deploy**. You can deploy the policy now or schedule it for a later time.

  To deploy the policy now, click the **Run Now** radio button and click **Apply**.

  To schedule policy deployment for a later date and time, click the **Schedule Later** radio button and define the date and time of the deployment. For more information, see Policy Scheduling, on page 302.

Note The site time zone setting is not supported for scheduling application policy deployments.

Save a Draft of an Application Policy

When creating, editing, or cloning a policy, you can save it as a draft so that you can continue to modify it later. You can also make changes to a deployed policy and save it as a draft.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Application** > **Application Policies**.

Step 2 Create, edit, or clone a policy.

Step 3 Click **Save Draft**.

For more information, see Policy Drafts, on page 301.

Deploy an Application Policy

If you make changes that affect a policy's configuration, such as adding a new application or marking an application as a favorite, you should redeploy the policy to implement these changes.

Note Before deploying the policy, Auto-QoS config is automatically removed from Cisco Catalyst 3850, Catalyst 3650, and Catalyst 9000 devices with IOS version 16.x or later.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Application** > **Application Policies**.

Step 2 Use the **Filter** field to locate the policy that you want to deploy.

Step 3 Click the radio button next to the policy that you want to deploy.

Step 4 From the **Actions** drop-down list, choose **Deploy**.

a) If you redeploy the policy, you will be prompted to take an appropriate actions for the devices that were removed from the policy scope. Choose any one of the following appropriate actions.

- Delete policy from the devices (Recommended)
- Remove devices from policy scope
- Remove devices from policy scope and restore devices to brownfield configuration

b) Click **Apply**.

Step 5 You are prompted to deploy your policy now or to schedule it for a later time. Do one of the following:

- To deploy the policy now, click the **Run Now** radio button and click **Apply**.
- To schedule policy deployment for a later date and time, click the **Schedule Later** radio button and define the date and time of the deployment.

Note The site time zone setting is not supported for scheduling application policy deployments.

Cancel a Policy Deployment

After you click **Deploy**, Cisco DNA Center begins to configure the policy on the devices in the site scope. If you realize that you made a mistake, you can cancel the policy deployment.

The policy configuration process is performed as a batch process, in that it configures 40 devices at a time. If you have 40 devices or fewer and you cancel a policy deployment, your devices might be configured anyway, because the deployment to the first batch of devices would have already taken place. However, if you have hundreds of devices, canceling the policy deployment can be useful when needed.

When you click **Abort**, Cisco DNA Center cancels the configuration process on devices whose configuration has not yet started, and changes the device status to **Policy Aborted**. Cisco DNA Center does not cancel the deployments that are in the process of being completed or have been completed. These devices retain the updated policy configuration and reflect the state of the policy configuration, whether it is Configuring, Successful, or Failed.

During a policy deployment, click **Abort** to cancel the policy configuration process.

Delete an Application Policy

You can delete an application policy if it is no longer needed.

Deleting policy deletes class maps, policy map, and association of policy map with wireless policy profile.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Application** > **Application Policies**.

Step 2 Use the **Filter** field to locate the policy that you want to delete.

Step 3 Click the radio button next to the policy that you want to delete.

Step 4 From the **Actions** drop-down list, choose **Undeploy Policy**.

Step 5 In the **Undeploy Policy** window, click the **Delete policy from devices** radio button and click **Apply**.

Step 6 To confirm the deletion, click **OK**. Otherwise, click **Cancel**.

Step 7 When the deletion confirmation message appears, click **OK** again.

You can view the deletion status of the policies in the **Application Policies** page. If the status shows deletion failed, do the following:

a) Click the failed state link under **Deployment Status** in the **Application Policies** page.
b) In the **Undeployment Status** window, click **Retry** to delete the policy.

Clone an Application Policy

If an existing application policy has most of the settings that you want in a new policy, you can save time by cloning the existing policy, changing it, and then deploying it to a different scope.

Before you begin

You must have created at least one policy.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Application** > **Application Policies**.

Step 2 Use the **Filter** field to locate the policy that you want to clone.

Step 3 Click the radio button next to the policy that you want to clone.

Step 4 From the **Actions** drop-down list, choose **Clone**.

Step 5 Configure the application policy, as needed. For information about the application policy settings, see Create an Application Policy, on page 305.

Step 6 Do one of the following tasks:

- Save the policy as a draft by clicking **Save Draft**. For more information, see Policy Drafts, on page 301.
- Deploy the policy by clicking **Deploy**. You can deploy the policy now or schedule it for a later time.

  To deploy the policy now, click the **Run Now** radio button and click **Apply**.

  To schedule the policy deployment for a later date and time, click the **Schedule Later** radio button and define the date and time of the deployment. For more information, see Policy Scheduling, on page 302.

  Note The site time zone setting is not supported for scheduling application policy deployments.

Restore an Application Policy

If you create or make changes to a policy and then decide that you want to start over, you can restore the original QoS configuration that was on the device before you configured it using Cisco DNA Center.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Application** > **Application Policies**.

Step 2 Use the **Filter** field to locate the policy that you want to reset.

Step 3 Click the radio button next to the policy.

Step 4 From the **Actions** drop-down list, choose **Undeploy Policy**.

Step 5 In the **Undeploy Policy** window, click the **Restore devices to original configurations** radio button and click **Apply**.

Step 6 Click **OK** to confirm the change or **Cancel** to cancel it.

You can view the restoration status of the policies in the **Application Policies** page. If the status shows restoration failed, do the following:

a) Click the failed state link under **Deployment Status** in the **Application Policies** page.

b) In the **Undeployment Status** window, click **Retry** to restore the policy.

Reset the Default CVD Application Policy

The CVD configuration is the default configuration for applications. If you create or make changes to a policy and then decide that you want to start over, you can reset the applications to the CVD configuration. For more information about the CVD configuration, see Application Policies, on page 291.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Application** > **Application Policies**.

Step 2 Use the **Filter** field to locate the policy that you want to reset.

Step 3 Click the radio button next to the policy.

Step 4 From the **Actions** drop-down list, choose **Edit**.

Step 5 Click **Reset to Cisco Validated Design**.

Step 6 Click **OK** to confirm the change or **Cancel** to cancel it.

Step 7 Do one of the following tasks:

- To save a draft of the policy, click **Save Draft**.
- To deploy the policy, click **Deploy**.

Preview an Application Policy

Before you deploy a policy, you can generate the CLI that will be applied to a device and preview the configuration.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Application** > **Application Policies**.

Step 2 Create or edit a policy, as described in Create an Application Policy, on page 305 or Edit an Application Policy, on page 309.

Step 3 Before deploying the policy, click **Preview**.

A list of the devices in the scope appears.

Step 4 Click **Generate** next to the device that you are interested in.

Cisco DNA Center generates the CLIs for the policy.

Step 5 Click **View** to view the CLIs or copy them to the clipboard.

Precheck an Application Policy

Before you deploy an application policy, you can check whether the devices in the site scope are supported. The precheck process includes validating a device's model, line cards, and software image.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Application** > **Application Policies**.

Step 2 Create or edit a policy, as described in Create an Application Policy, on page 305 or Edit an Application Policy, on page 309.

Step 3 Click **Pre-check**.

Cisco DNA Center checks the devices and reports failures, if any, in the **Pre-Check Result** column. The **Errors** tab shows the devices that do not support this policy. The **Warnings** tab shows the restrictions or features that are not supported if you chose to deploy this policy in the device. You can still deploy the policy for the devices listed under

Warnings tab. To resolve the failures, bring the devices into compliance with the specifications listed in Cisco DNA Center Supported Devices.

Display Application Policy History

You can display the version history of an application policy. The version history includes the series number (iteration) of the policy and the date and time on which the version was saved.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Application** > **Application Policies**.

Step 2 Click the radio button next to the policy that interests you.

Step 3 From the **Actions** drop-down list, choose **History**.

Step 4 From the **Policy History** dialog box, you can do the following:

- To compare a version with the current version, click **Difference** next to the version that interests you.
- To roll back to a previous version of the policy, click **Rollback** next to the version that you want to roll back to.

Roll Back to a Previous Policy Version

If you change a policy configuration, and then realize that it is incorrect, or that is not having the desired affect in your network, you can revert to a policy that is up to five versions back.

Before you begin

You must have created at least two versions of the policy to roll back to a previous policy version.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Application** > **Application Policies**.

Step 2 Click the radio button next to the policy that interests you.

Step 3 From the **Actions** drop-down list, choose **Show History**.

Previous versions of the selected policy are listed in descending order, with the newest version (highest number) at the top of the list and the oldest version (lowest number) at the bottom.

Step 4 (Optional) To view the differences between the selected version and the latest version of a policy, click **Difference** in the **View** column.

Step 5 When you determine the policy version that you want to roll back to, click **Rollback** for that policy version.

Note If the selected site scope changed between policy versions, rollback is not done on the current (latest) selected site. Only the policy content is rolled back.

Step 6 Click **Ok** to confirm the rollback procedure.

The rolled back version becomes the newest version.

Manage Queuing Profiles

The following sections provide details about the various tasks that you can perform to manage queuing profiles.

Create a Queuing Profile

Cisco DNA Center provides a default CVD queuing profile (CVD_QUEUING_PROFILE). If this queuing profile does not meet your needs, you can create a custom queuing profile.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Application** > **Queuing Profiles**.

Step 2 Click **Add Profile**.

Step 3 In the **Profile Name** field, enter a name for the profile.

Step 4 Configure the bandwidth for each traffic class by using the slider, clicking the plus (+) or minus (-) sign, or entering a specific number in the field.

The number indicates the percentage of the total interface bandwidth that will be dedicated to the selected application class. Because the total bandwidth equals 100, adding bandwidth to one application class subtracts bandwidth from another application class.

An open lock icon indicates that you can edit the bandwidth for the application class. A closed lock indicates that you cannot edit it.

If you make a mistake, you can return to the CVD settings by clicking **Reset to Cisco Validated Design**.

The graph in the middle helps you visualize the amount of bandwidth that you are setting for each application class.

Step 5 (For advanced users) To customize the DSCP code points that Cisco DNA Center uses for each of the traffic classes, from the **Show** drop-down list, choose **DSCP Values** and configure the value for each application class by entering a specific number in the field.

To customize the DSCP code points required within an SP cloud, configure an SP profile.

Step 6 Click **Save**.

Edit or Delete a Queuing Profile

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Application** > **Queuing Profiles**.

Step 2 From the **Queuing Profile** pane, click the radio button next to the queuing profile that you want to edit or delete.

Step 3 Do one of the following tasks:

- To edit the profile, change the field values, except the profile name, and click **Save**. For information about the fields, see Create a Queuing Profile, on page 315.
- To delete the profile, click **Delete**.

  You cannot delete a queuing profile if it is referenced in an application policy.

Manage Application Policies for WAN Interfaces

The following sections provide details about the various tasks that you can perform to manage application profiles for WAN interfaces.

Customize Service Provider Profile SLA Attributes

If you do not want to use the default SLA attributes assigned to your SP profile by its class model, you can customize the SP profile SLA attributes to fit your requirements. For more information about the default SP profile SLA Attributes, see Service Provider Profiles, on page 296.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Application** > **Application Policies**.

Step 2 Use the **Filter** field to locate the policy that you want to change.

Step 3 Select the radio button next to the policy.

Step 4 From the **Actions** drop-down list, choose **Edit**.

Step 5 Click **SP Profiles** and select an SP profile.

Step 6 You can modify the information in the following fields:

- **DSCP**: Differentiated Services Code Point (DSCP) value. Valid values are from 0 to 63.
  - Expedited Forwarding (EF)
  - Class Selector (CS): CS1, CS2, CS3, CS4, CS5, CS6
  - Assured Forwarding: AF11, AF21, AF41
  - Default Forwarding (DF)

  For more information about these DSCP values, see Marking, Queuing, and Dropping Treatments, on page 294.
- **SP Bandwidth %**: Percentage of bandwidth allocated to a specific class of service.
- **Queuing Bandwidth %**: Percentage of bandwidth allocated to each of the traffic classes. You can make one of the following changes:
  - To customize the queuing bandwidth, unlock the bandwidth settings by clicking the lock icon and adjust the bandwidth percentages.
  - To calculate the queuing bandwidth automatically from the SP bandwidth, lock the queuing bandwidth settings by clicking the lock icon and then clicking **OK** to confirm. By default, Cisco DNA Center automatically distributes the queuing bandwidth percentage such that the sum of the queuing bandwidth for all of the traffic classes in an SP class aligns with the SP bandwidth percentage of that class.

Step 7 Click **OK**.

Assign a Service Provider Profile to a WAN Interface

If you have already created an application policy and now want to assign SP profiles to WAN interfaces, you can edit the policy and perform this configuration, including setting the subline rate on the interface, if needed.

Before you begin

If you have not created a policy, you can create a policy and assign SP profiles to WAN interfaces at the same time. For more information, see Create an Application Policy, on page 305.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Application** > **Application Policies**.

Step 2 Use the **Filter** field to locate the policy that you want to edit.

Step 3 Click the radio button next to the policy.

Step 4 From the **Actions** drop-down list, choose **Edit**.

Step 5 From the **Site Scope** pane, click the gear icon next to the site you are interested in.

Step 6 Click **Configure** in the **SP Profile Settings** column for the device you are interested in.

Step 7 In the **WAN Interface** column, from the **Select Interface** drop-down list, choose an interface.

Step 8 In the **Role** column, from the **Select Role** drop-down list, choose a role according to the type of interface you are configuring:

- **Physical interface**: Choose **WAN**. This role is the only valid role for a physical interface.
- **Tunnel interface**: Choose either **DMVPN Branch** or **DMVPN Hub**. If you choose **DMVPN Hub**, you can also define the bandwidth to its corresponding branches.

  Note Make sure that the tunnel interfaces have been created on the devices before deploying these policy settings.

Step 9 In the **Service Provider Profile** column, click the **Select Profile** drop-down field and choose an SP profile.

Step 10 If necessary, in the **Sub-Line Rate (Mbps)** column, enter the upstream bandwidth that the interface requires.

Step 11 To configure additional WAN interfaces, click + and repeat Step 7 through Step 10.

Step 12 Click **Save**.

Step 13 Click < **Back to Site Scope**.

Step 14 Click **OK**.

Step 15 Click **Deploy**.

You are prompted to deploy your policy now or to schedule it for a later time.

Step 16 Do one of the following:

- To deploy the policy now, click the **Run Now** radio button and click **Apply**.
- To schedule policy deployment for a later date and time, click the **Schedule Later** radio button and define the date and time of the deployment.

  Note The site time zone setting is not supported for scheduling application policy deployments.

Traffic Copy Policies

Using Cisco DNA Center, you can set up an Encapsulated Remote Switched Port Analyzer (ERSPAN) configuration such that the IP traffic flow between two entities is copied to a specified destination for monitoring or troubleshooting.

To configure ERSPAN using Cisco DNA Center, create a traffic copy policy that defines the source and destination of the traffic flow that you want to copy. You can also define a traffic copy contract that specifies the device and interface where the copy of the traffic is sent.

Note Because traffic copy policies can contain either scalable groups or IP network groups, throughout this guide, we use the term *groups* to refer to both scalable groups and IP network groups, unless specified otherwise.

Sources, Destinations, and Traffic Copy Destinations

Cisco DNA Center simplifies the process of monitoring traffic. You do not have to know the physical network topology. You only have to define a source and destination of the traffic flow and the traffic copy destination where you want the copied traffic to go.

- **Source**: One or more network device interfaces through which the traffic that you want to monitor flows. The interface might connect to end-point devices, specific users of these devices, or applications. A source group comprises Ethernet, Fast Ethernet, Gigabit Ethernet, 10-Gigabit Ethernet, or port channel interfaces only.
- **Destination**: The IP subnet through which the traffic that you want to monitor flows. The IP subnet might connect to servers, remote peers, or applications.
- **Traffic Copy Destination**: Layer 2 or Layer 3 LAN interface on a device that receives, processes, and analyzes the ERSPAN data. The device is typically a packet capture or network analysis tool that receives a copy of the traffic flow for analysis.

Note At the destination, we recommend that you use a network analyzer, such as a Switch Probe device, or other Remote Monitoring (RMON) probe, to perform traffic analysis.

The interface type can be Ethernet, Fast Ethernet, Gigabit Ethernet, or 10-Gigabit Ethernet interfaces only. When configured as a destination, the interface can be used to receive only the copied traffic. The interface can no longer receive any other type of traffic and cannot forward any traffic except that required by the traffic copy feature. You can configure trunk interfaces as destinations. This configuration allows the interfaces to transmit encapsulated traffic.

Note There can be only one traffic copy destination per traffic copy contract.

Guidelines and Limitations of Traffic Copy Policy

The traffic copy policy feature has the following limitations:

- You can create up to 8 traffic copy policies, 16 copy contracts, and 16 copy destinations.
- The same interface cannot be used by more than one traffic copy destination.
- Cisco DNA Center does not show a status message to indicate that a traffic copy policy has been changed and is no longer consistent with the one that is deployed in the network. However, if you know that a traffic copy policy has changed since it was deployed, you can redeploy the policy.
- You cannot configure a management interface as a source group or traffic copy destination.

Workflow to Configure a Traffic Copy Policy

Before you begin

- To be monitored, a source scalable group that is used in a traffic copy policy needs to be statically mapped to the switches and their interfaces.
- A traffic copy policy destination group needs to be configured as an IP network group. For more information, see Create an IP Network Group, on page 287.

Step 1 Create a traffic copy destination.

This is the interface on the device where the traffic flow will be copied for further analysis. For information, see Create a Traffic Copy Destination, on page 319.

Step 2 Create a traffic copy contract.

The contract defines the copy destination. For information, see Create a Traffic Copy Contract, on page 320.

Step 3 Create a traffic copy policy.

The policy defines the source and destination of the traffic flow and the traffic copy contract that specifies the destination where the copied traffic is sent. For information, see Create a Traffic Copy Policy, on page 320.

Create a Traffic Copy Destination

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy > Traffic Copy > Traffic Copy Destination**.

Step 2 Enter a name and description for the traffic copy destination.

Step 3 Select the device and one or more ports.

Step 4 Click **Save**.

Edit or Delete a Traffic Copy Destination

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Traffic Copy** > **Traffic Copy Destination**.

Step 2 Check the check box next to the destination that you want to edit or delete.

Step 3 Do one of the following:

- To make changes, click **Edit**, make the necessary changes, and click **Save**.
- To delete the destination, click **Delete**.

Create a Traffic Copy Contract

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Traffic Copy** > **Traffic Copy Contract**.

Step 2 Click **Add**.

Step 3 In the dialog box, enter a name and description for the contract.

Step 4 From the **Copy Destination** drop-down list, choose a copy destination.

Note You can have only one destination per traffic copy contract.

If no copy destinations are available for you to choose, you can create one. For more information, see Create a Traffic Copy Destination, on page 319.

Step 5 Click **Save**.

Edit or Delete a Traffic Copy Contract

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Traffic Copy** > **Traffic Copy Contract**.

Step 2 Check the check box next to the contract that you want to edit or delete.

Step 3 Do one of the following:

- To make changes, click **Edit**, make the necessary changes, and click **Save**.
- To delete the contract, click **Delete**.

Create a Traffic Copy Policy

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Traffic Copy** > **Traffic Copy Policies**.

Step 2 Click **Add Policy**.

Step 3 In the **Policy Name** field, enter a name.

Step 4 In the **Description** field, enter a word or a phrase that identifies the policy.

Step 5 In the **Contract** field, click **Add Contract**.

Step 6 Click the radio button next to the contract that you want to use and then click **Save**.

Step 7 Drag and drop groups from the **Available Groups** area to the **Source** area.

Step 8 Drag and drop groups from the **Available Groups** area to the **Destination** area.

Step 9 Click **Save**.

Edit or Delete a Traffic Copy Policy

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy > Traffic Copy > Traffic Copy Policies**.

Step 2 Check the check box next to the policy that you want to edit or delete.

Step 3 Do one of the following:

- To make changes, click **Edit**, make the necessary changes, and click **Save**.
- To delete the policy, click **Delete**.

Virtual Networks

Virtual networks are isolated routing and switching environments. You can use virtual networks to segment your physical network into multiple logical networks.

Only the assigned user groups are allowed to enter a virtual network. Within a virtual network, users and devices can communicate with each other unless explicitly blocked by an access policy. Users across different virtual networks cannot communicate with each other. However, an exception policy can be created to allow some users to communicate across different virtual networks.

A typical use case is building management, where the user community needs to be segmented from building systems, such as lighting; heating, ventilation, and air conditioning (HVAC) systems; and security systems. In this case, you segment the user community and the building systems into two or more virtual networks to block unauthorized access of the building systems.

A virtual network may span across multiple site locations and across network domains (wireless, campus, and WAN).

By default, Cisco DNA Center has a single virtual network, and all users and endpoints belong to this virtual network. If Cisco DNA Center is integrated with Cisco Identity Services Engine (Cisco ISE), the default virtual network is populated with user groups and endpoints from Cisco ISE.

In Cisco DNA Center, the concept of virtual network is common across wireless, campus, and WAN networks. When a virtual network is created, it can be associated with sites that have any combination of wireless, wired, or WAN deployments. For example, if a site has a campus fabric deployed, which includes wireless and wired devices, the virtual network creation process triggers the creation of the Service Set Identifier (SSID) and Virtual Routing and Forwarding (VRF) in the campus fabric. If the site also has WAN fabric deployed, the VRF extends from the campus to WAN as well.

During site design and initial configuration, you can add wireless devices, wired switches, and WAN routers to the site. Cisco DNA Center detects that the virtual network and the associated policies have been created for the site, and applies them to the different devices.

Guidelines and Limitations for Virtual Networks

Virtual networks have the following guidelines and limitation:

- VRFs are common across all domains. The maximum number of VRFs is based on the device with the fewest VRFs in the domain.

Multiple Virtual Networks for Guest Access

You can create multiple virtual networks for guest access. With this feature, you can use different virtual networks for guest traffic in places where there is no enterprise traffic. You can now map the wireless guest SSIDs to IP pools from different virtual networks with no restrictions.

Create a Virtual Network

You can create a virtual network to segment your physical network into multiple logical networks.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Virtual Network**.

Step 2 Click **Create Virtual Network**.

The **Create Virtual Network** slide-in pane appears.

Step 3 In the **Name** field, enter the name of the virtual network.

Step 4 (Optional) From the **vManage VPN** drop-down list, choose a vManage VPN.

You must configure the vManage settings before adding the vManage VPN service. For more information, see the Cisco DNA Center Administrator Guide.

Step 5 Check the **Guest Virtual Network** check box to configure the virtual network as a guest network.

Step 6 Click **Save**.

Step 7 In the **Scalable Groups** column, click **Add** to add the scalable groups.

The **Add Scalable Group Associations** slide-in pane appears.

Step 8 Check the check boxes next to the scalable groups that you want to add to the virtual network and click **Save**.

Edit or Delete a Virtual Network

If you move a scalable group from a virtual network to another virtual network, the mappings for the scalable groups are changed. Be aware that users or devices in the group might be impacted by this change.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Virtual Network**.

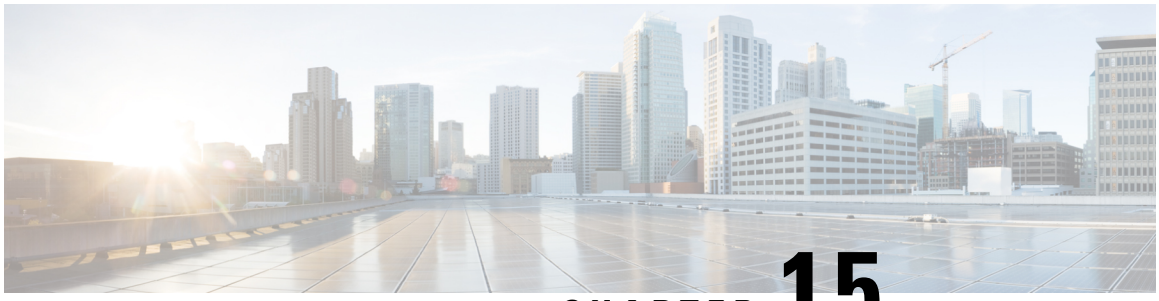
Step 2 To edit a virtual network, do one of the following:

- Click the name of the virtual network.
- Choose the virtual network and click **Actions > Edit**.

The **View Virtual Network** slide-in pane appears.

Field	Description
Name	This is a read-only field. You cannot edit the name of the virtual network.
Guest Virtual Network	Check this check box to configure the virtual network as a guest network.
Scalable Groups	Click **Add** in the **Scalable Groups** column to add the scalable groups. The **Add Scalable Group Associations** slide-in pane appears. Check the check boxes next to the scalable groups that you want to add and click **Save**. To edit or delete the scalable groups that are currently added to a virtual network: **a.** Click the link displayed in the **Scalable Groups** column. The **View Scalable Group Associations** slide-in pane appears. **b.** Click **Edit**. The following tabs are displayed: • **All**: Displays all the available scalable groups. The scalable groups that are currently added to the virtual network are highlighted in blue. • **Associated Groups**: Displays the scalable groups that are currently added to the virtual network. • **Other**: Displays the scalable groups that are not associated to this virtual network. **c.** Do the required changes and click **Save**.

Step 3 To delete a virtual network, choose the virtual network that you want to delete and then click **Actions > Delete**.



CHAPTER 15

Cisco AI Endpoint Analytics

Introduction to Cisco AI Endpoint Analytics

Visibility is the first step towards securing an endpoint. Cisco AI Endpoint Analytics is an endpoint visibility solution that helps you identify and profile endpoints and Internet of Things (IoT) devices. The Cisco AI Endpoint Analytics engine enables you to assign labels to endpoints, using the telemetry information received from the network from various sources.

You can assign profile labels to endpoints based on factors like the endpoint type, hardware model, manufacturer, operating system type, and so on. This is called multifactor classification.

Cisco AI Endpoint Analytics helps you gather endpoint telemetry from different sources. The primary source is the Network-Based Application Recognition (NBAR) mechanism. The NBAR mechanism is embedded in Cisco Catalyst 9000 Series switches (access devices) and performs deep packet inspection (DPI).

You can gather endpoint context information from various sources such as Cisco ISE, self-registration portals, and configuration management database (CMDB) software such as ServiceNow.

You can aggregate varied endpoint information and use the data to profile endpoints in Cisco AI Endpoint Analytics. After endpoints are profiled, AI and machine learning algorithms can also be used to reduce the number of unknown endpoints by intuitively leveraging different methods.

Key Features of Cisco AI Endpoint Analytics

- **Cisco AI Endpoint Analytics dashboard**

The Cisco AI Endpoint Analytics dashboard gives you a comprehensive view of the endpoints that are connected to your network. You can view the number of known, unknown, profiled, and unprofiled endpoints. You can also view intelligent profiling suggestions that are provided to enhance endpoint profiling and management.

- **Reduce net unknowns with machine learning capabilities**

  Cisco AI Endpoint Analytics provides profiling suggestions based on learnings from endpoint groupings. You can use these suggestions to reduce the number of unknown or unprofiled endpoints in your network.

- **Manage endpoints with system and custom profiling rules**

  Use Cisco-provided system rules and custom rules of your design to reliably profile and manage the endpoints connected to your network.

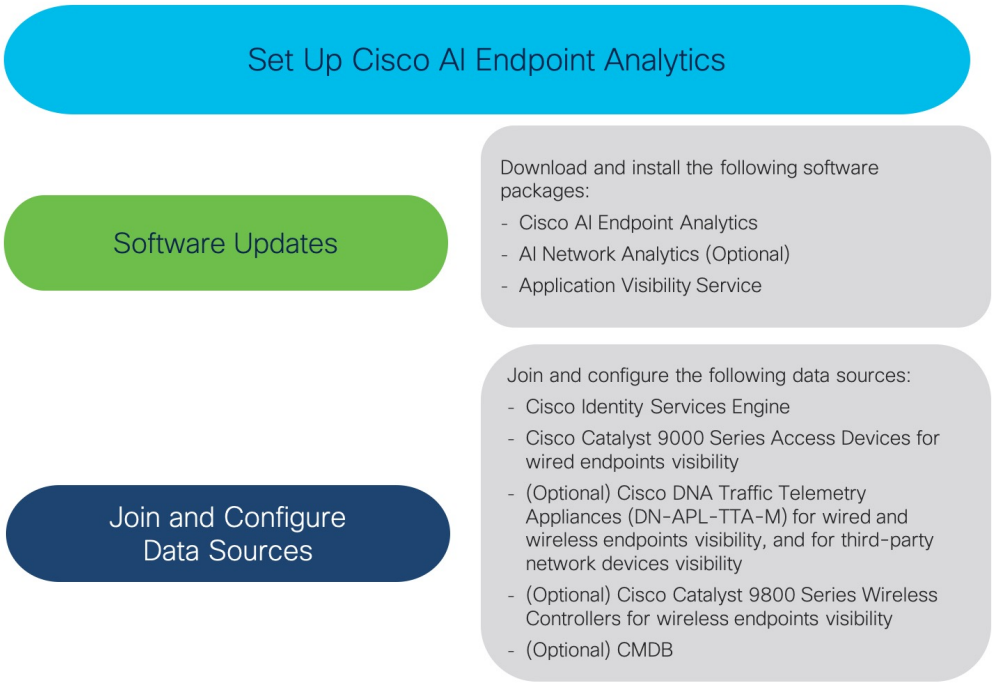
- **Registration of endpoints through Cisco AI Endpoint Analytics**

  You can onboard and profile endpoints using Cisco AI Endpoint Analytics. The endpoint attribute data that is collected through this registration process is used to profile the endpoints.

- **Registration of endpoints using external sources**

  You can connect some external sources of endpoint data, such as Configuration Management Databases (CMDB), to Cisco AI Endpoint Analytics. This allows you to easily register, manage, and profile endpoints in your network.

Set Up Cisco AI Endpoint Analytics in Cisco DNA Center



Install Software Updates

Install software updates in Cisco DNA Center to use Cisco AI Endpoint Analytics, as described in the following procedure.

Step 1 Log in to Cisco DNA Center.

Step 2 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **System** > **Software Updates**.

Step 3 In the **Updates** tab displayed, check if **Cisco AI Endpoint Analytics**, **AI Network Analytics**, and **Application Visibility Service** are listed in the **Application Updates** section. If any of these application updates are visible, click the **Install All** button.

- Install the **Cisco AI Endpoint Analytics** update to access the endpoint profiling solution in your Cisco DNA Center.
- Install the **AI Network Analytics** update to use machine learning and AI capabilities to receive intelligent profiling suggestions.
- Install the **Application Visibility Service** update to use NBAR and Controller-Based Application Recognition (CBAR) techniques to inform endpoint profiling.

Step 4 If any of these updates are not listed in the **Updates** tab, click **Installed Apps** tab to check if the updates are already installed and are available for use. The **Installed Apps** tab also confirms if the software installation has been successful.

Connect and Enable Data Sources

Note The data sources that Cisco AI Endpoint Analytics uses may already be connected to your Cisco DNA Center. If the data sources are connected, see the following instructions to ensure that the data sources are available for use by Cisco AI Endpoint Analytics.

You must add Cisco ISE or Catalyst 9000 Series access devices to Cisco DNA Center for Cisco AI Endpoint Analytics to provide results.

1. **Connect Cisco ISE to Cisco DNA Center.**

   See the "Integrate Cisco ISE with Cisco DNA Center" section in "Complete First-Time Setup" in the *Cisco DNA Center Appliance Installation Guide*.

   The following Cisco ISE releases support Cisco AI Endpoint Analytics:

   - 2.4 Patch 11 and later
   - 2.6 Patch 5 and later
   - 2.7 Patch 1 and later
   - 3.0

   In your Cisco ISE administration portal:

   a. Choose **Work Centers** > **Profiler** > **Settings**.

b. Check the **Enable Probe Data Publisher** check box.

After Cisco ISE authenticates endpoints through 802.1X or MAB authentication methods, the endpoint attributes collected are made available to Cisco AI Endpoint Analytics. The information is communicated through the probe data publisher.

2. **Connect Cisco 9000 Series access devices to Cisco DNA Center for wired endpoints visibility.**

   See "Discover Your Network" in the *Cisco DNA Center User Guide*.

   To enable Cisco AI Endpoint Analytics, upgrade your Cisco 9000 Series access devices to Cisco IOS-XE Release 17.3.1 or later.

   To enable CBAR for the required access devices, click the **Menu** icon (≡) in Cisco DNA Center:

   a. Choose **Provision** > **Services** > **All Services** > **Application Visibility**.

   b. Select the Cisco Catalyst 9000 access device that you need data from. Check the check box next to the device name in the **Site Devices** section.

   c. Click **Enable CBAR**.

3. **(Optional) Connect Cisco Catalyst 9800 Series Wireless Controllers to Cisco DNA Center for wireless endpoints visibility.**

   The following Cisco Catalyst 9800 Series Wireless Controller models are supported by Cisco AI Endpoint Analytics, in nonfabric mode:

   - 9800-CL
   - 9800-40
   - 9800-80
   - 9800-L

   To configure and provision a Cisco Catalyst 9800 Series Wireless Controller in Cisco DNA Center, see Cisco Catalyst 9800 Series Wireless Controller Overview, on page 391.

4. **(Optional) Connect Cisco DNA Traffic Telemetry Appliances to Cisco DNA Center for wired and wireless endpoints visibility, and for third-party network device visibility.**

   Cisco DNA Traffic Telemetry Appliances (DN-APL-TTA-M) generate telemetry from mirrored network traffic for endpoint analytics. This appliance enables Network-Based Application Recognition (NBAR)-based protocol inspection and endpoint attribute extraction.

   To receive endpoint attributes collected through the telemetry appliance in Cisco AI Endpoint Analytics, you must integrate Cisco ISE with Cisco DNA Center.

   See Cisco DNA Traffic Telemetry Appliances for information on installing the appliances, connectivity configurations, and managing the appliances in Cisco DNA Center.

   Enable CBAR on Switched Port Analyzer (SPAN)-receiving ports of access switches connected to Cisco DNA Traffic Telemetry Appliances with the following command:

   ```
   ip nbar protocol-discovery
   ```

   Not all endpoints that are connected to the telemetry appliances are visible in Cisco AI Endpoint Analytics. Only endpoints that are also connected to Network Access Devices (NADs) which are managed in Cisco DNA Assurance, are visible in Cisco AI Endpoint Analytics.

5. **(Optional) Enable ServiceNow in Cisco DNA Center.**

   After connecting ServiceNow to Cisco DNA Center, click the **Menu** icon (☰) in Cisco DNA Center and choose **Platform** > **Manage** > **Bundles**.

   If the **Status** of the bundle **Endpoint Attribute Retrieval with ITSM (ServiceNow)** is **New**, click **Enable** for the bundle.

6. **(Optional) Enable AI Endpoint Analytics in Cisco DNA Center.**

   To receive suggestions about AI-based endpoint groupings, automated custom profiling rules, and endpoint labels, you must enable **Cisco AI Analytics**.

   You must install the software AI Network Analytics to receive these AI-based suggestions.

   a. From the main menu of Cisco DNA Center, choose **System** > **Settings** > **External Services** > **Cisco AI Analytics**.

   b. Click the **AI Endpoint Analytics** toggle button to set it to green.

Endpoint Telemetry Sources

Cisco AI Endpoint Analytics receives telemetry data in the following ways.

- **Deep Packet Inspection**

  Deep packet inspection is an advanced method of packet analysis that is carried out by Cisco Catalyst 9000 Series access devices. These access devices run NBAR, which inspects application traffic and performs protocol analysis to discover, identify, and profile endpoints with high fidelity.

  Deep packet inspection profiling is based on various attributes that are collected from endpoint traffic to the network. These attributes are collected across multiple protocols, from packet header layers 4 to 7.

- **Configuration Management Database Connection**

  Cisco AI Endpoint Analytics receives endpoint data from your Configuration Management Database Connection (CMDB) for greater accuracy in endpoint profiling. The connection with ServiceNow enables you to receive information from the CMDB to Cisco AI Endpoint Analytics.

- **Machine Learning Capabilities**

  Data collected for profiling is anonymized and sent to a Cisco cloud location that serves as a device data lake. Here, machine learning algorithms analyze the data available to create profiling rules that you can evaluate and apply, as needed. Smart profiling rules are suggested through Cisco AI Endpoint Analytics to help make endpoint profiling and management simpler and more efficient for you. Existing rules too are evaluated and improvement suggestions provided based on this continuous learning.

Cisco AI Endpoint Analytics Overview Window

Choose **Policy** > **AI Endpoint Analytics** from the Cisco DNA Center main menu.

The **Overview** window displays the following dashlets:

- **Total Endpoints**

This dashlet displays the total number of endpoints in your network in two groups, **Fully Profiled** and **Missing Profiles**. Cisco AI Endpoint Analytics profiles endpoints on the basis of four factors, Endpoint Type, OS Type, Hardware Model, and Hardware Manufacturer. If one or more of these factors are missing for an endpoint, it is profiled in the **Missing Profiles** group.

- **AI Proposals**

  Cisco AI Endpoint Analytics uses smart grouping algorithms to group unknown endpoints in your network that have similar profiling data. If you have enabled AI Endpoint Analytics, you will receive the following types of rule proposals. These rule proposals are based on learnings from endpoint clusters:

  - New rules for profiling endpoints that may be similar.
  - Modification proposals for previously accepted rules.
  - Review of profiling rules that are no longer needed.

  For more details, see Modify Profiling Rule Suggestions, on page 347.

- **Endpoints Missing Profile Label**

  This dashlet displays the number of endpoints in your network with missing profiles, categorized by profile label type. There is some overlap in these displays. For example, if an endpoint does not have information for both OS Type and Hardware Model, the endpoint will be included in the count of both labels.

  To check the endpoints with a specific missing profile label, click the label in this dashlet. The **Endpoint Inventory** window displays a list of endpoints. This list is filtered to display the endpoints for which the selected profile label is unknown.

Endpoint Inventory

The endpoints that are connected to Cisco AI Endpoint Analytics through the data sources, in the **Endpoint Inventory** window. The window displays a table with the connected endpoints and their profiling information.

The window displays profiling information such as **Endpoint Type**, **OS Type**, **Location**, **LLDP System Description**, and so on.

To select the profiling information you want to view for the endpoints, click the vertical ellipsis icon at the top-right corner of the table. Choose one of the following sets of profiling information and click **Apply**:

- **All**: All the profiling information that are available is displayed. You cannot edit this set.
- **General**: This is a selection of profiling information that gives you a generic view of the endpoints. This is the set of columns displayed by default. You cannot edit this set.
- **Detailed**: This is a selection of profiling information that provides a deeper view of the endpoints. You cannot edit this set.
- **Custom**: This is the only set that you can edit. Check or uncheck the profiling information you want to view in the **Endpoint Inventory** window.

You can easily filter a set of endpoints based on your requirement. You can register endpoints, and edit, delete, and profile registered endpoints. To see the complete profiling details of an endpoint, click the **MAC Address** of the endpoint. The dialog box displayed contains user details, endpoint details, and attribute details of the

endpoint. In the **Endpoint Details** section, the following new fields are displayed in Cisco DNA Center Release 2.2.2 with the details received from Cisco ISE:

- **Authentication Status**: This field displays **Started** when an endpoint is authenticated through Cisco ISE, and **Disconnected** when it is not.
- **Authorization Profile**: The authorization policies configured for an endpoint in Cisco ISE are displayed here.
- **Scalable Group Tag**: The Scalable Group Tags configured for an endpoint in Cisco ISE are displayed here.

For information on these attributes, see the Cisco ISE Administrator Guide for the Cisco ISE release that you use.

You can select single or multiple endpoints by checking the check box adjacent to the MAC addresses to filter or perform the corresponding action.

To export a list of endpoints and their details from this window, click **Export**. If you apply any filters in the **Endpoint Inventory** window, only the filtered endpoints will be processed for export. To export the details of all the endpoints, ensure that no filters are applied when you click **Export.**

When you click **Export**, a new tab opens with the **Reports** window. The **Generated Reports** window contains a list of exports initiated, with the latest export request at the top of the list. A report generated from the Endpoint Inventory window contains **AI Endpoint Analytics** in its **Template Category** column. Report generation takes a few minutes. When a report is ready for download, the value in the **Last Run** column changes from **Not Initiated** to a timestamp with a download icon next to it. The timestamp refers to the time at which the export list was generated. Click the download icon to download a CSV file of the list of endpoints to your system.

You can also export Cisco AI Endpoint Analytics data from the **Reports** window, through the following steps:

Note You must run your first export of AI Endpoint Analytics data for endpoints from the **Endpoint Inventory** window. Then you can generate AI Endpoint Analytics reports directly from the **Reports** window.

1. Choose **Reports** from the main menu.
2. Click **Report Templates**, and choose **AI Endpoint Analytics** from the menu.
3. Click **Let's Do It** in the **Generate a New Report** dialog box.
4. In the **Select Report Template** window, the template **Endpoint Profiling** is applied by default. Click **Next**.
5. In the **Setup Report Scope** window, enter a value in the **Report Name** field. Define the filters that you want to apply to the list of endpoints to be exported from the **Endpoint Inventory** window. To export the details of all endpoints, do not choose any values in the **Scope** area. Click **Next**.
6. In the **Select File Type** window, the **Client Details** area allows you to review the chosen parameters. Edit the information to be exported by checking or unchecking the check boxes next to the relevant fields. Click **Next**.
7. In the **Schedule Report** window, click the radio button for **Run Now**, **Run Later (One-Time**, or **Run Recurring**. The **Run Later (One-Time** and **Run Recurring** options display scheduling fields to define the time of export. Click **Next**.

8. In the **Delivery and Notification** window, do not check the **Email Report** check box. Click **Next**.
9. In the **Summary** window, review all the configurations chosen in this workflow. To edit any configurations click the corresponding **Edit** option. Click **Next**.
10. The final window of the workflow informs you that your report is being generated. Click the **View Reports** link in this window for a list of generated reports. It takes a few minutes for the report to be generated and displayed in this window.

Filter Endpoints

Using the filter option, you can view and action upon a set of endpoints. These endpoints can you be filtered based their profiling data, primary profiling labels, known profiles, and health status.

In order to filter the endpoints, follow the below steps:

1. In the **Endpoint Inventory** window, click **Filter**.
2. Choose a value from each of the following drop-down list:
   - **Mac Address**
   - **Endpoint Type**
   - **Hardware Model**
   - **Hardware Manufacturer**
   - **OS Type**
   - **Registration status**
3. Click **Apply**.

You can also filter the profiled endpoints displayed by the four primary profiling labels. Click one or more of the labels in the **View Known Profiles** section.

The health status of endpoints is updated every five minutes.

Attribute Glossary

Attribute glossary is a list of all the profiling attributes available from Cisco ISE probe data.

In order to view all the profiling attributes, follow these steps:

1. In the **Endpoint Inventory** window, click the MAC address of an endpoint.
2. In the new area that is displayed on the right side, click **View Attribute Glossary**.

The **Attribute Glossary** window displays the following information for each attribute:

- **Key profiling attributes**
- **Description**
- **Associated Profile Labels**

- **Source**
- **Dictionary**
- **Discovery Method**

The glossary gives you a detailed view of all the profiling attributes. If a profiling attribute is frequently used to create a profile label, the label is listed in the **Associated Profile Labels** column.

You can also view the attribute glossary in the **Choose Attribute Condition** window while creating a logical condition for the rules. For more information, see Create a Custom Rule.

Register Endpoints

You can onboard and profile new endpoints by registering them in Cisco AI Endpoint Analytics. The profiling information of an endpoint is the source of truth for classification. You can also update new profile information for a registered endpoint using the **Register Endpoint** option.

Step 1 Choose **Actions** > **Register Endpoints**.

Step 2 Choose whether you want to register a single endpoint or multiple endpoints, by clicking the **Single** or **Bulk** radio button.

Option	Steps
Single	Enter the **MAC Address**, **Endpoint Type**, **Hardware Model** and **Hardware Manufacturer** for the endpoint.
Bulk	**a.** Download a .csv template by clicking the **Download .csv Template** option. **b.** In the downloaded .csv file, enter the following details for each endpoint you must register: MAC address, endpoint type, hardware model, and hardware manufacturer. Save this file. **c.** Upload the .csv file using the **Choose a File** option. You can register a maximum of 500 endpoints at a time using the **Bulk** option.

Step 3 Click **Next**.

Step 4 Review the endpoint details in the **Review Endpoint** window. You can also edit the endpoint details, if changes are required.

Note While registering an existing endpoint, the profile label changes of the endpoint are reflected in purple color and can be edited.

Step 5 Click **Next** to continue with the registration process.

Step 6 Click **Register**.

Edit Registered Endpoints

You can update the profiling information of registered endpoints from the **Endpoint Inventory** window.

Step 1 Check the check box adjacent to the MAC address of the endpoint that you want to edit.

Step 2 Click **Actions**.

Step 3 Click **Edit Endpoint**.

Step 4 Enter the **Endpoint Type**, **Hardware Model**, and **Hardware Manufacturer** details.

Step 5 Click **Save**.

Delete Registered Endpoints

If there are registered endpoints that are no a longer part of your network, you can delete them from Cisco AI Endpoint Analytics.

Step 1 Check the check box adjacent to the MAC address of the endpoints that you want to delete.

Step 2 Click **Actions**.

Step 3 Click **Delete Endpoint**.

The following message is displayed:

```
Do you really want to delete the selected endpoint(s)?
```

Step 4 Click **Yes** to permanently delete the endpoint from Cisco AI Endpoint Analytics.

Trust Scores for Endpoint Spoofing Detection

Cisco AI Endpoint Analytics analyzes NetFlow telemetry data, and network probe data from Cisco ISE and SD-AVC devices, to detect spoofed endpoints.

Each endpoint type has a behavior model that is developed using machine learning algorithms. If an endpoint's behavior is unexpected of its endpoint type profile, the endpoint is assigned a Trust Score and listed as a spoofed endpoint.

The applications and server ports that are used by an endpoint are analyzed in this spoofing detection process. For example, if an endpoint profiled as a printer uses a video calling application, it is identified as a spoofed endpoint and assigned a Trust Score.

The trust scores assigned range from 1 through 10, and are categorized as follows:

Trust Score Category	Range	Probability of Spoofing
Low	1–3	High
Medium	4–6	Moderate
High	7–10	Low

You can then apply Adaptive Network Control (ANC) policies from Cisco ISE to enforce appropriate remediation actions on the endpoints. See section "Adaptive Network Control" in Chapter "Cisco ISE Admin Guide: Maintain and Monitor" of the *Cisco ISE Administrator Guide*.

The ANC policies are defined in Cisco ISE and allow you to apply remediation actions on chosen endpoints. You can apply ANC policies to quarantine, shut down, or port bounce an endpoint, or force endpoint reauthentication. When you apply an ANC policy to an endpoint with an undesirable Trust Score in Cisco AI Endpoint Analytics, a Change of Authorization (CoA) is sent to the endpoint from Cisco ISE.

An endpoint is identified by its MAC address. Cisco ISE sends the CoA to the endpoints that hold an active session for the identified MAC address at the time of the ANC application. Any endpoint with the same MAC address that does not have an active session in Cisco ISE at the time will match the ANC policy when a new session starts or when it must reauthenticate at the end of the configured reauthentication timer.

To verify which endpoint is being acted upon by the ANC policy, log in to your Cisco ISE administration portal. From the main menu, choose **Operations** > **RADIUS** > **Live Sessions**. Enter the MAC address of the spoofed endpoint in the **Endpoint ID** column, to filter the endpoints that share the same MAC address and currently have live sessions in Cisco ISE. These are the endpoints that will be affected by the ANC policy.

To view a historic log of the RADIUS sessions in Cisco ISE, from the main menu, choose **Operations** > **Reports** > **Reports** > **Endpoints and Users** > **RADIUS Authentications**.

To view or modify ANC policy application on endpoints in Cisco ISE, from the main menu, choose **Context Visibility** > **Endpoints**. Check the check box next to the MAC address of an endpoint and click the options displayed at the top of the list, as required.

Prerequisites

Prerequisites for receiving Trust Scores for spoofed endpoints:

- Cisco DNA Center is upgraded to Release 2.2.2 or later.
- Cisco ISE is connected to your on-premise Cisco DNA Center.
- Network access devices are managed by both Cisco DNA Assurance and Cisco ISE.

Note The endpoint spoofing detection feature supports a maximum of 500 network access devices with NetFlow export flows, as Cisco DNA Assurance supports only 500 NetFlow exporters.

- Endpoints connected to network access devices are authenticated through Cisco ISE.
- **AI Spoofing Detection** must be enabled.

AI Spoofing Detection Capability

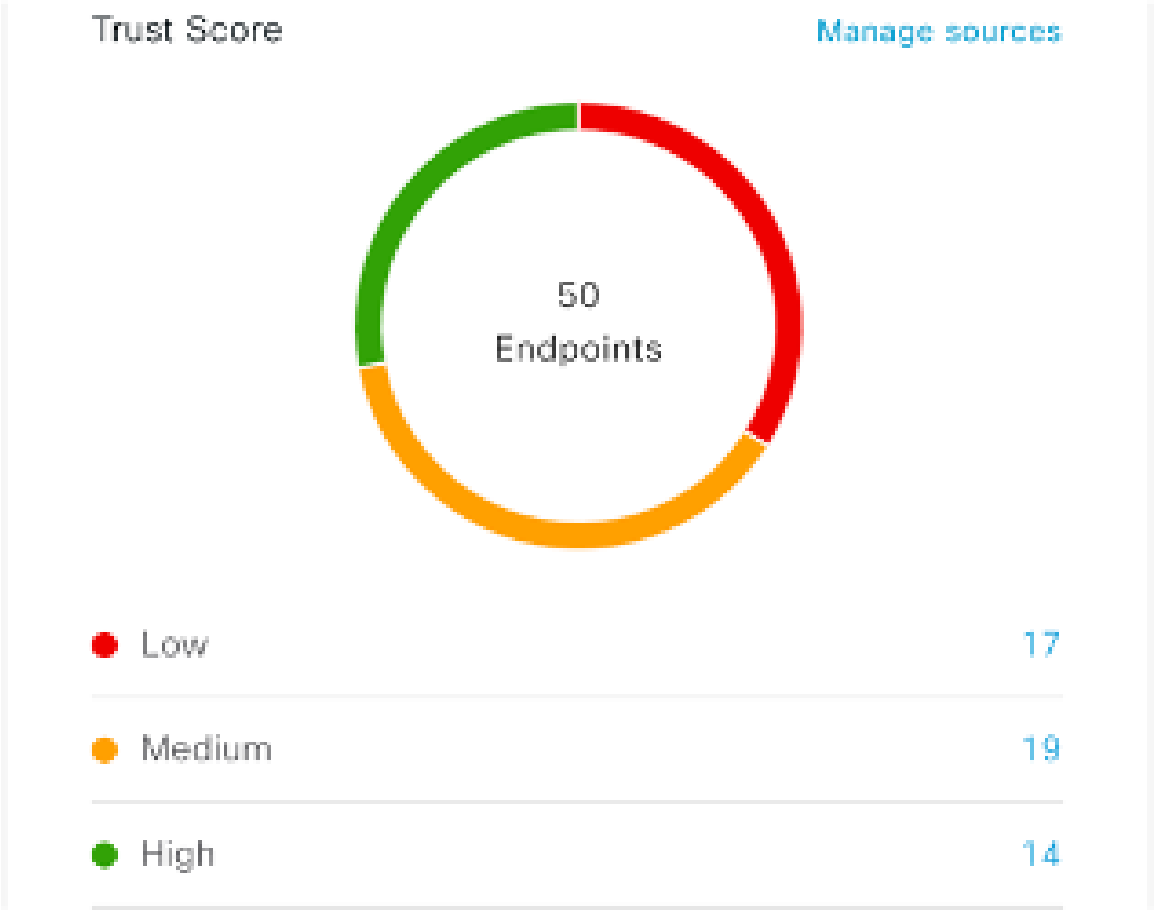
The **Cisco AI Analytics** software update for Cisco DNA Center Release 2.2.2 includes the capability **AI Spoofing Detection**. This capability is enabled by default.

From the main menu of Cisco DNA Center, choose **System** > **Settings** > **External Services** > **Cisco AI Analytics**. The **AI Spoofing Detection** section contains the **Enable AI Spoofing Detection** toggle button. This section also includes the **Send data to help Cisco improve the model** toggle button, also enabled by default.

You can disable either component by clicking the relevant toggle buttons in this window.

View and Manage Spoofed Endpoints

Figure 35: Trust Score dashlet in Cisco AI Endpoint Analytics Overview tab



After Cisco DNA Center is upgraded to Release 2.2.2 and AI Spoofing Detection is enabled, the Cisco AI Endpoint Analytics **Overview** tab (**Main Menu > Policy > AI Endpoint Analytics**) displays the **Trust Scores** dashlet. This dashlet contains the following:

- The total number of spoofed endpoints identified.
- A donut chart and a list of the number of endpoints with low, medium, and high trust scores.

To view the details of endpoints in a trust score category, click its endpoint count in the **Trust Scores** dashlet. The **Endpoint Inventory** tab is displayed with the appropriate filters applied.

In the **Endpoint Inventory** tab, you can view endpoints with Trust Scores in two ways:

- Click the **Focus:** drop-down list and choose **Trust Score** to see all the endpoints with Trust Scores assigned.

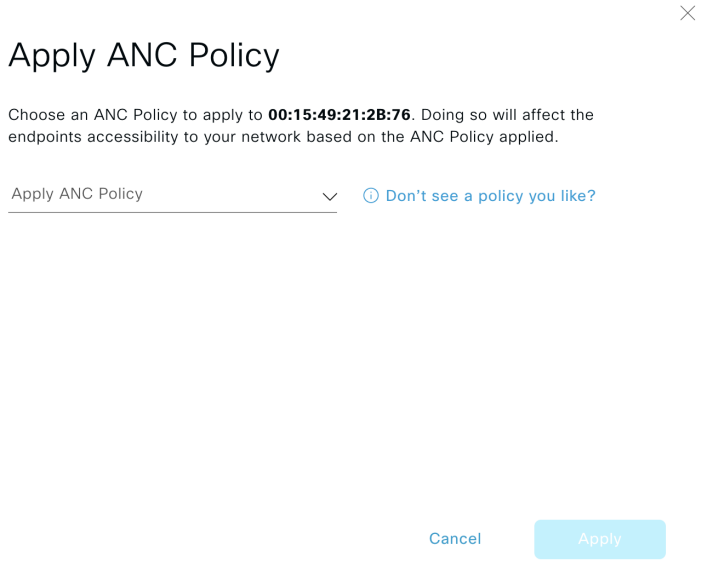
- Click **View endpoints in Trust Score View** from the caution message that is displayed, to see endpoints with Low and Medium scores.

The Trust Score views contain the following important columns, among others. You can also sort the data displayed according to these values:

- **Date Trust Score Reported**: The date and time when the endpoint's Trust Score was first reported.
- **Date ANC Policy Applied**: The date and time when the ANC Policy in use was applied to the endpoint.
- **Current ANC Policy**: The name of the ANC Policy in use.

You can perform the following actions on endpoints with Trust Scores:

- **Apply an ANC Policy**

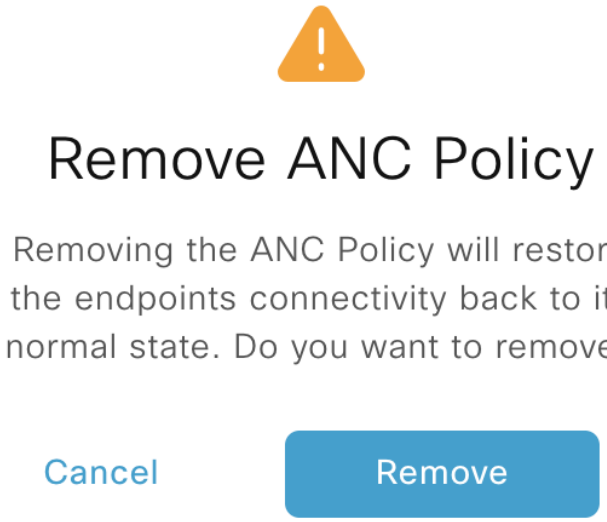


  Click the **Apply ANC Policy** button to choose an ANC policy to be applied to an endpoint. The endpoint's access to the network is modified accordingly. ANC policies are imported from Cisco ISE and displayed in the drop-down list in the pop-up window displayed.

- **Replace an ANC Policy**

Click **Change ANC Policy** button to replace an existing ANC policy of an endpoint with another ANC policy. From the pop-up window displayed, choose the new policy to be applied from the **Change ANC Policy** drop-down list.

- **Remove an ANC Policy**



Click the **Remove ANC Policy** button to remove an applied ANC policy from an endpoint. In the pop-up window displayed, click **Remove**. This removes the remediation policy that was applied to the endpoint, and allows the endpoint to connect to the network normally.

- **Reset Trust Score**

Figure 36: Reset Trust Score for an Endpoint Without an ANC Policy

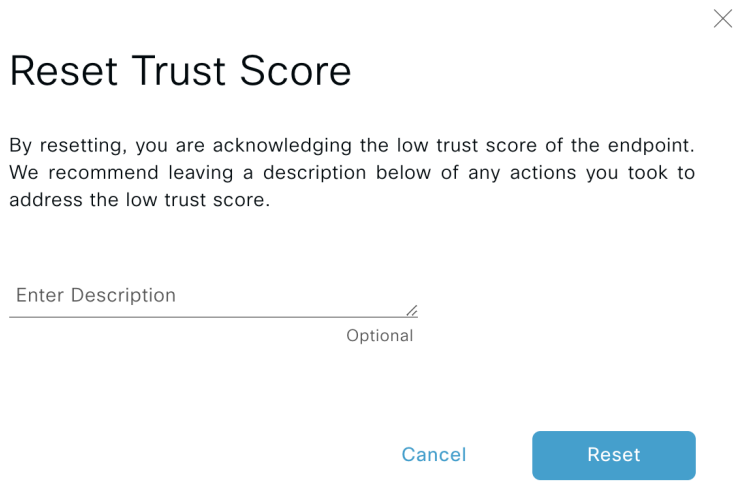
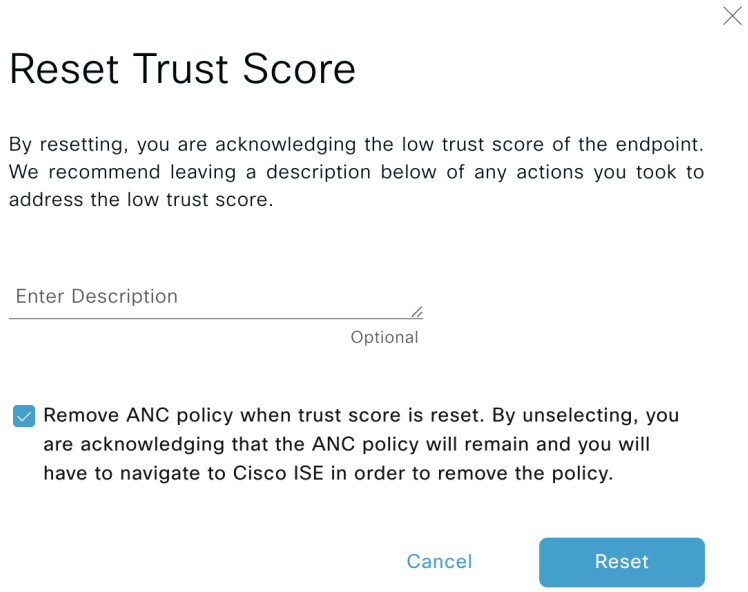


Figure 37: Reset Trust Score for an Endpoint with an ANC Policy



Click **Reset Trust Score** button to remove an endpoint from the Trust Score inventory. In the pop-up window displayed, click **Reset**.

If you choose this option for an endpoint after applying an ANC policy, you will not see this endpoint in the Trust Score inventory again. In this case, to modify the ANC policy for such an endpoint, you must remove the policy from Cisco ISE instead.

If you reset the score for an endpoint without applying an ANC policy, you may see the endpoint in the Trust Score inventory again with the next automatic refresh of Trust Score data.

The buttons for each of the actions are displayed in two locations in the **Endpoint Inventory** tab. The actions can be performed a single endpoint, or on multiple endpoints.

- **Manage Trust Score for Single Endpoint**

Figure 38: Trust Score Options for an Endpoint Without an ANC Policy

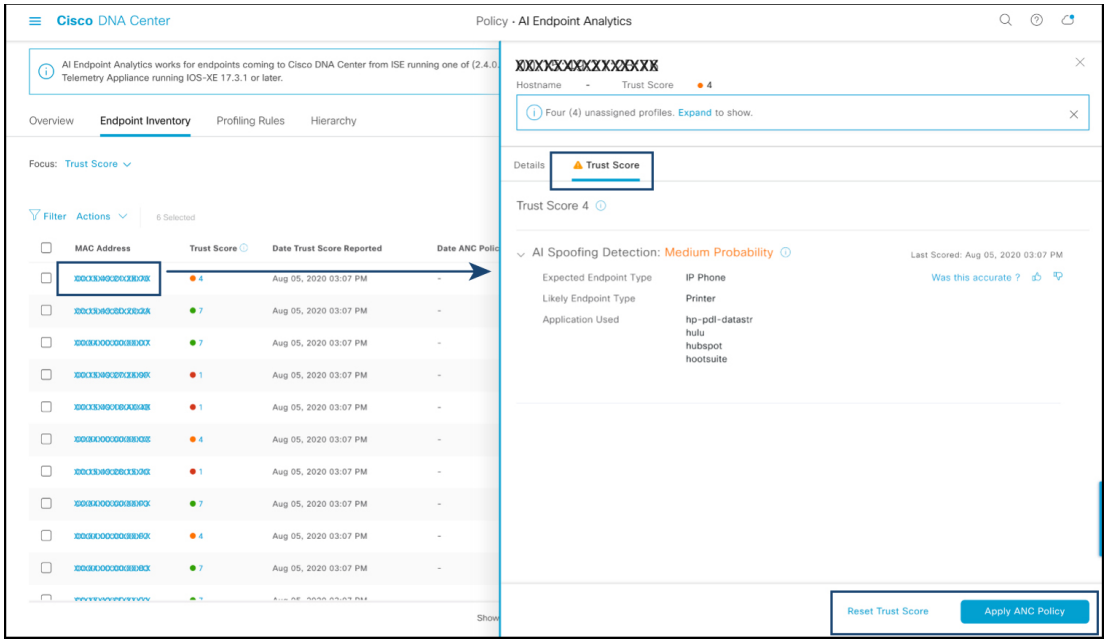
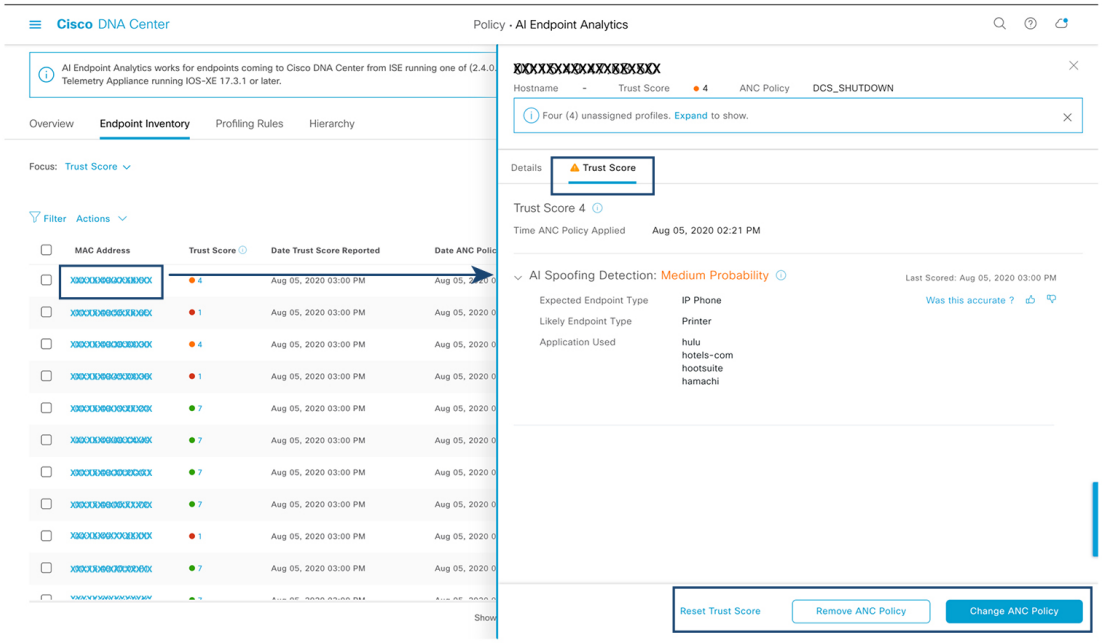


Figure 39: Trust Score Options for an Endpoint with an ANC Policy



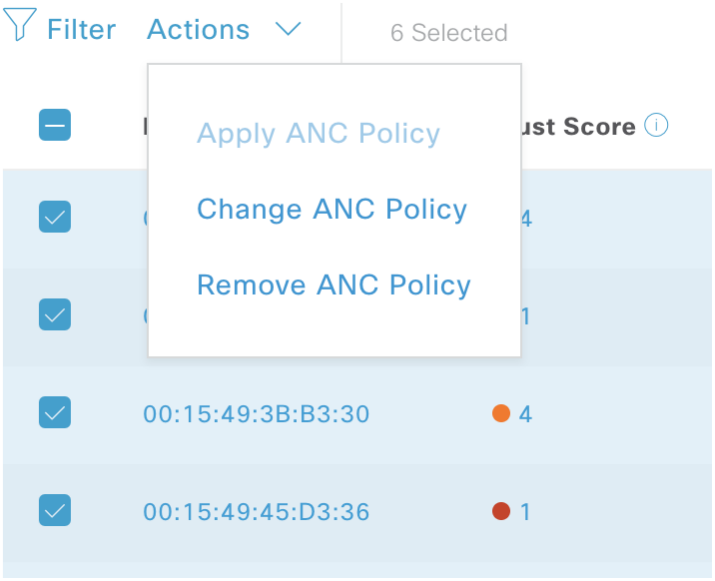
From the list of endpoints with a Trust Score, click the MAC Address of the endpoint you want to manage. In the endpoints details pane that is displayed, click the **Trust Score** tab.

Here, **Expected Endpoint Type** and **Likely Endpoint Type** values are displayed. The **Applications Used** field lists the applications that are used by the endpoint, that are unusual for the expected endpoint type.

This pane includes buttons to start the workflows of accepting and removing ANC policies, and to reset the Trust Score. Click the button for the intended task.

Alternatively, you can check the check box for an individual endpoint on the **Endpoint Inventory** window, click **Actions**, and choose the required option from the drop-down list.

- **Manage Trust Score for Multiple Endpoints**



In the **Endpoint Inventory** tab, check the check boxes for all the endpoints you must perform a specific action on. Click **Actions** and choose the required action from the drop-down list.

Profiling Rules

Profiling rules in Cisco AI Endpoint Analytics enable you to group endpoints with a combination of common attributes. These attributes allow endpoint identification by Endpoint Type, OS Type, Hardware model, and Hardware Manufacturer. The profiling rules help you administer and manage many endpoints with ease.

Cisco AI Endpoints Analytics receives profiling data from network devices through DPI, media protocols, medical industry protocols, and more. Profiling data from Cisco ISE is communicated through pxGrid. These profiling attributes are then available in the device dictionary for authoring profile rules.

You can view the profiling rules in the **Profiling Rules** tab of Cisco AI Endpoints Analytics. In the table that is displayed under this tab, click a **Rule Name** entry to view the assigned profiles and attributes used.

The profiling rules that are used to profile the endpoints in Cisco AI Endpoint Analytics are:

- System Rules
- Custom Rules
- Cisco AI Rules

Rule Prioritization

The profiling rules in Cisco AI Endpoint Analytics have an order of priority. Profiling rule execution follows this rule priority to profile endpoints with high fidelity.

As user inputs are primary in Cisco AI Endpoint Analytics, the priority of the profiling rules is as follows:

- Administrator-created static profiles, for example, profiles added using the **Register Endpoints** option.
- Administrator-created custom rules.
- Cisco-provided system rules that are available by default.
- Auto-generated rules through the machine learning-enabled Smart Grouping workflow.

To view the set rule priority, click **Rule Prioritization** in the **Profiling Rules** window.

A registered endpoint can be profiled by multiple Cisco AI Endpoint Analytics rules for different profiling labels. The following table shows the design of profiling rules for two endpoints.

Endpoint 1	Endpoint 2
Hardware Model profiled by System Rule	Hardware Model profiled by System Rule
OS Type profiled by Cisco AI Rule	Hardware Model profiled by Custom Rule
Hardware Manufacturer profiled by Custom Rule	Hardware Model profiled by Cisco AI Rule

For Endpoint 2, rule priority results in the precedence of the custom rule over the others. The Hardware Model label for Endpoint 2 is profiled by the custom rule.

For Endpoint 1, different rules define different profile labels, and each label is profiled accordingly.

Filter Profiling Rules

Step 1 In the **Profiling Rules** window, click **Filter**.

Step 2 Enter a name in the **Rule Name** field.

Step 3 Select values for endpoint attributes from the corresponding drop-down lists, to filter for a set of endpoints.

Step 4 Click **Apply**.

View Updated Profiling Rules

Step 1 Go to the **Endpoint Inventory** window.

Step 2 Click the check box adjacent to the MAC Address of the endpoint to view the profiling details of the endpoint.

Step 3 Click the information icon next to profile labels, and click the rule name to view the assigned profile and attributes details.

System Rules

Cisco AI Endpoint Analytics provides predefined rules called System rules for profiling endpoints. When Cisco AI Endpoint Analytics is deployed, it provides day zero visibility into endpoints without any need to configure specific rules.

Newly onboarded endpoints are profiled using system rules by default.

Network devices are managed in Cisco DNA Center in the **Provision** > **Network Devices** > **Inventory** window.

These network devices are profiled by the system rules and are not visible in the Cisco AI Endpoint Analytics **Endpoint Inventory** window. However, you can view the endpoints profiled by custom rules because the custom rules are created with network device as **Device Type**.

Automatic System Rule Updates for Endpoint Profiling

The system rules that are used for endpoint profiling in Cisco AI Endpoint Analytics are regularly updated to enhance profiling accuracy. Schedule automatic updates to receive updates in endpoint profiling system rules from Cisco. Your Cisco DNA Center receives updates at the configured time, and the changes are applied in Cisco AI Endpoint Analytics. In the **Profiling Rules** window (**Policy** > **AI Endpoint Analytics** > **Profiling Rules**), review the details of the changes in endpoint profiles, and accept or decline the system rule update.

If an endpoint's hardware model value changes due to an accepted system rule update, when you view the endpoint's details in the **Endpoint Inventory** tab, the **Hardware Model** field contains the name of the system rule update.

Before you begin

Configure and enable NBAR Cloud. See Configure the NBAR Cloud Connector, on page 467.

To check the status of NBAR Cloud, choose **Policy** > **AI Endpoint Analytics** > **Overview**, and click **Configuration**.

Step 1 From the main menu, choose **System** > **Settings** > **Cisco Accounts** > **Profile Rule Settings**.

The **Enabled** toggle button in the **Schedule Automatic Updates** area is set to active by default.

Step 2 Click the buttons for the days of the week on which you want to schedule updates. You can choose multiple days. Then, use the **Time Slot** text fields to select the time for the update. It takes 30 minutes for the updates to be received by Cisco DNA Center. The second time slot area is not editable and displays the time when the scheduled update is expected to complete.

Step 3 When your Cisco DNA Center receives a system rule update, a notification is displayed in the **Profiling Rules** window (**Policy** > **AI Endpoint Analytics** > **Profiling Rules**). The following notification is displayed when you click **Expand** in the dialog box:

You are updated to the latest version *Name of Latest Version* and a recent Cisco profiling rule has changed the profiles of some endpoints. Review Update.

Click **Review Update**

Step 4 The **Endpoint Profile Update Review** dialog box is displayed. The dialog box contains information on the current stable update applied, the latest update received, and more. It also contains the following sections that you can click to view the related endpoint profile updates:

a. **Major Updates**: Lists the endpoints whose profiles have had major changes, such as a Windows endpoint that is now recorded as a Linux endpoint.

b. **Minor Updates**: Lists the endpoints whose profiles have had minor changes, such as an updated version of Windows OS.

c. **Newly Profiled**: Lists the endpoints that were unprofiled previously and have now been assigned profile information.

Step 5 After you review the endpoint profile changes, to accept the profile update, click **Mark As Approved Version** in the **Endpoint Profile Update Review** dialog box. If you do not agree with the endpoint profile changes, click **Rollback**.

When you choose rollback, you must choose if you want to roll back to the last running version, or the last approved version, by clicking the corresponding option.

You can also perform the accept and rollback actions from the **AI Endpoint Analytics** > **Overview** > **Configuration** window.

Step 6 Click **X** to close the dialog box.

Custom Rules

In addition to the system rules, you can also create custom rules for profiling endpoints using a combination of endpoint attributes. Custom rules precede all the other endpoint profiling rules in Cisco AI Endpoint Analytics.

Logic and Conditions for Profiling Rules

You can create custom profiling rules in the **Endpoint Inventory** window. To create a custom profiling rule, you must create a logical condition based on endpoint attributes and values. These attributes are collected from network probe data and are different from the classification attributes available in the **Attribute Glossary** window.

A value is a user input that uniquely identifies the group of endpoints. The attributes and values create a regular expression with the help of the following operators.

Operators	Description
Contains	Attribute has the selected value.
Equals	Attribute is strictly mapped to the selected value.
Matches	Attribute should match the regular expression pattern of the selected value.
Starts With	Attribute should start with the selected value.

Note Contains, Equals, and Starts With are case-sensitive operators. For case-insensitive values, use the Matches operator.

These conditions can be further combined with the help of logic (**AND** and **OR**) to create a nested rule.

Create and Edit a Logical Condition

Follow the below instruction to create a logical condition.

Step 1 In the **Choose Attribute Conditions** window, check the check box adjacent to the **Attribute** that you want to update.

Step 2 Choose a option from the **Operator** drop-down lists.

Step 3 Enter the value in the **Value** field.

Step 4 Click **Next**.

Step 5 In the **Add Logic to Conditions** window that is displayed, drag and drop the **AND** logic or the **OR** logic between the conditions in order to create a logical sequence of conditions for a custom rule.

Note You can also add or edit an attribute condition in the **Add Logical Conditions** window using the vertical ellipsis next to a condition.

Step 6 Click **Next**.

Create a Custom Rule

Step 1 In the **Endpoint Inventory** window, check the check box adjacent to the MAC address of the endpoints that you want to profile.

Step 2 Click **Actions** and select **Profile with Custom Rules**.

Step 3 In the **Name Rule and Type** window that is displayed, in the **Rule Name** field, enter a name for the rule, and from the **Profile Label** drop-down list, choose a label.

Depending on what you choose from the **Profile Label** drop-down list, a corresponding field, whose name is dynamically updated, is displayed. For example, if you choose **Endpoint Type**, the **Endpoint Type** field appears.

Step 4 Enter a value in the new field that is displayed. As you start entering information, matching options are displayed. If an option matches your requirements, select the same. Otherwise, enter the complete type name.

Step 5 Click **Next**.

Step 6 In the **Choose Attribute Conditions** window that is displayed, create a logical condition.

For more information, see Logic and Conditions for Profiling Rules

Step 7 In the **Review Rule** window, review the list of endpoints that are going to be profiled with this custom rule.

Step 8 Click **Next**.

Step 9 Click **Profile**.

Edit a Custom Rule

Step 1 In the **Profiling Rules** window, check the check box adjacent to the admin rule you want to edit.

Step 2 Click **Actions** and select **Edit**.

Step 3 In the **Edit** window that is displayed, in the **Rule Name** field, enter a name for the rule, and select or enter the profile details based on the **Profile Label** selected during the rule creation.

Step 4 In the **Logic and Conditions** section, click on the vertical ellipsis and select **Edit** to update the logic and conditions for profiling rules. For more information, see Logic and Conditions for Profiling Rules.

Step 5 Click **Next**.

Step 6 Click **Apply**.
After the existing rule is updated with new profiling details, the endpoints profiled with this rule are updated with new profiling details.

Delete a Custom Rule

Step 1 In the **Profiling Rules** window, check the check box next to the rule that you want to delete.

Step 2 Click **Actions** and choose **Delete**.

The following message is displayed:

```
Do you really want to delete the selected Rule(s)?
```

Step 3 Click **Yes** to permanently delete the rule from Cisco AI Endpoint Analytics.

After the custom rule is deleted, the endpoints profiled with this rule are updated with system rules.

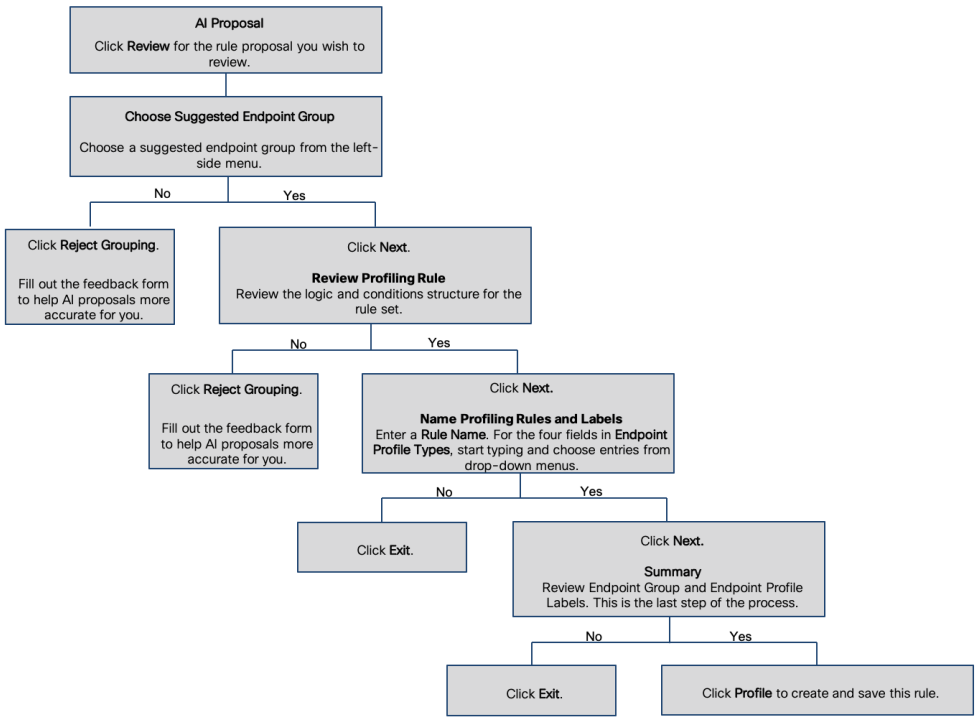
Cisco AI Rules or Smart Grouping

Cisco AI Endpoint Analytics uses ML cloud to group unknown endpoints on your network dynamically. It also allows you to assign custom labels to groups of unknown endpoints. You can review the clusters and accept or reject the profiling suggestions provided.

When you accept the profiling suggestions, a profiling rule is automatically created to profile the selected endpoints, and to profile similar endpoints that join your network in the future.

Modify Profiling Rule Suggestions

The **AI Proposal** dashlet on the **Endpoint Analytics** home page displays rule suggestions based on the endpoint clusters generated by Smart Grouping. To view an AI proposal, click **Review** adjacent to the corresponding proposal type and proceed according to the following decision chart.



Import Profiling Rules

You can migrate your custom profiling rules and Cisco AI rules by importing the .json files.

Step 1 In the **Profiling Rule** window, click **Actions**

Step 2 Choose **Import Profiling Rules**.

Step 3 Click **Choose a file** and browse to the .json file in your system.

Step 4 Click **Ok**.

Export Profiling Rules

You can export and back up custom rules and Cisco AI profiling rules from Cisco AI Endpoint Analytics. The **Export Profiling Rules** option exports all the available custom rules and Cisco AI profiling rules. You cannot selectively export rules.

Step 1 In the **Profiling Rules** window, click **Actions**.

Step 2 Choose **Export Profiling Rules**.

Step 3 Click **Yes** to export all the custom and ML profiling rules. Click **No** to exit.

Note You can import the same file again into Cisco AI Endpoint Analytics.

Hierarchy

Cisco AI Endpoint Analytics hierarchy helps you create logical groupings of endpoints, based on the endpoint types. Creating categories and subcategories for the endpoints focuses on endpoint visibility and simplifies the authorization process.

You can create categories from the **All Endpoints** default parent category. The category details such as total number of endpoints, endpoint types, and subcategories are listed within individual boxes in the **Hierarchy** window.

You can create, edit, and delete the categories to reorder the hierarchy.

Create Category and Subcategory

Step 1 In the **Hierarchy** window, click the horizontal ellipsis of the parent category.
Step 2 Click **Create Category**.
Step 3 Enter a category name.
Step 4 Click **Enter**.

What to do next

After you create a category, you can drag and drop endpoint types from the **Endpoint Type** window, or edit the category to add endpoints to it.

Edit a Category or Subcategory

Step 1 In the **Hierarchy** window, click on the horizontal ellipsis of the category.
Step 2 Click **Edit**.
Step 3 In the **Edit** window that is displayed, enter the **Category Name**.
Step 4 Enter the **Parent Category** from the drop-down menu, if you want to reassign the category.
Step 5 Click the **Endpoint Type** tab.
Step 6 Click **Actions** and select **Add Endpoint Type**.
Step 7 Choose the endpoint type from the **Search Dropdown** list.
Step 8 Click **Save**.

What to do next

In the Endpoint Type window, you can filter the endpoint types as **All**, **Available**, and **Assigned**.

Delete Endpoint Types from Category

Step 1 In the **Hierarchy** window, click the horizontal ellipsis of the category that you want to delete.

Step 2 Click **Edit**.

Step 3 In the **Edit** window, click the **Endpoint Type** tab.

Step 4 Check the check box adjacent to the endpoint type that you want to delete.

Step 5 Click **Actions** and choose **Remove From Category**.

The following message displays:

```
Are you sure you want to delete this category?
```

Step 6 Click **Yes** to delete the endpoint from the category. Click **No** to exit.

Reassign Endpoint Types from Category

Step 1 In the **Hierarchy** window, click the horizontal ellipsis of the category.

Step 2 Click **Edit**.

Step 3 In the **Edit** window, click the **Endpoint Type** tab.

Step 4 Check the check box adjacent to the endpoint type that you want to reassign.

Step 5 Click **Actions** and choose **Re-assign to existing category** or **Re-assign to a new category**.

Option	Steps
Re-assign to existing category	**a.** In the **Reassign** window, choose an existing category from the **Category** drop down list. **b.** Click **Save**.
Re-assign to a new category	**a.** In the **Reassign** window, choose **New Category** from the **Category** drop down list. **b.** Choose a parent category from the **Parent Category** drop down list. **c.** Enter the category name in the **New Category** field. **d.** Click **Save**

Delete a Category

Before you begin

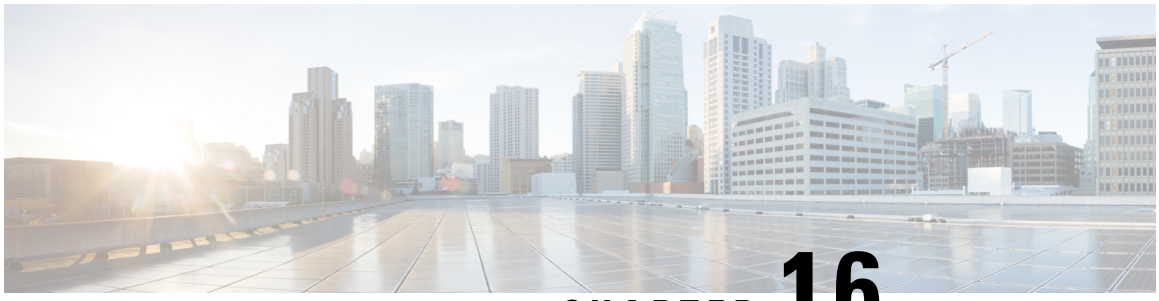
Before you delete a parent category, check its subcategories. You can reassign the subcategories to another existing category or to a new category. Otherwise, all the subcategories will get deleted along with the parent category. You can also reassign the subcategories while you are deleting a category.

Step 1 In the **Hierarchy** window, click on the horizontal ellipsis of the category.

Step 2 Click **Delete**.

If you are deleting a category that has subcategories assigned to it, the **Reassign Relationships** dialog box is displayed. Select the one of the following options:

Option	Condition	Steps
Reassign to an existing category	Reassign the subcategories to an existing category.	**a.** Select a category from the **Category** drop-down list. **b.** Click **Reassign**. The parent category is deleted and its subcategories will be reassigned to the selected category.
Reassign to a new category	Reassign the subcategories to an existing category.	**a.** Select a category from the **Parent Category** drop-down list. **b.** Enter the category name in the **New Category** field. **c.** Click **Reassign**. The parent category is deleted and its subcategories are reassigned to the new category.
Remove from category	Delete the subcategories along with the parent category.	Click **Reassign**. The parent category and its subcategories are deleted.



CHAPTER 16

Provision Your Network

Provisioning

After you have configured the policies for your network in Cisco DNA Center, you can provision your devices. In this stage, you onboard devices and deploy the policies across them.

Provisioning devices includes the following aspects:

- Onboarding devices with Plug and Play, which adds them to the inventory.
- Deploying the required settings and policies to devices in the inventory.
- Adding devices to sites.
- Creating fabric domains and adding devices to the fabric.

Cisco DNA Center provisioning supports only IBNS 2.0, which changes the AAA configuration and converts all relevant authentication commands to their Class-Based Policy Language (CPL) control policy equivalents. Because the CPL conversion disables the conversion CLI **authentication display [legacy|new-style]**, we recommend that you back up your current configuration. Also, plan your change management windows to support AAA configuration updates (aligned with IBNS 2.0).

Onboard Devices with Plug and Play Provisioning

Plug and Play provisioning provides a way to automatically and remotely provision and onboard new network devices with minimal network administrator and field personnel involvement.

Using Plug and Play provisioning, you can do the following:

- Provision devices by assigning a site, deploying site settings, installing a device software image, and applying a custom onboarding configuration.

- Plan devices before their installation by entering device information and choosing provisioning operations. When the device comes online, it contacts Cisco DNA Center and Plug and Play provisions and onboards the device automatically.
- Provision unclaimed network devices, which are new devices that appear on the network, without prior planning.
- Synchronize the device inventory from the Cisco Plug and Play Connect cloud portal in a Cisco Smart Account to Plug and Play, so that all the devices appear in Cisco DNA Center.
- Display the detailed onboarding status of network devices.

Prerequisites

Before using Plug and Play provisioning, do the following:

- Set the Cisco Smart Account credentials in the main Cisco DNA Center settings by using **System > Settings > Smart Account**.
- Accept the End User License Agreement (EULA) in the main Cisco DNA Center settings by using **System > Settings > Device EULA Acceptance**.
- Ensure that Cisco network devices to be provisioned have a supported software release and are in a factory default state. If you are using a network device that was previously configured or is in an unknown state, see the device clean-up and reset details in the Network Plug and Play Troubleshooting Guide for Cisco DNA Center.

The following sections describe typical use cases and workflows for Plug and Play provisioning.

Planned Provisioning

An administrator can plan the provisioning of a new site or other group of network devices as follows:

1. Define the site within the network hierarchy. See About Network Hierarchy, on page 110.
2. Optionally, define Onboarding Configuration templates to be applied to devices. Such templates contain basic network configuration commands to onboard a device so that it can be managed on the network. In many cases, such templates are not necessary unless you need to customize the Day 0 configuration. See Create Templates to Automate Device Configuration Changes, on page 193.
3. Define network profiles for the types of devices you are deploying. See Create Network Profiles, on page 164.
4. Define the device credentials (CLI and SNMP) for the devices you are deploying. If you are using SNMPv2c, both Read and Write credentials must be provided. See About Device Credentials, on page 174.
5. Optionally, ensure that software images for the devices to be provisioned are uploaded and marked as golden in the Image Repository. See Import a Software Image, on page 91.
6. Add details about planned devices one at a time or in bulk with a CSV file. See Add or Edit a Device, on page 361 or Add Devices in Bulk, on page 362.
7. Devices boot up and are automatically provisioned.

Unclaimed Provisioning

If a new network device is added to the network before it can be planned, it is labeled as an unclaimed device. An unclaimed device can be added manually by an administrator, or automatically through one of the discovery methods described in Controller Discovery Prerequisites, on page 355. An administrator can provision the device as follows:

1. Find the device on the devices list by filtering on unclaimed devices or searching for it by name. See View Devices, on page 359.
2. Claim the device by assigning a site, image, configuration template, or profile. See Provision a Device with Plug and Play, on page 364.

Cisco Smart Account Synchronization and Provisioning

Network devices can be automatically registered through a Cisco Smart Account with the Cisco Plug and Play Connect cloud service. An administrator can synchronize the device inventory from Cisco Plug and Play Connect to Cisco DNA Center Plug and Play, so that all the devices appear in Cisco DNA Center. These devices can then be claimed and provisioned.

1. Register a Smart Account and virtual account with which to synchronize. See Register or Edit a Virtual Account Profile, on page 362.
2. Synchronize the device inventory from the Smart Account. See Add Devices from a Smart Account, on page 363.
3. Find the device on the devices list by filtering on unclaimed devices or searching for it by name. See View Devices, on page 359.
4. Claim the device by assigning a site, image, configuration template, or profile. See Provision a Device with Plug and Play, on page 364.
5. Devices boot up and are automatically provisioned.

Controller Discovery Prerequisites

Plug and Play automates device onboarding and requires that devices must be able to discover and contact the Cisco DNA Center controller. Devices must be able to automatically discover the controller in one of the following ways:

- DHCP—See DHCP Controller Discovery, on page 355.
- DNS—See DNS Controller Discovery, on page 357.
- Cisco Plug and Play Connect cloud service—See Plug and Play Connect Controller Discovery, on page 357.

DHCP Controller Discovery

When a Cisco network device first starts up with no startup configuration, it attempts to discover the Cisco DNA Center controller by using DHCP Option 43.

The prerequisites for the DHCP discovery method are as follows:

- New devices can reach the DHCP server.

- The DHCP server is configured with Option 43 for Cisco Plug and Play. This option informs the network device of the IP address of the Cisco DNA Center controller.

  When the DHCP server receives a DHCP discover message from the device, with Option 60 containing the string “ciscopnp”, it responds to the device by returning a response that contains the Option 43 information. The Cisco Plug and Play IOS Agent in the device extracts the Cisco DNA Center controller IP address from the response and uses this address to communicate with the controller.

DHCP Option 43 consists of a string value that is configured as follows on a Cisco router CLI that is acting as a DHCP server:

```
ip dhcp pool pnp_device_pool         <-- Name of DHCP pool
network 192.168.1.0 255.255.255.0    <-- Range of IP addresses assigned to clients
default-router 192.168.1.1           <-- Gateway address
option 43 ascii "5A1N;B2;K4;I172.19.45.222;J80;"    <-- Option 43 string
```

The Option 43 string has the following components, delimited by semicolons:

- 5A1N;—Specifies the DHCP suboption for Plug and Play, active operation, version 1, no debug information. It is not necessary to change this part of the string.
- B2;—IP address type:
  - B1 = hostname
  - B2 = IPv4 (default)
- I*xxx.xxx.xxx.xxx*;—IP address or hostname of the Cisco DNA Center controller (following a capital letter i). In this example, the IP address is 172.19.45.222.
- J*xxxx*—Port number to use to connect to the Cisco DNA Center controller. In this example, the port number is 80. The default is port 80 for HTTP and port 443 for HTTPS.
- K4;—Transport protocol to be used between the device and the controller:
  - K4 = HTTP (default)
  - K5 = HTTPS
- T*trustpoolBundleURL*;—Optional parameter that specifies the external URL of the trustpool bundle if it is to be retrieved from a different location than the default, which is the Cisco DNA Center controller, which gets the bundle from the Cisco InfoSec cloud (http://www.cisco.com/security/pki/). For example, to download the bundle from a TFTP server at 10.30.30.10, you would specify the parameter like this: Tftp://10.30.30.10/ios.p7b

  If you are using trustpool security and you do not specify the T parameter, the device retrieves the trustpool bundle from the Cisco DNA Center controller.
- Z*xxx.xxx.xxx.xxx*;—IP address of the NTP server. This parameter is mandatory when using trustpool security to ensure that all devices are synchronized.

See the *Cisco IOS Command Reference* for additional details on DHCP configuration.

If DHCP Option 43 is not configured, the device cannot contact the DHCP server, or this method fails for another reason, the network device attempts discovery using DNS. For more information, see DNS Controller Discovery, on page 357.

If the Cisco DNA Center system certificate has an FQDN-only SAN field, you must edit the DHCP pool on the seed device to contain the Option 43 string with FQDN, B2 to B1, dns-server, and domain-name before starting PnP.

If the DHCP pool relies on Cisco switches or routers, a sample configuration is as follows:

```
ip dhcp pool PnP_Pool
network 214.2.64.0255.255.255.0
default-router 214.2.64.1
option 43 ascii "5A1D;B1;K4;I<FQDN>;J80"
domain-name sitdns.com
dns-server 17.1.104.100
```

DNS Controller Discovery

If DHCP discovery fails to get the IP address of the Cisco DNA Center controller, the network device falls back on the DNS lookup method. Based on the network domain name returned by the DHCP server, it constructs a fully qualified domain name (FQDN) for the controller, using the preset hostname pnpserver. The NTP server name is based on the preset hostname pnpntpserver.

For example, if the DHCP server returns the domain name “customer.com”, the network device constructs the controller FQDN of pnpserver.customer.com. It then uses the local name server to resolve the IP address for this FQDN. The NTP server name FQDN would be pnpntpserver.customer.com.

The prerequisites for the DNS discovery method are as follows:

- New devices can reach the DHCP server.
- The Cisco DNA Center controller is deployed with the hostname “pnpserver”.
- The NTP server is deployed with the hostname pnpntpserver.

Plug and Play Connect Controller Discovery

In situations where using the DHCP or DNS discovery methods is not an option, the Cisco Plug and Play Connect cloud service allows devices to discover the IP address of the Cisco DNA Center controller. When the network device boots up, if it cannot locate the controller through DHCP or DNS, then it tries Plug and Play Connect by contacting devicehelper.cisco.com to obtain the IP address of the appropriate controller that is defined for your organization. To secure the communications, the first thing that the device does when contacting Plug and Play Connect is to download and install the Cisco trustpool bundle.

The following steps summarize how to use Cisco Plug and Play to deploy a Cisco network device by using Plug and Play Connect for discovery.

Before you begin

Cisco network devices are running Cisco IOS images that support Cisco Plug and Play and have connectivity to the Cisco Plug and Play Connect cloud service.

Step 1 The network administrator configures the controller profile for the appropriate Cisco DNA Center controller for your organization by using Plug and Play Connect in the Cisco Smart Account web portal. For more information, see the Smart Account documentation in the web portal.

Step 2 If you order plug and play network devices through Cisco Commerce Workspace (CCW), these network devices are automatically registered with Plug and Play Connect as long as a Cisco Smart Account is assigned to the order and you include the NETWORK-PNP-LIC option for each device that you want to use with Cisco Plug and Play.

This option causes the device serial number and PID to be automatically registered in your Smart Account for plug and play. If you have specified a default controller, then the devices are automatically assigned to that controller when the order is processed.

Step 3 Alternatively, you can manually add devices in the Plug and Play Connect web portal.

Step 4 Register the Cisco DNA Center controller as a controller for Cisco Plug and Play Connect in a Cisco Smart Account, for redirection services. See Register or Edit a Virtual Account Profile, on page 362.

This step is required if you order plug and play network devices through CCW and these network devices are automatically registered with Plug and Play Connect through your Smart Account.

Step 5 Synchronize the device inventory from the Smart Account in the Cisco Plug and Play Connect cloud portal to Cisco DNA Center Plug and Play.

Devices registered in the Plug and Play Connect web portal are synced to the controller and appear in the plug and play device list with a source of SmartAccount.

Step 6 Claim the newly synced devices. See Provision a Device with Plug and Play, on page 364.

Step 7 The device installer installs and powers up the Cisco network device.

Step 8 The device discovers the Cisco DNA Center controller by querying the Plug and Play Connect service, identifies itself by serial number to Plug and Play in Cisco DNA Center, then is provisioned according to what was planned for it during the claim process.

Note The device will fail to contact Plug and Play Connect if the device cannot synchronize with the predefined NTP servers **time-pnp.cisco.com** or **pool.ntp.org**. To resolve this problem, either unblock NTP traffic to these two host names, or map these two NTP host names to local NTP server addresses on the DNS server.

Plug and Play Deployment Guidelines

Follow these recommendations when using Plug and Play:

- Device bring up order: In general, routing and upstream devices should be brought up first. Once the router and all upstream devices are up and provisioned, switches and downstream devices can be brought up. The Plug and Play agent in a device attempts to auto-discover the Cisco DNA Center controller only during initial device startup. If at this time, the device cannot contact the controller, device provisioning fails, so upstream devices should be provisioned first.
- Cisco Router Trunk/Access Port Configuration: Typical branch networks include routers and switches. One or more switches are connected to the WAN router and other endpoints like IP phones and access points connect to the switches. When a switch connects to an upstream router, the following deployment models are supported for Plug and Play:
  - Downstream switch is connected to the router using a switched port on the router. In this type of connection, the switched port on the router can be configured as a trunk or access port.
  - Downstream switch is connected to the router using a routed port on the router. In this case, the routed port can support multiple VLANs using sub-interfaces. During the Plug and Play process, the switch would automatically configure its port as a trunk port. In a large branch scenario, it becomes necessary to carry multiple VLANs between the router and the downstream switch. To support this use case, the switch must be connected to a routed port.

- Non-VLAN 1 configuration: Plug and Play supports devices using VLAN 1 by default. If you want to use a VLAN other than 1, adjacent upstream devices must use supported releases and you must configure the following global CLI command on the upstream device to push this CLI to the upcoming Plug and Play device: **pnp startup-vlan** *x*. When you execute this command on an adjacent upstream device, the VLAN membership change does not happen on that device. However, the active interfaces on the upcoming Plug and Play device that are connected to the upstream device are changed to the specified VLAN. This guideline applies to both routers and switches and should be used only for trunk mode scenarios and not access mode.

View Devices

This procedure shows how to view Plug and Play devices, how to perform actions on them, and how to add new devices.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Plug and Play**.

Step 2 View the devices in the table.

You can use the **Filter** option to find specific devices. Click **Refresh** to refresh the device list.

Step 3 Click the name of a device.

A window with the device details is displayed.

Step 4 Click the **Details**, **History**, and **Configuration** or **Stack** tabs to view the different types of information for the device. Some tabs have additional links that you can click for more information.

The **Stack** tab appears only for a switch stack device.

Step 5 Click the following actions at the top of the dialog box to perform specific tasks on the device. Available actions depend on the device state.

- **Refresh**: Refreshes the device state information.
- **Claim**: Claims and provisions the device. See Provision a Device with Plug and Play, on page 364.
- **Edit**: Edits the device. See Add or Edit a Device, on page 361.
- **Reset**: Resets the device if it is in an error state. See Reset a Device, on page 374.
- **Delete**: Deletes the device. See Delete a Device, on page 373.

Step 6 To perform an action on multiple devices, click the check box next to each device in the table view and choose an action from the **Actions** drop-down menu.

Step 7 Click **Add Device** to add a new device.

See the following for more information about adding devices in different ways: Add or Edit a Device, on page 361, Add Devices in Bulk, on page 362, or Add Devices from a Smart Account, on page 363.

The Device table displays the information shown in the following table for each device. Some of the columns support sorting. Click the column header to sort the rows in ascending order, if sorting is supported. Click the column header again to sort the rows in descending order.

Note Some of the columns are hidden in the default column view setting, which can be customized by clicking the three dots (⋮) at the right end of the column headings.

Table 49: Device Information

Column	Description
#	Row number.
Device Name	Hostname of the device. Click this link to open the device details window. A stack icon indicates a switch stack.
Serial Number	Device serial number.
Product ID	Device product ID.
IP Address	Device IP address.
Source	Source of the device entry: • User: User added the device through the GUI or API. • Network: Unclaimed device that has contacted the controller. • SmartAccount: Device was synced from a Smart Account.
State	• Unclaimed: Device has not been provisioned. • Planned: Device has been claimed but has not yet contacted the server. • Onboarding: Device onboarding is in progress. • Provisioned: Device is successfully onboarded and added to inventory. • Error: Device had an error and could not be provisioned.
Onboarding State	Onboarding state of the device. Click on the progress bar to go to the device history.
Site	Site with which the device is associated.
Last Contact	Last date and time the device contacted Plug and Play.
Smart Account	Cisco Smart Account with which the device is associated.
Virtual Account	Virtual Account (within the Cisco Smart Account) with which the device is associated.
Created	Date and time when the device was added to Plug and Play.

Add or Edit a Device

This procedure shows how to add or edit a device from the Plug and Play Devices list. Alternatively, you can edit a device from the device details window by clicking **Edit**.

Table 50: Device Fields

Field	Description
Serial Number	Device serial number (read only if you are editing a device).
Product ID	Device product ID (read only if you are editing a device).
Device Name	Device name.
Enable SUDI Authorization	Enables secure unique device identifier (SUDI) authorization on devices that support it.
SUDI Serial Numbers	Devices that support SUDI have two serial numbers: the chassis serial number and the SUDI serial number (called the License SN on the device label). Enter one or more comma-separated SUDI serial numbers in this field when adding a device that uses SUDI authorization. This field appears only if **Enable SUDI Authorization** is checked.
This Device Represents a Stack	Device represents a stack (this item is read only if you are editing a device). Applicable only for supported stackable switches.

Before you begin

If the device requires credentials, be sure that the global device credentials are set in the **Design** > **Network Settings** > **Device Credentials** page. For more information, see Configure Global CLI Credentials, on page 176.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Plug and Play**.

Step 2 View the devices in the table.

You can filter on device state by using one of the **Device State** buttons, or use the **Filter** option to find specific devices. Click **Refresh** to refresh the device list.

Step 3 Add or edit a device as follows:

- To add a device, click **Add Devices** and then click **Single Device**.
- To edit a device, check the check box next to the name of the device you want to edit and click **Actions > Edit** in the menu bar above the device table. The **Edit Device** dialog is displayed.

Step 4 Set the fields as needed, referring to the preceding table for more information.

Step 5 Save the settings by doing one of the following:

- If you are adding a device and will claim it later, click **Add Device**.
- If you are adding a device and want to claim it immediately, click **Add + Claim**. For more information on claiming a device, see Provision a Device with Plug and Play, on page 364.

- If you are editing a device, click **Edit Device**.

Add Devices in Bulk

This procedure shows how to add devices in bulk from a CSV file.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Plug and Play**.

Step 2 Click **Add Device**.

The **Add Devices** dialog is displayed.

Step 3 Click **Bulk Devices**.

Step 4 Click **Download File Template** to download the file template.

See the file template for information on which fields are mandatory and optional for different devices.

Step 5 Add the information for each device to the file and save the file. Note that certain fields are required, depending on the device type.

Step 6 Upload the CSV file by doing one of the following actions:

- Drag and drop the file to the drag and drop area.
- Click where it says "**click** to select" and select the file.

Step 7 Click **Import Devices**.

The devices in the CSV file are listed in a table.

Step 8 Check the box next to each device to import, or click the check box at the top to select all devices.

Step 9 Add the devices by doing one of the following:

- To add the devices and claim them later, click **Add Devices**.
- To add the devices and claim them immediately, click **Add + Claim**. For more information on claiming a device, see Provision a Device with Plug and Play, on page 364.

Register or Edit a Virtual Account Profile

This procedure lets you register the Cisco DNA Center controller as the default controller for Cisco Plug and Play Connect in a Cisco Smart Account, for redirection services. Also, this lets you synchronize the device inventory from the Cisco Plug and Play Connect cloud portal to Cisco DNA Center Plug and Play.

Table 51: Virtual Account Fields

Field	Description
Select Smart Account	Cisco Smart Account name.
Select Virtual Account	Virtual account name. Virtual accounts are subaccounts within a Cisco Smart Account.

Field	Description
Use as Default Controller Profile	Check this check box to register this Cisco DNA Center controller as the default controller in the Cisco Plug and Play Connect cloud portal.
Controller IP or **FQDN**	IP address or fully qualified domain name of this Cisco DNA Center controller.
Profile Name	Controller profile name.

Before you begin

Set the Cisco Smart Account credentials in the main Cisco DNA Center settings by using **System** > **Settings** > **Smart Account**.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Settings** > **PnP Connect**.

Step 2 View the virtual accounts in the table.

The table lists all of the registered Plug and Play Connect virtual account profiles.

Step 3 Either add or edit a virtual account profile, as follows:

- To register a virtual account, click **Register**. The register virtual account dialog is displayed.
- To edit a registered virtual account profile, click the radio button next to the name of the profile that you want to edit and click **Edit Profile** in the menu bar above the table. The edit virtual account dialog is displayed.

Step 4 Set the fields as needed by referring to the preceding Virtual Account Fields table.

Step 5 Save the settings by doing one of the following:

- If you are registering a new virtual account profile, click **Register**.
- If you are editing a virtual account profile, click **Change**.

What to do next

Synchronize the device inventory from the Cisco Plug and Play Connect cloud portal to Cisco DNA Center Plug and Play. For more information, see Add Devices from a Smart Account, on page 363.

Add Devices from a Smart Account

This task allows you to synchronize the device inventory from a Smart Account in the Cisco Plug and Play Connect cloud portal to Cisco DNA Center Plug and Play.

The Virtual Accounts table displays the following information for each profile.

Table 52: Virtual Accounts Information

Column	Description
Virtual Accounts	Virtual account name

Column	Description
Smart Accounts	Smart account that the virtual account is associated with
Sync Status	Status of the last synchronization process
Sync Result	Result of the last synchronization process

Before you begin

Before you can synchronize the device inventory from the Cisco Plug and Play Connect cloud portal, you must register a virtual account. See Register or Edit a Virtual Account Profile, on page 362. You can go directly to the PnP Connect settings page by clicking the **PnP Connect** link in the **Add Devices** > **Smart Account Devices** dialog.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Plug and Play**.

Step 2 Click **Add Device**.

The **Add Devices** dialog is displayed.

Step 3 Click **Smart Account Devices**.

Step 4 If you need to enter a Cisco.com ID (Cisco.com ID shows as Not Associated), follow these steps:

a) Click the **Add** link.
b) Enter the Cisco.com username and password.
c) Click **Save For Later** if you want to save the credentials permanently in Cisco DNA Center, or leave this check box unchecked to use these credentials one time only.
d) Click **Submit**.

Step 5 Click the radio button next to the name of the Plug and Play Connect virtual account profile from which you want to add devices.

If you need to register a PnP Connect virtual account profile, click the **PnP Connect** link. If you need to add Cisco.com credentials, click the **Add** link next to **Cisco.com ID**. If you want to change the Cisco ID, click the **Not me?** link.

Step 6 Click **Sync** to synchronize the device inventory from Cisco Plug and Play Connect in this virtual account to Cisco DNA Center Plug and Play.

Added devices appear in the Plug and Play Devices table with the source set to SmartAccount.

What to do next

Claim the newly synchronized devices. For more information on claiming a device, see Provision a Device with Plug and Play, on page 364.

Provision a Device with Plug and Play

Provisioning or claiming a device deploys an image and an onboarding configuration to the device. In the case of wireless devices, a network profile is configured. The device is then added to the inventory. If you claim a device that has not yet booted for the first time, you are planning the device configuration so that it is automatically provisioned when it boots up.

When provisioning or claiming a device, Cisco DNA Center does the following:

1. Deploys an image to the device.
2. Deploys an onboarding configuration for physically connected devices or a network profile for wireless devices.
3. Adds the device to the inventory.

The workflow for provisioning a device varies depending on the type of device, as follows:

- Switches and routers: See Provision a Switch or Router Device, on page 365
- Wireless LAN controllers, access points, and sensors: See Provision a Wireless or Sensor Device, on page 369

Provision a Switch or Router Device

Claiming a device provisions it by assigning it to a site, installing an image, deploying the site settings and onboarding configuration to it, and adding it to the inventory. If you claim a device that has not yet booted for the first time, then you are planning the device so that it is automatically provisioned when it boots up.

When a device is claimed, some system configuration CLI commands from Cisco DNA Center are pushed to the device first, before the Onboarding Configuration (Day-0) template that you have defined. If your Onboarding Configuration template has any of the same CLI commands, these will override the system configuration, since they are applied last. The CLI commands pushed by the system include the following:

- Device credentials (CLI and SNMP)
- Enable SSH v2 and SCP server
- Disable HTTP and HTTPS servers
- For switches, vtp mode transparent is enabled

Note When Device Controllability is enabled for a device (it is enabled by default), additional configurations are pushed to the device when it is added to the inventory or assigned to a site. For more information, see the Device Controllability section in the *Cisco DNA Center Administrator Guide*.

This procedure shows how to claim a device from the Plug and Play Devices list. Alternatively, you can claim a device from the device details window by clicking **Claim**.

Before you begin

- Ensure that Cisco network devices to be provisioned have a supported software release and are in a factory default state. If you are using a network device that was previously configured or is in an unknown state, see the device clean-up and reset details in the Network Plug and Play Troubleshooting Guide for Cisco Digital Network Architecture Center.
- Ensure that the devices being provisioned can discover and contact Cisco DNA Center. For more information, see Controller Discovery Prerequisites, on page 355.
- Define the site within the network hierarchy. See About Network Hierarchy, on page 110.

- Define the CLI and SNMP credentials for the devices. If you are using SNMPv2c, you must provide both Read and Write credentials. See About Device Credentials, on page 174.
- Optionally, ensure that software images for the devices to be provisioned are uploaded and marked as golden in the Image Repository, if you want to deploy images. See Import a Software Image, on page 91.

Note The image deployment process used by Plug and Play during Day-0 provisioning is not the same as that used when updating a device image later, which is described in Provision a Software Image, on page 95. During Plug and Play provisioning, there are no device prechecks, auto flash cleanup, or post-checks done, as it is expected that devices are in the factory default state.

- Optionally, define Onboarding Configuration templates to be applied to devices. Such templates contain basic network configuration commands to onboard a device so that it can be managed on the network. See Create Templates to Automate Device Configuration Changes, on page 193.

Note You can use the `ip http client source-interface` CLI command in the Onboarding Configuration template, which makes Cisco DNA Center use that IP address as the management IP address for device, especially for the scenario of multiple IPs or VRFs.

- Define network profiles for the devices. See Create Network Profiles, on page 164.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Plug and Play**.

Step 2 View the devices in the table.

You can use the **Filter** or **Find** option to find specific devices.

Step 3 Check the check box next to one or more devices that you want to claim.

Step 4 Click **Actions** > **Claim** in the menu bar above the device table.

The **Claim Devices** window opens, showing the first step, **Assign Site**. If, instead, you see a window that shows mandatory tasks such as defining a site and defining device credentials, you must click on **Add Site** to define a site, and **Add device credentials** to define device credentials. These are prerequisites for the claim process and, once these tasks are completed, you can return to claiming a device by clicking **Refresh** in this window.

Step 5 (Optional) Change the device hostname, if needed, in the first column.

Step 6 From the **Select a Site** drop-down list, choose a site to assign to each device.

To apply the same site as the first device to all other devices, click the **Apply Site to All** check box. To assign the site from any device to some other devices, click **Assign this Site to Other Devices**, choose the devices, and click.**Assign**

Step 7 Click **Next**.
The **Assign Configuration** window appears.

Step 8 (Optional) Make global changes to the device table as follows:

a) Change which columns are displayed in the table by clicking the 3 dots at the right end of the table headings and choosing the desired columns. Click **Apply** to save the changes.
b) Click **Clear Device Certificates** to clear any device certificates configured for devices. Click the check box for each device you want to clear the certificate from, and click **Clear**.
c) Click **Clear Images** to clear the default images configured for devices. Click the check box for each device you want to clear the image from, and click **Clear**.
d) Click **Clear Templates** to clear the default templates configured for devices. Click the check box for each device you want to clear the template from, and click **Clear**.
e) Click **Clear License Levels** to clear the license levels configured for devices. Click the check box for each device you want to clear the license level from, and click **Clear**.
f) You can apply an image or template from one device to other devices by clicking the 3 dots in the **Actions** column next to a device and choosing **Apply Image to Other Devices** or **Apply Template to Other Devices**. For stacked devices, you can apply the device license level to other devices by clicking **Apply License Level to Other Devices**.

Step 9 In the **Configuration** column, click on **Assign** for the device that you want to configure and follow these steps:

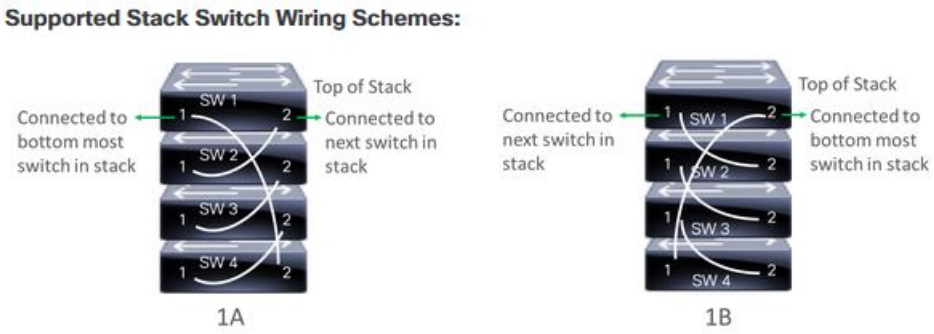
a) View the device configuration summary and click **Cancel** if no changes are needed.
b) (Optional) Check the check box **Apply the PKCS12 device certificate on the device** to deploy a PKCS12 certificate to the device. This option is available only for routers.
c) (Optional) In the **Device Name** field, change the device hostname, if needed.
d) (Optional) In the **Image** drop-down list, choose a golden software image to apply to the device. If there is only one golden image for this device type in the image repository, it is chosen by default.
e) (Optional) In the **Template** drop-down list, choose an onboarding configuration template to apply to the device. If there is only one onboarding configuration template for this device type defined, it is chosen by default.

   Click **Preview** next to a selected template to view the template.

f) (Optional) In the **Select a Cabling Scheme** drop-down list, choose the stack cabling scheme, if you want to renumber the stack.

   This item appears only for switches that support stacking, and only if they are connected as shown in one of the following cabling schemes.

Figure 40: Cabling Schemes



g) (Optional) In the **Select a Top of Stack serial Number** drop-down list, choose the serial number of the top of stack switch, if you want to renumber the stack.

   This item appears only for switches that support stacking, and only if they are connected as shown in the image.

h) (Optional) In the **Select a License Level** drop-down list, choose the stack license level.

   This item appears only for switches that support stacking.

i) If you made any changes, click **Save**, otherwise, click **Cancel** to return to the list and configure other devices.

Step 10 If you selected multiple devices to provision, click **Assign** for the next device in the list and repeat the configuration steps, until you have done this for all devices.

Step 11 Click **Next**.

The **Provision Templates** window appears, where you can specify the values for parameters that were defined in the template.

Step 12 Click on the name of a device that you want to configure and follow these steps:

a) Specify the values for the parameters that were defined in the template, if the device was assigned a configuration template.

Enter the values for each parameter in the fields for each device. A red asterisk indicates required fields.

b) If you want to copy the running configuration to the startup configuration on the selected device, check the box **Copy running config to startup config**.

c) If you selected multiple devices to provision, click the next device in the list at the left side of the window and enter the parameter values, until you have done this for all devices.

Step 13 To specify parameter values for all devices in bulk, do the following:

a) Click **Export** to save the CSV template file.

b) Add the values for each of the parameters to the file and save the file.

c) Click **Import**.

d) Drag and drop the file to the drag and drop area, or click where it says "**click** to select" and select the file.

e) Click **Import**.

Step 14 Click **Next**.

The **Summary** window appears, where you can view details about the devices and their configuration preview status.

Step 15 Check the **Day-0 Config** column for each device to see if the configuration preview was successful.

If the preview shows an error, you can click on the **Actions** link in the error message above the table to see what actions you need to take. You can click on an action to open a new tab with the window where a change is needed. You must resolve any issues before claiming the device, to avoid provisioning errors. You may need to go back to the **Provision Templates** step and change parameter values, change the template, revisit the **Design** area to update network design settings, or resolve any network connectivity issues. Once you have resolved the problem, you can go back to this tab and click the radio button **Retrying getting Day-0 configuration preview for failed device(s)**, and click **OK**.

Step 16 You can click the link in the **Day-0 Config** column to see more information about the device, its configuration, and any configuration preview errors.

Step 17 Click **Claim**.

A confirmation dialog box is displayed.

Step 18 Click **Yes** to claim the devices.

What to do next

To complete the provisioning process, after the device is added to the inventory, go to the **Inventory** tab, select the device and click **Actions > Provision > Provision Device**. Proceed through all the steps and click **Deploy** in the **Summary** step. In the **Summary**, you can see the remaining network settings that will be pushed to the device. For more information, see Provision Devices, on page 375. This process is required if

you intend to push the network settings that you may have configured in the **Design** area. During Plug and Play provisioning, only the device credentials and the Onboarding Configuration are pushed to the device; no other network settings are pushed until provisioning is completed from **Inventory**. Additionally, the device is added to ISE by Cisco DNA Center as a AAA client for RADIUS and TACACS, if these are configured.

Provision a Wireless or Sensor Device

Claiming a wireless device provisions it by assigning a configuration to the device and adding it to the inventory. If you claim a device that has not yet booted for the first time, you are planning the device so that it is automatically provisioned when it boots up.

Note When Device Controllability is enabled for a device (it is enabled by default), additional configurations are pushed to the device when it is added to the inventory or assigned to a site. For more information, see the Device Controllability section in the *Cisco DNA Center Administrator Guide*.

This procedure explains how to claim a device from the Plug and Play Devices list. Alternatively, you can claim a device from the device details window by clicking **Claim**.

Before you begin

- Ensure that Cisco network devices to be provisioned have a supported software release and are in a factory default state. If you are using a network device that was previously configured or is in an unknown state, see the device clean-up and reset details in the Network Plug and Play Troubleshooting Guide for Cisco Digital Network Architecture Center.
- Ensure that the devices being provisioned can discover and contact Cisco DNA Center. For more information, see Controller Discovery Prerequisites, on page 355.
- Define the site within the network hierarchy. See About Network Hierarchy, on page 110.
- Define the CLI and SNMP credentials for the devices. See About Device Credentials, on page 174.
- For provisioning a wireless access point device, ensure that the wireless LAN controller that is managing the wireless access point has been added to the inventory and assigned to the site where the wireless device is to be assigned. This is not needed for a Mobility Express access point.
- Optionally, ensure that the software images for any Cisco Catalyst 9800-CL devices to be provisioned are uploaded and marked as golden in the Image Repository, if you want to deploy images. See Import a Software Image, on page 91.

Note The image deployment process used by Plug and Play during Day-0 provisioning is not the same as that used when updating a device image later, which is described in Provision a Software Image, on page 95. During Plug and Play provisioning, there are no device prechecks, auto flash cleanup, or post-checks done, as it is expected that devices are in the factory default state.

- For provisioning a sensor device, ensure that the sensor is reachable through the Cisco DNA Center enterprise IP address (private/enp9s0). A DHCP option 43 string makes the device reachable in unclaimed mode in Cisco DNA Center, however, to claim the device, it must be reachable from the interface enp9s0 IP address. In the DHCP server, configure the NTP server (DHCP option 42) and the vendor-specific

DHCP option 43 with ACSII value "5A1D;B2;K4;I172.16.x.x;J80", where 172.16.x.x is the virtual IP address of Cisco DNA Center associated with the enp9s0 interface.

- Define wireless radio frequency profiles for wireless access point devices, except for Mobility Express access points. See Create a Wireless Radio Frequency Profile, on page 154.
- For Mobility Express access points, define an IP address pool and a management interface. See Configure IP Address Pools, on page 184.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Plug and Play**.

Step 2 View the devices in the table.

You can use the **Filter** or **Find** option to find specific devices.

Step 3 Check the check box next to one or more wireless devices that you want to claim.

Step 4 Choose **Actions** > **Claim** in the menu bar above the device table.

The **Claim Devices** window opens, showing the first step, **Assign Site**. If, instead, you see a window that shows mandatory tasks such as defining a site and defining device credentials, you must click on **Add Site** to define a site, and **Add device credentials** to define device credentials. These are prerequisites for the claim process and, once these tasks are completed, you can return to claiming a device by clicking **Refresh** in this window.

Step 5 (Optional) Change the device name, if needed, in the first column.

Step 6 (Optional) Change the device type, if needed, in the second column. You can choose AP (Access Point) or ME (Mobility Express), depending on which mode the device is using.

Choosing the wrong mode causes an error provisioning the device. This item does not appear for wireless LAN controller or sensor devices.

Step 7 From the **Select a Site** drop-down list, choose a site and floor to assign to each device. Access point devices must be assigned to a floor with a wireless controller.

To apply the same site as the first device to all other devices, click the **Apply Site to All** check box. To assign the site from any device to some other devices, click **Assign this Site to Other Devices**, choose the devices, and click **Assign**. Wireless devices can be assigned only to floors within a building, not to the building itself.

Step 8 Click **Next**.
The **Assign Configuration** window appears.

Step 9 (Optional) You can change which columns are displayed in the table by clicking the 3 dots at the right end of the table headings and choosing the desired columns. Click **Apply** to save the changes.

Step 10 In the **Configuration** column, click on **Assign** for the device that you want to configure and follow these steps:

a) View the device configuration summary and click **Cancel** if no changes are needed.
b) (Optional) In the **Device Name** field, change the device name, if needed.
c) For an access point device, in the **Radio Frequency Profile** drop-down list, choose a radio frequency profile to apply to the device. This may be set if you designated one profile as a default.
d) For a wireless LAN controller, enter values in the following fields: **Wireless management IP**, **Subnet mask**, **Gateway**, **IP interface name**, and optionally, **VLAN ID**.
e) For a Mobility Express device, enter values in the following fields: **Wireless management IP**, **Subnet mask**, and **Gateway**.
f) For a wireless sensor device, in the **Sensor Settings** drop-down list, choose the sensor device profile (backhaul) to apply to the device.

Note For Cisco Aironet 1800s Active Sensor, older than Software Release 1.3.1.2, make sure that you do not choose the sensor device profile **`CiscoProvisioningSSID`**. Instead, choose your own SSID for Backhaul purposes.

g) If you made any changes, click **Save**, otherwise, click **Cancel** to return to the list and configure other devices.
h) You can apply a configuration that you assigned to one device to other devices of the same type by clicking **Apply … to Other Devices** in the **Actions** column.

Step 11 If any devices are a Cisco Catalyst 9800-CL Wireless Controller, click **Assign** next to **Image** in the **Configuration** column and follow these steps:

a) (Optional) In the **Image** drop-down list, choose a golden software image to apply to the device. If there is only one golden image for this device type in the image repository, it is chosen by default.
b) Click **Save**.

Step 12 If you selected multiple devices to provision, click **Assign** for the next device in the list and repeat the configuration, until you have done this for all devices.

Step 13 Click **Next**.
The **Summary** window appears, where you can view details about the devices and configuration.

Step 14 Check the **Day-0 Config** column for each device to see if the configuration preview was successful.

If the preview shows an error, you can click on the **Actions** link in the error message above the table to see what actions you need to take. You can click on an action to open a new tab with the window where a change is needed. You must resolve any issues before claiming the device, to avoid provisioning errors. You may need to go back to the **Assign Configuration** step and change the configuration, revisit the **Design** area to update network design settings, or resolve any network connectivity issues. Once you have resolved the problem, you can go back to this tab and click the radio button **Retrying getting Day-0 configuration preview for failed device(s)**, and click **OK**. Ensure that the wireless LAN controller that is managing a device has been added to the inventory and assigned to the site where the wireless device is assigned.

Step 15 Click **Claim**.
A confirmation dialog box is displayed.

Step 16 Click **Yes** to claim the devices and start the provisioning process.

What to do next

To complete the provisioning process, after the device is added to the inventory, go to the **Inventory** tab, select the device and click **Actions > Provision > Provision Device**. Proceed through all the steps and click **Deploy** in the **Summary** step. In the **Summary**, you can see the remaining network settings that will be pushed to the device. For more information, see Provision Devices, on page 375. This process is required if you intend to push the network settings that you may have configured in the **Design** area. During Plug and Play provisioning, only the device credentials and the Onboarding Configuration are pushed to the device; no other network settings are pushed until provisioning is completed from **Inventory**. Additionally, the device is added to ISE by Cisco DNA Center as a AAA client for RADIUS and TACACS, if these are configured.

Provision a Cisco DNA Traffic Telemetry Appliance

This procedure shows how to claim a Cisco DNA Traffic Telemetry Appliance from the Plug and Play Devices list.

Before you begin

- Ensure that Cisco network devices to be provisioned have a supported software release and are in a factory default state. If you are using a network device that was previously configured or is in an unknown state, see the device clean-up and reset details in the Network Plug and Play Troubleshooting Guide for Cisco Digital Network Architecture Center.
- Ensure that the devices being provisioned can discover and contact Cisco DNA Center.
- Define the site within the network hierarchy. See About Network Hierarchy, on page 110.
- Define the CLI and SNMP credentials for the devices. If you are using SNMPv2c, you must provide both Read and Write credentials. See About Device Credentials, on page 174.

Note SNMPv3 Limitations:

- Supports SHA for Auth and AES128 for privacy.
- Does not support MD5/DES/3DES.

- If you want to deploy images, ensure that the software images for the devices to be provisioned are uploaded and marked as golden in the Image Repository. See Import a Software Image, on page 91.

Note The image deployment process that Plug and Play uses during Day-0 provisioning is not the same as the deployment process used when updating a device image later. For information, see Provision a Software Image, on page 95. During provisioning, Plug and Play performs no device prechecks, auto flash cleanup, or postchecks. Device must be in the factory default state.

- Define network profiles for the devices. See Create Network Profile for Cisco DNA Traffic Telemetry Appliance, on page 172.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Plug and Play**.

Step 2 View the devices in the table.

You can use the **Filter** or **Find** option to find the Cisco DNA Traffic Telemetry Appliance.

Step 3 Check the check box next to one or more devices that you want to claim.

Step 4 Click **Actions** > **Claim** in the menu bar above the device table.

The **Claim Devices** window opens, showing the first step, **Assign Site**. If instead, you see a window that shows mandatory tasks such as defining a site and defining device credentials, you must click **Add Site** to define a site, and **Add device credentials** to define device credentials. These mandatory tasks are prerequisites for the claim process. After these tasks are completed, you can return to claiming a device by clicking **Refresh** in this window.

Step 5 (Optional) Change the device hostname, if needed, in the first column.

Step 6 From the **Select a Site** drop-down list, choose a site to assign to each device.

To apply the same site as the first device to all other devices, click the **Apply Site to All** check box. To assign the site from any device to some other devices, click **Assign this Site to Other Devices**, choose the devices, and click **Assign**.

Step 7 Click **Next**.
The **Assign Configuration** window appears.

Step 8 In the **Configuration** column, click **Assign** for the device that you want to configure and follow these steps:

a) View the device configuration summary and, if no changes are needed, click **Cancel**.
b) (Optional) In the **Device Name** field, change the device hostname, if needed.
c) (Optional) In the **Image** drop-down list, choose a golden software image to apply to the device. If there is only one golden image for this device type in the image repository, it is chosen by default.
d) If you made any changes, click **Save**. Otherwise, click **Cancel** to return to the list and configure other devices.

Step 9 If you selected multiple devices to provision, click **Assign** for the next device in the list. Repeat the configuration steps, until you have configured all devices.

Step 10 Click **Next**.

The **Summary** window appears, where you can view details about the devices and their configuration preview status.

Step 11 Check the **Day-0 Config** column for each device to see if the configuration preview was successful.

If the preview shows an error, you can click the **Actions** link in the error message above the table to see what actions you need to take. You can click an action to open a new tab with the window where a change is needed. To avoid provisioning errors, you must resolve any issues before claiming the device. You may need to revisit the **Design** area to update network design settings or resolve any network connectivity issues. After you resolve the problem, return to this tab and click the **Retrying getting Day-0 configuration preview for failed device(s)** radio button. Then click **OK**.

Step 12 You can click the link in the **Day-0 Config** column to see more information about the device, its configuration, and any configuration preview errors.

Step 13 Click **Claim**.

A confirmation dialog box is displayed.

Step 14 Click **Yes** to claim the devices.

What to do next

To complete the provisioning process, after the device is added to the inventory, go to the **Inventory** tab, select the device and click **Actions > Provision > Provision Device**. Proceed through all the steps and click **Deploy** in the **Summary** step. In the **Summary** window, you can see the remaining network settings that are pushed to the device. For more information, see Provision Devices, on page 375. This process is required if you intend to push the network settings that you may have configured in the **Design** area. During Plug and Play provisioning, only the device credentials and the Onboarding Configuration are pushed to the device; no other network settings are pushed until provisioning is completed from **Inventory**.

Delete a Device

Deleting a device removes it from the Plug and Play database but does not reset the device. Use **Reset** if you want to reset a device that is in the Error state.

This procedure shows how to delete a device from the Plug and Play Devices list. Alternatively, you can delete a device from the device details window by clicking **Delete**.

Note If a device is in the Provisioned state, it can be deleted only from the **Inventory** tab.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Plug and Play**.

Step 2 View the devices in the table.

You can filter on device state by using one of the **Device State** buttons, or use the **Filter** option to find specific devices. Click **Refresh** to refresh the device list.

Step 3 Check the check box next to one or more devices that you want to delete.

Step 4 Click **Actions** > **Delete** in the menu bar above the device table.

A confirmation dialog box is displayed.

Step 5 Click **Yes** to confirm that you want to delete the devices.

Reset a Device

Resetting a device applies only to devices in the Error state and resets its state to Unclaimed and reloads the device, but does not remove it from the Plug and Play database. Use **Delete** if you want to delete a device.

Note If the saved configuration on the device is the factory default or a similar minimal configuration, then this option causes the device to restart the provisioning process. However, if the device has a previously saved startup configuration, then this could prevent the device from restarting the provisioning process and it will need to be reset to factory defaults. On wireless and sensor devices, only the device state is reset and the device is not reloaded.

This procedure shows how to reset a device from the Plug and Play Devices list. Alternatively, you can reset it from the device details window by clicking **Reset**.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Plug and Play**.

Step 2 View the devices in the table.

You can filter on device state by using one of the **Device State** buttons, or use the **Filter** option to find specific devices. Click **Refresh** to refresh the device list.

Step 3 Check the check box next to one or more devices that you want to reset.

Step 4 Click **Actions** > **Reset** in the menu bar above the device table.

A confirmation dialog box is displayed.

Step 5 Choose one of the following options:

- **Reset and keep current claim parameters**—Keep the current claim parameters and the device goes to the Planned state.
- **Reset and remove all claim parameters**—Remove the current claim parameters and the device goes to the Unclaimed state.

Step 6 Click **Reset**.

Provision Devices

The following sections provide information about how to provision various Cisco devices.

Provision a Cisco AireOS Controller

Before you begin

- Make sure that you have defined the following global network settings before provisioning a Cisco Wireless Controller:
  - Network servers, such as AAA, DHCP, and DNS.

    For more information, see Configure Global Network Servers, on page 189.
  - Device credentials, such as CLI, SNMP, HTTP, and HTTPS.

    For more information, see Configure Global CLI Credentials, on page 176, Configure Global SNMPv2c Credentials, on page 177, Configure Global SNMPv3 Credentials, on page 178, and Configure Global HTTPS Credentials, on page 180.
  - IP address pools.

    For more information, see Configure IP Address Pools, on page 184.
  - Wireless settings, such as SSIDs, wireless interfaces, and wireless radio frequency profiles.

    For more information, see Configure Global Wireless Settings, on page 141.
- Make sure that you have the Cisco Wireless Controller in your inventory. If not, use the **Discovery** feature to discover the controller.
- Make sure that the Cisco Wireless Controller is added to a site. For more information, see Add a Device to a Site, on page 72.
- You cannot reuse any pre-existing VLANs on devices. Provisioning fails if Cisco DNA Center pushes the same VLAN that already exists on the device.
- You cannot make any configuration changes to the wireless controller that is being managed by the Cisco DNA Center manually. You must perform all configurations from the Cisco DNA Center GUI.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The **Inventory** window appears, with the discovered devices listed.

Step 2 Expand the **Global** site in the left pane, and select the site, building, or floor that you are interested in.

The available devices in the selected site is displayed in the **Inventory** window.

Step 3 From the **DEVICE TYPE** list, click the **WLCs** tab, and from the **Reachability** list, click the **Reachable** tab to get the list of wireless controllers that are discovered and reachable.

Step 4 Check the check box next to the device name that you want to provision.

Step 5 From the **Actions** drop-down list, choose **Provision** > **Provision Device**.

The **Assign Site** window appears.

Step 6 Click **Choose a site** to assign a site for the wireless controller.

Step 7 In the **Add Sites** window, check the check box next to the site name to associate the wireless controller, and click **Save**.

Step 8 Click **Apply**.

Step 9 Click **Next**.

The **Configuration** window appears.

Step 10 Select a role for the wireless controller: **Active Main WLC** or **Guest Anchor WLC**.

Step 11 Click **Select Primary Managed AP Locations** to select the managed AP location for the wireless controller.

Step 12 In the **Managed AP Location** window, check the check box next to the site name. You can either select a parent site or the individual sites. If you select a parent site, the children under that parent site automatically gets selected.

Note Inheritance of managed AP locations allows you to automatically choose a site along with the buildings and floors under that site. One wireless controller can manage only one site.

Step 13 Click **Save**.

Step 14 Under **Interface and VLAN Configuration**, click **+ Add** and configure the interface and VLAN details for an active main wireless controller.

Interface and VLAN configuration is applicable for nonfabric wireless controller provisioning only.

The **Configure Interface and VLAN** window appears.

Step 15 From the **Interface Name** drop-down list, choose the interface name.

Step 16 In the **VLAN ID** field, enter a value for the VLAN.

Step 17 In the **Interface IP Address** field, enter a value for the interface IP address.

Step 18 In the **Interface Net Mask (in bits)** field, enter the subnet mask for the interface.

Step 19 In the **Gateway IP Address** field, enter the gateway IP address.

Step 20 From the **LAG/Port Number** drop-down list, choose the link aggregation or the port number.

Step 21 Click **OK**.

Step 22 (Optional) For a guest anchor wireless controller, change the VLAN ID configuration by changing the **VLAN ID** under **Assign Guest SSIDs to DMZ site**.

Step 23 Under **Mobility Group**, click **Configure** to configure the wireless controller as the mobility peer.

The **Configure Mobility Group** side panel appears.

Step 24 From the **Mobility Group Name** drop-down list, you can either add a new mobility group by clicking +, or choose a mobility group from the existing mobility groups.

The existing mobility peers information is loaded from the intent available in the Cisco DNA Center.

Step 25 In the **RF Group Name** text box, enter a name for the RF group.

Step 26 Under **Mobility Peers**, click **Add** to configure the wireless controller as a mobility peer.

Step 27 From the **Device Name** drop-down list, choose the controller.

After the device is provisioned, Cisco DNA Center creates a mobility group in the device, assigns the RF group, and configures all ends of peers. The mobility group configuration is deployed automatically to all the selected peer devices.

Step 28 Click **Save**.

Step 29 To reset the mobility group name and the RF group name, you can do one of the following:

- In the **Configure Mobility Group** side panel, choose **default** from the **Mobility Group Name** drop-down list.
- On the **Provision** > **Configuration** page, under **Mobility Group**, click **Reset**.

This automatically sets the **RF Group Name** to **default** and removes all peers. After provisioning, the mobility on the device is set and the device is removed from all other peers.

Step 30 Click **Next**.

The **Model Configuration** window appears.

Step 31 In the **Devices** pane, you can either search for a model config design by entering its name in the **Find** field, or expand the device and select a model config design.

The selected model config design appears in the right pane.

Step 32 Check the check box next to the **Design Name** that you want to provision, and click **Configure** to edit the model config design.

You cannot edit all the configurations at this step.

Step 33 After making the necessary changes, click **Apply**.

Step 34 Click **Next**.

The **Advanced Configuration** window appears, where you can enter values for predefined template variables.

Step 35 Search for the device or the template in the **Devices** panel.

Step 36 Enter a value for the predefined template variable in the **wlanid** field.

Step 37 Click **Next**.
The **Summary** window displays the following information:

- **Device Details**
- **Network Settings**
- **SSID**
- **Managed Sites**
- **Interfaces**
- **Advanced Configuration**
- **Mobility Group Configuration**
- **Model Config**

Step 38 Click **Deploy** to provision the controller.

Step 39 In the **Provision Devices** window, do the following to preview the CLI configuration:

- Click **Generate Configuration Preview** radio button.
- In the **Task Name** field, enter a name for the CLI preview task and click **Apply**.
- In the **Task Submitted** message, click the **Work Items** link.

  Note If you didn't notice the **Task Submitted** message, click the **Menu** icon (☰) and choose **Activity** > **Work Items**.

- In the **Work Items** window, click the CLI preview task for which you submitted the configuration preview request.
- View the CLI configuration details and click **Deploy**.
- To immediately deploy the device, click the **Now** radio button, and click **Apply**.
- To schedule the device deployment for a later date and time, click the **Later** radio button and define the date and time of the deployment.
- In the **Information** pop-up, do the following:
  - Click **Yes**, if you want to delete the CLI preview task from the **Work Items** window.
  - Click **No**, if you want to retain the task in the **Work Items** window.

  Note The CLI task will be marked as completed in the **Work Items** window. You can view the CLI configuration for this task but you cannot deploy it again.

Step 40 Provision the secondary controller.

Step 41 The **Status** column in the **Device Inventory** window shows `SUCCESS` after a successful deployment.

After provisioning, if you want to make any changes, click **Design**, change the site profile, and provision the wireless controller again.

Step 42 After the devices are deployed successfully, the **Provision Status** changes from **Configuring** to **Success**.

Step 43 In the **Device Inventory** window, click **See Details** in the **Provision Status** column to get more information about the network intent or to view a list of actions that you need to take.

Step 44 Click **See Details** under **Device Provisioning**.

Step 45 Click **View Details** under **Deployment of network intent**, and click the device name.

Step 46 Expand the **Configuration Summary** area to view the operation details, feature name, and the management capability.

The configuration summary also displays any errors that occurred while provisioning the device.

Step 47 Expand the **Provision Summary** area to view details of the exact configuration that is sent to the device.

Configure Cisco Wireless Controller High Availability from Cisco DNA Center

Cisco Wireless Controller High Availability (HA) can be configured through Cisco DNA Center. Currently, the formation of wireless controller HA is supported; the breaking of HA and switchover options is not supported.

Prerequisites for Configuring Cisco Wireless Controller High Availability

- The discovery and inventory features of wireless controller 1 and wireless controller 2 must be successful. The devices must be in Managed state.
- The service ports and the management ports of wireless controller 1 and wireless controller 2 must be configured.
- The redundancy ports of wireless controller 1 and wireless controller 2 must be physically connected.
- The management address of wireless controller 1 and wireless controller 2 must be in the same subnet. The redundancy management address of wireless controller 1 and wireless controller 2 must also be in the same subnet.
- Manually configure the following boot variables on the wireless controller:

```
config t
boot system bootflash::<device_iosxe_image_filename>
config-register 0x2102

show boot.  (IOSXE cli)

BOOT variable = bootflash:<device_iosxe_image_filename>,12;
Configuration register is 0x2102
```

Configure Cisco Wireless Controller HA

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The **Inventory** window appears, with the discovered devices listed.

Step 2 Check the check box next to the controller name that you want to configure as the primary controller.

Step 3 From the **Actions** drop-down list, choose **Provision** > **Configure WLC HA**.

The **High Availability** page appears.

Step 4 Enter the **Redundancy Management IP** and the **Peer Redundancy Management IP** address in the respective text boxes.

The IP addresses used for redundancy management IP and peer redundancy management IP should be configured in the same subnet as the management interface of the Cisco Wireless Controller. Ensure that these IP addresses are unused IP addresses within that subnet range.

Step 5 From the **Select Secondary WLC** drop-down list, choose the secondary controller.

Note When you select secondary controller, based on the wireless management interface IP subnet of primary controller, redundancy management IP auto populates and an **i** icon appears on the top of **High Availability** window, saying **Please make sure the Redundancy Management IP and Peer Redundancy Management IP are not assigned to any other network entities. If used, kindly change the IP accordingly and configure**.

Step 6 Click **Configure HA**.
The HA configuration is initiated in the background using the CLI commands. First, the primary wireless controller is configured. On success, the secondary wireless controller is configured. After the configuration is complete, both wireless controllers reboot. This process may take up to 2.5 minutes to complete.

Step 7 To verify the HA configuration, on the **Devices** > **Inventory** page, click the device that you configured as a HA device.

Step 8 Click the **Wireless Info** tab.

The **Redundancy Summary** displays the **Sync Status** as **In Progress**. When Cisco DNA Center finds that HA pairing succeeded, the **Sync Status** changes to **Complete**.

This is triggered by the inventory poller or by manual resynchronization. By now, the secondary wireless controller (wireless controller 2) is deleted from Cisco DNA Center. This flow indicates successful HA configuration on the wireless controller.

What Happens During or After the High Availability Process is Complete

1. Cisco wireless controller 1 and wireless controller 2 are configured with redundancy management, redundancy units, and SSO. The wireless controllers reboot in order to negotiate their role as active or stand by. Configuration is synced from active to stand by.
2. On the **Show Redundancy Summary** window, you can see these configurations:
   - SSO is Enabled
   - Wireless Controller is in Active state
   - Wireless Controller is in Hot Stand By state
3. The management port of the active wireless controller is shared by both the controllers and will be pointing to active controller. The user interface, Telnet, and SSH on the stand by wireless controller will not work. You can use the console and service port interface to control the stand by wireless controller.

Commands to Configure and Verify High Availability

Cisco DNA Center sends the following commands to configure Cisco Wireless Controller HA.

Cisco DNA Center sends the following commands to wireless controller 1:

- **config interface address redundancy-management 198.51.100.xx peer-redundancy-management 198.51.100.yy**
- **config redundancy unit primary**
- **config redundancy mode sso**

Cisco DNA Center sends the following commands to wireless controller 2:

- **config interface address redundancy-management 198.51.100.yy peer-redundancy-management 198.51.100.xx**
- **config redundancy unit secondary**
- **config port adminmode all enable**
- **config redundancy mode sso**

Enter the following commands to verify the HA configuration from the wireless controller:

- To check HA-related details: **config redundancy mode sso**
- To check the configured interfaces: **show redundancy summary**

Disable High Availability Configured Brownfield Device from Cisco DNA Center

The Cisco DNA Center disable high-availability feature is supported on Cisco Catalyst 9800 Series Wireless Controllers and Cisco AireOS Controllers.

Before you begin

Ensure that the high availability brownfield device is configured outside of Cisco DNA Center.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Device** > **Inventory**.

The **Inventory** window appears, with the discovered devices listed.

Step 2 Check the check box next to the name of the wireless controller that has the high-availability feature that you want to disable.

Step 3 From the **Actions** drop-down list, choose **Provision** > **Configure WLC HA**.

The **High Availability** page appears.

High Availability page shows the **REDUNDANCY SUMMARY** of selected wireless controller configured from outside Cisco DNA Center.

Step 4 In the **Warning** window, click **OK**.

A success message appears at the bottom of the screen indicating that high availability has been successfully disabled for the selected wireless controller.

Provision Routing and NFV Profiles

Before you begin

Make sure that you have defined the following global network settings before provisioning routing and NFV profiles:

- Network servers, such as AAA, DHCP, and DNS. For more information, see Configure Global Network Servers, on page 189.
- Device credentials, such as CLI, SNMP, HTTP, and HTTPS. For more information, see Configure Global CLI Credentials, on page 176, Configure Global SNMPv2c Credentials, on page 177, Configure Global SNMPv3 Credentials, on page 178, and Configure Global HTTPS Credentials, on page 180.
- IP address pools. For more information, see Configure IP Address Pools, on page 184.
- SP profiles. For more information, see Configure Service Provider Profiles, on page 189.

Note When provisioning Cisco Firepower Threat Defense Virtual through the NFV provisioning flow, the default credential username is retained and the password is updated based on the settings in the credential profile assigned to the site in Network Settings.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision**.

The **Device** > **Inventory** window appears, and all the discovered devices are listed in this window.

Step 2 To view devices available in a particular site, expand the Global site in the left pane, and select the site, building, or floor that you are interested in.

All the devices available in that selected site are displayed in the **Inventory** window.

Step 3 From the **Device Type** list, click the **Routers** tab, and from the **Reachability** list, click the **Reachable** tab to get a list of devices that are discovered and reachable.

Step 4 Check the check box next to the device name that you want to provision.

Step 5 Click **Assign** under the site; the **Assign Device to Site** window appears. Click **Choose a Site**.

Step 6 From the **Actions** drop-down list, choose **Provision** > **Provision Device**.

To provision an NFVIS device, do the following:

- Review the details in the **Confirm Profile** window, and click **Next**.
- Review the details in the **Router WAN Configuration** window. Click **O** and enter the WAN IP address. Review the details in the **+Edit Services** window. Click **Next**.

  Note You must configure vManage settings in the System Settings page before provisioning vEdge-related services. For more information, see Configure vManage Properties in the Cisco DNA Center Administrator Guide.

- Review the details in the **ENCS Integrated Switch Configuration** window, and click **Next**.
- Review the details in the **Custom Configuration** window, and click **Next**.
- Review the details in the **Summary** page.

To provision a router, do the following:

- Review the details in the **Confirm Profile** window, and click **Next**.
- Review the details in the **Router WAN Configuration** window.
  - If you selected Gigabit Ethernet as the line interface, click **O** and enter the WAN IP address if you select a static IP address. If you select DHCP, enter the IP address from the DHCP server. If the primary WAN is already configured using PnP, you can select **Do not Change** and select the interface that is configured as the primary WAN from the drop-down list.
  - If you selected cellular as the line interface, click **O**, choose **IP Negotiated**, select the **Interface Name** from the drop-down list, and enter the **Access Point Name (APN)**. Depending on your service provider, check the **PAP** or **CHAP** check box.
  - Enter the **IP SLA Address** for the backup WAN interface when you have multiple service providers.

  This window does not appear if you are provisioning a virtual router.
- Review the details in the **Router LAN Configuration** window, and click **Next**.

  You can now select one L3 interface or one or multiple L2 interfaces from the **Interface(s)** drop-down list.
- Review the details in the **Integrated Switch Configuration** window, and click **Next**.

- Review the details in the **Summary** page.

Step 7 Click **Deploy**.

Step 8 In the **Provision Devices** window, do the following to preview the CLI configuration:

- Click the **Generate Configuration Preview** radio button.
- In the **Task Name** field, enter a name for the CLI preview task and click **Apply**.
- In the **Task Submitted** pop-up, click the **Work Items** link.

  Note If you missed the **Task Submitted** pop-up, click the **Menu** icon (☰) and choose **Activity** > **Work Items**.

- In the **Work Items** window, click the CLI preview task for which you submitted the configuration preview request.
- View the CLI configuration details and click **Deploy**.
- To immediately deploy the device, click the **Now** radio button, and click **Apply**.
- To schedule the device deployment for a later date and time, click the **Later** radio button and define the date and time of the deployment.
- In the **Information** pop-up, do the following:
  - Click **Yes** if you want to delete the CLI preview task from the **Work Items** window.
  - Click **No** if you want to retain the task in the **Work Items** window.

  Note The CLI task will be marked as completed in the **Work Items** window. You can view the CLI configuration for this task, but you cannot deploy it again.

The **Provision Status** column in the **`Device Inventory`** window shows **SUCCESS** after a successful deployment. Click **SUCCESS** to see a detailed provisional log status.

VPC Inventory Collection

After successful cloud inventory collection, the **Cloud** tab in the **Provision** section provides a view of the collected AWS VPC Inventory. The navigation on the left can be expanded to show the cloud regions for a cloud profile or access key. You can filter the left navigation items by keyword and click to see the VPCs just for the selected region or access key.

In the VPC Inventory view you can also click on a VPC to see more details about it, like the subnets and virtual instances in that VPC and some more details about them. AWS VPC inventory collection is scheduled to occur at the default interval for all inventory collection and can also be triggered on demand by using the **Sync** action from the gear menu for a cloud access key. The status of the inventory collection can be viewed by clicking on **Show Sync Status** in the **VPC Inventory** view.

Provision Firewall Profiles

This procedure explains how to provision a Firepower Threat Defense (FTD) device managed by Firepower Management Center (FMC).

Before you begin

- Integrate FMC with Cisco DNA Center. See Integrate Firepower Management Center, on page 69.
- Create a site in a network hierarchy. See Create a Site in a Network Hierarchy, on page 111.
- Create a network profile for firewall and assign it to a site for which the FTD device is provisioned. See Create Network Profiles for Firewall, on page 167.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The Inventory page displays the device information that is gathered during the discovery process.

Step 2 Check the check box next to the FTD device that you want to provision and click **Assign** under the **Site** column.

Step 3 In the **Assign Device to Site** window, click **Choose a Site**.

Step 4 In the **Choose a Site** window, select a site from the hierarchy and click **Save**.

Step 5 Click **Next**.

Step 6 Click **Now** to assign the device to site immediately or click **Later** to schedule at a specific time.

Step 7 Click **Assign**.

Note You can view the status of assigning device to site in **Activity** > **Tasks**.

Step 8 From the **Actions** drop-down list, choose **Provision** > **Provision Device**.

The **Provision Firewall Profile** window appears.

Step 9 Review the details in the **Confirm Profile** page and click **Next**.

Step 10 Review the details in the **Firewall Type** page and click **Next**.

The **FTD Configuration** page appears.

Step 11 If you have associated a routed mode firewall with the site, do the following:

a) Expand the **Outside Interface** area, choose an outside interface from the **Select Physical Interface** drop-down list, and choose **Static IP** or **DHCP** radio button.

- **Static IP**: Enter the IP address and a subnet mask.
- **DHCP**: The IP address is obtained from DHCP.

b) Expand the **Inside Interface** area, choose an inside interface from the **Select Physical Interface** drop-down list, and choose **Static IP** or **DHCP** radio button.

- **Static IP**: Enter the IP address and a subnet mask.
- **DHCP**: The IP address is obtained from DHCP.

Step 12 If you have associated a transparent mode firewall with the site, do the following:

a) Expand the **Outside Interface** area and choose an outside interface from the **Select Physical Interface** drop-down list.

b) Expand the **Inside Interface** area and choose an inside interface from the **Select Physical Interface** drop-down list.

c) Expand the **Bridge Virtual Interface** area, and do the following:

- **Bridge Group Number**: Enter a bridge group number. The valid number is from 1 to 250.
- **IP**: Enter the IP address of the FTD device.
- **Subnet Mask**: Enter a subnet mask.

Step 13 Click **Next**.

The **Summary** page appears. This page summarizes the device specifications.

Step 14 Review the details in the **Summary** page and click **Deploy**.

The **Provision Firewall device(s)** dialog box appears.

Step 15 Click **Now**, **Later**, or **Generate configuration preview** radio button.

- **Now**: Starts the provision immediately.
- **Later**: Schedules the provisioning at a specific time.
- **Generate configuration preview:** Generates preview which can be later used to deploy on selected devices.

Step 16 Click **Apply**.

Note You can view the status of provisioning firewall device in **Activity** > **Tasks**. If you have chosen **Generate configuration preview** in the **Provision Firewall device(s)** dialog box, you can view the status in **Activity** > **Work Items**.

Provision a Cisco AP—Day 1 AP Provisioning

Before you begin

Make sure that you have Cisco APs in your inventory. If not, use the Discovery feature to discover APs. For more information, see Discover Your Network, on page 21.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The **Inventory** window appears, with the discovered devices listed.

Step 2 To view devices available in a particular site, expand the **Global** site in the left pane, and select the site, building, or floor that you are interested in.

All devices available in the selected site are displayed in the **Inventory** window.

Step 3 From the **Device Type** list, click the **APs** tab, and from the **Reachability** list, click the **Reachable** tab to see the APs that are discovered and reachable.

Step 4 Check the check box next to the AP device name that you want to provision.

Step 5 From the **Action** drop-down list, choose **Provision** > **Provision**.

The **Assign Site** window appears.

Step 6 Click **Choose a floor** and assign an AP to the site.

Step 7 In the **Choose a floor** window, select the floor to which you want to associate the AP, and click **Save**.

Step 8 Click **Next**.

The **Configuration** window appears.

Step 9 By default, the custom RF profile that you marked as default under **Design** > **Network Settings** > **Wireless** > **Wireless Radio Frequency Profile** is chosen in the **RF Profile** drop-down list.

You can change the default RF Profile value for an AP by selecting a value from the **RF Profile** drop-down list. The options are **High**, **Typical**, and **Low**.

The AP group is created based on the selected RF profile.

Step 10 Click **Next**.

Step 11 In the **Summary** window, review the device details, and click **Deploy** to provision the AP.

Step 12 In the **Provision Devices** window, do the following to preview the CLI configuration:

- Click the **Generate Configuration Preview** radio button.
- In the **Task Name** field, enter a name for the CLI preview task and click **Apply**.
- In the **Task Submitted** pop-up, click the **Work Items** link.

  Note If you missed the **Task Submitted** pop-up, click the **Menu** icon (☰) and choose **Activity** > **Work Items**.

- In the **Work Items** window, click the CLI preview task for which you submitted the configuration preview request.
- View the CLI configuration details and click **Deploy**.
- To immediately deploy the device, click the **Now** radio button, and click **Apply**.
- To schedule the device deployment for a later date and time, click the **Later** radio button and define the date and time of the deployment.
- In the **Information** pop-up, do the following:
  - Click **Yes** if you want to delete the CLI preview task from the **Work Items** window.
  - Click **No** if you want to retain the task in the **Work Items** window.

  Note The CLI task will be marked as completed in the **Work Items** window. You can view the CLI configuration for this task, but you cannot deploy it again.

Step 13 You are prompted with a message that creation or modification of an AP group is in progress, and then a message that APs will reboot after provisioning.

Step 14 Click **OK**.

The **Last Sync Status** column in the **Inventory** window shows `SUCCESS` for a successful deployment.

Enable ICMP Ping on APs in FlexConnect Mode

You can enable Internet Control Message Protocol (ICMP) ping on APs that are in FlexConnect mode and in an unreachable state. Cisco DNA Center uses the ICMP to ping FlexConnect APs that are in unreachable

state every five minutes to enhance reachability and then updates the reachability status in the **Inventory** window.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose

Step 2 Check the **Enable ICMP ping for unreachable access points in FlexConnect mode** check box to enable the ICMP ping.

Step 3 Click **Save**.

A success message saying `ICMP Ping status updated successfully` appears.

Cisco DNA Center starts pinging FlexConnect APs that are disassociated from Cisco Wireless Controller but are reachable. You can view the reachability status in the **Inventory** window.

Step 4 To view the reachability status, choose **Provision** > **Inventory**.

Step 5 The **Reachabilty** column shows **Ping Reachable** when the device is reachable by the ICMP ping.

Day 0 Workflow for Cisco AireOS Mobility Express APs

Before you begin

The Cisco Mobility Express wireless network solution comprises of at least one 802.11ac Wave 2 Cisco Aironet Series access point with an in-built software-based wireless controller managing other APs in the network. The AP acting as the wireless controller is referred to as the *primary AP*, while the other APs in the Cisco Mobility Express network, which are managed by this primary AP, are referred to as *subordinate APs*.

- Design your network hierarchy, with sites, buildings, floors, and so on. For more information, see Create a Site in a Network Hierarchy, on page 111, Add Buildings, on page 115, and Add a Floor to a Building, on page 116.
- Define the device credentials, such as CLI, SNMP, HTTP, and HTTPS at the global level. The credentials that are defined at the global level are inherited by the sites. For more information, see Configure Global CLI Credentials, on page 176, Configure Global SNMPv2c Credentials, on page 177, and Configure Global SNMPv3 Credentials, on page 178.
- Create WLANs, interfaces, RF profiles.
- Configure the DHCP server with Option #43 or Option #60. This is IP address of the Cisco DNA Center Plug and Play server. Using this, the APs contact the PnP server and downloads the configuration.
- Make sure that you have Mobility Express APs in the inventory. If not, discover using the Discovery feature. For more information, see Discover Your Network Using CDP, on page 26, Discover Your Network Using an IP Address Range, on page 31, and About Inventory, on page 47.
- The APs should be in the factory reset state without any Cisco Wireless Controller configurations.

Step 1 The Cisco Mobility Express contacts the DHCP server and connects to the Cisco DNA Center Plug and Play server.

Step 2 The DHCP server allocates the IP address with Option #43. Option #43 is the IP address of the Cisco DNA Center Plug and Play server.

Step 3 The Mobility Express AP starts the PnP agent and contacts the PnP server.

Note If you have a set of Mobility Express APs in the network, they go through an internal protocol. The protocol selects one Mobility Express AP, which will be configured on the Cisco Wireless Controller as the primary AP to reach the PnP server.

Step 4 Find the unclaimed AP in the **Provision** > **Devices** > **Plug and Play** tab.

The table lists all the unclaimed devices. The **State** column shows as **Unclaimed**. Use the **Filter** or **Find option** to find specific devices.

You must wait for the **Onboarding Status** to become **Initialized**.

Step 5 To claim the AP, check the check box adjacent the AP device name.

Step 6 Choose **Actions** > **Claim** in the menu bar above the device table.

The **Claim Devices** window appears.

Step 7 In the **Site Assignment** window, choose a site from the **Site** drop-down list.

Claiming the selected AP to this particular site also applies the associated configurations.

Step 8 Click **Next**.

Step 9 To configure a device, click the device name in the **Configuration** window.

Step 10 In the **Configuration for device name** page, assign the static IP details for the device:

- **Management IP**
- **Subnet Mask**
- **Gateway**

Step 11 Click **Save**.

Step 12 Click **Next**.

The **Summary** page appears.

Step 13 Click **Claim** in the **Summary** page.

Once the Mobility Express AP is claimed, the IP address configured is assigned to the Mobility Express AP.

Step 14 The claimed device, which is an AP and the wireless controller is now available under **Provision** > **Device Inventory** > **Inventory** window.

Step 15 You can also add devices in bulk from a CSV file.

For more information, see Add Devices in Bulk, on page 362.

When you bulk import Mobility Express APs through CSV, all the Mobility Express APs appear on **Devices** > **Plug and Play** page. Based on the VRRP protocol, only one Mobility Express AP among the imported ME APs becomes the primary AP, which come up for claim and the rest of them become subordinate APs. After claiming the primary AP, you need not claim the subordinate APs. Cisco DNA Center does not clear the subordinate APs from the Plug and Play page. You must delete those subordinate APs manually from the **Devices** > **Plug and Play** page.

Step 16 To provision the Cisco Wireless Controller, see Provision a Cisco AireOS Controller, on page 375.

Step 17 To provision the AP, see Provision a Cisco AP—Day 1 AP Provisioning, on page 385.

Brownfield Support for Cisco AireOS Controllers

Before you begin

With Cisco DNA Center, you can add and provision brownfield devices such as Cisco Wireless Controllers. Brownfield refers to devices that belong to existing sites with pre-existing infrastructure.

This procedure shows how to provision a brownfield Cisco AireOS Controller with Cisco DNA Center.

- Start by running a Discovery job on the device. All your devices are displayed on the **Inventory** window. For more information, see Discover Your Network, on page 21 and About Inventory, on page 47.
- The wireless controller should be reachable and in Managed state on the **Inventory** window. For more information, see About Inventory, on page 47.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The **Inventory** window appears, with the discovered devices listed.

Step 2 Click **Filter** and enter the appropriate values in the selected filter field. For example, for the **Device Name** filter, enter the name of the device.

The data that is displayed in the **Devices** table is automatically updated according to your filter selection.

Step 3 Check the check box next to the wireless controller device name that you want to provision.

Step 4 From the **Action** drop-down list, choose **Provision** > **Learn Device Config**.

The **Assign Site** window appears.

Step 5 Click **Choose a site** to assign a site for the controller.

Step 6 In the **Choose a site** window, select a site to which you want to associate the wireless controller, and click **Save**.

Step 7 Click **Next**.

Step 8 The **Resolve Conflict** window shows any conflicting configurations in Cisco DNA Center that you need to resolve.

Step 9 Click **Next**.

The **Design Object** window lists all the learned configurations.

Step 10 Click **Network** in the left pane.

The right pane displays network configurations that were learned as part of device configuration learning, and shows the following information:

- **AAA Server** details.
- **Systems Settings**, with details about the IP address and protocol of the AAA server.
- **DHCP Server** details.

Step 11 Enter the **Shared Secret** for the AAA server.

Step 12 Click **Wireless** in the left pane.

The right pane lists the enterprise SSIDs, guest SSIDs, and wireless interface details.

Step 13 For an SSID with a preshared key (PSK), enter the **passphrase key**.

Step 14 Click **Discarded Config** in the left pane.

The right pane lists the conflicting or the existing configurations on Cisco DNA Center. The discarded configuration entries are categorized as:

- Duplicate design entity
- Unknown device configuration for Radio Policy

Step 15 Click **Next**.

The **Network Profile** window lists the network profile or site profile that is created based on the AP and WLAN combination.

Step 16 Click **Save**.

A message saying `Brownfield Configuration is Successful` is displayed.

Step 17 Choose **Design** > **Network Profiles** to assign a site to the network profile.

Step 18 In the **Network Profiles** window, click **Assign Site** to add sites to the selected profile.

Step 19 In the **Add Sites to Profile** window, choose a site from the drop-down list, and click **Save**.

Step 20 Click the **Provision** tab.

Step 21 Click **Filter** and enter the appropriate values in the selected filter field.

The data that is displayed in the **Devices** table is automatically updated according to your filter selection.

Step 22 Check the check box next to the controller device name that you want to provision.

Step 23 From the **Action** drop-down list, choose **Provision**.

Step 24 Review the details in the **Assign Site** window, and click **Next**.

The **Configurations** window appears.

Step 25 Under **Interface and VLAN Configuration**, click **+Add** to configure interface and VLAN details.

Step 26 In the **Configure Interface and VLAN** window, configure the required fields, and click **OK**.

Step 27 Click **Next**.

Step 28 The **Summary** window displays the following information:

- **Device Details**
- **Network Settings**
- **SSID**
- **Managed Sites**
- **Interfaces**

Step 29 Click **Deploy**.

Step 30 In the **Provision Devices** window, do the following to preview the CLI configuration:

- Click the **Generate Configuration Preview** radio button.
- In the **Task Name** field, enter a name for the CLI preview task and click **Apply**.
- In the **Task Submitted** pop-up, click the **Work Items** link.

Note If you missed the **Task Submitted** pop-up, click the **Menu** icon (☰) and choose **Activity** > **Work Items**.

- In the **Work Items** window, click the CLI preview task for which you submitted the configuration preview request.
- View the CLI configuration details and click **Deploy**.
- To immediately deploy the device, click the **Now** radio button, and click **Apply**.
- To schedule the device deployment for a later date and time, click the **Later** radio button and define the date and time of the deployment.
- In the **Information** pop-up, do the following:
  - Click **Yes** if you want to delete the CLI preview task from the **Work Items** window.
  - Click **No** if you want to retain the task in the **Work Items** window.

  Note The CLI task will be marked as completed in the **Work Items** window. You can view the CLI configuration for this task, but you cannot deploy it again.

The **Provision Status** column in the **Device Inventory** window shows `SUCCESS` after a successful deployment.

Configure and Provision a Cisco Catalyst 9800 Series Wireless Controller

Cisco Catalyst 9800 Series Wireless Controller Overview

The Cisco Catalyst 9800 Series Wireless Controller is the next generation of wireless controllers built for intent-based networking. The Cisco Catalyst 9800 Series Wireless Controller is Cisco IOS XE based and integrates the RF excellence from Aironet with the intent-based networking capabilities of Cisco IOS XE to create the best-in-class wireless experience for your organization.

The Cisco Catalyst 9800 Series Wireless Controller is built on a modular operating system and uses open, programmable APIs that enable automation of day-0 and day-N network operations.

The Cisco Catalyst 9800 Series Wireless Controller is available in multiple form factors:

- Catalyst 9800-40 Wireless Controller.
- Catalyst 9800-80 Wireless Controller.
- Catalyst 9800-CL Cloud Wireless Controller: Deployable on private cloud (ESXi, KVM, Cisco ENCS, and Hyper-V) and manageable by Cisco DNA Center.
- Catalyst 9800 Embedded Wireless Controller for Catalyst 9300 Series Switches, Catalyst 9400 Series Switches, and Catalyst 9500H Series Switches.
- Cisco Catalyst 9800-L Wireless Controller: Provides seamless software updates for small- to mid-size enterprises. The Cisco Catalyst 9800-L Wireless Controller is available in two variations. You can choose between copper and fiber uplinks, which gives you flexibility in your network.

The following table lists the supported virtual and hardware platforms for the Cisco Catalyst 9800 Series Wireless Controller:

Platform	Description
Cisco Catalyst 9800-80 Wireless Controller	Supports up to 6000 access points and 64,000 clients. Supports up to 80 Gbps throughput and occupies a 2-rack unit space. Modular wireless controller with up to 100-GE uplinks and seamless software updates.
Cisco Catalyst 9800-40 Wireless Controller	A fixed wireless controller with seamless software updates for mid-sized organizations and campus deployments. Supports up to 2000 access points and 32,000 clients. Supports up to 40 Gbps throughput and occupies a 1-rack unit space. Provides four 1-GE or 10-GE uplink ports.
Cisco Catalyst 9800-CL Cloud Wireless Controller	Cisco Catalyst 9800-CL Cloud Wireless Controller can be deployed in a private cloud or a public cloud as Infrastructure as a Service (IaaS). Cisco Catalyst 9800-CL Cloud Wireless Controller is the next generation of enterprise-class virtual wireless controllers built for high availability and security. A virtual form factor of Cisco Catalyst 9800-CL Cloud Wireless Controller for private cloud supports ESXi, KVM, Cisco ENCS, and Hyper-V hypervisors.
Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches	Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches bring the wired and wireless infrastructure together with consistent policy and management. This deployment model supports only Cisco SD-Access, which is a highly secure solution for small campuses and distributed branches. The embedded controller supports access points (APs) only in Fabric mode.
Cisco Catalyst 9800-L Wireless Controller	Cisco Catalyst 9800-L Wireless Controller provides seamless software updates for small to mid-size enterprises. The Cisco Catalyst 9800-L Wireless Controller is available in two variations. You can choose between copper and fiber uplinks, which gives you flexibility in your network. • Cisco Catalyst 9800-L Copper Series Wireless Controller (9800-L-C RJ45) • Cisco Catalyst 9800-L Fiber Series Wireless Controller 9800-L-F SFP)

The following table lists the host environments supported by the Cisco Catalyst 9800 Series Wireless Controller:

Host Environment	Software Version
VMware ESXi	• VMware ESXi vSphere 6.0 • VMware ESXi vSphere 6.5[7] • VMware ESXi vCenter 6.0 • VMware ESXi VCenter 6.5
KVM	• Linux KVM based on Red Hat Enterprise Linux 7.1 and 7.2 • Ubuntu 14.04.5 LTS, Ubuntu 16.04.5 LTS

Host Environment	Software Version
NFVIS	Cisco ENCS 3.8.1 and 3.9.1

[7] Installing the .ova file of C9800-CL using ESXi vSphere does not work. This is not limited to the C9800 ova but affects other products. Cisco and VMware are actively working to fix the issue. Contact your Cisco account representative to see if the problem is fixed. There are issues specific to VMware 6.5 and C9800-CL OVA file deployment in which deployment fails with the warning "A required disk image was missing" and the error "Failed to deploy VM: postNFCData failed: Cannot POST to non-disk files." To install C9800-CL on VMware ESXi 6.5, do one of the following: 1) Install the .iso file of C9800-CL using the ESXi embedded GUI (ESXI 6.5 client version 1.29.0 is tested and required). 2) Install the .ova file of C9800-CL using the OVF tool.

The following table lists the Cisco Enterprise Network Function Virtualization Infrastructure Software (NFVIS) versions supported in Cisco DNA Center:

Note Cisco Enterprise NFVIS devices support the N-1 to N upgrade path only. For example, upgrade from Cisco Enterprise NFVIS 3.11.x to Cisco Enterprise NFVIS 3.12.x only is supported. Upgrade from Cisco Enterprise NFVIS 3.11.x to Cisco Enterprise NFVIS 4.1.x is not supported.

Cisco Enterprise NFVIS Version	Enterprise Network Compute System Device Platform	Notes
4.1.2 4.1.1 3.12.3 3.11.3 3.11.2 3.11.1	ENCS 5400 UCS-E UCS-C	Cisco DNA Center supports the following NFVIS upgrade paths: NFVIS v3.11.1 > 3.11.2 > 3.11.3 > 3.12.3 > 4.1.1 > 4.1.2. Cisco Enterprise NFVIS 3.12.1 is not supported on any versions of Cisco DNA Center. Upgrade to Cisco Enterprise NFVIS 3.12.1 from Cisco Enterprise NFVIS 3.11.x using Cisco DNA Center is not supported. Upgrade to Cisco Enterprise NFVIS 3.12.2 from Cisco Enterprise NFVIS 3.12.1 using Cisco DNA Center is not supported. Upgrade to Cisco Enterprise NFVIS 3.12.2 from 3.11.2 is supported using Cisco DNA Center. Cisco Enterprise NFVIS 3.12.2 is supported on Cisco DNA Center.
3.12.2 3.11.3 3.11.2 3.11.1	ENCS 5100	Cisco 5100 ENCS does not support Cisco Enterprise NFVIS 3.10.x.

Workflow to Configure a Cisco Catalyst 9800 Series Wireless Controller in Cisco DNA Center

1. Install Cisco DNA Center.

   For more information, see the Cisco DNA Center Installation Guide.

2. For information on software image upgrade, see Software Image Upgrade Support for Cisco Catalyst 9800 Series Wireless Controller, on page 396.

3. Log in to the Cisco DNA Center GUI and verify that the applications you need are in the **Running** state.

   In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System Settings** > **Software Updates** > **Installed Apps**.

4. Integrate Cisco Identity Services Engine with Cisco DNA Center. After integration, any devices that Cisco DNA Center discovers along with relevant configurations and data are pushed to Cisco ISE.

5. Discover the Cisco Catalyst 9800 Series Wireless Controller.

   You must enable NETCONF and set the port to 830 to discover the Cisco Catalyst 9800 Series Wireless Controller. NETCONF provides a mechanism to install, manipulate, and delete configurations of network devices.

   For more information, see Discover Your Network Using CDP, on page 26 or Discover Your Network Using an IP Address Range, on page 31.

   You must add the wireless management IP address manually.

   While performing discovery using the Cisco Discovery Protocol (CDP) or an IP address range in the **Discovery** window, choose **Use Loopback** from the **Preferred Management IP** drop-down list to specify the device's loopback interface IP address.

6. Make sure that the discovered devices appear in the Device Inventory page and are in **Managed** state.

   For more information, see About Inventory, on page 47 and Display Information About Your Inventory, on page 49.

   You must wait for the devices to move to a **Managed** state.

7. To verify the assurance connection with the Cisco Catalyst 9800 Series Wireless Controller, use the following commands:

   - **#show crypto pki trustpoints | sec DNAC-CA**

     ```
     Trustpoint DNAC-CA
         Subject Name:
         cn=kube-ca
               Serial Number (hex): 00E***************
         Certificate configured.
     ```

   - **#show crypto pki trustpoints | sec sdn-network**

     ```
     Trustpoint sdn-network-infra-iwan:
         Subject Name:
         cn=sdn-network-infra-ca
             Serial Number (hex): 378***************
         Certificate configured.
     ```

   - **#show telemetry ietf subscription all**

     ```
     Telemetry subscription brief

       ID               Type        State       Filter type
       ------------------------------------------------------
       1011             Configured  Valid       tdl-uri
       1012             Configured  Valid       tdl-uri
       1013             Configured  Valid       tdl-uri
     ```

- **#show telemetry internal connection**

```
Telemetry connection

Address Port Transport State Profile
------------------------------------------------------------
IP address 25103 tls-native Active sdn-network-infra-iwan
```

- **#show network-assurance summary**

```
Network-Assurance                       : True
Server Url                              : https://10.***.***.***
ICap Server Port Number                 : 3***
Sensor Backhaul SSID                    :
Authentication                          : Unknown
```

8. Configure a TACACS server while configuring authentication and policy servers.

   Configuring TACACS is not mandatory if you have configured the username locally on the Cisco Catalyst 9800 Series Wireless Controller.

9. Design your network hierarchy by adding sites, buildings, and floors so that later you can easily identify where to apply design settings or configurations.

   You can either create a new network hierarchy, or if you have an existing network hierarchy on Cisco Prime Infrastructure, you can import it into Cisco DNA Center.

   To import and upload an existing network hierarchy, see Upload an Existing Site Hierarchy, on page 113.

   To create a new network hierarchy, see Create a Site in a Network Hierarchy, on page 111, Add Buildings, on page 115, and Add a Floor to a Building, on page 116.

10. Add the location information of APs, and position them on the floor map to visualize the heatmap coverage.

    For more information, see Add, Position, and Delete APs, on page 119.

11. Define network settings, such as AAA (Cisco ISE is configured for Network and Client Endpoint), Netflow Collector, NTP, DHCP, DNS, syslog, and SNMP traps. These network servers become the default for your entire network. You can add a TACACS server while adding a AAA server.

    For more information, see About Global Network Settings, on page 173, Configure Global Network Servers, on page 189, and Add Cisco ISE or Other AAA Servers.

12. Create a wireless radio frequency profile with the parent profile as custom.

    For more information, see Create a Wireless Radio Frequency Profile, on page 154.

13. Create IP address pools at the global level.

    Cisco DNA Center uses IP address pools to automate the configuration and deployment of SD-Access networks.

    To create an IP address pool, see Configure IP Address Pools, on page 184.

    You must reserve an IP address pool for the building that you are provisioning. For more information, see Provision a LAN Underlay.

14. Create enterprise and guest wireless networks. Define the global wireless settings once; Cisco DNA Center then pushes the configurations to various devices across geographical locations.

Designing a wireless network is a two-step process. First, you must create SSIDs, and then associate the created SSID to a wireless network profile. This profile helps you to construct a topology, which is used to deploy devices on a site.

For more information, see Create SSIDs for an Enterprise Wireless Network, on page 141 and Create SSIDs for a Guest Wireless Network, on page 146.

15. Configure the backhaul settings. For more information.
16. Configure the following in the **Policy** window for the Cisco Catalyst 9800 Series Wireless Controller:
    - Create a virtual network. The virtual network segments your physical network into multiple logical networks. For more information, see Virtual Networks, on page 321 and Create a Virtual Network, on page 322.
    - Create a group-based access control policy and add a contract. For more information, see Create Group-Based Access Control Policy, on page 253.
17. Configure high availability.

    For more information, see Configure High Availability for Cisco Catalyst 9800 Series Wireless Controller, on page 397.
18. Provision the Cisco Catalyst 9800 Series Wireless Controller with the configurations added during the design phase.

    For more information, see Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 410.
19. Configure and deploy application policies on the Cisco Catalyst 9800 Series Wireless Controller.

    For more information, see Create an Application Policy, on page 305, Deploy an Application Policy, on page 310, and Edit an Application Policy, on page 309.

Note You must provision Cisco Catalyst 9800 Series Wireless Controller devices before deploying an application policy.

For Cisco Catalyst 9800 Series Wireless Controller devices, two different policies with different business relevance for two different SSIDs do not work. The last deployed policy always takes precedence when you are setting up relevance.

For Cisco Catalyst 9800 Series Wireless Controller devices, changing the default business relevance for an application does not work in FlexConnect mode.

You can apply an application policy only on a nonfabric SSID.

Software Image Upgrade Support for Cisco Catalyst 9800 Series Wireless Controller

Before you begin

- Discover the Cisco Catalyst 9800 Series Wireless Controller.

  Enable NETCONF and set the port to 830 to discover Cisco Catalyst 9800 Series Wireless Controller. NETCONF enables wireless services on the controller and provides a mechanism to install, manipulate, and delete the configuration of network devices.

For more information, see Discover Your Network Using CDP, on page 26, or Discover Your Network Using an IP Address Range, on page 31.

- Make sure that the devices appear in the device inventory and are in the **Managed** state.

  For more information, see About Inventory, on page 47 and Display Information About Your Inventory, on page 49.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Image Repository**.

The **Inventory** window appears, with the discovered devices listed.

Step 2 Import Cisco Catalyst 9800 Series Wireless Controller software image from your local computer or from a URL.

For more information, see Import a Software Image, on page 91.

Step 3 Assign the software image to a device family.

For more information, see Assign a Software Image to a Device Family, on page 92.

Step 4 You can mark a software image as golden by clicking star for a device family or for a particular device role.

For more information, see Specify a Golden Software Image, on page 93.

Step 5 Provision the software image.

In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Device** > **Inventory**.

Step 6 In the **Inventory** window, check the check box next to the Cisco Catalyst 9800 Series Wireless Controller whose image you want to upgrade.

Step 7 From the **Actions** drop-down list, choose **Software Image** > **Update Image**.

For more information, see Provision a Software Image, on page 95.

Configure High Availability for Cisco Catalyst 9800 Series Wireless Controller

Before you begin

Configuring High Availability (HA) on Cisco Catalyst 9800 Series Wireless Controller involves the following prerequisites:

- Both the Cisco Catalyst 9800 Series Wireless Controller devices are running the same software version and have active software image on the primary Catalyst 9800 Series Wireless Controller.
- The service port and the management port of Catalyst 9800 Series Wireless Controller 1 and Catalyst 9800 Series Wireless Controller 2 are configured.
- The redundancy port of Catalyst 9800 Series Wireless Controller 1 and Catalyst 9800 Series Wireless Controller 2 are physically connected.
- Preconfigurations such as interface configurations, route addition, ssh line configurations, netconf-yang configurations are completed on the Catalyst 9800 Series Wireless Controller appliance.

- The management interface of Catalyst 9800 Series Wireless Controller 1 and Catalyst 9800 Series Wireless Controller 2 are in the same subnet.
- The discovery and inventory of Catalyst 9800 Series Wireless Controller 1 and Catalyst 9800 Series Wireless Controller 2 devices are successful from Cisco DNA Center.
- The devices are reachable and are in **Managed** state.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The **Inventory** window appears, with the discovered devices listed.

Step 2 To view devices available in a particular site, expand the **Global** site in the left pane, and select the site, building, or floor that you are interested in.

All the devices available in that selected site is displayed in the **Inventory** window.

Step 3 From the **Device Type** list, click the **WLCs** tab, and from the **Reachability** list, click the **Reachable** tab to get the list of wireless controllers that are discovered and reachable.

Step 4 In the Inventory window, click the desired Cisco Catalyst 9800 Series Wireless Controller name to configure as a primary controller.

Step 5 Click the **High Availability** tab.

The selected Catalyst 9800 Series Wireless Controller by default becomes the primary controller and the **Primary C9800** field is grayed out.

Step 6 From the **Select Primary Interface** and **Secondary Interface** drop-down lists, choose the interface that is used for HA connectivity.

The HA interface serves the following purposes:

- Enables communication between the controller pair before the IOSd boots up.
- Provides transport for IPC across the controller pair.
- Enables redundancy across control messages exchanged between the controller pair. The control messages can be HA role resolution, keepalives, notifications, HA statistics, and so on.

Step 7 From the **Select Secondary C9800** drop-down list, choose the secondary controller to create a HA pair.

Note When you select secondary controller, based on the wireless management interface IP subnet of primary controller, redundancy management IP auto populates and an **i** icon appears on the top of **High Availability** window, saying **Please make sure the Redundancy Management IP and Peer Redundancy Management IP are not assigned to any other network entities. If used, kindly change the IP accordingly and configure**.

Step 8 Enter the **Redundancy Management IP** and **Peer Redundancy Management IP** addresses in the respective fields.

Note The IP addresses used for redundancy management IP and peer redundancy management IP should be configured in the same subnet as the management interface of the Cisco Catalyst 9800 Series Wireless Controller. Ensure that these IP addresses are unused IP addresses within the subnet range.

Step 9 In the **Netmask** field, enter the netmask address.

Step 10 Click **Configure HA**.

The HA configuration is initiated at the background using the CLI commands. First, the primary controller is configured. On success, the secondary controller is configured. Both the devices reboot once the HA is enabled. This process may take up to 2.5 minutes to complete.

Step 11 After the HA is initiated, the **Redundancy Summary** under **High Availability** tab displays the **Sync Status** as **HA Pairing is in Progress**. When Cisco DNA Center finds that the HA pairing is successful, the **SyncStatus** becomes **Complete**.

This is triggered by the inventory poller or by manual resynchronization. By now, the secondary controller (Catalyst 9800 Series Wireless Controller 2) is deleted from Cisco DNA Center. This flow indicates successful HA configuration in the Catalyst 9800 Series Wireless Controller.

Step 12 To manually resynchronize the controller, on the **Provision** > **Inventory** window, select the controller that you want to synchronize manually.

Step 13 From the **Actions** drop-down list, choose **Resync**.

Step 14 The following is the list of actions that occur after the process is complete:

- Catalyst 9800 Series Wireless Controller 1 and Catalyst 9800 Series Wireless Controller 2 are configured with redundancy management, redundancy units, and Single sign-on (SSO). The devices reboot in order to negotiate their role as an active controller or a standby controller. Configuration is synchronized from active to standby.
- On the **Show Redundancy Summary** window, you can see these configurations:
  - SSO is enabled
  - Catalyst 9800 Series Wireless Controller 1 is in active state
  - Catalyst 9800 Series Wireless Controller 2 is in standby state

Information About High Availability

High Availability (HA) allows you to reduce the downtime of wireless networks that occurs because of the failover of controllers. You can configure high availability for the Cisco Catalyst 9800 Series Wireless Controller through Cisco DNA Center.

Commands to Configure High Availability on Cisco Catalyst 9800 Series Wireless Controllers

Step 1 Use the following commands to configure HA on primary for Cisco Catalyst 9800 Series Wireless Controller:

- Run the **chassis ha-interface GigabitEthernet <redundancy interface num> local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** command to configure the HA chassis interface.

  This example shows how to configure a HA chassis interface:

  ```
  chassis ha-interface GigabitEthernet 3 local-ip 1.1.1.2 255.255.255.0 remote-ip
  1.1.1.3
  ```

- Run the **reload** command to reload devices for the changes to become effective.

Step 2 Use the following commands to configure HA on secondary for Cisco Catalyst 9800 Series Wireless Controller:

- Run the **chassis ha-interface GigabitEthernet <redundancy interface num> local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** command to configure the HA chassis interface.

This example shows how to configure a HA chassis interface:

```
chassis ha-interface GigabitEthernet 2 local-ip 1.1.1.3 255.255.255.0 remote-ip
1.1.1.2
```

Step 3 Run the **chassis clear** command to clear or delete all the HA-related parameters, such as local IP, remote IP, HA interface, mask, timeout, and priority.

Note Reload the devices for changes to take effect by running the **reload** command.

Step 4 Use the following commands to configure HA on primary for Cisco Catalyst 9800-40 Wireless Controller and Cisco Catalyst 9800-80 Wireless Controller devices:

- Run the **chassis ha-interface local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** command to configure the HA chassis interface.

  This example shows how to configure a HA chassis interface:

  ```
  chassis ha-interface local-ip 1.1.1.2 255.255.255.0 remote-ip 1.1.1.3
  ```

- Run the **reload** command to reload devices for the changes to become effective.

Step 5 Use the following commands to configure HA on secondary for Cisco Catalyst 9800-40 Wireless Controller and Cisco Catalyst 9800-80 Wireless Controller devices:

- Run the **chassis ha-interface local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** command to configure the HA chassis interface.

  This example shows how to configure a HA chassis interface:

  ```
  chassis ha-interface local-ip 1.1.1.3 255.255.255.0 remote-ip 1.1.1.2
  ```

Step 6 Run the **chassis clear** command to clear or delete all the HA-related parameters, such as local IP, remote IP, HA interface, mask, timeout, and priority.

Note Reload the devices for changes to take effect by running the **reload** command.

Commands to Verify Cisco Catalyst 9800 Series Wireless Controllers High Availability

Use the following commands to verify the high availability configurations from Cisco Catalyst 9800 Series Wireless Controller:

- Run the **config redundancy mode sso** command to check the HA-related details.
- Run the **show chassis** command to view chassis configurations about the HA pair, including the MAC address, role, switch priority, and current state of each controller device in the redundant HA pair.
- Run the **show ip interface brief** command to view the actual operating redundancy mode running on the device, and not the configured mode as set by the platform.
- Run the **show redundancy states** command to view the redundancy states of the active and standby controllers.
- Run the **show redundancy summary** command to check the configured interfaces.

- Run the **show romvar** command to verify high availability configuration details.

N+1 High Availability

Overview of N+1 High Availability

Cisco DNA Center supports N+1 High Availability (HA) on Cisco Wireless Controller and Cisco Catalyst 9800 Series Wireless Controller platforms.

N+1 HA with HA-SKU is supported on the Cisco 2504, 5500, 7500, and 8500 Series of standalone Wireless Controllers and WiSM2 controllers.

The N+1 HA architecture provides redundancy for controllers across geographically separated data centers with low-cost deployments.

N+1 HA allows a single Cisco Wireless Controller to be used as a backup controller for multiple primary controllers. These wireless controllers are independent of each other and do not share configuration or IP addresses on any of their interfaces.

Cisco DNA Center supports primary and secondary controller configurations for N+1 HA.

N+1 HA is configured per AP level; the configurations are pushed directly to the AP instead of to a global level.

When a primary wireless controller resumes operation, the APs fall back from the backup wireless controller to the primary wireless controller automatically if the AP fallback option is enabled.

Note The primary and secondary controllers must be of the same device type. For example, if the primary device is a Cisco Catalyst 9800 Series Wireless Controller, the secondary device must also be a Cisco Catalyst 9800 Series Wireless Controller.

APs with higher priority on the primary controller always connect first to the backup controller, even if they have to push out the lower priority APs.

The N+1 HA configuration has the following limitations in this release:

- Auto provisioning of a secondary controller is not supported because of the VLAN ID configuration.
- You must reprovision the secondary controller manually with the latest design configuration if you made any changes to the primary controller.
- Fault tolerance is not supported.
- Access Point Stateful Switch Over (AP SSO) functionality is not supported for N+1 HA. The AP Control and Provisioning of Wireless Access Points (CAPWAP) state machine is restarted when the primary controller fails.

Prerequisites for Configuring N+1 High Availability from Cisco DNA Center

- Discover primary and the secondary controller by running the **Discovery** feature.

  For more information, see Discover Your Network Using CDP, on page 26, or Discover Your Network Using an IP Address Range, on page 31.

- Make sure that the wireless controllers are reachable and in the managed state.

For more information, see About Inventory, on page 47 and Display Information About Your Inventory, on page 49.

- Verify the network connectivity between devices. If the primary controller goes down, the AP should be able to join the secondary controller as per the N+1 configuration.
- Create two buildings to manage the primary and secondary locations for both devices. For example, create two buildings, *Building A* and *Building B*, where Building A is the primary managed location for controller-1 and also the secondary managed location for controller-2, and Building B is configured only as a primary managed location for controller-2.

  For more information, see Create a Site in a Network Hierarchy, on page 111, Add Buildings, on page 115, and Add a Floor to a Building, on page 116.
- Add and position APs on a floor map to get a coverage heatmap visualization during the design phase.

  For more information, see Add, Position, and Delete APs, on page 119.
- Create two SSIDs and associate them as the backhaul SSIDs.

  For more information, see Create SSIDs for an Enterprise Wireless Network, on page 141 and Create SSIDs for a Guest Wireless Network, on page 146.

Configure N+1 High Availability from Cisco DNA Center

This procedure shows how to configure N+1 High Availability (HA) on Cisco Wireless Controller and Cisco Catalyst 9800 Series Wireless Controller.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The **Inventory** window appears, with the discovered devices listed.

Step 2 Check the check box next to the desired controller to provision it as a primary controller.

Step 3 From the **Actions** drop-down list, choose **Provision** > **Provision**.

The **Assign Site** window appears.

Step 4 Click **Choose a site** to assign a primary managed AP location for the primary controller.

Step 5 In the **Choose a site** window, select a site and click **Save**.

Step 6 Click **Next**.

The **Configuration** window appears, which displays the primary AP managed location for the primary device.

Step 7 Add or update the managed AP locations for the primary controller by clicking **Select Primary Managed AP Locations**.

Step 8 In the **Managed AP Location** window, check the check box next to the site name, and click **Save**.

You can either select a parent site or the individual sites.

Step 9 Configure the interface and VLAN details.

Step 10 Under **Configure Interface and VLAN** area, configure the IP address and subnet mask details, and click **Next**.

Step 11 In the **Advanced Configuration** window, configure values for the predefined template variables, and click **Next**.

Step 12 In the **Summary** window, verify the managed AP locations for the primary controller and other configuration details, and click **Deploy**.

- To deploy the device immediately, click the **Now** radio button and click **Apply**.

- To schedule the device deployment for a later date and time, click the **Later** radio button and define the date and time of the deployment.

Step 13 Next, provision the secondary controller.

Step 14 On the **Inventory** window, check the check box next to the desired controller to provision it as a secondary controller.

Step 15 From the **Actions** drop-down list, choose **Provision** > **Provision**.

The **Assign Site** window appears.

Step 16 Click **Choose a site** to assign the managed AP location for the secondary controller.

The managed AP location for the secondary controller should be same as the managed AP location of the primary controller.

Step 17 In the **Choose a site** window, check the check box next to the site name to associate the secondary controller, and click **Save**.

Step 18 Click **Next**.

The **Configuration** window appears, which displays the primary AP managed and secondary AP managed locations for the secondary device.

Step 19 Add or update the managed AP locations for the secondary controller by clicking **Select Secondary Managed AP Locations**.

Step 20 In the **Managed AP Location** window, check the check box next to the site name, and click **Save**.

You can either select a parent site or the individual sites.

Step 21 Configure the interface and VLAN details for the secondary controller.

Step 22 Under the **Configure Interface and VLAN** area, configure the IP address and subnet mask details for the secondary controller, and click **Next**.

Step 23 In the **Advanced Configuration** window, configure values for the predefined template variables, and click **Next**.

Step 24 In the **Summary** window, verify the managed AP locations for the secondary controller and other configuration details and click **Deploy**.

- To deploy the device immediately, click the **Now** radio button and click **Apply**.
- To schedule the device deployment for a later date and time, click the **Later** radio button and define the date and time of the deployment.

Step 25 To verify the managed locations of the primary and secondary controllers, click the device name of the controllers that you provisioned on the **Provision** > **Devices** > **Inventory** window.

Step 26 In the **Device details** window, click the **Managed ap locations** tab to view the primary and secondary managed location details.

Step 27 Provision the AP for the primary controller.

Step 28 On the **Devices** > **Inventory** window, check the check box next to the AP that you want to provision.

Step 29 From the **Action** drop-down list, choose **Provision** > **Provision**.

Step 30 In the **Assign Site** window, click **Choose a Floor** to select the floor from the primary managed location.

Step 31 Click **Next**.

The **Configuration** window appears.

Step 32 By default, the custom RF profile that you marked as the default under **Design** > **Network Settings** > **Wireless** > **Wireless Radio Frequency Profile** is chosen in the **RF Profile** drop-down list.

You can change the default RF Profile value for an AP by selecting a value from the **RF Profile** drop-down list.

Step 33 Click **Next**.

Step 34 In the **Summary** window, review the details.

Step 35 Click **Deploy** to provision the primary AP.

Step 36 You are prompted with a message that creation or modification of an AP group is in progress.

You are prompted with a message stating `After provisioning AP(s) will reboot. Do you want to continue?`.

Step 37 Click **OK**.

When deployment succeeds, the **Last Sync Status** column in the **Device Inventory** window shows `SUCCESS`.

Mobility Configuration Overview

The mobility configuration in Cisco DNA Center allows you to group a set of Cisco Wireless Controllers into a mobility group for a seamless roaming experience of wireless clients.

By creating a mobility group, you can enable multiple wireless controllers in a network to dynamically share information and forward traffic when inter-controller or inter-subnet roaming occurs. Mobility groups enable you to limit roaming between different floors, buildings, or campuses in the same enterprise by assigning different mobility group names to different wireless controllers within the same wireless network.

Cisco DNA Center allows you to create mobility groups between various platforms such as Cisco Catalyst 9800 Series Wireless Controller and Cisco AireOS Controllers.

Mobility configuration has the following guidelines and limitations:

- You cannot select multiple controllers for configuring mobility on the **Provision** page.
- You cannot create mobility groups with the group name as default. This resets the mobility and RF group names as default and deletes all the peers.
- You cannot configure a mobility group name on the anchor controller.
- You must reboot the wireless controller manually if there is change to the virtual IP address when configuring mobility groups on Cisco AireOS Controllers.
- Wireless controllers with the same mobility group name are automatically grouped into a single mobility group and are added as peers to each other.
- When configuring mobility groups on Cisco AireOS Controllers, if the wireless controllers do not have the IP address 192.0.2.1, Cisco DNA Center pushes the virtual IP address 192.0.2.1 to all the wireless controllers.
- Do not explicitly add guest anchor controllers to the mobility group. The provisioned guest anchor controllers do not appear in the drop-down list while adding peers in the mobility configuration page.
- If you provision a wireless controller as a guest anchor, ensure that it is not added to the mobility group.

Mobility Configuration Workflow

Here is the workflow that you can follow to configure mobility on Cisco Wireless Controller:

- To configure mobility, you must provision a wireless controller with mobility group name, RF group name, and mobility peers.
- The configuration that is applied during the wireless controller provisioning is automatically replicated to all the mobility peers configured in that group.
- Resynchronize the wireless controllers to get the latest tunnel status.

Mobility Configuration Use Cases

The following use cases explain the steps to configure mobility between controllers.

Use Case 1

Cisco Wireless Controller 1, wireless controller 2, and wireless controller 3 are newly added to Cisco DNA Center with the mobility group name as Default and is not provisioned yet.

1. Provision the wireless controller 1 by configuring mobility group name, RF group name, and adding wireless controller 2 and wireless controller 3 as peers.
2. Provision the wireless controller 2.

   In the **Provision** window, the mobility configuration is automatically populated for wireless controller 2 with the group name and peers.
3. Provision the wireless controller 3.
4. After provisioning all wireless controllers, resynchronize the wireless controllers to receive the latest tunnel status.

Use Case 2

Cisco Wireless Controller 1, wireless controller 2, and wireless controller 3 with different mobility group names are already added to Cisco DNA Center and are provisioned.

1. Provision the wireless controller 1 by configuring mobility group name, RF group name, and adding wireless controller 2 and wireless controller 3 as peers.
2. The mobility configuration is automatically replicated across other peers, such as wireless controller 2 and wireless controller 3.
   - After the successful provisioning of wireless controller 1, the wireless controller 2 and wireless controller 3 are added as peers on the wireless controller1.
   - The wireless controller 1 and wireless controller 3 are added as peers on wireless controller 2.
   - The wireless controller 1 and wireless controller 2 are added as peers on wireless controller 3.

Configure Mobility Group

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The **Inventory** window appears, which lists all the discovered devices.

Step 2 Choose **Provision** > **Devices** > **Inventory**.

Step 3 Check the check box next to the Catalyst 9800 Series Wireless Controller name for which you want to configure mobility.

Step 4 From the **Actions** drop-down list, choose **Provision** > **Provision WLC Mobility**.

The **Configure Mobility Group** panel appears.

For more information, see Mobility Configuration Overview, on page 404.

Step 5 From the **Mobility Group Name** drop-down list, you can either add a new mobility group by clicking **+**, or choose from the existing mobility groups.

The existing mobility peers information is loaded from the intent available in the Cisco DNA Center.

Step 6 In the **RF Group Name** text box, enter a name for the RF group.

Step 7 To enable or disable Cipher configuration for mobility, click the **DTLS High Cipher Only** button on.

Cipher configuration is applicable for Cisco Catalyst 9800 Series Wireless Controller Release 17.5 or later. You need to manually reboot the device for changes to take effect.

Step 8 To manually reboot the device after making changes in the DTLS (Data Datagram Transport Layer Security) cipher configuration to take effect after provision, click the **Restart for DTLS Ciphers to take effect** button on.

Step 9 To enable DTLS data encryption, click the **Data Link Encryption** button on.

Step 10 Under **Mobility Peers**, click **Add** to configure a mobility peer.

Step 11 From the **Device Name** drop-down list, choose the controller.

After the device is provisioned, the Cisco DNA Center creates a mobility group in device, assigns the RF group, and configures all ends of peers. The mobility group configuration is deployed automatically to all the selected peer devices.

Step 12 Click **Save**.

Step 13 You can reset the mobility group name and the RF group name using one of the following methods:

- In the **Configure Mobility Group** panel, choose **default** from the **Mobility Group Name** drop-down list.
- On the **Provision** > **Configuration** page, under **Mobility Group**, click **Reset**.

This automatically sets the **RF Group Name** to **default** and removes all peers. Once you provision, the mobility on the device is set and the device is removed from all other peers.

About DTLS Ciphersuites

Ciphersuites are a set of encryption and integrity algorithms designed to protect radio communication on your wireless LAN.

You can configure multiple DTLS (Data Datagram Transport Layer Security) Ciphersuites on Cisco Catalyst 9800 Series Wireless Controller, Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches, and Cisco Embedded Wireless Controller on Catalyst Access Points platforms running Release 17.5 or later.

Configure Multiple DTLS Ciphersuites

You can configure DTLS Ciphersuites either at the global level or at the site level.

Before you begin

- Make sure that the Device Controllability feature is enabled on the **System** > **Settings** > **Device Settings** > **Device Controllability** page.
- Discover Cisco Catalyst 9800 Series Wireless Controllers in your network using the **Discovery** functionality so that the discovered devices are listed in the Inventory window.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **Wireless**.

Step 2 In the left tree menu, select **Global** to configure all sites with the same DTLS Ciphersuite configuration.

In the left tree menu, select a site to configure DTLS Ciphersuites at the site level. The DTLS Ciphersuite configuration will be pushed to the controller available on that particular site.

Step 3 Uncheck the **Skip DTLS Ciphersuite Config** check box to configure Ciphersuites as part of Device Controllability.

Step 4 Configure either default Ciphersuites or custom Ciphersuites.

By default, the **Default** Ciphersuite is selected.

The Default Ciphersuite box shows the list of default Ciphersuites and these Ciphersuites are configured as default on the device. You cannot change the priority of these default ciphersuites.

Step 5 To configure custom Ciphersuites, click the **Custom** button.

Custom Ciphersuite overrides the default Ciphersuites with priority.

Step 6 From the **Version** drop-down list, choose the DTLS version.

Based on the DTLS version, Cisco DNA Center shows the available Ciphersuites.

Step 7 Click the blue button next to the Ciphersuite if you do not want to apply any of the Ciphersuites.

Step 8 To change the priority of Ciphersuites, hold and drag each Ciphersuite.

Step 9 Click **Save**.

The message `DTLS Ciphersuite Config Saved successfully` is displayed.

Step 10 To apply the Ciphersuite configuration, you must provision the device.

For more information, see Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 410.

About N+1 Rolling AP Upgrade

The rolling AP upgrade feature is supported on the Cisco AireOS Controller and Cisco Catalyst 9800 Series Wireless Controller in an N+1 High Availability setup. This feature helps you upgrade software images on the APs associated with the Cisco AireOS Controller or Cisco Catalyst 9800 Series Wireless Controller in your wireless LAN network. To achieve the zero downtime, it is possible to upgrade APs in a staggered way using the N+1 Rolling AP upgrade feature.

The primary controller identifies the candidate APs through the radio resource management neighbor AP map. The upgrade process starts with the software image downloading to the primary controller while the image is predownloaded to the candidate APs. After the candidate APs have been upgraded and rebooted, they join the secondary controller in a staggered manner. After all the APs have joined the secondary controller, the primary controller reboots. The APs rejoin the primary controller in a staggered manner after it is rebooted.

Here are the prerequisites for configuring Rolling AP Upgrade:

- An N+1 High Availability setup with two wireless controllers, one as the primary controller and the other one as the secondary.
- The primary and the N+1 controllers have the same configuration and managing the same location in the network.
- The N+1 controller is already running the Golden image so that rolling AP upgrade works with zero downtime.

  Golden images are standardized images for network devices and Cisco DNA Center automatically downloads the images from Cisco.com. Image standardization helps in device security and optimal device performance.
- The N+1 controller is reachable and in **Managed** state in Cisco DNA Center.
- Both the controllers are part of the same mobility group and a mobility tunnel is established between the primary and N+1 controller. The upgrade information between the primary and N+1 controllers are exchanged through the mobility tunnel.

Workflow to Configure Rolling AP Upgrade

This procedure shows how to configure rolling AP upgrade on Cisco AireOS Controller and Cisco Catalyst 9800 Series Wireless Controller.

Note N+1 rolling AP upgrade is supported on fabric and nonfabric deployments.

Step 1 Install Cisco DNA Center.

For more information, see the Cisco Digital Network Architecture Center Installation Guide.

Step 2 Log in to the Cisco DNA Center GUI and verify that the applications you need are in the **Running** state.

In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Software Updates** > **Installed Apps**.

Step 3 Discover the wireless controller using the Discovery feature.

You must enable NETCONF and set the port to 830 to discover the Catalyst 9800 Series Wireless Controller. NETCONF provides a mechanism to install, manipulate, and delete configurations of network devices.

For more information, see Discover Your Network Using CDP, on page 26 or Discover Your Network Using an IP Address Range, on page 31.

Step 4 Make sure that the discovered devices appear in the **Device Inventory** window and are in the **Managed** state.

For more information, see About Inventory, on page 47 and Display Information About Your Inventory, on page 49.

You must wait for devices to move to a **Managed** state.

Step 5 Design your network hierarchy by adding sites, buildings, and floors so that later you can easily identify where to apply design settings or configurations.

You can either create a new network hierarchy, or if you have an existing network hierarchy on Cisco Prime Infrastructure, you can import it into Cisco DNA Center.

To import and upload an existing network hierarchy, see Upload an Existing Site Hierarchy, on page 113.

To create a new network hierarchy, see Create a Site in a Network Hierarchy, on page 111, Add Buildings, on page 115, and Add a Floor to a Building, on page 116.

Step 6 Add the location information of APs, and position them on the floor map to visualize the heatmap coverage.

For more information, see Add, Position, and Delete APs, on page 119.

Step 7 Provision the primary controller with primary managed AP location, rolling AP upgrade enabled, and mobility group configured with the secondary controller as its peer.

To do this, choose **Provision** > **Devices** > **Inventory**, and check the check box next to the primary controller name.

Step 8 Configure the N+1 controller as the mobility peer in the Mobility Group configuration.

For more information, see Mobility Configuration Overview, on page 404.

Step 9 Provision the N+1 HA controller by configuring the primary controller's primary managed AP location as the N+1 controller's secondary managed AP location. This configures the secondary controller as the N+1 controller.

For more information, see Provision a Cisco AireOS Controller, on page 375 and Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 410.

Step 10 Provision the APs that are associated with the primary controller.

For more information, see Provision a Cisco AP—Day 1 AP Provisioning, on page 385.

Step 11 Import the software images to repository.

For more information, see Import a Software Image, on page 91.

Step 12 Assign the software image to a device family.

For more information, see Assign a Software Image to a Device Family, on page 92.

Step 13 Mark the software image as golden by clicking the star for a device family or a device role.

For more information, see Specify a Golden Software Image, on page 93.

Step 14 Before upgrading the image, make sure that the image readiness checks are successful for both devices.

Also make sure that the status of the **N+1 Device Check** and the **Mobility Tunnel Check** has a green tick mark.

- To do the image update readiness check, choose **Provision** > **Devices** > **Software Images**.
- Select the device whose image you want to upgrade.
- If the prechecks are successful for a device, the **Status** link in the **Image Precheck Status** column has a green tick mark. If any of the upgrade readiness prechecks fail for a device, the Image Precheck Status link has a red mark, and you cannot update the OS image for that device. Click the **Status** link and correct any errors before proceeding.

Step 15 Initiate the upgrade on primary controller.

Step 16 On the **Provision** > **Devices** > **Software Images** page, check the check box next to the primary controller.

Step 17 From the **Actions** drop-down list, choose **Software Image** > **Update Image**.

For more information, see Provision a Software Image, on page 95.

Step 18 To monitor the progress of the image upgrade, click **In Progress** in the **Software Image** column.

The **Device Status** page displays the following information:

- **Distribution Operation**: Provides information about the image distribution process. The image gets copied from the Cisco DNA Center to the primary device. The activate operation starts after the distribution process is complete.
- **Activate Operation**: Provides the activate operation details. The rolling AP upgrade starts during this process.
- **Rolling AP Upgrade Operation**: Provides a summary of the rolling AP upgrade, such as whether the rolling AP upgrade task is complete, the number of APs pending, the number of rebooting APs, and the number of APs that have joined the N+1 controller.

  Click **View AP Status** to view details about the primary controller, N+1 controller, device names, current status, and iterations.

Provision a Cisco Catalyst 9800 Series Wireless Controller

Before you begin

Before provisioning a Cisco Catalyst 9800 Series Wireless Controller make sure that you have completed the steps in Workflow to Configure a Cisco Catalyst 9800 Series Wireless Controller in Cisco DNA Center, on page 393.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The **Inventory** window appears, which lists all the discovered devices.

Step 2 Choose **Provision** > **Devices** > **Inventory**.

Step 3 Check the check box next to the Catalyst 9800 Series Wireless Controller name that you want to provision.

Step 4 From the **Actions** drop-down list, choose **Provision** > **Provision Device**.

Step 5 In the **Assign Site** window, click **Assign Site** to associate with a site.

Step 6 In the **Add Sites** window, check the check box next to the site name to associate a Catalyst 9800 Series Wireless Controller.

You can either select a parent site or the individual sites. If you select a parent site, all the children under the parent site are also selected. You can uncheck the check box to deselect an individual site.

Step 7 Click **Save**.

Step 8 Click **Next**.

The **Configuration** window.

This automatically sets the **RF Group Name** to **default** and removes all peers. Once you provision, the mobility on the device is set and the device is removed from all other peers.

Brownfield Support for Cisco Catalyst 9800 Series Wireless Controller

With Cisco DNA Center, you can add and provision brownfield devices such as the Cisco Wireless Controller and the Cisco Catalyst 9800 Series Wireless Controller to the network. Brownfield refers to devices that belong to existing sites with pre-existing infrastructure.

This section provides information about how to provision a brownfield Cisco Catalyst 9800 Series Wireless Controller with the Cisco DNA Center.

Before you begin

- Make sure that you have Cisco Catalyst 9800 Series Wireless Controller in the inventory. If you do not, discover using the Discovery feature.

  To discover the Cisco Catalyst 9800 Series Wireless Controller, you must enable NETCONF and set the port to 830.

  For more information, see About Discovery, on page 21.

- The Catalyst 9800 Series Wireless Controller should be reachable and in **Managed** state on the **Inventory** window. For more information, see About Inventory, on page 47.

- Design your network hierarchy by adding sites, buildings, and floors so that later you can easily identify where to apply design settings or configurations. You can either create a new network hierarchy or, if you have an existing network hierarchy on Cisco Prime Infrastructure, import it into Cisco DNA Center.

  For more information about importing and uploading an existing network hierarchy, see Upload an Existing Site Hierarchy, on page 113.

  For more information about creating a new network hierarchy, see Create a Site in a Network Hierarchy, on page 111, Add Buildings, on page 115, and Add a Floor to a Building, on page 116.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The **Inventory** window, which lists all the discovered devices that are available in the network, appears.

Step 2 Check the check box next to the Catalyst 9800 Series Wireless Controller that you want to provision.

Step 3 From the **Action** drop-down list, choose **Provision** > **Learn Device Config**.

Step 4 In the **Assign Site** window, click **Choose a site** to assign a site to the Catalyst 9800 Series Wireless Controller.

Step 5 In the **Choose a site** window, select the location to which you want to associate the Catalyst 9800 Series Wireless Controller, and click **Save**.

Step 6 Click **Next**.

Step 7 The **Resolve Conflict** window shows the available configurations in Cisco DNA Center and the Catalyst 9800 Series Wireless Controller. The conflicting configurations that you need to resolve are highlighted with a red box around them.

The **Choose this config in Cisco DNA Center** section shows the available configurations in Cisco DNA Center, while the **Choose this config in Device** section shows the available configurations on the Catalyst 9800 Series Wireless Controller device.

a. To retain the Cisco DNA Center configuration, from the **Choose this config** section, select the configuration that you want to retain by clicking the respective red box. This overwrites the device configuration.

For example, if the Cisco DNA Center is using Open as the authentication type for an SSID, and the device is using wpa2_enterprise as the authentication type, you can decide the configuration that you want to retain. To retain the Cisco DNA Center configuration, from the **Choose this config** section, select Open. Retaining the Cisco DNA Center configuration overwrites the device configuration.

To retain the device configuration, from the **Choose this config in Device** section, select the configuration that you want to retain by clicking the respective red box. Note that retaining the device configuration overwrites the Cisco DNA Center configuration.

b. Click **OK** in the **Warning** dialog box.

Step 8 Click **Next**.

The **Design Object** window lists the configurations learned by the device.

Step 9 Click **Network** in the left pane.

The right pane displays network configurations that were learned as part of the device configuration learning process, and shows the following information:

- **AAA Server** details.
- **Systems Settings**, with details about the IP address and protocol of the AAA server.
- **DHCP Server**, with details about all the DHCP servers available in the device.
- **NTP Server**, with details about all the NTP servers available in the device.

Step 10 Enter the **Shared Secret** for the AAA server.

Step 11 Click **Wireless** in the left pane.

This displays the enterprise SSIDs, guest SSIDs, wireless interfaces, and RF profiles that are present on the device.

Step 12 For an SSID with a preshared key (PSK), you must provide the **Passphrase key**.

Step 13 Click **Discarded Config** in the left pane.

This displays the conflicting and the existing configurations on the Cisco DNA Center. The discarded configuration entries are available under the following categories:

- Duplicate design entity
- Unknown device configuration for radio policy

Step 14 Click **Next**.

The **Network Profile** window lists the network profile or site profile that is created based on the AP and WLAN combination.

Step 15 Click **Save**.

A message saying `Brownfield Configuration is Successful` is displayed.

Step 16 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Design** > **Network Profiles** to assign a site to the network profile.

Step 17 In the **Network Profiles** window, click **Assign Site** to add sites to the selected profile.

Step 18 In the **Add Sites to Profile** window, check the check box next to the site to associate this profile.

Step 19 Click **Save**.

Step 20 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Provision** > **Devices** > **Inventory**.

Step 21 Click **Filter** and enter the appropriate values in the selected filter field.

The data that is displayed in the **Devices** table is automatically updated according to your filter selection.

Step 22 Check the check box next to the Catalyst 9800 Series Wireless Controller name that you want to provision.

Step 23 From the **Action** drop-down list, choose **Provision** > > **Provision Device**.

Step 24 Review the details in the **Assign Site** window, and click **Next**.

The **Configurations** window appears.

Step 25 Under **Interface and VLAN Configuration**, click **+Add** to configure interface and VLAN details.

Step 26 In the **Configure Interface and VLAN** window, configure the required fields, and click **OK**.

Step 27 Click **Next**.

Step 28 The **Summary** window displays the following information:

- **Device Details**
- **Network Setting**
- **SSID**
- **Managed Sites**
- **Rolling AP Upgrade**
- **Interfaces**

Step 29 Click **Deploy** to provision the device.

Step 30 You are prompted to deploy the device immediately or to schedule the deployment for a later time.

- To deploy the device now, click the **Now** radio button, and click **Apply**.
- To schedule device deployment for a later date and time, click the **Later** radio button, and define the date and time of the deployment.

Step 31 Next, provision the AP.

For more information, see Provision a Cisco AP—Day 1 AP Provisioning, on page 385.

Day 0 Workflow for Cisco Embedded Wireless Controller on Catalyst Access Points

The Cisco Embedded Wireless Controller on Catalyst Access Points (EWC-AP) is the next generation Wi-Fi solution, which combines Cisco Catalyst 9800 Series Wireless Controller with Cisco Catalyst 9100 Series Access Points, creating the best-in-class wireless experience for the evolving and growing organization.

Before you begin

- Design your network hierarchy, with sites, buildings, floors, and so on.

  For more information, see Create a Site in a Network Hierarchy, on page 111, Add Buildings, on page 115, and Add a Floor to a Building, on page 116.

- Define the device credentials, such as CLI, SNMP, HTTP, and HTTPS at the global level. The credentials that are defined at the global level are inherited by the sites.

  For more information, see Configure Global CLI Credentials, on page 176, Configure Global SNMPv2c Credentials, on page 177, and Configure Global SNMPv3 Credentials, on page 178.

- Create wireless SSIDs, wireless interfaces, and wireless Radio Frequency profiles.

  For more information, see Create SSIDs for an Enterprise Wireless Network, on page 141, Create SSIDs for a Guest Wireless Network, on page 146, Create a Wireless Interface, on page 153, and Create a Wireless Radio Frequency Profile, on page 154.

Note For Cisco Embedded Wireless Controller on Catalyst Access Points, only Flex-based SSID creation is supported.

- Configure the DHCP server with Option #43 on the switch where the Cisco Embedded Wireless Controller on Catalyst Access Points is connected.. This is IP address of the Cisco DNA Center Plug and Play server. Using this, the APs contact the PnP server and downloads the configuration.
- Make sure that you have Cisco Embedded Wireless Controller on Catalyst Access Points in the inventory. If not, discover using the Discovery feature. For more information, see Discover Your Network Using CDP, on page 26, Discover Your Network Using an IP Address Range, on page 31 , and About Inventory, on page 47.
- The APs should be in the factory reset state without any Cisco Wireless Controller configurations.

The Cisco Embedded Wireless Controller on Catalyst Access Points is available in multiple form factors:

- Cisco Embedded Wireless Controller on Catalyst 9115AX Access Points
- Cisco Embedded Wireless Controller on Catalyst 9117AX Access Points
- Cisco Embedded Wireless Controller on Catalyst 9120AX Access Points
- Cisco Embedded Wireless Controller on Catalyst 9130AX Access Points

Step 1 The Cisco Embedded Wireless Controller on Catalyst Access Points contacts the DHCP server.

The DHCP server in response provides the IP address along with Option #43. The option #43 contains the IP address of the Cisco Plug and Play server.

Step 2 Based on Option #43, the Cisco Embedded Wireless Controller on Catalyst Access Points turns on the Plug and Play agent and contacts the Cisco DNA Center Plug and Play server.

Note If you have a set of Cisco Embedded Wireless Controller on Catalyst Access Points in the network, they go through an internal protocol. The protocol selects one Cisco Embedded Wireless Controller on Catalyst Access Points, which is configured on the Cisco Wireless Controller as the primary AP to reach the PnP server.

Step 3 Find the unclaimed Cisco Embedded Wireless Controller on Catalyst Access Points in the **Provision** > **Devices** > **Plug and Play** tab.

The table lists all the unclaimed devices. The **State** column shows as **Unclaimed**. Use the **Filter** or **Find option** to find specific devices.

You must wait for the onboarding status to become **Initialized** under the **Onboarding State** column.

Step 4 To claim the Cisco Embedded Wireless Controller on Catalyst Access Points, check the check box adjacent the AP device name.

Step 5 Choose **Actions** > **Claim** in the menu bar above the device table.

The **Claim Devices** window appears.

Step 6 In the **Site Assignment** window, choose a site from the **Site** drop-down list.

Claiming the selected AP to this particular site also applies the associated configurations.

Step 7 Click **Next**.

Step 8 To configure a device, click the device name in the **Configuration** window.

Step 9 In the **Configuration for device name** page, assign the static IP details for the device:

- **Management IP**
- **Subnet Mask**
- **Gateway**

Step 10 Click **Save**.

Step 11 Click **Next**.

The **Summary** page appears.

Step 12 Click **Claim** in the **Summary** page.

Once the Cisco Embedded Wireless Controller on Catalyst Access Points is claimed, the IP address configured is assigned to the Cisco Embedded Wireless Controller.

Step 13 The claimed device, which is an Cisco Embedded Wireless Controller with internal AP is now available under **Provision** > **Devices** > **Inventory** window.

Step 14 To provision the AP, see Provision a Cisco AP—Day 1 AP Provisioning, on page 385.

Step 15 To provision the additional Cisco Embedded Wireless Controller on Catalyst Access Points, see Provision a Cisco AireOS Controller, on page 375.

Step 16 To bulk import devices from a CSV file, see Add Devices in Bulk, on page 362.

Step 17 To add devices manually, see Add or Edit a Device.

Migrate Cisco AireOS Controller to Cisco Catalyst 9800 Series Wireless Controller Using Cisco DNA Center

Before you begin

- Design your network hierarchy by adding sites, buildings, and floors.
- Discover the Cisco Catalyst 9800 Series Wireless Controller by running the discovery feature and add it to the Inventory. Make sure that the device status is reachable and in managed state.

  You must enable NETCONF and set the port to 830 to discover the Catalyst 9800 Series Wireless Controller. NETCONF provides a mechanism to install, manipulate, and delete configurations of network.
- Discover the Cisco AireOS Controllers and add it to the Inventory. Make sure that the device status is reachable and in managed state.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**..

The **Inventory** window appears, which lists the discovered devices.

Step 2 Check the check box next to the Cisco AireOS Controller.

Step 3 From the **Action** drop-down list, choose **Provision** > **Assign Device to Site**.

Step 4 In the **Assign Device to Site** window, click **Choose a Site** to which you want to associate the Cisco AireOS Controller.

Step 5 In the **Add Sites** window, check the check box next to the site name to associate a Cisco AireOS Controller.

Step 6 Click **Save**.

Step 7 From the **Action** drop-down list, choose **Provision** > **Learn Device Config** to learn configuration from the Cisco AireOS Controller device.

Step 8 Click **Next** in the **Assign Site** window.

Step 9 The **Resolve Conflict** window shows any conflicting configurations in Cisco DNA Center that you need to resolve.

Step 10 Click **Next**.

Step 11 Click **Next** in the **Design Object** window.

Step 12 Click **Network** in the left pane.

The right pane displays network configurations that were learned as part of the device configuration learning process, and shows the following information:

- AAA Server details.
- Systems Settings, with details about the IP address and protocol of the AAA server. Enter Shared Secret for the AAA server since the passwords are encrypted and Cisco DNA Center cannot learn passwords.
- DHCP Server, with details about all the DHCP servers available in the device.
- NTP Server, with details about all the NTP servers available in the device.

Step 13 Click **Next**.

Step 14 Click **Wireless** in the left pane.

The Wireless window displays the enterprise SSIDs, guest SSIDs, wireless interfaces, and RF profiles that are present on the device.

Step 15 For an SSID with a preshared key (PSK), you must provide the Passphrase key.

Step 16 Click **Discarded Config** in the left pane.

This displays the conflicting and the existing configurations on the Cisco DNA Center. The discarded configuration entries are available under the following categories:

- Duplicate design entity
- Unknown device configuration for radio policy

Step 17 Click Next.

Step 18 The **Network Profile** window lists the network profile or site profile that is created based on the AP and WLAN combination.

Step 19 Click **Save**.

A message saying Brownfield Configuration is Successful is displayed.

Step 20 Choose **Design** > **Network Settings** > **Wireless** to view the SSID and interface configurations that the Cisco DNA Center has learned from the Cisco AireOS Controller.

Step 21 Choose **Design** > **Network Profiles** to assign a site to the network profile.

Step 22 In the **Network Profiles** window, click **Assign Site** to add sites to the selected profile.

Step 23 In the **Add Sites to Profile window**, choose a site from the drop-down list, and click **Save**.

Step 24 Click the **Provision** tab.

Step 25 Check the check box next to the Cisco Catalyst 9800 Series Wireless Controller that you want to provision.

Step 26 From the **Action** drop-down list, choose **Provision**.

Step 27 Click **Choose a site** to assign a site for the Cisco Catalyst 9800 Series Wireless Controller.

Step 28 In the **Choose a site** window, check the check box next to the site name to associate a Catalyst 9800 Series Wireless Controller.

Step 29 Click **Next**.

The **Configuration** window appears.

Step 30 Select a role for the Cisco Catalyst 9800 Series Wireless Controller as **Active Main WLC**.

Step 31 Click **Select Primary Managed AP Locations** to configure a managed AP location for the primary controller.

Step 32 In the **Managed AP Location** window, check the check box next to the site name. You can either select a parent site or the individual sites. If you select a parent site, the children under that parent site automatically gets selected.

Step 33 Click **Save**.

Step 34 Click **Next**.

Step 35 The summary window shows the configurations that will be pushed to Cisco Catalyst 9800 Series Wireless Controller from the Cisco AireOS Controller.

Review the following details:

- Device Details
- Network Setting
- SSID
- Managed Sites
- Interfaces

- Advanced Configuration

Step 36 Click **Deploy** to provision the Catalyst 9800 Series Wireless Controller.

- To deploy the device immediately, click the **Now** radio button and click **Apply**.
- To schedule the device deployment for a later date and time, click the **Later** radio button and define the date and time of the deployment.

Step 37 After the devices are deployed successfully, the **Provision Status** changes from **Configuring** to **Success**.

Step 38 In the **Device Inventory** window, click **See Details** in the **Provision Status** column to get more information about the network intent or to view a list of actions that you need to take.

Step 39 To manually resynchronize Cisco Catalyst 9800 Series Wireless Controller, on the **Provision** > **Inventory** window, select the controller that you want to manually synchronize.

Step 40 From the **Actions** drop-down list, choose **Resync**.

Step 41 Provision the AP.

For more information, see: Provision a Cisco AP—Day 1 AP Provisioning, on page 385.

Configure and Provision a Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches

Supported Hardware Platforms

Device Role	Platforms
Embedded Wireless Controller	Cisco Catalyst 9300 Series Switches Cisco Catalyst 9400 Series Switches Cisco Catalyst 9500H Series Switches
Fabric Edge	Cisco Catalyst 9300 Series Switches Cisco Catalyst 9400 Series Switches Cisco Catalyst 9500H Series Switches Cisco Catalyst 3600 Series Switches Cisco Catalyst 3850 Series Switches
APs	Cisco 802.11ac Wave 2 APs: • Cisco Aironet 1810 Series OfficeExtend Access Points • Cisco Aironet 1810W Series Access Points • Cisco Aironet 1815i Access Point • Cisco Aironet 1815w Access Point • Cisco Aironet 1815m Access Point

Device Role	Platforms
	• Cisco 1830 Aironet Series Access Points • Cisco Aironet 1850 Series Access Points • Cisco Aironet 2800 Series Access Points • Cisco Aironet 3800 Series Access Points • Cisco Aironet 4800 Series Access Points Cisco 802.11ac Wave 1 APs • Cisco Aironet 1700 Series Access Points • Cisco Aironet 2700 Series Access Points • Cisco Aironet 3700 Series Access Points

Preconfiguration

On the Cisco Catalyst 9800 Series Wireless Controller, make sure that the following commands are present if the switch is already configured with **aaa new-model**:

```
aaa new-model
aaa authentication login default local
aaa authorization exec default local
aaa session-id common
```

This is required for NETCONF configuration. These configurations are not required if you are using an automated underlay for provisioning.

Workflow to Configure Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Switches

1. Install Cisco DNA Center.

   For more information, see the Cisco DNA Center Installation Guide.

2. Log in to the Cisco DNA Center GUI and verify that the applications you need are in the **Running** state.

   In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **System** > **Software Updates** > **Installed Apps**.

3. Integrate Cisco Identity Services Engine with Cisco DNA Center. After Cisco ISE is registered with Cisco DNA Center, any device that Cisco DNA Center discovers, along with relevant configurations and other data, is pushed to Cisco ISE.

4. Discover Cisco Catalyst 9000 Series Switches and the edge switches.

   You must enable NETCONF and set the port to 830 to discover Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches.

   Do not enable NETCONF to discover the edge switches.

   For more information, see Discover Your Network Using CDP, on page 26 and Discover Your Network Using an IP Address Range, on page 31.

Change the **Preferred Management IP** to **Use Loopback**.

5. Make sure that the devices appear in the device inventory and are in **Managed** state.

   For more information, see About Inventory, on page 47 and Display Information About Your Inventory, on page 49.

   Ensure that the devices are in the **Managed** state.

6. Design your network hierarchy, which represents your network's geographical location. You create sites, buildings, and floors so that later you can easily identify where to apply design settings or configurations.

   You can either create a new network hierarchy, or if you have an existing network hierarchy on Cisco Prime Infrastructure, you can import it into Cisco DNA Center.

   To import and upload an existing network hierarchy, see the Upload an Existing Site Hierarchy, on page 113.

   To create a new network hierarchy, see the Create a Site in a Network Hierarchy, on page 111, Add Buildings, on page 115, and Add a Floor to a Building, on page 116.

7. For a nonfabric network, add and position APs on a floor map to get heatmap visualization during the design phase.

   For a fabric network, you cannot place APs on a floor map during the design time. The APs are onboarded after adding devices to a fabric network.

   For more information, see Add, Position, and Delete APs, on page 119.

8. Define network settings, such as AAA (Cisco ISE is configured for Network and Client Endpoint), NetFlow Collector, NTP, DHCP, DNS, syslog, and SNMP traps. These network servers become the default for your entire network.

   For more information, see About Global Network Settings, on page 173, Configure Global Network Servers, on page 189, and Add Cisco ISE or Other AAA Servers.

9. Configure device credentials such as CLI, SNMP, and HTTPs.

   For more information, see About Global Device Credentials, on page 176, Configure Global CLI Credentials, on page 176, Configure Global SNMPv2c Credentials, on page 177, Configure Global SNMPv3 Credentials, on page 178, and Configure Global HTTPS Credentials, on page 180.

10. Configure IP address pools at the global level.

    To configure an IP address pool, see Configure IP Address Pools, on page 184.

    To reserve an IP address pool for the building that you are provisioning, see Provision a LAN Underlay.

11. Create enterprise and guest wireless networks. Define global wireless settings once and Cisco DNA Center then pushes configurations to various devices across geographical locations.

    Designing a wireless network is a two-step process. First, you must create SSIDs on the **Wireless** page. Then, associate the created SSID to a wireless network profile. This profile helps you to construct a topology, which is used to deploy devices on a site.

    For more information, see Create SSIDs for an Enterprise Wireless Network, on page 141 and Create SSIDs for a Guest Wireless Network, on page 146.

12. Configure backhaul settings. For more information.

13. Configure the following on the **Policy** page:
    - Create a virtual network. The virtual network segments your physical network into multiple logical networks. For more information, see Virtual Networks, on page 321 and Create a Virtual Network, on page 322.
    - Create a group-based access control policy, and add a contract. For more information, see Create Group-Based Access Control Policy, on page 253.
14. Provision Cisco Catalyst 9000 Series Switches and the edge node switches with the configurations added during the design phase.
    - Create a fabric domain.
    - Add devices to the fabric network by creating a CP+Border+Edge or CP+Border.
    - Enable embedded wireless capabilities on the Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches.
    - Onboard APs in the fabric domain.

    After the devices are deployed successfully, the deploy status changes from **Configuring** to **Success**.

Provision Embedded Wireless on Cisco Catalyst 9000 Series Switches

Before you begin

Before provisioning a Cisco Catalyst 9800 Embedded Wireless Controller on Catalyst 9000 Series Switches, ensure that you have completed the steps in Workflow to Configure Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Switches, on page 419.

This procedure explains how to provision embedded wireless on Cisco Catalyst 9300 Series Switches, Cisco Catalyst 9400 Series Switches, and Cisco Catalyst 9500H Series Switches.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The **Inventory** window appears, with the discovered devices listed.

Step 2 Check the check box next to the Catalyst 9000 Series Switch device and an edge switch that you want to associate to a site.

Step 3 From the **Actions** drop-down list, choose **Provision** > **Assign Device to Site**.

Step 4 In the **Assign Device to Site** window, click **Choose a site**.

Step 5 In the **Choose a site** window, check the check box next to the site to associate the device.

Step 6 Click **Save**.

Step 7 Click **Apply**.
The next step is to provision the Catalyst 9000 Series Switch and the edge node with the configurations that were added during the design phase.

Step 8 In the **Devices** > **Inventory**window, check the check box next to the device name that you want to provision.

Step 9 From the **Actions** drop-down list, choose **Provision** > **Provision Device**.

Step 10 Click **Next**.

Step 11 In the **Summary** window, verify the configurations, and click **Deploy**.

Step 12 In the **Provision Devices** window, do the following to preview the CLI configuration:

- Click **Generate Configuration Preview** radio button.
- In the **Task Name** field, enter a name for the CLI preview task and click **Apply**.
- In the **Task Submitted** pop-up, click the **Work Items** link.

  Note If you missed the **Task Submitted** pop-up, click the **Menu** icon (≡) and choose **Activity** > **Work Items**.

- In the **Work Items** window, click the CLI preview task for which you submitted the configuration preview request.
- View the CLI configuration details and click **Deploy**.
- To immediately deploy the device, click the **Now** radio button, and click **Apply**.
- To schedule the device deployment for a later date and time, click the **Later** radio button and define the date and time of the deployment.
- In the **Information** pop-up, do the following:
  - Click **Yes** if you want to delete the CLI preview task from the **Work Items** window.
  - Click **No** if you want to retain the task in the **Work Items** window.

    Note The CLI task will be marked as completed in the **Work Items** window. You can view the CLI configuration for this task, but you cannot deploy it again.

Step 13 To provision the edge switch, check the check box next to the edge switch that you want to provision.

Step 14 From the **Actions** drop-down list, choose **Provision**.

Step 15 Click **Next**.

Step 16 In the **Summary** window, verify the configurations, and click **Deploy**.

After the devices are deployed successfully, the **Provision Status** changes from **Configuring** to **Success**.

Step 17 To add devices to a fabric domain, in the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Provision** > **Fabric**.

Step 18 Create a fabric LAN. For more information.

Step 19 Add an IP transit network.

Step 20 Add devices and associate virtual networks to a fabric domain.

Step 21 Add the Cisco Catalyst 9000 Series Switch as a control plane, a border node, and an edge node or a control plane and a border node.

Click the device and choose **Add as CP+Border+Edge** or **Add as CP+Border**.

Step 22 Click the edge node and choose **Add to Fabric**.

Step 23 Click **Save**.

Step 24 To enable embedded wireless on the device, click the device that is added as a **Edge**, **CP+Border+Edge** or **CP+Border**, and click the **Embedded Wireless**.

If you have not installed the wireless package on Cisco Catalyst 9000 Series Switches before enabling the wireless functionality, Cisco DNA Center displays a warning message saying `9800-SW image is necessary for turning on the capability. Click "OK" to import the 9800-SW image manually.`

Step 25 Click **OK** to install the image manually.

Step 26 On the **Download Image** window, click **Choose File** to navigate to a software image stored locally or **Enter image URL** to specify an HTTP or FTP source from which to import the software image.

Step 27 Click **Import**.

The progress of the import is displayed.

Step 28 Click **Activate image on device**.

A warning message saying `Activate image on device will reboot the device. Are you sure you want to reboot the device?` appears.

Step 29 Click **Yes**.

The device reboots and comes online after the device package upgrade is complete.

Step 30 In the dialog box that appears, the AP locations that are managed by the controllers are displayed. You can change, remove, or reassign the site here.

Step 31 Click **Next**.

Step 32 Review the details on the **Summary** window, and click **Save**.

Step 33 On the **Modify Fabric Domain** window, click **Now** to commit the changes, and click **Apply** to apply the configurations. The next step is to onboard APs in a fabric domain.

Step 34 In the Cisco DNA Center GUI, click the **Provision** tab.

Step 35 Click the **Fabric** tab.

A list of fabric domains is displayed.

Step 36 Select the fabric domain that was created, and click the **Host Onboarding** tab to enable IP pool for APs.

Step 37 Select the authentication template that is applied for devices in the fabric domain. These templates are predefined configurations that are retrieved from Cisco ISE. After selecting the authentication template, click **Save**.

Step 38 Under **Virtual Networks**, click **INFRA_VN** to associate one or more IP pools with the selected virtual network.

Step 39 Under **Virtual Network**, click the guest virtual networks to associate IP pools for the selected guest virtual network.

Step 40 Check the **IP Pool Name** check box that was created for APs during the design phase.

Step 41 Click **Update** to save the setting.

The AP gets the IP address from the specified pool, which is associated with the AP VLAN and registers with the Cisco wireless controller through one of the discovery methods.

Step 42 Specify wireless SSIDs within the network that hosts can access. Under the **Wireless SSID** section, select the guest or enterprise SSIDs and assign address pools, and click **Save**.

Step 43 Manually trigger resynchronization by performing an **Inventory > Resync** to see the APs on Cisco DNA Center for embedded wireless.
The discovered APs are now displayed under **Inventory** in the **Provision** page and the **Status** is displayed as **Not Provisioned**.

Step 44 Provision the AP.

For more information, see Provision a Cisco AP—Day 1 AP Provisioning, on page 385.

Step 45 Configure and deploy application policies. For more information, see Create an Application Policy, on page 305, Deploy an Application Policy, on page 310, and Edit an Application Policy, on page 309.

Provision the Catalyst 9300 Series Switches and Cisco Catalyst 9500H Series Switches before deploying an application policy.

Two different policies with different business relevance for two different SSIDs do not work. Always the last deployed policy takes precedence when you are setting up the relevance.

Changing the default business relevance for an application does not work in FlexConnect mode.

You can apply an application policy only on a nonfabric SSID.

Fabric in a Box with Catalyst 9800 Embedded Wireless on Cisco Catalyst 9000 Series Switches

Information About Fabric in a Box

Cisco Catalyst 9000 Series Switches have the capability to host fabric edge, control plane, border, and embedded wireless functionalities on a single switch, which you can configure using Cisco DNA Center.

With this feature, configurations at the small site locations are simplified and the cost to deploy Cisco SD-Access is reduced.

For information on how to add CP+Border+Edge nodes on Cisco Catalyst 9000 Series Switches, see Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 410.

Scale Information

This table shows the device scalability information.

Fabric Constructs	Cisco Catalyst 9300 Series Switches	Cisco Catalyst 9400 Series Switches	Cisco Catalyst 9500 Series Switches	Cisco Catalyst 9500-H Series Switches
Virtual Networks	256	256	256	256
Local End Points/Hosts	4K	4K	4K	4K
SGT/DGT Table	8K	8K	8K	8K
SGACLs (Security ACEs)	5K	18K	18K	18K

Inter-Release Controller Mobility Introduction

Inter-Release Controller Mobility (IRCM) supports seamless mobility and wireless services across different Cisco Wireless Controllers with different software versions.

Cisco DNA Center supports guest anchor feature for the following device combinations:

- Configuration of a Cisco AireOS controller as a foreign controller with a Cisco AireOS controller as an anchor controller.

- Configuration of a Cisco AireOS controller as a guest anchor controller with a Cisco Catalyst 9800 Series Wireless Controller as a foreign controller.
- Configuration of a Cisco Catalyst 9800 Series Wireless Controller as a foreign controller with a Cisco Catalyst 9800 Series Wireless Controller as an anchor controller.

Configuring IRCM on controller devices has the following limitations:

- Configuration of a Cisco AireOS controller as a foreign controller and Cisco Catalyst 9800 Series Wireless Controller as an anchor controller is not supported.
- Configuration of a fabric guest anchor is not supported.
- Configuration of multiple anchor controllers and one foreign controller is not supported.
- Only guest SSID is supported.
- Broadcast of a nonguest anchor SSID in a guest anchor mode is not supported.
- Mobility tunnel is not encrypted.

Guest Anchor Configuration and Provisioning

Follow these steps to configure a guest anchor Cisco Wireless Controller.

Note Guest anchor configuration is not supported on the Cisco Catalyst 9800 Series Wireless Controller.

Step 1 Design a network hierarchy, with sites, buildings, floors, and so on. For more information, see Create a Site in a Network Hierarchy, on page 111, Add Buildings, on page 115, and Add a Floor to a Building, on page 116.

Step 2 Configure network servers, such as AAA, DHCP, and DNS servers. For more information, see Configure Global Network Servers, on page 189 and Add Cisco ISE or Other AAA Servers, on page 190.

Step 3 Create SSIDs for a guest wireless network with external web authentication and central web authentication along with configuring Cisco Identity Services Engine. For more information, see Create SSIDs for a Guest Wireless Network, on page 146.

Step 4 Discover the wireless controller using the Cisco Discovery Protocol (CDP) or an IP address range and that the devices are in the **Devices** > **Inventory** window and are in the **Managed** state. For more information, see About Discovery, on page 21.

Step 5 Provision a foreign wireless controller as the active main wireless controller. See Provision a Cisco AireOS Controller, on page 375.

Step 6 Choose the role for the wireless controller as guest anchor and provision the guest anchor controllers. For more information, see Provision a Cisco AireOS Controller, on page 375.

Step 7 Configure device credentials, such as CLI, SNMP, HTTP, and HTTPS. For more information, see Configure Global CLI Credentials, on page 176, Configure Global SNMPv2c Credentials, on page 177, Configure Global SNMPv3 Credentials, on page 178, and Configure Global HTTPS Credentials, on page 180.

IRCM: Cisco AireOS Controller and Cisco Catalyst 9800 Series Wireless Controller

Before you begin

- Discover the Cisco Catalyst 9800 Series Wireless Controller and Cisco AireOS Controllers.

  You must enable NETCONF and set the port to 830 to discover the Catalyst 9800 Series Wireless Controller. NETCONF provides a mechanism to install, manipulate, and delete configurations of network devices.

  For more information, see Discover Your Network Using CDP, on page 26 or Discover Your Network Using an IP Address Range, on page 31.

- Design your network hierarchy by adding sites, buildings, and floors so that later you can easily identify where to apply design settings or configurations.

  To create a new network hierarchy, see Create a Site in a Network Hierarchy, on page 111, Add Buildings, on page 115, and Add a Floor to a Building, on page 116.

- Add the location information of APs, and position them on the floor map to visualize the heatmap coverage.

  For more information, see Add, Position, and Delete APs, on page 119.

- Define network settings, such as AAA (Cisco ISE is configured for Network and Client Endpoint), NetFlow Collector, NTP, DHCP, DNS, syslog, and SNMP traps. These network servers become the default for your entire network. You can add a TACACS server while adding a AAA server.

  For more information, see About Global Network Settings, on page 173, Configure Global Network Servers, on page 189, and Add Cisco ISE or Other AAA Servers.

- Create SSIDs for a guest wireless network.

  For more information, see Create SSIDs for a Guest Wireless Network, on page 146.

- The WLAN profile name of the foreign controller and anchor controller should be the same for mobility.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The **Inventory** window appears, with the discovered devices listed.

Step 2 Check the check box next to the Catalyst 9800 Series Wireless Controller that you want to provision as a foreign controller.

Step 3 From the **Actions** drop-down list, choose **Provision** > **Provision**.

Step 4 In the **Assign Site** window, click **Choose a Site** to assign a site for the Catalyst 9800 Series Wireless Controller device.

Step 5 In the **Add Sites** window, check the check box next to the site name to associate a Catalyst 9800 Series Wireless Controller.

Step 6 Click **Save**.

Step 7 Click **Apply**.

Step 8 Click **Next**.

Step 9 Select a role for the Catalyst 9800 Series Wireless Controller as **Active Main WLC**.

Step 10 For an active main wireless controller, you need to configure interface and VLAN details.

Step 11 Under the **Assign Interface** area, do the following:

- **VLAN ID**: Enter a value for the VLAN ID.
- **IP Address**: Enter the interface IP address.
- **Gateway IP Address**: Enter the gateway IP address.
- **Subnet Mask (in bits)**: Enter the interface net mask details.

Note Assigning an IP address, gateway IP address, and subnet mask is not required for the Catalyst 9800 Series Wireless Controller.

Step 12 Click **Next**.

Step 13 In the **Summary** window, review the configurations details.

Step 14 Click **Deploy** to provision the Catalyst 9800 Series Wireless Controller as a foreign controller.

Step 15 On the **Devices** > **Inventory**window, check the check box next to the Cisco AireOS Controller that you want to provision as a guest anchor controller.

Step 16 Repeat Step 3 through Step 8.

Step 17 Select a role for the Cisco AireOS Controller as **Guest Anchor**.

Step 18 For a guest anchor wireless controller, you need to configure interface and VLAN details.

Step 19 Repeat Step 11 through Step 14.

Provision a Meraki Device

This procedure explains how to provision SSIDs to Cisco Meraki devices managed by a Meraki dashboard.

Before you begin

- Integrate the Meraki dashboard with Cisco DNA Center. See Integrate the Meraki Dashboard, on page 68.
- Create the SSID. See Create SSIDs for an Enterprise Wireless Network, on page 141.

Note The Meraki dashboard supports the following types of SSIDs:

- Open: This SSID corresponds to Open in the Meraki dashboard.
- WPA2 Personal: This SSID corresponds to the preshared key with WAP2 in the Meraki dashboard.
- WPA2 Enterprise: This SSID corresponds to WAP-2 Encryption with Meraki authentication or My Radius server in the Meraki dashboard. If you have defined AAA or Cisco ISE servers for client and endpoint authentication at the building level in Cisco DNA Center, the configuration will be provisioned to **my Radius server** in the Meraki dashboard. Otherwise, **Meraki Radius** will be used for authentication by the Meraki devices.

For every SSID, you can choose an interface name. If you choose the **Management** interface in Cisco DNA Center and the VLAN ID is 0, the configuration is not supported in the Meraki dashboard and VLAN tagging is disabled in the Meraki dashboard. If you create a custom interface for the SSID in Cisco DNA Center, an AP tag is created with the custom interface name and VLAN ID in the Meraki dashboard.

- Create the network profile and assign it to the sites for which the SSID is provisioned.

Note The Network Hierarchy **Sites > Buildings** in Cisco DNA Center corresponds to the **Organization > Network** in the Meraki dashboard. We recommend that you choose **Buildings** in the **Add Sites to Profile** window in the workflow.

Note Cisco DNA Center creates the Meraki network and provisions the SSIDs to the network. The Meraki dashboard provisions the Meraki network configuration to the Meraki devices.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision**.

The **Devices** > **Inventory** window appears, listing all discovered devices.

Step 2 To view the Meraki dashboard, expand the **Global** site in the left pane, and select a building.

All Meraki dashboards available in the selected building are displayed.

Step 3 Check the check box next to the Meraki dashboard name that you want to provision.

Step 4 From the **Actions** drop-down list, choose **Provision** > **Provision Device**.

The **Assign Site** window appears, where you can view the Meraki dashboard and the associated building.

Step 5 To change the associated building, click **Choose a site**.

Step 6 In the **Choose a site** window, select a building and click **Save**.

Step 7 Click **Next**.

The **Configuration** window appears. You can view the managed building in the Primary location.

Step 8 Click **Select Secondary Managed AP Locations** to select the secondary managed location for the Meraki dashboard.

Step 9 In the **Managed AP Location** window, check the check box next to the building name.

Step 10 Click **Save**.

Step 11 Click **Next**.

The **Summary** window displays the following information:

- **Device Details**
- **Network Settings**
- **SSID**

  Note Meraki deployment supports a maximum of 15 SSIDs in each network.

- **Managed Sites**

Step 12 Click **Deploy**.

Step 13 In the **Provision Devices** window, do the following to preview the CLI configuration:

- Click the **Generate Configuration Preview** radio button.
- In the **Task Name** field, enter a name for the CLI preview task and click **Apply**.
- In the **Task Submitted** pop-up, click the **Work Items** link.

  Note If you missed the **Task Submitted** pop-up, click the **Menu** icon (☰) and choose **Activity** > **Work Items**.

- In the **Work Items** window, click the CLI preview task for which you submitted the configuration preview request.
- View the CLI configuration details and click **Deploy**.
- To immediately deploy the device, click the **Now** radio button, and click **Apply**.
- To schedule the device deployment for a later date and time, click the **Later** radio button and define the date and time of the deployment.
- In the **Information** pop-up, do the following:
  - Click **Yes** if you want to delete the CLI preview task from the **Work Items** window.
  - Click **No** if you want to retain the task in the **Work Items** window.

    Note The CLI task will be marked as completed in the **Work Items** window. You can view the CLI configuration for this task, but you cannot deploy it again.

The **Provision Status** column in the **Device Inventory** window shows `SUCCESS` after a successful deployment.

Delete a Device After Provisioning

- If you are deleting a device that is already been added to the fabric domain, remove it from the fabric domain and then delete it from the **Provision** menu.
- You cannot delete a provisioned device from the **Inventory** window. Instead, you must delete provisioned devices from the **Provision** menu.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.

The **Inventory** window appears, with the discovered devices listed.

Step 2 Click the **Inventory** tab, which lists all discovered and provisioned devices.

Step 3 Check the check box next to the device that you want to delete.

Note APs are deleted only when the controller to which they are connected is deleted.

Step 4 From the **Action** drop-down list, choose **Delete Device**.

Step 5 At the confirmation prompt, click **OK**.

Provision a LAN Underlay

Use LAN automation to provision a LAN underlay.

Before you begin

- Configure your network hierarchy. (See Add a Device to a Site, on page 72.)
- Make sure you have defined the following global network settings:
  - Network servers, such as AAA, DHCP, and DNS servers. (See Configure Global Network Servers, on page 189.)
  - Device credentials, such as CLI, SNMP, HTTP, and HTTPS credentials. (See Configure Global CLI Credentials, on page 176, Configure Global SNMPv2c Credentials, on page 177, Configure Global SNMPv3 Credentials, on page 178, and Configure Global HTTPS Credentials, on page 180.)
  - IP address pools. (See Configure IP Address Pools, on page 184.)
- Make sure that you have at least one device in your inventory. If not, discover devices using the Discovery feature.

Note LAN automation is blocked if the discovered site is configured with CLI credentials that has a username "cisco".

- If you have a Cisco Catalyst 9400 Switch configured in the network, ensure the following operations are done on the switch for LAN automation to automatically enable the 40G port:

- Day-0 Configuration is performed on the switch.
- A 40G Quad Small Form-Factor Pluggable (QSFP) transceiver is inserted in either port 9 or port 10 of the Supervisor, and the ports numbered 1 to 8 on the Supervisor do not have a 10G or 1G Small Form-Factor Pluggable (SFP) transceiver inserted in them. If there are dual supervisor engines, ensure the 40G QSFP is inserted in port 9.

  For more information on the Catalyst 9400 Series Supervisor, see Cisco Catalyst 9400 Series Supervisor Installation Note.

Step 1 Reserve an IP address pool for the site that you will be provisioning.

Note The size of the LAN automation IP address pool must be at least 25 bits of netmask or larger.

a) In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Design** > **Network Settings** > **IP Address Pools**.
b) From the **Network Hierarchy** pane, choose a site.
c) Click **Reserve** and complete the following fields in the **Reserve IP Pool** window to reserve all or part of an available global IP address pool, for the specific site:
   - **IP Address Pool Name**: Unique name for the reserved IP address pool.
   - **Type**: Type of IP address pool. For LAN automation, choose **LAN**.
   - **IP Address Space**: Check **IPv4** or **IPv6** to create an address pool. To create a dual-stack pool, check both **IPv4** and **IPv6** check boxes.
   - **Global IP Pool**: IPv4 address pool from which you want to reserve all or part of the IP addresses.

     Note LAN automation uses only the IPv4 subnet.

   - **Prefix length / Number of IP Addresses**: IP subnet and mask address used to reserve all or part of the global IP address pool or the number of IP addresses that you want to reserve.
   - **Gateway**: Gateway IP address.
   - **DHCP Server(s)**: DHCP server(s) IP address(es).
   - **DNS Server(s)**: DNS Server(s) IP address(es).
d) Click **Reserve**.

Step 2 Discover and provision the devices.

a) In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Inventory**.

   All the discovered devices are displayed.
b) Click **Actions** > **Provision** > **LAN Automation**.
c) In the **LAN Automation** window, complete the following fields:
   - **Primary Site**: Select your Primary Device from this site.
   - **Peer Site**: This site is used for selection of Peer Device. Note that this site can be different from the Primary Site.

- **Primary Device**: Select the primary device that Cisco DNA Center uses as the starting point to discover and provision new devices.
- **Peer Device**: Select the peer device.
- **SELECTED PORTS OF PRIMARY DEVICE**: Ports to be used to discover and provision new devices. Click **Modify Selections** to enter the port numbers.
- **Discovered Device Site**: All newly discovered devices are assigned to this site. This site can be different from Primary and Peer Sites.
- **Main IP Pool**: IP address pool that was reserved for LAN automation. (See Step 1.)
- **Link Overlapping IP Pool**: IP address pool that is shared with other sites, is used to specifically configure the /31 IP addresses on point-to-point links in the underlay.

  A link overlapping IP pool can be a subpool that is inherited from a parent site or a subpool that is defined in any other site.

  A link overlapping IP pool allows you to overlap /31 IP addresses in a multisite deployment. Hosts in different sites will be able to reuse IP addresses on the /31 links.

  If you choose to define a link overlapping IP pool, the addresses defined in the **Main IP Pool** field are used for Management IPs (like loopback address, VLAN address, and so on).
- **ISIS Domain Password**: A user-provided IS-IS password when LAN automation starts. If the password already exists on the seed device, it is reused and is not overwritten. If no user-provided password is entered and there is no existing IS-IS password on the device, the default domain password is used. If both primary and secondary seeds have domain passwords, ensure that they match.
- **Enable Multicast**: Check this check box to enable underlay native multicast. LAN automation creates a multicast tree from seed devices as RPs and discovered devices as subscribers.
- **Device Name Prefix**: Name prefix for the devices being provisioned. As Cisco DNA Center provisions each device, it prefixes the device with the text that you provide and adds a unique number at the end. For example, if you enter **Access** as the name prefix, as each device is provisioned, it is named Access-1, Access-2, Access-3, and so on.
- **Choose a File**: Click **Browse** to choose a hostname map File. Configures user-provided names for discovered devices using the chosen CSV file that contains a mapping between serial numbers and hostnames. If the discovered device is a stack, all serial numbers of the stack are provided in the CSV file.

  Here is a sample CSV file:

```
standalone-switch,FCW2212L0NF
stack-switch,"FCW2212E00Y,FCW2212L0GV"
```

d) Click **Start**.

Cisco DNA Center begins to discover and provision the new devices.

LAN automation configures an IP address on the seed device of VLAN 1. If this VLAN 1 IP address of the seed device is not reachable from Cisco DNA Center, an error message is displayed on the LAN Automation Status window. Hover your cursor over the **See Details** link on this window to see the error details and possible remedial actions.

Step 3 Monitor and review the progress of the devices being provisioned.

a) Click **Actions** > **Provision** > **LAN Automation Status**.

The **LAN Automation Status** window displays the progress of the devices being provisioned.

Note The provisioning of new devices may take several minutes.

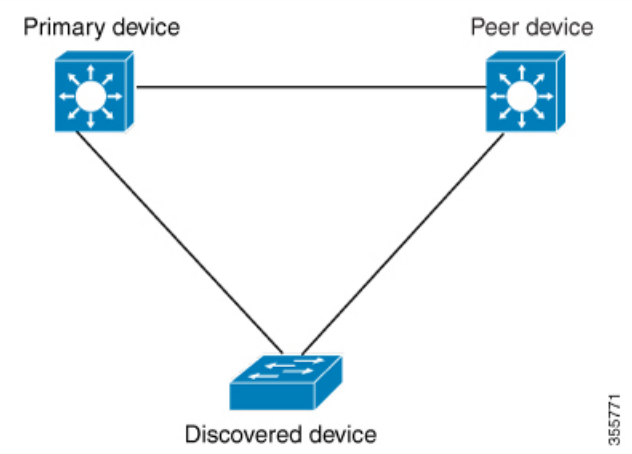
b) After all devices have been discovered, added to Inventory, and are in Managed state, click **Stop** in the **LAN Automation Status** window.

The LAN automation process is complete, and the new devices are added to the Inventory.

Peer Device in LAN Automation Use Case

Provision a Dual-Homed Switch

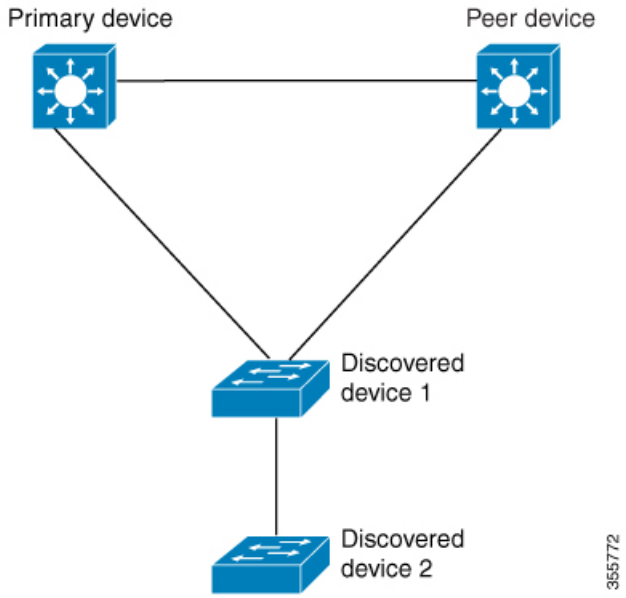
You must always select a peer device to provision the dual-homed switch.



Cisco DNA Center configures the DHCP server on the primary device. Because Cisco DNA Center understands that the discovered device is connected to both the primary and peer devices, it configures two Layer 3 point-to-point connections when the LAN automation task is stopped. One connection is established between the discovered device and the primary device; the other connection is established between the discovered device and the peer device.

Note If the link between the primary and the peer device is not configured before the LAN automation job is executed, you must select the interface of the primary device that connects to the peer device as part of the LAN automation configuration in Cisco DNA Center.

LAN Automation's Two-Hop Limitation



For the preceding topology, Cisco DNA Center configures the following links:

- A point-to-point Layer 3 routed connection from *Discovered device 1* to *Primary device*
- A point-to-point Layer 3 routed connection from *Discovered device 1* to *Peer device*
- A point-to-point Layer 3 routed connection from *Discovered device 1* to *Discovered device 2*

Consider the scenario where a device—named *Discovered device 3*—is directly connected below *Discovered device 2*. The connection between *Discovered device 2* and *Discovered device 3* is not configured as part of the LAN automation job, because it is more than two hops away from *Primary device*.

Check the LAN Automation Status

You can view the status of in-progress LAN automation jobs.

Before you begin

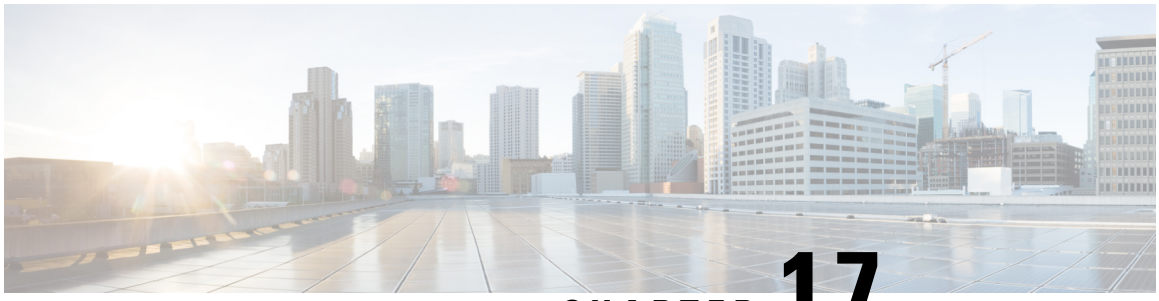
You must have created and started a LAN automation job.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Inventory**.

All discovered devices are displayed.

Step 2 Choose **Actions** > **Provision** > **LAN Automation Status**.

The **LAN Automation Status** window displays the status of all running or completed LAN automation jobs.



CHAPTER 17

Provision Fabric Networks

About Fabric Networks

A fabric network is a logical group of devices that is managed as a single entity in one or multiple locations. Having a fabric network in place enables several capabilities, such as the creation of virtual networks and user and device groups, and advanced reporting. Other capabilities include intelligent services for application recognition, traffic analytics, traffic prioritization, and steering for optimum performance and operational effectiveness.

Cisco DNA Center allows you to add devices to a fabric network. These devices can be configured to act as control plane, border, or edge devices within the fabric network.

Fabric Sites and Fabric Domains

A fabric site is an independent fabric area with a unique set of network devices: control plane, border, edge, wireless controller, ISE PSN. Different levels of redundancy and scale can be designed per site by including local resources: DHCP, AAA, DNS, Internet, and so on.

A fabric site can cover a single physical location, multiple locations, or only a subset of a location:

- Single location: branch, campus, or metro campus
- Multiple locations: metro campus + multiple branches
- Subset of a location: building or area within a campus

A fabric domain can consist of one or more fabric sites and transit site. Multiple fabric sites are connected to each other using a transit site.

There are two types of transit sites:

- SD-Access transit: Enables a native SD-Access (LISP, VXLAN, CTS) fabric, with a domain-wide control plane node for intersite communication.
- IP-based transit: Leverages a traditional IP-based (VRF-LITE, MPLS) network, which requires remapping of VRFs and SGTs between sites.

Multi-Site Fabric Domain

A multi-site fabric domain is a collection of fabric sites interconnected via a transit site. A fabric site is a portion of the fabric that has its own set of control plane nodes, border nodes, and edge nodes. A given fabric site can also include fabric WLC and APs, and a related site-specific ISE PSN. Multiple fabric sites in a single fabric domain are interconnected using a transit site.

A Software-Defined Access (SDA) fabric may comprise multiple sites. Each site has the benefits of scale, resiliency, survivability, and mobility. The overall aggregation of sites (that is, the fabric domain) must also be able to accommodate a very large number of endpoints and scale modularly or horizontally by aggregating sites contained within each site.

Transit Sites

A transit site is a site that connects two or more fabric sites with each other or connects the fabric site with external networks (Internet, data center, and so on). There are two types of transit networks:

- IP transit: Uses a regular IP network to connect to an external network or to connect two or more fabric sites.
- SDA transit: Uses LISP/VxLAN encapsulation to connect two fabric sites. The SDA transit area may be defined as a portion of the fabric that has its own Control Plane Nodes, but does not have Edge or Border Nodes. However, it can work with a fabric that has an external border. Using SDA transit, an end-to-end policy plane is maintained using SGT group tags.

Create an IP Transit Network

To add a new IP transit network:

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Fabric**.

Step 2 Hover the mouse pointer over **Add Fabric or Transit/Peer Network**.

Step 3 From the drop-down list, click **Transit/Peer Network**.

Step 4 Enter a transit name for the network.

Step 5 Choose **IP-Based** as the transit type.
The routing protocol is set to BGP by default.

Step 6 Enter the Autonomous System Number (ASN) for the transit network.

Step 7 Click **Save**.

Create an SDA Transit Network

To add a new SDA transit network:

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Fabric**.

Step 2 Hover the mouse pointer over **Add Fabric or Transit/Peer Network**.

Step 3 From the drop-down menu, click **Transit/Peer Network**.

Step 4 Enter a transit name for the network.

Step 5 Choose **SD-Access** as the transit type.

Step 6 Enter the **`Site for the Transit Control Plane`** for the transit network. Choose at least one transit map server.

Step 7 Enter the **`Transit Control Plane`** for the transit network.

Step 8 Repeat Step 7 and Step 8 to add a second map server.

Step 9 Click **Save**.

What to do next

After you create an SDA transit, go to the fabric site and connect the sites to which you want to connect the SDA transit. Go to **Provision** > **Fabric** > **Fabric Site**. Choose the fabric site that you created. Click **Fabric Site** > **Border** > **Edit Border** > **Transit**. From the drop-down list, point to your SDA transit site and click **Add**.

Create a Fabric Domain

Cisco DNA Center creates a default fabric domain called *Default LAN Fabric*.

Before you begin

Ensure that your network has been designed, the policies have been retrieved from the Cisco Integrated Services Engine (ISE) or created in the Cisco DNA Center, and the devices have been inventoried and added to the sites.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Fabric**.

Step 2 Hover the mouse pointer over **Add Fabric or Transit/Peer Network**.

Step 3 Click **Add Fabric** from the pop-up.

Step 4 Enter a fabric name.

Step 5 Choose one fabric site.

Step 6 Click **Add**.

Fabric Readiness and Compliance Checks

Fabric Readiness Checks

Fabric readiness checks are a set of preprovisioning checks done on a device to ensure that the device is ready to be added to the fabric. Fabric readiness checks are now done automatically when the device is provisioned. Interface VLAN and Multi VRF configuration checks are not done as part of fabric readiness checks.

Fabric readiness checks include the following:

- Connectivity checks: Checks for the necessary connectivity between devices; for example, connectivity from the edge node to map server, from edge node to border, and so on.
- Existing configuration check (brownfield check): Checks for any configuration on the device that conflicts with the configuration that is pushed through SD-Access and can result in a failure later.

- Hardware version: Checks if the hardware version of the device is supported.
- Image type: Checks if the device is running with a supported image type (IOS-XE, IOS, NXOS, Cisco Controller).
- Loopback interface: Checks for the loopback interface configuration on the device. A device must have a loopback interface configured on it to work with the SDA application.
- Software license: Checks if the device is running with an appropriate software license.
- Software version: Checks if the device is running with an appropriate software image.

For more information on the software versions supported, see the Cisco SD-Access Hardware and Software Compatibility Matrix.

If an error is detected during any of the fabric readiness checks, an error notification is displayed on the topology area. You can correct the problem and continue with the provisioning workflow for the device.

Fabric Compliance Checks

Fabric compliance is a state of a device to operate according to the user intent configured during the fabric provisioning. Fabric compliance checks are triggered based on the following:

- Every 24 hours for wired devices and every six hours for wireless devices.
- When there is a configuration change on the wired device.

  A configuration change on the wired device triggers an SNMP trap, which in turn triggers the compliance check. Ensure that you have configured the Cisco DNA Center server as an SNMP server.

The following compliance checks are done to ensure that the device is fabric compliant:

- Virtual Network: Checks whether the necessary VRFs are configured on the device to comply with the current state of user intent for the VN on Cisco DNA Center.
- Fabric Role: Checks whether the configuration on the device is compliant with the user intent for a fabric role on Cisco DNA Center.
- Segment: Checks the VLAN and SVI configuration for segments.
- Port Assignment: Checks the interface configuration for VLAN and Authentication profile.

Configure a Fabric Domain

You can add devices to sites and assign roles to these devices—border, control plane, or edge. You can also configure IP address pools to enable communication between hosts.

Add a Fabric Site

Before you begin

You can create a new fabric site only if IP Device Tracking (IPDT) is already configured for the site. This means that you should have enabled **Monitor wired clients** while configuring Telemetry settings for the site.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Fabric**.

Step 2 Hover the mouse pointer over **Add Fabric or Transit/Peer Network**.

Step 3 From the drop-down list, click **Fabric**.

Step 4 In the **Add Fabric Site** pane that slides in, choose a `Site` from the list of Sites that appears.

Step 5 Click **Next**.

Step 6 Select the virtual networks that are to be added to the fabric site.

Step 7 Click **Finish**.

If IPDT is not already enabled for the site (if **Monitor wired clients** is not selected during the Network Telemetry Settings), the fabric site is not added.

Add a Device to a Fabric

After you have created a fabric domain, you can add fabric sites, and then add devices to the fabric site. You can also specify whether the devices should act as a control plane node, an edge node, or a border node.

You can add a new device to the fabric site only if IP Device Tracking (IPDT) is configured for the fabric site.

A device which is assigned the Access role and has been provisioned before enabling IPDT on the site cannot be added to the fabric. Reprovision such devices before adding them to the fabric site. Check the Provision workflow to confirm the status of **Deployment of IPDT** on the device.

Note

- It is optional to designate the devices in a fabric domain as control plane nodes or border nodes. You might have devices that do not occupy these roles. However, every fabric domain must have at least one control plane node device and one border node device. In the current release for wired fabric, you can add up to six control plane nodes for redundancy.
- Currently, the Cisco Wireless Controller communicates only with two control plane nodes.

Before you begin

Provision the device if you have not already provisioned it:

1. In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Devices** > **Inventory**.
2. The **Inventory** window displays the discovered devices.
3. The topology view shows a device in gray color if it has passed the fabric readiness checks and is ready to be provisioned.
4. If an error is detected during any of the fabric readiness checks, an error notification is displayed on the topology area. Click **See more details** to check the problem area listed in the resulting window. Correct the problem and click **Re-check** to ensure that the problem is resolved.
5. If you update the device configuration as part of problem resolution, ensure that you resynchronize the device information by performing an **Inventory** > **Resync** for the device.

Note You can continue to provision a device that has failed the fabric readiness checks.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Fabric**.
The window displays all the provisioned fabric domains.

Step 2 From the list of fabric domains, choose a fabric.
The resulting screen displays all the sites in that fabric domain.

Step 3 Choose a site.

All devices in the network that have been inventoried are displayed in the topology view. Any device that is added to the fabric is shown in blue.

Step 4 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.

To configure a device as a fabric-in-a-box, select the **Control Plane**, **Border**, and **Edge** options.

To configure the device as a control plane and a border node, select both **Control Plane** and **Border**.

Step 5 Click **Add**.

What to do next

After a device is added to the fabric, fabric compliance checks are automatically performed to ensure that the device is fabric compliant. The topology displays a device that has failed the fabric compliance check in blue color with a cross-mark beside it. Click **See more details** on the error notification to identify the problem area and correct it.

Add a Device as a Border Node

When you are adding a device to a fabric, you can add it in various combinations to act as a control plane, border node, or edge node as explained in Add a Device to a Fabric, on page 439.

To add a device as a border node:

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Fabric**.
A list of all provisioned fabric domains is shown.

Step 2 From the list of fabric domains, choose a fabric.
A list of all fabric sites is shown.

Step 3 From the list of fabric sites, choose a site. The resulting topology view displays all devices in the network that have been inventoried. In the topology view, any device that is added to the fabric is shown in blue.

Step 4 Click a device.

Step 5 In the slide-in window that appears, click the **Border** toggle button.

Step 6 In the resulting window, click the **Layer 3 Handoff** tab.

Step 7 Check the **Enable Layer-3 Handoff** check box.

Step 8 Enter the **Local Autonomous Number** for the device.

If the Local Autonomous Number is already configured on the device, this field displays the configured number and is disabled. You cannot change the Local Autonomous Number if it is already configured on the device.

Step 9 From the **Select IP Pool** drop-down list, choose an IP address pool.

Select an IP pool only if you want to add an IP transit network.

Step 10 Choose a transit network that is enabled on the border device:

a) To enable SDA transit on the border, choose a user-created SDA transit domain from the **Select Transit/Peer Network** drop-down list.

Click **Add**.

b) To enable IP transit on the border, choose a user-created IP transit domain from the **Select Transit/Peer Network** drop-down list.

Click **Add**.

Do the following steps in the resulting window:

1. Choose an IP pool from Design Hierarchy. The selected pool is used to automate IP routing between the border node and the IP peer.
2. Click **Add Interface** to enter interface details on the next screen.
3. Choose **External Interface** from the drop-down list.
4. Enter a custom description for the interface at **Interface Description**.
5. Enter the **Remote AS Number**.
6. Check the **Virtual Network** from the list. This virtual network is advertised by the border to the remote peer. You can select one, multiple, or all virtual networks.
7. Click **Save**.

Step 11 By default, a border is designated as an external border, wherein it acts as a gateway to all unknown traffic, without importing any external routes. A border can be configured to be an internal border, wherein it acts as a gateway to known traffic and imports specific external routes. A border can also have a combined role of internal and external borders.

- Check both **Default to all Virtual Networks** and **Do not Import External Routes** check boxes to designate the border as an external border, providing connectivity to unknown networks.
- Do not check both **Default to all Virtual Networks** and **Do not Import External Routes** check boxes to designate the border as an internal border, operating as a gateway for specific network addresses.

- Check the **Default to all Virtual Networks** check box to designate this border node as an internal and external border. It acts as a gateway to all known and unknown traffic sent from the edge nodes. (Do not check the **Do not Import External Routes** check box.)

Step 12 (Optional) Perform this step only if you are connecting a nonfabric network to the fabric network or you are migrating from a traditional network to an SDA network. Click the **Layer 2 Handoff** tab. A list of virtual networks and the count of IP pools in each virtual network is displayed.

a) Click a virtual network that is to be handed off.

After you select a virtual network, a list of IP address pools that are present in the virtual network appears. A list of interfaces through which you can connect nonfabric devices is also displayed.

b) Select an **External Interface**.

In Cisco DNA Center Release 2.1.2.6, you can select more than one interface on which you can do a Layer 2 handoff.

c) Enter the **Interface Description**.

d) Enter the **External VLAN** number into which the fabric must be extended.

In releases earlier than Cisco DNA Center 2.1.2.6, a virtual network can only be handed off on a single interface. The same virtual network cannot be handed off through multiple interfaces.

In Cisco DNA Center Release 2.1.2.6 and later releases, a virtual network can be handed off on a single interface or on multiple interfaces. Layer 2 handoff for a segment can also be done on two different devices. In both cases, ensure that there are no loops formed in the network.

e) Click **Save**.

Step 13 Click **Add**.

Configure Host Onboarding

The **Host Onboarding** tab lets you configure settings for the various kinds of devices or hosts that can access the fabric domain.

The **Host Onboarding** tab has the following subtabs:

- **Authentication** tab: Select an authentication template for the fabric. An Authentication template is a predefined set of configurations that are retrieved from Cisco ISE. After selecting the authentication template, click **Save**.
- **Virtual Networks** tab: Associate IP address pools to virtual networks (default, guest, or user defined), and click **Update**. The IP address pools displayed are site-specific pools only.
- **Wireless SSIDs** tab: Specify wireless SSIDs within the network that hosts can access. You can select the guest or enterprise SSIDs and assign address pools, and click **Save**.
- **Port Assignment** tab: Apply specific configurations to each port, depending on the type of device that connects to the fabric domain. To do this, select the ports that need a specific assignment, click **Assign**, and choose the port type from the drop-down list.

  Note the following constraints:

- Cisco SD-Access deployments support only APs, extended nodes, user devices (such as a single computer or a single computer plus phone), and devices that need trunk ports like single servers.
- Servers with internal switches or virtual switches aren't supported.
- Other networking equipments (such as hubs, routers, or switches) aren't supported.

Select the Authentication Template

You can select the authentication template that applies to all devices in the fabric domain.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Fabric**.

Step 2 In the resulting window, click a fabric.

Step 3 From the **Fabric Sites** pane, choose a site.

Step 4 Click the **Host Onboarding** tab.

Step 5 In the **Authentication** tab, choose an authentication template for the site:

- **Closed Authentication**: Any traffic prior to authentication is dropped, including DHCP, DNS, and ARP.
- **Low Impact**: Security is added by applying an ACL to the switch port, to allow very limited network access prior to authentication. After a host has been successfully authenticated, additional network access is granted.
- **No Authentication**
- **Open Authentication**: A host is allowed network access without having to go through 802.1X authentication.

You can edit the settings of the selected authentication template to address site-specific authentication requirements.

Before you change the site-level authentication, you must resychronize any fabric devices where APs were onboarded through macros or autoconf and haven't yet undergone the periodic resynch.

Step 6 (Optional) To edit the settings of the chosen authentication method, click **Edit**.

A window slides in, displaying the parameters of the selected authentication method: **First Authentication Order**, **802.1x to MAB Fallback**, **Wake on LAN**, and **Number of hosts**.

Note **Number of hosts** specifies the number of data hosts that can be connected to a port. With **Single**, you can have only one data client on the port. With **Unlimited**, you can have multiple data clients and one voice client on the port.

Make the required changes and click **Save**.

The edit window closes. The saved modifications apply only to the site for which the authentication template is edited.

Step 7 Click **Deploy**.
The Hitless Authentication Change feature lets you switch from one authentication method to another without removing the devices from the fabric.

Associate Virtual Networks to the Fabric Domain

IP address pools enable host devices to communicate within the fabric domain.

When an IP address pool is configured, Cisco DNA Center immediately connects to each node to create the appropriate switch virtual interface (SVI) to allow the hosts to communicate.

You cannot add an IP address pool, but you can configure a pool from the ones that are listed. The IP address pools listed are created when the network is designed.

You can configure the following features of a virtual network using this procedure:

- Common IP address pool
- Wireless IP address pool
- Critical IP address pool
- IP Directed Broadcast
- Custom VLAN ID
- Layer 2 Flooding
- Anchored virtual network

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Provision** > **Fabric**.

Step 2 In the resulting window, click a fabric.

Step 3 In the **Fabric Sites** pane, select a site.

Step 4 In the **Host Onboarding** tab, click **Virtual Networks**.

Step 5 To associate one or more virtual network(s) to the selected fabric site, click the icon (**Add Virtual Network**).

a) In the **Add Virtual Network** slide-in pane, select the virtual networks to be added to the fabric site.
b) Click **Update**.

Step 6 To edit a virtual network, in the **Virtual Networks** tab, click a virtual network.

Step 7 Review the following fields in the **Edit Virtual Network** slide-in pane:

Field	Description
IP Pool Name	IP address pools that are associated with the virtual network.
VLAN	ID of the VLAN that is associated with the virtual network.
VLAN Name	Name of the VLAN associated with the virtual network.
Traffic Type	Type of traffic enabled on the virtual network.
Scalable Group	Group that the IP pool belongs to.
Common Pool	Selected IP pool is shared across multiple sites in a fabric. To enable or disable the common pool, choose **Actions** > **Enable/Disable Common Pool**.
Wireless Pool	Selected IP pool is enabled as a **Wireless Pool**. To enable or disable the selected IP pool as a wireless pool, choose **Actions** > **Enable/Disable Wireless Pool**.

Field	Description
	If enabled, you can choose from only the defined wireless pool while configuring wireless SSID for the fabric.
Layer-2 Only	Selected IP pool is used exclusively as a Layer 2 segment.
IP Directed Broadcast	IP Directed Broadcast setting for the selected IP pool. To enable this setting, check the check box. To disable it, uncheck the check box.
Layer-2 Flooding	Layer 2 flooding setting for the selected IP pool. To enable this setting, check the check box. To disable it, uncheck the check box. Layer 2 flooding is disabled by default.

Step 8 To associate one or more IP address pool(s) to the selected virtual network, click **Add**.

In the **Edit Virtual Network** slide-in pane, do the following:

a) Choose the **IP Address Pool** from the drop-down list.
b) Enter a valid **VLAN Name**.
c) Enter a custom **VLAN** number for the virtual network.

Note the following:

- VLAN IDs 1, 1002-1005, 2046, and 4095 are reserved and cannot be used.
- If you do not provide a custom VLAN ID, Cisco DNA Center generates a VLAN ID in the range of 1021 to 2020.

d) Choose a **Scalable Group** from the drop-down list.
e) Choose the **Traffic** type from the drop-down list.

You can choose to send voice or data traffic through the virtual network.

f) To enable Layer 2 flooding, check the **Layer-2 Flooding** check box.

Note Layer 2 flooding requires underlay multicast, which is configured during LAN Automation. If you do not provision the underlay through LAN Automation, configure underlay multicast manually.

g) To include this IP pool in the critical IP address pool, check the **Critical Pool** check box.

A critical pool is used for closed authentication profile when an authentication server is not available. A critical VLAN is assigned to the critical pool and all unauthenticated hosts are placed in the critical VLAN in the absence of an authentication server.

h) To enable this IP pool to be shared across multiple sites in a fabric, check the **Common Pool** check box.

The **Intersite Layer 2 Handoff** feature supports sharing an IP pool among multiple sites in a fabric.

i) To enable this IP pool as a wireless IP address pool, check the **Wireless Pool** check box.
j) To enable the IP Directed Broadcast feature, check the **IP Directed Broadcast** check box.

Note
- Enable Layer-2 flooding before enabling IP Directed Broadcast.
- You cannot enable the IP Directed Broadcast feature on a segment that has Intersite Layer 2 Handoff enabled on it.
- Routers and Nexus 7000 Series Switches do not support the IP Directed Broadcast feature.

k) Click **Add** to save the settings.

The settings you specify here are deployed to all devices in the virtual network.

l) To associate more IP pools, click the icon and repeat the steps.

Step 9 To anchor this virtual network and enable its border to be a common border for all traffic through this virtual network, check the **Use Border/CP for this site to be common for the Virtual Network** check box.

An anchored virtual network can be added to other fabric sites to enable multisite guest access to a common border.

An anchored virtual network is displayed with an anchor tag next to it.

Note
- You cannot anchor a virtual network if it contains segments.
- Before anchoring a virtual network, ensure that all control plane and border devices are provisioned.
- If you enable multicast on the anchored virtual network, multicast is configured on the edge devices of the inherited virtual network, provided the inherited virtual network has segments configured. If the inherited virtual network does not have a segment, multicast is deployed only after the first segment is created.

Step 10 After associating IP pools to all virtual networks, click **Save**.

Configure Wireless SSIDs for the Fabric Domain

Step 1 From the **Wireless SSID** section, specify the wireless SSIDs within the network that the hosts can access.

Step 2 Click **Choose Pool** and select an IP pool reserve for the SSID.

Step 3 From the **Assign SGT** drop-down list, choose a scalable group for the SSID.

Step 4 Check the **Enable Wireless Multicast** check box to enable wireless multicast on the SSIDs.

Configure Ports Within the Fabric Site

The **Port Assignment** tab lets you configure each access device on the fabric domain. You can specify network behavior settings for each port on a device.

Note The settings you make here for the ports override the general settings you made for the device in the **Virtual Networks** section.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Provision** > **Fabric**.

Step 2 In the resulting window, click a fabric.

Step 3 From the **Fabric Sites** pane, select a site.

Step 4 From the **Host Onboarding** tab, click **Port Assignment** tab.

Step 5 From the list of fabric devices displayed in the left pane, choose the device that you want to configure. The ports available on the device are displayed in the right pane.

Step 6 From the right pane, select the ports of the device and click **Assign**.

Step 7 In the **Port Assignment** pane that slides in, select the **Connected Device Type** from the following options in the drop-down list:

Option	Description
Trunk	Configure the port as trunk port.
Access Point(AP)	Configures the port to connect to an access point.
User Devices (ip-phone, computer, laptop)	Configures the port to connect to a host device.

a) To connect a trunk port, select **Trunk** and provide a **Description** for this port.

b) To connect an access point, select **Access Point(AP)** and do the following:

1. Select the VLAN and IP address from the **VLAN Name / IP Address Pool (Data)** drop-down list.
2. Select the **Authentication** type from the drop-down list.
3. Provide a **Description** about the connected device.

c) To connect host devices, select **User Devices (ip-phone, computer, laptop)** and do the following:

1. Select the IP address pool for data from the **VLAN Name / IP Address Pool (Data)** drop-down list.
2. Select the **Scalable Group**s, which are the groups you have provisioned.

   Scalable groups are supported only with No Authentication profile.
3. Select the IP address pool for voice from the **VLAN Name / IP Address Pool (Voice)** drop-down list.
4. Select the authentication template from the **Authentication** drop-down list.
5. Enter a **Description** for the connected device.

d) Click **Update**.

Step 8 After completing all port assignments, click **Deploy**.

Configure an Extended Node Device

Extended nodes are those devices that run in Layer 2 switch mode and do not support fabric technology natively. An extended node is configured by an automated workflow. After configuration, the extended node device is displayed on the fabric topology view. **Port Assignment** on the extended nodes is done on the **Host Onboarding** window.

Note Extended Nodes cannot be onboarded through the User Interface-based provisioning workflows. Extended nodes are onboarded only through the SD-Access automated workflow after resetting the device configuration to factory default and powering on the device.

Extended node devices support multicast traffic.

Policy extended nodes are extended nodes that support security policy within the virtual network. You can select a **Group** during port assignment for the policy extended node.

Cisco Catalyst Industrial Ethernet (IE) 3400, IE 3400 Heavy Duty series switches, and Cisco Catalyst 9000 series switches that run Cisco IOS XE 17.1.1s or later releases of the software are policy extended node devices.

Cisco Digital Building series switches, Cisco Catalyst 3560-CX switches, and Cisco Industrial Ethernet 4000, 4010, and 5000 series switches are not policy extended node devices. They do not support Cisco TrustSec and **Group** selection during port assignment.

Steps to Configure an Extended Node

When configured as a fabric edge, Cisco Catalyst 9300, Cisco Catalyst 9400, and Cisco Catalyst 9500 series switches support extended nodes.

The minimum supported software version on the edge nodes that support policy extended nodes is Cisco IOS XE 17.1.1s.

Note Cisco Catalyst 9200 series switches that are configured as fabric edge nodes do not support extended node devices.

The following are the minimum supported software versions on the extended nodes:

- Cisco Industrial Ethernet 4000, 4010, 5000 series switches: 15.2(7)E0s with LAN base license enabled
- Cisco Catalyst IE 3400, 3400 Heavy Duty (X-coded and D-coded) series switches: IOS XE 17.1.1s
- Cisco Catalyst IE 3300 series switches: IOS XE 16.12.1s
- Cisco Digital Building series switches, Cisco Catalyst 3560-CX switches: 15.2(7)E0s

Ensure the following before configuring a policy extended node:

- The minimum software version required on a policy extended node device and on the edge device supporting the policy extended node is Cisco IOS XE 17.1.1s.
- Both the policy extended node and the edge node supporting it must have the Network Advantage and DNA Advantage license levels enabled.

Step 1 Configure a network range for the extended node. See Configure IP Address Pools, on page 184. This comprises adding an IP address pool and reserving the IP pool at the site level. Ensure that the CLI and SNMP credentials are configured.

Step 2 Assign the extended IP address pool to INFRA_VN under the **Fabric** > **Host Onboarding** tab. Choose **extended node** as the pool type.

Cisco DNA Center configures the extended IP address pool and VLAN on the supported fabric edge device. This enables the onboarding of extended nodes.

Step 3 Configure the DHCP server with the extended IP address pool and Option 43. Ensure that the extended IP address pool is reachable from Cisco DNA Center.

Note For a detailed description of Option 43, see DHCP Controller Discovery, on page 355.

Step 4 Connect the extended node device to the fabric edge device. You can have multiple links from the extended node device to the fabric edge.

Step 5 Create a port channel on the fabric edge node connected to the extended node.

Complete this step only if the global authentication mode for the fabric is not **No Authentication**. Authentication modes can be **Open, Low Impact**, or **Closed**.

To create a port channel, complete the following steps:

a) Go to **Provision** > **Fabric** > **Fabric Infrastructure** and select the fabric edge node. A window with the device name as the title slides in.

b) In the **Port Channel** tab, click **Create Port Channel**.

c) Fill in all the fields in the pane:

- Select **Extended Node** from the **Connected Device Type** drop down.
- Select **Port Aggregation Protocol (PAgP)**.

  Starting with Cisco IOS XE Release 17.1.1s, IE 3300 and IE 3400 devices support PAgP.
- Select **On** for IE 3300 and IE 3400 devices if they are running versions earlier than Cisco IOS XE 17.1.1s.
- Note that Link Aggregation Control Protocol (LACP) does not work for extended node onboarding.
- Select the ports to be bundled as a port channel.

d) Click **Done**.

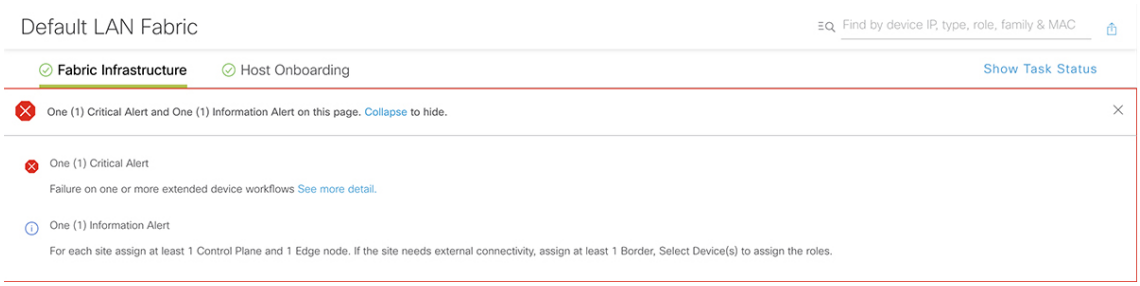
This creates a port channel on the fabric edge node to onboard an extended device.

Step 6 Power up the extended node device if it has no previous configuration. If the extended node device has configurations, write-erase the previous configurations and reload the extended node device.

Cisco DNA Center adds the extended node device to the Inventory and assigns the same site as the fabric edge. The extended node device is then added to the fabric. Now the extended node device is onboarded and ready to be managed.

After the configuration is complete, the extended node appears in the fabric topology with a tag (X) to indicate that it is an extended node.

If there are errors in the workflow while configuring an extended node, an error notification is displayed as a banner on the topology window.



Click **See more details** to see the error.

A Task Monitor window slides in, displaying the status of the extended node configuration task.

Click **See Details** to see the cause of error and possible solution.

Configure a Port Channel

A group of ports bundled together to act as a single entity is called a port channel. Port channels between a fabric edge and its remotely connected devices like extended nodes or servers increase the connection resiliency and bandwidth.

Create a Port Channel

Do the following steps only when authentication is Closed Authentication. Note that the following steps are automated for other authentication modes.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Fabric**.

Step 2 In the resulting window, click a fabric.

Step 3 From the **Fabric Sites** pane, select a site.

Step 4 When you click the **Fabric Infrastructure** tab, all fabric devices are displayed.

Step 5 Click a fabric edge node.

A window with the device name as the title slides in.

Step 6 In the **Port Channel** tab, click **Create Port Channel**.

Step 7 From the **Connected Device Type** drop-down, select the type of connected device.

- To create a port channel between a fabric edge node and an extended node or between two extended nodes, choose **Extended Node**.
- To create a port channel with a fabric edge node or extended node on one side and a third party device or a server port on the other side, choose **Trunk**.

Step 8 Enter a suitable **Description** for the new port channel.

Step 9 Select an appropriate protocol:

- For the extended nodes that run Cisco IOS XE Release 16.12.1s and earlier releases, select **On** as the protocol.
- For the extended nodes that run Cisco IOS XE Release 17.1.1s and later releases, select **Port Aggregation Protocol (PAgP)** as the protocol.
- Do not select **Link Aggregation Control Protocol (LACP)** as the protocol for extended nodes. You can only connect the trunk ports or the server ports in the LACP mode.

Step 10 From the list of ports displayed, choose the ports to be bundled.

Note You cannot have more than 16 members in a port channel that is connected in the LACP mode.

You cannot have a more than eight members in a port channel that is connected in the PAgP mode.

Step 11 Click **Done**.

A new port channel that is created is displayed in the window.

Update a Port Channel

Before you begin

Ensure that at least one member interface exists before you update a port channel.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Fabric**.

Step 2 In the resulting window, click a fabric.

Step 3 From the **Fabric Sites** pane, select a site.

Step 4 When you click the **Fabric Infrastructure** tab, all fabric devices are displayed.

Step 5 Click a fabric edge node.

A window with the device name as the title slides in.

Step 6 Select the **Port Channel** tab.

Step 7 From the list of port channels displayed, select the port channel to be updated.

The resulting window displays all the interfaces and the status of the selected port channel.

Step 8 Do the desired update on the port channel.

You can either add interfaces to the port channel or delete existing interfaces on the port channel.

Step 9 Click **Done**.

Delete a Port Channel

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Fabric** > **Fabric Infrastructure**.

Step 2 Click the device whose port channel you want to delete.

A window with the device name slides in.

Step 3 Click the **Port Channel** tab.

The resulting **Port Channel** view lists all the existing port channels.

Step 4 Select the port channel and click **Delete**.

Step 5 At the prompt, click **Yes**.

Multicast Overview

Multicast traffic is forwarded in different ways:

- Through shared trees by using a rendezvous point. PIM SM is used in this case.
- Through shortest path trees (SPT). PIM source-specific multicast (SSM) uses only SPT. PIM SM switches to SPT after the source is known on the edge router that the receiver is connected to.

See IP Multicast Technology Overview.

Configure Multicast

Cisco DNA Center provides a workflow that helps enable group communication or multicast traffic in the virtual networks. The workflow also allows you to choose multicast implementation in the network: native multicast or headend replication.

Note In Cisco DNA Center Release 2.2.2.4 and later, you can enable multicast on a virtual network whose border serves as a multisite remote border. Configuring multicast on such a virtual network configures multicast on the devices in the inherited virtual network too, provided the inherited virtual network already contains a segment. If the inherited virtual network does not have a segment, multicast is deployed only after the first segment is created. Ensure that a virtual network and its inherited networks deploy the same type of multicast implementation. The edge devices of an inherited virtual network cannot be configured as rendezvous point (RP).

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision**.
The window displays all provisioned fabric domains.

Step 2 From the list of fabric domains, choose a fabric. You can view all the sites configured for the fabric. Select the site for which you want to configure multicast.

Step 3 On the **Fabric Sites** pane, click the gear icon next to the selected site.

Step 4 Choose **Configure Multicast** from the drop-down list.

The resulting window starts a workflow for multicast configuration.

Step 5 In the **Enabling Multicast** window, choose the method of multicast implementation for the network, **Native Multicast** or **Head-end replication**, and click **Next**.

Step 6 In the **Virtual Networks** window, select the virtual network on which you want to set up multicast. Click **Next**.

Note You cannot select an inherited virtual network to set up multicast.

Step 7 In the **Multicast pool mapping** window, select an IP address pool from the **IP Pools** drop-down list. The selected IP address pool is associated with the chosen virtual network. Click **Next**.

Step 8 From the **Select multicast type** window, choose the type of multicast to implement, and click **Next**:

- **SSM** (Source Specific Multicast)
- **ASM** (Any Specific Multicast)

Step 9 Do the following:

a) On selecting **SSM**, configure the SSM list by adding an IP group range for each virtual network. You can add multiple IP group ranges for a virtual network.

1. Choose an IP group range from 225.0.0.0 to 239.255.255.255.
2. Enter the **Wildcard Mask** for the IP group.
3. Click **Next**.

b) On selecting **ASM**, choose the type of rendezvous point (RP):

- **Internal RP**
- **External RP**

Click **Next**.

Step 10 To configure a rendezvous point, do the following:

If you choose to configure an internal rendezvous point:

a) Select the devices that you need configured as internal rendezvous points. The second rendezvous point that you select will be the redundant rendezvous point. Click **Next**.
b) Assign internal rendezvous points to each of the listed virtual networks. Click **Next**.

If you choose to configure an external rendezvous point.:

a) In the **Setup your External RP** window, enter the IPv4 or IPv6 address of the external rendezvous point.

(Optional) You can enter a second set of IPv4 or IPv6 addresses.

Click **Next**.

b) In the **Select which RP IP Address(es) to utilize** window, select an IP address for each Virtual Network.

Click **Next**.

Step 11 Review the multicast settings displayed in the **Summary** window and modify, if required, before submitting the configuration.

Click **Finish** to complete the multicast configuration.

Intersite Layer 2 Handoff

The intersite Layer 2 handoff feature lets you extend an IP subnet across multiple sites in a fabric. The same IP subnet coexists across sites in a fabric.

Note the following restrictions:

- A device that is configured as fabric-in-a-box or as a border and an edge cannot be used for intersite Layer 2 handoff.
- Intersite Layer 2 handoff and SDA transit together are not supported.
- Wake on LAN feature is not supported on those segments where Intersite Layer 2 handoff is enabled.

Before you begin

- Ensure that all the devices are discovered and provisioned and that IP pools are reserved on the site from which the IP pools will be shared.
- Ensure that the sites that share an IP pool are underlay connected. Without this connection between the borders, DHCP might not work on the hosts that try to get IP addresses on the common subnet.
- Ensure that underlay multicast is configured, which is required for Layer 2 flooding to work. Underlay multicast gets configured during the LAN automation workflow.

Step 1 Associate Virtual Networks to the Fabric Domain. Ensure that you check the **Layer-2 Flooding** and **Common Pool** check boxes.

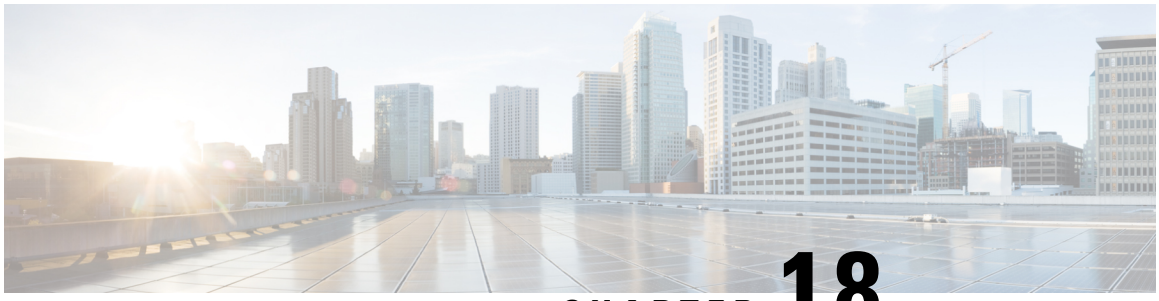
With **Layer-2 Flooding** and **Common Pool** enabled, the IP pool becomes eligible to be extended to other sites.

Step 2 Configure Layer 2 handoff on the border.

a) From the **Provision** > **Fabric** > **Fabric Infrastructure** tab, select the border device on which the intersite Layer 2 handoff is to be configured.
b) From the **L2 Handoff** section, select the virtual network to which the common IP pool is associated.
c) Configure the external interface of the border that connects it to other borders across sites.
d) Check the **Extend the subnet to other site** check box and assign an external VLAN number to the common IP pool.

Step 3 Repeat the preceding steps for the other sites that share the IP pool.

Ensure that you specify the same external VLAN number on all the interconnected borders.



CHAPTER 18

Provision Services

Applications

The following sections provide information about applications.

About Application Visibility

The Application Visibility service lets you manage your built-in and custom applications and application sets.

The Application Visibility service, hosted as an application stack within Cisco DNA Center, lets you enable the Controller-Based Application Recognition (CBAR) function on a specific device to classify thousands of network and home-grown applications and network traffic.

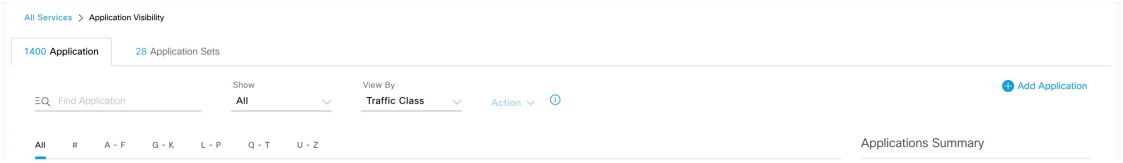
You install the following packages:

- **Application Policy**: Lets you automate QOS policies across LAN, WAN, and wireless within your campus and branch.
- **Application Registry**: Lets you view, manage, and create applications and application sets.
- **Application Visibility Service**: Provides application classification using Network-Based Application Recognition (NBAR) and CBAR techniques.

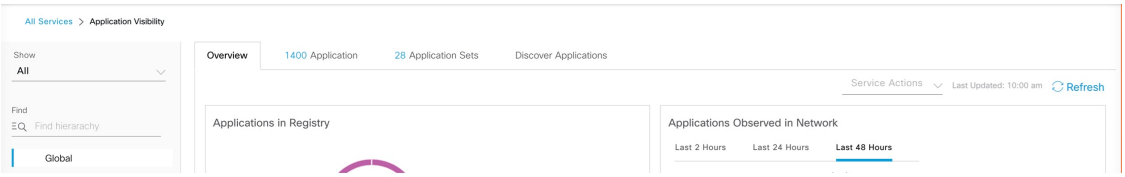
You can install the packages depending on your preferences.

Note To ensure compatibility, the preceding packages must have the same package version.

If you install Application Registry or both Application Registry and Application Policy, you can see the **Application** and **Application Sets** tabs when you click the **Menu** icon (☰) and choose **Provision** > **Services** > **Application Visibility**.



If you install Application Registry and Application Visibility Service or Application Registry, Application Policy, and Application Visibility Service, you can see the **Application**, **Application Sets**, and **Discover Applications** tabs when you click the **Menu** icon (☰) and choose **Provision** > **Services** > **Application Visibility**.



The Application Visibility service has the following phases:

- Day 0: First-time service enablement.
- Day N: Ongoing monitoring and configuration changes.

Day 0 Setup Wizard to Enable Application Visibility Service

Follow the Day 0 **Setup** wizard to enable the Application Visibility service in Cisco DNA Center.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Services** > **Application Visibility**.

You can view a brief introduction about the Application Visibility feature.

Step 2 In the Application Visibility page, click **Next**.

A pop-up window for enabling the Application Visibility service appears. Click **Yes** in the pop-up window to enable CBAR on Cisco DNA Center.

Step 3 (Optional) Check the **Enable CBAR on all Ready Devices** check box or choose devices with **CBAR Readiness Status** in **Ready** state.

If you want to choose a device that is not ready for enabling CBAR, follow the info message to move it to Ready state before proceeding in the **Setup** wizard.

Step 4 Click **Next** to enable CBAR on the devices.

Step 5 (Optional) Choose an external authoritative source, such as Microsoft Office 365 Cloud Connector, to either help classify the unclassified traffic or help generate improved signatures.

Step 6 Click **Finish**.

The **Overview** page provides a quick view of the application registry, device recognition method, device CBAR readiness, application observed in the network for the past 2, 24, or 48 hours (valid only if CBAR is enabled on at least one device), service health, and CBAR health score.

Day-N Application Visibility View

The Day-N Application Visibility page provides a quick view of application registry, device recognition method, device CBAR readiness, application observed in the network for the past 2, 24, or 48 hours (valid only in case CBAR was enabled on at least one device), and CBAR health.

The following table describes the charts that are available in the **Overview** tab in **Provision > Services > Application Visibility**.

Table 53: Day-N Application Visibility View: Charts

Chart	Description
Applications in Registry	This chart displays the number of applications available in the Cisco DNA Center application registry that can be used in Application Policy. The applications are classified as follows: • Custom: Applications added by a user • Built-in: Preinstalled applications in Cisco DNA Center • Discovered: Applications discovered by different recognition methods and imported into the application registry
Applications Observed in Network	This chart shows the applications observed in the past 2, 24, or 48 hours and lists the applications with highest network traffic ratio. **Note** The chart shows the applications observed only on CBAR-enabled devices.
Devices by Active Recognition Method	This chart displays the number of devices classified by each of the application recognition methods: • CBAR-enabled devices: Routers and switches • NBAR-based devices: Routers, switches, Cisco Wireless Controllers, and Cisco Catalyst 9800 Series Wireless Controller • IP/port-based devices: Switches • Not supported devices: Devices that are not supported by any of the preceding methods

Chart	Description
CBAR Readiness Status	This chart displays the device count in each CBAR readiness status. • Enabled: Devices that are CBAR-enabled • Ready: Devices that are ready for enabling CBAR • Not Ready: Devices that support CBAR but are not ready for enabling CBAR due to some issues • Not Supported: Devices that do not support CBAR
Service Health and CBAR Health	This widget displays the service health and the average health score for all CBAR-enabled devices. The device is healthy if there are no outstanding errors or warnings on that device. The CBAR health score is calculated across all CBAR-enabled devices. You can view the CBAR health of each CBAR-enabled device. A 0% CBAR health score indicates that the device has at least one error (P1). A 50% CBAR health score indicates that the device has no errors but has at least one warning (P2). A 100% CBAR health score indicates a healthy device. This widget also shows the service issues and remedies (P1, P2, and P3). The green tick mark indicates healthy service. The red cross mark indicates at least one P1 issue. The warning icon indicates at least one P2 issue. Click P1, P2, and P3 to view more about the services issues and remedies.
CBAR Health Issues and Remedies	All issues are classified by priority: • Errors (P1) • Warnings (P2) • Others (P3) Click the **P1**, **P2**, and **P3** tabs to view the device issues and remedy details.

Site Devices Table: This table provides device information and statuses. You can filter the devices using the **Quick Filter** and **Device Table Filter**.

Table 54: Day-N Application Visibility View: Site Devices Table

Column	Description
Device Name	Name of the device. Click the device name to view the CBAR Service Status.
Management IP	IP address of the device.
Device Type	Group of related devices, such as routers, switches and hubs, or wireless controllers.
Site	The site to which the device is assigned.
Fabric	The fabric domain to which the device is assigned.

Column	Description
Role	Role assigned to each discovered device during the scan process. The device role is used to identify and group devices according to their responsibilities and placement within the network. If Cisco DNA Center cannot determine a device role, it sets the device role to Unknown.
Active Recognition Method	Shows the device recognition method (CBAR, NBAR, IP/Port, or Not Supported).
OS Version	Cisco IOS software that is currently running on the device.
CBAR Readiness Status	Hover over the status displayed in the CBAR Readiness Status column to view the Remedy message.
Protocol Pack Version	Shows the current version of the protocol pack installed on the device and the protocol pack update status.
Device Registry Status	Shows the synchronization status of the device with the application registry. Hover over the info icon or the error icon to view more details about the synchronization status.
Deployment Status	Shows the CBAR deployment status.
Service Health Status	Click the issues in the Service Health Status column to open the CBAR Service status page, which displays a complete list of issues and the service status information of a device. If you click the Cisco Catalyst 9K device name, you can view the footprint (service load, CPU, and flows) of the CBAR service.
Application Policy	The application policy applied to the device. For Cisco Wireless Controllers with more than one application policy, the number of application policies applied and the name of all the applied application policies are displayed.
WAN Interfaces	Shows the number of WAN interfaces. Click the WAN interface details to view the WAN connectivity settings for the device.

Applications and Application Sets

Applications are the software programs or network signaling protocols that are used in your network. Cisco DNA Center supports all of the applications in the Cisco Next Generation Network-Based Application Recognition (NBAR2) library of approximately 1400 distinct applications.

Applications are grouped into logical groups called application sets. An application set can be assigned a business relevance within a policy.

Applications are mapped into industry standard-based traffic classes, as defined in RFC 4594, that have similar traffic treatment requirements. The traffic classes define the treatments (such as Differentiated Services Code Point [DSCP] marking, queuing, and dropping) that will be applied to the application traffic, based on the business relevance group that is assigned.

If you have additional applications that are not included in Cisco DNA Center, you can add them as custom applications and assign them to application sets.

Unidirectional and Bidirectional Application Traffic

Some applications are completely symmetrical and require identical bandwidth provisioning on both ends of the connection. Traffic for such applications is described as bidirectional. For example, if 100 kbps of Low-Latency Queueing (LLQ) is assigned to voice traffic in one direction, 100 kbps of LLQ must also be provisioned for voice traffic in the opposite direction. This scenario assumes that the same Voice over IP (VoIP) coder-decoders (codecs) are being used in both directions and do not account for multicast Music-on-Hold (MoH) provisioning. However, certain applications, such as streaming video and multicast MoH, are most often unidirectional. Therefore, it might be unnecessary, and even inefficient, to provision any bandwidth guarantees for such traffic on a branch router for the branch-to-campus direction of traffic flow.

Cisco DNA Center lets you specify whether an application is unidirectional or bidirectional for a particular policy.

On switches and wireless controllers, NBAR2 and custom applications are unidirectional by default. However, on routers, NBAR2 applications are bidirectional by default.

Custom Applications

Custom applications are applications that you add to Cisco DNA Center. An orange bar is displayed next to custom applications to distinguish them from the standard NBAR2 applications and application sets. For wired devices, you can define applications based on server name, IP address and port, or URL. You can define custom applications for Cisco Catalyst 9800 Series Wireless Controllers and not for Cisco AireOS controllers.

When you define an application according to its IP address and port, you can also define a DSCP value and port classification.

To simplify the configuration process, you can define an application based on another application that has similar traffic and service-level requirements. Cisco DNA Center copies the other application's traffic class settings to the application that you are defining.

Cisco DNA Center does not configure ACLs for port numbers 80, 443, 53, 5353, and 8080, even if they are defined as part of a custom application. If the custom application has a transport IP defined, Cisco DNA Center configures the application on the devices.

Note For a custom application to be programmed on devices when a policy is deployed, you must assign the custom application to one of the application sets defined in the policy.

Discovered Applications

Discovered applications are applications that are discovered by importing from recommended customization such as an Infoblox DNS server or by importing from the recommended unclassified applications flow.

The unclassified traffic can come from any flow that the CBAR-enabled device identifies but that is not recognized by the NBAR engine. In such cases, the applications that have a meaningful bit rate are reported as unclassified and can be imported and used as applications in Cisco DNA Center.

The Application Visibility service lets Cisco DNA Center connect with external authoritative sources like the Microsoft Office 365 Cloud Connector to help classify the unclassified traffic or help generate improved signatures.

Note You must configure an NBAR cloud connector before configuring the Microsoft Office 365 Cloud Connector.

The discovered applications are imported to the application registry.

Favorite Applications

Cisco DNA Center lets you flag applications that you want to configure on devices before all other applications. Flagging an application as a favorite helps to ensure that the QoS policies for your favorite applications get configured on devices. For more information, see Processing Order for Devices with Limited Resources, on page 299.

When custom applications are created they are marked as favorite applications.

Although there is no limit to the number of applications that you can mark as favorites, designating only a small number of favorite applications (for example, fewer than 25) helps to ensure that these applications are treated correctly from a business-relevance perspective in deployments with network devices that have limited ternary content addressable memory (TCAM).

Favorite applications can belong to any business-relevance group or traffic class and are configured system-wide, not on a per-policy basis. For example, if you flag the Cisco Jabber video application as a favorite, the application is flagged as a favorite in all policies.

Keep in mind that not only can business-relevant applications be flagged as favorites, even business-irrelevant applications can be flagged as such. For example, if administrators notice a lot of unwanted Netflix traffic on the network, they might chose to flag Netflix as a favorite application (despite it being assigned as business-irrelevant). In this case, Netflix is programmed into the device policies before other business-irrelevant applications, ensuring that the business intent of controlling this application is realized.

Configure Applications and Application Sets

The following subsections describe the various tasks that you can perform in the context of applications and application sets.

Note You can edit or delete only custom and discovered applications. You can edit or delete a maximum of 100 custom and discovered applications at one instance. If you choose NBAR applications for editing or deleting, a notification message indicates the number of applications that can be edited or deleted, excluding the number of chosen NBAR applications.

Change an Application's Settings

You can change the application set or traffic class of an existing NBAR, custom, or discovered application.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Provision** > **Services** > **Application Visibility** > **Application**.

Step 2 Use the **Search**, **Show**, or **View By** fields to locate the application that you want to change.

You can search applications based on their name, port number, and traffic class.

Step 3 Click the application name.

Step 4 In the dialog box, change one or both settings:

- **Traffic Class**: Choose a traffic class from the drop-down list. Valid traffic classes are BROADCAST_VIDEO, BULK_DATA, MULTIMEDIA_CONFERENCING, MULTIMEDIA_STREAMING, NETWORK_CONTROL, OPS_ADMIN_MGMT, REAL_TIME_INTERACTIVE, SIGNALING, TRANSACTIONAL_DATA, VOIP_TELEPHONY.
- **Application Set**: Choose an application set from the drop-down list. Valid application sets are authentication-services, backup-and-storage, collaboration-apps, consumer-browsing, consumer-file-sharing, consumer-gaming, consumer-media, consumer-misc, consumer-social-networking, database-apps, desktop-virtualization, email, enterprise-ipc, file-sharing, generic-browsing, generic-media, generic-misc, tunneling, local-services, naming-services, network-control, network-management, remote-access, saas-apps, signaling, software-development-tools, software-updates, streaming-media.

Step 5 Click **Save**.

Create a Server Name-Based Custom Application

If you have applications that are not in Cisco DNA Center, you can add them as custom applications.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Application** tab.

Step 3 Click **Add Application**.

Step 4 In the dialog box, provide the necessary information in the following fields:

Field	Description
Application name	Name of the custom application. The name can contain up to 24 alphanumeric characters, including underscores and hyphens. The underscore and hyphen are the only special characters allowed in the application name.
Type	Method by which users access the application. Choose **Server Name** for applications that are accessible through a server.
Server name	Name of the server that hosts the application.
Similar to	Application with similar traffic-handling requirements. Click the radio button to select this option, and then select an application from the drop-down list. Cisco DNA Center copies the other application's traffic class to the application that you are defining.
Traffic class	Traffic class to which the application belongs. Valid values are BULK_DATA, TRANSACTIONAL_DATA, OPS_ADMIN_MGMT, NETWORK_CONTROL, VOIP_TELEPHONY, MULTIMEDIA_CONFERENCING, MULTIMEDIA_STREAMING, BROADCAST_VIDEO, REAL_TIME_INTERACTIVE, and SIGNALING.

Field	Description
Application set	Application set is where you want the application to reside. Valid application sets are authentication-services, backup-and-storage, collaboration-apps, consumer-browsing, consumer-file-sharing, consumer-gaming, consumer-media, consumer-misc, consumer-social-networking, custom applications, database-apps, desktop-virtualization, email, enterprise-ipc, file-sharing, generic-browsing, generic-media, generic-misc, tunneling, local-services, naming-services, network-control, network-management, remote-access, saas-apps, signaling, software-development-tools, software-updates, streaming-media.

Step 5 Click **OK**.

Create an IP Address and Port-Based Custom Application

If you have applications that are not in Cisco DNA Center, you can add them as custom applications.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Application** tab.

Step 3 Click **Add Application**.

Step 4 In the **Application name** field, enter a name for the custom application. The name can contain up to 24 alphanumeric characters, including underscores and hyphens. The underscore and hyphen are the only special characters allowed in the application name.

Step 5 In the **Type** area, click the **Server IP/Port** radio button to indicate that the application is accessible through an IP address and port.

Step 6 Check the **DSCP** check box and define a DSCP value. If you do not define a value, the default value is Best Effort. Best-effort service is essentially the default behavior of the network device without any QoS.

Step 7 Check the **IP/Port Classifiers** check box to define the IP address and subnet, protocol, and port or port range for an application. Valid protocols are IP, TCP, UDP, and TCP/UDP. If you select the IP protocol, you do not define a port number or range. Click ✚ to add more classifiers.

Step 8 Define your application traffic-handling requirements using one of the following methods:

- **Similar To**: If your application has similar traffic-handling requirements as an existing application, click the **Similar To** radio-button and choose the application from the drop-down list. Cisco DNA Center copies the traffic class of the other application to the application that you are defining.
- **Traffic Class**: If you know the traffic class that you want to define for your application, click the **Traffic Class** radio button and choose the traffic class from the drop-down list. Valid values are BULK_DATA, TRANSACTIONAL_DATA, OPS_ADMIN_MGMT, NETWORK_CONTROL, VOIP_TELEPHONY, MULTIMEDIA_CONFERENCING, MULTIMEDIA_STREAMING, BROADCAST_VIDEO, REAL_TIME_INTERACTIVE, and SIGNALING.

Step 9 From the **Application Set** drop-down list, choose the application set to which the application will belong. Valid application sets are authentication-services, backup-and-storage, collaboration-apps, consumer-browsing, consumer-file-sharing, consumer-gaming, consumer-media, consumer-misc, consumer-social-networking, custom applications, database-apps, desktop-virtualization, email, enterprise-ipc, file-sharing, generic-browsing, generic-media, generic-misc, tunneling, local-services, naming-services, network-control, network-management, remote-access, saas-apps, signaling, software-development-tools, software-updates, streaming-media.

Step 10 Click **OK**.

Create a URL-Based Custom Application

If you have applications that are not in Cisco DNA Center, you can add them as custom applications.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Application** tab.

Step 3 Click **Add Application**.

The **Add Application** dialog box appears.

Step 4 In the **Application name** field, enter the name of the custom application. The name can contain up to 24 alphanumeric characters, including underscores and hyphens. (Underscores and hyphens are the only special characters allowed in the application name.)

Step 5 For **Type**, click the **URL** radio button.

Step 6 In the **URL** field, enter the URL used to reach the application.

Step 7 Configure the traffic class:

- To use the same traffic class as another application with similar traffic-handling requirements, click the **Similar To** radio button and choose an application from the drop-down list.
- To specify the traffic class, click the **Traffic Class** radio button and choose a traffic class from the drop-down list. Valid values are BULK_DATA, TRANSACTIONAL_DATA, OPS_ADMIN_MGMT, NETWORK_CONTROL, VOIP_TELEPHONY, MULTIMEDIA_CONFERENCING, MULTIMEDIA_STREAMING, BROADCAST_VIDEO, REAL_TIME_INTERACTIVE, and SIGNALING.

Step 8 From the **Application Set** drop-down list, choose an application set in which you want the application to reside.

Step 9 Click **OK**.

Edit or Delete a Custom Application

If required, you can change or delete a custom application.

Note You cannot delete a custom application that is directly referenced by an application policy. Application policies typically reference application sets and not individual applications. However, if a policy has special definitions for an application (such as a consumer or producer assignment or bidirectional bandwidth provisioning), the policy has a direct reference to the application. As such, you must remove the special definitions or remove the reference to the application entirely before you can delete the application.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Application** tab.

Step 3 Use the **Search**, **Show**, or **View By** fields to locate the application that you want to change.

You can search applications based on their name, port number, and traffic class.

Step 4 To edit the application:

a) Click the application name and make the required changes. For information about the fields, see Create a Server Name-Based Custom Application, on page 462, Create an IP Address and Port-Based Custom Application, on page 463, or Create a URL-Based Custom Application, on page 464.

b) Click **OK**.

Note When policy is redeployed, the edited custom applications are not reconfigured on Cisco Catalyst 9800 Series Wireless Controller.

Step 5 To delete the application, click in the application box, and then click **OK** to confirm.

Mark an Application as Favorite

You can mark an application as a favorite to designate that the application's QoS configuration must be deployed to devices before other applications' QoS configuration. An application marked as favorite has a yellow star next to it.

When you add or edit a policy, applications marked as a favorites are listed at the top of the application set.

Applications are configured system-wide, not on a per-policy basis. For more information, see Favorite Applications, on page 461.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Application** tab.

Step 3 Locate the application that you want to mark as a favorite.

Step 4 Click the star icon.

Create a Custom Application Set

If none of the application sets fits your needs, you can create a custom application set.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Application Sets** tab.

Step 3 Click **Add Application Set**.

Step 4 In the dialog box, enter a name for the new application set.

Cisco DNA Center creates the new application set; however, it contains no applications.

Step 5 Click **OK**.

Step 6 Use the **Search**, **Show**, or **View By** fields to locate the application set.

You can search applications based on their name, port number, and traffic class.

Step 7 Locate the applications that you want to move into the new application set.

Step 8 Check the check box next to the applications that you want to move.

Step 9 Drag and drop the applications into the new application set.

Edit or Delete a Custom Application Set

If required, you can change or delete a custom application set.

Note You cannot delete a custom application set that is referenced by an application policy. You must remove the application set from the policy before you delete the application set.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Application Sets** tab.

Step 3 Use the **Search**, **Show**, or **View By** fields to locate the application set that you want to change.

You can search applications based on their name, port number, and traffic class.

Step 4 Do one of the following:

- To edit the application set, drag and drop applications into or out of the application set. Click **OK** to confirm each change.
- To delete the application set, click 🗑 in the application set box, and then click **OK** to confirm.

Update the Protocol Pack on a CBAR-Enabled Device

You can upgrade the protocol pack on any device that supports CBAR to the latest or any specific protocol pack.

Before you begin

- Configure Cisco credentials on **System Settings**. For more information about configuring Cisco credentials, see the Cisco DNA Center Administrator Guide.
- Devices must support CBAR.
- CBAR must be enabled on the device.
- Protocol packs for the device must be available on cisco.com.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Provision** > **Services** > **Application Visibility**.

Step 2 In the Day-N **Overview** page, scroll down to view the **Site Devices** table.

Step 3 Check the status shown in the **Protocol Pack Version** column in the **Site Devices** table.

You can click the **Outdated** status to view the list of applicable protocols packs in the **Update Protocol Pack** window.

Step 4 Click **Update** corresponding to the required protocol pack version in the **Update Protocol Pack** window.

The **Protocol Pack Version** column shows **In progress** status. Click the info icon to view the current updating version. If the **Protocol Pack Version** column shows **Update failed** status, click the error icon to view the failure reason.

Step 5 If you want to update all the devices or selected devices to the latest protocol pack, do the following:

To update the protocol pack on all applicable CBAR-enabled devices:

- From the **Update Protocol Pack** drop-down list, choose **All Devices** and click **Yes** in the subsequent warning pop-up windows.

To update the protocol pack on the selected devices:

- Choose the devices in the **Site Devices** table.
- From the **Update Protocol Pack** drop-down list, choose **Selected Devices** and click **Yes** in the subsequent warning pop-up windows.

Discover Unclassified Applications

The Application Visibility service in Cisco DNA Center obtains information on classified and unclassified domains and sockets from devices and displays that information in the **Observed Traffic** chart. The number of unclassified server names and IP/ports that are discovered by the Application Visibility service is shown under **Recommendations**.

You can add the unclassified server names and IP/ports to the Application Registry.

Note You can add a maximum of 1100 discovered applications in the Application Registry.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Discover Applications** tab.

Step 3 Under **Recommendations**, click the **discovered server names** link or the **discovered IP/Ports** link.

The table lists the discovered servers or IP/ports that are not classified. Choose the server and check the **Hide Ignored Applications** check box if you want to hide the selected server or IP/ports in the table.

Step 4 Choose the server or IP/ports that you want to import as an application in the Application Registry.

Step 5 Choose the required **Application**, **Application Set**, and **Traffic Class** from the drop-down list.

Step 6 Click **Import**.

Step 7 Click the **Applications** tab and choose **Show** > **Discovered** to view the imported application.

Configure the NBAR Cloud Connector

The Application Visibility service uses the NBAR cloud connector to enrich the protocol pack and enhance visibility for unknown applications by sending and receiving data from the cloud.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Discover Applications** tab.

Step 3 In the **NBAR Cloud** window, click **Configure**.

Step 4 In the **Configure NBAR Cloud** window, click the toggle button to **Enable**.

Step 5 Click the **Cisco API Console** link to retrieve the key and client secret.

Step 6 Enter your Cisco credentials to open the **Cisco API Console** in a new browser tab and do the following:

a) In the **My Apps & Keys** tab, click **Register a New App**.

b) Complete the following fields in the **Register an Application** screen.

- **Name of Your Application**: Enter the application name.
- **OAuth2.0 Credentials**: Click the **Client Credentials** check box.
- **Select APIs**: Click the **Hello API** check box.

c) Click **Register**.

The registered application details appear in the **My Apps & Keys** tab.

d) Copy the key and client secret of the registered application from the **Cisco API Console**.

Step 7 Enter the copied key and client secret in the **Configure NBAR Cloud** window.

Step 8 Complete the following fields in the **Configure NBAR Cloud** window:

a) Enter the organization name.

b) Check the **Improve my network using NBAR Cloud telemetry** check box.

c) Choose the desired location in the **NBAR classification telemetry data is being sent to region** check box.

Step 9 Click **Save**.

Application Visibility Service Support for the Cisco DNA Traffic Telemetry Appliance

The Cisco DNA Traffic Telemetry Appliance generates endpoint telemetry from mirrored IP network traffic and shares the telemetry data with Cisco DNA Center for endpoint visibility and segmentation.

Prerequisites for enabling CBAR on the Cisco DNA Traffic Telemetry Appliance:

- The device must be assigned to a site.
- The device role must be set to **Distribution** mode.

Note Application policy support is not available for the Cisco DNA Traffic Telemetry Appliance.

Discover Infoblox Applications

You can integrate Cisco DNA Center with an organizational Infoblox DNS server to resolve unclassified traffic based on server names.

Before you begin

- The Infoblox WAPI version must be 1.5 or later. To check the Infoblox WAPI version, log in to the Infoblox server and choose **Help** > **Documentation** > **WAPI Documentation**.
- Create a role with at least Read Only permissions and assign the role to the Infoblox user. For more information, see Manage Users in the Cisco DNA Center Administrator Guide.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Discover Applications** tab.

Step 3 Under **Infoblox DNS Server**, click **Configure**.

Step 4 In the **Infoblox Connector Settings** window, click the **Here** link to configure IPAM/DNS server credentials in Cisco DNA Center.

Step 5 Complete the IPAM settings. For more information, see Configure an IP Address Manager in the Cisco DNA Center Administrator Guide.

Step 6 Go back to **Infoblox Connector Settings** and complete the following settings:

- Check the **All DNS Zones** check box, or choose the required DNS zones from the **DNS Zones to Inspect** drop-down list. The drop-down list shows the DNS zones defined in the Infoblox server.
- From the **Inspect** drop-down list, choose the required inspection record.
- Check the **Read Application name from** check box and click the **Extensible Attribute** or **AVC RRTYPE format** radio button. If you click the **Extensible Attribute** radio button, enter the extensible attribute name that contains descriptive application names.
- From **Default Traffic Class**, choose the default traffic class for classifying the Infoblox applications.
- From **Default Application Set**, choose the default application set for classifying the Infoblox applications.

Step 7 Click **Save**.

The **Poll Infoblox to Import Applications** link appears under **Recommendations**.

Step 8 Click the **Poll Infoblox to Import Applications** link to get a list of applications from the DNS zones configured in the **Infoblox Connector Settings**.

Step 9 Choose the application that you want to import and complete the following:

- If the application does not have a name defined in the Infoblox server, edit the application name.
- Choose the required application set and traffic class from the drop-down list if you want to change the default application set and traffic class defined in the **Infoblox Connector Settings**.

Step 10 Click **Import**.

Step 11 Click the **Applications** tab and choose **Discovered** in the **Show** drop-down list to view or edit the imported Infoblox applications.

If you change the server name of an application after importing the application, the **Application Status** column in the **Infoblox Discovered Applications** window shows the status of the application as **Updated**. The application name that you see in the **Application Status** column is the new server name of the application. Click the info icon to view the old server names of the application.

Resolve Unclassified Traffic Using Microsoft Office 365 Cloud Connector

Cisco DNA Center can connect to external authoritative sources like Microsoft Office 365 Cloud Connector that can help classify the unclassified traffic or help generate improved signatures.

Before you begin

- Ensure that Cisco DNA Center has connectivity to the internet.
- Ensure that the NBAR cloud is enabled.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Discover Applications** tab.

Step 3 Click the **MS Office 365 Cloud** toggle button to enable polling of MSFT signatures.

- When you enable Microsoft Office 365 Connector, the controller starts importing the new domains' information from Microsoft Office 365 and finds the correct application for the new domains.
- The new secondary pack is installed along with the Cisco DNA Center-based protocol pack and new domains are supported automatically.

Edit or Delete a Discovered Application

If required, you can edit or delete a discovered application.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Application** tab.

Step 3 Use the **Search**, **Show**, or **View By** fields to locate the discovered application that you want to change.

You can search for applications based on their name, port number, and traffic class.

Step 4 To edit the application:

a) Click the application name and make the required changes.

For discovered applications, you can edit only the **Attribute Set** and **Traffic Class**.

b) Click **OK**.

Step 5 To delete the application, click 🗑 in the application box, and then click **OK**.

Application Hosting

The following sections provide information about application hosting.

About Application Hosting

Application hosting lets you manage the lifecycle of third-party applications on devices managed by Cisco DNA Center. You can host third-party docker applications on Cisco Catalyst 9300 Series switches running Cisco IOS-XE software version 16.12.1s or later and Cisco Catalyst 9100 Series Access Points running Cisco IOS-XE software version 17.3.1 or later.

To limit the amount of disk space used by application hosting, Cisco DNA Center supports a maximum of eight applications.

Install or Update the Application Hosting Service Package

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Software Updates**. Alternatively, click the cloud icon and click the **Go to Software Updates** link.

Step 2 In the Software Updates window, review the following tabs:

- **Updates**: Shows the system and application updates. System Update shows the system version that is installed and the system updates that are available and have been downloaded from the Cisco cloud. Application Updates shows the available applications that can be downloaded and installed from the Cisco cloud, the size of the application, and the appropriate action (**Download**, **Install**, or **Update**). Hover your cursor over the package to view the available version and a basic description.
- **Installed Apps**: Shows the application packages that are currently installed.

Step 3 To download the Application Hosting package, click **Install** next to the Application Hosting name under **Updates** > **Application Updates**.

Step 4 To update the Application Hosting package, click **Update** next to the Application Hosting name under **Updates** > **Application Updates**.

Step 5 Ensure that the application has been updated by reviewing the version on the **Installed Apps** tab.

Note After installing the Application Hosting service package, you must log out of Cisco DNA Center, clear your browser cache, and log in to Cisco DNA Center again.

Prerequisites for Application Hosting

To enable application hosting on a Cisco Catalyst 9000 device, the following prerequisites must be fulfilled:

- Configure a secure HTTP server on the switch where the applications will be hosted.
- Configure local or AAA authentication server for HTTPS user authentication on the switch. You must configure the username and password with privilege level 15.
- Ensure Cisco Catalyst 9300 Series switches are running Cisco IOS XE 16.12.x or later version and Cisco Catalyst 9400 Series switches are running Cisco IOS XE 17.1.x or later version.
- Ensure that the device has an external USB SSD pluggable storage (only for the switches of 9300 family).
- Verify that the configuration on the switch is correct. Open the WebUI on the switch log in as the HTTPS user.

  The following example shows a working configuration on a switch:

```
prompt# sh run | sec http
ip http server
ip http authentication local
ip http secure-server
ip http max-connections 16
ip http client source-interface Loopback0
```

  Additional configuration for switches with a Cisco IOS XE release that is earlier than 17.3.3:

```
ip http secure-active-session-modules dnac
ip http session-module-list dnac NG_WEBUI
ip http active-session-modules none
```

  Additional configuration for switches with Cisco IOS XE release 17.3.3 or later:

```
ip http secure-active-session-modules webui
ip http session-module-list webui NG_WEBUI
ip http session-module-list pki OPENRESTY_PKI
ip http active-session-modules pki
```

- On Cisco DNA Center, configure the HTTPS credentials while manually adding the device. The HTTPS username, password, and port number are mandatory for application hosting. The default port number is 443. You can also edit the device credentials; see Update Network Device Credentials, on page 60. If you edit a device that is already managed, resynchronize that device in the inventory before it is used for application hosting-related actions.

Note Application hosting HA is not supported on three-node Cisco DNA Center clusters.

View Device Readiness to Host an Application

You must check the readiness of the Cisco Catalyst 9300 Series switch to host the application before you can install an application on the switch.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Provision** > **Services** > **App Hosting for Switches**.

Step 2 Click **All Devices**.

Step 3 View the list of devices that are capable of hosting applications. The **App Hosting Status** indicates the readiness of the device to host an application. If the status shows **Not Ready**, click the status to view the reason.

Add an Application

You can add a Cisco package or a docker application.

Before you begin

- **Cisco Package**: You must package the application using IOS SDK tools so that the application is compatible with IOS XE operating systems.
- **Docker**: You must save the docker image as a tar file. Enter the following command to store the docker image as a tar file:

```
docker save -o <path for generated tar file> <image name:tag>
Example: docker save -o alpine-tcpdump.tar itsthenetwork/alpine-tcpdump:latest
```

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Provision** > **Services** > **App Hosting for Switches**.

Step 2 Click **New Application**.

Step 3 Choose the application and category from the drop-down list.

Step 4 Click **Select** and choose the application to upload.

Step 5 Click **Upload**.

You can view the newly added application in the **App Hosting** page.

Automatic Download of ThousandEyes Enterprise Agent Application

The ThousandEyes Enterprise Agent application lets you monitor your network and oversee the network traffic paths across internal, external, carrier, and internet networks in real time. The advantage of the ThousandEyes Enterprise Agent application is that you do not have to import this application manually in your Cisco DNA Center Application Hosting Service. Within 10 minutes of starting the Application Hosting service, the ThousandEyes Enterprise Agent application is downloaded automatically. To manually download the application, click the following link to the ThousandEyes Enterprise Agent .tar file:

thousandeyes-enterprise-agent-4.1.0.cisco.tar

If there is no internet connection, you can set a proxy connection from the console using the following command:

```
magctl service setenv app-hosting http_proxy <proxy-value>
```

Set the proxy value to connect to the ThousandEyes Enterprise Agent application.

Update an Application

You can update the application added in Cisco DNA Center.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Provision** > **Services** > **App Hosting for Switches**.

You can view the available applications in the **App Hosting** page.

Step 2 Choose the application that you want to update.

Step 3 Click **Update Application**.

Step 4 Choose the application **Type** and **Category** from the drop-down list.

Step 5 Click **Select** and choose a new version of the application to be uploaded.

Step 6 Click **Upload**.

Start an Application

You can start an application in Cisco DNA Center.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Services** > **App Hosting for Switches**.

Step 2 Choose the application and click **Manage** to view the devices that use the application.

Step 3 Choose the device that has the application that you want to start.

Step 4 From the **Actions** drop-down list, choose **Start App**.

Stop an Application

You can stop an application in Cisco DNA Center.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Services** > **App Hosting for Switches**.

Step 2 Choose the application and click **Manage** to view the devices that use the application.

Step 3 Choose the device that has the application that you want to stop.

Step 4 From the **Actions** drop-down list, choose **Stop App**.

View Installed Hosting Applications on Cisco Catalyst 9300 Device

Before you begin

Complete the prerequisites. For more information, see Prerequisites for Application Hosting.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Services** > **App Hosting for Switches**.

Step 2 To view all devices, click **All Devices** at the top-right corner, or to view only the devices that use a particular application, choose the application and click **Manage**.

Note

- If you chose to view all devices, the **All Devices** page shows the following information about the devices that are capable of hosting applications: **Hostname**, **IP Address**, **App Hosting Status**, and **Last Updated**.
- If you chose to view a list of devices for a particular application, the **Devices** page shows the following information about the devices that are capable of hosting applications: **Hostname**, **Device IP**, **App Version**, **App Status**, **Last Heard, Platform Version**, and **Action Status**.

Step 3 In the **Devices** page, click **Summary** to view a summary of failed, stopped, and running applications on a device.

Step 4 To take an action on an application, click the **Action** drop-down list and choose **Start**, **Stop**, **Edit**, **Upgrade**, or **Uninstall**.

Step 5 Click the device link in which you want to view the installed hosting applications.

The **Applications** page shows the **Name**, **Version**, **App Status**, **IP Address**, **Health**, and **Details** of the installed applications.

Step 6 In the **Details** column, click **View** to get more information about an application status on the device.

App details window shows the **REOURCES** and **NETWORK** information of an application.

Step 7 To download the log for a particular application, select the application and click **Application Logs**.

Step 8 To download the tech support log for a particular application, select the application and click **Tech Support Logs**.

Install an Application on a Cisco Catalyst 9300 Device

Cisco DNA Center allows you to install an application on a Cisco Catalyst 9300 Series switch.

Before you begin

- Complete the prerequisites. For more information, see Prerequisites for Application Hosting, on page 471.
- Add the application to Cisco DNA Center. For more information, see Add an Application, on page 473.
- Check the readiness of the switch to host the application. For more information, see View Device Readiness to Host an Application, on page 472.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Services** > **App Hosting**.

Step 2 Choose the application and click **Install**.

Step 3 Choose the devices on which you want to install the application and click **Next**.

Step 4 Complete the following settings in the **Configuration App** tab:

- **App Networking**
  - **Device Network**: Click the **Select Network** drop-down list and choose a VLAN to configure the application.
  - **App IP address**: Choose **Static** or **Dynamic** from the **Address Type** drop-down list. If you choose **Static**, click the thumbnail icon and enter the **IP Address**, **Gateway**, **Prefix/Mask**, and **DNS** for the application.

- **Resource Allocation**: Check the **Allocate all resources available on a device** or **Customize resource allocation** check box. You can check the **Customize resource allocation** check box and modify the maximum **CPU**, **Memory**, and **Persistent Storage** values to a lower value.
- (Optional) **Custom Settings**: Applicable only for Cisco package applications. Enter the configuration details for the attributes that are specified by the application.
- (Optional) **App Data**: Browse and upload the application-specific files. To identify the required application-specific files, see the relevant application document.
- **Docker Runtime Options**: Enter the docker runtime options required by the application.

Step 5 Click **Next** and review the application configuration settings in the **Confirm** screen.

Step 6 Click **Finish**.

Step 7 In the confirmation window, click **Yes** to complete the application installation on the selected Cisco Catalyst 9300 devices.

What to do next

The installation of the application also modifies the Cisco IOS-XE configuration on the device. This change in the running configuration must be copied to the startup configuration to ensure applications function as expected after a router reload. After the application installation is complete, use the **Template Editor** to copy the running configuration to the startup configuration.

Uninstall an Application from a Cisco Catalyst 9300 Device

You can uninstall an application from a Cisco Catalyst 9300 Series switch.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Services** > **App Hosting for Switches**.

Step 2 Choose the application and click **Manage** to view the devices that use the application.

Step 3 Choose the devices that have the application that you want to uninstall.

Step 4 From the **Actions** drop-down list, choose **Uninstall App**.

Edit an Application Configuration in a Cisco Catalyst 9300 Device

You can edit an application configuration if the application requires a configuration to be up and running in a Cisco Catalyst 9300 Series switch.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Services** > **App Hosting for Switches**.

Step 2 Choose the application and click **Manage** to view the devices that use the application.

Step 3 Choose the device that has the application that you want to edit.

Step 4 From the **Actions** drop-down list, choose **Edit App Config**.

Delete an Application

You can delete an application from Cisco DNA Center.

Before you begin

You must uninstall the application from all devices that are using it. For more information, see Uninstall an Application from a Cisco Catalyst 9300 Device, on page 476.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Services** > **App Hosting for Switches**.

You can view the available hosted applications in the **App Hosting** page.

Step 2 Choose the application that you want to delete.

Step 3 Click **Delete Application**.

Step 4 In the confirmation dialog box, click **OK**.

The application is deleted only if it is not used by any of the devices managed by Cisco DNA Center.

Otherwise, an error message shows the number of devices that are using the application. Click **Cancel** in the confirmation dialog box and uninstall the application. For more information, see Uninstall an Application from a Cisco Catalyst 9300 Device, on page 476.

Download App Logs

You can download application logs from Cisco DNA Center.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Services** > **IoT Services**.

Step 2 Click **All Devices**.

You can view the list of devices that are capable of hosting applications.

Step 3 Click **App logs** to download the application logs from Cisco DNA Center.

Step 4 In the **App Logs** pop-up window, choose the application logs file that you want to download and click **Download**.

Download Device Tech Support Logs

You can download the device tech support logs from Cisco DNA Center for troubleshooting purposes.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Services** > **IoT Services**.

Step 2 Click **All Devices**.

A list of devices that are capable of hosting applications is displayed.

Step 3 Click **Tech Support logs** to download the device tech support logs.

Application Hosting on Cisco Catalyst 9100 Series Access Points

The following sections provide information about application hosting on Cisco Catalyst 9100 Series Access Points.

About Application Hosting on Cisco Catalyst Access Points

The move to virtual environments has prompted the need to build applications that are reusable, portable, and scalable. Application hosting gives administrators a platform for leveraging their own tools and utilities. An application, hosted on a network device, can serve a variety of purposes. This ranges from automation, configuration management monitoring, and integration with existing tool chains.

Application hosting lets you manage the lifecycle of third-party applications on devices managed by Cisco DNA Center. This release lets you bring in the third-party SES-imagotag IoT Connector application on Cisco Catalyst 9100 Series Access Points with Cisco IOS-XE software version 17.3 or later.

The SES-imagotag IoT Connector on Cisco Catalyst 9100 Series Access Points can handle all Electronic Shelf Label (ESL) communication.

Application Hosting Workflow to Install and Manage USB on Cisco Catalyst 9100 Series Access Points

Before you begin

To enable application hosting on a device, the following prerequisites must be completed:

- You must enable NETCONF and set the port to 830 to discover Cisco Catalyst 9100 Series Access Points.
- Cisco Catalyst 9100 Series Access Points must have direct IP reachability to Cisco DNA Center.
- Make sure that the Cisco Catalyst 9800 Series Wireless Controller is running Cisco IOS XE 17.3.x or later software.
- Make sure that the Cisco DNA Center appliance is running the latest Cisco DNA Center ISO.
- Make sure that the USB dongle is inserted in the AP. This is required for the SES-imagotag Connector application to run.

Step 1 Check the readiness of the Cisco Catalyst 9800 Series Wireless Controller and Cisco Catalyst 9100 Series Access Points to host the application before you install it.

For more information, see View Device Readiness to Host an Application, on page 472.

Step 2 Install the Application Hosting service on Cisco DNA Center.

For more information, see Install or Update the Application Hosting Service Package, on page 471.

Step 3 Add the Cisco Catalyst 9800 Series Wireless Controller to Cisco DNA Center.

For more information, see Add a Network Device, on page 56.

Note Make sure that you enable NETCONF and set the port to 830.

You must wait for the Cisco Catalyst 9800 Series Wireless Controller to move to a Managed state.

Step 4 Assign APs to a floor on the Network Hierarchy window.

For more information, see Add, Position, and Delete APs, on page 119.

Step 5 Upload the USB application (the SES-imagotag Connector) to Cisco DNA Center.

For more information, see Add an Application, on page 473.

Step 6 Enable the IoT services.

For more information, see Enable IoT Services on Cisco Catalyst 9100 Series Access Points, on page 504.

Step 7 Configure the container as described in the Application Hosting on Catalyst APs Deployment Guide.

View Installed Hosting Applications on Cisco Catalyst 9100 Series Access Points

Before you begin

Complete the prerequisites. For more information, see Prerequisites for Application Hosting.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Services** > **IoT Services**.

Step 2 To view all devices, click **All Devices** at the top-right corner, or to view only the devices that use a particular application, choose the application and click **Manage**.

Note
- If you chose to view all devices, the **All Devices** page shows the following information about the devices that are capable of hosting applications: **Hostname**, **IP Address**, **App Hosting Status**, and **Last Updated**.
- If you chose to view a list of devices for a particular application, the **Devices** page shows the following information about the devices that are capable of hosting applications: **Hostname**, **Device IP**, **App Version**, **App Status**, **Last Heard, Platform Version**, and **Action Status**.

Step 3 In the **Devices** page, click **Summary** to view the summary of failed, stopped, and running applications on a device.

Step 4 Click the **Action** drop-down list to start, stop, edit, upgrade, and uninstall an application.

Step 5 Click the device link in which you want to view the installed hosting applications.

The **Applications** page shows the **Name**, **Version**, **App Status**, **IP Address**, **Health**, and **Details** of the installed applications.

Step 6 In the **Details** column, click **View** to get more information about an application status on the device.

App details window shows the **REOURCES** and **NETWORK** information of an application.

Step 7 To download the application log, select an application for which you want to download the application log and click **Application Logs**.

Step 8 To download the tech support log, select an application for which you want to download the tech support log and click **Tech Support Logs**.

Uninstall an Application from a Cisco Catalyst 9100 Device

You can uninstall an application from a Cisco Catalyst 9100 Series AP.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Services** > **IoT Services**.

Step 2 Choose the application and click **Manage** to view the devices that use it.

Step 3 Choose the devices that have the application that you want to uninstall.

Step 4 From the **Actions** drop-down list, choose **Uninstall App**.

Delete an Application from a Cisco Catalyst 9100 Device

You can delete an application from a Cisco Catalyst 9100 Series AP.

Before you begin

You must uninstall the application from all devices that are using it. For more information, see Uninstall an Application from a Cisco Catalyst 9100 Device.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Services** > **IoT Services**.

You can view the available hosted applications in the **IoT Services** page.

Step 2 Choose the application that you want to delete.

Step 3 Click **Delete Application**.

Step 4 In the confirmation dialog box, click **OK**.

The application is deleted only if it is not used by any of the devices managed by Cisco DNA Center.

Otherwise, an error message shows the number of devices using the application. Click **Cancel** and uninstall the application. For more information, see Uninstall an Application from a Cisco Catalyst 9100 Device.

Configure a Site-to-Site VPN

You can create a site-to-site VPN and edit or delete existing site-to-site VPNs.

Create a Site-to-Site VPN

This procedure shows how to create a site-to-site VPN from the **Provision** > **All Services** window. Alternatively, you can create a site-to-site VPN from the **Workflows** > **Site to Site VPN** window.

Before you begin

- Define the sites within the network hierarchy. See About Network Hierarchy, on page 110.
- Configure IP address pools to be used for the VPN tunnels. The IP address pools must have a minimum of six free IP addresses. See Configure IP Address Pools, on page 184.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Site to Site VPN**.

Step 2 To create a VPN, click **Add**.
The **Choose Your Sites** workflow is displayed.

Step 3 Enter a VPN name in the first field.

Step 4 Select the first site, a device in that site, and a WAN interface on that device from the Site 1 drop-down lists. The WAN interface is set by default if the device is provisioned.

Step 5 Select the second site, a device in that site, and a WAN interface on that device from the Site 2 drop-down lists. The WAN interface is set by default if the device is provisioned.

Step 6 Click **Next** to go to the **Select Networks** screen.

Step 7 From the **Tunnel IP Pool** drop-down list, choose an IP address pool.

Step 8 Check the boxes next to the subnets that you want to use for each site.

Step 9 (Optional) If you want to add a custom network for a site, click the **Add Custom Networks** link at the bottom and complete the required fields.

Step 10 Click **Next** to go to the **Configure VPN** screen.

Step 11 Enter a preshared key for encryption.

Step 12 Set the encryption and integrity algorithms as desired. We recommend that you use the default settings. If you change any settings, you can go back to the default choices by checking the **Use Cisco recommended IKEV2 & Transform Set Values** check box.

Step 13 Click **Next** to go to the **Summary** screen.

Step 14 Review the VPN settings and click **Edit** in any section if you want to make a change.

Step 15 Click **Create VPN**.

In the status screen that follows, a check mark is shown next to each step as it is completed. Click **Services** to return to the **Site to Site VPN** screen, which shows the newly created VPN.

Edit a Site-to-Site VPN

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Site to Site VPN**.

Step 2 Check the check box next to the VPN that you want to edit.

Step 3 Click **Edit** in the menu bar above the list.

The **Summary** screen appears.

Step 4 Review the VPN settings and click **Edit** in any section if you want to make a change.

Step 5 Click **Edit VPN** to submit the changes.

In the status screen that follows, a check mark is shown next to each step as it is completed. Click **Services** to return to the **Site to Site VPN** screen.

Delete a Site-to-Site VPN

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Site to Site VPN**.

Step 2 Check the check box next to the VPN that you want to delete.

Step 3 Click **Delete** in the menu bar above the list.

A confirmation dialog box is displayed.

Step 4 Click **Yes** to confirm that you want to delete the VPN.

Create a User-Defined Network Service

The following sections provide information about configuring and viewing the Cisco User-Defined Network Service site provisioning status from the **Provision** > **Services** window in Cisco DNA Center.

Create the User-Defined Network Service

This procedure shows how to configure the Cisco User-Defined Network service from **Provision** > **Services** > **Cisco User Defined Network**. Alternatively, you can create a User-Defined Network service from **Workflows** > **Configure Cisco User Defined Network**.

Before you begin

- Define sites within the network hierarchy.
- Use the Cisco DNA Center Cloud application to generate an authentication token.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Services** > **Cisco User Defined Network**.

Step 2 Click **Add Sites**.

The **OK, now let's complete the connection with the cloud service** workflow appears.

Step 3 In the **Authentication Token** text box, paste the authentication token that you generated and copied in **Cisco DNA Center Cloud**, and click **Connect**.

If the token validates successfully, the message `Connection validated, click Next to proceed` appears.

If the token validation fails, click **Retry**, re-enter the authentication token, and click **Connect**.

Step 4 Click **Next** to select the sites where you want to enable the Cisco User-Defined Network service.

Step 5 From the **Select Sites** drop-down list, choose the sites.

Step 6 Check the **Disable User Defined Network Service** check box to disable the User-Defined Network service for all sites.

Step 7 Click **Next** to select the SSIDs for the sites you selected.

The provisioned nonfabric SSIDs are displayed for all the sites selected in the previous step.

Step 8 From the **SSID(s)** drop-down list, choose the SSIDs.

Step 9 To limit the unicast traffic for the selected SSID, turn the **Unicast Traffic Containment** button on.

Step 10 Do one of the following, and then click **Next**:

- Click **Apply Individually** to apply the unicast traffic containment for a specific site.
- Click **Apply to all** to apply to the unicast traffic containment for all sites.

Step 11 Select whether you want to provision the Cisco User-Defined Network service on your network now or schedule it for a later time.

- To provision the service on your network now, click the **Now** radio button and click **Next**.
- To schedule the service on your network for a later time, click the **Later** radio button, define the date and time, and click **Next**.

The **Configuration Summary** screen appears.

Step 12 Review the settings and click **Edit** in any section if you want to make a change.

Step 13 Click **Configure**.

In the screen that follows, a check mark is shown next to each step as it is completed.

Step 14 Click **View Provisioning Status**.

For more information, see View the User-Defined Network Service Provisioning Status, on page 483.

View the User-Defined Network Service Provisioning Status

This procedure shows you how to view the Cisco User-Defined Network service provisioning status from the **Provision** > **All Services** window. You can also click the **View Provisioning Status** button in the **Configure Cisco User Defined Network** screen after configuring a Cisco User-Defined Network successfully.

Before you begin

Configure and provision the Cisco User-Defined Network service from the **Workflows** > **Configure Cisco User Defined Network** window.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **All Services** > **Cisco User Defined Network**.

The **Site Provisioning Status** window displays the site name, device name, number of SSIDs used, and status of site provisioning.

Step 2 Click **Refresh** to see the latest provisioning status.

Step 3 Click the site name to view additional details for the provisioned device, such as SSID name, User-Defined Network (UDN) status, and Unicast Traffic Containment.

Step 4 Click **Activity** to track the scheduled task status in the **Scheduled Tasks** window.

Configure Cisco Umbrella

The following sections provide information about integrating Cisco Umbrella with Cisco DNA Center.

About Cisco Umbrella

The DNS-layer security in Cisco Umbrella provides the fastest and easiest way to improve your network security. It helps improve security visibility, detect compromised systems, and protect your users on and off the network by stopping threats over any port or protocol before they reach your network or endpoints.

Cisco DNA Center supports Cisco Umbrella configuration on the following devices:

- Cisco Catalyst 9800 Series Wireless Controllers with Cisco IOS-XE software version 16.12 or later
- Cisco Catalyst 9100 Series APs
- Cisco Catalyst 9200 Access Switch with Cisco IOS-XE software version 17.3.1 or later
- Cisco Catalyst 9300 Access Switch with Cisco IOS-XE software version 17.3.1 or later

Role-Based Access Control Settings for Cisco Umbrella

To configure Cisco Umbrella with Cisco DNA Center and to provision Cisco Umbrella on network devices, you must create a user role with the necessary RBAC permission for Cisco Umbrella. For more information, see "Manage Users" in the Cisco DNA Center Administrator Guide.

Table 55: RBAC Permission Matrix for Cisco Umbrella

Function	Access	Permission
Configure Cisco Umbrella with Cisco DNA Center	Network Design > Advanced Network Settings	Write
Add Umbrella dashlet in System 360	Network Design > Advanced Network Settings	Write

Function	Access	Permission
Provision Cisco Umbrella on network devices	Network Provision > Provision	Write
	Network Design > Network Hierarchy	Read
	Network Provision > Inventory Management	Read
	System	Read
	Network Provision > Scheduler	Write
	Network Services > Umbrella	Write

Configure Cisco Umbrella with Cisco DNA Center

Before you begin

- Create a Cisco Umbrella account.
- Log in to *login.umbrella.com* and create the necessary keys, such as the API key, legacy token, management key, and secret.
- Note down the organization ID from the Cisco Umbrella login URL.
- Create the local bypass domains in Cisco Umbrella.
- If Cisco DNA Center has a proxy server configured as an intermediary between itself and the network devices it manages or the Cisco cloud from which it downloads software updates, you must configure access to the proxy server. For more information, see the Configure the Proxy section in the Cisco DNA Center Administrator Guide.
- Install the Cisco Umbrella package in Cisco DNA Center. See the Download and Install Packages and Updates section in the Cisco DNA Center Administrator Guide.
- Create a user role with necessary RBAC permission for Cisco Umbrella. See Role-Based Access Control Settings for Cisco Umbrella, on page 484.

Note You cannot install Cisco Umbrella package on a Cisco DNA Center cluster configured with IPv6.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Settings** > **External Services** > **Umbrella**.

Step 2 Enter the following details that you retrieved manually from Cisco Umbrella:

- **Organization ID**
- **Network Device Registration API Key**
- **Network Device Registration Secret**

- **Management API Key**
- **Management Secret**
- **Legacy Device Registration Token**

Step 3 Click **Save**.

Add the Umbrella Dashlet

You can add the **Umbrella** dashlet in the **System 360** page. The **Umbrella** dashlet shows the configuration status of Cisco Umbrella with Cisco DNA Center.

Before you begin

You must install the Cisco Umbrella package.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **System 360**.

Step 2 From the **Actions** menu, choose **Edit Dashboard** and click **Add Dashlet**.

Step 3 Choose **Umbrella Dashlet** and click **Add**.

The **Umbrella** dashlet appears under **Externally Connected Systems** in the **System 360** page. The **Umbrella** dashlet shows the status as **Available** and displays the organization ID, if Cisco Umbrella is configured with Cisco DNA Center.

If Cisco Umbrella is not configured with Cisco DNA Center, you can click the **Configure** link and complete the fields in **System** > **Settings** > **External Services** > **Umbrella**. See Configure Cisco Umbrella with Cisco DNA Center, on page 485.

If the keys are changed in Cisco Umbrella, you can click the **Update** link and update the keys in **System** > **Settings** > **External Services** > **Umbrella**. See Configure Cisco Umbrella with Cisco DNA Center, on page 485.

View the Umbrella Service Statistics Dashboard

In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Services** > **Umbrella** to view the **Umbrella Service Stats** dashboard.

The dashboard displays the following dashlets:

- **Total Umbrella DNS Queries**: Shows the number of blocked DNS queries and allowed DNS queries for the selected site.
- **Blocked Umbrella DNS Queries**: Shows the number of DNS queries blocked by security policy and content policy for the selected site.

By default, the dashlet shows statistics for the last 3 hours. You can view statistics for the last 24 hours or 7 days by choosing the required time from the drop-down list in the top-left corner of the **Umbrella Service Stats** page.

Prerequisites for Provisioning Cisco Umbrella on Network Devices

Before provisioning Cisco Umbrella on network devices, ensure that:

- Cisco Umbrella is configured with Cisco DNA Center.
- Wireless provisioning is complete for the devices on which you want to provision Cisco Umbrella.
- The SSID configuration is nonfabric.
- The AP is provisioned, if the device is configured with a nonfabric SSID in FlexConnect mode.
- The device has direct internet access to establish connection with Cisco Umbrella.
- The Cisco Umbrella root certificate is available in the Cisco DNA Center trustpool. See Configure Trustpool in the Cisco DNA Center Administrator Guide.
- If the device has a Cisco Umbrella configuration that is not set from Cisco DNA Center, remove the Cisco Umbrella configuration from the device and resync the device with Cisco DNA Center.

Provision Cisco Umbrella on Network Devices

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Workflows** > **Umbrella Deployment**.
Alternatively, do the following:

- In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Services** > **Umbrella**.
- Choose a site from the network hierarchy for which you want to deploy Cisco Umbrella.
- The **Select Devices** window appears. Go to Step 4 to continue the deployment workflow.

Step 2 Click **Let's Start**.

To skip this screen in the future, check **Don't show this to me again**.

The **Choose Site** window appears. You can view the device readiness status in each site, as follows:

- **Eligible Devices**: Devices that are eligible for Cisco Umbrella configuration. See Prerequisites for Provisioning Cisco Umbrella on Network Devices, on page 487.
- **Enabled Devices**: Devices that are already configured from Cisco DNA Center.

Step 3 Choose a site to deploy and click **Next**.

You can choose only one site at a time. If you choose a parent site, Cisco Umbrella can be deployed on all child sites at the same time.

Step 4 In the **Select Device Type** window, choose **Switches** or **Wireless Controllers** and click **Next**.

Step 5 If you have chosen **Switches** in the **Select Device Type** window, do the following:

a) In the **Select Devices** window, choose the wired device and click **Next**.

b) In the **Configure Interface** window, do the following:

1. Choose the ports you want to configure and click **Define Umbrella Interfaces**.

2. In the **Select Configuration** dialog box, click the **Define Umbrella Interfaces** drop-down list and choose **IN(LAN)**, **OUT(WAN)** or **Disable Umbrella**.
3. Click **Save**.

Note You must choose at lease one **IN** and one **OUT** interface to proceed further.

c) In the **Define Umbrella Policy Mapping (Wired)** window, choose Umbrella policies at a global or interface level and click **Next**.
d) In the **Configure Policies for Your Devices** window, choose the **IN(LAN)** interface and click **Define Umbrella Policies**.
e) In the **Select Policy** dialog box, choose the policy for the selected interfaces and click **Save**.

Step 6 If you have chosen **Wireless Controllers** in the **Select Device Type** window, do the following:

a) In the **Select Devices** window, choose the wireless device and click **Next**.
b) Choose the SSIDs and select the required Cisco Umbrella policy for each SSID.

Note
- Only nonfabric SSIDs are listed on this page.
- If you choose an SSID and don't select the Cisco Umbrella policy, the default policy is mapped with the SSID.
- If you choose multiple policies, the order of enforcement of policies is defined in the Cisco Umbrella cloud portal.

c) Click **Next** and in the **Umbrella Policy Association (Wireless)** window, view the default policies applied to the SSIDs.

If you want to change the policies associated with the SSIDs, click the **Cisco Umbrella** link. In the Cisco Umbrella console, you can see the network identity after you have completed the deployment of Cisco Umbrella from Cisco DNA Center. For devices with Cisco IOS-XE software version 16.xx, the network identity is shown as global. For devices with a Cisco IOS-XE software version later than 16.xx, the network identity is shown as a custom name created based on the site and SSID name.

d) Click **Next**.

Step 7 In the **Review Internal Domains** window, add or delete the list of internal domains. The DNS queries that match a domain in the **Internal Domain** list are forwarded to the local DNS server instead of Cisco Umbrella.

Step 8 Click **Next**.

The **DNS Crypt** window appears. The **Enable DNS Packet Encryption** option is selected by default.

Step 9 In the **DNS Crypt** window, click **Next**.

If you don't want DNS packet encryption, uncheck the **Enable DNS Packet Encryption** check box and click **Next**.

Step 10 Review the details in the **Summary** window and click **Edit** if you want to make any changes.

Step 11 Click **Deploy**.

The **Schedule** window appears with **Now** and **Later** options.

Step 12 In the **Schedule** window, do one of the following:

- To deploy the configuration immediately, click the **Now** radio button and click **Apply**.

- To deploy the configuration at a later time, click the **Later** radio button, enter the **Task Name**, define the **Start Date and Time**, and click **Apply**.

Step 13 In the **Deployment** window, click **View Status** to view the deployment status in the **Scheduled Tasks** page.

You can view the Cisco Umbrella deployment status of the device and the device configuration status in Cisco Umbrella. You can also view the Cisco Umbrella deployment logs in the **Audit Logs** page.

Note Cisco umbrella deployment on your organization's network can be monitored only from *login.umbrella.com*.

Disable Cisco Umbrella on Network Devices

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Workflows** > **Umbrella Deployment**.

Alternately, do the following:

- In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Services** > **Umbrella**.
- Choose a site from the network hierarchy from which you want to disable Cisco Umbrella.
- The **Select Devices** window appears. Go to Step 4 to continue the disable workflow.

Step 2 Click **Let's Start**.

To skip this screen in the future, check **Don't show this to me again**.

The **Choose Site** window appears. You can view the device readiness status in each site, as follows:

- **Ready Devices**: Devices that meet the prerequisites for Cisco Umbrella configuration. See Prerequisites for Provisioning Cisco Umbrella on Network Devices, on page 487.
- **Not Ready Devices**: Devices that do not meet the prerequisites.
- **Enabled Devices**: Devices that are already configured from Cisco DNA Center.

Step 3 Choose the site that you want to disable, and click **Next**.

You can choose only one site at a time. If you choose a parent site, Cisco Umbrella is disabled on all the child sites at the same time.

Step 4 In the **Select Device Type** window, choose **Switches** or **Wireless Controllers** and click **Next**.

Step 5 In the **Select Devices** window, click the **Enabled** tab and choose the devices.

Step 6 Click the **Disable** radio button and choose the devices.

Step 7 Click **Next**.

Step 8 In the **Summary** window, click **Deploy**.

Step 9 In the **Schedule** window, do one of the following:

- To disable the configuration immediately, click the **Now** radio button and click **Apply**.

- To disable the configuration at a later time, click the **Later** radio button, enter the **Task Name**, define the **Start Date and Time**, and click **Apply**.

Step 10 In the Deployment window, click **View Status** to view the deployment status in the **Scheduled Tasks** page.

You can view the Cisco Umbrella deployment logs in the **Audit Logs** page.

Update the Cisco Umbrella Configuration on Network Devices

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Workflows** > **Umbrella Deployment**.

Alternately, do the following:

- In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Services** > **Umbrella**.
- Choose a site from the network hierarchy for which you want to update the Cisco Umbrella configuration.
- The **Select Devices** window appears. Go to Step 4 to continue the update workflow.

Step 2 Click **Let's Start**.

To skip this screen in the future, check **Don't show this to me again**.

The **Choose Site** window appears. You can view the device readiness status in each site, as follows:

- **Ready Devices**: Devices that meet the prerequisites for Cisco Umbrella configuration. See Prerequisites for Provisioning Cisco Umbrella on Network Devices, on page 487.
- **Not Ready Devices**: Devices that do not meet the prerequisites.
- **Enabled Devices**: Devices that are already configured from Cisco DNA Center.

Step 3 Choose the site that you want to update and click **Next**.

You can choose only one site at a time. If you choose a parent site, Cisco Umbrella is updated on all child sites at the same time.

Step 4 In the **Select Device Type** window, choose **Switches** or **Wireless Controllers** and click **Next**.

Step 5 If you have chosen **Switches** in the **Select Device Type** window, do the following:

a) In the **Select Devices** window, choose the wired device and click the **Update** radio button.
b) Click **Next**.
c) In the **Configure Interface** window, do the following:

1. Choose the ports and click **Define Umbrella Interfaces**.
2. In the **Select Configuration** dialog box, click the **Define Umbrella Interfaces** drop-down list and choose **IN(LAN)**, **OUT(WAN)** or **Disable Umbrella**.
3. Click **Save**.

Note You must choose at lease one **IN** and one **OUT** interface to proceed further.

d) In the **Define Umbrella Policy Mapping (Wired)** window, choose Umbrella policies at a global or interface level and click **Next**.
e) In the **Configure Policies for Your Devices** window, choose the **IN(LAN)** interface and click **Define Umbrella Policies**.
f) In the **Select Policy** dialog box, choose the policy for the selected interfaces and click **Save**.

Step 6 If you have chosen **Wireless Controllers** in the **Select Device Type** window, do the following:

a) In the **Select Devices** window, choose the wireless device and click the **Update** radio button.
b) Click **Next**.
c) In the **Define Umbrella Policy Map (Wireless)** window, choose the SSIDs and select the desired Cisco Umbrella policies to map, or unselect SSIDs to disable Cisco Umbrella.

Step 7 In the **Review Internal Domains** window, add or delete the list of internal domains. The DNS queries that match a domain in the **Internal Domain** list are forwarded to the local DNS server instead of Cisco Umbrella.

Step 8 Click **Next**.

The DNS Crypt window appears. The **Enable DNS Packet Encryption** option is selected by default.

Step 9 In the DNS Crypt window, click **Next**.

If you don't want DNS packet encryption, uncheck the **Enable DNS Packet Encryption** check box and click **Next**.

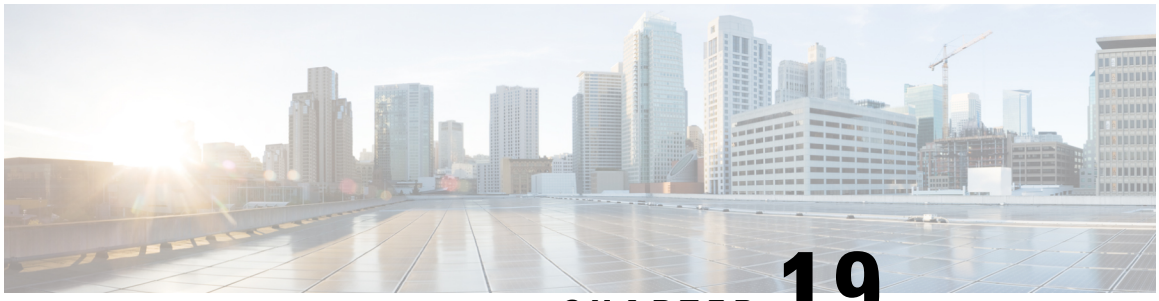
Step 10 In the **Summary** window, click **Deploy**.

Step 11 In the **Schedule** window, do one of the following:

- To update the configuration immediately, click the **Now** radio button and click **Apply**.
- To update the configuration at a later time, click the **Later** radio button, enter the **Task Name**, define the **Start Date and Time**, and click **Apply**.

Step 12 In the Deployment window, click **View Status** to view the deployment status in the **Scheduled Tasks** page.

You can view the Cisco Umbrella deployment logs in the **Audit Logs** page.



CHAPTER 19

Compliance Audit for Network Devices

Compliance Overview

Compliance helps in identifying any intent deviation or **out of band** changes in the network that may be injected or reconfigured without affecting the original content.

A network administrator can conveniently identify devices that do not meet compliance requirement for the different aspects of compliance such as Software Image, PSIRT, Network Profile and so on in Cisco DNA Center.

Compliance checks can be automated or performed on demand.

- Automated compliance check: Uses the latest data collected from devices in Cisco DNA Center. This compliance check listens to the traps and notification from various services such as inventory, SWIM, and so on to assess data.
- Manual compliance check: Enables user to manually trigger the compliance in Cisco DNA Center.
- Scheduled compliance check: A scheduled compliance job is a weekly compliance check that runs every Saturday at 11 pm.

Manual Compliance Run

You can trigger a compliance check manually in Cisco DNA Center.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Inventory**.

Step 2 For a bulk compliance check, do the following:

a) Choose all the applicable devices.

b) From the **Actions** drop-down list, choose **Compliance** > **Run Compliance**.

Step 3 For a per-device compliance check, do the following:

a) Choose the devices for which you want to run the compliance check.

b) From the **Actions** drop-down list, choose **Compliance** > **Run Compliance**.

c) Alternatively, click on compliance column (if available) and then click on **Run Compliance**.

Step 4 To view the latest compliance status of a device, do the following:

a) Choose the device and inventory. See Resynchronize Device Information, on page 78.

b) From the **Actions** drop-down list, choose **Compliance** > **Run Compliance**.

Note
- A compliance run cannot be triggered for unreachable or unsupported devices.
- If compliance is not run manually for a device, the compliance check is automatically scheduled to run after a certain period of time which depends on the type of compliance.

View Compliance Summary

The inventory page shows an aggregated status of compliance for each device.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Provision** > **Inventory**.

The compliance column shows the aggregated compliance status of each device.

Step 2 Click the compliance status to launch the compliance summary window, which shows the following compliance checks applicable for the selected device:

- Startup versus Running Configuration
- Software Image
- Critical Security Vulnerability
- Network Profile
- Fabric
- Application Visibility

Note Network Profile, Fabric and Application Visibility are optional and are displayed only if the device is provisioned with the required data.

Types of Compliance

Compliance Type	Compliance Check	Compliance Status

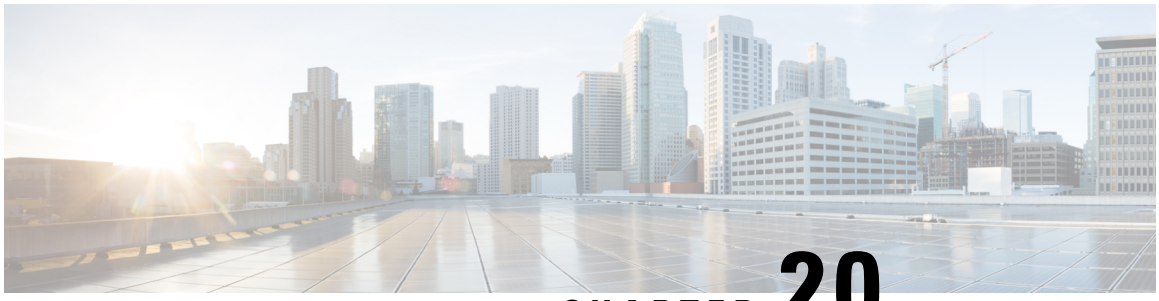
Startup versus Running Configuration	This compliance check helps in identifying whether the startup and running configurations of a device are in sync. If the startup and running configurations of a device are out of sync, then compliance is triggered and a detailed report of the out of band changes is displayed. The compliance for startup vs running configurations is triggered within five minutes of any **out of band** changes.	• Noncompliant: The Startup and Running configuration are not the same. On detail view, the system shows different startup versus running between or running versus previous running. • Compliant: Startup and Running Configuration are the same. • NA (Not Applicable): The device is not supported for this compliance type (for example, AireOS).
Software Image	This compliance check helps network administrator to see if tagged golden image in Cisco DNA Center is running on the device or not. It shows the difference in golden image and running image for a device. When there is a change in the software image, the compliance check is triggered immediately without any delay.	• Noncompliant: The device is not running the tagged golden image of the device family. • Compliant: The device is running the tagged golden image of the device family. • NA (Not Applicable): The golden image is not available for the selected device family.
Critical Security (PSIRT)	PSIRT Compliance check enables the network administrator in checking whether the network devices are running without any critical security vulnerabilities or not.	• Noncompliant: The device has critical advisories. A detailed report displays various other information. • Compliant: There are no critical vulnerabilities in the device. • NA (Not Applicable): The security advisory scan has not been done by network administrator in Cisco DNA Center or the device is not supported.
Network Profile	Cisco DNA Center allows you to define its intent configuration via Network Profile and pushes to device via provisioning. The Intent must be running on a device. If any violations are found at any time due to **out of band changes**, compliance identify, assess and flag it off. The violations are shown to the user under **Network Profiles** on the compliance summary page. The automatic compliance check is scheduled to run after a period of 5 hours. **Note** Network profile compliance is only applicable for routers and wireless LAN controllers and not for switches.	• Noncompliant: The device is not running the intent configuration of profile. • Compliant: The intent configurations are running on the device. • Error: The compliance could not compute status because of an underlying error. For more details, please refer to the error log.
Fabric (SDA Profile)	Fabric compliance helps to identify the fabric intent violations such as any out of band changes for fabric related configurations.	• Noncompliant: The device is not running the intent configuration. • Compliant: The device is running the intent configuration.

Application Visibility	Cisco DNA Center allows you to create application visibility intent and provision it to devices via CBAR and NBAR. If there is an intent violation on devices, compliance identity, assess, and show the violaion as compliant or noncompliant under **Application Visibility**. The automatic compliance check is scheduled to run after a period of 5 hours.	• Noncompliant: The CBAR/NBAR configuration is not running on the device. • Compliant: The intent configuration of CBAR/NBAR is running on the device.

Compliance Behavior After Device Upgrade

- A compliance check for all applicable devices (devices for which compliance never ran in the system) is triggered after successful device upgrade.
- Compliance calculates and shows the status of the devices in the inventory, except the Startup vs Running type.
- After upgrade, the Startup vs Running tile shows as NA with the text "Configuration data is not available."
- After a day of successful upgrade, a one-time scheduler runs and makes configuration data available for devices. The Startup vs Running tile starts showing the correct status (Compliant/Noncompliant) and detailed data.
- If any traps are received, the config archive service collects configuration data and the compliance check runs again.

Note In the upgrade setup, ignore any compliance mismatch for the **Flex Profile** interface. For the interface name, **1** maps to **management**.



CHAPTER 20

Build and Deploy Workflows

AP Refresh Workflow

The following sections provide information about replacing old access points with new access points using workflows in Cisco DNA Center.

Introduction to the AP Refresh Workflow

The AP Refresh feature allows you to replace older AP models with the newer AP models using the Cisco DNA Center workflow.

The AP Refresh workflow supports APs that are associated with Cisco AireOS Controllers and Cisco Catalyst 9800 Series Wireless Controllers.

The AP Refresh workflow supports the following APs:

- Cisco Aironet 1810 Series OfficeExtend Access Points
- Cisco Aironet 1810W Series Access Points
- Cisco Aironet 1815i Access Point
- Cisco Aironet 1815w Access Points
- Cisco Aironet 1815m Access Point
- Cisco Aironet 1830 Series Access Points
- Cisco Aironet 1850 Series Access Points
- Cisco Aironet 1800 Series Access Points
- Cisco Aironet 2800 Series Access Points
- Cisco Aironet 3800 Series Access Points

- Cisco Aironet 4800 Series Access Points
- Cisco Aironet 1700 Series Access Points
- Cisco Aironet 2700 Series Access Points
- Cisco Aironet 3700 Series Access Points
- Cisco Catalyst 9115 Series Wi-Fi 6 Access Points
- Cisco Catalyst 9117 Series Wi-Fi 6 Access Points
- Cisco Catalyst 9120 Series Wi-Fi 6 Access Points
- Cisco Catalyst 9130 Series Wi-Fi 6 Access Points

AP Refresh Workflow

This procedure shows how to replace old APs with new ones in Cisco DNA Center.

Before you begin

- The old AP must be provisioned and in Unreachable state.
- The new AP must be connected to a Cisco Wireless Controller and available in the Cisco DNA Center Inventory, in Reachable state.
- The old and new AP must be associated with the same wireless controller.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Workflows** > **Access Point Refresh**.

A library of available workflows is displayed. These workflows guide you step by step through a particular task.

Step 2 Click **Let's Do it**.

To skip this screen in the future, check **Don't show this to me again**.

The **Get Started** screen appears.

Step 3 In the **Task Name** field, enter a unique name for the workflow and click **Next**.

Step 4 In the **Select Network Sites** screen, navigate to the floor where you want to refresh the AP and click **Next**.

The right pane shows the selected building, floor, and the total number of APs provisioned on that floor.

You can replace APs that are already in provisioned state.

Step 5 In the **Select Access Points** screen, check the check box next to the device name that you want to replace and click **Next**.

Step 6 In the **Select procedure for providing New Access Points** screen, select a method through which you want to provide new AP details: **Add New Access Point detail via CSV file** or **Add New Access Point detail via GUI**.

- Click the **Add New Access Point detail via CSV file** radio button to upload a comma-separated value (CSV) file that contains the new device name and serial number.
  - To do this, click the **Download Selected Devices List** template and add the device name and serial number of the new AP. The downloaded CSV template file contains the old AP details. After adding the device name

and serial number of the new AP, you can either import the CSV file or drag and drop the CSV file to the drag and drop area.

- To import the CSV file, click **Choose file** and browse to the location of the CSV, then click **Open**.

  Cisco DNA Center performs a validation check. If the uploaded CSV file does not meet the requirement, an error message appears. Click **View Details** to get more details about the error message.

- To add the new AP details using the GUI, click the **Add New Access Point detail via GUI** radio button and click **Next**.

  The **Assign New Access Points** screen appears, where you can assign a new AP for each old AP.

  - The **Old Devices** area shows details such as the IP address of the old AP, old AP name, site details, platform, and AP series information. Under the **New Devices** area, provide details about the new device.
  - From the **Choose Serial Number** drop-down list, choose the serial number of the new AP.

    If the new AP is already associated with the wireless controller and is available in the Inventory, the serial number of that AP is displayed as **Managed** in the **Choose Serial Number** drop-down list.

    If the new AP has contacted Cisco DNA Center through PnP, the serial number of that AP is displayed as **Unclaimed** in the **Choose Serial Number** drop-down list.

    If the serial number of the new AP is not available in the Inventory, the **Serial Number** drop-down list does not contain the serial number. To add a new serial number that is not present in the Inventory, from the **Choose Serial Number** drop-down list, enter the serial number and click **+**.

    Note Cisco DNA Center performs a validation check and displays any errors. You must fix those errors before proceeding.

    You must resolve the following dependencies before provisioning new APs:

    - Device EULA acceptance by providing cisco.com credentials.
    - Update the Cisco Wireless Controller software image version. This validation does not stop you from proceeding with the AP refresh.
    - AP Connected SwitchPort: This validation message does not stop you from proceeding with the AP refresh.

Step 7 Click **Next**.

The configuration that is copied from the old AP to new AP is displayed in the **Configuration Copied from Old Access Point to New** screen.

Step 8 Click **Next**.

Step 9 In the **Submit Access Point Refresh Task** screen, click **Provision** to start the AP refresh task.

Step 10 In the **Track Replacement Status** screen, you can monitor the AP replacement status.

- Click **View Details** to get more information about the AP replacement status.
  - If the AP replacement succeeds, the **Replacement Status** window shows the **Replacement Status** as **REPLACED**.
  - If the AP replacement fails, the **Replacement Status** shows as **Error**.

- To delete the replacement entry, under the **Actions** column, click the three blue dots and click **Delete**. In the **Warning** dialog box, click **Yes**.
- Click **Export** to download the provisioning summary to a CSV file that you can save locally.
- Click **Download Report** to download the provisioning status report.

Note If the new AP is not yet discovered in the Inventory and the corresponding AP refresh entry is waiting for the new device to be connected, or if the PnP claim process is in progress, you must resynchronize the Cisco Wireless Controller.

Step 11 Click **Next** to view the summary details.

Step 12 After successful replacement, an AP refresh event is generated in Cisco DNA Assurance for the old and new AP.

You can view the AP refresh event under **Event Viewer** in the **AP View 360** window.

The new APs are automatically updated on the respective floor maps in the **Network Hierarchy** window.

Configure User-Defined Network Workflow

The following sections provide information about configuring the Cisco User-Defined Network service using workflows in Cisco DNA Center.

Introduction to User-Defined Network Service

Home, consumer, and IoT devices on the network such as printers, speakers, Apple TV, Google Chromecast, ring doorbells, smart bulbs, and so on, depend on the Simple Service Discovery Protocols (SSDP) such as Apple Bonjour, multicast DNS (mDNS), and Universal Plug and Play (UPnP) to provide the easy discovery and usage of devices.

Cisco User-Defined Network service provides secure and remote onboarding of client devices in shared environments such as dormitory rooms, residence halls, class rooms, and auditoriums. With the User-Defined Network service, users can securely use SSDP such as Apple Bonjour, mDNS protocol such as AirPlay, AirPrint, Screen Mirroring, Print, or UPnP protocol to interact and share with only their registered device in the shared environment.

The User-Defined Network service provides the following solution:

- Easy and secure onboarding of client devices.
- Automatic segmentation of client devices which belongs to a particular user.
- Ability to invite other users to share their devices.

The following software versions of Cisco DNA Center, Cisco Identity Services Engine, Cisco Catalyst 9800 Series Wireless Controller, and Access Points are supported:

- Cisco DNA Center Release 1.3.1.2 and later
- Cisco Identity Services Engine Release 2.7 and later

- Cisco Catalyst 9800 Series Wireless Controller Release 17.1.x
- Cisco 802.11ac Wave 2 APs:
  - Cisco Aironet 1810 Series OfficeExtend Access Points
  - Cisco Aironet 1810W Series Access Points
  - Cisco Aironet 1815i Access Point
  - Cisco Aironet 1815w Access Point
  - Cisco Aironet 1815m Access Point
  - Cisco 1830 Aironet Series Access Points
  - Cisco Aironet 1850 Series Access Points
  - Cisco Aironet 2800 Series Access Points
  - Cisco Aironet 3800 Series Access Points
  - Cisco Aironet 4800 Series Access Points
- Cisco 802.11ac Wave 1 APs
  - Cisco Aironet 1700 Series Access Points
  - Cisco Aironet 2700 Series Access Points
  - Cisco Aironet 3700 Series Access Points

Prerequisites for Configuring the User-Defined Network Service

Before configuring the Cisco User-Defined Network service, the following prerequisites must be completed:

- Confirm that APs have joined the Cisco Wireless Controller.
- Discover Cisco Wireless Controllers and APs in your network using the **Discovery** functionality so that the discovered devices are listed in the **Inventory** window.
- Map the AAA server client endpoint with Cisco Identity Services Engine.
- Add the authentication tokens to Cisco DNA Center.
- Create nonfabric enterprise SSIDs or guest wireless SSIDs with any security and map them to the network profile.
- Provision SSIDs.

Configure the User-Defined Network Service

This procedure shows how to configure the Cisco User-Defined Network service from the **Workflows** > **Configure Cisco User Defined Network** window. Alternatively, you can configure the Cisco User-Defined Network service from the **Provision** > **Services** > **Cisco User Defined Network** window.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Workflows** > **Configure Cisco User Defined Network**.

Step 2 Click **Let's Do It**.

The **Let's start with configuring the Service** screen appears. You must generate an authentication token using the Cisco DNA Center Cloud portal so that Cisco DNA Center connects with Cisco DNA Center Cloud.

Step 3 Click **Configure Cloud Service**.

The **Cisco DNA Center Cloud** application opens in a new tab.

Step 4 Log in to **Cisco DNA Center Cloud** using your cisco.com account ID and password.

- Click the **Authentication Token** tab in the left menu.

  The **Authentication Token** window appears.

- In the **Authentication Token** window, click **Generate New Token**.

  The authentication token is generated.

- Click **Copy Token** to copy the authentication token.

Step 5 Navigate back to the **Let's start with configuring the Service** screen in Cisco DNA Center.

Step 6 Click **Next** to validate the copied authentication token.

Step 7 In the **Authentication Token** text box, paste the authentication token that you generated and copied in **Cisco DNA Center Cloud**, and click **Connect**.

If the token is validated successfully, a message saying `Connection validated, click Next to proceed` appears.

If the token validation fails, click **Retry**, re-enter the authentication token, and click **Connect**.

Step 8 Click **Next** to select the sites where you want to enable the Cisco User-Defined Network service.

- From the **Select Sites** drop-down list, choose the sites.
- Check the **Disable User Defined Network Service** check box to disable the workflow for all the enabled sites.

Step 9 Click **Next** to select the SSIDs for the sites you selected.

The provisioned nonfabric SSIDs are displayed for all the sites selected in the previous step.

- From the **SSID(s)** drop-down list, choose the SSIDs where the User-Defined Network service will be enabled.
- To limit the unicast traffic for the selected SSID, turn on **Unicast Traffic Containment**.
- Click **Apply Individually** to apply the unicast traffic containment for a specific site.
- Click **Apply to all** to apply the unicast traffic containment for all sites.

Step 10 Click **Next**.

Step 11 Select whether you want to provision the Cisco User-Defined Network service on your network now or schedule it for a later time.

- To provision the service on your network now, click the **Now** radio button and click **Next**.

- To provision the service on your network for a later time, click the **Later** radio button, define the date and time, and click **Next**.

The **Configuration Summary** screen appears.

Step 12 Review the following details and click **Edit** in any of the sections if you want to make a change.

- **Authentication Token**
- **Selected Sites & SSIDs**
- **Scheduling**

Step 13 Click **Configure**.

In the next screen, a check mark is shown next to each step as it is completed.

Step 14 Click **View Provisioning Status**.

Enable Application Hosting on Switches

The following procedure helps you to enable docker applications such as ThousandEyes Enterprise Agent, iPerf on selected switches at a specific site.

Before you begin

- Complete the prerequisites. For more information, see Prerequisites for Application Hosting, on page 471.
- Add the application to Cisco DNA Center. For more information, see Add an Application, on page 473.
- Check the readiness of the switch to host the application. For more information, see View Device Readiness to Host an Application, on page 472.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Provision** > **Services** > **App Hosting for Switches**. Select the application and click **Install** at the bottom of the screen.

Step 2 You can also launch the workflow by choosing **Workflows** > **Enable Apps on Switches** > **Let's Do it**.

The workflow is launched.

Note At the top of the page, you can place your cursor on the blue progress bar and switch back to the previous steps listed there.

Step 3 In the **Select Site** window, navigate to the building where you want to enable the application.

Step 4 Click **Next**.

Step 5 In the **Select App** window, choose the application.

Step 6 Click **Next**.

Note You can access the **+ New App** link to add an application that is not present in Cisco DNA Center.

Step 7 In the **Select Switches** window, choose the device for which you want to enable the application.

Note You can import or export devices in bulk by providing the details in the specified template in the **Select Switches** dialog box.

Step 8 Click **Next**.

Step 9 Complete the following settings in the **Configuration App**window:

- **App Networking**
  - **Device Network**: Click the **Select Network** drop-down list and choose a VLAN to configure the application.
  - **App IP address**: Choose **Static** or **Dynamic** from the **Address Type** drop-down list. If you choose **Static**, click the thumbnail icon and enter the **IP Address**, **Gateway**, **Prefix/Mask**, and **DNS** for the application.
- **Resource Allocation**: Check the **Allocate resources as asked by the app** or **Allocate all resources available on the device** check box.
- **Custom Settings**: Applicable only for Cisco package applications. Enter the configuration details for the attributes that are specified by the application.
- **App Data**: Browse and upload the application-specific files. To identify the required application-specific files, see the relevant application document.
- **Docker Runtime Options**: Enter the docker runtime options required by the application.

Step 10 In the **Summary** page, review the details before installing the application on the selected switches.

Step 11 Click **Next**.

The **Provisioning Task** window displays the task name that tracks the deployment of the application on the switches.

Step 12 Review the automatically generated task name and click **Provision**.

Step 13 In the **Track Provisioning Status** window, you can track the progress of the deployment.

Step 14 Click **View Details** to view the provisioning status of the individual devices and any failures.

Step 15 Click **Next**.

The application is enabled successfully.

The summary of the task result and the success/failure counts are displayed.

Step 16 Click **Manage App**, where you can manage the lifecycle operations of the application to perform day-N tasks.

Enable IoT Services Workflow

The following sections provide information about enabling IoT technologies such as Bluetooth, Zigbee, and ESL on Cisco Catalyst 9100 Series Access Points using Workflows in Cisco DNA Center.

Enable IoT Services on Cisco Catalyst 9100 Series Access Points

This procedure helps you to enable IoT technologies such as Bluetooth, Zigbee, and ESL on selected Catalyst 9100 Series Access Points.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Workflows**.

A library of available workflows is displayed. These workflows guide you step by step through a particular task.

Step 2 Click **Enable IOT Services**.

Step 3 Click **Let's Do it** to start the installation workflow.

Step 4 In the **Select Site** window, navigate to the floor where you want to enable the IoT service.

Step 5 Click **Next**.

Step 6 In the **Select the Application** window, select the SES-imagotag ESL Connector application to enable IoT in your network, and click **Next**.

Note To add an application that is not present in the Cisco DNA Center, see Add an Application.

The **Select Access Points** window shows all the APs available on the particular floor.

Step 7 In the **Select Access Points** window, check the check box adjacent to the **Device Name** where you want to install the IoT connector application.

Step 8 Click **Next**.

Step 9 In the **Summary** window, review details before installing the application on selected APs, and click **Next**.

The **Provisioning Task** window appears which displays the task name which is created to track deployment of any application on APs.

Step 10 Review the auto generated task name and click **Provision**.

Step 11 In the **Track Provisioning Status** window you can track the progress of deployment.

Step 12 Click **View Details** to view the provisioning status.

Step 13 Click **Next**.

The **Done! Task Completed** window appears.

Step 14 Click **Manage IoT Application** to perform Day-N tasks.

Manage IoT Applications

This procedure shows how to manage IoT applications.

Before you begin

You must have enabled IoT services on Cisco Catalyst 9000 Series Access Points.

Step 1 After enabling IoT services, click **Manage IoT Application** in the **Done! Task Completed** window.

Step 2 Check the check box next to the **Hostname** and perform the following tasks:

- To start the application, from the **Actions** drop-down list, choose **Start App**.
- To stop the application, from the **Actions** drop-down list, choose **Stop App**.
- To edit the application configuration, from the **Actions** drop-down list, choose **Edit App Config**.

- To upgrade the application, from the **Actions** drop-down list, choose **Upgrade App**.
- To uninstall the application from the selected AP, from the **Actions** drop-down list, choose **Uninstall App**.

Step 3 Click the AP name to view the following details:

- AP Name
- AP Status
- IP Address
- Health

Step 4 Click **Tech Support logs** to collect application hosting logs.

About AP Configuration from Cisco DNA Center

The Configure Access Points workflow allows you to configure and deploy AP level and radio level parameters in Cisco DNA Center.

You can configure the following AP level parameters:

- AP location
- AP admin status
- AP mode
- AP LED status
- AP failover priority
- High availability

You can configure the following radio level parameters:

- Radio admin status
- Radio power settings
- Radio channel settings

Configure AP Workflow

This procedure shows how to configure AP and radio parameters in Cisco DNA Center.

Before you begin

Make sure that the AP is assigned to a site.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Workflows** > **Configure Access Points**.

Step 2 Click **Let's Do it**.

To skip this screen in the future, check the **Don't show this to me again** check box.

The **Get Started** screen appears.

Step 3 In the **Task Name** field, enter a unique name for the workflow, and click **Next**.

Step 4 In the **Select Site from the hierarchy** screen, navigate to the site where you want to apply AP-related configurations.

The right pane shows the selected floor and the number of APs available on that floor.

Step 5 Click **Next**.

The **Select Access Points** screen lists all the APs available in the selected site.

Step 6 In the **Select Access Points** screen, check the check boxes of the APs to bulk edit the AP Name.

Step 7 Click **Next**.

Step 8 The **Modify AP Name** screen shows the list of APs selected in the previous screen.
In this screen, you can enter a new name for the AP.

Step 9 Click **Next**.

Step 10 In the **Configure AP Parameters** screen, you can configure the following AP parameters:

- Check the **Location** check box and enter the location details.
- Check the **Admin Status** check box and click the **Disable** button to disable the admin status.
- Check the **AP LED Status** check box and click the **Disable** button to disable the AP LED status.
- Check the **AP Mode** check box and choose the **AP Mode** from the **Select AP Mode** drop-down list. You can either choose **Local/Flex** or **Monitor** mode.
- Check the **AP Failover Priority** check box and from the **AP Failover Priority** drop-down list, choose the priority to configure failover priority for APs. The options available are:
  - **Low**: Assigns access point to the level 1 priority, which is the lowest priority level. This is the default value.
  - **Medium**: Assigns the access point to the level 2 priority.
  - **High**: Assigns the access point to the level 3 priority.
  - **Critical**: Assigns the access point to the level 4 priority, which is the highest priority level.
- Check the **Controller Configuration** check box and configure the primary, secondary, and tertiary controller name and IP address for the access point.

Step 11 In the **Configure 802.11 a/n/ac/ax Parameters** screen, configure the following 802.11 a/n/ac/ax parameters:

- Check the **Admin Status** check box and click the Disable button to disable the admin status.
- Check the **Power Assignment** check box and click the **Custom** button and choose custom power from the **Select Custom Power** drop-down list.
- Check the **Channel Assignment** check box and click the **Custom** button and choose custom channel number from the **Select Custom Channel** drop-down list.
- Check the **Channel Width** check box and choose one of the channel bandwidth options from the **Select Channel Width** drop-down list:

- **20 MHz**
- **40 MHz**
- **80 MHz**
- **160 MHz**

- Check the **Antenna Name** check box and choose the antenna name from the **Select Antenna Name** drop-down list.
- If you select **Other** as the Antenna name, enter the **Antenna Gain** value in the **Antenna Gain (in dBi) (for Antenna-Other)** field. Enter a number to specify an external antenna's ability to direct or focus radio energy over a region of space. High-gain antennas have a more focused radiation pattern in a specific direction. The Antenna Gain value is 0–40.
- Check the **Azimuth** check box and enter a value for Azimuth orientation in degrees. The azimuth is the angle of the antenna measured relative to the x-axis. The azimuth range is 0–360.
- Check the **Elevation** check box and enter a value for Elevation orientation in degrees. The elevation orientation range is 0–90.
- Click **Next**.

Step 12 In the **Configure 802.11 b/g/n Parameters** screen, configure the following 802.11 b/g/n parameters:

- Check the **Admin Status** check box and click the **Disable** button to disable the admin status.
- Check the **Power Assignment** check box and click the **Custom** button and choose custom power from the **Select Custom Power** drop-down list.
- Check the **Channel Assignment** check box and click the **Custom** button and choose custom channel number from the **Select Custom Channel** drop-down list.
- Check the **Antenna Name** check box and choose the antenna name from the **Select Antenna Name** drop-down list.
- If you select **Other** as the Antenna name, enter the antenna gain value in the **Antenna Gain(in dBi) (for Antenna-Other)** field. Enter a number to specify an external antenna's ability to direct or focus radio energy over a region of space. High-gain antennas have a more focused radiation pattern in a specific direction. The Antenna Gain value is from 0 to 40.
- Check the **Azimuth** check box and enter a value for \Azimuth orientation in degrees. The azimuth is the angle of the antenna measured relative to the x-axis. The azimuth range is from 0 to 360.
- Check the **Elevation** check box and enter a value for Elevation orientation in degrees. The elevation orientation range is from 0 to 90.

Step 13 Click **Next** to view the summary details. In the **Summary** screen, review the following AP configuration details, and click **Edit** in any of the sections to make a change.

- Select Site from the hierarchy
- Select Access Points
- Modify AP Name
- Select AP Parameters

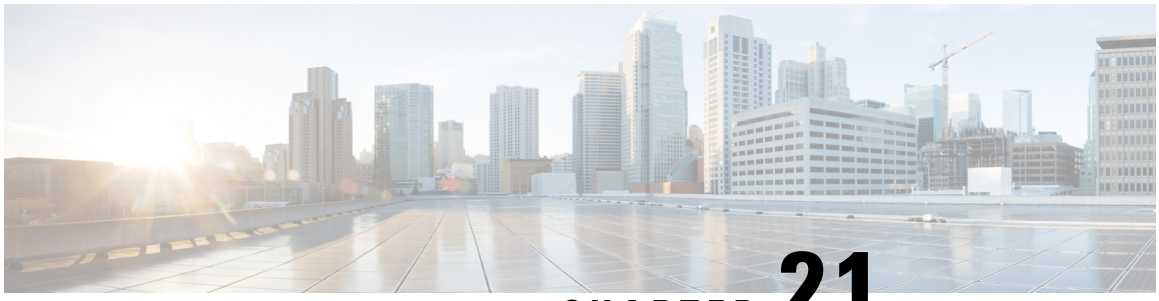
- Select 802.11 a/n/ac/ax Parameters
- Select 802.11 b/g/n/ax Parameters

Step 14 Click **Next**.

Step 15 Select whether you want to provision now or schedule it for a later time.

Step 16 To provision now, click the **Now** radio button and click **Next**. To provision for a later time, click the **Later** radio button, define the date and time, and click **Next**.

Step 17 In the **Track Provision Status** screen, you can view the **AP Configuration Provision** status.



CHAPTER 21

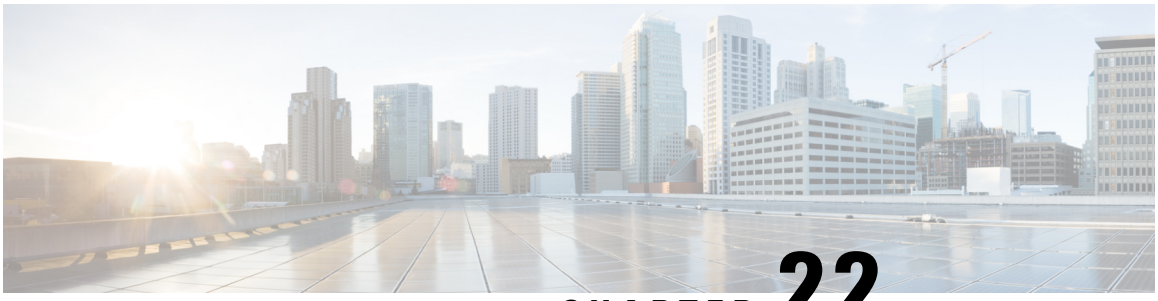
Cisco DNA Assurance

Cisco DNA Assurance

Cisco DNA Assurance is an application that is available from Cisco DNA Center.

For details about the Assurance application, including how to monitor and troubleshoot network health, client health, and application health, and enable NetFlow collection, see the Cisco DNA Assurance User Guide.

Cisco DNA Assurance



CHAPTER 22

Troubleshoot Cisco DNA Center Using Data Platform

About Data Platform

Data Platform provides tools that can help you monitor and troubleshoot Cisco DNA Center applications. **Data Platform** displays synthesized data from various inputs to help you identify patterns, trends, and problem areas in your network. For example, if something goes wrong in your network, you can quickly get answers to questions such as whether a pipeline is in an error state and what is the real-time traffic flow in a particular area. The main areas of Data Platform are:

- **Analytics Ops Center**: Provides a graphical representation of how data is streamed through collectors and pipelines and provides Grafana dashboards, which can help you identify patterns, trends, and problem areas in your network. See Troubleshoot Using the Analytics Ops Center, on page 514.
- **Collectors**: Collects a variety of network telemetry and contextual data in real time. As data is ingested, Cisco DNA Center correlates and analysis the data. You can view the status of collectors and quickly identify any problem areas. See View or Update Collector Configuration Information, on page 515.
- **Store Settings**: Allows you to specify how long data is stored for an application. See View Data Retention Settings, on page 516.
- **Pipelines**: Allows Cisco DNA Center applications to process streaming data. A data pipeline encapsulates an entire series of computations that accepts input data from external sources, transforms that data to provide useful intelligence, and produces output data. You can view the status of pipelines and quickly identify any problem areas. See View Pipeline Status, on page 517.

Troubleshoot Using the Analytics Ops Center

The Analytics Ops Center provides a graphical representation of how data is streamed through collectors and pipelines, and provides Grafana dashboards, which can help you identify patterns, trends, and problem areas in your network, such as:

- Missing data in Assurance.
- An inaccurate health score.
- Devices that appear as monitored under Inventory but unmonitored under Assurance.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Data Platform**.

Step 2 Click **Analytics Ops Center**.
A list of applications is displayed.

Step 3 Click the application name for which you want to view metrics; for example, **Assurance**.

A graphical representation of all existing collectors and pipelines in the application appears. CPU or throughput values corresponding to each pipeline are also provided.

The current health status of each component is indicated by its color:

- Red: error
- Yellow: warning
- Gray: normal operation

Step 4 To view historical data of pipelines, click **Timeline & Events**.

A timeline bar providing data for the time interval appears. You can also:

- Move the timeline slider to view data for a specific time.
- Hover your cursor over an event in the timeline bar to display additional details or a group of events that occurred at the same time.
- Click an event to display the Analytics Ops Center visualization at that particular time.

Step 5 To view additional details to help you troubleshoot an issue and determine the cause of an error or warning, click a collector name.

A slide-in pane appears with the following tabs:

- **Metrics**: Provides a selection of available metrics gathered during the last 30 minutes. It displays summary information indicating the component status, start and stop time, and error exceptions. You can also choose a different time interval.
- **Grafana**: Displays a dashboard associated with the respective component for deeper debugging.

Step 6 To view whether data is flowing through a specific pipeline, click a pipeline stream.

A slide-in pane appears with graphs. The graphs display whether the application is receiving data from the underlying pipelines. The graph information is based on the time interval you select from the drop-down list in the slide-in pane. Options are **Last 30 Min**, **Last Hour**, **Last 2 Hours**, and **Last 6 Hours**. The default is **Last 30 Min**.

Step 7 If a pipeline is not flowing at normal levels, hover your cursor over the stream to display the lag metrics.

Step 8 To view detailed information for a specific pipeline, click a pipeline name.

The appropriate *Pipeline* page displays with the following tabs:

Note Make sure to click the **Exceptions** tab to determine if any exceptions occurred in the pipeline. Under normal working conditions, this tab displays **null**.

- **Metrics**: Displays metrics, updated every 30 minutes in a graph.
- **Summary**: Displays summary information such as stats, run-time, and manifest.
- **Exceptions**: Displays any exceptions that occurred on the pipeline.
- **Stages**: Displays the pipeline stages.

Step 9 To change the metrics displayed on the Analytics Ops Center page, click **Key Metrics**, select up to two metrics, and then click **Apply**.

By default, Cisco DNA Center displays CPU and Throughput metrics.

Step 10 To view metrics for a particular flow, do the following:

a) Click **View Flow Details**.
b) Select three connected components (collector, pipeline, and store) by clicking the tilde (~) on the component's top-left corner.
c) Click **View Flow**.
Cisco DNA Center displays the metrics associated with that specific flow.

View or Update Collector Configuration Information

Collectors collect a variety of network telemetry and contextual data in real time. As data is ingested, Cisco DNA Center correlates and analyzes the data. You can view the status of collectors and quickly identify any problem areas.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Data Platform**.

Step 2 Click **Collectors**. The colored dot next to each collector indicates its overall status.

Step 3 To view additional details, click a collector name.

The appropriate *Collector* page appears. By default, Cisco DNA Center displays the **Configurations** tab which displays the list of current configurations.

Step 4 To view, update, or delete a configuration, click a specific configuration name.

Step 5 To add a new configuration, click **+ Add** in the **Configurations** tab.

A slide-in pane appears.

Step 6 In the slide-in pane, enter the required information for the configuration.

Step 7 (Optional) You can anonymize its data for some collectors such as **WIRELESSCOLLECTOR**, by checking the **Anonymize** check box.

Note When you check the **Anonymize** check box, the host name and user ID in the **Client Health** window is scrambled with one-way hash that cannot be decrypted.

Important If you want to anonymize your data, make sure that you check the **Anonymize** check box before you discover devices with the **Discovery** tool. If you anonymize the data after you discovered devices, the new data coming into the system is anonymized but the existing data will not be anonymized.

Step 8 Click **Save Configuration**.

Step 9 To view configured instances, click the **Instances** tab.

Step 10 To view summary information and metrics, choose an instance from the list.

Step 11 (Optional) If Cisco DNA Center integrates with Cisco Connected Mobile Experience (CMX), you have the option of anonymizing data on the CMX side. Do the following:

a) Using an SSH client, log in to Cisco CMX as the cmxadmin CLI user.

b) Change to the root user.

c) Go to `/opt/cmx/etc/node.conf` and under `[location]`, add **`user_options`**. For example:

```
[location]
…
user_options=-Dhideusername=true
```

d) On the Cisco CMX CLI, enter the following commands:

```
cmxctl agent restart
cmxctl location restart
```

View Data Retention Settings

You can view how long data is stored for an application.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Data Platform**.

Step 2 Click **Store Settings**.

Step 3 To view a list of historical purge jobs that have completed, click **Data Purge Schedule**.

The **HISTORY** table lists the name of the purge job, the result, time, and other data. You can sort, filter, and export data in the table.

Step 4 To view the current data retention and purge settings, click **Data Retention & Purge Configuration**. The following is displayed:

- **Document Store**: Settings for all time-based data, such as the maximum size and the low and high watermark threshold.

- **Metric Graph Store**: Settings for all time-based graphical data, such as the maximum size and the low and high watermark threshold.

View Pipeline Status

Data pipelines allow Cisco DNA Center applications to process streaming data. A data pipeline encapsulates an entire series of computations that accepts input data from external sources, transforms that data to provide useful intelligence, and produces output data. You can view the status of pipelines and quickly identify any problem areas.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Data Platform**.

Step 2 Click **Pipelines**.

Step 3 To view whether the application is receiving data from the underlying pipelines, click a pipeline name.

The appropriate *Pipeline* page displays with the following tabs:

Note Make sure to click the **Exceptions** tab to determine if any exceptions have occurred in the pipeline. Under normal working conditions, this tab displays **null**.

- **Metrics**: Displays metrics, updated every 30 minutes in a graph.
- **Summary**: Displays summary information such as stats, run-time, and manifest.
- **Exceptions**: Displays any exceptions that have occurred on the pipeline.
- **Stages**: Displays the pipeline stages.