## CONTENTS

### CHAPTER 1

**New and Changed Information**  
New and Changed Information 1

### CHAPTER 2

**Get Started with Cisco DNA Center** 3

- About Cisco DNA Center 3
- Log In 3
- Log In for the First Time as a Network Administrator 4
- Default Home Page 5
- Use Global Search 8
- Enable Localization 9
- Where to Start 10

### CHAPTER 3

**Discover Your Network** 11

- About Discovery 11
- Discovery Dashboard 12
- Discovery Prerequisites 12
- Discovery Credentials 13
  - Discovery Credentials and Cisco ISE 13
  - Guidelines and Limitations for Discovery Credentials 13
  - Discovery Credentials Example 14
- Preferred Management IP Address 15
- Discovery Configuration Guidelines and Limitations 15
- Perform Discovery 16
  - Discover Your Network Using CDP 16
  - Discover Your Network Using an IP Address Range 21
  - Discover Your Network Using LLDP 25
Manage Discovery Jobs 31
   Stop and Start a Discovery Job 31
   Edit a Discovery Job 31
   Change Credentials in a Discovery Job 31
   Clone a Discovery Job 34
   Delete a Discovery Job 34
   View Discovery Job Information 35

CHAPTER 4

Manage Your Inventory 37
   About Inventory 37
   Inventory and Cisco ISE Authentication 38
   Display Information About Your Inventory 39
   Types of Devices in the Cisco DNA Center Inventory 41
      Manage Network Devices 42
         Add a Network Device 42
         Update Network Device Credentials 44
      Manage Compute Devices 47
         Add a Compute Device 47
         Update Compute Device Credentials 48
      Manage Meraki Dashboards 48
         Integrate Meraki Dashboard 48
         Update Meraki Dashboard Credentials 49
   Filter Devices 49
   Change Device Role (Inventory) 51
   Update a Device's Management IP Address 52
   Update Device Resync Interval 52
   Resync Device Information 53
   Delete a Network Device 53
   Launch Command Runner (Inventory) 54
   Use a CSV File to Import and Export Device Configurations 54
      Import Device Configurations from a CSV File 55
      Export Device Configurations 56
      Export Device Credentials 56
Create a Site in a Network Hierarchy 76
Export a Site Hierarchy from Cisco Prime Infrastructure and Import into Cisco DNA Center 77
Upload an Existing Site Hierarchy 78
Search the Network Hierarchy 79
Edit Sites 79
Delete Sites 80
Add Buildings 80
Edit a Building 80
Delete Buildings 81
Add a Floor to a Building 81
Edit a Floor 82
Monitor a Floor Map 82
Edit Floor Elements and Overlays 84
Guidelines for Placing Access Points 85
Add, Position, and Delete APs 85
Quick View of APs 87
Add, Position, and Delete Sensors 88
Add Coverage Areas 89
Create Obstacles 90
Location Region Creation 90
Guidelines for Placing Inclusion and Exclusion Areas on a Floor Map 90
Define an Inclusion Region on a Floor 91
Define an Exclusion Region on a Floor 91
Edit Location Regions 92
Delete Location Regions 92
Create a Rail 92
Place Markers 93
Floor View Options 93
View Options for Access Points 93
View Options for Sensors 95
View Options for Overlay Objects 95
Configure Map Properties 95
Configure Global Maps Properties 95
Data Filtering 96
Filter Access Point Data  96
Filter Sensor Data  96

Configure Global Wireless Settings  97
  Create SSIDs for an Enterprise Wireless Network  97
  Preshared Key Override  100
  Create SSIDs for a Guest Wireless Network  100
  Create a Guest Portal Page  104
  Create a Wireless Interface  105
  Create a Wireless Radio Frequency Profile  106
  Create a Wireless Sensor Device Profile  108
  About Cisco Connected Mobile Experiences Integration  108
  Create Cisco CMX Settings  109
  Configure Native VLAN for a Flex Group  110

Create Network Profiles  111
  Create Network Profiles for Routing and NFV  111
  Create Network Profiles for Switching  113
  Create Network Profiles for Wireless  113

About Global Network Settings  114

About Device Credentials  115
  CLI Credentials  115
  SNMPv2c Credentials  116
  SNMPv3 Credentials  116
  HTTPS Credentials  117

About Global Device Credentials  117
  Configure Global CLI Credentials  117
  Configure Global SNMPv2c Credentials  118
  Configure Global SNMPv3 Credentials  119
  Configure Global HTTPS Credentials  121

Guidelines for Editing Global Device Credentials  122

Edit Global Device Credentials  123

Associate Device Credentials to Sites  124

Configure IP Address Pools  124

Import IP Address Pools from IP Address Manager  125

Import IP Address Pools from CSV File  125
Contents

Reserve an IP Pool 126
Configure Service Provider Profiles 126
Configure Global Network Servers 127
Add Cisco ISE or Other AAA Servers 127
Configure Cisco WLC High Availability from Cisco DNA Center 128
  Prerequisites for Configuring Cisco Wireless Controller High Availability 129
  Configure Cisco Wireless Controller HA 129
  What Happens During or After the High Availability Process is Complete 130
  Commands to Configure and Verify High Availability 130

CHAPTER 8
Create Templates to Automate Device Configuration Changes 131
  About Template Editor 131
  Create Projects 131
  Create Templates 132
    Create a Regular Template 132
    Blacklisted Commands 134
    Sample Templates 134
  Create a Composite Template 134
  Edit Templates 135
    Template Simulation 136
  Template Form Editor 136
    Variable Binding 137
    Special Keywords 138
  Associate Templates to Network Profiles 140

CHAPTER 9
Run Diagnostic Commands on Devices 143
  About Command Runner 143
  Run Diagnostic Commands on Devices 143

CHAPTER 10
Configure Telemetry Profile 145
  About Telemetry 145
  Configure a Telemetry Profile 145
  Apply a Telemetry Profile to the Devices 146
  Update Telemetry Profiles to Use a New Cluster Virtual IP Address 147
## CHAPTER 11 Configure Policies

**Policy Overview** 151

**Policy Dashboard** 151

**Group-Based Access Control Policies** 152

- Workflow to Configure a Group-Based Access Control Policy 153
- Create a Group-Based Scalable Group 153
- Create a Group-Based Access Control Contract 154
- Edit or Delete a Group-Based Access Control Contract 154
- Create a Group-Based Access Control Policy 155
- Edit or Delete a Group-Based Access Control Policy 155
- Deploy a Group-Based Access Control Policy 156

**IP-Based Access Control Policies** 156

- Workflow to Configure an IP-Based Access Control Policy 157
- Configure Global Network Servers 157
- Create an IP Network Group 158
- Edit or Delete an IP Network Group 158
- Create an IP-Based Access Control Contract 159
- Edit or Delete an IP-Based Access Control Contract 159
- Create an IP-Based Access Control Policy 160
- Edit or Delete an IP-Based Access Control Policy 161
- Deploy an IP-Based Access Control Policy 161

**Application Policies** 162

- CVD-Based Settings in Application Policies 163
- Site Scope 163
- Applications and Application Sets 163
- Business-Relevance Groups 164
- Unidirectional and Bidirectional Application Traffic 164
- Consumers and Producers 165
- Marking, Queuing, and Dropping Treatments 165
- Custom Applications 167
- Favorite Applications 167
- Service Provider Profiles 168
- Queuing Profiles 170
Provision Your Network 201

Provisioning 201

Onboarding Devices with Plug and Play Provisioning 201

Controller Discovery Prerequisites 203

DHCP Controller Discovery 203

DNS Controller Discovery 205

Plug and Play Connect Controller Discovery 205

View Devices 206

Add or Edit a Device 208

Add Devices in Bulk 209

Register or Edit a Virtual Account Profile 209

Add Devices from a Smart Account 210
Provision a Device With Plug and Play 211
Provision a Switch or Router Device 212
Provision a Wireless or Sensor Device 213
Delete a Device 215
Reset a Device 215
Add a Device to a Site 216
Tag Devices 216
Tag Devices Using Rules 217
Edit Device Tags 218
Provisioning Devices 218
Provision a Cisco Wireless Controller 218
Provision Routing and NFV Profiles 221
Provision a Cisco AP—Day 1 AP Provisioning 222
Provision a Brownfield Device 223
N+1 High Availability 225
  Overview of N+1 High Availability 225
  Prerequisites for Configuring N+1 High Availability from Cisco DNA Center 226
  Configure N+1 High Availability from Cisco DNA Center 227
Configure and Provision a Cisco Catalyst 9800 Series Wireless Controller 229
Cisco Catalyst 9800 Series Wireless Controller Overview 229
Workflow to Configure a Cisco Catalyst 9800 Series Wireless Controller in Cisco DNA Center 231
Software Image Upgrade Support for Cisco Catalyst 9800 Series Wireless Controller 234
Information About High Availability 234
Configure High Availability for Cisco Catalyst 9800 Series Wireless Controller 235
Provision a Cisco Catalyst 9800 Series Wireless Controller 238
Configure and Provision a Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches 240
Supported Hardware Platforms 240
Preconfiguration 241
Workflow to Configure Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Switches 241
Provision Embedded Wireless on Cisco Catalyst 9000 Series Switches 243
Fabric in a Box with Catalyst 9800 Embedded Wireless on Cisco Catalyst 9000 Series Switches 246
New and Changed Information

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network hierarchy</td>
<td>When you select an area, building, or floor on the Network Hierarchy, Network Settings, or Provision page, the hierarchical selection is retained when you switch between these pages.</td>
<td>—</td>
</tr>
<tr>
<td>Design usability enhancement</td>
<td>The options under the Design menu are available as a drop-down list.</td>
<td>—</td>
</tr>
<tr>
<td>Policy usability enhancement</td>
<td>The options under the Policy menu are available as a drop-down list.</td>
<td>—</td>
</tr>
<tr>
<td>Inventory</td>
<td>From Cisco DNA Center 1.3, the Inventory feature is merged with the Provision page. If you are upgrading from Cisco DNA Center 1.2.x to 1.3, when you choose the Inventory tool from the Cisco DNA Center home page, you are prompted to move to the Provision Devices page. From the Provision Devices page, choose Actions &gt; Inventory to view and use the inventory features. If you have a fresh installation of Cisco DNA Center 1.3, from the Cisco DNA Center home page, click Provision. From the Provision Devices page, choose Actions &gt; Inventory to view and use the inventory features.</td>
<td>About Inventory, on page 37</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Where Documented</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>IPv6 support</td>
<td>You can now create and reserve IPv6 address pools in addition to IPv4 address pools.</td>
<td>Configure IP Address Pools, on page 124</td>
</tr>
<tr>
<td>Schedule Discovery</td>
<td>You can schedule discovery to a later time.</td>
<td>Discover Your Network Using CDP, on page 16</td>
</tr>
<tr>
<td>Include SSH key information in exported device credentials</td>
<td>You can include information such as SSH key and initial SSH key algorithm, in the exported device credentials.</td>
<td>Export Device Credentials, on page 56</td>
</tr>
<tr>
<td>ROMMON upgrade</td>
<td>When a device is added, the latest ROMMON details will be fetched from cisco.com for applicable devices. Also, when there is base image import or tagging of base image, ROMMON image will be automatically downloaded from cisco.com.</td>
<td>View Software Images, on page 60</td>
</tr>
<tr>
<td>Device upgrade readiness rechecks</td>
<td>Included few more rechecks such as IP Domain name, Startup config, NVFIS Flash, Service Entitlement, Interface, CDP neighbors, Running Config, Spanning Tree Summary, and AP Summary checks.</td>
<td>List of Device Upgrade Readiness Prechecks, on page 64</td>
</tr>
<tr>
<td>Add a device as an Edge, Border or Control plane</td>
<td>All actions of adding a device from the topology view will result in a slide-in window with a new tab called Fabric, where you can perform the actions.</td>
<td>Add a Device to a Fabric, on page 257</td>
</tr>
<tr>
<td>Details of the fabric displayed on the fabric dashboard</td>
<td>The Fabric dashboard (Provision &gt; Fabric) displays the number of sites, control planes, and borders for each fabric.</td>
<td>—</td>
</tr>
<tr>
<td>LAN Automation Enhancements</td>
<td>LAN Automation uses only the IPv4 subnet. LAN Automation validates the LAN subnet reachability from Cisco DNA Center. If the LAN IP Pool is not reachable, Cisco DNA Center displays an error message.</td>
<td>Provision a LAN Underlay, on page 249</td>
</tr>
<tr>
<td>View additional device details in Topology page</td>
<td>You can view additional device details such as device IP and device name suffix in the Topology page.</td>
<td>Display Device Information, on page 71</td>
</tr>
<tr>
<td>View all options available in the Topology page.</td>
<td>You can view the details of all options available in the Topology page, by clicking the Take a Tour link.</td>
<td>Display the Topology of Areas, Sites, Buildings, and Floors, on page 70</td>
</tr>
<tr>
<td>Support for Extended Node</td>
<td>Extended nodes are those devices that run in Layer 2 switch mode and do not support fabric technology natively. You can now configure extended nodes in a Cisco SD-Access fabric.</td>
<td>Configure an Extended Node, on page 262</td>
</tr>
<tr>
<td>Support for Port Channel</td>
<td>You can now create or delete port channels between the fabric edge ports and the extended node uplinks.</td>
<td>Configure a Port Channel, on page 264</td>
</tr>
</tbody>
</table>
Get Started with Cisco DNA Center

- About Cisco DNA Center, on page 3
- Log In, on page 3
- Log In for the First Time as a Network Administrator, on page 4
- Default Home Page, on page 5
- Use Global Search, on page 8
- Enable Localization, on page 9
- Where to Start, on page 10

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 Digital Network Architecture 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 NETWORK-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. For details, see Log In for the First Time as a Network Administrator, on page 4.

**Step 3**  
To log out, click the Gear icon (⚙️) at the top-right corner and click Sign Out.

---

**Log In for the First Time as a Network Administrator**

If your user ID has the NETWORK-ADMIN-ROLE assigned, and no other user with the same role has logged in before, you will be redirected to the Get Started wizard.

The wizard is a quick way to get immediate value from Cisco DNA Center. It consists of a few screens that collect information needed to discover and monitor the condition of your network devices, and then help you visualize your network's overall health using the Cisco DNA Center home page dashboard.

You can perform all of the same tasks the wizard does using other Cisco DNA Center features. Using the wizard does not prevent you from using those features. You can choose to skip the wizard entirely at any point and it will not be shown again for you. However, Cisco DNA Center will continue to display the wizard at login to any user with the same role until one such user completes the wizard steps. After that, Cisco DNA Center never displays the wizard again.

If you skipped the Get Started wizard, you can always revisit it from the Get Started link at the top-right of the home page.

**Before you begin**

You need to have the following information to complete the wizard:

- The IP addresses of your SYSLOG and SNMP servers
- The IP address and port of your Netflow server
- For discovery: The IP address to start from (if choosing CDP discovery) or the starting and ending IP addresses (if choosing Range discovery)
- Optional: Your preferred management IP address
- Device CLI credentials, including the Enable password
- SNMP v2c credentials, including the read community string

---

**Step 1**  
If you have not already done so, log in to Cisco DNA Center normally, as explained in Log In, on page 3.

You will be redirected to Get Started wizard if this is your first time login.

**Step 2**  
Click Get Started in the Getting Started wizard to continue device discovery or Exit to return to the Home page.

**Step 3**  
Enter the network properties for device discovery and click Save & Next.

Click Back to return to the previous screen.
Step 4 Specify the Discovery Type, Starting IP Address, and CLI Credentials. By default Device Controllability is enabled. You can click Disable to disable device controllability.

Step 5 When you are finished, click Begin Discovery. Cisco DNA Center displays the home page, which slowly fills with network health information as discovery completes.

Default Home Page

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

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 page.

- **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 page.

- **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 page.

- **Network Profiles**: Provides the number of profiles discovered on your network. Clicking Manage Profiles takes you to the Network Profiles page.

- **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 page.

- **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 page.

The Network Configuration area includes:

- **Design**: 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.

- **Policy**: 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.

- **Provision**: Prepare and configure devices, including adding devices to sites, assigning devices to the inventory, deploying the required settings and policies, creating fabric domains, and adding devices to the fabric.

- **Assurance**: Provide proactive and predictive actionable insights about the performance and health of the network infrastructure, applications, and end-user clients.

- **Platform**: Allows you to programmatically access your network through Intent APIs, integrate with your preferred IT systems to create end-to-end solutions and add support for multi-vendor devices.
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 dashboard. 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 icons at the top-right corner of the home page to perform important common tasks:

- **Software Updates:** See a list of available software updates. Click the Go to Software Updates link to view system and application updates.
- **Search:** Search for devices, users, hosts, and other items, anywhere they are stored in the Cisco DNA Center database. For tips on using Search, see Use Global Search, on page 8.
- **Tools:** Access the available tools.
- **Settings:** Configure system settings, view audit logs, see the logged in username, and log out.
- **Help:**
  - **About:** Display the current Cisco DNA Center software version.
  - **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.
  - **Make a Wish:** Submit your comments and suggestions to the Cisco DNA Center product team.
- **Notifications:** See recently scheduled tasks and other notifications.
The notification icon may show a color badge next to it. The badge indicates a change in tasks or notifications. A blue badge indicates new notifications, new tasks, or successful tasks. A red badge indicates failed tasks.

If you are new to Cisco DNA Center, see Where to Start, on page 10 for tips and suggestions on how to begin.

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 Users > User Management, 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.
- **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.
- **Sites**: Search for them by name.
- **Users**: Search for them 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 the item you are looking for.

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 in the list. 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 of categories and items.

The summary panel includes links to more information. The link varies as appropriate for each category and item. For example, with Activities, the summary panel displays links to menu items and workflows elsewhere in the Cisco DNA Center system. For Applications, there is the Application 360 view. You will see links to Client 360 and Topology views for hosts and endpoints, and links to Device 360 and Topology views for network devices. Click the link to see the appropriate menu item, workflow, or detail view.

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

Global search can display a maximum of 500 results at a time.

### Enable Localization

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

**Note**

While most screens—including the home page, tools, online help, and REST APIs—are localized, the Assurance screens are not localized.

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.

**Step 2**

Log in to Cisco DNA Center.

The GUI screens are shown in the selected language.
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. For information about running Discovery, see Discover Your Network, on page 11.

- New or nonexisting infrastructure: If you have no existing infrastructure and are starting from scratch (greenfield deployment), create a network hierarchy.
Discover Your Network

• About Discovery, on page 11
• Discovery Dashboard, on page 12
• Discovery Prerequisites, on page 12
• Discovery Credentials, on page 13
• Preferred Management IP Address, on page 15
• Discovery Configuration Guidelines and Limitations, on page 15
• Perform Discovery, on page 16
• Manage Discovery Jobs, on page 31

About Discovery

The Discovery feature scans the devices in your network and sends the list of discovered devices to Inventory. The Discovery 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. For more information about Device Controllability, see the Cisco Digital Network Architecture Center Administrator Guide.

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.
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.

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**

From the Cisco DNA Center home page, choose Tools > Discovery to view the Discovery Dashboard. The Discovery Dashboard shows the inventory overview, latest discovery, discovery type, discovery status, and the 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 maximum network latency between Cisco DNA Center and devices is 50 ms.
- 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 13.
- 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 two criteria are 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 15.
- Configure anonymization. Anonymization scrambles the hostname and userid fields. For more information, see View or Update Collector Configuration Information, on page 275.
If you anonymize the data after you have run Discovery, the new data coming into the system will get anonymized but the existing data will not get anonymized.

**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:

- Standard Cisco devices: CLI and SNMP credentials.
- NFVIS devices: HTTP(S) credentials.
- Both standard and NFVIS devices: 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 define up to five saved 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 127.

**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 31.

• 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 rerun 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 re-run the Discovery job.

• If an ongoing Discovery polling cycle fails because of a device authentication failure, you can correct the situation using one of the 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 rerun 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 re-run the 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. For example, 25 minutes after you delete the credential, Discovery jobs that use it will fail.

### 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 logs one of the device's IP addresses as the preferred management IP address for the device. The IP address can be that of a built-in management interface of the device, or another physical interface, or a logical interface like Loopback0. You can configure Cisco DNA Center to log the device's loopback IP address as the preferred management IP address, provided the IP address is reachable from Cisco DNA Center.

If you choose to use a device's loopback IP address 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 52.

---

**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 21 and Discover Your Network Using LLDP, on page 25.

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 that they are connected to.

Before you begin

- Enable CDP on your network devices.
- Configure your network devices, as described in Discovery Prerequisites, on page 12.
- 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

From the Cisco DNA Center home page, click Discovery.

Step 2

In the Discovery Name field, enter a name.

Step 3

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 the [Preferred Management IP Address](#), on page 15.

  **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 4**

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

d) Click **SNMP v2c** and configure the following fields:
Table 3: SNMPv2c Credentials

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

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

Table 4: SNMPv3 Credentials

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Description</td>
<td>Name or description of the SNMPv3 settings that you are adding.</td>
</tr>
<tr>
<td>Username</td>
<td>Name associated with the SNMPv3 settings.</td>
</tr>
<tr>
<td>Mode</td>
<td>Security level that an SNMP message requires. Choose one of the following modes:</td>
</tr>
<tr>
<td></td>
<td>• noAuthNoPriv: Does not provide authentication or encryption.</td>
</tr>
<tr>
<td></td>
<td>• AuthNoPriv: Provides authentication, but does not provide encryption.</td>
</tr>
<tr>
<td></td>
<td>• AuthPriv: Provides both authentication and encryption.</td>
</tr>
<tr>
<td>Auth Type</td>
<td>Authentication type to be used. (Enabled if you select AuthPriv or AuthNoPriv as the authentication mode.) Choose one of the following authentication types:</td>
</tr>
<tr>
<td></td>
<td>• SHA: Authentication based on HMAC-SHA.</td>
</tr>
<tr>
<td></td>
<td>• MD5: Authentication based on HMAC-MD5.</td>
</tr>
</tbody>
</table>
SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least 8 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. (Enabled if you select AuthPriv as the authentication mode.) Choose one of the following privacy types:
- **DES**: DES 56-bit (DES-56) encryption in addition to authentication based on the CBC DES-56 standard.
- **AES128**: CBC mode AES for encryption.
- **None**: No privacy.

SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support DES or AES128 encryption. Passwords (or passphrases) must be at least 8 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.

### Table 5: SNMP Properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Retries</strong></td>
<td>Number of times Cisco DNA Center tries to communicate with network devices using SNMP.</td>
</tr>
<tr>
<td><strong>Timeout</strong></td>
<td>Number of seconds between retries.</td>
</tr>
</tbody>
</table>

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

(Optional) Click **HTTP(S)** and configure the following fields:
Table 6: HTTP(S) Credentials

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Specifies the kind of HTTPS credentials you are configuring. Valid types are Read or Write.</td>
</tr>
</tbody>
</table>

**Read**

- You can configure up to 5 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.
  - **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).

**Note**
The password must contain at least one lowercase, one uppercase, one digit, and a special character and must not contain <>@',;:! or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.

**Write**

- You can configure up to 5 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.
  - **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).

**Note**
The password must contain at least one lowercase, one uppercase, one digit, and a special character and must not contain <>@',;:! or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.

---

**Step 5** (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 6**

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 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 16 and Discover Your Network Using LLDP, on page 25.

**Before you begin**

Your devices must have the required device configurations, as described in Discovery Prerequisites, on page 12.

**Step 1**

From the Cisco DNA Center home page, click Discovery.

**Step 2**

In the Discovery Name field, enter a name.

**Step 3**

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

a) For Discovery Type, click 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) 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 15.

**Step 4**

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>
<thead>
<tr>
<th>Table 7: CLI Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
</tr>
<tr>
<td>-------------------------</td>
</tr>
<tr>
<td>Name/Description</td>
</tr>
<tr>
<td>Username</td>
</tr>
</tbody>
</table>
| Password                | Password that is used to log in to the CLI of the devices in your network.  
For security reasons, enter the password again 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, enter the enable password again.  
Note: Passwords are encrypted for security reasons and are not displayed in the configuration. |

d) Click SNMP v2c and configure the following fields:

<table>
<thead>
<tr>
<th>Table 8: SNMPv2c Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
</tr>
<tr>
<td>-------------------------</td>
</tr>
<tr>
<td>Read</td>
</tr>
</tbody>
</table>
• 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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Description</td>
<td>Name or description of the SNMPv3 settings that you are adding.</td>
</tr>
<tr>
<td>Username</td>
<td>Name associated with the SNMPv3 settings.</td>
</tr>
<tr>
<td>Mode</td>
<td>Security level that an SNMP message requires. Choose one of the following modes:</td>
</tr>
<tr>
<td></td>
<td>• noAuthNoPriv: Does not provide authentication or encryption.</td>
</tr>
<tr>
<td></td>
<td>• AuthNoPriv: Provides authentication, but does not provide encryption.</td>
</tr>
<tr>
<td></td>
<td>• AuthPriv: Provides both authentication and encryption.</td>
</tr>
<tr>
<td>Auth Type</td>
<td>Authentication type to be used. (Enabled if you select AuthPriv or AuthNoPriv as the authentication mode.) Choose one of the following authentication types:</td>
</tr>
<tr>
<td></td>
<td>• SHA: Authentication based on HMAC-SHA.</td>
</tr>
<tr>
<td></td>
<td>• MD5: Authentication based on HMAC-MD5.</td>
</tr>
<tr>
<td>Auth Password</td>
<td>SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least 8 characters in length.</td>
</tr>
<tr>
<td>Note</td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
<tr>
<td>Privacy Type</td>
<td>Privacy type. (Enabled if you select AuthPriv as the authentication mode.) Choose one of the following privacy types:</td>
</tr>
<tr>
<td></td>
<td>• DES: DES 56-bit (DES-56) encryption in addition to authentication based on the CBC DES-56 standard.</td>
</tr>
<tr>
<td></td>
<td>• AES128: CBC mode AES for encryption.</td>
</tr>
<tr>
<td></td>
<td>• None: No privacy.</td>
</tr>
</tbody>
</table>
SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support DES or AES128 encryption. Passwords (or passphrases) must be at least 8 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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Password</td>
<td>SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support DES or AES128 encryption. Passwords (or passphrases) must be at least 8 characters long.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retries</td>
<td>Number of times Cisco DNA Center tries to communicate with network devices using SNMP.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Number of seconds between retries.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Specifies the kind of HTTPS credentials you are configuring. Valid types are <strong>Read</strong> or <strong>Write</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read</td>
<td>You can configure up to 5 HTTPS read credentials:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name/Description</strong>: Name or description of the HTTPS credentials that you are adding.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Username</strong>: Name used to authenticate the HTTPS connection.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Password</strong>: Password used to authenticate the HTTPS connection.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Port</strong>: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).</td>
</tr>
</tbody>
</table>

**Note** The password must contain at least one lower case, one upper case, one digit, and a special character and must not contain `< > @ ` ; ` !` or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.
You can configure up to 5 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.
- **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).

**Note**: The password must contain at least one lower case, one upper case, one digit, and a special character and must not contain `< > @ , ; !` or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.

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 5** (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 6** 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 16 and Discover Your Network Using an IP Address Range, on page 21.
Discover Your Network Using LLDP

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 that they are connected to.

Before you begin
• Enable LLDP on your network devices.
• Configure your network devices, as described in Discovery Prerequisites, on page 12.
• 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
From the Cisco DNA Center home page, click Discovery.

Step 2
In the Discovery Name field, enter a name.

Step 3
Expand the IP Address/Range area if it is not already visible, 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
Choose to or choose to 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 15.

g) 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 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 15.

**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 4** 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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Description</td>
<td>Name or phrase that describes the CLI credentials.</td>
</tr>
<tr>
<td>Username</td>
<td>Name that is used to log in to the CLI of the devices in your network.</td>
</tr>
<tr>
<td>Password</td>
<td>Password that is used to log in to the CLI of the devices in your network.</td>
</tr>
<tr>
<td></td>
<td>For security reasons, enter the password again as confirmation.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
<tr>
<td>Enable Password</td>
<td>Password used to move to a higher privilege level in the CLI. Configure this password only if your network devices require it.</td>
</tr>
<tr>
<td></td>
<td>For security reasons, enter the enable password again.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read</td>
<td><strong>Name/Description</strong>—Name or description of the SNMPv2c settings that you are adding.</td>
</tr>
<tr>
<td></td>
<td><strong>Read Community</strong>—Read-only community string password used only to view SNMP information on the device.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
</tbody>
</table>
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.

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

### Table 14: SNMPv3 Credentials

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Description</td>
<td>Name or description of the SNMPv3 settings that you are adding.</td>
</tr>
<tr>
<td>Username</td>
<td>Name associated with the SNMPv3 settings.</td>
</tr>
</tbody>
</table>
| 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 8 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:

- **DES**: DES 56-bit (DES-56) encryption in addition to authentication based on the CBC DES-56 standard.
- **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 DES or AES128 encryption. Passwords (or passphrases) must be at least 8 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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retries</td>
<td>Number of times Cisco DNA Center tries to communicate with network devices using SNMP.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Number of seconds between retries.</td>
</tr>
</tbody>
</table>

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

**Table 16: HTTP(S) Credentials**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Specifies the kind of HTTPS credentials you are configuring. Valid types are <strong>Read</strong> or <strong>Write</strong>.</td>
</tr>
</tbody>
</table>
You can configure up to 5 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.
- **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).

**Note**  
The password must contain at least one lowercase, one uppercase, one digit, and one special character and must not contain `< > @ ', : ! or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.

You can configure up to 5 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.
- **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).

**Note**  
The password must contain at least one lowercase, one uppercase, one digit, and one special character and must not contain `< > @ ', : ! or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.

**Step 5**  
(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 6**  
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  From the Cisco DNA Center home page, click Discovery.

Step 2  To stop an active Discovery job, perform these steps:
  a) From the Discoveries pane, select the corresponding Discovery job.
  b) Click Stop.

Step 3  To restart an inactive Discovery job, perform these steps:
  a) From the Discoveries pane, select the corresponding Discovery job.
  b) Click Re-discover to restart the selected discover job.

Edit a Discovery Job

You can edit a Discovery job and then rerun the Discovery job.

Before you begin

You should have created at least one Discovery job.

Step 1  From the Cisco DNA Center home page, click Discovery.

Step 2  From the Discoveries pane, select the Discovery job.

Step 3  Click Edit.

Step 4  Depending on the Discovery type, you can change the type of Discovery 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 16.
  • IP Range—Discovery name, Discovery 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 21.
  • LLDP—Discovery name, Discovery type, IP address. For more information about the fields you can change, see Discover Your Network Using LLDP, on page 25.

Step 5  Click Start.

Change Credentials in a Discovery Job

You can change the credentials used in a Discovery job and then rerun the Discovery job.
Before you begin

You should have created at least one Discovery job.

Step 1  From the Cisco DNA Center homepage, click **Discovery**.

Step 2  From the **Discoveries** pane, select the Discovery job.

Step 3  Click **Edit**.

Step 4  Expand the **Credentials** area.

Step 5  Deselect the credentials that you do not want to use.

Step 6  Configure the credentials that you want to use:

a) Click **Add Credentials**.

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

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read</td>
<td><strong>Name/Description</strong>—Name or description of the SNMPv2c settings that you are adding.</td>
</tr>
<tr>
<td></td>
<td><strong>Read Community</strong>—Read-only community string password used only to view SNMP information on the device.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
</tbody>
</table>
d) (Optional) Click **SNMP v3** and configure the following fields:

### Table 19: SNMPv3 Credentials

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Description</td>
<td>Name or description of the SNMPv3 settings that you are adding.</td>
</tr>
<tr>
<td>Username</td>
<td>Name associated with the SNMPv3 settings.</td>
</tr>
<tr>
<td>Mode</td>
<td>Security level that an SNMP message requires. Choose one of the following modes:</td>
</tr>
<tr>
<td></td>
<td>- <strong>noAuthNoPriv</strong>: Does not provide authentication or encryption.</td>
</tr>
<tr>
<td></td>
<td>- <strong>AuthNoPriv</strong>: Provides authentication, but does not provide encryption.</td>
</tr>
<tr>
<td></td>
<td>- <strong>AuthPriv</strong>: Provides both authentication and encryption.</td>
</tr>
<tr>
<td>Auth Type</td>
<td>Authentication type to be used. (Enabled if you select <strong>AuthPriv</strong> or <strong>AuthNoPriv</strong> as the authentication mode.) Choose one of the following authentication types:</td>
</tr>
<tr>
<td></td>
<td>- <strong>SHA</strong>: Authentication based on HMAC-SHA.</td>
</tr>
<tr>
<td></td>
<td>- <strong>MD5</strong>: Authentication based on HMAC-MD5.</td>
</tr>
<tr>
<td>Auth Password</td>
<td>SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least 8 characters in length.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> • 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.</td>
</tr>
<tr>
<td></td>
<td>• Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
</tbody>
</table>
Clone a Discovery Job

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

Before you begin

You should have run at least one Discovery job.

Step 1
From the Cisco DNA Center home page, click Discovery.

Step 2
From the Discoveries pane, select the Discovery job.

Step 3
Click Clone & Edit.

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

Step 4
(Optional) Change the name of the Discovery job.

Step 5
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.
**Before you begin**

You should have run at least one Discovery job.

---

**Step 1**
From the Cisco DNA Center home page, click **Discovery**.

**Step 2**
From the **Discoveries** pane, select the Discovery job that you want to delete.

**Step 3**
Click **Delete**.

**Step 4**
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 can also 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**
From the Cisco DNA Center home page, click **Discovery**.

**Step 2**
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 3**
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.
View Discovery Job Information
CHAPTER 4

Manage Your Inventory

- About Inventory, on page 37
- Inventory and Cisco ISE Authentication, on page 38
- Display Information About Your Inventory, on page 39
- Types of Devices in the Cisco DNA Center Inventory, on page 41
- Filter Devices, on page 49
- Change Device Role (Inventory), on page 51
- Update a Device's Management IP Address, on page 52
- Update Device Resync Interval, on page 52
- Resync Device Information, on page 53
- Delete a Network Device, on page 53
- Launch Command Runner (Inventory), on page 54
- Use a CSV File to Import and Export Device Configurations, on page 54

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. For more information about Device Controllability, see the Cisco Digital Network Architecture Center Administrator Guide.

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 12.

After the initial discovery, Cisco DNA Center maintains the inventory by polling the devices at regular intervals. The default and minimum interval is every 25 minutes. However, you can change this interval up to 24 hours, as required for your network environment. For more information, see Update Device Resync Interval.
Polling occurs for each device, link, host, and interface. Only the devices that have been active for less than a day are displayed. This prevents stale device data, if any, from being displayed. On an average, polling 500 devices takes approximately 20 minutes.

From Cisco DNA Center 1.3, the **Inventory** feature is merged with the **Provision** page.

If you have upgraded from Cisco DNA Center 1.2.x to Cisco DNA Center 1.3, choose the **Inventory** tool from the Cisco DNA Center home page. You will be prompted to move to the **Provision Devices** page. From the **Provision Devices** page, choose **Actions > Inventory** to view and execute the inventory features.

## 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 of this, 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 127.

  **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 you troubleshoot issues related to the Cisco DNA Center and Cisco ISE inventories. For more information about the Cisco DNA Center audit logs, see the [Cisco Digital Network Architecture Center Administrator Guide](#).

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 13.

- If required, you can use Cisco ISE to enforce access control to groups of devices. For information about this use case, see the [Cisco Digital Network Architecture Center Administrator Guide](#).
Display Information About Your Inventory

The Inventory table displays information for each discovered device. All of the columns, except the Config column, support sorting. Click the column header to sort the rows in ascending order. Click the column header again to sort the rows in descending order.

Before you begin

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

From the Cisco DNA Center home page, click Provision.

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

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Name of the device.</td>
</tr>
<tr>
<td></td>
<td>Click the name to display a dialog box with the following information:</td>
</tr>
<tr>
<td></td>
<td>• Details: Displays details such as Device Name, Device type, IP address, Serial number, software image and so on.</td>
</tr>
<tr>
<td></td>
<td>• Configuration: displays detailed configuration information similar to what is displayed in the output of the show running-config command.</td>
</tr>
<tr>
<td></td>
<td>Note: This feature is not supported for access points (APs) and wireless controllers. Therefore, configuration data is not returned for these device types.</td>
</tr>
<tr>
<td></td>
<td>• Interface: Displays Interface Name, MAC Address, and Status of the interfaces on the device.</td>
</tr>
<tr>
<td></td>
<td>• Stack: Displays MAC Address, Role, State and Priority.</td>
</tr>
<tr>
<td></td>
<td>• Run Commands: Opens Command Runner to execute CLI commands on the device.</td>
</tr>
<tr>
<td></td>
<td>• View 360: Displays 360 page. For 360 to open, you must have the Assurance application installed.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the device.</td>
</tr>
</tbody>
</table>
### Column | Description
--- | ---
Reachability | The following is a list of the various statuses:

- **Connecting**: Cisco DNA Center is connecting to the device.

- **Reachable**: Cisco DNA Center has connected to the device and is able to execute Cisco commands using the CLI.

  **Note**: A failure indicates that Cisco DNA Center is connected to the device, but is unable to execute Cisco commands using the CLI. This status usually indicates that the device is not a Cisco device.

- **Authentication Failed**: Cisco DNA Center has connected to the device, but is unable to determine what type of device it is.

- **Unreachable**: Cisco DNA Center is unable to connect to the device.

  **Note**: Sometimes a device is unreachable because the Discovery job does not have its credentials or the Discovery job has the wrong credentials. If you suspect this might be the case, run a new Discovery job and make sure to specify the device's correct credentials.

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**
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.

For a complete list of supported devices, see the Cisco Digital Network Architecture Center Supported Devices document.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site</td>
<td>The site to which the device is assigned. Click <strong>Assign</strong> if the device is not assigned to any site. Click <strong>Choose a Site</strong>, select a site from the hierarchy and click <strong>Save</strong>. For more information, see About Network Hierarchy, on page 76.</td>
</tr>
<tr>
<td>Last Updated</td>
<td>Most recent date and time that Cisco DNA Center scanned the device and updated the database with new information about the device.</td>
</tr>
<tr>
<td>Device Family</td>
<td>Group of related devices, such as routers, switches and hubs, or wireless controllers.</td>
</tr>
<tr>
<td>Device Series</td>
<td>Series number of the device, for example, Cisco Catalyst 4500 Series Switches.</td>
</tr>
<tr>
<td>Resync Interval</td>
<td>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 the Cisco Digital Network Architecture Center Administrator Guide.</td>
</tr>
<tr>
<td>Last Sync Status</td>
<td>Status of the last Discovery scan for the device:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Managed</strong>: Device is in a fully managed state.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Partial Collection Failure</strong>: Device is in a partial collected state and not all the inventory information has been collected. Move the cursor over the <strong>Information</strong> (i) icon to display additional information about the failure.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unreachable</strong>: Device cannot be reached and no inventory information was collected due to device connectivity issues. This condition occurs when periodic collection takes place.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Wrong Credentials</strong>: If device credentials are changed after adding the device to the inventory, this condition is noted.</td>
</tr>
<tr>
<td></td>
<td>• <strong>In Progress</strong>: Inventory collection is occurring.</td>
</tr>
</tbody>
</table>
• **Meraki Dashboard**—Dashboard to the Cisco cloud management platform for managing Cisco Meraki products.

## Manage Network Devices

### Add a Network Device

You can add a network device to your inventory manually.

**Step 1**
From the Cisco DNA Center home page, click **Provision**.

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 **Network Device**.

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

**Step 5**
Expand the **SNMP** area, if it is not already visible.

**Step 6**
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 21: SNMPv2c Credentials**

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

| 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 22: SNMPv3 Credentials**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Description</td>
<td>Name or description of the SNMPv3 settings that you are adding.</td>
</tr>
<tr>
<td>Username</td>
<td>Name associated with the SNMPv3 settings.</td>
</tr>
</tbody>
</table>
### 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 8 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:
- **DES**: DES 56-bit (DES-56) encryption in addition to authentication based on the CBC DES-56 standard.
- **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 DES or AES128 encryption. Passwords (or passphrases) must be at least 8 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 7
Expand the **SNMP RETRIES AND TIMEOUT** area, if it is not already expanded, and configure the following fields.
Table 23: SNMP Properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retries</td>
<td>Number of attempts allowed to connect to the device. Valid values are from 1 to 3. The default is 3.</td>
</tr>
<tr>
<td>Timeout</td>
<td>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.</td>
</tr>
</tbody>
</table>

Step 8  
Expand the CLI area, if it is not already expanded, and configure the following fields:

Table 24: CLI Credentials

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Network protocol that enables Cisco DNA Center to communicate with remote devices. Valid values are SSH2 or Telnet. If you plan to configure the NETCONF port (see Step 9), choose SSH2 as the network protocol.</td>
</tr>
<tr>
<td>Username</td>
<td>Name that is used to log in to the CLI of the devices in your network.</td>
</tr>
</tbody>
</table>
| Password | Password that is used to log in to the CLI of the devices in your network. For security reasons, enter the password again 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, enter the enable password again.  
  **Note** Passwords are encrypted for security reasons and are not displayed in the configuration. |

Step 9  
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 10  
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  From the Cisco DNA Center homepage, click **Provision**.
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, select **Network Device** from the **Type** drop-down field, if it is not already selected.

Step 5  Expand the **SNMP** area, if it is not already expanded.

Step 6  From the **Version** field, choose the SNMP version (V2C or V3).

**Note**  Because both the SNMP and CLI credentials are updated together, we recommend that you provide both credentials. If you provide only SNMP credentials, Cisco DNA Center saves only the SNMP credentials, and the CLI credentials are not updated.

Step 7  Depending on the whether you choose V2C or V3, enter information in the remaining fields, which are described in the following tables.

**Table 25: SNMPv2c Credentials**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read</td>
<td></td>
</tr>
<tr>
<td>Name/Description</td>
<td>Name or description of the SNMPv2c settings that you are adding.</td>
</tr>
<tr>
<td>Read Community</td>
<td>Read-only community string password used only to view SNMP information on the device.</td>
</tr>
</tbody>
</table>

**Note**  Passwords are encrypted for security reasons and are not displayed in the configuration.

<table>
<thead>
<tr>
<th>Write</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Description</td>
<td>Name or description of the SNMPv2c settings that you are adding.</td>
</tr>
<tr>
<td>Write Community</td>
<td>Write community string used to make changes to the SNMP information on the device.</td>
</tr>
</tbody>
</table>

**Note**  Passwords are encrypted for security reasons and are not displayed in the configuration.

**Table 26: SNMPv3 Credentials**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Description</td>
<td>Name or description of the SNMPv3 settings that you are adding.</td>
</tr>
<tr>
<td>Username</td>
<td>Name associated with the SNMPv3 settings.</td>
</tr>
<tr>
<td>Mode</td>
<td>Security level that an SNMP message requires. Choose one of the following modes:</td>
</tr>
<tr>
<td></td>
<td>- noAuthNoPriv: Does not provide authentication or encryption.</td>
</tr>
<tr>
<td></td>
<td>- AuthNoPriv: Provides authentication, but does not provide encryption.</td>
</tr>
<tr>
<td></td>
<td>- AuthPriv: Provides both authentication and encryption.</td>
</tr>
</tbody>
</table>
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 8 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:
- DES: DES 56-bit (DES-56) encryption in addition to authentication based on the CBC DES-56 standard.
- 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 DES or AES128 encryption. Passwords (or passphrases) must be at least 8 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 complete the following fields:

Table 27: SNMP Properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retries</td>
<td>Number of attempts allowed to connect to the device. Valid values are from 1 to 3. The default is 3.</td>
</tr>
</tbody>
</table>
**Table 28: CLI Credentials**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Protocol</strong></td>
<td>Network protocol that enables Cisco DNA Center to communicate with remote devices. Valid values are <strong>SSH2</strong> or <strong>Telnet</strong>. If you plan to configure the NETCONF port (see next step), you need to choose <strong>SSH2</strong> as the network protocol.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>Name that is used to log in to the CLI of the devices in your network.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Password that is used to log in to the CLI of the devices in your network.</td>
</tr>
<tr>
<td></td>
<td>For security reasons, enter the password again as confirmation.</td>
</tr>
<tr>
<td><strong>Enable Password</strong></td>
<td>Password used to move to a higher privilege level in the CLI.</td>
</tr>
<tr>
<td></td>
<td>For security reasons, enter the enable password again.</td>
</tr>
</tbody>
</table>

**Step 9**
Expand the **CLI** area, if it is not already expanded, and complete the following fields:

**Note** Both the SNMP and CLI credentials are updated together, so you need to provide both credentials. If you provide only SNMP credentials, Cisco DNA Center saves only the SNMP credentials. The CLI credentials are not updated.

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

**Step 11**
Click **Update**.

---

### 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  From the Cisco DNA Center home page, click Provision.
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 / Name field, enter the IP address or name of the device.

Step 5  Expand the HTTP(S) area, if it is not already visible and configure the following fields:
   • 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  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  From the Cisco DNA Center home page, click Provision.
The Inventory page displays the device information 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, choose Compute Device from the Type drop-down list.

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  Click Update.

Manage Meraki Dashboards

Integrate Meraki Dashboard

You can integrate your Meraki dashboard with Cisco DNA Center.
**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**
From the Cisco DNA Center home page, click **Provision**.

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

**Step 2**
Click **Add Device**.

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

**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 used to access the Meraki dashboard.

Cisco DNA Center collects inventory data from the Meraki dashboard and displays the information.

---

**Manage Your Inventory**

**Update Meraki Dashboard Credentials**

**Step 1**
From the Cisco DNA Center home page, click **Provision**.

The Inventory page displays the device information 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, choose **Meraki Dashboard** from the **Type** drop-down list.

**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**
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** From the Cisco DNA Center home page, click **Provision**.
The Inventory page displays the device information gathered during the Discovery process.

**Step 2** Click **Filter**.
The following filters are displayed:
- Tag
- Device Name
- IP Address
- Device Family
- Site
- MAC Address
- Reachability
- Device Role
- Image Version
- Up Time
- Last Sync Status
- Resync Interval
- Serial Number
- Device Series
- Platform

**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 auto-complete values as you enter values in the other fields. Choose one of the suggested values or finish entering the desired value.
You can also 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.

**Step 4** Click **Apply** to filter the information.
You can also use the **Device Type** and **Reachability** quick filters, to filter the devices. Additionally you can click any site available in the left pane, to filter the devices based on the site assigned to the device.
The data displayed in the **Devices** table is automatically updated 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 icon next to the corresponding filter value.
Change 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 29: Device Roles and Topology Positions

<table>
<thead>
<tr>
<th>Topology Position</th>
<th>Device Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier 1</td>
<td>Internet (non-configurable)</td>
</tr>
<tr>
<td>Tier 2</td>
<td>Border Router</td>
</tr>
<tr>
<td>Tier 3</td>
<td>Core</td>
</tr>
<tr>
<td>Tier 4</td>
<td>Distribution</td>
</tr>
<tr>
<td>Tier 5</td>
<td>Access</td>
</tr>
<tr>
<td>Tier 6</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

Before you begin

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

Step 1

From the Cisco DNA Center home page, click Provision.

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

Step 2

Locate the device whose role you want to change and 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 Role tab and choose 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: From the Cisco DNA Center home page, click Provision.
The Inventory page displays the device information 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 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
Re-provision the device to update the source-interface configuration.

Update Device Resync Interval

From the Inventory window, you can configure device resynchronization in the following ways:

- You can enable and configure a custom resynchronization interval for a specific device.
- You can enable the preconfigured global resynchronization interval that is set for all the devices. (This setting is configured in the Settings > System Settings > Settings > Network Resync Interval window.
- You can disable resynchronization.

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

Step 1: From the Cisco DNA Center home page, click Provision.
The Inventory page displays the device information gathered during the Discovery process.

Step 2: Select the devices that you want to update.
Manage Your Inventory

Resync Device Information

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

Step 1  From the Cisco DNA Center home page, click Provision.

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

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

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

Step 4  Confirm the action by clicking 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.

Before you begin

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

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

Step 1  From the Cisco DNA Center home page, click Provision.

The Inventory page 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  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 Digital Network Architecture Center Administrator Guide.

Step 1  From the Cisco DNA Center home page, click Provision.
The Inventory page displays the device information gathered during the Discovery process.

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

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 143.

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 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, and 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 Telnet credentials in addition to manually entered SNMP credentials, the device is managed based on the manually entered SNMP credentials and the Telnet credentials in the credential profile.

Note

You must also 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the Cisco DNA Center home page, click <strong>Provision</strong>. The Inventory page displays the device information gathered during the Discovery process.</td>
</tr>
<tr>
<td>Step 2</td>
<td>From the <strong>Actions</strong> drop-down list, choose <strong>Inventory &gt; Import Inventory</strong> to export the device credentials.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Drag and drop the CSV file into the boxed area in the <strong>Bulk Import</strong> dialog box or click the dotted-line boxed area and browse to the CSV file.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>Import</strong>.</td>
</tr>
</tbody>
</table>
Export Device Configurations

You can export specific data pertaining to selected devices to a CSV file. The CSV file is compressed.

⚠️ 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**
From the Cisco DNA Center home page, click **Provision**.

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

**Step 2**
To export configuration information about only certain devices, check the check box next to the devices that you want to include. To include all the 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** dialog box appears.

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

**Step 5**
Check the check boxes next to the data that you want to include in the CSV file.

**Step 6**
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**
From the Cisco DNA Center home page, click **Provision**.

The Inventory page displays the device information 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 checkbox at the top of the list.

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

The **Export** dialog box appears.

**Step 4**
In **Select Export Type**, click **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.
CHAPTER 5

Manage Software Images

- About Image Repository, on page 59
- Integrity Verification of Software Images, on page 59
- View Software Images, on page 60
- Use a Recommended Software Image, on page 60
- Import a Software Image, on page 61
- Assign a Software Image to a Device Family, on page 61
- Upload Software Images for Devices in Install Mode, on page 62
- About Golden Software Images, on page 62
- Specify a Golden Software Image, on page 63
- Provision a Software Image, on page 63

About Image Repository

Cisco DNA Center stores all of the software images and software maintenance updates (SMUs) 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 Catalyst 3K, 4K, and 6K. After any system upgrades, you must re-enable TLS again. For more information, see “Configure Security for Cisco DNA Center” in the Cisco Digital Network Architecture 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 sub-packages for the devices.

Step 1
From the Cisco DNA Center home page, 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. You can toggle to Virtual tab to view software images for virtual devices.

Step 2
In the Image Name column, click the downward arrow to view all the software images for the specified device type family. The Using Image column indicates how many devices are using the specific image shown in the Image Name field. Click the number link 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, Sub-packages, and ROMMON upgrades for the base image.
Sub-packages are the additional features that can be added to the existing base image. The sub-package version that is the same as the image family and the base image version is displayed here.

Note
If you tag any SMU as golden, it will be automatically activated when the base image is installed.
You cannot tag a sub-package as golden.
For ROMMON upgrade, cisco.com configuration is mandatory. When a device is added, the latest ROMMON details will be fetched from cisco.com for applicable devices. Also, when there is base image import or tagging of base image, the ROMMON image will be automatically downloaded from cisco.com.

Step 4
In the Device Role column, select a device role for which you want to indicate this is a "golden" software image. For more information, see About Golden Software Images, on page 62 and Specify a Golden Software Image, on page 63.

Use a Recommended Software Image

Cisco DNA Center can display and allow you to select Cisco-recommended software images for the devices that it manages.

Step 1
From the Cisco DNA Center home page, choose ☀ > System Settings > Settings > Cisco Credentials and verify that you have entered the correct credentials to connect to Cisco.com.

Step 2
Choose Design > Image Repository.
Cisco DNA Center displays the Cisco-recommended software images according to device type.

Step 3
Designate the recommended image as golden. See Specify a Golden Software Image, on page 63 for more information.
After you designate the Cisco-recommended image as golden, Cisco DNA Center automatically downloads the image from cisco.com.

**Step 4** Push the recommended software image to the devices in your network. See Provision a Software Image, on page 63 for more information.

---

## Import a Software Image

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

**Step 1** From the Cisco DNA Center home page, 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 or 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 (not Cisco) vendor, select **Third Party** under **Source**. Then select 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 63 for more information.

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

---

## Assign a Software Image to aDevice Family

After importing a software image, you can assign it to available device families. Imported image can be assigned to multiple devices any time.

To assign an imported software image to device family:

**Step 1** From the Cisco DNA Center home page, choose **Design > Image Repository**.

**Step 2** Click **Imported Images**.

**Step 3** Click **Assign** link.

**Step 4** In the **Assign Device Family** window, select the device families you want to assign this image for.

**Step 5** Click **Assign**.
The software image will be assigned to the device family and the number of devices using that image will be shown in Using Image column. After assigning the image, you can mark the image as golden image. See Specify a Golden Software Image for more information.

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 golden image. When the device is made available in the inventory, the image assigned to the device family will be 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 will be provide 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 cisco.com credentials is not added in Cisco DNA Center, you need to 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 From the Cisco DNA Center home page, 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 greyed out.

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
From the Cisco DNA Center home page, 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
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.

If the software image you specified as golden is not already uploaded into the Cisco DNA Center repository, this process might take some time to complete. Under the Action column on the Image Repository page, if the trash can icon is greyed out, the image is not yet uploaded to the Cisco DNA Center repository. Cisco DNA Center must first upload the software image to its repository, and then it can mark the image as golden. If the software image is already uploaded to the Cisco DNA Center repository, indicated by the active trash can icon in the Action column, then the process to specify a golden image completes faster.

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, SCP and HTTPS file-transfer check, 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.

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, then Cisco DNA Center specifies the software image of the device as outdated. The upgrade readiness prechecks will be triggered for those devices. If all the prechecks are cleared, you can distribute (copy) the new image to the device and activate (make the new image as running image) it. The activation of the new image requires a reboot of the device. This might interrupt the current network activity. In that case, you can schedule the process to a later time.
If you have not designated a golden image for the device type, then the device's image cannot be updated. See Specify a Golden Software Image, on page 63 for more information.

**Step 1** From the Cisco DNA Center home page, click **Provision**.

**Step 2** Choose **Software Images** from the **Focus** drop-down list. Select the device whose image you want to upgrade.

**Note** If the prechecks are successful for a device, the **Outdated** link in the OS Image column will have a green tick mark. If any of the upgrade readiness prechecks fail for a device, the **Outdated** link will have a red into mark, and you cannot update the OS image for that device. Click on the **Outdated** link and correct the errors before proceeding further.

See List of Device Upgrade Readiness Prechecks, on page 64 for the list of prechecks.

**Step 3** From the **Actions** drop-down list, choose **Software Images > Update Image** and do the following.

a) **Distribute**: Click **Now** to start the distribution immediately or click **Later** if you want to schedule the distribution at a specific time.

   **Note** If the image is already distributed for the selected device, the Distribute process will be skipped and you will only be able to Activate the image.

b) Click **Next**.

c) **Activate**: Click **Now** to start the activation immediately or click **Later** if you want to schedule the activation at a specific time.

   **Note** You can skip this step, if you want to perform only the distribution process currently.

d) (Optional) Select the **Schedule Activation after Distribution is completed** check box as required.

e) **Confirm**: Click **Confirm** to confirm the update.

You can check the status of the update in the **OS Update Status** column. If this column is not displayed, click  

![](images/arrow.png)  
and choose **OS Update Status**.

**Step 4** (Optional) Click **Upgrade Status** to view the progress of the image upgrade.

**Note** If you have a device between Cisco DNA Center and another fabric device, such as an edge router, the software update process might fail if the *in between* device reloads while the software image is being provisioned to the other device.

---

### List of Device Upgrade Readiness Prechecks

<table>
<thead>
<tr>
<th>Precheck</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device management status</td>
<td>Checks if the device is successfully managed in Cisco DNA Center.</td>
</tr>
<tr>
<td>File transfer check</td>
<td>Checks if the device is reachable through SCP and HTTPS. If there is a connectivity problem, see Troubleshoot HTTPS and SCP Connectivity.</td>
</tr>
<tr>
<td>NTP clock check</td>
<td>Compares device time and Cisco DNA Center time to ensure successful Cisco DNA Center certificate installation.</td>
</tr>
</tbody>
</table>
Precheck | Description
---|---
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.
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.
Interface check | Checks the status of the device interface.
CDP neighbors check | Displays information about the connected routers and switches in the network that are discovered using CDP.
Running Config check | Checks the configuration that is currently running on the device.
Spanning Tree Summary check | Checks the information about the Spanning Tree Protocol (STP).
AP Summary check | Displays the AP Summary associated with the Cisco Wireless Controllers devices.

**Troubleshoot HTTPS and SCP Connectivity**

If the device is not reachable through SCP or HTTPS, use the steps in this section to resolve the connectivity problem.

**Troubleshoot HTTPS Connectivity**

Perform the following steps to troubleshoot HTTPS connectivity problems.

**Step 1**  
To verify that the device time is in sync with the Cisco DNA Center time zone, enter the `show clock` command. For example:  
`ASR1001-X-149#show clock`

**Step 2**  
To verify that the device is running TLS 1.2, enter:  
`show ip http client secure status`  
**Note** A running image version later than 16.x supports TLS 1.2.

**Step 3**  
To verify that the device is configured with `crypto key generate rsa modulus 1024`, enter:  
`show crypto key mypubkey rsa`
If the device is not configured with the crypto key, enter the following command to configure it:

```bash
config t
crypto key generate rsa
```

**Step 4**  
To verify that the device is configured with an IP domain name, enter:

```bash
sh running-config | sec ip domain
```

For example:

```bash
ip domain name Cisco.com
```

If the domain name is not configured, enter:

```bash
set : ip domain name <domain_name>
```

**Step 5**  
To validate the HTTPS communication between the device and Cisco DNA Center, enter:

```bash
copy https://<Cisco_DNA_Center_IP_address>/core/img/cisco-bridge.png flash:cisco-bridge.png
```

---

**Troubleshoot SCP Connectivity**

Perform the following steps to troubleshoot SCP connectivity problems.

**Step 1**  
To verify that SSH is configured, enter:

```bash
show run | inc ssh
```

For example:

```bash
ASR1001-X-149#show running-config | sec ssh
```

If SSH is not configured, enter the following commands to configure it on the device:

```bash
line vty 0 15
transport input all
ip ssh source-interface GigabitEthernet1/1
```

**Step 2**  
To enable SSH version 2 on the device, enter:

```bash
ip ssh version 2
```

**Step 3**  
To verify that SCP is configured on the device, enter:

```bash
show run | inc scp
```

For example:

```bash
ASR1001-X-149#show running-config | sec scp
```

**Step 4**  
If SCP is not configured, enter the following commands to configure it on the device:

```bash
config t
ip scp server enable
```
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.
Display Your Network Topology

- About Topology, on page 69
- Display the Topology of Areas, Sites, Buildings, and Floors, on page 70
- Filter Devices on the Topology Map, on page 70
- Display Device Information, on page 71
- Display Link Information, on page 72
- Pin Devices to the Topology Map, on page 72
- Assign Devices to Sites, on page 73
- Save a Topology Map Layout, on page 73
- Open a Topology Map Layout, on page 74
- Export the Topology Layout, on page 74

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
From the Cisco DNA Center home page, click 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 From the Cisco DNA Center home page, click 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

You can 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 From the Cisco DNA Center home page, click 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 is indicated under a switch, if the 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. Hover your mouse over the icon next to the items, to know more information.

- **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. If the license of a device is going to expire, it will be highlighted and a warning icon will appear next to the device. 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.

## Display Link Information

You can 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**  From the Cisco DNA Center home page, click **Topology**.

**Step 2**  In the tree view menu, select the area, site, building, or floor that you are interested in.

**Step 3**  Hover your mouse 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.

---

## 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.
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.

---

**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.
Open a Topology Map Layout

You can open previously saved topology maps.

Before you begin
You should have saved topology map layouts.

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 From the Cisco DNA Center home page, click Topology.
Step 2 Click Custom View.
Step 3 Click the name of the map that you want to display.

Step 1 From the Cisco DNA Center home page, click 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, on page 75
- About Network Hierarchy, on page 76
- Monitor a Floor Map, on page 82
- Edit Floor Elements and Overlays, on page 84
- Floor View Options, on page 93
- Data Filtering, on page 96
- Configure Global Wireless Settings, on page 97
- Create Network Profiles, on page 111
- About Global Network Settings, on page 114
- About Device Credentials, on page 115
- About Global Device Credentials, on page 117
- Guidelines for Editing Global Device Credentials, on page 122
- Edit Global Device Credentials, on page 123
- Associate Device Credentials to Sites, on page 124
- Configure IP Address Pools, on page 124
- Import IP Address Pools from IP Address Manager, on page 125
- Import IP Address Pools from CSV File, on page 125
- Reserve an IP Pool, on page 126
- Configure Service Provider Profiles, on page 126
- Configure Global Network Servers, on page 127
- Add Cisco ISE or Other AAA Servers, on page 127
- Configure Cisco WLC High Availability from Cisco DNA Center, on page 128

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 11.

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 76.
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.

- **Floors** are within buildings and consist of cubicles, walled offices, wiring closets, and so on. You can add floors only to buildings.

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 76.

  - Upload an existing network hierarchy from Cisco Prime Infrastructure. For more information, see Upload an Existing Site Hierarchy, on page 78.

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 application 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**
From the Cisco DNA Center home page, choose Design > Network Hierarchy.
A world map is displayed.

**Step 2**
On the Network Hierarchy window, click + Add Site, or click the gear icon next to the parent site in the left pane, and then select the appropriate option.

**Step 3**
You can also upload an existing hierarchy. For more information, see Upload an Existing Site Hierarchy, on page 78.

**Step 4**
Enter a name for the site, and select 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 menu.

---

**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 versions.

**Before you begin**
- Discover Cisco Wireless Controller and Access Points and are listed on Cisco DNA Center Inventory page.
- Add and position APs on a floor map.
- If you have manually created any sites in Cisco DNA Center, which may be present in Cisco Prime Infrastructure, you must remove those sites manually before importing into Cisco DNA Center.

**Step 1**
As a first step, you must export the location groups from Cisco Prime Infrastructure as a CSV file to your workstation.

**Step 2**
To export the location groups, on Cisco Prime Infrastructure, choose Inventory > Group Management > Network Device Groups.

**Step 3**
In the Device Groups window, click Export Groups.

**Step 4**
In the Export Groups dialog box, click the APIC-EM radio button to download the CSV file, and click OK.
Wait for CSV to download to workstation. The CSV file contains information about the geographic locations of various sites, buildings, and floors and their hierarchy in the network.
Step 5  Next, export maps from Cisco Prime Infrastructure. This downloads map information such as floor dimension and calibration information like RF attenuation model that has been applied to each floor in Cisco Prime Infrastructure.

Step 6  To export maps, choose Maps > Wireless Maps > Site Maps (New).

Step 7  From the Export drop-down list, choose Map Archive.

The Export Map Archive window appears, and Select Sites window appears by default.

Step 8  Check the check box of a specific site, campus, building, or floor, that you want to export, or check the Select All check box to export all the maps.

Step 9  Check if the Map Information and Calibration Information are selected. Selecting one option is mandatory. If not, click the On button against the Map Information and Calibration Information.

Step 10  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.

Step 11  Selecting Calibration Information exports Radio Frequency 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 will have to enter the calibration details manually in Cisco DNA Center.

Step 12  Click Generate Map Archive to generate the map archive.

A tar file that contains the various floor maps in your network hierarchy is created and saved on your workstation.

Step 13  To import the site hierarchy to Cisco DNA Center, from the Cisco DNA Center home page, choose Design > Network Hierarchy, and then click Import > Import Sites.

Step 14  In the Import Sites window, drag and drop the Prime Infrastructure location groups CSV file, or click Select a file from your computer to navigate to where the file is located, and click Import to import the Prime Infrastructure location groups CSV file.

Step 15  Next, import the map archive file that contains floor maps and related map information.

Step 16  To import the map archive file, choose Design > Network Hierarchy, and then click Import > Import Maps.

Step 17  In the Import Maps Archive window, drag and drop the map archive file, or select the file from your workstation.

Step 18  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 more information, see Export Maps Archive, on page 79 on how to export maps from Cisco Prime Infrastructure.

Note  Before importing a map archive file into Cisco DNA Center, make sure that the devices such as Cisco Wireless Controllers and its associated APs are discovered and listed on the Cisco DNA Center inventory page.

---

Step 1  From the Cisco DNA Center home page, choose Design > Network Hierarchy, and then click Import > Import Sites.

Step 2  Drag and drop your CSV file, or navigate to where your CSV file is located, then click Import to import the Cisco Prime Infrastructure Groups CSV file.
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, click **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**.

---

### 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**
From the Cisco DNA Center home page, choose **Design > Network Hierarchy**.
Delete Sites

Step 1  From the Cisco DNA Center home page, 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  From the Cisco DNA Center home page, choose Design > Network Hierarchy.
A world map is displayed.
Step 2  On the Network Hierarchy window, click + Add Site, or click the gear icon next to the parent site in the left pane and select Add Building.
Step 3  You can also upload an existing hierarchy. See Upload an Existing Site Hierarchy, on page 78.
Step 4  Enter a name for the building.
Step 5  In the Address text 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. 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  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 Buildings

Step 1  From the Cisco DNA Center home page, 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  From the Cisco DNA Center home page, 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 has a 21-character limit. The floor name must 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.
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: From the Cisco DNA Center home page, 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.

### Table 30: Map Icons

<table>
<thead>
<tr>
<th>Floor Map Icons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AP Mode</strong></td>
<td></td>
</tr>
<tr>
<td>L</td>
<td>Local</td>
</tr>
<tr>
<td>F</td>
<td>FlexConnect</td>
</tr>
<tr>
<td>B</td>
<td>Bridge</td>
</tr>
<tr>
<td><strong>Health Score</strong></td>
<td></td>
</tr>
<tr>
<td>🟢</td>
<td>Good Health</td>
</tr>
<tr>
<td>🟠</td>
<td>Fair Health</td>
</tr>
<tr>
<td>🟥</td>
<td>Poor Health</td>
</tr>
<tr>
<td><strong>AP Status</strong></td>
<td></td>
</tr>
<tr>
<td>🎖️</td>
<td>Not covered by sensor</td>
</tr>
<tr>
<td>🎖️</td>
<td>Covered by sensor</td>
</tr>
<tr>
<td><strong>Radio Band or Mode</strong></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>802.11 a/n/ac (5 GHZ)</td>
</tr>
<tr>
<td>2.4</td>
<td>802.11 b/g/n (2.4 GHZ)</td>
</tr>
<tr>
<td>n</td>
<td>802.11 a/b/g/n (2.4 GHZ)</td>
</tr>
<tr>
<td>Se</td>
<td>Sensor</td>
</tr>
<tr>
<td>M</td>
<td>Monitor 5 GHz</td>
</tr>
<tr>
<td>m</td>
<td>Monitor 2.4 GHz</td>
</tr>
<tr>
<td>Mx</td>
<td>Monitor XOR Mode</td>
</tr>
</tbody>
</table>
### Floor Map Icons

<table>
<thead>
<tr>
<th>Description</th>
<th>Floor Map Icons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rogue Detector</td>
<td>R</td>
</tr>
<tr>
<td>Other</td>
<td>...</td>
</tr>
</tbody>
</table>

### Radio Status

<table>
<thead>
<tr>
<th>Status</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ok</td>
<td>5</td>
</tr>
<tr>
<td>Minor Fault</td>
<td>5</td>
</tr>
<tr>
<td>Down</td>
<td>5</td>
</tr>
<tr>
<td>Admin Disable</td>
<td>...</td>
</tr>
</tbody>
</table>

### Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🌟</td>
<td>Access Points</td>
</tr>
<tr>
<td>🎯</td>
<td>Sensor</td>
</tr>
<tr>
<td>✐</td>
<td>Markers</td>
</tr>
</tbody>
</table>

### Rx Neighbors Line

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Icon</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4 GHz</td>
<td>—</td>
</tr>
<tr>
<td>5 GHz</td>
<td>—</td>
</tr>
</tbody>
</table>

---

**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

Guidelines for Placing Access Points

Follow these guidelines while placing APs on the floor map:

• Place access points along the periphery of coverage areas to keep devices close to the exterior of rooms and buildings. Access points 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. Hence, 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.

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 11.

The following 802.11ax APs are newly supported in Cisco DNA Center, Release 1.3:

• Cisco Catalyst 9100 Access Points
• Cisco Catalyst 9115 Access Points
• Cisco Catalyst 9117 Access Points
• Cisco Catalyst 9120 Access Points

Step 1 From the Cisco DNA Center home page, 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 APs in bulk, and click Add Selected. Alternatively click Add adjacent an access point.
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 3 points on the floor map and position APs using the points created. To do this:
    1. Click Position by 3 points.
    2. 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.
    3. Define the second and third points similarly, and click Save.

  - **Position by 2 Walls**—You can define 2 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.
    1. Click Position by 2 walls.
    2. 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.
    3. 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 feet.
- **y**—Indicates the vertical span of the map, in feet.
- **AP Height**—Indicates the height of the access point.
- **Protocol**—Protocol for this access point: 802.11a/n/ac, 802.11b/g/n (for Hyper Location APs), or 802.11a/b/g/n.
- **Antenna**—Antenna type for this access point.

  **Note** For external APs, you must select an antenna, otherwise, the AP will not be present in the map.

- **Antenna Image**—Shows the AP image.
• **Antenna Orientation**—Indicates the Azimuth and the Elevation orientations, in degrees.
• **Azimuth**—This option does not appear for Omnidirectional antennas because their pattern is nondirectional in azimuth.

**Step 9**

After you have completed placing and adjusting access points, click **Save**.

Heatmap is generated based on the new position of the AP.

If a Cisco Connected Mobile Experiences (CMX) is synchronized with Cisco DNA Center, then you can view the location of clients on the heatmap. See *Create Cisco CMX Settings*, on page 109.

**Step 10**

In the **Floor Elements** panel, next to **Access Points**, click **Delete**.

The **Delete APs** window appears which lists all the assigned and places access points, appears.

**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 click **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.

---

### 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). See the Monitor and Troubleshoot the Health of a Device topic in the Cisco DNA Assurance User Guide.

**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 AP 1800S sensor must be provisioned using Plug and Play for it to show up in the Inventory. See the Provision the Wireless Cisco Aironet 1800s Active Sensor topic in the Cisco DNA Assurance User Guide.

*A sensor device* is a dedicated AP 1800S sensor. The AP 1800S sensor gets bootstrapped using PnP. After it obtains the Assurance server reachability details, it directly communicates with the Assurance server.

---

## Step 1

From the Cisco DNA Center home page, 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 these 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
From the Cisco DNA Center home page, 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.

1. 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.

2. Move the drawing tool to the area you want to outline.

3. Click the tool to start and stop a line.

4. 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.

1. Enter the name of the area you are defining, and click Ok.

2. 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 to 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**  
From the Cisco DNA Center home page, 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, which results in the area getting highlighted.

**Step 10**  
Click **Done** in the **Obstacle Creation** window that appears.

**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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From the Cisco DNA Center home page, choose <strong>Design &gt; Network Hierarchy</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the left pane, select the floor.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the <strong>Overlays</strong> panel, next to <strong>Location Regions</strong>, click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the <strong>Location Region Creation</strong> dialog window, from the <strong>Inclusion Type</strong> drop-down list, choose an option.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click <strong>Add Location Region</strong>. A drawing icon appears to outline the inclusion area.</td>
</tr>
<tr>
<td>Step 6</td>
<td>To begin defining the inclusion area, move the drawing tool to a starting point on the map and click once.</td>
</tr>
<tr>
<td>Step 7</td>
<td>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.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Repeat Step 7 until the area is outlined and then double-click the drawing icon. A solid aqua line defines the inclusion area.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From the Cisco DNA Center home page, choose <strong>Design &gt; Network Hierarchy</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the left pane, select the floor.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Edit</strong>, which is located above the floor plan in the middle pane.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the <strong>Overlays</strong> panel, next to <strong>Location Regions</strong>, click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the <strong>Location Region Creation</strong> window, from the <strong>Exclusion Type</strong> drop-down list, choose a value.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click <strong>Location Region</strong>. A drawing icon appears to outline the exclusion area.</td>
</tr>
<tr>
<td>Step 7</td>
<td>To begin defining the exclusion area, move the drawing icon to a starting point on the map and click once.</td>
</tr>
<tr>
<td>Step 8</td>
<td>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.</td>
</tr>
<tr>
<td>Step 9</td>
<td>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.</td>
</tr>
<tr>
<td>Step 10</td>
<td>To define more exclusion regions, repeat Step 5 to Step 9.</td>
</tr>
<tr>
<td>Step 11</td>
<td>When all the exclusion areas are defined, click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>
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  From the Cisco DNA Center home page, 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 then 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 to delete.
Step 13 Click Save.

Place Markers

Step 1 From the Cisco DNA Center home page, 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 to delete.
Step 12 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

Click the On/Off button next to Access Points to view access points on the map. 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 1000 series APs accept a value between 1 and 5, the 1230 access points accept a value between 1 and 7, and the 1240 and 1100 series access points 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, or Coverage.

  • None

  • Coverage—If you have monitor mode access points on the floor plan, you can select coverage heatmap. A coverage heatmap excludes monitor mode access points.
• **Heatmap Opacity (%)**—Drag the slider between 0 to 100 to set the heatmap opacity.

• **RSSI Cut off (dBm)**—Drag the slider to set the RSSI cutoff level. The RSSI cutoff ranges from -60 dBm to -90 dBm.

• **Map Opacity (%)**—Drag the slider to set the map opacity.

The AP details are reflected on the map immediately. Hover your cursor over the AP icon on the map to view AP details and RX neighbor 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

### 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 Maps 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.
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.
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 wireless interfaces and wireless radio frequency applies only to nonfabric deployments.
Creating a wireless sensor device profile applies only to AP 1800S sensor devices.

Create SSIDs for an Enterprise Wireless Network

The following procedure describes how to configure SSIDs for an enterprise wireless network.

Note
All the SSIDs are created at the Global level. The site, building, and floor inherit settings from the Global level.

Step 1
From the Cisco DNA Center home page, choose Design.

Step 2
From the Network Settings drop-down list, choose Wireless.

Step 3
Under Enterprise Wireless, click + Add.
The Create an Enterprise Wireless Network window appears.

Step 4
In the Wireless Network Name (SSID) text box, enter a unique name for the wireless network or the SSID that you are creating.
The name can contain up to 32 alphanumeric characters, including one space. All special characters are allowed except < /
The following combination of substring is not allowed: .*

Step 5
From the Type of Enterprise Network drop-down list, select the type of enterprise network: 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 to access either voice or data traffic.
If you select Data Only option, the quality of service is optimized for wireless data traffic only.

Step 6
Check the Fast Lane check box to enable fastlane capabilities on the network.
By selecting Fast Lane, you can set the IOS devices to receive an optimized level of wireless connectivity and enhanced Quality of Service (QoS).

Step 7
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 8  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 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 9  Under Level of Security, set the encryption and authentication type for the network. The 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 preshared 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.

  **Note** 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 settings. For more information, see Preshared Key Override, on page 100.

- **Open**—Provides no security. Allows any device to access the wireless network without any authentication.

Step 10  Click Show Advanced Settings to configure the following.

Step 11  Set the Fast Transition (802.11r) to Enable, Adaptive, or Disable mode.

By default, the Fast Transition (802.11r) is in Adaptive mode.

The 802.11r allows wireless clients to quickly roam from AP to another AP. Fast transition ensures less disrupted connectivity when a wireless client roams from one AP to another AP.

Step 12  Click the Over the DS check box to enable Fast Transition over a distributed system. This option is available only if the Fast Transition is in Adaptive mode.

By default, the Over the DS is enabled.

Step 13  Check the MAC Filtering check box to enable MAC-based access control or security on the wireless network.

When you enable MAC filtering, only the MAC addresses that you add to the wireless LAN are allowed to join the network.

Step 14  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 15  Check the Client Exclusion check box, and enter a value to set the client exclusion timer.

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 16  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 select 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 17**
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 18**
Under 11v BSS Transition Support, configure the following.

**Step 19**
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 20**
Check the Client User Idle Timeout check box and enter a value to configure the user idle timeout for a WLAN.

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 21**
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 saves the battery power.

**Step 22**
Click Next.

The Wireless Profiles window is displayed. You can associate the SSID to a wireless profile.

**Step 23**
In the Wireless Profiles window, click +Add to create a new wireless profile.

**Step 24**
Configure the following in the Create a Wireless Profile window.

**Step 25**
In the Wireless Profile Name text box, enter a name for the wireless profile.

**Step 26**
Specify whether the SSID is fabric or non fabric by selecting Yes or No.

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.

**Step 27**
If you are creating a non fabric SSID, select No and configure the following parameters.

**Step 28**
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.

This is the VLAN ID that is associated with the wireless interface.

**Step 29**
From the Select Interface drop-down list, choose an interface name for the SSID or click + Create a Wireless Interface to create a new wireless interface.
This is the VLAN ID that is associated with the wireless interface.

**Step 30** Check the **Flex Connect Local Switching** 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.

**Step 31** The VLAN ID which is associated with the wireless interface is auto populated 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 32** To assign this profile to a site, click **Sites**.

**Step 33** In the **Sites** window, check the check box next to the site to associate this profile. 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 34** Click **OK**.

**Step 35** To associate a template with the network profile, click + **Add** under the **Attach Template(s)** area.

**Step 36** Select the device type, tag, and template from the **Device Type**, **Tag Name**, and **Template** drop-down lists.

**Step 37** Click **Add**.

The created profile appears in the **Wireless Profiles** window.

**Step 38** To associate the SSID to wireless profile, in the **Wireless Profile** window, check the **Profile Name** check box.

**Step 39** Click **Finish**.

---

**Preshared Key Override**

SSIDs are created at the Global hierarchy. The site, building, and floor 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 settings.

**Step 1** Choose **Design** > **Network Settings** > **Wireless**.

**Step 2** In the tree menu, select the site, building, or floor to edit the PSK.

**Step 3** Under **Enterprise Wireless**, click the **Passphrase** text box, and enter a new passphrase for the PSK SSID.

**Step 4** Click **Save**.

A success message displays "Passphrase for the SSID(s) updated successfully."

Click the Inherit icon next to the SSID to view the origin of the settings.

**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.

---

**Create SSIDs for a Guest Wireless Network**

This procedure explains how to create SSIDs for a guest wireless network.

**Step 1** From the Cisco DNA Center home page, choose **Design** > **Network Settings** > **Wireless**.
Step 2  Under **Guest Wireless**, click +Add to create new SSIDs.

The **Create a Guest Wireless Network** window is displayed.

Step 3  In the **Wireless Network Name (SSID)** text box, enter a unique name for the guest SSID that you are creating. The name can contain up to 32 alphanumeric characters, including one space. All special characters are allowed except for the following: < /

The following combination substring is not allowed: .*

Step 4  Under **Level of Security**, select the encryption and authentication type for this guest network: **Web Auth** and **Open**.

For an External Web Authentication (EWA), select **Web Auth** as the **Level of Security** and **External Authentication** as the **Authentication Server**.

For a Central Web Authentication (CWA), select **Web Auth** as the **Level of Security** and **ISE Authentication** as the **Authentication Server**.

The **Web Auth** encryption and authentication type provides a higher level of Layer 3 security.

The **Open** encryption and authentication type provides no security. It allows any device to connect to the wireless network without any authentication.

Step 5  If you choose **Web Auth**, you must configure the authentication server: **ISE Authentication** or **External Authentication**.

  - If you choose **External Authentication**, enter the redirect URL in the **Web Auth URL** text box.

  - If you choose **ISE Authentication**, select the type of portal you want to create from the 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.

Step 6  To redirect the guests after successful authentication, select from the 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** text box.

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 7  Click **Show Advanced Settings** to configure the following.

Step 8  Check the **Client Exclusion** check box, and enter a value to set the client exclusion timer.

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 9  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 10  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 select **Required**, 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 11  Under 802.11v BSS Transition Support, configure the following.

Step 12  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 13  Check the **Client User Idle Timeout** check box and enter a value to configure the user idle timeout for a WLAN.

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, the **Client User Idle Timeout** is enabled with a user idle timeout of 300 seconds.

Step 14  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 saves the battery power.

Step 15  Click **Next**.

The **Wireless Profiles** window is displayed.

Step 16  If you do not have an existing wireless profile, in the **Wireless Profiles** window, click +Add to create a new wireless profile.

Step 17  Enter a profile name in the **Wireless Profile Name** text box.

Step 18  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. Non-fabric is a traditional wireless network that does not require SD-Access.

Step 19  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, select **Yes**.

If you select **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.

Step 20  From the **Select Interface** drop-down list, select the interface or click + create a new wireless interface to create a new wireless interface.

This is the VLAN ID that is associated with the wireless interface.

Step 21  To assign this profile to a site, enter the full or partial name of the site in the **Site Selector** text box.
The available sites are auto populated and you can select the site that you want from the drop-down list.

**Step 22**  
Click **Save**.

The created profile appears in the **Wireless Profiles** window.

**Step 23**  
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 24**  
In the **Portal Customization** window, click + **Add** to create the guest portal.

The **Portal Builder** window appears.

**Step 25**  
Expand **Page Content** in the left menu to include various variables.

**Step 26**  
Drag and drop variables into the portal template window and edit them.

- The variables for the **Login** page are: **Access Code**, **Header Text**, **AUP**, and **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**, and **AUP**.
- The variables for the **Registration Success** page are: **Account Created** and **Header texts**.
- The variable for the **Success** page is: **Text fields**.

**Step 27**  
To customize the default color scheme in the portal, expand **Color** in the left menu and change the color.

**Step 28**  
To customize the font, expand **Font** in the left menu and change the font.

**Step 29**  
Click **Save**.

The created portal appears in the **Portal Customization** window.

**Step 30**  
Under **Portals**, click the radio button next to the corresponding **Portal Name** to assign the SSID to that guest portal.

**Step 31**  
Click **Finish**.

---

**What to do next**

1. Discover devices by using CDP or an IP address range. See Discover Your Network Using CDP, on page 16 and Discover Your Network Using an IP Address Range, on page 21.


4. Add a Cisco Wireless Controller to a site. See Add a Device to a Site, on page 216.

5. Provision the Cisco Wireless Controller and Cisco AP. See Provision a Cisco Wireless Controller, on page 218 and Provision a Cisco AP—Day 1 AP Provisioning, on page 222.

6. Add the Cisco Wireless Controller to a fabric domain. See Add a Device to a Fabric, on page 257.

7. Configure settings for the various kinds of devices (hosts) that can access the fabric domain. See Configure Host Onboarding.
Create a Guest Portal Page

You can create the following guest portal pages:

- Login page
- Registration page
- Registration success
- Success page

Step 1
From the Cisco DNA Center home page, choose Design > Network Settings > Wireless > Guest Wireless.

Step 2
Navigate to the portal page you are creating.

Step 3
Enter the portal name in the Portal Name text box.

Step 4
Expand Page Content in the left menu to include various variables while creating portal pages.

- List of variables for Login page:
  - Access Code
  - Header Text
  - AUP
  - Text Fields

- List variables for Registration page:
  - First Name
  - Last Name
  - Phone Number
  - Company
  - Sms Provider
  - Person being visited
  - Reason for a visit
  - Header text
  - User Name
  - Email Address
  - AUP

- List of variables for Registration page:
  - Account Created
  - Header texts
• Variables for Success page:
  • Text fields

**Step 5** Drag and drop variables into the portal template page and edit them.

**Step 6** To customize the default color scheme in the portal, expand **Color** in the left menu and change the color of these page elements:
  • Body text Border
  • Link text Page
  • Background
  • Border Color
  • Header Background

**Step 7** To customize the font, expand **Font** in the left menu and change the following:
  • Typeface
  • Header
  • Title text
  • Body text
  • Form label

**Step 8** Click **Save** to save the portal.

---

**Create a Wireless Interface**

You can create wireless interfaces only in nonfabric deployments.

**Step 1** From the Cisco DNA Center home page, 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**.
Create a Wireless Radio Frequency Profile

You can create a wireless radio frequency profile only in a nonfabric deployment.

Step 1
From the Cisco DNA Center home page, 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 adjacent 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 adjacent 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.
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.

  • UNII-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.
In the Warning window, click OK.

Create a Wireless Sensor Device Profile

Creating the wireless sensor device profile is applicable for the Cisco Aironet 1800s Active Sensor.

Before you begin

If you are using the Cisco Aironet AP 1800S Sensor without an Ethernet module, you must enable Cisco Provisioning SSID on the wireless controller. See the "Enable Cisco Provisioning SSID on the Cisco Wireless Controller" topic in the Cisco DNA Assurance User Guide.

Step 1  Choose Design > Network Settings > Wireless.

Step 2  Under Sensor Settings, click +Add.

The Create Sensor SSID Assignment window appears. Configure the following parameters:

- In the Settings Name field, enter a name for the sensor device profile.
- In the Wireless Network Name (SSID) field, enter a name for the SSID.
- In the Level of Security area, choose a security level, and then enter the appropriate credentials.

Note  To provision the Cisco Aironet 1800s Active Sensor with wired connection, enter any proxy name and SSID (for example wired_xyz), and in the Level of Security area, choose Open.

Step 3  Click Save.

About Cisco Connected Mobile Experiences Integration

Cisco DNA Center supports the integration of on-premise Connected Mobile Experiences (CMX) for wireless maps. With the CMX integration, you can get the exact location of your clients 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**
To add a CMX server to the Cisco DNA Center, from the Cisco DNA Center home page, click the gear icon (⚙️), and then choose **System Settings > Settings > 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, follow these steps.

**Step 8**
Choose **Design > Network Settings > Wireless**.

**Step 9**
In the left tree view menu, select either Global or the area, building, or floor that you are interested in.

**Step 10**
Under **CMX Servers**, from the **CMX Servers** drop-down list, select the CMX server.

**Step 11**
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 12**
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 13**
To edit the CMX server details, from the Cisco DNA Center click the gear icon (⚙️), and then choose **System Settings > Settings > CMX Servers**.

**Step 14**
Select the CMX server that you want to edit, and make any changes, and click **Update**.
Step 15

Step 16 To delete a CMX server, from the Cisco DNA Center click the gear icon (⚙️), and then choose System Settings > Settings > CMX Servers.

Step 17 Select the CMX server that you want to delete, and click Delete.

Step 18 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 UI.

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:
  ```bash
curl -k -u <user>:<password> -X GET /api/v1/dna-maps-service/domains/<floor group id>/clients?associated=true
  ```

---

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 From the Cisco DNA Center homepage, 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 97 and Create SSIDs for a Guest Wireless Network, on page 100.

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 Wireless Controller, on page 218.

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 222.

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

From the Cisco DNA Center home page, choose Design > Network Profiles. Click ☰ Add Profile to create network profiles for:

- Routing and NFV
- Switching
- Wireless

Create Network Profiles for Routing and NFV

This workflow shows how to:

1. Configure router WAN.
2. Configure router LAN.
3. Configure ENCS integrated switch.
4. Create custom configurations.
5. View profile summary.

Step 1  Choose Design > Network Profiles.
Step 2  Click ☰ Add Profiles and choose Routing & NFV.
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. A maximum of 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 126.
- 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 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 on 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 primary interface as gigabit ethernet and secondary as cellular, or both the interfaces as gigabit ethernet. You can also select primary interface as cellular and 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 cellular interface.
• Click +Add Services to add services to the profile. The Add Services window appears. Check the check box next to ISRv vEdge, WAN Optimizer, or Firewall. You can also select +Add Service or Network to add custom services or networks to the profile.

**Note** This option is available only on devices that support NFV functions like Cisco ENCS 5000 series, Cisco ISR 4300 and 4400 series and Cisco USC devices.

To configure the ISRv router, select Profile from the drop-down list. For more information, see Import a Software Image, on page 61. Click Save.

To configure vEdge, select Profile from the drop-down list.

To configure WAN optimizer, select Services and Profile from the drop-down lists.

To configure firewall, select Services, Profile and Mode from the drop-down lists.

To enable Direct Internet Access (DIA), select Firewall and check the check box next to DIA.

To configure custom networks, select +Add Custom Service or network and select Networks. Enter the network name in Network Name. Select Connection Type and Network Mode. Enter the VLAN ID in VLAN and select the services to connect. Click Save.

To configure custom service, select +Add Custom Service or network and select Service. Enter the Service name such as Linux or Windows server in the Add a Custom Service window. Click Save.

• Click Next.

**Step 4** The Router LAN Configuration page appears.

• Select L2, L3 or Skip services.

• If you select L2, select the Type from the drop-down list, enter the VLAN ID/Allowed VLAN and the Description.

• If you select L3, select the Protocol Routing from the drop-down list and enter the Protocol Qualifier.

• Click Next.

**Step 5** 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 6** The Custom Configuration page appears.

The custom configurations are optional. You may skip the step and apply the configurations any time in the Network Profiles.

If you choose to add the custom configurations:

• Select Onboarding Template(s) or Day-N Templates tab, as required.

• Select the Template from the drop-down list. The templates will be filtered by the Device Type and Tag Name.

• Click Next.

**Step 7** 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 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 76.

Create Network Profiles for Switching

You can apply two types of configuration templates to a switching profile: Onboarding template and 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 131.

Step 1
Choose Design > Network Profiles.
Step 2
Click +Add Profiles and choose Switching.
Step 3
The Switching Configuration window appears.
Click on either OnBoarding Template(s) or Day-N Template(s) depending on the type of template you want to create.
- 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 have selected has already been associated with a template, only that template is available in the Template drop-down.
- 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 thus 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
Choose Design > Network Profiles.
Step 2  Click +Add Profiles and choose Wireless.

Before assigning wireless network profile, ensure you have created wireless SSIDs under the Design > Network Settings > Wireless tab.

Step 3  The Add a Network Profile window appears.

Step 4  Enter a valid profile name in the Profile Name text box.

Step 5  Click + Add SSID.

Those SSIDs that were created under the Network Settings > Wireless tab gets populated.

Step 6  From the SSID drop-down list, choose the SSID.

The SSID type is displayed.

Step 7  Specify whether the SSID is fabric or non fabric by selecting Yes or No.

Step 8  If you are creating a non fabric SSID, then select No, and configure the following parameters.

Step 9  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 10  Check the Flex Connect Local Switching 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.

Step 11  The VLAN ID which is associated with the wireless interface is auto populated 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 12  Click Save to add a network profile.

The newly added network profile appears on the Design > Network Profiles page.

Step 13  To assign this profile to a site, click Assign Sites.

Step 14  In the Add Sites to Profile window, check the check box next to the site to associate this profile.

You can either 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 15  Click Select.

---

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 NTP, Syslog, SNMP Trap, NetFlow Collector, and so on; IP address pools; and device credential profiles.

- **Site settings**: Settings defined here override global settings and can include settings for servers, IP address pools, and device credential profiles.
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. For more information about Device Controllability and Audit Logs, see the Cisco Digital Network Architecture Center Administrator Guide.

You can define the following global network settings by choosing Design > Network Settings and selecting appropriate tabs such as Network, Device Credentials, IP Address Pools, SP Profiles, or Wireless.

- Network servers, such as AAA, DHCP, and DNS—For more information, see Configure Global Network Servers, on page 127.
- Device credentials, such as CLI, SNMP, and HTTP(S)—For more information, see Configure Global CLI Credentials, on page 117, Configure Global SNMPv2c Credentials, on page 118, Configure Global SNMPv3 Credentials, on page 119, and Configure Global HTTPS Credentials, on page 121.
- IP address pools—For more information, see Configure IP Address Pools, on page 124.
- Wireless settings as SSIDs, wireless interfaces, and wireless radio frequency profiles—For more information, see Configure Global Wireless Settings, on page 97.

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 need to 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 five read community strings and five 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.

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 five 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 31: SNMPv3 Security Models and Levels

<table>
<thead>
<tr>
<th>Level</th>
<th>Authentication</th>
<th>Encryption</th>
<th>What Happens</th>
</tr>
</thead>
<tbody>
<tr>
<td>noAuthNoPriv</td>
<td>User Name</td>
<td>No</td>
<td>Uses a username match for authentication.</td>
</tr>
<tr>
<td>AuthNoPriv</td>
<td>Either:</td>
<td>No</td>
<td>Provides authentication based on the Hashed Message Authentication Code-Secure</td>
</tr>
<tr>
<td></td>
<td>• HMAC-MD5</td>
<td></td>
<td>Hash Algorithm (HMAC-SHA).</td>
</tr>
<tr>
<td></td>
<td>• HMAC-SHA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AuthPriv</td>
<td>Either:</td>
<td>Either:</td>
<td>Provides authentication based on HMAC-MD5 or HMAC-SHA.</td>
</tr>
<tr>
<td></td>
<td>• HMAC-MD5</td>
<td>• CBC-DES</td>
<td>Provides Data Encryption Standard (DES) 56-bit encryption in addition to</td>
</tr>
<tr>
<td></td>
<td>• HMAC-SHA</td>
<td>• CBC-AES-128</td>
<td>authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard or CBC-mode AES for encryption.</td>
</tr>
</tbody>
</table>

HTTPS Credentials

HTTPS is a secure version of HTTP that is based on a special PKI certificate store. In Cisco DNA Center, HTTPS is used to discover Cisco Enterprise Network Function Virtualization Infrastructure Software (NFVIS) devices only.

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 five global CLI credentials.

Step 1 From the Cisco DNA Center home page, 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 32: CLI Credentials

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

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.

Before you begin
You must have your network's SNMP information.

Step 1
From the Cisco DNA Center home page, 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 33: SNMPv2c Credentials

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 From the Cisco DNA Center home page, 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 34: SNMPv3 Credentials

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Description</td>
<td>Name or description of the SNMPv3 settings that you are adding.</td>
</tr>
<tr>
<td>Username</td>
<td>Name associated with the SNMPv3 settings.</td>
</tr>
</tbody>
</table>
### Security Level

**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.

### Authentication Type

**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.

### SNMPv3 Password

**Auth Password**

SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least 8 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**

Privacy type. (Enabled if you select **AuthPriv** as the authentication mode.) Choose one of the following privacy types:

- **DES**: DES 56-bit (DES-56) encryption in addition to authentication based on the CBC DES-56 standard.
- **AES128**: CBC mode AES for encryption.
- **None**: No privacy.

### SNMPv3 Privacy Password

**Privacy Password**

SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support DES or AES128 encryption. Passwords (or passphrases) must be at least 8 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.
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** From the Cisco DNA Center home page, 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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Specifies the kind of HTTPS credentials you are configuring. Valid types are <strong>Read</strong> or <strong>Write</strong>.</td>
</tr>
<tr>
<td><strong>Read</strong></td>
<td>You can configure up to 5 HTTPS read credentials:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name/Description</strong>: Name or description of the HTTPS credentials that you are adding.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Username</strong>: Name used to authenticate the HTTPS connection.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Password</strong>: Password used to authenticate the HTTPS connection.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Port</strong>: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).</td>
</tr>
</tbody>
</table>

**Note** The password must contain at least one lower case, one upper case, one digit, and a special character and must not contain `< > @ `, `;` `!` or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.
You can configure up to 5 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.
- **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).

**Note** The password must contain at least one lower case, one upper case, one digit, and a special character and must not contain `< > @ ', : ; ! or spaces. For security reasons, enter the password again as confirmation. 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.

### Guidelines for Editing Global Device Credentials

The following are guidelines and limitations for editing existing global device credentials:

- When you edit global device credentials and then apply those changes, there are some device types for which Cisco DNA Center does not support this operation. For a list of devices on which you can apply edited global device credentials, click the **Learn More** link on the top of any Edit window from **Design > Network Settings > 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.
  2. After successfully pushing the credential to the device, Cisco DNA Center confirms it can reach the device using the new credential.
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 > Devices > Inventory screen 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.

See Guidelines for Editing Global Device Credentials, on page 122 for additional information on editing global device credentials.

### Step 1

From the Cisco DNA Center home page, choose Design > Network Settings > Device Credentials.

### Step 2

With the Global site selected, select the device credential you want to change, then under the Actions column on the right, click Edit.

**Note** When you edit global device credentials and then apply those changes, there are some device types for which Cisco DNA Center does not support this operation. For a list of devices on which you can apply edited global device credentials, click the Learn More link on the top of any Edit window from Design > Network Settings > Device Credentials.

### Step 3

Make the required changes, then click Save.

### Step 4

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 Run Now radio button and click Apply.
- To schedule the update for a later time, click the Schedule 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 appears indicating whether the device credential change was successful or if it failed.

**Step 5** To view the status of the credential change, from the Cisco DNA Center home page, 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 your cursor 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 your cursor 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** From the Cisco DNA Center home page, 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 from release 1.3.

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 Digital Network Architecture Center Administrator Guide**.

**Step 1** From the Cisco DNA Center home page, choose **Design > Network Settings > IP Address Pools**.

**Step 2** Click **Add** and complete the required fields in the resulting 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 IP address pool appears in the IP Address Pools table. You can click the **IPv4** or **IPv6** option in the **SUBNET TYPE** table 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 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 Digital Network Architecture Center Administrator Guide*.

---

**Step 1**  From the Cisco DNA Center home page, 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 chose the IP address pools to import, then click **Import**.

---

**Import IP Address Pools from CSV File**

You can import IP address pools from a CSV file.

---

**Step 1**  From the Cisco DNA Center home page, 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 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**.
What to do next

Reserve an IP Pool

Before you begin

Ensure that one or many IPAddressPools have been created

Step 1
From the Cisco DNA Center home page, choose **Design > Network Settings > IP Address Pools**.

Step 2
From the **Network Hierarchy** pane, 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 Pool Name**: Unique name for the reserved IP address pool.
- **Type**: Type of IP address pool. For LAN automation, choose **LAN**.
- **IP Address Space**: IPv4 and IPv6 address pool from which you want to reserve all or part of the IP addresses.
- **CIDR Prefix/No. 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 \( \text{\textbackslash}'64 \) as the **CIDR Prefix** for IPv6 IP pool, the **SLAAC** option is checked. (When **SLAAC** is selected, the devices automatically acquire an IP addresses without the need for DHCP servers.)
- **Gateway IP Address**: Gateway IP address.
- **DHCP Servers**: DHCP server(s) IP 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 revert to a single-stack IP pool. To switch back to single stack, release the IP pools and assign them afresh.

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
From the Cisco DNA Center home page, 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**.
Configure Global Network Servers

You can define global network servers that become the default for your entire network.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>From the Cisco DNA Center home page, choose <strong>Design &gt; Network Settings &gt; Network</strong>.</td>
</tr>
</tbody>
</table>
| **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** | (Optional) You can enter Syslog, SNMP Trap, and NetFlow Collector server information. Click **Add Servers** to add an NTP server.  
**Note** To trigger the fabric compliance checks, configure the SNMP server with the IP address of Cisco DNA Center. For more information, see **Add a Device to a Fabric**. |
| **Step 5** | 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 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 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. Subsequently, any changes to those devices in Cisco ISE are sent automatically to Cisco DNA Center.

**Step 1** From the Cisco DNA Center home page, 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 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 an ISE IP populates the primary and additional IP address drop-down lists with Policy Service Nodes (PSN) IP addresses for the selected 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-ISE AAA servers registered in the **System Settings**.

**Step 7** Click **Save**.

---

**Configure Cisco WLC 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.

This section contains information about the following topics:

- **Prerequisites for Configuring Cisco Wireless Controller High Availability**, on page 129
- **Configure Cisco Wireless Controller HA**, on page 129
- **What Happens During or After the High Availability Process is Complete**, on page 130
- **Commands to Configure and Verify High Availability**, on page 130
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 From the Cisco DNA Center home page, choose Provision > Devices.
Step 2 Click WLC-1 to configure the device as a primary controller.
Step 3 Click the High Availability tab.
Step 4 Choose the Select Secondary WLC drop-down list.
Step 5 Enter the Redundancy Management IP and Peer Redundancy Management IP addresses 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 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 After HA is initiated, the Redundancy Summary under the High Availability tab 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.
Note
There is no real-time data display for the Redundancy Summary. During HA pairing, under Device Inventory, the wireless controller shows Synching but under Provision > WLC, it shows Sync Completed.

You must perform HA on the wireless controller before adding it to the connectivity domain. Also, ensure that the Sync status is Complete before adding the wireless controller to the connectivity domain.

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 page, 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`
Create Templates to Automate Device Configuration Changes

- About Template Editor, on page 131
- Create Projects, on page 131
- Create Templates, on page 132
- Template Form Editor, on page 136
- Associate Templates to Network Profiles, on page 140

About Template Editor

Cisco DNA Center provides an interactive editor called Template Editor to author CLI templates. Template Editor is a centralized CLI management tool to help design a set of device configurations that you need to build devices in a branch. When you have a site, office, or branch that uses a similar set of devices and configurations, you can use Template Editor to build generic configurations and apply the configurations to one or more devices in the branch. With Template Editor, you can:

- Create, edit, and delete templates
- Add interactive commands
- Validate errors in the template
- Version control the templates for tracking purposes
- Simulate the templates

Create Projects

Projects are a logical grouping to a set of templates.

Step 1  From the Cisco DNA Center home page, choose **Tools > Template Editor**.
Step 2  In the left pane, click **+ > Create Project**.
Step 3  In the Add New Project window, enter a name, description, and tags for the project.
Step 4  Click Add.
Create Templates

Cisco DNA Center provides regular and composite configuration templates. CLI templates let you choose the elements in the configurations. Cisco DNA Center provides variables that you can replace with actual values and logic statements.

Create a Regular Template

Step 1
From the Cisco DNA Center home page, choose Tools > Template Editor. 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 tree pane, select the project under which you are creating templates, and click the gear icon > Add Templates. Alternately, click + > Add Templates.

Note
The template that you create for day 0 can also be applied for day N.

Step 3
In the Add New Template window, click Regular Template.

Step 4
In the Name text box, enter a unique name for the template.

Step 5
In the Project Name drop-down list, select the project.

The drop-down list is enabled if you are navigating from the > Add Templates path. The drop-down list is disabled if you select a project and click the gear icon > Add Templates in the tree pane.

Step 6
In the Description text box, enter a description for the template.

Step 7
In the Tags text box, enter an intuitive name to tag the templates. Tagging a configuration template helps you to:

- Search a template using the tag name in the search field.
- Use the tagged template as a reference to configure more devices.

Note
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."

Step 8
Click Edit to view the selected device types and choose the device types that you want to apply to the template.

To view the selected devices, choose Selected from the Show drop-down list. By default, all device types are displayed.

There are different granularity levels for choosing 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.
Step 9 After choosing the device types, click Back to Add New Template.

Step 10 From the Software Type drop-down list, choose the software type: IOS, IOS-XE, IOS-XR, NX-OS, Cisco Controller, Wide Area Application Services, Adaptive Security Appliance, NFV-OS, and Others.

For more information on the Cisco Wireless Controller supported software versions and the minimum supported version, see Cisco DNA Center Supported Devices document.

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.

Step 11 In the Software Version text box, enter the software version. 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 12 Click Add. The template is created and shown in the tree view under the project you selected.

Step 13 You can edit the template content by selecting the template that you created in the left menu. To edit the template content, see Edit Templates, on page 135.

Step 14 In the Template Editor window, enter content for the template. You can use the Velocity Template Language (VTL) to write the content in the template. For information about using VTL, see http://velocity.apache.org/engine/devel/vtl-reference.html.

After saving the template, Cisco DNA Center checks for any errors in the template. If there are any velocity 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. Local variables (variables that are used in for loops, assigned though a set, and so on) are ignored.

Step 15 To validate the template, from the Actions drop-down list, choose Check for errors.

Cisco DNA Center checks for the following errors and reports them:

- Velocity syntax errors.
- Conflicts with blacklisted commands. See Blacklisted Commands, on page 134.

Step 16 To save the template content, from the Actions drop-down list, choose Save.

Step 17 To commit the template, from the Actions drop-down list, choose Commit. You can see only the committed templates in the network profile section.

Note You can associate only a committed template to a network profile.

What to do next

1. Enter additional information for variables in the template. For more information, see Template Form Editor, on page 136.

2. Edit templates. For more information, see Edit Templates, on page 135.

3. Assign templates to profiles. For more information, see Associate Templates to Network Profiles, on page 140.
Blacklisted Commands

Blacklisted commands are commands that are added to the blacklisted category. You can use these commands only through the Cisco DNA Center applications. If you use blacklisted 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.

Use the following query to determine which blacklisted commands are part of Cisco DNA Center:

```
select commands from cliconfigtree where sdnconfig_id in (select id from SDNConfig where classname like 'SPFServiceConfig')
```

Sample Templates

**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 together 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**
From the Cisco DNA Center home page, choose **Tools > Template Editor**.

**Step 2**
In the left pane, select the project under which you are creating the templates. Choose ✂️ > Add Templates or click ✖️ > Add Templates.

**Step 3**
In the Add New Template window, click the Composite Template radio button to create a composite sequential template.

**Step 4**
In the Name text box, enter a unique name for the template.

**Step 5**
In the Project Name text box, enter a unique name for the project.

The text box is enabled if you are navigating from the ✂️ > Add Templates path. The text box is disabled if you select a project and choose ✂️ > Add Templates in the tree pane.
Step 6  In the Description text box, enter a description for the template.

Step 7  In the Tags text box, enter an intuitive name to tag the templates. Tagging a configuration template helps you to:
  • Search a template using the tag name in the search field.
  • Use the tagged template as a reference to configure more devices.

**Note** 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, the following error occurs during provisioning: "Cannot select the device. Not compatible with template."

Step 8  Click Edit to view the selected device types and choose the device types that you want to apply to the template.

You can view the selected devices by choosing Selected from the Show drop-down list. By default, all device types are displayed.

Step 9  Click Back to Add New Template.

Step 10  From the Software Type drop-down list, choose the software type. 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.

Step 11  In the Software Version text box, enter the software version. 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 12  Click Add. The composite template is created and is listed in the left menu under the project you selected.

Step 13  Click the composite template that you created in the tree view pane.

Step 14  In the Template Editor window, drag and drop templates from the tree view pane to create a sequence. 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 and 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 15  To abort 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 16  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 to it.

**Step 1**  From the Cisco DNA Center home page, choose Tools > Template Editor.

**Step 2**  Select the template that you want to edit in the left tree pane.

The Template Editor window appears in the right pane.
**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.

**Note**  Velocity template framework restricts the use of variables starting with a number. Hence, you must ensure that the variable name starts with a letter and not with a number.

**Step 4**  Validate the template by selecting **Check for errors** from the **Actions** drop-down list. Cisco DNA Center checks for these errors and reports them:

- Velocity syntax error
- Conflicts with blacklisted commands

**Step 5**  From the **Actions** drop-down list, choose **Save** to save the template content.

**Step 6**  From the **Actions** drop-down list, choose **Commit** to commit the template content.

---

**What to do next**

1. Assign templates to profiles and provision the template. See *Associate Templates to Network Profiles*, on page 140.

---

**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**  Choose **Tools > Template Editor**.

**Step 2**  From the left menu, choose the template that you want to edit.

The Template Editor window appears in the right pane.

**Step 3**  In the top-right corner, click the Simulator icon to run simulation on commands.

- From the **Actions** drop-down list, choose **New Simulation**. In the **New Simulation** window, enter a name for the simulation, and click **Submit**.
- In the **Simulation Input** form, complete the required fields, and click **Run**. The results are displayed in the **Template Preview** window.

---

**Template Form Editor**

**Step 1**  Select the template in the left tree pane. The template window opens.

**Step 2**  Click the **Form Editor** icon to add metadata to the template variables. All the variables that are identified in the template are displayed. You can configure the following metadata:
• 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 variable and check the Not a Variable check box if you don't 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.

• 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 3**
After configuring metadata information, from the Actions drop-down list, choose Save.

**Step 4**
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 5**
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. In Cisco DNA Center Release 1.1, you had to manually enter values for every variable defined in the template.

In Release 1.2 and later, 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.

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** From the Cisco DNA Center home page, 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`.
- 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.

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.

**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 user input is required.

An interactive command contains the input that must be entered following the execution of a command. To enter an interactive command in the CLI Content area, use the following syntax:
CLI Command

```plaintext
#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.

In response to the interactive command 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:

```plaintext
#INTERACTIVE
cfg 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:

```plaintext
#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:

```plaintext
<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

Choose Design > Network Profiles, and click Add Profile.

There are three types of profiles available:

- **Routing & NFV**—Select this to create a routing and NFV profile. See Routing &NFV for more information.
- **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.
  
  **Note** 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 132.

  - Click Save.

- **Wireless**—Select this to create a wireless profile. Before assigning 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 gets populated.
  - Under Attach Template(s) area, select the template you want to provision from the Template drop-down list.
  - Click Save to save the profile.

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.
Create Templates to Automate Device Configuration Changes

Associate Templates to Network Profiles

- 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 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 appears 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 which are bound to source from the drop-down lists.
  - 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**.
Associate Templates to Network Profiles
Run Diagnostic Commands on Devices

- About Command Runner, on page 143
- Run Diagnostic Commands on Devices, on page 143

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.

Before you begin

Perform the following procedures before you begin using Command Runner:

1. First, install the Command Runner application. From the Cisco DNA Center home page, click the gear icon (⚙️), and then choose System Settings > Software Updates > Installed Apps. Find the Command Runner application and click Install.

2. 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**
From the Cisco DNA Center home page, click Command Runner in Tools.

The Command Runner window appears.

**Step 2**
From the Select one or more device(s) drop-down list, choose a device or devices on which to run diagnostic CLI commands.

A Device List with your selection appears.

**Step 3**
Either select another device to add to the list or click your selected device or devices to close them.
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 4: In the Add a Command field, enter a CLI command and click Add.

Step 5: Click Run Command(s).

If successful, a Command(s) executed successfully message appears.

Step 6: Click the command displayed underneath the device to view the command output.

The complete command output is displayed in the Command Runner window.

Step 7: Click Copy CLI to copy the command output to your clipboard so that you can paste it to a text file, if necessary.

Step 8: Click Previous Page to return to the previous window.

Note: If necessary, click the x symbol next to a device name to remove the device from the device list. Similarly, click the x symbol next to a command to remove the command from the command list.
CHAPTER 10

Configure Telemetry Profile

- About Telemetry, on page 145
- Configure a Telemetry Profile, on page 145
- Apply a Telemetry Profile to the Devices, on page 146
- Update Telemetry Profiles to Use a New Cluster Virtual IP Address, on page 147

About Telemetry

The Telemetry tool allows you to configure and apply profiles on devices for monitoring and assessing their health.

Configure a Telemetry Profile

You can create telemetry assessment profiles for your network devices using the Telemetry tool.

Note

By default, the Disable-Telemetry profile is configured by Network Data Platform (NDP) on all interfaces on all capable devices.

Before you begin

Discover the devices in your network using Cisco DNA Center.

Step 1

From the Cisco DNA Center home page, choose Telemetry from the Tools area.

The Telemetry window appears.

Step 2

Click the Site View tab and check to see if network devices are listed in this window.

Note

After configuring telemetry profiles, you will have to return to this window and apply the telemetry profiles to your devices.

Step 3

Click the Profile View tab.

The Profile View table displays the following information:
Apply a Telemetry Profile to the Devices

You can apply telemetry assessment profiles to your network devices using the Telemetry tool.

Before you begin

Perform the following preliminary tasks:

- Discover the devices in your network using Cisco DNA Center.
- Review and configure the available telemetry profiles using the Telemetry Profile View options and fields.

Step 1
From the Cisco DNA Center home page, click Telemetry in Tools.

The Telemetry window appears.

Step 2
Click the Site View tab.

Step 3
Review the Site View table in this tab.

The following information is displayed:

- Device Name: Name of the device.
Configure Telemetry Profile

Update Telemetry Profiles to Use a New Cluster Virtual IP Address

- **Address**: IP address of the device.
- **Type**: Type of device.
- **Family**: Device category; for example, switch, router, access point.
- **Version**: Software version currently running on the device.
- **Profile**: Applied telemetry profile on the device.
- **Details**: Telemetry assessment of the device. This assessment includes information about SNMP, NetFlow, Syslog, and SNMP traps on the device. Additionally, information is provided as to whether the device is capable of sending telemetry data, is actually sending this telemetry data, or whether the device is enabled to send this telemetry data.

**Step 4** Check the check box next to the **Device Name** of a device to add a telemetry profile to that device.

**Step 5** Click the **Actions** button and select a telemetry profile from the drop-down list.

**Step 6** From the **Show** drop-down menu, select the telemetry profile you just applied.

The device should appear in the filtered list, along with any other devices that have also been configured with the same telemetry profile.

---

**What to do next**

Cisco DNA Center uses the telemetry profiles configured in this procedure to determine what data types to capture. These data types are then used in monitoring the health of the network devices.

Access Cisco DNA Assurance and review both **Assurance Health** and **Assurance Issues** to check the health of your network devices.

---

**Update Telemetry Profiles to Use a New Cluster Virtual IP Address**

If you are using the Cisco DNA Center Telemetry tool 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 the Cisco DNA Center that you are using. You can check this by logging in to the Cisco DNA Center web interface and using the **About** option to view the Cisco DNA Center version number. For example, if the version you are using begins with 1.1, it is in the 1.1.x release train.
- 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 master 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 Digital Network Architecture Center Installation Guide.
- Obtain the Linux username (**maglev**) and password configured on the master 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 Digital Network Architecture Center Installation Guide.

---

Step 1
Access the Cisco DNA Center GUI and use the Telemetry tool to push the Disable Telemetry profile to all the nodes, as follows:

a) From the Cisco DNA Center home page, scroll down to the Tools area and click Telemetry.

b) Click the Site View tab.

c) In the Site View table, choose all the sites and devices currently being monitored.

d) Click the Actions button and choose the Disable Telemetry profile from the drop-down list.

e) Wait for the Site View table to show that telemetry has been disabled for the sites and devices.

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 master 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 master node:

$$
\textit{sudo maglev-config update}
$$
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.

From Cisco DNA Center 1.2.5 and later, you must configure one virtual IP per configured interface. We recommend that you enter the \textit{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. Use the commands for the release train that is appropriate for your Cisco DNA Center version.

For versions of Cisco DNA Center in the 1.1.x release train (versions 1.1.1 and later, up to but not including 1.2.0), enter the following commands:

```
magctl service restart -d netflow-go
magctl service restart -d syslog
magctl service restart -d trap
magctl service restart -d wirelesscollector
```

For Cisco DNA Center in the 1.2.x release train (versions 1.2.0 and later), enter the following commands:

```
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. For example, if you are using a version of Cisco DNA Center in the 1.2.x release train, enter the following command:
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 use the Telemetry tool to push the **Optimal Visibility** profile to all nodes, as you did in Step 1.
Update Telemetry Profiles to Use a New Cluster Virtual IP Address
CHAPTER 11

Configure Policies

- Policy Overview, on page 151
- Policy Dashboard, on page 151
- Group-Based Access Control Policies, on page 152
- IP-Based Access Control Policies, on page 156
- Application Policies, on page 162
- Traffic Copy Policies, on page 194
- Virtual Networks, on page 197

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.

Policy Dashboard

The Policy Dashboard window shows the number of virtual networks, group-based access control policies, IP-based access control policies, traffic copy policies, scalable groups, and IP network groups that you have created. In addition, it shows the number of policies that have failed to deploy.

The Policy Dashboard window provides a list of policies and the following information about each policy:

- **Policy Name**—Name of policy.
- **Policy Type**—Type of policy. Valid types are Access Control and Traffic Copy.
- **Policy Version**—Iteration of policy. Each time a policy is changed and saved, it is incremented by one version. For example, when you create a policy and save, the policy is at Version 1. If you change the policy and save it again, the version of the policy is incremented to Version 2.
- **Modified By**—User who modified the particular version of a policy.
- **Description**—Word or phrase that identifies a policy.
Group-Based Access Control Policies

Group-based access control policies are Security Group Access Control Lists (SGACLs). Cisco DNA Center integrates with Cisco ISE to simplify the process of creating and maintaining SGACLs.

During the initial Cisco DNA Center and Cisco ISE integration, scalable groups and policies that are present in Cisco ISE are propagated to Cisco DNA Center and placed in the default virtual network.

Note

Cisco DNA Center does not support access control policies with logging as an action. Therefore, Cisco ISE does not propagate any such policies to Cisco DNA Center.

Depending on your organization's configuration and its access requirements and restrictions, you can segregate the scalable groups into different virtual networks to provide further segmentation.

A group-based access control policy has two main components:

- **Scalable Groups**: Scalable groups comprise a grouping of users, end-point devices, or resources that share the same access control requirements. These groups (known in Cisco ISE as security group) are defined in Cisco ISE. A scalable group may have as few as one item (one user, one end-point device, or one resource) in it.

- **Access Contract**: An access contract is a common building block that is used in both group-based and IP-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.

Before you can create group-based access control policies, make sure that Cisco ISE is integrated with Cisco DNA Center. Verify that the scalable groups have been propagated to Cisco DNA Center from Cisco ISE. To do this, from the Cisco DNA Center home page, choose Policy > Group-Based Access Control > Scalable Groups. You should see scalable groups populated under the Scalable Groups tab. If you do not see any scalable groups, verify that Cisco ISE is integrated correctly.

After you create a group-based access control policy, Cisco DNA Center translates the policy into an SGACL, which is ultimately deployed on a device.

The following sample procedure describes the process of authentication and access control that a user experiences after logging in to the network:

1. A user connects to a port on a switch and provides credentials.
2. The switch contacts Cisco ISE.
3. Cisco ISE authenticates the user and downloads the SGACLs to the port to which the user is connected.
4. The user is granted or denied access to specific users or devices (servers) based on the access granted in the SGACLs.
Workflow to Configure a Group-Based Access Control Policy

Before you begin

- Make sure that you have integrated Cisco ISE with Cisco DNA Center.
- In Cisco ISE, make sure that the work process setting is configured as **Single Matrix** so that there is only one policy matrix for all devices in the TrustSec network.

---

**Step 1**  
(Optional) Create virtual networks. Depending on your organization's configuration and its access requirements and restrictions, you can segregate your groups into different virtual networks to provide further segmentation.

For more information, see Create a Virtual Network, on page 198.

**Step 2**  
(Optional) Create scalable groups. After you integrate Cisco DNA Center with Cisco ISE, the scalable groups that exist in Cisco ISE are propagated to Cisco DNA Center. If a scalable group that you need does not exist, you can create it in Cisco ISE.

For more information, see Create a Group-Based Scalable Group, on page 153.

**Step 3**  
Create an access control contract. A contract defines a set of rules that dictate the action (allow or deny) that network devices perform based on the traffic matching particular protocols or ports.

For more information, see Create a Group-Based Access Control Contract, on page 154.

**Step 4**  
Create a group-based access control policy. The access control policy defines the access control contract that governs traffic between source and destination scalable groups.

For information, see Create a Group-Based Access Control Policy, on page 155.

---

Create a Group-Based Scalable Group

You can access Cisco ISE through the Cisco DNA Center interface to create scalable groups. After you have added a scalable group in Cisco ISE, it is synchronized with the Cisco DNA Center database so that you can use it in an access-control policy.

**Note**  
You cannot edit or delete scalable groups from Cisco DNA Center; you need to perform these tasks from Cisco ISE. After you delete a scalable group from Cisco ISE, the scalable group name is not removed from the Cisco DNA Center policy dashboard. Instead, the Cisco DNA Center policy dashboard displays the scalable group in red text to indicate that it has been deleted.

---

**Step 1**  
From the Cisco DNA Center home page, choose Policy > Group-Based Access Control > Scalable Groups.

All of the scalable groups that have been created in Cisco ISE are displayed.

**Step 2**  
Click Add Groups.

Cisco DNA Center opens a direct connection to the Cisco ISE server, where you can add the scalable group.
Step 3  In Cisco ISE, create scalable groups (called security groups in Cisco ISE).
For more information, see the Cisco Identity Services Engine Administrator Guide.

Step 4  Return to Cisco DNA Center.

Create a Group-Based Access Control Contract

Step 1  From the Cisco DNA Center home page, choose Policy > Group-Based Access Control > Access Contract.
Step 2  Click Add Contract.
Step 3  In the dialog box, 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 as the protocol.
  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.
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 a Group-Based Access Control Contract

If you edit a contract that is used in a policy, the policy's state changes to MODIFIED in the Group-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, redeploy the policy to the network.

Step 1  From the Cisco DNA Center home page, choose Policy > Group-Based Access Control > Access Contracts.
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 a Group-Based Access Control Contract, on page 154.
  Note  If you make changes to a contract that is used in a policy, you need to deploy the modified policy by choosing Policy > Group-Based Access Control > Group-Based Access Control Policies, checking the check box next to the policy name, and clicking Deploy.
  • To delete the contract, click Delete.
Create a Group-Based Access Control Policy

Step 1  From the Cisco DNA Center home page, choose Policy > Group-Based Access Control > Group-Based Access Control Policies.

Step 2  Click Add Policy. The Add Policy dialog box is displayed.

Step 3  In the Policy Name field, enter the name of the policy. The name can be up to 255 alphanumeric characters in length, including hyphens (-) and underscore (_) characters.

Step 4  In the Description field, enter a word or phrase that identifies the policy.

Step 5  In the Contract field, click Add Contract. Contract field has rules that govern the network interaction between the source and destination scalable groups.

Step 6  In the dialog box, click the radio button next to the contract that you want to use.

Step 7  Alternatively, you can select the permit (permit all traffic) or deny (deny all traffic) contract.

Step 8  Check the Enable Policy check box, if the policy is not active.

If you uncheck the Enable Policy check box, the policy is disabled and it is saved only to Cisco DNA Center. The policy is not synchronized with Cisco ISE or deployed in the network.

Step 9  Check the Enable Bi-directional check box, to enable the contract for traffic flowing in both directions (from the source to the destination and from the destination to the source).

If you want the traffic to flow only from the source to the destination, uncheck the Enable Bi-directional check box.

Step 10  To define the source-scalable groups, drag and drop the scalable groups from the Available Security Groups area to the Source Scalable Groups area.

Step 11  To define the destination scalable groups, drag and drop the scalable groups from the Available Security Groups area to the Destination Scalable Groups area.

Step 12  Click Save.

Edit or Delete a Group-Based Access Control Policy

You can edit or delete only the policies that you created in Cisco DNA Center. Policies that were imported from Cisco ISE during the Cisco DNA Center and Cisco ISE integration cannot be edited or deleted from Cisco DNA Center. You need to edit or delete these policies from Cisco ISE.

If you edit a policy, the policy's state changes to MODIFIED on the Group-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, redeploy the policy to the network.

Step 1  From the Cisco DNA Center home page, choose Policy > Group-Based Access Control > Group-Based Access Control 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 tasks:

- To make changes, click Edit, make the changes, and click Save. For field definitions, see Create a Group-Based Access Control Policy, on page 155.
Deploy a Group-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  From the Cisco DNA Center home page, choose Policy > Group-Based Access Control > Group-Based Access Control.
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.

The site time zone setting is not supported for scheduling application policy deployments.

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

- To create IP network groups from the Policy > IP Based Access Control > IP Network Groups window, make sure that you have integrated Cisco ISE with Cisco DNA Center. However, 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.

  Note Editing an IP network group on the Policy > IP Based Access Control window is possible without Cisco ISE. But the creation of IP network groups from the IP Based Access Control window requires Cisco ISE.

- 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 127.
  - Device credentials, such as CLI, SNMP, HTTP, and HTTPS: See About Global Device Credentials, on page 117.
  - IP address pools: See Configure IP Address Pools, on page 124.
  - Wireless settings as SSIDs, wireless interfaces, and wireless radio frequency profiles: See Configure Global Wireless Settings, on page 97.
  - Provision devices: See Provisioning, on page 201.

Step 1 Create IP network groups.
For more information, see Create an IP Network Group, on page 158.

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 159

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 160.

Configure Global Network Servers
You can define global network servers that become the default for your entire network.
You can override global network settings on a site by defining site-specific settings.

**Step 1**
From the Cisco DNA Center home page, 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**
(Optional) You can enter Syslog, SNMP Trap, and NetFlow Collector server information. Click **Add Servers** to add an NTP server.

*Note*
- To trigger the fabric compliance checks, configure the SNMP server with the IP address of Cisco DNA Center.
- For more information, see **Add a Device to a Fabric**.

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

---

### Create an IP Network Group

**Step 1**
From the Cisco DNA Center home page, 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**
From the Cisco DNA Center home page, 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 158.
Create an IP-Based Access Control Contract

Step 1  From the Cisco DNA Center home page, choose Policy > IP Based Access Control > Access Contract.
Step 2  Click Add Contract.
Step 3  In the dialog box, 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 as the protocol.
   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.
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  From the Cisco DNA Center home page, 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 159.
      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
From the Cisco DNA Center home page, choose Policy > IP Based Access Control > IP Based Access Control Policies.

Step 2
Click Add Policy.

Step 3
Complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Name</td>
<td>Name of the policy.</td>
</tr>
<tr>
<td>Description</td>
<td>Word or phrase that identifies the policy.</td>
</tr>
<tr>
<td>SSID</td>
<td>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. <strong>Note</strong> 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.</td>
</tr>
<tr>
<td>Site Scope</td>
<td>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 163.</td>
</tr>
<tr>
<td>Source</td>
<td>Origin of the traffic that is affected by the contract. From the SearchSource drop-down list, choose an IP network group. If the IP network that you want is not available, click +Group to create one.</td>
</tr>
<tr>
<td>Contract</td>
<td>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.</td>
</tr>
<tr>
<td>Destination</td>
<td>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.</td>
</tr>
</tbody>
</table>
Configure Policies

Configure 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**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direction</td>
<td>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 <strong>One-Way</strong>. To enable the contract for traffic flowing in both directions (from the source to the destination and from the destination to the source), select <strong>Bi-directional</strong>.</td>
</tr>
</tbody>
</table>

---

**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** From the Cisco DNA Center home page, 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 160.
- 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. From the Cisco DNA Center home page, choose Policy > IP Based Access Control > IP Based Access Control Policy.

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. For more information, see Applications and Application Sets, on page 163.

- **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. For more information, see Site Scope, on page 163.

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.


- 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.

Applications and Application Sets

Applications are the software programs or network signaling protocols that are being 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 also 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 it 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. For more information, see Custom Applications, on page 167. You can also create custom application sets to contain any applications that you want.

## 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 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.

## 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 Queuing (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 allows you to 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.

**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 36: Marking, Queuing, and Dropping Treatments

<table>
<thead>
<tr>
<th>Business Relevance</th>
<th>Application Class</th>
<th>Per-Hop Behavior</th>
<th>Queuing and Dropping</th>
<th>Application Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relevant</td>
<td>VoIP&lt;sup&gt;1&lt;/sup&gt;</td>
<td>Expedited Forwarding (EF)</td>
<td>Priority Queuing (PQ)</td>
<td>VoIP telephony (bearer-only) traffic; for example, Cisco IP phones.</td>
</tr>
<tr>
<td>Broadcast Video</td>
<td></td>
<td>Class Selector (CS) 5</td>
<td>PQ</td>
<td>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.)</td>
</tr>
<tr>
<td>Real-time Interactive</td>
<td></td>
<td>CS4</td>
<td>PQ</td>
<td>Inelastic high-definition interactive video applications and audio and video components of these applications; for example, Cisco TelePresence.</td>
</tr>
<tr>
<td>Multimedia Conferencing</td>
<td></td>
<td>Assured Forwarding (AF) 41</td>
<td>Bandwidth (BW) Queue and Differentiated Services Code Point (DSCP) Weighted Random Early Detect (WRED)</td>
<td>Desktop software multimedia collaboration applications and audio and video components of these applications; for example, Cisco Jabber and Cisco WebEx.</td>
</tr>
<tr>
<td>Multimedia Streaming</td>
<td></td>
<td>AF31</td>
<td>BW Queue and DSCP WRED</td>
<td>Video-on-Demand (VoD) streaming video flows and desktop virtualization applications, such as Cisco Digital Media System.</td>
</tr>
<tr>
<td>Network Control</td>
<td></td>
<td>CS6</td>
<td>BW Queue only&lt;sup&gt;2&lt;/sup&gt;</td>
<td>Network control-plane traffic, which is required for reliable operation of the enterprise network, such as EIGRP, OSPF, BGP, HSRP, IKE, and so on.</td>
</tr>
<tr>
<td>Signaling</td>
<td></td>
<td>CS3</td>
<td>BW Queue and DSCP</td>
<td>Control-plane traffic for the IP voice and video telephony infrastructure.</td>
</tr>
<tr>
<td>Operations, Administration, and Management (OAM)</td>
<td></td>
<td>CS2</td>
<td>BW Queue and DSCP&lt;sup&gt;2&lt;/sup&gt;</td>
<td>Network operations, administration, and management traffic, such as SSH, SNMP, syslog, and so on.</td>
</tr>
<tr>
<td>Transactional Data (Low-Latency Data)</td>
<td></td>
<td>AF21</td>
<td>BW Queue and DSCP WRED</td>
<td>Interactive (foreground) data applications, such as enterprise resource planning (ERP), customer relationship management (CRM), and other database applications.</td>
</tr>
<tr>
<td>Bulk Data (High-Throughput Data)</td>
<td></td>
<td>AF11</td>
<td>BW Queue and DSCP WRED</td>
<td>Noninteractive (background) data applications, such as email, file transfer protocol (FTP), and backup applications.</td>
</tr>
</tbody>
</table>
### 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 cannot define custom applications for wireless devices.

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, 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.

---

### Favorite Applications

Cisco DNA Center allows you to flag applications that you want to configure on devices before all other applications, except custom 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 171.
Although there is no limit to the number of applications that you can mark as favorite, designating only a small number of favorite applications, for example, less 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 an administrator notices a lot of unwanted Netflix traffic on his network, the administrator might chose to flag Netflix as a favorite application (despite it being assigned as business irrelevant). In this case, Netflix will be programmed into the device policies before other business-irrelevant applications, ensuring that the business intent of controlling this application is realized.

---

**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 37: Default SLA Attributes for SP Profiles with 4 Classes**

<table>
<thead>
<tr>
<th>Class Name</th>
<th>DSCP</th>
<th>Priority Class</th>
<th>SLA Bandwidth (%)</th>
<th>Remaining Bandwidth (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>EF</td>
<td>Yes</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Class 1 Data</td>
<td>AF31</td>
<td></td>
<td>44</td>
<td></td>
</tr>
<tr>
<td>Class 2 Data</td>
<td>AF21</td>
<td></td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>Default</td>
<td>0</td>
<td></td>
<td>31</td>
<td></td>
</tr>
</tbody>
</table>

**Table 38: Default SLA Attributes for SP Profiles with 5 Classes**

<table>
<thead>
<tr>
<th>Class Name</th>
<th>DSCP</th>
<th>Priority Class</th>
<th>SLA Bandwidth (%)</th>
<th>Remaining Bandwidth (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>EF</td>
<td>Yes</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Class 1 Data</td>
<td>AF31</td>
<td></td>
<td>44</td>
<td></td>
</tr>
<tr>
<td>Class 2 Data</td>
<td>AF21</td>
<td></td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>Class Name</td>
<td>DSCP</td>
<td>Priority Class</td>
<td>SLA</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>-------</td>
<td>----------------</td>
<td>--------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Bandwidth (%)</td>
<td>Remaining Bandwidth (%)</td>
</tr>
<tr>
<td>Class 3 Data</td>
<td>AF11</td>
<td>—</td>
<td>—</td>
<td>1</td>
</tr>
<tr>
<td>Default</td>
<td>Best Effort</td>
<td>—</td>
<td>—</td>
<td>30</td>
</tr>
</tbody>
</table>

*Table 39: Default SLA Attributes for SP Profiles with 6 Classes*

<table>
<thead>
<tr>
<th>Class Name</th>
<th>DSCP</th>
<th>Priority Class</th>
<th>SLA</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Bandwidth (%)</td>
</tr>
<tr>
<td>Class 1 Data</td>
<td>AF31</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Class 3 Data</td>
<td>AF11</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Video</td>
<td>AF41</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Voice</td>
<td>EF</td>
<td>Yes</td>
<td>10</td>
</tr>
<tr>
<td>Default</td>
<td>0</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Class 2 Data</td>
<td>AF21</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

*Table 40: Default SLA Attributes for SP Profiles with 8 Classes*
Queuing Profiles

Queuing profiles allow you to define an interface's bandwidth allocation based on the interface speed and the traffic class.

Note

Queueing 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 41: Default CVD LAN Queuing Policy

<table>
<thead>
<tr>
<th>Traffic Class</th>
<th>Default Bandwidth (Total = 100%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>10%</td>
</tr>
<tr>
<td>4</td>
<td>100%</td>
</tr>
<tr>
<td>Traffic Class</td>
<td>Default Bandwidth (Total = 100%)</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Broadcast Video</td>
<td>10%</td>
</tr>
<tr>
<td>Real-Time Interactive</td>
<td>13%</td>
</tr>
<tr>
<td>Multimedia Conferencing</td>
<td>10%</td>
</tr>
<tr>
<td>Network control</td>
<td>3%</td>
</tr>
<tr>
<td>Signaling</td>
<td>2%</td>
</tr>
<tr>
<td>OAM</td>
<td>2%</td>
</tr>
<tr>
<td>Transactional Data</td>
<td>10%</td>
</tr>
<tr>
<td>Bulk Data</td>
<td>4%</td>
</tr>
<tr>
<td>Scavenger</td>
<td>1%</td>
</tr>
<tr>
<td>Best Effort</td>
<td>25%</td>
</tr>
</tbody>
</table>

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.

   - Custom applications are assigned rank 1 by default.
   - Default NBAR applications are not assigned a rank until you mark them as favorites, at which point they are assigned rank 10,000.

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.

- Custom applications are assigned popularity 10 by default.
- 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:

<table>
<thead>
<tr>
<th>Application Configuration Order</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Custom application, custom_realtime</td>
<td>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.</td>
</tr>
<tr>
<td>2. Custom application, custom_salesforce</td>
<td>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 Transactional Data traffic class. Their popularity does not come into play because the processing order has been determined by their traffic class.</td>
</tr>
<tr>
<td>3. Favorite application, gss-http</td>
<td>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.</td>
</tr>
<tr>
<td>4. Favorite application, corba-iiop</td>
<td></td>
</tr>
<tr>
<td>5. All other, default NBAR applications</td>
<td></td>
</tr>
</tbody>
</table>
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 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, as follows:

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 figure below, 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 4: 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 174.
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 Digital Network Architecture 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.
Policy versioning does not capture changes to applications (such as rank, port, and protocol), application set members, LAN queuing profiles, and sites.

**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 effect.

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.
Application Policy Guidelines and Limitations

- Cisco DNA Center cannot learn multiple Wireless LANs (WLANs) with the same SSID name on a Wireless Controller (WLC). At any point, Cisco DNA Center will have 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 also cause issues. For example, one device has a WLAN configured as a non-fabric 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 non-fabric 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.

Configure Applications and Application Sets

The following subsections describe the various tasks that you can perform in the context of applications and application sets.

Change an Application's Settings

You can change the application set or traffic class of an existing NBAR application.

**Step 1**
From the Cisco DNA Center home page, choose Policy > Application > Applications.

**Step 2**
Use the Search, Show, or View By fields to locate the application that you want to change.

**Step 3**
Click the application name.

**Step 4**
In the dialog box, change one or both settings:
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 From the Cisco DNA Center home page, click Policy > Application > Applications.
Step 2 Click Add Application.
Step 3 In the dialog box, provide the necessary information in the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application name</td>
<td>Name of the custom application. The name can contain up to 24 alphanumeric characters, including underscores and hyphens. The underscore and hyphen characters are the only special character allowed in the application name.</td>
</tr>
<tr>
<td>Type</td>
<td>Method by which users access the application. Choose Server Name for applications that are accessible through a server.</td>
</tr>
<tr>
<td>Server Name</td>
<td>Name of the server that hosts the application.</td>
</tr>
<tr>
<td>Similar To</td>
<td>Application with similar traffic-handling requirements. Click the radio button to select this option, 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.</td>
</tr>
<tr>
<td>Traffic Class</td>
<td>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.</td>
</tr>
<tr>
<td>Application Set</td>
<td>Application set that 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-social-networking, database-apps, desktop-virtualization, email, enterprise-ipc, file-sharing, generic-browsing, generic-media, generic-misc, generic-tunneling, intranet-apps, naming-services, network-control, network-management, remote-access, saas-apps, signaling, software-development-tools, software-updates, streaming-media.</td>
</tr>
</tbody>
</table>
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 From the Cisco DNA Center home page, click Policy > Application > Applications.
Step 2 Click Add Application.
Step 3 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 characters are the only special character allowed in the application name.
Step 4 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 5 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 6 Check the IP/Port Classifiers check box to define the IP address or 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 7 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 8 From the Application Set drop-down list, chose 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, database-apps, desktop-virtualization, email, enterprise-ipc, file-sharing, generic-browsing, generic-media, generic-misc, generic-tunneling, intranet-apps, naming-services, network-control, network-management, remote-access, saas-apps, signaling, software-development-tools, software-updates, streaming-media.
Step 9 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 From the Cisco DNA Center home page, click Policy > Application > Applications.
Step 2 Click Add Application.
The Add Application dialog box appears.
**Step 3**
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. The underscore and hyphen characters are the only special character allowed in the application name.

**Step 4**
For **Type**, click the **URL** radio button.

**Step 5**
In the **URL** field, enter the URL used to reach the application.

**Step 6**
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 7**
From the **Application Set** drop-down list, choose an application set in which you want the application to reside.

**Step 8**
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**
From the Cisco DNA Center home page, choose **Policy > Application > Applications**.

**Step 2**
Use the **Search**, **Show**, or **View By** fields to locate the application that you want to change.

**Step 3**
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 177, Create an IP Address and Port-Based Custom Application, on page 178, or Create a URL-Based Custom Application, on page 178.
- b) Click **OK**

**Step 4**
To delete the application: Click ⌘ in the application box and then click **OK** to confirm.

---

### Move an Application from an Application Set

You can move applications from one application set to another application set.

**Step 1**
From the Cisco DNA Center home page, choose **Policy > Application > Application Sets**.

**Step 2**
Use the **Search**, **Show**, or **View By** fields to locate the applications or application sets that you want to change.
Create a Custom Application Set

If none of the application sets fit your needs, you can create a custom application set.

**Step 1** From the Cisco DNA Center home page, choose **Policy > Application > Application Sets**.
**Step 2** Click **Add Application Set**.
**Step 3** In the dialog box, enter a name for the new application set.
Cisco DNA Center creates the new application set; however, it will have no applications in it.
**Step 4** Click **OK**.
**Step 5** Use the **Search**, **Show**, or **View By** fields to locate the application set.
**Step 6** Locate the applications that you want to move into the new application set.
**Step 7** Check the check box next to the applications that you want to move.
**Step 8** 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** From the Cisco DNA Center **Home** page, choose **Policy > Application > Application Sets**.
**Step 2** Use the **Search**, **Show**, or **View By** fields to locate the application set that you want to change.
**Step 3** 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.
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 a favorite has a yellow star next to it.

When you add or edit a policy, applications marked as 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 167.

Step 1
From the Cisco DNA Center home page, choose Policy > Application > Applications.

Step 2
Locate the application that you want to mark as a favorite.

Step 3
Click ⭐.

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 Digital Network Architecture 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.

- 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 193.

- 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 Device Role (Inventory), on page 51.

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 Device Role (Inventory), on page 51.

• Add devices to sites. For more information, see Add a Device to a Site, on page 216.

• If you have applications that are not defined in Cisco DNA Center, you can add them and define their QoS attributes. For more information, see Custom Applications, on page 167.

• 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 ServiceProvider Profiles, on page 126.

• If you want some applications configured before others on devices, mark these applications as favorites. For more information, see Mark an Application as Favorite, on page 181.

---

**Step 1**  
From the Cisco DNA Center home page, 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 which 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** will be 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 site you are interested in.

  b)  
  From the list of devices in the site, click **Configure** in the **SP Profile Settings** column next to the device you are interested in.

  **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 favorites are listed at the top of the application set. To change favorites, go to the Applications registry. For information, see Mark an Application as Favorite, on page 181

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 application that you are interested in.
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 end points (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 endpoint.

Step 15 (Optional) Preview the CLI commands that will be sent to devices. For more information, see Preview an Application Policy, on page 189.

Step 16 (Optional) Precheck the devices on which you plan to deploy the policy. For more information, see Precheck an Application Policy, on page 189.

Step 17 Do one of the following tasks:

- Preview the policy configurations that will be applied to a device by clicking Preview. For more information, see Policy Preview, on page 174.
- Save the policy as a draft by clicking Save Draft. For more information, see Policy Drafts, on page 173.
- 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 174.

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 From the Cisco DNA Center home page, 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 173 and Policy Versioning, on page 174.
- Policy Status—State of the policy. If the policy applied on Cisco Catalyst 3850, Catalyst 4500, and Catalyst 9K devices, is impacted by the port channel update (createmodify/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 aborted.

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 displays the details of the effective marking policy that was deployed to the device. 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 | From the Cisco DNA Center home page, 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 181. |
| 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: |
  • Preview the policy configurations that will be applied to a device by clicking **Preview.** For more information, see Policy Preview, on page 174. |
  • Save the policy as a draft by clicking **Save Draft.** For more information, see Policy Drafts, on page 173. |
• 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 174.

**Note** 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** From the Cisco DNA Center home page, choose **Policy > Application > Application Policies**.

**Step 2** Create an Application Policy, Edit an Application Policy, or Clone an Application Policy a policy.

**Step 3** Click **Save Draft**.

For more information, see **Policy Drafts**, on page 173.

---

### 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** Auto-QoS config is automatically removed from Cisco Catalyst 3850, Catalyst 3650, and Catalyst 9K devices before the policy is deployed.

**Step 1** From the Cisco DNA Center home page, 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  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 have 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. So, if you have 40 devices or less 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, then 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.

**Procedure**

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.

---

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>From the Cisco DNA Center home page, choose Policy &gt; Application &gt; Application Policies.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Use the Filter field to locate the policy that you want to delete.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Click the radio button next to the policy that you want to delete.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>From the Actions drop-down list, choose Undeploy Policy.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>In the Undeploy Policy window, click the Delete policy from devices radio button and click Apply.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>To confirm the deletion, click OK. Otherwise, click Cancel.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>a) Click the failed state link under Deployment Status in the Application Policies page.</td>
</tr>
<tr>
<td></td>
<td>b) In the Undeployment Status window, click Retry to delete the policy.</td>
</tr>
</tbody>
</table>
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 From the Cisco DNA Center home page, 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 181.
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 173.
   • 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 174.

Note: 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 From the Cisco DNA Center home page, 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 Do one of the following tasks:
   • Click OK to confirm the change or Cancel to abort 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 162.

**Step 1** From the Cisco DNA Center home page, 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 abort 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** From the Cisco DNA Center home page, choose Policy > Application > Application Policies.

**Step 2** Create or edit a policy, as described in Create an Application Policy, on page 181 or Edit an Application Policy, on page 185.

**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** From the Cisco DNA Center home page, choose Policy > Application > Application Policies.

**Step 2** Create or edit a policy, as described in Create an Application Policy, on page 181 or Edit an Application Policy, on page 185.

**Step 3** Before deploying the policy, click Preview.
A list of the devices within the scope appears.

**Step 4** 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 Digital Network Architecture 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** From the Cisco DNA Center homepage, 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** From the Cisco DNA Center homepage, 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**  From the Cisco DNA Center home page, choose **Policy > Application > Queuing Profile**.

**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**  From the Cisco DNA Center home page, choose **Policy > Application > Queuing Profile**.

**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 191**.
- 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 168.

Before you begin

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

Step 1
From the Cisco DNA Center home page, 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 165.

- **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 181.

Step 1  From the Cisco DNA Center home page, 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.
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.
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 158.

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 195.

Step 2
Create a traffic copy contract.
The contract defines the copy destination. For information, see Create a Traffic Copy Contract, on page 196.

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 197.

Create a Traffic Copy Destination

Step 1
From the Cisco DNA Center home page, choose Policy > Traffic Copy > Traffic Copy Destination.

Step 2
Enter a name and description for the traffic copy destination.
Edit or Delete a Traffic Copy Destination

Step 1 From the Cisco DNA Center homepage, 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 From the Cisco DNA Center homepage, choose Policy > Traffic Copy > Traffic Copy Contracts.
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 195.
Step 5 Click Save.

Edit or Delete a Traffic Copy Contract

Step 1 From the Cisco DNA Center homepage, choose Policy > Traffic Copy > Traffic Copy Contracts.
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  From the Cisco DNA Center home page, 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  From the Cisco DNA Center home page, 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 (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 limitations:

- You can create only one guest virtual network.
- VRFs are common across all domains. The maximum number of VRFs is based on the device with the fewest VRFs in the domain.

Create a Virtual Network

You can create a virtual network to segment your physical network into multiple logical networks.

**Step 1**
From the Cisco DNA Center home page, choose **Policy > Virtual Network**.

**Step 2**
Click + to create a new Virtual Network.

**Step 3**
In the **Network Name** field, enter the name of the virtual network.

**Step 4**
Check the **Guest Virtual Network** check box, to configure the virtual network as a guest network. You can create only one guest virtual network.

Devices that are configured with special rules, which allows guests limited access.

**Step 5**
Drag and drop groups from the **Available Scalable Groups** area to the **Groups in the Virtual Network** area.

**Step 6**
Click Save.

Edit or Delete a Virtual Network

If you move a scalable group from one custom virtual network to another custom 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**
From the Cisco DNA Center home page, choose **Policy > Virtual Network**.

**Step 2**
Do one of the following tasks:

- To edit the virtual network, click the name of the virtual network from the left navigation pane and modify the information in the following table, except the virtual network name:
Table 42: Virtual Network Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Name</td>
<td>Name of the virtual network. (Cannot be modified.)</td>
</tr>
<tr>
<td>Guest Virtual Network</td>
<td>Devices that are configured with special rules, which allow guests limited access. Check this check box to configure the virtual network as a guest network. You can create only one guest virtual network.</td>
</tr>
<tr>
<td>Available Groups</td>
<td>Scalable groups that you can choose to include in the virtual network. Drag and drop groups from the Available Groups area to the Groups in the Virtual Network area.</td>
</tr>
<tr>
<td>Groups in the Virtual Network</td>
<td>Scalable groups that are in the virtual network. Drag and drop groups from the Available Groups area to the Groups in the Virtual Network area.</td>
</tr>
</tbody>
</table>

- To delete the virtual network, click and confirm the deletion.
Configure Policies

Edit or Delete a Virtual Network
Provision Your Network

- Provisioning, on page 201
- Onboarding Devices with Plug and Play Provisioning, on page 201
- Add a Device to a Site, on page 216
- Tag Devices, on page 216
- Tag Devices Using Rules, on page 217
- Edit Device Tags, on page 218
- Provisioning Devices, on page 218
- Check the LAN Automation Status, on page 253
- Delete a Device After Provisioning, on page 253
- Fabric Sites and Fabric Domains, on page 254
- Multi-Site Fabric Domain, on page 254
- Transit Sites, on page 254
- Configuring Fabric Domains, on page 256

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 inventory.
- Adding devices to sites.
- Creating fabric domains and adding devices to the fabric.

Onboarding 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 your Cisco credentials in the main Cisco DNA Center settings by using **System Settings > Settings > Cisco Credentials**. For more information, see "Configure Cisco Credentials" in the *Cisco Digital Network Architecture Center Administrator Guide*.

- Accept the End User License Agreement (EULA) in the main Cisco DNA Center settings by using **System Settings > Settings > Device EULA Acceptance**. For more information, see "Accept the License Agreement" in the *Cisco Digital Network Architecture Center Administrator Guide*.

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 76.

2. Define network profiles for the types of devices you are deploying. See *Create Network Profiles*, on page 111.

3. 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 61.

4. 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 most 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 131.

5. Add details about planned devices one at a time or in bulk with a CSV file. See *Add or Edit a Device*, on page 208 or *Add Devices in Bulk*, on page 209.

6. 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 203. 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 206.
2. Claim the device by assigning a site, image, configuration template, or profile. See Provision a Device With Plug and Play, on page 211.

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 to synchronize with. See Register or Edit a Virtual Account Profile, on page 209.
2. Synchronize the device inventory from the Smart Account. See Add Devices from a Smart Account, on page 210.
3. Find the device on the devices list by filtering on unclaimed devices or searching for it by name. See View Devices, on page 206.
4. Claim the device by assigning a site, image, configuration template, or profile. See Provision a Device With Plug and Play, on page 211.
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 203.
- DNS—See DNS Controller Discovery, on page 205.
- Cisco Plug and Play Connect cloud service—See Plug and Play Connect Controller Discovery, on page 205.

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)**
- **Ixxx.xxx.xxx.xxx;i**—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.
- **Jxxx**—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**
- **TtrustpoolBundleURL;**—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: Ttftp://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.
- **Zxxx.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 using DNS. For more information, see *DNS Controller Discovery, on page 205.*
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 pnpnntpserver.

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 pnpnntpserver.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 pnpnntpserver.

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 209.

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 211.

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.

---

### 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**  From the Cisco DNA Center home page, choose **Provision > Devices > 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 211.
- **Edit**: Edits the device. See Add or Edit a Device, on page 208.
- **Reset**: Resets the device if it is in an error state. See Reset a Device, on page 215.
- **Delete**: Deletes the device. See Delete a Device, on page 215.

**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 208, Add Devices in Bulk, on page 209, or Add Devices from a Smart Account, on page 210.

The Device table displays the information shown in the following table for each device. All of the columns support sorting. Click the column header to sort the rows in ascending order. 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 43: Device Information

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#</td>
<td>Row number.</td>
</tr>
<tr>
<td><strong>Device Name</strong></td>
<td>Name of the device. Click this link to open the device details window. A stack icon indicates a switch stack.</td>
</tr>
<tr>
<td><strong>Serial Number</strong></td>
<td>Device serial number.</td>
</tr>
<tr>
<td><strong>Product ID</strong></td>
<td>Device product ID.</td>
</tr>
<tr>
<td><strong>Source</strong></td>
<td>Source of the device entry:</td>
</tr>
<tr>
<td></td>
<td>• User: User added the device through the GUI or API.</td>
</tr>
<tr>
<td></td>
<td>• Network: Unclaimed device that has contacted the controller.</td>
</tr>
<tr>
<td></td>
<td>• SmartAccount: Device was synced from a Smart Account.</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>• Unclaimed: Device has not been provisioned.</td>
</tr>
<tr>
<td></td>
<td>• Planned: Device has been claimed but has not yet contacted the server.</td>
</tr>
<tr>
<td></td>
<td>• Onboarding: Device onboarding is in progress.</td>
</tr>
<tr>
<td></td>
<td>• Provisioned: Device is successfully onboarded and added to inventory.</td>
</tr>
<tr>
<td></td>
<td>• Error: Device had an error and could not be provisioned.</td>
</tr>
<tr>
<td><strong>Onboarding State</strong></td>
<td>Onboarding state of the device.</td>
</tr>
<tr>
<td><strong>Site</strong></td>
<td>Site with which the device is associated.</td>
</tr>
<tr>
<td><strong>Last Contact</strong></td>
<td>Last date and time the device contacted Plug and Play.</td>
</tr>
<tr>
<td><strong>Smart Acct</strong></td>
<td>Cisco Smart Account with which the device is associated.</td>
</tr>
<tr>
<td><strong>Virtual Acct</strong></td>
<td>Virtual Account (within the Cisco Smart Account) with which the device is associated.</td>
</tr>
</tbody>
</table>
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 44: Device Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Number</td>
<td>Device serial number (read only if you are editing a device).</td>
</tr>
<tr>
<td>Product ID</td>
<td>Device product ID (read only if you are editing a device).</td>
</tr>
<tr>
<td>Device Name</td>
<td>Device name.</td>
</tr>
<tr>
<td>Enable SUDI Authorization</td>
<td>Enables secure unique device identifier (SUDI) authorization on devices that support it.</td>
</tr>
<tr>
<td>SUDI Serial Numbers</td>
<td>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 <strong>Enable SUDI Authorization</strong> is checked.</td>
</tr>
<tr>
<td>This Device Represents a Stack</td>
<td>Device represents a stack (this item is read only if you are editing a device). Applicable only for supported stackable switches.</td>
</tr>
</tbody>
</table>

**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 117.

---

**Step 1** From the Cisco DNA Center home page, choose **Provision > Devices > 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** Add or edit a device as follows:

- **To add a device**, click **Add Device** and the **Add Devices** dialog is displayed.
- **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 211.
• 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.

Note
If you add a device that already exists in Plug and Play, there is no change to the existing device.

Step 1 From the Cisco DNA Center home page, choose Provision > Devices > Plug and Play.
Step 2 Click Add Device.
   The Add Devices dialog is displayed.
Step 3 Click the Bulk Devices tab.
Step 4 Click Download File Template to download the sample file.
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 211.

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 45: Virtual Account Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Smart Account</td>
<td>Cisco Smart Account name.</td>
</tr>
<tr>
<td>Select Virtual Account</td>
<td>Virtual account name. Virtual accounts are subaccounts within a Cisco Smart Account.</td>
</tr>
<tr>
<td>Use as Default Controller Profile</td>
<td>Check this check box to register this Cisco DNA Center controller as the default controller in the Cisco Plug and Play Connect cloud portal.</td>
</tr>
<tr>
<td>Controller IP or FQDN</td>
<td>IP address or fully qualified domain name of this Cisco DNA Center controller.</td>
</tr>
<tr>
<td>Profile Name</td>
<td>Controller profile name.</td>
</tr>
</tbody>
</table>

Before you begin

Set the Cisco Smart Account credentials in the main Cisco DNA Center settings by using System Settings > Settings > Cisco Credentials. For more information, see "Configure Cisco Credentials" in the Cisco Digital Network Architecture Center Administrator Guide.

Step 1
From the Cisco DNA Center home page, click System Settings > Settings > Cisco Credentials.

Step 2
Click the PnP Connect tab. 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 Add. 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 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.

Step 5
Save the settings by doing one of the following:

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 210.

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 information shown below for each profile.
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 209.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>From the Cisco DNA Center home page, choose <strong>Provision &gt; Devices &gt; Plug and Play</strong>.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Click <strong>Add Device</strong>. The <strong>Add Devices</strong> dialog is displayed.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Click the <strong>Smart Account Devices</strong> tab.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Click the radio button next to the name of the Plug and Play Connect virtual account profile from which you want to add devices.</td>
</tr>
</tbody>
</table>
| **Step 5** | 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 211.

**Provision a Device With Plug and Play**

Provisioning or claiming a device provisions it by deploying an image and an onboarding configuration to it, or a network profile for wireless devices, 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.

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 212
- **Wireless Access Points and Sensors**—See **Provision a Wireless or Sensor Device**, on page 213
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.

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 the devices being provisioned can discover and contact Cisco DNA Center. For more information, see Controller Discovery Prerequisites, on page 203.
- Define the site within the network hierarchy. See About Network Hierarchy, on page 76.
- Define network profiles for the devices. See Create Network Profiles, on page 111.
- 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 61.

---

**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 63. 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. In most 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 131.

---

**Step 1** From the Cisco DNA Center home page, choose Provision > Devices > 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, Site Assignment.

**Step 5** From the Site drop-down list, choose a site to assign to each device.

To apply the same site to all devices, click the Apply to all check box.

**Step 6** Click Next.

The Configuration window appears.

**Step 7** (Optional) In the Image drop-down list, choose a golden software image to apply to the device.
If you do not want to deploy an image, check the **Skip golden image upgrade** check box.

**Step 8**  
(Optional) In the **Template** drop-down list, choose an onboarding configuration template to apply to the device. Click the eye icon next to a selected template to view the template.

**Step 9**  
(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.

**Step 10**  
(Optional) In the **Select a License Level** drop-down list, choose the stack license level.  
This item appears only for switches that support stacking.

**Step 11**  
If you selected multiple devices to provision, click the next device in the list at the left side of the window and repeat the configuration steps, until you have done this for all devices.

**Step 12**  
Click **Next**.  
The **Advanced Configuration** window appears.

**Step 13**  
For each device, 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.

**Step 14**  
To specify parameter values 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 15**  
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 16**  
Click **Next**.  
The **Summary** window appears, where you can view details about the device, image, and configuration templates.

**Step 17**  
Click the **Day-0 Configuration Preview** section to expand it and check that the configuration preview was successful.  
If the preview was not successful, you should resolve any issues before claiming the device, to avoid provisioning errors. You may need to go back to the **Advanced Configuration** step and change parameter values, change the template, revisit the **Design** area to update network design settings, or resolve any network connectivity issues.

**Step 18**  
If you selected multiple devices to provision, click the next device in the list at the left side of the window and check if the configuration preview was successful, until you have done this for all devices.

**Step 19**  
Click **Claim** to claim the devices and start the provisioning process.

---

**Provision a Wireless or Sensor Device**

Claiming a device provisions it by assigning a network profile 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.
This procedure explains how to claim a device from the main Plug and Play tab. Alternatively, you can claim a device from the device details window by clicking Claim.

Before you begin

- Ensure that the devices being provisioned can discover and contact Cisco DNA Center. For more information, see Controller Discovery Prerequisites, on page 203.
- Define the site within the network hierarchy. See About Network Hierarchy, on page 76.
- 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.
- 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 ASCII 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 106.
- Define wireless sensor device profiles for wireless sensor devices. See Create a Wireless Sensor Device Profile, on page 108.
- For Mobility Express access points, define an IP address pool and a management interface. See Configure IP Address Pools, on page 124.

**Step 1**
From the Cisco DNA Center home page, choose Provision > Devices > Plug and Play.

**Step 2**
Click the Plug and Play tab.

The table lists all of the devices. 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**
Choose Actions > Claim in the menu bar above the device table.

The Claim Devices window opens, showing the first step, Site Assignment.

**Step 5**
From the Site drop-down list, choose a site to assign to each device.

To apply the same site to all devices, click the Apply to all check box. Wireless devices can be assigned only to floors within a building, not to the building itself.

**Step 6**
Click Next.

The Configuration window appears.

**Step 7**
For a wireless sensor device, in the Sensor Profile drop-down list, choose the sensor device profile to assign to the device.

**Step 8**
If you selected multiple devices to provision, click the next device in the list at the left side of the window and repeat the profile selection, until you have done this for all devices.

**Step 9**
Click Next.
The Advanced Configuration window appears.

**Step 10**
Click Next.

The Summary window appears, where you can view details about the device and configuration.

**Step 11**
Click the Day-0 Configuration Preview section to expand it and check that the configuration preview was successful. If the preview was not successful, you should resolve any issues before claiming the device, to avoid provisioning errors. Ensure that the wireless LAN controller that is managing the device has been added to the inventory and assigned to the site where the wireless device is assigned. You may need to resolve any network connectivity issues.

**Step 12**
Click Claim to claim the devices and start the provisioning process.

---

**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 tab. 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**
From the Cisco DNA Center home page, choose Provision > Devices > Plug and Play.

**Step 2**
Click the Plug and Play tab.

The table lists all of the devices. 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 delete.

**Step 4**
Click Actions > Delete in the menu bar above the device table.

A confirmation dialog box is displayed.

**Step 5**
Click Delete to confirm that you want to delete the devices.

---

**Reset a Device**

Resetting a device applies only to devices in the Error state 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.
This procedure shows how to reset a device from the Plug and Play tab. Alternatively, you can reset it from the device details window by clicking Reset.

**Step 1**
From the Cisco DNA Center home page, choose **Provision > Devices > Plug and Play**.

**Step 2**
Click the **Plug and Play** tab.

The table lists all of the devices. 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 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**.

---

**Add a Device to a Site**

**Step 1**
From the Cisco DNA Center home page, click **Provision**.

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**.

---

**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**
From the Cisco DNA Center home page, click **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.
- If you are creating a new tag, click **Create New Tag**. You can also create a new tag with a rule. See *Tag Devices Using Rules*, on page 217 for more information.
- If you are using an existing tag, select the tag from the list, 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, then click **Apply**.
- Hover your cursor over the tag icon or tag name, 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**
From the Cisco DNA Center home page, click **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** From the Cisco DNA Center home page, click **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 you want to edit.

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

---

### Provisioning Devices

#### Provision a Cisco Wireless 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 127.
  - Device credentials, such as CLI, SNMP, HTTP, and HTTPS. For more information, see **Configure Global CLI Credentials**, on page 117, **Configure Global SNMPv2c Credentials**, on page 118, **Configure Global SNMPv3 Credentials**, on page 119, and **Configure Global HTTPS Credentials**, on page 121.
  - IP address pools. For more information, see **Configure IP Address Pools**, on page 124.
  - Wireless settings as SSIDs, wireless interfaces, and wireless radio frequency profiles. For more information, see **Configure Global Wireless Settings**, on page 97.

- Discover devices in your network by running **Discovery** so that the discovered devices are listed in the **Inventory** window.
Make sure that Cisco Wireless Controller is added to a site. For more information, see Add a Device to a Site, on page 216.

You cannot make manual configuration changes to a Cisco Wireless Controller, that is managed by Cisco DNA Center. You must perform all configurations from the Cisco DNA Center user interface.

**Step 1**
From the Cisco DNA Center home page, choose **Provision**.

The **Devices > 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 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 controller 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.

**Step 7**
In the **Choose a site** window, select a site and click **Save**.

**Step 8**
Click **Next**.

The **Configuration** window appears.

**Step 9**
Select a role for the wireless controller: **Active Main WLC** or **Guest Anchor WLC**.

**Step 10**
Click **Select Primary Managed AP Locations** to select managed AP locations for the controller.

**Step 11**
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, all the children under the parent site are also selected. You can uncheck the check box to uncheck a particular site.

**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 12**
Click **Save**.

**Step 13**
For an active main wireless controller, you must configure the interface and VLAN details. Under the **Interface and VLAN Configuration** area, click + **Add**.

Interface and VLAN configuration is applicable for nonfabric wireless controller provisioning.

The **Configure Interface and VLAN** window appears.

**Step 14**
From the **Interface Name** drop-down list, choose the interface name.

**Step 15**
In the **VLAN ID** field, enter a value for the VLAN.

**Step 16**
In the **Interface IP Address** field, enter a value for the interface IP address.

**Step 17**
In the **Interface Net Mask (in bits)** field, enter the subnet mask of the interface.

**Step 18**
In the **Gateway IP Address** field, enter the IP address of the gateway.

**Step 19**
From the **LAG/Port Number** drop-down list, choose the link aggregation or the port number.
Step 20  Click OK.

Step 21  For a guest anchor wireless controller, you can change the VLAN ID configuration by changing the VLAN ID under Assign Guest SSIDs to DMZ site.

Step 22  Click Next.

The Advanced Configuration window appears, where you can enter values for predefined template variables.

Step 23  You can search for the device or the template in the Devices panel.

Step 24  Enter a value for the predefined template variable in the wlanid field.

Step 25  Click Next.

The Summary window displays the following information:

- Device Details
- Network Settings
- SSID
- Managed Sites
- Interfaces
- Advanced Configuration

Step 26  Click Deploy to provision the 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 27  Next, provision the secondary controller.

For more information, see Configure N+1 High Availability from Cisco DNA Center, on page 227.

Step 28  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 29  After the devices are deployed successfully, the Provision Status changes from Configuring to Success.

Step 30  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 further take.

Step 31  Click See Details under Device Provisioning.

Step 32  Click View Details under Deployment of network intent, and click the device name.

Step 33  Expand the Configuration Summary area to view the operation details, feature name, and the management capability. The configuration summary also displays any error that occurred while provisioning the device.

Step 34  Expand the Provision Summary area to view details of the exact configuration that is sent to the device.
Provision Routing and NFV Profiles

Before you begin

Make sure that you have defined the following global network settings before provisioning a NFV profile:

- Network servers, such as AAA, DHCP, and DNS. For more information, see Configure Global Network Servers, on page 127.

- Device credentials, such as CLI, SNMP, HTTP, and HTTPS. For more information, see Configure Global CLI Credentials, on page 117, Configure Global SNMPv2c Credentials, on page 118, Configure Global SNMPv3 Credentials, on page 119, and Configure Global HTTPS Credentials, on page 121.

- IP address pools. For more information, see Configure IP Address Pools, on page 124.

- SP profiles. For more information, see Configure Service Provider Profiles, on page 126.

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

From the Cisco DNA Center home page, 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 is 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 the 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 and Assign Device to Site window appears. Click Choose a Site to assign a site.

Step 6

From the Actions drop-down list, choose Provision > Provision.

To provision a 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 on O and enter the WAN IP address. Review the details in the +Edit Services window. Click Next.

  Note  You have to configure vManage settings in system setting page, before provisioning vEDGE related service. For more information see the section Configure vManage Properties in Cisco Digital Network Architecture 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 have selected Gigabit ethernet as the line interface, click **O** and enter the WAN IP address if you select static IP address. If you select DHCP, enter 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 which is configured as the primary WAN from the dropdown list.
  - If you have selected cellular as the line interface, click **O**, choose **IP Negotiated** and select the **Interface Name** from the drop down list and enter the **Access Point Name (APN)**. Check the check box next to **PAP** or **CHAP** depending on your service provider.
- Enter **IP SLA Address** for the backup WAN interface when you have multiple service providers.

This window will 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 **Interface(s)** drop down list.

**Note**  Only Cisco 1100 Series Integrated Services Routers are supported for switchport interface.

- Review the details in the **Custom Configuration** window, and click **Next**. This window will appear only if the routing profile has Day-0 and Day-N templates configured.
- Review the details in the **Summary** page.

**Step 7**  Click **Deploy** to provision the device.

The **Provision Status** column in the **Device Inventory** window shows **SUCCESS** after a successful deployment. Click **SUCCESS** to see detailed Provisional log status.

---

**Provision a Cisco AP—Day 1 AP Provisioning**

**Before you begin**

Make sure that you have Cisco AP in your inventory. If you do not, discover APs using the Discovery feature. See **Discover Your Network**, on page 11.

**Step 1**  From the Cisco DNA Center home page, choose **Provision**.

The **Devices > 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 is 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 get the list of APs that are discovered and reachable.
Step 4  Check the check box adjacent the AP device name that you want to provision.

Step 5  From the Action drop-down list, choose Provision > Provision.

Step 6  The Assign Site window appears.

Step 7  Click Choose a floor, and assign an AP to the site.

Step 8  In the Choose a floor window, select the floor to which you want to associate the AP, and click Save.

Step 9  Click Next.

The Configuration window appears.

Step 10 By default, the custom RF profile that you marked as default under 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 RF profile selected.

Step 11 Click Next.

Step 12 In the Summary window, review the device details, and click Deploy to provision the AP.

• To deploy the AP immediately, click the Now radio button, and click Apply.

• To schedule the AP deployment for a later date and time, click the Later radio button and define the date and time of the deployment.

Step 13 You are prompted with a message that creation or modification of an AP group in progress.

You are prompted with a message stating After provisioning AP(s) will reboot. Do you want to continue?

Step 14 Click OK.

The Last Sync Status column in the Device Inventory window shows SUCCESS if the deployment is successful.

---

Provision a Brownfield Device

**Before you begin**

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brownfield support is available for Cisco AireOS Wireless Controller devices and not for Cisco Catalyst 9800 Series Wireless Controller devices.</td>
</tr>
</tbody>
</table>

With the Cisco DNA Center, you can add and provision brownfield devices such as wireless controllers to the network. Brownfield refers to devices that belong to existing sites with pre-existing infrastructure.

• 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 11 and About Inventory, on page 37.

• The wireless controller should be reachable and in Managed state on the Inventory window. For more information, see About Inventory, on page 37.
Step 1
From the Cisco DNA Center home page, choose **Provision**.
The **Device > Inventory** window appears, which lists all the discovered devices available in the network.

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 adjacent the 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 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.
**N+1 High Availability**

**Overview of N+1 High Availability**

Cisco DNA Center Release 1.3 introduces support for 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.

The 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 configuration is done as per AP level and configurations are pushed directly to AP instead of 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 should be of the same device type. For example, if the primary device is a Cisco Catalyst 9800 Series Wireless Controller, then the secondary device should also be a Cisco Catalyst 9800 Series Wireless Controller.

Access Points 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:

• The N+1 HA configuration is supported only in a nonfabric deployment.
• 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 have made any changes to the primary controller.
• Fault tolerance is not supported in Cisco DNA Center Release 1.3.
• 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 16, or Discover Your Network Using an IP Address Range, on page 21.
• Make sure that the wireless controllers are reachable and in the managed state.
  For more information, see About Inventory, on page 37 and Display Information About Your Inventory, on page 39.
• Verify the network connectivity between devices. If the primary controller goes down, the AP should be able to join the secondary controller as per N+1 configuration.
• Create two buildings to manage the primary and secondary locations for both the devices. For example, if you have created two buildings such as 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 76, Add Buildings, on page 80, and Add a Floor to a Building, on page 81.
• 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 85.
• Create two SSIDs and associate them to a wireless network profile.
For more information, see Create SSIDs for an Enterprise Wireless Network, on page 97, Create SSIDs for a Guest Wireless Network, on page 100 and Create a Wireless Sensor Device Profile, on page 108.

**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 platforms in a nonfabric deployment.

**Step 1**
From the Cisco DNA Center home page, choose **Provision**.

The **Devices > Inventory** window appears, and all the discovered devices are listed in this window.

**Step 2**
Check the check box adjacent the desired controller to provision 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**
You can add or update the managed AP locations for primary controller by clicking the **Select Primary Managed AP Locations**.

**Step 8**
In the **Managed AP Location** window, check the check box adjacent 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, subnet mask details, and click **Next**.

**Step 11**
In the **Advanced Configuration** window, configure values for the pre-defined template variables, and click **Next**.

**Step 12**
In the **Summary** window, verify the managed AP locations for primary controller and other configuration details, and click **Deploy** to provision the primary 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 13**
Next, provision the secondary controller.

**Step 14**
On the **Inventory** window, check the check box adjacent the desired controller to provision 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 adjacent 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  You can add or update the managed AP locations for secondary controller by clicking **Select Secondary Managed AP Locations**.

Step 20  In the **Managed AP Location** window, check the check box adjacent 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 **Configure Interface and VLAN** area, configure the IP address, subnet mask details for the secondary controller, and click **Next**.

Step 23  In the **Advanced Configuration** window, configure values for the pre-defined template variables, and click **Next**.

Step 24  In the **Summary** window, verify the managed AP locations for secondary controller and other configuration details and, click **Deploy** to provision the secondary 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 25  To verify the managed locations of 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 primary controller.

Step 28  On the **Devices > Inventory** window, check the check box adjacent 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 default under **Network Settings > Wireless > Wireless Radio Frequency Profile** is chosen in the **RF Profile** drop-down list.

Step 33  You can change the default RF Profile value for an AP by selecting a value from the **RF Profile** drop-down list.

Step 34  Click **Next**.

Step 35  In the **Summary** window, review the details.

Step 36  Click **Deploy** to provision the primary AP.

Step 37  You are prompted with a message that creation or modification of an AP group in progress.

You are prompted with a message stating **After provisioning AP(s) will reboot. Do you want to continue?**.

Step 38  Click **OK**.  

The **Last Sync Status** column in the **Device Inventory** window shows **SUCCESS** if the deployment is successful.
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 manageable by Cisco DNA Center
- Catalyst 9800 Embedded Wireless Controller for Catalyst 9300 Series Switches, Catalyst 9400 Series Switches, and Catalyst 9500H Series Switches

The following table lists the supported virtual and hardware platforms for the Cisco Catalyst 9800 Series Wireless Controller:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Catalyst 9800-80 Wireless Controller</td>
<td>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.</td>
</tr>
<tr>
<td>Cisco Catalyst 9800-40 Wireless Controller</td>
<td>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.</td>
</tr>
</tbody>
</table>
Cisco Catalyst 9800 Series Wireless Controller Overview

<table>
<thead>
<tr>
<th>Platform</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9k Series Switches</td>
<td>Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9k 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.</td>
</tr>
</tbody>
</table>

The following table lists the host environments supported by the Cisco Catalyst 9800 Series Wireless Controller:

<table>
<thead>
<tr>
<th>Host Environment</th>
<th>Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware ESXi</td>
<td>• VMware ESXi vSphere 6.0</td>
</tr>
<tr>
<td></td>
<td>• VMware ESXi vSphere 6.5</td>
</tr>
<tr>
<td></td>
<td>• VMware ESXi vCenter 6.0</td>
</tr>
<tr>
<td></td>
<td>• VMware ESXi VCenter 6.5</td>
</tr>
<tr>
<td>KVM</td>
<td>• Linux KVM based on Red Hat Enterprise Linux 7.1 and 7.2</td>
</tr>
<tr>
<td></td>
<td>• Ubuntu 14.04.5 LTS, Ubuntu 16.04.5 LTS</td>
</tr>
<tr>
<td>NFVIS</td>
<td>Cisco ENCS 3.8.1 and 3.9.1</td>
</tr>
</tbody>
</table>

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 N-1 to N upgrade path only. For example, upgrade from Cisco Enterprise NFVIS Release 3.8.x to Cisco Enterprise NFVIS 3.9.x only is supported. Upgrade from Cisco Enterprise NFVIS Release 3.8.x to Cisco Enterprise NFVIS Release 3.10.x is not supported.
## Cisco Enterprise NFVIS Version

<table>
<thead>
<tr>
<th>Cisco Enterprise NFVIS Version</th>
<th>Enterprise Network Compute System (ENCS) Device Platform</th>
<th>Notes</th>
</tr>
</thead>
</table>
| • 3.8.1                       | • ENCS 5400  
• 3.9.1                       | • UCS-E  
• 3.9.2                       | • UCS-C |
| • 3.10.1                      | • 3.10.2    
• 3.10.3                      | • 3.11.1    
• 3.11.2                      | • 3.10.3    
• 3.11.2                      | • 3.11.2    |

| • 3.8.1                       | ENCS 5100   |            |
| • 3.9.1                       | • 3.9.2     | Cisco 5100 Enterprise Network Compute System (ENCS) does not support 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 Digital Network Architecture Center Installation Guide.

2. For information on software image upgrade, see Software Image Upgrade Support for Cisco Catalyst 9800 Series Wireless Controller, on page 234.

3. Log in to the Cisco DNA Center GUI and verify that the applications you need are in the **Running** state.
   To verify, from the Cisco DNA Center home page, click the gear icon 🔄, and then 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 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 16 or Discover Your Network Using an IP Address Range, on page 21.
   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 37 and Display Information About Your Inventory, on page 39.

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 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 78.

To create a new network hierarchy, see Create a Site in a Network Hierarchy, on page 76, Add Buildings, on page 80, and Add a Floor to a Building, on page 81.

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 85.

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 114, Configure Global Network Servers, on page 127, 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 106.

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 124.

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 97 and Create SSIDs for a Guest Wireless Network, on page 100.

15. Create a network profile. For more information, see Create a Wireless Sensor Device Profile, on page 108.

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 197 and Create a Virtual Network, on page 198.

   - Create a group-based access control policy and add a contract. For more information, see Create a Group-Based Access Control Policy, on page 155.

17. Configure high availability.

For more information, see Configure High Availability for Cisco Catalyst 9800 Series Wireless Controller, on page 235.
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 238.

**Software Image Upgrade Support for Cisco Catalyst 9800 Series Wireless Controller**

**Before you begin**

- Discover the Catalyst 9800 Series Wireless Controller.

  Enable NETCONF and set the port to 830 to discover 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 16, or Discover Your Network Using an IP Address Range, on page 21.

- Make sure that the devices appear in the device inventory and are in the Managed state.

  For more information, see About Inventory, on page 37 and Display Information About Your Inventory, on page 39.

---

**Step 1**
From Cisco DNA Center home page, choose Design > Image Repository, or click Image Repository in the Cisco DNA Center home page.

**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 61.

**Step 3**
Assign the software image to a device family.

For more information, see Assign a Software Image to a Device Family, on page 61.

**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 63.

**Step 5**
To provision a software image, click Provision in the Cisco DNA Center home page.

The Devices > Inventory window appears.

**Step 6**
In the Inventory window, check the check box adjacent the Catalyst 9800 Series Wireless Controller whose image you want to upgrade.

**Step 7**
From the Actions drop-down, choose Software Image > Update Image.

For more information, see the Provision a Software Image, on page 63.

---

**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 of Cisco Catalyst 9800 Series Wireless Controller through Cisco DNA Center.
Configure High Availability for Cisco Catalyst 9800 Series Wireless Controller

Before you begin

Here are the prerequisite tasks for configuring High Availability (HA) on Cisco Catalyst 9800 Series Wireless Controller:

- 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
From the Cisco DNA Center home page, choose Provision.

Step 2
The Devices > Inventory window appears, and all the discovered devices are listed in this window.

Step 3
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.

Step 4
All the devices available in that selected site is displayed in the Inventory window.

Step 5
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 6
In the Inventory window, click the desired Catalyst 9800 Series Wireless Controller name to configure as a primary controller.

Step 7
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 8
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 8 From the Select Secondary C9800 drop-down list, choose the secondary controller to create a HA pair.

Step 9 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 Catalyst 9800 Series Wireless Controller. Ensure that these IP addresses are unused IP addresses within the subnet range.

Step 10 In the Netmask field, enter the netmask address.

Step 11 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 12 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 Sync Status 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 13 To manually resynchronize the controller, on the Provision > Inventory window, select the controller that you want to synchronize manually.

Step 14 From the Actions drop-down list, choose Resync.

Step 15 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

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.
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 231.

Step 1
From the Cisco DNA Center home page, choose Provision.

The Devices > Inventory window appears with a list of discovered devices.

Step 2
Check the check box next to the Catalyst 9800 Series Wireless Controller name 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 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.

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 6
Click Save.

Step 7
Click Apply.

Step 8
Provision the device with the configurations that were added during the design phase.

Step 9
Choose Provision > Devices > Inventory.

Step 10
Check the check box next to the Catalyst 9800 Series Wireless Controller name that you want to provision.

Step 11
From the Actions drop-down list, choose Provision > Provision.

Step 12
In the Assign Site window, click Next.

The Configuration window appears.

Step 13
Select a wireless controller role for the Catalyst 9800 Series Wireless Controller device: Active Main WLC.

Step 14
Click Select Primary Managed AP Locations to select a managed AP location for the primary controller.

Step 15
Click Select Secondary Managed AP Locations to select a managed AP location for the secondary controller.

Step 16
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 a particular site.

Note Inheritance of managed AP locations allows you to automatically choose a site along with the buildings and floors under that particular site. One site is managed by only one wireless controller.

Step 17
Click Save.

Step 18
For an active main wireless controller, you need to configure interface and VLAN details.
Step 19  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 20  Click Next.

The Advanced Configuration window appears, where you enter values for the predefined template variables.

Step 21  Search for the device or the template in the Devices panel.

Step 22  Enter a value for the predefined template variable in the wlanid field.

Step 23  Click Next.

Step 24  On the Summary window, review the following configurations:

- Device Details
- Network Setting
- SSID
- Managed Sites
- Interfaces
- Advanced Configuration

Step 25  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 26  To verify configurations that are pushed from Cisco DNA Center to the device, use the following commands on the Catalyst 9800 Series Wireless Controller device:

- `#show wlan summary`
- `#show run | sec line`
- `#show running-configuration`

Step 27  Once the devices are deployed successfully, the Provision Status changes from Configuring to Success.

Step 28  In the Inventory window, click See Details in the Provision Status column against a device to get more information about network intent or to view a list of actions.

Step 29  Click See Details under Device Provisioning.

Step 30  Click View Details under Deployment of network intent, and click the device name.
**Configure and Provision a Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches**

**Supported Hardware Platforms**

<table>
<thead>
<tr>
<th>Device Role</th>
<th>Platforms</th>
</tr>
</thead>
</table>
| 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                                      |
|                         | • 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                                               |

Step 31: Click and expand the device name.

Step 32: Expand the **Configuration Summary** area to view the operation details, feature name, and the management capability. The configuration summary also displays any error that occurred while provisioning device with reasons for failure.

Step 33: Expand the **Provision Summary** area to view details of the exact configuration that is sent to the device.

Step 34: Provision the AP.

For more information, see *Provision a Cisco AP—Day 1 AP Provisioning*, on page 222.
Preconfiguration

On Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9300 Series Switches, 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 automated underlay for provisioning.

Workflow to Configure Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Switches

1. Install Cisco DNA Center.
   See the Cisco Digital Network Architecture Center Installation Guide.
2. Log in to the Cisco DNA Center GUI and verify that the applications you need are in the Running state.
   To verify, from the Cisco DNA Center home page, click the gear icon 🔄, and then choose System Settings > 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 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.
   You do not have to enable NETCONF to discover the edge switches.
   For more information, see Discover Your Network Using CDP, on page 16 or Discover Your Network Using an IP Address Range, on page 21.
   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 37 and Display Information About Your Inventory, on page 39.
   You must wait for all the devices to get into a 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 78.

To create a new network hierarchy, see the Create a Site in a Network Hierarchy, on page 76, Add Buildings, on page 80, and Add a Floor to a Building, on page 81.

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 85.

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 114, Configure Global Network Servers, on page 127, 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 117, Configure Global CLI Credentials, on page 117, Configure Global SNMPv2c Credentials, on page 118, Configure Global SNMPv3 Credentials, on page 119, and Configure Global HTTPS Credentials, on page 121.

10. Configure IP address pools at the global level. These IP addresses are used for end clients and APs.

   To configure an IP address pool, see Configure IP Address Pools, on page 124.

   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; 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 97 and Create SSIDs for a Guest Wireless Network, on page 100.

12. Create a network profile. For more information, see Create a Wireless Sensor Device Profile, on page 108.

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 197 and Create a Virtual Network, on page 198.
14. Provision Cisco Catalyst 9000 Series Switches and the edge node switches with the configurations added during the design phase.

   - Create a group-based access control policy, and add a contract. For more information, see Create a Group-Based Access Control Policy, on page 155.

   - 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. For more information, see Provision Embedded Wireless on Cisco Catalyst 9000 Series Switches, on page 243.

**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 241.

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**  
From the Cisco DNA Center home page, choose **Provision**.

The **Devices > Inventory** window appears with a list of discovered devices.

**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**.

**Step 10**  
Click **Next**.

**Step 11**  
In the **Summary** window, verify the configurations, and click **Deploy**.

**Step 12**  
To provision the edge switch, check the check box next to the edge switch that you want to provision.

**Step 13**  
From the **Actions** drop-down list, choose **Provision**.
Step 14  Click Next.

Step 15  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 16  To add devices to a fabric domain, from the Cisco DNA Center home page, choose Provision > Fabric.

Step 17  Create a fabric LAN. For more information, see Create a Fabric Domain, on page 256.

Step 18  Add an IP transit network.

An IP transit network is used in a regular IP network to connect externally or to connect two or more fabric sites. For more information, see Create an IP Transit Network, on page 255.

Step 19  Add devices and associate virtual networks to a fabric domain. For more information, see Add a Device to a Fabric, on page 257.

Step 20  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.

In the dialog box that appears, configure the following:

- From the Border to field, click one of the radio buttons:
  - Rest of Company (Internal): Designate the device as a border for IP routes inside your company. A border exports fabric routes and imports outside routes.
  - Outside World (External): Designate the device as a default border for IP routes outside your company. A border exports fabric routes only.
  - Anywhere (Internal & External): Designate the device as a border for both internal and external IP routes. A border exports fabric routes and imports outside routes, except default-route.

- In the Local Autonomous Number field, enter the local autonomous number for the device.

- From the Select the IP Pool drop-down list, choose the IP address pool that should be part of the virtual network. Cisco DNA Center uses this IP pool to configure the automatic border handoff from the fabric.

- Check the Connected to the Internet check box to select this border node to advertise internet services to other fabric borders.

- From the Select Transit drop-down list, click Add to choose a transit network to enable on the border device.

- Click Add Interface.

The Add Interface dialog box appears.

- From the External Interface drop-down list, choose the interface connecting from a fabric network to an IP transit network.

- In the Remote AS Number field, enter the autonomous system number for the device.

- Expand the Virtual Network drop-down list, and check the virtual network check box. This virtual network should be advertised by the border to the remote peer. You can select one, multiple, or all virtual networks.

- Click Save.

- Click Add.
- Click Save.

  A success message saying Devices updated to fabric domain successfully is displayed.

**Step 21**
Click the edge switch and choose Add to Fabric.

**Step 22**
Click Save.

**Step 23**
To enable embedded wireless on the device, click the device that is added as a CP+Border+Edge or CP+Border, and choose Enable 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 24**
Click OK to install the image manually.

**Step 25**
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 26**
Click Import.

The progress of the import is displayed.

**Step 27**
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 28**
Click Yes.

The device reboots and comes online after the device package upgrade is complete.

**Step 29**
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 30**
Click Next.

**Step 31**
Review the details on the Summary window, and click Save.

**Step 32**
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 33**
From the Cisco DNA Center home page, click the Provision tab.

**Step 34**
Click the Fabric tab.

A list of fabric domains is displayed.

**Step 35**
Select the fabric domain that was created, and click the Host Onboarding tab to enable IP pool for APs.

**Step 36**
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 37**
Under Virtual Networks, click INFRA_VN to associate one or more IP pools with the selected virtual network.

**Step 38**
Check the IP Pool Name check box that was created for APs during the design phase.

**Step 39**
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 40**
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.
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 238.

Scale Information

This table shows the device scalability information.

<table>
<thead>
<tr>
<th>Fabric Constructs</th>
<th>Cisco Catalyst 9300 Series Switches</th>
<th>Cisco Catalyst 9400 Series Switches</th>
<th>Cisco Catalyst 9500 Series Switches</th>
<th>Cisco Catalyst 9500-H Series Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Networks</td>
<td>256</td>
<td>256</td>
<td>256</td>
<td>256</td>
</tr>
<tr>
<td>Local End Points/Hosts</td>
<td>4K</td>
<td>4K</td>
<td>4K</td>
<td>4K</td>
</tr>
<tr>
<td>SGT/DGT Table</td>
<td>8K</td>
<td>8K</td>
<td>8K</td>
<td>8K</td>
</tr>
<tr>
<td>SGACLs (Security ACEs)</td>
<td>5K</td>
<td>18K</td>
<td>18K</td>
<td>18K</td>
</tr>
</tbody>
</table>

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.

Here are the limitations for configuring IRCM on the controller devices in this release:

• Configuration of Cisco AireOS controller as a foreign 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 scenario is not supported.

• Only guest SSID is supported.

• Broadcast of a non-guest anchor SSID in a guest anchor node 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 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 76, *Add Buildings*, on page 80, and *Add a Floor to a Building*, on page 81.

**Step 2**  Configure network servers, such as AAA, DHCP, and DNS servers. For more information, see *Configure Global Network Servers*, on page 127 and *Add Cisco ISE or Other AAA Servers*, on page 127.

**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 100.

**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 11.

**Step 5**  Provision a foreign wireless controller as the active main wireless controller. See *Provision a Cisco Wireless Controller*, on page 218.

**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 Wireless Controller*, on page 218.

**Step 7**  Configure device credentials, such as CLI, SNMP, HTTP, and HTTPS. For more information, see *Configure Global CLI Credentials*, on page 117, *Configure Global SNMPv2c Credentials*, on page 118, *Configure Global SNMPv3 Credentials*, on page 119, and *Configure Global HTTPS Credentials*, on page 121.
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 16 or Discover Your Network Using an IP Address Range, on page 21.

- 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 76, Add Buildings, on page 80, and Add a Floor to a Building, on page 81.

- 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 85.

- 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 114, Configure Global Network Servers, on page 127, 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 100.

- The WLAN profile name of the foreign controller and anchor controller should be the same for mobility.

---

**Step 1**  From the Cisco DNA Center home page, choose **Provision**.

The Devices > Inventory window appears with a list of discovered devices.

**Step 2**  Check the check box adjacent 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 adjacent 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 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 216](#).)
- 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 127](#).)
  - Device credentials, such as CLI, SNMP, HTTP, and HTTPS credentials. (See [Configure Global CLI Credentials, on page 117](#), [Configure Global SNMPv2c Credentials, on page 118](#), [Configure Global SNMPv3 Credentials, on page 119](#), and [Configure Global HTTPS Credentials, on page 121](#).)
  - IP address pools. (See [Configure IP Address Pools, on page 124](#).)
- 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 the *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 in size or larger.

a) From the Cisco DNA Center home page, choose **Design > Network Settings > IP Address Pools**.

b) From the **Network Hierarchy** pane, choose a site.

c) Click **Reserve IP Pool** and complete the following fields to reserve all or part of an available global IP address pool for the specific site:

- **IP Pool Name**: Unique name for the reserved IP address pool.

- **Type**: Type of IP address pool. For LAN automation, choose **LAN**.

- **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.

- **CIDR Prefix/No. 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.

- **Gateway IP Address**: Gateway IP address.

- **DHCP Servers**: DHCP server(s) IP address(es).

d) Click **Reserve**.

**Step 2**

Discover and provision devices.

a) From the Cisco DNA Center home page, choose **Provision > Devices > Inventory**.

All the discovered devices are displayed.

b) From the **LAN Automation** drop-down list, choose **LAN Automation**.

c) In the **LAN Automation** dialog box, 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.

- **Choose Primary Device Ports**: Ports to be used to discover and provision new devices.
• **Discovered Device Site:** All newly discovered devices are assigned to this site. This site can be different from Primary and Peer Sites.

• **IP Pool:** IP address pool that was reserved for LAN automation. (See Step 1.)

• **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:** 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.

• **Hostname Map File:** Configures user-provided names for discovered devices using a 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:

```plaintext
standalone-switch,FCW2212L0NF
stack-switch,"FCW2212E00Y,FCW2212LOGV"
```

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 details of error and possible remedial actions.

**Step 3** Monitor and review the progress of the devices being provisioned.

a) From the **Provision > Devices > Inventory** tab, click **LAN Automation > LAN Auto Status**.

The **LAN Automation Status** dialog box displays the progress of the devices being provisioned.

**Note** The provisioning process might take several minutes for the new devices to be provisioned.

b) After all devices have been discovered, added to Inventory, and are in Managed state, click **Stop** in the **LAN Automation Status** dialog box.

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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the Cisco DNA Center home page, choose Provision &gt; Devices.</td>
</tr>
<tr>
<td>2</td>
<td>Click the Inventory tab. All discovered devices are displayed.</td>
</tr>
<tr>
<td>3</td>
<td>Click LAN Auto Status. The status of any running or completed LAN automation jobs is displayed.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the Cisco DNA Center home page, choose Provision &gt; Devices. The Device Inventory window appears.</td>
</tr>
<tr>
<td>2</td>
<td>Click the Inventory tab, which lists all discovered and provisioned devices.</td>
</tr>
<tr>
<td>3</td>
<td>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.</td>
</tr>
<tr>
<td>4</td>
<td>From the Action drop-down list, choose Delete Device.</td>
</tr>
<tr>
<td>5</td>
<td>At the confirmation prompt, click OK.</td>
</tr>
</tbody>
</table>
Fabric Sites and Fabric Domains

A fabric site is an independent fabric area with a unique set of network devices: control plane, border node, edge node, 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 From the Cisco DNA Center home page, click **Provision**.
Step 2 Click the **Fabric** tab.
Step 3 Click the **Add Fabric Domain or Transit** tab.
Step 4 Choose **Add Transit** from the pop-up.
Step 5 Enter a transit name for the network.
Step 6 Choose **IP-Based** as the transit type.
   The routing protocol is set to BGP by default.
Step 7 Enter the autonomous system number (ASN) for the transit network.
Step 8 Click **Save**.

Create an SDA Transit Network

To add a new SDA transit network:

Step 1 From the Cisco DNA Center home page, click **Provision**.
Step 2 Click the **Fabric** tab.
Step 3 Click the **Add Fabric Domain or Transit** tab.
Step 4 Choose **Add Transit** from the pop-up.
Step 5 Enter a transit name for the network.
Step 6 Choose **SD-Access** as the transit type.
Step 7 Enter the **Site for the Transit Control Plane** for the transit network. Choose at least one transit map server.
Step 8 Enter the **Transit Control Plane** for the transit network.
Step 9 Repeat Step 7 and Step 8 for all map servers that you want to add.
Step 10 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, point to your SDA transit site and click **Add**.
Configuring Fabric Domains

Fabric Overview

A fabric is a logical group of devices that is managed as a single entity in one or multiple locations. Having a fabric 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.

The 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.

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.

Create a Fabric Domain

Cisco DNA Center creates a default fabric domain called Default LAN Fabric.

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:

- Software version—checks if the device is running with an appropriate software image.
- Software license—checks if the device is running with an appropriate software license.
- Hardware version—checks if the hardware version of the device is supported.

---

| Step 1 | From the Cisco DNA Center home page, click **Provision**. |
| Step 2 | Click the **Fabric** tab. |
| Step 3 | Click the **Add Fabric Domain or Transit** tab. |
| Step 4 | Choose **Add Fabric** from the pop-up. |
| Step 5 | Enter a fabric name. |
| Step 6 | Choose one fabric site. |
| Step 7 | Click **Add**. |
• 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.

• 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.

For more information on the software versions supported, see 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 current state of user intent for Virtual Network 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 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.
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 play 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, Cisco Wireless Controller communicates only with two control plane nodes.

**Before you begin**

Provision the device. To provision a device, click the **Provision** tab and choose **Devices**. The topology displays a device in gray color if it has passed the fabric readiness checks and is ready to be provisioned.

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. 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.

You can continue to provision a device that has failed the fabric readiness checks.

**Step 1**

From the Cisco DNA Center home page, click **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. Choose a Site. All devices in the network that have been inventoried are displayed in the topology view. In the topology view, any device that is added to the fabric is shown in blue.

**Step 3**

Click a device; the device details window slides in with the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edge Node</td>
<td>Click the toggle button next to this option to enable the selected device as an edge node.</td>
</tr>
<tr>
<td>Border Node</td>
<td>Click the toggle button next to this option to enable the selected device as a border node. For more information, see the <strong>Add Device as a Border Node</strong> section.</td>
</tr>
<tr>
<td>Control Plane</td>
<td>Click the toggle button next to this option to enable the selected device as a control plane node.</td>
</tr>
</tbody>
</table>
| Guest Border / Control Plane | Allows the following options:  
  • Control Plane: Check this check box if you want the device to act as a control plane.  
  • Border: Check this check box if you want the device to act as a border node.  
  • Select One Guest Virtual Network: All guest virtual networks created are listed. Check the check box of the guest virtual network and click **Enable**. |
To configure a device as a fabric-in-a-box, select the Control Plane, Border Node and Edge Node options.

To configure the device as a control plane and a border node, select both Control Plane and Border Node.

**Step 4**

Click Save.

---

**What to do next**

Once 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 257**.

To add a device as a border node:

**Step 1**

From the Cisco DNA Center home page, click **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-enabled 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 and choose **Border Node**.

**Step 5**

A slide-in window appears with the name of the device that you want to add.

- **a)** From the **Border to** field, click one of the radio buttons:

  - **Rest of Company (Internal)**: Designate the device as a border for IP routes inside your company. A border exports fabric routes and imports outside routes.

  - **Outside World (External)**: Designate the device as a default border for IP routes outside your company. A border exports fabric routes only. An external border node connects to unknown networks such as the internet or a transit area.

  - **Anywhere (Internal & External)**: Designate the device as a border for both internal and external IP routes. A border exports fabric routes and imports outside routes, except default-route.

- **b)** Enter the **Local Autonomous Number** for the device.
c) From the **Select IP Address Pools** drop-down list, choose an IP address pool.

d) Check the **connected to the internet** check box to choose this border node to advertise internet services to other fabric borders.

e) Choose a transit network to enable on the border device:

   - To enable SDA transit on the border, choose a user-created SDA transit domain from the **Select Transit** drop-down list. Click **Add**.
   - To enable IP transit on the border, choose a user-created IP transit domain from the **Select Transit** drop-down list. Click **Add**.

Choose an IP pool from Design Hierarchy. The selected pool will be used to automate IP routing between the border node and IP peer. Click **Add Interface** to enter interface details on the next screen.

Choose **External Interface** from the drop-down list. Enter the **Remote AS Number**. Check the **Virtual Network** from the list. This virtual network should be advertised by the border to the remote peer. You can select one, multiple, or all virtual networks. Click **Save**.

---

**Step 6**

Click **Layer 2**. You will see a table of the virtual networks and the number of pools in each virtual network. Click one of the virtual networks.

If a check box in the virtual network list is not clickable, it indicates that the segments under the virtual network have been handed off to an external VLAN.

After you select a virtual network, the list of IP address pools present in the virtual network appears. A list of interfaces through which you can connect nonfabric devices is displayed.

Enter the **External VLAN** into which the fabric must be extended. A virtual network can only be handed off on a single interface. The same virtual network cannot be handed off via multiple interfaces.

Click **Save**.

**Step 7**

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.

In this tab, you can:

- Select an authentication template to apply to the fabric. These templates are predefined configurations that are retrieved from Cisco ISE. After selecting the authentication template, click **Save**.

- 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.

- 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**.

- Apply specific configurations for each port for the specific type of device that is connecting 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 single servers.

- Each port can learn up to a maximum of 10 MAC addresses.
- Servers with internal switches or virtual switches are not supported.
- Other networking equipment (such as hubs, routers, and switches) is not supported.

**Select Authentication Template**

You can select the authentication template that will apply to all the devices in the fabric domain.

**Step 1**

From the **Auth Template** section, choose an authentication template:

- **Closed Authentication**: Any traffic prior to authentication is dropped, including DHCP, DNS, and ARP.
- **Easy Connect**: 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.

**Step 2**

Click **Save**.

**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 here were created when the network was designed.

**Step 1**

From the **Virtual Networks** section, click a virtual network.

**Step 2**

Configure the virtual network.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Pool Name</td>
<td>From the list of IP address pools, choose the ones that should be part of the virtual network.</td>
</tr>
<tr>
<td>Traffic Type</td>
<td>Choose to send voice or data traffic through the virtual network.</td>
</tr>
<tr>
<td>Wireless Mgmt Pool</td>
<td>Choose whether the virtual network should be part of the wireless management pool of the fabric domain.</td>
</tr>
<tr>
<td>AP Provisioning Pool</td>
<td>Choose whether the virtual network should be part of the access point provisioning pool.</td>
</tr>
<tr>
<td>Layer-2 Extension</td>
<td>Enables Layer-2 MAC Address registration for the IP Pool and Layer-2 VNI.</td>
</tr>
<tr>
<td>Layer-2 Flooding</td>
<td>Layer 2 Flooding is disabled by default.</td>
</tr>
</tbody>
</table>
Choose which group the IP Pool should belong to. Displays whether the IP address pool assigned to this virtual network belongs to the critical IP address pool. Displays the authentication policy for the virtual network.

---

**Step 3**  
Click **Update** to save the settings. The settings you specify here will be deployed to all devices on the network.

**Step 4**  
After all the virtual networks have been configured, click **Save**.

---

**Configure Wireless SSIDs for the Fabric Domain**

The **Wireless SSID** section allows you to specify wireless SSIDs within the network that the hosts can access.

**Configure Ports Within the Fabric Domain**

The **Select Port Assignment** section lets you configure each access device on the fabric domain. You can specify network behavior settings for each port on each 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**  
From the **Select Fabric Device** section, choose the access device that you want to configure. The ports available on the device are displayed.

**Step 2**  
Choose the ports on the device and specify the allowed IP address pool, the groups that have been provisioned, the voice or data pool, and the authentication type for the port.

**Step 3**  
Click **Save**.

---

**Configure an Extended Node**

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 can be done on the Host Onboarding window.

Actual packet forwarding, authentication, and policy application, happen at the fabric edge layer above the extended node. Every packet that enters an extended node is forwarded to the fabric edge which decides what to do with the packet. This ensures that we are not restricted by the limited Ternary Content-Addressable Memory (TCAM) and other capabilities in the extended nodes. Policy segmentation and automation benefits of the fabric are available to the extended switch ports too.
**Steps to Configure an Extended Node**

Cisco Catalyst 9300, Cisco Catalyst 9400, and Cisco Catalyst 9500 series switches when configured as fabric edge, support extended nodes.

---

**Note**

Cisco Catalyst 9200 series switches do not support extended nodes.

The following are the minimum supported software versions on the extended nodes:

- Cisco Industrial Ethernet 4000, 4010, 5000 series: Minimum supported version is 15.2.7E
- Cisco Catalyst IE 3300, 3400 series: Minimum supported version is IOS XE 16.11.1
- Cisco Digital Building series switches, Cisco Catalyst 3560-CX switches: Minimum supported versions are 15.2(6)E2, 15.2.7

---

**Step 1**

Configure a network range for the extended node. Refer Configure IP Address Pools, on page 124 for steps to configure an IP address pool. This comprises adding an IP address pool and reserving the IP pool at the Site level. Ensure the CLI and SNMP credentials are configured.

**Step 2**

Assign the extended IP address pool to INFRA_VN under the Fabric > Host Onboarding tab. Select 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 the Cisco DNA Center.

**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** *(Optional)*

Create a Port Channel.

Do this step only if the global authentication mode for the fabric is dot1x closed.

Create a port-channel on the fabric edge node connected to the extended node. To create a port-channel, perform the following steps:

a) Go to Provision > Fabric > Fabric Infrastructure tab and select the fabric edge node. A window with the device name as the title slides in.

b) Click Create Port Channel.

c) Fill all the fields in the resulting window. Note that LACP does not work for extended node onboarding.

   - Do not select LACP.

   - Use PAGP for all devices other than IE 3300 and IE 3400 devices.

   - Use Static mode for IE 3300 and IE 3400 devices.

d) Navigate to Provision > Fabric > Host Onboarding page. Select the port channel that is created. In the resulting window, select Extended Node as the Connected Device Type.

   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 on-boarded and ready to be managed. Once the configuration is complete, the extended node appears in the Fabric topology with a tag (X) indicating 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 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. Border nodes also support port channels.
Create a Port Channel

**Step 1** View the devices that support port channels by turning on the Port Channel toggle button under Display mode of the topology view.

Port channel capable devices are highlighted.

**Step 2** Click on the required device. A window with the device name slides in.

**Step 3** Select the Port Channel tab. Click Create Port Channel.

A window titled Create Port Channel comes up.

**Step 4** From the list of ports displayed, select the ports to be bundled and an appropriate protocol.

**Step 5** Click Create.

A new port channel is created and you can see a Success message.

In the topology view, the newly created port channel link appears.
Assign an IP Pool for a Port Channel

Step 1  From the Home page, navigate to Provision > Fabric > Host Onboarding
Step 2  Port Channel Assignment tab lists all the created port channels.
Step 3  Select a Port Channel and click Assign.

Port Assignment window slides in.

Step 4  If the connected device is an extended node device, choose Extended Node as the Connected Device Type. For an extended node, INFRA_VN is the default pool that is already selected. You can add more pools to this Port Channel by clicking on the plus icon next to the last pool. This brings up a drop-down list of IP pools. Choose from this list and assign the IP pool.

If the connected device is a server, you can add multiple pools by clicking on the plus icon in the Port Assignment window.
Delete a Port Channel

Step 1  From the Home Page, navigate to Provision > Fabric > Fabric Infrastructure topology view.
Step 2  Click on the device whose port channel is to be deleted. A window with the device name slides-in.
Step 3  Select the Port Channel tab. The resulting Port Channel view lists all the existing Port Channels.
Step 4  Select the Port Channel to be deleted and click Delete.
Step 5  Click Yes on the delete confirmation message that appears. This deletes the Port Channel.

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 Settings

After devices are added to the fabric domain, you can create multicast IP address pools and rendezvous points (RPs). Applicable multicast configurations will be automated on all fabric devices operating in that fabric domain.

An RP is a router in a multicast network domain that acts as a shared root for a multicast shared tree.

Create a Multicast IP Address Pool

Before you begin

A multicast IP address pool is used for internal PIM communication within the fabric domain. There is an option to define multiple multicast pools, and each can be associated with a separate virtual network. There is a requirement that each virtual network must have a separate multicast IP address pool created and associated with it.

Step 1  From the Cisco DNA Center home page, choose Design > Network Settings > IP Address Pools. A list of all IP address pools is displayed.
Step 2  Click Add and specify the multicast addresses to form the pool:

- **IP Pool Name**: Enter a name for the multicast IP address pool.
- **Subnet/Mask**: Enter the subnet IP address and subnet mask for the multicast pool.
- **Gateway IP Address**: Enter the IP address of the gateway.
Step 3  Click Save.

Step 4  To enable multicast in multiple virtual networks, create a separate IP multicast pool for each virtual network. (Repeat Step 2 and Step 3.)

---

**Native Fabric Multicast**

*Note*  For a brownfield deployment of Native Multicast, manually configure the underlay multicast commands. If you enable multicast using LAN Automation, the multicast commands are configured during discovery of devices.

To enable and disable native fabric multicast on a fabric site:

---

**Add a Device as a Rendezvous Point**

Step 1  From the Cisco DNA Center home page, click **Provision**. The screen displays all provisioned fabric domains.

Step 2  From the list of fabric domains, choose a fabric. The screen displays all devices in the network that have been inventoried. You can view the devices in the topology view or list view. In the topology view, any device that is added to the fabric is shown in blue.

Step 3  By default, native multicast is disabled for a site. To enable native multicast for a site, click the gear box next to the listed fabric and choose **Enable Native Multicast for IPv4**. Save the fabric.

Step 4  To disable native multicast for a fabric site, click the gear box next to the listed fabric and choose **Disable Native Multicast for IPv4**. Save the fabric.
Only a single IP address pool is currently supported for each virtual network for multicast. To enable multicast in multiple virtual networks, you must create multiple multicast IP address pools.

Step 7  
Associate the corresponding virtual network and click Enable.

Step 8  
Click Save on the main screen. Apply the changes.

Verify the Rendezvous Point

Step 1  
From the Cisco DNA Center homepage, click the Provision tab. By default, the Devices window is shown.

Step 2  
Click the Fabric tab. A list of fabric domains is shown.

Step 3  
Choose a fabric. The Fabric - Devices window appears, showing all devices in the network. Virtual networks that are enabled for IP multicast are marked with an M.

Add a Device as a Redundant Rendezvous Point

Note  
Dual RP is supported only for EXTERNAL or INTERNAL BORDERNODE. When a redundant RP is added to the network, the MSDP session is enabled. Each fabric device that hosts the RP creates two loopbacks per VRF: one for the RP, and one to establish an MSDP session.
Add a Device as a Redundant Rendezvous Point

Step 1  From the Cisco DNA Center home page, click **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-enabled sites is displayed.

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 the fabric device that you want to add as a redundant RP. A slide-in window displays the list of virtual networks.

Step 5  Expand the **Virtual Networks** for which you want to add a redundant RP. A multicast IP address pool should be prepopulated. Click **Next**.

Step 6  Associate the virtual networks and click **Enable**.

Step 7  Click **Save** on the main screen. **Apply** the changes.
Cisco DNA Assurance

Cisco DNA Assurance is an application that is available from Cisco DNA Center. From Cisco DNA Center, Release 1.2.5 onward, we are providing you with a user guide that deals exclusively with Cisco DNA Assurance.

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 on this listing page.
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 274.

- **Collectors**: Collects 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. See View or Update Collector Configuration Information, on page 275.

- **Store Settings**: Allows you to specify how long data is stored for an application. See Configure Data Retention Settings, on page 276.

- **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 277.
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**
From the Cisco DNA Center home page, click the gear icon and choose **System Settings > 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** From the Cisco DNA Center home page, click the gear icon 🛠 and choose System Settings > 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.
Configure Data Retention Settings

You can specify how long data is stored for an application.

**Step 1** From the Cisco DNA Center home page, click the gear icon and then choose System Settings > 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 or modify the current data retention and purge settings, click Data Retention & Purge Configuration.

Click the data for which you want to view or modify data retention and purge configuration settings:

- **Time Series Document Store**: Settings for all time-based data.
**Trigger Store**: Storage space dedicated to issues detected by various data analysis algorithms.

**Time Series Graph Store**: Settings for all time-based graphical data.

---

**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**
From the Cisco DNA Center home page, click the gear icon 🔄 and choose **System Settings > 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.
Troubleshoot Cisco DNA Center Using Data Platform

View Pipeline Status