



Manage Your Inventory

- [About Inventory, on page 1](#)
- [Inventory and Cisco ISE Authentication, on page 2](#)
- [Display Information About Your Inventory, on page 3](#)
- [Manage User-Defined Fields, on page 11](#)
- [Launch Topology Map from Inventory, on page 12](#)
- [Types of Devices in the Cisco DNA Center Inventory, on page 13](#)
- [Filter Devices, on page 28](#)
- [Manage Devices in Inventory, on page 29](#)
- [Create Port Groups, on page 33](#)
- [Assign Tags to Ports, on page 33](#)
- [Maintenance Mode for Devices, on page 34](#)
- [Inventory Insights, on page 35](#)
- [Manage System Beacon, on page 36](#)
- [Change the Device Role \(Inventory\), on page 37](#)
- [Update a Device's Management IP Address, on page 38](#)
- [Update the Device Polling Interval, on page 39](#)
- [Resynchronize Device Information, on page 40](#)
- [Delete a Network Device, on page 40](#)
- [Launch Command Runner \(Inventory\), on page 40](#)
- [Troubleshoot Device Reachability Issues Using Run Commands, on page 41](#)
- [Use a CSV File to Import and Export Device Configurations, on page 41](#)
- [View Configuration Drift of a Device, on page 44](#)
- [Label Configuration Drift, on page 45](#)
- [Replace a Faulty Device, on page 46](#)
- [Replace a Faulty Access Point, on page 48](#)
- [Limitations of the RMA Workflow in Cisco DNA Center, on page 49](#)
- [Reboot the Access Point, on page 51](#)

About Inventory

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

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

Inventory uses the following protocols, as required:

- Link Layer Discovery Protocol (LLDP).
- IP Device Tracking (IPDT) or Switch Integrated Security Features (SISF). (IPDT or SISF must be enabled on the device.)
- LLDP Media Endpoint Discovery. (This protocol is used to discover IP phones and some servers.)
- Network Configuration Protocol (NETCONF). For a list of devices, see [Discovery Prerequisites](#).

After the initial discovery, Cisco DNA Center maintains the inventory by polling the devices at regular intervals. The default interval is every 24 hours. However, you can change this interval as required for your network environment. For more information, see [Update the Device Polling Interval, on page 39](#). Also, a configuration change in the device triggers an SNMP trap, which in turn triggers device resynchronization. Polling occurs for each device, link, host, and interface. Only the devices that have been active for less than one day are displayed. This prevents stale device data, if any, from being displayed. On average, polling 500 devices takes approximately 20 minutes.

Inventory and Cisco ISE Authentication

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

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



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

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

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

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


To avoid this situation, make sure that before you provision devices using Cisco DNA Center, you have configured the devices in Cisco ISE with the same device credentials that you are using in Cisco DNA

Center. Also, make sure that you configured valid discovery credentials. For more information, see [Discovery Credentials](#).

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

Display Information About Your Inventory

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

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

When you select devices and choose a different view from the **Focus** drop-down list, your selection persists in each new view.

If you choose the **Default** view from the **Focus** drop-down list, the **Inventory** table displays only the **Device Name**, **IP Address**, **Device Family**, and **MAC Address** of listed devices.

By default, 25 entries are shown in the **Inventory** table. Click **Show More** to view more entries. You can view up to 500 entries in the **Inventory** table.

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

Before you begin


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

Click the menu icon () and choose **Provision > Network Devices > Inventory**.

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

Table 1: Inventory

Column	Description
Device Name	

Column	Description
	<p>Name of the device.</p> <p>Click the device name to view the following device details:</p> <p>Details: Displays details such as the device name, reachability status, manageability status, IP address, device model, role, uptime, site, and so on.</p> <ul style="list-style-type: none"> • View Assurance 360: Displays the Assurance 360 window. For the window to open, you must have installed the Assurance application. • Interfaces <ul style="list-style-type: none"> • Ethernet Ports (for all devices): Displays the operational status and administrative status of the Ethernet ports. <p>Use the toggle button () to switch between Ports view and Ports table. Click a port in the Ports view or click a port name in the Ports table to view the details about the port.</p> <p>For Cisco Catalyst 4000 Series, 6000 Series, and 9000 Series switches and Cisco ASR 1000 Series Aggregation Services Routers, the Ports view displays the details of line cards and supervisor cards if they are available.</p> <p>Line card details include information about the platform, address, serial number, role, and stack member number. Supervisor card details include information about the part number, serial number, switch number, and slot number.</p> <p>The Ports table displays the operational status, admin status, type, Native VLAN, Voice VLAN, MAC address, PoE status, speed, MTU, and description details of the port.</p> <p>For Cisco Catalyst 2000, 3000, and 9000 Series switches, either click a port in the Ports view or click a port name in the Ports table to view the maximum allocated power and power drawn details of that port.</p> <ul style="list-style-type: none"> • Neighbor Details: <p>Click a port in the Ports view or a port name in the Ports table to view the port details. The Port Details window displays the details of the device connected to the port. In the Neighbor Details area, the device name, the name of the port to which the device is connected, and the capabilities of the device are shown.</p> <p>The port shows the details of the CDP neighbor. If CDP is not present, the LLDP neighbor details are shown. If both CDP and LLDP neighbors are not present, Neighbor Details is hidden from the Port Details window.</p> • Color Code: This drop-down list catalogs the following views: <ul style="list-style-type: none"> • Status: Displays the default view of Ethernet ports. • VLANs: Displays the VLAN assigned to a particular port. The VLANs view allows you to select a maximum of five VLANs and list only the VLANs that are associated with the port. <p>The VLANs view displays the Selected, Not Configured, Default, and VLAN color code of the VLAN port mapping.</p> • Port Channels: Displays the top five port channels configured on the device.


Column	Description
	<p>The Port Channels view displays the Selected and the Port-channel color code of the configured port channels on the device.</p> <ul style="list-style-type: none"> • Port Actions: <ul style="list-style-type: none"> • Clear Mac Address: You can clear the MAC address of a port. Click a port in the Ports view, and then, from the Port Actions drop-down list, choose Clear Mac Address. • Port Shut: You can shut down a port. Click a port in the Ports view, and then, from the Port Actions drop-down list, choose Port Shut. Click Okay to confirm. The admin status of the port changes to Down. To change the admin status of the port to Up, from the Port Actions drop-down list, choose Port No Shut, and click Okay. <p>Error-disabled ports are shown in yellow. Click an error-disabled port in the Ports view to view the error reason. To activate an error-disabled port, clear the MAC address and shut down the port.</p> <ul style="list-style-type: none"> • Port Description: Click the Edit icon next to PORT DESCRIPTION, enter a description, click Save, and then click Okay to add a description to the port. Click the Delete icon to delete the description. • Update Native VLAN: Click the Edit icon next to Native VLAN, choose a VLAN from the Edit Native VLAN drop-down list, and then click Save to update the VLAN. You cannot update VLAN for the ports that have two VLANs preconfigured. <ul style="list-style-type: none"> • The device software type must be Cisco IOS or Cisco IOS-XE to update a VLAN, add a port description, clear the MAC address, and shut down the port. • For wireless controllers, VLAN update, clear MAC address, and port shutdown are not supported. • VLAN update, clear MAC address, and port shutdown are supported only on access ports. • Port shutdown disrupts traffic on the port. • Update Voice VLAN: Click the Edit icon next to Voice VLAN, choose a VLAN from the Edit Voice VLAN drop-down list, and then click Save to update the VLAN. • Native VLAN (only for switches and hubs): Displays the operational status, admin status, VLAN type, and IP address. The table also displays the ID of the following types of VLANs: <ul style="list-style-type: none"> • VLAN ID of the manufacturing-supplied default VLAN • VLAN ID of the configured default VLAN • VLAN ID of the configured VLAN <p>Click Search or Filter to view the details of a VLAN.</p>

Column	Description
	<ul style="list-style-type: none"> • Virtual Ports (only for wireless devices, controllers, and routers): Displays the operational status, admin status, type, MAC address, PoE status, speed, and MTU. Click Search or Filter to view the details of a port. • Hardware and Software: Displays the hardware and software details of the device. • Configuration: Displays detailed configuration information that is similar to what is displayed in the output of the show running-config command. This feature is not supported for APs and wireless controllers. Therefore, configuration data is not returned for these device types. • Power: Displays details about the power budgeted for, power consumed by, and power remaining for the device. The Power Supplies table shows the operational status, serial number, and vendor equipment type details. • Fans: Displays the operational status, serial number, and vendor equipment type of fans. • SFP Modules: Displays the details of the platform, serial number, manufacturer, and ports to which Small Form-Factor Pluggable (SFP) modules are connected. Click Search or Filter to view the details of ports. • User Defined Fields: Displays the user-defined fields associated with the device. • Config Drift: Displays the configuration changes and allows you to pick any two versions of the same device and compare their running configuration data. • Wireless Info: Displays the primary and secondary managed locations. • Mobility: Displays the mobility group name, RF group name, virtual IP, and mobility MAC address. <p>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.</p>
IP Address	IP address of the device.

Column	Description
Support Type	<p>Shows the device support level:</p> <ul style="list-style-type: none"> • Supported: The device pack is tested for all applications on Cisco DNA Center. You can open a service request if any of the Cisco DNA Center functionalities for these devices do not work. • Limited: The Device Pack for legacy devices is tested only for the following features on Cisco DNA Center. <ul style="list-style-type: none"> • Discovery • Topology • Device Reachability • Config Change Audit • Inventory: Support is provided for device details such as Device Name, IP Address, Support Type, Device Family, Site, Reachability, MAC Address, Device Role, Image Version, Uptime, Last Sync Status, Last Updated, Serial Number, Device Series, and Platform. • Software Image Management: Software images may not be available for EOL devices on cisco.com. Not recommended for EOL devices. • Template Provisioning: Applicable only for switches. <p>For more information, see Cisco DNA Center Compatibility Matrix.</p> <ul style="list-style-type: none"> • Unsupported: All remaining Cisco and third-party devices that are not tested and certified on Cisco DNA Center. You may try out various functionalities on Cisco DNA Center for these devices, as a best effort. However, we do not expect you to raise a service request or a bug if Cisco DNA Center features do not work as expected. • Third Party: Device pack is built by customers or business partners and goes through the certification process. Third-party devices will support base automation capabilities such as Discovery, Inventory, Topology, and so on. Cisco TAC provides an initial level of support for these devices. However, if there is a problem with the device pack, you need to contact the business partner.
Reachability	<p>The following is a list of the various statuses:</p> <ul style="list-style-type: none"> • Reachable: The device is reachable by Cisco DNA Center using SNMP, HTTP(S), and NETCONF polling. • Ping Reachable: The device is reachable by Cisco DNA Center using ICMP polling and not reachable using SNMP, HTTP(S), and NETCONF polling. • Unreachable: The device is not reachable using SNMP, HTTP(S), NETCONF, or ICMP polling.

Column	Description
EoX Status	<p>Shows the EoX scan status:</p> <ul style="list-style-type: none"> • Success: The device is scanned for EoX alerts successfully. • Not Scanned: The device is not scanned for EoX alerts. • Scan Failed: Cisco DNA Center is not able to scan the device for EoX alerts. • Scanning: Cisco DNA Center is scanning the device for EoX alerts. <p>For the devices that are scanned successfully, the EoX Status column shows the number of alerts, if any.</p> <p>Click the number of alerts to view the alerts in detail.</p> <p>In the slide-in pane, click the Hardware, Software, and Module tabs to view the hardware, software, and module EoX alerts.</p>
Manageability	<p>Shows the device status:</p> <ul style="list-style-type: none"> • Managed with green tick icon: Device is reachable and is fully managed. • Managed with orange error icon: Device is managed with some error such as unreachable, authentication failure, missing NETCONF ports, internal error, and so on. You can hover the cursor over the error message to view more details about the error and the impacted applications. • Unmanaged: Device cannot be reached and no inventory information was collected due to device connectivity issues.
MAC Address	MAC address of the device.
Image Version	Cisco IOS software that is currently running on the device.
Platform	Cisco product part number.
Serial Number	Cisco device serial number.
Uptime	Period of time that the device has been up and running.
Device Role	<p>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.</p> <p>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.</p> <p>If required, you can use the drop-down list in this column to change the assigned device role.</p>
Site	The site to which the device is assigned. Click Assign if the device is not assigned to any site. Click Choose a Site , select a site from the hierarchy, and click Save . For more information, see Network Hierarchy Overview .
Last Updated	Most recent date and time that Cisco DNA Center scanned the device and updated the database with new information about the device.

Column	Description
Device Family	Group of related devices, such as routers, switches, hubs, or wireless controllers.
Device Series	Series number of the device, such as Cisco Catalyst 4500 Series Switches.
Resync Interval	The polling interval for the device. This interval can be set globally in Settings or for a specific device in Inventory. For more information, see the Cisco DNA Center Administrator Guide .
Last Sync Status	<p>Status of the last Discovery scan for the device:</p> <ul style="list-style-type: none"> • Managed: Device is in a fully managed state. • Partial Collection Failure: Device is in a partial collected state and not all the inventory information has been collected. Hover the cursor over the Information (i) icon to display additional information about the failure. • Unreachable: Device cannot be reached and no inventory information was collected due to device connectivity issues. This condition occurs when periodic collection takes place. • Wrong Credentials: If device credentials are changed after adding the device to the inventory, this condition is noted. • In Progress: Inventory collection is occurring.
Provisioning Status	<p>Shows the status of the last provisioning operation attempted on a device. Click See Details to view the status of past provisioning operations.</p> <ul style="list-style-type: none"> • Success: The latest operation on the device was successful. • Success with a warning icon: The latest operation on the device was successful. But there are failures from past provisioning operations that may need user attention. • Failed: The latest operation on the device has failed. • Failed with a warning icon: The latest operation on the device has failed and there are failures from past provisioning operations that may need user attention. • Configuring: The device is currently being configured. • Pending: The system is trying to determine if the device will be impacted by an ongoing provisioning operation. • Not Provisioned: The device has not been provisioned ever once. • Out of Sync: The Network Settings or Network Profiles of a device has been modified after the last provisioning operation.


Column	Description
Credential Status	<p>Shows the device credential status:</p> <ul style="list-style-type: none"> • Not Applied: The device credential is not applied on the device. • Success: The device credential is applied on the device successfully. • Failed: The device credential failed on the device. <p>Click See Details to view the details about the credentials.</p> <p>The Credential Status slide-in pane shows the Type, Name/Description, Status, and Details of the credential.</p> <p>For a device whose status is Failed, hover the cursor over the ellipsis icon () in the Actions column and choose Retry or Clear.</p> <ul style="list-style-type: none"> • Retry: Applies the credential on the device. • Clear: Clears the device credential.
AP Ethernet Mac Address	Displays details about the AP Ethernet MAC address.
AP CDP Neighbors	Displays details about the switch and port connected to an AP in the inventory listing page. The inventory listing page displays the information about AP CDP neighbors, even if the connected access switch is managed by Cisco DNA Center.

Manage User-Defined Fields

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

Create User-Defined Fields

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

- Step 1** Click the menu icon () and choose **Provision > Network Devices > Inventory**.
- The **Inventory** page displays the device information that is gathered during the discovery process.
- Step 2** From the **Actions** drop-down list, choose **Provision > Inventory > Manage User Defined Fields**.
- Step 3** In the **Manage User Defined Fields** dialog box, click **Create New Field**.
- Step 4** In the **Create New Field** dialog box, enter a name and description for user-defined field in the **Field Name** and **Field Description** fields.
- Note** You can add device details that are not already present in the device details page, such as customer IP address and customer device name, in user-defined fields.

- Step 5** Click **Save**.
Similarly, you can create more user-defined fields. The user-defined fields appear in a table.
- Step 6** If you want to edit a user-defined field, click the corresponding edit icon, make the required changes, and click **Save**.
- Step 7** If you want to delete a user-defined field, click the corresponding delete icon and click **Yes** in the subsequent warning message.

Add User-Defined Fields to a Device

Before you begin

You must have created at least one user-defined field in the **Manage User Defined Fields** window. See [Create User-Defined Fields, on page 11](#).

- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
The **Inventory** page displays the device information that is gathered during the discovery process.
- Step 2** Click the name of the device for which you want to add user-defined fields.
- Step 3** In the left pane, click **User Defined Fields**.
- Step 4** Click **Add**.
- Step 5** From the **Field Name** drop-down list, choose a user-defined field and enter its value in the **Value** field.
For example, if you created a user-defined field for the customer IP address, choose it in the **Field Name** drop-down list, and enter the customer IP address in the **Value** field.
- Step 6** If you want to remove a user-defined field from the device, click the corresponding delete icon.
- Step 7** Click **Save**.

Launch Topology Map from Inventory

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

- Step 1** Click the menu icon (☰) and choose **Provisioning > Inventory**.



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

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

Types of Devices in the Cisco DNA Center Inventory

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

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

For a complete list of supported devices, see the [Cisco DNA Center Compatibility Matrix](#).

Manage Network Devices

Add a Network Device

You can add a network device to your inventory manually.

Before you begin

Make sure you configure your network device. For more information, see [Discovery Prerequisites](#).

Step 1 Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

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

Step 2 Click **Add Device**.

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

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

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

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

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

Note If no CLI global credentials are available, create the global CLI credentials in the **Network Settings > Device Credentials** window. See [Configure Global CLI Credentials](#).

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

Table 2: CLI Credentials

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

Step 6

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

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

Note If no SNMP global credentials are available, create the global SNMP credentials in the **Network Settings > Device Credentials** window. See [Configure Global SNMPv2c Credentials](#) and [Configure Global SNMPv3 Credentials](#).

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

Step 7

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

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

Table 3: SNMPv2c Credentials

Field	Description
Read	<ul style="list-style-type: none"> • 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. <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>
Write	<ul style="list-style-type: none"> • 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. <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

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

Table 4: SNMPv3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Choose one of the following modes: <ul style="list-style-type: none"> • 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 Mode .) Choose one of the following authentication types: <ul style="list-style-type: none"> • SHA: Authentication based on HMAC-SHA. • MD5: Authentication based on HMAC-MD5.
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. <p>Note</p> <ul style="list-style-type: none"> • 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 Mode .) Choose one of the following privacy types: <ul style="list-style-type: none"> • AES128: 128-bit CBC mode AES for encryption. • CISCOAES192: 192-bit CBC mode AES for encryption on Cisco devices. • CISCOAES256: 256-bit CBC mode AES for encryption on Cisco devices. <p>Note</p> <ul style="list-style-type: none"> • Privacy types CISCOAES192 and CISCOAES256 are supported only for use with Discovery and Inventory features. Assurance features are not supported. • Privacy type AES128 is supported for Discovery, Inventory, and Assurance.

Field	Description
Privacy Password	<p>SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support encryption standards. Passwords (or passphrases) must be at least eight characters long.</p> <p>Note</p> <ul style="list-style-type: none"> Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. Passwords are encrypted for security reasons and are not displayed in the configuration.

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

Table 5: SNMP Properties

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

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

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

Note If no HTTP(S) global credentials are available, create the global HTTP(S) credentials in the **Network Settings > Device Credentials** window. See [Configure Global HTTP\(S\) Credentials](#).

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

Table 6: HTTP(S)

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

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

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

- Step 11** Select one of the network **Protocol** radio button that enables Cisco DNA Center to communicate with remote devices. Valid values are **SSH2** or **Telnet**.
- Step 12** (Optional) Click **Validate** next to **Credentials**. Cisco DNA Center validates the device credentials and shows valid credentials with a green tick mark and invalid credentials with a red cross mark.
- All the credentials will be validated except the SNMP Write credentials.
- Step 13** Click **Add**.

Update Network Device Credentials

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

Before you begin

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

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

- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
- The Inventory page displays the device information gathered during the Discovery process.
- Step 2** Select the network devices that you want to update.
- Step 3** From the **Actions** drop-down list, choose **Inventory > Edit Device**.
- Step 4** In the **Edit Device** dialog box, choose **Network Device** from the **Type** drop-down field, if it is not already selected.
- Step 5** Expand the **CLI** area, if it is not already expanded, and do one of the following:
- If you want to use the global CLI credentials that have been already created, click the **Select global credential** radio button.
- Note** If no CLI global credentials are available, create them in the **Network Settings > Device Credentials** page. See [Configure Global CLI Credentials](#).
- Click the **Edit device specific credential** radio button and configure the following fields:

Table 7: CLI Credentials

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

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

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

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

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

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

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

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

Table 8: SNMPv2c Credentials

Field	Description
Read	<ul style="list-style-type: none"> • 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. <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>
Write	<ul style="list-style-type: none"> • 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. <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

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

Table 9: SNMPv3 Credentials

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

Field	Description
Mode	Security level that an SNMP message requires. Choose one of the following modes: <ul style="list-style-type: none"> • 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 Mode .) Choose one of the following authentication types: <ul style="list-style-type: none"> • SHA: Authentication based on HMAC-SHA. • MD5: Authentication based on HMAC-MD5.
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. <p>Note</p> <ul style="list-style-type: none"> • 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 Mode .) Choose one of the following privacy types: <ul style="list-style-type: none"> • AES128: 128-bit CBC mode AES for encryption. • CISCOAES192: 192-bit CBC mode AES for encryption on Cisco devices. • CISCOAES256: 256-bit CBC mode AES for encryption on Cisco devices. <p>Note</p> <ul style="list-style-type: none"> • Privacy types CISCOAES192 and CISCOAES256 are supported only for use with Discovery and Inventory features. Assurance features are not supported. • Privacy type AES128 is supported for Discovery, Inventory, and Assurance.

Field	Description
Privacy Password	<p>SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support encryption standards. Passwords (or passphrases) must be at least eight characters long.</p> <p>Note</p> <ul style="list-style-type: none"> Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. Passwords are encrypted for security reasons and are not displayed in the configuration.

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

Table 10: SNMP Properties

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

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

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

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

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

Table 11: HTTP(S)

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

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

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

- Step 11** Select one of the network **Protocol** radio buttons that enables Cisco DNA Center to communicate with remote devices. Valid values are **SSH2** or **Telnet**.
- Step 12** (Optional) Click **Validate** next to **Credentials**. Cisco DNA Center validates the device credentials and shows the valid credentials with green tick mark and invalid credentials with red cross mark.
- If you have chosen more than one device for updating the credentials, the **Validation** button will be disabled.
- Step 13** Click **Update**.
-

Security Focus for Network Devices

The Cisco DNA Center security focus allows you to view the results of the trustworthy checks on your devices. Few security checks are performed to ensure that your Cisco devices are authentic and are not compromised or altered physically.

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

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

These checks are triggered under the following circumstances:

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

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

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

Perform an Integrity Verification Check

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

- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
- The Inventory page displays the device information that is gathered during the Discovery process.
- Step 2** From the **Inventory** drop-down menu, select **Security**.
- Step 3** View the device details listed in the table.
- Step 4** To customize the table, click the three vertical dots at the end of the table to choose either **Add** or **Delete**. The **Integrity Verification** column displays the results.
- Step 5** If the **Integrity Verification** column for your device displays **Failed** as the status, click the Information icon to display the reason.

The following integrity verification statuses are possible:

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

Manage Compute Devices

Add a Compute Device

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

Step 1 Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

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

Step 2 Click **Add Device**.

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

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

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

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

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

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

Table 12: HTTP(S)

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

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

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

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

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

Table 13: CLI Credentials

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

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

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

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

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

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

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

Table 14: SNMPv2c Credentials

Field	Description
Read	<ul style="list-style-type: none"> 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. <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>
Write	<ul style="list-style-type: none"> 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. <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

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

Table 15: SNMPv3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Choose one of the following modes: <ul style="list-style-type: none"> • 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 Mode .) Choose one of the following authentication types: <ul style="list-style-type: none"> • SHA: Authentication based on HMAC-SHA. • MD5: Authentication based on HMAC-MD5.
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. <p>Note</p> <ul style="list-style-type: none"> • 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 Mode .) Choose one of the following privacy types: <ul style="list-style-type: none"> • AES128: 128-bit CBC mode AES for encryption. • CISCOAES192: 192-bit CBC mode AES for encryption on Cisco devices. • CISCOAES256: 256-bit CBC mode AES for encryption on Cisco devices. <p>Note</p> <ul style="list-style-type: none"> • Privacy types CISCOAES192 and CISCOAES256 are supported only for use with Discovery and Inventory features. Assurance features are not supported. • Privacy type AES128 is supported for Discovery, Inventory, and Assurance.

Field	Description
Privacy Password	<p>SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support encryption standards. Passwords (or passphrases) must be at least eight characters long.</p> <p>Note</p> <ul style="list-style-type: none"> Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. Passwords are encrypted for security reasons and are not displayed in the configuration.

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

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

Step 10 Click **Add**.

Update Compute Device Credentials

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

Before you begin

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

Step 1 Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
The Inventory page displays the device information that is gathered during the Discovery process.

Step 2 Select the devices that you want to update.

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

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

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

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

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

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

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

Step 9 Click **Update**.

Manage Meraki Dashboards

Integrate the Meraki Dashboard

You can integrate your Meraki dashboard with Cisco DNA Center.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
The Inventory page displays the device information that is gathered during the Discovery process.
- Step 2** Click **Add Device**.
- Step 3** In the **Add Device** dialog box, from the **Type** drop-down list, choose **Meraki Dashboard**.
- Step 4** Expand the **HTTP(S)** area, if it is not already expanded.
- Step 5** In the **API Key/Password** field, enter the API key and password credentials and click the **Get Organization details** link.
- Step 6** From the **Organization** drop-down list, select the organization options, or search for an organization name.
- Step 7** (Optional) Click **Validate** next to **Credentials**. Cisco DNA Center validates the device credentials and shows valid credentials with a green tick mark and invalid credentials with a red cross mark.
- Step 8** Click **Add**.
Only the selected organizations start collecting for the Meraki dashboard and devices.
-

Update Meraki Dashboard Credentials

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

Before you begin

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

-
- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
The Inventory page displays the device information that is gathered during the Discovery process.
- Step 2** Select the devices that you want to update.
- Step 3** From the **Actions** drop-down list, choose **Inventory > Edit Device**.
- Step 4** In the **Edit Device** dialog box, from the **Type** drop-down list, choose **Meraki Dashboard**.
- Step 5** Expand the **HTTP(S)** area, if it is not already expanded.
- Step 6** In the **API Key / Password** field, enter the API key and password credentials used to access the Meraki dashboard.
- Step 7** In the **Port** field, enter the port number.
- Step 8** (Optional) Click **Validate** next to **Credentials**. Cisco DNA Center validates the device credentials and shows valid credentials with a green tick mark and invalid credentials with a red cross mark.
If you have chosen more than one device for updating the credentials, the **Validation** button is disabled.

Step 9 Click **Update**.

Manage Firepower Management Center

Integrate Firepower Management Center

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

Step 1 Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

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

Step 2 Click **Add Device**.

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

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

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

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

Step 6 Enter the following information:

- a) **Username:** Name used to authenticate the HTTPS connection.
- b) **Password:** Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration.
- c) **Port:** The number of the TCP/UDP port used for HTTPS traffic. The default port number is 443.

Step 7 Click **Add**.

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

Update Firepower Management Center Credentials

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

Before you begin

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

Step 1 Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

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

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

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

- Step 3** From the **Actions** drop-down list, choose **Inventory > Edit Device**.
The **Edit Device** dialog box appears.
- Step 4** Click **Credentials**.
- Step 5** Expand the HTTP(S) area if it is not already expanded.
The **Add device specific credential** radio button is chosen by default.
- Step 6** Enter the following information:
- Username:** Name used to authenticate the HTTPS connection.
 - Password:** Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration.
 - Port:** The number of the TCP/UDP port used for HTTPS traffic. The default port number is 443.
- Step 7** Click **Management IP** and enter the IP address or name of the device in the **Device IP / DNS Name** field.
- Step 8** Click **Resync Interval** and choose a resync interval type:
- **Custom:** You can enter the resync interval in minutes. The valid ranges are from 25 to 1440 minutes (24 hours).
 - **Global:** By default, resync interval is set to 1440 minutes (24 hours).
 - **Disable:** Resync interval is disabled or set to zero.
- Step 9** Click **Role** and choose a role in the **Device Role** drop-down list.
- Step 10** Click **Update**.


Filter Devices



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

Before you begin

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

- Step 1** Click the menu icon () and choose **Provision > Network Devices > Inventory**.
The Inventory page displays the device information that is gathered during the Discovery process.
- Step 2** Click **Filter**.
The following types of filters are available:
- Quick Filter
 - Advanced Filter
 - Recent Filters

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

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

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

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

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

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

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

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

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

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

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

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


Manage Devices in Inventory

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

Add a Device to a Site

Step 1 Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

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

- Step 2** Check the check box for the devices that you want to assign to a site.
- Step 3** From the **Actions** menu, choose **Provision > Assign Device to Site**.
- Step 4** In the **Assign Device to Site** slide-in pane, click the link next to the  icon for the device.
- 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 **Next**.
- Step 9** In the **Task Name** name field, enter a task name of your choice.
- Step 10** To immediately assign the device to a site, click the **Now** radio button and click **Assign**.
- Step 11** To schedule the device assignment to a site for a later date and time, click the **Later** radio button to define the date and time of the deployment and click **Assign**.
- Step 12** To preview the CLI configuration, click the **Generate Configuration Preview** radio button and do the following:
- In the **Task Name** name field, enter a task name of your choice and click **Preview**.
Later, you can use the created configuration preview to deploy to the selected devices.
 - In the **Task Submitted** message, click the **Work Items** link.

Note If you didn't notice the **Task Submitted** message, click the menu icon and choose **Activities > Work Items**.
 - In the **Work Items** window, click the CLI preview task for which you submitted the configuration preview request.
 - View the CLI configuration details and click **Deploy**.
 - To immediately deploy the device, click the **Now** radio button, and click **Apply**.
 - To schedule the device deployment for a later date and time, click the **Later** radio button and define the date and time of the deployment.
 - In the confirmation window, click **Yes**.

Note The CLI task is marked as completed in the **Work Items** window. You can view the CLI configuration for this task, but you cannot deploy it again.
- Step 13** When assigning devices to a site, if Device Controllability is enabled, a workflow is automatically triggered to push the device configuration from the site to the devices.
From the **Focus** drop-down list, choose **Provision** and click **See Details** in the **Provision Status** column. The configuration that is pushed to the device is shown in a separate window if you enabled Device Controllability.

Tag Devices

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

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

-
- Step 1** Click the menu icon (☰) and choose **Provision**. The Device Inventory page displays device information gathered during the discovery process.
- Step 2** Check the check box next to the device(s) for which you want to apply a tag, and then click **Tag Device**.
- Step 3** Enter a tag name in the **Tag Name** field.
- If you are creating a new tag, click **Create New Tag**. You also can create a new tag with a rule. See [Tag Devices Using Rules, on page 31](#).
 - If you are using an existing tag, select the tag from the list, and then click **Apply**.
- A tag icon and the tag name(s) appear under the device name(s) for which you applied the tag(s).
- Step 4** To remove a tag from a device, do one of the following:
- Click **Create New Tag**, unselect all tags, and then click **Apply**.
 - Hover the cursor over the tag icon or tag name, and then click **X** to disassociate the tag from the device.
-

Tag Devices Using Rules

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

-
- Step 1** Click the menu icon (☰) and choose **Provision**. The Device Inventory page displays device information gathered during the discovery process.
- Step 2** Check the check box next to the device(s) for which you want to apply a tag, then click **Tag Device**.
- Step 3** Enter a tag name in the **Tag Name** field, then click **Create New Tag with Rule**.
- The Create New Tag window appears.
- The **Manually Added** field under **Total Devices Tagged Count** indicates the number of devices you selected.
- 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** Click the menu icon (☰) and choose **Provision**. The Device Inventory page displays device information gathered during the discovery process.
- In the **Device Name** column, you can see any previously created device tags listed under the device names.
- Step 2** Without selecting any devices, click **Tag Device**.
- The previously created tags are listed.
- Step 3** Hover your cursor over the tag you want to edit, then click the pencil icon next to the tag name.
- Alternatively, you can select **Tag Device > View All Tags**, then click the pencil icon next to the tag that you want to edit.
- Step 4** Make changes to the tag, then click **Save**.
-

Delete Tags

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

Before you begin

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

Remove the tag that is associated with a template.

- Step 1** Click the menu icon (☰) and choose **Provision**.
- The Device Inventory page displays device information gathered during the discovery process.
- Step 2** Without selecting any devices, choose **Tag Device > Manage Tags**.
- Step 3** Hover your cursor over the tag that you want to delete, then click the delete icon next to the tag name.
- Step 4** At the prompt, click **Yes**.
- An error message is generated if the tag is associated with a device or template. Remove the tag associated with the device or template and delete the tag.
-

Create Port Groups

Use this procedure to group ports, based on an attribute or rule.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Inventory**. The **Inventory** window displays device information gathered during the discovery process.
- Step 2** To create a new port tag, click **Tag** and choose **Create New Tag**.
The **Create New Tag** slide-in pane appears.
- Step 3** In the **Tag Name** field, enter the tag name. You can add a description for the tag in the **Description** field.
- Note** The **WAN** tag is a reserved tag name. You can't create a new port tag named **WAN**, because the system autogenerates the **WAN** tag.
- Step 4** In the **Tag Rules** area, click the **Port** tab.
- Step 5** In the **Device Scope** area, click the drop-down list and choose **Location** or **Tag Name** of the device to define the filters.
- Step 6** To add rules for tagging the ports, click the + icon. You can tag the ports based on port status, speed, tag name, operational status, and description. You can add additional conditions using Boolean operators (**AND**, **OR**).
To delete a condition, click the delete icon.
- Step 7** As the conditions are set, you can find the link for ports matching the condition at the bottom-left corner of the pane.
Click the link to view the ports. The **Matching Ports** slide-in pane appears. You can view the device to which the port belongs and the port name.
- Step 8** Click **Save**.
-

Assign Tags to Ports

You can manually assign tags to ports. For example, you can manually assign the system-generated **WAN** tag to a port.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Inventory**.
- Step 2** In the **Inventory** window, click a device name and choose **View Device Details**.
- Step 3** In the left pane, expand **Interfaces** and click **Ethernet Ports**.
- Step 4** In the top-right corner of the window, switch to the table view.
- Step 5** Choose the port or ports to tag and click **Tag**.
- Step 6** Choose the appropriate tags.
- Step 7** Click **Apply**.
-

Maintenance Mode for Devices

Schedule Maintenance for Devices

You can place one or more devices under maintenance mode in Cisco DNA Center. If a device is placed under maintenance mode, Cisco DNA Center will not process any telemetry data associated with the device. By placing faulty devices under maintenance mode, you can avoid receiving unnecessary alerts from the devices.



Note From the devices in maintenance mode, you cannot collect any information and perform polling operations.

While scheduling the maintenance mode for Cisco Wireless Controllers and APs, note the following:

- When you schedule maintenance for a Cisco Wireless Controller, all the APs associated with the wireless controller are moved under maintenance mode with the same schedule.
- When a wireless controller is in maintenance mode, you cannot modify the maintenance schedule of a single AP associated with the wireless controller. A warning message saying that the device is already scheduled for maintenance is displayed. If you modify the schedule of the wireless controller, then all the APs under the wireless controller will be impacted.
- When an AP moves from one wireless controller to another, the maintenance mode is impacted as below:
 - If the AP is moving from a wireless controller which is in maintenance mode to a wireless controller which is not under maintenance, then the AP will not have maintenance mode after moving.
 - If the AP is moving from a wireless controller which is not in maintenance mode to a wireless controller which is under maintenance, then the AP will be in maintenance mode after moving.

Step 1 Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

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

Step 2 Choose the devices that you want to schedule maintenance.

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

The **Schedule Maintenance** slide-in pane appears.

Step 4 In the **Reason For Maintenance** field, enter a reason for placing the device under maintenance mode.

By default, Cisco DNA Center adds a reason, and you can modify it.

Step 5 In the **Define Maintenance Window** area, do the following:

- a) Choose the start date and time for maintenance.
- b) Choose the end date and time for maintenance.
- c) Alternately, click **Days/Hours** and enter days and hours for maintenance.

Note: To choose recurrence for maintenance, choose **Days/Hours** option.

Step 6 In the **Maintenance Recurrence** area, click **None**, **Daily**, or **Weekly**.

- **None:** Maintenance will not recur.
- **Daily:** Enter the interval in days in the **Run at Interval (Days)** field.
- **Weekly:** Enter the interval in weeks in the **Run at Interval (Weeks)** field.

Step 7 If you have chosen **Daily** or **Weekly** for recurrence, check the **Set Schedule End** check box.

Step 8 Click **End Date** or **End After (Occurrences)**.

- **End Date:** Enter month, date, and year for maintenance end.
- **End After (Occurrences):** Enter the number of occurrences after you want maintenance to end.

Step 9 In the **Maintenance Time Zone** area, choose time zone for maintenance.

Step 10 Click **Submit**.

Manage Maintenance Schedule for Devices

Step 1 Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

Step 2 From the **Actions** drop-down list, choose **Inventory > Manage Maintenance**.

The **Manage Maintenance** slide-in pane appears. The **Status** column shows the current status of maintenance schedules.

Step 3 Click the **Search** or **Filter** icon to search or filter maintenance schedules.

Step 4 In the **Actions** column, click the **Edit** icon to edit the maintenance schedule.

Note For in-progress maintenance schedules, you can only extend the maintenance end time.

Step 5 Click the **Delete** icon in the **Actions** column to delete the maintenance schedule.

Note You cannot delete in-progress maintenance schedules.

Inventory Insights

The **Inventory Insights** window displays devices that have configuration inconsistencies with other directly-connected devices. It also displays devices that are misconfigured, as compared with the Cisco DNA Center best-practice recommendations. Additionally, you can view whether the link between the devices is up (active) or down (inactive), a link is down when the connection between devices no longer exists. Historical data is retained for future reference.

For example, assume that there is a network link between *device A* and *device B*. If you remove the link from *device B* and connect it to a new *device C*:

- The old link between *device A* and *device B* remains present and can be manually deleted by the user from the **Tools > Topology** window. No action is required by the user on the **Inventory Insights** window, it is shown to retain the historical data for your reference.

- The new link between *device A* and *device C* is shown as up.

Cisco DNA Center provides the following insights with suggested actions.

Speed/Duplex Settings Mismatch

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

-
- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory Insights**.
The **Inventory Insights** window appears.
- Step 2** Click **Speed/Duplex settings mismatch** to see the suggested actions that can be performed on devices.
The suggested actions appear in the right pane.
- Step 3** Click the number of instances to see the mismatches.
The **Speed/Duplex settings mismatch** window highlights the mismatches of speed and duplex.
- Step 4** Make the required changes in the device configuration by following the suggested actions.
-

VLAN Mismatch

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

-
- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory Insights**.
The **Inventory Insights** window appears.
- Step 2** Click **VLAN Mismatch** to see the suggested actions that can be performed on devices.
The suggested actions appear in the right pane.
- Step 3** Click the number of instances to see the mismatches.
The **VLAN Mismatch** window highlights the mismatches of Allowed VLAN and Native VLAN.
- Step 4** Make the required changes in the device configuration by following the suggested actions.
-

Manage System Beacon

You can highlight switches in Cisco DNA Center inventory by using system beacon.

System beacon supports the following devices:

- Cisco Catalyst 9200 Series Switches

- Cisco Catalyst 9300 Series Switches
- Cisco catalyst 3850 Series Ethernet Stackable Switches

Step 1 Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

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

Step 2 Choose the devices for which you want to enable or disable beacon.

Note

- You can enable beacon on up to five standalone devices at a time.
- If you want to enable beacon on stacked devices, you must choose only one device at a time. In a stacked device, you can enable beacon on one or more stack members.

Step 3 From the **Actions** drop-down list, choose **Inventory > Manage System Beacon**.

Step 4 In the **Manage System Beacon** slide-in pane, click **Enabled** radio button under **System Beacon State** and then click **Apply** to enable beacon on the chosen devices.

Once the system beacon is enabled, the blue beacon (🔵) appears next to the device name in the inventory.

Step 5 If you have chosen a stacked device, do the following in the **Manage System Beacon** slide-in pane:

- Check the **Update System Beacon Status?** check box corresponding to the stack members that you want to enable beacon.
- Under **System Beacon State**, check the **Enabled** radio button.
- Click **Apply**.

Step 6 To disable beacon on the chosen devices, do the following in the **Manage System Beacon** slide-in pane:

- Under **System Beacon State**, check the **Disabled** radio button.
- Click **Apply**.

Alternatively, in the Inventory window, hover the cursor over the blue beacon (🔵) next to the device name and click **Disable**.

Change the Device Role (Inventory)

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

Table 16: Device Roles and Topology Positions

Topology Position	Device Role
Tier 1	Internet (not configurable)
Tier 2	Border Router
Tier 3	Core


Topology Position	Device Role
Tier 4	Distribution
Tier 5	Access
Tier 6	Unknown



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

Before you begin

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

Step 1 Click the menu icon () and choose **Provision > Network Devices > Inventory**.

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

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

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

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


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

Update a Device's Management IP Address

You can update the management IP address of a device.



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

Step 1 Click the menu icon () and choose **Provision > Network Devices > Inventory**.

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

- Step 2** Select the device that you want to update.
- Step 3** From the **Actions** drop-down list, choose **Inventory > Edit Device**.
The **Edit Device** dialog box is displayed.
- Step 4** Click the **Management IP** tab, and enter the new management IP address in the **Device IP/ DNS Name** field.
- Note** Make sure that the new management IP address is reachable from Cisco DNA Center and that the device credentials are correct. Otherwise, the device might enter an unmanaged state.
-

What to do next

Reprovision the device to update the source-interface configuration.

Update the Device Polling Interval

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

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

Before you begin

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

- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
- Step 2** Select the devices that you want to update.
- Step 3** Click **Update Polling Interval**.
- Step 4** From the **Update Resync Interval** dialog box, in the **Status** field, click **Enabled** to turn on polling or click **Disabled** to turn off polling.
- Step 5** In the **Polling Time** field, enter the time interval (in minutes) between successive polling cycles. Valid values are from 25 to 1440 minutes (24 hours).
- Note** The device-specific polling time supersedes the global polling time. If you set the device-specific polling time and then change the global polling time, Cisco DNA Center continues to use the device-specific polling time.
- Step 6** Click **Update**.
-

Resynchronize Device Information

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

-
- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
The Inventory page displays the device information gathered during the Discovery process.
- Step 2** Select the devices about which you want to gather information.
- Step 3** From the **Actions** drop-down list, choose **Inventory > Resync Device**.
- Step 4** Click **OK**.
-

Delete a Network Device

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

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

Before you begin

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

-
- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
The **Inventory** window displays the device information gathered during the **Discovery** process.
- Step 2** Check the check box next to the device or devices that you want to delete.
- Note** You can select multiple devices by checking additional check boxes, or you can select all the devices by checking the check box at the top of the list.
- Step 3** From the **Actions** drop-down list, choose **Inventory > Delete Device**.
- Step 4** In the **Warning** window, check the **Config Clean-Up** check box to remove the network settings and telemetry configuration from the selected device.
- Step 5** Confirm the action by clicking **OK**.
-

Launch Command Runner (Inventory)

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

Before you begin

Install the Command Runner application. For more information, see the [Cisco DNA Center Administrator Guide](#).

-
- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
The Inventory page displays the device information that is gathered during the Discovery process.
- Step 2** Select the devices on which you want to run commands.
- Step 3** From the **Actions** drop-down list, choose **Others > Launch Command Runner**.
For information about the commands that you can run and how to run them, see [Run Diagnostic Commands on Devices](#).
-

Troubleshoot Device Reachability Issues Using Run Commands

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



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

Before you begin

Install the Command Runner application. For more information, see the [Cisco DNA Center Administrator Guide](#).

-
- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
- Step 2** From the **Actions** drop-down list, choose **Others > Run Commands**.
You can enter **man** anytime to retrieve a list of currently supported commands and shortcuts.
-

Use a CSV File to Import and Export Device Configurations

CSV File Import

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

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

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



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

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

- Device IP address
- SNMP version
- SNMP read-only community strings
- SNMP write community strings
- SNMP retry value
- SNMP timeout value

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

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

CSV File Export

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

Import Device Configurations from a CSV File

You can import device configurations from a CSV file.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
The Inventory page displays the device information gathered during the Discovery process.
- Step 2** From the **Actions** drop-down list, choose **Inventory > Import Inventory** to import the device credentials.
- Step 3** Drag and drop the CSV file into the boxed area in the **Bulk Import** dialog box or click the dotted-line boxed area and browse to the CSV file.
- Step 4** Click **Import**.
-

Export Device Data

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



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

-
- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
The Inventory page displays the device information gathered during the Discovery process.
- Step 2** To export configuration information for only certain devices, check the check box next to the devices that you want to include. To include all devices, check the check box at the top of the device list.
- Step 3** From the **Actions** drop-down list, choose **Inventory > Export Inventory** to export the device configurations.
The **Export Inventory** dialog box appears.
- Step 4** In the **Password** field, enter a password that will be used to encrypt the exported CSV file.
Note The password is required to open the exported file.
- Step 5** Confirm the encryption password.
- Step 6** Check the **Include SSH key information** check box to include information such as initial SSH key, initial SSH key algorithm, current SSH key, and current SSH key algorithm in the exported CSV file.
- Step 7** Click **Export**.


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

Export Device Credentials

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



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

Step 1 Click the menu icon () and choose **Provision > Network Devices > Inventory**.

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

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

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

The **Export** dialog box appears.

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

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

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

Note The password is required to open the exported file.

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

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

View Configuration Drift of a Device

Configuration changes made on your device are saved in the internal Cisco DNA Center server. You can view detailed information about config changes made to the device from outside Cisco DNA Center.

Step 1 Click the menu icon () and choose **Provision > Inventory**.

Step 2 Click the device name.

The **Device Details** window appears.

Step 3 In the left pane, choose **Config Drift**.

The **Configuration Changes** window shows the number of configuration drifts saved, which includes labeled configs and config drift versions.

Step 4 Expand the **Change History** tab to view the following details:

- a) **Config drift date range:** Click the **Start Date** and **End date** to choose the date range for which you want to view the config drift. By default, the start and end dates are set to display the config drift for the last 15 days.
- b) **Config drift timeline graph:** Shows the config drift for the chosen date range. By default, the last 15 days of config drift are shown in the timeline graph.

The timeline graph shows the following details:

- **In-band Config Drift:** Configuration changes done by Cisco DNA Center are shown as a blue bubble in the timeline graph.
 - **Out-of-band Config Drift:** Configuration changes done outside Cisco DNA Center are shown as a purple bubble in the timeline graph.
 - **Labeled Config:** The config version labeled and archived in Cisco DNA Center is shown as an orange bubble in the timeline graph. For more information, see [Label Configuration Drift](#).
- c) **Config Drift Version:** Click the down arrow to view all the available config drift versions.
 - d) **Running Config:** Click the config drifts on the timeline graph. The comparison is shown under the **Running Config** tab. The differences between the config versions are marked in different colors for better visibility.

Label Configuration Drift

You can label the config drift on the time-line graph for future reference.

Step 1 Click the menu icon (☰) and choose **Provision > Inventory**.

Step 2 In the **Inventory** window, click the device name to view device details.

Step 3 From the left side pane, choose **Config Drift** tab. The **Configuration Changes** window appears.

Step 4 Choose the config drift in time-line graph that you want to label. The timestamp of the chosen config drift is shown in the **Config Drift Version** below the time-line graph.

Step 5 Click **Label Config** corresponding to the chosen config drift version.

Step 6 In the **Label Configuration** window, enter a name for the config version. The prefix of label config is fixed as CCA_.

Note Do not use special characters for config version name.

Step 7 Click **Save**. The labeled config drift is shown in orange in the time-line graph.

If the number of labeled config version is greater than the chosen range, change the total number of config drifts to be saved. For more information on how to configure number of config drifts to be saved, see the "Configure Device Configuration Backup Settings" section in the [Cisco DNA Center Administrator Guide](#).

Step 8 To remove the label, select the labeled config version and click **Remove label**.

Replace a Faulty Device

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

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



Note You can also replace a faulty device using the **Replace Device** workflow. For more details, see [Replace Device Workflow](#).

Before you begin

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

Step 1 To mark a faulty device for replacement, do the following:

- a) Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

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

- b) Select the faulty device that you want to replace.
- c) From the **Actions** drop-down list, choose **Inventory > Device Replacement > Mark Device for Replacement**.
- d) In the **Mark for Replacement** window, click **Mark**.

Note To achieve seamless replacement of fabric devices, a DHCP server is configured on the neighbor device. This is required to assign an IP address to the replacement device for onboarding the device to Cisco DNA Center through PnP. This DHCP server is removed after successful replacement of the faulty device.

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

- e) From the **Inventory** drop-down list, choose **Marked for Replacement**.
A list of devices marked for replacement is displayed.
- f) (Optional) If you do not want to replace the device, select the device and choose **Actions > Unmark for Replacement**.

Step 2

(Optional) To replace the device, do the following:

- a) Select the device that you want to replace and choose **Actions > Replace Device**.
- b) In the **Choose Replacement Device** window, choose a replacement device from the **Unclaimed** tab or **Managed** tab.

The **Unclaimed** tab shows the devices that are onboarded through PnP. The **Managed** tab shows the devices that are onboarded through Inventory or Discovery process.

- c) (Optional) If the replacement device is not yet onboarded, do the following:
 1. In the **Choose Replacement Device** window, click **Add Device**.
 2. In the **Add New Device** window, enter the **Serial Number** of the device and click **Add New Device**.

Or

1. In the **Choose Replacement Device** window, click **Sync with Smart Account**.
2. In the **Sync with Smart Account** window, click **Sync**.

- d) Click **Next**.
- e) In the **Schedule Replacement** window, click **Now** to start the device replacement immediately or click **Later** to schedule the device replacement at a specific time.

If the replacement device is not yet onboarded, the **Now** option is disabled. You can click **Later** to schedule the device replacement at a specific time.

- f) Click **Review** to view the chosen device type, faulty device details, and replacement device details.
- g) Click **Next** to view the details in the **Summary** window.
- h) In the **Summary** window, do the following:
 1. Click **Edit** if you want to change the device type, faulty device, or replacement device chosen in the previous steps.
 2. Under **Replacement Device**, click **View** to view the configuration of the replacement device.
 3. Click **Replace**.
- i) Click **Monitor Replacement Status** to go to the **Mark for Replacement** view in the **Provision** window.
- j) Click **Replace Status** for the replacement device to view the status of the RMA workflow progress, as follows:

- Claim the (PnP) replacement device.
- Distribute and activate the software image to the replacement device.
- Deploy licenses.
- Provision VLAN configurations.
- Provision startup configurations.
- Reload the replacement device.
- Check for reachability of the replacement device.
- Deploy SNMPv3 credentials to the replacement device.
- Synchronize the replacement device.

- Remove the faulty device from CSSM.
- Add the replacement device to CSSM.
- Revoke and create the PKI certificate.
- Update Cisco ISE.
- Delete the faulty device.

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

- If an error message appears, click the error link.
- Click **Retry** to retrigger the workflow with the same set of faulty and replacement devices.

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

The preceding tasks of marking the device for replacement and replacing the device can be done at different times.

Replace a Faulty Access Point

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

Before you begin

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

Step 1 Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

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

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

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

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

- Step 5** From the **Actions** drop-down list, choose **Replace Device**.
- Step 6** In the **Replace Device** window, click **Start**.
- Step 7** In the **Available Replacement Devices** table, click the radio button next to the replacement device name.
- Step 8** Click **Next**.
- Step 9** Review the **Replacement Summary** and then click **Next**.
- Step 10** In the **Schedule Replacement** window, select whether to replace the device now, or schedule the replacement for a later time, and then click **Submit**.
The RMA workflow begins.
- Step 11** To monitor the replacement status, under **What's Next**, click **Monitor Replacement Status**.
The **Mark For Replacement** window lists the devices that are marked for replacement.
Check the status of the replacement in the **Replace Status** column, which initially shows **In-Progress**.
- Step 12** Click **In-Progress** in the **Replace Status** column.
The **Replace Status** tab shows the various steps that Cisco DNA Center performs as part of the device replacement.
- Step 13** In the **Marked for Replacement** window, click **Refresh** and click **Replace Status** to view the replacement status.
If the faulty AP replacement fails, then the **Replace Status** column shows the reason for failure with an error message.
You can either replace the faulty AP with another new AP or retry the failed replacement using the AP RMA Retry feature.
- Step 14** To retry the failed replacement, click the error message in the **Replace Status** column against the device name.
- Step 15** Click **Retry**.
- Step 16** In the **Marked for Replacement** window, click **In-Progress** against the **Replace Status** column.
The **Replace Status** tab shows success after successful replacement of the faulty AP.
- Step 17** The **Replace Status** in the **Replacement History** window shows **Replaced** after the faulty device is replaced successfully.
- Step 18** (Optional) If you do not want to replace the device, select the device and choose **Actions** > **Unmark for Replacement**.
-

Limitations of the RMA Workflow in Cisco DNA Center

- RMA supports replacement of similar devices only. For example, a Cisco Catalyst 3650 switch can be replaced only with another Cisco Catalyst 3650 switch. Also, the platform IDs of the faulty and replacement devices must be the same.
- RMA supports replacement of all switches, routers, and Cisco SD-Access devices, *except for the following*:
 - Devices with embedded wireless controllers
 - Cisco Wireless Controllers
 - Chassis-based Nexus 7700 Series Switches
 - Switch stacks (hardware and SVL stacking)

- RMA supports devices with an external SCEP broker PKI certificate. The PKI certificate is created and authenticated for the replacement device during the RMA workflow. The PKI certificate of the replaced faulty device must be manually deleted from the certificate server.
- The RMA workflow supports device replacement only if:
 - Both faulty and replacement devices have the same extension cards.
 - The number of ports in both devices does not vary because of the extension cards.
 - The faulty device is managed by Cisco DNA Center with a static IP. (RMA is not supported for devices that are managed by Cisco DNA Center with a DHCP IP, except for extended node and AP in fabric.)
- Fabric edge replacement does not support the DHCP server configuration in the neighbor device if the neighbor device is not part of the fabric. Because intermediate nodes are not part of the Cisco SD-Access fabric, the DHCP server with option 43 is not pushed.
- Make sure that the replacement device is connected to the same port to which the faulty device was connected.
- Cisco DNA Center does not support legacy license deployment.

The RMA workflow deregisters the faulty device from Cisco SSM and registers the replacement device with Cisco SSM.

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

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

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

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

- Cisco DNA Center supports PnP onboarding of the replacement device in a fabric network, except for the following:
 - The faulty device is connected to an uplink device using multiple interfaces.
 - LAN automation using an overlapping pool.
- If the replacement device onboards through PnP-DHCP functionality, make sure that the device gets the same IP address after every reload and the lease timeout of DHCP is longer than two hours.

Reboot the Access Point

Using the AP Reboot feature, you can reboot one or more APs for troubleshooting and maintenance.

Before you begin

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

-
- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
- Step 2** Check the check box of the APs that you want to reboot.
- Step 3** From the **Actions** drop-down list, choose **Inventory > Reboot Device**.
- Step 4** In the Reboot Device slide-in pane, you are prompted to reboot the AP now or schedule the reboot for a later time.
- To reboot the AP now, click the **Now** radio button, and enter a name for the reboot task.
 - To schedule the reboot for a later time, click the **Later** radio button, enter a name for the task, and define the date and time of the reboot.
- Step 5** Expand **Selected Devices** to view the AP name and floor details of the reboot AP.
- Step 6** Click **Reboot**.
- After the Cisco Wireless Controller initiates rebooting the selected APs, a message saying `Reboot Initiated Successfully` is displayed.
- Step 7** In the **Task Submitted** pop-up, click the **Task** link.
- If you missed the **Task Submitted** pop-up, click the menu icon (☰) and choose **Activities > Tasks**.
- Step 8** Under AP Reboot, click the AP reboot task name to view the reboot initiation status.
-

