



Manage Your Inventory

- [About Inventory, on page 2](#)
- [Inventory and Cisco ISE Authentication, on page 2](#)
- [Display Information About Your Inventory, on page 3](#)
- [Manage User-Defined Fields, on page 17](#)
- [Launch Topology Map from Inventory, on page 18](#)
- [Types of Devices in the Cisco DNA Center Inventory, on page 18](#)
- [Filter Devices, on page 38](#)
- [Manage Devices in Inventory, on page 39](#)
- [Configure a REP Ring for Devices, on page 43](#)
- [Add a Node to a REP Ring for Nonfabric Deployment, on page 44](#)
- [Create Port Groups, on page 45](#)
- [Assign Tags to Ports, on page 46](#)
- [Port Usage Information, on page 46](#)
- [Maintenance Mode for Devices, on page 47](#)
- [Inventory Insights, on page 48](#)
- [Manage System Beacon, on page 50](#)
- [Change the Device Role \(Inventory\), on page 50](#)
- [Update a Device's Management IP Address, on page 51](#)
- [Update the Device Polling Interval, on page 52](#)
- [Resynchronize Device Information, on page 53](#)
- [Delete a Network Device, on page 53](#)
- [Launch Command Runner \(Inventory\), on page 54](#)
- [Troubleshoot Device Reachability Issues Using Run Commands, on page 54](#)
- [Use a CSV File to Import and Export Device Configurations, on page 55](#)
- [Configuration Drift of a Device, on page 57](#)
- [View Configuration Drift of a Device, on page 58](#)
- [Label Configuration Drift, on page 59](#)
- [Visibility of Configurations Workflow, on page 60](#)
- [Replace a Faulty Device, on page 61](#)
- [Replace a Faulty Access Point, on page 63](#)
- [Limitations of the RMA Workflow in Cisco DNA Center, on page 64](#)
- [Reboot Access Point, on page 65](#)

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 52](#). 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





You can display and filter for information about discovered devices in your inventory. You can also customize or change the information displayed in the **Devices** table.

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 > Inventory**.

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

Step 2 (Optional) To change the Inventory view, use the toggle button (☰    ) in the top-right corner. You can change your default view (the list layout) to other layouts, such as the topology or map layout.

Step 3 (Optional) To change the **Devices** table's focus views, from the **Focus** drop-down list, choose a view, such as **Default**, **Inventory**, or **Software Images**.

Note

- The displayed columns change depending on the chosen focus view.
- Selected devices persist in each new focus view.

Step 4 (Optional) To filter for specific device details in the **Devices** table, you can do the following:

- To filter for a device family, choose one or more of the device family buttons at the top of the **Inventory** window. For example, you can click **Routers** to display only routers in the table.
- To filter for device work items, in the left pane, check the check box of one or more work items. The table is immediately filtered for the work item. For example, you can check the **Unreachable** check box to display only unreachable devices in the table.
- To filter for specific device details, click **Filter devices** and choose from the filter options: **Quick Filters**, **Advanced Filters**, or **Recent Filters**. Then click **Apply**.

For more information, see [Filter Devices, on page 38](#).

Step 5 (Optional) To take a guided tour of the **Inventory** window, click **Take a tour** in the top-right corner.

Step 6 (Optional) To export all the data in the **Devices** table, click **Export** in the top-right corner.


Step 7 (Optional) To customize the **Devices** table, click the settings icon (⚙️) in the top-right corner, choose from the following options in the **Table Settings** slide-in pane, and then click **Apply**.

- **Table Appearance:** Choose if you want the default or compact table view and table striping.
- **Edit Table Columns:** Choose if you want to create a custom view and if you want to hide or display columns. Note that the column selection does not persist across sessions.

The following table provides key information relevant to certain table columns.


Column	Description
Device Name	<p>Name of the device.</p> <p>Click the device name for more information about that device.</p> <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>
Support Type	<p>Shows the device support level:</p> <ul style="list-style-type: none"> • Supported: The device profile 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 profile for legacy devices is tested only for the following features and tested only on a best-effort basis on Cisco DNA Center. <ul style="list-style-type: none"> • Discovery • Topology • Device Reachability • Config Change Audit • Inventory • 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 the Cisco DNA Center Legacy Device Compatibility Matrix.</p> • Third Party: The device profile has been tested on Cisco DNA Center for third-party devices that are capable of populating SNMP MIB 2 values. Cisco DNA Center support limited base automation capabilities, such as Inventory and Topology as a best effort basis. <p>For more information, see the Cisco DNA Center Compatibility Matrix.</p> • Unsupported: All remaining Cisco and third-party devices that are not tested and certified on Cisco DNA Center. You can try out various functionalities on Cisco DNA Center for these devices, as a best effort. However, you cannot raise a service request or a bug if Cisco DNA Center features do not work as expected.

Column	Description
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.
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>Hover your cursor over the i icon next to EoX Status, and click Click here to accept to initiate an EoX scan.</p> <p>For the devices that are scanned successfully, the EoX Status column shows the number of alerts, if any. 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. Hover your 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 because of device connectivity issues.
Platform	Cisco product part number.
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	<p>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.</p>

Column	Description
Last Updated	Most recent date and time on which Cisco DNA Center scanned the device and updated the database with new information about the device.
Resync Interval	The polling interval for the device. Set the resync interval from the Inventory window by choosing Actions > Edit Device > Resync Interval . To set the resync type as Global , from the main menu, choose System > Settings . For more information, see the Cisco DNA Center Administrator Guide .
Provisioning Status	Shows the status of the last provisioning operation attempted on a device. Click See Details to view the status of past provisioning operations. <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 never been provisioned. • Out of Sync: The network settings or network profiles for a device have been modified after the last provisioning operation.
Credential Status	Shows the device credential status: <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 your 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 CDP Neighbors	Displays details about the switch and port connected to an AP in the Inventory window. This window displays information about AP CDP neighbors even if the connected access switch is managed by Cisco DNA Center.

- **Edit Custom Views:** First you must create a custom view in the **Edit Table Columns** tab, and then you can edit the custom view.
- **Reset All Settings:** Reset the table settings to the default settings.

Step 8 (Optional) To manage your devices from the **Devices** table, you can use the following options:

Name	Description
Add Device	<p>You can click Add Device to add a network or compute device, or integrate a Meraki dashboard or Firepower Management Center (FMC) with Cisco DNA Center.</p> <p>For more information, see Types of Devices in the Cisco DNA Center Inventory, on page 18.</p>
Tag	<p>You can click Tag to tag devices, edit and delete tags, or create port groups.</p> <p>For more information, see Manage Devices in Inventory, on page 39.</p>
Actions drop-down list	<p>You can use the Actions drop-down list to manage your devices, software images, telemetry, and more.</p> <p>To view more details about each action option, click the right-adjacent information icon ().</p>

Step 9 (Optional) In the **Devices** table, you can do the following:

- To sort the columns in either ascending or descending order, click the column header.
- To view more details about a device, click the device name and then click **View Device Details**.
- To view a device's compliance details, click either **Non-Compliant** or **Compliant** under the **Compliance** column.
- To assign a site to a device, click **Assign** under the **Site** column.
- To change a device role, click the edit icon under the **Device Role** column and then choose from the options, such as **ACCESS** or **CORE**.
- To mark an image as Golden or view its needed updates, click **Mark Golden** or **Needs Update** under the **Software Image** column.
- To change the number of entries, scroll down to the bottom of the window, and from the **Show Records** drop-down list, choose the number of entries that you want displayed.

Note that if there are more than 25 entries in the table and you choose a different focus view, the same number of entries is displayed in each new view.

Note Each focus view displays different columns, and you can customize a table view to include columns, such as **Compliance**, **Site**, **Device Role**, and **Software Image**.

Display Information About a Device

You can display, filter, and search for information about a discovered device, its security, and its compliance.

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 > Inventory**.

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



Step 2 In the **Devices** table, click the name of a device and more information about the device is displayed.



Step 3 Click **View Device Details**.

The device details are displayed in the window.

Step 4 Use the following table that describes the available information in this window to display, filter, and search for details about a device.

Name	Description
Run Commands	<p>This link is only available for routers, wireless controllers, switches, and hubs.</p> <p>Launch the Command Runner application to run diagnostic CLI commands and view the resulting command output on a device.</p> <p>To launch Command Runner, you must have installed the Command Runner application. For more information, see the Cisco DNA Center Administrator Guide.</p>
Learn WLC Config	<p>This link is only available for wireless controllers.</p> <p>Click the link to open Learn Device Configuration window, where you can provision a wireless controller.</p> <p>To open this window, the wireless controller must be reachable and in a Managed state.</p>
View 360	<p>This link is available for all devices.</p> <p>Displays the Device 360 window for that device.</p> <p>To open this window, you must have installed the Assurance application.</p>
Interfaces	<p>This tab is available for all devices except APs.</p> <p>Displays information about the device's ports, such as its Ethernet ports, in a topology or table view.</p> <p>For more information about device interfaces, see Display Information About a Device's Interface, on page 12.</p>

Name	Description
Hardware & Software	<p>This tab is available on all devices.</p> <p>Displays the device's hardware and software details, such as its uptime and provision status, with an operational summary.</p>
Configuration	<p>This tab is only available for APs, routers, switches, and hubs.</p> <p>For routers, switches, and hubs, this tab displays detailed configuration information that is similar to what is displayed in the output of the show running-config command. You can hide line numbers, search for a command line or piece of text, or export the CLI output.</p> <p>For APs, this tab displays information about the AP configuration, 2.4-GHz radio configuration, and 5-GHz radio configuration.</p> <p>This feature is not supported for wireless controllers, so configuration data is not returned for this device type.</p>
Power	<p>This tab is only available for routers, switches, and hubs.</p> <p>Displays details about the device's power usage and supplies.</p> <p>To specify or narrow down the data in the Power Supplies table, you can either:</p> <ul style="list-style-type: none"> • Click Search Table, manually enter a value, and then press the Enter key. The narrowed search results are displayed with the value highlighted throughout the table. • Click the filter icon () to display power supplies by any combination of values, such as values for the Name, Operational Status, and Serial Number fields.
Fans	<p>This tab is only available for routers, switches, and hubs.</p> <p>Displays details about fans.</p> <p>To specify or narrow down the data in the Fans table, you can either:</p> <ul style="list-style-type: none"> • Click Search Table, manually enter a value, and then press the Enter key. The narrowed search results are displayed with the value highlighted throughout the table. • Click the filter icon () to display fans by any combination of values for the Name and Operational Status fields.

Name	Description
SFP Modules	<p>This tab is only available for routers, switches, and hubs.</p> <p>Displays details such as the manufacturer and the ports that Small Form-Factor Pluggable (SFP) modules are connected to.</p> <p>To specify or narrow down the data in the SFP Modules table, you can either:</p> <ul style="list-style-type: none"> • Click Search Table, manually enter a value, and then press the Enter key. The narrowed search results are displayed with the value highlighted throughout the table. • Click the filter icon () to display SFP modules by any combination of values, such as values for the Name, Platform, and Serial Number fields.
User Defined Fields	<p>This tab is available for all devices.</p> <p>Displays the user-defined fields that are associated with the device.</p> <p>Click Manage User Defined Fields to display the Manage User Defined Fields slide-in pane. You can do the following:</p> <ul style="list-style-type: none"> • Click Create New Fields to create a new field. • Click Search Table, manually enter a value, and then press the Enter key. The narrowed search results are displayed with the value highlighted throughout the table. • Click the filter icon () to display user-defined fields by any combination of values, such as values for the Name, Description, and Action fields. <p>To add a user-defined field to a device, you first must create a user-defined field in the Manage User Defined Fields slide-in pane. For more information, see Create User-Defined Fields, on page 17.</p> <p>To display a user-defined field, you must assign it to a device and add a value to it. For more information, see Add User-Defined Fields to a Device, on page 18.</p>
Config Drift	<p>This tab is available for all devices.</p> <p>Displays configuration changes on the device, including a change history, and compares two configuration versions. You can do the following:</p> <ul style="list-style-type: none"> • Label the configuration drift on the time line for future reference. For more information, see Label Configuration Drift, on page 59. • Pick any two versions of the same device and compare their running configuration data.

Name	Description
REP Rings	<p>This tab is available for all devices.</p> <p>Displays details about Resilient Ethernet Protocol (REP) rings, such as its name, ring size, first adjacent device, and so on.</p> <p>Click Create REP Ring and follow the workflow to create a REP ring.</p> <p>For more information, see Delete a Node from a REP Ring or Delete a REP Ring.</p>
Wireless Info	<p>This tab is only available for wireless controllers.</p> <p>Displays details about managed sites, wireless, redundancy, health parameters, and more.</p> <p>In the Wireless Summary tab, in the SSIDs table, you can search for a specific value by clicking Search Table, manually entering a value, and then pressing the Enter key. The narrowed search results are displayed with the value highlighted throughout the table.</p>
Mobility	<p>This tab is only available for wireless controllers.</p> <p>Displays mobility details, such as the mobility group name, RF group name, and so on.</p> <p>The Mobility Peers table is displayed if mobility peers are configured on the device. If mobility peers are not configured, see Configure Mobility Group.</p> <p>You can filter the table to display specific mobility peers by any combination of values, such as values for MAC address, Device Name, and IP Address fields.</p>
Advisories	<p>This tab is available for all devices.</p> <p>Displays a device's advisory details in the Advisories table. You can do the following:</p> <ul style="list-style-type: none"> • Click Manage All to display the Security Advisories window to manage your devices and advisories. • Click Filter to display advisories by any combination of values, such as values for the Advisory ID and Advisory Title fields. Then click Apply. • Click an advisory ID to display more information about that advisory. • In the Custom Match Pattern column, click Add match pattern to add or update a condition to match with devices in the CONDITIONS text box. Then you can save the match pattern and run a scan to check the number of devices that match with the match pattern.
Field Notices	<p>Displays information about field notices for the device. See View Field Notices.</p>
Potential Field Notices	<p>Displays information about potential field notices for the device.</p>

Name	Description
Summary	<p>This tab is available for all devices.</p> <p>Displays a device's compliance summary, such as when compliance last ran for the Startup vs Running configuration. You can do the following:</p> <ul style="list-style-type: none"> • Click Run Compliance Check to check the device for compliance. • Click View Preference for Acknowledged Violations to view the list of acknowledged violation attributes. You can unlist a violation to open it.

Display Information About a Device's Interface

For routers, wireless controllers, switches, or hubs, you can display, search, and filter for information about a device's interface. Depending on the device, certain information is available.

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



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

Step 2 In the **Devices** table, click the name of a device, and then click **View Device Details**.

Step 3 In the left pane, expand **Interfaces**.


Step 4 Use the following table that describes the **Interfaces** drop-down list options to display details about an interface.


Name	Description
Ethernet Ports	<ul style="list-style-type: none"> • This tab is available for all devices except APs. • Displays Ethernet ports details in two views: topology and table. <ul style="list-style-type: none"> • The topology view displays the Ethernet port topology of a device with a color-coded system of each port's connection status. • The table view displays Ethernet ports details, such as the ports' operational status, admin status, and so on. • For more information about the two views, see Display Information About Ethernet Ports, on page 13.

Name	Description
VLANs	<ul style="list-style-type: none"> • This tab is only available for switches and hubs. • Displays VLAN details, such as its operational status and admin status, in table format. • The VLANs table 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>To specify or narrow down the data in the VLANs table, you can either:</p> <ul style="list-style-type: none"> • Click Search Table, manually enter a value, and then press the Enter key. The narrowed search results are displayed with the value highlighted throughout the table. • Click the filter icon () to display VLANs by any combination of values, such as values for the VLAN Name, VLAN ID, and Operational Status fields.
Virtual Ports	<ul style="list-style-type: none"> • This tab is only available for wireless controllers and routers. • Displays details about ports, such as its operational status, admin status, and so on. • To specify or narrow down the data in the VLANs table, you can either: <ul style="list-style-type: none"> • Click Search Table, manually enter a value, and then press the Enter key. The narrowed search results are displayed with the value highlighted throughout the table. • Click the filter icon () to display virtual ports by any combination of values, such as values for the Port Name, Operational Status, and Admin Status fields.

Display Information About Ethernet Ports

In the **Ethernet Ports** tab, you can display, search, and filter for certain information about a port or ports through either the topology view or table view.

- Step 1** Click the menu icon () and choose **Provision > Inventory**.
- Step 2** In the **Devices** table, click a device name, and then click **View Device Details**.
- Step 3** In the left pane, expand **Interfaces** and choose **Ethernet Ports**.

Step 4 In the upper-right corner, click **Topology View** () to view the Ethernet port topology if it's not already displayed. This view displays the Ethernet port topology of a device with a color-coded system of each port's connection status. Hover your cursor over a port for more details.

Note For Cisco Catalyst 4000 Series, 6000 Series, and 9000 Series Switches and Cisco ASR 1000 Series Aggregation Services Routers, this view displays line cards and supervisor cards details, such as the part number and serial number, if the cards are available.

Step 5 In the topology view, you can do the following:

- To view the error reason for an error-disabled port, click the port.
- To filter for a specific Ethernet port, use the **Color Code** drop-down list. The following table describes the available drop-down list options.


Table 1: Color Code Drop-Down List Options

Name	Description
Status	Displays the default view of the topology view.
Access VLANs	Displays the access VLAN assigned to a particular port. The Access VLANs view allows you to select a maximum of five access VLANs and lists only the access VLANs associated with the port. This option displays the access VLANs in the following color-coded system: Selected , Not Configured , Default , and VLAN .
Port Channels	Displays the top five port channels that are configured on the device. This option only displays the configured port channels on the device in the following color-coded system: Selected and Port-channel with a corresponding number.

Step 6 In the upper-right corner, click **Table View** () to view the **Ports** table.

The **Ports** table displays Ethernet ports details, such as a ports' operational status, admin status, and so on.

Step 7 (Optional) To specify or narrow down the data in the **Ports** table, you can:

- Click **Search Table**, manually enter a value, and then press the **Enter** key. The narrowed search results are displayed with the value highlighted throughout the table.
- Click the filter icon () to display ports by any combination of values, such as values for the **Tags**, **Port Name**, and **Type** fields. Enter the wanted values, and click **Search**.

Step 8 (Optional) In the table view, you can do the following:

- Click **Tag** to tag a port or ports, search for a tag, or manage tags.

For more information, see [Assign Tags to Ports, on page 46](#).

- Click **Export** to export the **Ports** table data.

Manage Port Details

You can manage and edit certain port details of a device.

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

Step 2 In the **Devices** table, click a device name, and then click **View Device Details**.

Step 3 In the left pane, expand **Interfaces** and choose **Ethernet Ports**.

Step 4 Click a port in the topology view (🏠 📄), or click a port name in the table view (🏠 📄).

Information about the port is displayed.

- Note**
- For Cisco Catalyst 2000, 3000, and 9000 Series Switches, port details include the port's maximum allocated power and power drawn.
 - This window displays the details of the CDP neighbor. If CDP is not present, the LLDP neighbor details displays. If both CDP and LLDP neighbors are not present, the **Neighbor Details** area is hidden from this window.

Step 5 (Optional) Click **Tag** to tag the port, search for a tag, manage tags, or create a new tag.

For more information, see [Assign Tags to Ports, on page 46](#).

Step 6 (Optional) To manage the port, click the **Port Actions** drop-down list and choose from the following options:

- To shut down the port and change the port's admin status to Down, choose **Port Shut**. Then click **Okay** to confirm. This option is only available when the port is open and the admin status is Up.
- To open the port and change the port's admin status to Up, choose **Port No Shut**. Then click **Okay** to confirm. This option is only available when the port is shut and the admin status is Down.
- To clear the port's MAC address, choose **Clear Mac Address**.
- To activate an error-disabled port, clear the MAC address and shut down the port.

- Note**
- The device software type must be Cisco IOS or Cisco IOS XE to clear the MAC address and shut down a port.
 - For wireless controllers, clearing the MAC address and shutting down the port are not supported.
 - Clearing the MAC address and shutting down the port are supported only on access ports.
 - Port shutdown disrupts the traffic on a port.

Step 7 To edit certain port details, such as the port description area, use the following table.

Name	Description
Access VLAN	Click the Edit icon. In the Edit Access VLAN dialog box, choose an access VLAN from the drop-down list, and then click Save to assign the access VLAN to the port. You cannot update the access VLAN for the ports that have two access VLANs preconfigured.
Voice VLAN	Click the Edit icon next to Voice VLAN . In the Edit Voice VLAN dialog box, choose a voice VLAN from the Select Value drop-down list, and then click Save to assign the voice VLAN to the port.
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. In the Warning dialog box, click Okay .

- Note**
- The device software type must be Cisco IOS or Cisco IOS-XE to edit VLAN details and the port description.
 - Editing VLAN details is supported only on access ports.
 - For wireless controllers, editing VLAN details is not supported.

Inventory User Interface Enhancement

The enhanced Cisco DNA Center inventory user interface provides the existing inventory features while improving filters and layout for a better user experience.

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 > Inventory**.
- The enhanced **Inventory** window appears by default and displays the device information gathered during the discovery process.
- Step 2** Click the location option in the top menu bar to select the site, building, or floor from the network hierarchy to manage your device.
- Step 3** Use the device families area appears at the top of the **Inventory** window to select one or more device families.
- The available device families are: **Routers**, **Switches**, **Wireless Controllers**, **Access Points**, and **Sensors**.
- Step 4** Use the **Focus** drop-down list to filter the devices based on **Inventory**, **Default**, **Software Image**, **Provision**, **Security**, or **Device Replacement**.
- Step 5** Use the divider bar at the left corner of the **Device** table to collapse or expand the table width.

- Step 6** In the **DEVICE WORK ITEMS** area, select one or more filter criteria to narrow down the devices in the table.
- Step 7** Click **Add Device** to add a new device in the inventory. For more information, see [Add a Device to a Site](#).
- Step 8** Use **Tag** to tag a device. For more information, see [Manage Devices in Inventory, on page 39](#).
- Step 9** Use the **Action** drop-down list to perform the device actions on one or more devices.
- Step 10** Click the **i** icon to learn about the list of actions and their respective functionalities.
- Step 11** To edit or customize the inventory table, click the gear icon in the right corner at the top of the table and do the following:
- Click **Table Appearance** to define the **Table Density** and **Table Striping**.
 - Click **Edit Table Columns** to select the device information that you want to include in the inventory table during the discovery process.
 - Click **Edit Custom Views** to customize your current view.
 - Click **Apply** to save the changes or click **Reset All Settings** to apply the default settings for the inventory table.
- Step 12** Use the **Filter Devices** option to apply the advanced filter in your device table. For more information, see [Filter Devices](#).
- Step 13** Click the toggle buttons at the top-right corner to switch between **Dashboard**, **Table**, **Topology**, and **Map** view.
- Step 14** Click **Go to old page** to navigate to old inventory window.
- Step 15** Use **Export** to export all data in the device table.
-

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. 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** window 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** slide-in pane, click **Create New Field**.
- Step 4** In the **Create New Field** dialog box, enter a name and description in the **Field Name** and **Field Description** fields.
- Note** You can add device details that are not already present in the **Device Details** window, 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. These fields are displayed in a table.
- Step 6** (Optional) To edit a user-defined field, click the corresponding edit icon, make the required changes, and click **Save**.

- Step 7** (Optional) 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 17](#).

- 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 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 from the **Field Name** drop-down list, and enter the customer IP address in the **Value** field.
- Step 6** (Optional) 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 **Provision > 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.
- **Third-Party Device:** Third-party devices are capable of populating SNMP MIB 2 values. Cisco DNA Center support limited base automation capabilities, such as Inventory and Topology as a best effort basis.

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 > 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) To use global credentials, click the **Select global credential** radio button.

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) To configure credentials for the specific device, click the **Add device specific credential** radio button and configure the following fields:

Table 2: CLI Credentials

Field	Description
Name/Description	Name or phrase that describes the CLI credentials. If authentication fails for CLI, Cisco DNA Center retries the authentication process for 300 seconds (5 minutes).
Username	Name that is used to log in to the CLI of the devices in your network.
Password	Password that is used to log in to the CLI of the devices in your network. For security reasons, re-enter the password as confirmation. Note Passwords are encrypted for security reasons and are not displayed in the configuration.
Enable Password	Password used to move to a higher privilege level in the CLI. Configure this password only if your network devices require it. For security reasons, re-enter the enable password. Note Passwords are encrypted for security reasons and are not displayed in the configuration.

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

- a) To use global credentials, click the **Select global credential** radio button.

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 choose **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>

Field	Description
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 choose **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"> • Authentication and Privacy: Provides both authentication and encryption. • Authentication, No Privacy: Provides authentication, but does not provide encryption. • No Authentication, No Privacy: Does not provide authentication or encryption.
Auth. Type	Authentication type to be used. (Enabled if you select Authentication and Privacy or Authentication, No Privacy as Mode .) Choose one of the following authentication types: <ul style="list-style-type: none"> • SHA: Authentication based on HMAC-SHA. • MD5 (not recommended): 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.

Field	Description
Privacy Type	<p>Privacy type. (Enabled if you select Authentication and Privacy as Mode.) Choose one of the following privacy types:</p> <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.
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 times Cisco DNA Center tries to communicate with network devices using SNMP.
Timeout (in Seconds)	Amount of time, in seconds, between retries.

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

- 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](#).

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

Table 6: HTTP(S) Credentials

Field	Description
Type	Specifies the kind of HTTPS credentials you are configuring. Valid types are Read or Write .
Read	<p>You can configure up to 10 HTTPS read credentials:</p> <ul style="list-style-type: none"> • Name/Description: Name or description of the HTTPS credentials that you are adding. • Username: Name used to authenticate the HTTPS connection. • Password: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • Port: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). <p>The password must contain between 7 and 128 characters, including at least one of the following:</p> <ul style="list-style-type: none"> • Lowercase letter (a to z) • Uppercase letter (A to Z) • Number (0 to 9) • Special character: # _ * ? - <p>The password cannot contain spaces or angle brackets (<>). Note that some Cisco IOS XE devices do not allow a question mark (?).</p>
Write	<p>You can configure up to 10 HTTPS write credentials:</p> <ul style="list-style-type: none"> • Name/Description: Name or description of the HTTPS credentials that you are adding. • Username: Name used to authenticate the HTTPS connection. • Password: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • Port: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). <p>The password must contain between 7 and 128 characters, including at least one of the following:</p> <ul style="list-style-type: none"> • Lowercase letter (a to z) • Uppercase letter (A to Z) • Number (0 to 9) • Special character: # _ * ? - <p>The password cannot contain spaces or angle brackets (<>). Note that some Cisco IOS XE devices do not allow a question mark (?).</p>

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

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

Table 7: NETCONF Setting

Field	Description
Port	<p>Port on the device. You can use one of the following ports:</p> <ul style="list-style-type: none"> • Port 830 (default). • Any other port that is available on the device. • A custom port that Cisco DNA Center configures. (You can use a custom port only if Device Controllability is enabled. For more information, see the Device Controllability section in the <i>Cisco DNA Center Administrator Guide</i>.) <p>If authentication fails for NETCONF, Cisco DNA Center retries the authentication process for 300 seconds (5 minutes).</p>

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.



Note You cannot update credentials of a third-party device discovered by Cisco DNA Center.

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 > Inventory**.

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

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

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

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

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

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

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

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

Table 8: 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 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** window. 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 9: 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>

Field	Description
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 10: 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"> • Authentication and Privacy: Provides both authentication and encryption. • Authentication, No Privacy: Provides authentication, but does not provide encryption. • No Authentication, No Privacy: Does not provide authentication or encryption.
Auth. Type	Authentication type to be used. (Enabled if you select Authentication and Privacy or Authentication, No Privacy as Mode .) Choose one of the following authentication types: <ul style="list-style-type: none"> • SHA: Authentication based on HMAC-SHA. • MD5 (not recommended): 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.

Field	Description
Privacy Type	<p>Privacy type. (Enabled if you select Authentication and Privacy as Mode.) Choose one of the following privacy types:</p> <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.
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 11: 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** window. See [Configure Global HTTP\(S\) Credentials](#).

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

Table 12: HTTP(S)

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

- Step 10** Expand the **NETCONF** area, if it is not already expanded, and configure the **Port** field. NETCONF requires that you configure SSH as the CLI protocol and define the SSH credentials.
- Step 11** Select one of the network **Protocol** radio buttons that enables Cisco DNA Center to communicate with remote devices. Valid values are **SSH2** or **Telnet**.
- Step 12** (Optional) Click **Validate** next to **Credentials**. Cisco DNA Center validates the device credentials and shows the valid credentials with green tick mark and invalid credentials with red cross mark.
If you have chosen more than one device for updating the credentials, the **Validation** button will be disabled.
- Step 13** Click **Update**.

Security Focus for Network Devices

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

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

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

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

These checks are triggered under the following circumstances:

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

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

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

View the Integrity Verification Status of a Device

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

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

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

Step 2 From the **Focus** drop-down menu, choose **Security**.

Step 3 In the **Devices** table, if the **Integrity Verification** column for your device displays **Failed** as the status, click the information icon (i) to display the reason.

Note If the **Integrity Verification** column is not displayed, see [Display Information About Your Inventory, on page 3](#).

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 > Inventory**.

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

Step 2 Click **Add Device**.

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

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

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

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

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

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

Table 13: HTTP(S)

Field	Description
Username	Name used to authenticate the HTTPS connection.
Password	Password used to authenticate the HTTPS connection.

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

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

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

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

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

Table 14: 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 15: 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 16: 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"> • Authentication and Privacy: Provides both authentication and encryption. • Authentication, No Privacy: Provides authentication, but does not provide encryption. • No Authentication, No Privacy: Does not provide authentication or encryption.
Auth. Type	Authentication type to be used. (Enabled if you select Authentication and Privacy or Authentication, No Privacy as Mode .) Choose one of the following authentication types: <ul style="list-style-type: none"> • SHA: Authentication based on HMAC-SHA. • MD5 (not recommended): Authentication based on HMAC-MD5.

Field	Description
Auth. Password	<p>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> <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	<p>Privacy type. (Enabled if you select Authentication and Privacy as Mode.) Choose one of the following privacy types:</p> <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.
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 > Inventory**.
The **Inventory** window 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 > Inventory**.
The **Inventory** window 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 > Inventory**.
The **Inventory** window 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** slide-in pane, 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 > Inventory**.
The **Inventory** window 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:
- 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 **Add**.
- Note** When you add FMC to inventory, the Firepower Threat Defense (FTD) devices managed by FMC are also added to inventory automatically. The available High Availability (HA) pairs with details of active and standby FTDs are shown in the **Inventory** window.
- Step 8** To view the HA details of the paired FTDs, do the following:
- Click the device name of FTD.
 - Click **View Device Details**.
- The paired FTD name is shown in the Device Details window. You can click the paired FTD name to view the paired FTD details.
- In the Device Details window, click **High Availability Details**.
- You can view the **HA Pair Info**, **High Availability Link**, and **State Link** details.
-

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 > Inventory**.
- The **Inventory** window 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**.
- Step 4** In the **Edit Device** slide-in pane, 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.

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

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

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

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

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

Step 10 Click **Update**.

Add a Third-Party Device

You can add a third-party device to your inventory manually. Third-party devices are capable of populating SNMP MIB 2 values. Cisco DNA Center support limited base automation capabilities, such as Inventory and Topology as a best effort basis.

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

Before you begin

Make sure you configure your network device.

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

The **Inventory** window displays the device information.

Step 2 Click **Add Device**.

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

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

Step 5 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 and click **Network Settings > Device Credentials** link to add credentials. See [Configure Global SNMPv2c Credentials](#) and [Configure Global SNMPv3 Credentials](#).
- b) Click the **Add device specific credential** radio button and do the following:

Step 6 From the **Select Value** drop-down list, choose **V2C** (SNMP Version 2c) or **V3** (SNMP Version 3).

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

Table 17: SNMPv2c Credentials

Field	Description
Read	<ul style="list-style-type: none"> • 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"> • 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 choose **V3**, configure the following fields:

Table 18: SNMPv3 Credentials

Field	Description
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"> • Authentication and Privacy: Provides both authentication and encryption. • Authentication, No Privacy: Provides authentication, but does not provide encryption. • No Authentication, No Privacy: Does not provide authentication or encryption.
Authentication Type	Authentication type to be used (enabled if you select Authentication and Privacy or Authentication, No Privacy as Mode). Choose one of the following authentication types: <ul style="list-style-type: none"> • SHA: Authentication based on HMAC-SHA. • MD5 (not recommended): Authentication based on HMAC-MD5.
Authentication 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.

Field	Description
Privacy Type	<p>Privacy type. (Enabled if you select Authentication and Privacy as Mode.) Choose one of the following privacy types:</p> <p>AES128: 128-bit CBC mode AES for encryption.</p> <p>Note Privacy type AES128 is supported for Discovery, Inventory, and Assurance.</p>
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 7 In the **SNMP Retries and Timeout** area, configure the following fields:

Table 19: SNMP Properties

Field	Description
Retries	Number of times Cisco DNA Center tries to communicate with network devices using SNMP.
Timeout (in Seconds)	Time interval between the retries.

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.

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

Step 9 Click **Add**.

Filter Devices

In the **Inventory** window, you can choose from basic or advanced filtering options to filter for device details in the **Devices** table.

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

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

Step 2 Click **Filter devices**.

The following table describes the available filtering options.

Name	Description
Quick Filters	You can choose from basic filtering options to narrow down the device details. For example, you can toggle the Manageability filter option to Managed to see all the managed devices.
Advanced Filters	You can set the filtering criteria using operators, such as Contains and Regex (Regular Expression), to narrow down the device details. For example, in the Tags drop-down list, you can choose the Contains operator and enter ipsec in the Tags field. Then from the autocomplete drop-down list, you can choose one option, such as branch-router-ipsec , which would filter for branch routers that are tagged with IP Security. You must enter filter criteria values based on the available data.
Recent Filters	In the RECENT area, you can choose a recent filter to reapply. To save a recent filter, drag and drop a recent filter to the SAVED area.

Step 3 Choose a filtering option and enter the appropriate value in the selected filter field.

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 wanted value.

You can also use a wildcard (asterisk) with these filters. For example, you can enter values with an asterisk at the beginning, end, or in the middle of a string value. 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.**Step 6** (Optional) To remove all the filters, in the **Filter devices** field, click the **x** and then click **Apply**.**Step 7** (Optional) To delete a specific filter value, in the **Filter devices** field, drag your cursor over the value, press **Delete**, and then click **Apply**.

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.
- Note** You cannot assign Firepower Threat Defense (FTD) high availability (HA) paired devices to different sites. Both the paired devices must be assigned to the same 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 and click **Save**.
- Step 6** (Optional) If you select multiple devices to add to the same location, check the **Apply to All** check box for the first device to assign its location to the rest of the devices and click **Next**.
- Step 7** Check **Application and Endpoint Visibility is enabled on all applicable devices. Check this to skip enabling it on all devices** check box.
- Note** **Application and Endpoint Visibility** enablement is skipped by default for the devices that does not support Controller-Based Application Recognition (CBAR) enablement or undeployed Application Visibility Service (AVS).
- Step 8** Review summary settings and click **Next**.
- Step 9** Based on the Visibility of Configurations settings, choose an available option. For more information, see [Visibility of Configurations Workflow, on page 60](#).
- To immediately assign the device to a site, click the **Now** radio button.
 - To schedule the task for a later date and time, click the **Later** radio button and define the date and time of the deployment.
 - Cisco DNA Center allows you to review the configurations before deploying them on Cisco network devices. The configuration can be reviewed from the **Preview Configuration** window.
 - To preview the CLI configuration, click the **Generate configuration preview** radio button.
- Step 10** In the **Task Name** field, enter a task name.
- Step 11** Click **Assign**.
- You can view the status of the task on the **Work Items** window. To navigate to the **Work Items** window, click the menu icon (☰) and choose **Activities > Work Items**.
- Step 12** 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 **Inventory** window.

-
- 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(s) for which you want to apply a tag, and then click **Tag**.
- 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 42](#).
 - 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:
- Select the device and click **Tag**. Unselect all tags, and then click **Apply**.
 - Hover the cursor over the yellow tag icon or tag name, and then click delete icon to disassociate the tag from the device.

Create a Network Device Group Tag

Use this procedure to create a Network Device Group (NDG) tag.

-
- 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 for which you want to apply a tag, and then click **Tag**.
- Step 3** Click **Create New Tag**.
- For the naming pattern, use the prefix **NDG:** and set the tag with the parent child hierarchy. For example, use #Location#All Locations, Device Type#All Device Types, or IPSEC#Is IPSEC.
- Note**
- Custom roots are not allowed while creating the NDG tag.
 - Only one NDG tag can be added per NDG type for a device.
 - The maximum level of hierarchy, including parent and roots, is limited to seven.
 - Each level name cannot exceed 32 characters. The tag length cannot exceed 100.
 - NDG tags support the basic ASCII character set.

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

Note Tags that are prefixed with **NDG :** are reflected in Cisco ISE.

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 > 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(s) for which you want to apply a tag, then click **Tag**.

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 > Network Devices > Inventory**.
The **Inventory** window 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**.

The previously created tags are listed.

Step 3 Click **Manage Tags**.

The **All Tags** slide-in pane is displayed.

Step 4 Click the pencil icon next to the tag that you want to edit.

Step 5 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 > Network Devices > Inventory**.

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

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

Configure a REP Ring for Devices

The Resilient Ethernet Protocol (REP) ring provides a way to control network loops, handle link failures, and improve convergence time.



Note

- Limitation of a REP Ring: You should not select a root node that has connectivity only through interfaces of the ring.
 - Device support for REP Ring (nonfabric): Cisco Catalyst Industrial Ethernet Series Switch 3200, 3300, 3400, 4000, and 5000. Cisco Embedded Services 3300 Series Switches (ESS3300), and S5800.
-

Before you begin

- Make sure the devices are onboarded and are in reachable state.
- Identify the devices and its interfaces that terminate the REP ring.

- Make sure all the interfaces which are part of the ring are configured with “switchport mode trunk”.

-
- Step 1** Click the menu icon (☰) and choose **Workflows > Configure REP Ring (Non-Fabric)**.
Alternatively, you can navigate to the **Inventory** Site topology view, select the device node on which you want to create the REP ring, and click **Create REP Ring** under the **REP Rings** tab.
- Step 2** If a task overview window appears, click **Let's Do It** to go directly to the workflow.
- Step 3** In the **Select a root device** window, select the root device.
Note The device must be in reachable state and have upstream connection.
- Step 4** In the **Select adjacent devices connected to root device** window, choose one adjacent device that is part of the ring and connected to the root device.
- Step 5** In the **Select adjacent devices connected to root device** window, choose other adjacent device that is part of the same ring and connected to the root device.
You need to choose two devices, part of the same ring and directly connected to the root device.
- Step 6** **Review** and **Edit** your root device, and the chosen adjacent devices.
- Step 7** To initiate the REP ring configuration, click **Provision**.
You can see a detailed status of the configuration progress on the **REP Ring Configuration Status** window.
- Step 8** The **REP Ring Summary** window displays the details of the REP ring that is created along with the discovered devices. After the creation of the REP ring, a success message is displayed.
- Step 9** To verify the creation of the REP ring, go to the **Inventory** window topology view and click any device that is part of the ring. In the slide-in pane, under the **REP Rings** tab, you can see the list of all REP rings that exist on that device.
Click a REP ring name in the list to view the REP ring details, such as the devices present in the ring, ports of each device that connect to the ring, and so on.
-

Add a Node to a REP Ring for Nonfabric Deployment

Use this procedure to add a node to an existing REP ring.



Note The feature supports the following platforms: IE2000, IE3200, IE3300, IE3400, IE3400H, IE4000, IE4010, IE5000, IE9300 and ESS3300.

Before you begin

Make sure you add the device to Cisco DNA Center. For information on how to add a device, see [Add or Edit a Device](#).

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

The device onboarded is shown in the **Plug and Play** window.

Step 2 From the **Actions** drop-down list, click **Claim**.

Step 3 In **Assign Site** window, click **Assign** to assign the device to a site and click **Next**.

Step 4 To deploy the configuration to the device, click **Assign** and click **Next**.

Note Plug and Play provisioning automatically deploys a device onboarding configuration template that corresponds to the type of device. For more information, see [Plug and Play Provisioning Overview](#).

Step 5 In the **Provision Templates** window, click **Preview Configuration** to review the configuration and click **Claim**.

Step 6 Click **Ok** and **Yes**.

A success message is displayed upon claiming the device.

Step 7 Click **Refresh**. The device onboarding process might take some time.

By default, the devices table gets refreshed every 30 seconds. Click the **Auto-Refresh** drop-down list and choose a refresh time.

On completion of the process, the device is moved to the **Provisioned** tab.

Step 8 Click the menu icon (☰) and choose **Provision > Inventory**.

Step 9 Click **Refresh** and wait until the device is in managed state.

Step 10 Use the toggle button (☰ | ☰ | 🏠) to switch between the Topology map view and the Inventory view. The change in the topology automatically triggers device rediscovery and the device is added to the REP.

Step 11 Click the REP and in the slide-in pane, click the **REP Rings** tab. The node insertion status is **Success** for successful addition of the device to the REP.

Step 12 In the REP Rings tab, click the **REP** link to view the steps executed. If any failure occurs, you can view the step at which the device insertion failed.

Step 13 (Optional) Under the **Actions** column, click the ellipsis to rediscover the failed node insertion.

Create Port Groups

You can 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 is displayed.

Step 3 In the **Tag Name** field, enter the tag name. In the **Description** field, add a description for the tag.


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. In the **Matching Ports** slide-in pane, 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**.
-

Port Usage Information

You can check the last input received and last output sent by the port.

- Step 1** Click the menu icon () and choose **Provision > Inventory**.
- Step 2** In the **Devices** table, click a device name, and then click **View Device Details**.
The device details are displayed in the window.
- Step 3** In the left pane, choose **Interfaces > Ethernet Ports**.
Note This tab is available for all devices except APs.
- Step 4** Click the port to view its details.
In the window, you can view the timestamp of **Last Input** received by the port and **Last Output** transmitted by the port.
-

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 the wireless controller is not in maintenance mode, you can select the APs individually and schedule them for maintenance.
- 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.
 - If the AP is in maintenance mode and is moving from a wireless controller which is not under maintenance mode to a wireless controller which is also not under maintenance, then the AP will retain its maintenance mode after moving.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Inventory**.
The **Inventory** window 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 is displayed.
- 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 > Inventory**.

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

The **Manage Maintenance** slide-in pane is displayed. 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 below 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.
- Step 4** Make the required changes in the device configuration by following the suggested actions.
-

Manage System Beacon

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

You can enable a system beacon on 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 > Inventory**.

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

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

Note

- You can enable beacons on up to five standalone devices at a time.
- To enable beacons on stacked devices, you must choose only one device at a time. In a stacked device, you can enable beacons 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 the **Enabled** radio button under **System Beacon State** and then click **Apply** to enable a beacon on the chosen devices.

After the system beacon is enabled, a blue beacon icon (📶) is displayed next to the device name in the inventory.

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

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

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

- a) Under **System Beacon State**, click the **Disabled** radio button.
- b) Click **Apply**.

Alternatively, in the **Inventory** window, hover the cursor over the blue beacon icon (📶) 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 20: Device Roles and Topology Positions

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



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

Before you begin

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

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

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

Step 2 To update the device role in the **Edit Device** slide-in pane:

- a) Select the device whose role you want to change.
- b) From the **Actions** drop-down list, choose **Inventory > Edit Device**.
- c) 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 > Inventory**.
The **Inventory** window 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** slide-in pane 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 > Inventory**.
- 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** slide-in pane, click **Resync Interval**.
- Step 5** Select the resync type.
- Note**
- To set the resync type as global, go to **System > Settings**.
 - 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** In the **Resync Interval (in Mins)** field, enter the time interval (in minutes) between successive polling cycles.

Step 7 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 > Inventory**.

The **Inventory** window 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 > 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**.

Note When you delete DNAC devices integrated with ISE, those deleted devices are moved to new NDG group in Cisco ISE.

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 > Inventory**.

The **Inventory** window 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 **More > 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 > Inventory**.

Step 2 From the **Actions** drop-down list, choose **More > 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 **Inventory** window 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** window 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** window 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** window 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.

Configuration Drift of a Device

Configuration changes made on devices are saved in the internal Cisco DNA Center server. For information on how to view the configuration drift, see [View Configuration Drift of a Device, on page 58](#).

Configuration drifts are captured when the following events occur:

- **First Time Collection:** On adding a device to Cisco DNA Center, device configuration is collected.
- **Syslog-Based Collection:** Cisco DNA Center monitors Syslog events sent by devices, and identifies the configuration changes. The configuration archive is triggered after 5 minutes, on occurrence of the latest event. Based on the login IP Address in Syslog events, configuration drifts are marked in-band (configuration changes done by Cisco DNA Center) or out-of-band (configuration changes done outside Cisco DNA Center).



Note New traps within the 5 minutes window will restart the timer to avoid multiple archives with partial changes. For accurate results, we recommend you to wait for at least 5 minutes.

- **Weekly Backup Collection:** Cisco DNA Center performs periodic weekly backup of device configurations. When no events are received for a device, the configuration changes made outside or from Cisco DNA Center are captured by the weekly backup archive. For more information, see [Configure Device Configuration Backup Settings in the Cisco DNA Center Administrator Guide](#).




Note Configuration drifts detected by weekly backup archive are classified as in-band (configuration changes done by Cisco DNA Center), even though it is possible that the configuration changes were done outside Cisco DNA Center.



Note Disk utilization is optimized by ignoring the collected archive when no changes are present. Disk space optimization is not applicable for the First Time Collection.

View Configuration Drift of a Device

-
- Step 1** Click the menu icon () and choose **Provision > Inventory**.
- Step 2** In the **Devices** table, click the device name, and more information about the device is displayed.
- Step 3** Click **View Device Details**.
The device details are displayed in the window.
- Step 4** In the left pane, click **Config Drift**.
The **Configuration Changes** window shows the number of configuration drifts saved, which includes labeled configs and config drift versions.
- Step 5** Expand the **Change History** tab to view the following details:
- 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.
 - 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, on page 59](#).
- 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 timeline graph for future reference.

- Step 1** Click the menu icon (☰) and choose **Provision > Inventory**.
- Step 2** Click the device name, and more information about the device is displayed.
- Step 3** Click **View Device Details**.
Device details are displayed in the window.
- Step 4** In the left pane, click **Config Drift**.
The **Configuration Changes** window is displayed.
- Step 5** Choose the config drift in timeline graph that you want to label. The timestamp of the chosen config drift is shown in the **Config Drift Version** below the timeline graph.
- Step 6** Click **Label Config** corresponding to the chosen config drift version.
- Step 7** 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 the config version name.
- Step 8** Click **Save**. The labeled config drift is shown in orange in the timeline 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 9** To remove the label, select the labeled config version and click **Remove label**.
-

Visibility of Configurations Workflow

The Visibility of Configurations feature provides a solution to further secure your planned network configurations before deploying them on to your devices. With enhanced visibility, you can enforce the previewing of device configurations (CLI and NETCONF commands) before deploying them.

Ensure that you opt for **Configuration Preview** on the **Visibility of Configurations** window. For more information on how to enable configuration preview, see the "Configure Visibility of Configurations" topic in the *Cisco DNA Center Administrator Guide*.



Note

- By default, the **Configuration Preview** is enabled for workflows that support configuration visibility.
- A workflow supports configuration visibility, if it displays the following banner message when you schedule the deployment of your task:

This workflow supports enhanced visibility into the generated configuration. The settings for this can be viewed and modified in **System > Settings > Configuration Visibility and Control**.
- If **Configuration Preview** is enabled, you must review your planned network configurations before deploying them. When you schedule the deployment of your configurations, the **Now** and **Later** options are dimmed (unavailable). You must first generate a configuration preview of your planned network configurations to review them.

When you generate a preview configuration, you can do one of the following on the **Preview Configuration** window:

- Click **Preview Configuration Later**, if you are not ready to deploy the configurations and would like to review them later on the **Activities > Work Items** window.
- Click **Discard**, if you want to discard the work item and return to the current activity.

If you discard this work item, you can't recover it later.



Note

If there is a conflicting operation when you deploy your planned network configurations, the **Pending Operations** dialog box is displayed. To proceed with the current deployment, you must either wait for the existing operation to complete or discard the other operations.

-
- Click **Deploy** when you are ready to submit the configurations for all the devices listed.

If there are multiple devices, you must click each device to preview its configuration. However, when you click **Deploy**, the configurations are pushed to all the devices.
 - If **Save Intent** displays instead of **Deploy**, the parameters that you chose during the workflow are already present on the device. To save those parameters to the database, click **Save Intent**. No configuration will be pushed to the device because the device already has the required configuration.

Replace a Faulty Device

The Return Material Authorization (RMA) workflow lets you replace failed devices quickly. 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. For Cisco Switch stacks (hardware stacking), you do not need to follow a separate procedure in Cisco DNA Center for member switch replacement, it is handled by the active switch. The member switch is replaced by the active switch by providing software image and configuration. Full stack replacement is handled by Cisco DNA Center.



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.
- For switch stacks replacement, the number of stacks for faulty and replacement device should be same.

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

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

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

- d) From the **Inventory** drop-down list, choose **Marked for Replacement**.

A list of devices marked for replacement is displayed.

e) (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 the Inventory or the 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, choose whether you want to start the device replacement immediately (if yes, click **Now**) or schedule it for later.

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.

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

h) To make changes, click **Edit**.

i) Click **Monitor Replacement Status** to go to the **Mark for Replacement** view in the **Provision** window.

j) Click **Replace Status** to view the status of the RMA workflow progress, as follows:

- Running readiness checks for device replacement.
- 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**.

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

The main inventory window displays the details of the new replacement device.

Note 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 > Inventory**.
The **Inventory** window 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 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 (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 the 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 extended node and AP in fabric.)
- Make sure that the replacement device is connected to the same port to which the faulty device was connected.
- 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.
- 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 when*:
 - The faulty device is connected to an uplink device using multiple interfaces.
 - LAN automation uses overlapping pools.
- If the replacement device onboards through the 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 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 > 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, choose whether you want to reboot the AP **Now** or schedule it for later.
- 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 the task of rebooting the selected APs, a message saying *Reboot Initiated Successfully* is displayed.

- Step 7** In the **Task Submitted** dialog box, click the **Task** link.
- This dialog box displays for a few seconds and then disappears. To navigate to the task, click the menu icon () and choose **Activities > Tasks**.
- Step 8** Click the task name to view the reboot initiation status.
-