



# Managing Devices and Hosts

- [Managing Your Device Inventory, page 1](#)
- [Managing Your Host Inventory, page 30](#)

## Managing Your Device Inventory

The **Device Inventory** window displays the results of the discovery scan. To access the **Discovery** window, from the **Navigation** pane, click **Device Inventory**.

Figure 1: Device Inventory Window

Device Name	IP Address	Reachability Status	Up Time	Last Updated Time	Poller Time	Last Inventory Collection Status
SDN-DEV-2969-BR4.cisco.com	10.10.10.10	Reachable	9 days, 18:36:36.81	a few seconds ago	00:25:00	ERROR-ENABLE-PASSWORD ⓘ
SDN-DEV-3659-BR4	10.10.10.11	Reachable	9 days, 18:35:15.72	a few seconds ago	00:25:00	ERROR-ENABLE-PASSWORD ⓘ
SDN-DEV-4332-1-CA2.cisco.com	10.10.10.12	Reachable	9 days, 18:37:19.58	a minute ago	00:25:00	ERROR-ENABLE-PASSWORD ⓘ
SDN-DEV-4506-CA2	10.10.10.13	Reachable	9 days, 18:35:52.88	a minute ago	00:25:00	ERROR-ENABLE-PASSWORD ⓘ
SDN-DEV-5176-CA2	10.10.10.14	Reachable	102 days, 0:26:42.43	a few seconds ago	00:25:00	Managed

10 ▾ 5 Devices First Previous 1 Next Last



**Note**

The information that is displayed depends on the **Layout** that you selected.

After the initial discovery, network devices are polled every 30 minutes. Polling occurs for each device, link, host, and interface. Only devices that have been active for less than a day are displayed. This prevents any stale device data from being displayed. On average, polling 500 devices takes approximately 20 minutes.

For information about the actions that you can perform from the **Device Inventory** window, see [Device Inventory Tasks](#), on page 8.

The following table describes the main elements in the **Device Inventory** table.

Window Element	Description
Device Selection check boxes	Allows you to select devices to perform tasks.  When you select a device, the action buttons appear above the <b>Device Inventory</b> table. For information about these buttons and the actions that you can perform with them, see <a href="#">Device Inventory Tasks</a> , on page 8.
<b>Filters</b>	Allows you to refine the list of devices that are displayed in the table by name, location tag, and IP address.  To remove filters, click <b>Clear Filters</b> .
<b>Layout</b>	Allows you to choose from three predefined layouts or a customized layout: <ul style="list-style-type: none"> <li>• <b>Status</b>—Layout shows the device name, IP address, state of the device, how long it has been up, and the last time it was updated.</li> <li>• <b>Hardware</b>—Layout shows the device name, IP address, device family, platform, serial number, MAC address, and role, along with its IOS/firmware version and a link to its configuration file.</li> <li>• <b>Tagging</b>—Layout shows the device name, IP address, MAC address, device role, location, and tags.</li> <li>• <b>Customize</b>—Layout shows the information in the columns that you have selected to display.</li> </ul> <p>For descriptions of the columns of information that you can display, see the Device Inventory Information table below.</p>

Below the **Device Inventory** table, you can adjust the number of devices displayed in the table (10, 25, 50, 100), and you can click **First**, **Previous**, **Next**, **Last**, or the page number to navigate through the table.

## Device Inventory Information

The **Device Inventory** table displays the following information for each discovered device. All of the columns, except the **Config** column, support sorting. Clicking on the column header sorts the rows in an ascending order. Clicking on the column header again sorts the rows in descending order.

For more information, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

**Table 1: Device Inventory Information**

Column Name	Description
Device Status	<p>State of the device.</p> <ul style="list-style-type: none"><li>• <b>Connecting</b>—Controller is connecting to the device.</li><li>• <b>Reachable:</b><ul style="list-style-type: none"><li>◦ <b>Discovered</b>—Controller has connected to the device and is able to execute Cisco commands using the CLI .</li><li>◦ <b>Failure</b>—Controller has connected to the device, but is unable to execute Cisco commands using the CLI. This status usually indicates that the device is not a Cisco device.</li></ul></li><li>• <b>Authentication Failed</b>—Controller has connected to the device but is unable to determine what type of device it is. This device status also usually indicates that the device is not a Cisco device.</li><li>• <b>Unreachable</b>—Controller is unable to connect to the device.</li></ul> <p><b>Note</b> If credentials are not provided at the time a discovery request is made or earlier, then the device status could be displayed as "Not reachable." You need to perform a new discovery with the correct credentials.</p>

Column Name	Description
Device Name	<p>Name of the device. Click the device name to display the <b>Device Overview</b> dialog box with the following information:</p> <ul style="list-style-type: none"> <li>• Device serial number</li> <li>• Device IP address</li> <li>• MAC address</li> <li>• Cisco OS version</li> <li>• Up time</li> <li>• Product ID</li> <li>• Vendor</li> <li>• Memory size</li> </ul> <p><b>Note</b> The device name appears red for any device whose inventory has not been updated for more than 30 minutes.</p> <p>The <b>Device Overview</b> dialog box also includes an <b>Interfaces</b> tab with the following interface data:</p> <ul style="list-style-type: none"> <li>• Status—Up or down</li> <li>• Interface name—Name of the interface.</li> <li>• MAC address—MAC address of the interface.</li> </ul>
MAC Address	MAC address of the device.
IP Address	IP address of the device.
IOS/Firmware	Cisco IOS software currently running on the device.
Platform	Cisco product part number.
Serial Number	Cisco device serial number.
Up Time	Period of time that the device has been up and running.
Config	<p>Click <b>View</b> to display detailed configuration information similar to the CLI <b>show running-config</b> command output.</p> <p><b>Note</b> This feature is not supported for access points and wireless LAN controllers, therefore configuration data is not returned for these device types.</p>

Column Name	Description
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 the controller is unable to determine a device role, it sets the device role as unknown.</p> <p><b>Note</b> The controller can change the device role as the network topology changes, but if you manually change the device role, then the role will not change as the network topology changes.</p> <p>If desired, you can use the drop-down list in this column to change the assigned device role. The following device roles are available:</p> <ul style="list-style-type: none"><li>• Unknown</li><li>• Access</li><li>• Core</li><li>• Distribution</li><li>• Border Router</li></ul>

Column Name	Description
<b>Location</b>	<p>Tag that you can apply to a device to denote its geographic location. By applying the same tag to several devices, you can group them based on a common attribute. The <b>Device Inventory</b> window and <b>Topology</b> window support location tags.</p> <p>Use the following guidelines when creating location tags:</p> <ul style="list-style-type: none"> <li>• Location tag information is maintained on the controller only and not deployed to or derived from the device itself.</li> <li>• A location defined on the controller is not the "civic-location" property that some devices support.</li> <li>• You cannot create, use, or search for location tags in the <b>Topology</b> window.</li> <li>• Location tags cannot be attached to hosts.</li> <li>• You can apply only one location tag to a device. However, you can use both a location tag and a device tag together.</li> </ul> <p>For information about adding location tags, see <a href="#">Adding or Removing Location Tags</a>, on page 19.</p> <p>Along with the location tag, you can add a geographical marker on a world map to a device. For information, see <a href="#">Adding or Changing a Location Marker</a>, on page 21.</p>
<b>Device Tag</b>	<p>Tag assigned to devices to identify them by a common attribute. For example, you can create a tag and use it to group devices based on a platform ID or Cisco IOS release.</p> <p>A number in the <b>Tag</b> column indicates how many tags have been applied to that device.</p> <p><b>Note</b> You are permitted to use both a location tag and a device tag together.</p> <p>For information about adding or removing device tags, see <a href="#">Adding or Removing a Device Tag in Device Inventory</a>, on page 17.</p> <p>For information about deleting a tag from the controller database, see <a href="#">Deleting a Tag</a>, on page 22.</p>

Column Name	Description
<b>Policy Tag</b>	<p>Tag applied to a group of devices that will share the same policy.</p> <p>After applying a policy tag, you need to configure the policies that will be applied to the devices with the same policy tag. For information about configuring QoS policies, see the <i>Cisco EasyQoS Application for APIC-EM User Guide</i>.</p>
<b>Last Updated Time</b>	Date and time that the device was last scanned and the controller database was updated.
<b>Device Family</b>	<p>Group of related devices, as follows:</p> <ul style="list-style-type: none"> <li>• Cisco Interfaces and Modules</li> <li>• Routers</li> <li>• Switches and Hubs</li> <li>• Third Party Device</li> <li>• Unsupported Cisco Device</li> <li>• Wireless Controller</li> </ul>
<b>Device Series</b>	Series number of the device, for example, Cisco Catalyst 4500 Series Switches.
<b>Last Inventory Collection Status</b>	<p>Status of the last discovery scan for the device:</p> <ul style="list-style-type: none"> <li>• <b>Managed</b>—Device is in a fully managed state.</li> <li>• <b>Partial Collection Failure</b>—Device is in a partial collected state and not all the inventory information has been collected. Move the cursor over the <b>Information</b> (i) icon to display additional information about the failure.</li> <li>• <b>Unreachable</b>—Due to device connectivity issues, the device could not be reached and no inventory information was collected. This condition can occur when periodic collection happens.</li> <li>• <b>Wrong Credentials</b>—If the device credentials are changed after adding the device to the inventory, this condition is noted.</li> <li>• <b>In Progress</b>—Inventory collection is occurring.</li> </ul>

## Device Inventory Tasks

The actions that you can perform from the **Device Inventory** window depend on the layout that you choose. When you select one or more devices, you can click any of the following buttons to perform the corresponding action.

**Table 2: Device Inventory Buttons**

Button	Action
<b>Add Device</b>	Allows you to discover a specific device and add it to your inventory. If authentication of the device fails due to invalid credentials, the device enters the collection failure state. For information, see <a href="#">Adding a Device Manually</a> , on page 9.
<b>Set Location</b>	Sets the location of the devices associated with a location tag on a geographical map. For information, see <a href="#">Adding or Changing a Location Marker</a> , on page 21.
<b>Set Device Tags</b>	Groups devices according to common attributes. For information, see <a href="#">Adding or Removing a Device Tag in Device Inventory</a> , on page 17.
<b>Set Policy Tag</b>	Groups devices so that you can deploy the same QoS policy to those devices at the same time. For information, see <a href="#">Adding or Removing a Policy Tag in Device Inventory</a> , on page 18.
<b>Delete</b>	Deletes the selected devices from inventory. For information, see <a href="#">Deleting a Device</a> , on page 12.
<b>Update Credentials</b>	Changes the credentials of the selected devices. In future discoveries, these credentials are used for the selected devices instead of the global or discovery job-specific credentials. For information, see <a href="#">Updating Device Credentials</a> , on page 24.
<b>Update Polling Interval</b>	You can update the polling interval of selected devices. These device-specific settings override the global and job-specific settings for the selected devices. For information, see <a href="#">Updating a Device's Polling Interval</a> , on page 28.
<b>Resync (Resynchronize Devices)</b>	Immediately polls the selected device for updated device information and status. For information, see <a href="#">Resynchronizing Device Information</a> , on page 27.



Button	Action
Command Runner	Sends CLI commands to the selected devices using API commands. Currently, <b>show</b> and other read-only commands are permitted. For information, see <a href="#">Running Commands on Devices</a> , on page 28.

## Adding a Device Manually

You can manually add a device to your inventory.

**Figure 2: Add Device Dialog box**

**Add Device**

\* Device IP

▼ SNMP

\* Version

\* Read Community

Write Community

▶ SNMP RETRIES AND TIMEOUT

▶ CLI

**i** Please make sure the authenticity of credentials, in case of invalid credentials device will go in collection failure state.

**Add** **Cancel**

### Before You Begin

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

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

- Step 1** From the **Navigation** pane, click **Device Inventory**.
- Step 2** Click **Add Device**.
- Step 3** From the **Add Device** dialog box, enter the device's IP address in the **Device IP** field.
- Step 4** In the **Version** field, choose the SNMP version from the drop-down list: **V2C** or **V3** and complete the corresponding fields:

**Table 3: SNMP V2C Fields**

Field	Description
<b>Read Community</b>	Read-Only community string value configured on devices that allows the controller to connect to and access the devices. This community string value must match the community string value that was pre-configured on the devices.
<b>Write Community</b>	Write community string value configured on devices that allows the controller to connect to, access, and change the devices. This community string value must match the community string value pre-configured on the devices.

**Table 4: SNMP V3 Fields**

Field	Description
<b>Mode</b>	Authentication mode to be used. Valid modes are <b>Authentication and Privacy</b> , <b>Authentication, No Privacy</b> , <b>No Authentication, No Privacy</b> .
<b>Auth. Type</b>	Valid only if you chose <b>Authentication and Privacy</b> or <b>Authentication, No Privacy</b> . Two authentication types are available: <ul style="list-style-type: none"> <li>• <b>SHA</b>—Authentication based on the Secure Hash algorithm (SHA). SHA is a hash algorithm that is used to authenticate packet data.</li> <li>• <b>MD5</b>—Authentication based on the Message Digest 5 (MD5) algorithm. MD5 is a hash algorithm that is used to authenticate packet data.</li> </ul>
<b>Username</b>	Valid only if you chose <b>SHA</b> or <b>MD5</b> . Text string associated with the SNMP user and the chosen authentication type (SHA or MD5).

Field	Description
<b>Auth. Password</b>	Valid only if you chose <b>SHA</b> or <b>MD5</b> . Encrypted text string stored as the SNMP user password and associated with the authentication type (SHA or MD5).
<b>Privacy Type</b>	Valid only if you chose <b>Authentication and Privacy</b> mode. Two privacy types are available: <ul style="list-style-type: none"> <li>• <b>DES</b>—Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.</li> <li>• <b>AES128</b>—Cipher Block Chaining (CBC) mode AES for encryption.</li> </ul>
<b>Privacy Password</b>	SNMPv3 privacy password associated with the chosen privacy type (DES or AES128) and used to generate the secret key to encrypt messages that are exchanged with devices.

**Step 5** Expand the **SNMP RETRIES AND TIMEOUT** area, if it is not already expanded, and complete the following fields:

**Table 5: SNMP Retries and Timeout Fields**

Field	Description
<b>Retries</b>	Number of attempts the controller makes to communicate with the devices using SNMP. The default is 3 tries.
<b>Timeout</b>	Number of seconds the controller waits while attempting to communicate with the devices using SNMP before the attempt fails. The default is 5 seconds.

**Step 6** Expand the **CLI** area, if it is not already expanded, and complete the following fields:

**Table 6: CLI Fields**

Field	Description
<b>Protocol</b>	Protocol used from a remote management station to connect device CLI. Valid options are <b>Telnet</b> (Telnet TCP/IP) or <b>SSH2</b> (Secure Shell 2.0).
<b>Username</b>	Identification used to log into a device's CLI.
<b>Password</b>	Password used to log into a device's CLI.

Field	Description
Enable Password	After successful login to the CLI, password used to access Privileged EXEC mode.

**Step 7** Click **Add**.

---

## Deleting a Device

You can delete devices from the Cisco APIC-EM database.

### Before You Begin

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

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

---

**Step 1** From the **Navigation** pane, click **Device Inventory**.

**Step 2** Click the check box next to the device that you want to delete.  
A toolbar opens.

**Note** Even after the toolbar opens, you can select multiple devices by clicking additional check boxes, or you can select all devices by clicking the checkbox at the top of the list.

**Step 3** From the open toolbar, click **Delete**.

---

## Filtering Devices in the Device Inventory Window

You can filter the devices displayed in the **Devices Inventory** window by device name, location, IP address and VRF instance.



**Note** To remove the filters, click **Clear Filters**.

**Figure 3: Device Inventory Window Showing Filters**

The screenshot shows the Cisco APIC Enterprise Module interface. On the left, there is a sidebar with a 'Filters' section containing four filter fields: 'DEVICE NAME', 'DEVICE LOCATION', 'DEVICE IP ADDRESS', and 'DEVICE VRF'. Each field has a search box and a plus icon. The main area displays a table of devices with columns: Device Name, IP Address, Reachability Status, Up Time, Last Updated Time, Poller Time, and Last Inventory Collection Status. The table lists five devices, all with a 'Reachable' status. At the bottom right, there are pagination controls showing '5 Devices' and 'First Previous 1 Next Last'.

Device Name	IP Address	Reachability Status	Up Time	Last Updated Time	Poller Time	Last Inventory Collection Status
SDN-DEV-2960-BR4-cisco.com	10.10.10.1	Reachable	9 days, 18:36:36.81	a few seconds ago	00:25:00	ERROR-ENABLE-PASSWORD
SDN-DEV-3650-BR4	10.10.10.2	Reachable	9 days, 18:35:15.72	a few seconds ago	00:25:00	ERROR-ENABLE-PASSWORD
SDN-DEV-4332-1-CA2-cisco.com	10.10.10.3	Reachable	9 days, 18:37:19.58	a minute ago	00:25:00	ERROR-ENABLE-PASSWORD
SDN-DEV-4506-CA2	10.10.10.4	Reachable	9 days, 18:35:52.88	a minute ago	00:25:00	ERROR-ENABLE-PASSWORD
SDN-DEV-N7K-CA2	10.10.10.5	Reachable	102 days, 0:26:42.43	a few seconds ago	00:25:00	Managed

### Before You Begin

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

**Step 1** From the **Device Inventory** toolbar, click **Filters**.  
The following filters display:

- **Device Name**
- **Device Location**
- **Device IP Address**
- **Device VRF**

**Step 2** Enter the appropriate value in the selected filter field.  
For example, for the **Device Name** filter, enter the name of a device.

The controller presents you with auto-complete values as you enter values in the other fields. Choose one of the suggested values or finish entering the desired value.

**Note** You can also use a wildcard (asterisk) with these filters. You can enter values with the asterisk at the beginning, end, or in the middle of the string value.

**Step 3** Click the plus (+) icon to perform the filter.  
The data displayed in the **Devices** table automatically updates according to your filter selection.

**Step 4** (Optional) If needed, add more filters following the above steps.

**Note** You can filter on more than one value per filter or across several different filter types.

**Step 5** To remove the filter, click the **x** icon next to the filter value.

### What to Do Next

Review the updated information displayed in the **Device Inventory** window. If required for your network configuration, make changes to the displayed columns within the **Devices** table view.

## Changing the Devices Layout View

You can change the information that is displayed in the **Devices** table by selecting different layout views or by customizing a layout view for the devices in your network.

**Figure 4: Device Inventory Window Showing Layout Options**

DEVICE NAME	DEVICE LOCATION	DEVICE IP ADDRESS	DEVICE VRF	Status	IP Address	Reachability Status	Up Time	Last Updated Time	Poller Time	Last Inventory Collection Status
SDN-DEV-3650-BR4	SDN-DEV-3650-BR4	SDN-DEV-4332-1-CA2.cisco.com	SDN-DEV-4506-CA2	Reachable	10.10.10.10	Reachable	9 days, 18:36:36.81	a few seconds ago	00:25:00	ERROR-ENABLE-PASSWORD
SDN-DEV-3650-BR4	SDN-DEV-3650-BR4	SDN-DEV-4332-1-CA2.cisco.com	SDN-DEV-4506-CA2	Reachable	10.10.10.10	Reachable	9 days, 18:35:15.72	a few seconds ago	00:25:00	ERROR-ENABLE-PASSWORD
SDN-DEV-3650-BR4	SDN-DEV-3650-BR4	SDN-DEV-4332-1-CA2.cisco.com	SDN-DEV-4506-CA2	Reachable	10.10.10.10	Reachable	9 days, 18:37:19.58	a minute ago	00:25:00	ERROR-ENABLE-PASSWORD
SDN-DEV-3650-BR4	SDN-DEV-3650-BR4	SDN-DEV-4332-1-CA2.cisco.com	SDN-DEV-4506-CA2	Reachable	10.10.10.10	Reachable	9 days, 18:35:52.88	a minute ago	00:25:00	ERROR-ENABLE-PASSWORD
SDN-DEV-3650-BR4	SDN-DEV-3650-BR4	SDN-DEV-4332-1-CA2.cisco.com	SDN-DEV-4506-CA2	Reachable	10.10.10.10	Reachable	102 days, 0:26:42.43	a few seconds ago	00:25:00	Managed

### Before You Begin

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

**Step 1** From the **Device Inventory** toolbar, click the **Layout** field and choose one of the following layout options from the drop-down list:

- **Status**—Displays general device status information, including up time, update frequency, and number of updates.

- **Hardware**—Displays hardware information, including IOS/firmware, serial number, and device role.
- **Tagging**—Displays tagging information, including device role, location, and tag.
- **Customize**—Displays a list of options to choose from to create your own layout.

APIC-EM displays the information for the chosen layout.

**Step 2**

To customize a specific layout, choose **Customize** and select the desired display options. Display options toggle on and off. Blue options with checkmarks indicate that the option is on and is displayed in the table.

---

**What to Do Next**

Review the updated information displayed in the **Device Inventory** window. If required for your network configuration, make any adjustments.

## Changing the Device Role

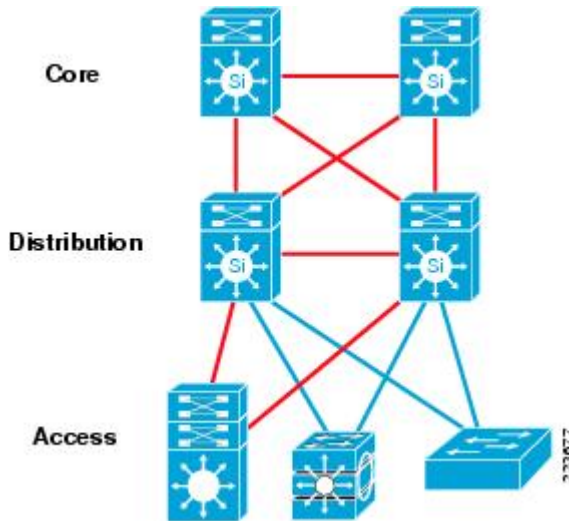
During the scan process, the controller assigns a role to each discovered device. The device role is used to identify and group devices according to their responsibilities and placement in the network.

A device can have one of the following roles:

- **Unknown**—Device role is unknown.
- **Access**—Device is located in and performs tasks required of the access layer or first tier/edge of the network.
- **Border Router**—Device performs tasks required of a border router.
- **Distribution**—Device is located in and performs tasks required of the distribution layer of the network.

- **Core**—Device is located in and performs tasks required of the core of the network.

**Figure 5: Device Roles and Network Locations**



You can change the device role in the **Device Inventory** window.



**Note** You can also change the device role from the **Topology** window. See [Changing a Device's Role From the Topology Window](#).

### Before You Begin

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

You must have either administrator (ROLE\_ADMIN) or policy administrator (ROLE\_POLICY\_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

- 
- Step 1** From the **Navigation** pane, click **Device Inventory**.  
The **Devices Inventory** window appears.
- Step 2** From the **Device Inventory** toolbar, choose one of the options from the **Layout** drop-down list.  
Valid options are **Hardware**, **Tagging**, or **Customize > Device Role**. The table refreshes and includes a column for the **Device Role**.
- Step 3** Locate the device you want to change and choose a new role from the drop-down list in the **Device Role** column.  
Valid choices are **Unknown**, **Access**, **Core**, **Distribution**, or **Border Router**.
- 

### What to Do Next

If required, change the role of other devices in the **Device Inventory** window.



## Adding or Removing a Device Tag in Device Inventory

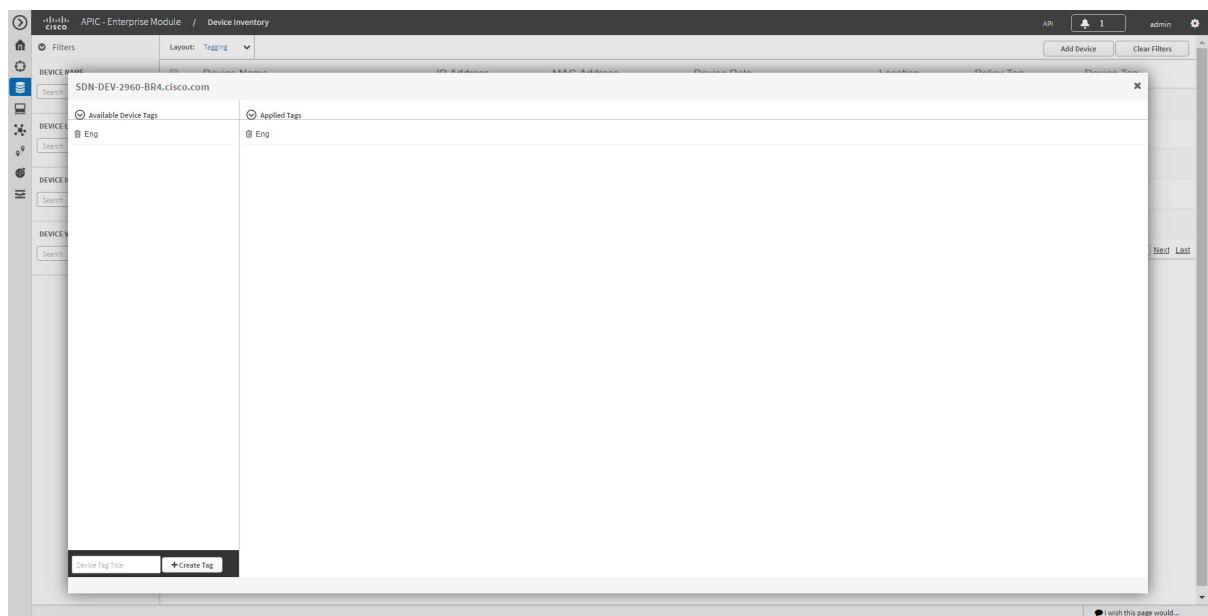
You can group devices according to common attributes by applying device tags. For example, you may want to apply device tags to group devices by their platform ID or Cisco IOS release. A single device can have multiple device tags; similarly, a single device tag can be applied to multiple devices.



### Note

For information about Policy tags and Location tags, see [Adding or Removing a Policy Tag in Device Inventory](#), on page 18 and [Adding or Removing Location Tags](#), on page 19.

**Figure 6: Device Tags Dialog Box**



### Before You Begin

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

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

- 
- Step 1** From the **Navigation** pane, click **Device Inventory**.
  - Step 2** From the **Device Inventory** toolbar, choose **Layout > Tagging** from the drop-down list. The table refreshes and displays a **Device Tag** column in addition to other columns.
  - Step 3** Select the check box to the left of the desired devices and click **Set Device Tags**.  
**Note** For a single device, you can also click the number displayed in the **Device Tag** column.
  - Step 4** Do one of the following:

- To apply a device tag, from the **Available Tags** list, click the tags that you want to apply to the selected devices.

**Note** If the desired tag is not in the list, enter a name for the tag and click **+New Tag**.

- To remove a device tag, from the **Applied Tags** list, click the **Trash can** icon next to the tag that you want to remove from the selected devices.

**Note** The **Applied Tags** list is populated only if at least one of the selected devices has a tag applied to it.

**Step 5** Click **x** to close the dialog box.

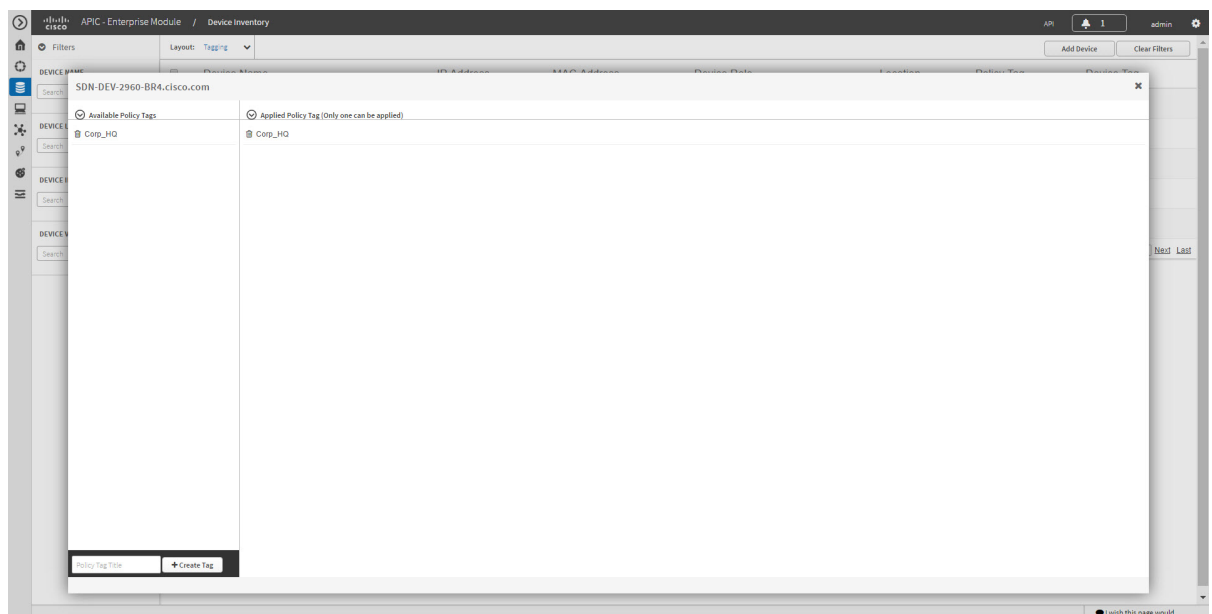
### What to Do Next

If required for your network configuration, add location or policy tags to your devices.

## Adding or Removing a Policy Tag in Device Inventory

You can apply a policy tag applied to a group of devices so that you can deploy the same QoS policy to those devices at the same time.

**Figure 7: Policy Tag Dialog Box**



### Before You Begin

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

## SUMMARY STEPS

1. From the **Navigation** pane, click **Device Inventory**.
2. From the **Device Inventory** toolbar, choose **Layout > Tagging** from the drop-down list.
3. Select the check box to the left of the desired devices and click **Set Policy Tag**.
4. Do one of the following:
5. Click **x** to close the dialog box.

## DETAILED STEPS

- 
- Step 1** From the **Navigation** pane, click **Device Inventory**.
- Step 2** From the **Device Inventory** toolbar, choose **Layout > Tagging** from the drop-down list. The table refreshes and displays a **Policy Tag** column in addition to other columns.
- Step 3** Select the check box to the left of the desired devices and click **Set Policy Tag**.  
**Note** For a single device, you can also click **Add** displayed in the **Policy Tag** column.
- Step 4** Do one of the following:
- To apply a policy tag, from the **Available Tags** list, click the tag that you want to apply to the selected devices.
- Note** If the desired tag is not in the list, enter a name for the tag and click **+New Tag**.
- To remove a policy tag, from the **Applied Tags** list, click the **Trash can** icon next to the tag that you want to remove from the selected devices.
- Note** The **Applied Tags** list is populated only if at least one of the selected devices has a tag applied to it.
- Step 5** Click **x** to close the dialog box.
- 

### What to Do Next

If you added a policy tag to devices and now want to configure QoS policies, see the *Cisco EasyQoS Application for APIC-EM User Guide*.

## Adding or Removing Location Tags

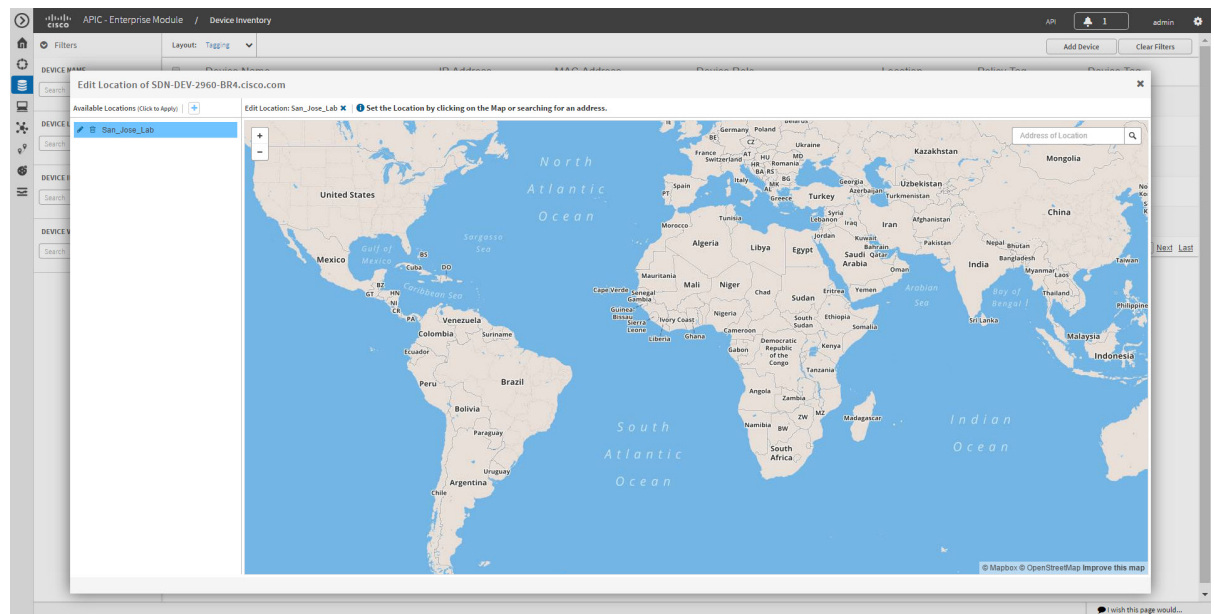
You can apply a location tag to a device to name a device's geographic location. By applying the same tag to several devices, you can group them based on their common location. You can create a location tag and, optionally, place a corresponding location marker on a geographical map. For information, see [Adding or Changing a Location Marker](#), on page 21.

Use the following guidelines when adding location tags:

- Location tag information is maintained on the controller only and not deployed to or derived from the device itself.
- When location tags and markers are used, the **Topology** window displays them on a geographical map.

- A location defined on the controller is not the "civic-location" property that some devices support.
- Location tags cannot be attached to hosts.
- You can apply only one location tag to a device. However, you can use both a location tag and a device tag together.

**Figure 8: Set Location Tag Dialog Box**



### 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** From the **Navigation** pane, click **Device Inventory**.
- Step 2** From the **Device Inventory** toolbar, choose **Layout > Tagging** from the drop-down list. The table refreshes and displays a **Location** column in addition to other columns.
- Step 3** Select the check box to the left of the desired devices (or select the check box at the top of the list to select all devices) and click **Set Location**.
- Note** For a single device, you can also click the **Add** link displayed in the **Location** column for that device.
- Step 4** Do one of the following:
- To apply a location tag, from the **Available Tags** list, click the tag that you want to apply to the selected devices. If the desired tag is not in the list, click the plus icon (+), enter a name for the tag, and click the check mark icon.
  - To remove a location tag assignment from the devices, in the **Edit Location** field, click the **x** icon. The devices now have no location tag assignment.
  - To change the current location tag to another one, click the new location tag that you want to assign.

- To delete the location tag, first make sure that it is not in use (either change device assignments to other location tags or remove the tag assignment altogether). Then, click the trash can icon next to the location tag that you want to delete.

**Step 5** When you are done, click **x** to close the dialog box.

---

### What to Do Next

If required for your network configuration, add or remove other location tags to other devices or add location markers.

### Related Topics

[Adding or Changing a Location Marker, on page 21](#)

## Adding or Changing a Location Marker

A location marker is an icon used to indicate the location of the devices associated with a location tag on a geographical map. You can add a location marker to devices in the **Device Inventory** window.

### Before You Begin

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

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

You have already added location tags to your devices.

---

**Step 1** From the **Navigation** pane, click **Device Inventory**.

**Step 2** From the **Device Inventory** toolbar, choose **Layout > Tagging** from the drop-down list. The table refreshes and displays a **Location** column in addition to other columns.

**Step 3** (Optional) To display devices with a specific location tag, from the **Device Inventory** toolbar, click **Filters**, enter a location tag in the **Device Location** field, and click the + icon.

**Step 4** Select the desired location tag from the **Locations** column.

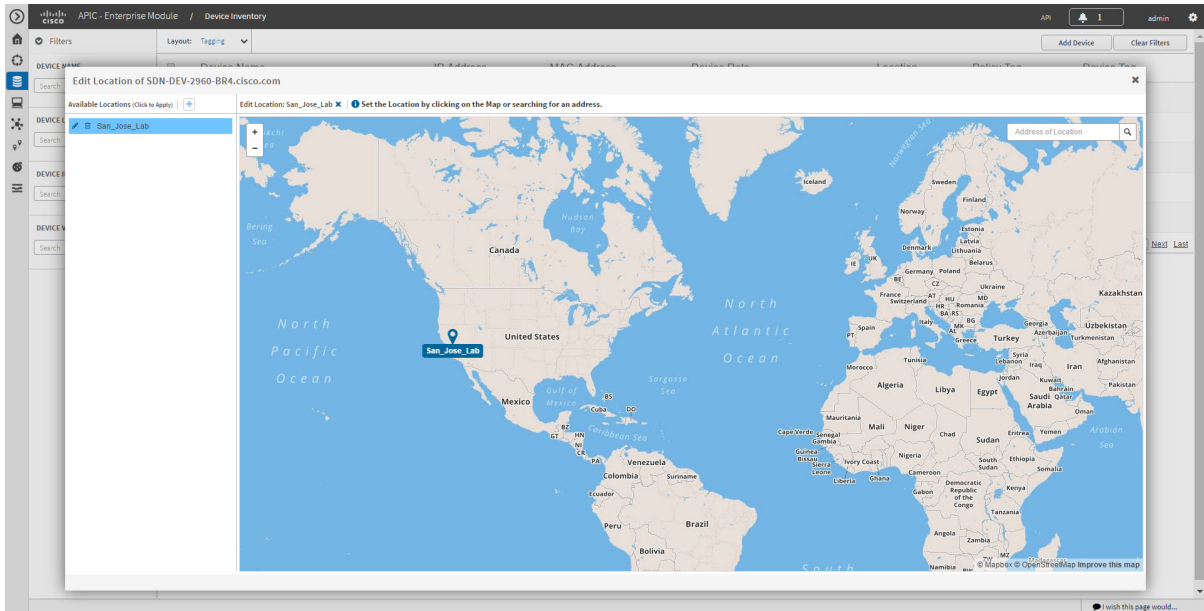
**Note** Because you are not assigning a location tag, it is not important which device you choose. When you add or remove a location marker, the change is applied to the location tag, and all devices that have the location tag will be updated.

**Step 5** To add or change a location marker, select the location tag from the **Available Locations** pane and do one of the following:

- In the **Address of Location** field on the right side of the geographical map, enter the address where you want to place the location marker. You can enter a complete address or part of an address, for example, a city name or zip code. Cisco APIC-EM displays the location on the map. Click the map where you want the marker to be placed and confirm the action in the confirmation dialog box that appears.
- Position the map as close to the desired location as possible using your mouse to drag and drop, zoom in, and zoom out on the map, then click the map.

**Note** If you need to reposition the marker, click the map again where you want the marker to be placed.

**Figure 9: Edit Location Dialog Box Showing Location Marker**



**Step 6** (Optional) To add additional location markers, click another location tag and repeat Step 5.

**Step 7** When you are done, click **x** to close the dialog box.

## Deleting a Tag

When a device tag, policy tag, or location tag is no longer needed, you can delete it, and it is removed permanently from the controller. You can delete device tags using the **Device Inventory** window or the **Topology** window. Policy tags and location tags can be deleted only from the **Device Inventory** window. This procedure shows you how to delete tags from the **Device Inventory** window.

### Before You Begin

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

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

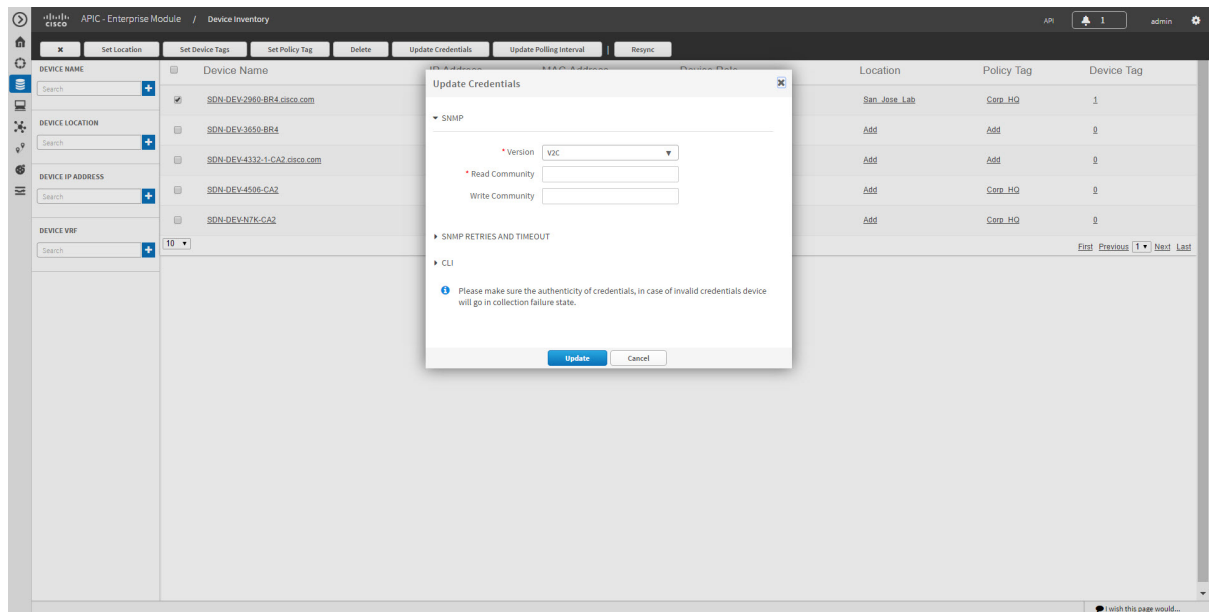
Before you can delete a tag, you need to remove it from all devices that have been assigned the tag.

- 
- Step 1** From the **Navigation** pane, click **Device Inventory**.
- Step 2** From the **Device Inventory** toolbar, choose **Layout > Tagging** from the drop-down list.
- Step 3** Do one of the following:
- To delete a device tag, click any number in the **Device Tag** column. From the **Available Tags** list, click the **Trash can** icon next to the tag or tags that you want to delete.
  - To delete a policy tag, click **Add** or the name of a policy tag in the **Policy Tag** column. From the **Available Tags** list, click the **Trash can** icon next to the tag or tags that you want to delete.
  - To delete a location tag, click **Add** or the name of a location tag in the **Location** column. From the **Available Locations** list, click the **Trash can** icon next to the tag or tags that you want to delete.
- Step 4** Click **OK** to confirm the deletion.  
The tag is removed permanently from the controller.  
If the deletion fails, the tag might still be assigned to devices. Remove the tag from these devices and try to delete the tag again.
- Step 5** Click **x** to close the dialog box.
-

## Updating Device Credentials

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

**Figure 10: Update Device Credentials Dialog Box**



### Before You Begin

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

You must have either administrator (ROLE\_ADMIN) or policy administrator (ROLE\_POLICY\_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

- 
- Step 1** From the **Navigation** pane, click **Device Inventory**.
  - Step 2** Select the devices that you want to update.
  - Step 3** Click **Update Credentials**.
  - Step 4** Click **OK** to confirm this action.
  - Step 5** From the **Update Credentials** dialog box, expand the **SNMP** area, if it is not already expanded.
  - Step 6** In the **Version** field, choose the SNMP version from the drop-down list: **V2C** or **V3** and complete the corresponding fields:
- Note** Both the SNMP and CLI credentials are updated together, so you need to provide both credentials. If you provide only SNMP credentials, Cisco APIC-EM saves only the SNMP credentials. The CLI credentials are not updated.



Table 7: SNMP V2C Fields

Field	Description
<b>Read Community</b>	Read-Only community string value configured on devices that allows the controller to connect to and access the devices. This community string value must match the community string value that was pre-configured on the devices.
<b>Write Community</b>	Write community string value configured on devices that allows the controller to connect to, access, and change the devices. This community string value must match the community string value pre-configured on the devices.

Table 8: SNMP V3 Fields

Field	Description
<b>Mode</b>	Authentication mode to be used. Valid modes are <b>Authentication and Privacy</b> , <b>Authentication, No Privacy</b> , <b>No Authentication, No Privacy</b> .
<b>Auth. Type</b>	Valid only if you chose <b>Authentication and Privacy</b> or <b>Authentication, No Privacy</b> . Two authentication types are available: <ul style="list-style-type: none"> <li>• <b>SHA</b>—Authentication based on the Secure Hash algorithm (SHA). SHA is a hash algorithm that is used to authenticate packet data.</li> <li>• <b>MD5</b>—Authentication based on the Message Digest 5 (MD5) algorithm. MD5 is a hash algorithm that is used to authenticate packet data.</li> </ul>
<b>Username</b>	Valid only if you chose <b>SHA</b> or <b>MD5</b> . Text string associated with the SNMP user and the chosen authentication type (SHA or MD5).
<b>Auth. Password</b>	Valid only if you chose <b>SHA</b> or <b>MD5</b> . Encrypted text string stored as the SNMP user password and associated with the authentication type (SHA or MD5).

Field	Description
<b>Privacy Type</b>	Valid only if you chose <b>Authentication and Privacy</b> mode. Two privacy types are available: <ul style="list-style-type: none"> <li>• <b>DES</b>—Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.</li> <li>• <b>AES128</b>—Cipher Block Chaining (CBC) mode AES for encryption.</li> </ul>
<b>Privacy Password</b>	SNMPv3 privacy password associated with the chosen privacy type (DES or AES128) and used to generate the secret key to encrypt messages that are exchanged with devices.

**Step 7** Expand the **SNMP RETRIES AND TIMEOUT** area, if it is not already expanded, and complete the following fields:

**Table 9: SNMP Retries and Timeout Fields**

Field	Description
<b>Retries</b>	Number of attempts the controller makes to communicate with the devices using SNMP. The default is 3 tries.
<b>Timeout</b>	Number of seconds the controller waits while attempting to communicate with the devices using SNMP before the attempt fails. The default is 5 seconds.

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

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

**Table 10: CLI Fields**

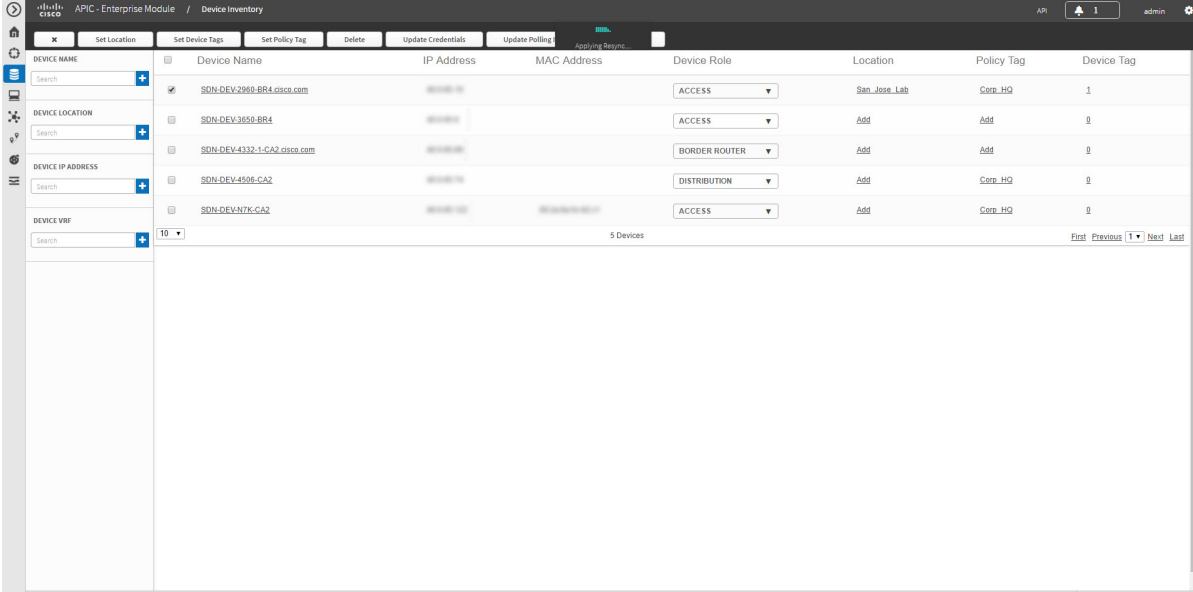
Field	Description
<b>Protocol</b>	Protocol used from a remote management station to connect device CLI. Valid options are <b>Telnet</b> (Telnet TCP/IP) or <b>SSH2</b> (Secure Shell 2.0).
<b>Username</b>	Identification used to log into a device's CLI.
<b>Password</b>	Password used to log into a device's CLI.
<b>Enable Password</b>	After successful login to the CLI, password used to access Privileged EXEC mode.

**Step 9** Click **Update**.

## Resynchronizing Device Information

You can select devices to be polled immediately for updated device and status information, regardless of the polling interval that is set. A maximum of 40 devices can be resynchronized at the same time.

**Figure 11: Device Inventory Window Showing Resync in Progress**



Device Name	IP Address	MAC Address	Device Role	Location	Policy Tag	Device Tag
<input checked="" type="checkbox"/> SDN-DEV-2960-BR4.cisco.com	10.10.10.10	00:00:00:00:00:00	ACCESS	San_Jose_Lab	Core_HQ	1
<input type="checkbox"/> SDN-DEV-3650-BR4	10.10.10.11	00:00:00:00:00:00	ACCESS	Add	Add	0
<input type="checkbox"/> SDN-DEV-4332-1-CA2.cisco.com	10.10.10.12	00:00:00:00:00:00	BORDER ROUTER	Add	Add	0
<input type="checkbox"/> SDN-DEV-4506-CA2	10.10.10.13	00:00:00:00:00:00	DISTRIBUTION	Add	Core_HQ	0
<input type="checkbox"/> SDN-DEV-57K-CA2	10.10.10.14	00:00:00:00:00:00	ACCESS	Add	Core_HQ	0

**Step 1** From the **Navigation** pane, click **Device Inventory**.

**Step 2** Select the device or devices on which you want to gather information about.

**Step 3** Click **Resync**.

**Step 4** Confirm the resynchronization by clicking **OK**.

## Running Commands on Devices

You can run **show** commands and other read-only commands on selected devices and display the output in Cisco APIC-EM. To determine the allowed command keywords, from the global toolbar, click **API > Network Poller > network-device-poller > /network-device-poller/cli/legit-reads > Try it out!**

From the GUI, you can run a maximum of 5 commands per device, with a maximum of 20 devices per request. When a device is part of another request that has not completed yet, no other commands are executed on it.

Access points are not supported. If you choose access points, they are omitted from executing commands. Commands are only run on the other selected devices.

### Before You Begin

The command runner application is not installed on Cisco APIC-EM by default. To use the command running application, you need to download the image from Cisco.com, install it, and enable the Command Runner application. For information, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

You must have either administrator (ROLE\_ADMIN) or policy administrator (ROLE\_POLICY\_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

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

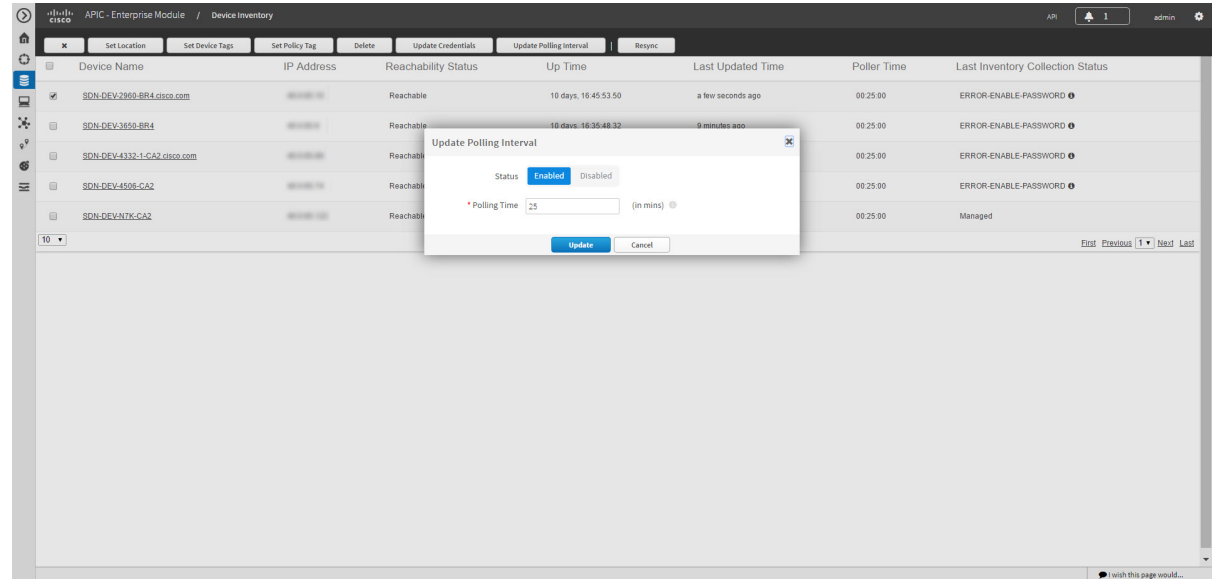
- 
- Step 1** From the **Navigation** pane, click **Device Inventory**.
  - Step 2** Select the device on which you want to run commands.
  - Step 3** Click **Command Runner**.
  - Step 4** In the **Command** field, enter the command that you want to run and click the plus sign (+) icon to add the command to the list of commands to be run.  
You can add only one command at a time and up to 5 commands total.
  - Step 5** When you have defined all of the commands that you want to run, click **Run**.  
Cisco APIC-EM runs the commands on the selected devices and displays the command output.
- Note** Command Runner does not maintain any cache or history of the command results. If you run commands and then close or navigate to a different window, all actions performed in command runner and their results are lost.
- 

## Updating a Device's Polling Interval

You can update the polling interval at the global level for all devices on the **Settings > Polling Interval** page or at the device level for a specific device in the **Device Inventory** window. When you set the polling interval at the device level, that value takes precedence over the global polling interval value.

For information about setting the polling interval at the global level, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

**Figure 12: Update Polling Interval Dialog Box**



### Before You Begin

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

You must have either administrator (ROLE\_ADMIN) or policy administrator (ROLE\_POLICY\_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

- 
- Step 1** From the **Navigation** pane, click **Device Inventory**.
  - Step 2** Select the devices that you want to update.
  - Step 3** Click **Update Polling Interval**.
  - Step 4** Click **OK** to confirm this action.
  - Step 5** From the **Update Polling Interval** dialog box, in the **Status** field, click **Enabled** to turn on polling or click **Disabled** to turn off polling.
  - Step 6** In the **Polling Time** field, enter the time interval (in minutes) between successive polling cycles. Valid values are from 25 to 1440 minutes (24-hours).
    - Note** The device-specific polling time supersedes the global polling time. If you set the device-specific polling time and then change the global polling time, Cisco APIC-EM continues to use the device-specific polling time.
  - Step 7** Click **Update**.
-

# Managing Your Host Inventory

Cisco APIC-EM displays information about the discovered hosts in the **Host Inventory** window.

The following table describes the information that is displayed about the hosts in your inventory.



## Note

Use the filters located below the **Host Inventory** table to limit the number of hosts displayed in the table (10, 25, 50, 100) or to view groups of hosts at a time (First, Previous, Next, Last, or 1-3).

**Figure 13: Host Inventory Window**

Host MAC Address	Host IP Address	Host Type	Connected Device IP Address	Connected Interface Name	Host Name
02:50:56:b0:70:02	10.10.10.1	WIRED	10.10.10.1	GigabitEthernet1/0/1	
02:50:56:b0:75:03	10.10.10.2	WIRED	10.10.10.1	GigabitEthernet1/0/2	
02:50:56:b0:75:04	10.10.10.3	WIRED	10.10.10.1	GigabitEthernet1/0/3	
02:50:56:b0:75:05	10.10.10.4	WIRED	10.10.10.1	GigabitEthernet1/0/4	
02:50:56:b0:75:06	10.10.10.5	WIRED	10.10.10.1	GigabitEthernet1/0/5	
02:50:56:b0:75:07	10.10.10.6	WIRED	10.10.10.1	GigabitEthernet1/0/6	
02:50:56:b0:75:08	10.10.10.7	WIRED	10.10.10.1	GigabitEthernet1/0/7	
02:50:56:b0:75:09	10.10.10.8	WIRED	10.10.10.1	GigabitEthernet1/0/8	
02:50:56:b0:75:10	10.10.10.9	WIRED	10.10.10.1	GigabitEthernet1/0/9	
02:50:56:b0:75:11	10.10.10.10	WIRED	10.10.10.1	GigabitEthernet1/0/10	

The following table describes the information that is displayed about the hosts in your inventory.

**Table 11: Host Inventory**

Host Inventory	Description
Host Name	Name of the host.
Host MAC address	MAC address of the host.
Host IP address	IP address of the host.
Host type	Type of host (wired or wireless).
Connected Network Device IP Address	IP address of the device that is connected to the host. <b>Note</b> IP addresses of only wired devices are shown.

Host Inventory	Description
Connected Interface Name	Name of the interface that the device is connected to. For example, GigabitEthernet1/0/24.

## Filtering Hosts in the Host Inventory Window

You can filter the hosts displayed in the **Host Inventory** window by host MAC address, host IP address, host name, host type, connected network device IP address, or connected interface name.

**Figure 14: Host Inventory Window Showing Filters Pane**

Host MAC Address	Host IP Address	Host Type	Connected Device IP Address	Connected Interface Name	Host Name
02:50:56:00:70:02	10.10.10.1	WIRED	10.10.10.1	GigabitEthernet1/0/1	
02:50:56:00:75:03	10.10.10.2	WIRED	10.10.10.1	GigabitEthernet1/0/2	
02:50:56:00:75:04	10.10.10.3	WIRED	10.10.10.1	GigabitEthernet1/0/3	
02:50:56:00:75:05	10.10.10.4	WIRED	10.10.10.1	GigabitEthernet1/0/4	
02:50:56:00:75:06	10.10.10.5	WIRED	10.10.10.1	GigabitEthernet1/0/5	
02:50:56:00:75:07	10.10.10.6	WIRED	10.10.10.1	GigabitEthernet1/0/6	
02:50:56:00:75:08	10.10.10.7	WIRED	10.10.10.1	GigabitEthernet1/0/7	
02:50:56:00:75:09	10.10.10.8	WIRED	10.10.10.1	GigabitEthernet1/0/8	
02:50:56:00:75:10	10.10.10.9	WIRED	10.10.10.1	GigabitEthernet1/0/9	
02:50:56:00:75:11	10.10.10.10	WIRED	10.10.10.1	GigabitEthernet1/0/10	

### Before You Begin

Make sure that you have hosts in your inventory. If not, discover them using the Discovery function.

#### Step 1

From the **Host Inventory** toolbar, click **Filters**.  
You can choose from the following filter options:

- **Host MAC Address**
- **Host IP Address**
- **Host Name**
- **Host Type**
- **Connected Network Device IP Address**
- **Connected Interface Name**

- Step 2** Enter the appropriate value in the selected filter field.  
For example, for the **Host Name** filter, enter the name of the host.
- The controller presents you with auto-complete values as you enter values in the other fields. Choose one of the suggested values or finish entering the value.
- Note** You can also use a wildcard (asterisk) with these filters. You can enter values with the asterisk at the beginning, end, or in the middle of the string value.
- Step 3** Click the plus (+) icon to perform the filter.  
The data displayed in the **Devices** table automatically updates according to your filter selection.
- Step 4** (Optional) If needed, add more filters following the above steps.
- Note** You can filter on more than one value per filter or across several different filter types.
- Step 5** To remove the filter, click the x icon next to the filter value.
-