# Cisco Network Visibility Application on APIC-EM User Guide, Release 1.6.0.x

**First Published:** 2015-11-02

**Last Modified:** 2017-10-23

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

# CONTENTS

# Preface

## Audience

This publication is intended for experienced network administrators who will configure and maintain the Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM). This guide is part of a documentation set that is designed to help you install, troubleshoot, and upgrade your Cisco APIC-EM. For a complete list of the Cisco APIC-EM documentation set, see Related Documentation, on page viii.

**Note** In this guide, the Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM) is also referred to as the controller.

## Document Conventions

This documentation uses the following conventions:

| Convention | Description |
|---|---|
| ^ or **Ctrl** | The ^ and **Ctrl** symbols represent the Control key. For example, the key combination **^D** or **Ctrl-D** means hold down the **Control** key while you press the **D** key. Keys are indicated in capital letters but are not case sensitive. |
| *string* | A string is a unquoted set of characters shown in italics. For example, when setting an SNMP community string to public, do not use quotation marks around the string or the string will include the quotation marks. |

Command syntax descriptions use the following conventions:

| Convention | Description |
|---|---|
| **bold** | Bold text indicates commands and keywords that you enter exactly as shown. |
| *italics* | Italic text indicates arguments for which you supply values. |
| [x] | Square brackets enclose an optional element (keyword or argument). |
| \| | A vertical line indicates a choice within an optional or required set of keywords or arguments. |
| [x \| y] | Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice. |

| Convention | Description |
|---|---|
| {x \| y} | Braces enclosing keywords or arguments separated by a vertical line indicate a required choice. |

Nested sets of square brackets or braces indicate optional or required choices within optional or required elements. For example:

| Convention | Description |
|---|---|
| [x {y \| z}] | Braces and a vertical line within square brackets indicate a required choice within an optional element. |

Examples use the following conventions:

| Convention | Description |
|---|---|
| `screen` | Examples of information displayed on the screen are set in Courier font. |
| **`bold screen`** | Examples of text that you must enter are set in Courier bold font. |
| < > | Angle brackets enclose text that is not printed to the screen, such as passwords. |
| ! | An exclamation point at the beginning of a line indicates a comment line. |
| [ ] | Square brackets enclose default responses to system prompts. |

**Caution** Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

**Note** Means *reader take note*. Notes contain helpful suggestions or references to materials that may not be contained in this manual.

# Related Documentation

This section lists the Cisco APIC-EM and related documents available on Cisco.com at the following url:

http://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/tsd-products-support-series-home.html

- Cisco APIC-EM Documentation:
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Release Notes*

- *Cisco APIC-EM Quick Start Guide* (directly accessible from the controller's GUI)
- *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*
- *Cisco Application Policy Infrastructure Controller Enterprise Module Upgrade Guide*
- *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*
- *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*
- *Open Source Used In Cisco APIC-EM*

- Cisco EasyQoS Application for Cisco APIC-EM
  - *Cisco EasyQoS Application for APIC-EM Release Notes*
  - *Cisco EasyQoS Application for APIC-EM Supported Platforms*
  - *Cisco EasyQoS Application for APIC-EM User Guide*

- Cisco Network Visibility Application for the Cisco APIC-EM
  - *Cisco Network Visibility Application for APIC-EM Release Notes*
  - *Cisco Network Visibility Application for APIC-EM Supported Platforms*
  - *Cisco Network Visibility Application for APIC-EM User Guide*

- Cisco Path Trace Application for Cisco APIC-EM
  - *Cisco Path Trace Application for APIC-EM Release Notes*
  - *Cisco Path Trace Application for APIC-EM Supported Platforms*
  - *Cisco Path Trace Application for APIC-EM User Guide*

- Cisco IWAN Documentation for the Cisco APIC-EM:
  - *Release Notes for Cisco IWAN*
  - *Release Notes for Cisco Intelligent Wide Area Network Application (Cisco IWAN App)*
  - *Configuration Guide for Cisco IWAN on Cisco APIC-EM*
  - *Software Configuration Guide for Cisco IWAN on APIC-EM*
  - *Open Source Used in Cisco IWAN and Cisco Network Plug and Play*

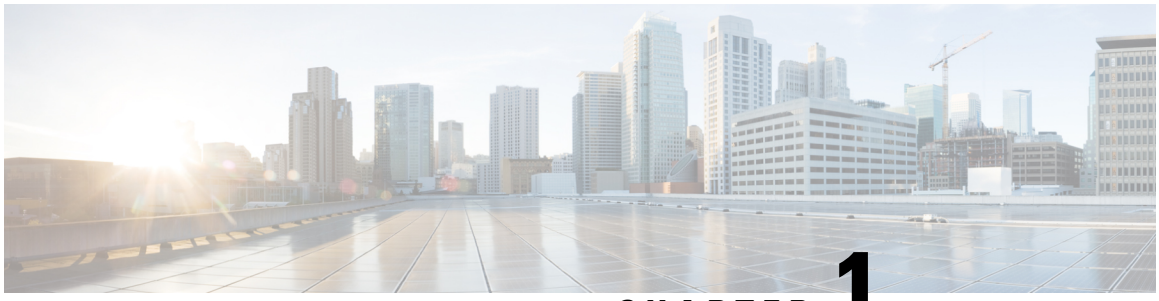
- Cisco Network Plug and Play Documentation for the Cisco APIC-EM:
  - *Release Notes for Cisco Network Plug and Play*
  - *Solution Guide for Cisco Network Plug and Play*
  - *Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM*
  - *Cisco Network Plug and Play Agent Configuration Guide* or *Cisco Open Plug-n-Play Agent Configuration Guide* (depending on the Cisco IOS XE release)
  - *Mobile Application User Guide for Cisco Network Plug and Play*

- Cisco Active Advisor Documentation for the Cisco APIC-EM:
  - *Cisco Active Advisor for APIC-EM Release Notes*
- Cisco Integrity Verification Documentation for the Cisco APIC-EM:
  - *Cisco Integrity Verification Application (Beta) for APIC-EM Release Notes*
  - *Cisco Integrity Verification Application (Beta) for APIC-EM User Guide*
- Cisco Remote Troubleshooter Documentation for the Cisco APIC-EM:
  - *Cisco Remote Troubleshooter Application for APIC-EM Release Notes*
  - *Cisco Remote Troubleshooter Application for APIC-EM User Guide*

**Note** For information about developing your own application that interacts with the controller by means of the northbound REST API, see the https://developer.cisco.com/site/apic-em/ Web site.

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.



CHAPTER 1

# New and Changed Information

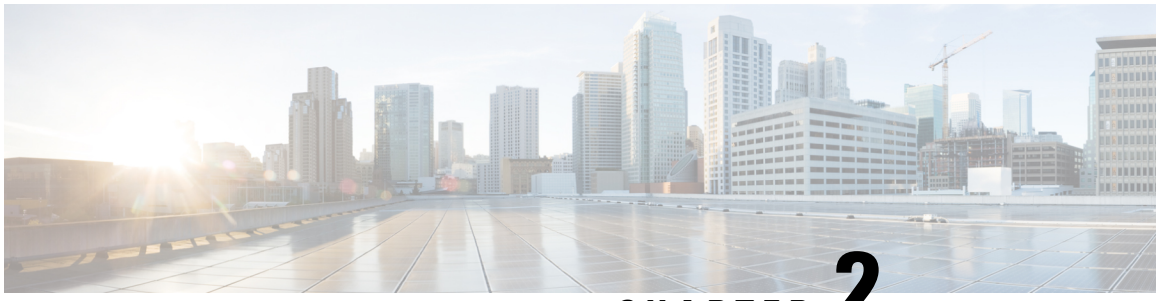


## New and Changed Information

The Cisco APIC-EM software release provides the following new network visibility applications (Discovery, Inventory, Host) features and functionality:

- Support for Cisco 4221 Series Integrated Services Routers (ISR).
- Support for Cisco 1100 Series Integrated Service Routers (ISR).

New and Changed Information



CHAPTER 2

# Overview



## About the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM)

The Cisco Application Policy Infrastructure Controller - Enterprise Module (APIC-EM) is Cisco's Software Defined Networking (SDN) Controller for Enterprise Networks (Access, Campus, WAN and Wireless).

The platform hosts multiple applications (SDN apps) that use open northbound REST APIs that drive core network automation solutions. The platform also supports a number of south-bound protocols that enable it to communicate with the breadth of network devices that customers already have in place, and extend SDN benefits to both greenfield and brownfield environments.

The Cisco APIC-EM platform supports both wired and wireless enterprise networks across the Campus, Branch and WAN infrastructures. It offers the following benefits:

- Creates an intelligent, open, programmable network with open APIs
- Saves time, resources, and costs through advanced automation
- Transforms business intent policies into a dynamic network configuration
- Provides a single point for network wide automation and control

The following table describes the features and benefits of the Cisco APIC-EM.

***Table 1: Cisco APIC Enterprise Module Features and Benefits***

| Feature | Description |
|---|---|
| Network Information Database | The Cisco APIC-EM periodically scans the network to create a “single source of truth” for IT. This inventory includes all network devices, along with an abstraction for the entire enterprise network. |

| Feature | Description |
|---|---|
| Network topology visualization | The Cisco APIC-EM automatically discovers and maps network devices to a physical topology with detailed device-level data. The topology of devices and links can also be presented on a geographical map. You can use this interactive feature to troubleshoot your network. |
| EasyQoS application | The EasyQoS application abstracts away the complexity of deploying Quality of Service across a heterogeneous network. It presents users with a workflow that allows them to think of QoS in terms of business intent policies that are then translated by Cisco APIC-EM into a device centric configuration. |
| Cisco Network Plug and Play (PnP) application | The Cisco Network PnP solution extends across Cisco's enterprise portfolio. It provides a highly secure, scalable, seamless, and unified zero-touch deployment experience for customers across Cisco routers, switches and wireless access points.<br>**Note** This application is not bundled with the Cisco APIC-EM controller for this release. You need to download, install, and enable this application to use it. For information about these procedures, see the *Cisco Application Infrastructure Controller Enterprise Module Upgrade Guide*. |
| Cisco Intelligent WAN (IWAN) application | The separately licensed IWAN application for APIC-EM simplifies the provisioning of IWAN network profiles with simple business policies. The IWAN application defines business-level preferences by application or groups of applications in terms of the preferred path for hybrid WAN links. Doing so improves the application experience over any connection and saves telecom costs by leveraging cheaper WAN links.<br>**Note** This application is not bundled with the Cisco APIC-EM controller for this release. You need to download, install, and enable this application to use it. For information about these procedures, see the *Cisco Application Infrastructure Controller Enterprise Module Upgrade Guide*. |

| Feature | Description |
|---|---|
| Cisco Active Advisor application | The Cisco Active Advisor application for APIC-EM offers personalized life cycle management for your network devices by keeping you up-to-date on:<br>• End-of-life milestones for hardware and software<br>• Product advisories, including Product Security Incident Response Team (PSIRT) bulletins and field notices<br>• Warranty and service contract status<br>**Note** This application is not bundled with the Cisco APIC-EM controller for this release. You need to download, install, and enable this application to use it. For information about these procedures, see the *Cisco Application Infrastructure Controller Enterprise Module Upgrade Guide*. |
| Cisco Integrity Verification application | The Cisco Integrity Verification (IV) application provides automated and continuous monitoring of network devices, noting any unexpected or invalid results that may indicate compromise. The objective of the Cisco IV application is early detection of the compromise, so as to reduce its impact. The Cisco IV application operates within the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) as a beta version for this release.<br>**Note** This application is not bundled with the Cisco APIC-EM controller for this release. You need to download, install, and enable this application to use it. For information about these procedures, see the *Cisco Application Infrastructure Controller Enterprise Module Upgrade Guide*. |
| Cisco Remote Troubleshooter application | The Cisco Remote Troubleshooter application uses the Cisco IronPort infrastructure to create a tunnel that enables a support engineer to connect to an APIC-EM cluster and troubleshoot issues with your system. The app uses outbound SSH to create a secure connection to the cluster through this tunnel.<br>As an administrator, you can use the Remote Troubleshooter application to control when a support engineer has access to a particular cluster and for how long (since a support engineer cannot establish a secure tunnel on their own). You will receive indication that a support engineer establishes a remote access session, and you can end a session at any time by disabling the tunnel they are using. |
| Public Key Infrastructure (PKI) server | The Cisco APIC-EM provides an integrated PKI service that acts as Certificate Authority (CA) or sub-CA to automate X.509 SSL certificate lifecycle management. Applications, such as IWAN and PnP, use the capabilities of the embedded PKI service for automatic SSL certificate management. |

| Feature | Description |
|---|---|
| Path Trace application | The path trace application helps to solve network problems by automating the inspection and interrogation of the flow taken by a business application in the network. |
| High Availability (HA) | HA is provided in N+ 1 redundancy mode with full data persistence for HA and Scale. All the nodes work in Active-Active mode for optimal performance and load sharing. |
| Back Up and Restore | The Cisco APIC-EM supports complete back up and restore of the entire database from the controller GUI. |
| Audit Logs | The audit log captures user and network activity for the Cisco APIC-EM applications. |

# Logging into the Cisco APIC-EM

You access the Cisco APIC-EM GUI by entering its network IP address in your browser. The IP address was configured for the Cisco APIC-EM network adapter during the initial setup using the configuration wizard. This IP address connects to the external network.

**Step 1** In your browser address bar, enter the IP address of the Cisco APIC-EM in the following format:

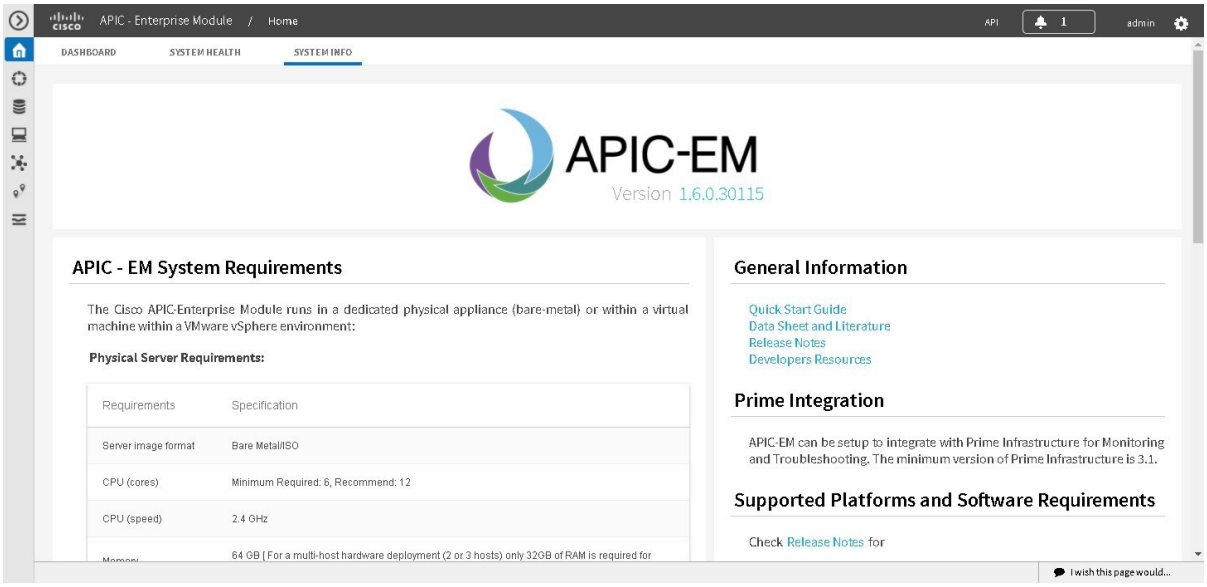
**https://***IP address*

**Step 2** On the launch page, enter your username and password that you configured during the deployment procedure.

The **Home** page of the APIC-EM controller appears. The **Home** page consists of the following three tabs:

- **DASHBOARD**
- **SYSTEM HEALTH**
- **SYSTEM INFO**

*Figure 1: SYSTEM INFO Tab*




### What to do next

Click on each tab and review the data provided in the GUI.

# Cisco APIC-EM GUI

### First GUI Window

When you log into the Cisco APIC-EM, the GUI appears. See the following tables for descriptions of the GUI elements.

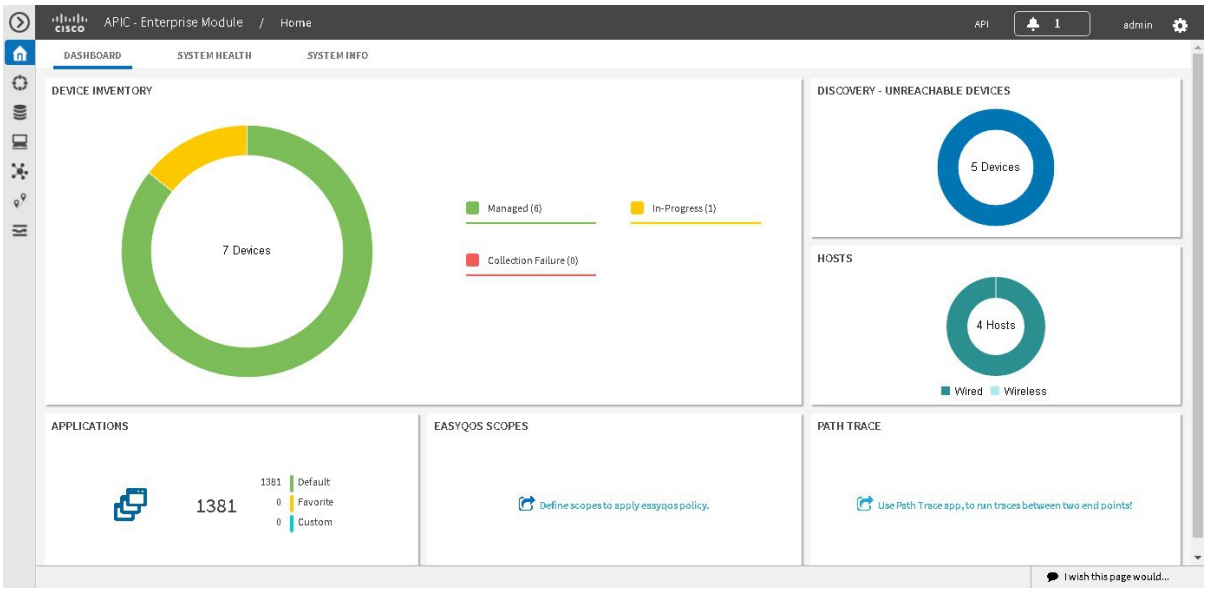



*Table 2: Cisco APIC-EM GUI Elements*

| Name | Description |
|---|---|
| **Navigation** pane | At the left side of the window, the **Navigation** pane provides access to the Cisco APIC-EM functions and additional applications, such as EasyQoS, Path Trace, IWAN, and Network Plug and Play. |
| **Global** toolbar | At the top of the window, the **Global** toolbar provides access to tools, such as API documentation, settings, and notifications. For a full explanation of the icons on the **Global** toolbar, see the Global Toolbar Options table below. |
| Application or Function Pane | In the main window area, the application or function pane displays the interface of the application or function. When you click an option in the **Navigation** pane or from the **Global** toolbar, the corresponding application or function opens in this pane. |
| **I wish this page would...** feedback link | At the bottom of the window, the **I wish this page would...** feedback link opens a preaddressed email in your email application, where you can provide input about your experience using the Cisco APIC-EM and suggestions for improvements. |

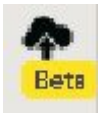
## Navigation Pane Options

The **Navigation** pane provides options to access the major Cisco APIC-EM features and applications.

*Table 3: Navigation Pane Options*

| Icon | Name | Description |
|---|---|---|
|  | **Hide/Unhide Navigation** | Allows you to hide and unhide the **Navigation** pane. |

| Icon | Name | Description |
|---|---|---|
|  | **Home** | Provides information about the APIC-EM, such as its network status, system health, and system information. |
|  | **Discovery** | Allows you to configure discovery options for scanning the devices and hosts in your network. |
|  | **Device Inventory** | Provides access to the inventory database, where you can display, filter, and sort tabular information about the discovered devices in your network. |
|  | **Host Inventory** | Provides access to the inventory database, where you can display, filter, and sort tabular information about the discovered hosts in your network. |
|  | **Topology** | Presents the devices and links that the Cisco APIC-EM discovers as a physical topology map with detailed device-level data. The topology of devices and links can also be presented on a geographical map. You can use this interactive feature to troubleshoot your network. |
|  | **IWAN** | Simplifies the provisioning of IWAN network profiles with simple business policies. The IWAN application defines business-level preferences by application or groups of applications with preferred paths for hybrid WAN links. Doing so improves the application experience over any connection and saves telecommunication costs by leveraging cheaper WAN links. |
|  | **EasyQoS** | Enables you to configure quality of service on previously discovered Cisco network devices that support the EasyQoS feature. Using EasyQoS, you can group devices and then define the business relevance of applications that are used in your network. The Cisco APIC-EM takes your QoS selections, translates them into the proper command line interface (CLI) commands, and deploys them onto the selected devices. |
|  | **Path Trace** | Helps to solve network problems by automating the inspection and interrogation of the flow taken by a business application in the network. |
|  | **Network Plug and Play** | Provides a highly secure, scalable, seamless, and unified zero-touch deployment experience for customers across Cisco routers, switches and wireless access points. |

| Icon | Name | Description |
|---|---|---|
|  | **Active Advisor** | Provides information about devices in your Cisco APIC-EM inventory that have hardware End-of-Life warnings and vulnerabilities that have been identified by the Cisco Product Security Incident Response Team (PSIRT), Cisco Active Advisor provides Software End-of-Life, Field Notice, warranty, and service contract coverage information about those devices. |
|  | **Integrity Verification** | Provides automated and continuous monitoring of network device integrity measurements, noting any unexpected or invalid results that may indicate compromise. The objective of the IV application is early detection of a compromise to reduce its impact. |
|  | **Remote Troubleshooter** | Utilizes the Cisco IronPort infrastructure to create a tunnel that enables a support engineer to connect to an APIC-EM cluster and troubleshoot issues. The application uses outbound SSH to create a secure connection to the cluster through this tunnel. |
|  | **Wide Area Bonjour** | Provides controller functions in the network, as it enables discovery and distribution of policy-based Apple Bonjour services independent of network boundaries. |

### Global Toolbar Options

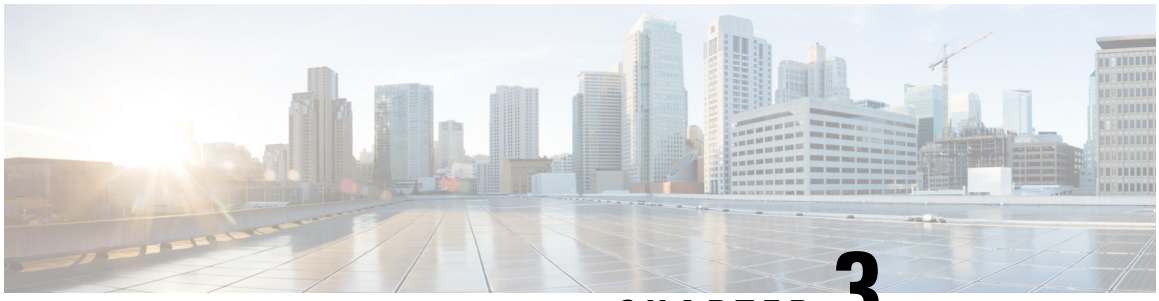
The **Global** toolbar provides access to API information, administrative functions, system notifications.

***Table 4: Global Toolbar Options***

| Icon | Option | Description |
|---|---|---|
|  | **API** | Displays the automatically generated documentation for the northbound REST APIs. |

| Icon | Option | Description |
|---|---|---|
|  | **System Notifications** | Opens the **System Notifications** dialog box, which provides information about system notifications that have occurred.<br>The icons at the top provide a total of the number of notifications in each of the following categories:<br>• Minor (yellow triangle icon)<br>• Major (orange triangle icon)<br>• Critical (red octagon icon)<br>If notifications have occurred, they are listed below the icons. For example, any notifications about software updates or security certificates updates appear in this window.<br>Click the **Notification History** link to open the **Notifications** window. This window provides information about the notification, such as its severtiy, source, timestamp, and status.<br>You can perform the following actions in this window:<br>• Acknowledge a notification.<br>• Filter notifications by status or security level.<br>• Sort notifications by source, detail, description, timestamp, or status. |

| Icon | Option | Description |
|---|---|---|
|  | **Administrative Functions** | Opens a menu of options. From this menu, you can choose the following administrative options:<br>• **Settings**—Allows you to configure controller settings, such user profiles, discovery credentials, network security settings, backup and restore, and other controller settings.<br>• **App Management**—Allows you to individually upload and enable Cisco and third-party applications, backup and restore the controller data, and update the Cisco APIC-EM software.<br>• **System Administration**—Allows you to manage and troubleshoot controller services.<br>**Important** Only advanced users should access the **System Administration** console to attempt to troubleshoot the controller services.<br>• **Audit Logs**—Provides information to help you monitor policy creation and application.<br>• **About APIC-EM**—Displays the installed Cisco APIC-EM software version.<br>You can perform the following user functions:<br>• **Change Password**—Allows you to change your own password.<br>• **Sign Out**—Logs you out of the Cisco APIC-EM. |



CHAPTER 3

# Device Configuration Prerequisites



## Required Platform Configurations

You need to make the following configuration changes on these platforms for Discovery to work properly.

***Table 5: Required Platform Configurations***

| Feature | Platform | Required Configuration |
|---|---|---|
| Discovery (device inventory collection) | Cisco ASR 9000 router or any other Cisco device that requires NETCONF support for their device pack. | Configure NETCONF on these platforms.<br>For information, see NETCONF Configuration, on page 14. |
| Discovery (host inventory collection) | Devices connected to hosts using SNMP. | Configure SNMP traps on these devices.<br>For information, see SNMP Trap Configuration, on page 14. |
| | Devices connected to hosts using IPDT. | Enable IPDT for these devices.<br>For information, see IP Device Tracking Configuration, on page 15. |
| | • Cisco Series 2504 WLC<br>• Cisco Series 5508/5520 WLC<br>• Cisco Series 8510/8540 WLC | Configure SNMP traps and object identifiers on these wireless LAN controllers.<br>For information, see Wireless LAN Controller Configuration, on page 15. |

# NETCONF Configuration

You must enable the NETCONF protocol for the Cisco ASR 9000 router or for any other Cisco device that requires NETCONF support for their device pack. If NETCONF is not enabled, then the controller's inventory collection process will be incomplete for that device.

**Note** Though NETCONF typically runs over SSH or on its own port, with the Cisco APIC-EM and for the Cisco ASR 9000 router NETCONF is run over a CLI session.

For specific information about enabling NETCONF for your own Cisco device, refer to that device's documentation. As an example, a typical configuration sequence on a terminal to enable NETCONF on a Cisco device is as follows:

```
#ssh server v2
#netconf agent tty
#!
#xml agent tty
#!
#commit
#end
#crypto key generate rsa
```

**Note** The rsa key needs to be generated to succeed with SSH. For this reason, the crypto key generate rsa command needs to be executed in exec mode at the end of the configuration sequence if it has not already been done.

# SNMP Trap Configuration

To ensure that Cisco APIC-EM captures data about the hosts connected to your network devices, you must set up SNMP traps or notifications. Enter the following SNMP commands to set up SNMP traps on the devices that connect to hosts within your network:

1. **snmp-server enable traps snmp linkdown linkup**
2. **snmp-server host** *IP address* **version 2c public**

**Note** For Cisco Nexus devices, enter the following SNMP commands instead of the commands listed above:

1. **snmp-server enable traps snmp linkdown linkup**
2. **snmp-server host** *IP address* **use-vrf default**

After configuring SNMP traps on the network devices, the following data is captured and made available in the controller's GUI:

- Host data including the MAC address, IP address, and type
- Device interface status

# IP Device Tracking Configuration

The Cisco APIC-EM discovery function uses several protocols and methods to retrieve network information, such as hosts IP addresses, MAC addresses, and network attachment points. To use IP Device Tracking (IPDT) for discovery, you must manually enable IPDT on the devices and interfaces for this protocol to be used to collect host information. To enable IPDT on your devices, refer to your specific device documentation. For general information about IPDT, see IP Device Tracking (IPDT) Overview.

# Wireless LAN Controller Configuration

The Cisco APIC-EM accepts SNMP traps from several Cisco Wireless LAN Controllers (WLCs). The SNMP traps are used to update the host inventory database. You need to configure the WLCs so that the Cisco APIC-EM is the trap receiver, and the WLCs send the enhanced traps to the Cisco APIC-EM.

The following WLCs require SNMP traps to be enabled:

- Cisco Series 2504 Wireless LAN Controller
- Cisco Series 5508/5520 Wireless LAN Controller
- Cisco Series 8510/8540 Wireless LAN Controller

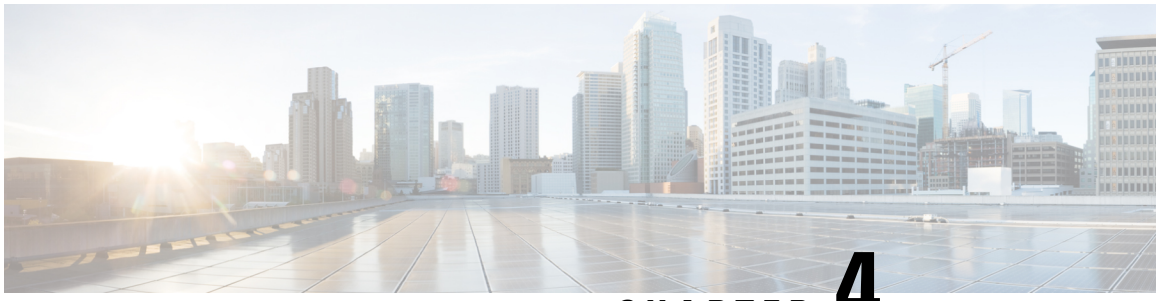
The following table specifies the SNMP traps and object identifiers that must be set on the WLCs.

| Trap Name | OID |
|---|---|
| ciscoLwappDot11ClientAssocTrap | 1.3.6.1.4.1.9.9.599.0.9 |
| ciscoLwappDot11ClientDeAuthenticatedTrap | 1.3.6.1.4.1.9.9.599.0.10 |
| ciscoLwappDot11ClientMovedToRunStateNewTrap | 1.3.6.1.4.1.9.9.599.0.11 |
| ciscoLwappDot11ClientMobilityTrap | 1.3.6.1.4.1.9.9.599.0.12 |

The following configurations must be set to enable the above SNMP traps:

- config trapflags client enhanced-802.11-associate enable
- config trapflags client enhanced-802.11-deauthenticate enable
- config trapflags client enhanced-authentication enable
- config trapflags client enhanced-802.11-stats enable

**Note** When setting the SNMP traps on the WLCs, ensure you configure the IP address of the Cisco APIC-EM as the SNMP trap destination IP address. You set the Cisco APIC-EM IP address using the configuration wizard during the deployment process. For information about this process and the controller IP address, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide* for additional information.



CHAPTER 4

# Discovering Devices and Hosts



## About Discovery

The process of finding network devices and hosts is known as discovery. The Discovery function scans the devices and hosts in your network and populates the Cisco APIC-EM database with the information that it retrieves. To discover devices and hosts, you need to provide the controller with information about the devices so that the Discovery function can reach as many of the devices in your network as possible and gather as much information as it can.

The Discovery function uses the following protocols and methods to retrieve device information, such as hosts IP addresses, MAC addresses, and network attachment points:

- Cisco Discovery Protocol (CDP)
- Community-based Simple Network Management Protocol Version 2 (SNMPv2c)
- Simple Network Management Protocol version 3 (SNMPv3)
- Link Layer Discovery Protocol (LLDP)
- IP Device Tracking (IPDT) (For Discovery to collect host information, you must manually enable IPDT on devices. After IPDT is enabled, Discovery collects host information on a best-effort basis, because in addition to IPDT, Discovery relies on ARP entries for host information.)
- LLDP Media Endpoint Discovery (LLDP-MED) (IP phones and some servers are discovered using LLDP-MED).

For information about the required protocol configuration for your devices, see Device Configuration Prerequisites, on page 13.

# Understanding Discovery Credentials

The Cisco APIC-EM supports two different types of discovery credentials: global and job specific (or discovery request-specific). Both types of discovery credentials can consist of CLI or SNMP credentials that are configured using the controller's GUI.

Global credentials can be configured in either the **Discovery** window or the **Discovery Credentials** windows (as described in this chapter). Job specific credentials are only configured in the **Discovery** window.

**Note** For information about the procedure to configure global and/or job specific credentials in the **Discovery** window, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

Both CLI and SNMP credentials are required for a successful discovery. The SNMP credentials (either global or job specific) are used for *device* discovery. The CLI credentials (either global or job specific) are used for capturing or applying *device configurations* for the controller's inventory.

You should enter at least one set of SNMP credentials, either SNMPv2c or SNMPv3, for your device discovery. If you are going to configure SNMPv2 settings in your network, then SNMP Read Only (RO) community string values should be entered in the controller to assure a successful discovery and populated inventory. However, if an SNMP RO community string and SNMP Read Writer (RW) community string is not entered into the controller, as a *best effort*, discovery will run with the default SNMP RO community string "public." Additionally, if no SNMP RO community string is entered but a SNMP RW community string is entered, then the SNMP RW community string will be used as SNMP RO community string.

**Note** You can enter values for both SNMP versions (SNMPv2c and SNMPv3) for a single discovery. The controller supports multiple SNMP credential configurations. Altogether, you can enter a maximum of 5 global device credentials (SNMP or CLI) using the **Discovery Credentials** windows as described in this chapter, with an additional credentials set being created in the **Discovery** window. Therefore, for a single discovery scan request, you can configure a total of 6 credential sets of each type (CLI or SNMP).

## Global Credentials

Global credentials are defined as preexisting credentials that are common to the devices in a network. Global credentials (CLI and SNMP) are configured on the devices using the GUI (**Discovery** window or **Discovery Credentials** window) and permit successful login to the devices. Global credentials are used by the Cisco APIC-EM to authenticate and access the devices in a network that share this device credential when performing network discoveries.

You can configure the global CLI credentials in the **CLI Credentials** window. You access this window by clicking either **admin** or the **Settings** icon (gear) on the menu bar at the upper right of the screen. You then click the **Settings** link from the drop-down menu and then click **CLI Credentials** on the Setting Navigation pane. You can also configure global CLI credentials in the **Credentials** field in the **Discovery** window. For information about the procedure to configure global CLI credentials in the **Discovery** window, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

You configure the global SNMP credentials in the **SNMPv2c** or **SNMPv3** window . You access these windows by clicking either **admin** or the **Settings** icon (gear) on the menu bar at the upper right of the screen.

You then click the **Settings** link from the drop-down menu and then click one of the SNMP window links on the Setting Navigation pane. You can also configure global SNMP credentials in the **Credentials** field in the **Discovery** window. For information about the procedure to configure global SNMP credentials in the **Discovery** window, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

**Note** Multiple credentials can be configured in the **CLI Credentials** window.

# Job Specific Credentials

Job specific credentials (request-specific credentials) are defined as preexisting *device* credentials for a specific network device or set of devices that do not share the global credentials.

You configure job specific credentials in the **Discovery** window prior to performing a discovery that is exclusive for that set of network devices. You access this window by clicking **Discovery** on the Navigation pane.

# Discovery Credentials Example

Assume a network of 200 devices that form a CDP neighborship (neighboring devices discovered using Cisco Discovery Protocol (CDP)). In this network, 190 devices share a global credential (Credential-0) and the 10 remaining devices each have their own unique or job specific credentials (Credential 1- 5)

To properly authenticate and access the devices in this network by the Cisco APIC-EM, you perform the following tasks:

1. Configure the CLI global credentials as Credential-0 for the controller.

   You can configure the global credentials in the **CLI Credentials** window. You access this window, by clicking either **admin** or the **Settings** icon (gear) on the menu bar at the upper right of the screen. You then click the **Settings** link from the drop-down menu and then click **CLI Credentials** on the Setting Navigation pane.

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

   You can configure these global credentials in the two SNMP windows. You access these GUI windows by clicking the **Settings** button at the top right and then clicking **SNMPv2c** or **SNMPv3** on the Setting Navigation pane.

3. Run a **CDP** discovery using one of the 190 device IP addresses (190 devices that share the global credentials) and selecting the global credentials in the GUI. You run a **CDP** discovery in the **Discovery** window. You access this window, by clicking **Discovery** on the Navigation pane.

4. Run 10 separate **Range** discoveries for each of the remaining 10 devices using the appropriate job specific credentials and SNMP values (for example, Credential-1, Credential-2-5, etc.).

   You configure the job specific credentials in the **Discovery** window. You access this window, by clicking **Discovery** on the Navigation pane.

5. Review the **Device Inventory** table in the **Device Inventory** window to check the discovery results

# Discovery Credentials Rules

Discovery credentials (global and job specific) operate under the rules as described in the bullet list and table below.

### Job Specific Credential Rules

- Job specific credentials can be provided when creating a new network discovery, but only a single set of job specific credentials is allowed per network discovery.
- Job specific credentials take precedence over any configured global credentials.
- If the job specific credentials are provided as part of a network discovery and cause an authentication failure, then discovery is attempted a second time with the configured global credentials (if explicitly selected in the **Discovery** window of the controller's GUI). If discovery fails with the global credentials then the device discovery status will result in an authentication failure.
- When using Cisco APIC-EM APIs for a network discovery and the job specific credentials (both CLI and SNMP) are *not* provided as part of the network discovery, then the global credentials (both CLI and SNMP provided by the user) are used to authenticate devices.

### Global Credential Rules

***Table 6: Global Credential Rules***

| Global Credentials | Job Specific Credentials | Result |
|---|---|---|
| Not configured | Not configured | If the network discovery is run from the controller's GUI, then the default SNMP read community string (public) is used for the discovery scan. A discovery failure will not occur in this case.<br>If the network discovery is run using Cisco APIC-EM APIs, then a discovery failure will occur since both CLI and SNMP credentials must be configured for a successful device discovery using the Cisco APIC-EM APIs. |
| Not configured | Configured | The specified job specific credentials will be used for discovery. |
| Configured | Not configured | All the configured global credentials will be used. |
| Configured but not selected | Configured | Only the job specific credentials will be used. |
| Configured and selected | Not configured | Only selected global credential will be used. |

| Global Credentials | Job Specific Credentials | Result |
|---|---|---|
| Configured and selected | Configured | Both specified credentials (global and job specific) will be used for discovery. |
| Configured, but wrong global credential IDs are mentioned in the discovery POST REST API. | Correct job specific credentials configured | Discovery fails.<br>**Note** This scenario is only possible by API not from the controller GUI. |
| Configured, but wrong global credential IDs are mentioned in the discovery POST REST API. | Not configured | Discovery fails.<br>**Note** This scenario is only possible by API not from the controller GUI. |

# Discovery Credentials Caveats

The following are caveats for the Cisco APIC-EM discovery credentials:

- If a device credential changes in a network device or devices after Cisco APIC-EM discovery is completed for that device or devices, any subsequent polling cycles for that device or devices will fail. To correct this situation, an administrator has following options:
  - Start a new discovery scan with changed job specific credentials that matches the new device credential.
  - Edit the existing discovery by updating or modifying the global credentials, and then rerun the discovery scan.
- If the ongoing discovery fails due to a device authentication failure (for example, the provided discovery credential is not valid for the devices discovered by current discovery), then the administrator has following options:
  - Stop or delete the current discovery. Create one or more new network discovery jobs (either a **CDP** or **Range** discovery type) with a job specific credential that matches the device credential.
  - Create a new global credential and execute a new discovery selecting the correct global credential.
  - Edit an existing global credential and re-run the discovery.
- Deleting a global credential does not affect already discovered devices. These already discovered devices will not report an authentication failure.
- The Cisco APIC-EM provides a REST API which allows the retrieval of the list of managed network devices in the Cisco APIC-EM inventory. The purpose of this API is to allow an external application to synchronize its own managed device inventory with the devices that have been discovered by the Cisco APIC-EM. For example, for Cisco IWAN scenarios, Prime Infrastructure makes use of this API in order to populate its inventory with the IWAN devices contained in the Cisco APIC-EM inventory in order to provide monitoring of the IWAN solution.

**Note** Only the username is provided in clear text. SNMP community strings and passwords are not provided in cleartext for security reasons.

# Configuring Global Discovery Credentials

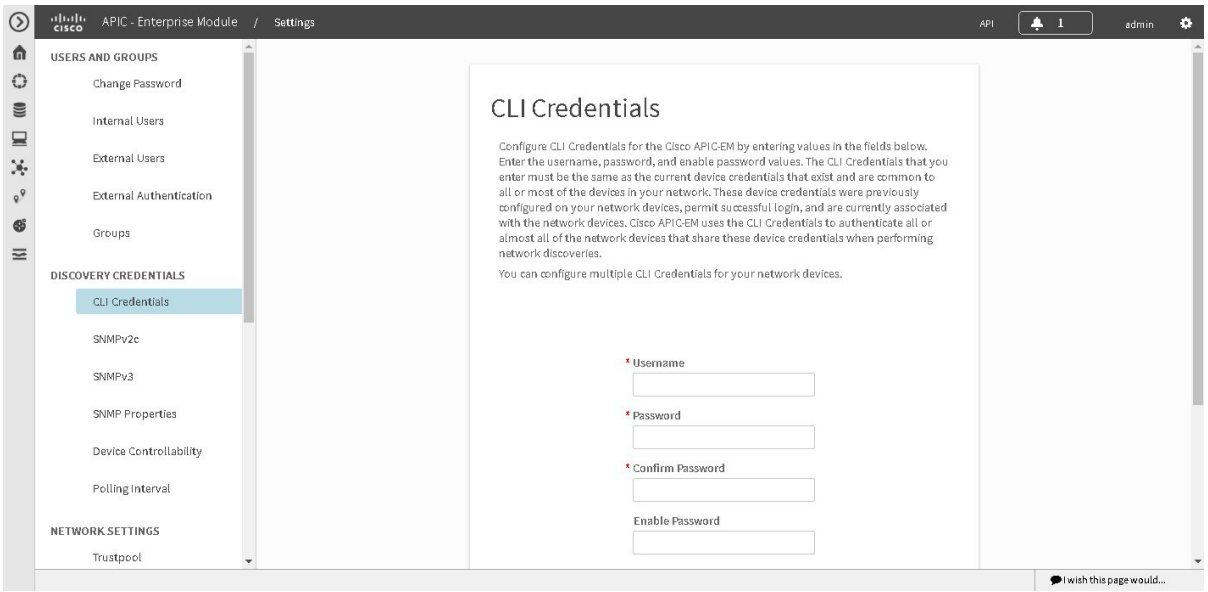
## Configuring CLI Credentials

CLI credentials are defined as preexisting *device* credentials that are common to most of the devices in a network. CLI credentials are used by the Cisco APIC-EM to authenticate and access the devices in a network that share this CLI credential when performing devices discoveries.

You configure the CLI global credentials in the **CLI Credentials** window or the **Discovery** window. This procedure describes how to configure CLI global credentials in the **CLI Credentials** window.

**Note** You can configure up to five CLI credentials.

***Figure 2: CLI Credentials Window***




### Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create

a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

**Step 1** In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

**Step 2** Click the **Settings** link from the drop-down menu.

**Step 3** In the **Settings** navigation pane, click **CLI Credentials** to view the **CLI Credentials** window.

In the **CLI Credentials** window, enter the appropriate CLI global credentials for the devices within your network or networks.

**Step 4** Enter the CLI Credentials username in the **Username** field.

**Step 5** Enter the CLI Credentials password in the **Password** field.

**Step 6** Reenter the CLI Credentials password in the **Confirm Password** field to confirm the value that you just entered.

**Step 7** If your network devices have been configured with an enable password, then enter the CLI Credentials for the enable password in the **Enable Password** field.

**Note** Both the CLI credentials password and enable password are saved in the controller in encrypted form. You cannot view these original passwords after you enter them.

**Step 8** If you entered an enable password in the **Enable Password** field, reenter it in the **Confirm Enable Password** field to confirm the value that you just entered.

**Step 9** In the **CLI Credentials** window, click **Add** to save the credentials to the Cisco APIC-EM database.

### What to do next

Proceed to configure SNMP values for your network device discovery.

For a successful device discovery (with all the device information to be collected), CLI credentials (global and/or job specific) should be configured using the controller. The global credentials for CLI and SNMP (v2c or v3) can be configured in the **Discovery Credentials** windows (as described in this chapter) or the **Discovery** window, and are used in addition to any job specific credentials (for CLI and SNMP) that are also configured in the **Discovery** window.

# Configuring SNMP

You configure SNMP for device discovery using the following **Discovery Credentials** windows in the Cisco APIC-EM GUI:

- **SNMPv2c**
- **SNMPv3**
- **SNMP Properties**

**Note** You can also configure SNMP for device discovery in the **Discovery** window of the controller's GUI. For information about the procedures to configure SNMP for device discovery in the **Discovery** window, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

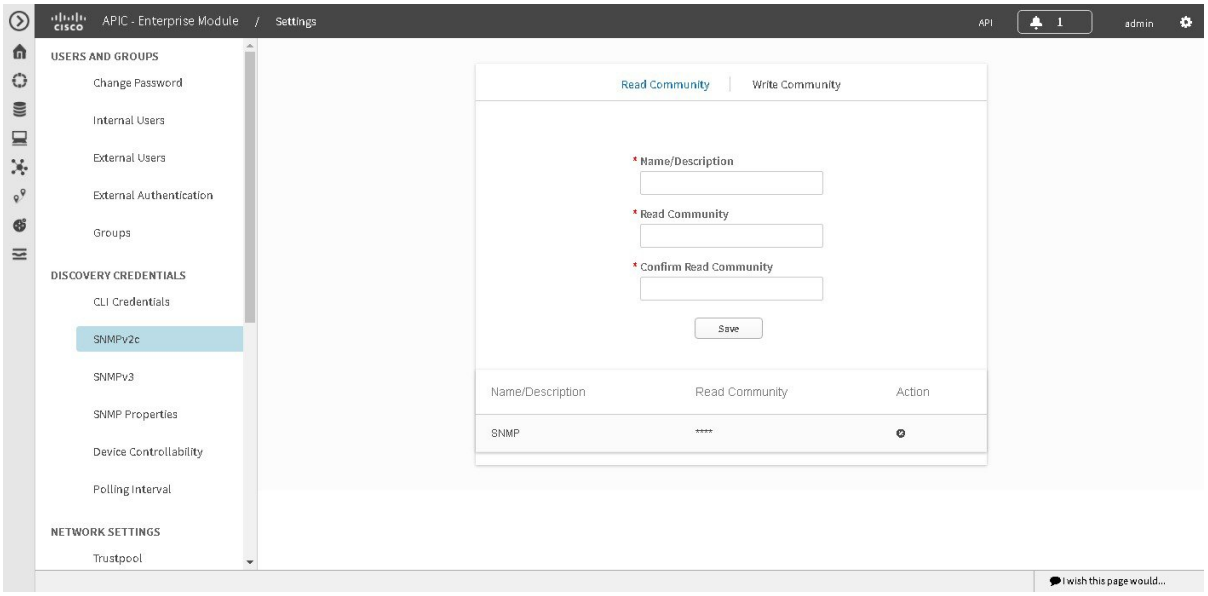
**Important** You can use SNMP and the existing security features in SNMP v3 to secure communications between the controller and the devices in your network. SNMP v3 provides both privacy (encryption) and authentication capabilities for these communications. If possible for your network, we recommend that you use SNMPv3 with both privacy and authentication enabled.

## Configuring SNMPv2c

You configure SNMPv2c for device discovery in the **SNMPv2c** window in the Cisco APIC-EM GUI. The SNMP values that you configure for SNMPv2c for the controller must match the SNMPv2c values that have been configured for your network devices.

**Note** You can configure up to five read community strings and five write community strings.

***Figure 3: Configuring SNMPv2c***




SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network. The different versions of SNMP are SNMPv1, SNMPv2, SNMPv2c, and SNMPv3.

SNMPv2c is the community string-based administrative framework for SNMPv2. Community string is a type of password, which is transmitted in clear text. SNMPv2c does not provide authentication or encryption (noAuthNoPriv level of security).

**Note** In addition to configuring SNMPv2c for device discovery in the controller, a "best effort" Cisco APIC-EM discovery is in place, meaning that devices having SNMP with Read-Only (RO) community string set to "public" will be discovered all the time irrespective of the configured SNMP Read/Write community string.

### Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have your network's SNMP information available for this configuration procedure.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

**Step 1** In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

**Step 2** Click the **Settings** link from the drop-down menu.

**Step 3** In the **Settings** navigation pane, click **SNMPv2c** to view the **SNMPv2c** window.

**Step 4** In the **SNMPv2c** window, click **Read Community**.

Enter your **Read Community** values:

- **Name/Description**—Description of the Read-Only (RO) community string value and/or the device or devices that are configured with it.
- **Read Community**—Read-Only community string value configured on devices that you need the controller to connect to and access. This community string value must match the community string value pre-configured on the devices that the controller will connect to and access.
- **Confirm Read Community**—Reenter the Read-Only community string to confirm the value that you just entered.

**Note** If you are configuring SNMPv2c for your discovery, then configuring **Read Community** values is mandatory.

**Step 5** Click **Save** to save your **Read Community** values.

The **Read Community** values will appear in the table below.

**Step 6** (Optional) In the **SNMPv2c** window, click **Write Community**.

Enter your **Write Community** values:

- **Name/Description**—Description of the Write community string value and/or the device or devices that are configured with it.

- **Write Community**—Write community string value configured on devices that you need the controller to connect to and access. This community string value must match the community string value pre-configured on the devices that the controller will connect to and access.
- **Confirm Write Community**—Reenter the Write community string to confirm the value that you just entered.

**Step 7** (Optional) Click **Save** to save your **Write Community** values.

The **Write Community** values will appear in the table below.

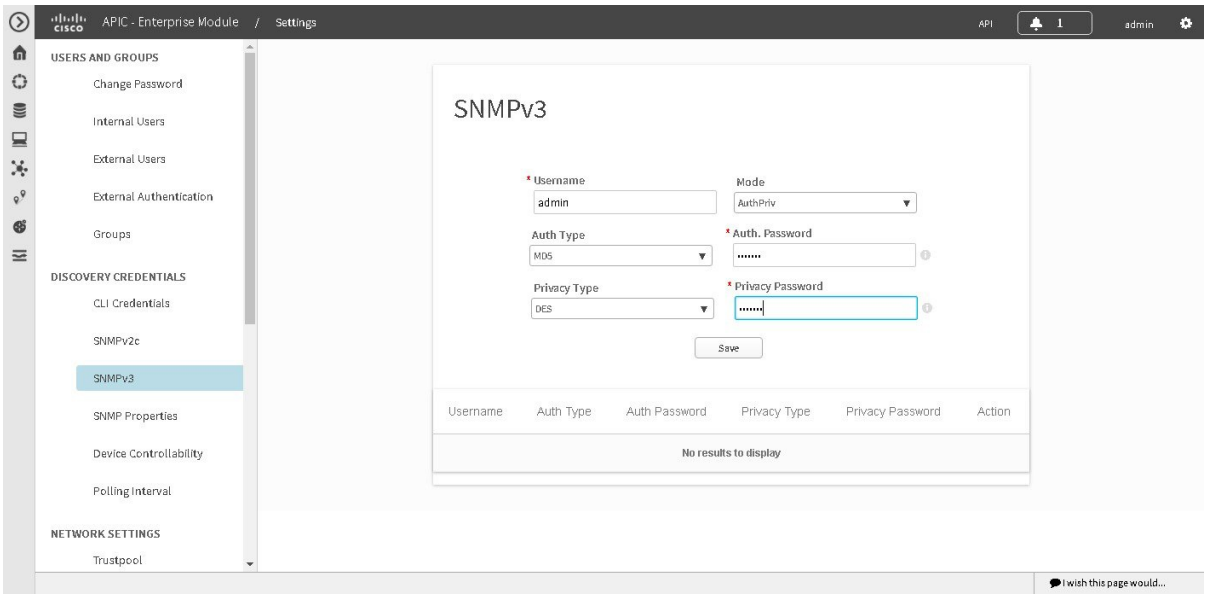
### What to do next

If required for your SNMP configuration, proceed to configure either **SNMPv3** or **SNMP Properties** using the GUI.

## Configuring SNMPv3

You configure SNMPv3 for device discovery in the **SNMPv3** window in the Cisco APIC-EM GUI. The SNMP values that you configure for SNMPv3 for the controller must match the SNMPv3 values that have been configured for your network devices. You can configure up to five SNMPv3 settings.

***Figure 4: Configuring SNMPv3***




SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network. The different versions of SNMP are SNMPv1, SNMPv2, SNMPv2c, and SNMPv3.

SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. The following are supported SNMPv3 security models:

- Message integrity—Ensures that a packet has not been tampered with in-transit.

- Authentication—Determines the message is from a valid source
- Encryption—Scrambles the packet contents to prevent it from being seen by unauthorized sources

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

The security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The various security levels that exist within a security model are as follows:

- noAuthNoPriv—Security level that does not provide authentication or encryption
- AuthNoPriv—Security level that provides authentication but does not provide encryption
- AuthPriv—Security level that provides both authentication and encryption

The following table identifies what the combinations of security models and levels mean:

***Table 7: SNMP Security Models and Levels***

| Model | Level | Authentication | Encryption | What Happens |
|---|---|---|---|---|
| v2c | noAuthNoPriv | Community String | No | Uses a community string match for authentication. |
| v3 | noAuthNoPriv | User Name | No | Uses a username match for authentication. |
| v3 | AuthNoPriv | Either:<br>• HMAC-MD5<br>• HMAC-SHA | No | Provides authentication based on the Hash-Based Message Authentication Code (HMAC) Message Digest 5 (MD5) algorithm or the HMAC Secure Hash algorithm (SHA) |

| Model | Level | Authentication | Encryption | What Happens |
|---|---|---|---|---|
| v3 | AuthPriv | Either:<br>• HMAC-MD5<br>• HMAC-SHA | Either:<br>• CBC-DES<br>• CBC-AES-128 | Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.<br>Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard or CBC-mode AES for encryption. |

### Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have your network's SNMP information available for this configuration procedure.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

**Note** With SNMPv3, passwords (or passphrases) must be at least 8 characters in length (minimum). Additionally, for several Cisco Wireless LAN controllers, passwords (or passphrases) must be at least 12 characters in length (minimum). Failure to ensure these required minimum character lengths for the passwords will result in devices not being discovered, monitored, and/or managed by the controller.

**Step 1** In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

**Step 2** Click the **Settings** link from the drop-down menu.

**Step 3** In the **Settings** navigation pane, click **SNMPv3** to view the **SNMPv3** window.

If you use SNMPv3 in your network to monitor and manage devices, then configure the SNMPv3 values for discovery for your network.

**Step 4** In the **SNMPv3** window, enter a **Username** value and choose a **Mode** from the drop down menu.

The following **Mode** options are available:

- **AuthPriv**
- **AuthNoPriv**
- **NoAuthNoPriv**

**Note** Subsequent **SNMPv3** configuration options might or might not be available depending upon your selection for this step.

**Step 5** If you selected **AuthPriv** or **AuthNoPriv** as a **Mode** option, then choose an **Authentication** type from the drop down menu and enter an authentication password.

The following **Authentication** options are available:

- **SHA**—Authentication based on the Hash-Based Message Authentication Code (HMAC), Secure Hash algorithm (SHA) algorithm
- **MD5**—Authentication based on the Hash-Based Message Authentication Code (HMAC), Message Digest 5 (MD5) algorithm

**Step 6** If you selected **AuthPriv** as a **Mode** option, then choose a **Privacy** type from the drop down menu and enter a SNMPv3 privacy password.

The SNMPv3 privacy password is used to generate the secret key used for encryption of messages exchanged with devices that support DES or AES128 encryption.

The following **Privacy** type options are available:

- **DES**—Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.
- **AES128**—Cipher Block Chaining (CBC) mode AES for encryption.

**Step 7** Click **Save** to save your SNMPv3 configuration values.

The **SNMPv3** configured values will appear in the table below.

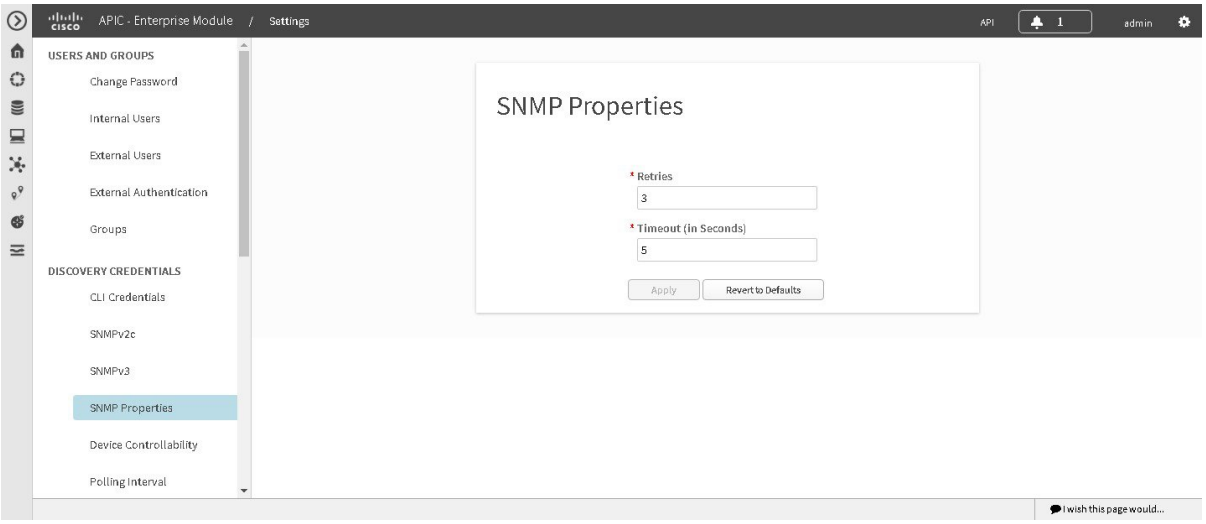
### What to do next

If required for your SNMP configuration, proceed to configure either **SNMPv2c** or **SNMP Properties** using the GUI.

## Configuring SNMP Properties

You configure SNMP properties for device discovery in the **SNMP Properties** window in the Cisco APIC-EM GUI.

*Figure 5: Configuring SNMP Properties*




### Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have your network's SNMP information available for this configuration procedure.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

**Step 1** In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

**Step 2** Click the **Settings** link from the drop-down menu.

**Step 3** In the **Settings** navigation pane, click **SNMP Properties** to view the **SNMP Properties** window.

Configure the SNMP property settings for discovery in your network.

**Step 4** In the **SNMP Properties** window, enter a value in the **Retries** field.

The value entered in this field is the number of attempts the controller attempts to use SNMP to communicate with your network devices.

**Step 5** In the **SNMP Properties** window, enter a value in the **Timeout** field.

The value entered in this field is the length of time in seconds the controller attempts to use SNMP to communicate with your network devices.

**Step 6** Click **Apply** to save your SNMP configuration values.

You can also click **Revert to Defaults** to revert to the SNMP property default values. The following are the SNMP property default values:

- **Retries**—3

- **Timeout**—5

### What to do next

If required for your SNMP configuration, proceed to configure either **SNMPv2c** or **SNMPv3** using the GUI.

# Enabling Device Controllability

You can enable device controllability in the **Device Controllability** window of the Cisco APIC-EM GUI. When you enable device controllability, the controller performs two actions during a discovery:

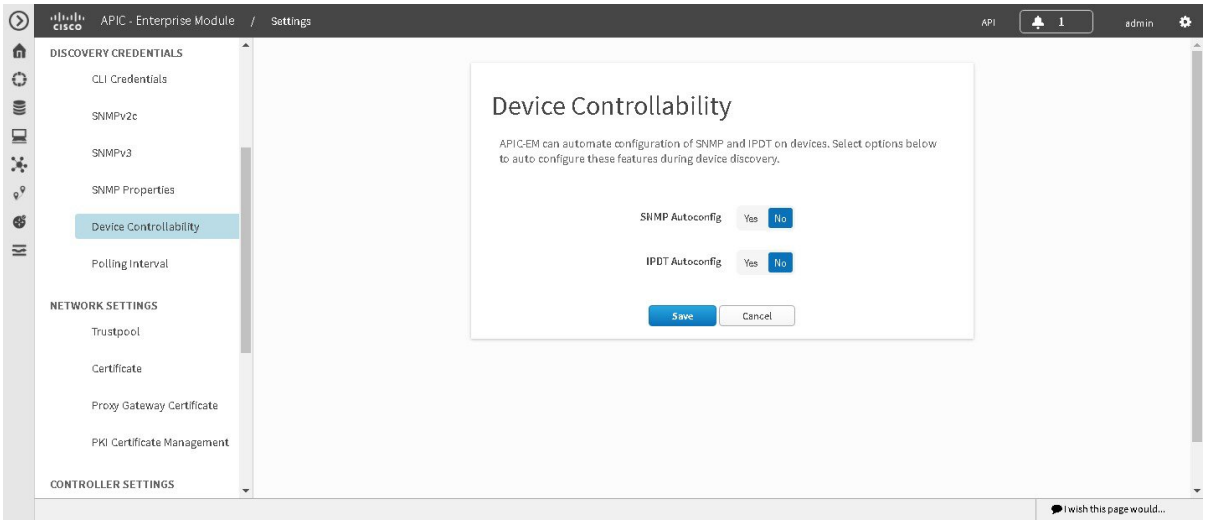
- The controller automatically configures (applies) the SNMP credentials that you entered using the controller's GUI on any network devices without SNMP credentials (SNMPv2c and/or SNMPv3).
- The controller automatically enables IP device tracking (IPDT) on any network devices where it is supported.

**Note** If you want to discover hosts through a trunk interface, you must manually enable IPDT on the trunk interface.

IPDT is enabled only on devices that are identified as Access role in **Device Inventory** window during the initial inventory collection. The device does not need to be in a **Managed** state to have IPDT enabled. The IPDT configuration is applied to devices as long as Device Inventory has the device's software version, role, and so on.

**Note** The device controllability functionality depends upon whether the CLI credentials provided by the user permits the controller to log into the device in enable mode (privilege level 15 for Cisco IOS devices).

***Figure 6: Enabling Device Controllability***



### Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

**Step 1** In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

**Step 2** Click the **Settings** link from the drop-down menu.

**Step 3** In the **Settings** navigation pane, click **Device Controllability** to view the **Device Controllability** window.

**Step 4** (Optional) Click **Yes** for **SNMP Autoconfig** to automatically to enable this feature.

Clicking **Yes** for **SNMP Autoconfig** automatically applies the SNMP credentials you configured using the controller's GUI to any devices in your network without an SNMP configuration.

**Step 5** (Optional) Click **Yes** for **IPDT Autoconfig** to enable this feature.

Clicking **Yes** for **IPDT Autoconfig** automatically enables IP device tracking (IPDT) on any devices in your network where it is supported but not enabled.

**Step 6** Click **Save** to save your configuration.

### What to do next

If you have not already done so, configure SNMP in either the **Discovery** window or the appropriate **CLI Credentials** window for SNMP in **Settings**.

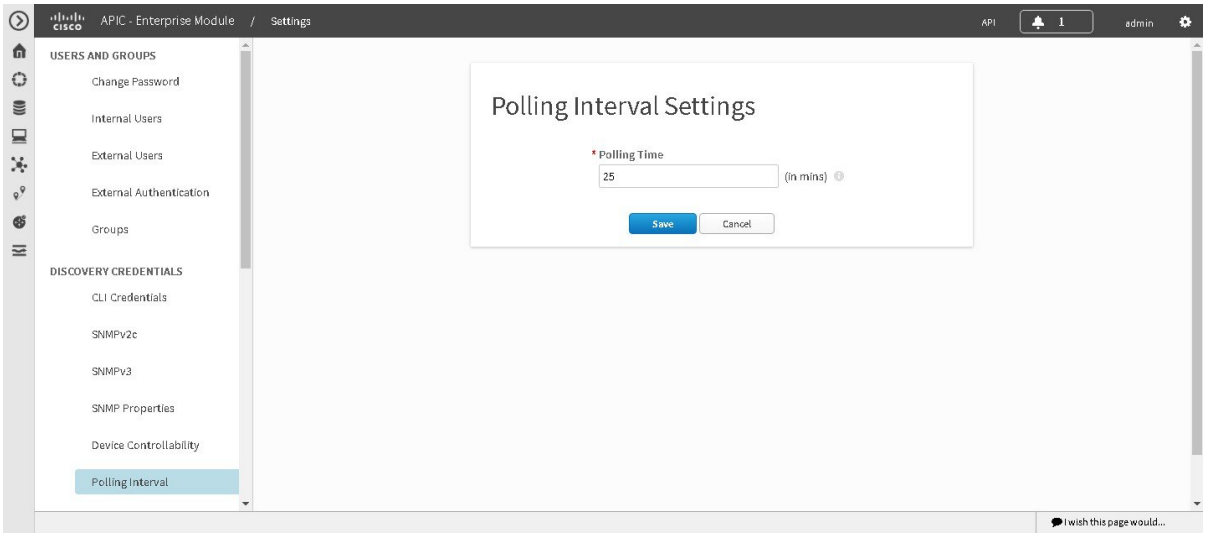
# Configuring the Polling Interval

You can configure the polling interval for inventory data collection for devices managed by Cisco APIC-EM. This polling interval configuration will be used for all managed devices, unless the polling interval of a device is updated specifically in the **Inventory** page.

You configure the polling interval in the **Polling Interval Settings** window of the Cisco APIC-EM GUI.

**Note** The polling interval value that you configure is a global value used for performing periodic inventory data collection, it is not used for discovering the device.

*Figure 7: Polling Interval Window*




### Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

**Step 1** In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

**Step 2** Click the **Settings** link from the drop-down menu.

**Step 3** In the **Settings** navigation pane, click **Polling Interval** to view the **Polling Interval** window.

**Step 4** Enter a polling interval value in minutes in the **Polling Interval** field.

The default polling interval is 25 minutes for device discovery by the controller.

**Step 5** Click **Save** to save your polling interval configuration.

# Performing Discovery

## Performing Discovery Using CDP

You can discover devices and hosts using CDP.

*Figure 8: Discovery Using CDP*

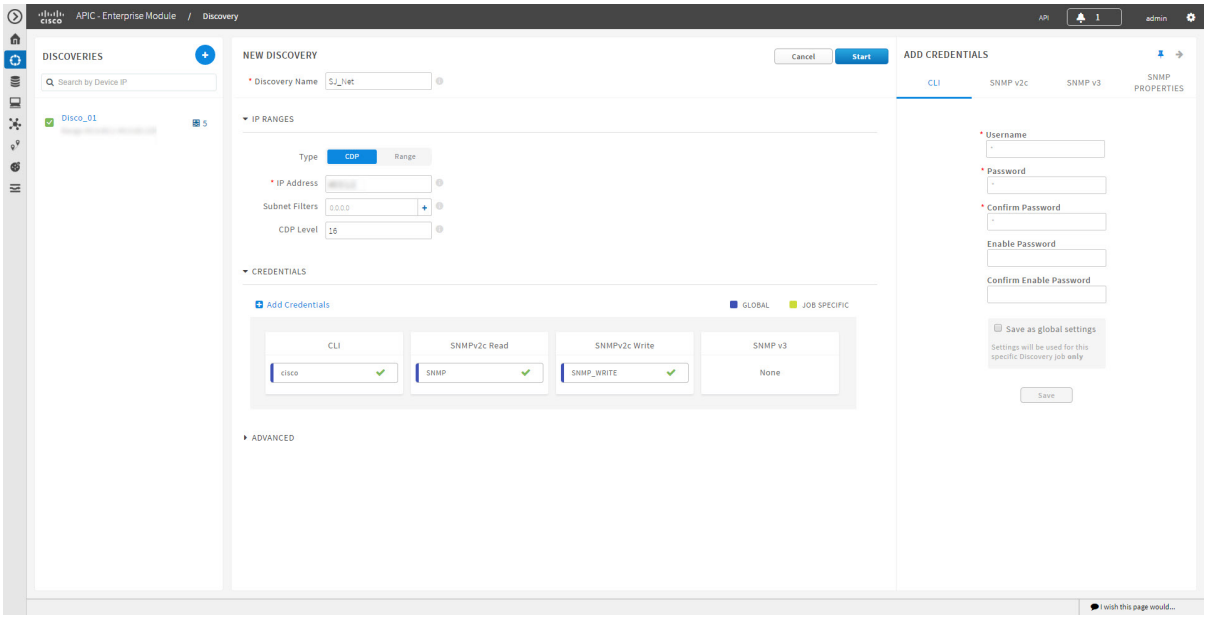
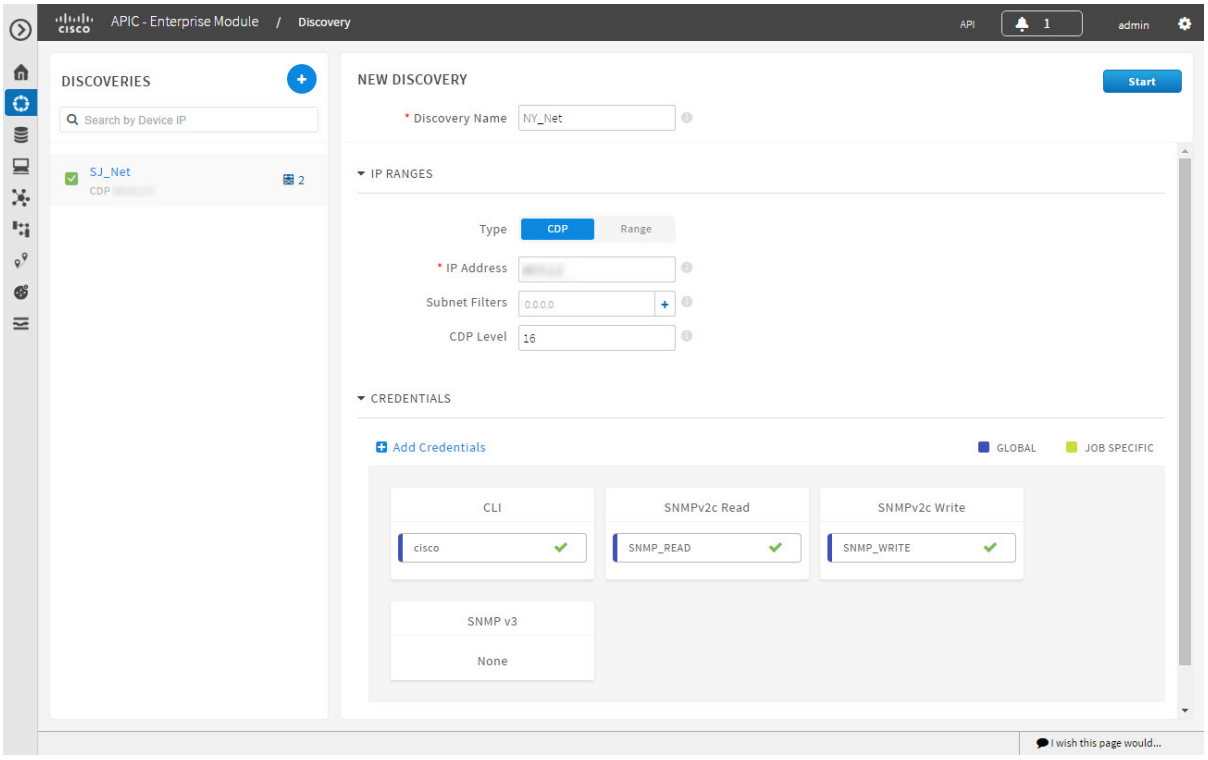



*Figure 9: Discovery Using CDP*



### Before you begin

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

CDP must be enabled on the devices in order for them to be discovered.

**Note** CDP is required for the **hostname** column to be populated.

Your devices must have the required device configurations, as described in Device Configuration Prerequisites, on page 13.

**Step 1** From the **Navigation** pane, click **Discovery**.

**Step 2** From the **Discovery** window, click **+ New Discovery**.

The **New Discovery** pane appears.

**Step 3** In the **Discovery Name** field, enter a unique name for the discovery job.

**Step 4** In the **IP Ranges** area, configure the following settings:

a) In the **Type** field, choose **CDP**.

b) In the **IP Address** field, enter a seed IP address for the Cisco APIC-EM to use to start the discovery scan.

c) (Optional) In the **Subnet Filter** field, enter the IP address or subnet and click + the plus sign..

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

Repeat this step to exclude multiple subnets from the discovery job.

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

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

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

You can configure credentials to be used for the current discovery job, or you can check the **Save as global settings** checkbox to save the credentials for future discovery jobs.

a) Make sure that any global credentials that you want to use are checked. If you do not want to use a credential, remove it by clicking the check mark.

b) To add additional credentials, click **+ Add Credentials**, complete the fields in the following tables for the credentials that you want to use, and click **Add**.

With the **SNMP Autoconfig** option enabled under **Settings > Device Controllability**, Cisco APIC-EM configures devices that do not have SNMP credentials with the SNMP credentials set in Global Settings or in the specific discovery job, whichever one takes priority.

Discovery requires the correct SNMP Read Only (RO) community string. If an SNMP RO community string is not provided, as a *best effort*, discovery uses the default SNMP RO community string, "public."

**Note** CLI credentials are not required to discover hosts; hosts are discovered through the devices that they are connected to.

*Table 8: CLI Credentials*

| Field | Description |
|---|---|
| **Username** | Username that is used to log into the command line interface (CLI) of the devices in your network. |
| **Password**<br>**Confirm Password** | Password that is used to log into the CLI of the devices in your network.<br>For security reasons, you must enter the password again as confirmation.<br>Passwords are encrypted for security reasons and are not displayed in the configuration. |
| **Enable Password**<br>**Confirm Enable Password** | Password used to move to a higher privilege level in the CLI.<br>For security reasons, you must enter the enable password again as confirmation.<br>Passwords are encrypted for security reasons and are not displayed in the configuration. |

*Table 9: SNMP v2c Credentials*

| Field | Description |
|---|---|
| **Read** | SNMP read-only (RO) community string configuration, which comprises the following fields:<br>• **Name/Description**—Name or description of the SNMP v2c settings that you are adding.<br>• **Read Community** and **Confirm Read Community**—Read-only community string password used only to view SNMP information on the device.<br>**Note** Passwords are encrypted for security reasons and are not displayed in the configuration.<br>**Note** To enable discovery on the network devices, configure the network device's IP host address as the client address. |
| **Write** | SNMP read-write (RW) community string configuration, which comprises the following fields:<br>• **Name/Description**—Name or description of the SNMP v2c settings that you are adding.<br>• **Write Community** and **Confirm Write Community**—Read/Write community string password used to view and make changes to SNMP information on the device.<br>**Note** Passwords are encrypted for security reasons and are not displayed in the configuration.<br>**Note** To enable discovery on the network devices, configure the network device's host IP address as the client IP address. |

*Table 10: SNMP v3 Credentials*

| Field | Description |
|---|---|
| **Username** | Username associated with the SNMPv3 settings. |
| **Mode** | Specifies the security level that an SNMP message requires and whether the message needs to be authenticated. Choose one of the following modes:<br>• noAuthNoPriv—Security level that does not provide authentication or encryption<br>• AuthNoPriv—Security level that provides authentication but does not provide encryption<br>• AuthPriv—Security level that provides both authentication and encryption |
| **Auth Password** | SNMPv3 password used for gaining access to information from devices that use SNMPv3.<br>**Note** Passwords are encrypted for security reasons and are not displayed in the configuration. |
| **Auth Type** | Specifies the authentication type to be used.<br>• **SHA**—Authentication based on the Hash-Based Message Authentication Code (HMAC), Secure Hash algorithm (SHA) algorithm<br>• **MD5**—Authentication based on the Hash-Based Message Authentication Code (HMAC), Message Digest 5 (MD5) algorithm<br>• **None**—No authentication |
| **Privacy Password** | SNMPv3 privacy password is used to generate the secret key used for encryption of messages exchanged with devices that support DES or AES128 encryption.<br>**Note** Passwords are encrypted for security reasons and are not displayed in the configuration. |
| **Privacy Type** | Specifies the privacy type:<br>• **DES**—Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.<br>• **AES128**—Cipher Block Chaining (CBC) mode AES for encryption.<br>• **None**—No privacy |

*Table 11: SNMP Properties*

| Field | Description |
|---|---|
| **Retries** | Number of attempts to connect to the device. Valid values are from 0 to 4 attempts. |
| **Timeout (in Seconds)** | Number of seconds the controller waits when trying to establish a connection with a device before timing out. Valid values are from 5 to 120 seconds in intervals of 5 seconds. |

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

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

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

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

**Step 7** Click **Start Discovery**.

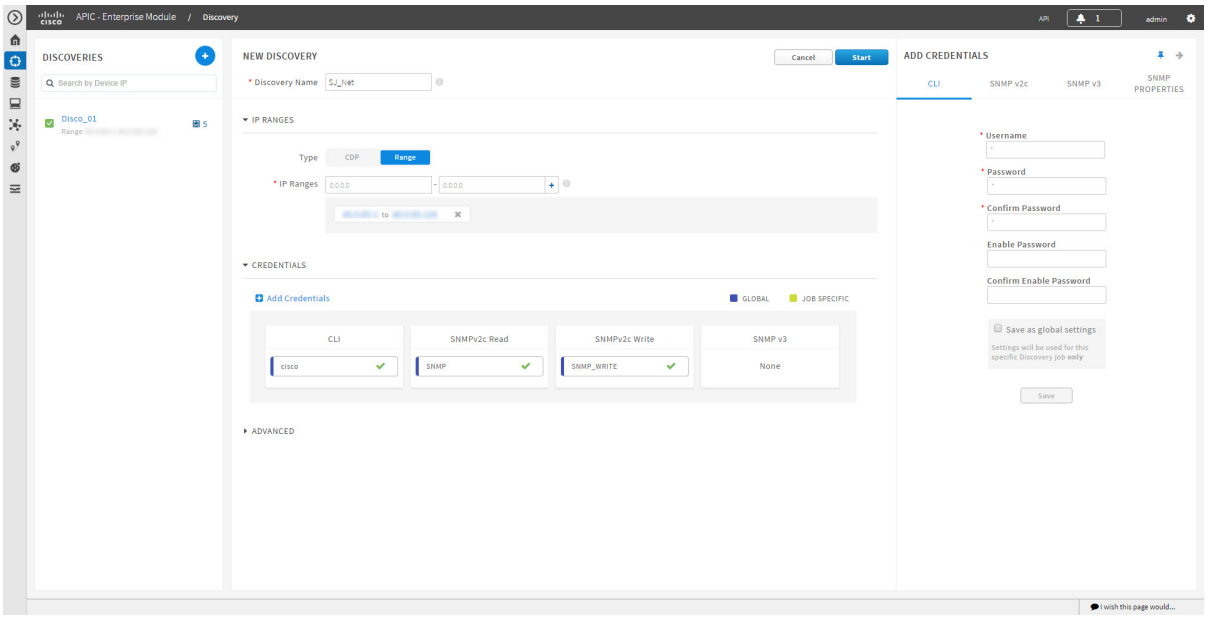
The **Discoveries** window displays the results of your scan.

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

# Performing Discovery Using an IP Address Range

You can discover devices using an IP address range.

***Figure 10: Discovery Using IP Address Range***




### Before you begin

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

Your devices must have the required device configurations, as described in Device Configuration Prerequisites, on page 13.

**Step 1** From the **Navigation** pane, click **Discovery**.

**Step 2** From the **Discovery** window, click + **New Discovery**.

The **New Discovery** pane appears.

**Step 3** In the **Discovery Name** field, enter a unique name for the discovery job.

**Step 4** If the **Discovery Details** pane does not appear, click **Add New**.

**Step 5** In the **Discovery Name** field, enter a unique name for this discovery.

**Step 6** In the **IP Ranges** area, do the following:

a) From the **Discovery Type** field, choose **Range** for the discovery scan type.

b) In the **IP Address** field, enter the beginning and ending IP addresses (IP range) for the devices being discovered and click + (the plus sign).

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

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

**Step 7** Open the **Credentials** area and configure the credentials that you want to use for the discovery job.

You can configure credentials to be used for the current discovery job, or you can check the **Save as global settings** checkbox to save the credentials for future discovery jobs.

a) Make sure that any global credentials that you want to use are checked. If you do not want to use a credential, remove it by clicking the check mark.

b) To add additional credentials, click **+ Add Credentials**, complete the fields in the following tables for the credentials that you want to use, and click **Save**.

With the **SNMP Autoconfig** option enabled under **Settings > Device Controllability**, Cisco APIC-EM configures devices that do not have SNMP credentials with the SNMP credentials set in Global Settings or in the specific discovery job, whichever one takes priority.

Discovery requires the correct SNMP Read Only (RO) community string. If an SNMP RO community string is not provided, as a *best effort*, discovery uses the default SNMP RO community string, "public."

**Note** CLI credentials are not required to discover hosts; hosts are discovered through the devices that they are connected to.

***Table 12: CLI Credentials***

| Field | Description |
|---|---|
| **Username** | Username that is used to log into the command line interface (CLI) of the devices in your network. |
| **Password**<br>**Confirm Password** | Password that is used to log into the CLI of the devices in your network.<br>For security reasons, you must enter the password again as confirmation.<br>Passwords are encrypted for security reasons and are not displayed in the configuration. |
| **Enable Password**<br>**Confirm Enable Password** | Password used to move to a higher privilege level in the CLI.<br>For security reasons, you must enter the enable password again as confirmation.<br>Passwords are encrypted for security reasons and are not displayed in the configuration. |

*Table 13: SNMP v2c Credentials*

| Field | Description |
|---|---|
| **Read** | SNMP read-only (RO) community string configuration, which comprises the following fields:<br>• **Name/Description**—Name or description of the SNMP v2c settings that you are adding.<br>• **Read Community** and **Confirm Read Community**—Read-only community string used only to view SNMP information on the device.<br>**Note** Passwords are encrypted for security reasons and are not displayed in the configuration.<br>**Note** To enable discovery on the network devices, configure the network device's IP host address as the client address. |
| **Write** | SNMP read-write (RW) community string configuration, which comprises the following fields:<br>• **Name/Description**—Name or description of the SNMP v2c settings that you are adding.<br>• **Write Community** and **Confirm Write Community**—Read/Write community string used to view and make changes to SNMP information on the device.<br>**Note** Passwords are encrypted for security reasons and are not displayed in the configuration.<br>**Note** To enable discovery on the network devices, configure the network device's IP host address as the client address. |

*Table 14: SNMP v3 Credentials*

| Field | Description |
|---|---|
| **Username** | Username associated with the SNMPv3 settings. |
| **Mode** | Specifies the security level that an SNMP message requires and whether the message needs to be authenticated. Choose one of the following modes:<br>• noAuthNoPriv—Security level that does not provide authentication or encryption<br>• AuthNoPriv—Security level that provides authentication but does not provide encryption<br>• AuthPriv—Security level that provides both authentication and encryption |
| **Auth Password** | SNMPv3 password used for gaining access to information from devices that use SNMPv3. |
| **Auth Type** | Specifies the authentication type to be used.<br>• **SHA**—Authentication based on the Hash-Based Message Authentication Code (HMAC), Secure Hash algorithm (SHA) algorithm<br>• **MD5**—Authentication based on the Hash-Based Message Authentication Code (HMAC), Message Digest 5 (MD5) algorithm<br>• **None**—No authentication |

| Field | Description |
|---|---|
| **Privacy Password** | SNMPv3 privacy password is used to generate the secret key used for encryption of messages exchanged with devices that support DES or AES128 encryption. |
| **Privacy Type** | Specifies the privacy type:<br>• **DES**—Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.<br>• **AES128**—Cipher Block Chaining (CBC) mode AES for encryption.<br>• **None**—No privacy |

*Table 15: SNMP Properties*

| Field | Description |
|---|---|
| **Retries** | Number of attempts to connect to the device. Valid values are from 0 to 4 attempts. |
| **Timeout (in Seconds)** | Number of seconds the controller waits when trying to establish a connection with a device before timing out. Valid values are from 5 to 120 seconds in intervals of 5 seconds. |

**Step 8** Click **Start Discovery**.

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

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

**Step 9** (Optional) To configure the protocols to be used to connect with devices, open the **Advanced** area and do the following:

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

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

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

# Copying a Discovery Job

You can copy a discovery job and retain all of the information defined for the job, except the SNMP and CLI credentials. The SNMP and CLI credentials are included in the copy only if you used global credentials (saved in **Settings**) for the original job. If you defined specific (one-time only) SNMP and CLI credentials for the original job, the credentials are not copied.

### Before you begin

You have created at least one discovery scan.

**Step 1** From the **Navigation** pane, click **Discovery**.

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

**Step 3** From the **Discovery Details** pane, click **Copy**.

The discovery job is copied, and the new job is named Copy of *Discovery_Job*.

**Step 4** (Optional) Change the name of the discovery job.

**Step 5** Define or update the SNMP and CLI credentials and any other parameters for the discovery job.

# Stopping and Starting a Discovery Job

You can stop a discovery job that is in progress, and restart it.

### 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 **Discovery**.

**Step 2** To stop an active discovery job, do the following:

a) From the **Discoveries** pane, select the discovery job.
b) From the **Discovery Details** pane, click **Stop**.
c) Click **OK** to confirm that you want to stop the discovery job.

**Step 3** To restart an inactive discovery, do the following:

a) From the **Discoveries** pane, select the discovery job.
b) From the **Discovery Details** pane, click **Start**.

# Deleting a Discovery Job

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

### 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 **Discovery**.

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

**Step 3** From the **Discovery Details** pane, click **Delete**.

**Step 4** Click **OK** to confirm that you want to delete the discovery.

# Understanding the Discovery Results

The **Discovery Results** pane provides information about the selected scan.

To access the **Discovery Results** pane, do the following:

1. From the **Navigation** pane, click **Discovery**.
2. From the **Discoveries** pane, select the discovery job that you want to display.

The **Discovery Results** pane appears. See the following figures and table for information.

***Figure 11: Discovery Results Window—List***

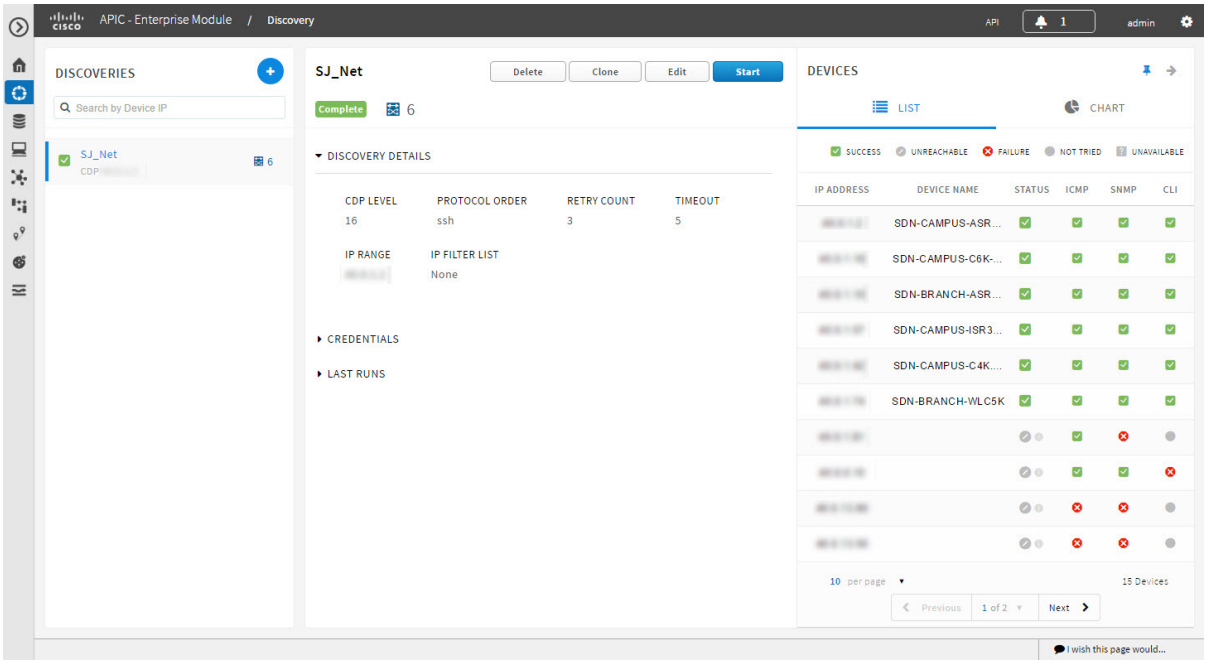


*Figure 12: Discovery Results Window—Chart*

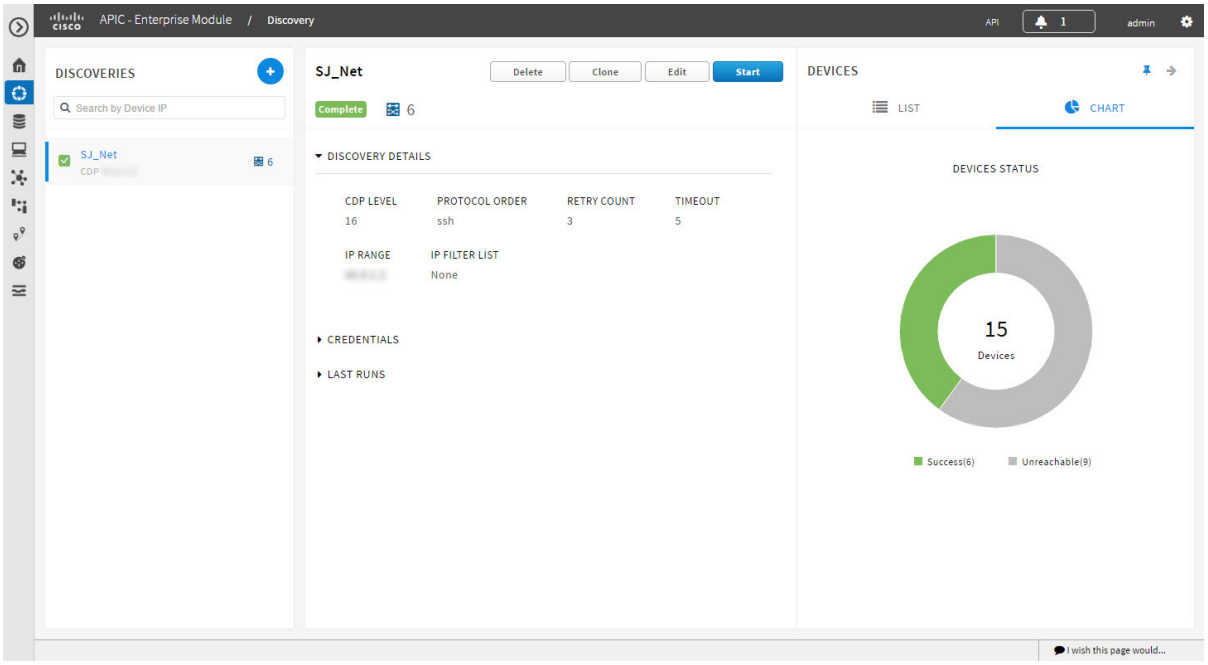
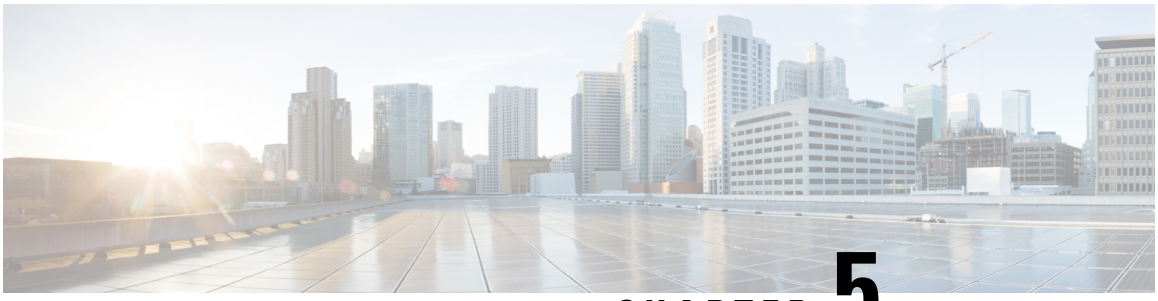



*Table 16: Discovery Pane*

| Name | Description |
|---|---|
| Discovery Identification and Action Area | Displays the following information:<br>• Name of the discovery job.<br>• Status of the discovery job.<br>• Number of devices discovered.<br>From this area, you can delete, clone, edit, or start a discovery job. |
| **Discovery Details** area | Open this area to display detailed information about the parameters that were used to perform the discovery, including the CDP level (if used), protocol order, retry count, timeout value, IP address (seed) or range of IP addresses used, and IP address filter list. |
| **Credentials** area | Open this area to display the credentials used in the discovery job and identifies them as either global or job-specific. |
| **Last Runs** area | Open this area to display a table showing information about each iteration of the discovery job, including the job number, its status, an option to view the devices discovered, and the duration of the job. Clicking the **View** link in the **Devices** column opens the **Devices** pane. |

| Name | Description |
|---|---|
| **Devices** pane | (Shown when you open the **Last Runs** area and click the **View** link in the **Devices** column.)<br>The devices pane displays the results of the device discovery in two forms:<br>• **List**—For each device, provides the following information:<br>  • **IP address**—IP addresses of the devices that Cisco APIC-EM discovered or attempted to discover.<br>  • **Device name**—Name of the device, if available.<br>  • **Status**—Status of the discovery for the device. Possible states are success, unreachable, failure, not tried, or unavailable.<br>  • **Internet Control Message Protocol (ICMP)**—Status of the ICMP for the device.<br>  • **SNMP**—Status of theCisco APIC-EM's use of the SNMP settings to gather SNMP information from the device.<br>  • **CLI**—Status of theCisco APIC-EM's use of the CLI username and passwords to gather information from the device.<br>• **Chart**—Displays a circle graph showing the proportional representation of successful versus failed discovered devices. |



CHAPTER 5

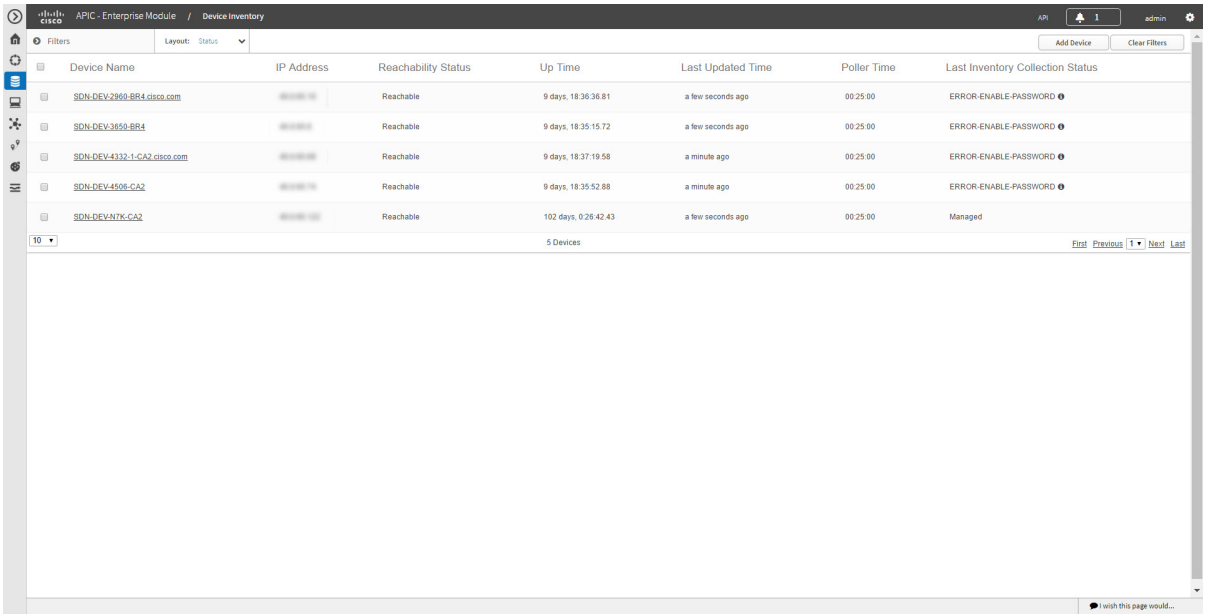
# Managing Devices and Hosts



# 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 13: Device Inventory Window***




**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 54.

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.<br>When you select a device, the action buttons appear above the **Device Inventory** table. For information about these buttons and the actions that you can perform with them, see Device Inventory Tasks, on page 54. |
| **Filters** | Allows you to refine the list of devices that are displayed in the table by name, location tag, and IP address.<br>To remove filters, click **Clear Filters**. |
| **Layout** | Allows you to choose from three predefined layouts or a customized layout:<br>• **Status**—Layout shows the device name, IP address, state of the device, how long it has been up, and the last time it was updated.<br>• **Hardware**—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.<br>• **Tagging**—Layout shows the device name, IP address, MAC address, device role, location, and tags.<br>• **Customize**—Layout shows the information in the columns that you have selected to display.<br>For descriptions of the columns of information that you can display, see the Device Inventory Information table below. |

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 17: Device Inventory Information*

| Column Name | Description |
|---|---|
| **Device Status** | State of the device.<br>• **Connecting**—Controller is connecting to the device.<br>• **Reachable**:<br>  • Discovered—Controller has connected to the device and is able to execute Cisco commands using the CLI .<br>  • Failure—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.<br>• **Authentication Failed**—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.<br>• **Unreachable**—Controller is unable to connect to the device.<br>**Note** 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. |

| Column Name | Description |
|---|---|
| **Device Name** | Name of the device. Click the device name to display the **Device Overview** dialog box with the following information:<br>• Device serial number<br>• Device IP address<br>• MAC address<br>• Cisco OS version<br>• Up time<br>• Product ID<br>• Vendor<br>• Memory size<br>**Note** The device name appears red for any device whose inventory has not been updated for more than 30 minutes.<br>The **Device Overview** dialog box also includes an **Interfaces** tab with the following interface data:<br>• Status—Up or down<br>• Interface name—Name of the interface.<br>• MAC address—MAC address of the interface. |
| **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** | Click **View** to display detailed configuration information similar to the CLI **show running-config** command output.<br>**Note** This feature is not supported for access points and wireless LAN controllers, therefore configuration data is not returned for these device types. |

| Column Name | Description |
|---|---|
| **Device Role** | Role assigned to each discovered device during the scan process. The device role is used to identify and group devices according to their responsibilities and placement within the network. If the controller is unable to determine a device role, it sets the device role as unknown.<br>**Note** 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.<br>If desired, you can use the drop-down list in this column to change the assigned device role. The following device roles are available:<br>• Unknown<br>• Access<br>• Core<br>• Distribution<br>• Border Router |

| Column Name | Description |
|---|---|
| **Location** | 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 **Device Inventory** window and **Topology** window support location tags.<br><br>Use the following guidelines when creating location tags:<br><br>• Location tag information is maintained on the controller only and not deployed to or dirived from the device itself.<br><br>• A location defined on the controller is not the "civic-location" property that some devices support.<br><br>• You cannot create, use, or search for location tags in the **Topology** window.<br><br>• Location tags cannot be attached to hosts.<br><br>• You can apply only one location tag to a device. However, you can use both a location tag and a device tag together.<br><br>For information about adding location tags, see Adding or Removing Location Tags, on page 64.<br><br>Along with the location tag, you can add a geographical marker on a world map to a device. For information, see Adding or Changing a Location Marker, on page 66. |
| **Device Tag** | 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.<br><br>A number in the **Tag** column indicates how many tags have been applied to that device.<br><br>**Note** You are permitted to use both a location tag and a device tag together.<br><br>For information about adding or removing device tags, see Adding or Removing a Device Tag in Device Inventory, on page 62.<br><br>For information about deleting a tag from the controller database, see Deleting a Tag, on page 67. |

| Column Name | Description |
|---|---|
| **Policy Tag** | Tag applied to a group of devices that will share the same policy.<br>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 *Cisco EasyQoS Application for APIC-EM User Guide*. |
| **Last Updated Time** | Date and time that the device was last scanned and the controller database was updated. |
| **Device Family** | Group of related devices, as follows:<br>• Cisco Interfaces and Modules<br>• Routers<br>• Switches and Hubs<br>• Third Party Device<br>• Unsupported Cisco Device<br>• Wireless Controller |
| **Device Series** | Series number of the device, for example, Cisco Catalyst 4500 Series Switches. |
| **Last Inventory Collection Status** | Status of the last discovery scan for the device:<br>• **Managed**—Device is in a fully managed state.<br>• **Partial Collection Failure**—Device is in a partial collected state and not all the inventory information has been collected. Move the cursor over the **Information** (i) icon to display additional information about the failure.<br>• **Unreachable**—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.<br>• **Wrong Credentials**—If the device credentials are changed after adding the device to the inventory, this condition is noted.<br>• **In Progress**—Inventory collection is occurring. |

# 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.

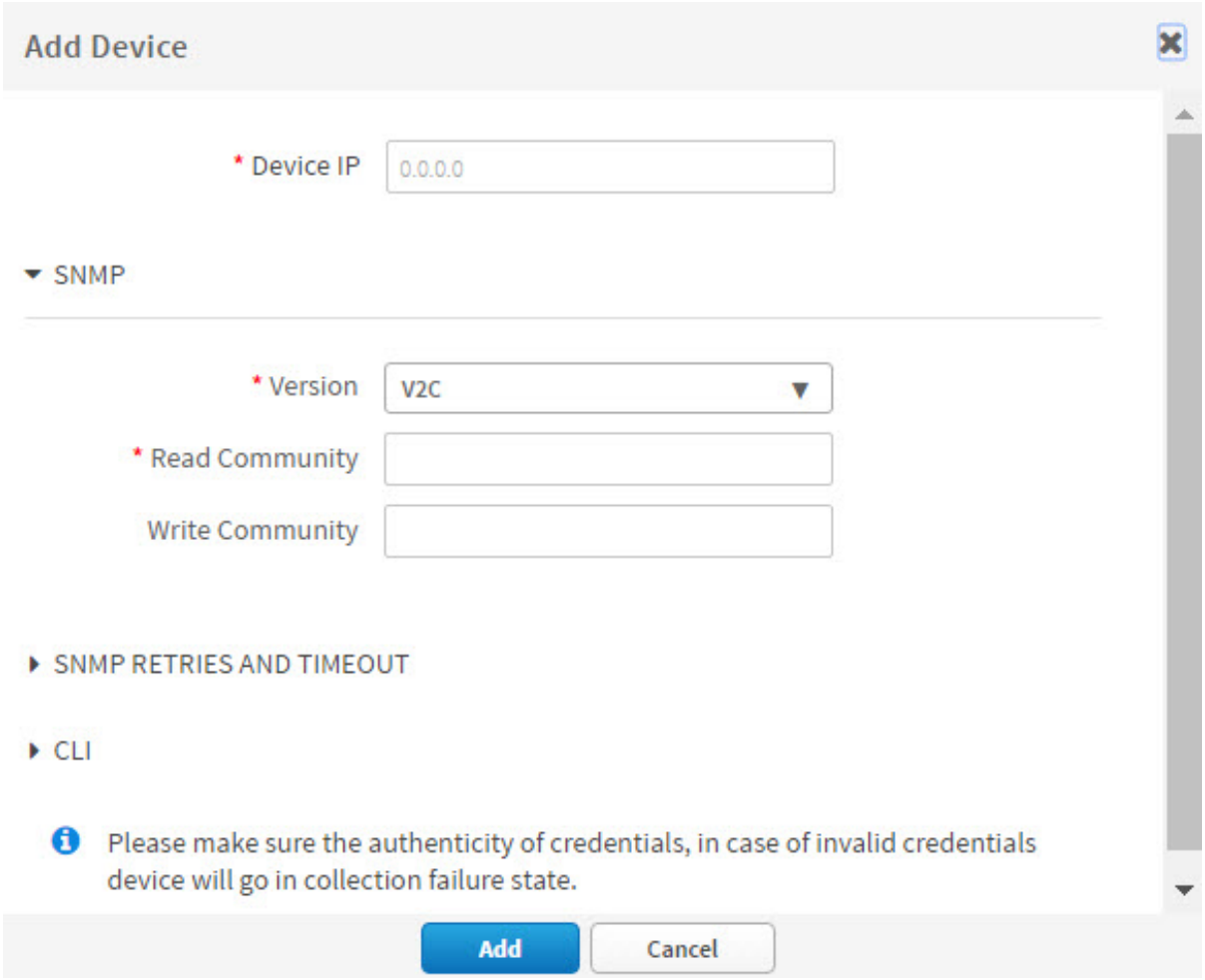
***Table 18: Device Inventory Buttons***

| Button | Action |
|---|---|
| **Add Device** | 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 Adding a Device Manually, on page 55. |
| **Set Location** | Sets the location of the devices associated with a location tag on a geographical map. For information, see Adding or Changing a Location Marker, on page 66. |
| **Set Device Tags** | Groups devices according to common attributes. For information, see Adding or Removing a Device Tag in Device Inventory, on page 62. |
| **Set Policy Tag** | Groups devices so that you can deploy the same QoS policy to those devices at the same time. For information, see Adding or Removing a Policy Tag in Device Inventory, on page 63. |
| **Delete** | Deletes the selected devices from inventory. For information, see Deleting a Device, on page 57. |
| **Update Credentials** | 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 Updating Device Credentials, on page 68 |
| **Update Polling Interval** | 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 Updating a Device's Polling Interval, on page 72. |
| **Resync** (Resynchronize Devices) | Immediately polls the selected device for updated device information and status. For information, see Resynchronizing Device Information, on page 71. |
| **Command Runner** | Sends CLI commands to the selected devices using API commands. Currently, **show** and other read-only commands are permitted. For information, see Running Commands on Devices, on page 71. |

# Adding a Device Manually

You can manually add a device to your inventory.

***Figure 14: Add Device 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** 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 19: SNMP V2C Fields*

| Field | Description |
|---|---|
| **Read Community** | 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. |
| **Write Community** | 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 20: SNMP V3 Fields*

| Field | Description |
|---|---|
| **Mode** | Authentication mode to be used. Valid modes are **Authentication and Privacy**, **Authentication, No Privacy**, **No Authentication, No Privacy**. |
| **Auth. Type** | Valid only if you chose **Authentication and Privacy** or **Authentication, No Privacy**. Two authentication types are available:<br>• **SHA**—Authentication based on the Secure Hash algorithm (SHA). SHA is a hash algorithm that is used to authenticate packet data.<br>• **MD5**—Authentication based on the Message Digest 5 (MD5) algorithm. MD5 is a hash algorithm that is used to authenticate packet data. |
| **Username** | Valid only if you chose **SHA** or **MD5**.<br>Text string associated with the SNMP user and the chosen authentication type (SHA or MD5). |
| **Auth. Password** | Valid only if you chose **SHA** or **MD5**.<br>Encrypted text string stored as the SNMP user password and associated with the authentication type (SHA or MD5). |
| **Privacy Type** | Valid only if you chose **Authentication and Privacy** mode. Two privacy types are available:<br>• **DES**—Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.<br>• **AES128**—Cipher Block Chaining (CBC) mode AES for encryption. |
| **Privacy Password** | 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 21: SNMP Retries and Timeout Fields*

| Field | Description |
|---|---|
| **Retries** | Number of attempts the controller makes to communicate with the devices using SNMP. The default is 3 tries. |
| **Timeout** | 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 22: CLI Fields*

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

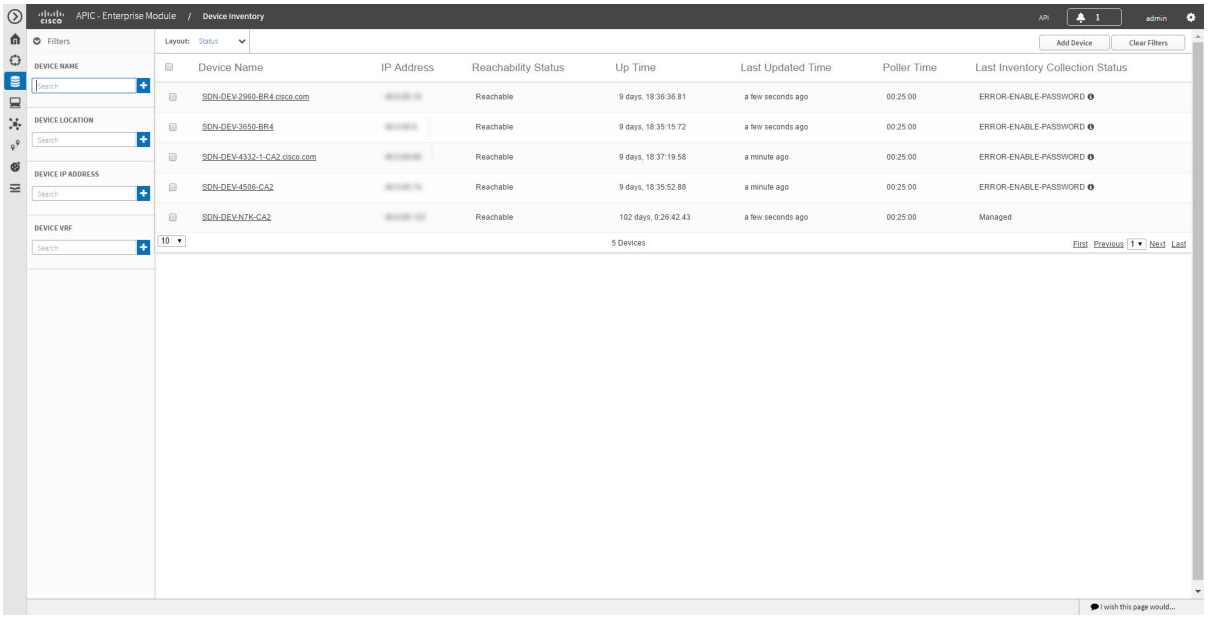
**Step 3** From the open toolbar, click **Delete**.

# 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 15: Device Inventory Window Showing Filters***




### 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.

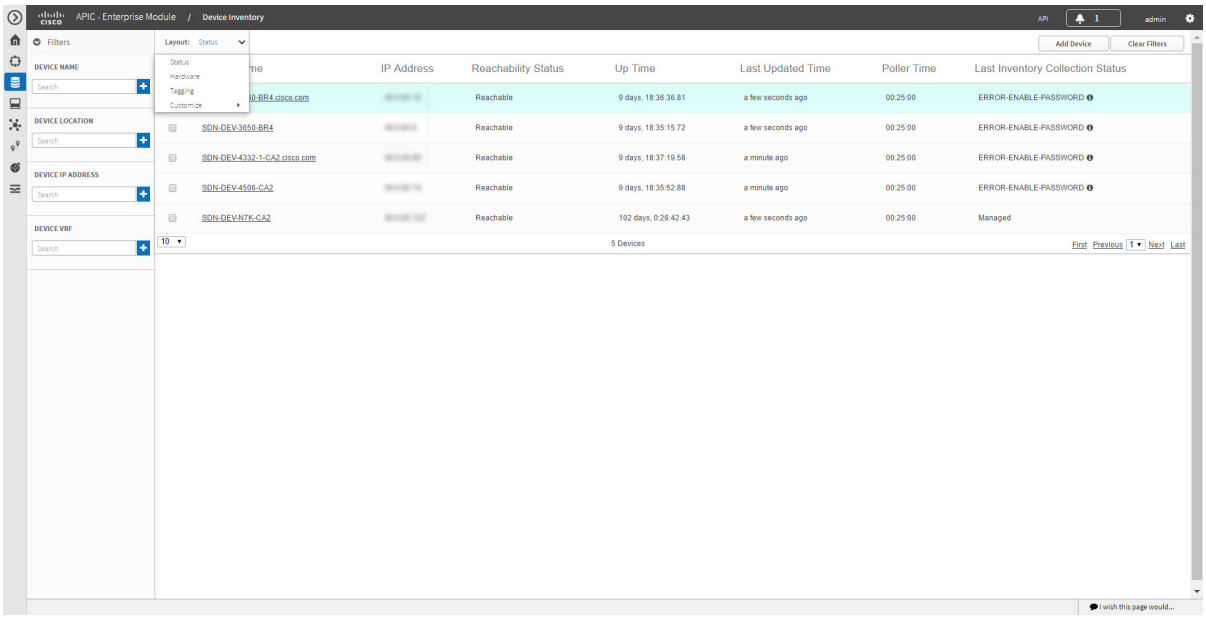
### What to do next

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 16: Device Inventory Window Showing Layout Options***



### 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.

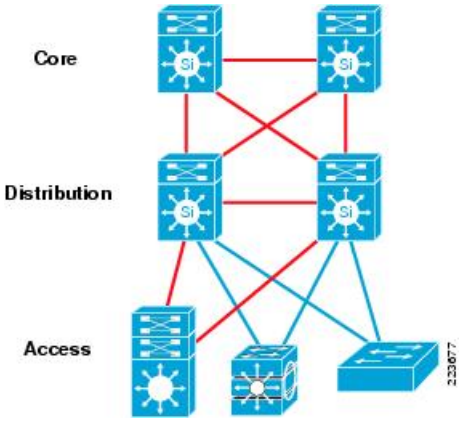
# Changing the Device Role

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 17: 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, on page 92.

### 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

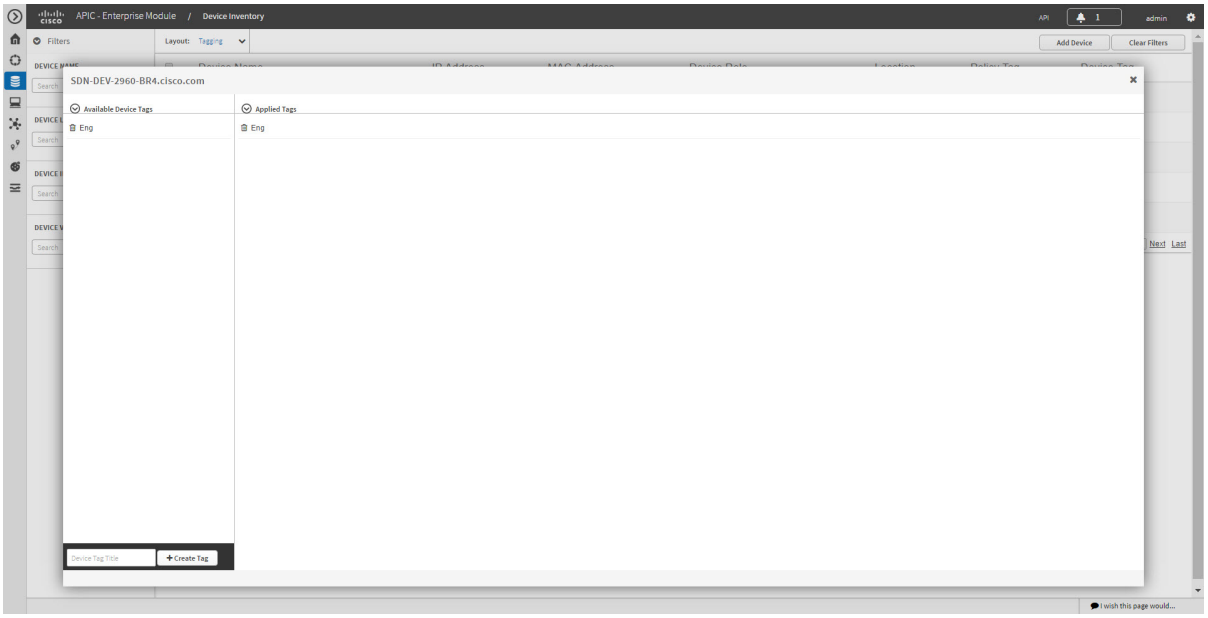
If required, change the role of other devices in the **Device Inventory** window.

# 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 63 and Adding or Removing Location Tags, on page 64.

***Figure 18: 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.

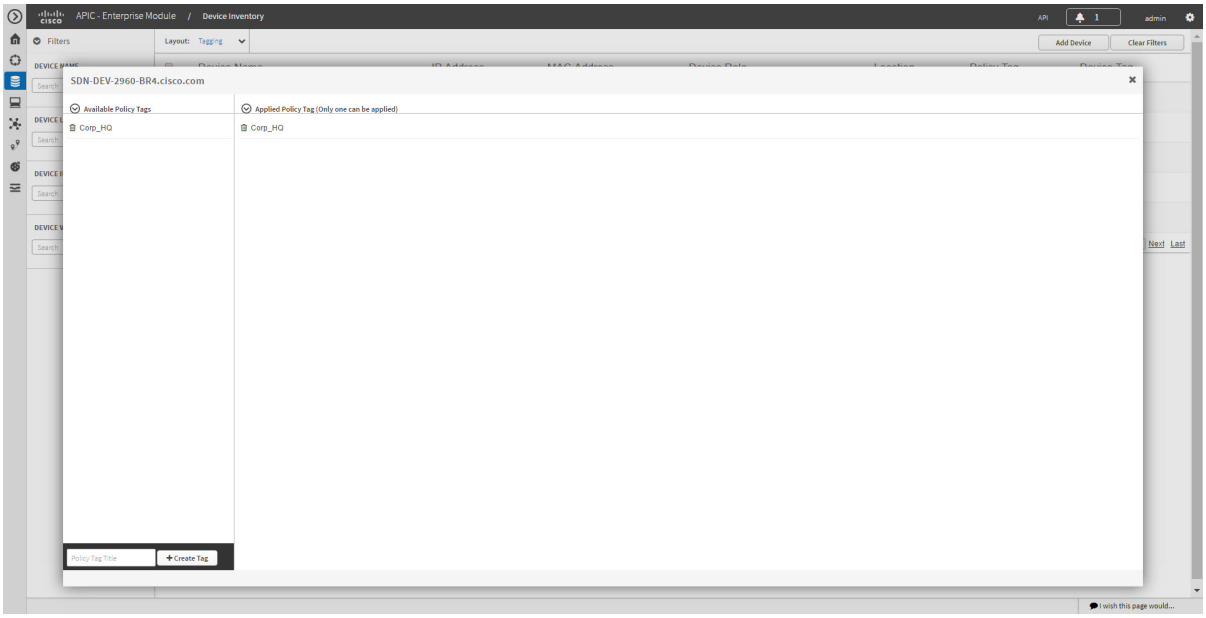
### What to do next

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 19: 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*.

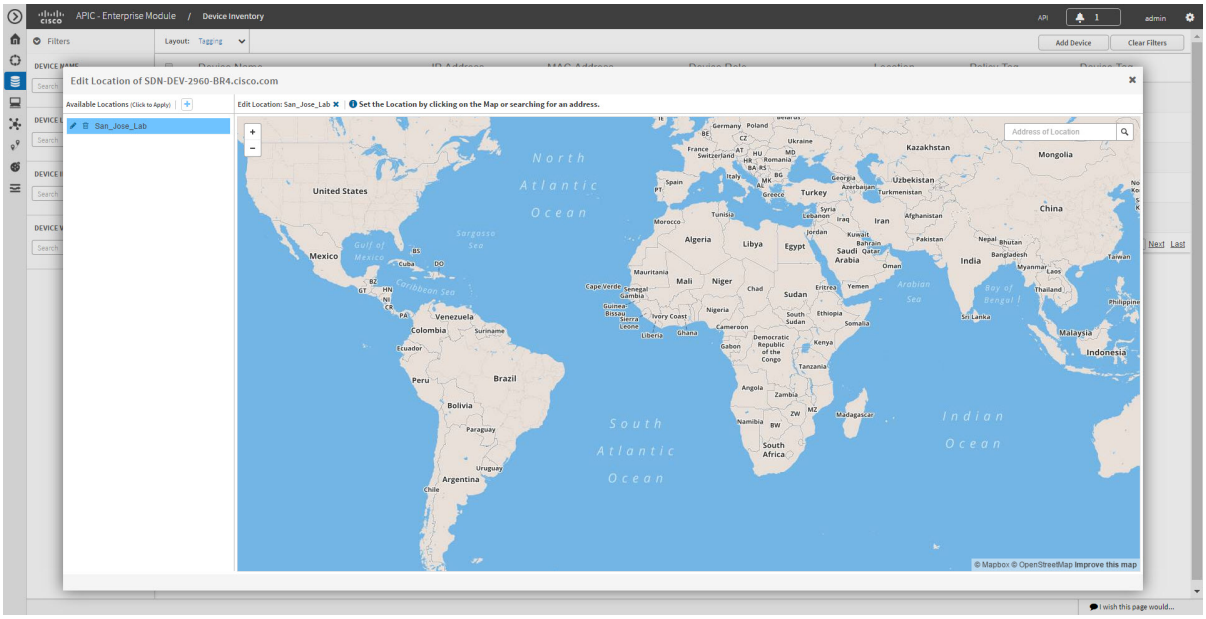
# Adding or Removing Location Tags

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 66.

Use the following guidelines when adding location tags:

- Location tag information is maintained on the controller only and not deployed to or dirived 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 20: 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 66

# 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.

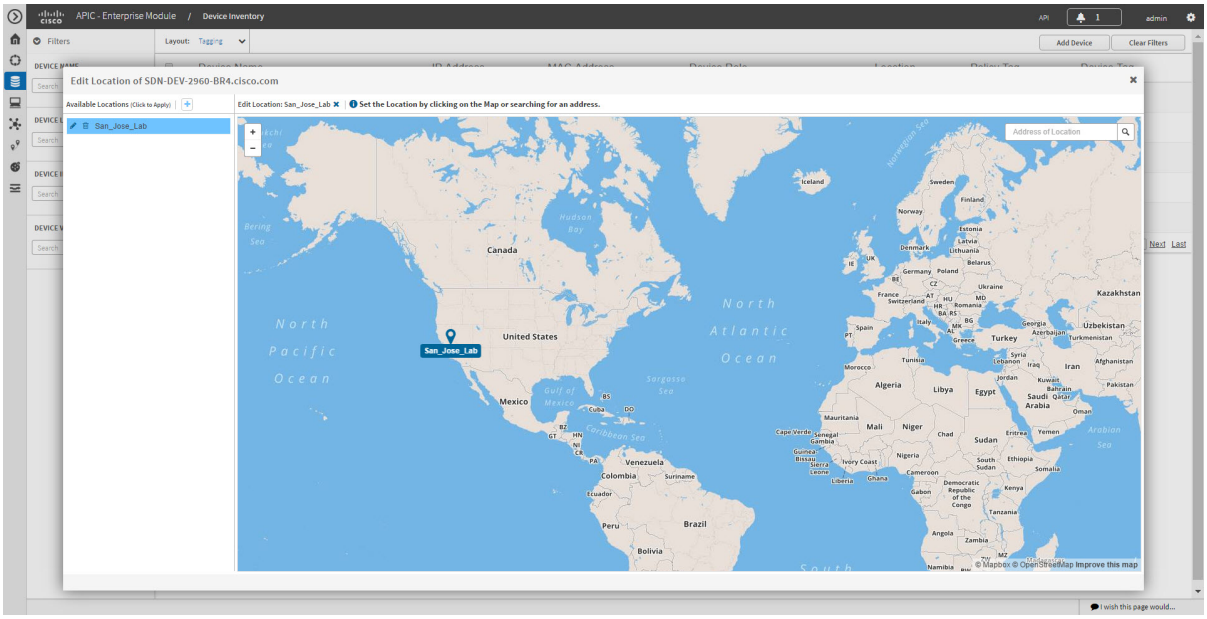
**Note** Because you are not assigning a location tag, it is not important which device you choose. When you add or remove a location marker, the change is applied to the location tag, and all devices that have the location tag will be updated.

**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 21: 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.

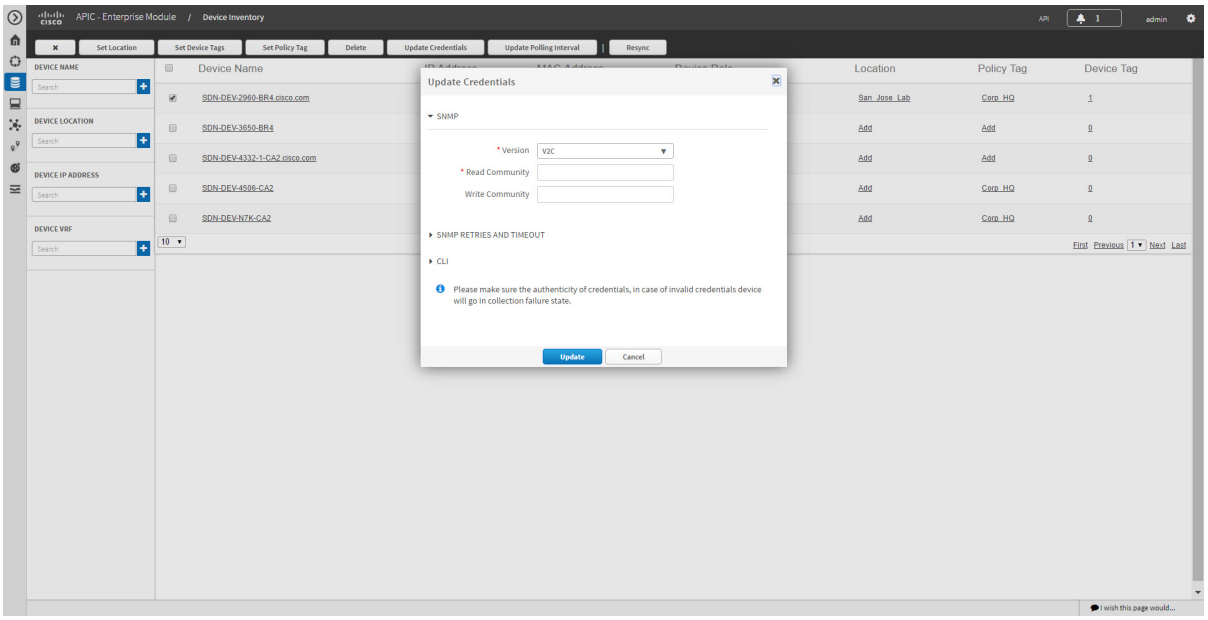
If the deletion fails, the tag might still be assigned to devices. Remove the tag from these devices and try to delete the tag again.

**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 22: 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 23: SNMP V2C Fields*

| Field | Description |
|---|---|
| **Read Community** | 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. |
| **Write Community** | 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 24: SNMP V3 Fields*

| Field | Description |
|---|---|
| **Mode** | Authentication mode to be used. Valid modes are **Authentication and Privacy**, **Authentication, No Privacy**, **No Authentication, No Privacy**. |
| **Auth. Type** | Valid only if you chose **Authentication and Privacy** or **Authentication, No Privacy**. Two authentication types are available:<br>• **SHA**—Authentication based on the Secure Hash algorithm (SHA). SHA is a hash algorithm that is used to authenticate packet data.<br>• **MD5**—Authentication based on the Message Digest 5 (MD5) algorithm. MD5 is a hash algorithm that is used to authenticate packet data. |
| **Username** | Valid only if you chose **SHA** or **MD5**.<br>Text string associated with the SNMP user and the chosen authentication type (SHA or MD5). |
| **Auth. Password** | Valid only if you chose **SHA** or **MD5**.<br>Encrypted text string stored as the SNMP user password and associated with the authentication type (SHA or MD5). |

| Field | Description |
|---|---|
| **Privacy Type** | Valid only if you chose **Authentication and Privacy** mode. Two privacy types are available:<br>• **DES**—Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.<br>• **AES128**—Cipher Block Chaining (CBC) mode AES for encryption. |
| **Privacy Password** | 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 25: SNMP Retries and Timeout Fields*

| Field | Description |
|---|---|
| **Retries** | Number of attempts the controller makes to communicate with the devices using SNMP. The default is 3 tries. |
| **Timeout** | 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 26: CLI Fields*

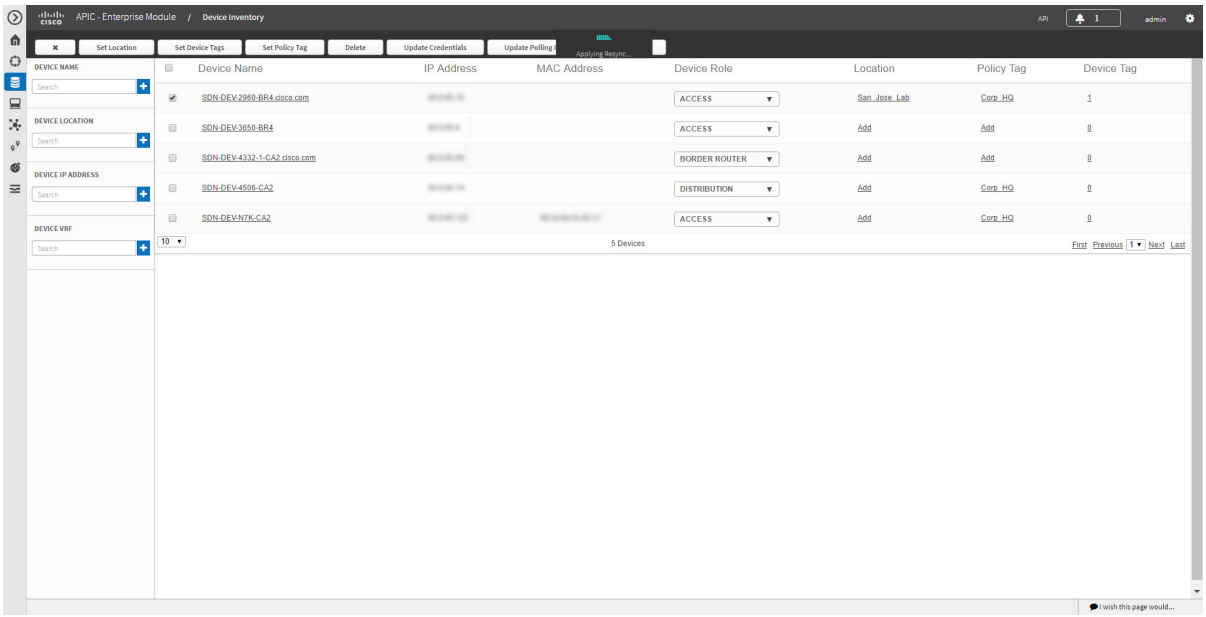
| Field | Description |
|---|---|
| **Protocol** | Protocol used from a remote management station to connect device CLI. Valid options are **Telnet** (Telnet TCP/IP) or **SSH2** (Secure Shell 2.0). |
| **Username** | Identification used to log into a device's CLI. |
| **Password** | Password used to log into a device's CLI. |
| **Enable Password** | 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 23: Device Inventory Window Showing Resync in Progress***




**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.

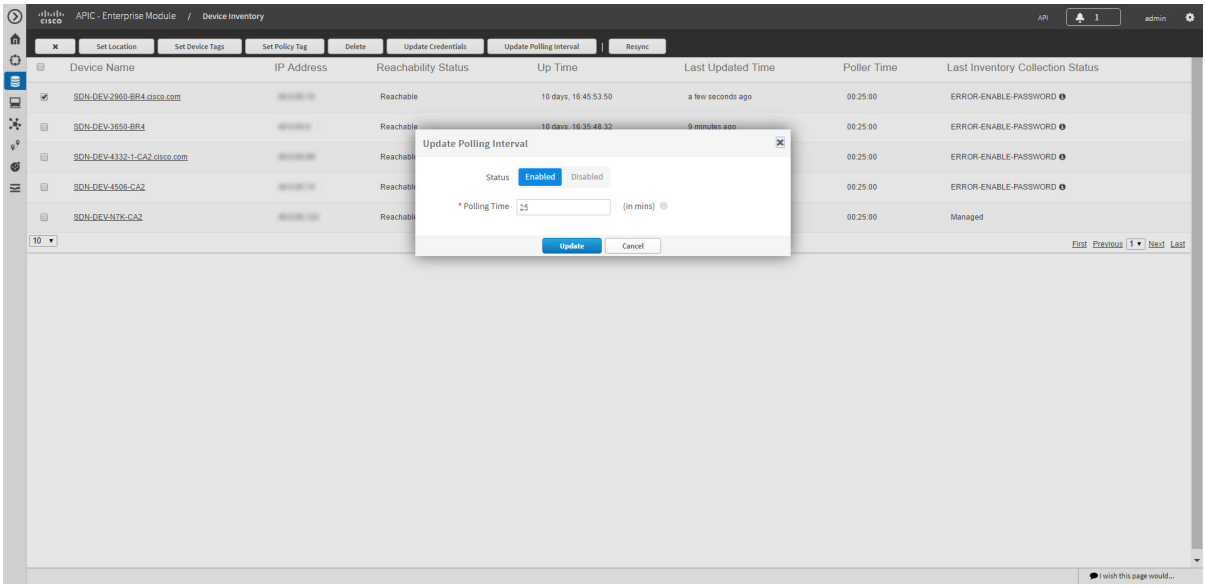
**Note** Command Runner does not maintain any cache or history of the command results. If you run commands and then close or navigate to a different window, all actions performed in command runner and their results are lost.

# 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 24: 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**.

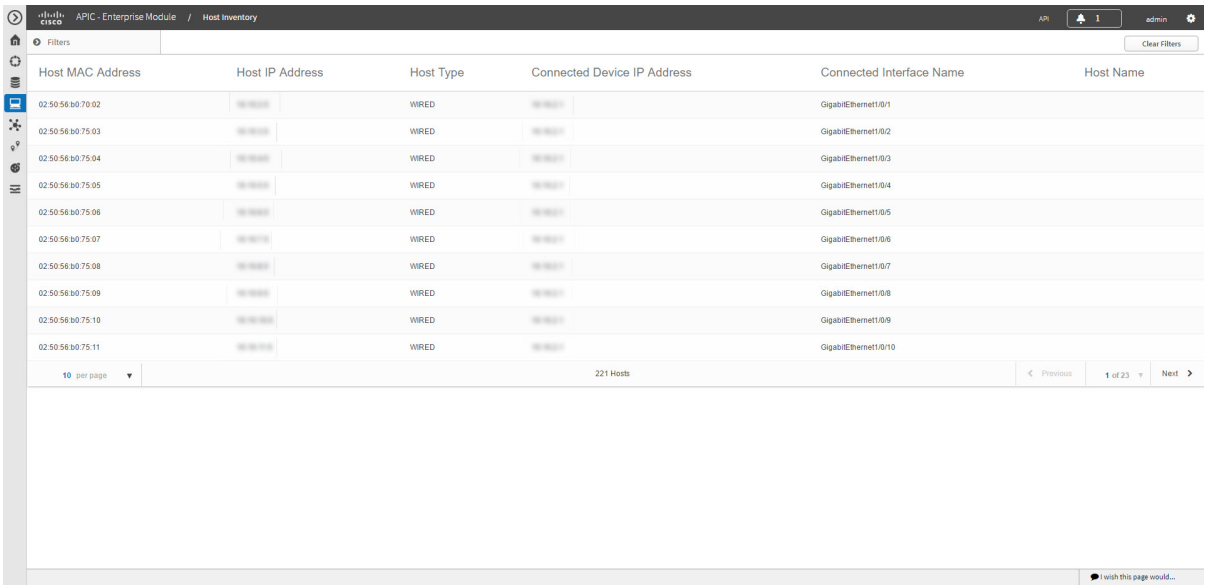
# Managing Your Host Inventory

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 25: Host Inventory Window***




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

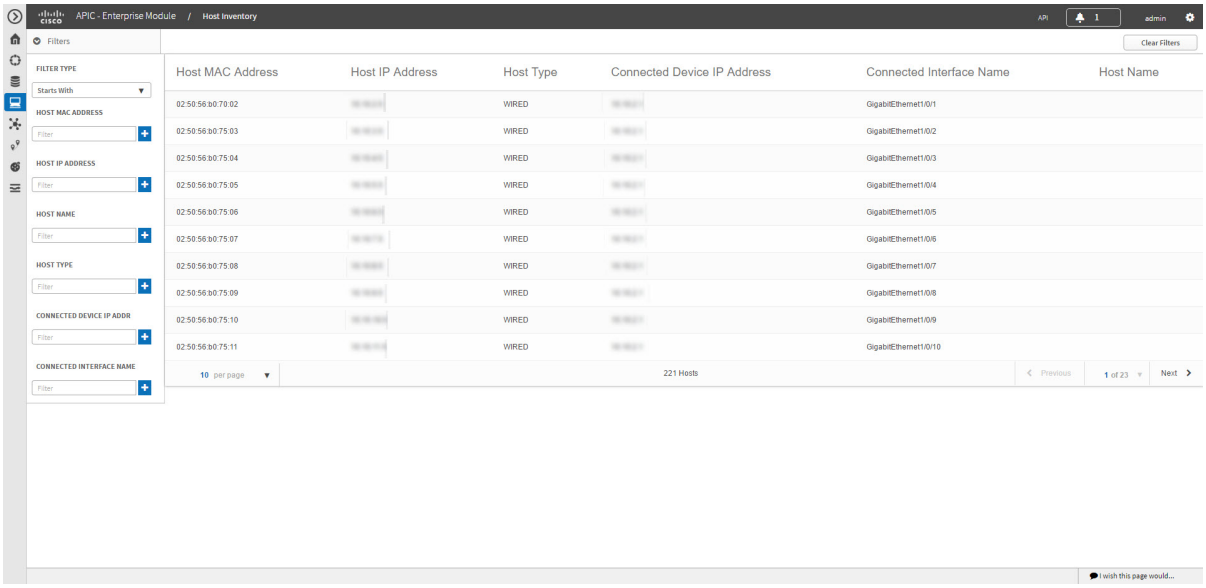
***Table 27: Host Inventory***

| 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.<br>**Note** IP addresses of only wired devices are shown. |
| 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 26: Host Inventory Window Showing Filters Pane*




### 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.

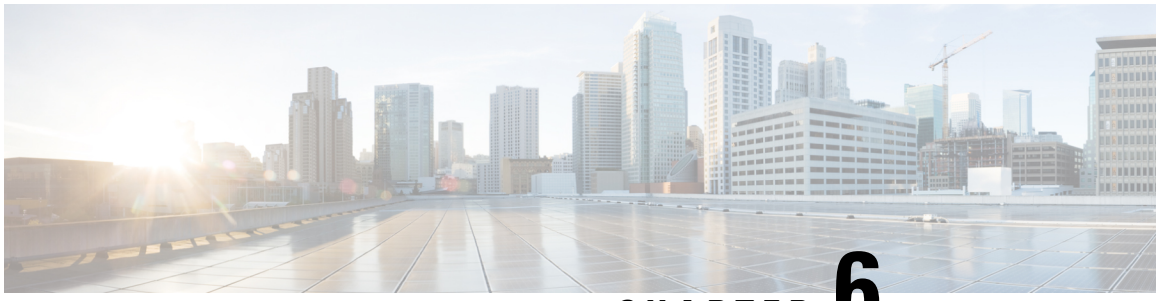
**Step 3** Click the plus (+) icon to perform the filter.

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.



CHAPTER 6

# Using the Topology Map



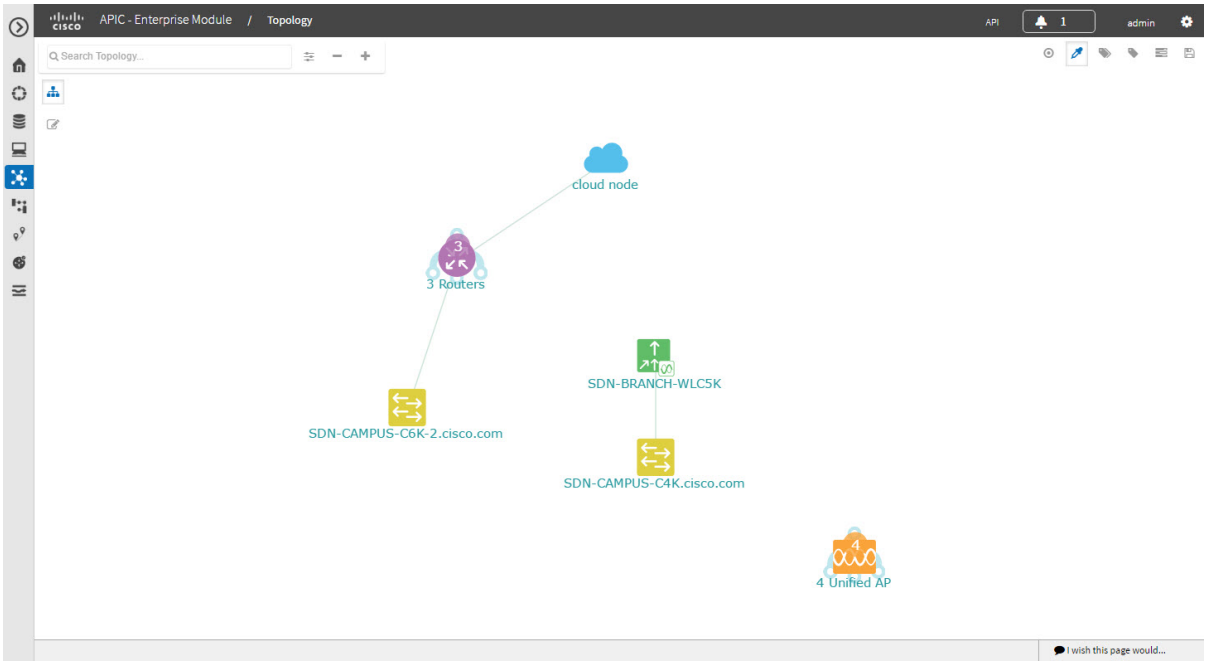
## About Topology

The **Topology** window displays a graphical view of your network. Using the discovery settings that you have configured, the Cisco APIC-EM discovers and maps devices to a physical topology with detailed device-level data.

**Note** The entire network topology is displayed. However, you will only have access to device information and functions if the device is listed in the device scope in your user profile. If the device is not in your device scope, then you will not be able to view additional information about the device, or, in the case of a user profile with ROLE_ADMIN or ROLE_POLICY_ADMIN, tag devices or change device roles.

To access the **Topology** window, from the **Navigation** pane, click **Topology**. The **Topology** window appears and displays a topology map of your network.

*Figure 27: Topology Window*




The topology map includes the following key features:

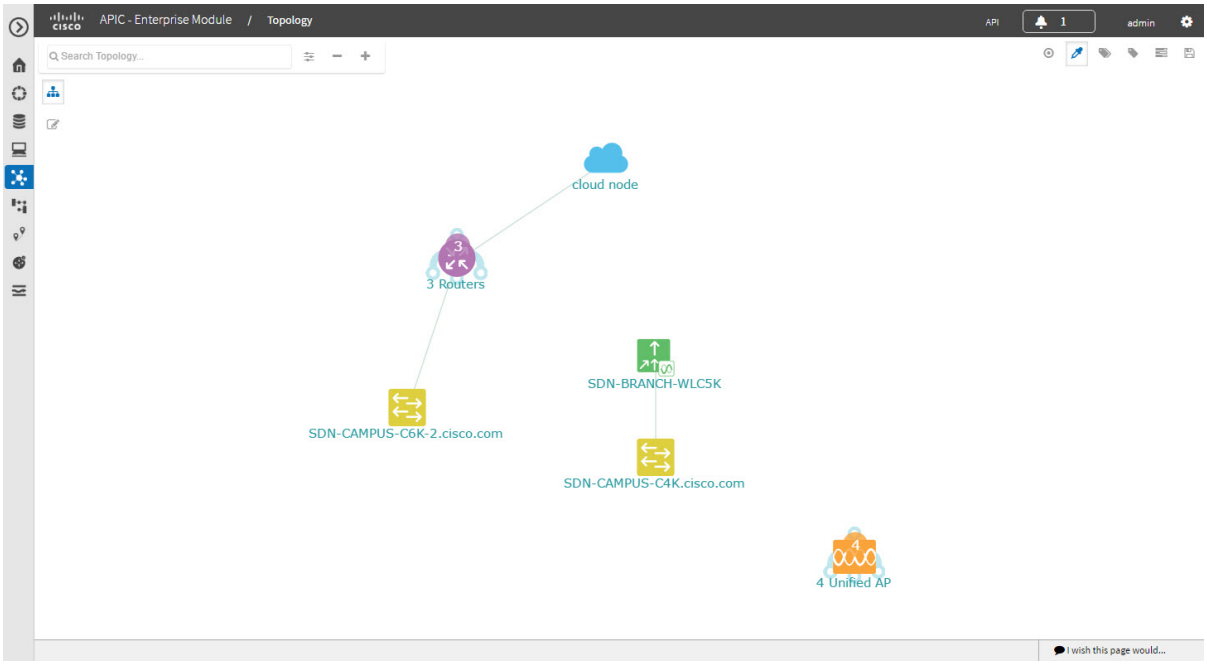
- Auto-visualization of Layer 2 and 3 topologies on top of the physical topology for a granular view for design planning and simplified troubleshooting.
- For a Layer 2 topology, display of configured VLANs within your network. For a Layer 3 topology, display of OSPF, IS-IS, and so on, depending on what is currently configured and in use in your network.
- Device information.
- Display of a path trace in the topology map. For additional information about performing a path trace, see the *Cisco Path Trace Application for APIC-EM User Guide*.

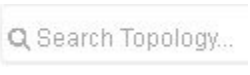
**Note** Individual device configurations are retrieved and stored in a network information database (NIDB).

# Topology Toolbar

The Topology toolbar is located at the top of the **Topology** window.

*Figure 28: Topology Window*




| Icon | Name | Description |
|---|---|---|
|  | **Toggle Aggregation** | Enables or disables device aggregation. Aggregating devices means grouping devices together. You can group devices in any way that makes sense to you.<br>You can save the layout for future reference by clicking the **Save** icon.<br>This grouping does not effect the physical configuration on the devices. Aggregation is enabled by default. |
|  | **Toggle Multiselect** | Allows you to select multiple devices by dragging the mouse over the desired devices or shift-clicking on devices. You can also select multiple groups of devices by clicking shift and dragging the mouse over a group of devices. After selecting the group of devices, you can aggregate or tag them. If you aggregate devices of different product families, the Cisco APIC-EM shows them as generic devices (without a device type) and the number of devices. Multiselect is off by default. |
|  | **Search Topology** | Searches for a host or device by host name, device name, device type, or IP address. As you enter information into this field, the Cisco APIC-EM displays matches. Select the host or device from the results that appear. The selected host or device appears in the **Topology** window. |

| Icon | Name | Description |
|---|---|---|
|  | **Filters** | Allows you to choose a filter that you can apply to the topology map. For each filter, you can make additional adjustments using the **Advanced** options. For information, see Configuring the Topology Structure, on page 88.<br>• **Enterprise** (Default)—Displays your network topology, separating your devices on connection branches. For example, if a group of devices are connected to Router A, and another group of devices are connected to Router B, the topology would show this division and would separate the devices.<br>• **Connections**—Displays the devices according to their number of connections. Starting from the left, the devices with no connections are displayed, then devices with one connection, then devices with two connections, and so on.<br>• **Type and Role**—Displays the devices according to their role in the network: access router, distribution switch, core switch and hub, and boarder router.<br>• **Advanced**—Provides options for you to refine the topology display. |
|  | **Zoom out** | **Note** Adjusts the **Topology** window's view. Click the **-** (minus) icon to minimize the view of the network hosts and devices. |
|  | **Zoom in** | Adjusts the **Topology** window's view. Click the + (plus) icon on the menu bar to maximize the view of the network hosts and devices. |
|  | **Toggle Color Code** | Toggles between displaying the device icons in different colors or in a single color. Color coding is enabled by default. |
|  | **Device Tags** | Displays the available device tags. Clicking on an individual tag highlights the device or devices in the **Topology** window that have this tag.<br>You can also apply tags to devices by selecting the device, clicking **Device Tagging** in the **Device Information** dialog box, and then creating and applying the tags. |

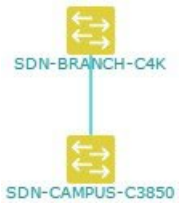
| Icon | Name | Description |
|---|---|---|
|  | **Policy Tags** | Displays the available policy tags. Clicking on an individual tag adds the device to the policy scope.<br>You can also applypolicy tags to devices in the **EasyQoS > Policy Scopes**. |
|  | **Layers** | Displays devices with the following attributes on the topology map:<br>• **Layer 2**—Displays devices based on the selected VLAN or Layer 2 protocol. Select either a VLAN from the drop-down menu or one of the Layer 2 protocols.<br>**Note** You can also access a management network view by choosing a management selection from the drop-down menu.<br>• **Layer 3**—Displays devices based on the selected Layer 3 protocol. The following Layer 3 protocols are available:<br>• **Intermediate System-to-Intermediate System (IS-IS)**<br>• **Open Shortest Path First (OSPF)**<br>• **Enhanced Interior Gateway Routing Protocol (EIGRP)**<br>• **Static-Route**<br>**Note** The default Layer 3 topology has all Layer 3 protocols.<br>• **VRF**—Displays devices that have Virtual Routing and Forwarding (VRF) tables. |
|  | **Save and Load Options** | Displays the following options:<br>• **Save Current Layout**—Saves the current layout, device aggregations, and labels.<br>• **Load Saved Layout**—Loads the previously saved layout, device aggregations, and labels) options. |

| Icon | Name | Description |
|---|---|---|
| | **Map view** | Displays the **Topology** map view. Click this icon to view the network topology in a graphical representation of your network's physical location.<br>**Note** This icon is displayed only if you have added location markers for your devices from the **Device Inventory** window. |

# Topology Icons

The following icons appear in the **Topology** window:

| Icon | Network Element | Description |
|---|---|---|
|  | **Cloud** | Representation of the external network. |
|  | **Router** | Displays the device name. |
|  | **Switch** | Displays the device name. |
|  | **Access Point** | Displays the device name. |
|  | **Wireless LAN Controller** | Displays the device name. |
|  | **Aggregated Devices** | Displays the number of aggregated devices and the device type.<br>**Note** If different devices types are aggregated, only the number of aggregated devices is displayed. |

| Icon | Network Element | Description |
|---|---|---|
|  | **Location Marker** | Displays the device name. The device icon is displayed with a location marker as a background.<br>If you add location markers to your devices (from the **Device Inventory** window) and then click **Topology** in the navigation pane or click the **Map** button on the Topology toolbar, the Topology map view appears. The map view shows where you have placed your location markers (for example, San Jose and London). Click a location marker on the map to display the topology for that location (for example, San Jose).<br>Devices that use a different location marker (for example, London) are shown with a location marker as a background. |
|  | **Links** | Lines between devices.<br>Click on a link to display information about the connected devices.<br>**Note** Some of the links may be hidden due to device aggregations. |

# Displaying Device Data

You can display data for a specific device in the **Topology** window. Displaying device data is helpful when troubleshooting network connectivity issues between devices.

**Note** The device data that is accessible in the **Topology** window is also accessible in the **Device Inventory** window.

The following device data is available:

- Location (Location information is displayed if the selected device icon has a location marker background. Click the **Location** link to display the topology for devices that share that location marker.)
- Type
- Device role (For information about changing the device role, see Changing the Device Role, on page 60.
- IP address
- MAC address
- OS (operating system)
- Software version
- Ports

- Gigabit Ethernet ports
- 10-Gigabit Ethernet ports
- Management ports

- VLAN (if exists)
- Number of connections
- List of connected devices (Each connected device shows its device type (icon) and the number of connections. Clicking on a connected device displays the details for that device.)
- Tags

**Step 1** From the **Navigation** pane, click **Topology**.

The **Topology** window appears.

**Note** If you have added location markers for your devices from the **Device Inventory** window, the Topology map view appears. Click a location marker to display the **Topology** for that location.

**Step 2** To display data for a specific device, click that device in the **Topology** window.

**Step 3** To display a list of aggregated devices, do the following:

a) In the **Topology** window, click an **aggregated devices** icon.
b) In the **Device Details** pane, click the **Details** link for each device to view the device data.
c) Click the **Aggregated Results** link to return to the list of aggregated devices.

### What to do next

Select and review data from other devices within your network, or perform other tasks including the following:

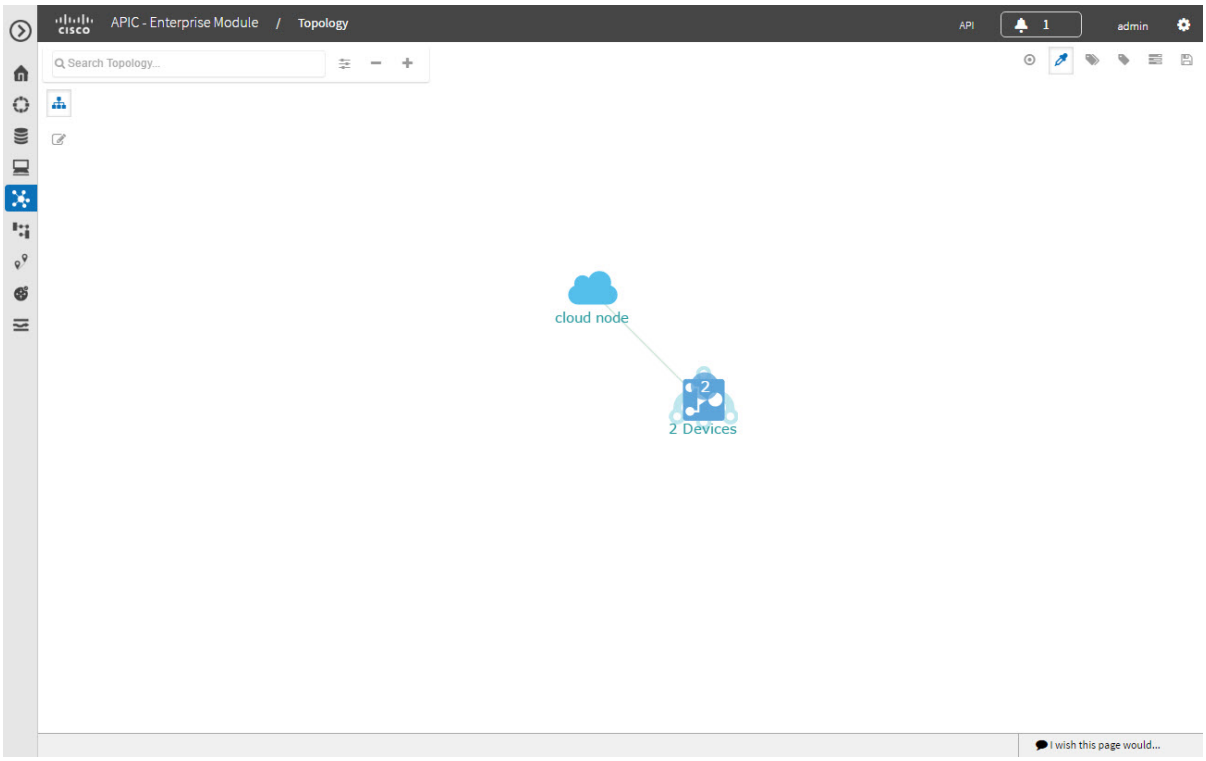
- Aggregate or disaggregate selected groups
- Search for device using device names and IP addresses
- Apply tags to devices within your network
- Change the device role

# Aggregating Devices

You use the Cisco APIC-EM device aggregation feature to adjust how devices are displayed in the **Topology** window. This feature enhances network navigation and manageability.

## Aggregating Devices in the Topology Window

You can aggregate and disaggreate devices into and out of groups in the **Topology** window.




### Before you begin

Scan your network using the discovery functionality of the Cisco APIC-EM to populate device and host inventory for the database.

Determine how the devices within your network configuration are to be visually grouped and organized.

**Step 1** Click **Topology** in the navigation pane.

The **Topology** window appears.

**Note** If you have added location markers for your devices from the **Device Inventory** window, the Topology map view appears. Click a location marker to display the **Topology** for that location.

**Step 2** Click the **Toggle Aggregation** icon to enable device aggregation.

**Note** Device aggregation is enabled by default.

**Step 3** Drag and drop a device icon onto another device icon.

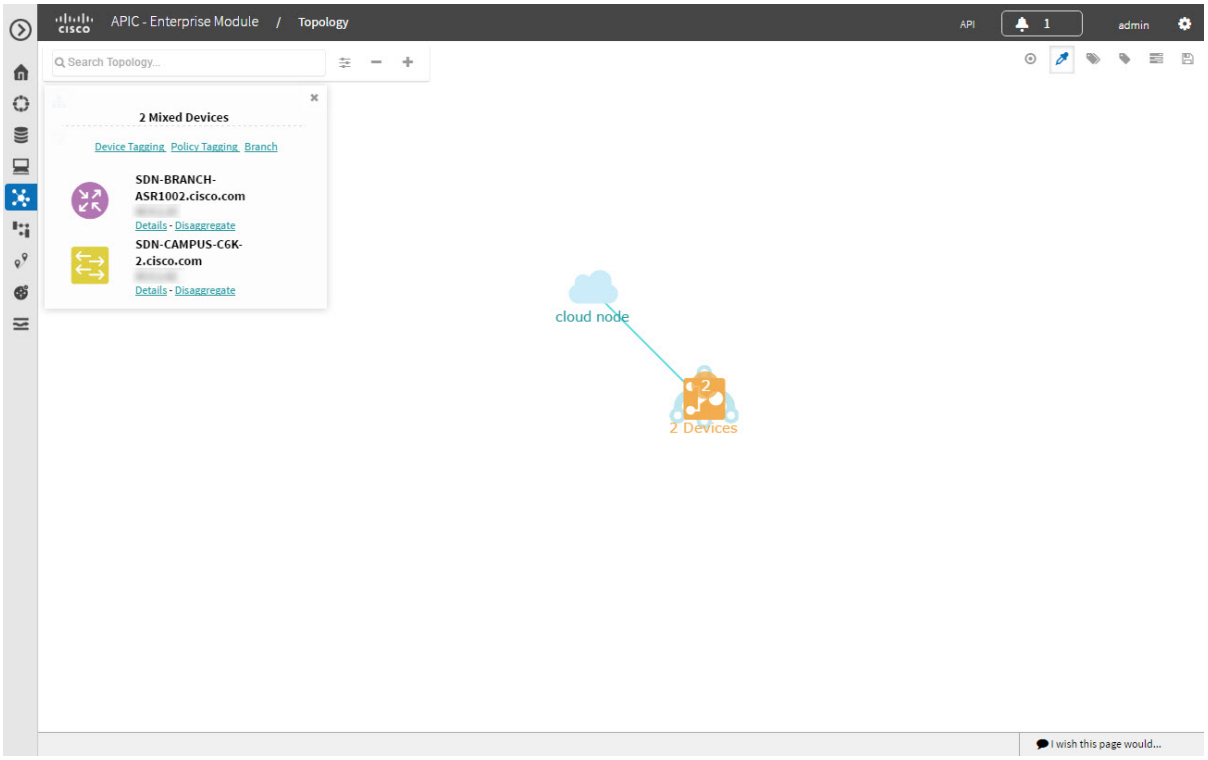
The device icon changes to an aggregated devices icon. For more information about the aggregated devices icon, see Topology Icons, on page 82.

**Note** You can also select multiple devices by clicking the **Multiselect** icon, dragging the mouse over the desired devices, and clicking the **Aggregate Selected** link.

# Disaggregating Devices in the Topology Window

You can ungroup devices by disaggregating them in the **Topology** window.

***Figure 29: Topology Window Showing Disaggregate Option in Devices List***




### Before you begin

Scan your network using the discovery functionality of the Cisco APIC-EM to populate device inventory for the database.

Determine how the devices within your network configuration are to be visually grouped and organized.

**Step 1** From the Navigation pane, click **Topology**.

The **Topology** window appears.

**Note** If you have added location markers for your devices from the **Device Inventory** window, the Topology map view appears. Click a location marker to display the **Topology** for that location.

**Step 2** Click on an **aggregated devices** icon.

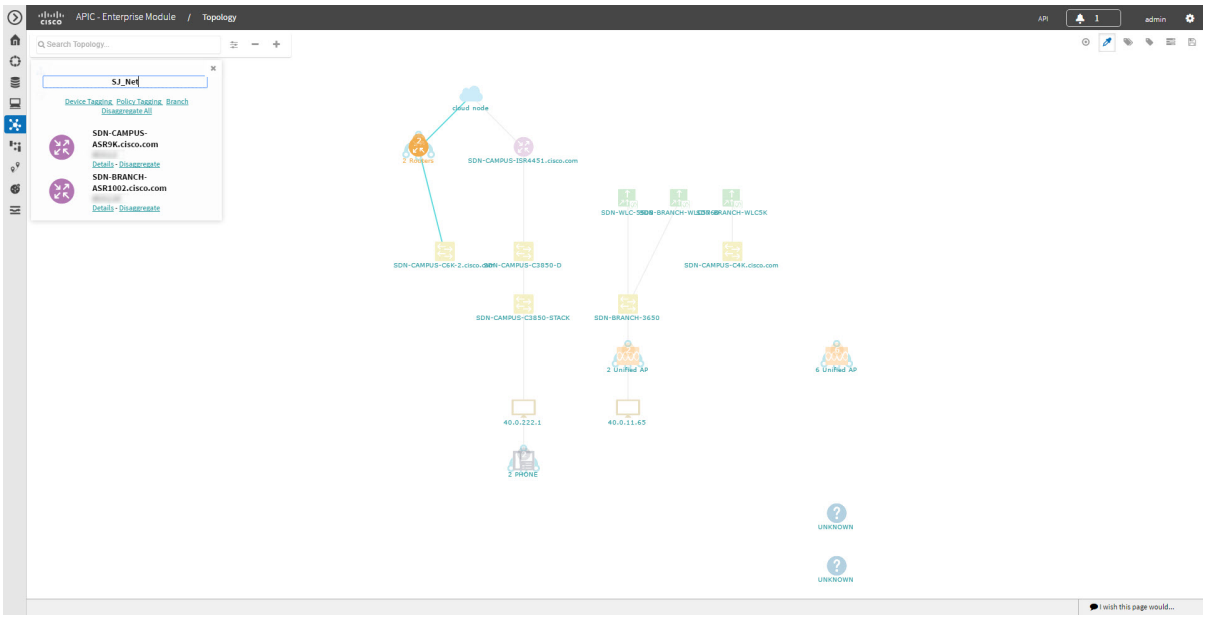
A list of the aggregated devices appears.

**Step 3** From the list, click the **Disaggregate** link for each device that you want to remove from the aggregated devices.

The device is removed from the list and from the aggregated devices icon. The aggregated device label and the aggregated devices icon are updated to reflect the number of devices.

# Changing the Aggregated Devices Label

The default label for aggregated devices is the number of devices and the device type (# *devicetype* Devices). However, you can change the default label to one that is meaningful in the context of your network topology.




### Before you begin

Scan your network using the discovery functionality of the Cisco APIC-EM to populate device inventory for the database.

Determine how the devices within your network configuration are to be visually grouped and organized.

**Step 1** From the Navigation pane, click **Topology**.

The **Topology** window appears.

**Note** If you have added location markers for your devices from the **Device Inventory** window, the Topology map view appears. Click a location marker to display the **Topology** for that location.

**Step 2** Click an **aggregated devices** icon.

A list of the aggregated devices appears. At the top of the list is the aggregated devices label.

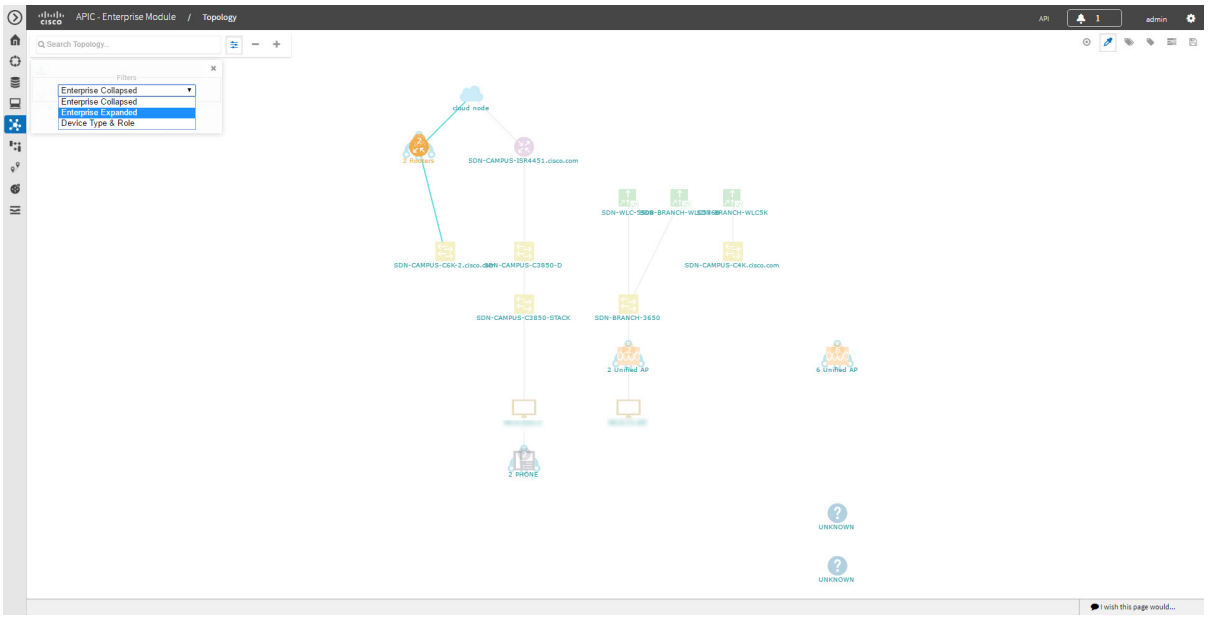
**Step 3** Click the aggregated devices label to open an edit field where you can change the label.

**Step 4** Change the label, then click outside of the edit field to save your changes.

# Configuring the Topology Structure

You can choose from three default topology layouts. You can also use advanced settings to modify these layouts, such as the overall size of the topology graph, the spacing that separates individual elements, and more.

***Figure 30: Topology Window Showing Filters Drop-Down List***




### Before you begin

Scan your network using the discovery functionality of the Cisco APIC-EM to populate device inventory for the database.

**Step 1** From the **Navigation** pane, click **Topology**.

The **Topology** window appears.

**Note** If you have added location markers for your devices from the **Device Inventory** window, the Topology map view appears. Click a location marker to display the **Topology** for that location.

**Step 2** From the **Topology** toolbar, click the **Filters** icon.

**Step 3** Select a filter from the drop down list. Available options are **Enterprise Collapsed**, **Enterprise Expanded**, or **Device Type & Role**.

**Step 4** Click the **Advanced View** button to configure how each filter is displayed. Click the **Basic View** button to return to the basic view.

| Filter | Basic View | Advanced View |
|---|---|---|
| **Enterprise** | Arranges the device icons into a structured connection hierarchical view, from top to bottom. | **Device type**—Use the slider to adjust the amount of space between device icons based on their device types.<br>**cloud-centralizeX**— When checked (default), the device icons are centered along the X axis. When unchecked, the device icons are aligned to the X axis.<br>**Device role**—Use the slider to adjust the amount of space between device icons based on their device roles.<br>**Branch**— Use the slider to adjust the amount of space between branches.<br>**Node overlap**—Use the slider to adjust the amount of space between nodes.<br>**Note** Select **x** or **y** from the drop down next to each slider to change how the device icons are displayed, horizontally or vertically. |
| **Connections** | Arranges the device icons from left to right based on the number of connections, from least to most.<br>**Note** Aggregated devices are disaggregated in this view. | **Connections**—Use the slider to adjust the amount of space between connections.<br>**Node overlap**—Use the slider to adjust the amount of space between nodes.<br>**centralizeY**—When checked, the device icons are centered along the Y axis. When unchecked, the device icons are aligned to the Y axis.<br>**Note** Select **x** or **y** from the drop down next to each slider to change how the device icons are displayed, horizontally or vertically. |
| **Type and Role** | Arranges the device icons from top to bottom based on device type (cloud, router, WLC, switch, access point, wired, wireless) and role (border router, core, distribution, and access)<br>**Note** Aggregated devices are disaggregated in this view. | **Device type**—Use the slider to adjust the amount of space between device icons based on their device types.<br>**Device role**—Use the slider to adjust the amount of space between device icons based on their device roles.<br>**Node overlap**—Use the slider to adjust the amount of space between nodes.<br>**centralizeX**—When checked, the device icons are centered along the X axis. When unchecked, the device icons are aligned to the X axis.<br>**Note** Select **x** or **y** from the drop down next to each slider to change how the device icons are displayed, horizontally or vertically. |

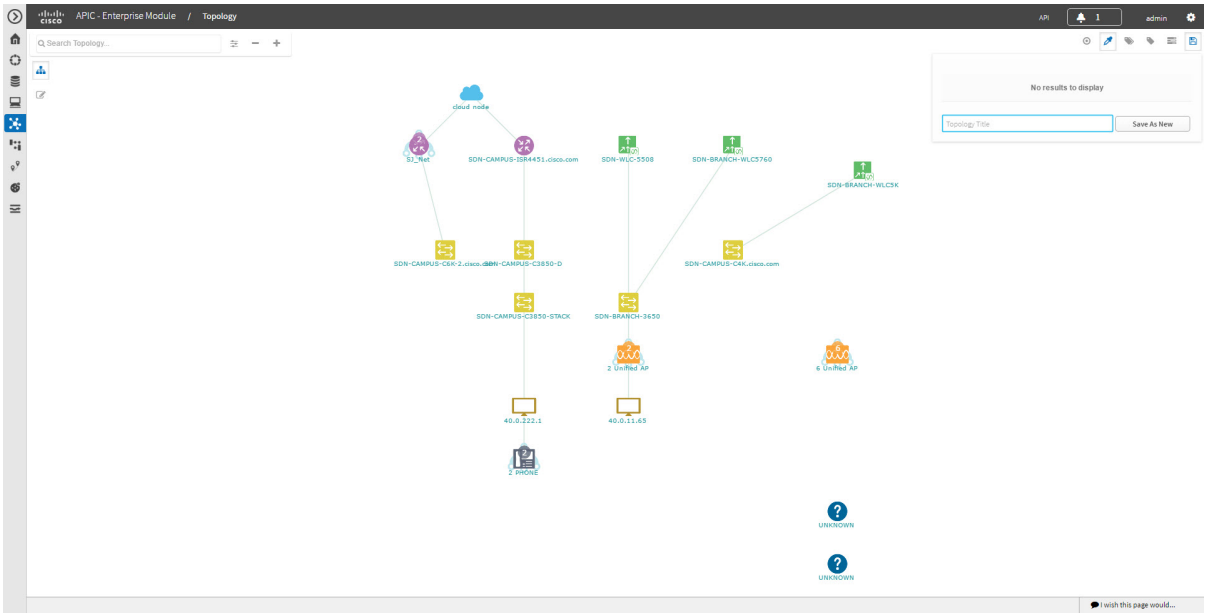
### What to do next

Save the current layout or load a previously saved layout. For information, see Saving a Topology Layout, on page 90 and Opening a Saved Topology Layout, on page 91.

# Saving a Topology Layout

You can save a topology layout so that you can open and view it later.

***Figure 31: Topology Window Showing Save Dialog Box***




### Before you begin

You must have administrator role permissions.

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 **Topology**.

The **Topology** window appears.

**Step 2** From the **Topology** toolbar, click the **Save** icon.

**Step 3** In the **Topology Title** field, enter a name for the topology and click **Save as New**.

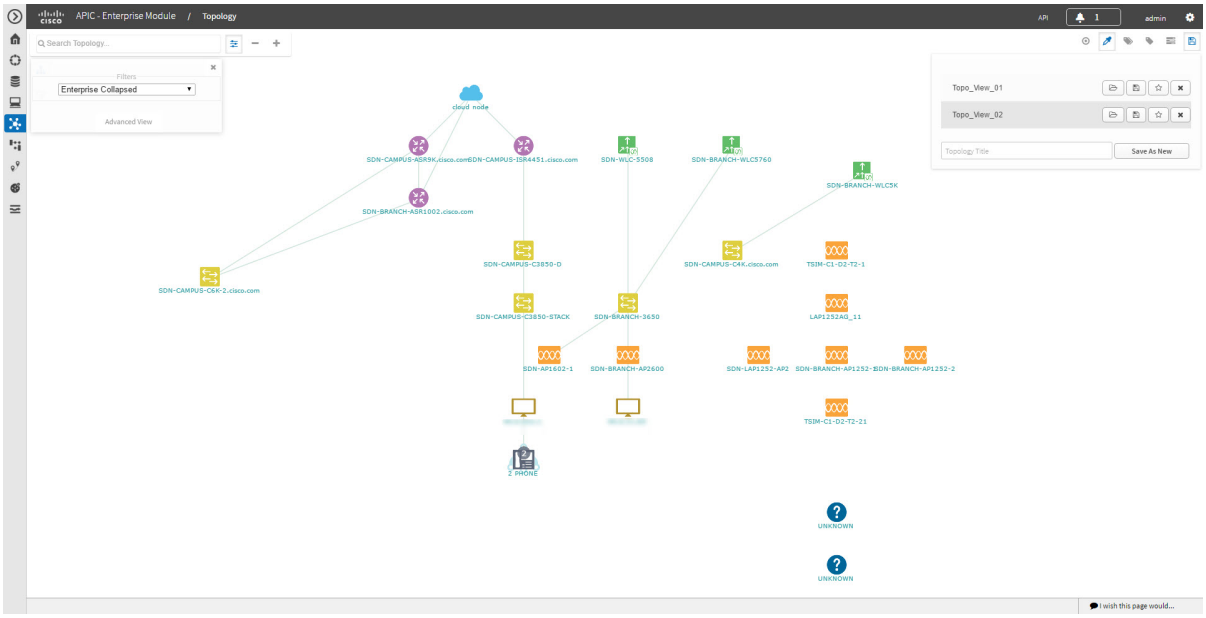
**Step 4** Click **OK** to confirm the save.

The topology is saved and the name appears at the top of the dialog box.

# Opening a Saved Topology Layout

You can open a topology layout that you have previously saved.

***Figure 32: Topology Window Showing Previously Saved Topology Layouts in Save 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 **Topology**.

The **Topology** window appears.

**Step 2** From the **Topology** toolbar, click the **Save** icon.

A dialog box appears listing the saved topology layouts.

**Step 3** For the topology layout that you want to open, click the **Folder** icon..

**Step 4** Click **OK** to confirm.

The topology layout opens in the **Topology** window.

# Changing a Device's Role From the Topology Window

During the scan process, a device role is automatically assigned to each discovered device. The device role is used for identifying and grouping devices according to their responsibilities and placement within the network.

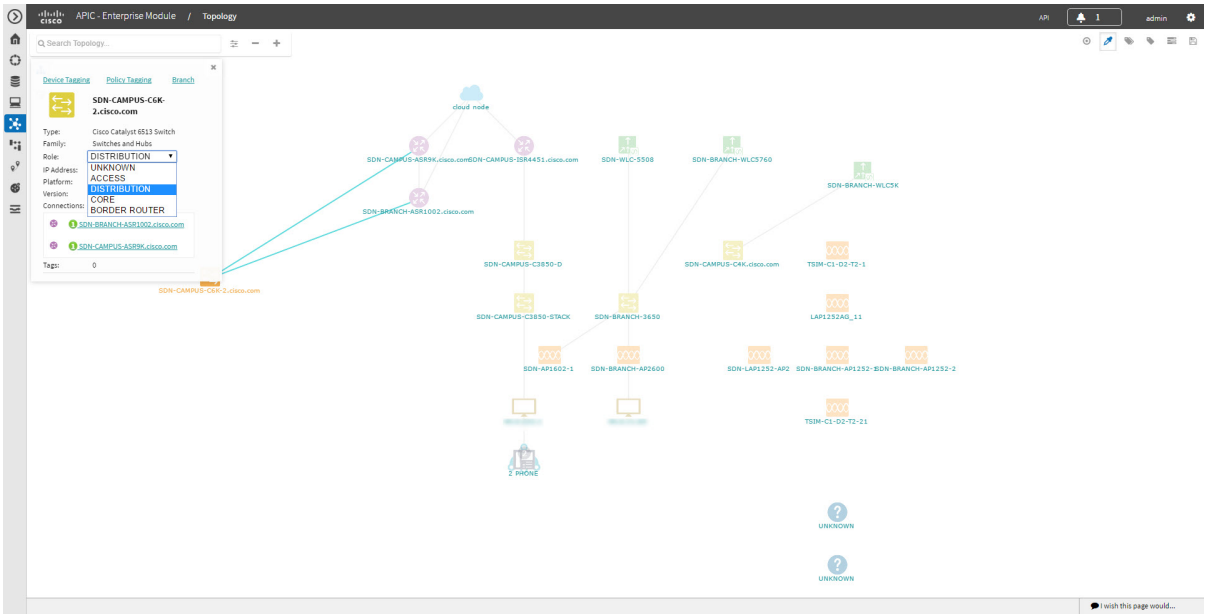
A device can have one of the following roles within the Cisco APIC-EM:

- Unknown—Device role is unknown.
- Access—Device is located within and performs tasks required for the access layer or first tier/edge.
- Border Router—Device performs the tasks required for a border router.
- Distribution—Device is located within and performs tasks required for the distribution layer.
- Core—Device is located within and performs tasks required for the core.

You can change the device role when you select a device and display the device data.

**Note** You can also change the device role from the **Device Inventory** window.

***Figure 33: Topology Window Showing Role Drop-Down List***




### Before you begin

Scan your network using the discovery functionality of the Cisco APIC-EM to populate device inventory for the database.

**Step 1** From the **Navigation** pane, click **Topology**.

The **Topology** window appears.

**Note** If you have added location markers for your devices from the **Device Inventory** window, the Topology map view appears. Click a location marker on the map to display the Topology for that location.

**Step 2** Click a specific device in the **Topology** window to select it.

**Step 3** Choose a role from the **Role** drop-down list: **Access**, **Core**, **Distribution**, or **Border Router**.

**Step 4** (Optional) Select additional devices and change device roles.

**Step 5** Click the **Filters** icon on the **Topology** toolbar.

**Step 6** (Optional) Select a filter from the drop down list. Available options are **Branch**, **Connections**, or **Device and Role**.

**Step 7** Click the refresh button to the right of the filter type to update all of the device roles.
The **Topology** structure refreshes showing the changed device roles.

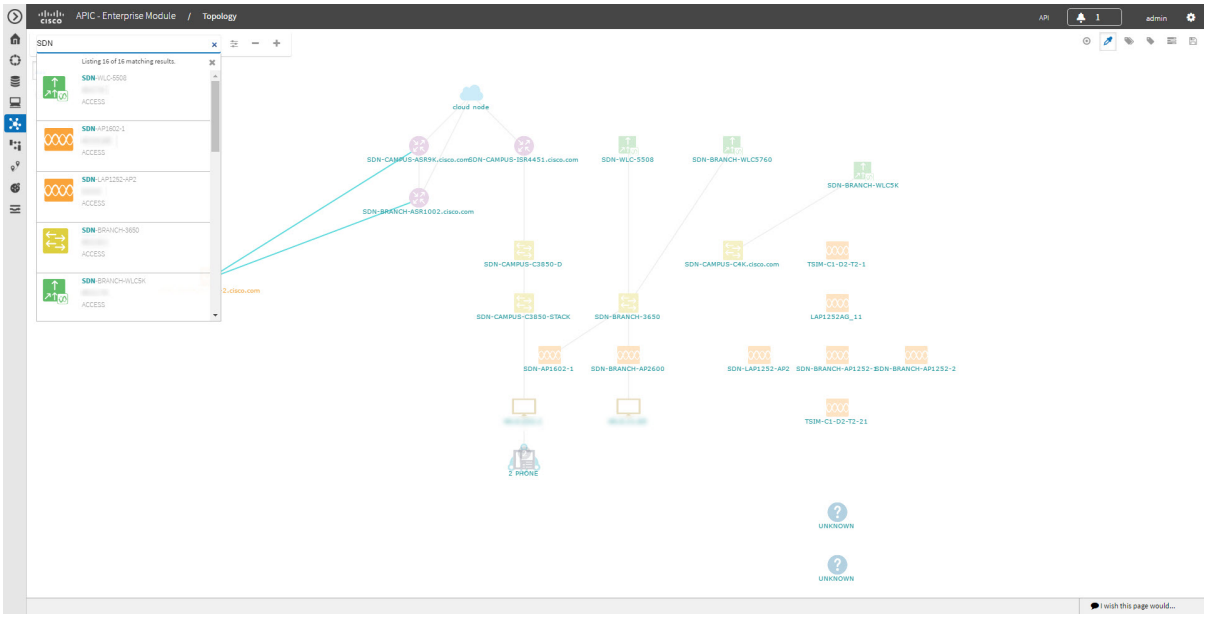
# Searching for Devices and Hosts

You use the Cisco APIC-EM search function to locate specific devices or hosts within your network. This function allows you to search the network using any string value. To locate a specific device or host quickly, use any of the following values in the search field:

- Device or host name
- Aggregation label
- IP address
- Device role
- Device type

**Note** The search function supports fragmented results. For example, if you enter **12** in the search field, you will get results for devices with IP addresses or device names that contain 1 and 2 (.12, .120, .102, 10.20, 1-switch2, etc).

*Figure 34: Topology Window Showing Device Search List*




### Before you begin

Scan your network using the discovery functionality of the Cisco APIC-EM to populate device and host inventory for the database.

Determine the string value to be used within your network for your search.

**Step 1** Click **Topology** in the navigation pane.

The **Topology** window appears.

**Note** If you have added location markers for your devices from the **Device Inventory** window, the Topology map view appears. Click a location marker on the map to display the Topology for that location.

**Step 2** From the Topology toolbar, enter a keyword in the **Search Topology** field.

As you begin typing, the controller displays a list of possible matches to your entry.

**Note** You can click the **x** in the search field to clear the search keyword field and the results.

**Step 3** Click on a device from the search results to highlight that device and its links in the **Topology** window. Click on the device again to display detailed data for that device.

**Step 4** Proceed with any provisioning or troubleshooting tasks on the located devices or hosts.

### What to do next

Search using other string values for other devices or hosts within your network, or perform other tasks including the following:

- Viewing the data for specific devices
- Applying tags to devices within your network
- Host a meeting using the topology co-editor to collaborate with other users in real-time on the network

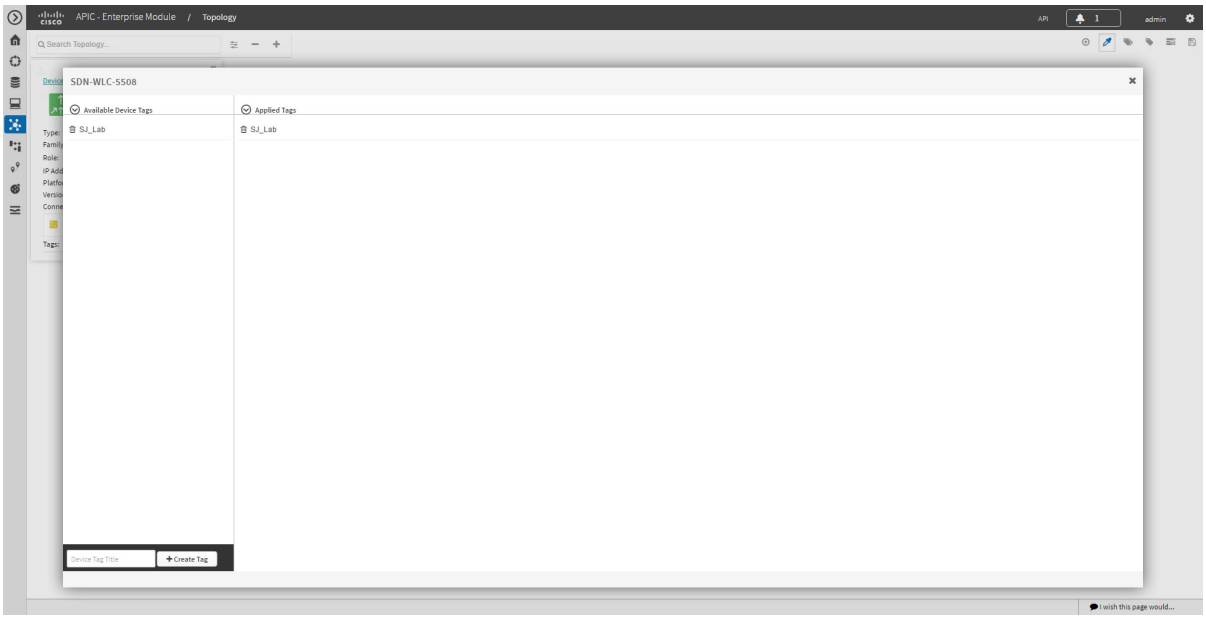
# Adding or Removing a Device Tag in Topology

In the **Topology** window, you can add device tags to associate devices that share a common attribute. For example, you can create a tag and use it to group devices based upon a platform ID, Cisco IOS releases, or location. Similarly, you can remove tags from devices.

You can also add or remove device tags from the **Device Inventory** window or from the **EasyQoS** window. For information, see Adding or Removing a Device Tag in Device Inventory, on page 62 or the *Cisco EasyQoS Application for APIC-EM User Guide*.

**Note** Applying a tag to a host is not supported.

***Figure 35: Device Tag Dialog Box***




### Before you begin

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

**Step 1** From the Navigation pane, click **Topology**.

**Step 2** Click the device or devices you want to tag. To select more than one device, click the **Multiselect** icon. For information about how to use the multiselect function, see Topology Icons, on page 82.

**Note** To deselect devices in your selection, click outside of the selected device.

The **Device Information** dialog box appears.

**Step 3** Click **Device Tagging**.

The **Device Tagging** dialog box appears.

**Step 4** From the **Available Tags** column, click a tag to apply it to the selected device or devices. If the tag you want does not exist, you can create it by entering the name of the tag in the **Device Tag Title** field and clicking **+Create Tag**.

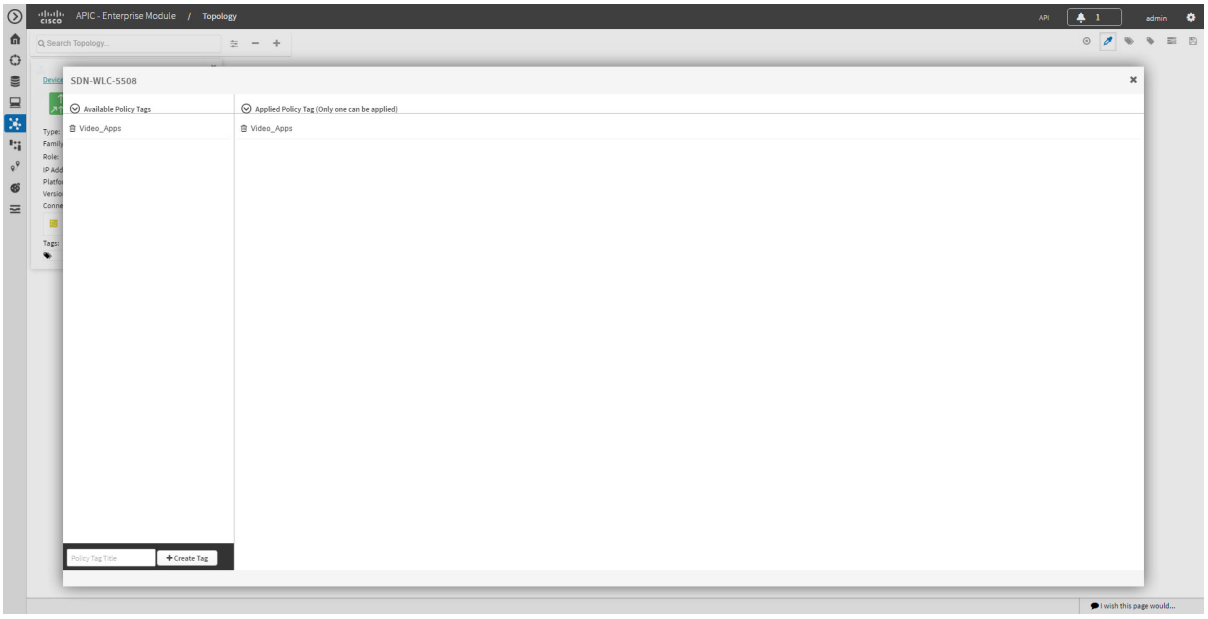
**Step 5** When you are done, click **x** to close the dialog box.

# Adding or Removing a Policy Tag in Topology

Before you can create a QoS policy, you need to identify the policy scope, that is, the devices that will be configured with QoS policies. You identify the devices by tagging them with a policy tag.

You can also add or remove policy tags from the **Device Inventory** window or the **EasyQoS** window. For information, see Adding or Removing a Device Tag in Device Inventory, on page 62 or the *Cisco EasyQoS Application for APIC-EM User Guide*.

***Figure 36: Policy Tag Dialog Box***




### Before you begin

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

From the **Topology** or **Device Inventory** window, verify that the device roles assigned to devices during discovery are appropriate for your network design. If necessary, change any of the device roles that are not appropriate.

**Step 1** From the Navigation pane, click **Topology**.

**Step 2** Click the device or devices you want to tag. To select more than one device, click the **Multiselect** icon. For information about how to use the multiselect function, see Topology Icons, on page 82.

**Note** To deselect devices in your selection, click outside of the selected device.

The **Device Information** dialog box appears.

**Step 3** Click **Policy Tagging**.

The **Multiple Policy Tagging** dialog box appears.

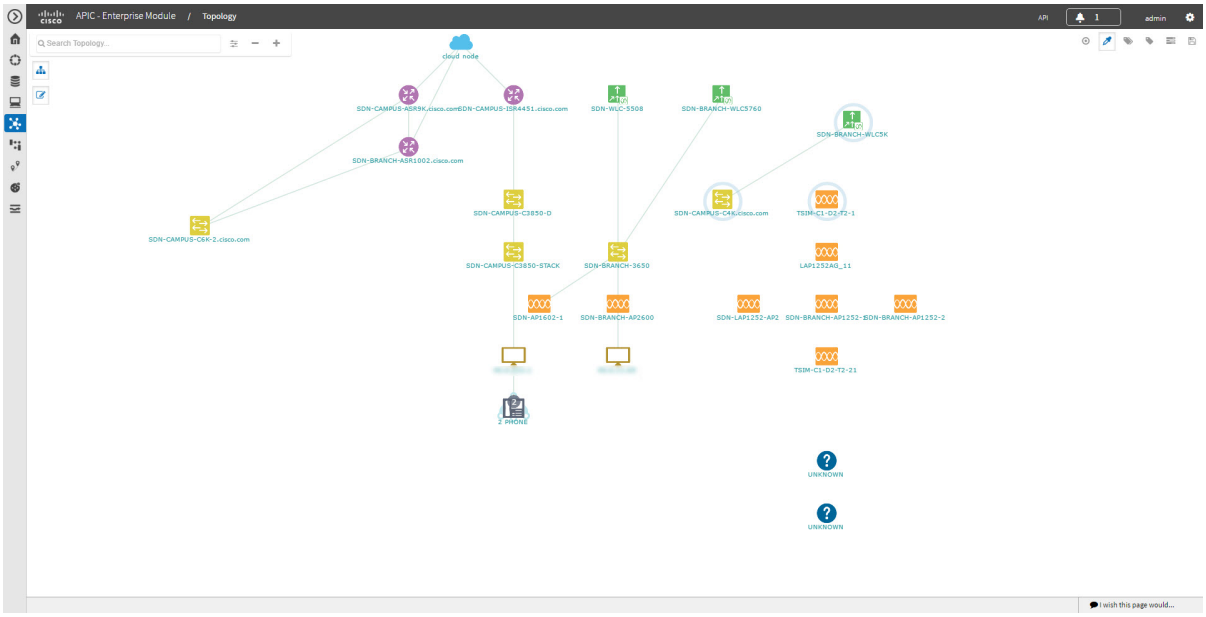
**Step 4** From the **Available Policy Tags** column, click a tag to apply it to the selected device or devices. If the tag you want does not exist, you can create it by entering the name of the tag in the **Policy Tag Title** field and clicking **+Create Tag**.

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

# Displaying Devices with Tags

To display tagged devices from the **Topology** window, perform the following steps.

***Figure 37: Topology Window Showing Devices with Tags***




### Before you begin

You should have performed the following tasks:

- Discovered the devices on your network to populate the device inventory database.
- Created tags and applied them either through the **Device Inventory** or **Topology** window.

**Step 1** From the Navigation pane, click **Topology**.

The **Topology** window appears.

**Step 2** From the Topology toolbar, click the **Tags**.

A tag selection box appears.

**Step 3** To identify the devices associated with a tag, click the tag. To return the devices to their normal display, click the tag again.

Tags are color-coded, so when you click a tag, a circle of the same color is drawn around its associated devices.

**Note** You can click more than one tag at a time. The tag that you chose to display first is the innermost circle around the device, followed by the next tag as the next circle, and so on.

# INDEX

## R



## S



## T