



## **Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide, Release 1.0.x**

**First Published:** November 02, 2015

### **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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### Preface

#### Preface vii

Audience vii

Document Conventions vii

Related Documentation ix

Obtaining Documentation and Submitting a Service Request x

---

### CHAPTER 1

#### Overview 1

About the Cisco Application Policy Infrastructure Controller Enterprise Module 1

Cisco APIC-EM GUI Overview 3

---

### CHAPTER 2

#### Discovering Devices and Hosts 7

About Discovery 7

Understanding Device and Host Discovery 9

Understanding Wireless LAN Controller Discovery 10

Using Discovery 10

Performing Discovery Using CDP 10

Performing a Discovery Using an IP Address Range 13

Stopping and Starting a Discovery 16

Deleting a Discovery 16

Understanding the Discovery Results 17

---

### CHAPTER 3

#### Managing Devices and Hosts 21

Managing Your Device Inventory 21

Filtering the Devices Table View 28

Changing the Devices Layout View 28

Changing the Device Role 29

Deleting a Device 30

Adding or Removing a Tag	31
Deleting a Tag	32
Adding or Removing a Location Tag	33
Adding and Removing Location Markers	34
Adding a Location Marker	34
Removing a Location Marker	37
Managing Your Host Inventory	38
Changing the Hosts Table View	39

---

**CHAPTER 4****Managing Users and Roles 41**

About Role-Based Access Control	41
About User Roles	41
Administrator Role	42
Observer Role	42
Installer Role	43
Users and Domains	43
About AAA	43
Authentication and Authorization	43
Cisco APIC-EM Resources and Permissions	44
Accounting	45
Changing Your Password	45
Configuring Users and Roles	47
Adding a User	48
Deleting a User	49
Viewing and Editing User Information	49
Viewing User Access Status	50
Reviewing the User Logs	51

---

**CHAPTER 5****Managing Applications 53**

Cisco Network Plug and Play	53
Cisco Intelligent WAN (IWAN)	54
Topology	55
Topology Toolbar	56
Topology Icons	60
Displaying Device Data	61

Device Aggregation	63
Aggregating Devices in the Topology Window	63
Disaggregating Devices in the Topology Window	63
Changing the Aggregated Devices Label	64
Configuring the Topology Structure	65
Saving a Topology Layout	66
Opening a Saved Topology Layout	67
Changing the Device Role in the Topology Window	67
Searching for Devices and Hosts	68
Applying Tags to Devices	69
Displaying Devices with Tags	70
Performing Path Traces	71
About Path Trace	71
Path Trace Support	74
Path Trace Protocols and Network Connections	74
Performing a Path Trace	79
Understanding Path Trace Results	80
<hr/>	
<b>CHAPTER 6</b>	<b>Reviewing the API Documentation 83</b>
	About the Cisco APIC-EM API Documentation 83
	Supported HTTPS Methods and General Structure 86
	Common External RESTful Services HTTP Response Codes 87
	Testing the Cisco APIC-EM APIs 88





## Preface

---

- [Audience](#), page vii
- [Document Conventions](#), page vii
- [Related Documentation](#), page ix
- [Obtaining Documentation and Submitting a Service Request](#), page x

## Audience

This publication is for experienced network administrators who will configure and maintain the Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM). Use this configuration guide to understand the Cisco APIC-EM GUI, manage connected devices and hosts within your network, and perform a path trace through your network devices.

See the following guides for additional information about the Cisco APIC-EM:

- For information about the Cisco APIC-EM itself, including information regarding installation, deployment, verification, and troubleshooting, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.
- For information about using the controller's GUI for the first time, see the *Cisco APIC-EM Quick Start Guide*.



---

**Note**

The Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM) is also referred to within this configuration guide as a controller.

---

## Document Conventions

This document uses the following conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination <b>^D</b> or <b>Ctrl-D</b> means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
<b>bold font</b>	Commands and keywords and user-entered text appear in <b>bold font</b> .
<i>Italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
Courier font	Terminal sessions and information the system displays appear in <code>courier font</code> .
<b>Bold Courier font</b>	<b>Bold Courier</b> font indicates text that the user must enter.
[x]	Elements in square brackets are optional.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x   y]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
{x   y}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x {y   z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
<>	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

### Reader Alert Conventions

This document may use the following conventions for reader alerts:



**Note**

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

**Tip**

Means *the following information will help you solve a problem*.

**Caution**

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

**Timesaver**

Means *the described action saves time*. You can save time by performing the action described in the paragraph.

**Warning****IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

## Related Documentation

- Cisco APIC-EM Documentation:
  - *Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module*
  - *Cisco APIC-EM Quick Start Guide* (directly accessible from the controller's GUI)
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Hardware Installation Guide*
  - *Open Source Used In Cisco APIC-EM*
- Cisco IWAN Documentation for the Cisco APIC-EM:
  - *Release Notes for Cisco IWAN*
  - *Release Notes for Cisco Intelligent Wide Area Network (Cisco IWAN)*
  - *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 Open Plug-n-Play Agent Configuration Guide*
  - *Mobile Application User Guide for Cisco Network Plug and Play*

**Note**

---

For information about developing your own application that interacts with the controller by means of the Northbound REST API, see the [developer.cisco.com/site/apic-em](http://developer.cisco.com/site/apic-em) Web site.

---

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: <http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.



## Overview

---

- [About the Cisco Application Policy Infrastructure Controller Enterprise Module, page 1](#)
- [Cisco APIC-EM GUI Overview, page 3](#)

# About the Cisco Application Policy Infrastructure Controller Enterprise Module

The Cisco Application Policy Infrastructure Controller - Enterprise Module (APIC-EM) is Cisco's 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**

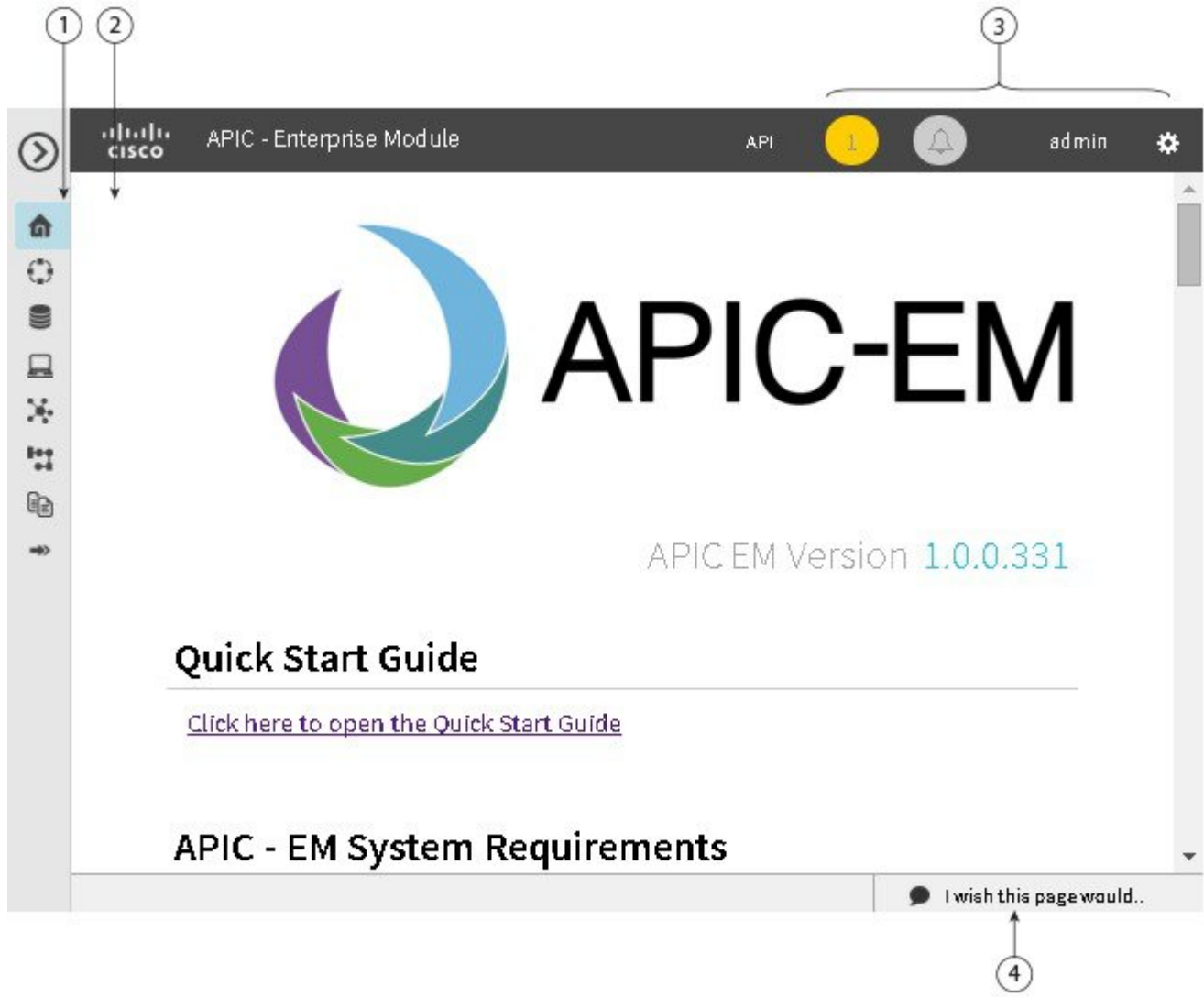
Feature	Description
Network Information Database (NIDB)	The Cisco APIC-EM periodically scans the network to create a “single source of truth” for IT. This inventory includes all network devices, along with an abstraction for the entire enterprise network.

Feature	Description
Network topology visualization	The Cisco APIC-EM automatically discovers and maps network devices to a physical topology with detailed device-level data. You can use this interactive feature to troubleshoot your network.
Cisco Plug and Play application	The Cisco Network Plug and Play solution is a converged solution that 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.
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. This feature saves costs by application experience over any connection and using otherwise inactive or backup links.
Public Key Infrastructure (PKI) server	The Cisco APIC-EM provides an integrated PKI server for Trust manager service. It automates the lifecycle management of issuing, renewing, and revoking the PKI X.509 certificate for applications such as IWAN application. With this feature, the IWAN application greatly simplifies the process of establishing and keeping trust in the network.
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.

# Cisco APIC-EM GUI Overview

When you log into the Cisco APIC-EM, the **Home** page appears.

Figure 1: Home Page










Callout Number	Name	Description
1	Navigation pane	Provides access to the Cisco APIC-EM features and additional applications, such as IWAN and Network Plug and Play.
2	Window	Area where the feature or application interface is displayed. When you click an option in the <b>Navigation</b> pane, its corresponding window opens.

Callout Number	Name	Description
3	<b>Global</b> toolbar	Area that provides access to tools, such as API documentation, settings, and notifications. For a full explanation of the icons on the <b>Global</b> toolbar, see the Global Toolbar Options table below.
4	Feedback link	Link to a form where you can provide input about your experience using the Cisco APIC-EM features and its GUI and provide suggestions for improvements.

### Navigation Pane Options

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




**Table 2: Navigation Pane Options**


Icon	Name	Description
	<b>Hide/Unhide Navigation</b>	Allows you to hide and unhide the <b>Navigation</b> pane.
	<b>Home</b>	Displays information about system requirements and supported platforms.
	<b>Discovery</b>	Allows you to configure discovery options for scanning the devices and hosts in your network.
	<b>Device Inventory</b>	Provides access to the inventory database, where you can display, filter, and sort tabular information about the discovered devices in your network.
	<b>Topology</b>	Displays graphical representations of your physical, Layer 2, and Layer 3 networks.
	<b>Host Inventory</b>	Provides access to the inventory database, where you can display, filter, and sort tabular information about the discovered hosts in your network. Users can have one of three possible states: active, inactive, and deleted.
	<b>IWAN</b>	Allows you to configure your network-wide settings, provision sites, and configure application policies.
	<b>Path Trace</b>	Allows the controller to review and collect protocol and other types of data from discovered devices in your network and use this data to calculate a path between two hosts or Layer 3 interfaces.
	<b>Network Plug and Play</b>	Provides access to the remote deployment application for your network devices.

### Global Toolbar Options

The **Global** toolbar provides access to other system functions and displays system notifications.

**Table 3: Global Toolbar Options**

Icon	Option	Description
	<b>API</b>	Displays the auto-generated documentation of the northbound REST APIs.
	<b>System Notifications</b>	Opens the <b>System Notifications</b> view. This view provides information about any system notifications. For example, any notifications about software updates or security certificates updates appear in this window. Each notification contains a brief description and an icon that if clicked opens the source Cisco APIC-EM UI window for the notification (where you can take further action).
	<b>Application Notifications</b>	<p>Opens the <b>Application Notifications</b> view. A red square indicates a notification that has not yet been reviewed. A blue square indicates that either there are no notifications or that notifications exist and have been reviewed. Each notification is listed in the order that it occurred with the most recent at the top of the list. Each notification contains a brief description and an icon that, if clicked, opens the source Cisco APIC-EM application for the notification.</p> <p><b>Note</b> You can also configure to be notified only for events in the current open window (application). By clicking on the link in the <b>Notifications</b> view for the current window (for example, <b>Show only notifications for Discovery</b>), you limit notifications to events that occur in that application.</p>

Icon	Option	Description
	<b>Administrative Functions</b>	<p>Opens a window where you can perform functions that are specific to Cisco APIC-EM or to the user:</p> <ul style="list-style-type: none"><li>• Cisco APIC-EM functions:<ul style="list-style-type: none"><li>◦ <b>Settings</b>—Allows you to configure controller settings, such as user accounts, discovery credentials, network settings, and other security and maintenance settings.</li><li>◦ <b>Logs</b>—Allows you to search the controller's service logs.</li></ul></li><li>• User functions:<ul style="list-style-type: none"><li>◦ <b>Change Password</b>—Allows you to change your own password.</li><li>◦ <b>Sign Out</b>—Logs you out of the Cisco APIC-EM.</li></ul></li></ul>





## Discovering Devices and Hosts

---

- [About Discovery, page 7](#)
- [Using Discovery, page 10](#)

### About 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 do this, you need to tell the controller some information about your network 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 the information about your network:

- 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)—IPDT is enabled automatically for all devices by the controller. For this configuration, privileges must be given to the controller during discovery.
- LLDP-MED—IP phones and possibly some servers are discovered using LLDP Media Endpoint Discovery

To access the Discovery function, from the **Navigation** pane, click **Discovery**. The **Discovery** window opens.

**Figure 2: Discovery Window**

The screenshot shows the Discovery Window interface. It is divided into three main sections:

- Section 1 (Left):** A list of Discoveries. It includes an "Add New" button at the top right. Under "ACTIVE", there is an entry for "Boston" with "cdp 40.0.84.2". Under "INACTIVE", there is an entry for "SFNet" with "cdp 40.0.84.21". A small box with the number "5" is next to the "SFNet" entry.
- Section 2 (Middle):** Configuration options for a new discovery. It includes:
  - Discovery Name:** A text input field labeled "Scan Name".
  - IP Ranges:** A section titled "IPs of the devices you want to scan" with a "Discovery Type" dropdown menu set to "CDP".
  - SNMP:** A section titled "Try different SNMP settings than global ones" with a "show SNMP settings" button.
  - CLI Credentials:** A section titled "Credentials are what you use to log in the devices." with a "show CLI Credentials settings" button.
  - Advanced:** A section titled "Specify advanced settings" with a "show Advanced settings" button.
  - A "Start Discovery" button at the bottom.
- Section 3 (Right):** A light blue informational panel titled "Add a New Discovery". It contains text explaining the purpose of Discovery and a section titled "DISCOVERY TYPE" which describes the "CDP" and "Range" scan types. At the bottom, there is a section titled "CREDENTIALS".

Numbered callouts (1, 2, 3, 5) point to the "Add New" button, the "Discovery Name" field, the "Discovery Type" dropdown, and the "SFNet" entry respectively.

Numbered Callout	Name	Description
1	Discoveries pane	Lists the names of the discovery scans that have been created, along with the method and IP addresses used for discovery. The list is divided between active and inactive discoveries.  A successful scan (one with discovered and authenticated devices) has the number of discovered devices indicated in a box to the right of the discovery name. An unsuccessful scan shows no box or number of devices discovered.  From the <b>Discoveries</b> pane, clicking on a discovery name displays the information in the <b>Discovery Details</b> and <b>Device Details</b> panes.
2	Discovery Details pane	Provides detailed information about the discovery parameters that were used to perform the discovery, the state of the discovery, and the number of devices that were discovered. The buttons on this pane allow you to <b>Start</b> , <b>Stop</b> , and <b>Delete</b> discoveries.
3	In-tool guide	Provides guidance about how to configure discovery.

## Understanding Device and Host Discovery

The Cisco APIC-EM discovers devices and hosts and populates the device and host inventory database with the results of the discovery.

To discover devices and hosts, you must configure SNMPv2c credentials or SNMPv3 credentials or both SNMPv2c and SNMPv3 credentials (depending on your network). For SNMPv2, only the SNMP read community credentials are mandatory.

CLI credentials are also mandatory. Configure CLI credentials to access to the configuration files on the devices.

These credentials can be configured in two different places in the Cisco APIC-EM GUI:

- **Settings > Discovery Credentials** window—You configure SNMP and CLI credentials in this window when they are common to all or most of the devices in your network. These credentials are referred to as *global* credentials.
- **Discovery** window—You configure SNMP and CLI credentials in this window when you want to discover devices on the fly or when you need to devices that do not have the typical SNMP and CLI credentials that the majority of the devices have in your network and that were configured in the **Settings > Discovery Credentials** window. These credentials are referred to as *exception* credentials.

Wireless LAN Controllers (WLCs) have additional setup requirements in order to be discovered. For more information, see [Understanding Wireless LAN Controller Discovery](#), on page 10.

## Understanding Wireless LAN Controller Discovery

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 Wireless LAN Controller
- Cisco Series 8510 Wireless LAN Controller
- Cisco Wireless Service Module 2 (WiSM2)

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.

## Using Discovery

### Performing Discovery Using CDP

You can perform a discovery using CDP.

Note that while a discovery is in progress, you can do any of the following actions:

- Create a new discovery by clicking **Add New** from the **Discoveries** pane.
- Stop an active discovery by selecting the discovery name in the **Discoveries** pane and clicking **Stop** in the **Discovery Details** pane.
- Start an inactive discovery by selecting the discovery name in the **Discoveries** pane and clicking **Stop** in the **Discovery Details** pane.
- Delete a discovery by selecting the discovery name in the **Discoveries** pane and clicking **Delete** in the **Discovery Details** pane.

**Before You Begin**

You must have administrator permissions. For information about user permissions, see [Managing Users and Roles, on page 41](#).

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

- 
- Step 1** From the **Navigation** pane, click **Discovery**.  
The **Discovery** window appears.
- Step 2** (Optional) In the **Discovery Name** field, enter a unique name for this discovery.
- Step 3** In the **IP Ranges** area, do the following:
- From the **Discovery Type** field, choose **CDP**.
  - In the **IP Address** field, enter the IP address for the Cisco APIC-EM to use as the starting point for the discovery scan.
- Step 4** In the **SNMP** area, configure one or both of the SNMP versions that are being used by the devices that you want to discover.  
Use the following guidelines and the information in the tables to help you enter the correct values in the fields:
- The controller supports multiple SNMP credential configurations, but if you configure more than 5 credential sets (global and/or exception, SNMPv2c and/or SNMPv3 credentials), you will receive an error message.
  - An SNMP Read Only (RO) community string is required to assure a successful discovery and populated inventory. However, if an SNMP RO community string is not provided, as a *best effort*, discovery will run with the default SNMP RO community string "public."

**Table 4: SNMPv2c**

Field	Description
Read Community	SNMP read-only (RO) or read/write (RW) community string.  The SNMP community string that you configure in this field is used only for this specific discovery. To set up default SNMP community strings that can be saved and used for all discoveries, go to <b>Settings &gt; Discovery Credentials</b> .  <b>Note</b> To enable discovery on the network devices, configure the network device's IP host address as the client address.
Write Community	SNMP read-only (RO) or read/write (RW) community string.

**Note** Certain **SNMPv3** configuration options are or are not available depending upon your selections.

**Table 5: SNMPv3**

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: <ul style="list-style-type: none"> <li>• <b>noAuthNoPriv</b>—Security level that does not provide authentication or encryption</li> <li>• <b>AuthNoPriv</b>—Security level that provides authentication but does not provide encryption</li> <li>• <b>AuthPriv</b>—Security level that provides both authentication and encryption</li> </ul>
Auth Type	Specifies the authentication type to be used. <ul style="list-style-type: none"> <li>• <b>SHA</b>—Authentication based on the Hash-Based Message Authentication Code (HMAC), Secure Hash algorithm (SHA) algorithm</li> <li>• <b>MD5</b>—Authentication based on the Hash-Based Message Authentication Code (HMAC), Message Digest 5 (MD5) algorithm</li> <li>• <b>None</b>—No authentication</li> </ul>
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3.
Privacy Type	Specifies the privacy type: <ul style="list-style-type: none"> <li>• <b>DES</b>—Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.</li> <li>• <b>AES128</b>—Cipher Block Chaining (CBC) mode AES for encryption.</li> <li>• <b>None</b>—No privacy</li> </ul>
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.

**Table 6: SNMP Properties**

Field	Description
Connection 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.
Retry Count	Number of attempts to connect to the device. Valid values are from 0 to 4 attempts.

**Step 5** In the **CLI Credentials** area, enter the username, password, and enable password in the fields for the devices that you want the Cisco APIC-EM to discover.

Both the password and enable password are encrypted for security reasons and cannot be seen when viewing the configuration.

Discovery credentials are preexisting device credentials used by the Cisco APIC-EM to authenticate and discover the Cisco devices in your network. The Cisco APIC-EM supports two types of discovery credentials: common discovery credentials and exception discovery credentials.

**Note** Although you are limited to only one set of discovery credentials per discovery scan, you can run several different discovery scans with different credentials to authenticate and discover all of the Cisco devices within your network.

**Step 6** (Optional) In the **Advanced** area, configure the protocols that the Cisco APIC-EM uses to connect to devices. By default, the Cisco APIC-EM uses the following protocols:

- SSH
- Telnet

To remove a protocol from the scan, click the protocol name. The checkmark next to the protocol disappears and the protocol fades from the display.

To customize the order that protocols are used to connect to devices, drag and drop a selected protocol to the desired location in the list.

**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 a Discovery Using an IP Address Range

You can discover devices using an IP address range.

Note that while a discovery is in progress, you can do any of the following actions:

- Create a new discovery by clicking **Add New** from the **Discoveries** pane.
- Stop an active discovery by selecting the discovery name in the **Discoveries** pane and clicking **Stop** in the **Discovery Details** pane.
- Start an inactive discovery by selecting the discovery name in the **Discoveries** pane and clicking **Start** in the **Discovery Details** pane.
- Delete a discovery by selecting the discovery name in the **Discoveries** pane and clicking **Delete** in the **Discovery Details** pane.

### Before You Begin

You must have administrator permissions. For information about the user permissions, see [Managing Users and Roles](#), on page 41.

- 
- Step 1** From the **Navigation** pane, click **Discovery**.  
The **Discovery** window appears.
- Step 2** (Optional) In the **Discovery Name** field, enter a unique name for this discovery.
- Step 3** In the **IP Ranges** area, do the following:
- From the **Discovery Type** field, choose **Range** for the discovery scan type.
  - In the **IP Address** field, enter the beginning and ending IP addresses (IP range) for the devices being discovered and click **Add**.  
You can enter a single IP address range or multiple IP addresses for the discovery scan.
  - Enter any additional IP addresses in the IP address fields and click **Add**.
- Step 4** In the **SNMP** area, configure one or both of the SNMP versions that are being used by the devices in your network. Use the following guidelines and the information in the following tables to help you enter the correct values in the fields:
- The controller supports up to five SNMP credential configurations.
  - An SNMP Read Only (RO) community string is required to assure a successful discovery and populated inventory. However, if an SNMP RO community string is not provided, discovery runs with the default SNMP RO community string "public" as a *best effort* discovery scan.

**Table 7: SNMPv2c**

Field	Description
Read Community	SNMP read-only (RO) or read/write (RW) community string.  The SNMP community string that you configure in this field is used only for this specific discovery only. To set up default SNMP community strings that can be saved and used for all discoveries, go to <b>Settings &gt; Discovery Credentials</b> .  <b>Note</b> To enable discovery on the network devices, configure the network device's IP host address as the client address.
Write Community	SNMP read-only (RO) or read/write (RW) community string.

**Note** Depending on your selections, certain **SNMPv3** configuration options are or are not available.

**Table 8: SNMPv3**

Field	Description
Username	Username associated with the SNMPv3 settings.



Field	Description
Mode	Specifies the security level that an SNMP message requires and whether the message needs to be authenticated. Choose one of the following modes: <ul style="list-style-type: none"> <li>• <b>noAuthNoPriv</b>—Security level that does not provide authentication or encryption</li> <li>• <b>AuthNoPriv</b>—Security level that provides authentication but does not provide encryption</li> <li>• <b>AuthPriv</b>—Security level that provides both authentication and encryption</li> </ul>
Auth Type	Specifies the authentication type to be used. <ul style="list-style-type: none"> <li>• <b>SHA</b>—Authentication based on the Hash-Based Message Authentication Code (HMAC), Secure Hash algorithm (SHA) algorithm</li> <li>• <b>MD5</b>—Authentication based on the Hash-Based Message Authentication Code (HMAC), Message Digest 5 (MD5) algorithm</li> <li>• <b>None</b>—No authentication</li> </ul>
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3.
Privacy Type	Specifies the privacy type: <ul style="list-style-type: none"> <li>• <b>DES</b>—Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.</li> <li>• <b>AES128</b>—Cipher Block Chaining (CBC) mode AES for encryption.</li> <li>• <b>None</b>—No privacy</li> </ul>
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.

**Table 9: SNMP Properties**

Field	Description
Connection 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.
Retry Count	Number of attempts to connect to the device. Valid values are from 0 to 4 attempts.

**Step 5** In the **CLI Credentials** area, enter the *exception* username, password, and enable password for the devices that you want to discover. You can add up to five CLI credentials.

**Note** Both the password and enable password are encrypted for security reasons and cannot be seen when viewing the configuration.

**Note** Although you are limited to only one set of discovery credentials per discovery scan, you can run several different discovery scans with different credentials to authenticate and discover all of the Cisco devices within your network.

**Step 6** (Optional) In the **Advanced** area, configure the protocols that the Cisco APIC-EM uses to connect to devices. By default, the Cisco APIC-EM attempts to connect to devices using the following protocols:

- SSH
- Telnet

To remove a protocol from the scan, click the protocol name. The checkmark next to the protocol disappears and the protocol fades from the view.

To customize the order that protocols are used to connect, drag and drop a selected protocol to the top of the list.

**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.

---

## Stopping and Starting a Discovery

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

### Before You Begin

You must have administrator permissions. For information about the user permissions, see [Managing Users and Roles](#), on page 41.

---

**Step 1** From the **Navigation** pane, click **Discovery**. The **Discovery** window appears.

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

- From the **Discoveries** pane, select the discovery.
- From the **Discovery Details** pane, click **Stop**.
- Click **OK** to confirm that you want to stop the discovery.

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

- From the **Discoveries** pane, select the discovery.
- From the **Discovery Details** pane, click **Start**.

---

## Deleting a Discovery

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

### Before You Begin

You must have administrator permissions. For information about the user permissions, see [Managing Users and Roles](#), on page 41.

- 
- Step 1** From the **Navigation** pane, click **Discovery**.  
The **Discovery** window appears.
- Step 2** From the **Discoveries** pane, select the discovery 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 window provides information about the selected scan. To access the **Discovery** window, from the **Navigation** pane, click **Discovery**. The **Discovery Results** window has three main panes.



**Note** You must have created at least one discovery scan for the **Discovery Results** window to display.

Figure 3: Discovery Results Window

The screenshot shows the Discovery Results window with three numbered callouts:

- 1**: Points to the Discoveries list on the left, showing an active discovery 'Boston' and an inactive discovery 'SFNet'.
- 2**: Points to the device status and details for 'SFNet', showing 5 devices, an 'Inactive' status, and a 'Start' button. The details include CDP Level (16), Protocol Order (ssh telnet), Retry Count (3), TimeOut (5), Discovery Condition (Complete), and IP List (40.0.64.21).
- 3**: Points to the table of devices found in this discovery, listing host names, IP addresses, and their status.

Host Name	IP	Status
SDN-DEV-2960.cisc o.com	40.0.64.21	Success
SDN-DEV-3750.cisc o.com	40.0.64.19	Success
SDN-DEV-6K1	40.0.64.17	Success
SDN-DEV-3650.cisc o.com	40.0.64.20	Success
SDN-DEV-6K2.cisc o.com	40.0.64.18	Success
	40.0.64.13	Unreachable

Callout Number	Name	Description
1	Discoveries pane	<p>Lists the names of the discovery scans that have been created, along with the method and IP addresses used for discovery. The list is divided between active and inactive discoveries.</p> <p>A successful scan (one with discovered and authenticated devices) has the number of discovered devices indicated in a box to the right of the discovery name. An unsuccessful scan shows no box or number of devices discovered.</p> <p>From the <b>Discoveries</b> pane, clicking on a discovery name displays the information in the <b>Discovery Details</b> and <b>Device Details</b> panes.</p>
2	Discovery Details pane	<p>Provides detailed information about the discovery parameters that were used to perform the discovery, the state of the discovery, and the number of devices that were discovered. The buttons on this pane allow you to <b>Start</b>, <b>Stop</b>, and <b>Delete</b> discoveries.</p>
3	Devices pane	<p>Displays the host name, IP address, and status of the devices found during the scan.</p>





## Managing Devices and Hosts

- [Managing Your Device Inventory, page 21](#)
- [Managing Your Host Inventory, page 38](#)

### 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**. The **Device Inventory** window appears.

Figure 4: Device Inventory Window

Device Name	IP Address	Device Status	Up Time	Last Updated Time	Last Inventory Collection Status
<a href="#">SDN-DEV-2960.cisco.com</a>	40.0.64.21	Reachable	42 days, 23:46:46.77	9 minutes ago	Partial Collection Failure
<a href="#">SDN-DEV-3650.cisco.com</a>	40.0.64.20	Reachable	42 days, 23:27:57.08	22 minutes ago	Partial Collection Failure
<a href="#">SDN-DEV-3750.cisco.com</a>	40.0.64.19	Reachable	42 days, 23:48:01.21	8 minutes ago	Partial Collection Failure
<a href="#">SDN-DEV-6K1</a>	40.0.64.17	Reachable	42 days, 23:35:44.71	21 minutes ago	Partial Collection Failure
<a href="#">SDN-DEV-6K2.cisco.com</a>	40.0.64.18	Reachable	42 days, 23:44:12.06	13 minutes ago	Partial Collection Failure

10 5 Devices First Previous 1 Next Last



**Note**

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

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

Callout Number	Name	Description
1	Device Selection check boxes	Select devices to perform tasks.
2	<b>Filters</b>	Allows you to selectively screen the devices that are displayed in the table by name, location tag, and IP address.
3	<b>Layout</b>	Allows you to choose from three predefined layouts or a customized layout: <ul style="list-style-type: none"> <li>• <b>Status</b>—Layout shows the device name, IP address, state of the device, how long it has been up, and the last time it was updated.</li> <li>• <b>Hardware</b>—Layout shows the device name, IP address, device family, platform, serial number, MAC address, and role, along with its IOS/firmware version and a link to its configuration file.</li> <li>• <b>Tagging</b>—Layout shows the device name, IP address, MAC address, device role, location, and tags.</li> </ul>

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.

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.



**Table 10: Device Inventory**

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

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

Device Inventory	Description
Device Role	<p>Role assigned to each discovered device during the scan process. The device role is used to identify and group devices according to their responsibilities and placement within the network. If the controller is unable to determine a device role, it sets the device role as unknown.</p> <p><b>Note</b> The controller can change the device role as the network topology changes, but if you manually change the device role, then the role will not change as the network topology changes.</p> <p>If desired, you can use the drop-down list in this column to change the assigned device role. The following device roles are available:</p> <ul style="list-style-type: none"><li>• Unknown</li><li>• Access</li><li>• Core</li><li>• Distribution</li><li>• Border Router</li></ul>

Device Inventory	Description
Location	<p>Exactly one location can be applied to a device. Location information is maintained only by the APIC-EM controller; the location applied to a device is not available from the device itself. An APIC-EM location is not the "civic-location" property that some devices support. You cannot create or use locations in Topology view; therefore, locations cannot be attached to hosts, and you cannot search on location in Topology view. Location is a specific type of tag that can be applied to a device. A tag enables a grouping of devices based on an attribute.</p> <p>Click <b>Add</b> in this column to open a <b>Location</b> window. You can add either an existing or new location in this window.</p> <p>You can also add a geographical marker on a world map to the device. To add a geographical marker to a device:</p> <ul style="list-style-type: none"> <li>• Click <b>Add Marker</b> and move the marker icon to a location on the world map.</li> <li>• Click <b>Set Coordinates</b> to set the exact coordinates for the location on the world map.</li> <li>• Click <b>Remove Marker</b> to remove the marker from the world map.</li> </ul> <p>To view the world map, from the <b>Topology</b> window, click the <b>Map</b> icon.</p> <p><b>Note</b> You can apply only one location tag per device.</p>
Tag	<p>Attribute assigned to a device to identify it or to group it with other devices with the same attribute. For example, you can create a tag and use it to group devices based on a platform ID, Cisco IOS releases, or location.</p> <p>A number in the <b>Tag</b> column indicates how many tags have been applied to that device.</p> <p>Click the number or <b>Add</b> in this column to open a <b>Tag</b> dialog box. You can add an existing tag or create a new tag.</p> <p><b>Note</b> You are permitted to use both a location tag and a device tag together.</p> <p><b>Note</b> To globally delete a tag, first remove the tag from devices that it is attached to.</p>
Last Updated Time	<p>The date and time that the device was last scanned and the controller database was updated.</p>

Device Inventory	Description
Device Family	Group of related devices, as follows: <ul style="list-style-type: none"> <li>• Cisco Interfaces and Modules</li> <li>• Routers</li> <li>• Switches and Hubs</li> <li>• Third Party Device</li> <li>• Unsupported Cisco Device</li> <li>• Wireless Controller</li> </ul>
Device Series	Series number of the device, for example, Cisco Catalyst 4500 Series Switches.
Average Update Frequency	Average number of minutes between updates to the device. By default, devices are polled every 25 minutes.
Last Inventory Collection Status	Status of the last discovery scan for the device: <ul style="list-style-type: none"> <li>• <b>Managed</b>—Device is in a fully managed state.</li> <li>• <b>Partial Collection Failure</b>—Device is in a partial collected state and not all the inventory information has been collected.</li> <li>• <b>Unreachable</b>—Due to device connectivity issues, the device could not be reached and no inventory information was collected. This condition can occur when periodic collection happens.</li> <li>• <b>Wrong Credentials</b>—If the device credentials are changed after adding the device to the inventory, this condition is noted.</li> <li>• <b>In Progress</b>—Inventory collection is occurring.</li> </ul>

### Related Topics

- [Changing the Device Role, on page 29](#)
- [Adding or Removing a Tag, on page 31](#)
- [Adding or Removing Tags to Multiple Devices](#)
- [Adding or Removing a Location Tag, on page 33](#)
- [Adding a Location Marker, on page 34](#)

## Filtering the Devices Table View

You can filter the devices displayed in the **Devices** table by device name, location, and IP address.

### Before You Begin

Access the **Device Inventory** window by clicking **Device Inventory** from the **Navigation** pane.

---

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

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

**Step 2** Enter the appropriate value in a selected filter field.  
For example, for the **Device IP Address** filter enter an IP address.

**Note** The controller presents you with auto-complete values as you enter the IP address or any of the other fields. Choose one of the suggested values or finish entering the IP address.

**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 required for your filter, add one or 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** Click the x icon to close the filter field or fields and return to the original **Devices** table display.

---

### 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.

### Before You Begin

Access the **Device Inventory** window by clicking **Device Inventory** from the **Navigation** pane.

---

**Step 1** From the **Device Inventory** toolbar, choose a layout option.

The following layout options are available:

- **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.

After selecting a specific layout, the information in the **Devices** table adjusts for the new display.

## Step 2

To customize a specific layout, choose **Customize** and the desired display option.

**Note** Display options toggle on and off with a checkmark indicating that the option is on (displayed in the table).

After making a selection, a new column is added to the **Devices** table and your selected option on the list turns blue with a check mark.

---

### What to Do Next

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

- Device Role
- Location
- Tag

## 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.

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 the Device Role in the Topology Window](#), on page 67.

---

### Before You Begin

Access the **Device Inventory** window to change the role of a device.



**Note** You must have administrator permissions to perform the following procedure. For information about the user permissions required to perform tasks using the Cisco APIC-EM, see Chapter 4, *Managing Users and Roles*.

- 
- 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.

### Related Topics

[Managing Your Device Inventory, on page 21](#)

## Deleting a Device

From the **Device Inventory** window, you can delete a device from the Cisco APIC-EM database.

### Before You Begin

Ensure that you have administrator permissions. For information about the user permissions, see [Managing Users and Roles, on page 41](#).

Ensure that your network has been scanned using the discovery functionality of the Cisco APIC-EM to populate device inventory database.

- 
- Step 1** From the **Navigation** pane, click **Device Inventory**.  
The **Devices Inventory** window appears.
- 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 toolbar that opens, click **Delete**.

---

## Adding or Removing a Tag

A device tag allows you to group devices based on an attribute. For example, you can add a tag and group devices based on a platform ID, Cisco IOS release, or location.



**Note** A single device can have multiple tags; similarly, a single tag that can be applied to multiple devices.

You can add tags to or remove tags from devices in the **Device Inventory** window.

### Before You Begin



**Note** You must have administrator permissions. For information about the user permissions, see [Managing Users and Roles](#), on page 41.

---

**Step 1** From the **Navigation** pane, click **Device Inventory**.  
The **Devices Inventory** window appears.

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

**Step 3** Click the check box to the left of the name of the device that you want to apply a tag to or remove a tag from. You can select more than one device.  
The **Set Location** and **Add Tag** drop-down buttons appear.

**Note** If you want to add or remove tags on one device only, you can also click the number in the **Tag** column for the desired device. This action brings up the **Multiple Device Tagging** dialog box. Proceed to Step 5.

**Step 4** Click **Add Tag**.  
The **Multiple Device Tagging** dialog box appears.

**Step 5** Do one of the following:

- Apply a tag.
- a) From the **Available Tags** list, click the tag or tags that you want to apply to the selected devices.  
After the tag is applied to the device, it appears in the **Applied Tags** list.
- b) If the tag is not in the list, enter a name for the tag and click **+New Tag**.  
The new tag appears in the **Available Tags** list. Return to the previous step and apply the tag.
- c) Click **x** to close the dialog box.
- Remove a tag.

- a) From the **Applied Tags** list, click the **Trash can** icon next to the tag or tags that you want to remove from the selected devices.

**Note** The **Applied Tags** list is populated if at least one device has a tag applied to it. The **Applied Tags** list displays the number of devices each tag has applied to it or whether all devices are applied to it. The tag is removed from the device and is removed from the **Applied Tags** list.

- b) Click **x** to close the dialog box.
- 

### What to Do Next

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

### Related Topics

[Managing Your Device Inventory, on page 21](#)

## Deleting a Tag

Before you delete a tag, you need to remove it from all devices.

You can delete tags from the controller in the **Device Inventory** window or the **Topology** window. This procedure shows you how to delete tags from the **Device Inventory** window.

### Before You Begin

Access the **Device Inventory** window by clicking **Device Inventory** from the **Navigation** pane.



#### Note

You must have administrator permissions. For information about the user permissions, see [Managing Users and Roles, on page 41](#).

---

### 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. Click the check box to the left of the name of the device that you want to remove a tag from. You can select more than one device.
4. Click **Add Tag**.
5. From the **Applied Tags** list, click the **Trash can** icon next to the tag or tags that you want to remove from the selected devices.
6. From the **Available Tags** list, click the **Trash can** icon next to the tag or tags that you want to delete from the controller.
7. Click **OK** to confirm the deletion.
8. Click **x** to close the dialog box.

## DETAILED STEPS

---

- Step 1** From the **Navigation** pane, click **Device Inventory**.  
The **Devices Inventory** window appears.
- Step 2** From the **Device Inventory** toolbar, choose **Layout > Tagging** from the drop-down list.  
The table refreshes and, in addition to other information, displays a **Tag** column.
- Step 3** Click the check box to the left of the name of the device that you want to remove a tag from. You can select more than one device.  
The **Set Location** and **Add Tag** buttons appear in the **Device Inventory** toolbar.
- Note** If you want remove and delete tags from one device only, you can also click the number in the **Tag** column for the desired device. This action brings up the **Multiple Device Tagging** dialog box. Proceed to Step 5.
- Step 4** Click **Add Tag**.  
The **Multiple Device Tagging** dialog box appears.
- Step 5** From the **Applied Tags** list, click the **Trash can** icon next to the tag or tags that you want to remove from the selected devices.
- Note** The **Applied Tags** list is populated if at least one device has a tag applied to it. The **Applied Tags** list displays the number of devices each tag has applied to it or whether all devices are applied to it.  
The tag is removed from the device and is removed from the **Applied Tags** list.
- Step 6** From the **Available Tags** list, click the **Trash can** icon next to the tag or tags that you want to delete from the controller.  
A confirmation dialog box appears.
- Step 7** Click **OK** to confirm the deletion.  
The tag is removed from the **Available Tags** list. If the deletion fails, it may be due to the tag still being assigned to devices. Remove the tag from these devices and try to delete the tag again.
- Step 8** Click **x** to close the dialog box.
- 

### What to Do Next

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

## Adding or Removing a Location Tag

A location tag enables the grouping of devices based upon a location attribute.

You add or remove locations to a device in the **Devices** table.

### Before You Begin

Access the **Device Inventory** window to add or remove a location to a device in the **Devices** table.

**Note**

You must have administrator permissions to perform the following procedure. For information about the user permissions required to perform tasks using the Cisco APIC-EM, see Chapter 4, *Managing Users and Roles*.

- 
- Step 1** Select **Tagging** from the **Layout** field at the top of the **Devices** table, or select **Customize** and choose **Location** from the drop-down list.  
The **Devices** table adjusts its display to include a **Location** column.
- Step 2** (Optional) To add a new location to the **Available Locations** column, enter a location for the device and click the + **New Location** button in this window.  
The new location then appears in the **Available Locations** column.
- Step 3** Click an existing location in the **Available Locations** column to add that location to the device. The new location is then moved to the **Applied Location** column.  
**Note** To remove an existing location, click the **trash can** icon to the left of the location in the **Applied Location** column. The location is then moved to the **Available Locations** column.
- Step 4** Click the **X** icon at the upper right of the **Location** window to save your new location to the device.
- 

**What to Do Next**

If required for your network configuration, add or remove other locations to other devices.

**Related Topics**

[Managing Your Device Inventory](#), on page 21

[Adding a Location Marker](#), on page 34

## Adding and Removing Location Markers

In addition to adding a location tag to a device, you can add a location marker that represents your device's geographical location on a world map. You can view these markers in the **Topology** window.

### Adding a Location Marker

You can add a location marker to the devices in the **Device Inventory** window.

**Before You Begin**

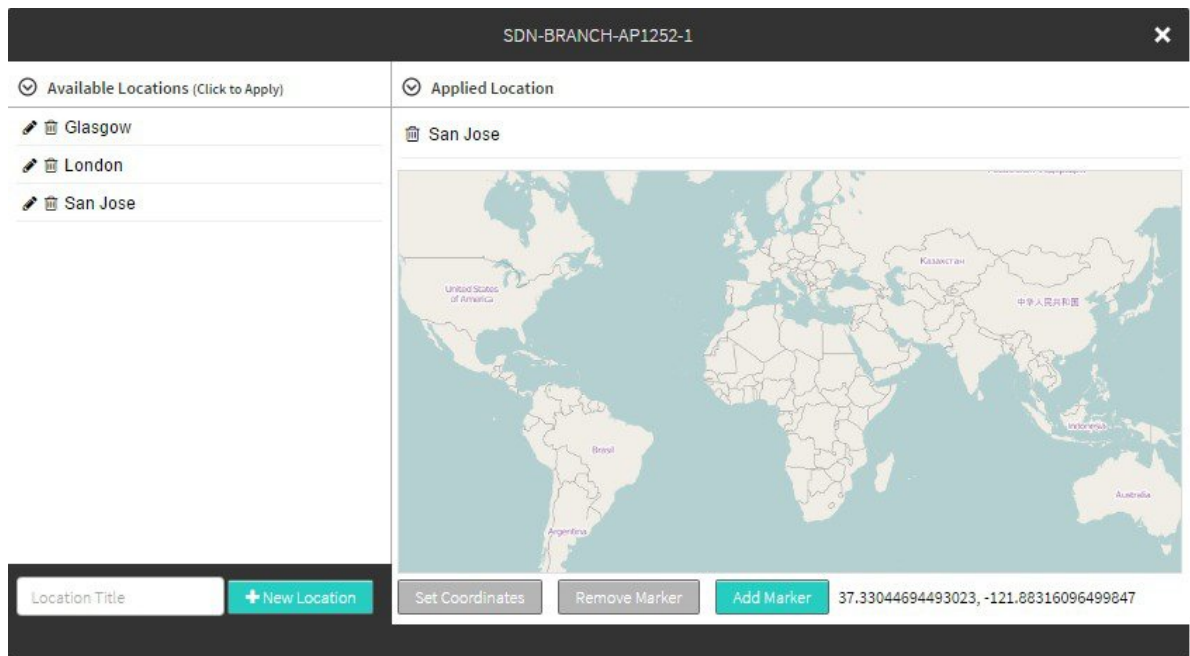
You must have administrator permissions.

You have already added location tags to your devices.

- 
- Step 1** From the **Navigation** pane, click **Device Inventory**.  
The **Device Inventory** window appears.

- Step 2** From the **Device Inventory** toolbar, choose **Layout > Tagging** from the drop-down list. The table refreshes and, in addition to other columns, displays a **Location** column.
- 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** Click a location from the **Location** column. The **Location** dialog box appears with the name of the device at the top. The location tag appears in the **Applied Locations** list.

**Figure 5: Location Window**

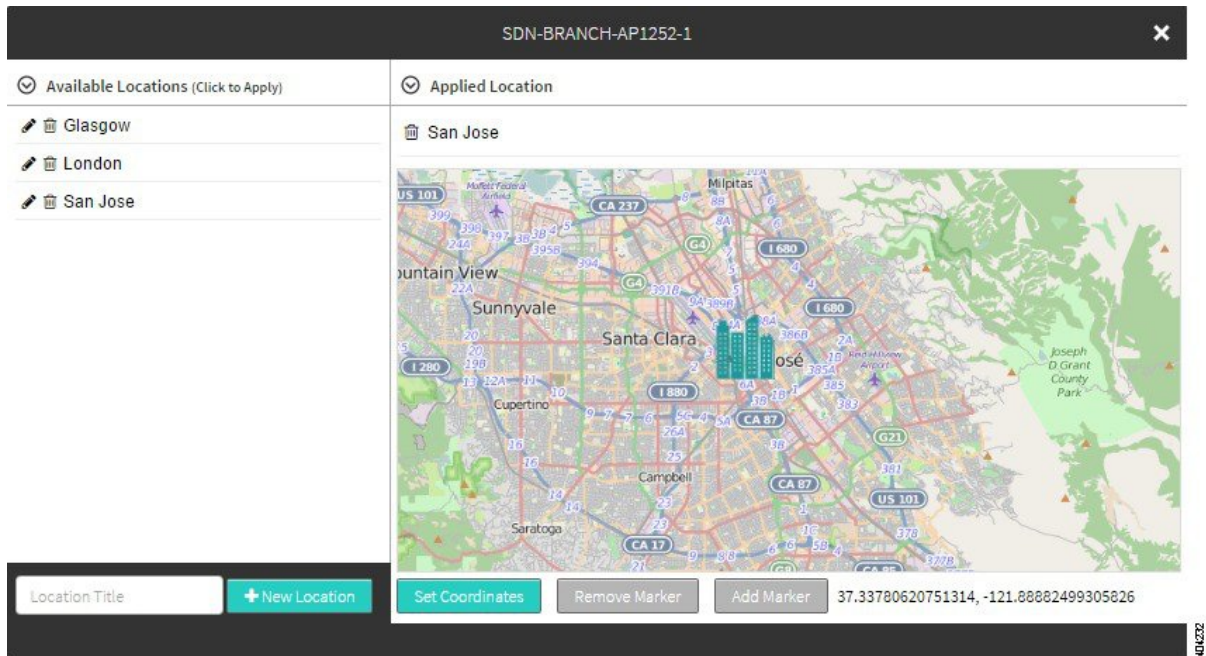


**Step 5** (Optional) Drag and zoom the map to get a detailed location on the map.

**Step 6** Click **Add Marker** to add a location marker to the map.

**Step 7** Drag the marker to the specific location on the map.

**Figure 6: Placing the Location Marker**



**Step 8** Click **Set Coordinates** to set the coordinates of the marker.

**Step 9** Click **X** to close the dialog box.

**Note** To add additional location markers, close the **Location** dialog box and click another location from the **Location** column. If you select another location in the current **Location** dialog box, you will apply that location to the currently selected device.

### What to Do Next

Add additional location markers for all of your locations.

Access the **Topology** window to view the location markers on a map.

### Related Topics

[Managing Your Device Inventory](#), on page 21

[Topology](#)

[Topology Icons](#), on page 60

[Topology Toolbar](#)

## Removing a Location Marker

You can remove location markers from the devices in the **Device Inventory** window.

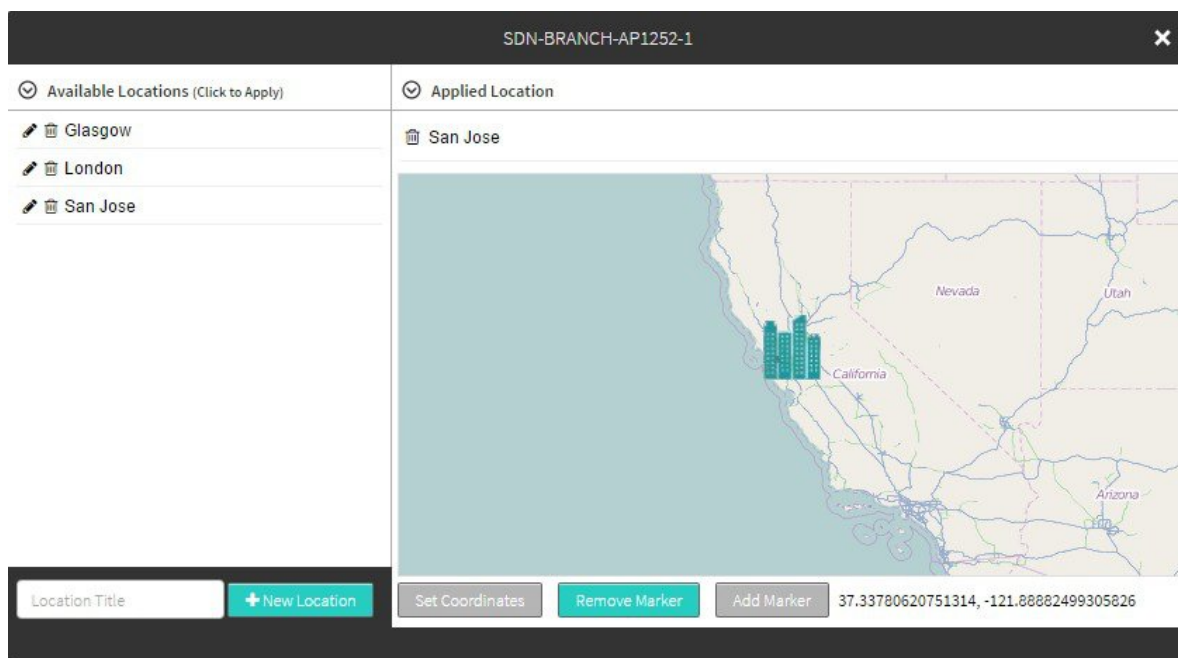
### Before You Begin

You must have administrator permissions.

You have already added a location marker.

- 
- Step 1** From the **Navigation** pane, click **Device Inventory**.  
The **Device Inventory** window appears.
- Step 2** From the **Device Inventory** toolbar, choose **Layout > Tagging** from the drop-down list.  
The table refreshes and, in addition to other columns, displays a **Location** column.
- 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** For the desired device, click the location in the **Location** column.  
The **Location** dialog box appears with the name of the device at the top. The location tag appears in the **Applied Locations** list.

**Figure 7: Location Window**



- Step 5** Click the **Remove Marker** button.
- Step 6** Click **X** to close the dialog box.

**Note** To add additional location markers, close the **Location** dialog box and click another location from the **Location** column. If you select another location in the current **Location** dialog box, you will apply that location to the currently selected device.

## Managing Your Host Inventory

The **Host Inventory** window displays the discovered hosts and users in your network.

To view your host inventory, click **Host Inventory** in the Navigation pane. The **Host Inventory** window opens, listing the discovered hosts in your network. 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 a hosts at a time (First, Previous, Next, Last, or 1-3).

**Figure 8: Host Inventory Window**

Host Name	Host MAC Address	Host IP Address	Host Type	Connected Network Device IP Address
ise-12-9	00:0c:29:84:a2:d5	10.108.107.100	WIRED	10.108.107.100
ova3495	00:0c:29:85:38:bd	10.108.255.252	WIRED	10.108.255.87
platinum-pap1	00:0c:29:87:06:7a	10.108.107.100	WIRED	10.108.107.100
	00:0c:29:9b:eb:8f	10.108.107.100	WIRED	10.108.107.100
	00:0c:29:9d:ca:3a	10.108.107.111	WIRED	10.108.107.100
	00:0c:29:a0:c3:8e	10.108.107.148	WIRED	10.108.107.100
	00:0c:29:a4:60:cf	10.108.142.110	WIRED	10.108.142.101
	00:0c:29:b7:0b:01	10.108.107.100	WIRED	10.108.107.100
	00:0c:29:bd:4c:49	10.108.255.100	WIRED	10.108.255.100
	00:0c:29:bf:c7:c1	10.108.255.25	WIRED	10.108.255.100

10 per page ▼ 300 Hosts < Previous 5 of 30 Next >

**Table 11: Host Inventory**

Host Inventory	Description
Host Name	Name of the host.
Host MAC address	MAC address of the host.
Host IP address	IP address of the host.



Host Inventory	Description
Host type	Type of host (wired or wireless).
Connected Network Device IP Address	IP address of the device that is connected to the host.
Connected Interface Name	Name of the interface that the device is connected to. For example, GigabitEthernet1/0/24.

### Related Topics

[Changing the Hosts Table View, on page 39](#)

## Changing the Hosts Table View

You can change the information that is displayed in the **Hosts** table by accessing a **Hosts** checklist and choosing the data that you wish to display.

### Before You Begin

Access the **Host Inventory** window to change the information that is displayed within the **Hosts** table.

- 
- Step 1** Place your cursor over the **Wheel** icon at the top left of the **Hosts** table in the **Host Inventory** window to access a **Host Inventory** checklist.  
After placing your cursor over the **Wheel** icon, the **Hosts** checklist appears.
- Step 2** Choose the information that you want displayed in the **Hosts** table by checking the appropriate box on the list. For example, if you want the **Hosts** table to display the host type (wired or wireless), choose **Host Type** from the list by checking it.
- Step 3** Close the **Host Inventory** checklist by clicking anywhere outside of it.
- 

### What to Do Next

Review the updated information displayed in the **Host Inventory** window.

### Related Topics

[Managing Your Host Inventory, on page 38](#)





## Managing Users and Roles

---

- [About Role-Based Access Control, page 41](#)
- [About User Roles, page 41](#)
- [About AAA, page 43](#)
- [Changing Your Password, page 45](#)
- [Configuring Users and Roles, page 47](#)

### About Role-Based Access Control

The Cisco APIC-EM supports role-based access control (RBAC). RBAC is a method of restricting or authorizing controller access for users based on their user roles. A role defines the privileges of a user on the controller. Because users are not directly assigned privileges, the management of individual user privileges is simply a matter of assigning the appropriate roles to users who need access the Cisco APIC-EM GUI.

### About User Roles

When you deploy the Cisco APIC-EM for the first time, the configuration wizard prompts for a username and password. This first-time user is given full administrative (read and write) permissions for the controller and is able to create user accounts for other users.



**Note**

---

Only users with the administrative role can create users and assign user roles.

---

Users are assigned roles that determine the functions that they are permitted to perform:

- Administrator (ROLE\_ADMIN)—Provides full administrative privileges to all Cisco APIC-EM resources, including the ability to add or remove users and accounts. For more information, see [Administrator Role, on page 42](#).




---

**Note** We highly recommend that you configure at least two users with administrator (ROLE\_ADMIN) privileges. In the unlikely event that one user is locked out or forgets his or her password, you have another user with administrative privileges who can help you to recover from this situation.

---

- Observer (ROLE\_OBSERVER)—Provides primarily read-only privileges to the Cisco APIC-EM. For information, see [Observer Role, on page 42](#).
- Installer (ROLE\_INSTALLER)—Allows an installer to use the Cisco Plug and Play Mobile App to remotely access the APIC-EM controller to deploy devices and view their status. An installer cannot directly access the Cisco APIC-EM GUI.

For information, see [Installer Role, on page 43](#).

## Administrator Role

Users with the administrator role have full administrative privileges to all Cisco APIC-EM resources, including the ability to add or remove users and accounts. Users with the administrator role (ROLE\_ADMIN) can perform the following tasks:

- Change their own password (by providing current password).
- Create a new user with administrator (ROLE\_ADMIN) or observer (ROLE\_OBSERVER) privileges.
- View all other users with their role and scope.
- Edit any other user role including their own.
- Delete any user including themselves.

Although an administrator cannot directly change another user's password in the GUI, an administrator can delete and then re-create the user with a new password using the GUI.

For information about the specific resources available to the administrator role, see [Cisco APIC-EM Resources and Permissions, on page 44](#).




---

**Note** For security reasons, passwords are not displayed to any user, not even those with administrator privileges.

---




---

**Note** We highly recommend that you configure at least two users with administrator (ROLE\_ADMIN) privileges. In the unlikely event that one user is locked out or forgets his or her password, you have another user with administrative privileges who can help you to recover from this situation.

---

## Observer Role

The observer role provides read-only privileges to the Cisco APIC-EM. Users who are assigned the observer role (ROLE\_OBSERVER) can change their own password (by providing current password).

They cannot perform the following tasks:

- Edit their role or scope
- Delete themselves
- View their own password
- View the list of devices in the device inventory.

For information about the specific resources available to the observer role, see [Cisco APIC-EM Resources and Permissions](#), on page 44.

**Note**

---

For security reasons, passwords are not displayed to any user, not even those with administrator privileges.

---

## Installer Role

Users who are assigned the installer role (ROLE\_INSTALLER) can use the Cisco Plug and Play Mobile App to access the Cisco APIC-EM remotely to perform the following functions:

- View device status.
- Trigger device deployments.

Installers cannot directly access the Cisco APIC-EM GUI.

**Note**

---

For security reasons, passwords are not displayed to any user, not even those with administrator privileges.

---

## Users and Domains

You can create multiple users for the different domains (network or sub-networks) in your network. Each user can have a different role in a different domain. For example, a user can have an observer role in Network A and an administrator role in Network B.

## About AAA

### Authentication and Authorization

Users and their roles are subject to an authentication and authorization process.

With the Cisco APIC-EM, each resource for the controller is mapped to an action and each action is mapped to a required permission for a user. All REST APIs are therefore protected by the controller authentication process. For a list of resources and the roles that are allowed access to them, see [Cisco APIC-EM Resources and Permissions](#), on page 44.

**Note**

Depending upon your user role and its permissions, certain Cisco APIC-EM GUI functionality will not display. To view the role behavior (for example, administrator, installer, and observer) side-by-side in the GUI, you need to either use multiple Chrome browsers or incognito mode in the Chrome browser. You will not be able to view the role behavior side-by-side in a single Chrome browser using tabs.

## Cisco APIC-EM Resources and Permissions

The following table describes the role permissions that are required for each Cisco APIC-EM resource.

**Note**

Depending upon your role and its permissions, certain Cisco APIC-EM GUI functionality will not display. To view the role behavior (for example, administrator and observer) side-by-side in the GUI, you need to either use multiple browsers or incognito mode in the browser. You will not be able to view the role behavior side-by-side in a single browser using tabs.

**Table 12: Cisco APIC-EM Resources and Permissions**

Resource	Role Permissions
Discovery: Scan	<ul style="list-style-type: none"> <li>• Administrator</li> </ul>
Inventory: Retrieving inventory list with device credentials	<ul style="list-style-type: none"> <li>• Administrator</li> </ul>
Inventory: Adding tags	<ul style="list-style-type: none"> <li>• Administrator</li> <li>• Observer</li> </ul>
Inventory: Creating device roles	<ul style="list-style-type: none"> <li>• Administrator</li> <li>• Observer</li> </ul>
Inventory: Actions other than adding tags and creating device roles	<ul style="list-style-type: none"> <li>• Administrator</li> <li>• Observer</li> </ul>
Role-based access control: Creating and deleting users and security roles	<ul style="list-style-type: none"> <li>• Administrator</li> <li>• Observer can view and change own password.</li> </ul>
File Service	<ul style="list-style-type: none"> <li>• Administrator</li> </ul>

Resource	Role Permissions
Host	<ul style="list-style-type: none"> <li>• Administrator</li> <li>• Observer</li> </ul>
Task ID	<ul style="list-style-type: none"> <li>• Administrator</li> <li>• Observer</li> </ul>
Telemetry	<ul style="list-style-type: none"> <li>• Administrator</li> <li>• Observer</li> </ul>
Topology	<ul style="list-style-type: none"> <li>• Administrator</li> <li>• Observer</li> </ul>
Path Analysis	<ul style="list-style-type: none"> <li>• Administrator</li> <li>• Observer</li> </ul>

## Accounting

As an administrator, you can access the content of logs for authenticated sessions. The following information about users, actions, and APIs are captured in these logs for security or troubleshooting purposes:

- Northbound API access data
- Authentication successes with the user name or failures for any method

### Related Topics

[Reviewing the User Logs, on page 51](#)

## Changing Your Password

You can change the password that you use to log into the Cisco APIC-EM.



### Note

You can change only your own password. To change another user's password, you must have administrator privileges. Changing the password involves deleting the user from the controller database and then recreating the user as a new user with a new password.

You can use the password generator provided in the **Change Password** window or the following guidelines to create a secure password.

Create a password of at least 8 characters and one that contains characters from at least three of the following four classes:

- Uppercase alphabet
- Lowercase alphabet
- Numerical digits
- Special characters—include the space character or any of the following characters or character combinations:

! @ # \$ % ^ & \* ( ) - = + \_ { } [ ] \ | ; : " ' , < . > ? / :: # ! . / ; ; >> << ( ) \*\*

In addition to a complex password, you should also ensure that user names do not create security vulnerabilities. To avoid user names that can create security vulnerabilities, the following rules should be followed:

- All users should have unique user names and passwords.
- Do not allow users to use the admin login and password

To avoid creating security vulnerabilities, we recommend that you follow the Cisco APIC-EM password policies when creating a password. For information, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

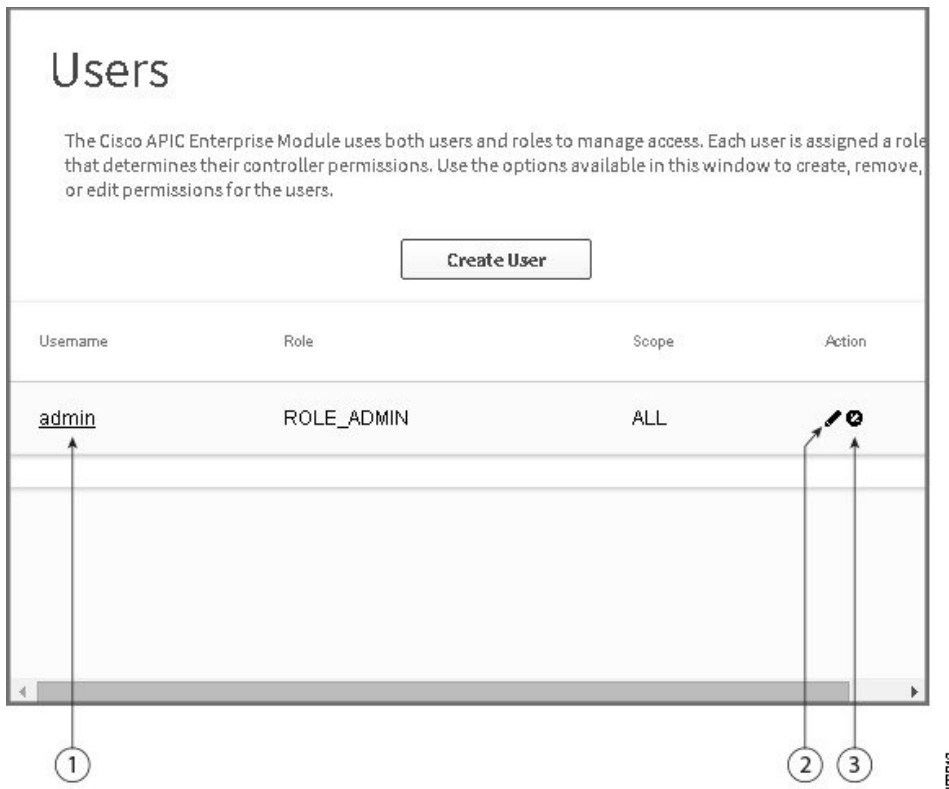
- 
- Step 1** From the **Global** toolbar, click the **Settings** icon.  
The **Settings** window appears.
- Step 2** From the navigation pane in the **Settings** window, click **Change Password**.  
The **Change Password** window appears.
- Step 3** In the **Change Password** window, enter the appropriate values in the following fields:
- **Username**—Your user name appears in this field by default.
  - **Current Password**—Your current password.
  - **New Password**—Your new password. Create your own or, to create a stronger password, click **Generate**, enter a seed phrase, and click **Generate**. You can apply the generated password by clicking **Apply Password**, or you can copy and paste it or any part of it before or after your new password entry.
- Note** We highly recommend that you use the password generator to create a stronger password.
- **Confirm New Password**—Your new password entered a second time as confirmation.
- Step 4** When you are finished, click **Update** to update and save the new password.  
Click **Cancel** to cancel the password change.
-



# Configuring Users and Roles

To access the **Users** window, from the **Global** toolbar click the **Settings** icon. Then from the navigation pane on the Settings window, click **Users**.

Figure 9: Users Window



Numbered Callout	Name	Description
1	Actual username	Displays the user's current access status.
2	Create User	Allows you to add a new user. <a href="#">1</a>
3	Edit	Allows you to change the user role setting. You cannot change any other settings. <a href="#">2</a>
4	Delete	Removes the user from the Cisco APIC-EM database. The deleted user is no longer able to log into the controller. <a href="#">3</a>

- 1 You must be logged in as an administrator (ROLE\_ADMIN) to perform this function.
- 2 You must be logged in as an administrator (ROLE\_ADMIN) to perform this function.
- 3 You must be logged in as an administrator (ROLE\_ADMIN) to perform this function.

## Adding a User

Only a user with the administrator role (ROLE\_ADMIN) can add a user to the Cisco APIC-EM.



**Note** User information (credentials) is stored in a local database on the controller.



**Note** We highly recommend that you configure at least two users with administrator (ROLE\_ADMIN) privileges. In the unlikely event that one user is locked out or forgets his or her password, you have another user with administrative privileges who can help you to recover from this situation.

### Before You Begin

You must be an administrator (ROLE\_ADMIN).

- 
- Step 1** From the **Global** toolbar, click the **Settings** icon.  
The **Settings** window appears.
- Step 2** From the navigation pane in the **Settings** window, click **Users**.  
The **Users** window appears with the following information displayed about the users:
- **Username**—Username assigned to the user.
  - **Role**—Role that defines the user's privileges within the APIC-EM. Valid roles are ROLE\_ADMIN, ROLE\_OBSERVER, or ROLE\_INSTALLER.
  - **Scope**—Domain or tenancy that the user is allowed to access.
  - **Actions**—Icons that allow you to edit user information or delete a user.
- Step 3** Click **Create User**.
- Step 4** In the **Create User** dialog box, enter the username, password (twice), and role of the new user. The scope is set to **SCOPE ALL** by default.
- Step 5** Click **Add**.  
The new user appears in the **Users** window.
- 

### Related Topics

[Users and Roles](#)

## Deleting a User

A user with the administrator role (ROLE\_ADMIN) can delete a user from the Cisco APIC-EM.

### Before You Begin

You must be an administrator (ROLE\_ADMIN).

---

**Step 1** From the **Global** toolbar, click the **Settings** icon.  
The **Settings** window appears.

**Step 2** From the navigation pane in the **Settings** window, click **Users**.  
The **Users** window appears with the following information displayed about the users:

- **Username**—Username assigned to the user.
- **Role**—Role that defines the user's privileges within the APIC-EM. Valid roles are ROLE\_ADMIN, ROLE\_OBSERVER, or ROLE\_INSTALLER.
- **Scope**—Domain or tenancy that the user is allowed to access.
- **Actions**—Icons that allow you to edit user information or delete a user.

**Step 3** Locate the user that you want to delete and, in the **Actions** column, click the **Delete** icon icon  
The user is deleted from the Cisco APIC-EM database and is unable to access the controller.

**Note** You cannot delete the default administrative user. The Cisco APIC-EM requires at least one administrative user who can log into the controller.

---

### Related Topics

[Users and Roles](#)

## Viewing and Editing User Information

A user with the administrator role (ROLE\_ADMIN) can view and change user settings and roles.



---

**Note** User information (credentials) is stored in a local database on the controller.

---

### Before You Begin

You must be an administrator (ROLE\_ADMIN).

---

**Step 1** From the **Global** toolbar, click the **Settings** icon.  
The **Settings** window appears.

- Step 2** From the navigation pane in the **Settings** window, click **Users**.  
The **Users** window appears with the following information displayed about the users:
- **Username**—Username assigned to the user.
  - **Role**—Role that defines the user's privileges within the APIC-EM. Valid roles are `ROLE_ADMIN`, `ROLE_OBSERVER`, or `ROLE_INSTALLER`.
  - **Scope**—Domain or tenancy that the user is allowed to access.
  - **Actions**—Icons that allow you to edit user information or delete a user.
- Step 3** If you want to edit a user's information, from the **Actions** column, click the **Edit** icon.  
The username and scope are configured by default so you cannot change their settings. However, you can change the role setting. Valid roles are `ROLE_ADMIN`, `ROLE_OBSERVER`, or `ROLE_INSTALLER`.
- Step 4** When you are finished editing the user information, click **Update**.
- 

### Related Topics

[Users and Roles](#)

## Viewing User Access Status

You can view a user's access status to the Cisco APIC-EM.

### Before You Begin

You must be an administrator (`ROLE_ADMIN`).

- 
- Step 1** From the **Global** toolbar, click the **Settings** icon.  
The **Settings** window appears.
- Step 2** From the navigation pane in the **Settings** window, click **Users**.  
The **Users** window appears with the following information displayed about the users:
- **Username**—Username assigned to the user.
  - **Role**—Role that defines the user's privileges within the APIC-EM. Valid roles are `ROLE_ADMIN`, `ROLE_OBSERVER`, or `ROLE_INSTALLER`.
  - **Scope**—Domain or tenancy that the user is allowed to access.
  - **Actions**—Icons that allow you to edit user information or delete a user.
- Step 3** Click the individual username (link) to view the user's current access status.  
The **User Status** dialog box opens, displaying the following information:
- Username
  - Account status—Locked or unlocked

- Account Locked Expiration—Time until user account is unlocked

If you are an administrator, you can unlock the user account by clicking **Unlock**.

**Note** See the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide* for information about configuring a password policy for user access to the controller.

**Step 4** When you are finished viewing or editing the user information, click **Close**.

---

## Reviewing the User Logs

You are able to review the user logs using the Elastic Service Platform (Grapevine) developer console.



**Note** We recommend that only advanced users use the developer console to perform the steps described in this procedure.

---

### Before You Begin

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

---

- Step 1** Review the status of each service listed in the **Overview** window in the console. Each service is represented as a square. A green square represents an active instance of the service, and a red square represents a service with a faulty or failed instance. Squares without color represents inactive services (no instances initiated and running).
- Step 2** Review the version of each service in the **Overview** window in the console. The version is located in the header of each listed service.
- Step 3** Review the service logs by clicking a specific active instance of a service (green square icon) and then viewing the **Instance** logs located at the bottom of the window.
- Step 4** Search through the logs for the keyword: USER-ACCOUNTING. The following data is displayed for these log entry types:
- Date and timestamp
  - Username—Administrator, Installer, or Observer
  - Username—Administrator, Installer, or Observer
  - API
  - Action—GET, POST, PUT, or DELETE method
  - Successful or unsuccessful
- Note** You can also use the **grep** command to search on the keyword in the logs.
-

**What to Do Next**

After reviewing the user data in the logs, proceed to troubleshoot any user activity.

When finished with the developer console, click **Logout**.

**Related Topics**

[Accounting](#), on page 45



## Managing Applications

---

- [Cisco Network Plug and Play](#), page 53
- [Cisco Intelligent WAN \(IWAN\)](#), page 54
- [Topology](#), page 55
- [Performing Path Traces](#), page 71

### Cisco Network Plug and Play

The Cisco Network Plug and Play application provides a simple and secure solution for day-zero deployment of Cisco routers, switches, and wireless access points. The Cisco Network Plug and Play application allows users to preprovision devices by specifying the required image, configuration, and other details. When the device installer installs and powers up a Cisco network device, the device automatically discovers the Cisco APIC-EM controller using DHCP or DNS. After the discovery process is complete, the Cisco Network Plug and Play application provisions the device with the preconfigured information. If a device is not preconfigured, after it discovers and connects to the Cisco APIC-EM, it is listed as an unplanned device in the Cisco Network Plug and Play application. You can use the Cisco Network Plug and Play application to claim the unplanned device and configure it with a new configuration and Cisco IOS image. Cisco APIC-EM supports an embedded Plug and Play (PnP) protocol server that simplifies network device provisioning by securely and automatically delivering an image and configuration file to Cisco devices that support PnP. The PnP server communicates with a Cisco PnP agent installed on the PnP-supported Cisco devices.

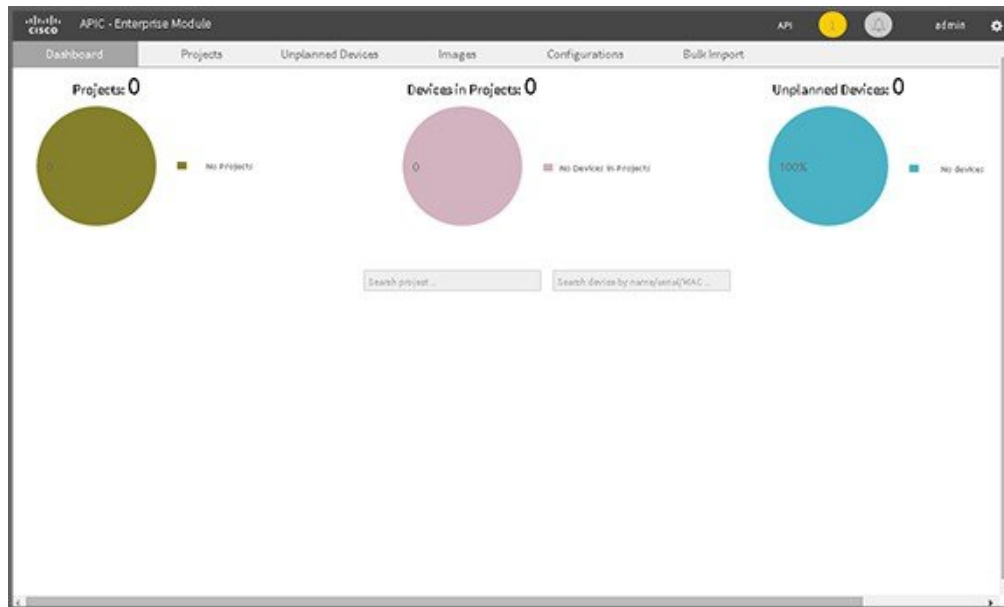
From the Network Plug and Play dashboard page, you can check the status of your site deployment. You can also start defining new sites using the **Projects** link, or view unclaimed devices using the **Unplanned Devices** link.

See the Cisco Network Plug and Play documentation for information about Cisco Network Plug and Play configuration procedures.

**Note**

You may need to import a proxy gateway certificate if the PnP application is enabled on the controller and a proxy gateway exists in the DMZ between the PnP-enabled devices and the controller. For more information, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

**Figure 10: Cisco Network Plug and Play Dashboard**



## Cisco Intelligent WAN (IWAN)

The Cisco Intelligent WAN (IWAN) helps IT deliver an uncompromised user experience over any connection while lowering operational costs. IWAN also simplifies IT operations through a software-based controller model, automating management tasks to ensure faster, more successful deployments.

The Cisco IWAN Application leverages the APIC-EM to abstract the network devices into one system to eliminate network complexity, and provide centralized provisioning of the infrastructure to speed up application and service roll outs.

The Cisco IWAN Application with APIC-EM extends Software Defined Networking to the branch with an application-centric approach based on business policy and application rules. This provides IT centralized management with distributed enforcement across the network.

From the IWAN dashboard page, you can configure your network-wide settings, provision sites, and configure application policies.

See the Cisco IWAN documentation for information about Cisco IWAN network configuration procedures.



**Note**

You may need to import a proxy gateway certificate if the IWAN application is enabled on the controller and a proxy gateway exists in the DMZ between network devices and the controller. For more information, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

**Figure 11: IWAN Dashboard**



## 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.

To access the **Topology** window, click **Topology** in the Navigation pane. The **Topology** window appears.

In addition, auto-visualization of Layer 2 and 3 topologies on top of the physical topology provides a granular view for design planning and simplified troubleshooting.

For a Layer 2 topology, the controller discovers configured VLANs within your network to display in the **Topology** window. For a Layer 3 topology, the controller discovers all forms of a Layer 3 topology (OSPF, IS-IS, etc.), depending on what is currently configured and in use within your network to display in the **Topology** window.

**Note**

Individual device configurations are retrieved and stored in a network information base (NIB).

Clicking on a device icon provides information about that device.

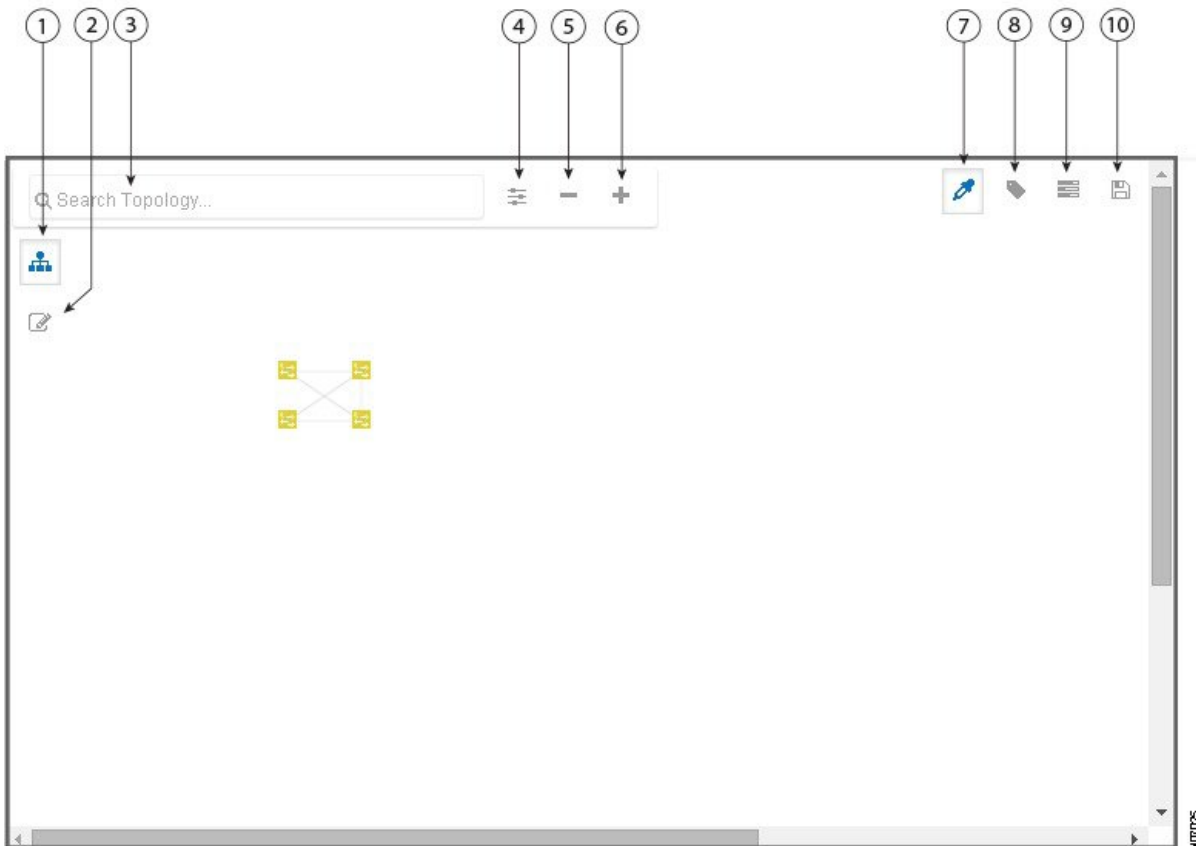
**Note**

For additional detailed information about the paths between hosts and through the network devices, use the **Path Trace** feature. Click **Path Trace** in the Navigation pane to access this application.

## Topology Toolbar

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

**Figure 12: Topology Window**










<b>Callout Number</b>	<b>Icon Name</b>	<b>Description</b>
1	<b>Multiselect</b>	<p>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.</p>
2	<b>Toggle Aggregation</b>	<p>Enables or disables device aggregation. Aggregating devices means grouping devices together. You can group devices in any way that makes sense to you.</p> <p>You can save the layout for future reference by clicking the <b>Save</b> icon.</p> <p>This grouping does not effect the physical configuration on the devices. Aggregation is enabled by default.</p>
3	<b>Search Topology</b>	<p>Searches for a device by device name, device type, or IP address. As you enter information into this field, the Cisco APIC-EM displays matches. Select the device from the results that appear. The selected device appears in the <b>Topology</b> window.</p>


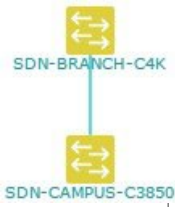
Callout Number	Icon Name	Description
4	<b>Filters</b>	<p>Displays options to change the default view of the topology:</p> <ul style="list-style-type: none"> <li>• <b>Enterprise (Default)</b>— Displays your network topology, separating your devices on connection branches. For example, if a group of devices 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.</li> <li>• <b>Connections</b>—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.</li> <li>• <b>Type and Role</b>—Displays the devices according to their role in the network: access router, distribution switch, core switch and hub, and boarder router.</li> </ul>
5	<b>Zoom out</b>	<p><b>Note</b> Adjusts the <b>Topology</b> window's view. Click the - (minus) icon to minimize the view of the network devices.</p>
6	<b>Zoom in</b>	<p>Adjusts the <b>Topology</b> window's view. Click the + (plus) icon on the menu bar to maximize the view of the network devices.</p>
7	<b>Toggle Color Code</b>	<p>Toggles between displaying the device icons in different colors or in a single color. Color coding is enabled by default.</p>
8	<b>Tags</b>	<p>Displays the available tags. Clicking on an individual tag highlights the device or devices in the <b>Topology</b> window that have this tag.</p> <p>You can also apply tags to devices by selecting the device, clicking <b>Device Tagging</b> in the <b>Device Information</b> dialog box, and then creating and applying the tags.</p>

Callout Number	Icon Name	Description
9	Layers	<p>Displays the Layer 2 and Layer 3 options:</p> <ul style="list-style-type: none"> <li>• <b>Layer 2</b>—Displays a topology of 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.</li> </ul> <p><b>Note</b> You can also access a management network view by choosing a management selection from the drop-down menu.</p> <ul style="list-style-type: none"> <li>• <b>Layer 3</b>—Displays a topology of devices based on the selected Layer 3 protocol. The following Layer 3 protocols are available: <ul style="list-style-type: none"> <li>◦ <b>Intermediate System-to-Intermediate System (IS-IS)</b></li> <li>◦ <b>Open Shortest Path First (OSPF)</b></li> <li>◦ <b>Enhanced Interior Gateway Routing Protocol (EIGRP)</b></li> <li>◦ <b>Static-Route</b></li> </ul> </li> </ul> <p><b>Note</b> The default Layer 3 topology that displays contains all Layer 3 protocols.</p>
10	Save and Load Options	<p>Displays the following options:</p> <ul style="list-style-type: none"> <li>• <b>Save Current Layout</b>—Saves the current layout, device aggregations, and labels.</li> <li>• <b>Load Saved Layout</b>—Loads the previously saved layout, device aggregations, and labels) options.</li> </ul>
11	Map view (Not shown)	<p>Displays the <b>Topology</b> map view. Click this icon to view the network topology in a graphical representation of your network's physical location.</p> <p><b>Note</b> This icon is displayed only if you have added location markers for your devices from the <b>Device Inventory</b> window.</p>

## Topology Icons

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

Icon	Network Element	Description
 cloud	Cloud	Representation of the external network.
 hostname	Host	Displays the hostname or IP address of the host.
 DEVICE-NAME	Router	Displays the device name.
 DEVICE-NAME	Switch	Displays the device name.
 DEVICE-NAME	Access Point	Displays the device name.
 DEVICE-NAME	Wireless LAN Controller	Displays the device name.
 3 accesspoint	Aggregated Devices	Displays the number of aggregated devices and the device type. <b>Note</b> If different devices types are aggregated, only the number of aggregated devices is displayed.

Icon	Network Element	Description
	<p><b>Location Marker</b></p>	<p>Displays the device name. The device icon is displayed with a location marker as a background.</p> <p>If you add location markers to your devices (from the <b>Device Inventory</b> window) and then click <b>Topology</b> in the navigation pane or click the <b>Map</b> 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).</p> <p>Devices that use a different location marker (for example, London) are shown with a location marker as a background.</p>
	<p><b>Links</b></p>	<p>Lines between devices.</p> <p>Click on a link to display information about the connected devices.</p> <p><b>Note</b> Some of the links may be hidden due to device aggregations.</p>

**Related Topics**

- [Applying Tags to Devices](#)
- [Viewing Device Data](#)
- [Searching for Devices and Hosts, on page 68](#)
- [Configuring the Topology Structure, on page 65](#)
- [Changing the Aggregated Devices Label, on page 64](#)
- [Removing Tags from Devices](#)
- [Viewing Devices with Tags](#)
- [Adding a Location Marker, on page 34](#)
- [Aggregating Devices in the Topology Window, on page 63](#)
- [Configuring the Topology Structure, on page 65](#)
- [Topology](#)

## 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 29.)
- 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



## Device Aggregation

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 disaggregate 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 60.
- 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.
- 

#### Related Topics

- [Topology](#)
- [Topology Icons](#), on page 60
- [Topology Toolbar](#)

### Disaggregating Devices 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** 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 and host 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.
- 

### Related Topics

[Topology](#)

[Topology Icons](#), on page 60

[Topology Toolbar](#)

## 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.

### Before You Begin

Scan your network using the discovery functionality of the Cisco APIC-EM to populate device and host 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 **Branch**, **Connections**, or **Device & 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.	<p><b>Device type</b>—Use the slider to adjust the amount of space between device icons based on their device types.</p> <p><b>cloud-centralizeX</b>— When checked (default), the device icons are centered along the X axis. When unchecked, the device icons are aligned to the X axis.</p> <p><b>Device role</b>—Use the slider to adjust the amount of space between device icons based on their device roles.</p> <p><b>Branch</b>— Use the slider to adjust the amount of space between branches.</p> <p><b>Node overlap</b>—Use the slider to adjust the amount of space between nodes.</p> <p><b>aggregate-WIRED</b>—When checked (default), wired hosts are aggregated. When unchecked, wired hosts are disaggregated.</p> <p><b>aggregate-WIRELESS</b>—When checked (default), wireless hosts are aggregated. When unchecked, wireless hosts are disaggregated.</p> <p><b>Note</b> Select x or y from the drop down next to each slider to change how the device icons are displayed, horizontally or vertically.</p>

Filter	Basic View	Advanced View
<b>Connections</b>	<p>Arranges the device icons from left to right based on the number of connections, from least to most.</p> <p><b>Note</b> Aggregated devices are disaggregated in this view.</p>	<p><b>Connections</b>—Use the slider to adjust the amount of space between connections.</p> <p><b>Node overlap</b>—Use the slider to adjust the amount of space between nodes.</p> <p><b>centralizeY</b>—When checked, the device icons are centered along the Y axis. When unchecked, the device icons are aligned to the Y axis.</p> <p><b>Note</b> Select <b>x</b> or <b>y</b> from the drop down next to each slider to change how the device icons are displayed, horizontally or vertically.</p>
<b>Type and Role</b>	<p>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, host, and access)</p> <p><b>Note</b> Aggregated devices are disaggregated in this view.</p>	<p><b>Device type</b>—Use the slider to adjust the amount of space between device icons based on their device types.</p> <p><b>Device role</b>—Use the slider to adjust the amount of space between device icons based on their device roles.</p> <p><b>Node overlap</b>—Use the slider to adjust the amount of space between nodes.</p> <p><b>centralizeX</b>—When checked, the device icons are centered along the X axis. When unchecked, the device icons are aligned to the X axis.</p> <p><b>Note</b> Select <b>x</b> or <b>y</b> from the drop down next to each slider to change how the device icons are displayed, horizontally or vertically.</p>

### What to Do Next

Save the current layout or load a previously saved layout. For information, see [Saving a Topology Layout, on page 66](#) and [Opening a Saved Topology Layout, on page 67](#).

### Related Topics

- [Topology](#)
- [Topology Icons, on page 60](#)
- [Topology Toolbar](#)
- [Topology](#)
- [Topology Icons, on page 60](#)
- [Topology Toolbar](#)

## Saving a Topology Layout

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

### Before You Begin

You must have administrator role permissions.

You must have scanned your network using discovery to populate device and host inventory into the database.

- 
- 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.

### Before You Begin

You must have administrator role permissions.

You must have scanned your network using discovery to populate device and host inventory into the database.

You must have saved a topology layout.

- 
- 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 the Device Role in 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.

**Before You Begin**

Scan your network using the discovery functionality of the Cisco APIC-EM to populate device and host 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 hosts or devices within your network. This function allows you to search the network using any string value. To locate a specific host or device 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).

### 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 hosts or devices.

### What to Do Next

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

- Viewing the data for specific devices
- Applying tags to devices within your network

### Related Topics

[Topology](#)

[Topology Icons](#), on page 60

[Topology Toolbar](#)

## Applying Tags to Devices

You use the Cisco APIC-EM tag feature to associate devices within your network with a single attribute. A tag also enables the grouping of devices based upon an attribute. For example, you can create a tag and use it to group devices based upon a platform ID, Cisco IOS releases, or location.

To apply tags to devices within your network in the **Topology** window, perform the following steps.



---

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

---

### Before You Begin

You should have performed the following tasks:

- Scanned your network using the discovery functionality of the Cisco APIC-EM to populate device and host inventory for the database.
- Determined the tags that you will use to apply to devices within your network.

- 
- Step 1** From the Navigation pane, click **Topology**.  
The **Topology** window appears.
- 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 60](#).  
**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 following these steps:  
a) Enter the name of the tag in the **Tag Title** field.  
b) Click **+New Tag**.
- Step 5** When you are done tagging, click **x** to close the dialog box.
- Step 6** You can verify the tagging by clicking on one of the devices that you tagged.  
The **Device Information** dialog box shows the **Tags** field with the total number and the names of the tags applied to the device.
- 

## Displaying Devices with Tags

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

### Before You Begin

You should have performed the following tasks:

- Discovered the devices on your network to populate the device and host 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.

**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 **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.

**Step 4** To close the tag selection box, click the **Tags** icon in the **Topology** toolbar.

---

## Performing Path Traces

### About Path Trace

Path trace involves the controller reviewing and collecting protocol and other types of data from discovered devices in your network, and then using this data to calculate a path between two hosts or Layer 3 interfaces. You can use the path trace application to monitor and debug traffic paths that are distributed among the various devices throughout your network.

You perform these tasks by running a path trace between two nodes in your network. The two nodes can be a combination of wired or wireless hosts and/or Layer 3 interfaces. In addition, you can specify the protocol for the controller to use to establish the path trace connection, either TCP or UDP.

At every node in the path, the controller reports information about the device and path. For example, if a Layer 2 protocol is used to discover a node, the controller reports that the path is a switched path and labels it as **Switched**. If the controller detects load balancing decisions being made on a discovered device, it reports the path as an ECMP path and labels it as **ECMP**. Path trace can identify the following information about the devices and paths:

- HSRP
- SVI
- Layer 2
- Layer 2 Port Channel
- Layer 3 Routing Protocol
- ECMP/TR

- Netflow
- ECMP over SVI
- Subinterface
- EIGRP
- Level 3 Recursive Loop

For nodes that are unknown devices within a path trace (usually non-Cisco devices), the controller calculates the path between the unknown devices starting from the last known Cisco device (from the **Host Source IP**) to the next, neighboring Cisco device (sometimes the **Destination Source IP**). The collected IP address data about the unknown device is then sent from this neighboring Cisco device to the controller to calculate the trace path. The unknown device is displayed in the controller's GUI as a question mark (?).



---

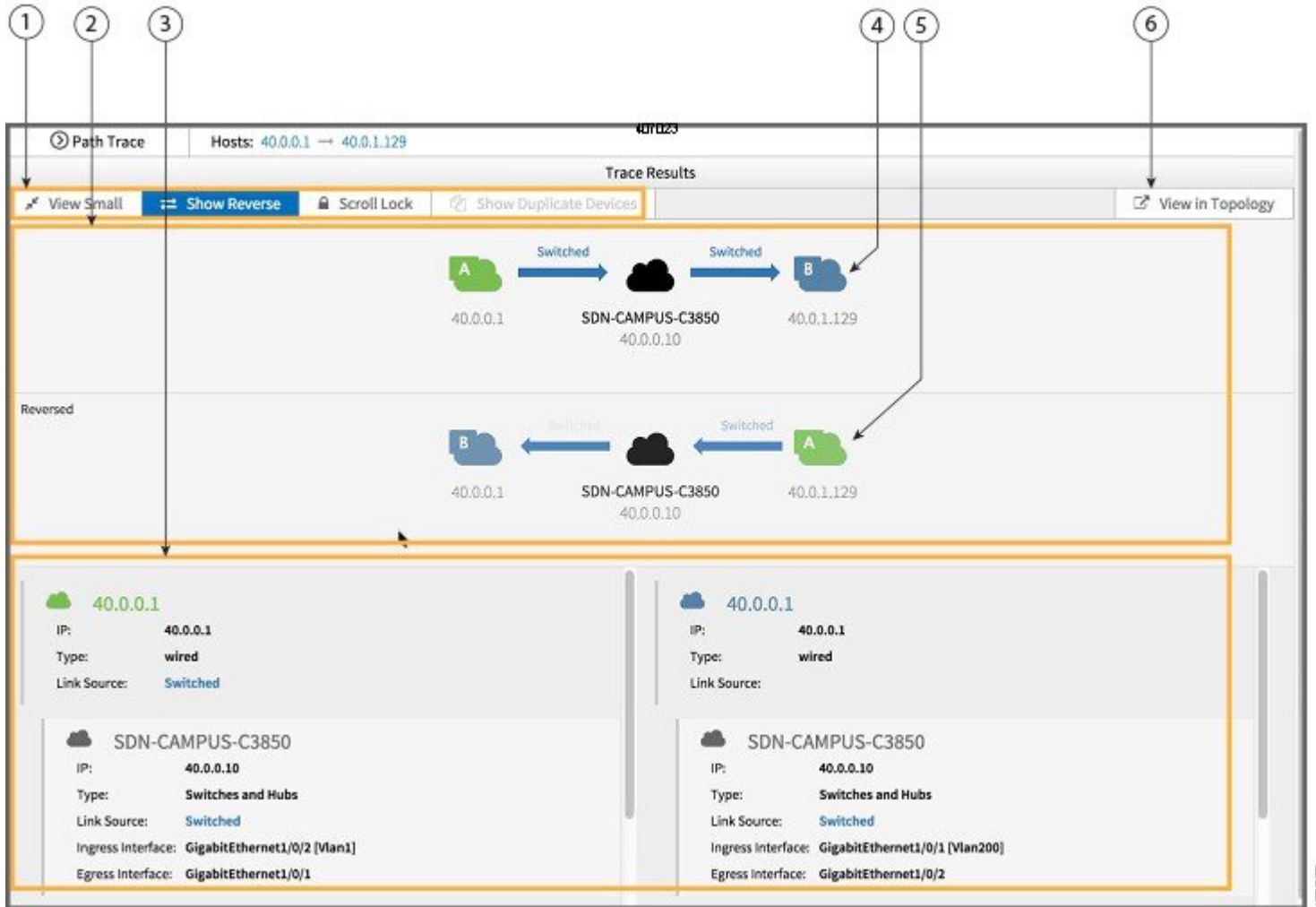
**Note**

In certain circumstances, a path trace may flow between one of two (or more) devices. To determine which device actually received the flow for the path trace, the controller reads the NetFlow configurations and records on the devices (if they exist). By reading this data from the devices, the controller can determine the likelihood of the actual path.

---

To perform a path trace, from the Navigation pane, click **Path Trace**. The **Path Trace** window opens.

Figure 13: Path Trace Window



Callout Number	Name	Description
1	Toolbar	Contains tools that act on the path trace shown in the <b>Trace Results Graphical Display</b> .
2	<b>Trace Results Graphical Display</b>	Shows a graphical representation of the path trace.
3	<b>Trace Results Details</b>	Provides detailed information about the devices along the path.
4	<b>Original Trace Results</b>	Shows the path trace from the source host to the destination host.

Callout Number	Name	Description
5	<b>Reverse Results</b>	Shows the path trace in reverse order, from the destination host to the source host.
6	<b>View in Topology</b> button	Displays the trace results in the Topology window.  <b>Note</b> The trace results are not preserved when you exit the <b>Path Trace</b> window. If you click <b>View in Topology</b> to view the trace results in the <b>Topology</b> window and then return to the <b>Path Trace</b> window, the trace results that you were previously viewing are no longer shown.

### Related Topics

[Performing a Path Trace, on page 79](#)

## Path Trace Support

Cisco APIC-EM can perform path trace calculations for both campus and WAN networks based on physical connectivity and the protocols used by devices within the path. Specifically, the Cisco APIC-EM supports path traces through the following networking environments:

- Campus/data center to campus/data center
- Campus/data center to branch
- Branch to campus/data center
- Branch to branch




---

**Note** If the controller can not complete a path trace for the selected hosts or interfaces, it displays the results of a partial trace.

---

## Path Trace Protocols and Network Connections

The following table describes the supported device protocols and network connections (physical, wireless, and virtual) for a Cisco APIC-EM path trace.




---

**Note** For detailed information about protocol, wireless, and AP support by platform and scenario, see the *Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module*.

---

**Table 13: Path Trace Supported Device Protocols and Network Connections**

Supported Device Protocols and Network Connections	Description
Border Gateway Protocol (BGP)	<p>When BGP is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking.</p> <p>The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.</p>
Equal Cost Multi Path (ECMP)	<p>When an ECMP routing strategy is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking.</p> <p>The data used for this path trace calculation is obtained through an on-demand query made through the network device at the time the path calculation request is made.</p> <p><b>Note</b> The controller's GUI will display when ECMP is used between devices in a path trace segment.</p>
Hot Standby Router Protocol (HSRP)	<p>When HSRP is used in a network, the controller automatically looks up the HSRP active router for a given segment and calculates the path appropriately for a path trace.</p> <p>The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.</p>
Intermediate System-to-Intermediate System (IS-IS) Protocol	<p>When IS-IS is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking.</p> <p>The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.</p>
Layer 3 Forwarding Interface	<p>The controller can perform path traces between two Layer 3 forwarding interfaces or between a Layer 3 forwarding interface and a host.</p>

Supported Device Protocols and Network Connections	Description
MPLS-VPN (WAN)	<p>The controller provides path trace support for a branch-to-branch connected and provider-managed MPLS-VPN service. Supported devices for this type of path trace include:</p> <ul style="list-style-type: none"> <li>• Cisco ASR 1000 Series Aggregation Services Router</li> <li>• Cisco ASR 9000 Series Aggregation Services Router</li> <li>• Cisco Integrated Services Routers (ISR) G2</li> </ul> <p>All customer edge (CE) routers should have NetFlow enabled with traffic running between the hosts and routers.</p> <p><b>Note</b> The above supported devices will be tagged as <b>Border Routers</b> for their <b>Device Role</b> in the <b>Device Inventory</b>. You must keep the above supported devices tagged as <b>Border Routers</b> when performing a path trace.</p> <p>The data used for this path trace calculation is obtained through an on-demand query made through the network device at the time the path calculation request is made.</p>
Open Shortest Path First Protocol (OSPF)	<p>When OSPF is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking.</p> <p>The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.</p>
Physical connectivity (Ethernet, Serial and Packet over SONET (PoS))	<p>The path trace for a given application flow can be displayed over Ethernet, Serial over SONET, and Packet over SONET.</p> <p>The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.</p>
Spanning Tree Protocol (STP)	<p>The controller provides Layer 2 support for Spanning Tree Protocol (STP).</p> <p>The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.</p>

Supported Device Protocols and Network Connections	Description
Static Routing	<p>When static routing is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking.</p> <p>The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.</p>
Virtual connectivity—Layer 2 Port Channel	<p>When virtual connectivity (Layer 2 port channel) is used within a network, the path trace for a given application flow is displayed. The path trace over virtual interfaces (port channels) is displayed, so that the user can visualize an end-to-end path for an application.</p>
Virtual connectivity—VLAN/SVI	<p>When virtual connectivity (VLAN/SVI) is used within a network, the path trace for a given application flow is displayed. The path trace is displayed, so that the user can visualize an end-to-end path for an application.</p> <p>The data used for this path calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.</p>
Wireless	<p>The controller provides path trace support for Control and Provisioning of Wireless Access Points (CAPWAP), 802.11, and mobility.</p> <p>When wireless network elements are used, the path trace for a given application flow is displayed. The user knows the exact path a particular application is taking.</p> <p><b>Note</b> The controller's GUI will display CAPWAP and mobility tunneling (for roaming) when either is discovered during a path trace.</p> <p>The data used for this path calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.</p>

<b>Supported Device Protocols and Network Connections</b>	<b>Description</b>
Equal Cost Multipath/Trace Route (ECMP/TR)	<p>When ECMP/TR is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking.</p> <p>The data used for this path trace calculation is obtained on demand by polling the device. When performing a path trace on ECMP, Cisco Express Forwarding (CEF) lookup is performed on the device on demand for requested tuples. When a path trace detects a number of unknown or unmanaged devices in the path, the path trace is executed on demand from the last known or managed Cisco device and the path calculation is restarted from the first known or managed Cisco device in the trace route result. The unknown or unmanaged hops discovered using path trace are added to the path as unknown devices along with their IP addresses.</p>
Netflow	<p>When Netflow is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking.</p> <p>When we have multiple border routers in the destination island, the Netflow cache from the devices are used to find the actual ingress border router. The Netflow record is matched from these devices on demand for a given tuple. It is essential to configure Netflow on the border routers. If Netflow is not configured, trace route is used to find the ingress interfaces, which might not be accurate.</p>
Sub interfaces	<p>When sub interfaces are used within a network, the path trace for a given application flow is displayed. The path trace between the two sub interfaces is displayed, so that the user can visualize an end-to-end path for an application.</p>
Enhanced Interior Gateway Routing Protocol (EIGRP)	<p>When EIGRP is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking.</p> <p>The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.</p>



Supported Device Protocols and Network Connections	Description
Layer 3 Recursive Lookup	<p>When Layer 3 Recursive Lookup is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking. Up to three recursive lookups are supported.</p> <p>The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.</p>

## Performing a Path Trace

You can perform a path trace between two nodes in your network. The two nodes may be two hosts and/or Layer 3 interfaces.



### Note

The path trace application may display an accuracy notice—a red box with a percentage number in. An accuracy notice that appears on a node or path segment indicates the accuracy level of the path based on the information used to determine the path. Click the accuracy notice to display suggestions for you to take to improve that path trace's accuracy. You can use these suggestions to adjust the device configurations on the path and then perform an second trace for a more accurate result.

### Before You Begin

Scan your network using the discovery function to populate device and host inventory for the database.

Ensure that the controller has SSH or Telnet access to the devices.

### Step 1

In the Navigation pane, click **Path Trace**.  
The **Path Trace** window appears.

### Step 2

In the **Source IP** field, enter the IP address of the first host or the Layer 3 forwarding interface.  
To determine the current list of hosts recognized by the controller, display the **Host Inventory** table.  
To list the Layer 3 forwarding interfaces for a device, enter the device name or IP address followed by a colon ":". All interfaces with IP addresses on the device are displayed.

### Step 3

In the **Destination IP** field, enter the IP address of the second host or the Layer 3 forwarding interface.  
To determine the current list of hosts recognized by the controller, display the **Host Inventory** table.  
To list the Layer 3 forwarding interfaces for a device, enter the device name or IP address followed by a colon ":". All interfaces with IP addresses on the device are displayed.

- Step 4** (Optional) In the **Source Port** field, enter the port number of the first host.
- Step 5** (Optional) In the **Destination Port** field, enter the port number of the second host.
- Step 6** (Optional) In the **Protocol** field, choose either **tcp** or **udp** from the drop-down menu for the Layer 4 path trace protocol.
- Step 7** Click **Trace**.  
Review the path trace output. For more information, see [Understanding Path Trace Results, on page 80](#).
- Step 8** To view the path trace in the **Topology** window. Click **View in Topology**.  
The **Topology** window opens with the path trace highlighted in your network. For more information about the **Topology** window, see [Topology, on page 55](#).
- Note** If you added location markers for your devices, the location markers appear in the Topology map. Click a location marker to display the **Topology** for that location.

### Related Topics

[About Path Trace, on page 71](#)

## Understanding Path Trace Results

After you run a path trace, the controller displays the results in the **Path Results** pane.

### Toolbar

At the top of the **Path Results** pane, the toolbar provides buttons for adjusting the path trace display.

<b>View Small</b>	Minimizes the trace path graphic to better view the trace path details.
<b>Show Reverse</b>	Displays the trace path graphic from the host destination IP to the host source IP.  The reverse path trace graphic is displayed directly below the original path trace.  The reverse path trace details are displayed to the right of the original path trace details.
<b>Scroll Lock</b>	Locks the scrolling of the path trace and reverse path trace details windows. (Available when <b>Show Reverse</b> is enabled.)
<b>Show Duplicate Devices</b>	Displays or hides duplicate devices within a path trace.
<b>View in Topology</b>	Opens the <b>Topology</b> window and highlights the path trace results in your network topology. For more information about using the Topology window, see <a href="#">Topology, on page 55</a> .



---

**Note** Depending upon the trace results, some of the above buttons may be grayed out and not available.

---

### Trace Results Graphical Display

The controller graphically displays the path direction and the devices and networks that the path traverses. The following information is also provided:

- Hosts and devices (including their IP addresses) on the path trace between the source and destination.
- Link Information Source—Whether the path source between devices is either **Switched**, **STP**, **ECMP**, **Routed**, **Trace Route**, or other source type.



---

**Note** If the path trace is lengthy and involves many devices, clicking an individual device in the path trace adjusts the GUI view to focus on that specific device. You can then scroll the view either up or down from that specific device.

---

### Trace Results Details

Review the detailed information displayed for each device in the path trace:

<b>IP</b>	IP address of the device.
<b>Type</b>	Wired or wireless device (access point, switch, or router).

<b>Link Source</b>	<p>Assuming two devices in a path (device A and device B) and the path direction is from device A to device B, then depending upon your network configuration, the following link information source types might be displayed:</p> <ul style="list-style-type: none"> <li>• <b>BGP</b>—Link is based on the BGP routes configured on device A.</li> <li>• <b>ECMP</b>—Link is based on a Cisco Express Forwarding (CEF) load balancing decision.</li> <li>• <b>EIGRP</b>— Link is based on EIGRP routers configured on the device A.</li> <li>• <b>Connected</b>—Device B is directly connected to device A.</li> <li>• <b>InterVlan Routing</b>—There is an SVI configuration on the device A from which the path is switched to device B.</li> <li>• <b>ISIS</b>—Link is based upon the IS-IS routes configured on device A.</li> <li>• <b>NetFlow</b>—Link is based on NetFlow records collected on device A for source and destination.</li> <li>• <b>OSPF</b>—Link is based on the OSPF routes configured on device A.</li> <li>• <b>Static</b>—Link is based on a static route.</li> <li>• <b>Switched</b>—Link is based on Layer 2 VLAN forwarding.</li> <li>• <b>Trace Route</b>—Link is based on trace route.</li> <li>• <b>Wired</b>—Device A is a wired host connected to device B.</li> <li>• <b>Wireless</b>—Device A is a wireless host connected to device B (Access Point).</li> </ul>
<b>Tunnels</b>	<p>CAPWAP data (wireless) or mobility tunneling</p> <p><b>Note</b> The controller provides a graphical view of path trace CAPWAP tunnel around the devices involved. You are able to auto-adjust the view by zooming in or out.</p>
<b>Ingress interface</b>	<p>Ingress interface of the device for the path trace (physical or virtual).</p> <p>For example, a physical ingress interface is <b>GigabitEthernet1/0/1</b> and a virtual ingress interface is <b>GigabitEthernet1/3 [Vlan1]</b>.</p>
<b>Egress interface</b>	<p>Egress interface of the device for the path trace (physical or virtual).</p> <p>For example, a physical interface is <b>GigabitEthernet1/0/2</b> and a virtual ingress interface is <b>GigabitEthernet1/4 [Vlan2]</b>.</p>
<b>Accuracy note</b>	<p>If there is uncertainty about the path trace on a segment between devices, a note about the accuracy of the computed path on this segment is displayed as a percentage.</p>



## Reviewing the API Documentation

---

- [About the Cisco APIC-EM API Documentation, page 83](#)
- [Testing the Cisco APIC-EM APIs, page 88](#)

### About the Cisco APIC-EM API Documentation

Cisco APIC-EM controller provides interactive, northbound Representational State Transfer (REST) API documentation. You can use the REST API documentation to help you integrate the controller with your larger network management system and administer your network.



---

**Note**

The controller displays northbound REST API documentation based upon services that have been installed in the service catalog on the root.

---

To access the northbound REST API documentation, from the **Global** toolbar, click **API**.

**Note**

The REST API documentation is based on Swagger 1.2 specifications.

**Figure 14: API Window**

**Available APIs**

- [File](#)
- [Flow Analysis](#)
- [IP Geolocation](#)
- [IP Pool Manager](#)
- [Inventory](#)
- [Network Discovery](#)
- [Network Plug and Play](#)
- [PKI Broker Service](#)
- [Policy Administration](#)
- [Role Based Access Control](#)
- [Scheduler](#)
- [Task](#)
- [Topology](#)

**File**

APIC-EM Service API based on the Swagger™ 1.2 specification

- [Terms of service](#)
- [Cisco DevNet](#)

**file-service : File Service API** Show/Hide | List Operations | Expand Operations | Raw

[ BASE URL: <https://172.19.172.83/api/v1/api-docs/file-service> , API VERSION: 1.0 ]

The interactive northbound REST API documentation provides:

- Links to information about the northbound REST APIs terms of services and the Cisco developer community website:
  - **Terms of Service**—Review the terms and services for accessing the server where the APIs are located.
  - **Cisco DevNet**—Access the Cisco developer community website. This website offers developer information, community forums, a developer sandbox, and other developer aids.
- A list of supported northbound REST APIs used by the controller and organized by application:
  - **File**
  - **IP Pool Manager**
  - **Network Plug and Play Service**
  - **Policy Administration**
  - **Role Based Access Control**
  - **Scheduler**
  - **Task**
  - **Topology**



---

**Note** Only applications with an active service running display in the menu list.

---

- A list of supported methods for each northbound REST API including:
  - **GET**—To retrieve a resource.
  - **POST**—To create a resource.
  - **PUT**—To change the state of a resource or to update it.
  - **DELETE**— To remove or delete a resource.
- Methods of the API:
  - **Show/Hide**—Displays or hides supported methods of the API (GET, POST, PUT, and DELETE).
  - **List Operations**—Displays the supported methods of the API (GET, POST, PUT, and DELETE).
  - **Expand Operations**—Displays an expanded view of the methods of the API including:
    - **Implementation Notes**—Brief descriptions of what the northbound REST API does, including some specific details of the implementation.
    - **Response Class**—Model and Model Schema views, as well as a Response Content Type:
    - **Parameters**—Parameter, Description, Parameter Type, Data Type definitions (string, integer, or model), as well as input fields if required for testing.
    - **Error Status Codes**—HTTP status code and reason definitions.

- Raw content—Provides **Raw** content for the external Swagger UI (user provided) to access the northbound REST API. Content is provided in text file format.

To get a better understanding of the northbound REST APIs, you can run sample methods and get resultant outputs. For more information, see [Testing the Cisco APIC-EM APIs](#), on page 88.

### Related Topics

[Reviewing and Testing the Cisco APIC-EM APIs](#)

[Common External RESTful Services HTTP Response Codes](#), on page 87

## Supported HTTPS Methods and General Structure

The following table describes the supported HTTPS methods and structure for the Cisco APIC-EM.

HTTPS Method Type	Structure
GET	Use the following values with the GET method type: <ul style="list-style-type: none"> <li>• /noun</li> <li>• /noun/count</li> <li>• /noun/{start}/{end}</li> <li>• /noun/{noun-id}</li> </ul>
POST	The POST method type returns a 409 response code if posting a duplicated resource, or the following response: <pre>{"response":"id-of-created-resource"}</pre>
PUT	The PUT method type returns the following response: <pre>{"response":"message-about-attributes-that-changed"}</pre>
DELETE	The DELETE method type returns a 404 response code if it fails, or the following response: <pre>{"response":"message-about-deletion"}</pre>

The following are general guidelines for the supported HTTPS methods for the Cisco APIC-EM:

- Each method is used as an operation on a single resource
- Each resource is expressed as a singular noun (for example: network-device, link, interface, host, etc.)
- The resource is referenced in the HTTPS method by an ID number (not by name)
- The maximum number of entries returned by a GET API is 500 (default). No API should provide more than 500 (default) entries in a single call.
- A CRUD (Create, READ, Update, Delete) operation on all resources is not allowed in a single API call.



## Common External RESTful Services HTTP Response Codes

External RESTful services return common HTTP response codes as described in the tables below. In addition to the status codes returned in the response header, each response may have additional content (in JSON file format) according to the nature of the request.

**Table 14: Success (2xx) Codes**

Status Code	Description
200 OK	The request was successful. The result is contained in the response body.
201 Created	The POST/PUT request was fulfilled and a new resource has been created. Information about the resource is in the response body.
202 Accepted	The request was accepted for processing, but the processing has not been completed.
204 No Content	The request was successful, however no content was returned.
206 Partial Content	The GET request included a Range Header, and the server responded with the partial content matching the range.

**Table 15: Client Error (4xx) Codes**

Status Code	Description
400 Bad Request	The client made a request that the server could not understand (for example, the request syntax is incorrect).
401 Unauthorized	The client's authentication credentials included with the request are missing or invalid.
403 Forbidden	The server recognizes the authentication credentials, but the client is not authorized to perform this request.
404 Not Found	The client made a request for a resource that does not exist.
409 Conflict	The target resource is in a conflicted state (for example, an edit conflict where a resource is being edited by multiple users). Retrying the request later might succeed.
415 Unsupported Media Type	The client sent a request body in a format that the server does not support (for example, XML to a server that only accepts JSON).

**Table 16: Server Error (5xx) Codes**

Status Code	Description
500 Internal Server Error	The server could not fulfill the request.
501 Not Implemented	The server has not implemented the functionality required to fulfill the request.
503 Service Unavailable	The server is (temporarily) unavailable.

**Related Topics**

[Reviewing and Testing the Cisco APIC-EM APIs](#)

[About the Cisco APIC-EM API Documentation, on page 83](#)

# Testing the Cisco APIC-EM APIs

**Before You Begin**

You can test the Cisco APIC-EM northbound REST APIs in the **API** window.

- 
- Step 1** From the **Global** toolbar, click **API**.
- Step 2** From the list of available APIs, choose an API.  
For example, choose the **Role Based Access Control** API.
- Step 3** From the list of Role Based Access Control APIs, choose an API to view its supported methods.

For example, choose the **user** API.

***Figure 15: Supported Methods for User Management API***

APIC - Enterprise Module
API 1 🔔
admin ⚙️

## Role Based Access Control

APIC-EM Service API based on the Swagger™ 1.2 specification

[Terms of service](#)  
[Cisco DevNet](#)

**role** : Role Description API Show/Hide | List Operations | Expand Operations | Raw

---

**ticket** : Ticket Management API

Show/Hide | List Operations | Expand Operations | Raw

---

**user** : User Management API

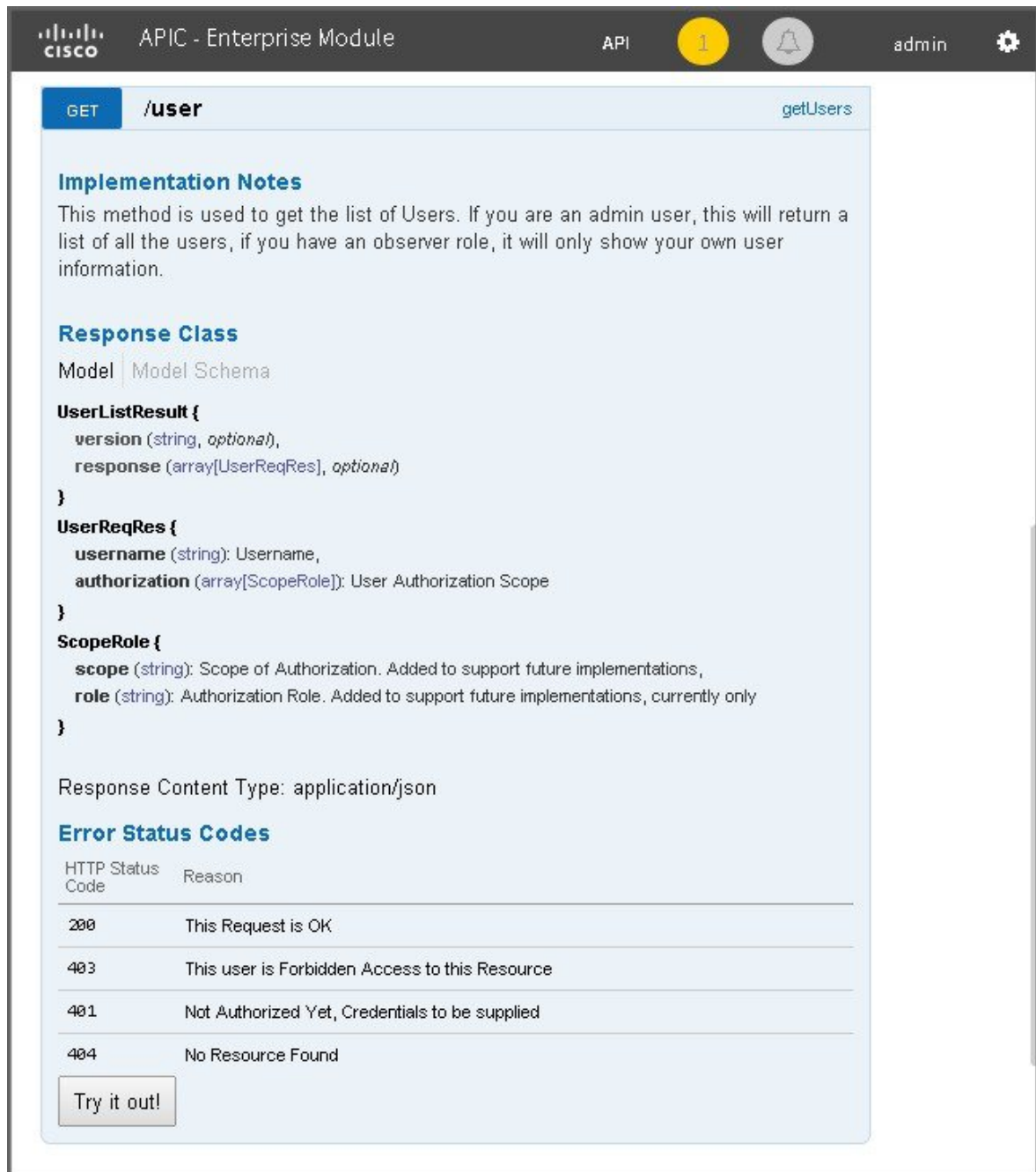
Show/Hide | List Operations | Expand Operations | Raw

POST	/user	addUser
GET	/user	getUsers
PUT	/user	updateUser
GET	/user/passphrase/auto	getAutoPassphrase
GET	/user/passphrase/auto/{seedPhrase}	getAutoPassphrase
GET	/user/password-policy/invalid-attempt-count	getAttemptCount
PUT	/user/password-policy/invalid-attempt-count	updateAttemptCount
PUT	/user/password-policy/lock-expiry-time	updateLockExpiryTimeout
GET	/user/password-policy/lock-expiry-time	getLockExpiry
PUT	/user/status	updateUserStatus
GET	/user/status/{username}	getUserStatus
GET	/user/{username}	getUser
DELETE	/user/{username}	deleteUser

407041

**Step 4** Click **Expand Operations**.

**Figure 16: Expanded View of getUsers API**



**Step 5** Test the API by clicking the **Try it out!** button located at the bottom of each expanded API method window.

**Note** Enter content into any of the required content fields prior to testing the API.

For example, click the **Try it out!** button for **GET /user** and review the following output:

- **Request URL**—Displays the request URL created and sent to the controller for the appropriate method (GET, POST, PUT, DELETE)
- **Response Body**—Displays an example of a response to the request URL.
- **Response Code**—Displays the error status code for example response.

- **Response Headers**— Displays the responses returned by the RESTful Services; the specific HTTP headers used are displayed.

**Figure 17: Output the getUsers API**









## INDEX

### A

administrator [42](#)  
API [3](#)  
API documentation [83](#)  
audience [vii](#)  
authentication [43](#)  
authorization [43](#)

### B

Border Gateway Protocol (BGP) [74](#)

### C

change password [3](#)  
Cisco APIC-EM [1](#)  
    overview [1](#)  
Cisco Network Plug and Play [3](#)

### D

device inventory [3, 21](#)  
    Average Update Frequency [21](#)  
    Configuration [21](#)  
    Device Family [21](#)  
    Device Name [21](#)  
    Device role [21](#)  
    device status [21](#)  
    IOS [21](#)  
    IP Address [21](#)  
    Last Updated Time [21](#)  
    Location [21](#)  
    MAC Address [21](#)  
    Platform [21](#)  
    Serial number [21](#)  
    Tag [21](#)  
    Up Time [21](#)

device inventory (*continued*)  
    window [21](#)  
device role [29, 67](#)  
devices table [21, 28](#)  
    changing view [28](#)  
    filtering [28](#)  
discovery [3, 9, 10, 13](#)  
    devices [9](#)  
    using CDP [10](#)  
    using IP address range [13](#)  
discovery results [17](#)

### E

Equal Cost Multi Path (ECMP) [74](#)

### F

feedback [3](#)

### G

GUI overview [3](#)

### H

host inventory [3, 38](#)  
    window [38](#)  
Hosts table [38, 39](#)  
    changing view [39](#)  
    filters [38](#)  
Hot Standby Router Protocol (HSRP) [74](#)  
HTTPS methods [86](#)

**I**

installer [43](#)  
 Intermediate System-to-Intermediate System, See [IS-IS](#)  
 inventory [21, 38](#)  
   device [21](#)  
   host [38](#)  
 IS-IS [56, 74](#)  
   path trace [74](#)  
   topology [56](#)  
 IWAN [3](#)

**L**

location marker [34, 37](#)  
   adding [34](#)  
   removing [37](#)  
 location tag [33](#)

**N**

northbound REST API documentation [88](#)  
 northbound REST APIs [83](#)  
 notifications [3](#)  
 Notifications [3](#)  
   system [3](#)

**O**

observer [42](#)  
 Open Shortest Path First Protocol (OSPF) [74](#)  
 OSPF [56](#)

**P**

Packet over SONET (PoS) [74](#)  
 path trace [71, 74, 79](#)  
 Path Trace [74](#)  
   protocols [74](#)  
 plug and play [3](#)  
 port channel [74](#)

**R**

RBAC [41, 45](#)  
   accounting [45](#)  
 related documentation [ix](#)

role [42, 43](#)  
   administrator [42](#)  
   observer [42](#)

**S**

Settings [3](#)  
 sign out [3](#)  
 Spanning Tree Protocol (STP) [74](#)  
 static routing [74](#)  
 Static-Route [56](#)

**T**

tag [31, 32](#)  
   adding [31](#)  
   deleting [32](#)  
   removing [31](#)  
 topology [3, 55, 56, 60, 63, 65, 67, 68, 70](#)  
   aggregate [63](#)  
   configuring structure [65](#)  
   device role [67](#)  
   disaggregate [63](#)  
   icons [60](#)  
   L2 [56](#)  
   L3 [56](#)  
   searches [68](#)  
   tags [70](#)  
   toolbar [56](#)  
   window [55](#)  
 Topology [66](#)  
   saving [66](#)

**U**

user [44, 45, 48, 49, 50](#)  
   access [50](#)  
   adding [48](#)  
   delete [49](#)  
   password [45](#)  
   permissions [44](#)  
   roles [44](#)  
   viewing user information [49](#)  
 user logs [51](#)  
 users and domains [43](#)

**W**

wildcard characters [28](#)