



Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide, Release 1.2.x

First Published: November 02, 2015

Last Modified: May 26, 2016

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)

© 2015-2016 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface

Preface ix

Audience ix

Document Conventions ix

Related Documentation xi

Obtaining Documentation and Submitting a Service Request xii

CHAPTER 1

New and Changed Information 1

New and Changed Information 1

CHAPTER 2

Overview 3

About the Cisco Application Policy Infrastructure Controller Enterprise Module 3

Logging into the Cisco APIC-EM 5

Home Tab 6

System Health Tab 6

Cisco APIC-EM GUI 9

Management Applications 13

Cisco Network Plug and Play 13

Cisco Intelligent WAN (IWAN) 14

CHAPTER 3

Managing Users and Roles 15

About User Profiles 15

About User Roles 16

Administrator Role 16

Policy Administrator Role 17

Observer Role 17

Installer Role 17

Users and Domains 18

About AAA	18
Authentication and Authorization	18
Cisco APIC-EM Resources and Permissions	19
Accounting	21
Changing Your Password	21
Configuring Users and Roles	23
Adding a User	24
Deleting a User	25
Viewing and Editing User Information	26
Viewing User Access Status	26
Configuring External Authentication	28

CHAPTER 4

Discovering Devices and Hosts	33
About Discovery	33
Understanding Device and Host Discovery	34
Discovery Credentials Rules	34
Discovery Credentials Caveats	35
Performing Discovery	36
Performing Discovery Using CDP	37
Performing Discovery Using an IP Address Range	41
Copying a Discovery Job	45
Stopping and Starting a Discovery Job	45
Deleting a Discovery Job	46
Understanding the Discovery Results	46

CHAPTER 5

Managing Devices and Hosts	49
Managing Your Device Inventory	50
Filtering Devices in the Device Inventory Window	57
Changing the Devices Layout View	58
Changing the Device Role	60
Deleting a Device	61
Adding or Removing a Device Tag in Device Inventory	62
Adding or Removing a Policy Tag in Device Inventory	63
Adding or Removing a Location Tag	64
Adding or Removing a Location Marker	66

- Deleting a Tag 68
- Managing Your Host Inventory 69
 - Changing the Hosts Table View 71

CHAPTER 6**Using the Topology Map 73**

- About Topology 73
 - Topology Toolbar 75
 - Topology Icons 78
- Displaying Device Data 80
- Aggregating Devices 81
 - Aggregating Devices in the Topology Window 81
 - Disaggregating Devices in the Topology Window 82
 - Changing the Aggregated Devices Label 84
- Configuring the Topology Structure 85
- Saving a Topology Layout 87
- Opening a Saved Topology Layout 88
- Changing a Device's Role From the Topology Window 89
- Searching for Devices 91
- Adding or Removing a Device Tag in Topology 93
- Adding or Removing a Policy Tag in Topology 94
- Displaying Devices with Tags 95

CHAPTER 7**Configuring Quality of Service 97**

- About EasyQoS 97
- EasyQoS Prerequisites 98
- Understanding QoS Policies 98
 - Policy Scope 99
 - Static and Dynamic QoS Policies 99
 - Policy Versioning 100
 - Processing Order for Devices with Limited Resources 100
- Understanding Applications 102
 - Business-Relevance Groups 102
 - Marking, Queuing, and Dropping Treatments 102
 - Custom Applications 105
 - Favorite Applications 106

Understanding Dynamic QoS	106
EasyQoS Guidelines and Limitations	106
Enabling the EasyQoS Beta Feature	107
Getting Started with EasyQoS	108
Configuring QoS Policies	111
Defining a Policy Scope	114
Creating a Policy	115
Editing a Policy	116
Rolling Back a Policy to a Previous Version	117
Cloning a Policy	118
Deleting a Policy	119
Configuring Favorite Applications	120
Enabling and Disabling Dynamic QoS Policies	121
Creating a Custom Application	122
Editing a Custom Application	123
Deleting a Custom Application	124

CHAPTER 8**Performing Path Traces 127**

About Path Trace	127
Supported Network Environments	129
Supported Protocols, Network Connections, and Features	129
Performing a Path Trace	133
Performing an ACL-Based Path Trace	135
Collecting Statistics During a Path Trace	137
Understanding Path Trace Results	140
Understanding the Statistics Retrieved During a Path Trace	144
Device Statistics	144
Interface Statistics	145
QoS Statistics	147
Performance Monitor Statistics	149
Understanding VRF Path Trace Results	150
Understanding ACL Path Trace Results	150

CHAPTER 9**Reviewing the API Documentation 153**

About the Cisco APIC-EM API Documentation	153
---	-----

Supported HTTPS Methods and General Structure	156
Common External RESTful Services HTTP Response Codes	156
Using the Cisco APIC-EM REST API Window	157

APPENDIX A

Required Device Configuration	161
Required Platform Configurations	161
NETCONF Configuration	162
Cisco NetFlow Configuration	163
SNMP Trap Configuration	163
IP Device Tracking Configuration	163
Wireless LAN Controller Configuration	164
WAN Interface Configuration for EasyQoS	164
Performance Monitor Configuration	167



Preface

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

Audience

This publication is for experienced network administrators who will configure and maintain the Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM).

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 ^D or Ctrl-D 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.)
bold font	Commands and keywords and user-entered text appear in bold font .
<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> .
Bold Courier font	Bold Courier 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*
 - *Supported Platforms 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 Upgrade Guide*
 - *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*
 - *Cisco Application Policy Infrastructure Controller Enterprise Module Hardware Installation Guide*
 - *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting 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 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](#).

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the [What's New in Cisco Product Documentation RSS feed](#). RSS feeds are a free service.



New and Changed Information

This chapter provides release-specific information for each new and changed feature in the *Cisco Application Policy Infrastructure Controller - Enterprise Module Configuration Guide*.

- [New and Changed Information, page 1](#)

New and Changed Information

The table below summarizes the new and changed features for the Cisco APIC-EM Release 1.2.0.x that are covered in this document. For information about all of the features in the release, see the Release Notes. For the latest caveats, see the Bug Search Tool at <https://tools.cisco.com/bugsearch/>.

Feature	Description	Where Documented
Home page	The home page now consists of two tabs: the Home tab and the System Health tab. The Home tab provides the same information that used to display on the Home page in previous releases. The System Health tab provides status information about the controller, its applications, and services.	Overview, on page 3
EasyQoS	The EasyQoS GUI has been enhanced to make it easier to configure and manage your QoS policies. In addition, you can now perform the following tasks: <ul style="list-style-type: none">• Rollback to one of the past 5 policies.• Delete policies.• Edit and delete custom applications.	Configuring Quality of Service, on page 97

Feature	Description	Where Documented
Discovery	<p>You can copy a discovery job to use as a basis of another discovery job.</p> <p>In addition, when performing Cisco Device Protocol (CDP) discovery, you can enter one or more subnets to be excluded from the discovery scan. You can also designate the number of hops from the seed device that you want to discover.</p>	Discovering Devices and Hosts, on page 33
Inventory	Device inventory now shows the reason why a device failed to be discovered as a managed device.	Policy Administrator Role, on page 17
Path Trace	<p>Path Trace can analyze and display the following information:</p> <ul style="list-style-type: none"> • Device statistics • Performance Monitor statistics • Virtual Routing and Forwarding (VRF) instances <p>In addition, you now have the ability to perform a path trace to a destination device that is not managed by APIC-EM.</p>	Performing Path Traces, on page 127



CHAPTER 2

Overview

- [About the Cisco Application Policy Infrastructure Controller Enterprise Module, page 3](#)
- [Logging into the Cisco APIC-EM, page 5](#)
- [Cisco APIC-EM GUI, page 9](#)
- [Management Applications, page 13](#)

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.
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.
EasyQoS	The EasyQoS feature enables you to configure quality of service on the devices in your network that have been discovered by the Cisco APIC-EM. Using EasyQoS, you can group devices and then define the business relevance of applications that are used in your network. The Cisco APIC-EM takes your QoS selections, translates them into the proper command line interface (CLI) commands, and deploys them onto the selected devices.
Cisco Network 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. Doing so improves the application experience over any connection and saves telecom costs by leveraging cheaper WAN links.
Public Key Infrastructure (PKI) server	The Cisco APIC-EM provides an integrated PKI service that acts as Certificate Authority (CA) to automate X.509 SSL certificate lifecycle management. Applications, such as IWAN and PnP, use the capabilities of the imbedded PKI service for automatic SSL certificate management.
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.

Feature	Description
Audit Logs (IWAN)	The Cisco APIC-EM provides a direct link to the IWAN Audit Logs, which allows you to view Cisco APIC-EM- and IWAN-related log entries.

Logging into the Cisco APIC-EM

Procedure

- Step 1** From your browser, enter the IP address or fully qualified domain name (FQDN) of the Cisco APIC-EM in the address bar.
- Step 2** From the login page, enter your username and password. The **Home** page of the APIC-EM controller appears. The **Home** page consists of the following two tabs:
- **Home** tab—For information, see [Home Tab](#), on page 6.
 - **System Health** tab—For information, see [System Health Tab](#), on page 6.

Note All users can access the contents of the **Home** tab. However, only administrators (users with ROLE_ADMIN privileges) can access the **System Health** tab.

The screenshot shows the Cisco APIC-EM Home page. The breadcrumb navigation at the top reads "APIC - Enterprise Module / Home". The page features a navigation sidebar on the left with icons for Home, System Health, and other functions. The main content area is divided into two columns:

- APIC - EM System Requirements:** This section explains that the module runs in a dedicated physical appliance or a virtual machine. It includes a table of physical server requirements:

Requirements	Specification
Server image format	Bare Metal/ISO
CPU (cores)	Minimum Required: 6, Recommend: 12
CPU (speed)	2.4 GHz
Memory	64 GB [For a multi-host hardware deployment (2 or 3 hosts) only 32GB of RAM is required for each host.]
Disk Capacity	500 GB of available/usable storage after hardware RAID
RAID Level	Hardware-based RAID at RAID Level 10
- General Information:** This section provides links to the [Quick Start Guide](#), [Data Sheet and Literature](#), [Release Notes](#), and [Developers Resources](#).
- EasyQoS Beta Information:** This section announces a beta version of the EasyQoS application, noting its support for Static QoS policies across LAN, WAN, and Wireless infrastructures.
- Prime Integration:** This section states that APIC-EM can be set up to integrate with Prime Infrastructure for Monitoring and Troubleshooting, with a minimum version of 3.1.
- Supported Platforms and Software Requirements:** This section is partially visible at the bottom of the page.

Home Tab

The **Home** tab provides you with the following features:

- Direct access to the **Quick Start Guide**.
- List of System Requirements.
- Information about Prime Integration.
- Information and links to other controller resources.

The screenshot shows the APIC-EM Home tab interface. The page title is "APIC - Enterprise Module / Home". The navigation menu includes "HOME" and "SYSTEM HEALTH". The main content area features the APIC-EM logo and version "1.2.0.1594".

APIC - EM System Requirements

The Cisco APIC-Enterprise Module runs in a dedicated physical appliance (bare-metal) or within a virtual machine within a VMware vSphere environment:

Physical Server Requirements:

Requirements	Specification
Server image format	Bare Metal/ISO
CPU (cores)	Minimum Required: 6, Recommend: 12
CPU (speed)	2.4 GHz
Memory	64 GB [For a multi-host hardware deployment (2 or 3 hosts) only 32GB of RAM is required for each host.]
Disk Capacity	500 GB of available/usable storage after hardware RAID
RAID Level	Hardware-based RAID at RAID Level 10

General Information

- [Quick Start Guide](#)
- [Data Sheet and Literature](#)
- [Release Notes](#)
- [Developers Resources](#)

EasyQoS Beta Information

This release includes a beta version of the new EasyQoS application. This beta version supports management of Static QoS policies across LAN, WAN and Wireless infrastructures. It also supports Dynamic QoS policies for Wired Access Devices. Note that all other applications shipped with this release are production status. Please visit the [Settings](#) page to enable the EasyQoS application.

Prime Integration

APIC-EM can be setup to integrate with Prime Infrastructure for Monitoring and Troubleshooting. The minimum version of Prime Infrastructure is 3.1.

Supported Platforms and Software Requirements

System Health Tab

The **System Health** tab provides you with the following information:

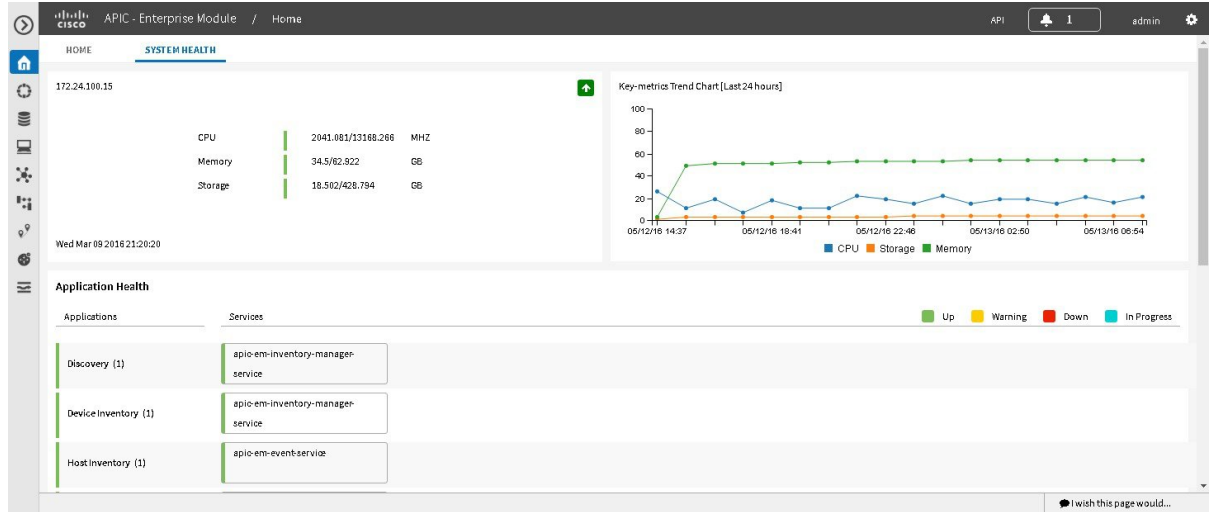
- System health data
- Application health data



Note

You must have administrator privileges (ROLE_ADMIN) to access the **System Health** tab.

Figure 1: System Health Tab



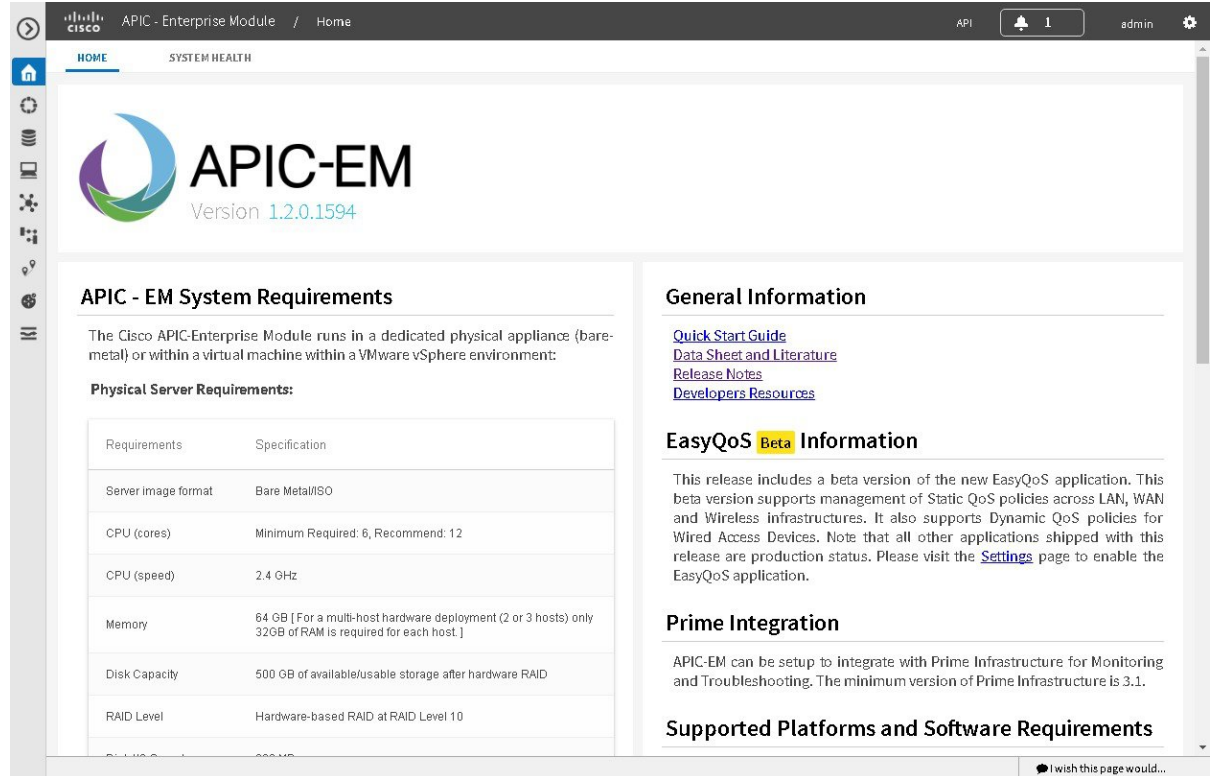
The following information is displayed in the **System Health** tab.

<p>System (Host) Health Data</p>	<p>Data displayed include:</p> <ul style="list-style-type: none"> • Host IP address • CPU—Host CPU usage is displayed in MHZ. Both the currently used and available host CPU is displayed. • Memory—Host memory usage is displayed in GB. Both the currently used and available host memory is displayed. • Storage—Host storage usage is displayed in GB. Both the currently used and available host storage is displayed. <p>Color indicates status for the above host data:</p> <ul style="list-style-type: none"> • Green—Indicates proper usage and support. • Yellow—Indicates usage is approaching improper levels and triggers this warning (color change). • Red—Indicates a failure based upon the usage exceeding the maximum supported value. <p>Additionally, a graphical representation of the above data over the last 24 hours is displayed in this tab. Moving your cursor or mousing over the graph displays a data summation for specific date and time.</p> <p>Note By placing your cursor over (mouseover) a color warning in the window, further information about the warning or failure message appears.</p>
<p>Application Health Data</p>	<p>Displays applications available from the Navigation pane, and the services that support each application. For example, the Topology application accessible in the GUI is supported by topology-service.</p> <p>Color bars indicate the status for the applications and the supporting service(s):</p> <ul style="list-style-type: none"> • Green —Indicates that an application instance is starting. An application instance is the aggregation of the service instances. You can configure a minimum or maximum number of service instances, as well as grow and harvest these service instances (spin up or spin down the services). • Yellow—Indicates application instance and its supporting service instance(s) are experiencing issues and triggers this warning (color change). • Red—Indicates a failure of the application instance and its supporting service instance(s). You can harvest a service instance and then regrow it using the GUI. If the service instance does not regrow using the GUI, then you can manually regrow it. When you harvest a service instance, the controller will determine which instance is regrown (load balancing among them). • Blue—Indicates an in-progress state for the application or service instance (growing or harvesting).

Cisco APIC-EM GUI

Home window

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








Name	Description
Navigation pane	Provides access to the Cisco APIC-EM features and additional applications, such as IWAN and Network Plug and Play.






Name	Description
Window	<p>Area where the feature or application interface is displayed. The Home page consists of two tabs that display information about the applications installed on the controller and controller's system health:</p> <ul style="list-style-type: none"> • Home tab—Displays the Cisco APIC-EM logo and installed software version. Includes links to the <i>Cisco APIC-EM Quick Start Guide</i> and other documentation on Cisco.com. Additionally, information about system and software requirements is listed. • System Health tab—Displays the status of the host IP address, CPU, memory, and storage, the status of the applications that are currently installed, and the services that are currently installed that support the installed applications. <p>When you click an option in the Navigation pane, its corresponding window opens.</p>
Global toolbar	Area that provides access to tools, such as API documentation, settings, and notifications. For a full explanation of the icons on the Global toolbar, see the Global Toolbar Options table below.
I wish this page would... 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
	Hide/Unhide Navigation	Allows you to hide and unhide the Navigation pane.
	Home	Displays information about system requirements and supported platforms.
	Discovery	Allows you to configure discovery options for scanning the devices and hosts in your network.
	Device Inventory	Provides access to the inventory database, where you can display, filter, and sort tabular information about the discovered devices in your network.
	Host Inventory	Provides access to the inventory database, where you can display, filter, and sort tabular information about the discovered hosts in your network. Users can have one of three possible states: active, inactive, and deleted.



Icon	Name	Description
	Topology	Displays graphical representations of your physical, Layer 2, and Layer 3 networks.
	IWAN	Allows you to configure your network-wide settings, provision sites, and configure application policies.
	EasyQoS	Allows you to configure quality of service on selected devices in your network.
	Path Trace	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.
	Network Plug and Play	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
	API	Displays the auto-generated documentation of the northbound REST APIs.

Icon	Option	Description
	System Notifications	<p>Opens the System Notifications dialog box, which provides information about system notifications that have occurred..</p> <p>The icons at the top provide a total of the number of notifications in each of the following categories:</p> <ul style="list-style-type: none"> • Minor (yellow triangle icon) • Major (orange triangle icon) • Critical (red octagon icon) <p>If notifications have occurred, they are listed below the icons. For example, any notifications about software updates or security certificates updates appear in this window.</p> <p>Click the Notification History link to open the Notifications window. This window provides information about the notification, such as its severity, source, timestamp, and status.</p> <p>You can perform the following actions in this window:</p> <ul style="list-style-type: none"> • Acknowledge a notification. • Filter notifications by status or security level. • Sort notifications by source, detail, description, timestamp, or status.
	Administrative Functions	<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"> • Cisco APIC-EM functions: <ul style="list-style-type: none"> ◦ Settings—Allows you to configure controller settings, such user accounts, discovery credentials, network settings, and other security and maintenance settings. ◦ Logs—Allows you to search the controller's service logs. • User functions: <ul style="list-style-type: none"> ◦ Change Password—Allows you to change your own password. ◦ Sign Out—Logs you out of the Cisco APIC-EM.

Management Applications

Cisco Network Plug and Play

The Cisco Network Plug and Play application provides a simple and secure solution for new infrastructure deployments of Cisco routers, switches, and wireless access points.

Using the Cisco Network Plug and Play application, you can pre-provision devices by specifying the required image, configuration, and other details. When you install and power up a Cisco network device, the device automatically connects with the Cisco APIC-EM controller using DHCP or DNS, and the Cisco Network Plug and Play application provisions the device with the preconfigured information.

The PnP solution comprises the PnP server, the PnP app, and the PnP agent. The PnP server interacts with the PnP app (which resides on the controller) and the PnP agent (which resides on PnP-enabled network devices.)

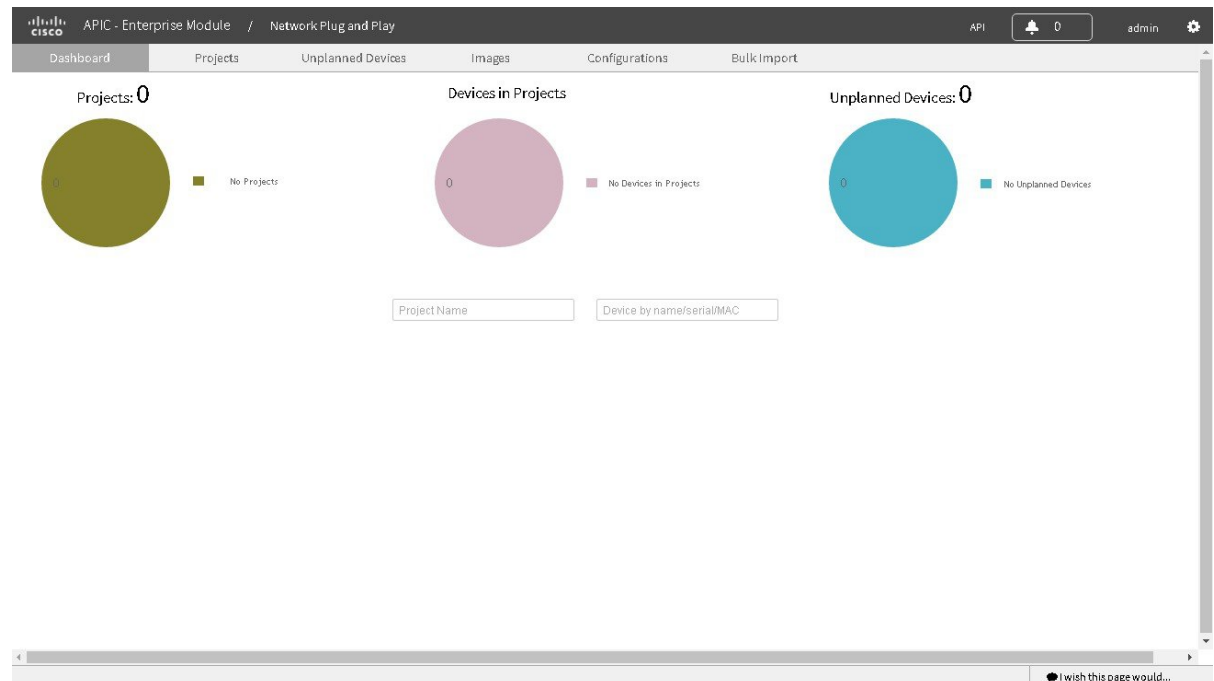
See the Cisco Network Plug and Play documentation for information about Cisco Network Plug and Play configuration procedures.



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 2: Cisco Network Plug and Play Dashboard



Cisco Intelligent WAN (IWAN)

The Cisco Intelligent WAN (IWAN) application with APIC-EM extends Software Defined Networking (SDN) 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.

The IWAN application 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.

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

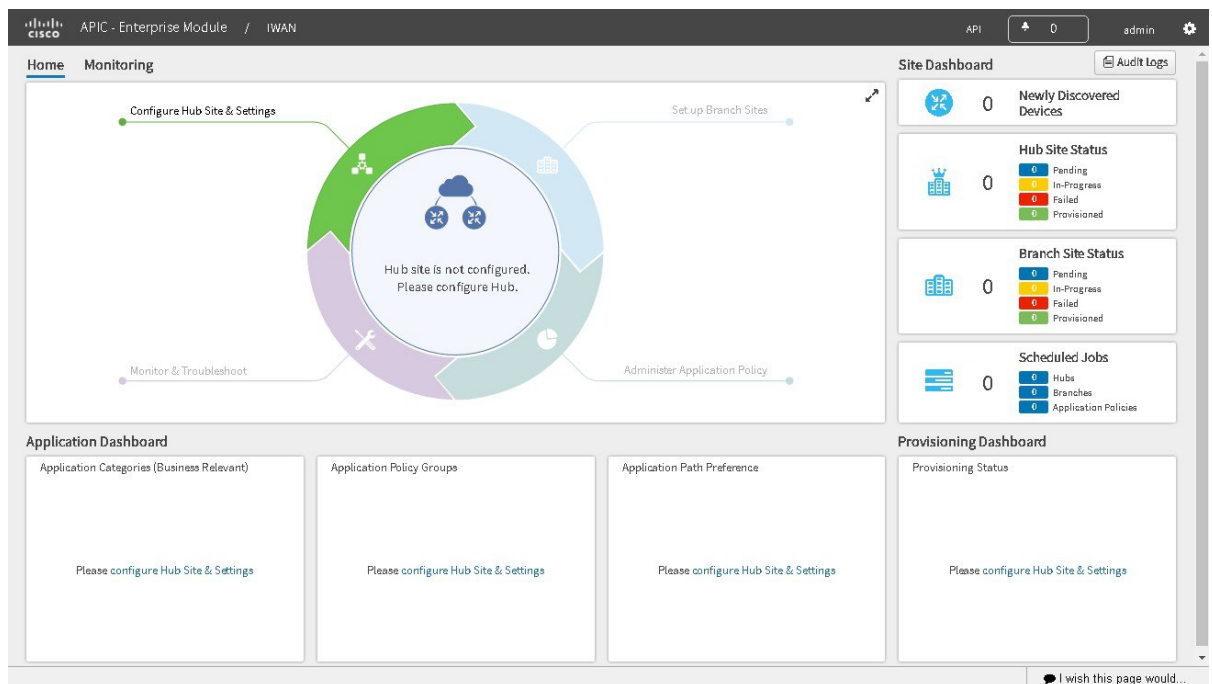
See the Cisco IWAN documentation for information about Cisco IWAN network configuration procedures.



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 3: IWAN Dashboard





Managing Users and Roles

- [About User Profiles, page 15](#)
- [About User Roles, page 16](#)
- [About AAA, page 18](#)
- [Changing Your Password, page 21](#)
- [Configuring Users and Roles, page 23](#)
- [Configuring External Authentication, page 28](#)

About User Profiles

Cisco APIC-EM supports both internal and external user profiles.

- **Internal User Profiles**—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 profiles for other users.

Cisco APIC-EM controls access to the controller through 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. Available roles are Administrator (ROLE_ADMIN), Policy Administrator (ROLE_POLICY_ADMIN), Observer (ROLE_OBSERVER), and Installer (ROLE_INSTALLER). Only users with the administrative role (ROLE_ADMIN) can create user profiles and assign user roles.

- **External User Profiles**—External user profiles exist on an external AAA server. Cisco APIC-EM can discover and use credentials from this external AAA server to manage access to the controller. To enable this functionality, you need to configure external authentication for the Cisco APIC-EM. Once configured, you can view external user profiles and their roles in the **External Users** window.

**Note**

You can only view the external user profiles and their roles in the **External Users** window. You cannot create, edit, or delete them from the controller. These tasks must be performed on the external AAA server.

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 (ROLE_ADMIN) 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 16](#).

**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.

- Policy Administrator (ROLE_POLICY_ADMIN)—Allows you to create and manage policies. For more information, see [Policy Administrator Role, on page 17](#).
- Observer (ROLE_OBSERVER)—Provides primarily read-only privileges to the Cisco APIC-EM. For information, see [Observer Role, on page 17](#).
- 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 17](#).

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 and assign any existing role to it.
- View all other users with their role and scope.
- Edit their own user role and the user role of any other user.
- 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 19.



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.

Policy Administrator Role

The policy administrator role has full read/write access to policy-administration functionality and APIs, including Discovery, Discovery Credentials (global and discovery-specific), Inventory, Topology, Path Trace, and EasyQoS. In particular, a user in this role can create, modify, and deploy application quality-of-service policies.

This role cannot access system-wide controller-administration functions, such as Network Settings (Trustpool, Controller Certificate, Proxy Certificate) and system-wide Controller Settings (Update, Backup & Restore, Logging Level, Auth Timeout, Password Policy, Telemetry Collection and Controller Proxy.) This role cannot create or delete any user accounts but it can change its own password and read its own account information. This role cannot access Prime Credentials.

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

For information about the specific resources available to the observer role, see [Cisco APIC-EM Resources and Permissions](#), on page 19.



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 application to access the Cisco APIC-EM remotely to perform the following functions:

- View device status.
- Trigger device deployments.

Installers cannot 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.

**Note**

Currently, Cisco APIC-EM supports authentication and authorization. Accounting is not yet supported.

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 19](#).

You can configure the following types of authentication for user access to the Cisco APIC-EM:

- Internal—Local controller authentication based upon the usernames and passwords created using the controllers's own GUI.
- External—External controller authentication based upon the usernames and passwords that exist on other servers, including:
 - AAA server authentication—Authentication performed with a pre-configured AAA server using the RADIUS protocol.

When performing user authentication, the controller attempts to authenticate the user in the following order:

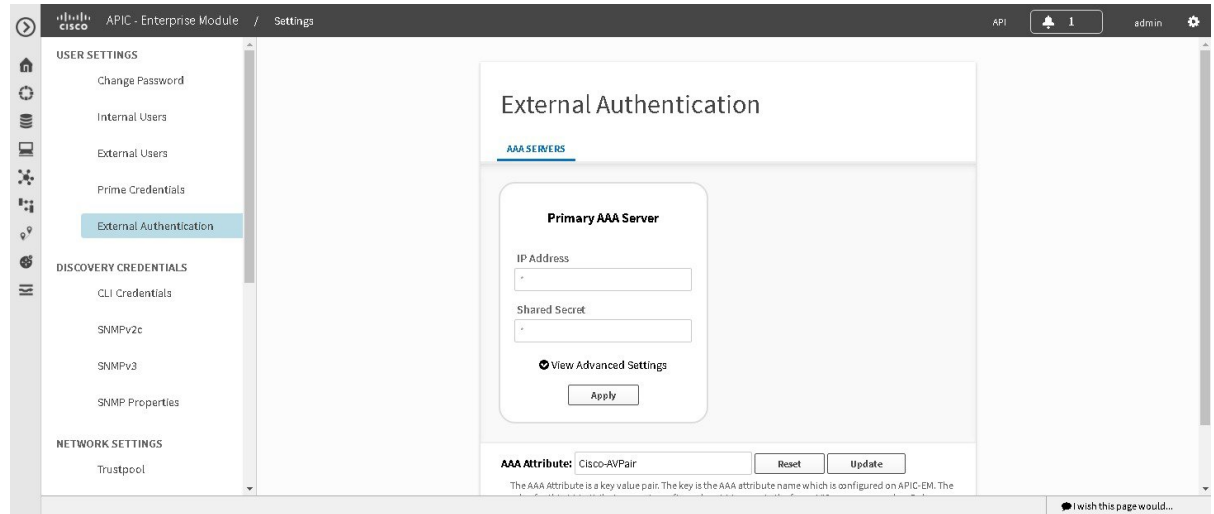
- 1 Authenticate with AD credentials (number of times attempted per user configuration using the controller GUI)
- 2 Authenticate with AAA (RADIUS) server directory credentials (number of times attempted per user configuration using the APIs)

- 3 Authenticate with the user configured controller credentials (number of times attempted per user configuration using the controller GUI)

If the user credentials are authenticated in any of the above steps, then controller access is immediately granted.

You can configure external authentication parameters using the **External Authentication** window in the Cisco APIC-EM GUI. For information about prerequisites and the procedure to set up external authentication, see the *Cisco Application Policy Infrastructure Controller Enterprise Module*.

Figure 4: External Authentication Window



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 4: Cisco APIC-EM Resources and Permissions

Resource	Role Permissions
Discovery: Scan	<ul style="list-style-type: none"> • Administrator • Policy Administrator
Inventory: Retrieving inventory list with device credentials	<ul style="list-style-type: none"> • Administrator • Policy Administrator

Resource	Role Permissions
Inventory: Adding tags	<ul style="list-style-type: none"> • Administrator • Policy Administrator • Observer
Inventory: Creating device roles	<ul style="list-style-type: none"> • Administrator • Policy Administrator • Observer
Inventory: Actions other than adding tags and creating device roles	<ul style="list-style-type: none"> • Administrator • Policy Administrator • Observer
Role-based access control: Creating and deleting users and security roles	<ul style="list-style-type: none"> • Administrator • Observer can view and change own password.
File Service	<ul style="list-style-type: none"> • Administrator • Policy Administrator
Host	<ul style="list-style-type: none"> • Administrator • Policy Administrator • Observer
Task ID	<ul style="list-style-type: none"> • Administrator • Policy Administrator • Observer
Telemetry	<ul style="list-style-type: none"> • Administrator • Policy Administrator • Observer

Resource	Role Permissions
Topology	<ul style="list-style-type: none"> • Administrator • Policy Administrator • Observer
Path Analysis	<ul style="list-style-type: none"> • Administrator • Policy Administrator • Observer

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

Changing Your Password



Note

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

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*.

The screenshot shows the Cisco APIC-EM Settings page. The left navigation pane is expanded to 'Change Password'. The main content area displays the 'Change Password' form with the following fields and buttons:

- Username:** A text input field containing 'admin'.
- Current Password:** A password input field with a masked character (*).
- New Password:** A password input field with a masked character (*). A '(Generate)' link is visible next to the field.
- Confirm New Password:** A password input field with a masked character (*).
- Buttons:** 'Cancel' and 'Update' buttons are located at the bottom of the form.

The top of the page shows the breadcrumb 'APIC - Enterprise Module / Settings' and the user 'admin' is logged in. The bottom right corner has a feedback link: 'I wish this page would...'.

Procedure

Step 1 From the **Global** toolbar, click the **Administrative Functions** (Gear) icon > **Settings**.

Step 2 From the navigation pane in the **Settings** window, click **Change Password**.

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.

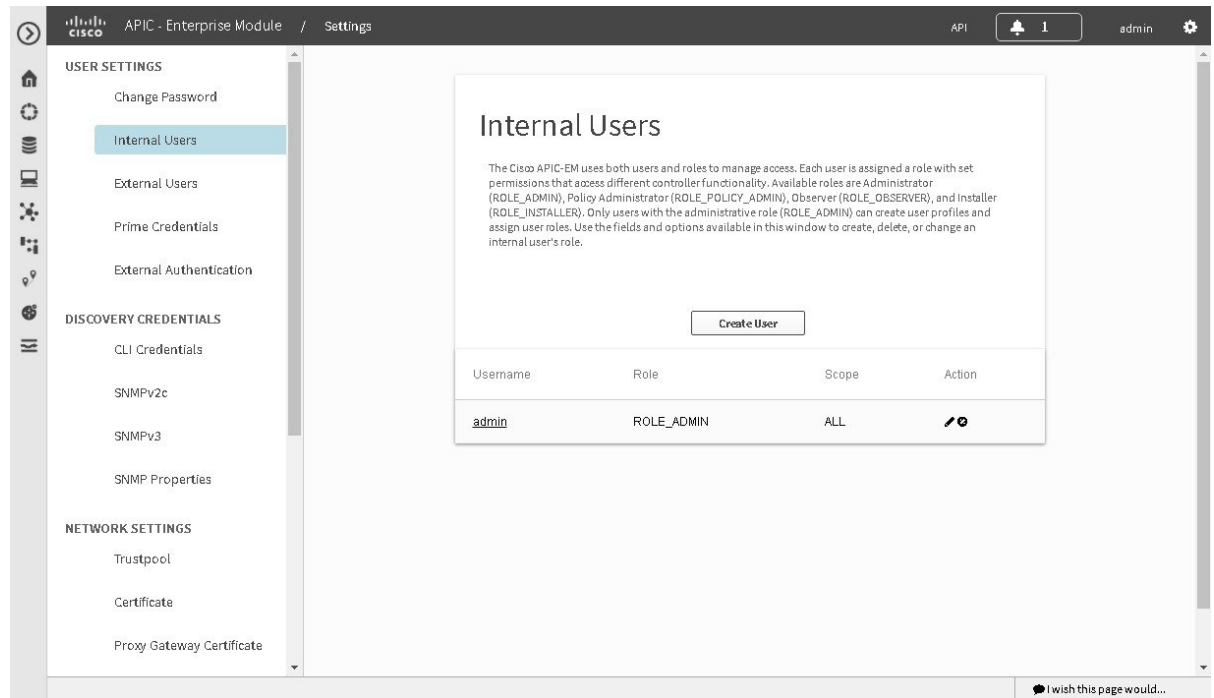
- **Confirm New Password**—Your new password entered a second time as confirmation.

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 5: Users Window



Name	Description
Username	Displays the user's current access status.
Create User	Allows you to add a new user. You must have administrator (ROLE_ADMIN) permissions to perform this procedure.
Edit	Allows you to change the user role settings. You cannot change any other settings. You must have administrator (ROLE_ADMIN) permissions to perform this procedure.
Delete	Removes the user from the Cisco APIC-EM database. The deleted user is no longer able to log into the controller. You must have administrator (ROLE_ADMIN) permissions to perform this procedure.

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.

The screenshot shows the Cisco APIC-EM Settings page. The left navigation pane is expanded to 'Internal Users'. The main content area displays the 'Internal Users' section with a 'Create User' button and a table of users.

Username	Role	Scope	Action
admin	ROLE_ADMIN	ALL	

Before You Begin

You must be an administrator (ROLE_ADMIN).

Procedure

- Step 1** From the **Global** toolbar, click the **Administrative Functions** (Gear) icon > **Settings**.
- Step 2** From the navigation pane in the **Settings** window, click **Users**.
The **Users** window is displayed with the following information 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_POLICY_ADMIN, ROLE_OBSERVER, or ROLE_INSTALLER.
- **Scope**—Domain or tenancy that the user is allowed to access. In this release, the scope is set to ALL and cannot be changed.
- **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.

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 have administrator (ROLE_ADMIN) permissions to perform this procedure.

Procedure

Step 1 From the **Global** toolbar, click the **Administrative Functions** (Gear) icon > **Settings**.

Step 2 From the navigation pane in the **Settings** window, click **Users**.
The **Users** window is displayed with the following information 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_POLICY_ADMIN, ROLE_OBSERVER, or ROLE_INSTALLER.
- **Scope**—Domain or tenancy that the user is allowed to access. In this release, the scope is set to ALL and cannot be changed.
- **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.
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.

Viewing and Editing User Information

You can view and change user information.

**Note**

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

Before You Begin

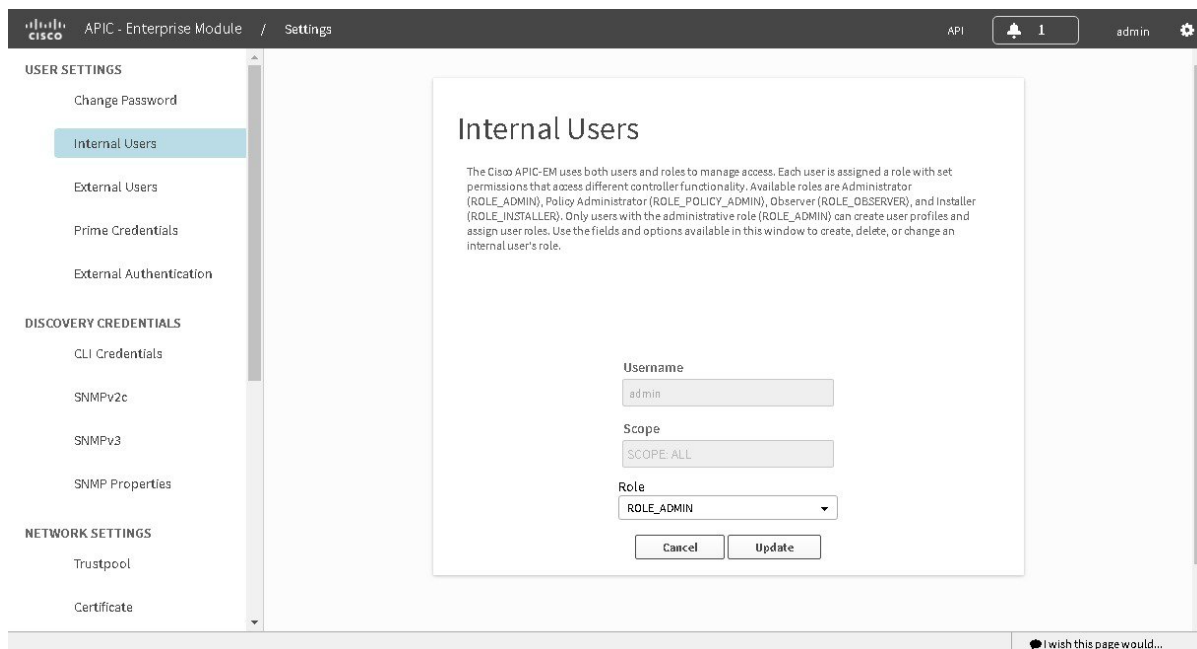
You must have administrator (ROLE_ADMIN) permissions to perform this procedure.

Procedure

-
- Step 1** From the **Global** toolbar, click the **Administrative Functions** (Gear) icon > **Settings**.
- Step 2** From the navigation pane in the **Settings** window, click **Users**.
The **Users** window is displayed with the following information about the uses:
- **Username**—Username assigned to the user.
 - **Role**—Role that defines the user's privileges within the APIC-EM. Valid roles are ROLE_ADMIN, ROLE_POLICY_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_POLICY_ADMIN, ROLE_OBSERVER, or ROLE_INSTALLER.
- Step 4** When you are finished editing the user information, click **Update**.
-

Viewing User Access Status

As an administrator, you can display the access status of a Cisco APIC-EM user.



Before You Begin

You must have administrator (ROLE_ADMIN) permissions to perform this procedure.

Procedure

Step 1 From the **Global** toolbar, click the **Administrative Functions** (Gear) icon > **Settings**.

Step 2 From the navigation pane in the **Settings** window, click **Users**.

The **Users** window is displayed with the following information 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_POLICY_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 At—Date and time user account was locked
- 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**.

Configuring External Authentication

The Cisco APIC-EM supports external authentication and authorization for users from a AAA server. The external authentication and authorization is based upon usernames, passwords, and attributes that already exist on a pre-configured AAA server. With external authentication and authorization, you log into controller with credentials that already exist on the AAA server. The RADIUS protocol is used to connect the controller to the AAA server.

The controller attempts to authenticate and authorize the user in the following order:

- 1 Authenticate/authorize with the user's credentials on a primary AAA server.
- 2 Authenticate/authorize with the user's credentials on a redundant or secondary AAA server.
- 3 Authenticate/authorize with the user's credentials managed by the Cisco APIC-EM.

A user is granted access only if both authentication and authorization is successful.

When authentication/authorization is attempted using a AAA server, the response from that AAA server may be either a timeout or rejection:

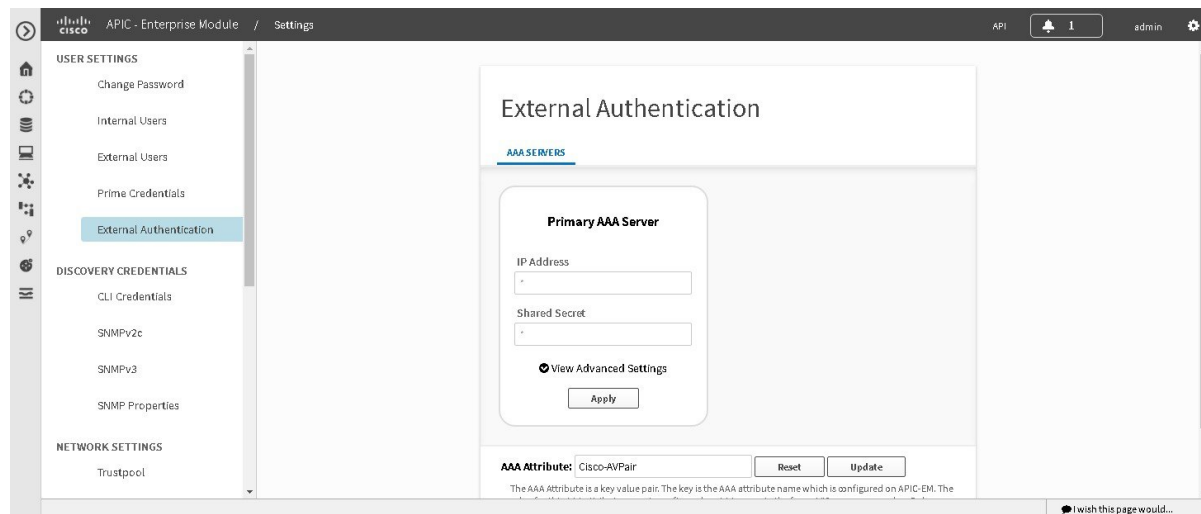
- A timeout occurs when there is no response received from the AAA server within a specific period of time. If the AAA server times out for the authentication/authorization request on the first configured AAA server, then there is a failover to the secondary AAA server. If the secondary AAA server also times out for the authentication/authorization request, then a fall back to local authentication/authorization occurs.
- A rejection is an explicit denial of credentials. If the AAA server rejects an authentication/authorization attempt made from the controller, then there is a fall back to local authentication/authorization.

You configure parameters for the controller to connect to and communicate with an external AAA server, using the **External Authentication** window in the Cisco APIC-EM GUI.

**Note**

External authentication is only supported for the Cisco APIC-EM UI and not the Grapevine console UI.

Figure 7: External Authentication Window



Before You Begin

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

You must have administrator (ROLE_ADMIN) permissions to perform this procedure.

For information about the user permissions required to perform tasks using the Cisco APIC-EM, see the chapter, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

You must have a AAA server already preconfigured, set up, and running. You must also configure the AAA server to interact with the Cisco APIC-EM. When configuring the AAA server to interact with the Cisco APIC-EM, proceed with the following additional steps:

- Register the Cisco APIC-EM with the AAA server.

**Note**

This could also involve configuring a shared-secret on both the AAA server and Cisco APIC-EM controller.

- Configure an attribute name with a value on the AAA server (the attribute name must match on both the AAA server and controller, see step 10 in the following procedure).
- For a Cisco APIC-EM multi-host configuration, configure all individual host IP addresses and the Virtual IP address for the multi-host cluster on the AAA server.

As an example of using the Cisco Identity Services Engine (ISE) GUI to configure values on an AAA server, you select **Authorization Profiles** in the Cisco ISE GUI navigation pane and proceed to configure an authorization profile. When configuring an authorization profile, you enter the following values:

- **Description:** Enter a description for the profile
- **Access Type:** ACCESS_ACCEPT
- **Network Device Profile:** Cisco
- **Advance Attribute Settings:**
 - **Attribute Name:** cisco-av-pair (default value)
 - **Scope:** Scope:ALL, Role:ROLE_ADMIN

Figure 6: AAA Server Configuration Example (Cisco ISE GUI)

The screenshot displays the Cisco ISE GUI for configuring an Authorization Profile. The breadcrumb navigation shows: Home > Operations > Policy > Guest Access > Administration > Work Centers > Policy Elements > Results. The left-hand navigation pane includes: Authentication, Authorization, Profiling, Posture, and Client Provisioning. The main content area is titled 'Authorization Profile' and shows the following configuration:

- Name:** APIC_ADMIN
- Description:** (empty text field)
- Access Type:** ACCESS_ACCEPT
- Network Device Profile:** Cisco
- Service Template:**
- Track Movement:**

Below the main configuration, there are sections for 'Common Tasks' (with checkboxes for DAACL Name, ACL (Filter-ID), VLAN, and Voice Domain Permission) and 'Advanced Attributes Settings'. In the 'Advanced Attributes Settings' section, the attribute 'Cisco:cisco-av-pair' is configured with the value 'Scope=ALL;Role=ROLE_ADMIN'. The 'Attributes Details' section shows: Access Type = ACCESS_ACCEPT and cisco-av-pair = Scope:Role=ROLE_ADMIN. At the bottom, there are 'Save' and 'Reset' buttons.

Procedure

- Step 1** In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.
- Step 2** Click the **Settings** link from the drop-down menu.
- Step 3** In the **Settings** navigation pane, click **External Authentication** to view the **External Authentication** window.
- Step 4** Click the **AAA Server** tab to configure the controller with AAA server credential authentication values.
- Step 5** Configure access to the AAA server for the controller by entering the following *required* information:

- **IP address**—Enter the IP address of your AAA server
- **Shared Secret**—Enter the AAA server's shared secret.

Click either **View Advanced Settings** to enter additional information for the configuration or **Apply** to save and apply your configuration.

Step 6 (Optional) Configure access to the AAA server for the controller by entering the following information:

- **Protocol**—RADIUS
The Protocol field is grayed out, since RADIUS is the default protocol.
- **Authentication Port**—The default value for this field is 1812. Enter a different value if you do not use this common value for your AAA server.
- **Account Port**—The default value for this field is 1813. Enter a different value if you do not use this common value for your AAA server.
Note Accounting is not supported in this controller release.
- **Retries**—Enter the number of times for the controller to attempt authentication, or accept the default value of 1.
- **Timeout (seconds)**—Enter the time interval for the controller to attempt authentication, or accept the default value of 2 seconds.

Click **Apply** to save and apply your configuration.

Step 7 Click the **Add AAA Server** tab to configure a *secondary* AAA server for the controller. The *secondary* AAA server is the backup AAA server that is used for high availability.

Step 8 Configure access to the *secondary* AAA server for the controller by entering the following *required* information:

- **IP address**—Enter the IP address of your second AAA server
- **Shared Secret**—Enter the second AAA server's shared secret.

Important We recommend that the secondary AAA server has the same configuration as the primary AAA server, otherwise results are unpredictable.

Click either **View Advanced Settings** to enter additional information for the configuration or **Apply** to save and apply your configuration.

Step 9 (Optional) Configure access to the *secondary* AAA server for the controller by entering the following information:

- **Protocol**—RADIUS
The Protocol field is grayed out, since RADIUS is the default protocol.
- **Authentication Port**—The default value for this field is 1812. Enter a different value if you do not use this common value for your AAA server.
- **Account Port**—The default value for this field is 1813. Enter a different value if you do not use this common value for your AAA server.
- **Retries**—Enter the number of times for the controller to attempt authentication, or accept the default value of 1.

- **Timeout (seconds)**—Enter the time interval for the controller to attempt authentication, or accept the default value of 2 seconds.

Click **Apply** to save and apply your configuration.

Step 10 Enter the **AAA Attribute**.

As part of the earlier AAA server configuration, you must have already configured an AAA attribute on the AAA server. The AAA attribute is a key value pair that consists of both a key and its value. The key is the AAA attribute name. On the Cisco APIC-EM, you register this AAA attribute name in the controller's GUI in this field. By doing so, you are instructing the controller to search for this key (AAA attribute name) in the AAA server response, after logging in with your AAA credentials.

Note The default AAA attribute name on the controller is Cisco-AVPair.

On the AAA server, you configure *both* the key (AAA attribute name) and its value. The key must be the same as that being configured on the Cisco APIC-EM. The value (which is only configured on the AAA server) requires the following format: `Scope=scope_value:Role=role_value`

For example: `Scope=ALL:Role=ROLE_ADMIN`

Click **Update** to save the **AAA Attribute** name.

What to Do Next

Log out of the Cisco APIC-EM.

Using your AAA server credentials, log back into the Cisco APIC-EM.

Access the **External Users** window on the controller's GUI to view the AAA server users, roles, and scope.



Note

If the authentication/authorization is successful and access is granted, then the user's external authentication/authorization is saved in the controller's database. All users successfully granted access can be viewed in the **External Users** window.



Discovering Devices and Hosts

- [About Discovery, page 33](#)
- [Understanding Device and Host Discovery, page 34](#)
- [Discovery Credentials Rules, page 34](#)
- [Discovery Credentials Caveats, page 35](#)
- [Performing Discovery, page 36](#)
- [Understanding the Discovery Results, page 46](#)

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 provide the controller with 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 network information, such as hosts IP addresses, MAC addresses, and network attachment points:

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

For information about the required protocol configuration for your devices, see [Required Device Configuration, on page 161](#).

Understanding Device and Host Discovery

The process of finding network devices and hosts is known as discovery. You populate the Cisco APIC-EM database by discovering the devices and hosts in your network. To discover network devices, you need to provide the Cisco APIC-EM with discovery credentials for the devices in your network in the form of SNMP settings and CLI credentials. When you perform a discovery, the Cisco APIC-EM scans the network and attempts to log in to newly found devices by presenting these credentials.

The Cisco APIC-EM uses the CDP, LLDP and wireless controller databases on the network devices to discover hosts, such as wireless laptops, handheld devices, printers, and IP phones. To discover wired laptops, the Cisco APIC-EM uses the IP Device Tracking database, which needs to be enabled on some switches. (This feature is enabled by default on some switches.)

Wireless LAN Controllers (WLCs) have additional setup requirements in order to be discovered. For more information, see [Wireless LAN Controller Configuration](#), on page 164.

Discovery Credentials Rules

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

Discovery request-specific credentials rules:

- These credentials can be provided when creating a new network discovery, but only a single set of these credentials is allowed per network discovery.
- These credentials take precedence over any configured global credentials.
- If the discovery request-specific credentials cause an authentication failure, then discovery is attempted a second time with the configured global credentials (if explicitly selected in the **Discovery** window). If discovery fails with the global credentials then the device discovery status will result in an authentication failure.
- If the discovery request-specific credentials (both CLI and SNMP) are not provided as part of network discovery, then the global credentials (both CLI and SNMP) are used to authenticate devices.

Global credentials rules:

Table 5: Global Credentials Rules

Global Credentials	Discovery Request-Specific Credentials	Result
Not configured	Not configured	The default SNMP read community string (public) is used for the discovery scan, but the device discovery will fail since both CLI and SNMP credentials must be configured for a successful device discovery.

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

Discovery Credentials Caveats

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

- If a device credential changes in a network device or devices after Cisco APIC-EM discovery is completed for that device or devices, any subsequent polling cycles for that device or devices will fail. To correct this situation, an administrator has following options:
 - Start a new discovery scan with changed discovery request-specific credentials that matches the new device credential.
 - Update the global credentials with the new device credential. Execute a new discovery scan with the new global credentials.
- If the ongoing discovery fails due to a device authentication failure (for example, the provided discovery credential is not valid for the devices discovered by current discovery), then the administrator has following options:
 - Stop or delete the current discovery. Create one or more new network discovery jobs (either a **CDP** or **Range** discovery type) with a discovery request-specific credential that matches the device credential.

- Create a new global credential or modify one of the global credentials, and execute a new discovery selecting the correct global credential.
- Deleting a global credential does not affect already discovered devices. These already discovered devices will not report an authentication failure.
- The Cisco APIC-EM provides a REST API which allows the retrieval of the list of managed network devices in the Cisco APIC-EM inventory, including certain administrative credentials (SNMP community strings and CLI usernames). The purpose of this API is to allow an external application to synchronize its own managed device inventory with the devices that have been discovered by the Cisco APIC-EM. For example, for Cisco IWAN scenarios, Prime Infrastructure makes use of this API in order to populate its inventory with the IWAN devices contained in the Cisco APIC-EM inventory in order to provide monitoring of the IWAN solution. Any user account with a `ROLE_ADMIN` has access to this API.



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

Performing Discovery

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

Figure 8: Discovery Window

Name	Description
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 Discoveries pane, clicking on a discovery name displays the information in the Discovery Details and Device Details panes.</p>
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 Start, Stop, and Delete discoveries.</p>
In-tool guide	<p>Provides guidance about how to configure discovery.</p>

Performing Discovery Using CDP

You can discover devices and hosts using CDP.



Note

While a discovery job is in progress, you can perform any of the following actions:

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

Before You Begin

You must have administrator (ROLE_ADMIN) permissions to perform this procedure.

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

Your devices must have the required device configurations, as described in [Required Device Configuration](#), on page 161.

Procedure

- Step 1** From the **Navigation** pane, click **Discovery**.
The **Discovery** window appears.
- Step 2** If the **Discovery Details** pane does not appear, click **Add New**.
- Step 3** In the **Discovery Name** field, enter a unique name for this discovery job.
- Step 4** In the **IP Ranges** area, do the following:
 - a) From the **Discovery Type** field, choose **CDP**.
 - b) In the **IP Address** field, enter a seed IP address for the Cisco APIC-EM to use to start the discovery scan.
- Step 5** (Optional) In the **Subnet Filter** field, enter the IP address or subnet and click **Add**.
You can enter the address as an individual IP address ($x.x.x.x$) or as a classless inter-domain routing (CIDR) address ($x.x.x.x/y$) where $x.x.x.x$ refers to the IP address and y refers to the subnet mask. The subnet mask can be a value from 0 to 32.

Repeat this step to exclude multiple subnets from the discovery job.
- Step 6** (Optional) In the **CDP Level** field, enter the number of hops from the seed device that you want to scan.

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

Step 7 In the **SNMP** area, choose one of the previously configured SNMP settings from the **Saved SNMP** drop-down list. If the settings that you need are not available in the list, you can configure SNMP settings for the current discovery.

Use the following guidelines to help you enter the correct values in the fields:

- You can configure up to five SNMP credential sets per type (SNMPv2c and SNMPv3) in **Settings** and an additional SNMP credential set per type (SNMPv2c and SNMPv3) as part of the discovery scan in **Discovery**. If you try to configure more than that, Cisco APIC-EM displays an error message.
- Discovery requires the correct SNMP Read Only (RO) community string. If an SNMP RO community string is not provided, as a *best effort*, discovery uses the default SNMP RO community string, "public."

Table 6: 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"> • noAuthNoPriv—Security level that does not provide authentication or encryption • AuthNoPriv—Security level that provides authentication but does not provide encryption • AuthPriv—Security level that provides both authentication and encryption
Auth Type	Specifies the authentication type to be used. <ul style="list-style-type: none"> • SHA—Authentication based on the Hash-Based Message Authentication Code (HMAC), Secure Hash algorithm (SHA) algorithm • MD5—Authentication based on the Hash-Based Message Authentication Code (HMAC), Message Digest 5 (MD5) algorithm • None—No authentication
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"> • DES—Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard. • AES128—Cipher Block Chaining (CBC) mode AES for encryption. • None—No privacy

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

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. Note 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.

Table 8: 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 8 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. For host discovery, credentials are not required as hosts are discovered through the devices.

Note Cisco APIC-EM uses both the request-specific discovery credentials and the global discovery credentials (set in the **Settings > Discovery Credentials** window) to help you discover all of the Cisco devices within your network.

Step 9 (Optional) In the **Advanced** area, configure the protocols that the Cisco APIC-EM uses to connect to devices. Valid protocols are **SSH** (default) and **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 10 Click **Start Discovery**.

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

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

Performing Discovery Using an IP Address Range

**Note**

You can discover devices using an IP address range.

While a discovery job is in progress, you can perform any of the following actions:

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

The screenshot shows the 'Add a New/Copy Discovery' configuration page in the Cisco APIC - Enterprise Module. The page is divided into several sections:

- Discoveries:** A list of existing discoveries on the left, including 'Discovery1', 'Discovery2', and 'Discovery3'.
- Discovery Name:** A field to enter a unique name for the discovery.
- IP Ranges:** A section for defining the IP addresses to scan, including a 'Discovery Type' dropdown set to 'Range' and input fields for IP ranges.
- SNMP:** A section for selecting saved SNMP settings from a dropdown menu.
- CLI Credentials:** A section for selecting saved CLI credentials from a dropdown menu.
- Advanced:** A section for specifying advanced settings, with a 'show Advanced settings' link.
- Start Discovery:** A button to initiate the discovery process.
- Right-hand Panel:** A detailed guide for 'Add a New/Copy Discovery', explaining the 'DISCOVERY TYPE' (Cisco Discovery Protocol (CDP) vs. Range of IP addresses) and 'SNMP' settings.

Before You Begin

You must have administrator (ROLE_ADMIN) permissions to perform this procedure.

Your devices must have the required device configurations, as described in [Required Device Configuration, on page 161](#).

Procedure

- Step 1** From the **Navigation** pane, click **Discovery**.
The **Discovery** window appears.
- Step 2** If the **Discovery Details** pane does not appear, click **Add New**.
- Step 3** In the **Discovery Name** field, enter a unique name for this discovery.
- Step 4** In the **IP Ranges** area, do the following:
 - a) From the **Discovery Type** field, choose **Range** for the discovery scan type.
 - b) In the **IP Address** field, enter the beginning and ending IP addresses (IP range) for the devices being discovered and click **Add**.
You can enter a single IP address range or multiple IP addresses for the discovery scan.
 - c) Repeat Step b to enter additional IP address ranges.
- Step 5** In the **SNMP** area, choose one of the previously configured SNMP settings from the **Saved SNMP** drop-down list. If the settings that you need are not available in the list, you can configure SNMP settings for the current discovery.
Use the following guidelines to help you enter the correct values in the fields:

- You can configure up to five SNMP credential sets per type (SNMPv2c and SNMPv3) in **Settings** and an additional SNMP credentials set per type (SNMPv2c and SNMPv3) as part of the discovery scan in **Discovery**. If you try to configure more than that, Cisco APIC-EM displays an error message.
- Discovery requires the correct SNMP Read Only (RO) community string. If an SNMP RO community string is not provided, as a *best effort*, discovery uses the default SNMP RO community string, "public."

Table 9: 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"> • noAuthNoPriv—Security level that does not provide authentication or encryption • AuthNoPriv—Security level that provides authentication but does not provide encryption • AuthPriv—Security level that provides both authentication and encryption
Auth Type	Specifies the authentication type to be used. <ul style="list-style-type: none"> • SHA—Authentication based on the Hash-Based Message Authentication Code (HMAC), Secure Hash algorithm (SHA) algorithm • MD5—Authentication based on the Hash-Based Message Authentication Code (HMAC), Message Digest 5 (MD5) algorithm • None—No authentication
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"> • DES—Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard. • AES128—Cipher Block Chaining (CBC) mode AES for encryption. • None—No privacy
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 10: 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. Note 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.

Table 11: 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 6 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. For host discovery, credentials are not required as hosts are discovered through the devices.

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 7 (Optional) In the **Advanced** area, configure the protocols that the Cisco APIC-EM uses to connect to devices. Valid protocols are **SSH** (default) and **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 8 Click **Start Discovery**. The **Discoveries** window displays the results of your scan.

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

Copying a Discovery Job

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

Before You Begin

You have created at least one discovery scan.

Procedure

- Step 1** From the **Navigation** pane, click **Discovery**.
 - Step 2** From the **Discoveries** pane, select the discovery job.
 - Step 3** From the **Discovery Details** pane, click **Copy**.
The discovery job is copied, and the new job is named *Copy of Discovery_Job*.
 - Step 4** (Optional) Change the name of the discovery job.
 - Step 5** Define or update the SNMP and CLI credentials and any other parameters for the discovery job.
-

Stopping and Starting a Discovery Job

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

Before You Begin

You must have administrator (ROLE_ADMIN) permissions to perform this procedure.

Procedure

- Step 1** From the **Navigation** pane, click **Discovery**.
 - Step 2** To stop an active discovery job, do the following:
 - a) From the **Discoveries** pane, select the discovery job.
 - b) From the **Discovery Details** pane, click **Stop**.
 - c) Click **OK** to confirm that you want to stop the discovery job.
 - Step 3** To restart an inactive discovery, do the following:
 - a) From the **Discoveries** pane, select the discovery job.
 - b) From the **Discovery Details** pane, click **Start**.
-

Deleting a Discovery Job

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

Before You Begin

You must have administrator (ROLE_ADMIN) permissions to perform this procedure.

Procedure

- Step 1** From the **Navigation** pane, click **Discovery**.
 - Step 2** From the **Discoveries** pane, select the discovery job that you want to delete.
 - Step 3** From the **Discovery Details** pane, click **Delete**.
 - Step 4** Click **OK** to confirm that you want to delete the discovery.
-

Understanding the Discovery Results

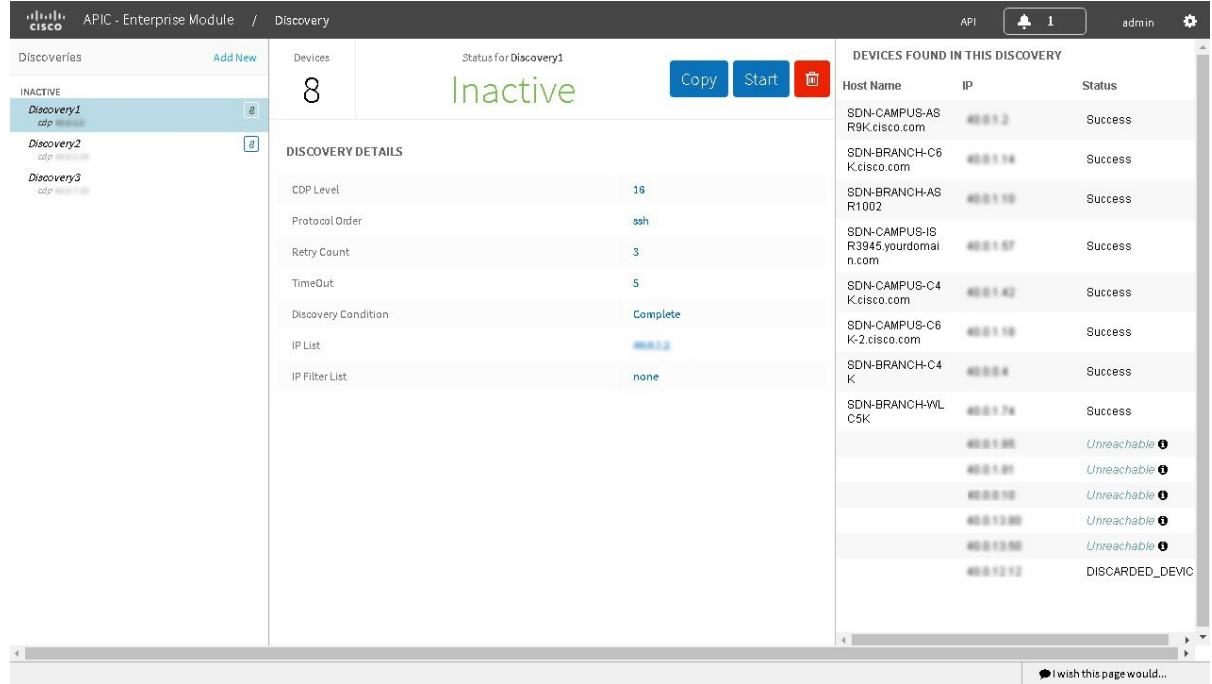
The Discovery window provides information about the selected scan. To access the **Discovery** window, from the **Navigation** pane, click **Discovery**. The **Discovery Results** window has three main panes.



Note

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

Figure 9: Discovery Results Window



Name	Description
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 Discoveries pane, clicking on a discovery name displays the information in the Discovery Details and Device Details panes.</p>
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 Start, Stop, and Delete discoveries.</p>
Devices pane	<p>Displays the host name, IP address, and status of the devices found during the scan.</p> <p>Discovery displays devices as discarded if the IP address belongs to an access point (associated with a wireless controller) or the device was filtered based on input given in the Subnet Filter field.</p>



Managing Devices and Hosts

- [Managing Your Device Inventory, page 50](#)
- [Managing Your Host Inventory, page 69](#)

Managing Your Device Inventory

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

Figure 10: Device Inventory Window

Device Name	IP Address	Device Status	Up Time	Last Updated Time	Last Inventory Collection Status
SDN-BRANCH-AP1252-1	0.0.0.0	Reachable	NA	20 minutes ago	Managed
SDN-BRANCH-ASR1002	40.0.1.10	Reachable	77 days, 0:53:56.50	2 minutes ago	Partial Collection Failure
SDN-BRANCH-C4K	40.0.0.4	Reachable	113 days, 0:29:49.51	7 minutes ago	Partial Collection Failure
SDN-BRANCH-C6K.cisco.com	40.0.1.14	Reachable	15 days, 16:18:10.25	3 minutes ago	Partial Collection Failure
SDN-BRANCH-WLC5K	40.0.1.74	Reachable	34 days, 3:55:40.99	20 minutes ago	Partial Collection Failure
SDN-CAMPUS-ASR9K.cisco.com	40.0.1.2	Reachable	113 days, 0:28:50.37	5 minutes ago	Partial Collection Failure
SDN-CAMPUS-C4K.cisco.com	40.0.1.42	Reachable	113 days, 0:29:55.03	7 minutes ago	Partial Collection Failure
SDN-CAMPUS-C6K-2.cisco.com	40.0.1.18	Reachable	106 days, 23:00:31.92	4 minutes ago	Partial Collection Failure
SDN-CAMPUS-ISR3945.yourdomain.com	40.0.1.57	Reachable	77 days, 0:48:26.70	7 minutes ago	Partial Collection Failure
SDN-LAP1252-AP2	0.0.0.0	Reachable	NA	20 minutes ago	Managed



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.

Name	Description
Device Selection check boxes	Allows you to select devices to perform tasks.
Filters	Allows you to refine the list of devices that are displayed in the table by name, location tag, and IP address.

Name	Description
Layout	<p>Allows you to choose from three predefined layouts or a customized layout:</p> <ul style="list-style-type: none"> • Status—Layout shows the device name, IP address, state of the device, how long it has been up, and the last time it was updated. • Hardware—Layout shows the device name, IP address, device family, platform, serial number, MAC address, and role, along with its IOS/firmware version and a link to its configuration file. • Tagging—Layout shows the device name, IP address, MAC address, device role, location, and tags. • Customize—Layout shows the information in the columns that you have selected to display. <p>For descriptions of the columns of information that you can display, see the Device Inventory Information table below.</p>

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

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

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

Table 12: Device Inventory Information

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

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

Column Name	Description
Device Role	<p data-bbox="922 283 1481 472">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 data-bbox="922 493 1481 640">Note The controller can change the device role as the network topology changes, but if you manually change the device role, then the role will not change as the network topology changes.</p> <p data-bbox="922 651 1481 745">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 data-bbox="966 766 1136 987" style="list-style-type: none">• Unknown• Access• Core• Distribution• Border Router

Column Name	Description
Location	<p>Tag that you can apply to a device to denote its geographic location. By applying the same tag to several devices, you can group them based on a common attribute. The Device Inventory window and Topology window support location tags.</p> <p>Use the following guidelines when creating location tags:</p> <ul style="list-style-type: none"> • Location tag information is maintained on the controller only and not deployed to or derived from the device itself. • A location defined on the controller is not the "civic-location" property that some devices support. • You cannot create, use, or search for location tags in the Topology window. • Location tags cannot be attached to hosts. • You can apply only one location tag to a device. However, you can use both a location tag and a device tag together. <p>For information about adding location tags, see Adding or Removing a Location Tag, on page 64.</p> <p>Along with the location tag, you can add a geographical marker on a world map to a device. For information, see Adding or Removing a Location Marker, on page 66.</p>
Device Tag	<p>Tag assigned to devices to identify them by a common attribute. For example, you can create a tag and use it to group devices based on a platform ID or Cisco IOS release.</p> <p>Tags are useful when applying policies; they allow you to apply policies to a single tag (and therefore multiple devices), instead of having to apply multiple policies to multiple devices.</p> <p>A number in the Tag column indicates how many tags have been applied to that device.</p> <p>Note You are permitted to use both a location tag and a device tag together.</p> <p>For information about adding or removing device tags, see Adding or Removing a Device Tag in Device Inventory, on page 62.</p> <p>For information about deleting a tag from the controller database, see Deleting a Tag, on page 68.</p>

Column Name	Description
Policy Tag	<p>Tag applied to a group of devices that will share the same policy.</p> <p>After applying a policy tag, you need to configure the policies that will be applied to the devices with the same policy tag. For information about configuring QoS policies, see Configuring Quality of Service, on page 97.</p>
Last Updated Time	Date and time that the device was last scanned and the controller database was updated.
Device Family	<p>Group of related devices, as follows:</p> <ul style="list-style-type: none"> • Cisco Interfaces and Modules • Routers • Switches and Hubs • Third Party Device • Unsupported Cisco Device • Wireless Controller
Device Series	Series number of the device, for example, Cisco Catalyst 4500 Series Switches.
Last Inventory Collection Status	<p>Status of the last discovery scan for the device:</p> <ul style="list-style-type: none"> • Managed—Device is in a fully managed state. • Partial Collection Failure—Device is in a partial collected state and not all the inventory information has been collected. Move the cursor over the Information (i) icon to display additional information about the failure. • Unreachable—Due to device connectivity issues, the device could not be reached and no inventory information was collected. This condition can occur when periodic collection happens. • Wrong Credentials—If the device credentials are changed after adding the device to the inventory, this condition is noted. • In Progress—Inventory collection is occurring.

Related Topics

[Changing the Device Role, on page 60](#)

[Adding or Removing a Device Tag in Device Inventory, on page 62](#)

[Adding or Removing Tags to Multiple Devices](#)

[Adding or Removing a Location Tag, on page 64](#)

[Adding or Removing a Location Marker, on page 66](#)

Filtering Devices in the Device Inventory Window

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

Device Name	IP Address	Device Status	Up Time	Last Updated Time	Last Inventory Collection Status
SDN-BRANCH-AP1252-1	0.0.0.0	Reachable	NA	20 minutes ago	Managed
SDN-BRANCH-ASR1002	40.0.1.10	Reachable	77 days, 0:53:56.50	2 minutes ago	Partial Collection Failure
SDN-BRANCH-C4K	40.0.0.4	Reachable	113 days, 0:29:49.51	7 minutes ago	Partial Collection Failure
SDN-BRANCH-C6K.cisco.com	40.0.1.14	Reachable	15 days, 16:18:10.25	3 minutes ago	Partial Collection Failure
SDN-BRANCH-WLC5K	40.0.1.74	Reachable	34 days, 3:55:40.99	20 minutes ago	Partial Collection Failure
SDN-CAMPUS-ASR9K.cisco.com	40.0.1.2	Reachable	113 days, 0:28:50.37	5 minutes ago	Partial Collection Failure
SDN-CAMPUS-C4K.cisco.com	40.0.1.42	Reachable	113 days, 0:29:55.03	7 minutes ago	Partial Collection Failure
SDN-CAMPUS-C6K-2.cisco.com	40.0.1.18	Reachable	106 days, 23:00:31.92	4 minutes ago	Partial Collection Failure
SDN-CAMPUS-ISR3945.yourdomain.com	40.0.1.57	Reachable	77 days, 0:48:26.70	7 minutes ago	Partial Collection Failure
SDN-LAP1252-AP2	0.0.0.0	Reachable	NA	20 minutes ago	Managed

Before You Begin

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

Procedure

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

- **Device Name**
- **Device Location**

- **Device IP Address**
- **Device VRF**

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

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

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

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

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

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

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

What to Do Next

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

Changing the Devices Layout View

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

Device Name	IP Address	MAC Address	Device Role	Location	Policy Tag	Device Tag
SDN-BRANCH-AP1252-1	0.0.0.0	00:23:eb:d1:a2:40	ACCESS	Add	Not Available	0
SDN-BRANCH-ASR1002	40.0.1.10		BORDER ROUTER	Add	Add	0
SDN-BRANCH-C4K	40.0.0.4		DISTRIBUTION	Add	Add	0
SDN-BRANCH-C6K.cisco.com	40.0.1.14		DISTRIBUTION	Add	Add	0
SDN-BRANCH-WLC5K	40.0.1.74	28:94:0f:ae:19:e0	ACCESS	Add	Add	0
SDN-CAMPUS-ASR9K.cisco.com	40.0.1.2		BORDER ROUTER	Add	Add	0
SDN-CAMPUS-C4K.cisco.com	40.0.1.42		DISTRIBUTION	Add	Add	0
SDN-CAMPUS-C6K-2.cisco.com	40.0.1.18		DISTRIBUTION	Add	Add	0
SDN-CAMPUS-ISR3945.yourdomain.com	40.0.1.57		BORDER ROUTER	Add	Add	0
SDN-LAP1252-AP2	0.0.0.0	00:17:df:a7:5d:80	ACCESS	Add	Not Available	0

12 Devices

Before You Begin

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

Procedure

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.

APIC-EM displays the information for the chosen layout.

Step 2 To customize a specific layout, choose **Customize** and select the desired display options. Display options toggle on and off. Blue options with checkmarks indicate that the option is on and is displayed in the table.

What to Do Next

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

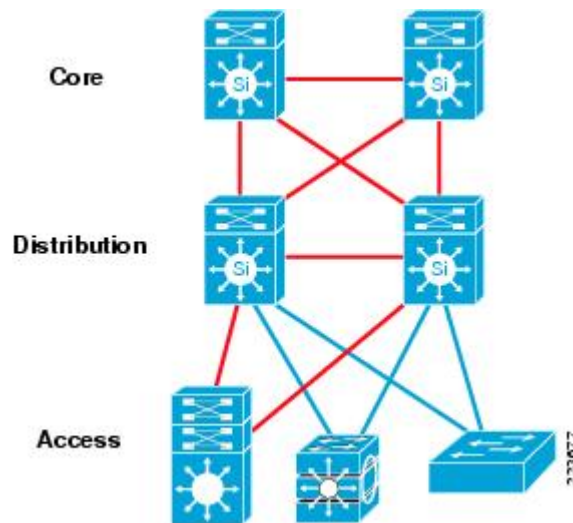
Changing the Device Role

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

A device can have one of the following roles:

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

Figure 11: Device Roles and Network Locations



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



Note

You can also change the device role from the **Topology** window. See [Changing a Device's Role From the Topology Window](#), on page 89.

Before You Begin

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

You must have administrator permissions to perform this procedure. For information, see [Managing Users and Roles](#), on page 15.

Procedure

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

What to Do Next

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

Related Topics

[Managing Your Device Inventory](#), on page 50

Deleting a Device

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

Before You Begin

You must have administrator (ROLE_ADMIN) permissions to perform this procedure.

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

Procedure

- Step 1** From the **Navigation** pane, click **Device Inventory**.
- Step 2** Click the check box next to the device that you want to delete.
A toolbar opens.
- Note** Even after the toolbar opens, you can select multiple devices by clicking additional check boxes, or you can select all devices by clicking the checkbox at the top of the list.
- Step 3** From the open toolbar, click **Delete**.
-

Adding or Removing a Device Tag in Device Inventory

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



Note

For information about Policy tags and Location tags, see the Device Inventory table in [Managing Your Device Inventory](#), on page 50.

The screenshot shows the Cisco APIC Device Inventory interface. A modal window titled "SDN-BRANCH-AP1252-1" is open, displaying a list of available device tags and applied tags. The "Available Device Tags" list includes "Eng". The "Applied Tags" list is currently empty. At the bottom of the modal, there is a "Device Tag Title" input field and a "+ Create Tag" button. The background shows a table of devices with columns for Device Name, IP Address, MAC Address, Device Role, Location, Policy Tag, and Device Tag. The table is filtered to show 13 devices, and the layout is set to "Tagging".

Before You Begin

You must have administrator (ROLE_ADMIN) permissions to perform this procedure.

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

Procedure

- Step 1** From the **Navigation** pane, click **Device Inventory**.
- Step 2** From the **Device Inventory** toolbar, choose **Layout > Tagging** from the drop-down list. The table refreshes and displays a **Device Tag** column in addition to other columns.
- Step 3** Select the check box to the left of the desired devices and click **Set Device Tags**.

Note For a single device, you can also click the number displayed in the **Device Tag** column.
- Step 4** Do one of the following:
 - To apply a device tag, from the **Available Tags** list, click the tags that you want to apply to the selected devices.

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

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

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

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

What to Do Next

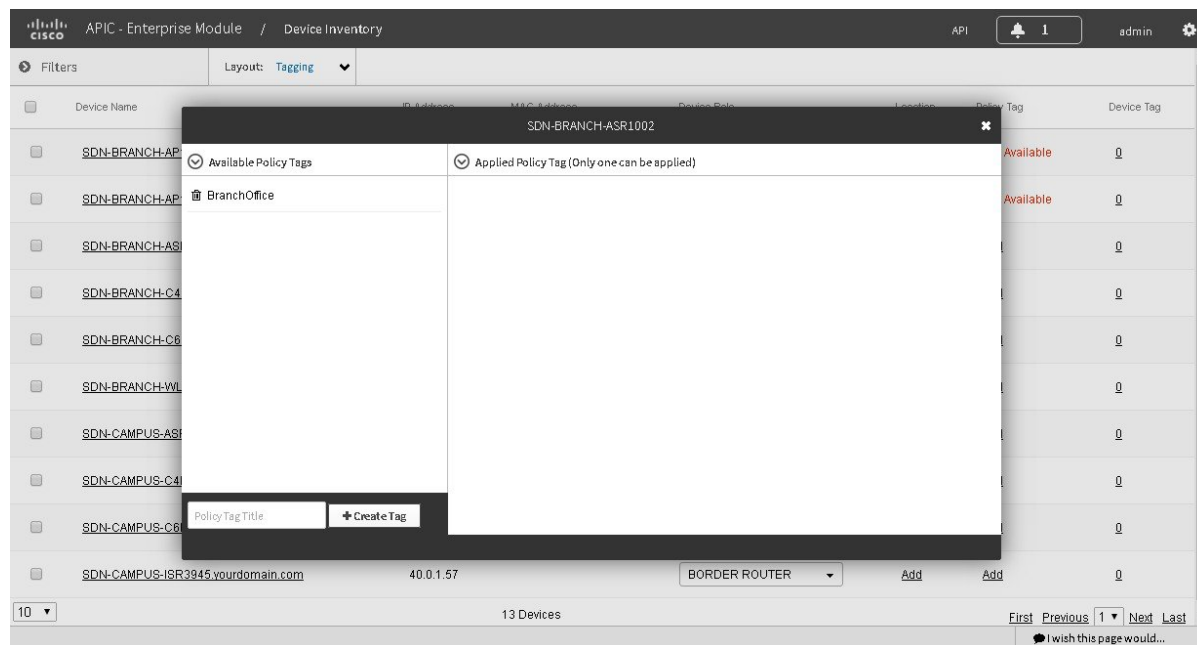
If required for your network configuration, add location or policy tags to your devices.

Related Topics

[Managing Your Device Inventory, on page 50](#)

Adding or Removing a Policy Tag in Device Inventory

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



Before You Begin

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

Procedure

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

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

Step 3 Select the check box to the left of the desired devices and click **Set Policy Tag**.

Note For a single device, you can also click **Add** displayed in the **Policy Tag** column.

Step 4 Do one of the following:

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

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

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

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

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

What to Do Next

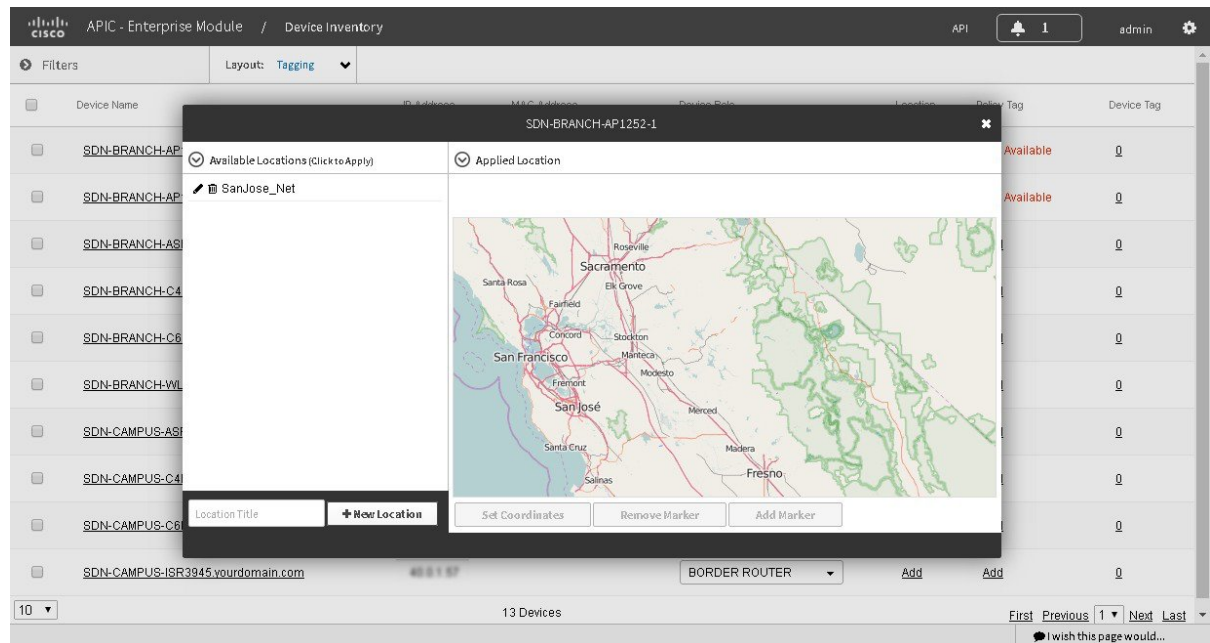
If you added a policy tag to devices and now want to configure QoS policies, see [Configuring Quality of Service, on page 97](#).

Adding or Removing a Location Tag

You can apply a location tag to a device to denote the device's geographic location. By applying the same tag to several devices, you can group them based on a common attribute. The **Device Inventory** window and **Topology** window support location tags.

Use the following guidelines when adding location tags:

- Location tag information is maintained on the controller only and not deployed to or derived from the device itself.
- A location defined on the controller is not the "civic-location" property that some devices support.
- You cannot create, use, or search for location tags in the **Topology** window.
- Location tags cannot be attached to hosts.
- You can apply only one location tag to a device. However, you can use both a location tag and a device tag together.



Before You Begin

You must have administrator (ROLE_ADMIN) permissions to perform this procedure.

Procedure

- Step 1** From the **Navigation** pane, click **Device Inventory**.
- Step 2** From the **Device Inventory** toolbar, choose **Layout > Tagging** from the drop-down list. The table refreshes and displays a **Device Tag** column in addition to other columns.
- Step 3** Select the check box to the left of the desired devices and click **Set Device Tags**.

Note For a single device, you can also click the number displayed in the **Device Tag** column.
- Step 4** Do one of the following:
 - To apply a location tag, from the **Available Tags** list, click the tags that you want to apply to the selected devices.

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

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

Note The **Applied Tags** list is populated only if at least one of the selected devices has a tag applied to it.
- Step 5** Click **x** to close the dialog box.

What to Do Next

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

Related Topics

[Managing Your Device Inventory](#), on page 50

[Adding or Removing a Location Marker](#), on page 66

Adding or Removing a Location Marker

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

Before You Begin

You must have administrator (ROLE_ADMIN) permissions to perform this procedure.

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

You have already added location tags to your devices.

Procedure

- Step 1** From the **Navigation** pane, click **Device Inventory**.
- Step 2** From the **Device Inventory** toolbar, choose **Layout > Tagging** from the drop-down list. The table refreshes and displays a **Location** column in addition to other columns.
- Step 3** (Optional) To display devices with a specific location tag, from the **Device Inventory** toolbar, click **Filters**, enter a location tag in the **Device Location** field, and click the + icon.
- Step 4** Select the desired location from the **Locations** column.
- Note** Because you are not assigning a location tag, it is not important which device you choose. When you add or remove a location marker, the change is applied to the location tag, and all devices that have the location tag will be updated.
- Step 5** Do one of the following:
- To add a location marker, position the map as close to the desired location as possible and click **Add Marker**. When the location marker is in the desired location, click **Set Coordinates**.
- Note** You can position the map using your mouse to drag the map and to zoom in and out on the map. If needed, drag and drop the location marker (building icon) to where you want it.

Note To add additional location markers, close the **Location** dialog box and, from the **Device Inventory** window, 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.

Figure 12: Adding a Location Marker

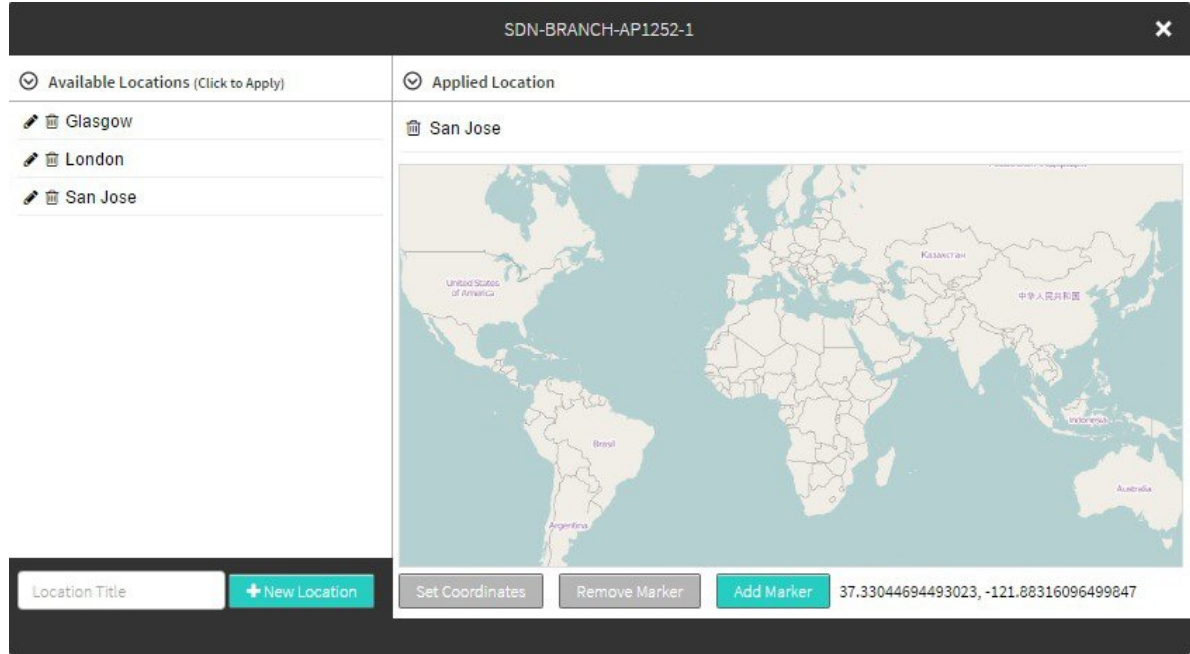
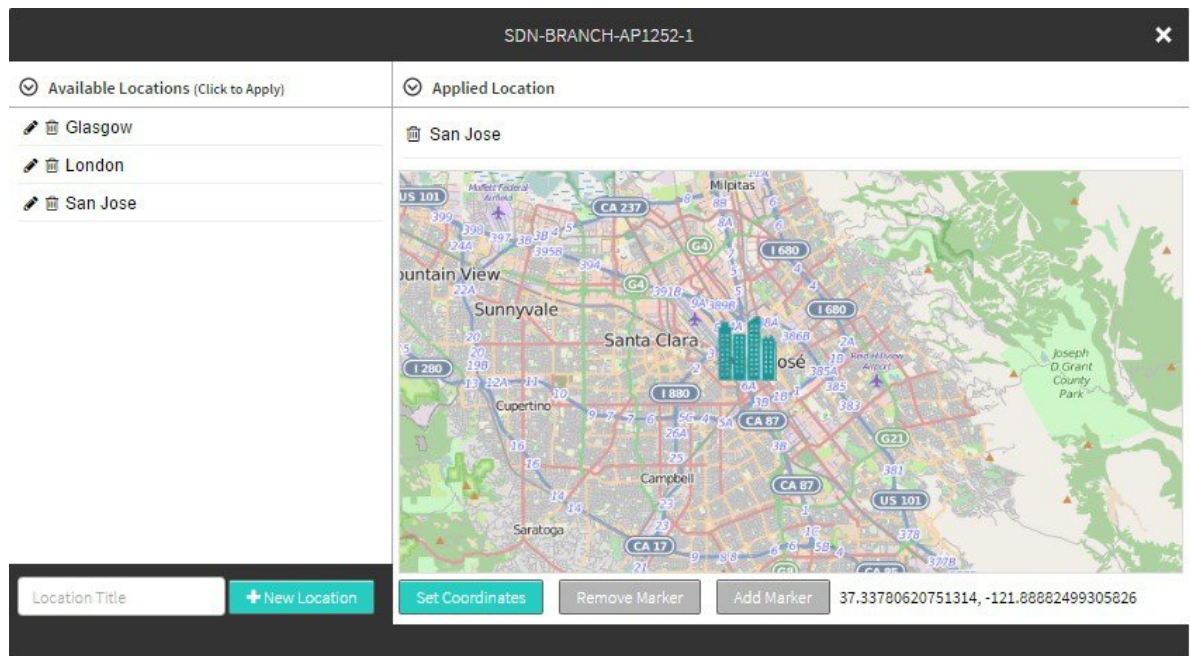
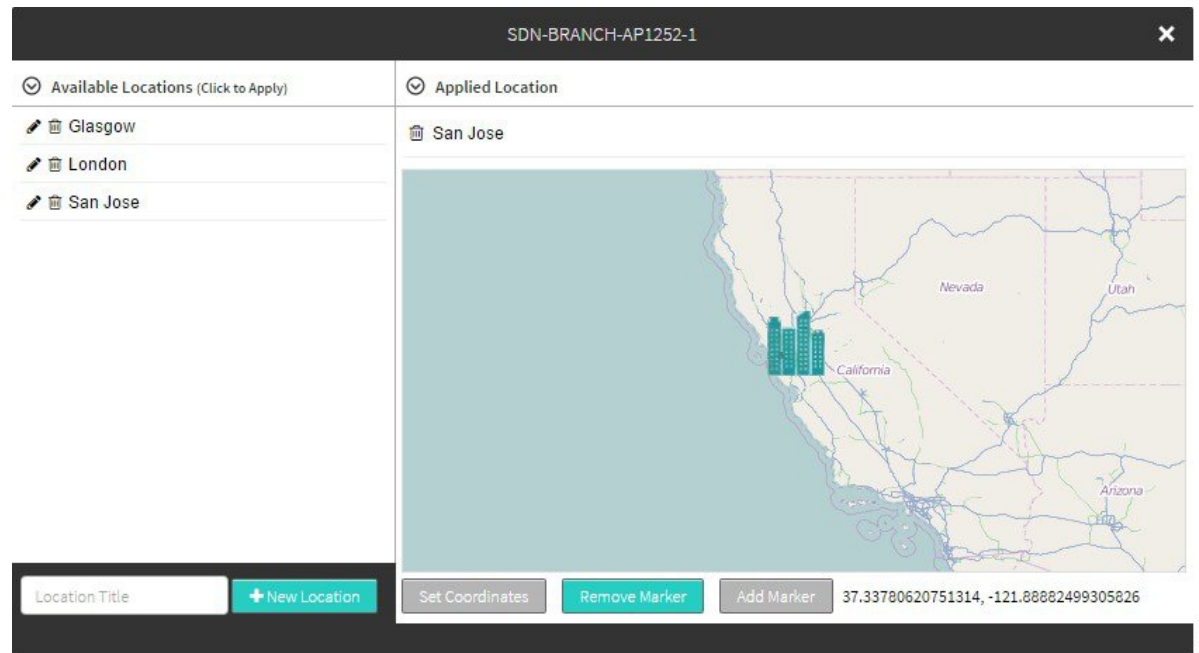


Figure 13: Placing the Location Marker



- b) To remove the location marker, click **Remove Marker**.

Figure 14: Location Window



- Step 6** Click **X** to close the dialog box.

What to Do Next

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

Related Topics

[Managing Your Device Inventory, on page 50](#)

[Topology](#)

[Topology Icons, on page 78](#)

[Topology Toolbar](#)

Deleting a Tag

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

Before You Begin

You must have administrator (ROLE_ADMIN) permissions to perform this procedure.

Make sure that you have devices in your inventory. If not, discover devices using the Discovery function. Before you can delete a tag, you need to remove it from all devices that have been assigned the tag.

Procedure

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

Managing Your Host Inventory

Cisco APIC-EM displays information about the discovered hosts in the **Host Inventory** window. The following table describes the information that is displayed about the hosts in your inventory.

**Note**

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

Figure 15: Host Inventory Window

Host MAC Address	Host IP Address	Host Type	Connected Network Device IP Address	Connected Interface Name	Host Name
00:1b:d5:13:39:ca	40.0.0.10	WIRED	40.0.21.2	GigabitEthernet1/0/2	
00:22:90:91:3b:d5	40.0.0.51	WIRED	40.0.21.2	GigabitEthernet1/0/2	
00:22:90:a3:36:6a	40.0.10.219	WIRED	40.0.21.2	GigabitEthernet1/0/2	
00:24:14:d2:48:f4	40.0.11.85	WIRED	40.0.21.2	GigabitEthernet1/0/2	
00:26:cb:7e:d2:dc	40.0.20.100	WIRED	40.0.21.2	GigabitEthernet1/0/2	
00:50:56:8a:1c:2d	40.0.7.15	WIRED	40.0.21.3	GigabitEthernet1/0/2	
00:50:56:ae:06:9e	40.0.7.13	WIRED	40.0.21.3	GigabitEthernet1/0/3	
00:50:56:ae:1d:df	40.0.7.14	WIRED	40.0.21.3	GigabitEthernet1/0/3	
24:e9:b3:3f:48:00	40.0.04.10	WIRED	40.0.04.20	GigabitEthernet1/0/2	
50:87:89:90:9d:aa	40.0.7.7	WIRED	40.0.21.3	GigabitEthernet1/0/3	

10 per page 20 Hosts < Previous 1 of 2 Next >

I wish this page would..

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

Table 13: Host Inventory

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

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

Related Topics

[Changing the Hosts Table View, on page 71](#)

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.

Procedure

-
- 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 69](#)



Using the Topology Map

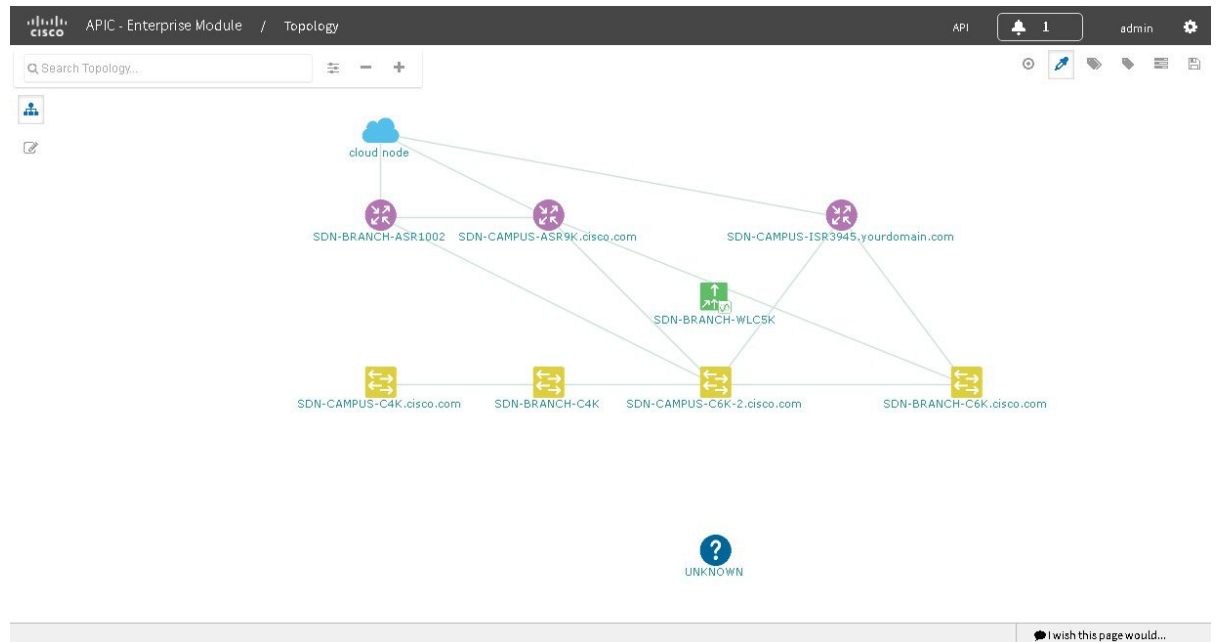
- [About Topology, page 73](#)
- [Displaying Device Data, page 80](#)
- [Aggregating Devices, page 81](#)
- [Configuring the Topology Structure, page 85](#)
- [Saving a Topology Layout, page 87](#)
- [Opening a Saved Topology Layout, page 88](#)
- [Changing a Device's Role From the Topology Window, page 89](#)
- [Searching for Devices, page 91](#)
- [Adding or Removing a Device Tag in Topology , page 93](#)
- [Adding or Removing a Policy Tag in Topology, page 94](#)
- [Displaying Devices with Tags, page 95](#)

About Topology

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

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

Figure 16: Topology Window



The topology map includes the following key features:

- Auto-visualization of Layer 2 and 3 topologies on top of the physical topology for a granular view for design planning and simplified troubleshooting.
- For a Layer 2 topology, display of configured VLANs within your network. For a Layer 3 topology, display of OSPF, IS-IS, and so on, depending on what is currently configured and in use in your network.
- Device information.
- Display of a path trace in the topology map. For additional information about the performing a path trace, see [About Path Trace](#), on page 127.



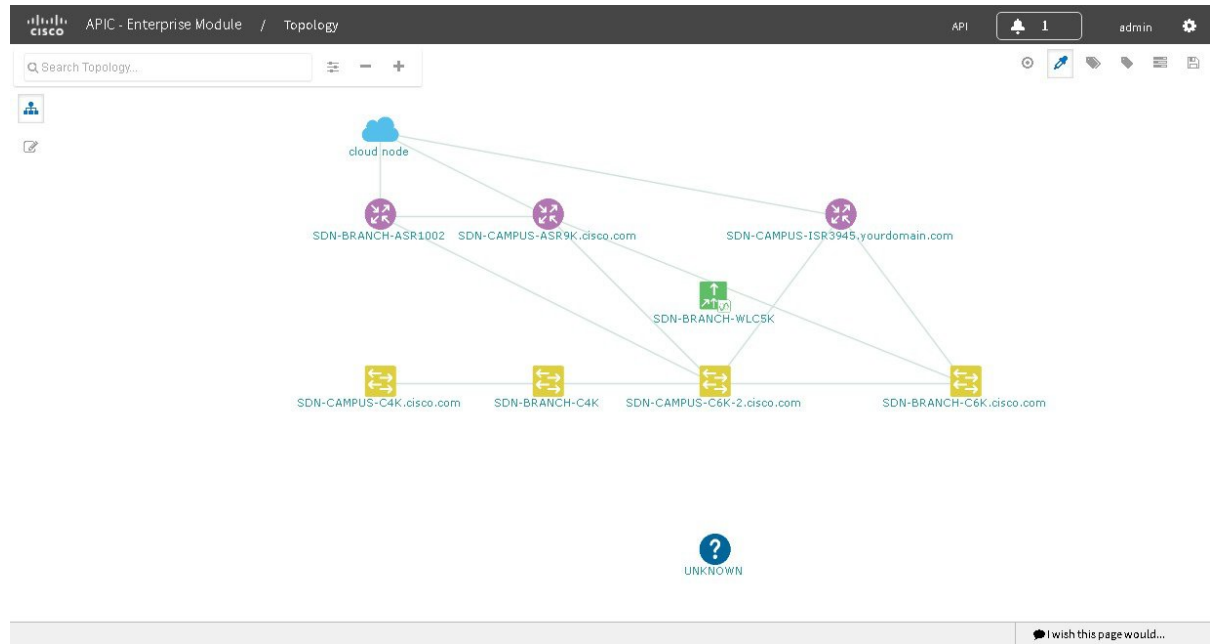
Note



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

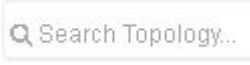




Topology Toolbar




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



Figure 17: Topology Window



Icon	Name	Description
	Toggle Aggregation	<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 Save icon.</p> <p>This grouping does not effect the physical configuration on the devices. Aggregation is enabled by default.</p>
	Toggle Multiselect	<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>






Icon	Name	Description
	Search Topology	Searches for a host or device by host name, device name, device type, or IP address. As you enter information into this field, the Cisco APIC-EM displays matches. Select the host or device from the results that appear. The selected host or device appears in the Topology window.
	Filters	<p>Allows you to choose a filter that you can apply to the topology map. For each filter, you can make additional adjustments using the Advanced options. For information, see Configuring the Topology Structure, on page 85.</p> <ul style="list-style-type: none"> • Enterprise (Default)—Displays your network topology, separating your devices on connection branches. For example, if a group of devices are connected to Router A, and another group of devices are connected to Router B, the topology would show this division and would separate the devices. • Connections—Displays the devices according to their number of connections. Starting from the left, the devices with no connections are displayed, then devices with one connection, then devices with two connections, and so on. • Type and Role—Displays the devices according to their role in the network: access router, distribution switch, core switch and hub, and boarder router. • Advanced—Provides options for you to refine the topology display.
	Zoom out	Note Adjusts the Topology window's view. Click the - (minus) icon to minimize the view of the network hosts and devices.
	Zoom in	Adjusts the Topology window's view. Click the + (plus) icon on the menu bar to maximize the view of the network hosts and devices.
	Toggle Color Code	Toggles between displaying the device icons in different colors or in a single color. Color coding is enabled by default.



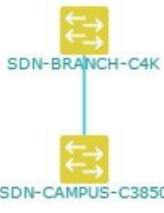
Icon	Name	Description
	Device Tags	<p>Displays the available device tags. Clicking on an individual tag highlights the device or devices in the Topology window that have this tag.</p> <p>You can also apply tags to devices by selecting the device, clicking Device Tagging in the Device Information dialog box, and then creating and applying the tags.</p>
	Policy Tags	<p>Displays the available policy tags. Clicking on an individual tag adds the device to the policy scope.</p> <p>You can also apply policy tags to devices in the EasyQoS > Policy Scopes.</p>
	Layers	<p>Displays devices with the following attributes on the topology map:</p> <ul style="list-style-type: none"> • Layer 2—Displays devices based on the selected VLAN or Layer 2 protocol. Select either a VLAN from the drop-down menu or one of the Layer 2 protocols. <ul style="list-style-type: none"> Note You can also access a management network view by choosing a management selection from the drop-down menu. • Layer 3—Displays devices based on the selected Layer 3 protocol. The following Layer 3 protocols are available: <ul style="list-style-type: none"> ◦ Intermediate System-to-Intermediate System (IS-IS) ◦ Open Shortest Path First (OSPF) ◦ Enhanced Interior Gateway Routing Protocol (EIGRP) ◦ Static-Route <ul style="list-style-type: none"> Note The default Layer 3 topology has all Layer 3 protocols. • VRF—Displays devices that have Virtual Routing and Forwarding (VRF) tables.

Icon	Name	Description
	Save and Load Options	Displays the following options: <ul style="list-style-type: none"> • Save Current Layout—Saves the current layout, device aggregations, and labels. • Load Saved Layout—Loads the previously saved layout, device aggregations, and labels) options.
	Map view	Displays the Topology map view. Click this icon to view the network topology in a graphical representation of your network's physical location. <p>Note This icon is displayed only if you have added location markers for your devices from the Device Inventory window.</p>

Topology Icons

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

Icon	Network Element	Description
	Cloud	Representation of the external network.
	Router	Displays the device name.
	Switch	Displays the device name.
	Access Point	Displays the device name.
	Wireless LAN Controller	Displays the device name.

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

Related Topics

[Applying Tags to Devices](#)

[Viewing Device Data](#)

[Searching for Devices, on page 91](#)

[Configuring the Topology Structure, on page 85](#)

[Changing the Aggregated Devices Label, on page 84](#)

[Removing Tags from Devices](#)

[Viewing Devices with Tags](#)

[Adding or Removing a Location Marker, on page 66](#)

[Aggregating Devices in the Topology Window, on page 81](#)

[Configuring the Topology Structure, on page 85](#)

[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 60.)
- IP address
- MAC address
- OS (operating system)
- Software version
- Ports
 - Gigabit Ethernet ports
 - 10-Gigabit Ethernet ports
 - Management ports
- VLAN (if exists)
- Number of connections
- List of connected devices (Each connected device shows its device type (icon) and the number of connections. Clicking on a connected device displays the details for that device.)
- Tags

Procedure

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

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

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

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

- a) In the **Topology** window, click an **aggregated devices** icon.

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

What to Do Next

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

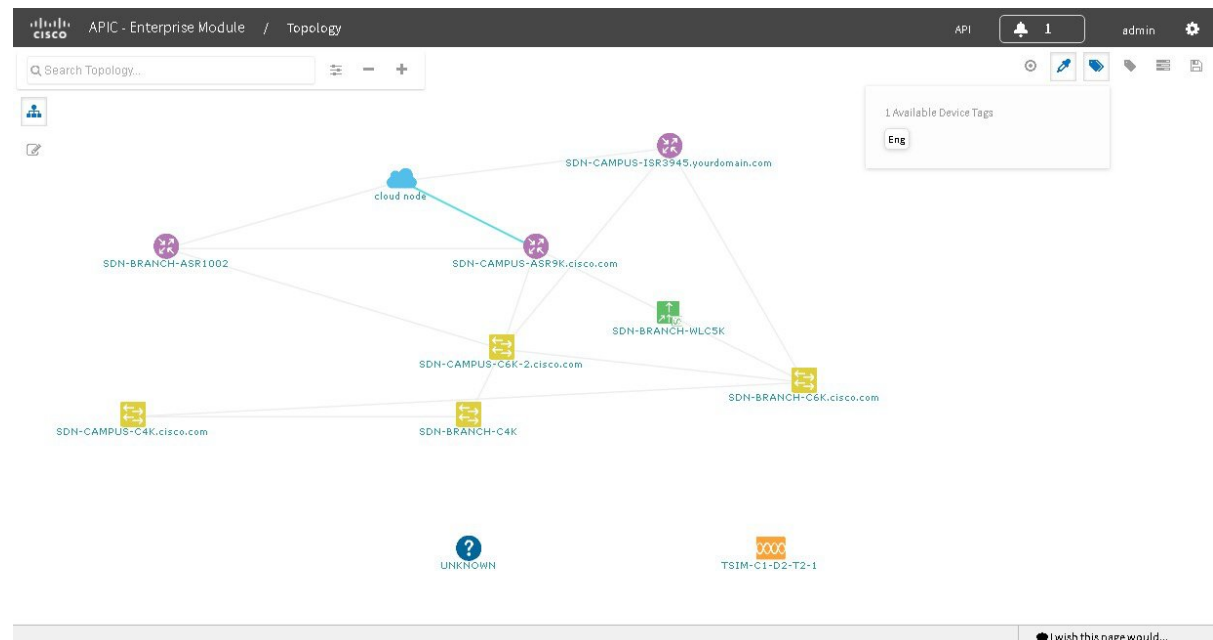
- Aggregate or disaggregate selected groups
- Search for device using device names and IP addresses
- Apply tags to devices within your network
- Change the device role

Aggregating Devices

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

Aggregating Devices in the Topology Window

You can aggregate and 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 inventory for the database.

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

Procedure

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 78.

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 78

[Topology Toolbar](#)

Disaggregating Devices in the Topology Window

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

The screenshot displays the 'Applications' page in the Cisco APIC-EM interface. At the top, there is a navigation bar with a back arrow, the title 'Applications', a 'Scope' dropdown set to 'BranchTag1', and an 'Apply Policy' button. Below the navigation bar, there are options to 'Add Application', 'Favorite Applications', and a search bar. The main content area is divided into sections: 'Custom Applications' and '#'. The 'Custom Applications' section contains one entry: 'TrueUp (TrueUp)' with protocol 'TRANSACTIONAL_DATA' and port '10.1.1.1 tcp 1500'. The '#' section contains several entries, each with a star icon, a description, protocol, port, and a policy dropdown menu. The entries are: '3Com AMP3 (scom-amp3)' with protocol 'BULK_DATA' and port 'tcp 829 udp 829' (policy: Default); '3Com TSMUX (scom-tsmux)' with protocol 'BULK_DATA' and port 'tcp 106 udp 106' (policy: Default); '4chan - Website that hosts found images and discussions on them. (4chan)' with protocol 'TRANSACTIONAL_DATA' and port 'tcp 80,443' (policy: Business-Irrelevant); '58 City - Classified information about 58 cities in China. (58-city)' with protocol 'TRANSACTIONAL_DATA' and port 'tcp 80,443' (policy: Business-Irrelevant); 'A network traffic monitoring and IP information collection protocol (ipfix)' with protocol 'BULK_DATA' (policy: Default); 'A network traffic monitoring and IP information collection protocol (netflow)' with protocol 'BULK_DATA' (policy: Default); 'A remote network server system (ams)' with protocol 'BULK_DATA' and port 'tcp 384 udp 384' (policy: Default); and 'ABC - Web Portal for television network. (abc-news)' with protocol 'TRANSACTIONAL_DATA' and port 'tcp 80,443' (policy: Business-Irrelevant).

Before You Begin

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

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

Procedure

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

The **Topology** window appears.

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

Step 2 Click on an **aggregated devices** icon.
A list of the aggregated devices appears.

Step 3 From the list, click the **Disaggregate** link for each device that you want to remove from the aggregated devices. The device is removed from the list and from the aggregated devices icon. The aggregated device label and the aggregated devices icon are updated to reflect the number of devices.

Changing the Aggregated Devices Label

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

Before You Begin

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

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

Procedure

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.

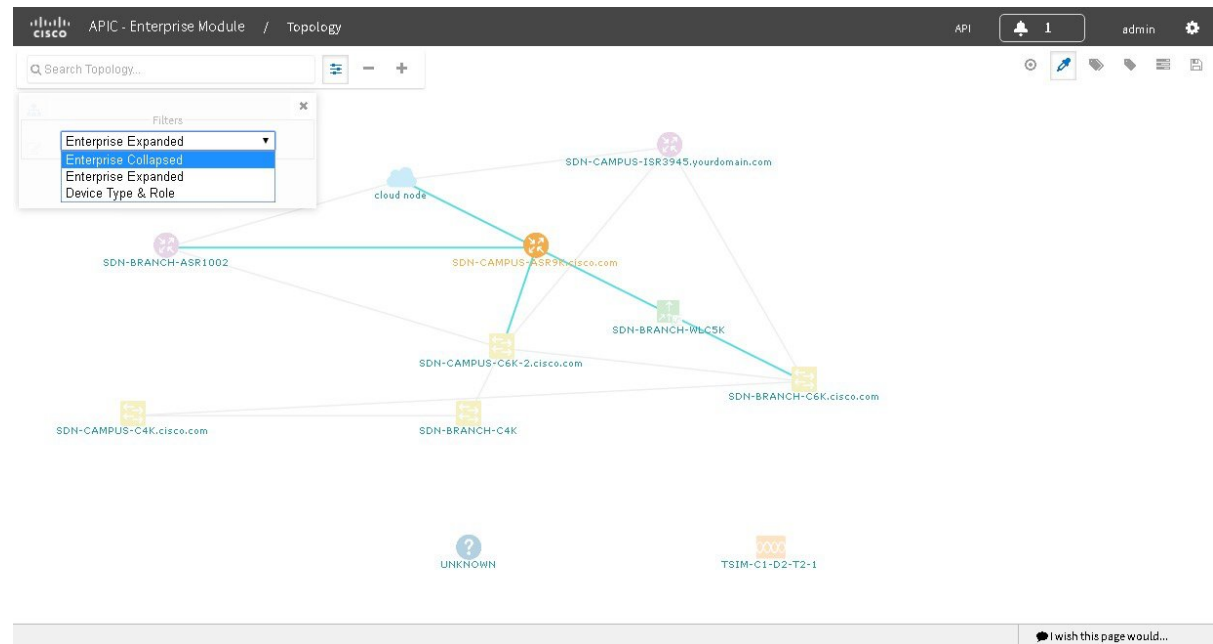
- Step 2** Click an **aggregated devices** icon.
A list of the aggregated devices appears. At the top of the list is the aggregated devices label.
- Step 3** Click the aggregated devices label to open an edit field where you can change the label.
- Step 4** Change the label, then click outside of the edit field to save your changes.

Related Topics

- [Topology](#)
- [Topology Icons, on page 78](#)
- [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 inventory for the database.

Procedure

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

What to Do Next

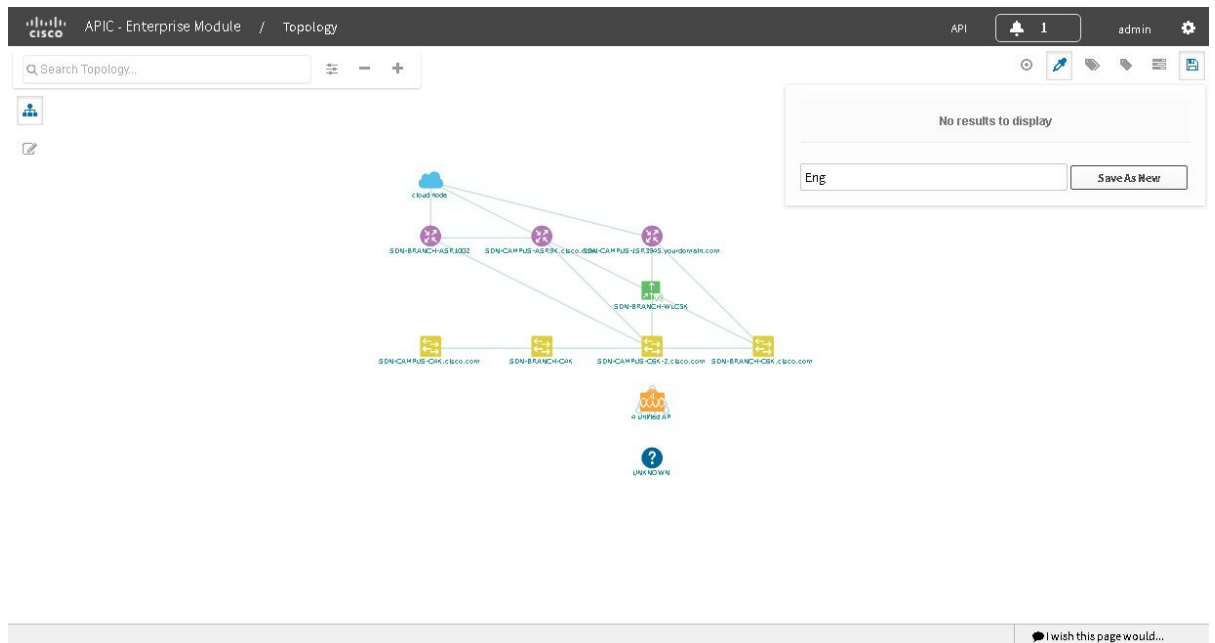
Save the current layout or load a previously saved layout. For information, see [Saving a Topology Layout, on page 87](#) and [Opening a Saved Topology Layout, on page 88](#).

Related Topics

- [Topology](#)
- [Topology Icons, on page 78](#)
- [Topology Toolbar](#)
- [Topology](#)
- [Topology Icons, on page 78](#)
- [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 administrator (ROLE_ADMIN) permissions to perform this procedure.

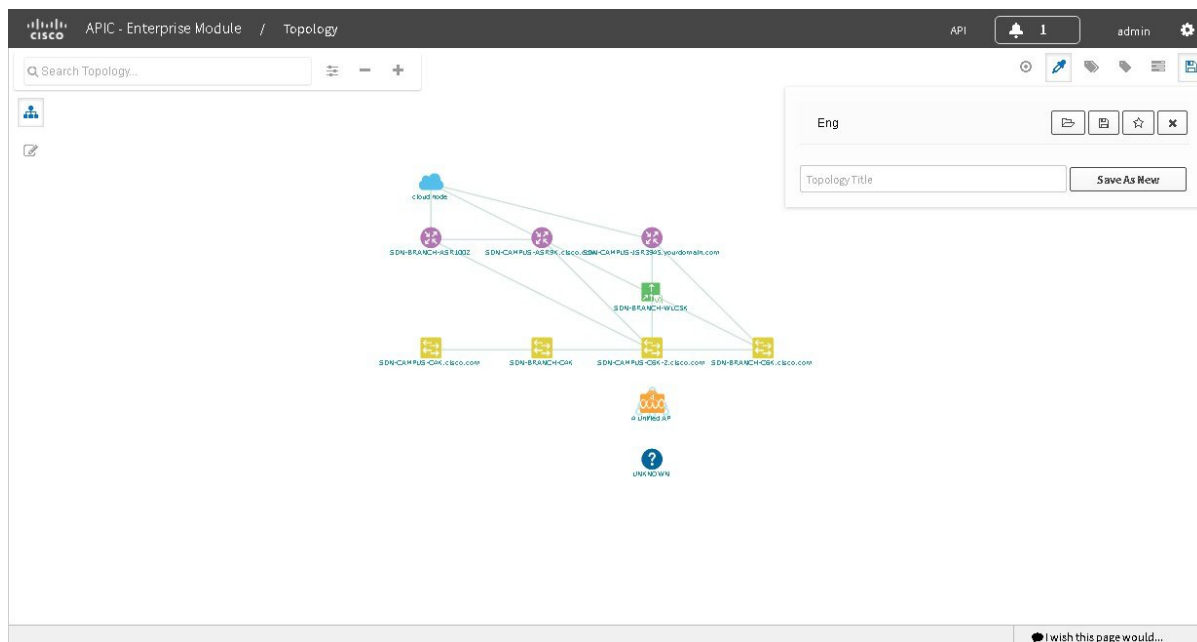
Make sure that you have devices in your inventory. If not, discover devices using the Discovery function.

Procedure

- 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_ADMIN) permissions to perform this procedure.

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

Procedure

- Step 1** From the **Navigation** pane, click **Topology**.
The **Topology** window appears.
- Step 2** From the **Topology** toolbar, click the **Save** icon.
A dialog box appears listing the saved topology layouts.
- Step 3** For the topology layout that you want to open, click the **Folder** icon..
- Step 4** Click **OK** to confirm.
The topology layout opens in the **Topology** window.

Changing a Device's Role From the Topology Window

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

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

- Unknown—Device role is unknown.

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

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



Note

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

The screenshot shows the Cisco APIC-EM interface. The main window displays a network topology map with various nodes and connections. A 'Device Tapping' dialog box is open, showing details for a device named 'SDN-CAMPUS-ASR9K.cisco.com'. The dialog box includes fields for Type, Family, Role, IP, Platform, Version, Connections, and Tags. The 'Role' dropdown menu is currently set to 'BORDER ROUTER' and is expanded to show other options: UNKNOWN, ACCESS, DISTRIBUTION, and CORE. The 'Connections' list shows the device is connected to a 'cloud node' and several other devices: 'SDN-BRANCH-ASR1002', 'SDN-BRANCH-C6K.cisco.com', and 'SDN-CAMPUS-C6K-2.cisco.com'. The network map in the background shows a central 'SDN-CAMPUS-ASR9K.cisco.com' node connected to a 'cloud node' and several 'SDN-BRANCH' nodes. A 'TSIM-C1-D2-T2-1' node is also visible at the bottom right of the map.

Before You Begin

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

Procedure

- 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

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

- Device 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).



I wish this page would...

Before You Begin

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

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

Procedure

-
- Step 1** Click **Topology** in the navigation pane. The **Topology** window appears.
- Note** If you have added location markers for your devices from the **Device Inventory** window, the Topology map view appears. Click a location marker on the map to display the Topology for that location.
- Step 2** From the Topology toolbar, enter a keyword in the **Search Topology** field. As you begin typing, the controller displays a list of possible matches to your entry.
- Note** You can click the **x** in the search field to clear the search keyword field and the results.
- Step 3** Click on a device from the search results to highlight that device and its links in the **Topology** window. Click on the device again to display detailed data for that device.
- Step 4** Proceed with any provisioning or troubleshooting tasks on the located devices.
-

What to Do Next

Search using other string values for other 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 78](#)
- [Topology Toolbar](#)

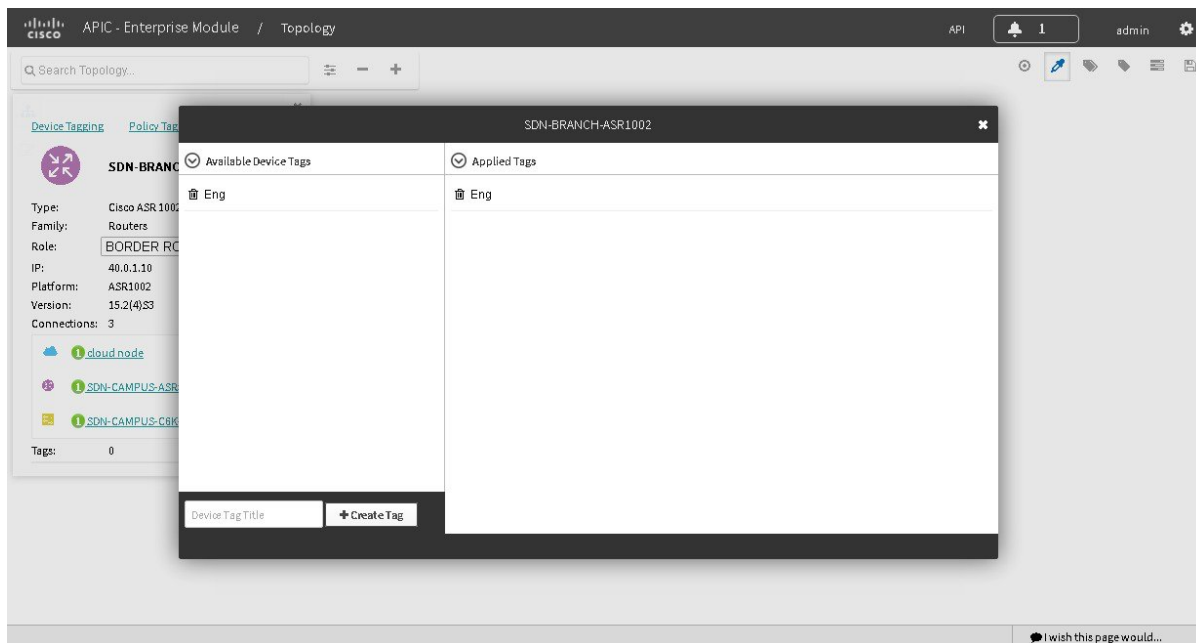
Adding or Removing a Device Tag in Topology

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

You can also add or remove device tags from the **Device Inventory** window or from the **EasyQoS** window. For information, see [Adding or Removing a Device Tag in Device Inventory, on page 62](#) and [Defining a Policy Scope, on page 114](#).

**Note**

Applying a tag to a host is not supported.

**Before You Begin**

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

Procedure

- Step 1** From the Navigation pane, click **Topology**.
- Step 2** Click the device or devices you want to tag. To select more than one device, click the **Multiselect** icon. For information about how to use the multiselect function, see [Topology Icons](#), on page 78.
- Note** To deselect devices in your selection, click outside of the selected device.
- The **Device Information** dialog box appears.
- Step 3** Click **Device Tagging**.
The **Device Tagging** dialog box appears.
- Step 4** From the **Available Tags** column, click a tag to apply it to the selected device or devices. If the tag you want does not exist, you can create it by entering the name of the tag in the **Device Tag Title** field and clicking **+Create Tag**.
- Step 5** When you are done, click **x** to close the dialog box.
-

Adding or Removing a Policy Tag in Topology

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

You can also add or remove policy tags from the **Device Inventory** window or the **EasyQoS** window. For information, see [Adding or Removing a Device Tag in Device Inventory](#), on page 62 or [Defining a Policy Scope](#), on page 114.

Before You Begin

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

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

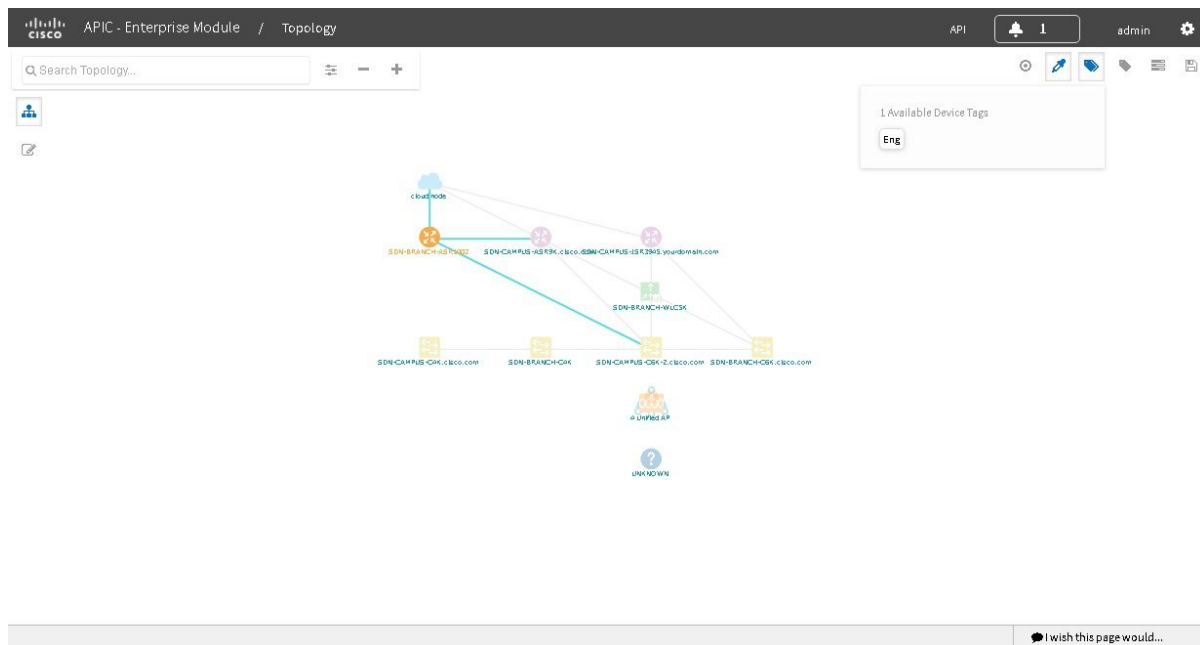
Procedure

- Step 1** From the Navigation pane, click **Topology**.
- Step 2** Click the device or devices you want to tag. To select more than one device, click the **Multiselect** icon. For information about how to use the multiselect function, see [Topology Icons](#), on page 78.
- Note** To deselect devices in your selection, click outside of the selected device.
- The **Device Information** dialog box appears.
- Step 3** Click **Policy Tagging**.
The **Multiple Policy Tagging** dialog box appears.

- Step 4** From the **Available Policy Tags** column, click a tag to apply it to the selected device or devices. If the tag you want does not exist, you can create it by entering the name of the tag in the **Policy Tag Title** field and clicking **+Create Tag**.
- Step 5** When you are done, click **x** to close the dialog box.

Displaying Devices with Tags

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



Before You Begin

You should have performed the following tasks:

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

Procedure

- Step 1** From the Navigation pane, click **Topology**.
The **Topology** window appears.
- Step 2** From the Topology toolbar, click the **Tags**.
A tag selection box appears.
- Step 3** To identify the devices associated with a tag, click the tag. To return the devices to their normal display, click the tag again.
Tags are color-coded, so when you click a tag, a circle of the same color is drawn around its associated devices.

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



Configuring Quality of Service

- [About EasyQoS, page 97](#)
- [EasyQoS Prerequisites, page 98](#)
- [Understanding QoS Policies, page 98](#)
- [Understanding Applications, page 102](#)
- [Understanding Dynamic QoS, page 106](#)
- [EasyQoS Guidelines and Limitations, page 106](#)
- [Enabling the EasyQoS Beta Feature, page 107](#)
- [Getting Started with EasyQoS, page 108](#)
- [Configuring QoS Policies, page 111](#)

About EasyQoS

Quality of service (QoS) refers to the ability of a network to provide preferential or deferential service to selected network traffic. The Cisco APIC-EM enables you to configure quality of service on the devices in your network using the EasyQoS feature.

You define the scope of the devices that you want to apply a QoS policy on. Then you define the QoS policy for the scope. The Cisco APIC-EM takes your selections, translates them into the proper device command line interface (CLI) commands, and deploys them onto the devices defined in the scope.

EasyQoS configures quality of service policies on devices based on the QoS feature set available on the device. For more information about a specific device's QoS implementation, see the device product documentation.



Note

To configure QoS on the devices in your network, you must be assigned either administrative permissions (ADMIN_ROLE) or policy administrator permissions (POLICY_ADMIN_ROLE) to use EasyQoS. For information, see [Managing Users and Roles, on page 15](#).

EasyQoS Prerequisites

To use EasyQoS to configure QoS policies, make sure that you address the following requirements:

- Enable the EasyQoS feature on the controller. For information, see [Enabling the EasyQoS Beta Feature, on page 107](#).
- EasyQoS supports most of the Cisco LAN, WAN, WLAN devices. To verify whether the devices and software versions in your network are supported, see the *Supported Platforms for the Cisco Application Policy Infrastructure Controller Enterprise Module* document.
- Make sure that your Cisco network devices, such as the ISR-G2, the ASR 1000, and Wireless LAN Controller, have the AVC (Application Visibility and Control) feature license installed. For information, see the *NBAR2 (Next Generation NBAR) Protocol Pack FAQ* at the following URL: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/network-based-application-recognition-nbar/qa_C67-723689.html.
- For the Cisco APIC-EM to identify the WAN interfaces that need policies, you must specify the interface type (WAN) and (optionally) its subline rate and service-provider Class-of-Service model. For information about how to configure these settings on WAN interfaces, see [Required Device Configuration, on page 161](#).
- From the **Topology** or **Device Inventory** window, verify that the device roles assigned to devices during discovery are appropriate for your network design. If necessary, change any of the device roles that are not appropriate.

Understanding QoS Policies

A QoS policy defines how network traffic should be handled so that you can make the most efficient use of network resources while still adhering to the objectives of the business (such as guaranteeing voice quality meets enterprise standards or ensuring a high Quality of Experience (QoE) for video). To achieve these goals, a policy comprises the following elements:

- **Policy Scope**—Group of devices that will be configured with the policy.
- **Applications**—Software programs or network signaling protocols that are being used in your network. EasyQoS includes the Cisco Network Based Application Recognition, second generation (NBAR2) application library of approximately 1400 distinct applications. For more information about NBAR2, see the following URL: <http://www.cisco.com/c/en/us/products/ios-nx-os-software/network-based-application-recognition-nbar/index.html>.
- **Traffic Classes**—Groups of applications that make configuring policies easier, because the groups contain applications that have similar traffic needs.
- **Business-relevance**—Attribute that classifies a given application according to how relevant it is to your business and operations. The attributes are business relevant, default, and business irrelevant. For information, see [Business-Relevance Groups, on page 102](#).

EasyQoS comes with the Cisco NBAR2 applications preconfigured into application categories and sorted into business-relevancy groups. You can apply this preconfigured policy to your network devices, or you can modify it to meet the needs of your business objectives and your network configuration.

For example, YouTube is set as business-irrelevant (by default), because most customers typically classify this application this way. However, this classification may not be the true for all companies; for example, some businesses may be using YouTube for training purposes. In such cases, an administrator can change this business-relevancy setting to **business-relevant** to align with their business objectives.

The QoS trust and QoS queuing functionality is preconfigured for the current release and cannot be changed. QoS trust and QoS queuing is set per device according to the Cisco Validated Design (CVD) for Enterprise Medianet Quality of Service Design.

The latest validated designs are published in the Cisco Press book, *End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks*, 2nd Edition, available at: <http://www.ciscopress.com/store/end-to-end-qos-network-design-quality-of-service-for-9781587143694>. For additional information about Cisco Validated Design (CVD) for Enterprise Medianet Quality of Service, see the following Cisco documentation:

- [Cisco Validated Designs](#)
- [Enterprise Medianet Quality of Service Design 4.0](#)
- [Medianet Campus QoS Design 4.0](#)
- [Medianet WAN Aggregation QoS Design 4.0](#)

Policy Scope

A policy scope defines a specific set of devices for the purpose of applying a QoS policy to manage a particular kind of traffic. Up to 2,000 devices can be configured per scope. Scopes cannot overlap. That is, an individual device cannot be a member of more than one scope. Each policy scope can provide one policy for all wired devices in the scope and one policy for each wireless segment in the scope. For each policy (wired or wireless-segment), you can include or exclude any applications (including custom) and customize the treatment of the traffic for that application.

In practice, you should include all devices (wired or wireless) that compose the end-to-end path for a particular kind of traffic. Within the policy scope, you create policies for managing traffic on the entire set of wired devices and on individual wireless segments. This allows you to make tradeoffs as necessary to compensate for differences in the behaviors of various network segments. For example, wireless networks typically have lower bandwidth, lower speed, and increased packet loss in comparison to wired networks. Individual wireless segments may exhibit further variation due to local conditions of RF interference, congestion, and other factors, such as the varying capabilities of network devices. The ability to apply per-segment policies to individual wireless segments enables the adjustment of traffic-handling rules to ensure that the highest-priority traffic is least affected by degradation of the wireless network.

After you define a policy scope, you can configure a QoS policy for it, and apply the policy to the devices in the policy scope. Applying a QoS policy deploys and configures the QoS policy on the devices.

You define policy scopes from the **EasyQoS** window or by applying policy tags to devices in the **Device Inventory** or **Topology** windows. For more information, see [Defining a Policy Scope, on page 114](#) or [Adding or Removing a Policy Tag in Device Inventory, on page 63](#).

Static and Dynamic QoS Policies

There are two types of QoS policies, named for the way in which the policies are implemented:

- **Static policies**—Deployed to devices and in effect until you change or remove them. Static policies comprise the majority of the deployments.
- **Dynamic policies**—Used on LAN interfaces only. Dynamic policies are applied to the relevant network devices for the duration of an event, for example, during a voice or video call. When the call ends, the policy is removed from the device. For more information, see [Understanding Dynamic QoS, on page 106](#).

Policy Versioning

Policies are versioned. You can display previous versions of a policy and select a version to reapply to the devices in a scope.

Editing one version of a policy does not affect other versions of that policy or the components of the policy, such as the applications that the policy manages. For example, deleting an application from a policy does not delete the application from EasyQoS, other versions of that policy, or even other policies. Because policies and applications exist independent of each other, you may reapply a policy version that contains applications in it that no longer exist.



Note

Application level modifications like rank, port, and protocol are not or captured in policy versioning.

Processing Order for Devices with Limited Resources

Some network devices have a limited memory (called Ternary Content Addressable Memory or TCAM) for storing network access control lists (ACLs) and access control entries (ACEs). So, as ACLs and ACEs for applications are configured on these devices, the available TCAM space is used. When the TCAM space is depleted, QoS settings for no additional applications can be configured on that device.

To ensure that QoS policies for the most important applications get configured on these devices, EasyQoS allocates TCAM space based on the following order:

- 1 **Rank**—Number assigned to custom and favorite applications, but not to existing, default NBAR applications. The lower the rank number, the higher the priority. For example, an application with rank 1 has a higher priority than an application with rank 2, and so on. Having no rank is the lowest priority.
 - Custom applications are assigned rank 1 by default.
 - Default NBAR applications are not assigned a rank until you mark them as favorites, at which point they are assigned rank 10,000.
- 2 **Traffic Class**—By traffic class in the following order: Signaling, Bulk Data, Network Control, Operations Administration Management (Ops Admin Mgmt), Transactional Data, Scavenger, Multimedia Streaming, Multimedia Conferencing, Real Time Interactive, Broadcast Video, and VoIP Telephony
- 3 **Popularity**—Number (1–10) that is based on Cisco Validated Design (CVD) criteria. The popularity number cannot be changed. An application with a popularity of 10 has a higher priority than an application with a popularity of 9, and so on.
 - Custom applications are assigned popularity 10 by default.

- Default NBAR applications are assigned a popularity number (1–10) that is based on Cisco Validated Design (CVD) criteria. When you mark an application as a favorite, this does not change the popularity number (only rank is changed).

4 Alphabetization—If two or more applications have the same rank and/or popularity number, they are sorted alphabetically by the application’s name, and assigned a priority accordingly.

For example, you define a policy that has the following applications:

- Custom application, custom_realtime, which has been assigned rank 1 and popularity 10 by default.
- Custom application, custom_salesforce, which has been assigned rank 1 and popularity 10 by default.
- Application named corba-iiop, which is in the transactional data traffic class, and you have designated as a favorite, giving that application a ranking of 10,000 and popularity of 9 (based on CVD).
- Application named gss-http, which is in the Ops Admin Mgmt traffic class, and you have designated as a favorite, giving that application a ranking of 10,000 and popularity of 10 (based on CVD).
- All other, default NBAR applications, which have no rank, but will be processed according to their traffic class and default popularity (based on CVD).

According to the prioritization rules, the applications are configured on the device in this order:

Application Configuration Order	Reason
1. Custom application, custom_realtime	Custom applications are given highest priority. Given that the custom_salesforce and custom_realtime applications have the same rank and popularity, they are sorted alphabetically, custom_realtime before custom_salesforce.
2. Custom application, custom_salesforce	
3. Favorite application, gss-http	Because both of these applications have been designated as favorites, they have the same application ranking. So, then EasyQoS evaluates them according to their traffic class. Because gss-http is in the Ops Admin Mgmt traffic class, it is processed first, followed by the corba-iiop application, which is in the Transactional Data traffic class. Their popularity does not come into play because the processing order has been determined by their traffic class.
4. Favorite application, corba-iiop	
5. All other, default NBAR applications	All other applications are next and are prioritized according to traffic class and then popularity, with any applications having the same popularity being alphabetized according to the application’s name.

In the **QoS Policy Manager** window, you can view the results of the policy configuration that was applied on the devices. With a policy selected, EasyQoS displays the list of the devices in the policy scope and the status of the configuration on each device.

Understanding Applications

EasyQoS pre-allocates all of the applications in the Cisco Next Generation Network-Based Application Recognition (NBAR2) library into industry standard-based traffic classes (as defined in RFC 4594). These traffic classes define the network QoS treatments of the applications assigned to them; these treatments include DSCP marking, queuing and dropping treatments.

Some devices require an NBAR2 license. For information, see [EasyQoS Prerequisites](#), on page 98.



Note

You cannot change an application's traffic class; however, you can change the business-relevance of an application when you configure QoS policies.

You can view the applications that are in the EasyQoS registry. From the **Navigation** toolbar, click **EasyQoS**.

The applications are listed, and you can sort them by traffic class, group, or alphabetically by application name. The right pane displays the total number of applications, favorite applications, and custom applications.

If you have additional applications that are not included in EasyQoS, you can add them as custom applications. For information, see [Custom Applications](#), on page 105.

Business-Relevance Groups

The EasyQoS feature provides three levels of business-relevance groupings that provide different levels of service to the applications that have been assigned to them. The business-relevance groups essentially map to three types of traffic: high priority, neutral, and low priority. These groups include:

- **Business Relevant**—(High-priority traffic) The applications in this group directly contribute to organizational objectives and, as such, may include a variety of applications, including voice, video, streaming and collaborative multimedia applications, database applications, enterprise resource applications, email, file-transfers, content distribution, and so on. Applications designated as business-relevant are treated according to industry best-practice recommendations, as prescribed in IETF RFC 4594.
- **Default**—(Neutral traffic) This group is intended for applications that may or may not be business-relevant. For example, generic HTTP/HTTPS traffic may contribute to organizational objectives at times, while at other times such traffic may not. You may not have insight into the purpose of some applications (for instance, legacy applications or even newly deployed applications), so the traffic flows for these applications should be treated with the Default Forwarding service, as described in RFC 2747 and 4594.
- **Business Irrelevant**—*(Low-priority traffic) This group is intended for applications that have been identified to have no contribution towards achieving organizational objectives. They are primarily consumer- and/or entertainment-oriented in nature. We recommend that this type of traffic be treated as a "Scavenger" service, as described in RFC 3662 and 4594.

Marking, Queuing, and Dropping Treatments

Cisco EasyQoS bases its marking, queuing, and dropping treatments on RFC 4594 and the business relevancy category that you have assigned to the application. EasyQoS assigns all of the applications in the Default

category to the Default Forwarding application class and all of the applications in the Irrelevant Business category to the Scavenger application class. For applications in the Relevant Business category, EasyQoS assigns traffic classes to applications based on the type of application. See the table below for a list of application classes and their treatments.

Table 14: Marking, Queuing, and Dropping Treatments

Business Relevance	Application Class	Per-Hop Behavior	Queuing and Dropping	Application Description
Relevant	VoIP 1	Expedited Forwarding (EF)	Priority Queuing (PQ)	VoIP telephony (bearer-only) traffic, for example, Cisco IP Phones.
	Broadcast Video	Class Selector (CS) 5	PQ	Broadcast TV, live events, video surveillance flows, and similar inelastic streaming media flows, for example Cisco IP Video Surveillance and Cisco Enterprise TV. (Inelastic flows refer to flows that are highly drop sensitive and have no retransmission and/or flow-control capabilities.)
	Realtime Interactive	CS4	PQ	Inelastic high-definition interactive video applications and audio and video components of these applications, for example, Cisco TelePresence.
	Multimedia Conferencing	Assured Forwarding (AF) 41	Bandwidth (BW) Queue and Differentiated Services Code Point (DSCP) 24 Weighted Random Early Detect (WRED)	Desktop software multimedia collaboration applications and audio and video components of these applications, for example, Cisco Jabber and Cisco WebEx.
	Multimedia Streaming	AF31	BW Queue and DSCP WRED	Video-on-Demand (VoD) streaming video flows and desktop virtualization applications, such as Cisco Digital Media System.
	Network Control	CS6	BW Queue only 2	Network control plane traffic, which is required for reliable operation of the enterprise network, such as EIGRP, OSPF, BGP, HSRP, IKE, and so on.
	Signaling	CS3	BW Queue and DSCP 24	Control-plane traffic for the IP voice and video telephony infrastructure.
	Operations, Administration, and Management (OAM)	CS2	BW Queue and DSCP 16 3	Network operations, administration, and management traffic, such as SSH, SNMP, syslog, and so on.

Business Relevance	Application Class	Per-Hop Behavior	Queuing and Dropping	Application Description
	Transactional Data (Low-Latency Data)	AF21	BW Queue and DSCP 18 WRED	Interactive (foreground) data applications, such as enterprise resource planning (ERP), crew resource management (CRM), and other database applications.
	Bulk Data (High-Throughput Data)	AF11	BW Queue and DSCP 10 WRED	Noninteractive (background) data applications, such as E-mail, file transfer protocol (FTP), and backup applications.
Default	Default Forwarding (Best Effort)	DF	Default Queue and RED	Default applications and applications assigned to the default business-relevant group. Because only a small minority of applications are assigned to priority, guaranteed-bandwidth, or even to deferential service classes, the vast majority of applications continue to default to this best-effort service.
Irrelevant	Scavenger	CS1	Minimum BW Queue (Deferential) and DSCP 8	Nonbusiness related traffic flows and applications assigned to the business-irrelevant group, such as data or media applications that are entertainment-oriented. Examples include YouTube, Netflix, iTunes, and Xbox Live.

- ¹ VoIP signaling traffic is assigned to the Call Signaling class.
- ² WRED is not be enabled on this class, as network control traffic should not be dropped.
- ³ WRED is not enabled on this class, as OAM traffic should not be dropped.

Custom Applications

Custom applications are applications that you add to the EasyQoS application library. You can define the protocol, port numbers for specific host IP addresses, and the traffic class for the application. You can also add URL-based applications. Alternatively, you can choose an existing application that closely matches the traffic requirements of the application you are adding. In this case, EasyQoS copies the other application's traffic class, category, and subcategory settings to the application that you are defining.

EasyQoS does not configure Access Control Lists (ACEs) for port numbers 80, 443, and 8080, even if they are defined as part of a custom application. If the custom application has a transport IP defined, EasyQoS configures the application on the devices.



Note

Unless custom applications are assigned to a policy, they are not programmed on the devices.

Favorite Applications

Cisco APIC-EM allows you to flag applications that you want EasyQoS to configure on devices before all other applications, except custom applications. Flagging an application as a favorite helps to ensure that the QoS policies for your favorite applications get configured on devices. For more information, see [Processing Order for Devices with Limited Resources](#), on page 100.

Although there is no limit to the number of favorite applications that you can create, selecting only a small number of favorite applications (for example, less than 25) will help to ensure that these applications are treated correctly from a business-relevance perspective in deployments with network devices that have limited TCAM.

Favorite applications can belong to any business relevancy group or traffic class and are configured system-wide, not on a per-scope basis. For example, if you flag the cisco-jabber-video application as a favorite, the application is flagged as a favorite in all policies.

Keep in mind that not only business-relevant applications may be flagged as favorites, but even business-irrelevant applications may be flagged as such. For example, if an administrator notices a lot of unwanted Netflix traffic on his network, he may choose to flag Netflix as a favorite application (despite its being assigned as business-irrelevant). In this case, Netflix would be programmed into the device policies before other business-irrelevant applications, ensuring that the business-intent of controlling this application is realized.

Understanding Dynamic QoS

Dynamic QoS is used on LAN interfaces where you need a specific class of service to be in effect for the duration of some event. You can configure another software application to signal the Cisco APIC-EM (through REST APIs) when a specified event occurs so that a corresponding QoS policy is applied to the relevant network devices for the duration of the event. When you enable the dynamic policy capability, it is enabled on a per scope basis—not globally.

Dynamic policies are used primarily in business applications, such as voice and video applications. For example, you configure Cisco Unified Call Manager (CUCM) to signal the Cisco APIC-EM of a proceeding call. Cisco APIC-EM responds by setting up QoS policies for the video or voice traffic flow on all of the relevant network devices. When the call is over, CUCM signals the APIC-EM to remove the QoS policies. Note that the call does not wait for the QoS policies to be in effect before proceeding. The call *proceeds* while the Cisco APIC-EM applies the QoS policies to the relevant LAN access interfaces on which hosts (such as, IP phones or telepresence end-points) are connected.

For dynamic QoS to take effect when you enable dynamic QoS on policies, you must apply (or reapply) the policy for each scope. Dynamic QoS is not applied to each scope automatically.

EasyQoS Guidelines and Limitations

When configuring policies, be sure to follow these guidelines and limitations:

- When you apply a Cisco APIC-EM policy tag to a device, you cannot provision the same device in IWAN. If you want to provision a device using IWAN, you must first remove the APIC-EM policy tag.

- When you provision a device using IWAN, you cannot apply a Cisco APIC-EM policy tag to the same device. To apply a Cisco APIC-EM policy tag, you must delete the device from the IWAN device inventory and then rediscover it in the Cisco APIC-EM.
- Changing a policy tag *does not* automatically roll back or change the policy on the device. You must reapply the policy in order for the updated configuration to be deployed to the device.
- Policies are not removed from a device when the policy tag is removed from the device.
- Policies are not reapplied automatically when you change the policy tag on a device to a different policy tag that has already been applied to devices.
- Policies are not reapplied automatically when you enable dynamic QoS. You must reapply the policy to the devices for the change to take effect.
- EasyQoS supports Out Of Band (OOB) changes, that is, changes made to the device configurations from any means other than Cisco APIC-EM. However, after you make the OOB change, you must wait at least 30 minutes until the inventory synchronization occurs and then click **Reapply Policy**.
- EasyQoS supports applications that have names consisting of up to 24 alphanumeric characters, including underscores and hyphens. The underscore and hyphen characters are the only special character allowed in the application name.
- Some network devices have a limited memory (called Ternary Content Addressable Memory or TCAM) for storing network access control lists (ACLs) and access control entries (ACEs). For more information about this limitation and how it is handled, see [Processing Order for Devices with Limited Resources](#), on page 100.
- You cannot create custom applications for wireless devices.
- EasyQoS does not configure ACEs for a custom application that does not define an IP address but does define port number 80, 443, or 8080. However, EasyQoS does configure ACEs for a custom application that does define an IP address and port number 80, 443, or 8080.

Enabling the EasyQoS Beta Feature

To use EasyQoS, you need to enable the EasyQoS Beta feature.

**Note**

You must reenab the EasyQoS Beta feature after rebooting the controller, performing a backup/restore, or upgrading the controller software.

Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions to perform this procedure.

Procedure

- Step 1** From the **Global** toolbar, click the **Administrative Functions** (Gear) icon > **Settings**.
- Step 2** From the navigation pane in the **Settings** window, click **EasyQoS Beta**.
- Step 3** Click **EasyQoS Enabled**.
-

Getting Started with EasyQoS

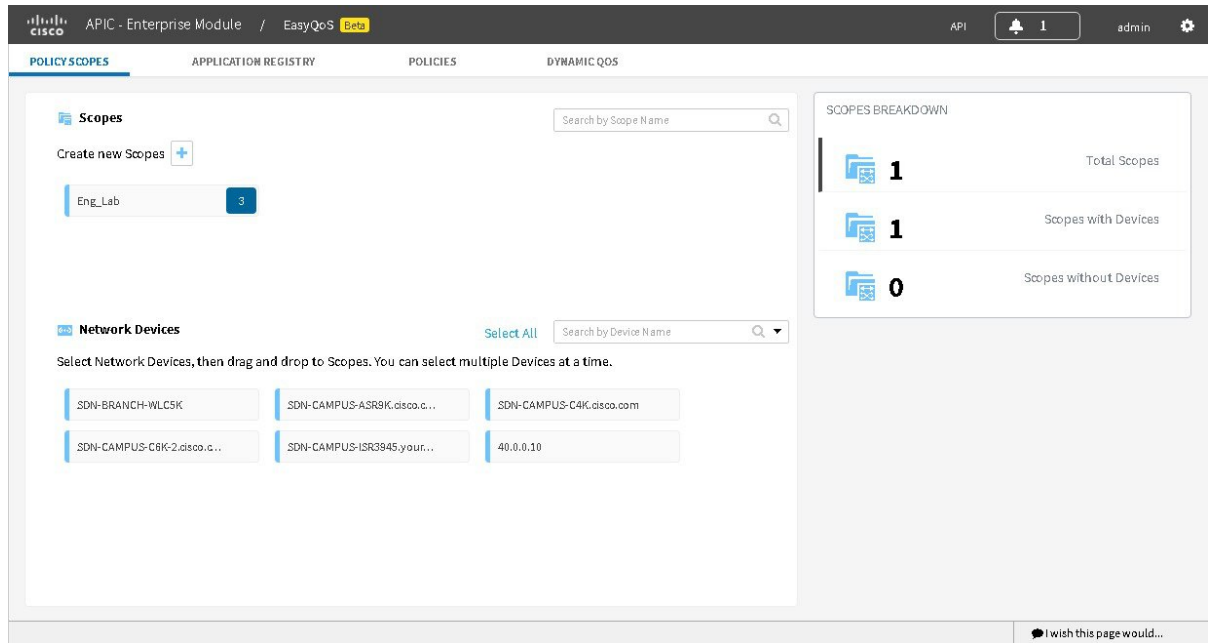
You can use EasyQoS to apply quality of service (QoS) policies throughout your network. Use the following high-level steps to guide you through the process of setting up EasyQoS policies for your devices.

Before You Begin

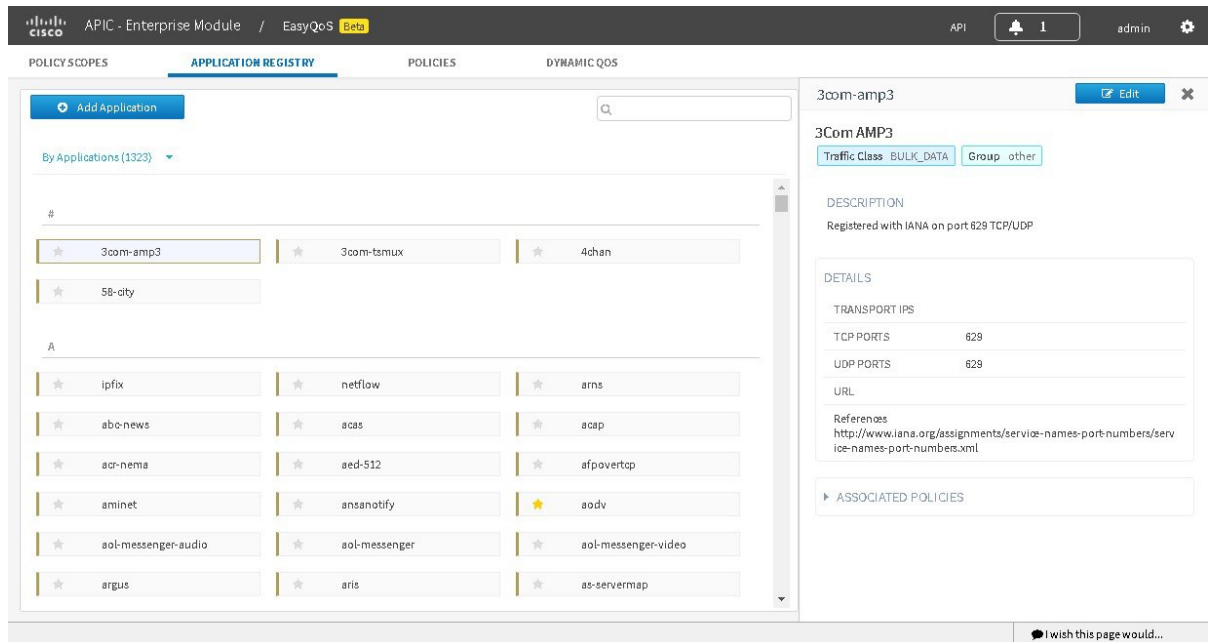
EasyQoS supports most of the Cisco LAN, WAN, WLAN devices. To verify whether the devices and software versions in your network are supported, see the *Supported Platforms for the Cisco Application Policy Infrastructure Controller Enterprise Module* document.

Procedure

- Step 1** Define your business objectives.
For example, your business objective might be to improve user productivity by minimizing network response times or to identify and deprioritize non-business applications.
- Step 2** With your business objectives in mind, determine the business relevance of your applications. Decide which category your applications fall into:
- **Relevant**—The application directly contributes to organizational objectives. Such applications include voice, video, streaming and collaborative multimedia applications, database applications, enterprise resource applications, email, file-transfers, content distribution, and so on. These applications are classified, marked, and treated marked according to industry best-practice recommendations (RFC 4594).
 - **Default**—The application may or may not be business-relevant. For example, generic HTTP/HTTPS traffic may contribute to organizational objectives at times, while at other times such traffic may not. Applications of this type are treated with a Default Forwarding service (RFC 2474).
 - **Irrelevant**—The application has no contribution towards achieving organizational objectives. It is primarily consumer- and/or entertainment-oriented in nature. Applications of this type are treated with a less-than Best Effort service (RFC 3662).
- Step 3** Define the scope of devices for a policy.
The scope defines the group of devices that will be configured with the policy.
- Note** From the **Topology** or **Device Inventory** window, verify that the device roles assigned to devices during discovery are appropriate for your network design. If necessary, change any of the device roles that are not appropriate.
- For more information, see [Defining a Policy Scope](#), on page 114.

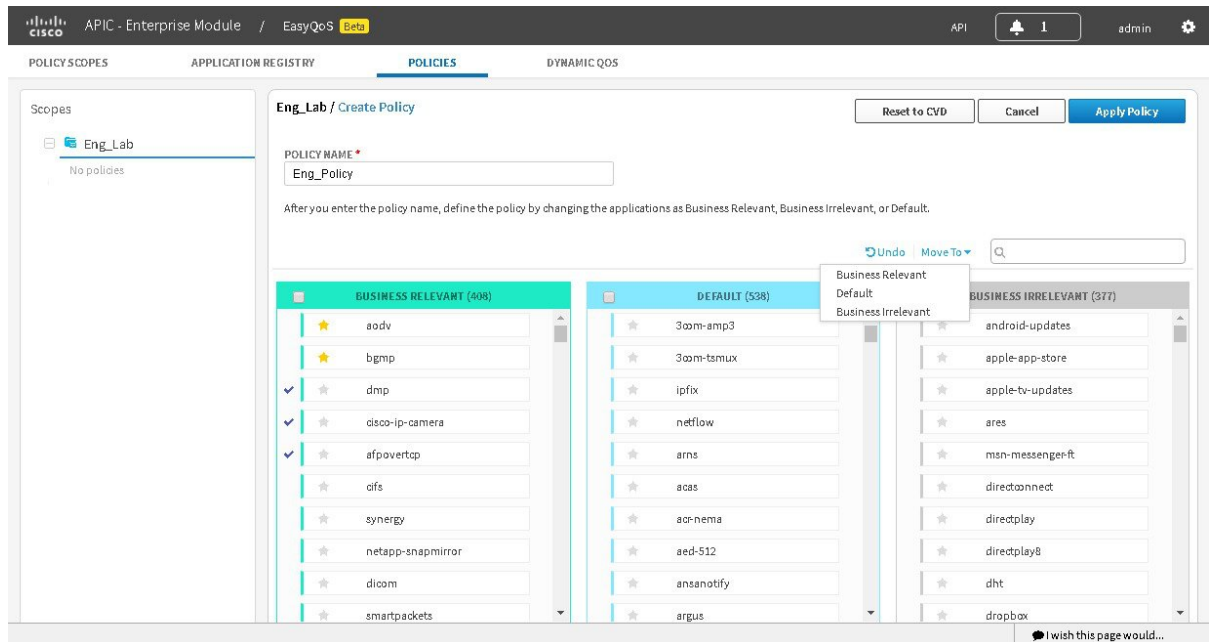


Step 4 Create custom applications.
 If you have applications that are not already defined in EasyQoS, you can add them and define their QoS attributes. For more information, see [Custom Applications](#), on page 105.

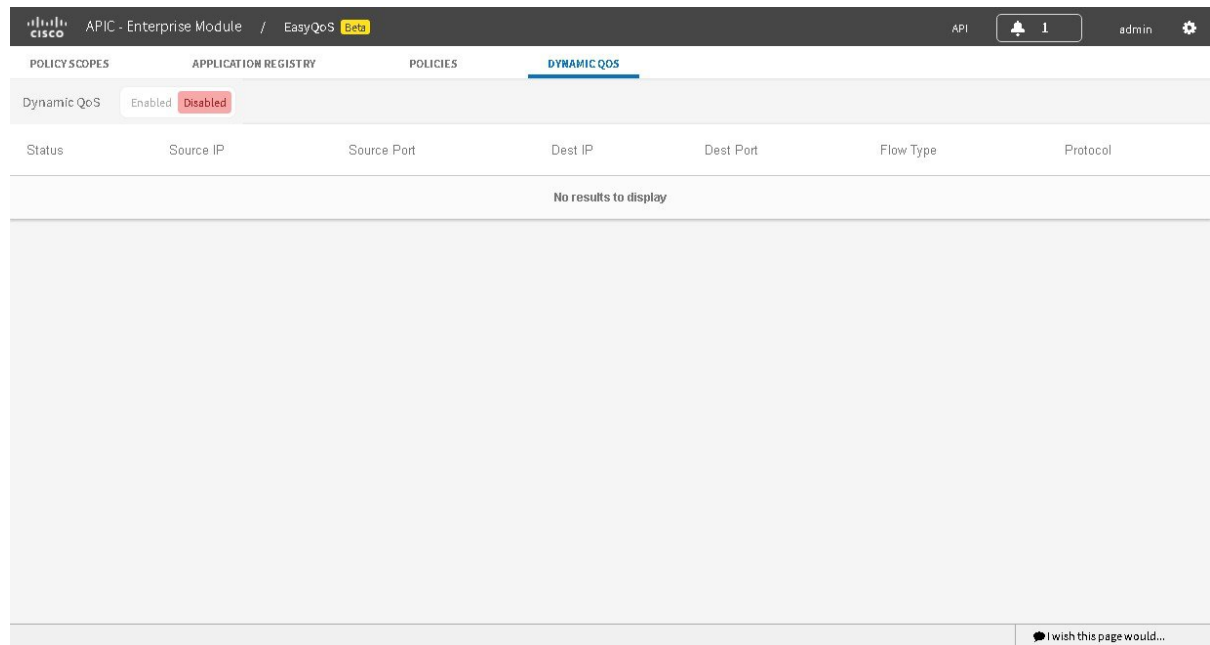


Step 5 Create the policy on wired devices or wireless segments. For information, see [Creating a Policy](#), on page 115. As part of creating the policy, do the following:

- Configure the business relevance of the applications used in your network. EasyQoS comes with the applications preconfigured into business-relevancy groups. You can keep this configuration or modify it to meet the needs of your business objectives and network configuration. For more information, see [Business-Relevance Groups](#), on page 102.
- Select favorite applications. Cisco APIC-EM allows you to flag applications that you want EasyQoS to configure on devices before all other applications (except custom applications). This feature increases the chances that favorite applications are configured on network devices that have a limited memory for storing network access control lists (ACLs) and access control entries (ACEs). For more information, see [Favorite Applications](#), on page 106 and [Processing Order for Devices with Limited Resources](#), on page 100.



- Step 6** If you are defining a policy for LAN interfaces that are being used for voice or video applications, you can configure the policy as a dynamic policy. With dynamic policies, APIC-EM deploys dynamic ACLs for voice and/or video to the specific switch ports hosting the endpoints and then removes the dynamic ACLs when they are no longer needed.



Step 7 Apply the policy to the scope of devices.

What to Do Next

You can see how the deployed policy is working in your network by performing a path trace on two devices and capturing QoS data. For more information, see [Performing Path Traces, on page 127](#).

Configuring QoS Policies

You configure QoS policies using the **EasyQoS** window. To access this window, from the **Navigation** pane, click **EasyQoS**.

The **EasyQoS** window has four tabs from which you can create and manage QoS policies:

- **Policy Scopes**—Allows you to define a group of devices to which policies are applied.
- **Application Registry**—Lists all of the applications that EasyQoS supports, including any custom applications that you have added.
- **Policies**—Allows you to configure policies for the selected scope of devices.

- **Dynamic QoS**—Allows you to enable and disable dynamic QoS on policies.

Figure 18: 411235.jpg

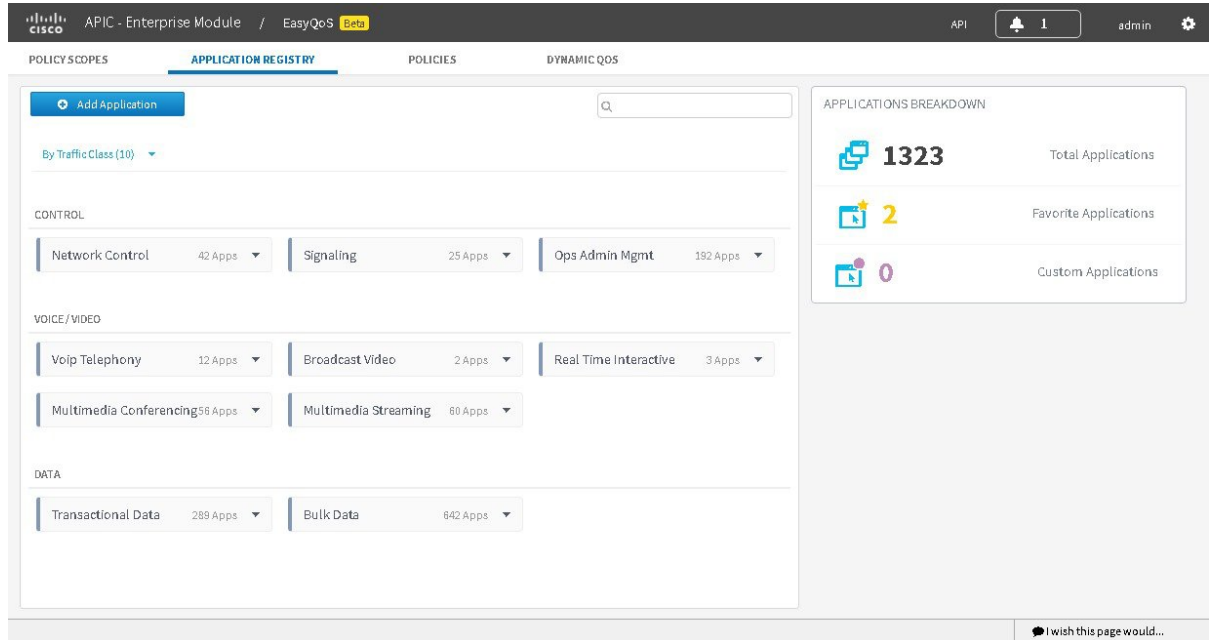


Table 15: Application Registry Tab

Name	Description
Add Application	Allows you to add applications that are not in the list. (For more information, see the next row.)
Search	Finds a specific application by name.
View By icon	Allows you to choose how you want the applications to be displayed: <ul style="list-style-type: none"> • Applications—Lists the applications alphabetically by name. • Application Groups—Lists that applicaitons according to the group to which they belong. For example, the Pop3-Group contains two applications: PostOfficeProtocol3 (pop3) and Secure POP3 (Post Office Protocol), standard for email retrieval over SSL (secure pop3). • Traffic Class—Lists the applications according to the traffic class to which they belong: Custom Applications, Broadcast Video, Bulk Data, Multimedia Conferencing, Multimedia Streaming, Network Control, Ops Admin Mgmt, Real Time Interactive, Signaling, Transactional Data, and Voip Telephony.

Table 16: Policies Tab

Name	Description
Scopes pane	<p>Lists the QoS policy tags that have been created in the Device Inventory window.</p> <p>Click a policy tag from the Scopes pane to display the devices defined for the tag. Wired and wireless devices are listed separately. From this window, you can create a new policy or view an existing policy.</p>
Wired Devices pane	<p>Lists the wired devices defined for the selected policy tag.</p> <p>To display device details, place the cursor over the device name.</p> <p>Create Policy—Allows you to create a policy for wired devices. Click Create Policy, enter a name in the Policy Name field, and click Create. The Policy Details pane appears. For more information, see the Policy Details pane entry in the QoS Policy Manager Window— Policy Details table.</p>
Wireless Segments	<p>Lists the wireless devices defined for the selected policy tag.</p> <p>Click the wireless segment name to display the device to which the segment belongs.</p> <p>Create Policy—</p> <p>View Policy—Allows you to display details about a policy that has already been created. For more information, see the Policy Details pane entry in the QoS Policy Manager Window— Policy Details table.</p>
Create Policy	<p>Allows you to create a policy. After you name the policy and define the business relevance of your applications, click Create.</p>

Table 17: Dynamic QoS Tab

Name	Description
Dynamic QoS pane	<p>Allows you to enable or disable dynamic QoS. Click Enabled to enable QoS</p>

Name	Description
Status pane	<p>State of the dynamic policy for the flow. Valid states are as follows:</p> <ul style="list-style-type: none"> • ACCEPTED_ADD—Controller has accepted the dynamic flow for adding the policy to the network. • CONFIGURING_ADD—Dynamic policy for the flow is being configured in the network. • CONFIG_ADD_SUCCESS—Dynamic policy for the flow was successfully configured in the network. • CONFIG_ADD_FAILURE—Errors have occurred while configuring the dynamic policy for the flow. The failureReason field contains the reason for the error. Possible errors include invalid source IP address, EasyQoS not applied to the access device, device unreachable, and so on. • ACCEPTED_DELETE—Controller has accepted the dynamic flow for deleting the policy from the network. • CONFIGURING_DELETE—Dynamic policy for the flow is in the process of being deleted from the network. The deletion is successful when the flow is no longer displayed on the controller. • CONFIG_DELETE_FAILURE—Errors have occurred while deleting the dynamic policy for the flow. The failureReason field contains the reason for the error.
Source IP	Source IP address of the flow.
Source Port	Source transport port number of the flow.
Dest IP	Destination IP address of the flow.
Dest Port	Destination port number of the flow.
Flow Type	Type of flow, either VOICE or VIDEO.
Protocol	Transport protocol of the flow, either TCP or UDP.

Defining a Policy Scope

Before you can create a QoS policy, you need to identify the policy scope. That is, you need to define the group of devices that will be configured with the same QoS policy. For more information, see [Policy Scope, on page 99](#).

**Note**

You can also define a policy scope by applying policy tags to devices from the **Device Inventory** window or the **Topology** window. For information, see [Adding or Removing a Policy Tag in Device Inventory, on page 63](#) and [Adding or Removing a Policy Tag in Topology, on page 94](#).

Before You Begin

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

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

Procedure

- Step 1** From the **Navigation** pane, click **EasyQoS**.
- Step 2** Click the **Create new Scopes by clicking** plus (+) icon.
- Step 3** In the **Create Policy Scope** field, enter a name for the policy and click the green check mark icon.
- Step 4** From the **Wired Devices** or **Wireless Segments** lists below, drag and drop the selected device to the field where you named the policy.
EasyQoS adds the device and saves the policy automatically.

The panes on the right show statistics, including how many scopes have and do not have devices, number of wired devices that are assigned and unassigned to scopes, and the number of wireless segments that are assigned and unassigned to scopes.

What to Do Next

You can create policies for wired devices or wireless segments. For information, see [Creating a Policy, on page 115](#).

Creating a Policy

You can create a QoS policy for a group of devices that have the same policy scope. When you apply the policy, it is configured on the devices.

**Note**

Each policy scope can have a maximum of one wired-devices policy. However, it can have multiple wireless-segment policies, one policy for each wireless segment.

Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions to perform this procedure.

Make sure that you have discovered your complete network topology.

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

You must have created at least one policy tag. Policy tags define the scope of devices that will be configured with QoS policies.

Procedure

- Step 1** From the **Navigation** pane, click **EasyQoS**.
- Step 2** Click the **Policies** tab.
- Step 3** From the **Scopes** pane, select a policy scope.
- Step 4** Do one of the following:
- To create a policy for wired devices, click the **Create Policy** button.
 - To create a policy for a wireless-device segment, click the plus sign (+) icon next to the chosen wireless segment.
- Step 5** Enter a name for the policy in the **Policy Name** field.
- Step 6** If you want to change the business relevance of an application, proceed to the next step. Otherwise, click **Create Policy** to configure the current application settings to the devices.
- Step 7** To change an application's business relevance, drag and drop the application from the current business relevancy group to the chosen business relevancy group.
- Note** To change an application's business relevance, you can also select the application and use the **Move To** drop down list to select the chosen business relevancy group.
- If you make a mistake, you can click the **Undo** button.
- Step 8** (Optional) If you want, you can designate applications as favorites by clicking the star icon next to the application name.
- For information about how favorite applications work, see [Favorite Applications](#), on page 106.
- Step 9** Click **Create Policy**.
- The policy is configured on the devices in the scope.
-

Editing a Policy

You can edit a QoS policy and then reapply it to the devices in its scope.



Note Each policy scope can have a maximum of one wired-devices policy. However, it can have multiple wireless-segment policies, one policy for each wireless segment.

Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions to perform this procedure.

Make sure that you have discovered your complete network topology.

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

You must have created at least one policy tag. Policy tags define the scope of devices that will be configured with QoS policies.

Procedure

- Step 1** From the **Navigation** pane, click **EasyQoS**.
 - Step 2** Click the **Policies** tab.
 - Step 3** From the **Scopes** pane, select a policy scope.
 - Step 4** Under the policy scope name, select a policy.
 - Step 5** To change an application's business relevance, drag and drop the application from the current business relevancy group to the chosen business relevancy group.
 - Note** To change an application's business relevance, you can also select the application and use the **Move** To drop down list to select the chosen business relevancy group.If you make a mistake, you can click the **Undo** button.
 - Step 6** (Optional) To set an application as a favorite, click the star icon next to the application name. To remove the favorite setting, click the start icon again.
For information about how favorite applications work, see [Favorite Applications](#), on page 106.
 - Step 7** Click **Reapply**.
The policy is updated on the devices in the scope.
-

Rolling Back a Policy to a Previous Version

If you change a policy configuration, and then realize that it is incorrect, or it is not having the desired affect in your network, you can revert to a policy that is up to five versions back.

Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions to perform this procedure.

You must have created at least one policy tag. Policy tags define the scope of devices that will be configured with QoS policies.

You must have created at least two versions of the policy to roll back to a previous policy version.

Procedure

- Step 1** From the **Navigation** pane, click **EasyQoS**.
- Step 2** Click the **Policies** tab.
- Step 3** From the **Scopes** pane, select a policy scope and then the policy that you want to rollback.
- Step 4** Click **Show History**.
Previous versions of the selected policy are listed in descending order with the newest version (highest number) at the top of the list and the oldest version (lowest number) at the bottom.
- Step 5** (Optional) To view the differences between the selected version and the latest version of a policy, click **Difference** in the **View** column.
- Step 6** When you determine the policy version that you want to rollback to, click **Rollback** for that policy version.
- Step 7** Click **Ok** to confirm the rollback procedure.
The rolled back version becomes the newest version.
- Step 8** Click **Reapply**.
The newest policy version is configured on the devices in the scope.
-

Cloning a Policy

If a policy exists that has most of the settings that you want in a new policy, you can clone the existing policy, change it, and apply it to specific scope of devices.

Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions to perform this procedure.

From the **Device Inventory** window, verify that the device roles (assigned during discovery) are appropriate for your network design. If necessary, change any of the device roles that are not appropriate. For information, see [Changing the Device Role](#), on page 60.

You must have created at least one policy tag. Policy tags define the scope of devices that will be configured with QoS policies.

You must have created at least one policy.

Procedure

- Step 1** From the **Navigation** pane, click **EasyQoS**.
 - Step 2** Click the **Policies** tab.
 - Step 3** From the **Scopes** pane, select a policy scope and then the policy that you want to clone.
 - Step 4** Click **Clone**.
 - Step 5** Enter a name for the policy in the **Policy Name** field.
 - Step 6** Enter the name of the policy scope in the **Scope Name** field.
 - Step 7** If you want to change the business relevancy groups to which applications belong, proceed to the next step. Otherwise, click **Create Policy** to configure the same policy settings as the policy that you are cloning.
 - Step 8** To change an application's business relevancy group, drag and drop the application to the chosen business relevancy group.
 - Step 9** (Optional) If desired, designate applications as favorites by clicking the star icon next to the application name. For information about how favorite applications work, see [Favorite Applications](#), on page 106.
 - Step 10** Click **Create Policy**.
The policy is configured on the devices in the scope.
-

Deleting a Policy

You can delete a QoS policy if it is no longer needed.

Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions to perform this procedure.

Procedure

- Step 1** From the **Navigation** pane, click **EasyQoS**.
 - Step 2** Click the **Policies** tab.
 - Step 3** From the **Scopes** pane, select a policy scope.
 - Step 4** Under the policy scope name, select a policy.
 - Step 5** Click **Delete**.
 - Step 6** To confirm the deletion, click **Ok**. Otherwise, click **Cancel**.
 - Step 7** When the deletion confirmation message appears, click **Ok** again.
-

Configuring Favorite Applications

You can designate applications as favorites, which effects the order that the applications are configured on devices. This setting is applied to applications globally, across policies. If you set an application as a favorite, it is set as a favorite in all policies.

You can also configure favorite applications while creating or editing a policy. For more information, see [Creating a Policy, on page 115](#) or [Editing a Policy, on page 116](#)

For information about how favorite applications work, see [Favorite Applications, on page 106](#).

The screenshot displays the Cisco EasyQoS Application Registry interface. The main area shows a list of applications under the 'APPLICATION REGISTRY' tab, sorted by Applications (1323). Applications are listed in an alphabetical grid, with '3com-amp3' selected. A right-hand pane shows details for '3com-amp3', including its traffic class (BULK_DATA), group (other), and transport ports (629).

Before You Begin

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

You must have policy administrator (ROLE_POLICY_ADMIN) permissions to perform this procedure.

You must have created at least one policy tag. Policy tags define the scope of devices that will be configured with QoS policies.

Procedure

- Step 1** From the **Navigation** pane, click **EasyQoS**.
- Step 2** From the **EasyQoS** window, select the **Application Registry** tab.
By default, the applications are listed by traffic class. To change how applications are listed, click the **View By** down arrow at the top of the list and choose **Applications** to view the applications in an alphabetical list or **Application Groups** to view the applications according to their business-relevance group.
- Step 3** Click the star icon next to the applications that you want to set as favorites.
For information about how favorite applications work, see [Favorite Applications, on page 106](#).

Step 4 For these changes to take effect on the devices, you need to apply (or reapply) the relevant policies.

Enabling and Disabling Dynamic QoS Policies

You can enable a policy to be dynamically applied to devices. For more information, see [Static and Dynamic QoS Policies](#), on page 99.

The screenshot shows the Cisco EasyQoS interface. At the top, there's a navigation bar with 'APIC - Enterprise Module / EasyQoS Beta' and user information 'API 1 admin'. Below this are tabs for 'POLICY SCOPES', 'APPLICATION REGISTRY', 'POLICIES', and 'DYNAMIC QoS'. The 'DYNAMIC QoS' tab is selected. Underneath, there's a 'Dynamic QoS' field with two buttons: 'Enabled' and 'Disabled'. The 'Disabled' button is highlighted. Below this is a table with the following columns: 'Status', 'Source IP', 'Source Port', 'Dest IP', 'Dest Port', 'Flow Type', and 'Protocol'. The table is currently empty, with the text 'No results to display' centered below the header. At the bottom right of the interface, there is a small icon and the text 'I wish this page would...'.

Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions to perform this procedure.

You must have created a QoS policy with the appropriate configuration. For information, see [Creating a Policy](#), on page 115.

Procedure

- Step 1** From the **Navigation** pane, click **EasyQoS**.
- Step 2** From the **EasyQoS** window, click the **Dynamic QoS** tab.
- Step 3** In the **Dynamic QoS** field, click **Enabled** to turn on dynamic policy creation or **Disabled** to turn off dynamic policy creation.
- Step 4** To apply these configuration changes to the devices, you must reapply the policy to each scope.

Creating a Custom Application

To help you quickly configure QoS policies, EasyQoS supports the NBAR2 library, which classifies traffic as belonging to any of approximately 1400 known applications. . However, if you have applications that are not in the the library, you can add them as custom applications.

Add Application

Cancel

Create Application

Name	<input type="text" value="Application Name"/>	
Type	<input type="radio"/> URL	<input checked="" type="radio"/> Server IP/Port
Protocol	<input checked="" type="radio"/> TCP	<input type="radio"/> UDP
Value	<input type="text" value="0.0.0.0"/>	: <input type="text" value="8080"/>
<input checked="" type="radio"/> Traffic Class	<input type="text" value="BROADCAST_VIDEO"/>	
<input type="radio"/> Similar To	<input type="text" value="Application"/>	

Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions to perform this procedure.

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

You must have created at least one policy tag. Policy tags define the scope of devices that will be configured with QoS policies.

Procedure

- Step 1** From the **Navigation** pane, click **EasyQoS**.
- Step 2** From the **EasyQoS** window, select the **Application Registry** tab.
- Step 3** Click **Add Application**.
- Step 4** In the **Add Application** pane, enter information in the following fields:
- **Name**—Name of the application. The name can contain up to 24 alphanumeric characters, including underscores and hyphens. The underscore and hyphen characters are the only special character allowed in the application name.
 - **Type**—Type of application. Choose either **URL** for applications that are accessible through URL or **Server IP/Port** for applications that are accessible through a server IP address and port number.
 - **Protocol**—Supported protocol for application. Choose either **TCP** or **UDP**. UDP is available only for applications that are accessible through a server IP address and port number.
 - **Value**—The value entered depends on the type of application that is being added. For URL type applications, enter the application URL. For Server IP/Port applications, enter the server IP address and port number through which you access the application.
 - **Traffic Class**—Traffic class to which the application belongs. Valid values are BULK_DATA, TRANSACTIONAL_DATA, OPS_ADMIN_MGMT, NETWORK_CONTROL, VOIP_TELEPHONY, MULTIMEDIA_CONFERENCING, MULTIMEDIA_STREAMING, BROADCAST_VIDEO, REAL_TIME_INTERACTIVE, and SIGNALING.
 - **Similar To**—Application with the similar traffic-handling requirements. Click the radio-button to select this option and select an application from the drop-down field. EasyQoS copies the other application's traffic class, category, and subcategory settings to the application that you are defining.
- Step 5** Click **Create Application** to save the new application.
- Step 6** When you create a custom applicaiton, it is not assigned to a business-relevancy group. It is placed in a group called Unassigned. To change this setting, see [Editing a Policy, on page 116](#).
-

What to Do Next

You can create policies using the newly added application. If you already have policies that have been deployed to devices, you need to reapply the policies for the custom policy to be configured on the policy scope.

Editing a Custom Application

If you need to change the settings of a custom application, you can edit it.

Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions to perform this procedure.

Procedure

- Step 1** In the **Navigation** pane, click **EasyQoS**.
- Step 2** From the **EasyQoS** window, select the **Application Registry** tab.
- Step 3** Navigate to and select the custom application that you want to edit.
- Note** You can locate the custom application by its application group, traffic class, or by its name in an alphabetical list. You can also enter its name in the search field.
- Information about the application displays in the right hand pane.
- Note** You can review the policies that use the custom application by clicking **Associated Policies**. **EasyQoS** displays the scope, policy name, and relevance.
- Step 4** Click **Edit**.
- Step 5** Change the desired settings for the custom application:
- **Name**—Name of the application. This value cannot be changed.
 - **Type**—Type of application. Choose either **URL** for applications that are accessible through URL or **Server IP/Port** for applications that are accessible through a server IP address and port number.
 - **Protocol**—Supported protocol for application. Choose either **TCP** or **UDP**. UDP is available only for applications that are accessible through a server IP address and port number.
 - **Value**—The value entered depends on the type of application that is being added. For URL type applications, enter the application URL. For Server IP/Port applications, enter the server IP address and port number through which you access the application.
 - **Traffic Class**—Traffic class to which the application belongs. Valid values are BULK_DATA, TRANSACTIONAL_DATA, OPS_ADMIN_MGMT, NETWORK_CONTROL, VOIP_TELEPHONY, MULTIMEDIA_CONFERENCING, MULTIMEDIA_STREAMING, BROADCAST_VIDEO, REAL_TIME_INTERACTIVE, and SIGNALING.
 - **Similar To**—Application with the similar traffic-handling requirements. Click the radio-button to select this option and select an application from the drop-down field. EasyQoS copies the other application's traffic class, category, and subcategory settings to the application that you are defining.
- Step 6** Click **Save Application**.
-

What to Do Next

You need to reapply the policies that use the custom application for the changes to be configured on the devices.

Deleting a Custom Application

You can delete a custom application, if you no longer need it.

Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions to perform this procedure.

Make sure that the custom application that you want to delete is not used in any policies.

Procedure

Step 1 In the **Navigation** pane, click **EasyQoS**.

Step 2 From the **EasyQoS** window, select the **Application Registry** tab.

Step 3 Navigate to and select the custom application that you want to delete.

Note You can locate the custom application by its application group, traffic class, or by its name in an alphabetical list. You can also enter its name in the search field.

Information about the application displays in the right hand pane.

Note Verify that no policies use the custom application by clicking **Associated Policies**. The status should indicate that there are no policies associated with the application.

Step 4 Click **Delete**.

Step 5 To confirm the deletion, click **Ok**. Otherwise, click **Cancel**.

Step 6 When the deletion confirmation message appears, click **Ok** again.

What to Do Next

For the changes to be configured on the devices, you need to reapply the policies that used the custom application that you deleted.



Performing Path Traces

- [About Path Trace, page 127](#)
- [Performing a Path Trace, page 133](#)
- [Performing an ACL-Based Path Trace, page 135](#)
- [Collecting Statistics During a Path Trace, page 137](#)
- [Understanding Path Trace Results, page 140](#)
- [Understanding the Statistics Retrieved During a Path Trace, page 144](#)
- [Understanding VRF Path Trace Results, page 150](#)
- [Understanding ACL Path Trace Results, page 150](#)

About Path Trace

With Path Trace, the controller reviews and collects network topology and routing data from discovered devices. Then it uses this data to calculate a path between two hosts or Layer 3 interfaces.

Optionally, you can choose to collect interface, QoS, device, and Performance Monitor statistics for a path. You can use the information gathered through Path Trace 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.



Note

Path traces from the a router's loopback interface or a wireless controler's management interface are not supported.



Note

For devices connected to a voice or video endpoint (for example, Cisco IP phones), you need to enable IP Device Tracking (IPDT) for these devices to discover voice/data VLAN information about the endpoints. For information, see [IP Device Tracking Configuration, on page 163](#).

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
- VRF
- ACLs

For 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.

Path Trace also supports unknown destinations, where the device is not managed by the Cisco APIC-EM but is reachable.

After the Cisco APIC-EM performs an initial scan, additional on-going network scans are performed at regular intervals every few minutes. Information captured during the on-going scans are displayed in the **Devices** table. Click **Device Inventory** in the navigation pane to view the **Devices** table. Each time the Cisco APIC-EM performs a scan, it also reads and records access control list, quality of service, and SPAN policy configuration information from the network.

Supported Network Environments

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.

Supported Protocols, Network Connections, and Features

The following table describes the device protocols, network connections (physical, wireless, and virtual), and features that Path Trace supports.



Note For detailed information about protocol, wireless connection, and feature support by platform and scenario, see the *Supported Platforms for the Cisco Application Policy Infrastructure Controller Enterprise Module*.

Table 18: Path Trace Supported Device Protocols and Network Connections

Supported Device Protocols and Network Connections	Description
Access Control List (ACL)	<p>Access Control List (ACL) Trace analyzes how a flow is affected by ACLs programmed on the path. After the path is calculated between the source and the destination, the ACL Trace analyzes both ingress and egress interfaces of all devices on the path.</p> <p>Analysis is independent among the ACLs throughout the path. For example, if an ACL has entries that would deny the traffic on an interface along the path, the results of the analysis are reported as if the traffic had reached the destination without being denied by the ACL. However, analysis of entries within an individual ACL is cumulative. That is, if a higher priority ACE is a match, lower-priority ACEs are ignored.</p>

Supported Device Protocols and Network Connections	Description
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>
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>
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>Note 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>

Supported Device Protocols and Network Connections	Description
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>
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>
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"> • Cisco ASR 1000 Series Aggregation Services Router • Cisco ASR 9000 Series Aggregation Services Router • Cisco Integrated Services Routers (ISR) G2 <p>All customer edge (CE) routers should have NetFlow enabled with traffic running between the hosts and routers.</p> <p>Note The above supported devices will be tagged as Border Routers for their Device Role in the Device Inventory. You must keep the above supported devices tagged as Border Routers 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>

Supported Device Protocols and Network Connections	Description
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>
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>
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>
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>

Supported Device Protocols and Network Connections	Description
Virtual connectivity—Layer 2 Port Channel	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.
Virtual connectivity—VLAN/SVI	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. 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.
Virtual Routing and Forwarding (VRF)	Path trace supports VRF Lite and VRF route leaking.
Wireless	The controller provides path trace support for Control and Provisioning of Wireless Access Points (CAPWAP), 802.11, and mobility. 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. Note The controller's GUI will display CAPWAP and mobility tunneling (for roaming) when either is discovered during a path trace. 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.

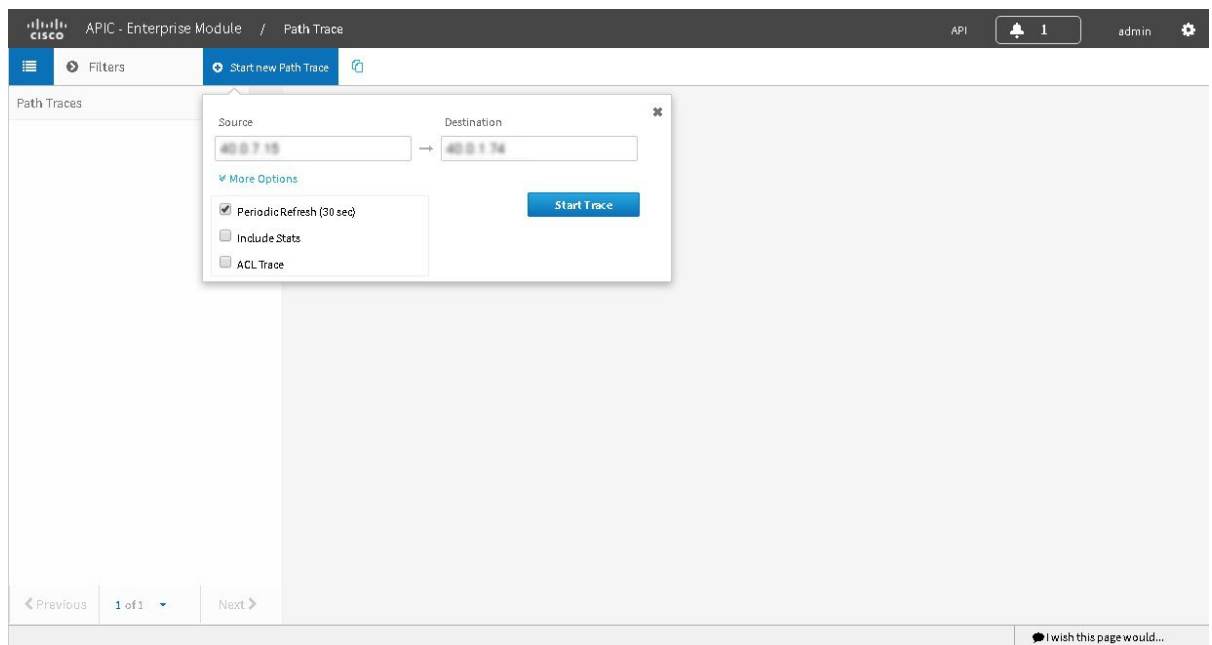
Performing a Path Trace

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 accuracy notes. Accuracy notes are red boxes that appears on a node or path segment indicating the accuracy of the computed path as a percentage. Place your cursor over the note to view suggestions of corrective actions to take to improve the path trace accuracy. For example, you may be prompted to enter port values and run the path trace again.



Before You Begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery function. Ensure that the controller has SSH or Telnet access to the devices.

Procedure

- Step 1** In the Navigation pane, click **Path Trace**.
- Step 2** From the path trace toolbar, click **Start new Path Trace**.
- Step 3** In the **Source** field, enter the IP address of the host or the Layer 3 forwarding interface where you want the trace to start.
If you enter the device IP address manually, you need to select the device from the list and then the interfaces for that device.
- Step 4** In the **Destination** field, enter the IP address of the host or Layer 3 forwarding interface where you want the trace to end. You can also enter an IP address of an unmanaged device (called an unknown destination).
If you enter the device IP address manually, you need to select the device from the list and then the interfaces for that device.
- Step 5** (Optional) To configure source and destination ports or protocols, click **More Options**.
- Step 6** (Optional) In the **Source Port** field, enter the port number of the host where you want the trace to end.
- Step 7** (Optional) In the **Destination Port** field, enter the port number of the host where you want the trace to end.
- Step 8** (Optional) In the **Protocol** field, choose **tcp** or **udp** from the drop-down menu for the Layer 4 path trace protocol.
- Step 9** (Optional) To configure the path trace to refresh every 30 seconds, check the **Periodic Refresh (30 sec)** check box.
- Step 10** (Optional) To configure the path trace to collect additional statistics, check the **Stats** check box and any of the following check boxes, as desired:

- **QoS**—Collects and displays information about quality of service.
- **Interface**—Collects and displays information about the interfaces on the devices along the path.
- **Device**—Collects and displays information, such as a device's CPU and memory usage.
- **Perf Mon**—Collects and displays performance monitoring information about the devices along the path.

Note When you choose the **Perf Mon** option, APIC-EM enables performance monitoring configuration for all of the flows on the devices in the path. To proceed, you need to confirm this configuration.

Step 11 (Optional) Select the **ACL Trace** check box to run an ACL-based path trace.

Step 12 Click **Start Trace**.

Review the path trace output. For more information, see [Understanding Path Trace Results, on page 140](#).

Step 13 Unless you performed a path trace to an unknown destination, you can view the path trace in the **Topology** window. To do so, click **View in Topology**.

The **Topology** window opens in a new window with the path trace highlighted in your network. For more information about the **Topology** window, see [About Topology, on page 73](#).

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.

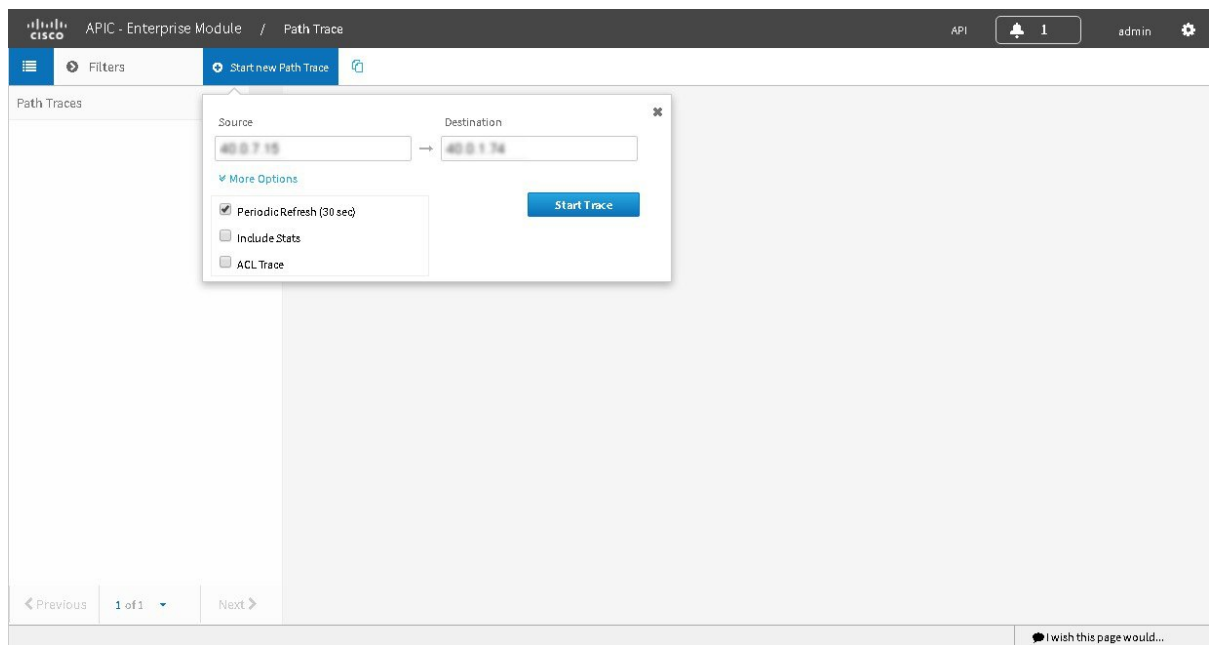
Performing an ACL-Based Path Trace

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 accuracy notes. Accuracy notes are red boxes that appears on a node or path segment indicating the accuracy of the computed path as a percentage. Place your cursor over the note to view suggestions of corrective actions to take to improve the path trace accuracy. For example, you may be prompted to enter port values and run the path trace again.



Before You Begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery function. Ensure that the controller has SSH or Telnet access to the devices.

Procedure

- Step 1** In the Navigation pane, click **Path Trace**.
- Step 2** From the path trace toolbar, click **Start new Path Trace**.
- Step 3** In the **Source** field, enter the IP address of the host or the Layer 3 forwarding interface where you want the trace to start.
If you enter the device IP address manually, you need to select the device from the list and then the interfaces for that device.
- Step 4** In the **Destination** field, enter the IP address of the host or Layer 3 forwarding interface where you want the trace to end. You can also enter an IP address of an unmanaged device (called an unknown destination).
If you enter the device IP address manually, you need to select the device from the list and then the interfaces for that device.
- Step 5** (Optional) To configure source and destination ports or protocols, click **More Options**.
- Step 6** (Optional) In the **Source Port** field, enter the port number of the host where you want the trace to end.
- Step 7** (Optional) In the **Destination Port** field, enter the port number of the host where you want the trace to end.
- Step 8** (Optional) In the **Protocol** field, choose **tcp** or **udp** from the drop-down menu for the Layer 4 path trace protocol.
- Step 9** (Optional) To configure the path trace to refresh every 30 seconds, check the **Periodic Refresh (30 sec)** check box.
- Step 10** (Optional) To configure the path trace to collect additional statistics, check the **Stats** check box and any of the following check boxes, as desired:

- **QoS**—Collects and displays information about quality of service.
- **Interface**—Collects and displays information about the interfaces on the devices along the path.
- **Device**—Collects and displays information, such as a device's CPU and memory usage.
- **Perf Mon**—Collects and displays performance monitoring information about the devices along the path.

Note When you choose the **Perf Mon** option, APIC-EM enables performance monitoring configuration for all of the flows on the devices in the path. To proceed, you need to confirm this configuration.

Step 11 Select the **ACL Trace** check box to run an ACL-based path trace.

Step 12 Click **Start Trace**.

Review the path trace output. For more information, see [Understanding ACL Path Trace Results, on page 150](#).

Step 13 Unless you performed a path trace to an unknown destination, you can view the path trace in the **Topology** window. To do so, click **View in Topology**.

The **Topology** window opens with the path trace highlighted in your network. For more information about the **Topology** window, see [About Topology, on page 73](#).

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.

Collecting Statistics During a Path Trace

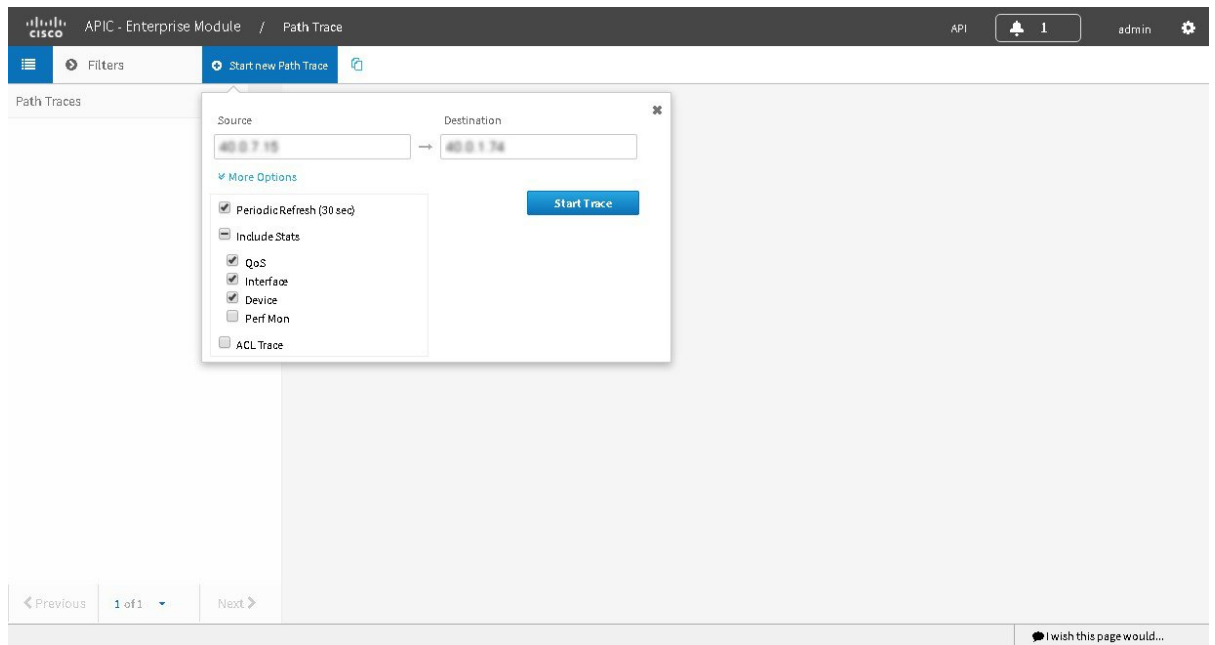
You can perform a path trace between two nodes in your network and collect the following types of statistics about the path:

- Quality of Service (QoS)
- Interface
- Device
- Performance Monitor (If you choose to run a path trace to collect **Perf Mon** statistics, the Cisco APIC-EM configures all of the devices in the requested path with the necessary flow monitor configuration. For information about this configuration, see [Performance Monitor Configuration, on page 167](#).)



Note

The path trace application may display accuracy notes. Accuracy notes are red boxes that appears on a node or path segment indicating the accuracy of the computed path as a percentage. Place your cursor over the note to view suggestions of corrective actions to take to improve the path trace accuracy. For example, you may be prompted to enter port values and run the path trace again.



Before You Begin

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

Procedure

- Step 1** In the **Navigation** pane, click **Path Trace**.
- Step 2** From the path trace toolbar, click **Start new Path Trace**.
- Step 3** In the **Source** field, enter the IP address of the host or the Layer 3 forwarding interface where you want the trace to start.
- Step 4** In the **Destination** field, enter the IP address of the host or Layer 3 forwarding interface where you want the trace to end.
- Step 5** (Optional) To configure source and destination ports or protocols, click **More Options**.
- Step 6** (Optional) In the **Source Port** field, enter the port number of the host where you want the trace to start.
- Step 7** (Optional) In the **Destination Port** field, enter the port number of the host where you want the trace to end.
- Step 8** (Optional) In the **Protocol** field, choose either **tcp** or **udp** from the drop-down menu for the Layer 4 path trace protocol.
- Step 9** (Optional) To configure the path trace to refresh every 30 seconds, check the **Periodic Refresh (30 sec)** check box.
- Step 10** Check the **Stats** check box.
- Step 11** Check any of the following check boxes corresponding to the type of statistics that will be collected:
 - **QoS Stats**
 - **Interface Stats**
 - **Device Stats**

- **Perf Mon Stats**

Note If you choose to run a path trace to collect **Perf Mon** statistics, you need to grant the Cisco APIC-EM permission to configure all of the devices in the requested path with the necessary flow monitor configuration. When the confirmation dialog box appears, click **OK** to allow this configuration or **Cancel** to discontinue this action. For information about this configuration, see [Performance Monitor Configuration](#), on page 167.

Step 12 Click **Start Trace**.

The results are displayed in the **Trace Results Device Details** pane. For information, see the following topics:

- [QoS Statistics](#), on page 147
- [Interface Statistics](#), on page 145
- [Device Statistics](#), on page 144
- [Performance Monitor Statistics](#), on page 149

Step 13 (Optional) 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.

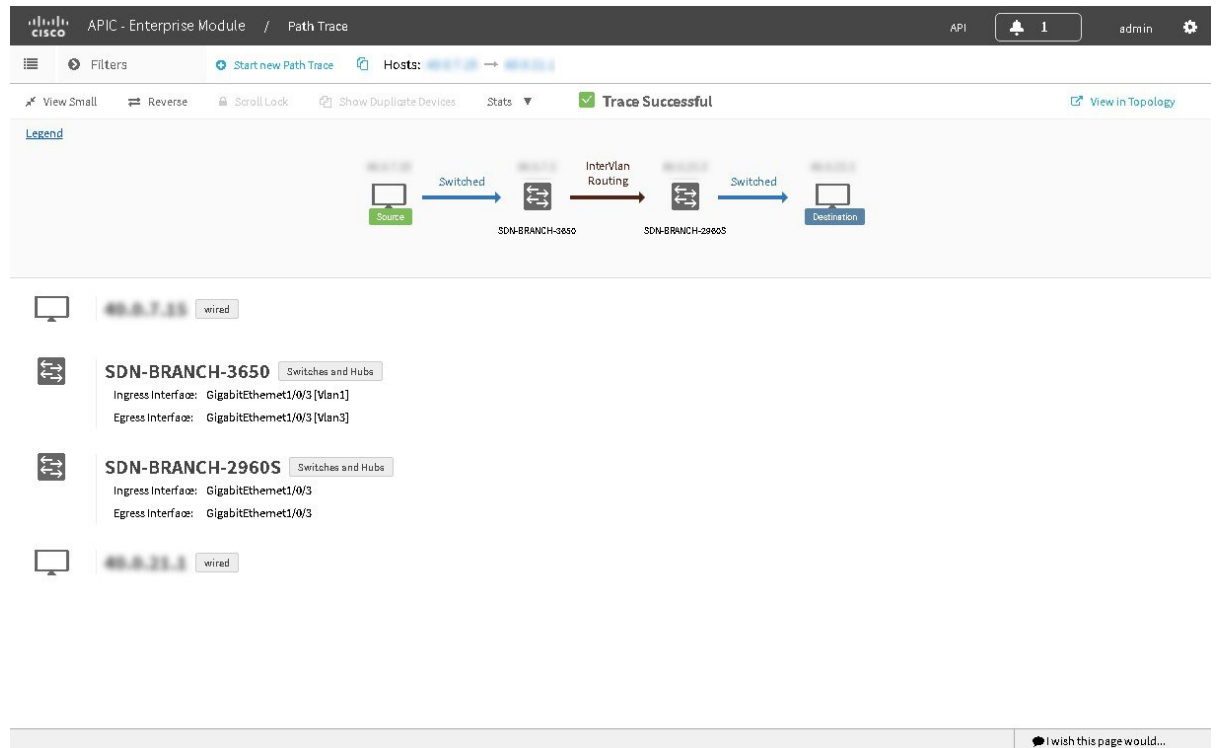
Note If you added location markers for your devices, the location markers appear in the Topology map. Click a location marker to display the **Topology** for that location.

For more information about the **Topology** window, see [About Topology](#), on page 73.

Understanding Path Trace Results

After you run a path trace, the results are displayed in the **Path Trace** window.

Figure 19: Path Trace Window



Path Trace Toolbar

The **Path Trace Toolbar** provides the following options and information:

- **Filters**—Allows you to search for path traces by source or destination IP address, source or destination ports, protocol, creation date, or statistics gathered (QoS, Device, Interface, Perf Mon, and ACL trace)
- **Start new Path Trace**—Displays a dialog box where you can define the parameters for your path trace.
- **Copy icon**—Allows you to create a new path trace using the parameters that are defined in the selected (source) path trace. You can keep any of the values from the source path trace and change, add, or deselect any parameters for the new path trace.

Path Traces Pane

The Path Traces pane lists the path traces in one of three categories:

- **IN PROGRESS**—Path is currently being calculated. No results to show yet.
- **ACTIVE**—A path has been calculated and will be refreshed every 30 seconds. Statistics may also be collected periodically.

- **COMPLETED**—The path has been calculated one time and is not being refreshed. However, statistics may still be collected periodically.

Trace Results Toolbar

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

Table 19: Trace Results Toolbar

Name 4	Description
View Small	Minimizes the trace results to view the details better.
Reverse	<p>Displays the trace results 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.</p> <p>Note If you performed a path trace to an unknown destination, you cannot display the reverse path trace.</p>
Scroll Lock	Locks the scrolling of the path trace and reverse path trace details windows. (Available when Show Reverse is enabled.)
Show Duplicate Devices	Displays or hides duplicate devices within a path trace.
ACL Trace checkbox 5	Displays an icon at each device or interface that indicates whether any ACLs are blocking traffic on the path.
Stats	If statistics were collected for the trace, you can select one or more of the interface, QoS, device, and performance monitor check boxes to display the corresponding information in the graphical display.
View in Topology	Opens the Topology window and highlights the path trace results in your network topology. If you performed a path trace to an unknown destination, this option is not available. For more information about using the Topology window, see About Topology, on page 73 .

⁴ Depending on the trace results, some of these items on the toolbar might be unavailable.

⁵ Available only if you performed an ACL Path Trace.

Trace Results Graphical Display

The controller graphically displays the path direction and the hosts and devices (including their IP addresses) along the path between the source (host A) and destination (host B). Clicking an individual device in the path trace highlights the device in the **Trace Results Device Details** area. The display also shows the protocol of the path source between devices along the path: **Switched**, **STP**, **ECMP**, **Routed**, **Trace Route**, or other source type.

If you performed an ACL trace, the devices show whether the traffic matching your criteria would be permitted or denied based on the ACLs configured on the interfaces. For more information, see [Performing an ACL-Based Path Trace, on page 135](#).

Trace Results Device Details

You can review the detailed information displayed for each device in the path trace.

Table 20: Trace Results Device Details

Name	Description
IP	IP address of the device.
Type	Wired or wireless device (access point, switch, or router).

Name	Description
Link Source	<p>Information about the link between two devices (source and destination). Link information is based on the configuration of the source device.</p> <ul style="list-style-type: none"> • BGP—Link is based on the BGP routes configured on the source device. • ECMP—Link is based on a Cisco Express Forwarding (CEF) load balancing decision. • EIGRP— Link is based on EIGRP routes configured on the source device. • Connected—The source host (host A) is directly connected to the destination host (host B). In the case of a reverse path, the destination host (host B) is directly connected to the source host (host A). • InterVlan Routing—There is an SVI configuration on the source device. A VLAN is configured on the source device from which the path is switched to the destination device. • ISIS—Link is based upon the IS-IS routes configured on the source device. • NetFlow—Link is based on NetFlow records collected on the source device. • OSPF—Link is based on the OSPF routes configured on the source device. • Static—Link is based on a static route configured on the source device. • Switched—Link is based on Layer 2 VLAN forwarding. • Trace Route—Link is based on trace route. • Wired—The source device is wired to the destination device. • Wireless—The source device is a wireless host connected to the destination device (access point).
Tunnels	<p>CAPWAP data (wireless) or mobility tunneling.</p> <p>Note Path trace provides a graphical view of the CAPWAP tunnel around the devices involved. You are able to adjust the view by zooming in or out.</p>
Ingress interface	<p>Ingress interface of the device for the path trace (physical or virtual). For example, a physical ingress interface is GigabitEthernet1/0/1 and a virtual ingress interface is GigabitEthernet1/3 [Vlan1].</p> <p>If statistics were gathered for this path trace, clicking the View Stats button displays the interface or QoS statistics. For information, see Interface Statistics, on page 145 or QoS Statistics, on page 147.</p>

Name	Description
Egress interface	Egress interface of the device for the path trace (physical or virtual). For example, a physical interface is GigabitEthernet1/0/2 and a virtual ingress interface is GigabitEthernet1/4 [Vlan2] . If statistics were gathered for this path trace, clicking the View Stats button displays the interface or QoS statistics. For information, see Interface Statistics, on page 145 or QoS Statistics, on page 147 .
Accuracy note	If there is uncertainty about the path trace on a segment between devices, path trace displays a note that indicates the accuracy of the computed path as a percentage. For example, 10 percent would indicate lower accuracy than 90 percent. Place your cursor over the note to view suggestions of corrective actions to take to improve the path trace accuracy. For example, you may be prompted to enter port values and run the path trace again.
VRF	If Path Trace detects a VRF on a router, it displays the VRF in the graphical display and provides the interface name and VRF name. For more information, see Understanding VRF Path Trace Results, on page 150 .

Trace Results Statistics

If you specified that device statistics be included in the path trace, statistical information about the device is gathered and displayed. You can select or deselect one or more of the options from the **Stats** drop-down list so that you can isolate different information.

For information about the statistics, see the following sections:

- [Device Statistics, on page 144](#)
- [Interface Statistics, on page 145](#)
- [QoS Statistics, on page 147](#)
- [Performance Monitor Statistics, on page 149](#)

Understanding the Statistics Retrieved During a Path Trace

Device Statistics

If you specified that device statistics be included in the path trace, Path Trace gathers and displays statistical information about the device. Not all device types support all of the parameters (5 minutes, 5 seconds, and 1 minute). If a device does not support a particular parameter, Path Trace displays N/A (not supported).

Table 21: Path Trace Device Statistics

Parameter	Description
CPU Usage	
5 Mins Usage(%)	Percentage of the device's CPU usage for the last 5 minutes.
5 Secs Usage(%)	Percentage of the device's CPU usage for the last 5 seconds.
1 Min Usage(%)	Percentage of the device's CPU usage for the last minute.
Refreshed At	Date and time when the information was gathered.
Memory Usage	
Refreshed At	Date and time when the information was gathered.
Memory Usage(bytes)	The amount of memory (in bytes) that the device is using.

Interface Statistics

When you perform a path trace, you can collect interface statistics that show how the interfaces are performing. In this way, you can monitor the effect of the QoS policies on the network and make any changes, if necessary. The following table lists the interface statistics that are retrieved.

The screenshot shows the Cisco APIC Path Trace interface. At the top, it indicates 'APIC - Enterprise Module / Path Trace' and 'Trace Successful'. A legend at the top shows the path: Source (Host) -> SDN-BRANCH-2960S (Switched) -> SDN-BRANCH-3650 (InterVlan Routing) -> SDN-BRANCH-2960S (Switched) -> Destination (Host). Below the legend, the interface statistics for SDN-BRANCH-2960S are displayed, with a yellow highlight around the statistics table.

SDN-BRANCH-2960S			
Ingress Interface: GigabitEthernet1/0/2			
Hide Stats			
Admin Status	up	Input Packets	635545
Input Queue Drops	0	Input Queue Max Depth	75
Input Queue Count	0	Input Queue Flushes	0
Input Rate(bps)	0	Operational Status	up
Output Drop	0	Output Packets	6793814
Output Queue Count	0	Output Queue Depth	40
Output Rate(bps)	0	Refreshed At	5/16/2016, 10:33:17 PM

Below the statistics, the egress interface is listed as GigabitEthernet1/0/3 with a 'View Stats' button.

Table 22: Interface Statistics by Policy

Parameter	Description
Admin Status	Administrative status of the interface: <ul style="list-style-type: none"> • Up—Interface has been enabled through the CLI. • Down—Interface has been disabled through the CLI.
Input Packets	Number of packets being received on the interface.
Input Queue Drops	Number of packets dropped from the input queue due to the queue reaching its maximum threshold.
Input Queue Max Depth	Maximum number of packets that the input queue can hold before it must start dropping packets.
Input Queue Count	Number of packets in the input queue.
Input Queue Flushes	Number of packets dropped due to Selective Packet Discard (SPD). SPD is a mechanism that quickly drops low priority packets when the CPU is overloaded in order to save some processing capacity for high priority packets.

Parameter	Description
Input Rate (bps)	Number of bits per second at which packets are entering the interface.
Operational Status	Operational status of the interface: <ul style="list-style-type: none"> • Up—Interface is transmitting or receiving traffic as desired. To be in this state, an interface must be administratively up, the interface link layer state must be up, and the interface initialization must be completed. • Down—Interface cannot transmit or receive (data) traffic.
Output Drop	Number of packets dropped from the output queue due to the queue reaching its maximum threshold.
Output Packets	Number of packets leaving the interface.
Output Queue Count	Number of packets in the output queue.
Output Queue Depth	Maximum number of packets that the output queue can hold before it must start dropping packets.
Output Rate (bps)	Number of bits per second at which packets are leaving the interface.
Refreshed At	Date and time that the current statistics were gathered.

QoS Statistics

When you perform a path trace, you can collect QoS statistics that show how the QoS policies are performing. The only interface statistics included in the QoS statistics are those for the border router egress interface. Collecting QoS statistics helps you to monitor the effect of the QoS policies on your network devices and make any changes, if necessary. The following table lists the QoS Statistics that are retrieved.

The screenshot displays the Cisco APIC Path Trace tool. At the top, it shows the path trace status as 'Trace Successful'. The path diagram illustrates the flow from a source through several network devices: a Switched device, PS_AC_1, an InterVlan Routing device, a Traceroute device (marked with a red question mark), another Traceroute device, PS_BR_2921, PS_BR_AC_1, and finally a destination Switched device. Below the path diagram, the details for the 'name' device are shown, including ingress and egress interfaces (GigabitEthernet0/0 and GigabitEthernet0/2) and a QoS table for the 'class-default' policy.

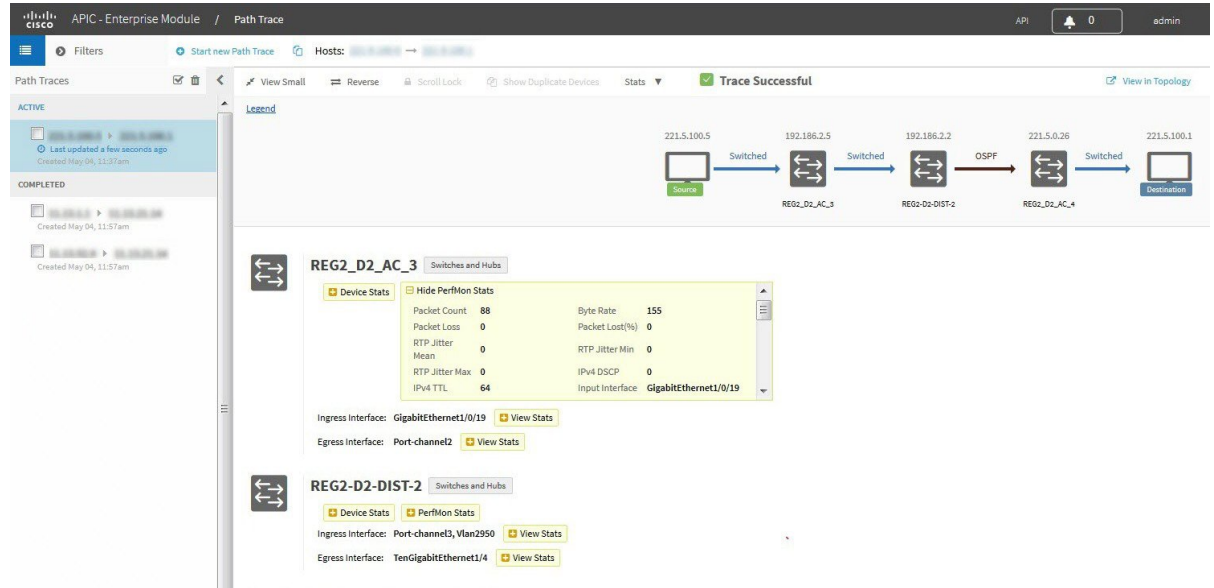
Class Map Name	class-default	Drop Rate	0
Num of Bytes	140901428	Num of Packets	609248
Offered Rate	0	Queue Depth	0
Queue Bandwidth(bps)	N/A	Queue No Buffer Drops	0
Queue Total Drops	0	Refreshed At	5/17/2016, 11:17:42 AM

Table 23: QoS Statistics by Policy

Parameter	Description
Policy Name	Drop-down list of policy names that QoS statistics have been collected about.
Class Map Name	Name of the class map.
Num of Bytes	Average number of bytes forwarded by the queue.
Offered Rate	Traffic rate offered for that particular traffic.
Queue Bandwidth (bps)	Rate (bps) at which the queue can process packets.
Queue Total Drops	Number of packets dropped from the queue due to the queue reaching its maximum threshold.
Drop Rate	Number of bits per second at which packets are being dropped from the queue.
Num of Packets	Number of packets that the queue can hold.
Queue Depth	Maximum number of packets that the queue can hold before it must start dropping packets.
Queue No Buffer Drops	Number of times that packets were dropped due to not enough buffer allocated.
Refreshed At	Date and time that the current statistics were gathered.

Performance Monitor Statistics

When you run a path trace to collect **Perf Mon** statistics, the Cisco APIC-EM automatically configures all of the devices in the requested path with the necessary flow monitor configuration, and then removes the configuration when it is no longer needed (no pending performance monitor path trace for the path or 24 hours, whichever is first). For information about this configuration, see [Performance Monitor Configuration](#), on page 167.



The following table lists the performance monitor statistics that are retrieved.

Table 24: Performance Monitor Statistics

Parameter	Description
Packet Count	Total number of IP packets sent.
Byte Rate	Average number of packets or bits (as configured) that were processed by the monitoring system per second during the monitoring interval.
Packet Loss	Total number of IP packets lost by any intermediate system in the monitored flow.
Packet Loss (%)	Percentage of IP packets lost by any intermediate system in the monitored flow.
RTP Jitter Mean	Mean value of the Real-time Transport Protocol (RTP) jitter.

Parameter	Description
RTP Jitter Min	Minimum value of the Real-time Transport Protocol (RTP) jitter.
RTP Jitter Max	Maximum value of the Real-time Transport Protocol (RTP) jitter.
IPv4 DSCP	Value of the IPv4 differentiated services code point (DSCP) type of service (ToS).
IPv4 TTL	Value of the IPv4 time-to-live (TTL).
Input Interface	Name of the input interface that was used as match criteria.
Output Interface	Name of the output interface that was used as match criteria.
Refreshed At	Date and time that the performance monitor statistics were gathered.
Source IP	IP address of the source interface for all of the packets sent by a flow exporter.
Destination IP	IP address of the destination interface for all of the packets sent by a flow exporter.

Understanding VRF Path Trace Results

Path trace supports VRF Lite and VRF route leaking. If Path Trace detects a VRF on a router, it displays the VRF in the graphical display and provides the interface name and VRF name. VRFs are shown as a colored circle, making it easy to see where they are along the path. VRFs with the same name have the same color.

Understanding ACL Path Trace Results

An ACL path trace shows whether the traffic matching your criteria would be permitted or denied based on the ACLs configured on the path.

The following rules effect the ACL path trace results:

- Only matching ACEs are reported.
- If you leave out the protocol, source port, or destination port when defining a path trace, the results include ACE matches for all possible values for these fields.
- If no matching ACEs exists in the ACL, the flow is reported to be implicitly denied.

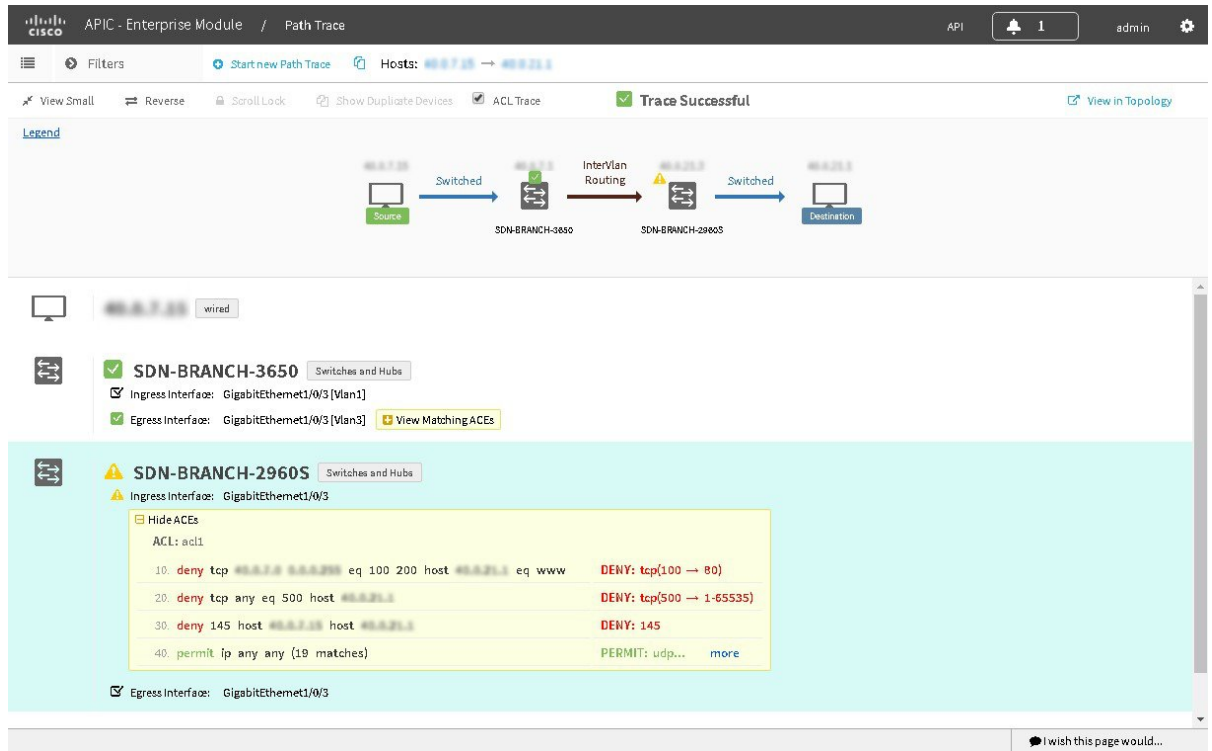


Table 25: ACL Path Trace Icons

Icon	Description
	There are ACLs that permit the traffic applied on the interface.
	Traffic may or may not be blocked. For example, if your traffic matches a deny access control entry (ACE), traffic is denied. However, if your traffic matches any other ACEs, it is permitted. You can get this type of results if you leave out the protocol, source port, or destination port when defining a path trace.
	There is an ACL on the device or interface that is blocking the traffic on the path.
	There are no ACLs applied on the interface.



Reviewing the API Documentation

- [About the Cisco APIC-EM API Documentation, page 153](#)
- [Using the Cisco APIC-EM REST API Window, page 157](#)

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.

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 20: API Window

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**
 - **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**
- **Visibility**



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 [Using the Cisco APIC-EM REST API Window, on page 157](#).

Related Topics

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

[Common External RESTful Services HTTP Response Codes, on page 156](#)

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"> • /noun • /noun/count • /noun/{start}/{end} • /noun/{noun-id}
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>

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 format) according to the nature of the request.

Table 26: 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 27: 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 28: 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 153](#)

Using the Cisco APIC-EM REST API Window

Before You Begin

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

Procedure

- 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 21: Supported Methods for User Management API

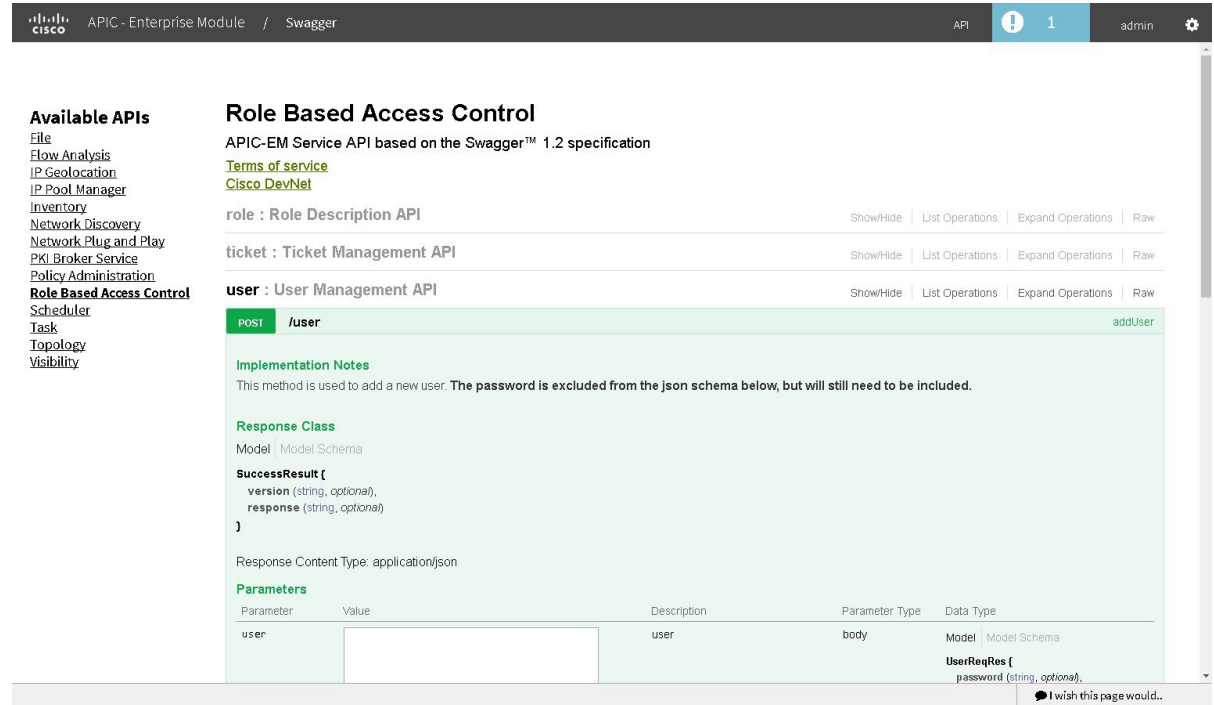
The screenshot shows the Swagger UI for the APIC-EM Enterprise Module. The breadcrumb trail is 'APIC - Enterprise Module / Swagger'. The user is logged in as 'admin'. The main content area is titled 'Role Based Access Control' and describes it as an 'APIC-EM Service API based on the Swagger™ 1.2 specification'. It includes links for 'Terms of service' and 'Cisco DevNet'. A list of APIs is shown, with 'user : User Management API' selected. Below this, a table lists the supported methods for the user API:

Method	Endpoint	Action
POST	/user	addUser
GET	/user	getUsers
PUT	/user	updateUser
GET	/user/cache	getUsersCache
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

At the bottom right of the interface, there is a feedback link: 'I wish this page would...'.

Step 4 Click **Expand Operations**.

Figure 22: Expanded View of getUsers API



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

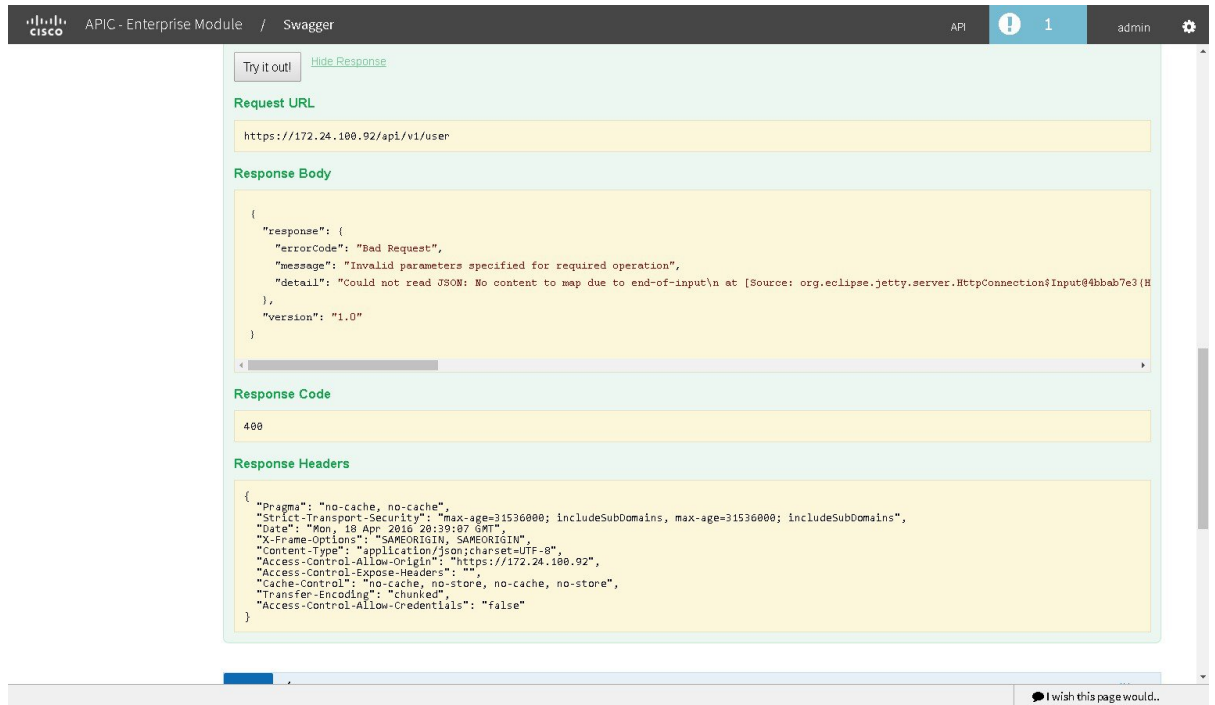
Note Enter content into any of the required content fields prior to testing the API.

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 23: Output the getUsers API



- Step 6** Click **Hide the Response** to close the expanded API method window. Test out additional methods for this API or try a new API and its methods.

What to Do Next

Test out additional methods for this API or try a new API and its methods.



Required Device Configuration

- [Required Platform Configurations, page 161](#)

Required Platform Configurations

You must make the following configuration changes on these platforms for the corresponding Cisco APIC-EM features to properly work.

Table 29: Required Platform Configurations

Feature	Platform	Required Configuration
Discovery (device inventory collection)	Cisco ASR 9000 router or any other Cisco device that requires NETCONF support for their device pack.	Configure NETCONF on these platforms. For information, see NETCONF Configuration, on page 162 .
Discovery (host inventory collection)	Devices connected to hosts using SNMP.	Configure SNMP traps on these devices. For information, see SNMP Trap Configuration, on page 163 .
	Devices connected to hosts using IPDT.	Enable IPDT for these devices. For information, see IP Device Tracking Configuration, on page 163 .
	<ul style="list-style-type: none"> • Cisco Series 2504 WLC • Cisco Series 5508/5520 WLC • Cisco Series 8510/8540 WLC 	Configure SNMP traps and object identifiers on these wireless LAN controllers. For information, see Wireless LAN Controller Configuration, on page 164 .

Feature	Platform	Required Configuration
Path Trace	<ul style="list-style-type: none"> • Cisco ASR 1000 • Cisco ASR 9000 • Cisco ISR-G2 • Cisco ISR-4451 -X 	Configure NetFlow on these routers. For information, see Cisco NetFlow Configuration , on page 163.
	Devices connected to a voice or video endpoint (for example, Cisco IP phones).	Enable IPDT for these devices to discover voice/data VLAN information about the endpoints. For information, see IP Device Tracking Configuration , on page 163.

NETCONF Configuration

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



Note

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

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

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



Note

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

Cisco NetFlow Configuration

Cisco NetFlow needs to be enabled on the following devices to support the Cisco APIC-EM path trace functionality:

- Cisco ASR 1000
- Cisco ASR 9000
- Cisco ISR-G2
- Cisco ISR-4451 -X

The controller pulls cached NetFlow records from the device for path trace. To enable NetFlow on your devices, refer to your specific device documentation. For general information about Cisco NetFlow technology, see [Cisco IOS Flexible NetFlow Technology Q&A](#).

SNMP Trap Configuration

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

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

**Note**

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

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

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

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

IP Device Tracking Configuration

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

Wireless LAN Controller Configuration

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

The following WLCs require SNMP traps to be enabled:

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

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

Trap Name	OID
ciscoLwappDot11ClientAssocTrap	1.3.6.1.4.1.9.9.599.0.9
ciscoLwappDot11ClientDeAuthenticatedTrap	1.3.6.1.4.1.9.9.599.0.10
ciscoLwappDot11ClientMovedToRunStateNewTrap	1.3.6.1.4.1.9.9.599.0.11
ciscoLwappDot11ClientMobilityTrap	1.3.6.1.4.1.9.9.599.0.12

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

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



Note

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

WAN Interface Configuration for EasyQoS

In order for the Cisco APIC-EM to identify the WAN interfaces that need policies, you must specify the interface type (WAN) and (optionally) its subline rate and service-provider Class-of-Service model.

When the Cisco APIC-EM discovers the device and places it in its inventory, the Cisco APIC-EM identifies these specifically marked interfaces as WAN interfaces. The subline rate information is used to trigger a

congestion event on the device when this contracted rate is reached (even if the physical WAN interface itself is not congested). As a result of the congestion event, the Cisco APIC-EM updates the device configuration with the queuing policy that reflects the configured business-intent.

Before you can implement a policy of this type, you need to configure the following strings on the device using the command line interface (CLI):

- WAN interface—To indicate to the Cisco APIC-EM that the interface needs special handling, you need to include `#WAN#` in the interface description.
- Subline rate (MB)—You need to indicate the interface subline rate by including `#rateM#` in the interface description. The rate must be a value below the actual line rate of the interface.
- Service provider profile—You need to specify one of the following four Service Provider profiles by including `#SPPProfileNumber#` in the interface description.

Table 30: SP Profile 1 (SPP1): 4-Class Model

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Default	0	—	—	31
Voice	EF	Yes	10	—
Class 1 Data	AF31	—	—	44
Class 2 Data	AF21	—	—	25

Table 31: SP Profile 2 (SPP2): 5-Class Model

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Class 3 Data	AF11	—	—	1
Voice	EF	Yes	10	—
Class 1 Data	AF31	—	—	44
Class 2 Data	AF21	—	—	25

Table 32: SP Profile 3 (SPP3): 6-Class Model

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Class 1 Data	AF31	—	—	10
Class 3 Data	AF11	—	—	1
Video	AF41	—	—	34
Voice	EF	Yes	10	—
Default	0	—	—	30
Class 2 Data	AF21	—	—	25

Table 33: SP Profile 4 (SPP4): 8-Class Model

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Network-Control Management	CS6	—	—	5
Streaming Video	AF31	—	—	10
Call Signalling	CS3	—	—	4
Scavenger	CS1	—	—	1
Interactive Video	AF41	—	—	30
Voice	EF	Yes	10	—
Default	0	—	—	25
Critical Data	AF21	—	—	25

Example

```
interface GigabitEthernet0/2
  description AT&T Circuit from SJ-13-12 to RTP-Ridge-7 #WAN#50M#SPP4#
```



Note You may want to create a script to automate these device configuration changes.

Performance Monitor Configuration

When you run a path trace to collect **Perf Mon** statistics, the Cisco APIC-EM automatically configures all of the devices in the requested path with the necessary flow monitor commands. The Cisco APIC-EM removes the configuration from the device if there is no corresponding path trace request present or after 24 hours of the path trace request, whichever is first.

The following configuration is sent to each device in the requested path:

```

flow record type performance-monitor APIC_EM-FLOW_ANALYSIS_PERFMON_RECORD
  match ipv4 protocol
  match ipv4 source address
  match ipv4 destination address
  match transport source-port
  match transport destination-port
  match transport rtp ssrc
  collect ipv4 dscp
  collect ipv4 ttl
  collect transport rtp jitter mean
  collect transport rtp jitter minimum
  collect transport rtp jitter maximum
  collect interface input
  collect interface output
  collect counter bytes long
  collect counter packets long
  collect counter bytes rate
  collect counter packets drop (not applicable to routers)
flow monitor type performance-monitor APIC_EM-FLOW_ANALYSIS_PERFMON_MONITOR
  description APIC_EM flow-analysis request monitor
  record APIC_EM-FLOW_ANALYSIS_PERFMON_RECORD

ip access-list extended APIC_EM-FLOW_ANALYSIS_ACL
  class-map APIC_EM-FLOW_ANALYSIS_PERFMON_CLASSMAP
  match access-group name APIC_EM-FLOW_ANALYSIS_ACL
policy-map type performance-monitor APIC_EM-FLOW_ANALYSIS_PERFMON_POLICYMAP
  class APIC_EM-FLOW_ANALYSIS_PERFMON_CLASSMAP
  flow monitor APIC_EM-FLOW_ANALYSIS_PERFMON_MONITOR
interface GigabitEthernet x/y
  service-policy type performance-monitor input APIC_EM-FLOW_ANALYSIS_PERFMON_POLICYMAP

ip access-list extended APIC_EM-FLOW_ANALYSIS_ACL
  permit ip host aa.bb.cc.dd host ww.xx.yy.zz

```

⁶

⁶ aa.bb.cc.dd is source ip and ww.xx.yy.zz is destination ip.



INDEX

A

administrator [16](#)
API [9](#)
API documentation [153](#)
audience [ix](#)
authentication [18, 28](#)
authorization [18](#)

B

Border Gateway Protocol (BGP) [129](#)

C

change password [9](#)
Cisco APIC-EM [3](#)
 overview [3](#)
Cisco Network Plug and Play [9](#)

D

device inventory [9, 50](#)
 Average Update Frequency [50](#)
 Configuration [50](#)
 Device Family [50](#)
 Device Name [50](#)
 Device role [50](#)
 device status [50](#)
 Device Tag [50](#)
 IOS [50](#)
 IP Address [50](#)
 Last Updated Time [50](#)
 Location [50](#)
 MAC Address [50](#)
 Platform [50](#)
 Policy Tag [50](#)
 Serial number [50](#)

device inventory (*continued*)

 Up Time [50](#)
 window [50](#)
device role [60, 89](#)
devices table [50, 57, 58](#)
 changing view [58](#)
 filtering [57](#)
discovery [9, 34, 37, 41](#)
 devices [34](#)
 using CDP [37](#)
 using IP address range [41](#)
discovery credentials caveats [35](#)
discovery results [46](#)

E

Equal Cost Multi Path (ECMP) [129](#)

F

feedback [9](#)

G

GUI overview [9](#)

H

host inventory [9, 69](#)
 window [69](#)
Hosts table [69, 71](#)
 changing view [71](#)
 filters [69](#)
Hot Standby Router Protocol (HSRP) [129](#)
HTTPS methods [156](#)

I

installer [17](#)
 Intermediate System-to-Intermediate System, See [IS-IS](#)
 inventory [50, 69](#)
 device [50](#)
 host [69](#)
 IS-IS [75, 129](#)
 path trace [129](#)
 topology [75](#)
 IWAN [9](#)

L

location marker [66](#)
 adding [66](#)
 location tag [64](#)
 logging into GUI [5](#)

N

northbound REST API documentation [157](#)
 northbound REST APIs [153](#)
 notifications [9](#)
 Notifications [9](#)
 system [9](#)

O

observer [17](#)
 Open Shortest Path First Protocol (OSPF) [129](#)
 OSPF [75](#)

P

Packet over SONET (PoS) [129](#)
 path trace [127, 129, 133](#)
 Path Trace [129](#)
 protocols [129](#)
 plug and play [9](#)
 port channel [129](#)

Q

QoS application [102, 122](#)
 predefined priority class [102](#)
 Quality of Service [97](#)

R

RADIUS server [28](#)
 RBAC [21](#)
 accounting [21](#)
 related documentation [xi](#)
 role [16, 17](#)
 administrator [16](#)
 observer [17](#)

S

Settings [9](#)
 sign out [9](#)
 Spanning Tree Protocol (STP) [129](#)
 static routing [129](#)
 Static-Route [75](#)

T

tag [62, 68](#)
 adding [62](#)
 deleting [68](#)
 removing [62](#)
 topology [9, 75, 78, 81, 82, 85, 89, 91, 95](#)
 aggregate [81](#)
 configuring structure [85](#)
 device role [89](#)
 disaggregate [81, 82](#)
 icons [78](#)
 L2 [75](#)
 L3 [75](#)
 searches [91](#)
 tags [95](#)
 toolbar [75](#)
 VRF [75](#)
 Topology [87](#)
 saving [87](#)

U

user [19, 21, 24, 25, 26](#)
 access [26](#)
 adding [24](#)
 delete [25](#)
 password [21](#)
 permissions [19](#)
 roles [19](#)
 viewing user information [26](#)
 users and domains [18](#)