



## **Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide, Release 1.1.x**

**First Published:** November 02, 2015

**Last Modified:** March 24, 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 NONINFRINGEMENT 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 vii

Audience vii

Document Conventions vii

Related Documentation ix

Obtaining Documentation and Submitting a Service Request x

---

### 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

Cisco APIC-EM GUI Overview 4

Management Applications 8

Cisco Network Plug and Play 8

Cisco Intelligent WAN (IWAN) 9

---

### CHAPTER 3

#### Managing Users and Roles 11

About Role-Based Access Control 11

About User Roles 11

Administrator Role 12

Policy Administrator Role 13

Observer Role 13

Installer Role 13

Users and Domains 14

About AAA 14

Authentication and Authorization 14

Cisco APIC-EM Resources and Permissions 14

Accounting	16
Changing Your Password	16
Configuring Users and Roles	17
Adding a User	18
Deleting a User	18
Viewing and Editing User Information	19
Viewing User Access Status	20

---

**CHAPTER 4****Discovering Devices and Hosts 21**

About Discovery	21
Understanding Device and Host Discovery	22
Understanding Wireless LAN Controller Discovery	22
Understanding the Discovery Results	23
Discovery Credentials Rules	24
Discovery Credentials Caveats	25
Using Discovery	26
Performing Discovery Using CDP	26
Performing a Discovery Using an IP Address Range	29
Stopping and Starting a Discovery	32
Deleting a Discovery	32

---

**CHAPTER 5****Managing Devices and Hosts 35**

Managing Your Device Inventory	35
Filtering Devices in the Device Inventory Window	42
Changing the Devices Layout View	43
Changing the Device Role	43
Deleting a Device	45
Adding or Removing a Device Tag in Device Inventory	45
Adding or Removing a Policy Tag in Device Inventory	46
Adding or Removing a Location Tag	47
Adding or Removing a Location Marker	48
Deleting a Tag	49
Managing Your Host Inventory	50
Changing the Hosts Table View	51

---

**CHAPTER 6****Using the Topology Map 53**

- About Topology 53
  - Topology Toolbar 54
  - Topology Icons 57
- Displaying Device Data 59
- Aggregating Devices 60
  - Aggregating Devices in the Topology Window 60
  - Disaggregating Devices in the Topology Window 61
  - Changing the Aggregated Devices Label 61
- Configuring the Topology Structure 62
- Saving a Topology Layout 64
- Opening a Saved Topology Layout 65
- Changing a Device's Role From the Topology Window 65
- Searching for Devices 66
- Applying Tags to Devices 67
- Displaying Devices with Tags 68

---

**CHAPTER 7****Configuring Quality of Service 71**

- About EasyQoS 71
  - Policies 71
    - Policy Scope 72
    - Applications 73
    - Traffic Classes 73
    - Business-Relevance Groups 74
  - Custom Applications 75
  - Favorite Applications 75
  - Static and Dynamic QoS Policies 76
  - Device Configuration Prerequisites for WAN Policies 76
  - Processing Order for Devices with Limited Resources 78
  - EasyQoS Guidelines and Limitations 80
- Configuring QoS Policies 80
  - Enabling the EasyQoS Beta Feature 83
  - Creating a Policy for Wired Devices 83
  - Creating a Policy for a Wireless Segment 84

Editing a Policy	85
Changing the Business Relevance of an Application	86
Configuring Favorite Applications	87
Creating a Custom Application	88
Editing a Custom Application	89
Enabling Dynamic QoS Policies	90
Viewing Dynamic Policies	90

---

**CHAPTER 8****Performing Path Traces 93**

About Path Trace	93
Path Trace Support	95
Path Trace Protocols and Network Connections	96
Understanding Path Trace Results	100
Understanding the Interface Statistics Retrieved During a Path Trace	103
Understanding the QoS Statistics Retrieved During a Path Trace	105
Performing a Path Trace	105
Collecting QoS and Interface Statistics in a Path Trace	107

---

**CHAPTER 9****Reviewing the API Documentation 109**

About the Cisco APIC-EM API Documentation	109
Supported HTTPS Methods and General Structure	111
Common External RESTful Services HTTP Response Codes	111
Using the Cisco APIC-EM REST API Window	112



## Preface

---

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

## Audience

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

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

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



---

**Note**

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

---

## Document Conventions

This document uses the following conventions:

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

### Reader Alert Conventions

This document may use the following conventions for reader alerts:



**Note**

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

**Tip**

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

**Caution**

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

**Timesaver**

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

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

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

**SAVE THESE INSTRUCTIONS**

## Related Documentation

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

- Cisco Network Plug and Play Documentation for the Cisco APIC-EM:
  - *Release Notes for Cisco Network Plug and Play*
  - *Solution Guide for Cisco Network Plug and Play*
  - *Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM*
  - *Cisco Open Plug-n-Play Agent Configuration Guide*
  - *Mobile Application User Guide for Cisco Network Plug and Play*

**Note**

---

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

---

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see [What's New in Cisco Product Documentation](#).

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.



## CHAPTER

# 1

## 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 this document and shows the releases in which each feature is supported. Your software release might not support all the features in this document. For information about the features that are supported in your release, see the Release Notes. For the latest caveats, see the Bug Search Tool at <https://tools.cisco.com/bugsearch/>.

Feature	Description	Changed in Release	Where Documented
EasyQoS	Added a new application, called EasyQoS, which allows configuration of static and dynamic policies on campus networks.	1.1.0.x	<a href="#">Configuring Quality of Service, on page 71</a>
Discovery	Enhanced the Discovery window to allow you to choose from credentials that were configured in the Settings window and to save Discovery profiles that were configured in the Discovery window for future use.	1.1.0.x	<a href="#">Discovering Devices and Hosts, on page 21</a>
Policy Admin Role	Added a new user role that allows you to manage application policies.	1.1.0.x	<a href="#">Policy Administrator Role, on page 13</a>
Path Trace	Enhanced the Path Trace user interface.	1.1.0.x	<a href="#">Performing Path Traces, on page 93</a>





## Overview

- [About the Cisco Application Policy Infrastructure Controller Enterprise Module, page 3](#)
- [Cisco APIC-EM GUI Overview, page 4](#)
- [Management Applications, page 8](#)

## About the Cisco Application Policy Infrastructure Controller Enterprise Module

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

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

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

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

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

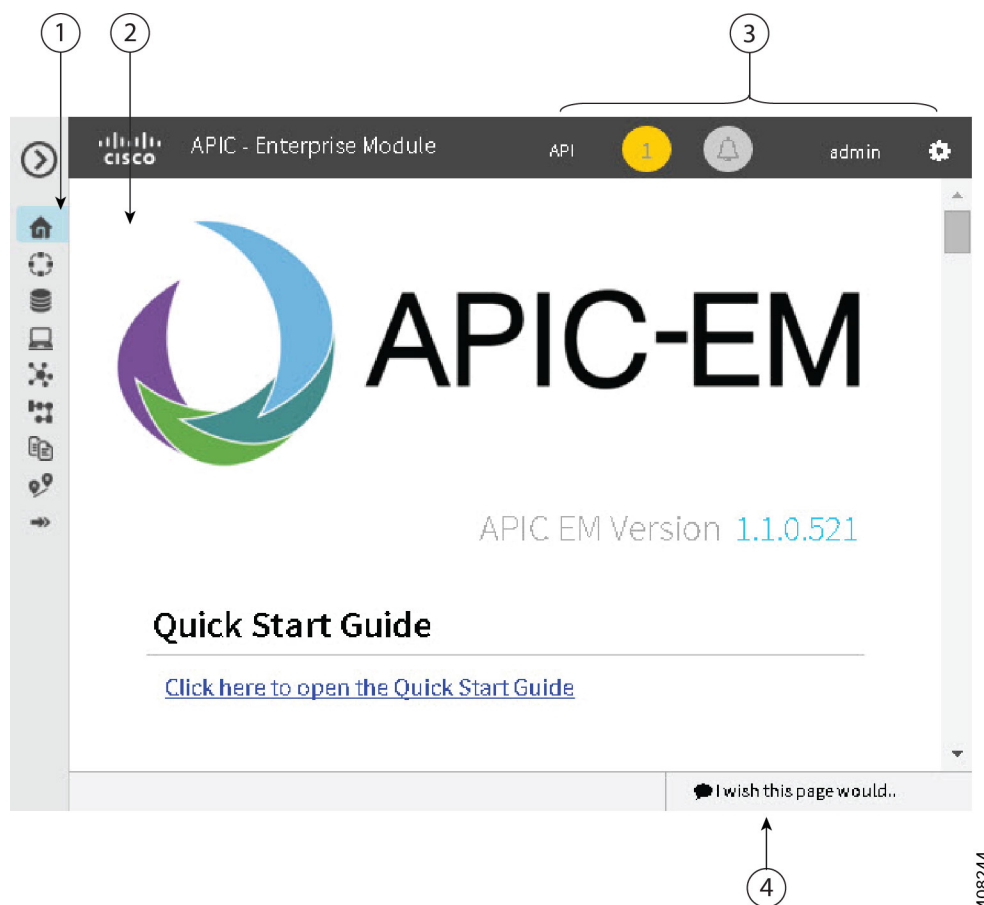
**Table 1: Cisco APIC Enterprise Module Features and Benefits**

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

Feature	Description
Network topology visualization	The Cisco APIC-EM automatically discovers and maps network devices to a physical topology with detailed device-level data. You can use this interactive feature to troubleshoot your network.
EasyQoS	<p>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.</p> <p>Using EasyQoS, you can group devices and then assign classes of service to those devices. The Cisco APIC-EM takes your QoS selections, translates them into the proper device configurations, and deploys the configurations onto those devices.</p>
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.

## Cisco APIC-EM GUI Overview

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













Callout Number	Name	Description
1	<b>Navigation</b> pane	Provides access to the Cisco APIC-EM features and additional applications, such as IWAN and Network Plug and Play.
2	Window	Area where the feature or application interface is displayed. When you click an option in the <b>Navigation</b> pane, its corresponding window opens.
3	<b>Global</b> toolbar	Area that provides access to tools, such as API documentation, settings, and notifications. For a full explanation of the icons on the <b>Global</b> toolbar, see the Global Toolbar Options table below.
4	Feedback link	Link to a form where you can provide input about your experience using the Cisco APIC-EM features and its GUI and provide suggestions for improvements.

### Navigation Pane Options

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


**Table 2: Navigation Pane Options**

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




**Global Toolbar Options**

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

**Table 3: Global Toolbar Options**

Icon	Option	Description
	<b>API</b>	Displays the auto-generated documentation of the northbound REST APIs.



Icon	Option	Description
	<b>System Notifications</b>	Opens the <b>System Notifications</b> view. This view provides information about any system notifications. For example, any notifications about software updates or security certificates updates appear in this window. Each notification contains a brief description and an icon that if clicked opens the source Cisco APIC-EM UI window for the notification (where you can take further action).
	<b>Application Notifications</b>	<p>Opens the <b>Application Notifications</b> view. A red square indicates a notification that has not yet been reviewed. A blue square indicates that either there are no notifications or that notifications exist and have been reviewed. Each notification is listed in the order that it occurred with the most recent at the top of the list. Each notification contains a brief description and an icon that, if clicked, opens the source Cisco APIC-EM application for the notification.</p> <p><b>Note</b> You can also configure to be notified only for events in the current open window (application). By clicking on the link in the <b>Notifications</b> view for the current window (for example, <b>Show only notifications for Discovery</b>), you limit notifications to events that occur in that application.</p>
	<b>Administrative Functions</b>	<p>Opens a window where you can perform functions that are specific to Cisco APIC-EM or to the user:</p> <ul style="list-style-type: none"> <li>• Cisco APIC-EM functions: <ul style="list-style-type: none"> <li>◦ <b>Settings</b>—Allows you to configure controller settings, such as user accounts, discovery credentials, network settings, and other security and maintenance settings.</li> <li>◦ <b>Logs</b>—Allows you to search the controller's service logs.</li> </ul> </li> <li>• User functions: <ul style="list-style-type: none"> <li>◦ <b>Change Password</b>—Allows you to change your own password.</li> <li>◦ <b>Sign Out</b>—Logs you out of the Cisco APIC-EM.</li> </ul> </li> </ul>

# 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.

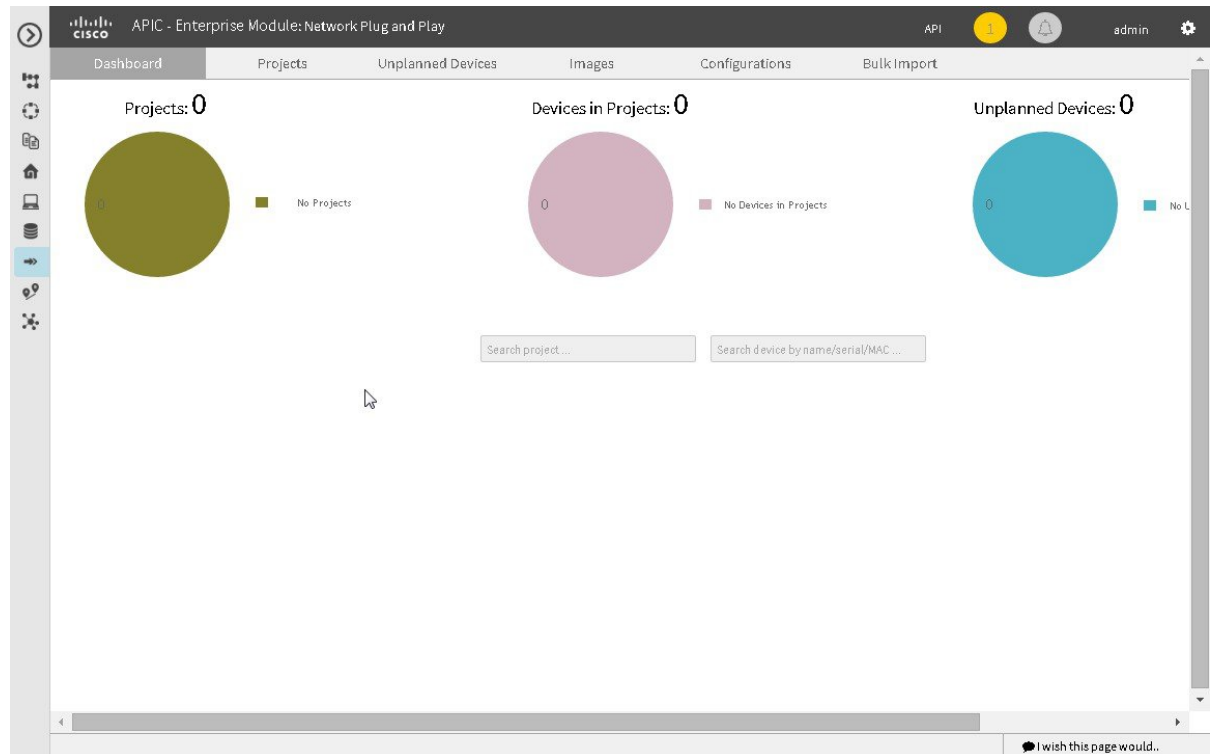
The PnP solution comprises the PnP server, the PnP app, and the PnP agent. The PnP server interacts with the PnP app (which resides on the controller) and the PnP agent (which resides on PnP-enabled nnetwork devices.)

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 1: 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.

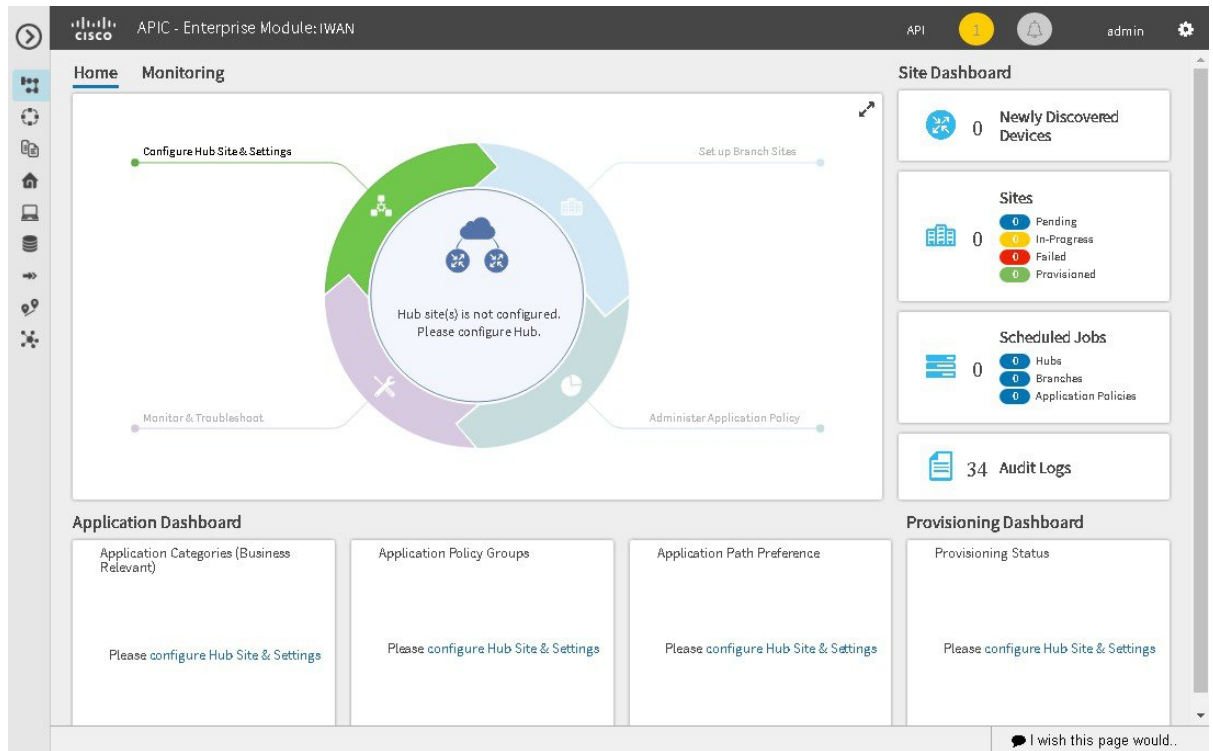
From the IWAN application, you can configure your network-wide settings, provision sites, and configure application policies.

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 2: IWAN Dashboard**





## Managing Users and Roles

- [About Role-Based Access Control, page 11](#)
- [About User Roles, page 11](#)
- [About AAA, page 14](#)
- [Changing Your Password, page 16](#)
- [Configuring Users and Roles, page 17](#)

### About Role-Based Access Control

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

### About User Roles

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



**Note**

---

Only users with the administrative role (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 12](#).

**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 13](#).
- Observer (ROLE\_OBSERVER)—Provides primarily read-only privileges to the Cisco APIC-EM. For information, see [Observer Role, on page 13](#).
- 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 13](#).

## 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 14](#).

**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 14.

**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.

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 14.

### 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"><li>• Administrator</li><li>• Policy Administrator</li></ul>
Inventory: Retrieving inventory list with device credentials	<ul style="list-style-type: none"><li>• Administrator</li><li>• Policy Administrator</li></ul>
Inventory: Adding tags	<ul style="list-style-type: none"><li>• Administrator</li><li>• Policy Administrator</li><li>• Observer</li></ul>



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

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

## Accounting

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

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

## Changing Your Password

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



### Note

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

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

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

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

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

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

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

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

### 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**.

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.

### 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**.
-



## Discovering Devices and Hosts

---

- [About Discovery, page 21](#)
- [Discovery Credentials Rules, page 24](#)
- [Discovery Credentials Caveats, page 25](#)
- [Using Discovery, page 26](#)

### 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) (You must manually enable IPDT on devices and interfaces for this protocol to be used to collect host information.)
- LLDP Media Endpoint Discovery (LLDP-MED) (IP phones and some servers are discovered using LLDP-MED).

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

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 <b>Discoveries</b> pane, clicking on a discovery name displays the information in the <b>Discovery Details</b> and <b>Device Details</b> panes.</p>
Discovery Details pane	<p>Provides detailed information about the discovery parameters that were used to perform the discovery, the state of the discovery, and the number of devices that were discovered. The buttons on this pane allow you to <b>Start</b>, <b>Stop</b>, and <b>Delete</b> discoveries.</p>
In-tool guide	<p>Provides guidance about how to configure discovery.</p>

## Understanding Device and Host Discovery

The Cisco APIC-EM controller scans network devices and attempts to log in to newly found devices by presenting credentials that this guide refers to as discovery credentials.

The Cisco APIC-EM controller discovers network devices automatically by conducting a network scan that attempts to authenticate each network element that it finds. The process of finding network devices is known as discovery. The discovery scanner attempts to log in to a newly found network element by presenting credentials that this guide refers to as discovery credentials. To enable automated discovery of devices made by a variety of manufacturers, the Cisco APIC-EM supports several kinds of discovery credentials.

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

Wireless LAN Controllers (WLCs) have additional setup requirements in order to be discovered. For more information, see [Understanding Wireless LAN Controller Discovery](#), on page 22.

## Understanding Wireless LAN Controller Discovery

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

The following WLCs require SNMP traps to be enabled:

- Cisco Series 2504 Wireless LAN Controller
- Cisco Series 5508 Wireless LAN Controller
- Cisco Series 8510 Wireless LAN Controller

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.

## 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.

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 <b>Discoveries</b> pane, clicking on a discovery name displays the information in the <b>Discovery Details</b> and <b>Device Details</b> panes.</p>

Name	Description
Discovery Details pane	Provides detailed information about the discovery parameters that were used to perform the discovery, the state of the discovery, and the number of devices that were discovered. The buttons on this pane allow you to <b>Start</b> , <b>Stop</b> , and <b>Delete</b> discoveries.
Devices pane	Displays the host name, IP address, and status of the devices found during the scan.  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 <b>Subnet Filter</b> field.

## 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	Configured global credentials will be used for discovery if selected in <b>Discovery</b> .
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. <b>Note</b> 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. <b>Note</b> 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:
  - Update the global credentials with the new device credential. Execute a new discovery scan with the new global credentials.
  - Start a new discovery scan with changed discovery request-specific credentials that matches the new device credential.
- 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.

## Using Discovery

### Performing Discovery Using CDP

You can perform a discovery using CDP.

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

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

#### Before You Begin

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

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

#### Procedure

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

The **Discovery** window appears.

**Step 2** (Optional) In the **Discovery Name** field, enter a unique name for this discovery.

**Step 3** In the **IP Ranges** area, do the following:

- a) From the **Discovery Type** field, choose **CDP**.
- b) In the **IP Address** field, enter the IP address for the Cisco APIC-EM to use as the seed IP address for the discovery scan.

**Step 4** 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 and the information in the tables to help you enter the correct values in the fields:

- The controller supports multiple SNMP credential configurations, but if you configure more than six credential sets (global and/or exception, SNMPv2c and/or SNMPv3 credentials), you will receive an error message.
- An SNMP Read Only (RO) community string is required to assure a successful discovery and populated inventory. However, if an SNMP RO community string is not provided, as a *best effort*, discovery will run with the default SNMP RO community string "public."

**Table 6: 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. <b>Note</b> To enable discovery on the network devices, configure the network device's IP host address as the client address.
Write Community	SNMP read-only (RO) or read/write (RW) community string.

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

**Table 7: SNMPv3**

Field	Description
Username	Username associated with the SNMPv3 settings.
Mode	Specifies the security level that an SNMP message requires and whether the message needs to be authenticated. Choose one of the following modes: <ul style="list-style-type: none"> <li>• noAuthNoPriv—Security level that does not provide authentication or encryption</li> <li>• AuthNoPriv—Security level that provides authentication but does not provide encryption</li> <li>• AuthPriv—Security level that provides both authentication and encryption</li> </ul>

Field	Description
Auth Type	Specifies the authentication type to be used. <ul style="list-style-type: none"> <li>• <b>SHA</b>—Authentication based on the Hash-Based Message Authentication Code (HMAC), Secure Hash algorithm (SHA) algorithm</li> <li>• <b>MD5</b>—Authentication based on the Hash-Based Message Authentication Code (HMAC), Message Digest 5 (MD5) algorithm</li> <li>• <b>None</b>—No authentication</li> </ul>
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3.
Privacy Type	Specifies the privacy type: <ul style="list-style-type: none"> <li>• <b>DES</b>—Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.</li> <li>• <b>AES128</b>—Cipher Block Chaining (CBC) mode AES for encryption.</li> <li>• <b>None</b>—No privacy</li> </ul>
Privacy Password	SNMPv3 privacy password is used to generate the secret key used for encryption of messages exchanged with devices that support DES or AES128 encryption.

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

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

Discovery credentials are preexisting device credentials used by the Cisco APIC-EM to authenticate and discover the Cisco devices in your network. For host discovery, credentials are not required as hosts are discovered through the devices.

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

- SSH
- Telnet

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

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

**Step 7** (Optional) To save these settings, select the **Save these settings to be used again in the future** check box.

**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.

---

## Performing a Discovery Using an IP Address Range

You can discover devices using an IP address range.

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

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

### Before You Begin

You must have administrator (ROLE\_ADMIN) permissions to perform this procedure.

### Procedure

---

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

The **Discovery** window appears.

**Step 2** (Optional) In the **Discovery Name** field, enter a unique name for this discovery.

**Step 3** In the **IP Ranges** area, do the following:

- 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) Enter any additional IP addresses in the IP address fields and click **Add**.

**Step 4** 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 and the information in the tables to help you enter the correct values in the fields:

- The controller supports multiple SNMP credential configurations, but if you configure more than 5 credential sets (global and/or exception, SNMPv2c and/or SNMPv3 credentials), you will receive an error message.
- An SNMP Read Only (RO) community string is required to assure a successful discovery and populated inventory. However, if an SNMP RO community string is not provided, as a *best effort*, discovery will run with the default SNMP RO community string "public."

**Table 9: 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.  <b>Note</b> To enable discovery on the network devices, configure the network device's IP host address as the client address.
Write Community	SNMP read-only (RO) or read/write (RW) community string.

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

**Table 10: SNMPv3**

Field	Description
Username	Username associated with the SNMPv3 settings.
Mode	Specifies the security level that an SNMP message requires and whether the message needs to be authenticated. Choose one of the following modes: <ul style="list-style-type: none"> <li>• noAuthNoPriv—Security level that does not provide authentication or encryption</li> <li>• AuthNoPriv—Security level that provides authentication but does not provide encryption</li> <li>• AuthPriv—Security level that provides both authentication and encryption</li> </ul>



Field	Description
Auth Type	Specifies the authentication type to be used. <ul style="list-style-type: none"> <li>• <b>SHA</b>—Authentication based on the Hash-Based Message Authentication Code (HMAC), Secure Hash algorithm (SHA) algorithm</li> <li>• <b>MD5</b>—Authentication based on the Hash-Based Message Authentication Code (HMAC), Message Digest 5 (MD5) algorithm</li> <li>• <b>None</b>—No authentication</li> </ul>
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3.
Privacy Type	Specifies the privacy type: <ul style="list-style-type: none"> <li>• <b>DES</b>—Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.</li> <li>• <b>AES128</b>—Cipher Block Chaining (CBC) mode AES for encryption.</li> <li>• <b>None</b>—No privacy</li> </ul>
Privacy Password	SNMPv3 privacy password is used to generate the secret key used for encryption of messages exchanged with devices that support DES or AES128 encryption.

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

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

Discovery credentials are preexisting device credentials used by the Cisco APIC-EM to authenticate and discover the Cisco devices in your network. 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 6** (Optional) In the **Advanced** area, configure the protocols that the Cisco APIC-EM uses to connect to devices. By default, the Cisco APIC-EM uses the following protocols:

- SSH
- Telnet

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

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

**Step 7** (Optional) To save these settings, select the **Save these settings to be used again in the future** check box.

**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.

## Stopping and Starting a Discovery

You can stop a discovery 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, do the following:

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

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

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

## Deleting a Discovery

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

### Before You Begin

You must have administrator (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 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.
-





## Managing Devices and Hosts

- [Managing Your Device Inventory, page 35](#)
- [Managing Your Host Inventory, page 50](#)

### 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**.



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

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

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

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



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

Column Name	Description
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 <b>Device Inventory</b> window and <b>Topology</b> window support location tags.</p> <p>Use the following guidelines when creating location tags:</p> <ul style="list-style-type: none"> <li>• Location tag information is maintained on the controller only and not deployed to or derived from the device itself.</li> <li>• A location defined on the controller is not the "civic-location" property that some devices support.</li> <li>• You cannot create, use, or search for location tags in the <b>Topology</b> window.</li> <li>• Location tags cannot be attached to hosts.</li> <li>• You can apply only one location tag to a device. However, you can use both a location tag and a device tag together.</li> </ul> <p>For information about adding location tags, see <a href="#">Adding or Removing a Location Tag</a>, on page 47.</p> <p>Along with the location tag, you can add a geographical marker on a world map to a device. For information, see <a href="#">Adding or Removing a Location Marker</a>, on page 48.</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>A number in the <b>Tag</b> column indicates how many tags have been applied to that device.</p> <p><b>Note</b> You are permitted to use both a location tag and a device tag together.</p> <p>For information about adding or removing device tags, see <a href="#">Adding or Removing a Device Tag in Device Inventory</a>, on page 45.</p> <p>For information about deleting a tag from the controller database, see <a href="#">Deleting a Tag</a>, on page 49.</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 <a href="#">Configuring Quality of Service, on page 71</a>.</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"> <li>• Cisco Interfaces and Modules</li> <li>• Routers</li> <li>• Switches and Hubs</li> <li>• Third Party Device</li> <li>• Unsupported Cisco Device</li> <li>• Wireless Controller</li> </ul>
Device Series	Series number of the device, for example, Cisco Catalyst 4500 Series Switches.
Last Inventory Collection Status	<p>Status of the last discovery scan for the device:</p> <ul style="list-style-type: none"> <li>• <b>Managed</b>—Device is in a fully managed state.</li> <li>• <b>Partial Collection Failure</b>—Device is in a partial collected state and not all the inventory information has been collected. Move the cursor over the <b>Information</b> (i) icon to display additional information about the failure.</li> <li>• <b>Unreachable</b>—Due to device connectivity issues, the device could not be reached and no inventory information was collected. This condition can occur when periodic collection happens.</li> <li>• <b>Wrong Credentials</b>—If the device credentials are changed after adding the device to the inventory, this condition is noted.</li> <li>• <b>In Progress</b>—Inventory collection is occurring.</li> </ul>

### Related Topics

- [Changing the Device Role, on page 43](#)
- [Adding or Removing a Device Tag in Device Inventory, on page 45](#)
- [Adding or Removing Tags to Multiple Devices](#)
- [Adding or Removing a Location Tag, on page 47](#)
- [Adding or Removing a Location Marker, on page 48](#)

## 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.

### 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.

### 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

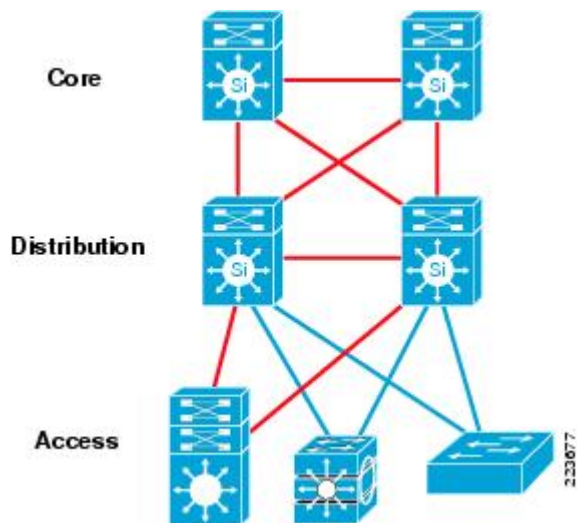
During the scan process, the controller assigns a role to each discovered device. The device role is used to identify and group devices according to their responsibilities and placement in the network.

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 3: 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 65.

### 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 11.

### 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 35](#)

## 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 35](#).

---

**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 35](#)

## 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 71](#).

## 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 35](#)

[Adding or Removing a Location Marker, on page 48](#)

## 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:

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

**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 35](#)

[Topology](#)

[Topology Icons, on page 57](#)

## 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

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

To view your host inventory, click **Host Inventory** in the Navigation pane. The **Host Inventory** window opens, listing the discovered hosts in your network. The following table describes the information that is displayed about the hosts in your inventory.



**Note**

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

**Figure 4: Host Inventory Window**

Host Name	Host MAC Address	Host IP Address	Host Type	Connected Network Device IP Address
ise-12-9	00:0c:29:84:a2:d5	10.126.107.109	WIRED	10.126.107.100
ova3495	00:0c:29:85:38:bd	10.126.255.252	WIRED	10.126.255.251
platinum-pap1	00:0c:29:87:06:7a	10.126.107.106	WIRED	10.126.107.100
	00:0c:29:9b:eb:8f	10.126.107.106	WIRED	10.126.107.100
	00:0c:29:9d:ca:3a	10.126.107.111	WIRED	10.126.107.100
	00:0c:29:a0:c3:8e	10.126.107.146	WIRED	10.126.107.100
	00:0c:29:a4:60:cf	10.126.142.112	WIRED	10.126.142.101
	00:0c:29:b7:0b:01	10.126.107.104	WIRED	10.126.107.100
	00:0c:29:bd:4c:49	10.126.255.106	WIRED	10.126.255.102
	00:0c:29:bf:c7:c1	10.126.255.251	WIRED	10.126.255.250
10 per page ▼		300 Hosts		< Previous    5 of 30    Next >

**Table 13: Host Inventory**

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

Host Inventory	Description
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.
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 51](#)

## 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 50](#)





## Using the Topology Map

- [About Topology, page 53](#)
- [Displaying Device Data, page 59](#)
- [Aggregating Devices, page 60](#)
- [Configuring the Topology Structure, page 62](#)
- [Saving a Topology Layout, page 64](#)
- [Opening a Saved Topology Layout, page 65](#)
- [Changing a Device's Role From the Topology Window, page 65](#)
- [Searching for Devices, page 66](#)
- [Applying Tags to Devices, page 67](#)
- [Displaying Devices with Tags, page 68](#)

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

The topology map includes the following key features:

- Auto-visualization of Layer 2 and 3 topologies on top of the physical topology provides a granular view for design planning and simplified troubleshooting.
- For a Layer 2 topology, the controller discovers configured VLANs within your network to display in the **Topology** window. For a Layer 3 topology, the controller discovers all forms of a Layer 3 topology (OSPF, IS-IS, etc.), depending on what is currently configured and in use within your network to display in the **Topology** window.
- You can click on a device icon to display information about that device.
- You can perform a path trace and then view the trace in the topology map. For additional information about the performing a path trace, see [About Path Trace, on page 93](#).

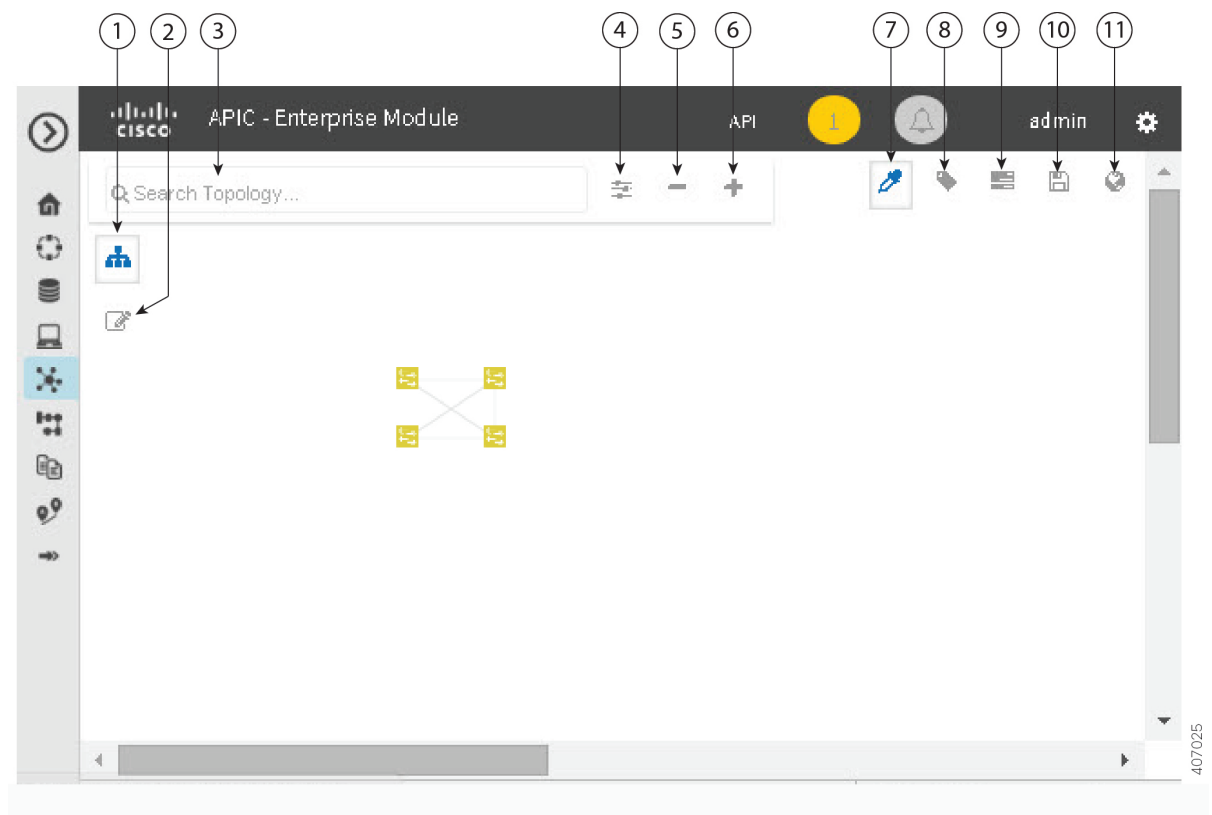
**Note**

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

## Topology Toolbar

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

**Figure 5: Topology Window**



Callout Number	Icon Name	Description
1	<b>Toggle Aggregation</b>	<p>Enables or disables device aggregation. Aggregating devices means grouping devices together. You can group devices in any way that makes sense to you.</p> <p>You can save the layout for future reference by clicking the <b>Save</b> icon.</p> <p>This grouping does not effect the physical configuration on the devices. Aggregation is enabled by default.</p>








Callout Number	Icon Name	Description
2	<b>Toggle Multiselect</b>	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.
3	<b>Search Topology</b>	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 <b>Topology</b> window.
4	<b>Filters</b>	<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 <b>Advanced</b> options. For information, see <a href="#">Configuring the Topology Structure, on page 62</a>.</p> <ul style="list-style-type: none"> <li>• <b>Enterprise</b> (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.</li> <li>• <b>Connections</b>—Displays the devices according to their number of connections. Starting from the left, the devices with no connections are displayed, then devices with one connection, then devices with two connections, and so on.</li> <li>• <b>Type and Role</b>—Displays the devices according to their role in the network: access router, distribution switch, core switch and hub, and boarder router.</li> <li>• <b>Advanced</b>—Provides options for you to refine the topology display.</li> </ul>
5	<b>Zoom out</b>	<p><b>Note</b> Adjusts the <b>Topology</b> window's view. Click the - (minus) icon to minimize the view of the network hosts and devices.</p>



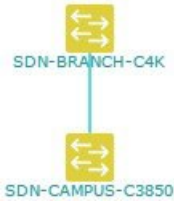
Callout Number	Icon Name	Description
6	<b>Zoom in</b>	Adjusts the <b>Topology</b> window's view. Click the + (plus) icon on the menu bar to maximize the view of the network hosts and devices.
7	<b>Toggle Color Code</b>	Toggles between displaying the device icons in different colors or in a single color. Color coding is enabled by default.
8	<b>Tags</b>	<p>Displays the available tags. Clicking on an individual tag highlights the device or devices in the <b>Topology</b> window that have this tag.</p> <p>You can also apply tags to devices by selecting the device, clicking <b>Device Tagging</b> in the <b>Device Information</b> dialog box, and then creating and applying the tags.</p>
9	<b>Layers</b>	<p>Displays devices with the following attributes on the topology map:</p> <ul style="list-style-type: none"> <li>• <b>Layer 2</b>—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.</li> </ul> <p><b>Note</b> You can also access a management network view by choosing a management selection from the drop-down menu.</p> <ul style="list-style-type: none"> <li>• <b>Layer 3</b>—Displays devices based on the selected Layer 3 protocol. The following Layer 3 protocols are available: <ul style="list-style-type: none"> <li>◦ <b>Intermediate System-to-Intermediate System (IS-IS)</b></li> <li>◦ <b>Open Shortest Path First (OSPF)</b></li> <li>◦ <b>Enhanced Interior Gateway Routing Protocol (EIGRP)</b></li> <li>◦ <b>Static-Route</b></li> </ul> </li> </ul> <p><b>Note</b> The default Layer 3 topology has all Layer 3 protocols.</p> <ul style="list-style-type: none"> <li>• <b>VRF</b>—Displays devices that have Virtual Routing and Forwarding (VRF) tables.</li> </ul>

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

## Topology Icons

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

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

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

## Related Topics

[Applying Tags to Devices](#)

[Viewing Device Data](#)

[Searching for Devices, on page 66](#)

[Configuring the Topology Structure, on page 62](#)

[Changing the Aggregated Devices Label, on page 61](#)

[Removing Tags from Devices](#)

[Viewing Devices with Tags](#)

[Adding or Removing a Location Marker, on page 48](#)

[Aggregating Devices in the Topology Window, on page 60](#)

[Configuring the Topology Structure, on page 62](#)

[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 43.)
- 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 57.

**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 57

## Disaggregating Devices in the Topology Window

You can ungroup devices by disaggregating them 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** 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 57](#)

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

Filter	Basic View	Advanced View
<b>Type and Role</b>	<p>Arranges the device icons from top to bottom based on device type (cloud, router, WLC, switch, access point, wired, wireless) and role (border router, core, distribution, and access)</p> <p><b>Note</b> Aggregated devices are disaggregated in this view.</p>	<p><b>Device type</b>—Use the slider to adjust the amount of space between device icons based on their device types.</p> <p><b>Device role</b>—Use the slider to adjust the amount of space between device icons based on their device roles.</p> <p><b>Node overlap</b>—Use the slider to adjust the amount of space between nodes.</p> <p><b>centralizeX</b>—When checked, the device icons are centered along the X axis. When unchecked, the device icons are aligned to the X axis.</p> <p><b>Note</b> Select <b>x</b> or <b>y</b> from the drop down next to each slider to change how the device icons are displayed, horizontally or vertically.</p>

### What to Do Next

Save the current layout or load a previously saved layout. For information, see [Saving a Topology Layout, on page 64](#) and [Opening a Saved Topology Layout, on page 65](#).

### Related Topics

[Topology](#)  
[Topology Icons, on page 57](#)  
[Topology](#)  
[Topology Icons, on page 57](#)

## 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\_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.

### 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).

### 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 57

## Applying Tags to Devices

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

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



---

**Note**

Applying a tag to a host is not supported.

---

### Before You Begin

You should have performed the following tasks:

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

### Procedure

---

- Step 1** From the Navigation pane, click **Topology**.  
The **Topology** window appears.
- Step 2** Click the device or devices you want to tag. To select more than one device, click the **Multiselect** icon. For information about how to use the multiselect function, see [Topology Icons, on page 57](#).  
**Note** To deselect devices in your selection, click outside of the selected device.  
The **Device Information** dialog box appears.
- Step 3** Click **Device Tagging**.  
The **Device Tagging** dialog box appears.
- Step 4** From the **Available Tags** column, click a tag to apply it to the selected device or devices. If the tag you want does not exist, you can create it by following these steps:
- Enter the name of the tag in the **Tag Title** field.
  - Click **+New Tag**.
- Step 5** When you are done tagging, click **x** to close the dialog box.
- Step 6** You can verify the tagging by clicking on one of the devices that you tagged.  
The **Device Information** dialog box shows the **Tags** field with the total number and the names of the tags applied to the device.
- 

## Displaying Devices with Tags

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

### Before You Begin

Discover the devices in your network.

Create tags and apply 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 71](#)
- [Configuring QoS Policies, page 80](#)

### 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.

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 11](#).

You define the scope of the devices that you want to apply QoS policies on. Then you define the QoS policy for the scope. The Cisco APIC-EM takes your selections, translates them into the proper device configurations, 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

EasyQoS is not enabled by default. To enable EasyQoS, you need to enable EasyQoS in the **Settings** window. For information, see [Enabling the EasyQoS Beta Feature, on page 83](#).

### 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 detailed information about these attributes, see [Business-Relevance Groups](#), on page 74.

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

You define the scope of a policy by applying policy tags to devices that have similar QoS level needs. A policy tag groups the devices so that you can deploy the same QoS policy to more than one device at the same time. You can apply policy tags from the **Device Inventory** window. Then in the **EasyQoS** window, you configure the QoS policies for the scopes and save them to the devices. Applying the QoS policies deploys the QoS configurations onto the devices.

For example, you have three devices that need the same quality of service level. From the **Device Inventory** window, you create a policy tag and apply it to the three devices. From the **EasyQoS** window, you choose the scope of your policy by selecting the policy tag that contains the three devices. Then, you configure the QoS policies by assigning the applications to a business-relevancy group. When you apply the QoS policies that you have defined for the policy tag, the three devices are updated with the corresponding QoS configurations.

**Note**

Because QoS (by nature) needs to be deployed end-to-end, it is important to add all devices in a path to the scope in order for the QoS policy as a whole to have effect.

## 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.

**Note**

Changing an application's traffic class is not supported; only changing the business-relevance of an application is supported.

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 75.

## Traffic Classes

The Cisco APIC-EM provides the following traffic classes, which have preconfigured QoS settings to support the specific types of application traffic.

**Table 14: Traffic Classes**

Traffic Class	Supported Types of Application Traffic
Voice	VoIP telephony (bearer-only) traffic. (VoIP signaling traffic is assigned to the Call Signaling class.) Traffic in this class is marked EF (DSCP 46). Voice is treated with a strict priority service.
Broadcast Video	Broadcast TV, live events, video surveillance flows, and similar inelastic streaming media flows. (Inelastic flows refer to flows that are highly drop sensitive and have no retransmission and/or flow-control capabilities.) Traffic in this class is marked as Class Selector 5 (CS5/DSCP 40) and may be treated with a strict-priority service.
Realtime Interactive	Inelastic high-definition interactive video applications and audio and video components of these applications. Traffic in this class is marked CS4 (DSCP 32) and may be treated with a strict-priority service.
Multimedia Conferencing	Desktop software multimedia collaboration applications and audio and video components of these applications. Traffic in this class is marked as Assured Forwarding Class 4 (AF41/DSCP 34) and is provisioned with a guaranteed bandwidth queue with DSCP-based Weighted-Random Early Detect (DSCP-WRED) enabled.

<b>Traffic Class</b>	<b>Supported Types of Application Traffic</b>
Multimedia Streaming	Video-on-Demand (VoD) streaming video flows and desktop virtualization applications. Traffic in this class is marked as AF Class 3 (AF31) and is provisioned with a guaranteed bandwidth queue with DSCP-based WRED enabled.
Network Control	Network control plane traffic, which is required for reliable operation of the enterprise network. Traffic in this class is marked as CS6 and provisioned with a (moderate, but dedicated) guaranteed bandwidth queue. WRED should not be enabled on this class, as network control traffic should not be dropped. Example traffic includes EIGRP, OSPF, BGP, HSRP, IKE, and so on.
Signaling	Control-plane traffic for the IP voice and video telephony infrastructure. Traffic in this class is marked as CS3 (DSCP 24) and provisioned with a moderate, but dedicated, guaranteed bandwidth queue.
Network Management	Network operations, administration, and management traffic, such as SSH, SNMP, syslog, and so on. This class is important to the ongoing maintenance and support of the network. Traffic in this class is marked as CS2 (DSCP 16) and provisioned with a (moderate, but dedicated) guaranteed bandwidth queue. WRED is not enabled on this class, as OAM traffic cannot be dropped.
Transactional Data (Low-Latency Data)	Interactive (foreground) data applications. Traffic in this class is marked as Assured Forwarding Class 2 (AF21/DSCP 18) and is provisioned with a dedicated bandwidth queue with DSCP-WRED enabled.
Bulk Data (High-Throughput Data)	Noninteractive (background) data applications. Traffic in this class is marked as Assured Forwarding Class 1 (AF11/DSCP 10) and is provisioned with a moderate, but dedicated, bandwidth queue with DSCP-WRED enabled.
Default Forwarding (Best Effort)	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. Traffic in this class is marked as Default Forwarding (DF or DSCP 0) and is provisioned with a dedicated queue.
Scavenger	Nonbusiness related traffic flows and applications assigned to the business-irrelevant group, such as data or media applications that are entertainment-oriented. Traffic in this class is marked CS1 (DSCP 8) and is provisioned with a minimal bandwidth queue that is the first to starve if network congestion occurs.

## Business-Relevance Groups

The EasyQoS feature provides three levels of business-relevance groupings. These groupings provide different levels of service to the applications that have been assigned to them. These groups include:

- **Business Relevant**—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**—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**—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.

## 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 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**

When you define a custom application in Cisco APIC-EM, the application is available to be assigned in IWAN; however, in IWAN, unless custom applications are assigned to a policy, they are not available in Cisco APIC-EM.

## 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. The benefit of this feature is that 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), and flagging an application as a favorite helps to ensure that the QoS policies for your favorite applications get configured on devices.

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 Dynamic Host Configuration Protocol (DHCP) as a favorite, the DHCP protocol is flagged as a favorite in all other 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.

## Static and Dynamic QoS Policies

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

- **Static policies**—The Cisco APIC-EM deploys the QoS policies to the devices and the policies are in effect until you change or remove them. Static policies comprise the majority of the deployments.
- **Dynamic policies**—(Used on LAN interfaces only.) You 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 globally on all policies, not on a per scope basis.

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..

## Device Configuration Prerequisites for WAN Policies

In order for the Cisco APIC-EM to identify the WAN interfaces that need dynamic 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 15: 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 16: 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 17: 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 18: 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.

## 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:

Applications are given priority according to the following criteria and 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. So, 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.



- Existing, default NBAR applications are not assigned a rank until you mark them as favorites, at which point they are assigned rank 10,000.
- 2 **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.
    - Existing, 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).
  - 3 **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 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 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 have the 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	Next, favorite applications have priority because their rank is 10,000. However, because the gss-http application has a higher popularity (10), it is given a higher priority than the corba-iiop application (popularity 9).
4. Favorite application, corba-iiop	
5. All other, default NBAR applications	All other applications are next and are prioritized according to 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.

## 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. 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 rollback 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.
- EasyQoS supports Out Of Band (OOB) changes. 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 78](#).
- You cannot create custom applications for wireless devices.
- You cannot delete custom applications using the GUI.
- 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.

## Configuring QoS Policies

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

**Table 19: QoS Policy Manager Window—Policy Tag Details**

Name	Description
<b>Policy Scopes</b> pane	<p>Lists the QoS policy tags that have been created in the <b>Device Inventory</b> window.</p> <p>Click a policy tag from the <b>Policy Scopes</b> pane to display the devices defined for the tag. The <b>Wired Devices</b> and <b>Wireless Devices</b> panes appear. From this window, you can create a new policy or view an existing policy.</p> <p>Click the <b>Plus</b> icon (+) to list any policies that have been created for the policy tag.</p>
<b>Wired Devices</b> 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><b>Create Policy</b>—Allows you to create a policy for wired devices. Click <b>Create Policy</b>, enter a name in the <b>Policy Name</b> field, and click <b>Create</b>. The <b>Policy Details</b> pane appears. For more information, see the <b>Policy Details</b> pane entry in the <b>QoS Policy Manager Window— Policy Details</b> table.</p>
<b>Wireless Devices</b>	<p>Lists the wireless devices defined for the selected policy tag.</p> <p>To display device details, place the cursor over the device name.</p> <p><b>Create Policy</b>—Allows you to create a policy for wireless devices. After you name the policy and click <b>Create</b>, the <b>QoS Policy Manager</b> pane (Create Policy) appears.</p> <p><b>View Policy</b>—Allows you to display details about a policy that has already been created. For more information, see the <b>Policy Details</b> pane entry in the <b>QoS Policy Manager Window— Policy Details</b> table.</p>
<b>Dynamic QoS Area</b>	<p>Allows you to enable or disable dynamic QoS and lists the active dynamic policies.</p>

**Table 20: QoS Policy Manager Window— Policy Details**

Name	Description
<b>Policy Details</b> pane	<p>Displays the following information and elements:</p> <ul style="list-style-type: none"> <li>• <b>Policy Name</b>—Name of the policy.</li> <li>• <b>Scope</b>—Name of the policy tag.</li> <li>• <b>Apply Policy</b> or <b>Reapply Policy</b>—Allows you to create a new policy or deploy the existing policy to the devices again.</li> <li>• <b>Enabled on</b>—Displays the number of devices that have been successfully updated with the QoS policy.</li> <li>• <b>Edit Policy</b>—Allows you to change the business relevance of applications.</li> <li>• <b>Refresh Status</b>—Display updated information.</li> <li>• <b>Devices</b>—Lists the devices that have been assigned the policy.</li> <li>• <b>Status</b>—Displays the state of the deployment of the QoS configuration onto the devices.</li> <li>• <b>Policy</b>—Policy that has been assigned to the device.</li> </ul>
<b>Application Details</b> pane	<p>Displays the following information and elements:</p> <ul style="list-style-type: none"> <li>• Total number of applications that are in each of the three business categories.</li> <li>• Number of applications in each of the traffic classes by business relevancy group.</li> <li>• <b>Reset to Default</b>—Resets the QoS policy configuration to the Cisco Verified Design (CVD) settings.</li> </ul>

**Table 21: QoS Policy Manager Window—Edit Applications Pane**

Name	Description
<b>Add Application</b>	Allows you to add applications that are not in the list. (For more information, see the next row.)
<b>Star</b> icon	Allows you to flag applications that you want EasyQoS to configure on devices before all other applications, except custom applications. Favorite applications are configured system-wide, not on a per scope basis. For more information, see <a href="#">Processing Order for Devices with Limited Resources</a> , on page 78.

Name	Description
<b>Additional Options</b>	<p>Provides more actions that you can perform:</p> <ul style="list-style-type: none"> <li>• <b>Search</b> field—Finds a specific application by name.</li> <li>• <b>Sort</b>—Sorts applications by name, traffic class, application group, or popularity.</li> <li>• <b>Collapse All</b>—Closes all of the application groupings.</li> <li>• <b>Show Changes</b>—Shows only the applications that have been changed. Applications with changed business relevancy settings have a <b>BR</b> (Business Relevant), <b>IR</b> (Business Irrelevant), or <b>D</b> (Default) designator next to the application name.</li> </ul>

## Enabling the EasyQoS Beta Feature

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

### 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**.
- 

## Creating a Policy for Wired Devices

You can create a QoS policy for a group of devices that have the same policy tag. When you apply the policy, it is deployed to the devices.



### Note

Each policy tag can have only one QoS policy assigned to it. You cannot assign more than one QoS policy to a policy tag

---

### 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 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 devices that you are going to configure policies on.

### Procedure

- 
- Step 1** From the **Navigation** pane, click **EasyQoS**.
  - Step 2** From the **Policy Scopes** pane, select the desired policy tag.
  - Step 3** Click **Create Policy**.
  - Step 4** Enter a name for the policy in the **Policy Name** field and click **Create**.
  - Step 5** If you want to change the policy settings, proceed to the next step. Otherwise, click **Apply Policy** to deploy the default policy settings to the devices.
  - Step 6** To change the policy settings, from the **Policy Manager** pane, click **Edit Policy**.  
The Business Relevancy pane lists the business relevant groups and the applications that are assigned to each group.
  - Step 7** To change the business-relevancy group of an application (including custom applicaitons), select the business-relevancy group from the drop-down list next to the desired application.  
Valid options are **Business Relevant**, **Default**, and **Business Irrelevant**. For information about these options, see [Business-Relevance Groups](#), on page 74.
  - Step 8** (Optional) If desired, designate applications as favorites by clicking the star icon next to the application.  
For information about how favorite applications work, see [Favorite Applications](#), on page 75.
  - Step 9** (Optional) If desired, create a custom applicaiton. For information, see [Creating a Custom Application](#), on page 88.
  - Step 10** Click **Apply Policy**.  
The policy configuration is deployed to the devices.
- 

## Creating a Policy for a Wireless Segment

You can create a QoS policy for wireless devices that have the same policy tag. When you apply the policy, it is deployed to the devices.



#### Note

Each policy tag can have only one QoS policy assigned to it. You cannot assign more than one QoS policy to a policy tag

### 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 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 devices that you are going to configure policies on.

### Procedure

---

- Step 1** From the **Navigation** pane, click **EasyQoS**.
  - Step 2** From the **Policy Scopes** pane, select the desired policy tag.
  - Step 3** In the **Wireless Segments** pane, click **Create Policy** next to the wireless segment that you want to create a policy for.
  - Step 4** Enter a name for the policy in the **Policy Name** field and click **Create**.
  - Step 5** From the **Policy Manager** pane, click **Edit Policy**.
  - Step 6** If you want to change the policy settings, proceed to the next step. Otherwise, click **Apply** to deploy the default policy settings to the devices.
  - Step 7** To change the business-relevancy group of an application (including custom applicaitons), select the business-relevancy group from the drop-down list next to the desired application. Valid options are **Business Relevant**, **Default**, and **Business Irrelevant**. For information about these options, see [Business-Relevance Groups](#), on page 74.
  - Step 8** (Optional) If desired, designate applications as favorites by clicking the star icon next to the application. For information about how favorite applications work, see [Favorite Applications](#), on page 75.
  - Step 9** (Optional) If desired, create a custom applicaiton. For information, see [Creating a Custom Application](#), on page 88.
  - Step 10** Click **Apply Policy**.  
The policy configuration is deployed to the devices.
- 

## Editing a Policy

You can edit an existing QoS policy. After editing, when you apply the policy, it is deployed to the devices.

**Note**

Each policy tag can have only one QoS policy assigned to it. You cannot assign more than one QoS policy to a policy tag

---

### Before You Begin

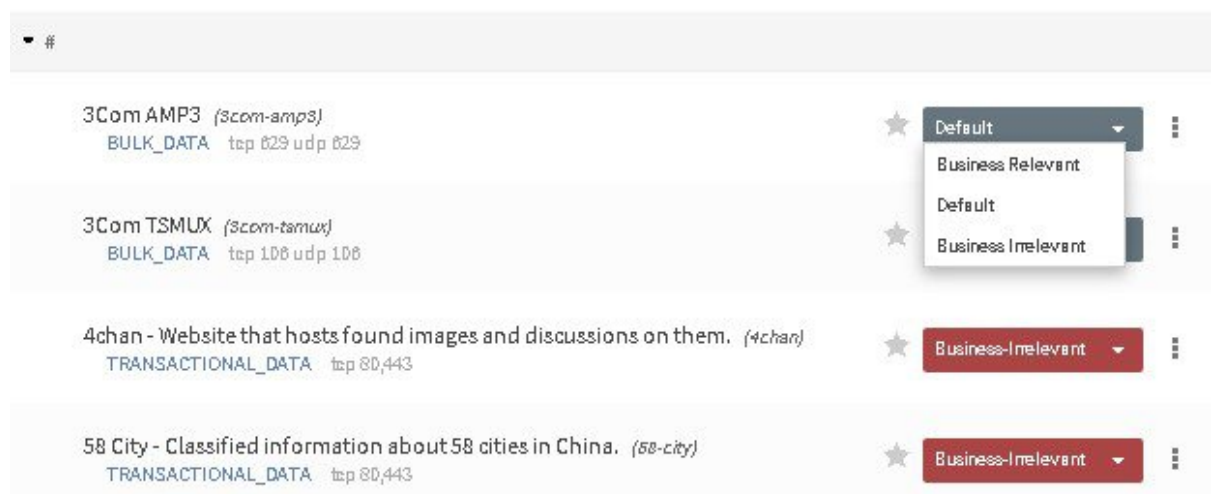
You must have either administrator (ROLE\_ADMIN) or policy administrator (ROLE\_POLICY\_ADMIN) permissions to perform this procedure.

## Procedure

- 
- Step 1** From the **Navigation** pane, click **EasyQoS**.
- Step 2** From the **Policy Scopes** pane, select the desired policy tag.
- Step 3** To change the policy settings, from the **Policy Manager** pane, click **Edit Policy**.  
The Business Relevancy pane lists the business relevant groups and the applications that are assigned to each group.
- Step 4** To change the business-relevancy group of an application (including custom applicaitons), select the business-relevancy group from the drop-down list next to the desired application.  
Valid options are **Business Relevant**, **Default**, and **Business Irrelevant**. For information about these options, see [Business-Relevance Groups](#), on page 74.
- Step 5** (Optional) If desired, designate applications as favorites by clicking the star icon next to the application.  
For information about how favorite applications work, see [Favorite Applications](#), on page 75.
- Step 6** (Optional) If desired, create a custom applicaiton. For information, see [Creating a Custom Application](#), on page 88.
- Step 7** Click **Apply Policy**.  
The updated policy configuration is deployed to the devices.
- 

## Changing the Business Relevance of an Application

You can change an application's business-relevancy group. For information, see [Business-Relevance Groups](#), on page 74.



### 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 devices that you are going to configure policies on.

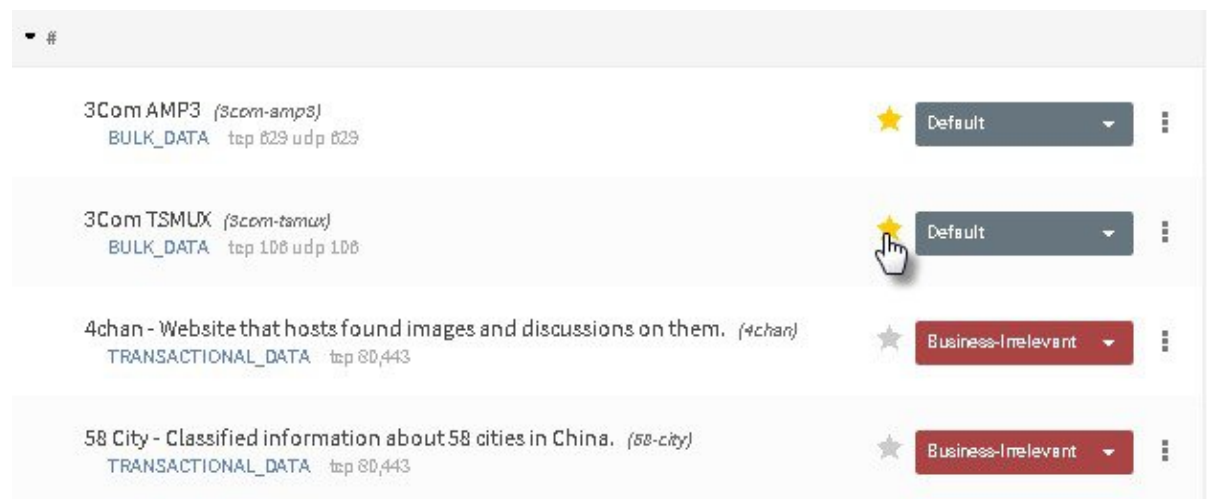
### Procedure

- Step 1** From the **Navigation** pane, click **EasyQoS**.
- Step 2** From the **Policy Scopes** pane, select the desired policy tag.
- Step 3** To change the policy settings for these devices, click **Edit Policy**.
- Step 4** To change the business-relevancy group of an application, do one of the following:
  - Click the business-relevancy group drop-down list next to the desired application and choose the group that you want to assign.
  - Click the icon next to the traffic class to list the applications in that traffic class, then drag and drop the desired application to one of the three business-relevancy groups (boxes) above.
- Step 5** Click **Reapply Policy**.  
The updated policy configuration is deployed to the devices.

## Configuring Favorite Applications

You can designate applications as favorites for an existing policy.

For information about how favorite applications work, see [Favorite Applications](#), on page 75.



### 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 devices that you are going to configure policies on.

### Procedure

- 
- Step 1** From the **Navigation** pane, click **EasyQoS**.
- Step 2** From the **Policy Scopes** pane, select the desired policy tag.
- Step 3** To change the policy settings for these devices, click **Edit Policy**.
- Step 4** Click the star icon next to the applications that you want to designate as favorites.  
For information about how favorite applications work, see [Favorite Applications](#), on page 75.
- Step 5** Click **Replay Policy**.  
The updated policy configuration is deployed to the devices.
- 

## Creating a Custom Application

To help you quickly configure QoS policies, EasyQoS provides a number of applications that support the NBAR2 protocol library. However, if you have applications that are not in the the library, you can add them.

### 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 devices that you are going to configure policies on.

### Procedure

- 
- Step 1** From the **Navigation** pane, click **EasyQoS**.
- Step 2** From the **Policy Scopes** pane, select the desired policy tag.
- Step 3** Next to the policy that you want to change, click **View Policy**.
- Step 4** From the **Policy Manager** pane, click **Add Application**.
- Step 5** 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 6** Click **Create Application** to save the new application.  
The application is listed in the **Custom Applications** group.
- Step 7** Choose the business relevance of the custom application from the drop-down list. (When you create a custom application, the business relevance defaults to **none**.) Valid values are **Business Relevant**, **Default**, and **Business Irrelevant**.
- Step 8** (Optional) If desired, continue configuring the policy or deploy these changes to the devices by clicking **Reapply Policy**.
- 

## Editing a Custom Application

You can any of the applications that you have added.

### 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 **Policy Scopes** pane, expand the scope where the policy that you want to edit resides.
- Step 3** Select the policy that you want to edit.
- Step 4** From the **Policy Details** pane, click **Edit Policy**.
- Step 5** From the **Edit Applications** pane, click the **More Options** icon (icon) next to the application that you want to edit and select **Edit**.
- Step 6** Change the desired settings for the custom application:
- **Name**—Application name. This value cannot be changed.
  - **Description**—Description of application.
  - **Helper Text**—Descriptive content for application from the API.
  - **Category**—Category for the application.

- **Protocol**—Supported protocol for application.
- **Port**—Supported port for the application.

**Step 7** Click **Save Application**.

**Step 8** To change the business-relevancy group of the custom application, click the business-relevancy group drop-down list next to the custom application and choose the group that you want to assign to the application. Valid options are **Business Relevant**, **Default**, and **Business Irrelevant**. For more information about these options, see [Business-Relevance Groups, on page 74](#).

**Step 9** (Optional) If desired, continue configuring the policy or deploy these changes to the devices by clicking **Reapply Policy**.

---

## Enabling 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 76](#).



### Note

Each policy tag can have only one QoS policy assigned to it. You cannot assign more than one QoS policy to a policy tag

---

### 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 for Wired Devices, on page 83](#).

### Procedure

---

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

**Step 2** From the **Policy Scopes** pane, select the desired policy tag.

**Step 3** In the **Dynamic QoS** field (below the **Policy Scopes** pane), click **Enabled** to configure a dynamic policy.

**Step 4** To apply these configuration changes to the devices, click **Reapply Policy**.

---

## Viewing Dynamic Policies

You can view the dynamic policies that you have created.

### 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** From the **Policy Scopes** pane, select the desired policy tag.
- Step 3** Below the **Dynamic QoS** field, click **View Dynamic Policy**.  
The following information is displayed about the dynamic policies:

- **Status**—State of the dynamic policy for the flow. Valid states are as follows:
    - 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.
-





## Performing Path Traces

- [About Path Trace, page 93](#)
- [Performing a Path Trace, page 105](#)
- [Collecting QoS and Interface Statistics in a Path Trace, page 107](#)

### 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 and QoS 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.

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

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

- EIGRP
- Level 3 Recursive Loop

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

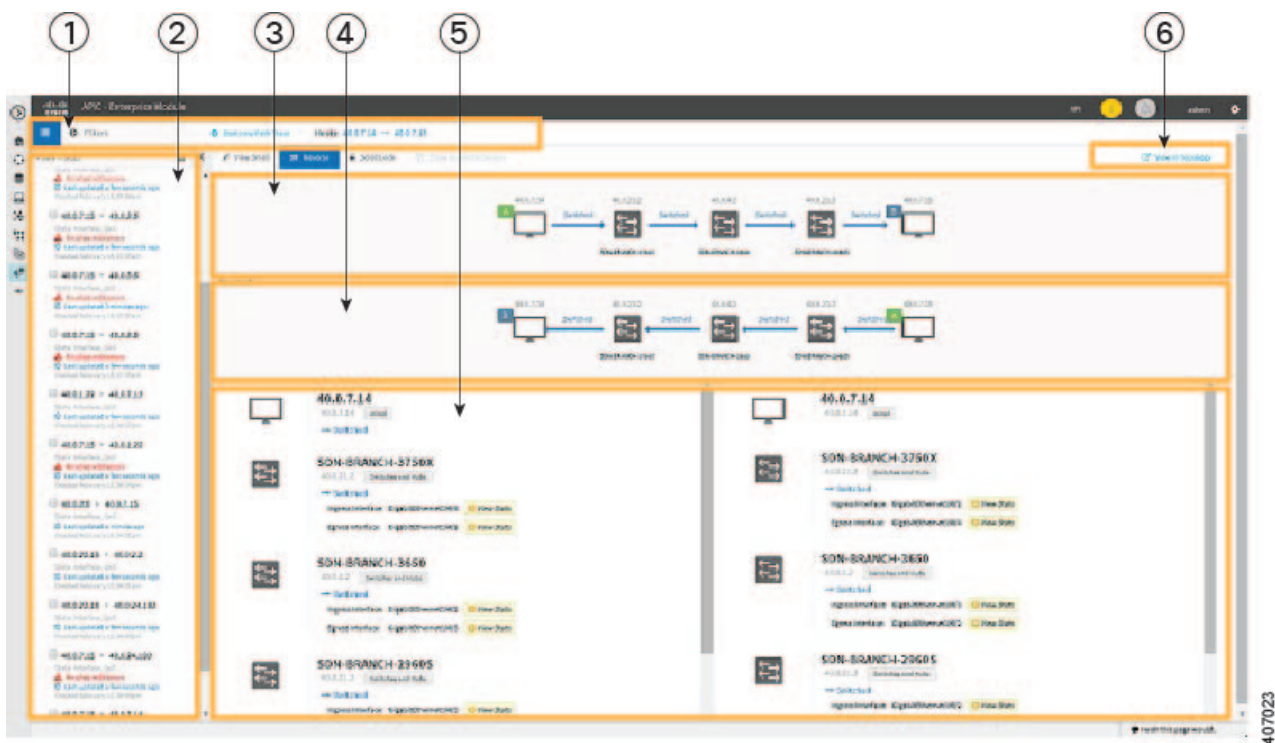


#### Note

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

To access the **Path Trace** window, from the Navigation pane, click **Path Trace**.

Figure 6: Path Trace Window





Callout Number	Name	Description
1	<b>Toolbar</b>	<p>Provides the following functions:</p> <ul style="list-style-type: none"> <li>• <b>Path Traces List</b> icon—Toggles the display of the list of completed path traces. You can delete path traces that you no longer need by placing your cursor over the path trace and clicking the <b>Trash Can</b> icon.</li> <li>• <b>Filters</b>—Allows you to search for devices by source or destination IP address.</li> <li>• <b>Start new Path Trace</b>—Displays a dialog box for you to specify the parameters of the path trace and then start the trace.</li> </ul> <p>You must enter the source and destination IP address for the path trace. Optionally, you can specify whether to refresh the path trace every 30 seconds and whether to collect QoS and interface statistics. Additional options allow you to specify the source and destination ports and the protocol (TCP or UDP).</p> <ul style="list-style-type: none"> <li>• <b>Hosts</b>—Displays the IP addresses of the source and destination devices for the current path trace.</li> </ul>
2	<b>In-progress, Active, and Completed Path Traces</b>	In-progress path traces are those that have not completed yet. Active path traces are completed and being updated once every 30 seconds. Completed path traces are calculated once and are not updated.
3	<b>Trace Results Graphical Display</b>	Displays the results of the path trace. For information, see <a href="#">Understanding Path Trace Results, on page 100</a> .
4	<b>Reversed Results Graphical Display</b>	Shows the path trace in reverse order, from the destination host to the source host. For information, see <a href="#">Understanding Path Trace Results, on page 100</a> .
5	<b>Trace Results Device Details</b>	Provides detailed information about the devices along the path. For information, see <a href="#">Understanding Path Trace Results, on page 100</a> .
6	<b>View in Topology</b> button	Displays the trace results in the <b>Topology</b> window.

## Path Trace Support

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

- Campus/data center to campus/data center

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

**Note**

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

## Path Trace Protocols and Network Connections

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

**Note**

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

**Table 22: Path Trace Supported Device Protocols and Network Connections**

Supported Device Protocols and Network Connections	Description
Border Gateway Protocol (BGP)	<p>When BGP is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking.</p> <p>The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.</p>
Equal Cost Multi Path (ECMP)	<p>When an ECMP routing strategy is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking.</p> <p>The data used for this path trace calculation is obtained through an on-demand query made through the network device at the time the path calculation request is made.</p> <p><b>Note</b> The controller's GUI will display when ECMP is used between devices in a path trace segment.</p>

Supported Device Protocols and Network Connections	Description
Hot Standby Router Protocol (HSRP)	<p>When HSRP is used in a network, the controller automatically looks up the HSRP active router for a given segment and calculates the path appropriately for a path trace.</p> <p>The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.</p>
Intermediate System-to-Intermediate System (IS-IS) Protocol	<p>When IS-IS is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking.</p> <p>The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.</p>
Layer 3 Forwarding Interface	<p>The controller can perform path traces between two Layer 3 forwarding interfaces or between a Layer 3 forwarding interface and a host.</p>
MPLS-VPN (WAN)	<p>The controller provides path trace support for a branch-to-branch connected and provider-managed MPLS-VPN service. Supported devices for this type of path trace include:</p> <ul style="list-style-type: none"> <li>• Cisco ASR 1000 Series Aggregation Services Router</li> <li>• Cisco ASR 9000 Series Aggregation Services Router</li> <li>• Cisco Integrated Services Routers (ISR) G2</li> </ul> <p>All customer edge (CE) routers should have NetFlow enabled with traffic running between the hosts and routers.</p> <p><b>Note</b> The above supported devices will be tagged as <b>Border Routers</b> for their <b>Device Role</b> in the <b>Device Inventory</b>. You must keep the above supported devices tagged as <b>Border Routers</b> when performing a path trace.</p> <p>The data used for this path trace calculation is obtained through an on-demand query made through the network device at the time the path calculation request is made.</p>

Supported Device Protocols and Network Connections	Description
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>
Virtual connectivity—Layer 2 Port Channel	<p>When virtual connectivity (Layer 2 port channel) is used within a network, the path trace for a given application flow is displayed. The path trace over virtual interfaces (port channels) is displayed, so that the user can visualize an end-to-end path for an application.</p>
Virtual connectivity—VLAN/SVI	<p>When virtual connectivity (VLAN/SVI) is used within a network, the path trace for a given application flow is displayed. The path trace is displayed, so that the user can visualize an end-to-end path for an application.</p> <p>The data used for this path calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.</p>

Supported Device Protocols and Network Connections	Description
Wireless	<p>The controller provides path trace support for Control and Provisioning of Wireless Access Points (CAPWAP), 802.11, and mobility.</p> <p>When wireless network elements are used, the path trace for a given application flow is displayed. The user knows the exact path a particular application is taking.</p> <p><b>Note</b> The controller's GUI will display CAPWAP and mobility tunneling (for roaming) when either is discovered during a path trace. The data used for this path calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.</p>
Equal Cost Multipath/Trace Route (ECMP/TR)	<p>When ECMP/TR is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking.</p> <p>The data used for this path trace calculation is obtained on demand by polling the device. When performing a path trace on ECMP, Cisco Express Forwarding (CEF) lookup is performed on the device on demand for requested tuples. When a path trace detects a number of unknown or unmanaged devices in the path, the path trace is executed on demand from the last known or managed Cisco device and the path calculation is restarted from the first known or managed Cisco device in the trace route result. The unknown or unmanaged hops discovered using path trace are added to the path as unknown devices along with their IP addresses.</p>
Netflow	<p>When Netflow is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking.</p> <p>When we have multiple border routers in the destination island, the Netflow cache from the devices are used to find the actual ingress border router. The Netflow record is matched from these devices on demand for a given tuple. It is essential to configure Netflow on the border routers. If Netflow is not configured, trace route is used to find the ingress interfaces, which might not be accurate.</p>

Supported Device Protocols and Network Connections	Description
Sub interfaces	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.
Enhanced Interior Gateway Routing Protocol (EIGRP)	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.  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.
Layer 3 Recursive Lookup	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.  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.

## Understanding Path Trace Results

After you run a path trace, the results are displayed in the **Trace Results Graphical Display** pane.

### 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 Graphical Display

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

**Table 23: Trace Results Toolbar**

Name <sup>1</sup>	Description
<b>View Small</b>	Minimizes the trace results to view the details better.
<b>Show Reverse</b>	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.
<b>Scroll Lock</b>	Locks the scrolling of the path trace and reverse path trace details windows. (Available when <b>Show Reverse</b> is enabled.)
<b>Show Duplicate Devices</b>	Displays or hides duplicate devices within a path trace.
<b>View in Topology</b>	Opens the <b>Topology</b> window and highlights the path trace results in your network topology. For more information about using the Topology window, see <a href="#">About Topology</a> , on page 53.

<sup>1</sup> Depending on the trace results, some of these items on the toolbar might be unavailable.

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

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

**Note**

Clicking an individual device in the path trace highlights the device in the **Trace Results Device Details** area.

**Trace Results Device Details**

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

**Table 24: Trace Results Device Details**

Name	Description
<b>IP</b>	IP address of the device.

Name	Description
Type	Wired or wireless device (access point, switch, or router).
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"> <li>• <b>BGP</b>—Link is based on the BGP routes configured on the source device.</li> <li>• <b>ECMP</b>—Link is based on a Cisco Express Forwarding (CEF) load balancing decision.</li> <li>• <b>EIGRP</b>—Link is based on EIGRP routes configured on the source device.</li> <li>• <b>Connected</b>—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).</li> <li>• <b>InterVlan Routing</b>—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.</li> <li>• <b>ISIS</b>—Link is based upon the IS-IS routes configured on the source device.</li> <li>• <b>NetFlow</b>—Link is based on NetFlow records collected on the source device.</li> <li>• <b>OSPF</b>—Link is based on the OSPF routes configured on the source device.</li> <li>• <b>Static</b>—Link is based on a static route configured on the source device.</li> <li>• <b>Switched</b>—Link is based on Layer 2 VLAN forwarding.</li> <li>• <b>Trace Route</b>—Link is based on trace route.</li> <li>• <b>Wired</b>—The source device is wired to the destination device.</li> <li>• <b>Wireless</b>—The source device is a wireless host connected to the destination device (access point).</li> </ul>
Tunnels	<p>CAPWAP data (wireless) or mobility tunneling</p> <p><b>Note</b> 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>



Name	Description
<b>Ingress interface</b>	<p>Ingress interface of the device for the path trace (physical or virtual).</p> <p>For example, a physical ingress interface is <b>GigabitEthernet1/0/1</b> and a virtual ingress interface is <b>GigabitEthernet1/3 [Vlan1]</b>.</p> <p>If statistics were gathered for this path trace, clicking the <b>View Stats</b> button displays the interface or QoS statistics. For information, see <a href="#">Understanding the Interface Statistics Retrieved During a Path Trace, on page 103</a> or <a href="#">Understanding the QoS Statistics Retrieved During a Path Trace, on page 105</a>.</p>
<b>Egress interface</b>	<p>Egress interface of the device for the path trace (physical or virtual).</p> <p>For example, a physical interface is <b>GigabitEthernet1/0/2</b> and a virtual ingress interface is <b>GigabitEthernet1/4 [Vlan2]</b>.</p> <p>If statistics were gathered for this path trace, clicking the <b>View Stats</b> button displays the interface or QoS statistics. For information, see <a href="#">Understanding the Interface Statistics Retrieved During a Path Trace, on page 103</a> or <a href="#">Understanding the QoS Statistics Retrieved During a Path Trace, on page 105</a>.</p>
<b>Accuracy note</b>	<p>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.</p> <p>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.</p>

## Understanding the Interface Statistics Retrieved During a Path Trace

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.

**Table 25: Interface Statistics by Policy**

Parameter	Description
<b>Admin Status</b>	<p>Administrative status of the interface:</p> <ul style="list-style-type: none"> <li>• <b>Up</b>—Interface has been enabled through the CLI.</li> <li>• <b>Down</b>—Interface has been disabled through the CLI.</li> </ul>
<b>Input Packets</b>	Number of packets being received on the interface.

Parameter	Description
<b>Input Queue Drops</b>	Number of packets dropped from the input queue due to the queue reaching its maximum threshold.
<b>Input Queue Max Depth</b>	Maximum number of packets that the input queue can hold before it must start dropping packets.
<b>Input Queue Count</b>	Number of packets in the input queue.
<b>Input Queue Flushes</b>	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.
<b>Input Rate (bps)</b>	Number of bits per second at which packets are entering the interface.
<b>Operational Status</b>	Operational status of the interface: <ul style="list-style-type: none"> <li>• <b>Up</b>—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.</li> <li>• <b>Down</b>—Interface cannot transmit or receive (data) traffic.</li> </ul>
<b>Output Drop</b>	Number of packets dropped from the output queue due to the queue reaching its maximum threshold.
<b>Output Packets</b>	Number of packets leaving the interface.
<b>Output Queue Count</b>	Number of packets in the output queue.
<b>Output Queue Depth</b>	Maximum number of packets that the output queue can hold before it must start dropping packets.
<b>Output Rate (bps)</b>	Number of bits per second at which packets are leaving the interface.
<b>Refreshed At</b>	Date and time that the current statistics were gathered.

## Understanding the QoS Statistics Retrieved During a Path Trace

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.

**Table 26: 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.

## 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.  
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 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** (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 Stats**—Collects and displays information about quality of service.
  - **Interface Stats**—Collects and displays information about the interfaces on the devices along the path.
- Step 11** Click **Start Trace**.  
Review the path trace output. For more information, see [Understanding Path Trace Results, on page 100](#).
- Step 12** To view the path trace in the **Topology** window. Click **View in Topology**.  
The **Topology** window opens with the path trace highlighted in your network. For more information about the **Topology** window, see [About Topology, on page 53](#).
- 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 QoS and Interface Statistics in a Path Trace

You can perform a path trace between two nodes in your network and collect interface and/or QoS statistics about the devices in the path.

**Note**

The path trace application may display accuracy notes. Accuracy notes are red boxes that appear 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.  
To list the Layer 3 forwarding interfaces for a device, enter the device name or IP address followed by a colon ":". All interfaces with IP addresses on the device are displayed.
- Step 4** In the **Destination** field, enter the IP address of the host or Layer 3 forwarding interface where you want the trace to end.  
To list the Layer 3 forwarding interfaces for a device, enter the device name or IP address followed by a colon ":". All interfaces with IP addresses on the device are displayed.
- Step 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 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 one or both of the following check boxes:
  - **QoS Stats**
  - **Interface Stats**
- Step 12** Click **Start Trace**.  
The results are displayed in the **Trace Results Device Details** pane. For information, see [Understanding the Interface Statistics Retrieved During a Path Trace, on page 103](#) and [Understanding the QoS Statistics Retrieved During a Path Trace, on page 105](#).

**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 53](#).

---

### What to Do Next

Review the path trace output. For information, see [Understanding the Interface Statistics Retrieved During a Path Trace, on page 103](#) and [Understanding the QoS Statistics Retrieved During a Path Trace, on page 105](#).



## Reviewing the API Documentation

- [About the Cisco APIC-EM API Documentation](#), page 109
- [Using the Cisco APIC-EM REST API Window](#), page 112

### 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.

---

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 112](#).

### Related Topics

- [Reviewing and Testing the Cisco APIC-EM APIs](#)
- [Common External RESTful Services HTTP Response Codes, on page 111](#)



## Supported HTTPS Methods and General Structure

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

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

## 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 27: 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 28: 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 29: 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 109](#)

## 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.
- Step 4** Click **Expand Operations**.
- 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.
- 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.





## INDEX

### A

administrator [12](#)  
API [4](#)  
API documentation [109](#)  
audience [vii](#)  
authentication [14](#)  
authorization [14](#)

### B

Border Gateway Protocol (BGP) [96](#)

### C

change password [4](#)  
Cisco APIC-EM [3](#)  
    overview [3](#)  
Cisco Network Plug and Play [4](#)

### D

device inventory [4](#), [35](#)  
    Average Update Frequency [35](#)  
    Configuration [35](#)  
    Device Family [35](#)  
    Device Name [35](#)  
    Device role [35](#)  
    device status [35](#)  
    Device Tag [35](#)  
    IOS [35](#)  
    IP Address [35](#)  
    Last Updated Time [35](#)  
    Location [35](#)  
    MAC Address [35](#)  
    Platform [35](#)  
    Policy Tag [35](#)  
    Serial number [35](#)

device inventory (*continued*)

    Up Time [35](#)  
    window [35](#)  
device role [43](#), [65](#)  
devices table [35](#), [42](#), [43](#)  
    changing view [43](#)  
    filtering [42](#)  
discovery [4](#), [22](#), [26](#), [29](#)  
    devices [22](#)  
    using CDP [26](#)  
    using IP address range [29](#)  
discovery credentials caveats [25](#)  
discovery results [23](#)

### E

Equal Cost Multi Path (ECMP) [96](#)

### F

feedback [4](#)

### G

GUI overview [4](#)

### H

host inventory [4](#), [50](#)  
    window [50](#)  
Hosts table [50](#), [51](#)  
    changing view [51](#)  
    filters [50](#)  
Hot Standby Router Protocol (HSRP) [96](#)  
HTTPS methods [111](#)

**I**

installer [13](#)  
 Intermediate System-to-Intermediate System, See [IS-IS](#)  
 inventory [35, 50](#)  
     device [35](#)  
     host [50](#)  
 IS-IS [54, 96](#)  
     path trace [96](#)  
     topology [54](#)  
 IWAN [4](#)

**L**

location marker [48](#)  
     adding [48](#)  
 location tag [47](#)

**N**

northbound REST API documentation [112](#)  
 northbound REST APIs [109](#)  
 notifications [4](#)  
 Notifications [4](#)  
     system [4](#)

**O**

observer [13](#)  
 Open Shortest Path First Protocol (OSPF) [96](#)  
 OSPF [54](#)

**P**

Packet over SONET (PoS) [96](#)  
 path trace [93, 95, 105](#)  
 Path Trace [96](#)  
     protocols [96](#)  
 plug and play [4](#)  
 port channel [96](#)

**Q**

QoS application [73, 88](#)  
     predefined priority class [73](#)  
 Quality of Service [71](#)

**R**

RBAC [11, 16](#)  
     accounting [16](#)  
 related documentation [ix](#)  
 role [12, 13](#)  
     administrator [12](#)  
     observer [13](#)

**S**

Settings [4](#)  
 sign out [4](#)  
 Spanning Tree Protocol (STP) [96](#)  
 static routing [96](#)  
 Static-Route [54](#)

**T**

tag [45, 49](#)  
     adding [45](#)  
     deleting [49](#)  
     removing [45](#)  
 topology [4, 54, 57, 60, 61, 62, 65, 66, 68](#)  
     aggregate [60](#)  
     configuring structure [62](#)  
     device role [65](#)  
     disaggregate [60, 61](#)  
     icons [57](#)  
     L2 [54](#)  
     L3 [54](#)  
     searches [66](#)  
     tags [68](#)  
     toolbar [54](#)  
     VRF [54](#)  
 Topology [64](#)  
     saving [64](#)

**U**

user [14, 16, 18, 19, 20](#)  
     access [20](#)  
     adding [18](#)  
     delete [18](#)  
     password [16](#)  
     permissions [14](#)  
     roles [14](#)  
     viewing user information [19](#)  
 users and domains [14](#)