Cisco EasyQoS Application for APIC-EM User Guide, Release 1.5.0.x

First Published: 2016-03-24

Last Modified: 2017-06-23

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

CONTENTS

Audience

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

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

Document Conventions

This documentation uses the following conventions:

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

Command syntax descriptions use the following conventions:

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

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

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

Examples use the following conventions:

Convention	Description
`screen`	Examples of information displayed on the screen are set in Courier font.
`bold screen`	Examples of text that you must enter are set in Courier bold font.
< >	Angle brackets enclose text that is not printed to the screen, such as passwords.
!	An exclamation point at the beginning of a line indicates a comment line. (Exclamation points are also displayed by the Cisco IOS XE software for certain processes.)
[ ]	Square brackets enclose default responses to system prompts.

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

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

Related Documentation

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

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

- Cisco APIC-EM Documentation:
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Release Notes*
  - *Cisco APIC-EM Quick Start Guide* (directly accessible from the controller's GUI)
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Upgrade Guide*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*
  - *Open Source Used In Cisco APIC-EM*
- Cisco Network Visibility Application for the Cisco APIC-EM
  - *Cisco Network Visibility Application for APIC-EM Release Notes*
  - *Cisco Network Visibility Application for APIC-EM Supported Platforms*
  - *Cisco Network Visibility Application for APIC-EM User Guide*
- Cisco Path Trace Application for Cisco APIC-EM
  - *Cisco Path Trace Application for APIC-EM Release Notes*
  - *Cisco Path Trace Application for APIC-EM Supported Platforms*
  - *Cisco Path Trace Application for APIC-EM User Guide*
- Cisco EasyQoS Application for Cisco APIC-EM
  - *Cisco EasyQoS Application for APIC-EM Release Notes*
  - *Cisco EasyQoS Application for APIC-EM Supported Platforms*

- *Cisco EasyQoS Application for APIC-EM User Guide*

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

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

- Cisco Active Advisor Documentation for the Cisco APIC-EM:
  - *Cisco Active Advisor for APIC-EM Release Notes*

- Cisco SD-Bonjour Documentation for the Cisco APIC-EM:
  - *Cisco SD-Bonjour Application for APIC-EM Release Notes*

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

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

Obtaining Documentation and Submitting a Service Request

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

CHAPTER 1

New and Changed Information

New and Changed Information

The table below summarizes the new and changed EasyQoS Release 1.5.0.x features that are included in this document. For information about all of the features in EasyQoS Release 1.5.0.x, see the Release Notes. For the latest caveats, see the Bug Search Tool at https://tools.cisco.com/bugsearch/.

Feature	Description	Where Documented
Traffic class modification.	Cisco EasyQoS now supports the modification of standard traffic classes for NBAR apps. Previously, only custom applications supported this feature.	See Modifying Traffic Class in an Application, on page 29
Excluding interfaces from QoS policies.	Cisco EasyQoS now permits individual device interfaces to be excluded from QoS policy provisioning.	See Creating or Editing a Policy, on page 36
Configuring DSCP for traffic classes.	Cisco EasyQoS now permits the user to change the DSCP value for each traffic class per scope/policy.	See Configuring Queuing Profiles, on page 47.
Monitoring and troubleshooting functionality.	Cisco EasyQoS now supports a monitoring and troubleshooting beta functionality in the EasyQoS app.	See Enabling Monitoring for EasyQoS, on page 59.
Fastlane QoS feature.	Support for the Fastlane QoS feature on wireless LAN controllers (WLCs).	See Configuring an Apple Fastlane Solution using APIC-EM, on page 70.

New and Changed Information

CHAPTER 2

Overview

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

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

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

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

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

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

Table 1: Cisco APIC Enterprise Module Features and Benefits

Feature	Description
Network Information Database	The Cisco APIC-EM periodically scans the network to create a "single source of truth" for IT. This inventory includes all network devices, along with an abstraction for the entire enterprise network.
Network topology visualization	The Cisco APIC-EM automatically discovers and maps network devices to a physical topology with detailed device-level data. The topology of devices and links can also be presented on a geographical map. You can use this interactive feature to troubleshoot your network.
EasyQoS application	The EasyQoS application abstracts away the complexity of deploying Quality of Service across a heterogeneous network. It presents users with a workflow that allows them to think of QoS in terms of business intent policies that are then translated by Cisco APIC-EM into a device centric configuration.
Cisco Network Plug and Play (PnP) application	The Cisco Network PnP application is one of the components in the Cisco Network PnP solution. The Cisco Network PnP solution extends across Cisco's enterprise portfolio. It provides a highly secure, scalable, seamless, and unified zero-touch deployment experience for customers across Cisco routers, switches and wireless access points.
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.
Cisco Active Advisor	The Cisco Active Advisor application for APIC-EM offers personalized life cycle management for your network devices by keeping you up-to-date on: • End-of-life milestones for hardware and software • Product advisories, including Product Security Incident Response Team (PSIRT) bulletins and field notices • Warranty and service contract status
Cisco SD-Bonjour	The Cisco SD-Bonjour application provides controller functions in the network. It enables discovery and distribution of policy-based Cisco SD-Bonjour services, independent of network boundaries.

Feature	Description
Cisco Integrity Verification	The Cisco Integrity Verification (IV) application provides automated and continuous monitoring of network devices, noting any unexpected or invalid results that may indicate compromise. The objective of the Cisco IV application is early detection of the compromise, so as to reduce its impact. The Cisco IV application operates within the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) as a beta version for this release.
Cisco Remote Troubleshooter	The Cisco Remote Troubleshooter application uses the Cisco IronPort infrastructure to create a tunnel that enables a support engineer to connect to an APIC-EM cluster and troubleshoot issues with your system. The app uses outbound SSH to create a secure connection to the cluster through this tunnel. As an administrator, you can use the Remote Troubleshooter application to control when a support engineer has access to a particular cluster and for how long (since a support engineer cannot establish a secure tunnel on their own). You will receive indication that a support engineer establishes a remote access session, and you can end a session at any time by disabling the tunnel they are using.
Public Key Infrastructure (PKI) server	The Cisco APIC-EM provides an integrated PKI service that acts as Certificate Authority (CA) or sub-CA to automate X.509 SSL certificate lifecycle management. Applications, such as IWAN and PnP, use the capabilities of the embedded PKI service for automatic SSL certificate management.
Path Trace application	The path trace application helps to solve network problems by automating the inspection and interrogation of the flow taken by a business application in the network.
High Availability (HA)	HA is provided in N+ 1 redundancy mode with full data persistence for HA and Scale. All the nodes work in Active-Active mode for optimal performance and load sharing.
Back Up and Restore	The Cisco APIC-EM supports complete back up and restore of the entire database from the controller GUI.
Audit Logs	The audit log captures user and network activity for the Cisco APIC-EM applications.

About EasyQoS

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

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

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

Note To configure QoS on the devices in your network, you must be assigned either administrative permissions (ADMIN_ROLE) or policy administrator permissions (POLICY_ADMIN_ROLE).

Understanding Policy Scope

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

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

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

You define policy scopes from the **EasyQoS** window or by applying policy tags to devices in the **Device Inventory** or **Topology** windows. For more information, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

Understanding Applications

EasyQoS supports all of the applications in the Cisco Next Generation Network-Based Application Recognition (NBAR2) library. 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 10.

The NBAR2 applications are pre-allocated into the industry standard-based traffic classes, as defined in RFC 4594. The traffic classes define the treatments (such as DSCP marking, queuing and dropping) that are applied to an application's traffic. You can change an application's traffic class, as well as the business-relevance of an application when you configure QoS policies. For information, see Understanding QoS Policies, on page 13.

Business-Relevance Groups

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

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

Unidirectional and Bidirectional Application Traffic

Some applications are completely symmetrical and require identical bandwidth provisioning on both ends of the connection. Traffic for such applications is described as bidirectional. For example, if 100 kbps of LLQ are assigned to voice in one direction, 100 kbps of LLQ also must be provisioned for voice in the opposite direction (assuming that the same VoIP codecs are being used in both directions, and putting aside for a moment multicast Music-on-Hold [MoH] provisioning). However, certain applications, such as Streaming-Video and multicast MoH, are most often unidirectional. Therefore, it might be unnecessary and even inefficient to provision any bandwidth guarantees for such traffic on a branch router for the branch-to-campus direction of traffic flow.

EasyQoS allows you to specify whether an application is unidirectional or bidirectional for a particular policy.

On switches and wireless controllers, NBAR2 and custom applications are unidirectional by default. However, on routers, because only NBAR applications are supported, NBAR2 applications are bidirectional by default.

Consumers and Producers

You can configure relationships between applications such that when traffic from one application is sent to another application (thus creating a specific a-to-b traffic flow), the traffic is handled in a specific way. The applications in this relationship are called procucers and consumers and are defined as follows:

Producer—Sender of the application traffic. For example, in a client/server architecture, the application-server would be considered the producer, as the traffic primarily flows in the server-to-client direction. In the case of a peer-to-peer application, the remote peer is considered the producer.

Consumer—Receiver of the application traffic. The consumer may be a client endpoint in a client/server architecture or it may be the local device in a peer-to-peer application. Consumers may be endpoint devices but may, at times, be specific users of such devices (typically identified by IP Addresses and/or specific subnets). There may also be times when an application is the consumer of another application's traffic flows.

Setting up this relationship allows you to configure specific service levels for traffic matching this scenario.

Marking, Queuing, and Dropping Treatments

Cisco EasyQoS bases its marking, queuing, and dropping treatments on RFC 4594 and the business relevancy category that you have assigned to the application. EasyQoS assigns all of the applications in the Default category to the Default Forwarding application class and all of the applications in the Irrelevant Business category to the Scavenger application class. For applications in the Relevant Business category, EasyQoS assigns traffic classes to applications based on the type of application. See the table below for a list of application classes and their treatments.

Table 2: Marking, Queuing, and Dropping Treatments

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

Business Relevance	Application Class	Per-Hop Behavior	Queuing and Dropping	Application Description
	Transactional Data (Low-Latency Data)	AF21	BW Queue and DSCP WRED	Interactive (foreground) data applications, such as enterprise resource planning (ERP), customer relationship management (CRM), and other database applications.
	Bulk Data (High-Throughput Data)	AF11	BW Queue and DSCP WRED	Non-interactive (background) data applications, such as E-mail, file transfer protocol (FTP), and backup applications.
Default	Default Forwarding (Best Effort)	DF	Default Queue and RED	Default applications and applications assigned to the default business-relevant group. Because only a small minority of applications are assigned to priority, guaranteed-bandwidth, or even to deferential service classes, the vast majority of applications continue to default to this best-effort service. This default class should be adequately provisioned (a minimum bandwidth recommendation, for this class is 25%).
Irrelevant	Scavenger	CS1	Minimum BW Queue (Deferential) and DSCP	Non-business related traffic flows and applications assigned to the business-irrelevant group, such as data or media applications that are entertainment-oriented. Examples include YouTube, Netflix, iTunes, and Xbox Live.

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

Custom Applications

Custom applications are applications that you add to the EasyQoS NBAR2 application library. You can define URL-based applications and server IP address-based applications.

When you define an application according to its server IP address, you can also define a Differentiated Services Code Point (DSCP) value and port classification.

To simplify the configuration process, if you know of an application that has similar traffic and service level needs, you can define a similar application. EasyQoS copies the other application's traffic class, category, and subcategory settings to the application that you are defining.

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

If you are using the IWAN application, and you create a custom application that IWAN does not support, EasyQoS displays a warning, and the new custom application is not visible from the IWAN application.

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

Favorite Applications

Cisco APIC-EM allows you to flag applications that you want EasyQoS to configure on devices before all other applications, except custom applications. Flagging an application as a favorite helps to ensure that the QoS policies for your favorite applications get configured on devices. For more information, see Processing Order for Devices with Limited Resources, on page 11

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

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

Keep in mind that not only business-relevant applications may be flagged as favorites, but even business-irrelevant applications may be flagged as such. For example, if an administrator notices a lot of unwanted Netflix traffic on his network, he may chose 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.

Processing Order for Devices with Limited Resources

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

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

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

3 **Popularity—**Number (1–10) that is based on Cisco Validated Design (CVD) criteria. The popularity number cannot be changed. An application with a popularity of 10 has a higher priority than an application with a popularity of 9, and so on.

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

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

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

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

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

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

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

Understanding QoS Policies

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

- **Policy Scope—**Group of devices that will be configured with a 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 1300 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.
- **Business-relevance—**Attribute that classifies a given application according to how relevant it is to your business and operations. The attributes are business relevant, default, and business irrelevant. For information, see Business-Relevance Groups, on page 7 .

  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

Static and Dynamic QoS Policies

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

- **Static policies—**Deployed to devices and in effect until you change or remove them. Static policies comprise the majority of the deployments.

- **Dynamic policies—**Used on LAN interfaces only. Dynamic policies are applied to the relevant network devices for the duration of an event, for example, during a voice or video call. When the call ends, the policy is removed from the device. For more information, see Understanding Queuing Profiles, on page 18.

Policy Preview

You can preview the command line interface (CLI) commands that EasyQoS will send to a device when you apply the policy. At any time, for example, after a policy change, you can generate the specific commands for a specified device. After reviewing the commands, you can apply the policy to all of the devices in the scope, or you can continue to make changes to the policy.

Policy Scheduling

After you create or change a policy, you need to apply or reapply the policy to the devices associated with it. When you click **Apply** or **Reapply**, EasyQoS gives you the option to apply (or reapply) the policy immediately or at a specific date and time, for example, on a weekend during off-peak hours. You can schedule a policy deployment for wired or wireless devices.

After you've scheduled a policy to be deployed, the policy and policy scope are locked. You can view the policy, but you cannot edit it. If you change your mind about deploying the policy, you can cancel it up until the time that it is deployed. Once deployment begins, you cannot cancel it.

Policy Versioning

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

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

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

Original Policy Restore

The first time that you apply an EasyQoS policy configuration to devices, EasyQoS detaches the device's original MQC policies (leaving the MQC policy configurations on the device) and stores the device's original NBAR configurations on the Cisco APIC-EM controller. This action allows you to restore the original MQC policies and NBAR configuration onto the devices later, if needed.

Note Because the MQC policies are detached and not deleted from the device conifguration, if you remove these policies, you will not be able to restore them using the EasyQoS original policy restore feature.

When you restore the original policy configuration onto a device, EasyQoS removes the existing EasyQoS policy configuration that you applied to the devices and reverts to the original configuration that was on the device before you applied any EasyQoS policy configurations.

Any marking and queuing (MQC) policy configurations that existed before any EasyQoS policies were configured are reattached to the interfaces. Queuing policies (MLS configurations) are not restored; instead, the devices retain the MLS configurations that were last applied through EasyQoS.

After you restore the original policy configuration to the device, the EasyQoS policy is deleted from the Cisco APIC-EM, and the status of the devices shows **Policy Restored**. The devices are counted in **WIRED NEW DEVICES** after successful restore, **WIRED FAILED** if unsuccessful.

Note the following additional guidelines and limitations for this feature:

- Original policy restore does not work for policies that were created and applied to devices using the Cisco APIC-EM Release 1.2.x or below, because the Cisco APIC-EM did not store devices' original policy configurations before Cisco APIC-EM Release 1.3.x
- If the first attempt to push an EasyQoS policy to a device fails, EasyQoS automatically attempts to restore the original policy configurations onto the devices.

Understanding Service Provider Profiles

Service provider profiles define the Differentiated Services Code Point (DSCP), priority, and bandwidth for traffic that is destined for a service provider. Cisco APIC-EM provides four predefined service provider profiles (SPPs or SP profiles): SPP1, SPP2, SPP3, and SPP4. (See tables below.)

You can use any of the predefined SP profiles, or you can create a customized SP profile for your unique requirements. Creating a customized SP profiles allows you to define the DSCP value and bandwidth for each traffic class in the profile. You can define 4-class, 5-class, 6-class, and 8-class models. To create a customized SP profile, see Creating a Customized Service Provider Profile, on page 49.

After you determine and create, if necessary, the service model that you want to use, you need to configure it on the WAN interfaces. To configure WAN interfaces, see WAN Interface Configuration for EasyQoS, on page 23.

Table 3: SP Profile 1 (SPP1): 4-Class Model

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

Table 4: SP Profile 2 (SPP2): 5-Class Model

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Voice	EF	Yes	10	—
Class 1 Data	AF31	—	—	44
Class 2 Data	AF21	—	—	25
Class 3 Data	AF11	—	—	1
Default	Best Effort	—	—	30

Table 5: 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 6: 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

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Scavenger	CS1	—	—	1
Interactive Video	AF41	—	—	30
Voice	EF	Yes	10	—
Default	0	—	—	25
Critical Data	AF21	—	—	25

Understanding Bandwidth Profiles

Bandwidth profiles allow you to define an interface's bandwidth allocation based on the interface speed and the traffic class.

Note Bandwidth profiles do not apply to wireless policies or service provider interfaces.

The following interface speeds are supported:

- 100 Gbps
- 10/40 Gbps
- 1 Gbps
- 100 Mbps
- 10 Mbps
- 1 Mbps

If the speed of an interface falls between two interface speeds, Cisco EasyQoS treats the interface as the lower interface speed.

Note EasyQoS tries to determine the switch port's operational speed as best it can, in order to apply the correct policy, based on the interface speed. However, in situations where the switch port is administratively down, EasyQoS has to rely on the interfaces supported speed, since the port is currently not operational.

After you define a bandwidth policy, you assign it to a QoS policy. When you apply (or reapply) the QoS policy, the devices in the policy scope are configured with the assigned bandwidth policy. If no bandwidth policy is assigned, the QoS policy uses the default, Cisco Validated Design (CVD) bandwidth policy.

If you change a bandwidth policy that is already assigned to a QoS policy, the QoS policy changes to a stale state. You need to reapply the QoS policy to deploy the changes to the bandwidth policy.

Table 7: Default CVD Bandwidth Policy

Traffic Class	Default Bandwidth (Total = 100%) [4]
Voice	10%
Broadcast Video	10%
Real-Time Interactive	13%
Multimedia Conferencing	10%
Network control	3%
Signaling	2%
OAM	2%
Transactional Data	10%
Bulk Data	4%
Scavenger	1%
Best Effort	25%

4 We recommend that the total bandwidth for Voice, Broadcast Video, and Real-Time Interactive traffic classes equals no more than 33%.

Understanding Queuing Profiles

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

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

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

As dynamic policies are applied to interfaces, the **Dynamic QoS** window is updated with information about the policy status (whether the configuration was added successfully or not), source IP address and port, destination IP address and port, flow type (for example, voice or video), and protocol used. In addition, you

have the capability to run a path trace on a specific flow. This capability is particularly useful if a policy fails to be successfully applied to an interface. In this case, you can quickly troubleshoot the failure by viewing the path trace of the flow.

In some situations, an external host that integrates with APIC-EM might not be able to provide the destination IP address or port number in its traffic flow. To mitigate this limitation, EasyQoS retrieves the application name (if provided) from the traffic flow and uses it to obtain the missing destination IP address or port number from the EasyQoS application registry. EasyQoS then applies the destination IP address or port number to the traffic flow. If an application has both TCP and UDP port classifiers, only the ones matching the flow protocol are used. This feature is supported by the following traffic classes:

- voip-telephony
- multimedia-conferencing
- real-time-interactive

EasyQoS Prerequisites

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

- EasyQoS supports most of the Cisco LAN, WAN, WLAN devices. To verify whether the devices and software versions in your network are supported, see the *Cisco EasyQoS Application for APIC-EM Supported Platforms* document.
- Make sure that your Cisco network devices, such as the ISR-G2, the ASR 1000, and Wireless LAN Controller, have the AVC (Application Visibility and Control) feature license installed. For information, see the *NBAR2 (Next Generation NBAR) Protocol Pack FAQ* at the following URL: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/network-based-application-recognition-nbar/qa_C67-723689.html.
- For the Cisco APIC-EM to identify the WAN interfaces that need policies, you must specify the interface type (WAN) and (optionally) its subline rate and service-provider Class-of-Service model. For information about how to configure these settings on WAN interfaces, see Device Configuration Prerequisites, on page 23.
- From the **Topology** or **Device Inventory** window, verify that the device roles assigned to devices during discovery are appropriate for your network design. If necessary, change any of the device roles that are not appropriate.

EasyQoS Guidelines and Limitations

EasyQoS and IWAN Interaction

- When you apply a Cisco APIC-EM policy tag to a device, you cannot provision the same device in IWAN. If you want to provision a device using IWAN, you must first remove the APIC-EM policy tag.
- When you provision a device using IWAN, you cannot apply a Cisco APIC-EM policy tag to the same device. To apply a Cisco APIC-EM policy tag, you must delete the device from the IWAN device inventory and then rediscover it in the Cisco APIC-EM.

Policy Scope

- Changing a policy scope *does not* automatically roll back or change the policy on the device. You must reapply the policy in order for the updated configuration to be deployed to the device.
- Policies are not removed from a device when the device is removed from a policy scope.
- Policies are not automatically reapplied if you move a device from one policy scope to another policy scope after a policy has already been applied to devices.

Applications

- 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 11.
- You cannot create custom applications for wireless devices.
- EasyQoS supports custom application names 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.
- 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.

Policies

- EasyQoS supports Out Of Band (OOB) changes, that is, changes made to the device configurations from any means other than Cisco APIC-EM. However, after you make the OOB change, you must wait until the next inventory discovery cycle occurs (configurable to be from every 25 minutes to once per day) and then click **Reapply Policy**. Alternatively, you can manually resynchronize selected devices in the **Device Inventory** window. For information, see the *Cisco Network Visibility Application for APIC-EM User Guide*.
- EasyQoS cannot restore an original configuration to a device if the device has a pre-existing EasyQoS configuration that was applied before adding the device to the current policy.

Queuing Profiles

- If you update a queuing profile that is associated with a policy, the policy is marked as stale. You need to reapply the queuing profile to provision the latest changes.
- Traffic class bandwidth customization does not affect interfaces on Cisco service provider switches and routers. You continue to configure these interfaces without using Cisco EasyQoS.
- Traffic class bandwidth profiles are not applicable to wireless policies. DSCP customization is applicable to wireless policies.

Dynamic QoS

- Policies are not reapplied automatically when you enable dynamic QoS. You must reapply the policy to the devices for the change to take effect.

Logging into the Cisco APIC-EM

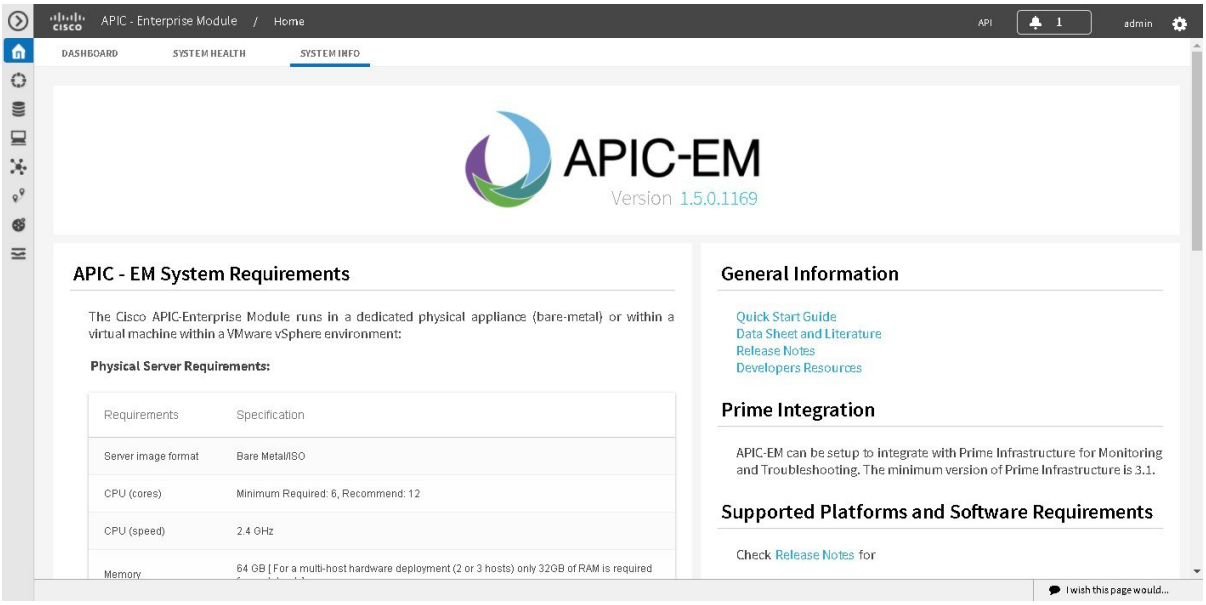
You access the Cisco APIC-EM GUI by entering its network IP address in your browser. The IP address was configured for the Cisco APIC-EM network adapter during the initial setup using the configuration wizard. This IP address connects to the external network.

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

Step 2 On the launch page, enter your username and password that you configured during the deployment procedure. The **Home** page of the APIC-EM controller appears. The **Home** page consists of the following three tabs:

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

Figure 1: SYSTEM INFO Tab



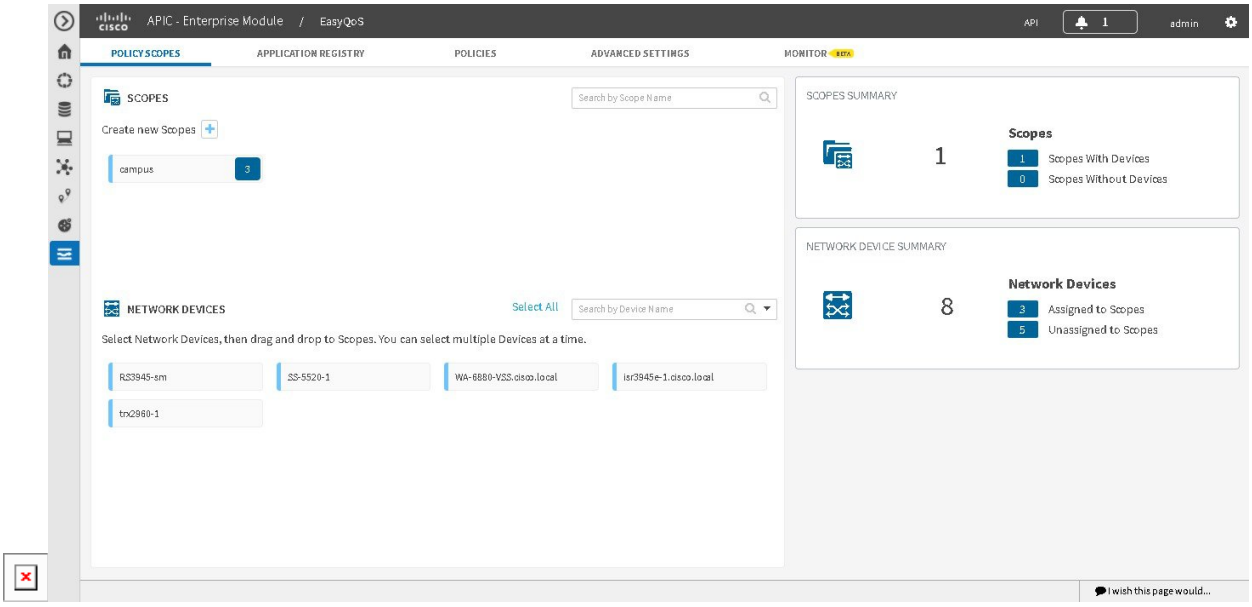
What to Do Next

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

Navigating the EasyQoS Application

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

Figure 2: EasyQoS Window



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

- **Policy Scopes—**Allows you to define a set of devices to which policies are applied.
- **Application Registry—**Lists all of the applications that EasyQoS supports, including any custom applications that you have added.
- **Policies—**Allows you to configure policies for the selected scope of devices.
- **Advanced Settings—**Allows you to define the following:
  - **Bandwidth Profiles—**Profiles that define bandwidth allocation.
  - **SP Profiles—**Profiles that define the Differentiated Services Code Point (DSCP), priority, and bandwidth for traffic that is destined for a service provider.
  - **Dynamic QoS—**A feature that enables a specific class of service for the duration of some event, for example, during a Cisco Unified Call Manager call.
- **Monitor—**Allows you to monitor the application health and application provisioning status on the devices.

CHAPTER 3

Device Configuration Prerequisites

WAN Interface Configuration for EasyQoS

In order for the Cisco APIC-EM to identify the discovered WAN interfaces or subinterfaces that need policies, you need to configure the following tag as the interface (or subinterface) description using the command line interface (CLI) **description** command:

```
switch# description #WAN#rate#SPProfileName#
```

- **#WAN#**—Keyword that indicates special traffic handling on the interface or subinterface.
- *#rate#*—Subline rate (MB) 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, Cisco APIC-EM updates the WAN interface or sub-interface in the device with the designated SP policy. The rate must be a value below the actual line rate of the interface or subinterface.
- *#SPProfileName#*—Service Provider Profile to use.

  The service provider profile defines the Differentiated Services Code Point (DSCP), priority, and bandwidth for traffic that is destined for a service provider. Cisco APIC-EM provides four predefined service provider

  profiles (SPPs or SP profiles): SPP1, SPP2, SPP3, and SPP4. You can use any of the predefined SP profiles, or you can create a customized SP profile for your unique requirements.

  For information about the preconfigured SP profiles, see Understanding Service Provider Profiles, on page 15. To create a customized SP profile, see Creating a Customized Service Provider Profile, on page 49.

Example

```
interface GigabitEthernet0/2
     description AT&T Circuit from SJ-13-12 to RTP-Ridge-7 #WAN#50M#SPP1-4Class#
```

Note You need to wait for Cisco APIC-EM's next discovery polling cycle to complete (configurable to be from every 25 minutes to once per day) or manually resynchronize the device before applying the policy configuration.

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

CHAPTER 4

Configuring Quality of Service

Getting Started With EasyQoS

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

Before You Begin

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

Step 1 Define your business objectives.
For example, your business objective might be to improve user productivity by minimizing network response times or to identify and deprioritize non-business applications.

Step 2 With your business objectives in mind, determine the business relevance of your applications.
Decide which category your applications fall into:

- **Relevant—**The application directly contributes to organizational objectives. Such applications include voice, video, streaming and collaborative multimedia applications, database applications, enterprise resource applications, email,

file-transfers, content distribution, and so on. These applications are classified, marked, and treated according to industry best-practice recommendations (RFC 4594).

- **Default—**The application may or may not be business-relevant. For example, generic HTTP/HTTPS traffic may contribute to organizational objectives at times, while at other times such traffic may not. Applications of this type are treated with a Default Forwarding service (RFC 2474).
- **Irrelevant—**The application has no contribution towards achieving organizational objectives. It is primarily consumer- and/or entertainment-oriented in nature. Applications of this type are treated with a less-than Best Effort service (RFC 3662).

Step 3 Define the scope (or group) of devices that you will configure with a policy.

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

For more information, see Defining Policy Scopes, on page 27.

Step 4 (Optional) Create custom applications.

If you have applications that are not already defined in EasyQoS, you can add them and define their QoS attributes. For more information, see Custom Applications, on page 10.

Step 5 (Optional) View the default service provider profiles and, if necessary, create a new service provider profile to fit your needs. For information, see Creating a Customized Service Provider Profile, on page 49.

Step 6 Create the policy on wired devices or wireless segments. For information, see Creating or Editing a Policy, on page 36. As part of creating the policy, do the following:

- Configure the business relevance of the applications used in your network. EasyQoS comes with the applications preconfigured into business-relevancy groups. You can keep this configuration or modify it to meet the needs of your business objectives and network configuration. For more information, see Business-Relevance Groups, on page 7.
- Select favorite applications. Cisco APIC-EM allows you to flag applications that you want EasyQoS to configure on devices before all other applications (except custom applications). This feature increases the chances that favorite applications are configured on network devices that have a limited memory for storing network access control lists (ACLs) and access control entries (ACEs). For more information, see Favorite Applications, on page 11 and Processing Order for Devices with Limited Resources, on page 11.

Step 7 (Optional) Validate the policy.

You can view the command line interface (CLI) commands that will be applied to a device when the policy is deployed. For more information, see Policy Preview, on page 14.

Step 8 Apply the policy to the scope of devices.

Step 9 (Optional) Proceed to monitor the application provisioning status and health.

For additional information, see Information about Monitoring EasyQoS, on page 57.

Step 10 (Optional) Configure Cisco APIC-EM for Apple Fastlane.

For additional information, see About Cisco APIC-EM and Apple Fastlane, on page 69.

What to Do Next

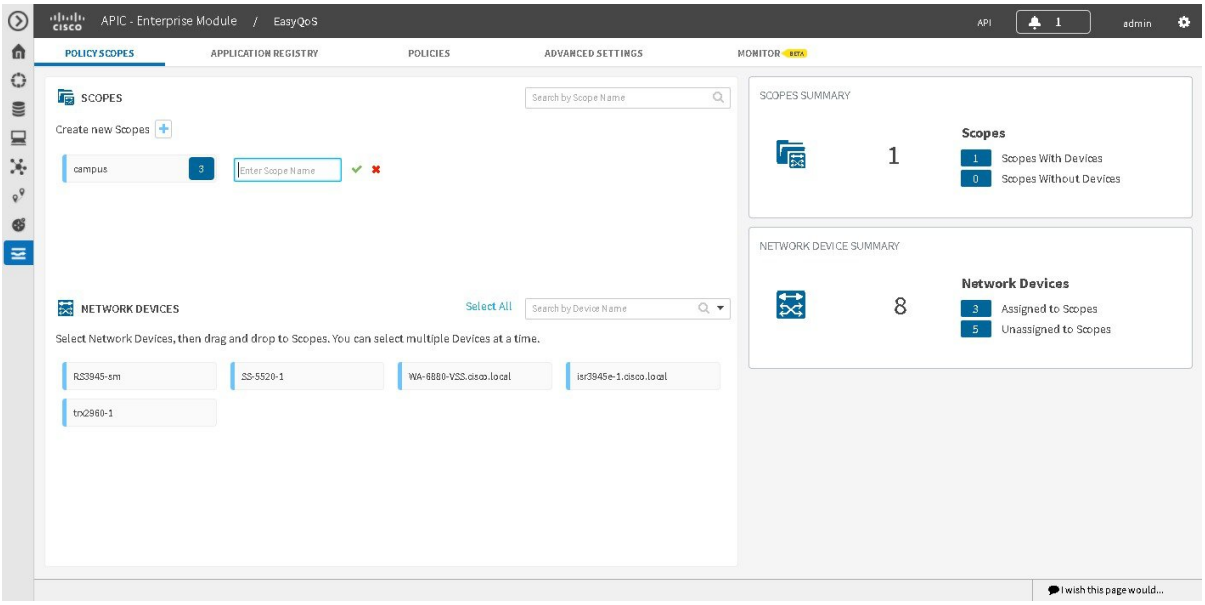
You can see how the deployed policy is working in your network by performing a path trace on two devices and capturing QoS data. For more information, see the *Cisco Path Trace Application for APIC-EM User Guide*.

Defining Policy Scopes

Before you can create a QoS policy, you need to define the policy scope. That is, you need to define the group of devices that will be configured with the same QoS policy. For more information, see Understanding Policy Scope, on page 6.

Note You can also define a policy scope by applying policy tags to devices from the **Device Inventory** window or the **Topology** window. For information, see *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

Figure 3: Policy Scope Window



Before You Begin

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

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

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

Step 2 Create new Scopes by clicking the plus (+) icon.

Step 3 In the **Create Policy Scope** field, enter a name for the policy and click the green check mark icon.

Step 4 From the **Wired Devices** or **Wireless Segments** lists below, drag and drop the selected device to the field where you named the policy.
EasyQoS adds the device and saves the policy automatically.

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

What to Do Next

You can create policies for wired devices or wireless segments. For information, see Creating or Editing a Policy, on page 36.

Configuring Applications

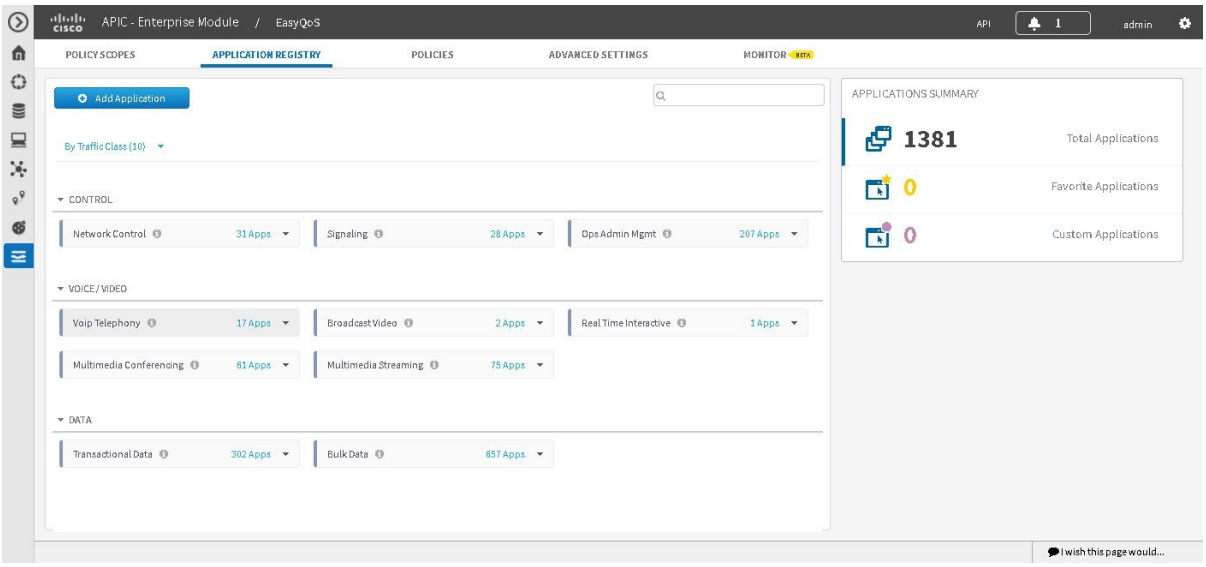
Configuring Favorite Applications

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

You can also configure favorite applications while creating or editing a policy. For more information, see Creating or Editing a Policy, on page 36.

For information about how favorite applications work, see Favorite Applications, on page 11.

Figure 4: Application Registry Window



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 and the appropriate resource scope to perform this procedure.

Define the scope of devices that you want to be configured with this QoS policy. You can do this by creating a policy tag in Topology or Device Inventory or by creating a policy scope in EasyQoS.

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

Step 2 From the **EasyQoS** window, select the **Application Registry** tab.
By default, the applications are listed by traffic class. To change how applications are listed, click the **View By** down arrow at the top of the list and choose **Applications** to view the applications in an alphabetical list or **Application Groups** to view the applications according to their business-relevance group.

Step 3 Click the star icon next to the applications that you want to set as favorites.
For information about how favorite applications work, see Favorite Applications, on page 11.

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

Modifying Traffic Class in an Application

You can modify the traffic class of an NBAR application.

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 and the appropriate resource scope to perform this procedure.

Define the scope of devices that you want to be configured with this QoS policy. You can do this by creating a policy tag in Topology or Device Inventory or by creating a policy scope in EasyQoS.

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

Step 2 From the **EasyQoS** window, select the **Application Registry** tab.
By default, the applications are listed by traffic class. To change how applications are listed, click the **View By** down arrow at the top of the list and choose **Applications** to view the applications in an alphabetical list or **Application Groups** to view the applications according to their business-relevance group.

Step 3 Select the NBAR application whose traffic class you wish to change from the **Application Groups** listed in the GUI. After selecting an application, its application pane opens with the following fields: DESCRIPTION, DETAILS, ASSOCIATED POLICIES.

Step 4 Click the **Edit** button in the application pane to view the edit fields.

Step 5 Select a new traffic class from the Traffic Class drop-down menu.

Step 6 Click **Save** to save the new traffic class.

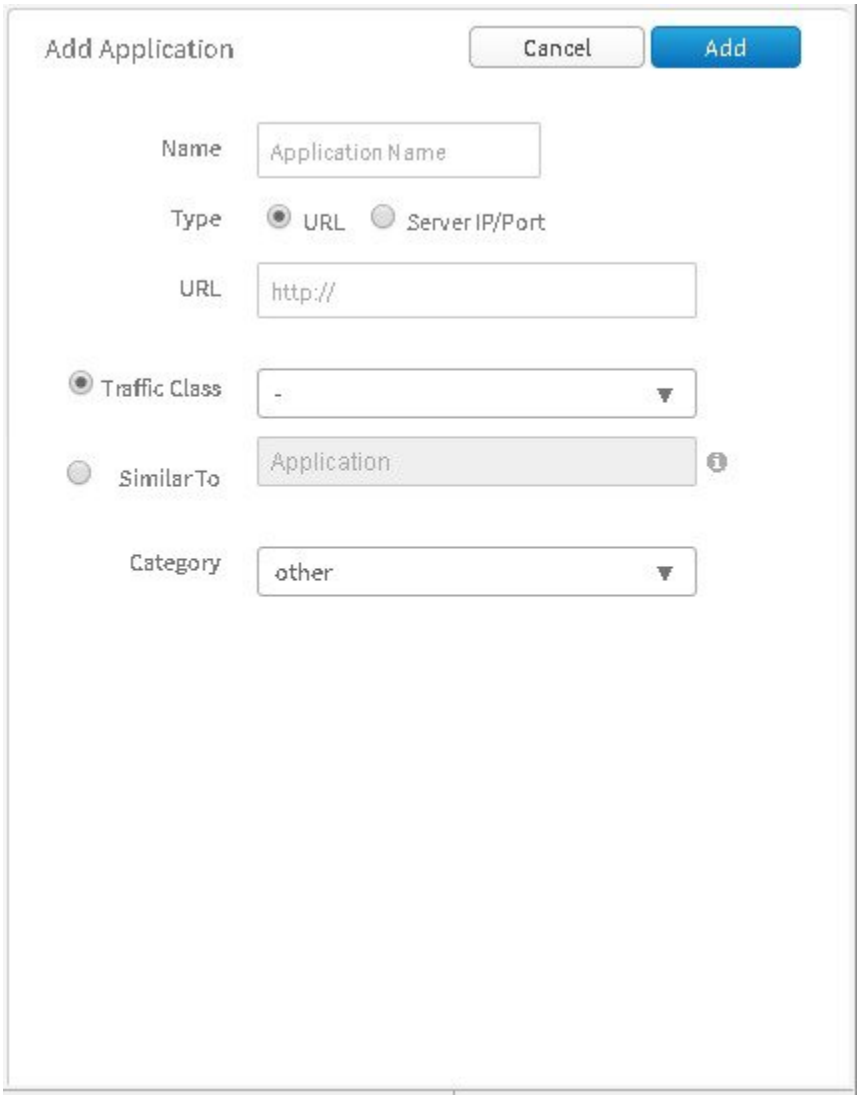
What to Do Next

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

Creating a URL-Based Custom Application

If you have applications that are not in the NBAR2 application library, you can add them as custom applications. This procedure shows you how to create a custom application that is accessible through its URL.

Figure 5: Add Application Pane for URL-Based Applications



Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

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

Define the scope of devices that you want to be configured with this QoS policy. You can do this by creating a policy tag in Topology or Device Inventory or by creating a policy scope in EasyQoS.

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

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

Step 3 Click **Add Application**.

Step 4 In the **Add Application** pane, enter information in the following fields:

- **Name—**Name of the application. The name can contain up to 24 alphanumeric characters, including underscores and hyphens. The underscore and hyphen characters are the only special character allowed in the application name.
- **Type—**Method by which users access the application. Choose **URL** for applications that are accessible through a URL.
- **URL—**URL used to reach 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 similar traffic-handling requirements. Click the **Similar To** radio-button and select an application from the drop-down field. EasyQoS copies the other application's traffic class, category, and subcategory settings to the application that you are defining.

Step 5 Click **Create Application** to save the new application.

Step 6 When you create a custom applicaiton, it is not assigned to a business-relevancy group. It is placed in a group called Unassigned. To change this setting, see Creating or Editing a Policy, on page 36.

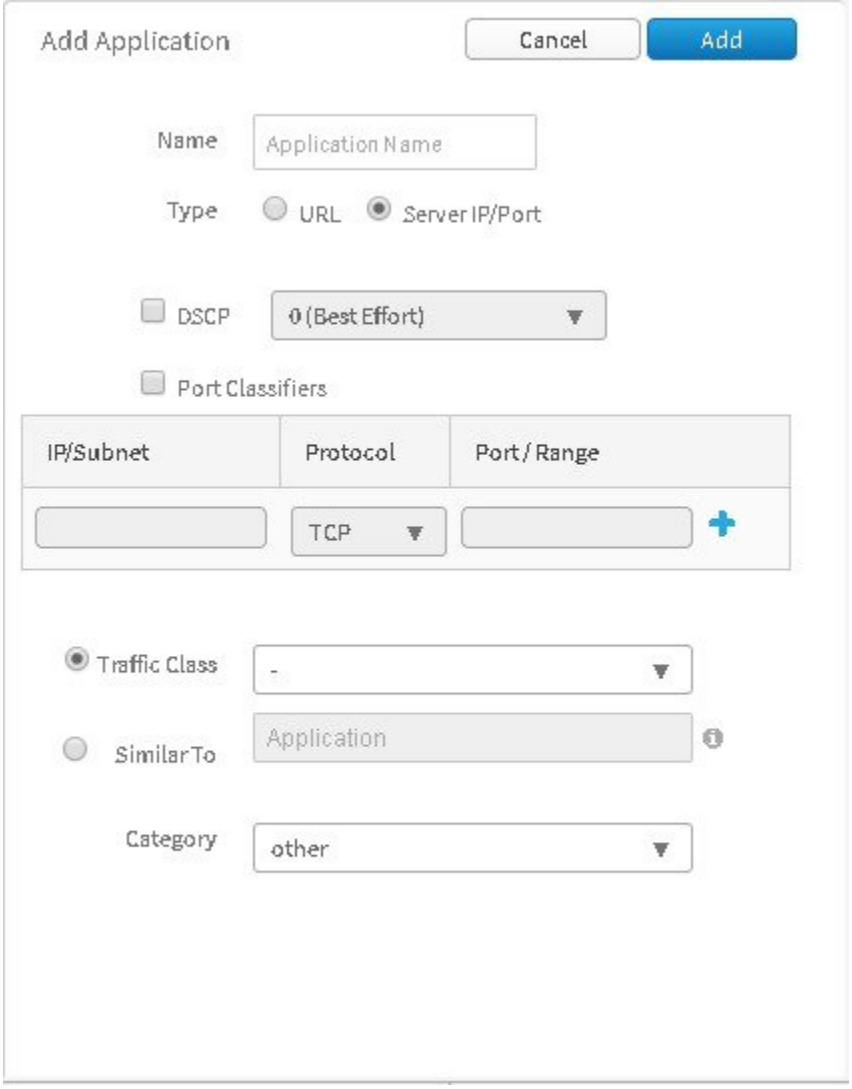
What to Do Next

You can now include the custom application to existing or new policies. If you include the custom application in an existing policy that has already been deployed to devices, you need to reapply the policy so that the devices are updated with the class of service settings for the custom application.

Creating a Server-Based Custom Application

If you have applications that are not in the NBAR2 application library, you can add them as custom applications.

Figure 6: Add Application Pane for Server-Based Applications



Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

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

Define the scope of devices that you want to be configured with this QoS policy. You can do this by creating a policy tag in Topology or Device Inventory or by creating a policy scope in EasyQoS.

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

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

Step 3 Click **Add Application**.

Step 4 In the **Add Application** pane, complete the following fields:

- **Name—**Name of the custom 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—**Method by which users access the application. Choose **Server IP/Port** for applications that are accessible through a server.
- **DSCP—**Differentiated Services Code Point (DSCP) value. Check the **DSCP** check box and define a DSCP value. If you do not define a value, the default value is **Best Effort**. Best-effort service is essentially the default behavior of the network device without any QoS.
- **Port Classifiers—**Classification of traffic based on IP address, protocol, and port number. Check the **Port Classifiers** check box to define the IP address or subnet, protocol, and port or port range for an application. Valid protocols are **IP**, **TCP**, **UDP**, and **TCP/UDP**. If you select the **IP** protocol, you do not define a port number or range.
- **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, then select an application from the drop-down field. EasyQoS copies the other application's traffic class, category, and subcategory settings to the application that you are defining.

Step 5 Click **Create Application** to save the application.

Step 6 When you create a custom applicaiton, it is not assigned to a business-relevancy group. It is placed in a group called Unassigned. To change this setting, see Creating or Editing a Policy, on page 36.

What to Do Next

You can now include the custom application in existing or new policies. If you include the custom application in an existing policy that has already been deployed to devices, you need to redeploy the policy so that the devices are updated with the settings for the custom application.

Editing a Custom Application

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

Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

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

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

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

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

Information about the application displays in the right hand pane.

Note You can review the policies that use the custom application by clicking **Associated Policies**. **EasyQoS** displays the scope, policy name, and relevance.

Step 4 Click **Edit**.

Step 5 Change the desired settings for the custom application:

- **Name—**Name of the application. This value cannot be changed.
- **Type—**Type of application. Choose either **URL** for applications that are accessible through URL or **Server IP/Port** for applications that are accessible through a server IP address and port number.
- **Protocol—**Supported protocol for application. Choose either **TCP** or **UDP**. UDP is available only for applications that are accessible through a server IP address and port number.
- **Value—**The value entered depends on the type of application that is being added. For URL type applications, enter the application URL. For Server IP/Port applications, enter the server IP address and port number through which you access the application.
- **Traffic Class—**Traffic class to which the application belongs. Valid values are BULK_DATA, TRANSACTIONAL_DATA, OPS_ADMIN_MGMT, NETWORK_CONTROL, VOIP_TELEPHONY, MULTIMEDIA_CONFERENCING, MULTIMEDIA_STREAMING, BROADCAST_VIDEO, REAL_TIME_INTERACTIVE, and SIGNALING.
- **Similar To—**Application with the similar traffic-handling requirements. Click the radio-button to select this option and select an application from the drop-down field. EasyQoS copies the other application's traffic class, category, and subcategory settings to the application that you are defining.

Step 6 Click **Save Application**.

What to Do Next

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

Deleting a Custom Application

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

Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

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

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

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

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

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

Information about the application displays in the right hand pane.

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

Step 4 Click **Delete**.

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

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

What to Do Next

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

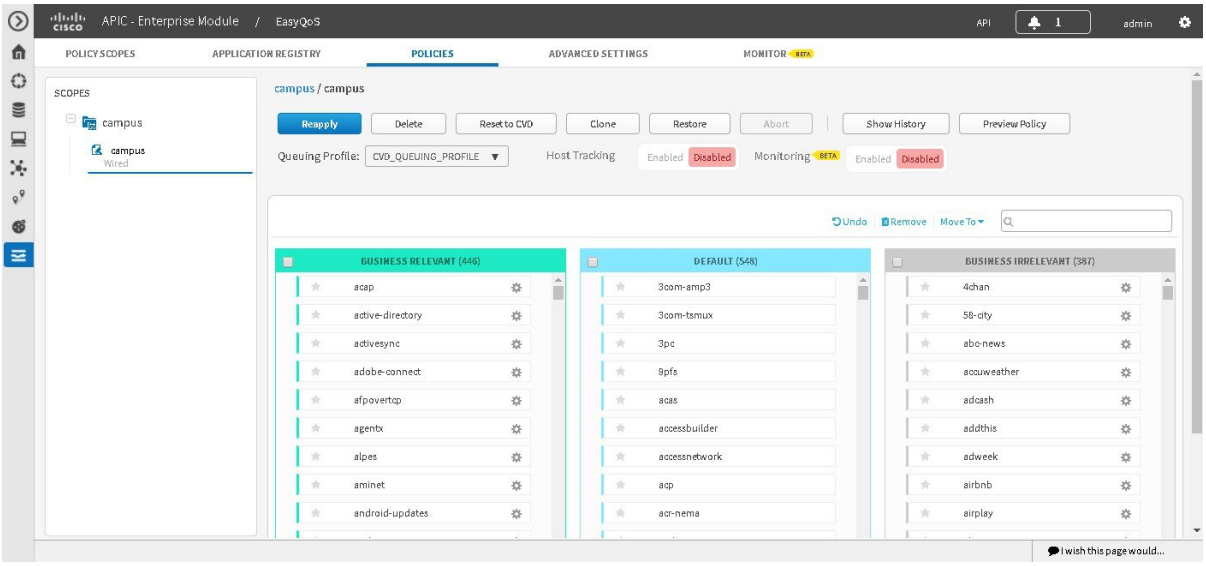
Configuring QoS Policies

Creating or Editing a Policy

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

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

Figure 7: Policies Tab



Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

Make sure that you have discovered your complete network topology.

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

Define the scope of devices that you want to be configured with this QoS policy. You can do this by creating a policy tag in Topology or Device Inventory or by creating a policy scope in EasyQoS.

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

Step 2 Click the **Policies** tab.

Step 3 From the **Scopes** pane, select a policy scope.

Step 4 Do one of the following:

- To create a policy for the wired devices, click the **Create Policy** button and enter a name for the policy in the **Policy Name** field.
- To create a policy for a wireless-device segment, click the plus sign (+) icon next to the chosen wireless segment and enter a name for the policy in the **Policy Name** field.

- To edit a policy, select the policy from the **Scopes** pane.

Step 5 In the **Queuing Profile** field, choose a user-created profile or the default customer validated design profile (CVD_QUEUING_PROFILE).

Step 6 To enable host tracking, click **Enable** in the **Host Tracking** field.
You are then prompted to confirm host tracking. Click **OK** to confirm.

Note The host tracking feature tracks collaboration endpoints in your network and dynamically reapplies policies to match voice and video traffic.

Step 7 To enable monitoring, click **Enable** in the **Monitoring** field.
You are then prompted to confirm monitoring. Click **OK** to confirm.

For information about the monitoring functionality enabled at this step, see Information about Monitoring EasyQoS, on page 57.

Step 8 Change an application's business relevance by dragging and dropping the application from the current business relevance group to the chosen business relevance group.

Note To change an application's business relevance, you can also select the application and use the **Move To** drop down list to select a business relevancy group.

If you make a mistake, you can click the **Undo** button.

Step 9 (Optional) You can designate applications as favorites by clicking the star icon next to the application name.
For information about how favorite applications work, see Favorite Applications, on page 11.

Step 10 (Optional) You can select interfaces on the Cisco devices to exclude from the QoS policy by clicking the icon next to the device name.
After clicking this icon, a field will appear that lists the interfaces on the device. Check the interfaces that you do not wish the QoS policy to be applied to.

Step 11 (Optional) You can change some of an application's settings by clicking the **Edit** icon next to the application name.

Note You cannot edit applications that have not been assigned a business relevance. If there are unassigned applications, the **Unassigned** link indicates the number of unassigned applications. To assign an unassigned application to a business relevance group, click **Unassigned**, then drag and drop the application into the appropriate business relevance group.

Complete the following fields in the **Edit Application Details** dialog box and click **Save** when you are done:

- **Application Name—**Name of the application. This field is not editable.
- **Show Details** and **Hide Details** toggle**—**Displays and hides the application's settings, for example, the application's URL or TCP and UDP port assignments. These settings are not editable.
- **Advanced Policy Settings—**You can configure these advanced settings:
  - **Traffic Direction—**Indicates whether the policy is applied to unidirectional or bidirectional application traffic. For more information, see Unidirectional and Bidirectional Application Traffic, on page 7.
  - **Consumer—**Application that receives traffic from the application that you are editing. Use this setting to apply a policy to traffic that flows between these applications. For more information, see Consumers and Producers, on page 7
- **Associated Policies—**If present, lists the policies that include the application that you are editing.

Step 12 Do one of the following actions:

- To save and apply a new policy, click **Apply Policy**.
- To save your changes and reapply the policy, click **Reapply Policy**.

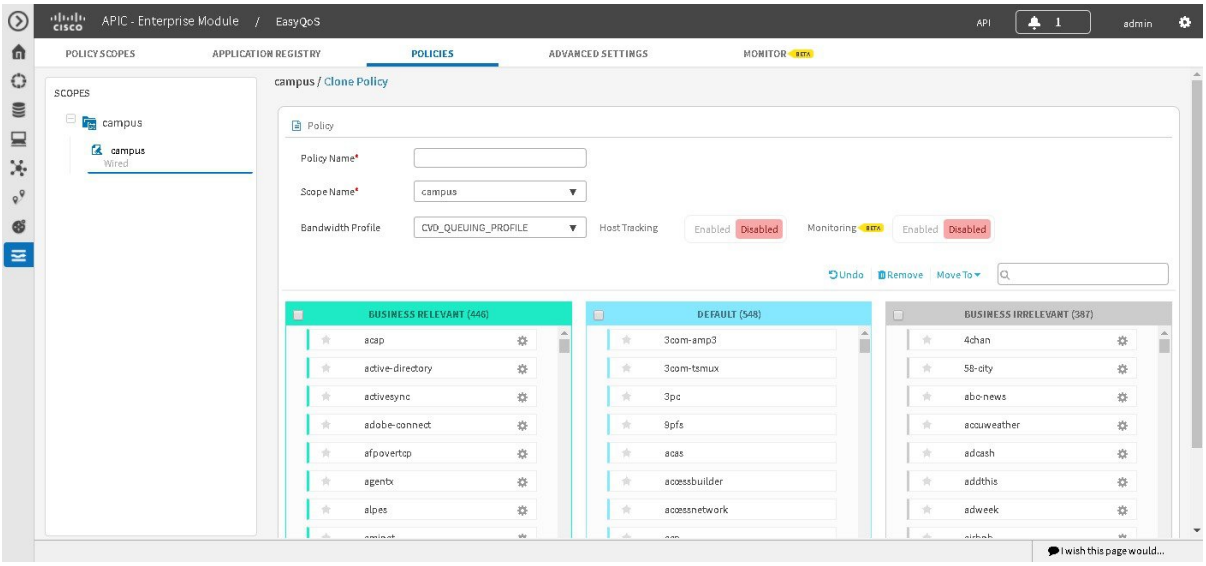
Step 13 In the **Apply Policy** dialog box, do one of the following actions:

- To schedule a policy to be applied to devices at a later date and time, use the calendar and time tools to select the month, day, year, and time. Then click **Schedule**.
- To apply the policy to devices immediately, click **Apply Now**.
- To cancel the action, click **Cancel**.

Cloning a Policy

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

Figure 8: Policies Tab



Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

From the **Device Inventory** window, verify that the device roles (assigned during discovery) are appropriate for your network design. If necessary, change any of the device roles that are not appropriate. For information, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

Define the scope of devices that you want to be configured with this QoS policy. You can do this by creating a policy tag in Topology or Device Inventory or by creating a policy scope in EasyQoS.

You must have created at least one policy.

You need to define a bandwidth profile in this procedure. Determine whether the default customer validated design (CVD) bandwidth profile is adequate for your QoS needs or create a customized bandwidth profile. For information, see Understanding Queuing Profiles.

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

Step 2 Click the **Policies** tab.

Step 3 From the **Scopes** pane, expand the policy scope and select the policy that you want to clone.

Step 4 Click **Clone**.

Step 5 Enter a name for the policy in the **Policy Name** field.

Step 6 Choose a policy scope from the **Scope Name** drop-down list.

Step 7 Change an application's business relevancy group by dragging and dropping the application into the chosen business relevancy group.

Step 8 Designate applications as favorites by clicking the star icon next to the application name.
For information about how favorite applications work, see Favorite Applications, on page 11.

Step 9 Click **Create Policy**.

Step 10 Click **Reapply Policy**.

Step 11 In the **Apply Policy** dialog box, do one of the following actions:

- To schedule a policy to be applied to devices at a later date and time, use the calendar and time tools to select the month, day, year, and time. Then click **Schedule**.
- To apply the policy to devices immediately, click **Apply Now**.
- To cancel the action, click **Cancel**.

Deleting a Policy

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

Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

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

Step 2 Click the **Policies** tab.

Step 3 From the **Scopes** pane, select a policy scope.

Step 4 Under the policy scope name, select a policy.

Step 5 Click **Delete**.

Step 6 To confirm the deletion, click **Ok**. Otherwise, click **Cancel**.

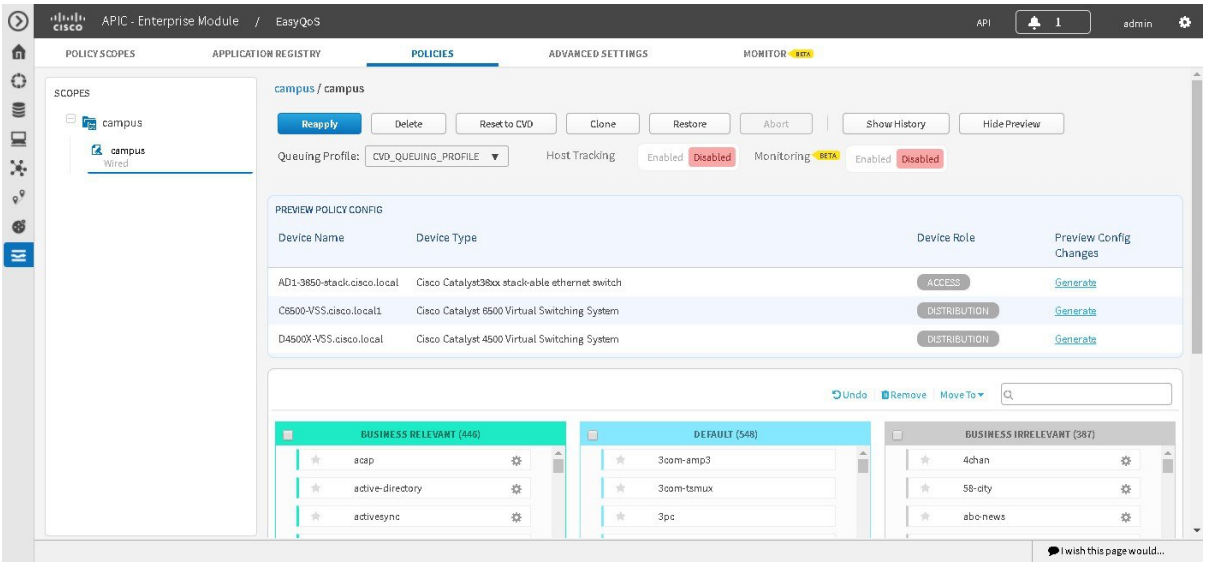
Step 7 When the deletion confirmation message appears, click **Ok** again.

Managing QoS Policies

Previewing a Device's Policy Configuration

You can preview the EasyQoS policy configuration that will be applied to a device.

Figure 9: Policies Tab Showing Policy Preview Configuration



Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

You must have created an EasyQoS policy.

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

Step 2 Click the **Policies** tab.

Step 3 From the **Scopes** pane, select a policy scope.

Step 4 Under the policy scope name, select a policy.

Step 5 Click the **Preview Policy** button.
The **Preview Policy** table displays, listing all of the devices in the scope along with their device type, device role, option to generate the configuration.

Step 6 Click **Ok**.

Step 7 Click **Generate** to produce the configuration for the corresponding device.

Step 8 Click **View** to display the policy configuration for the corresponding device.
EasyQoS displays the command line interface (CLI) commands that comprise the policy configuration for the corresponding device in a separate dialog box.

Step 9 To generate additional configurations for other devices, repeat Steps 5 and 6.

Cancelling a Policy Configuration Process

After you click **Apply** or **Reapply**, EasyQoS begins to configure the policy on the devices in the policy scope. If you realize that you have made a mistake, you can cancel the policy configuration process.

The policy configuration process is performed as a bulk process in that it configures 40 devices at a time. So, if you have fewer than 40 devices, cancelling the process has no real effect. However, if you have hundreds of devices, cancelling the policy configuration process can be useful when needed.

When you click **Abort**, EasyQoS cancels the configuration process on devices that have not started to be configured and changes the device status to **Policy Aborted**. EasyQoS does not cancel configurations that are in the process of being completed or have been completed. These devices retain the updated policy configuration and reflect the state of the policy configuration, whether it is configuring, successful, or failed.

Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

Procedure

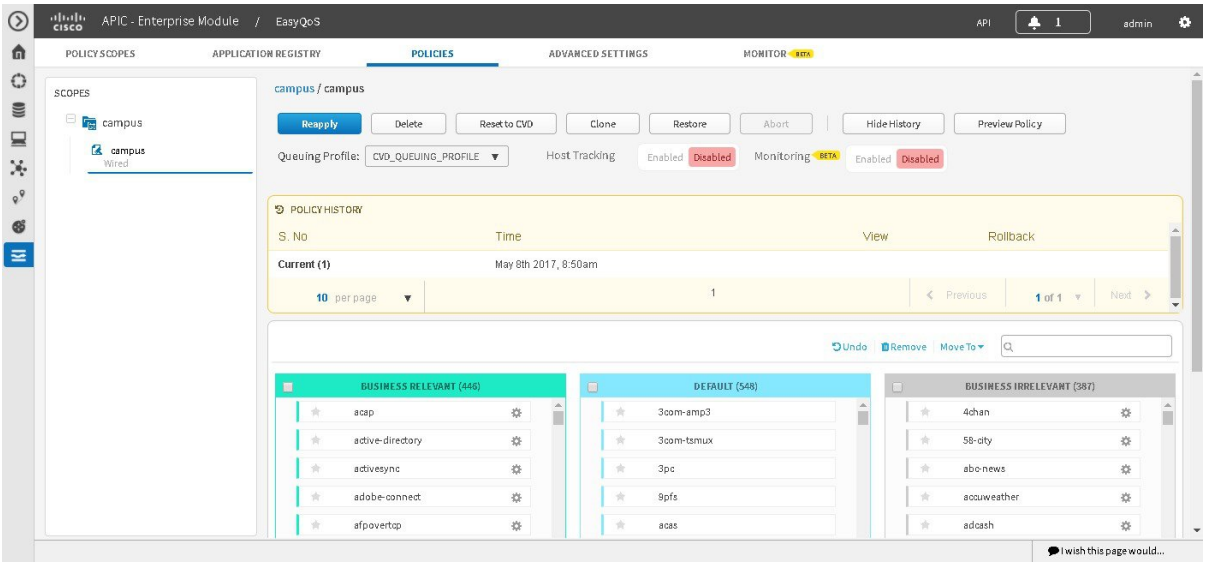
Click **Abort** to cancel the policy configuration process.

Displaying the Version History of Policies

You can display the version history of QoS policies. The version history includes the series number (iteration) of the policy and the date and time that the version was saved. In addition, the version history allows you to perform the following actions:

- Display the differences between a selected policy and the current one. For information, see Comparing Policy Versions, on page 44.
- Roll back to a previous version of a policy. For information, see Rolling Back to a Previous Policy Version, on page 45.

Figure 10: Policies Tab Showing Version History of Policies



Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

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

Step 2 Click the **Policies** tab.

Step 3 From the **Scopes** pane, select a policy scope.

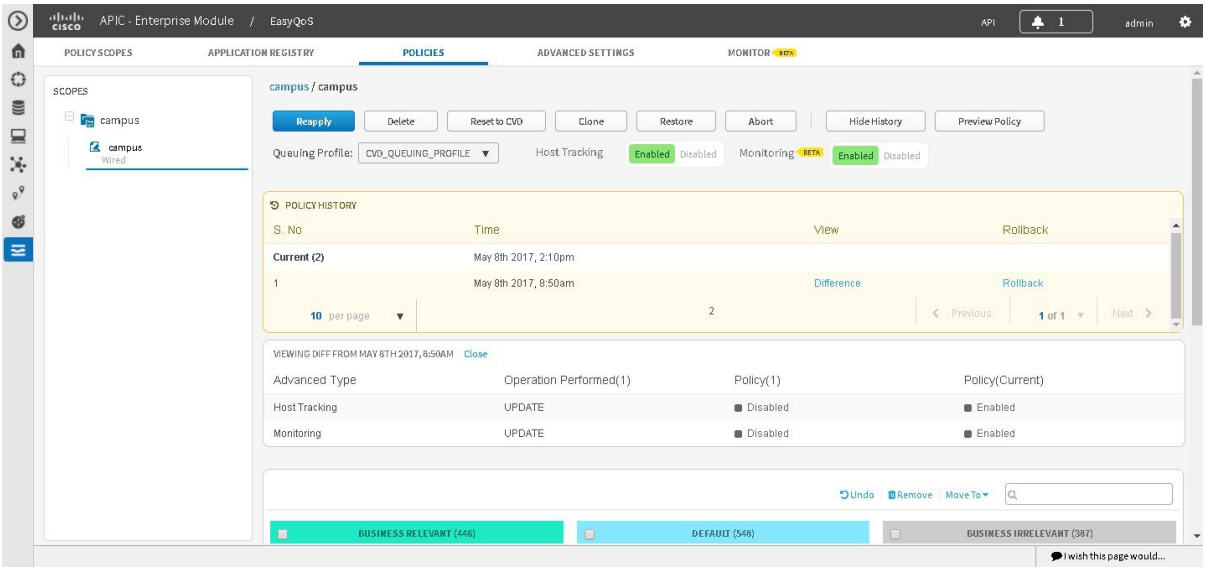
Step 4 Click **Show History**.

EasyQoS displays the version history of the selected policy in the **Policy History** area.

Comparing Policy Versions

You can view the differences between the selected version and the current version.

Figure 11: Policies Tab Showing Policy Versions



Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

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

Step 2 Click the **Policies** tab.

Step 3 From the **Scopes** pane, select a policy scope.

Step 4 Click **Show History**.

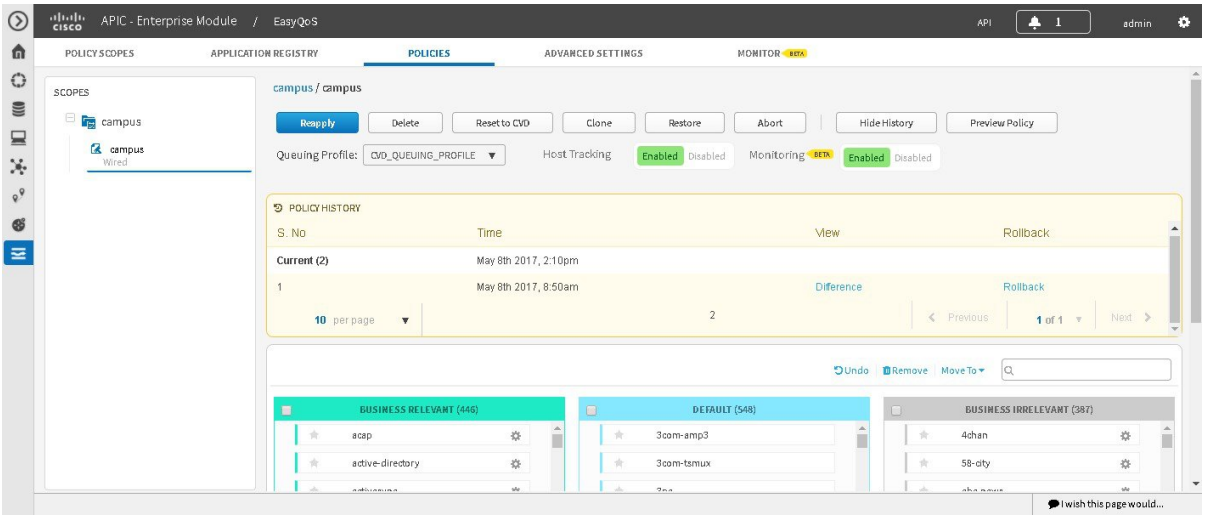
Step 5 Click **Difference** corresponding to the version that you want to compare with the current version.

EasyQoS displays the results of the comparison below the **Policy History** area. The results include applications that were changed, and the operations performed to them.

Rolling Back to a Previous Policy Version

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

Figure 12: Policies Tab Showing Rollback Option



Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

Define the scope of devices that you want to be configured with this QoS policy. You can do this by creating a policy tag in Topology or Device Inventory or by creating a policy scope in EasyQoS.

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

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

Step 2 Click the **Policies** tab.

Step 3 From the **Scopes** pane, select a policy scope and then the policy that you want to rollback.

Step 4 Click **Show History**.
Previous versions of the selected policy are listed in descending order with the newest version (highest number) at the top of the list and the oldest version (lowest number) at the bottom.

Step 5 (Optional) To view the differences between the selected version and the latest version of a policy, click **Difference** in the **View** column.

Step 6 When you determine the policy version that you want to rollback to, click **Rollback** for that policy version.

Step 7 Click **Ok** to confirm the rollback procedure.
The rolled back version becomes the newest version.

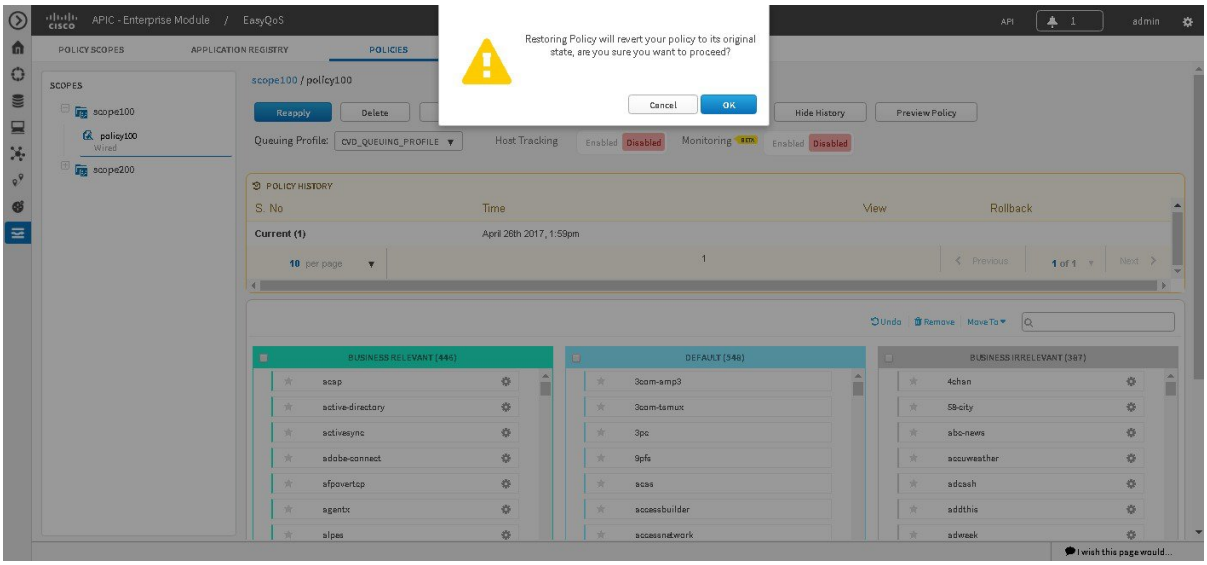
Step 8 Click **Reapply**.

The newest policy version is configured on the devices in the scope.

Resetting Applications to the Cisco Validated Design Configuration

The Cisco Validated Design (CVD) configuration is the default configuration for the applications in EasyQoS. If you create or make changes to a policy and then decide that you want to start over, you can reset the applications to the Cisco Validated Design (CVD) configuration. For more information about the CVD configuration, see Understanding QoS Policies, on page 13.

Figure 13: Policy Tab Showing Reset to CVD Confirmation Dialog Box



Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

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

Step 2 Click the **Policies** tab.

Step 3 From the **Scopes** pane, select a policy scope.

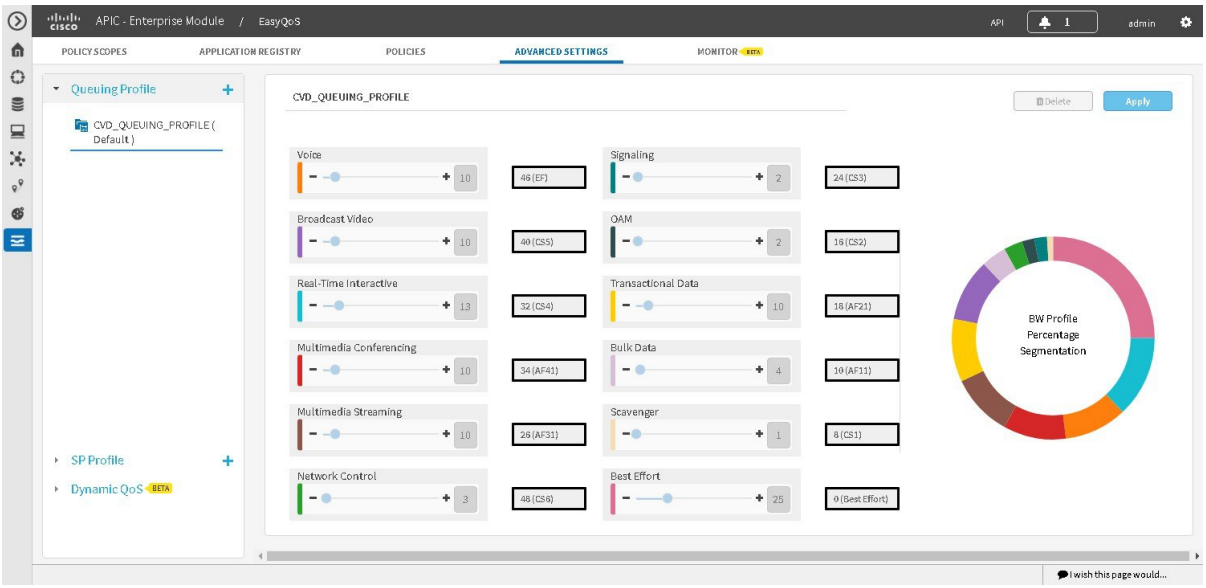
Step 4 Click **Reset to CVD**.

Step 5 Click **Ok** to confirm this change.

Configuring Queuing Profiles

You can configure a queuing profile by changing the default Cisco Validated Design (CVD) settings to meet the needs of your business and network.

Figure 14: Queuing Profile Pane



Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

You must have created a QoS policy with the appropriate configuration. For information, see Creating or Editing a Policy, on page 36.

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

Step 2 From the **EasyQoS** window, click the **Advanced Settings** tab.

Step 3 From the pane on the left, click the plus sign (+) icon next to the **Queuing Profile** option.

Step 4 In the **Queuing Profile Name** field, enter a name for the profile.

Step 5 Do one of the following:

- To apply the queuing profile to all EasyQoS policies, check the **Apply to All References** check box.
- To apply the queuing profile only to policies that have interfaces of a specific speed, uncheck the **Apply to All References** check box and select one of the following options: **100 Gbps**, **10/40 Gbps**, **1 Gbps**, **100 Mbps**, **10 Mbps**, or **1 Mbps**.

Step 6 Configure the bandwidth for each application class by using the slider, clicking the plus (+) or minus (-) sign, or entering a specific number in the field.

The number indicates the percentage of the total interface bandwidth that will be dedicated to the selected application class. Because the total bandwidth equals 100, adding bandwidth to one application class subtracts bandwidth from another application class.

An open lock icon indicates that you can edit the bandwidth for the application class. A closed lock indicates that you cannot edit it.

If you make a mistake, you can return to the Cisco Validated Design (CVD) settings by clicking the **Reset to CVD** icon.

The graph on the right can help you visualize the amount of bandwidth that you are setting for each application class.

Note You can only configure bandwidth for each application class by clicking the **Apply to All References** check box.

Step 7 Configure the queuing profile (DSCP value) for each application class by clicking on the field next to each application class and entering a specific number in the field.
For example, for the **Voice** application class, click on the drop-down arrow in the **Voice** field with the number and select a new DSCP value.

Step 8 When you are satisfied with the bandwidth allocation and the queuing profile, click **Create**.
Note You can edit queuing profiles after creating them. If you edit the profile, then you will also need to reapply the policies that are using for this queuing profile.

Configuring Service Provider Profiles on WAN Interfaces

You can configure your WAN interfaces so that the Cisco APIC-EM can identify them and apply a corresponding service provider (SP) profile to them when a congestion event is triggered on the device (even if the physical WAN interface itself is not congested).

Use the following high-level procedure to configure SP profiles on WAN interfaces.

Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

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

Define the scope of devices that you want to be configured with this QoS policy. You can do this by creating a policy tag in Topology or Device Inventory or by creating a policy scope in EasyQoS.

Step 1 Determine whether you can use any of the preconfigured service provider profiles (SSPs or SP).
For information about the preconfigured SP profiles, see Understanding Service Provider Profiles, on page 15.

Step 2 If you are using one of the preconfigured SP profiles, proceed to Step 3. Otherwise, you can create a custom SP profile.
To create a custom SP profile, see Creating a Customized Service Provider Profile, on page 49.

Step 3 Associate the SP profile with the WAN interface.
For information, see WAN Interface Configuration for EasyQoS, on page 23.

Step 4 Verify that the Cisco APIC-EM recognizes the SP profile on the WAN interface.

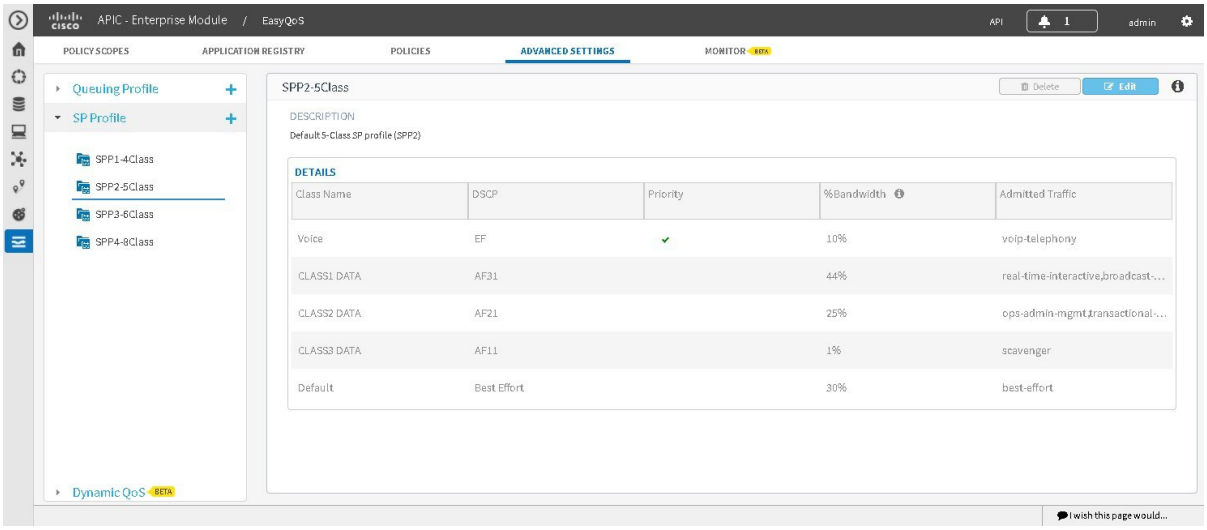
Note You need to wait for Cisco APIC-EM's next discovery polling cycle to complete (configurable to be from every 25 minutes to once per day) or manually resynchronize the device before applying the policy configuration. For information, see Verifying the WAN Interface Synchronization Status, on page 52.

Creating a Customized Service Provider Profile

If you do not want to use any of the preconfigured service provider profiles (SSPs or SP profiles), you can create a customized SP profile to fit your requirements. For information about the preconfigured SP profiles, see Understanding Service Provider Profiles, on page 15.

Note After creating your custom SP profile, you need to configure the WAN interfaces with the SP profile. For information, see WAN Interface Configuration for EasyQoS, on page 23.

Figure 15: Service Provider Profile Window Showing Add SP Profile Pane



Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

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

Define the scope of devices that you want to be configured with this QoS policy. You can do this by creating a policy tag in Topology or Device Inventory or by creating a policy scope in EasyQoS.

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

Step 2 From the **EasyQoS** window, click the **Advanced Settings** tab.

Step 3 From the pane on the left, click the plus sign (+) icon next to the **SP Profile** option.

Step 4 In the **Add SP Profile** pane, enter information in the following fields:

- **Name—**Name of the SP profile. The name can contain from 3 to 12 alphanumeric characters, including underscores and hyphens. The underscore and hyphen characters are the only special character allowed in the name.

  Note You configure the SP profile on WAN interfaces using the name defined in this field.

- **Description—**Word or phrase that identifies the SP profile.
- **Class Model—**Choose one of the class models from the drop down list. Valid class models are **4 classes**, **5 classes**, **6 classes**, and **8 classes**.
- **Class Name—**Name of the QoS class.
- **DSCP—**Differentiated Services Code Point (DSCP) value. Valid values are as follows:
  - Expedited Forwarding (EF)
  - Class Selector (CS)—CS1, CS2, CS3, CS4, CS5, CS6
  - Assured Forwarding—AF11, AF21, AF41
  - Default Forwarding (DF)

  For more information about these DSCP values, see Marking, Queuing, and Dropping Treatments, on page 8.

- **Priority—**Setting that designates a class of service as a priority service. This is a default setting and cannot be changed.
- **%Bandwidth—**Percentage of the bandwidth that is allocated to a particular Class of Service.

  Note Bandwidth for interfaces configured as part of a SP Profile are configured here. Bandwidths configured within custom Queuing Policies do not apply to WAN interfaces, which are part of an SP Profile.

- **Admitted Traffic—**Types of application traffic that have a particular Class of Service.

Step 5 Click **Create SP Profile** to save the new profile.

What to Do Next

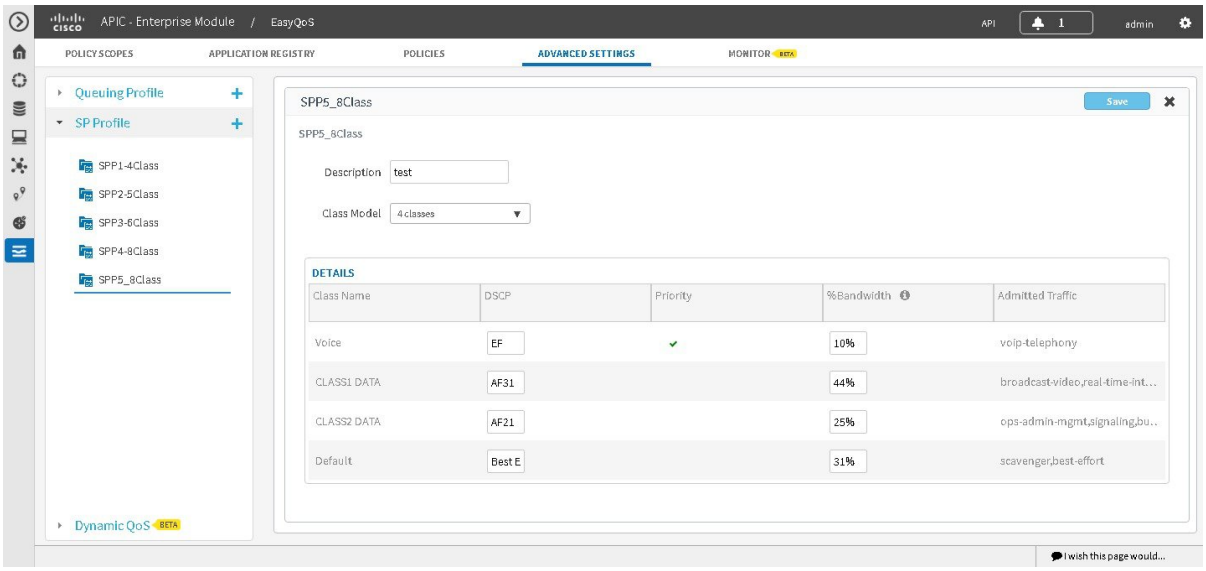
After creating your customized SP profile, you need to configure the WAN interfaces with the SP profile. For information, see WAN Interface Configuration for EasyQoS, on page 23.

Editing a Customized Service Provider Profile

If you need to change the configuration of a custom service provider profile (SSP or SP profile), you can edit it.

Note If you have not already done so, after configuring your SP profile, you need to configure the WAN interfaces with the new SP profile. For information, see WAN Interface Configuration for EasyQoS, on page 23.

Figure 16: Service Provider Profile Window Showing Edit SP Profile Pane



Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

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

Define the scope of devices that you want to be configured with this QoS policy. You can do this by creating a policy tag in Topology or Device Inventory or by creating a policy scope in EasyQoS.

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

Step 2 From the **EasyQoS** window, click the **Advanced Settings** tab.

Step 3 From the left pane, expand the **SP Profile** option.

Step 4 Select the SP profile that you want to edit.

Step 5 From the configuration pane on the right, click **Edit**.

Step 6 In the **Edit SP Profile** pane, you can change the values in any of the following fields:

Note If you need to change an SP profile name, you must delete the SP profile and then add it again with the new name.

- **Description—**Word or phrase that identifies the SP profile.
- **Class Model—**Choose one of the class models from the drop down list. Valid class models are **4 classes**, **5 classes**, **6 classes**, and **8 classes**.
- **Class Name—**Name of the QoS class. 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 name.
- **DSCP—**Dynamic Host Configuration Protocol (DHCP) value. Valid values are as follows:
  - Expedited Forwarding (EF)
  - Class Selector (CS)—CS1, CS2, CS3, CS4, CS5, CS6
  - Assured Forwarding—AF11, AF21, AF41
  - Default Forwarding (DF)

  For more information about these DHCP values, see Marking, Queuing, and Dropping Treatments, on page 8.
- **Priority—**Setting that designates a class of service as a priority service. This is a default setting and cannot be changed.
- **%Bandwidth—**Percentage of the bandwidth that is allocated to a particular Class of Service.
- **Admitted Traffic—**Types of application traffic that have a particular Class of Service.

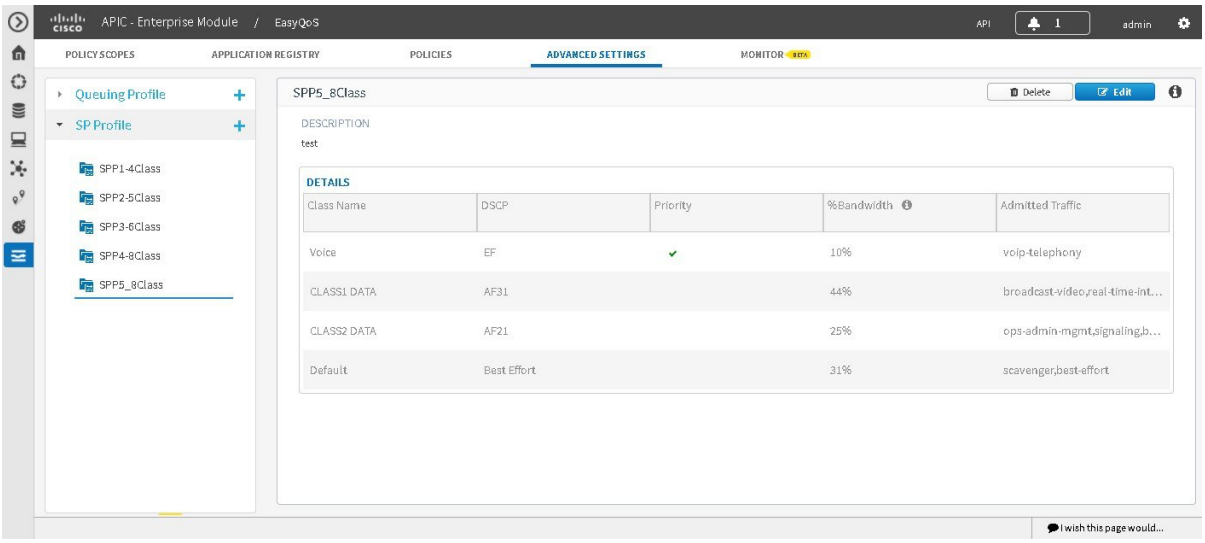
Step 7 Click **Save** to save your changes.

Verifying the WAN Interface Synchronization Status

After you have determined the service provider profile (SP profile) to use or created your custom SP profile (if necessary) and specified the SP profile on your WAN interfaces, you need to make sure that the WAN

interface is properly configured and that the Cisco APIC-EM recognizes it. You can check this configuration on the **SP Profile** window.

Figure 17: SP Profile Tab Showing Associated Interfaces Status



Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

You must have completed all the steps in Configuring Service Provider Profiles on WAN Interfaces, on page 48.

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

Step 2 From the **EasyQoS** window, select the **SP Profiles** tab.

Step 3 Select the SP profile that you want to verify.
The **Associate Interfaces** pane appears, listing the scope, device name, interface name, synchronization status, and last update time.

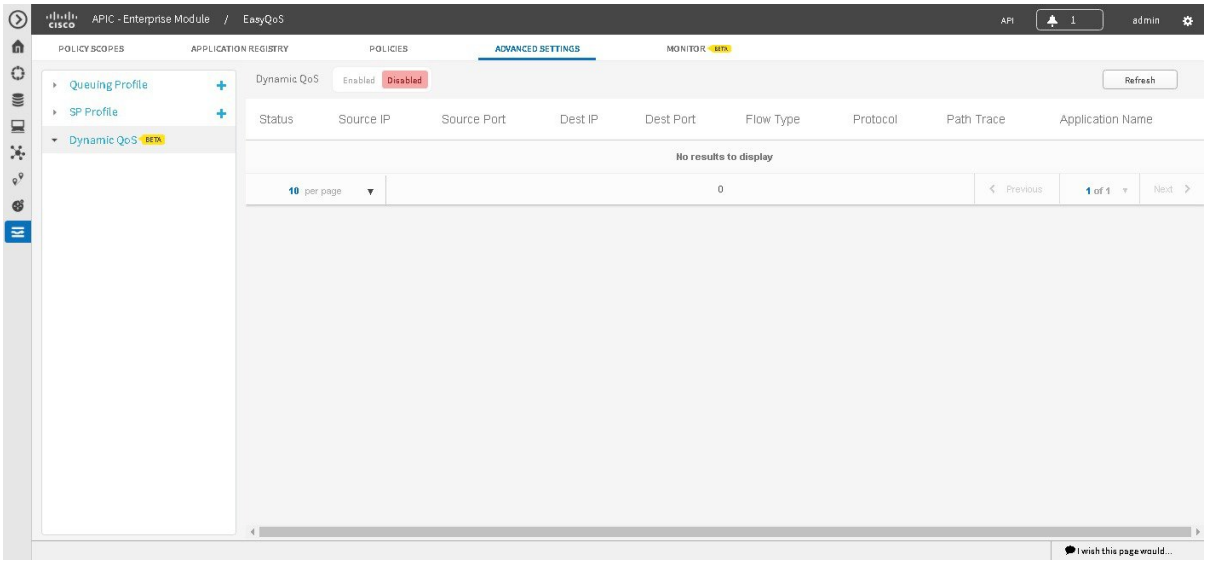
If the Cisco APIC-EM recognizes the SP profile on the WAN interface, the synchronization status shows a check mark icon ( ). If not, the synchronization status shows a red X icon ( ). You need to troubleshoot the issue. Check that the name that you entered as the description of the interface is exactly as it appears in the Cisco APIC-EM and correct it, if needed.

Configuring Dynamic QoS

Enabling and Disabling Dynamic QoS

You can enable a policy to be dynamically applied to devices. For more information, see Static and Dynamic QoS Policies, on page 13.

Figure 18: Dynamic QoS Tab



Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

You must have created a QoS policy with the appropriate configuration. For information, see Creating or Editing a Policy, on page 36.

SUMMARY STEPS

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

DETAILED STEPS

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

Step 2 From the **EasyQoS** window, click the **Advanced Settings** tab.

Step 3 From the pane on the left, expand the **Dynamic QoS** option.

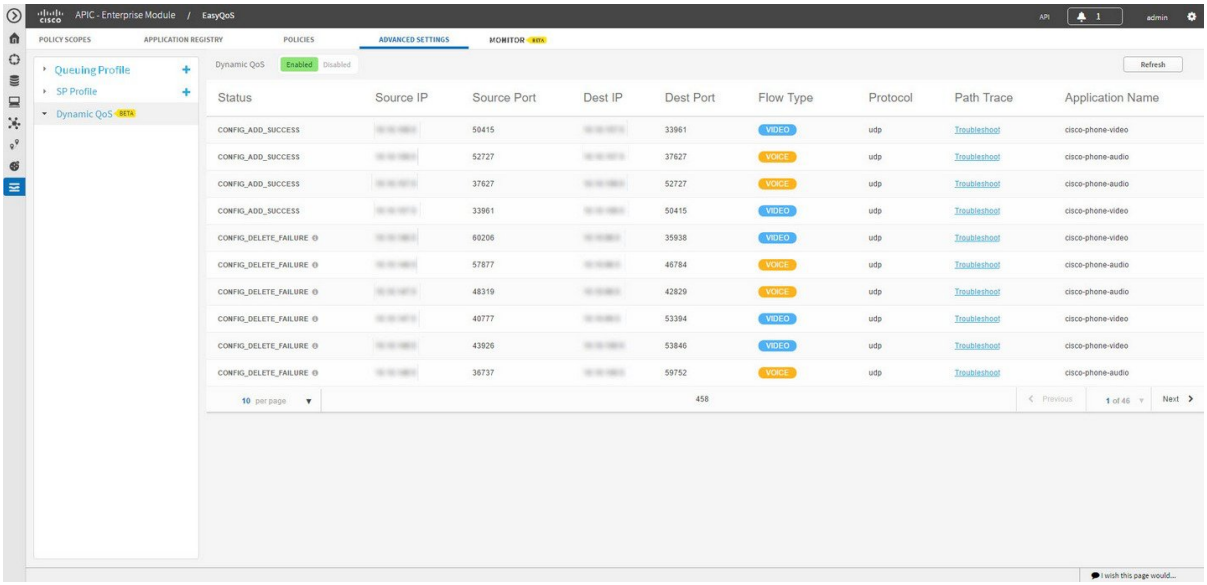
Step 4 In the **Dynamic QoS** field, click **Enabled** to turn on dynamic policy creation or **Disabled** to turn off dynamic policy creation.

Step 5 To apply these configuration changes to the devices, you must reapply the policy to each scope.

Troubleshooting Dynamic QoS

You can use Path Trace to help you troubleshoot your dynamic QoS implementation.

Figure 19: Dynamic QoS Tab Showing Troubleshooting Link in Path Trace Column



Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

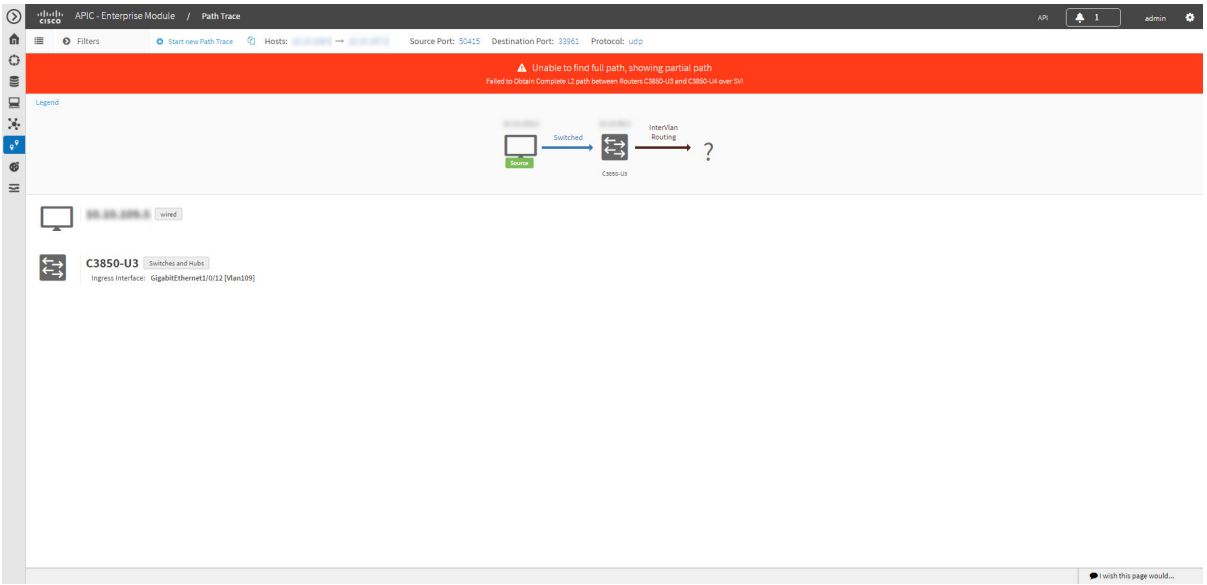
You must have enabled Dynamic QoS and applied or reapplied policies for Dynamic QoS to be in effect. For information, see Enabling and Disabling Dynamic QoS, on page 54.

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

Step 2 From the **EasyQoS** window, click the **Dynamic QoS** tab.

Step 3 Locate the flow that you want to troubleshoot.

Step 4 For that flow, click **Troubleshoot** in the **Path Trace** column.
A path trace is conducted on the selected flow, and the results are displayed in **Path Trace** in a separate browser window. For information about interpreting path trace results, see the *Cisco Path Trace Application for APIC-EM User Guide*.



CHAPTER 5

Monitoring EasyQoS

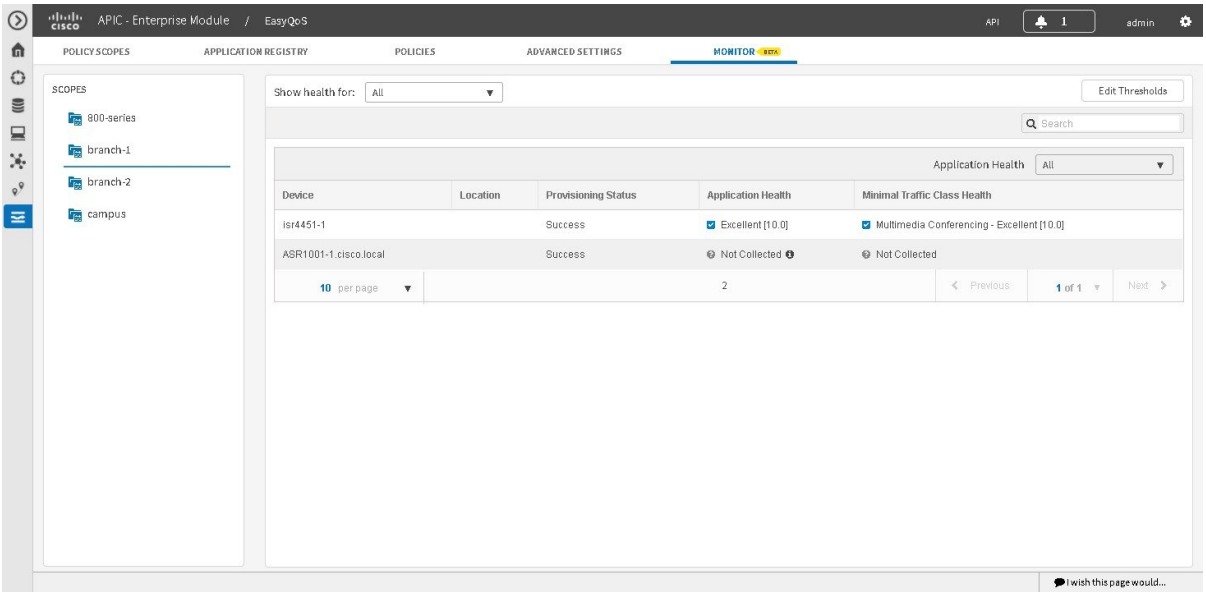
Information about Monitoring EasyQoS

Cisco EasyQoS permits you to monitor an application's health on router WAN interfaces in your network for troubleshooting purposes. You view this data from the **Monitoring** window.

Note For this release, EasyQoS monitoring is provided as a beta functionality. The supported scale for this feature is 4000 managed devices including 400 monitored interfaces (200 routers with 2 interfaces each.)

The network devices are polled every 10 minutes to obtain the monitoring statistics.

Figure 20: Monitoring Window



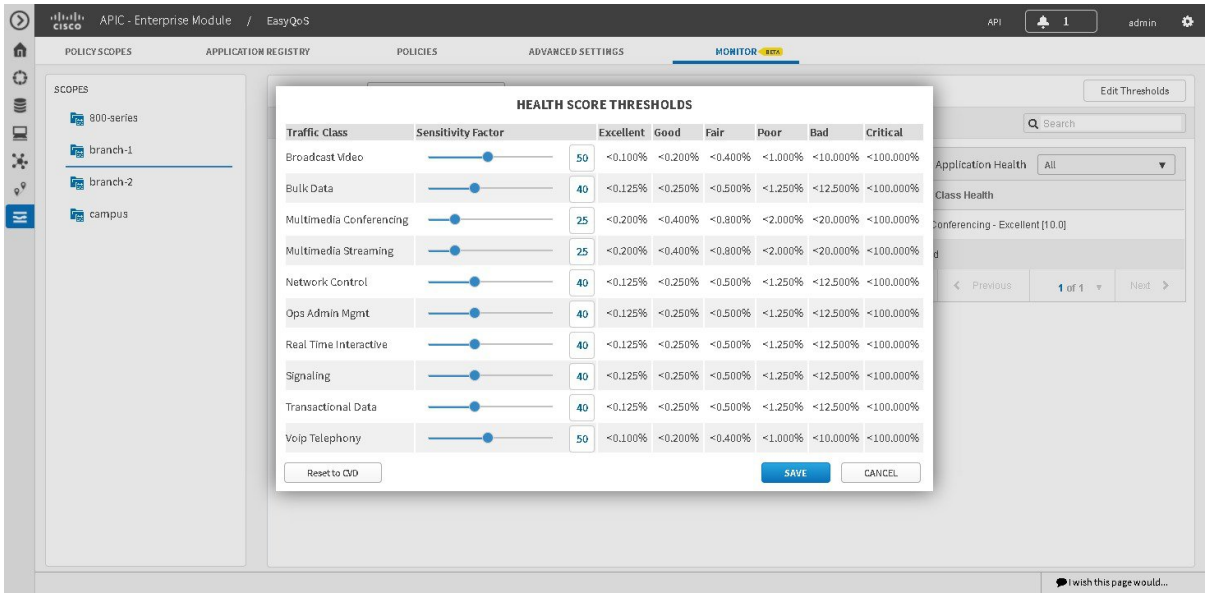
The health of each application is measured as a sensitivity to packet loss on the device's WAN interface. This sensitivity is given a numerical value. The higher the sensitivity factor the more sensitive for packet loss (e.g. factor =5 => Excellent < 1%, factor = 100 => Excellent < 0.05%). The lower the sensitivity factor the less sensitive for packet loss.

Sensitivity to packet loss is different for each traffic class; for example, broadcast video is very sensitive to packet loss as compared to other applications. For this reason, each application (within a traffic class) has a different threshold.

You can view the sensitivity factor and thresholds for the traffic class in the **Health Score Thresholds** table. The **Health Score Thresholds** table is accessible from the **Monitoring** window by clicking the **Edit Threshold** button. This table displays how the default thresholds for the different traffic classes are defined. For each traffic class row there exists a range of values that is mapped to one of the Health Score Grades (Excellent, Good, Fair, Poor, Bad, Critical). The 0-100 percentage value (score) is calculated for each grade by linerly splitting the range into two parts and deciding upon the correct score.

You are able to reconfigure the sensitivity factor for each traffic class and therefore, each application. For information, see Changing Sensitivity Factor for the Traffic Class, on page 66.

Figure 21: Health Score Thresholds

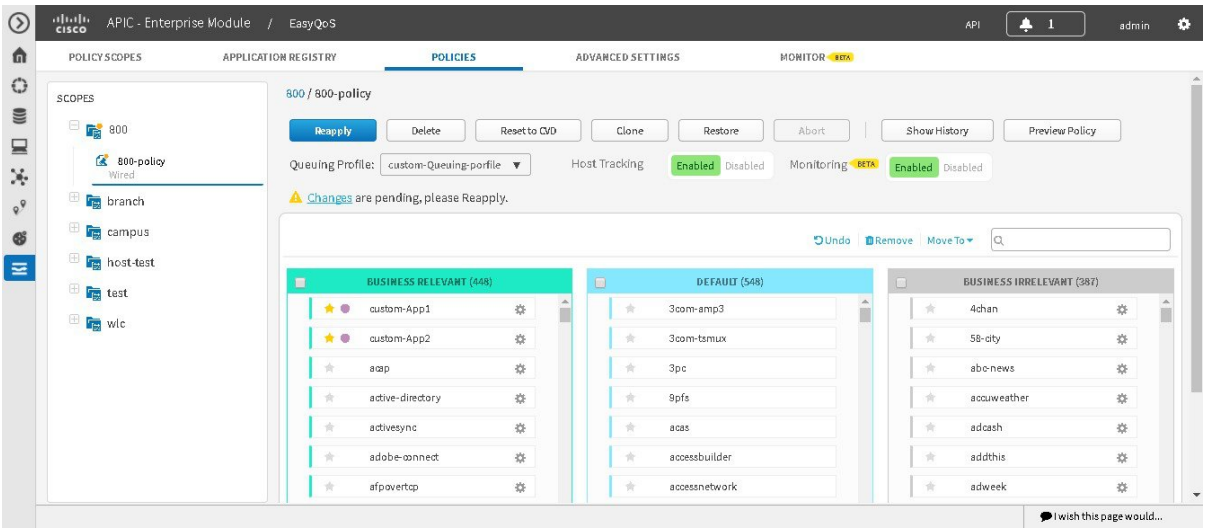


Enabling Monitoring for EasyQoS

Cisco EasyQoS permits you to monitor the health of the applications on the devices in your network. You can use this information to assist in troubleshooting any issues with the applications and devices.

The health of applications is measured as a sensitivity to packet loss on the router's WAN interface. To monitor the health of applications, you must first enable this feature in the **Scopes** pane of the **Policies** window.

Figure 22: Enabling Monitoring for EasyQoS



Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

Make sure that you have discovered your complete network topology.

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

Define the scope of devices that you want to be configured with this QoS policy. You can do this by creating a policy tag in Topology or Device Inventory or by creating a policy scope in EasyQoS.

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

Step 2 Click the **Policies** tab.

Step 3 From the **Scopes** pane, select a policy scope.

Step 4 Click the **Enabled** button in the **Monitoring** field.
When prompted to confirm you selection, click **OK**.

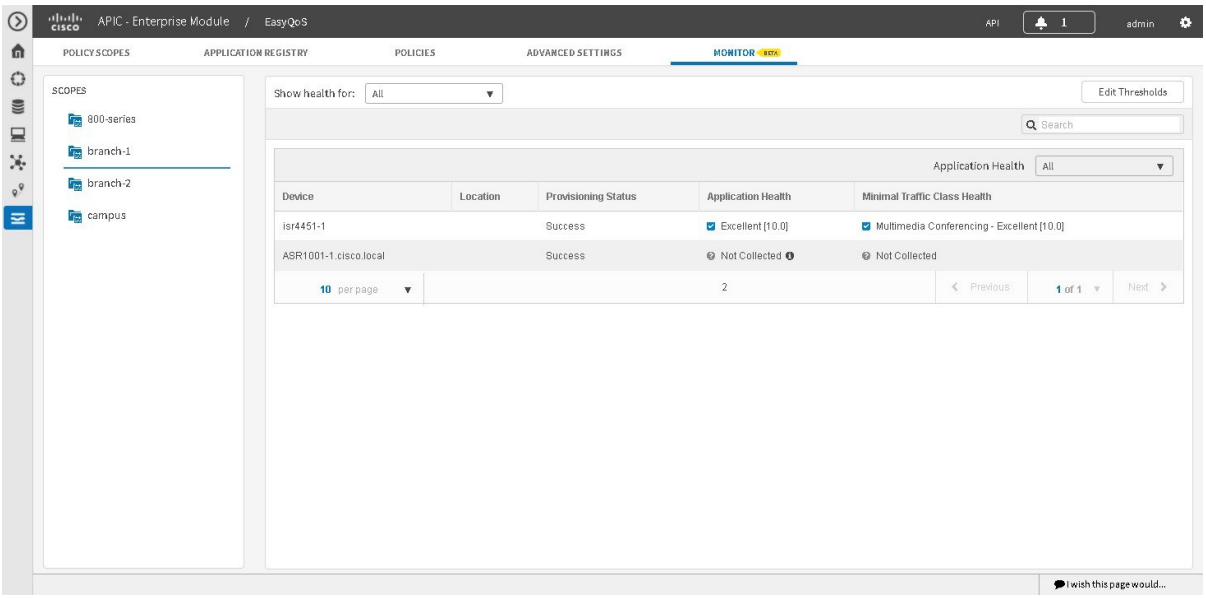
What to Do Next

Click the **Monitor** tab to access the **Monitor** window.

Filtering for the Device and its Application Health

You can filter for a specific device and view its application health using the monitoring function of EasyQoS. Follow the procedures described below to perform this task.

Figure 23: Monitoring Window



Note For device and its application data to appear in the **Monitoring** window, the following requirements must be met:

- The device is a router. Only Cisco router data appears in the **Monitoring** window.
- The device has an active NBAR license.
- The device's interface is a WAN interface.
- Monitoring has been enabled for the scope. For information about this procedure, see Enabling Monitoring for EasyQoS, on page 59.

Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

Make sure that you have discovered your complete network topology.

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

Define the scope of devices that you want to be configured with this QoS policy. You can do this by creating a policy tag in Topology or Device Inventory or by creating a policy scope in EasyQoS.

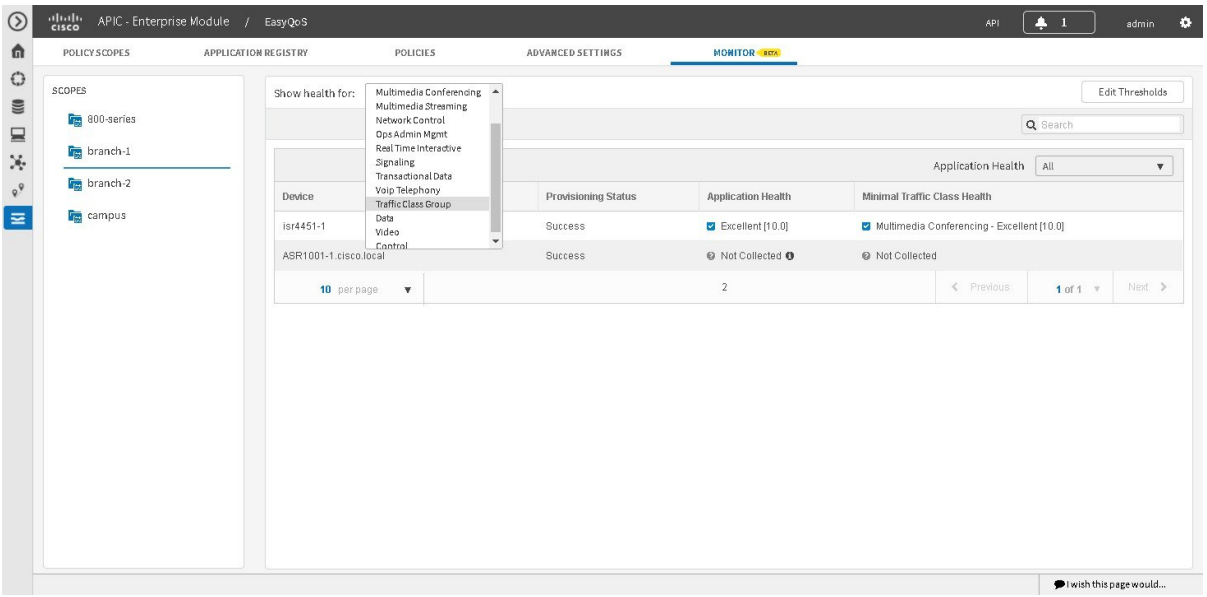
Step 1 From the **Navigation** pane, click **EasyQoS**.

Step 2 Click the **Monitoring** tab.
The EasyQoS **Monitoring** window opens.

Step 3 In the **Scopes** pane, click the specific scope for the health of the devices.

Step 4 In the **Show health for:** field, click the drop-down arrow and select a traffic class.
For example, select BROADCAST_VIDEO from the menu.

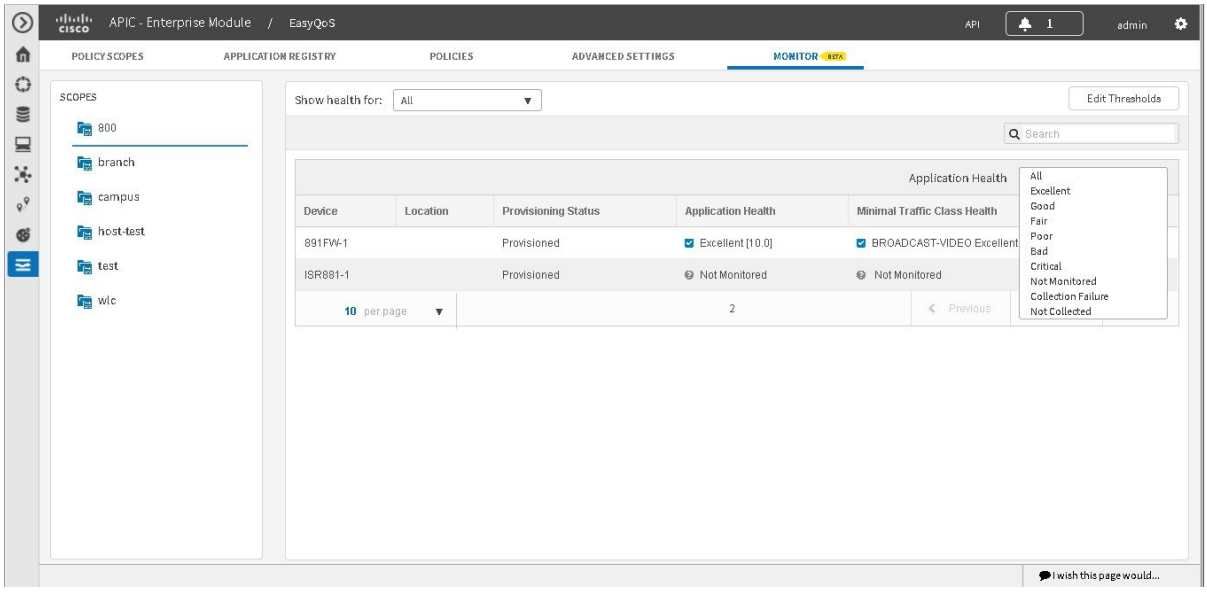
Figure 24: Option for Traffic Class Selection



Step 5 In the **Search** field, enter the device name to display the device in the **Monitoring** window.

Step 6 Select the appropriate filter in the **Application Health** field.

Figure 25: Option for Application Health Selection



The following application health filters are available:

- **Excellent**
- **Good**
- **Fair**
- **Bad**
- **Poor**
- **Not Monitored**
- **Collection Failure**
- **Not Collected**

The application health filters (and values) are determined by pre-configured thresholds for packet sensitivity. You can reconfigure these pre-configured thresholds. For information about this procedure, see Changing Sensitivity Factor for the Traffic Class, on page 66.

Step 7 Proceed to review the device and its application health.
The following information is displayed:

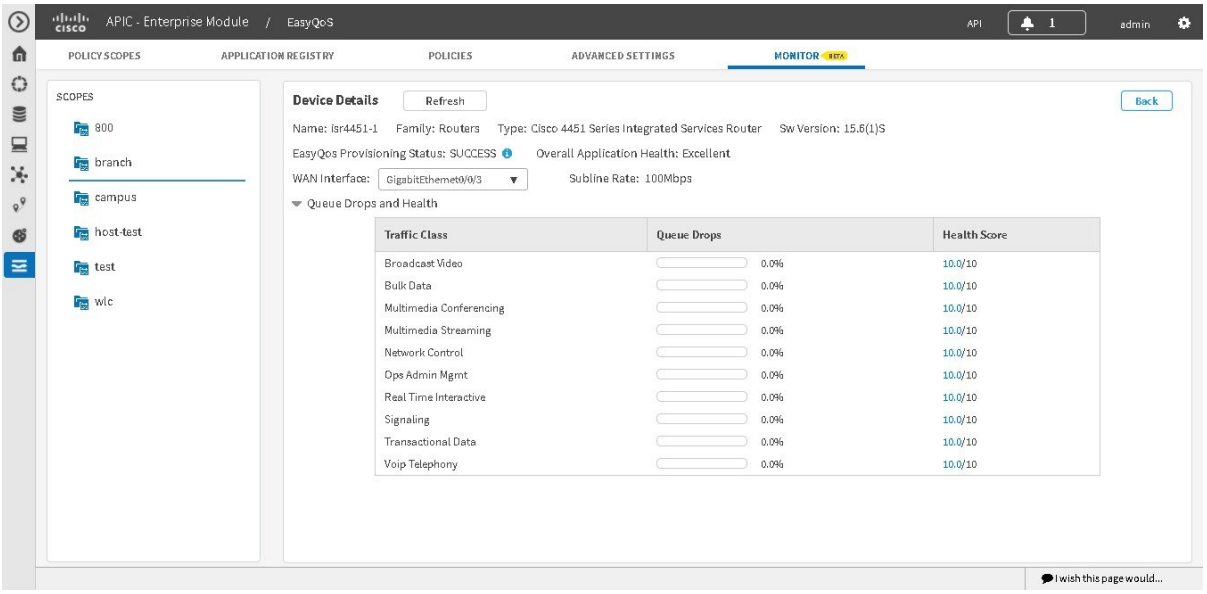
- **Device**
- **Location**
- **Provisioning Status**

- **Application Health**
- **Minimal Traffic Class Health**

Note The interface can have traffic from multiple traffic classes flowing through it. The Monitoring tool captures packet loss for each traffic class and aggregates this information for an application health score for the interface. Due to this aggregation, one or more traffic classes can actually have packet loss, but this fact could be hidden at this level since the rest of the traffic classes health are good. Therefore to provide additional information, the minimal traffic class health provides the health of the traffic class with the lowest traffic score.

Step 8 Click on the name of the device in the table to view its device data.

Figure 26: Device Details



The following device data appears:

- **Name**
- **Family**
- **Type**
- **Software Version**
- **EasyQoS Provisioning Status**
- **Overall Application Health**
- **WAN Interface**

  Based on the interface selection, you are able to view the queue drops and health for all traffic classes.
- **Subline Rate**
- **Queue Drops and Health** (by Traffic Class)

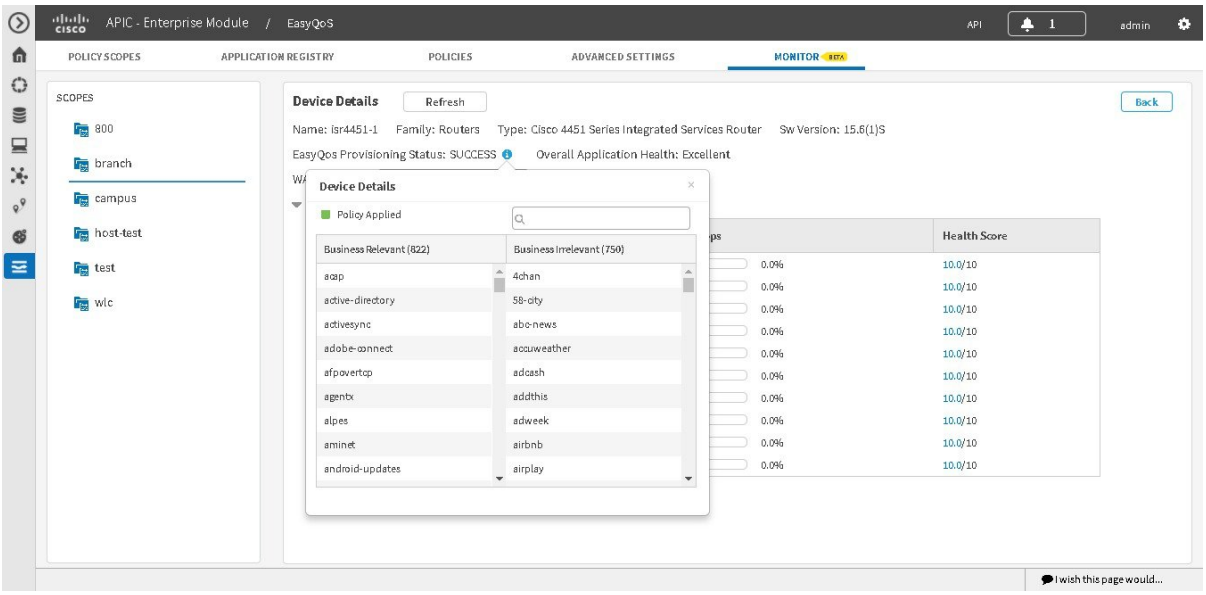
  Based on the health score values, the progress bar displays the appropriate color.

Note In case of a Cisco router with Cisco IOS Polaris greater than or equal to 16.3, then this GUI view also includes a WebUI link.

Clicking **Back** closes the device data pop-up.

Step 9 Clicking the information icon (**i**), displays EasyQoS policies on the device.

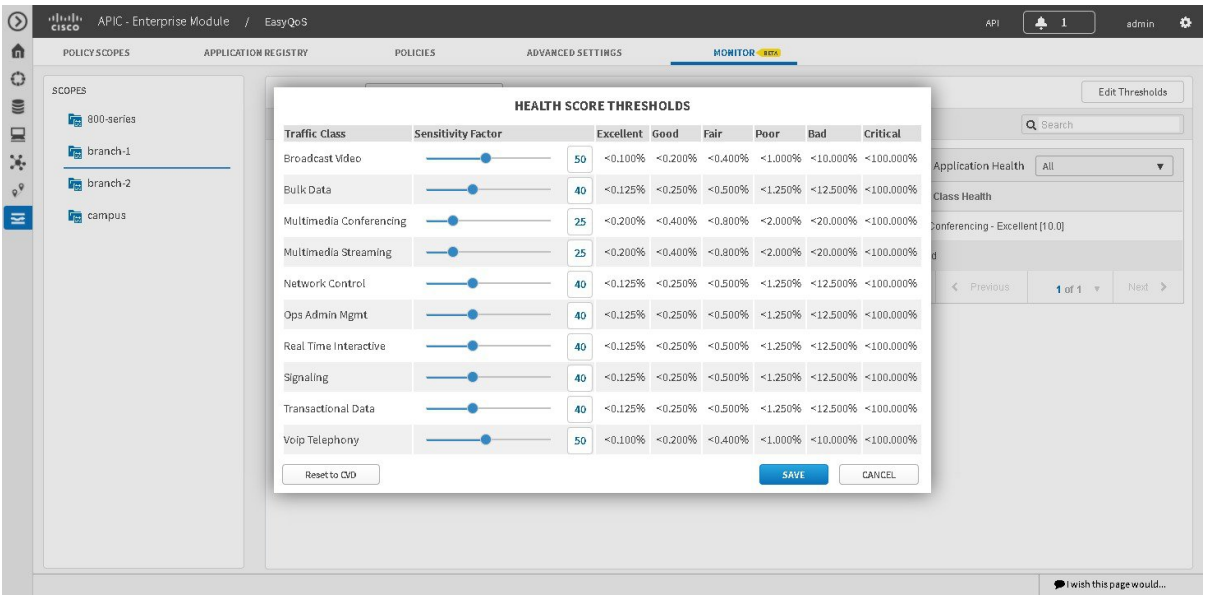
Figure 27: Device Details - Policy Applied



Changing Sensitivity Factor for the Traffic Class

You can change the sensitivity factor for a traffic class to assist in monitoring an application's health. Follow the procedures described below to perform this task.

Figure 28: Health Score Thresholds



Before You Begin

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

Make sure that you have discovered your complete network topology.

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

Define the scope of devices that you want to be configured with this QoS policy. You can do this by creating a policy tag in Topology or Device Inventory or by creating a policy scope in EasyQoS.

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

Step 2 Click the **Monitoring** tab.
The EasyQoS **Monitoring** window opens.

Step 3 In the **Scopes** pane, click the specific scope for the health of the devices.

Step 4 Click the **Edit Threshold** button at the upper right of this window.
The **Health Scores Thresholds** window then appears.

The **Health Score Thresholds** table displays how the default thresholds for the different traffic classes are defined. For each row there exists a range of values that is mapped to one of the Health Score Grades (Excellent, Good, Fair, Poor, Bad, Critical). The 0-100 percentage value (score) is calculated by linerly splitting the range into two parts and deciding upon the correct score.

Note Only Cisco router data appears in the **Health Score Thresholds** table. When applying an EasyQoS policy, relevant interfaces on the devices in the scope are registered or unregistered to display in this table. The criteria for registering an interface (and displaying in the table) is as follows: the device is a router, the device supports NBAR, the device interface is a WAN interface, and monitoring is enabled for the scope.

Step 5 To adjust the sensitivity for a traffic class, click on the blue circle icon in the sensitivity column and move it (with the bar) to either increase to decrease sensitivity.
All of the information in the table is read-only, except for the sensitivity factor for each traffic class which can be modified to be any number between 1-100 by adjusting the bar.

Step 6 Click the **Save** button to save the changes and exit the menu pop-up.
To cancel and exit the menu pop-up, click **Cancel**. You can also reset to the defaults, by clicking **Reset to CD**.

APPENDIX A

Cisco APIC-EM and Apple Fastlane

About Cisco APIC-EM and Apple Fastlane

Cisco APIC-EM through its EasyQoS application supports Apple Fastlane. This support provides the following benefits to your network:

- Optimization of Wi-Fi connectivity for Apple iOS devices in the network, as well as most other wireless clients running real-time applications. This feature provides support for a reliable voice experience even in a congested network environment.
- Prioritization of business applications. With Cisco EasyQoS, the network administrator can prioritize the applications as per the environment.

Cisco APIC-EM and Apple Fastlane Requirements

The following are the requirements for Cisco EasyQoS support for Apple Fastlane in your network:

- Cisco APIC-EM with release version 1.5.x installed and running
- Supported Apple devices with Apple iOS 10 installed and running

Note For a list of the supported Apple devices, see Cisco APIC-EM and Apple Fastlane Recommended Platforms, Devices, Software, and Licenses, on page 70.

- Cisco AireOS controllers running release 8.3.112 and higher.

Cisco APIC-EM and Apple Fastlane Recommended Platforms, Devices, Software, and Licenses

The following are recommended platforms, devices, software, and licenses for running Apple Fastlane in your network with the Cisco APIC-EM.

- **Infrastructure and Platforms Recommendations**
  - Cisco WLC: Running AireOS 8.3.112 and higher.
  - Cisco WLC: Running 802.11ac Aironet
  - Cisco Catalyst switches
  - Software licenses, maintenance, and support for the above network infrastructure
- **iOS Devices Recommendations (Fastlane)**
  - iPhone 5 and later versions
  - iPad mini 2 and later versions
  - iPad Air and later versions
  - iPad Pro
  - iPod touch (6th generation)

Configuring an Apple Fastlane Solution using APIC-EM

You can use the Cisco APIC-EM controller to assist in configuring support for Apple Fastlane on your network devices (Cisco Wireless LAN controllers). The following procedure describes how the Fastlane macro on the Cisco WLCs configure support for Fastlane, as well as how the Cisco APIC-EM controller assists in configuring support for Apple Fastlane.

The Cisco APIC-EM controller and EasyQoS application will apply the Fastlane QoS policy to WLANs/SSIDs added to a policy scope when the AireOS version is 8.3.112 or higher. Cisco EasyQoS simply replaces the default AVC Profile generated by Fastlane with a new AVC profile which contains the applications selected within the EasyQoS graphical user interface.

Before You Begin

Map out the network path or paths for IP traffic for your Apple Fastlane solution.

Determine the Cisco Wireless LAN Controllers (WLCs) in the network path or paths that must be configured for Apple Fastlane.

Ensure that you have met all of the software requirements for the Apple devices and Cisco WLCs that are to be part of your Apple Fastlane solution.

Step 1 On the Cisco Wireless LAN (WLAN) Controllers (WLC) in your network that are to be part of the Apple Fastlane traffic paths, configure the Platinum profile by setting unmarked and multicast traffic to "best effort".

Note Fastlane is a macro which runs on the Cisco WLC platforms. When you enable Fastlane, the Cisco WLC automatically performs this step and configures the Platinum profile by setting unmarked and multicast traffic to "best effort".

Refer to your Cisco WLC documentation for information about the Platinum profile.

Step 2 On the Cisco WLCs, disable UDP bandwidth limitations for the Platinum profile.

Note When you enable Fastlane, the Cisco WLC automatically performs this step and disables UDP bandwidth limitations for the Platinum profile.

Refer to your Cisco WLC documentation for information about UDP bandwidth limitations for the Platinum profile.

Step 3 Apply the Platinum profile to the target WLAN(s).

Note When you enable Fastlane, the Cisco WLC automatically performs this step and applies the Platinum profile to the target WLAN(s).

Refer to your Cisco WLC documentation for information about the Platinum profile to the target WLAN(s).

Step 4 Enable both Aironet Client Monitor (ACM) and Call Admission Control (CAC).

Note When you enable Fastlane, both Aironet Client Monitor (ACM) and Call Admission Control (CAC) are automatically enabled.

Refer to your Cisco WLC documentation for information about ACM and CAC.

Step 5 Limit voice bandwidth reservation to fifty (50) percent.

Note When you enable Fastlane, the voice bandwidth reservation is automatically limited to fifty (50) percent.

Refer to your Cisco WLC documentation for information about voice bandwidth reservation on the Cisco devices.

Step 6 Enable WMM EDCA (Wi-Fi Multimedia Enhanced Distributed Channel Access) profiles.

Note When you enable Fastlane, the WMM EDCA (Wi-Fi Multimedia Enhanced Distributed Channel Access) profiles are automatically enabled.

Refer to your Cisco WLC documentation for information about the WMM EDCA profiles.

Step 7 On the Cisco APIC-EM controller, create a QOS-PROFILE with customized applications.

Note When you enable Fastlane, it automatically performs this step and creates the QoS-Profile with customized applications. However, EasyQoS will create it's own AVC Profile based on the applications selected within the EasyQoS graphical user interfaces for the policy scope. EasyQoS will replace the system generated QOS-PROFILE with the AVC Profile it generates.

For information about configuring an EasyQoS profile, see Creating or Editing a Policy, on page 36.

Step 8 On the Cisco WLCs in your network, configure best practice UP-to-DSCP and DSCP-to-UP mapping.

Note When you enable Fastlane, best practice UP-to-DSCP and DSCP-to-UP mappings are automatically configured.

Refer to your Cisco WLC documentation for information about UP-to-DSCP and DSCP-to-UP mapping.

Step 9 Enable upstream QoS trust.

Note When you enable Fastlane, upstream QoS trust is automatically enabled..

Refer to your Cisco WLC documentation for information about upstream QoS trust in your network.