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 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. **Note** This application is not bundled with the Cisco APIC-EM controller for this release. You need to download, install, and enable this application to use it. For information about these procedures, see the *Cisco Application Infrastructure Controller Enterprise Module Upgrade Guide*.
Cisco Intelligent WAN (IWAN) application	The separately licensed IWAN application for APIC-EM simplifies the provisioning of IWAN network profiles with simple business policies. The IWAN application defines business-level preferences by application or groups of applications in terms of the preferred path for hybrid WAN links. Doing so improves the application experience over any connection and saves telecom costs by leveraging cheaper WAN links. **Note** This application is not bundled with the Cisco APIC-EM controller for this release. You need to download, install, and enable this application to use it. For information about these procedures, see the *Cisco Application Infrastructure Controller Enterprise Module Upgrade Guide*.

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

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

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*.

Related Topics

Defining Policy Scopes

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 8.

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 11.

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.)
		AF21	BW Queue and DSCP WRED	

Business Relevance	Application Class	Per-Hop Behavior	Queuing and Dropping	Application Description
	Transactional Data (Low-Latency Data)			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 9

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 5 .

  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 Dynamic QoS, on page 16.

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 independent of each other, you may reapply a policy version that contains applications in it that no longer exist.

Note Application level modifications like rank, port, and protocol are not 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 configuration, 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) through EasyQoS should be removed. Previous configurations may not be restored.

After you restore the original policy configuration to the device, the EasyQoS policy is deleted from the Cisco APIC-EM. 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.
- If a device is removed from an EasyQoS policy after that policy has been applied to the device, then the EasyQoS policy will remain on that device. In other words, EasyQoS will not automatically attempt to delete the QoS policy provisioned to the device, nor will EasyQoS attempt to restore the QoS configuration on that device to the original (pre-EasyQoS) configurations.

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.)

Each of the four predefined SP profiles support the following features:

- A fixed number of traffic classes (4, 5, 6, and 8 classes).
- A fixed mapping of the DSCP values and priority treatment from the traffic classes within the organization to the traffic classes within the service provider network.
- Fixed bandwidth allocations between the service provider traffic classes.

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.

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.

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 Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
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

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

Related Topics

Creating a Customized Service Provider Profile
Editing a Customized Service Provider Profile
Verifying the WAN Interface Synchronization Status

Understanding Queuing Profiles

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

Important Queuing 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 queuing 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 queuing policy. If no queuing policy is assigned, the QoS policy uses the default, Cisco Validated Design (CVD) queuing policy.

If you change a queuing 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 queuing policy.

Table 7: Default CVD Queuing Policy

Traffic Class	Default Bandwidth (Total = 100%) [4]
Voice	10%
Broadcast Video	10%
Real-Time Interactive	13%
Multimedia Conferencing	10%
Multimedia Streaming	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%.

Related Topics

Configuring Queuing Profiles

Understanding Dynamic QoS

Dynamic QoS is used on LAN interfaces where you need a specific class of service to be in effect for the duration of some event. You can configure another software application to signal the Cisco APIC-EM (through REST APIs) when a specified event occurs so that a corresponding QoS policy is applied to the relevant network devices for the duration of the event.

Important 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

Related Topics

Enabling and Disabling Dynamic QoS
Troubleshooting Dynamic QoS

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.
- 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.

Note The Core, Distribution, and Access device roles apply to Cisco Catalyst switches. The Access device role also applies to Wireless LAN Controller platforms. The Border Router device role applies only to Cisco ISR and ASR router platforms. You should verify that the particular device selected has been characterized with the correct role, in order to ensure that the correct QoS policy is applied to the device by the EasyQoS application. This applies primarily to Cisco Catalyst switches. If necessary, you can change the device role using the controller's GUI.

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 9.
- 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*

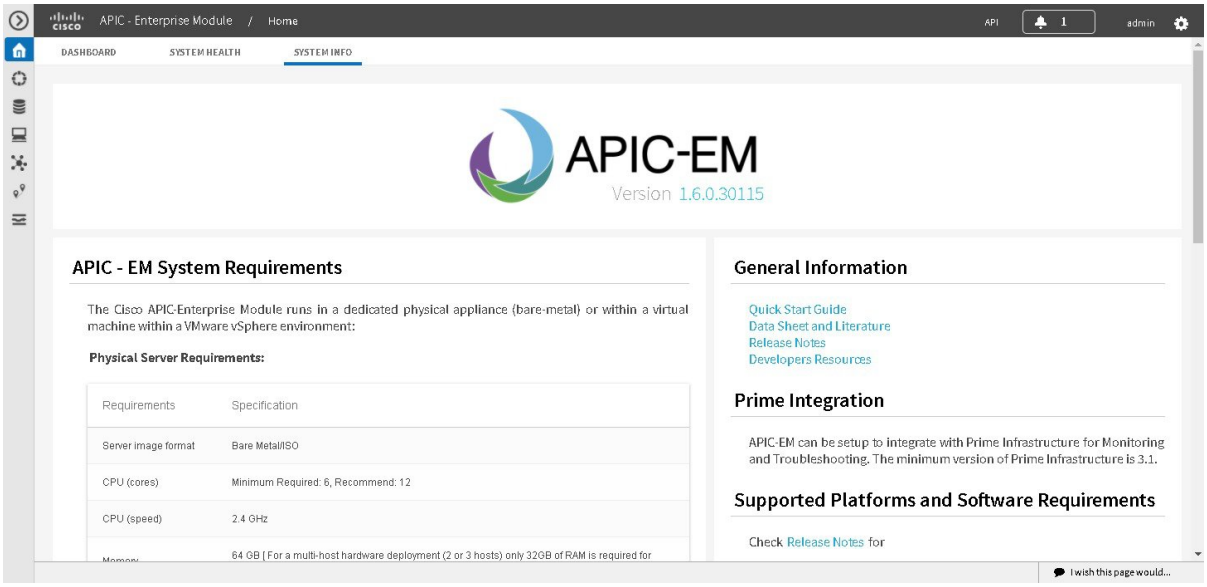
Step 2 On the launch page, enter your username and password that you configured during the deployment procedure.

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



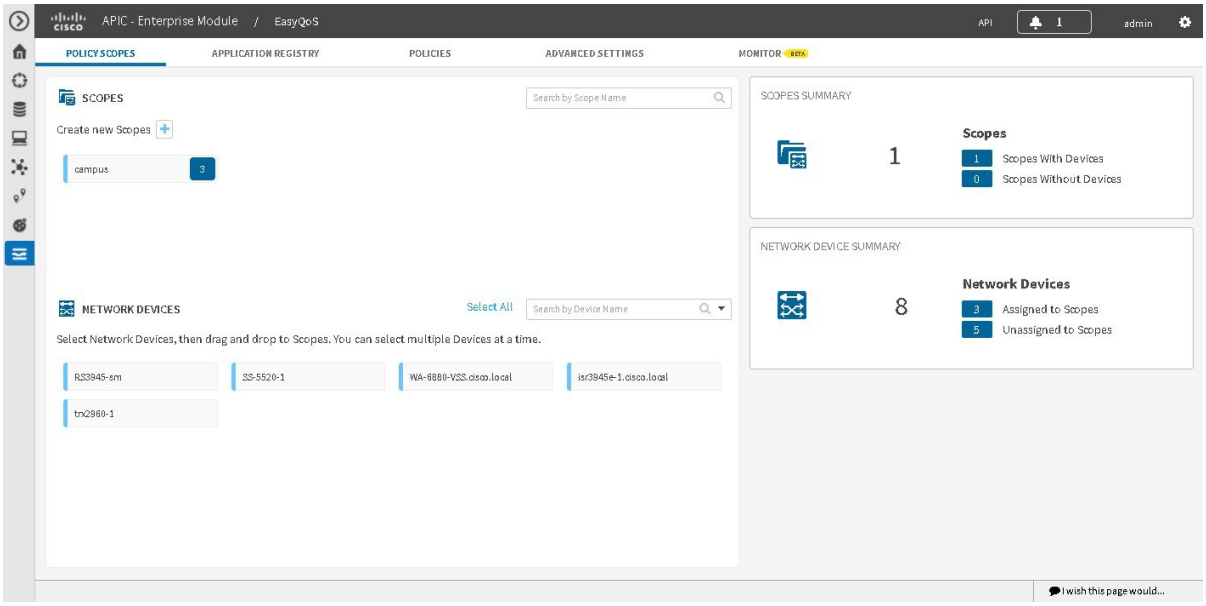
What to do next

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:
  - **Queuing 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.

Note Monitor is a beta functionality for this release.