Configuring Quality of Service

About EasyQoS

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

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

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

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

EasyQoS Prerequisites

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

- Enable the EasyQoS feature on the controller. For information, see Enabling the EasyQoS Beta Feature, on page 10.
- EasyQoS supports most of the Cisco LAN, WAN, WLAN devices. To verify whether the devices and software versions in your network are supported, see the *Supported Platforms for the Cisco Application Policy Infrastructure Controller Enterprise Module* document.
- Make sure that your Cisco network devices, such as the ISR-G2, the ASR 1000, and Wireless LAN Controller, have the AVC (Application Visibility and Control) feature license installed. For information, see the *NBAR2 (Next Generation NBAR) Protocol Pack FAQ* at the following URL: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/network-based-application-recognition-nbar/qa_C67-723689.html.
- For the Cisco APIC-EM to identify the WAN interfaces that need policies, you must specify the interface type (WAN) and (optionally) its subline rate and service-provider Class-of-Service model. For information about how to configure these settings on WAN interfaces, see Required Device Configuration.
- From the **Topology** or **Device Inventory** window, verify that the device roles assigned to devices during discovery are appropriate for your network design. If necessary, change any of the device roles that are not appropriate.

Understanding QoS Policies

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

- **Policy Scope—**Group of devices that will be configured with the policy.
- **Applications—**Software programs or network signaling protocols that are being used in your network. EasyQoS includes the Cisco Network Based Application Recognition, second generation (NBAR2) application library of approximately 1400 distinct applications. For more information about NBAR2, see the following URL: http://www.cisco.com/c/en/us/products/ios-nx-os-software/network-based-application-recognition-nbar/index.html.
- **Traffic Classes—**Groups of applications that make configuring policies easier, because the groups contain applications that have similar traffic needs.
- **Business-relevance—**Attribute that classifies a given application according to how relevant it is to your business and operations. The attributes are business relevant, default, and business irrelevant. For information, see Business-Relevance Groups, on page 6.

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

  For example, YouTube is set as business-irrelevant (by default), because most customers typically classify this application this way. However, this classification may not be the true for all companies; for

example, some businesses may be using YouTube for training purposes. In such cases, an administrator can change this business-relevancy setting to **business-relevant** to align with their business objectives.

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

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

- Cisco Validated Designs
- Enterprise Medianet Quality of Service Design 4.0
- Medianet Campus QoS Design 4.0
- Medianet WAN Aggregation QoS Design 4.0

Policy Scope

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

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

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

You define policy scopes from the **EasyQoS** window or by applying policy tags to devices in the **Device Inventory** or **Topology** windows. For more information, see Defining a Policy Scope, on page 17 or Adding or Removing a Policy Tag in Device Inventory.

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 9.

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 or captured in policy versioning.

Processing Order for Devices with Limited Resources

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

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

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

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

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

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

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

Application Configuration Order	Reason
1. Custom application, custom_realtime	Custom applications are given highest priority. Given that the custom_salesforce and custom_realtime applications have the same rank and popularity, they are sorted alphabetically, custom_realtime before custom_salesforce.
2. Custom application, custom_salesforce	
3. Favorite application, gss-http	Because both of these applications have been designated as favorites, they have the same application ranking. So, then EasyQoS evaluates them according to their traffic class. Because gss-http is in the Ops Admin Mgmt traffic class, it is processed first, followed by the corba-iiop application, which is in the 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 Applications

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

Some devices require an NBAR2 license. For information, see EasyQoS Prerequisites, on page 2.

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

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

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

If you have additional applications that are not included in EasyQoS, you can add them as custom applications. For information, see Custom Applications, on page 8.

Business-Relevance Groups

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

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

Marking, Queuing, and Dropping Treatments

Cisco EasyQoS bases its marking, queuing, and dropping treatments on RFC 4594 and the business relevancy category that you have assigned to the application. EasyQoS assigns all of the applications in the Default category to the Default Forwarding application class and all of the applications in the Irrelevant Business cateogry 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 1: Marking, Queuing, and Droping Treatments

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

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

1 VoIP signaling traffic is assigned to the Call Signaling class.

2 WRED is not be enabled on this class, as network control traffic should not be dropped.

3 WRED is not enabled on this class, as OAM traffic should not be dropped.

Custom Applications

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

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

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

Favorite Applications

Cisco APIC-EM allows you to flag applications that you want EasyQoS to configure on devices before all other applications, except custom applications. Flagging an application as a favorite helps to ensure that the QoS policies for your favorite applications get configured on devices. For more information, see Processing Order for Devices with Limited Resources, on page 4.

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.

Understanding Dynamic QoS

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

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

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

EasyQoS Guidelines and Limitations

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

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

- When you provision a device using IWAN, you cannot apply a Cisco APIC-EM policy tag to the same device. To apply a Cisco APIC-EM policy tag, you must delete the device from the IWAN device inventory and then rediscover it in the Cisco APIC-EM.
- Changing a policy tag *does not* automatically roll back or change the policy on the device. You must reapply the policy in order for the updated configuration to be deployed to the device.
- Policies are not removed from a device when the policy tag is removed from the device.
- Policies are not reapplied automatically when you change the policy tag on a device to a different policy tag that has already been applied to devices.
- Policies are not reapplied automatically when you enable dynamic QoS. You must reapply the policy to the devices for the change to take effect.
- EasyQos supports Out Of Band (OOB) changes, that is, changes made to the device configurations from any means other than Cisco APIC-EM. However, after you make the OOB change, you must wait at least 30 minutes until the inventory synchronization occurs and then click **Reapply Policy**.
- EasyQoS supports applications that have names consisting of up to 24 alphanumeric characters, including underscores and hyphens. The underscore and hyphen characters are the only special character allowed in the application name.
- Some network devices have a limited memory (called Ternary Content Addressable Memory or TCAM) for storing network access control lists (ACLs) and access control entries (ACEs). For more information about this limitation and how it is handled, see Processing Order for Devices with Limited Resources, on page 4.
- You cannot create custom applications for wireless devices.
- EasyQoS does not configure ACEs for a custom application that does not define an IP address but does define port number 80, 443, or 8080. However, EasyQoS does configure ACEs for a custom application that does define an IP address and port number 80, 443, or 8080.

Enabling the EasyQoS Beta Feature

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

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

Before You Begin

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

Procedure

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

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

Step 3 Click **EasyQoS Enabled**.

Getting Started with EasyQoS

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

Before You Begin

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

Procedure

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

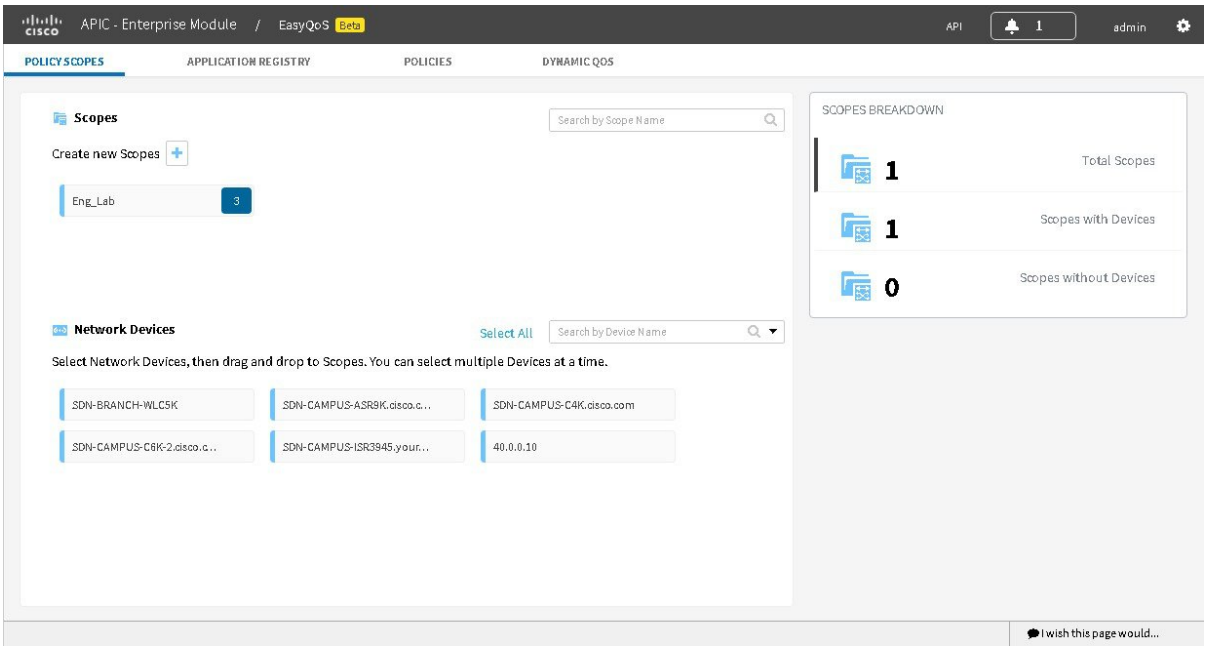
Step 2 With your business objectives in mind, determine the business relevance of your applications.
Decide which category your applications fall into:

- **Relevant—**The application directly contributes to organizational objectives. Such applications include voice, video, streaming and collaborative multimedia applications, database applications, enterprise resource applications, email, file-transfers, content distribution, and so on. These applications are classified, marked, and treated marked according to industry best-practice recommendations (RFC 4594).
- **Default—**The application may or may not be business-relevant. For example, generic HTTP/HTTPS traffic may contribute to organizational objectives at times, while at other times such traffic may not. Applications of this type are treated with a Default Forwarding service (RFC 2474).
- **Irrelevant—**The application has no contribution towards achieving organizational objectives. It is primarily consumer- and/or entertainment-oriented in nature. Applications of this type are treated with a less-than Best Effort service (RFC 3662).

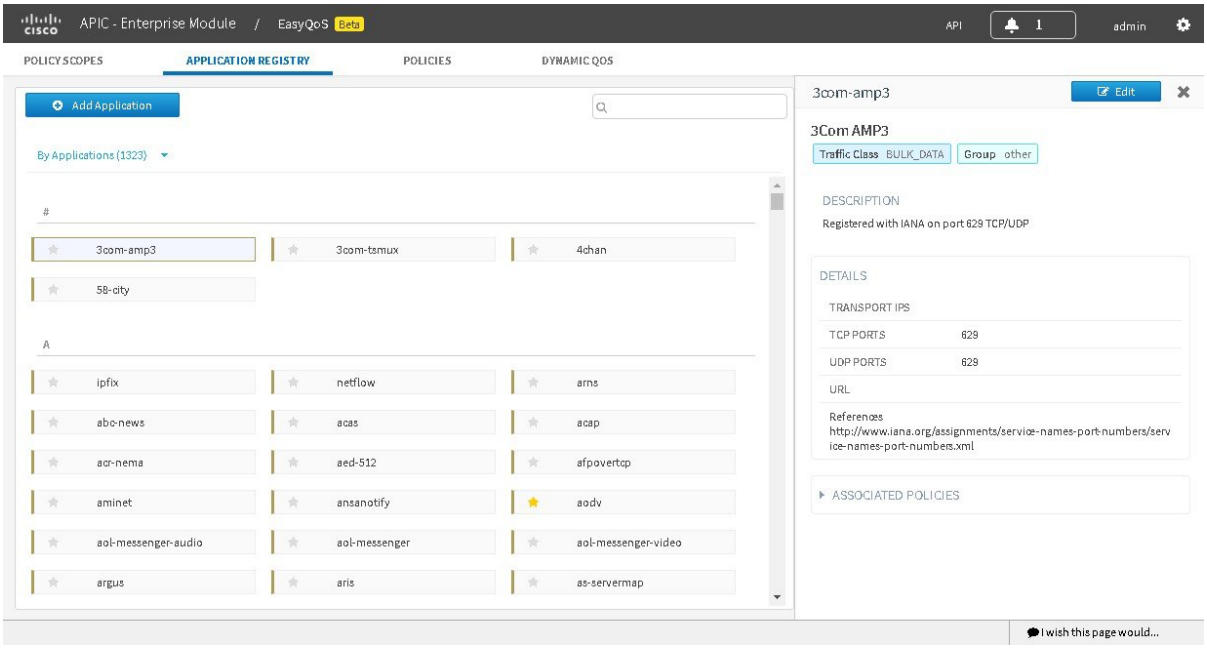
Step 3 Define the scope of devices for a policy.
The scope defines the group of devices that will be configured with the policy.

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

For more information, see Defining a Policy Scope, on page 17.

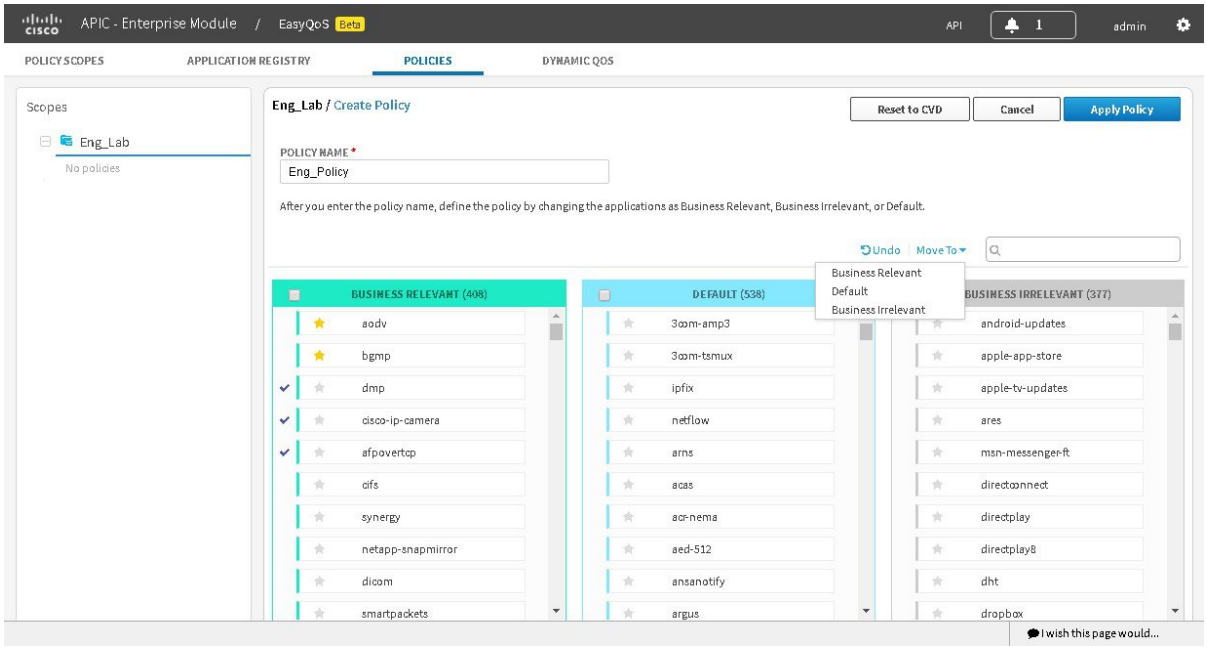


Step 4 Create custom applications.
If you have applications that are not already defined in EasyQoS, you can add them and define their QoS attributes. For more information, see Custom Applications, on page 8.

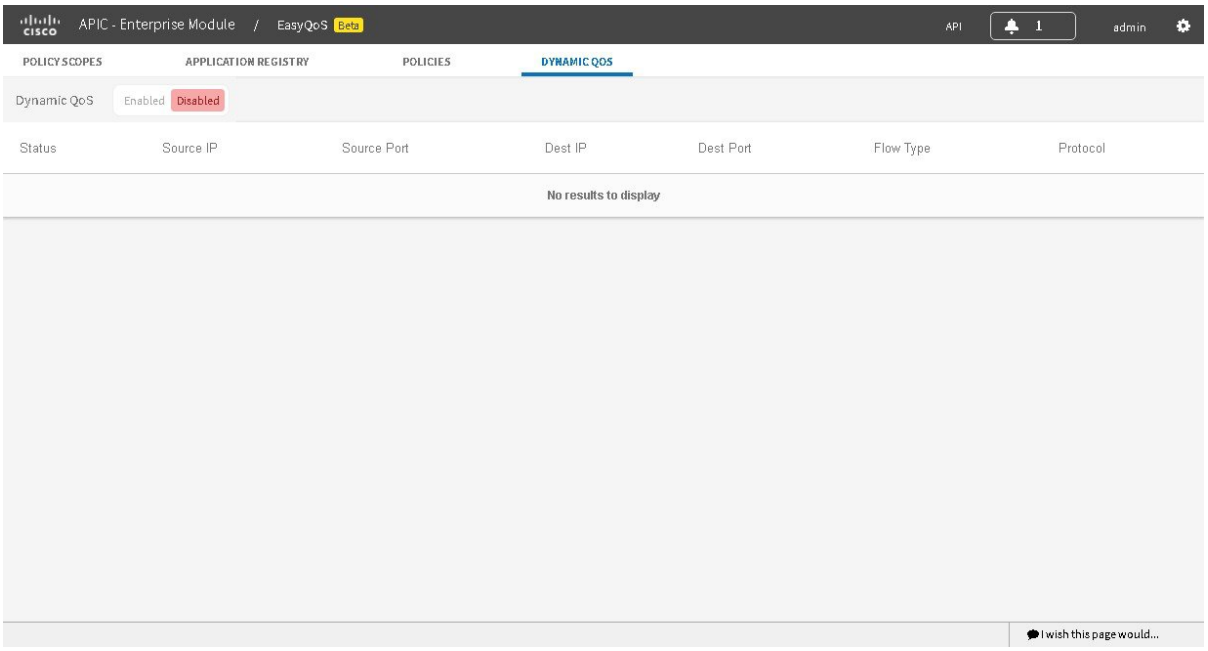


Step 5 Create the policy on wired devices or wireless segments. For information, see Creating a Policy, on page 18.
As part of creating the policy, do the following:

- 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 6.
- 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 9 and Processing Order for Devices with Limited Resources, on page 4.



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



Step 7 Apply the policy to the scope of devices.

What to Do Next

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

Configuring QoS Policies

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

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

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

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

Figure 1: 411235.jpg

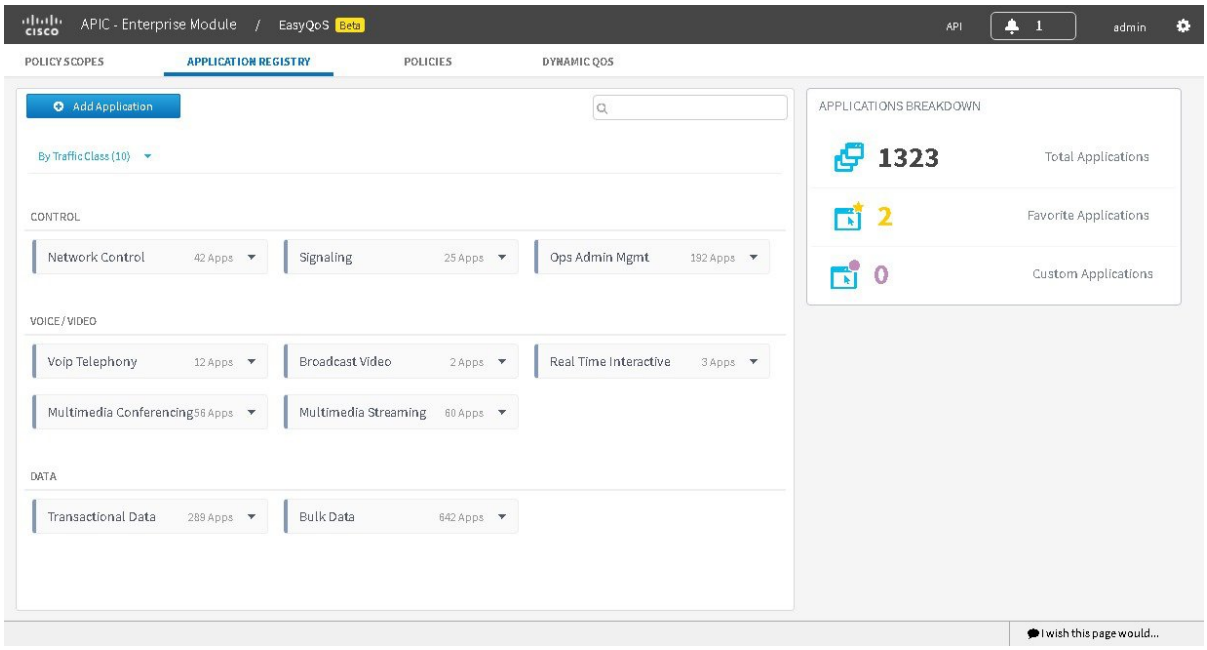


Table 2: Application Registry Tab

Name	Description
Add Application	Allows you to add applications that are not in the list. (For more information, see the next row.)
Search	Finds a specific application by name.
View By icon	Allows you to choose how you want the applications to be displayed: • **Applications—**Lists the applications alphabetically by name. • **Application Groups—**Lists that applicaitons according to the group to which they belong. For example, the **Pop3-Group** contains two applcations: **PostOfficeProtocol3 (pop3)** and **Secure POP3 (Post Office Protocol), standard for email retrieval over SSL (secure pop3)**. • **Traffic Class—**Lists the applications according to the traffic class to which they belong: Custom Applications, Broadcast Video, Bulk Data, Multimedia Conferencing, Multimedia Streaming, Network Control, Ops Admin Mgmt, Real Time Interactive, Signaling, Transactional Data, and Voip Telephony.

Table 3: Policies Tab

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

Table 4: Dynamic QoS Tab

Name	Description
Dynamic QoS pane	Allows you to enable or disable dynamic QoS. Click **Enabled** to enable QoS

Name	Description
Status pane	State of the dynamic policy for the flow. Valid states are as follows: • **ACCEPTED_ADD—**Controller has accepted the dynamic flow for adding the policy to the network. • **CONFIGURING_ADD—**Dynamic policy for the flow is being configured in the network. • **CONFIG_ADD_SUCCESS—**Dynamic policy for the flow was successfully configured in the network. • **CONFIG_ADD_FAILURE—**Errors have occurred while configuring the dynamic policy for the flow. The failureReason field contains the reason for the error. Possible errors include invalid source IP address, EasyQoS not applied to the access device, device unreachable, and so on. • **ACCEPTED_DELETE—**Controller has accepted the dynamic flow for deleting the policy from the network. • **CONFIGURING_DELETE—**Dynamic policy for the flow is in the process of being deleted from the network. The deletion is successful when the flow is no longer displayed on the controller. • **CONFIG_DELETE_FAILURE—**Errors have occurred while deleting the dynamic policy for the flow. The failureReason field contains the reason for the error.
Source IP	Source IP address of the flow.
Source Port	Source transport port number of the flow.
Dest IP	Destination IP address of the flow.
Dest Port	Destination port number of the flow.
Flow Type	Type of flow, either VOICE or VIDEO.
Protocol	Transport protocol of the flow, either TCP or UDP.

Defining a Policy Scope

Before you can create a QoS policy, you need to identify the policy scope. That is, you need to define the group of devices that will be configured with the same QoS policy. For more information, see Policy Scope, on page 3.

Note You can also define a policy scope by applying policy tags to devices from the **Device Inventory** window or the **Topology** window. For information, see Adding or Removing a Policy Tag in Device Inventory and Adding or Removing a Policy Tag in Topology.

Before You Begin

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

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

Procedure

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

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

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

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

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

What to Do Next

You can create policies for wired devices or wireless segments. For information, see Creating a Policy, on page 18.

Creating a Policy

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

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

Before You Begin

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

Make sure that you have discovered your complete network topology.

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

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

Procedure

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

Step 2 Click the **Policies** tab.

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

Step 4 Do one of the following:

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

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

Step 6 If you want to change the business relevance of an application, proceed to the next step. Otherwise, click **Create Policy** to configure the current application settings to the devices.

Step 7 To change an application's business relevance, drag and drop the application from the current business relevancy group to the chosen business relevancy group.

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

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

Step 8 (Optional) If you want, you can designate applications as favorites by clicking the star icon next to the application name.
For information about how favorite applications work, see Favorite Applications, on page 9.

Step 9 Click **Create Policy**.
The policy is configured on the devices in the scope.

Editing a Policy

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

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

Before You Begin

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

Make sure that you have discovered your complete network topology.

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

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

Procedure

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

Step 2 Click the **Policies** tab.

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

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

Step 5 To change an application's business relevance, drag and drop the application from the current business relevancy group to the chosen business relevancy group.

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

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

Step 6 (Optional) To set an application as a favorite, click the star icon next to the application name. To remove the favorite setting, click the start icon again.
For information about how favorite applications work, see Favorite Applications, on page 9.

Step 7 Click **Reapply**.
The policy is updated on the devices in the scope.

Rolling Back a Policy to a Previous Version

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

Before You Begin

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

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

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

Procedure

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

Step 2 Click the **Policies** tab.

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

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

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

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

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

Step 8 Click **Reapply**.
The newest policy version is configured on the devices in the scope.

Cloning a Policy

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

Before You Begin

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

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

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

You must have created at least one policy.

Procedure

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

Deleting a Policy

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

Before You Begin

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

Procedure

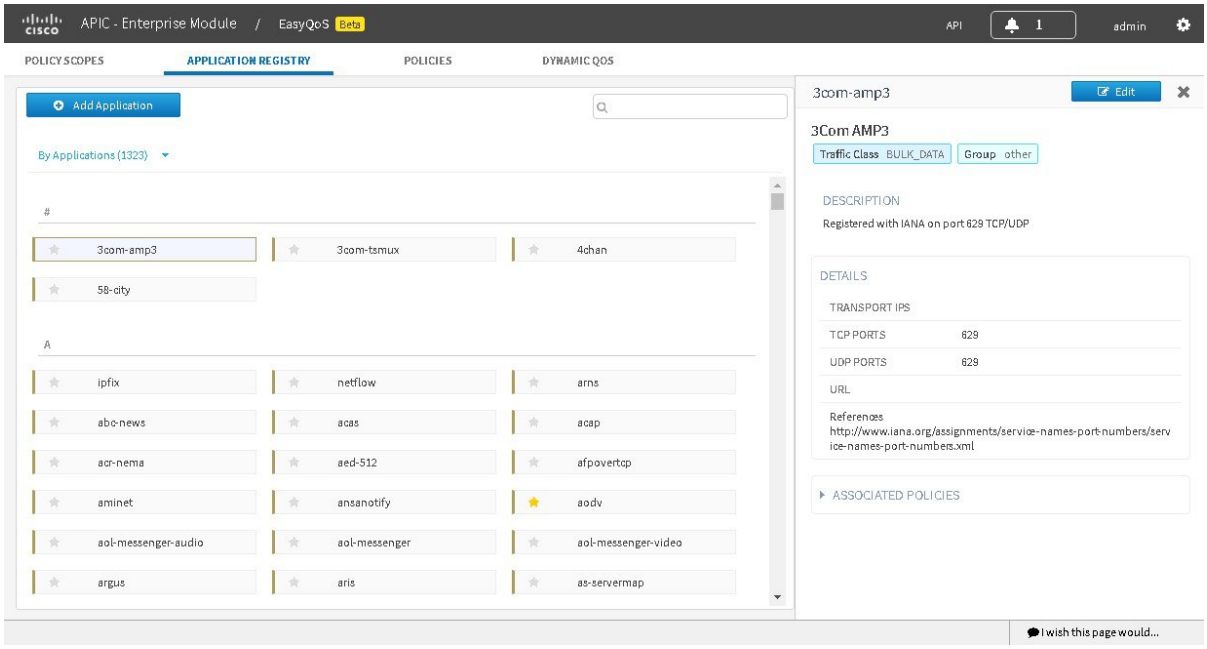
Step 1 From the **Navigation** pane, click **EasyQoS**.
Step 2 Click the **Policies** tab.
Step 3 From the **Scopes** pane, select a policy scope.
Step 4 Under the policy scope name, select a policy.
Step 5 Click **Delete**.
Step 6 To confirm the deletion, click **Ok**. Otherwise, click **Cancel**.
Step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

Configuring Favorite Applications

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

You can also configure favorite applications while creating or editing a policy. For more information, see Creating a Policy, on page 18 or Editing a Policy, on page 19

For information about how favorite applications work, see Favorite Applications, on page 9.



Before You Begin

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

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

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

Procedure

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

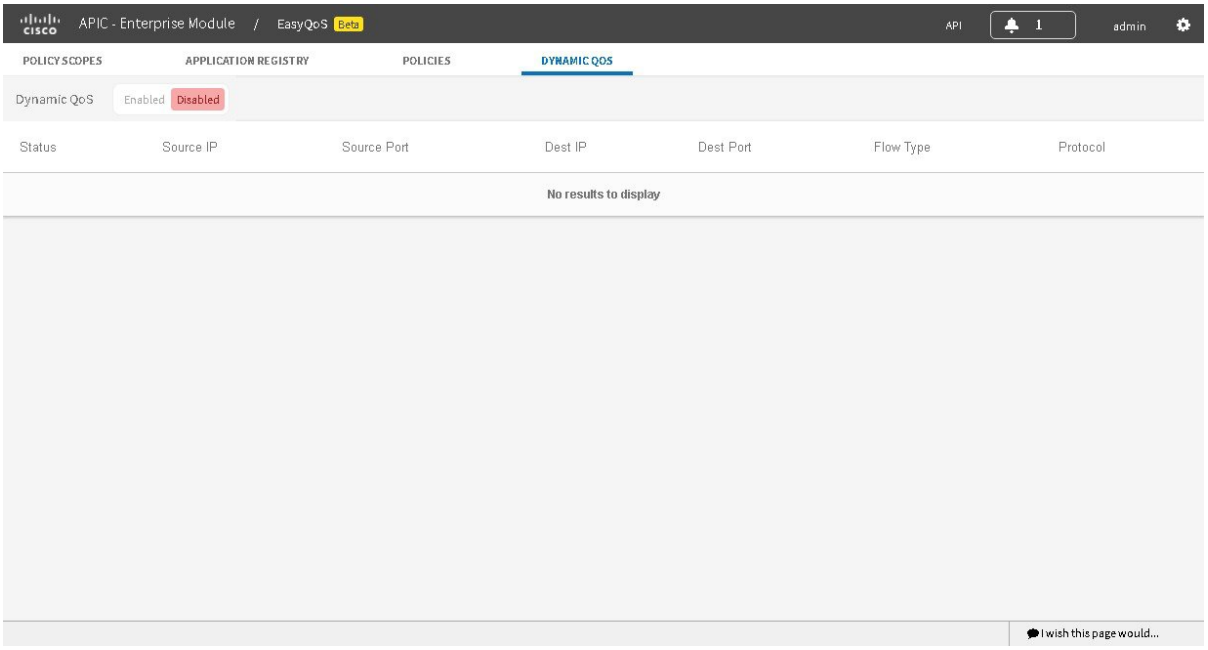
Step 2 From the **EasyQoS** window, select the **Application Registry** tab.
By default, the applications are listed by traffic class. To change how applications are listed, click the **View By** down arrow at the top of the list and choose **Applicaitons** to view the applications in an alphabetical 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 9.

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

Enabling and Disabling Dynamic QoS Policies

You can enable a policy to be dynamically applied to devices. For more information, see Static and Dynamic QoS Policies, on page 3.



Before You Begin

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

You must have created a QoS policy with the appropriate configuration. For information, see Creating a Policy, on page 18.

Procedure

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

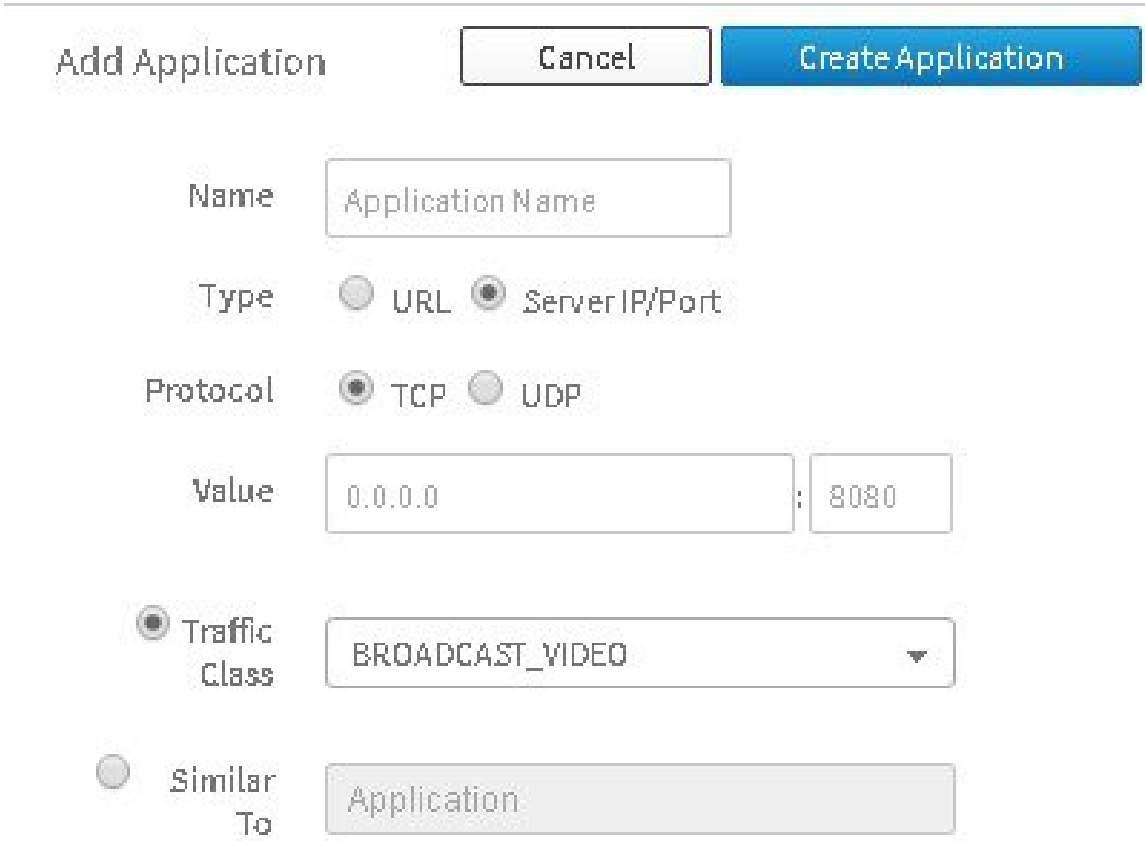
Step 2 From the **EasyQoS** window, click the **Dynamic QoS** tab.

Step 3 In the **Dynamic QoS** field, click **Enabled** to turn on dynamic policy creation or **Disabled** to turn off dynamic policy creation.

Step 4 To apply these configuration changes to the devices, you must reapply the policy to each scope.

Creating a Custom Application

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



Before You Begin

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

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

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

Procedure

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

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

Step 3 Click **Add Application**.

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

- **Name—**Name of the application. The name can contain up to 24 alphanumeric characters, including underscores and hyphens. The underscore and hyphen characters are the only special character allowed in the application name.
- **Type—**Type of application. Choose either **URL** for applications that are accessible through URL or **Server IP/Port** for applications that are accessible through a server IP address and port number.
- **Protocol—**Supported protocol for application. Choose either **TCP** or **UDP**. UDP is available only for applications that are accessible through a server IP address and port number..
- **Value—**The value entered depends on the type of application that is being added. For URL type applications, enter the application URL. For Server IP/Port applications, enter the server IP address and port number through which you access the application.
- **Traffic Class—**Traffic class to which the application belongs. Valid values are BULK_DATA, TRANSACTIONAL_DATA, OPS_ADMIN_MGMT, NETWORK_CONTROL, VOIP_TELEPHONY, MULTIMEDIA_CONFERENCING, MULTIMEDIA_STREAMING, BROADCAST_VIDEO, REAL_TIME_INTERACTIVE, and SIGNALING.
- **Similar To—**Application with the similar traffic-handling requirements. Click the radio-button to select this option and select an application from the drop-down field. EasyQoS copies the other application's traffic class, category, and subcategory settings to the application that you are defining.

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

Step 6 When you create a custom applicaiton, it is not assigned to a business-relevancy group. It is placed in a group called Unassigned. To change this setting, see Editing a Policy, on page 19.

What to Do Next

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

Editing a Custom Application

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

Before You Begin

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

Procedure

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

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

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

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

Information about the application displays in the right hand pane.

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

Step 4 Click **Edit**.

Step 5 Change the desired settings for the custom application:

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

Step 6 Click **Save Application**.

What to Do Next

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

Deleting a Custom Application

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

Before You Begin

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

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

Procedure

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

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

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

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

Information about the application displays in the right hand pane.

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