Configuring Quality of Service

Getting Started With EasyQoS

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

Before You Begin

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

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

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

- **Relevant—**The application directly contributes to organizational objectives. Such applications include voice, video, streaming and collaborative multimedia applications, database applications, enterprise resource applications, email, file-transfers, content distribution, and so on. These applications are classified, marked, and treated according to industry best-practice recommendations (RFC 4594).

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

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

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

For more information, see Defining Policy Scopes, on page 3.

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

Step 5 (Optional) View the default service provider profiles and, if necessary, create a new service provider profile to fit your needs. For information, see Creating a Customized Service Provider Profile, on page 24.

Step 6 Create the policy on wired devices or wireless segments. For information, see Creating or Editing a Policy, on page 11.
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.
- 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 and Processing Order for Devices with Limited Resources.

Step 7 (Optional) Validate the policy.
You can view the command line interface (CLI) commands that will be applied to a device when the policy is deployed. For more information, see Policy Preview.

Step 8 Apply the policy to the scope of devices.

Step 9 (Optional) Proceed to monitor the application provisioning status and health.
For additional information, see Information about Monitoring EasyQoS.

Step 10 (Optional) Configure Cisco APIC-EM for Apple Fastlane.
For additional information, see About Cisco APIC-EM and Apple Fastlane.

What to Do Next

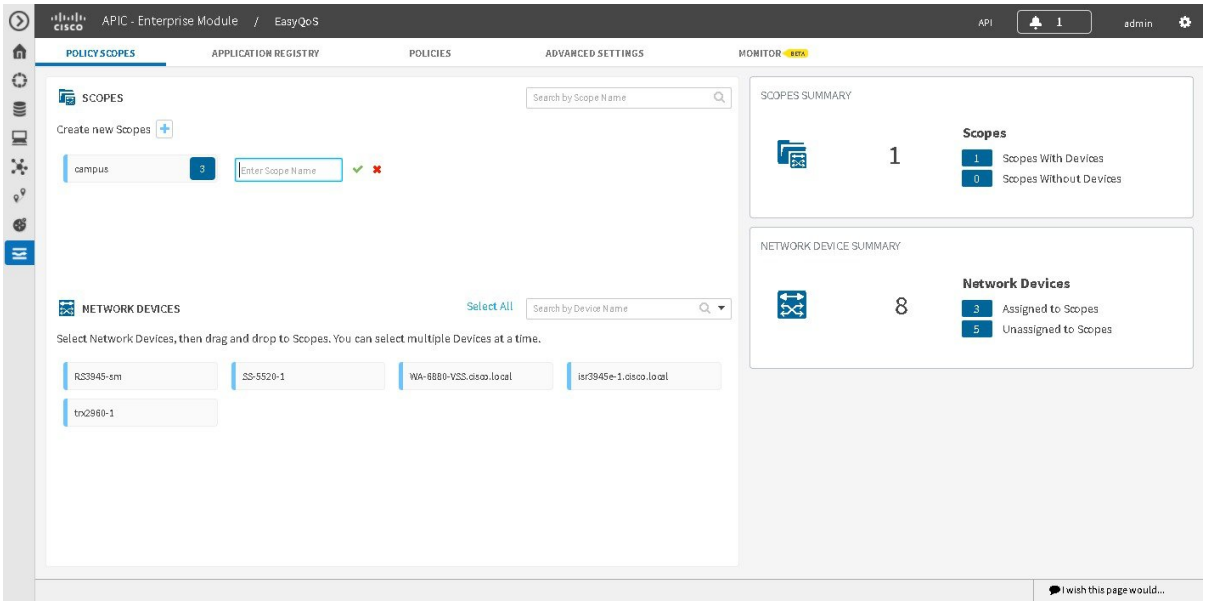
You can see how the deployed policy is working in your network by performing a path trace on two devices and capturing QoS data. For more information, see the *Cisco Path Trace Application for APIC-EM User Guide*.

Defining Policy Scopes

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

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

Figure 1: Policy Scope Window



Before You Begin

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

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

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

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

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

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

EasyQoS adds the device and saves the policy automatically.

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

What to Do Next

You can create policies for wired devices or wireless segments. For information, see Creating or Editing a Policy, on page 11.

Configuring Applications

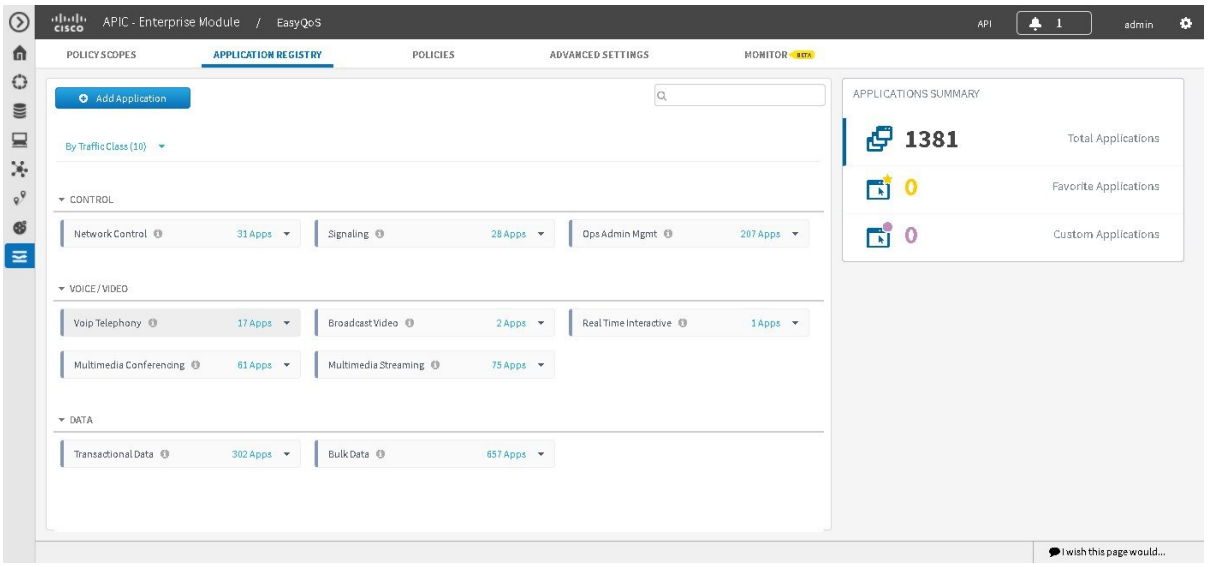
Configuring Favorite Applications

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

You can also configure favorite applications while creating or editing a policy. For more information, see Creating or Editing a Policy, on page 11.

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

Figure 2: Application Registry Window



Before You Begin

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

You must have policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate resource scope to perform this procedure.

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

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

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

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

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

Modifying Traffic Class in an Application

You can modify the traffic class of an NBAR application.

Before You Begin

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

You must have policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate resource scope to perform this procedure.

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

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

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

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

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

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

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

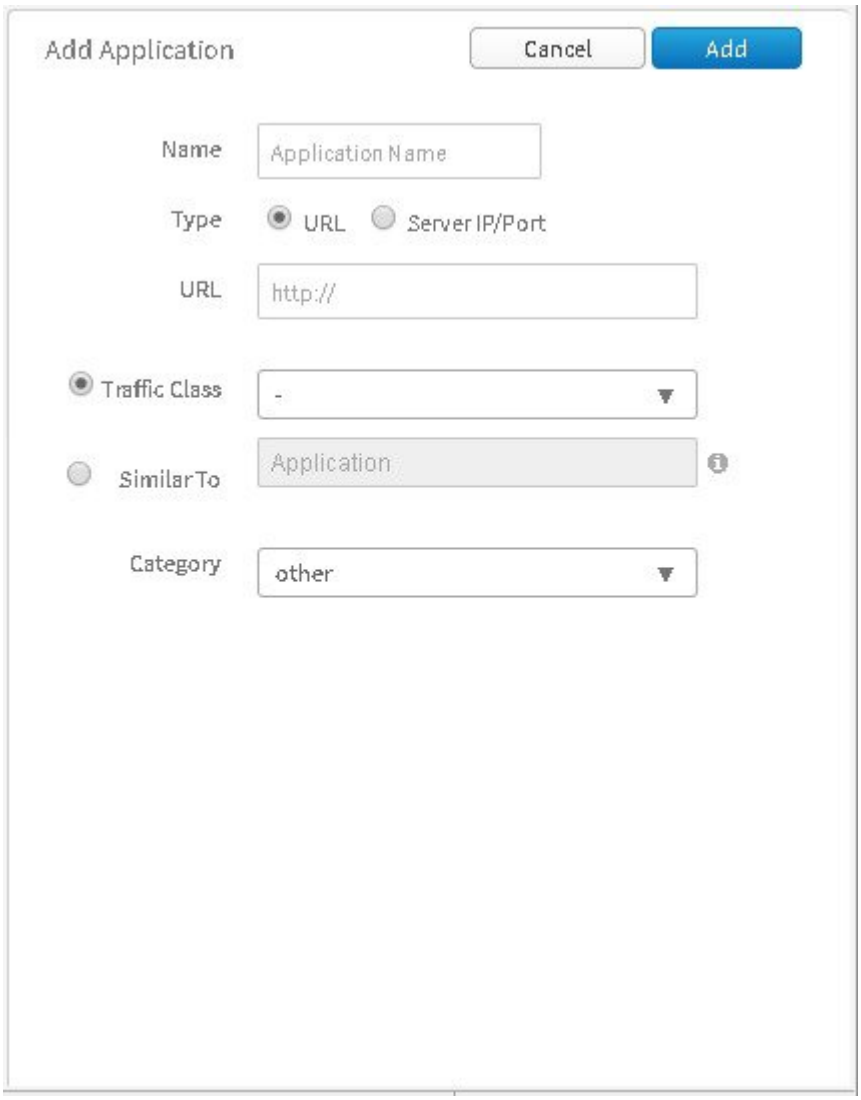
What to Do Next

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

Creating a URL-Based Custom Application

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

Figure 3: Add Application Pane for URL-Based Applications



Before You Begin

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

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

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

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

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

Step 3 Click **Add Application**.

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

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

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

Step 6 When you create a custom applicaiton, it is not assigned to a business-relevancy group. It is placed in a group called Unassigned. To change this setting, see Creating or Editing a Policy, on page 11.

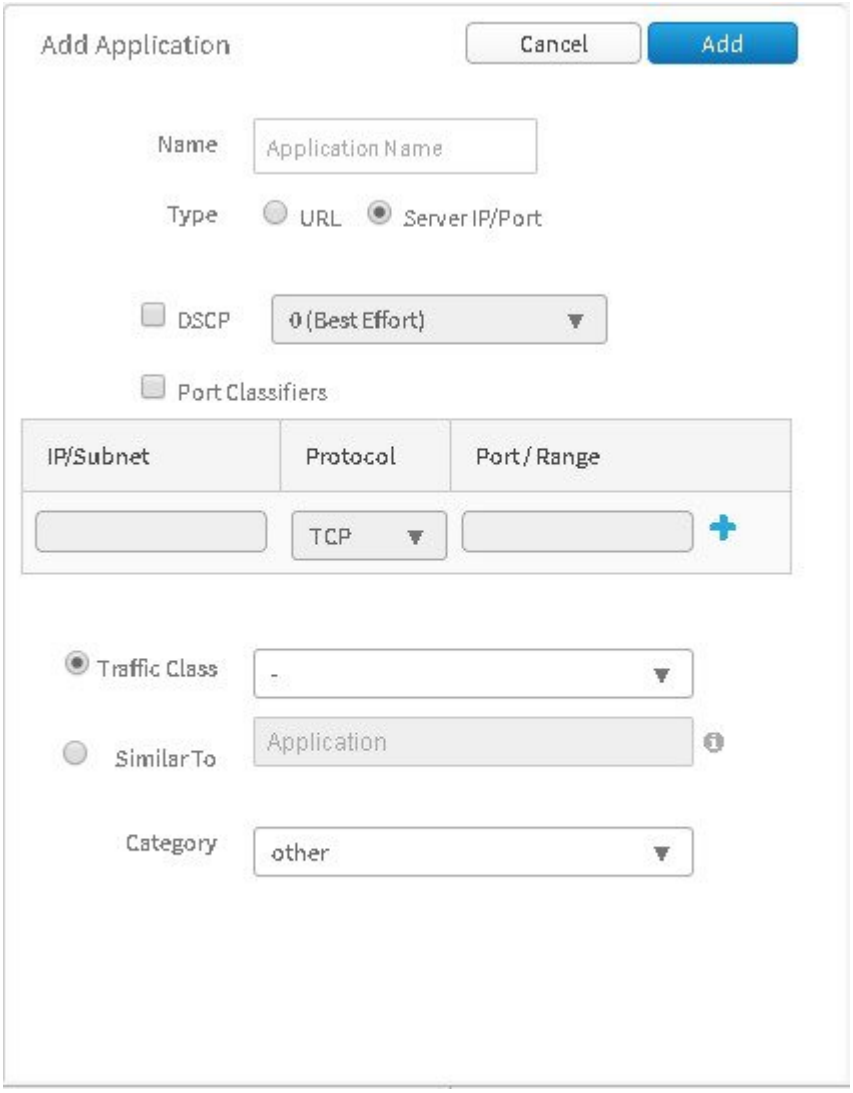
What to Do Next

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

Creating a Server-Based Custom Application

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

Figure 4: Add Application Pane for Server-Based Applications



Before You Begin

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

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

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

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

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

Step 3 Click **Add Application**.

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

- **Name—**Name of the custom application. The name can contain up to 24 alphanumeric characters, including underscores and hyphens. The underscore and hyphen characters are the only special character allowed in the application name.
- **Type—**Method by which users access the application. Choose **Server IP/Port** for applications that are accessible through a server.
- **DSCP—**Differentiated Services Code Point (DSCP) value. Check the **DSCP** check box and define a DSCP value. If you do not define a value, the default value is **Best Effort**. Best-effort service is essentially the default behavior of the network device without any QoS.
- **Port Classifiers—**Classification of traffic based on IP address, protocol, and port number. Check the **Port Classifiers** check box to define the IP address or subnet, protocol, and port or port range for an application. Valid protocols are **IP**, **TCP**, **UDP**, and **TCP/UDP**. If you select the **IP** protocol, you do not define a port number or range.
- **Traffic Class—**Traffic class to which the application belongs. Valid values are BULK_DATA, TRANSACTIONAL_DATA, OPS_ADMIN_MGMT, NETWORK_CONTROL, VOIP_TELEPHONY, MULTIMEDIA_CONFERENCING, MULTIMEDIA_STREAMING, BROADCAST_VIDEO, REAL_TIME_INTERACTIVE, and SIGNALING.
- **Similar To—**Application with the similar traffic-handling requirements. Click the radio-button to select this option, then select an application from the drop-down field. EasyQoS copies the other application's traffic class, category, and subcategory settings to the application that you are defining.

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

Step 6 When you create a custom applicaiton, it is not assigned to a business-relevancy group. It is placed in a group called Unassigned. To change this setting, see Creating or Editing a Policy, on page 11.

What to Do Next

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

Editing a Custom Application

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

Before You Begin

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

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

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

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

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

Information about the application displays in the right hand pane.

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

Step 4 Click **Edit**.

Step 5 Change the desired settings for the custom application:

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

Step 6 Click **Save Application**.

What to Do Next

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

Deleting a Custom Application

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

Before You Begin

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

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

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

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

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

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

Information about the application displays in the right hand pane.

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

Step 4 Click **Delete**.

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

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

What to Do Next

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

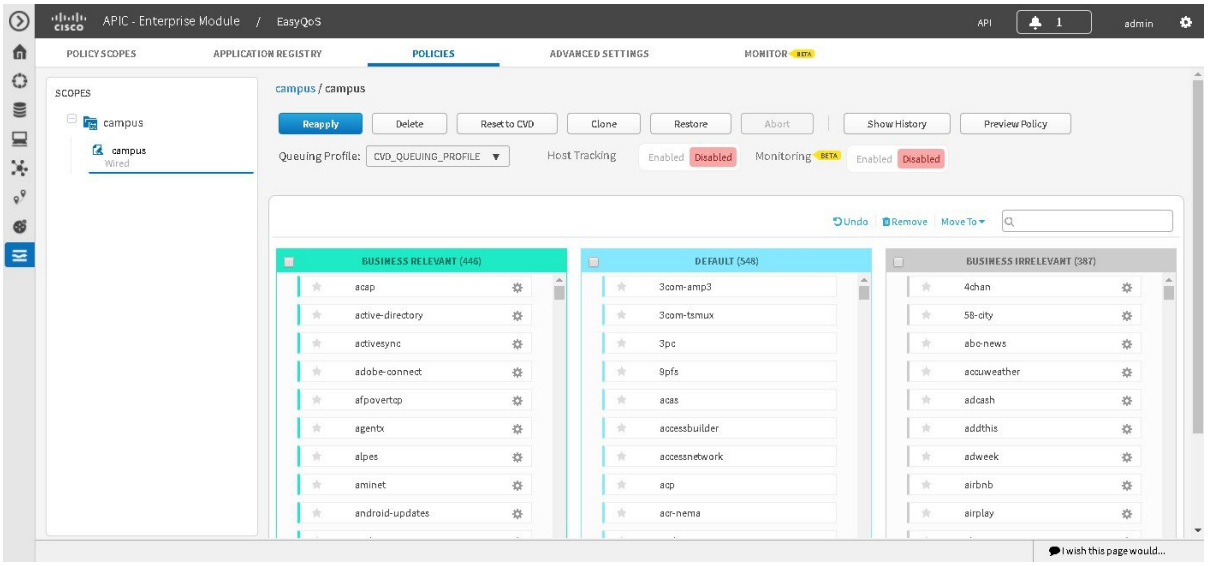
Configuring QoS Policies

Creating or Editing a Policy

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

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

Figure 5: Policies Tab



Before You Begin

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

Make sure that you have discovered your complete network topology.

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

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

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

Step 2 Click the **Policies** tab.

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

Step 4 Do one of the following:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Step 12 Do one of the following actions:

- To save and apply a new policy, click **Apply Policy**.

- To save your changes and reapply the policy, click **Reapply Policy**.

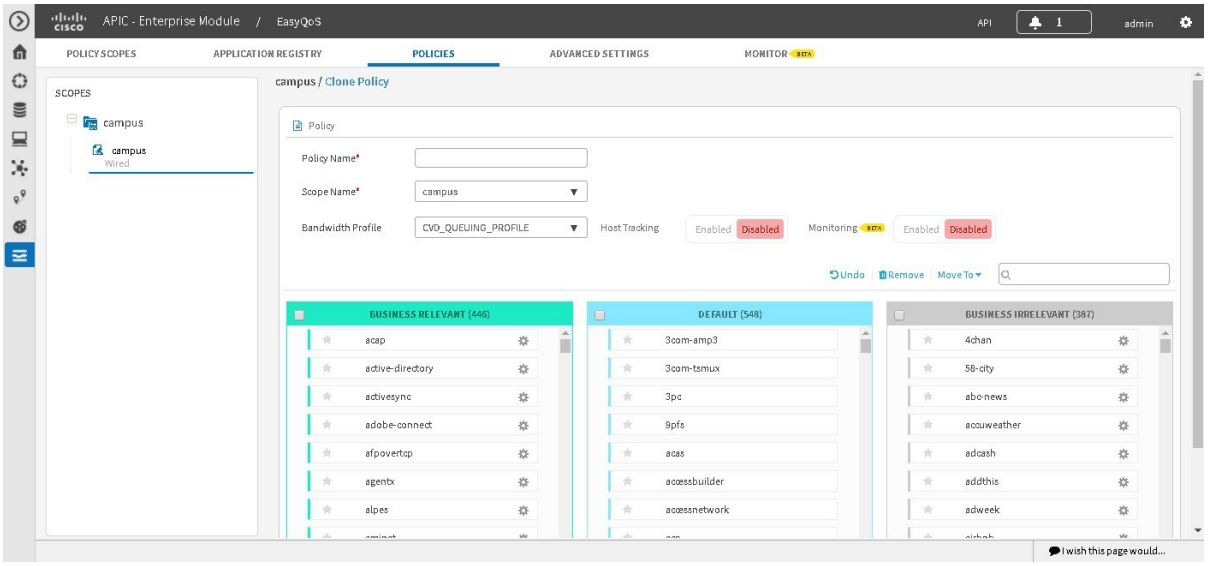
Step 13 In the **Apply Policy** dialog box, do one of the following actions:

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

Cloning a Policy

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

Figure 6: Policies Tab



Before You Begin

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

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

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

You must have created at least one policy.

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

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

Step 2 Click the **Policies** tab.

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

Step 4 Click **Clone**.

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

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

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

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

Step 9 Click **Create Policy**.

Step 10 Click **Reapply Policy**.

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

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

Deleting a Policy

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

Before You Begin

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

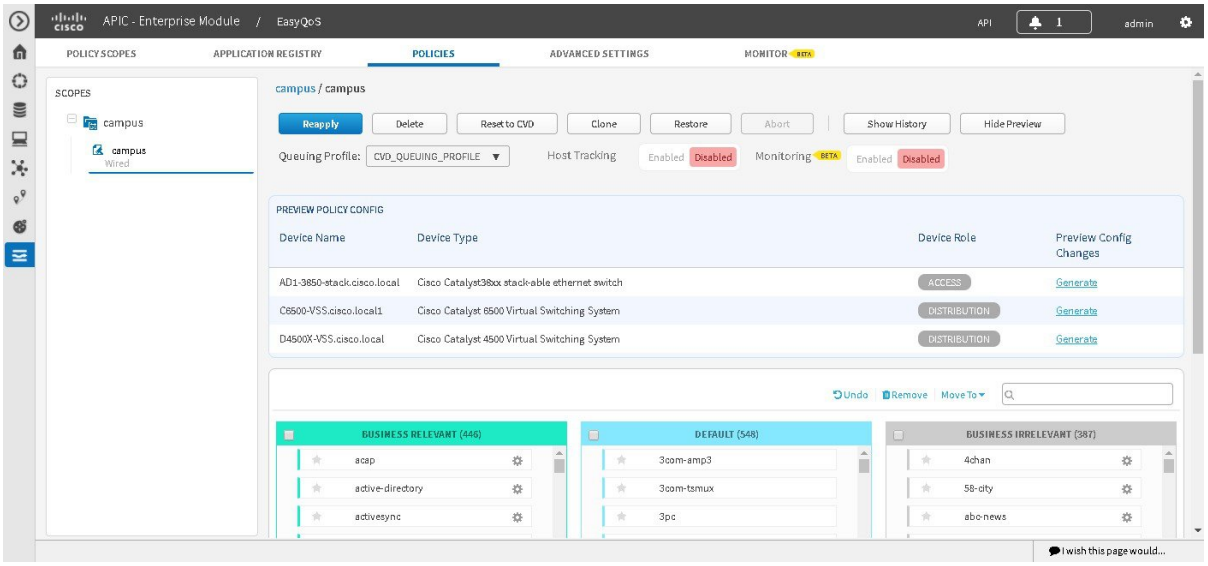
Step 1 From the **Navigation** pane, click **EasyQoS**.
Step 2 Click the **Policies** tab.
Step 3 From the **Scopes** pane, select a policy scope.
Step 4 Under the policy scope name, select a policy.
Step 5 Click **Delete**.
Step 6 To confirm the deletion, click **Ok**. Otherwise, click **Cancel**.
Step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

Managing QoS Policies

Previewing a Device's Policy Configuration

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

Figure 7: Policies Tab Showing Policy Preview Configuration



Before You Begin

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

You must have created an EasyQoS policy.

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

Step 2 Click the **Policies** tab.

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

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

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

Step 6 Click **Ok**.

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

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

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

Cancelling a Policy Configuration Process

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

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

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

Before You Begin

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

Procedure

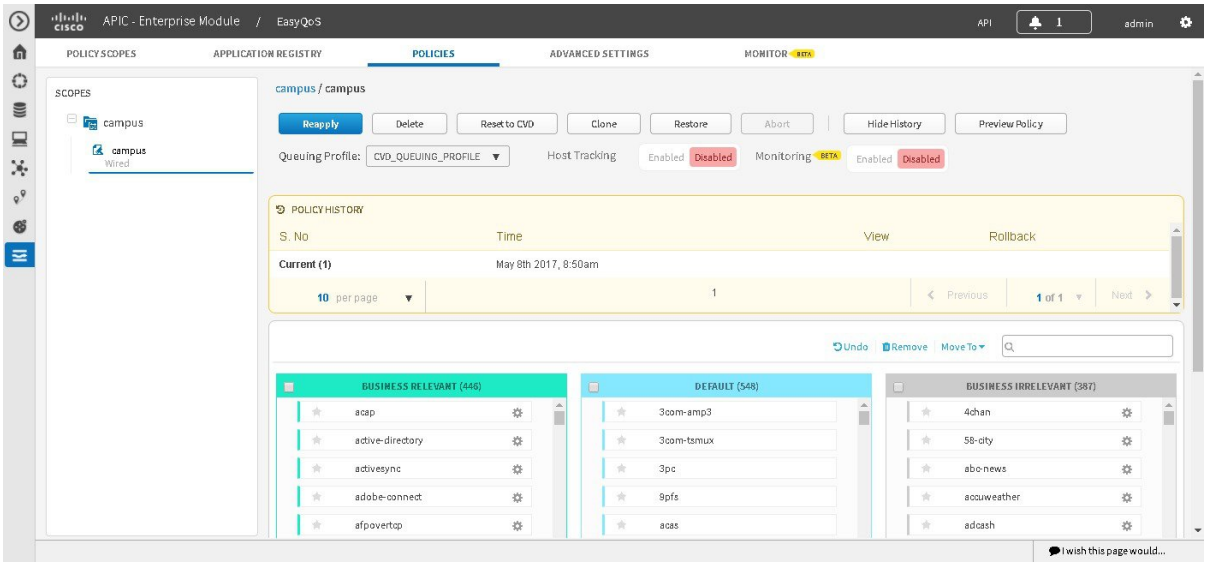
Click **Abort** to cancel the policy configuration process.

Displaying the Version History of Policies

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

- Display the differences between a selected policy and the current one. For information, see Comparing Policy Versions, on page 19.
- Roll back to a previous version of a policy. For information, see Rolling Back to a Previous Policy Version, on page 20.

Figure 8: Policies Tab Showing Version History of Policies



Before You Begin

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

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

Step 2 Click the **Policies** tab.

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

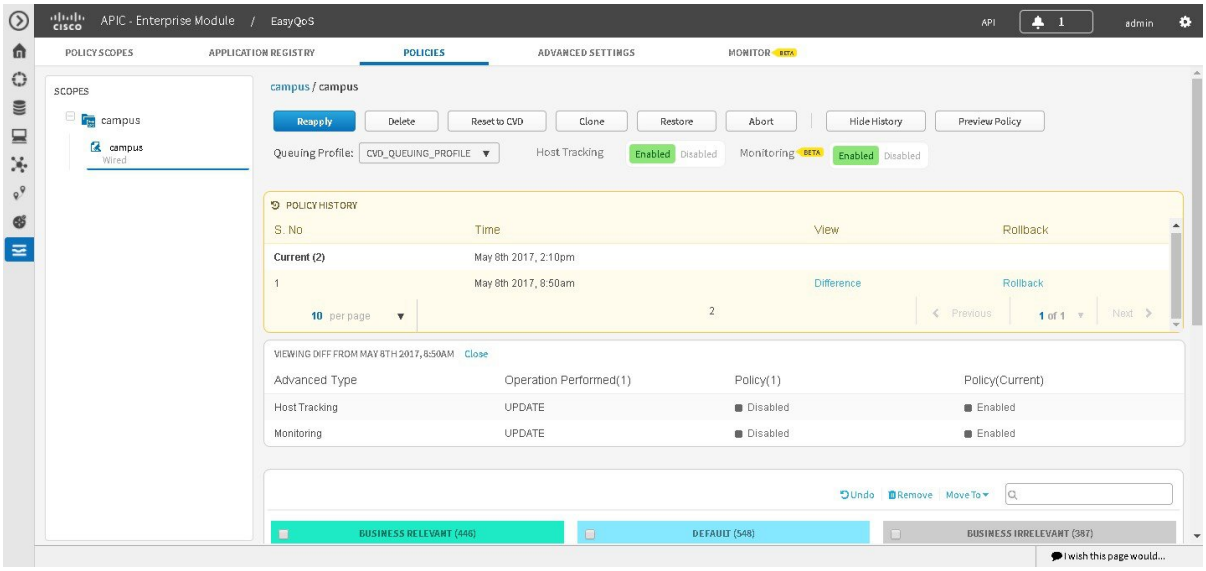
Step 4 Click **Show History**.

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

Comparing Policy Versions

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

Figure 9: Policies Tab Showing Policy Versions



Before You Begin

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

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

Step 2 Click the **Policies** tab.

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

Step 4 Click **Show History**.

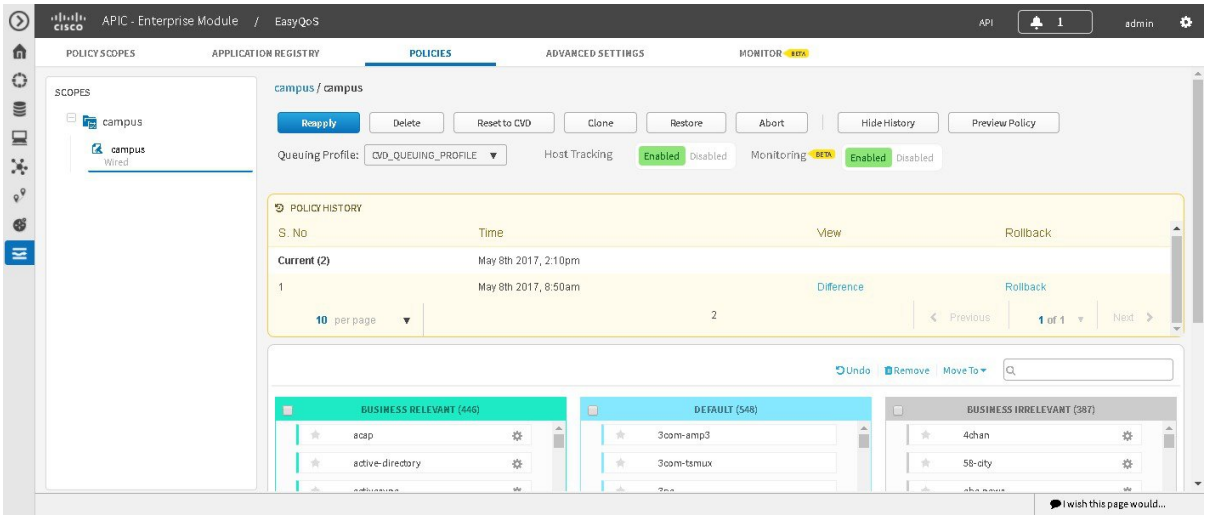
Step 5 Click **Difference** corresponding to the version that you want to compare with the current version.

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

Rolling Back to a Previous Policy Version

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

Figure 10: Policies Tab Showing Rollback Option



Before You Begin

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

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

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

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

Step 2 Click the **Policies** tab.

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

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

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

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

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

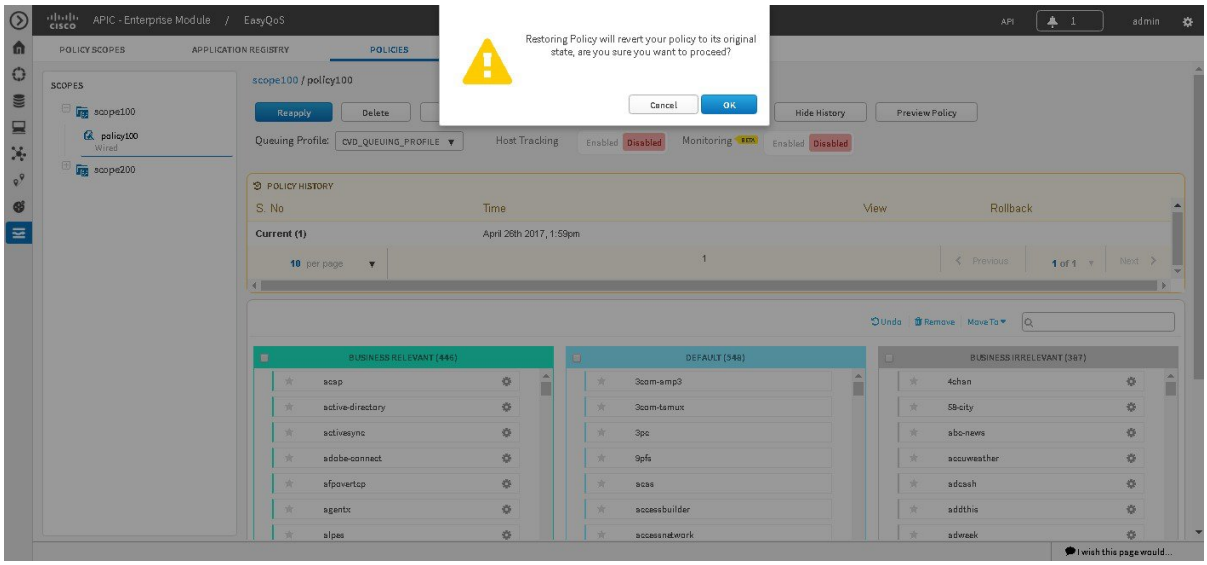
Step 8 Click **Reapply**.

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

Resetting Applications to the Cisco Validated Design Configuration

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

Figure 11: Policy Tab Showing Reset to CVD Confirmation Dialog Box



Before You Begin

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

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

Step 2 Click the **Policies** tab.

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

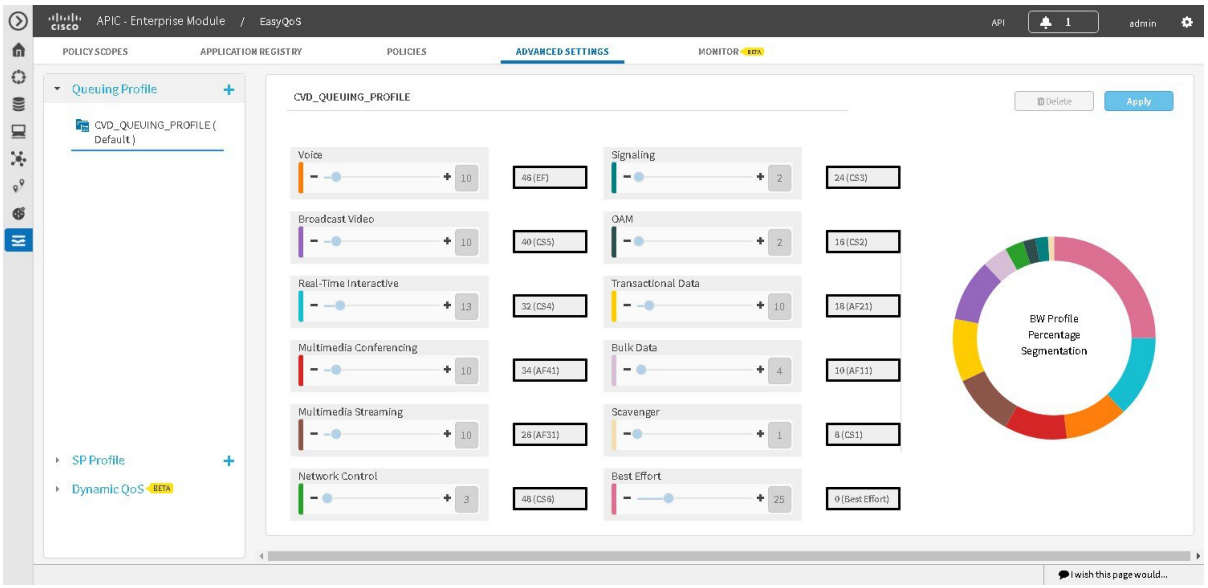
Step 4 Click **Reset to CVD**.

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

Configuring Queuing Profiles

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

Figure 12: Queuing Profile Pane



Before You Begin

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

You must have created a QoS policy with the appropriate configuration. For information, see Creating or Editing a Policy, on page 11.

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

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

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

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

Step 5 Do one of the following:

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

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

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

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

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

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

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

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

Step 8 When you are satisfied with the bandwidth allocation and the queuing profile, click **Create**.

Note You can edit queuing profiles after creating them. If you edit the profile, then you will also need to reapply the policies that are using for this queuing profile.

Configuring Service Provider Profiles on WAN Interfaces

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

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

Before You Begin

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

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

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

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

Step 2 If you are using one of the preconfigured SP profiles, proceed to Step 3. Otherwise, you can create a custom SP profile.
To create a custom SP profile, see Creating a Customized Service Provider Profile, on page 24.

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

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

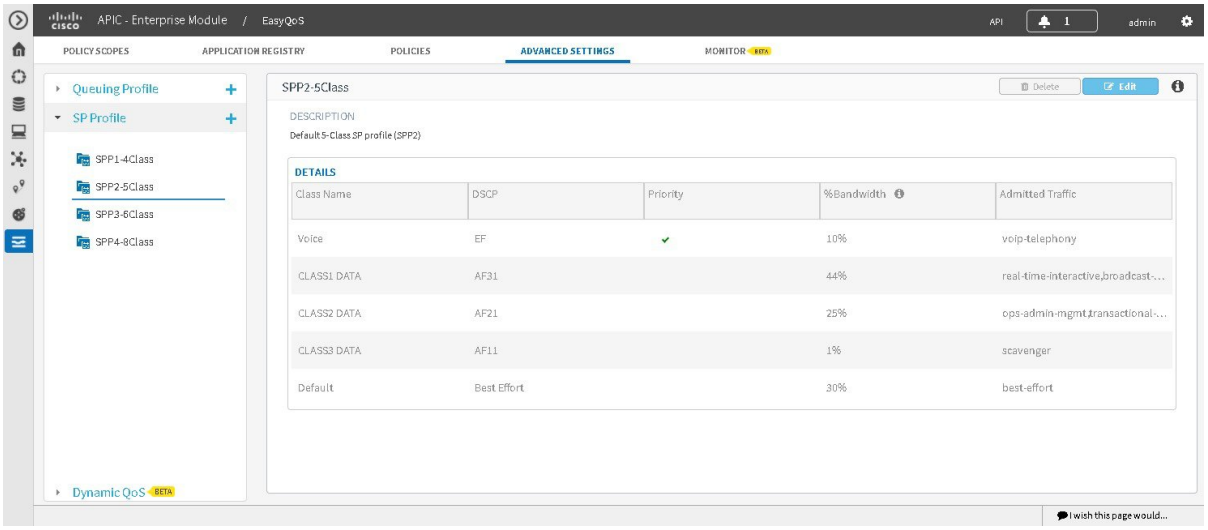
Note You need to wait for Cisco APIC-EM's next discovery polling cycle to complete (configurable to be from every 25 minutes to once per day) or manually resynchronize the device before applying the policy configuration. For information, see Verifying the WAN Interface Synchronization Status, on page 27.

Creating a Customized Service Provider Profile

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

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

Figure 13: Service Provider Profile Window Showing Add SP Profile Pane



Before You Begin

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

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

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

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

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

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

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

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

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

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

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

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

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

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

What to Do Next

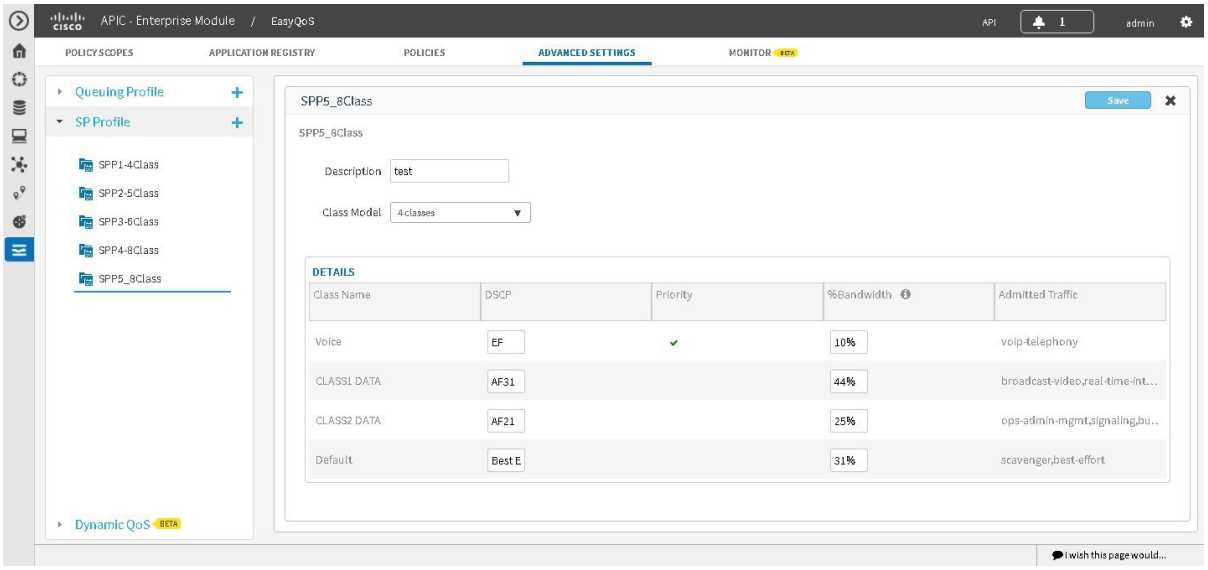
After creating your customized SP profile, you need to configure the WAN interfaces with the SP profile. For information, see WAN Interface Configuration for EasyQoS.

Editing a Customized Service Provider Profile

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

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

Figure 14: Service Provider Profile Window Showing Edit SP Profile Pane



Before You Begin

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

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

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

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

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

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

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

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

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

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

- **Description—**Word or phrase that identifies the SP profile.
- **Class Model—**Choose one of the class models from the drop down list. Valid class models are **4 classes**, **5 classes**, **6 classes**, and **8 classes**.
- **Class Name—**Name of the QoS class. The name can contain up to 24 alphanumeric characters, including underscores and hyphens. The underscore and hyphen characters are the only special character allowed in the name.
- **DSCP—**Dynamic Host Configuration Protocol (DHCP) value. Valid values are as follows:
  - Expedited Forwarding (EF)
  - Class Selector (CS)—CS1, CS2, CS3, CS4, CS5, CS6
  - Assured Forwarding—AF11, AF21, AF41
  - Default Forwarding (DF)

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

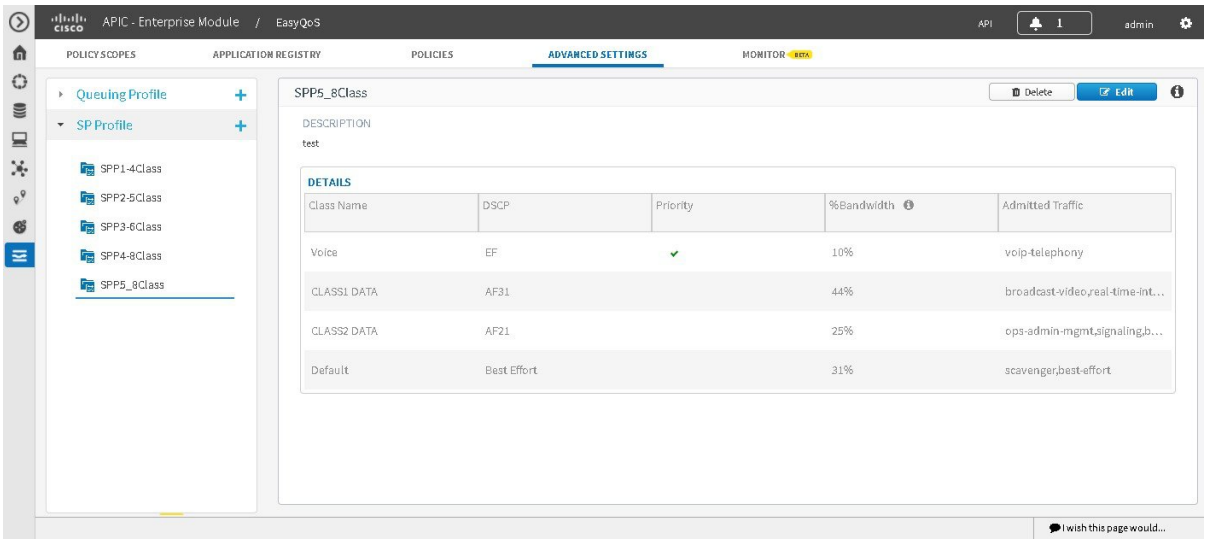
Step 7 Click **Save** to save your changes.

Verifying the WAN Interface Synchronization Status

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

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

Figure 15: SP Profile Tab Showing Associated Interfaces Status



Before You Begin

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

You must have completed all the steps in Configuring Service Provider Profiles on WAN Interfaces, on page 23.

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

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

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

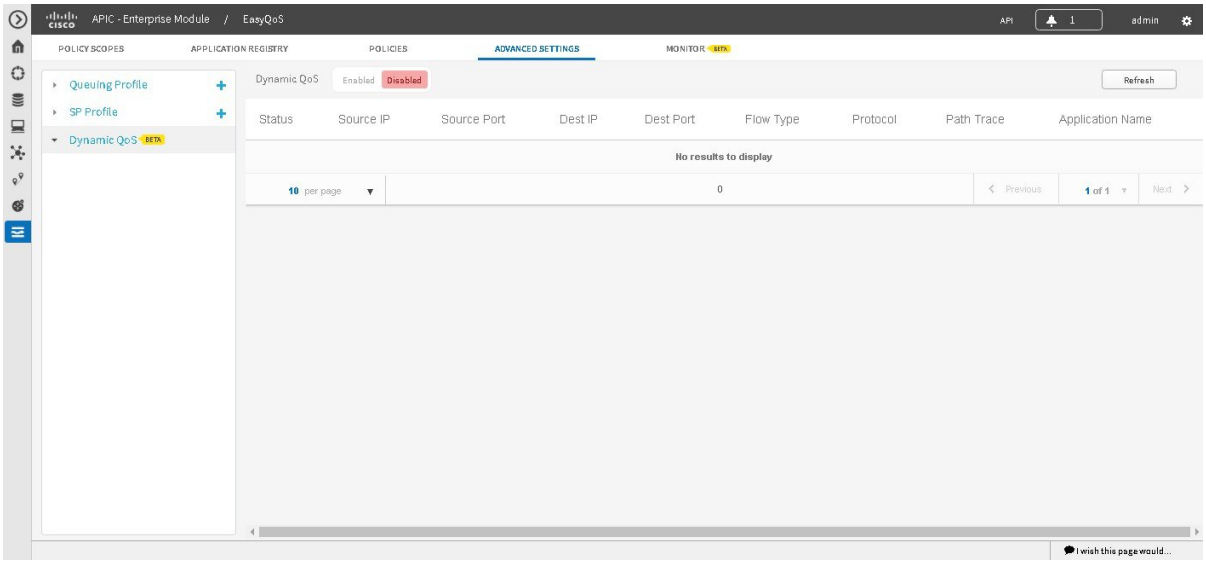
If the Cisco APIC-EM recognizes the SP profile on the WAN interface, the synchronization status shows a check mark icon ( ). If not, the synchronization status shows a red X icon ( ). You need to troubleshoot the issue. Check that the name that you entered as the description of the interface is exactly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

Configuring Dynamic QoS

Enabling and Disabling Dynamic QoS

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

Figure 16: Dynamic QoS Tab



Before You Begin

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

You must have created a QoS policy with the appropriate configuration. For information, see Creating or Editing a Policy, on page 11.

SUMMARY STEPS

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

DETAILED STEPS

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

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

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

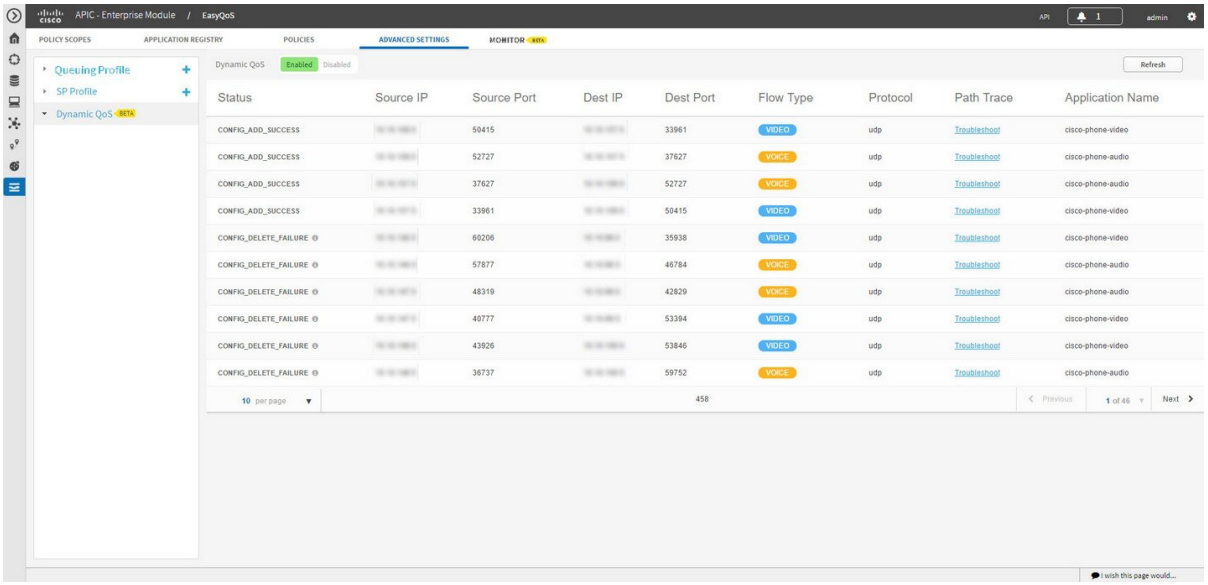
Step 4 In the **Dynamic QoS** field, click **Enabled** to turn on dynamic policy creation or **Disabled** to turn off dynamic policy creation.

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

Troubleshooting Dynamic QoS

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

Figure 17: Dynamic QoS Tab Showing Troubleshooting Link in Path Trace Column



Before You Begin

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

You must have enabled Dynamic QoS and applied or reapplied policies for Dynamic QoS to be in effect. For information, see Enabling and Disabling Dynamic QoS, on page 29.

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

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

Step 3 Locate the flow that you want to troubleshoot.

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