Monitoring EasyQoS

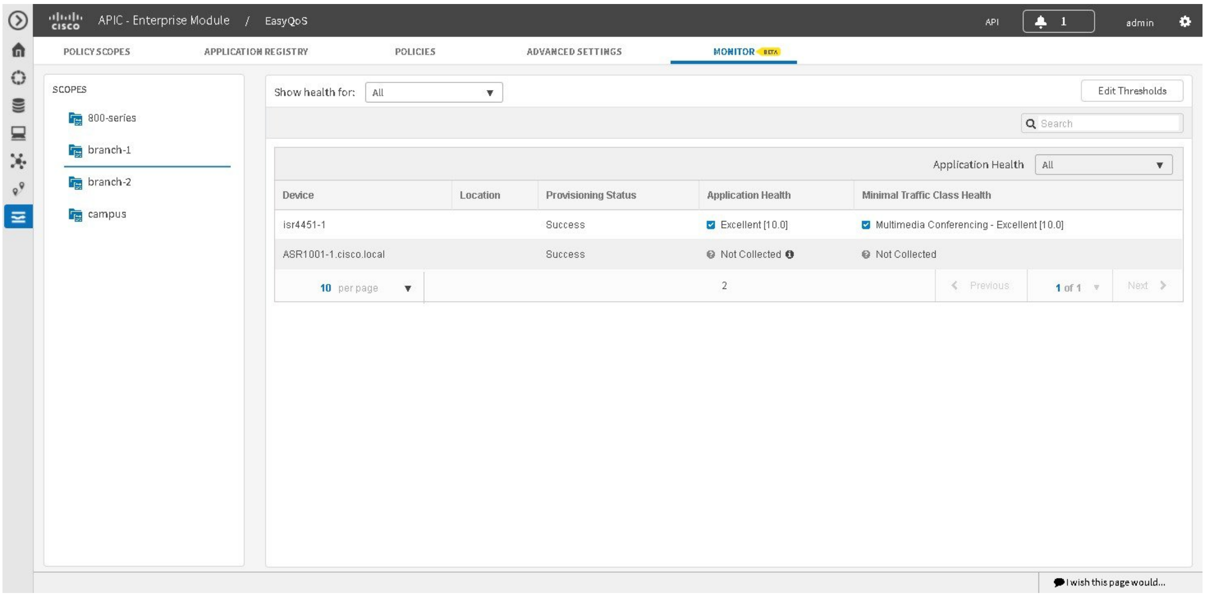
Information about Monitoring EasyQoS

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

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

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

Figure 1: Monitoring Window



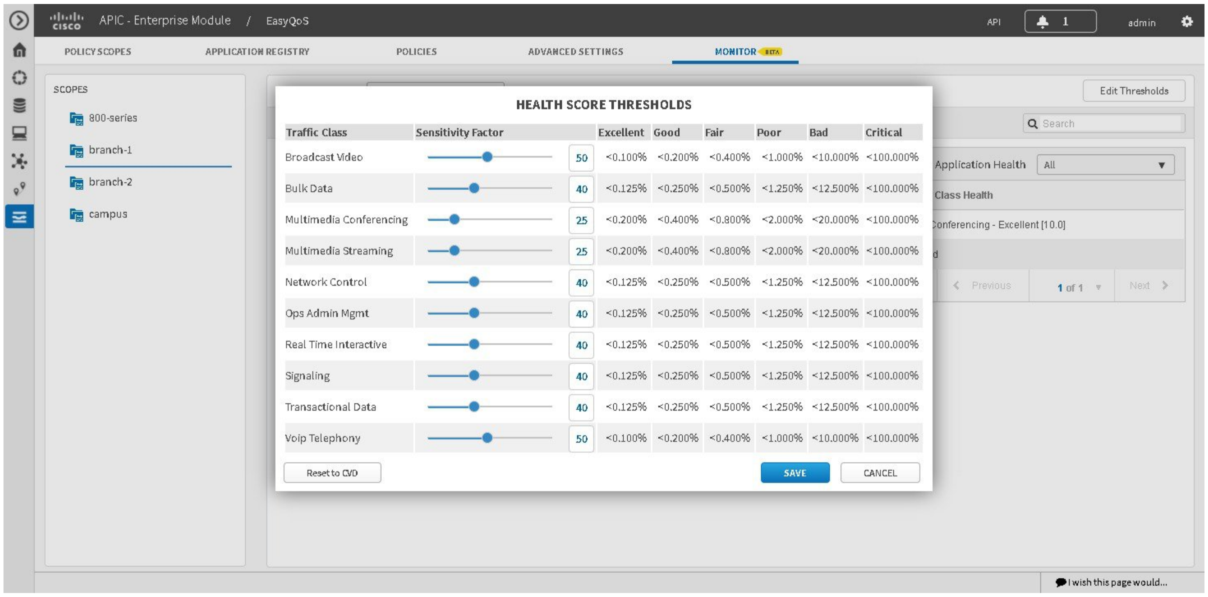
The health of each application is measured as a sensitivity to packet loss on the device's WAN interface. This sensitivity is given a numerical value. The higher the sensitivity factor the more sensitive for packet loss (e.g. factor =5 => Excellent < 1%, factor = 100 => Excellent < 0.05%). The lower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

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

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

You are able to reconfigure the sensitivity factor for each traffic class and therefore, each application. For information, see Changing Sensitivity Factor for the Traffic Class, on page 10.

Figure 2: Health Score Thresholds

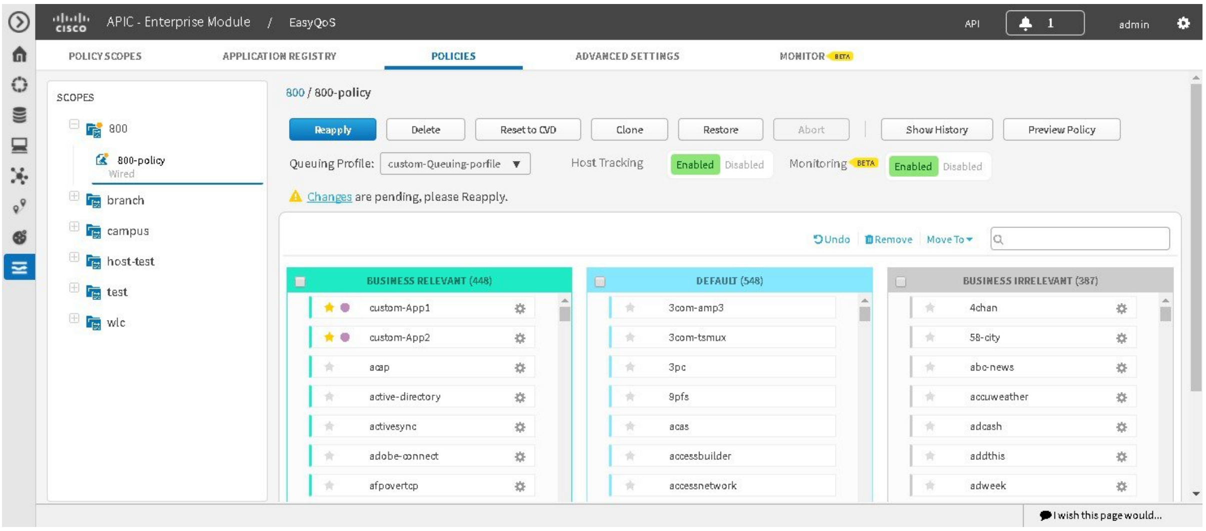


Enabling Monitoring for EasyQoS

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

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

Figure 3: Enabling Monitoring for EasyQoS



Before You Begin

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

Make sure that you have discovered your complete network topology.

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

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

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

Step 2 Click the **Policies** tab.

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

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

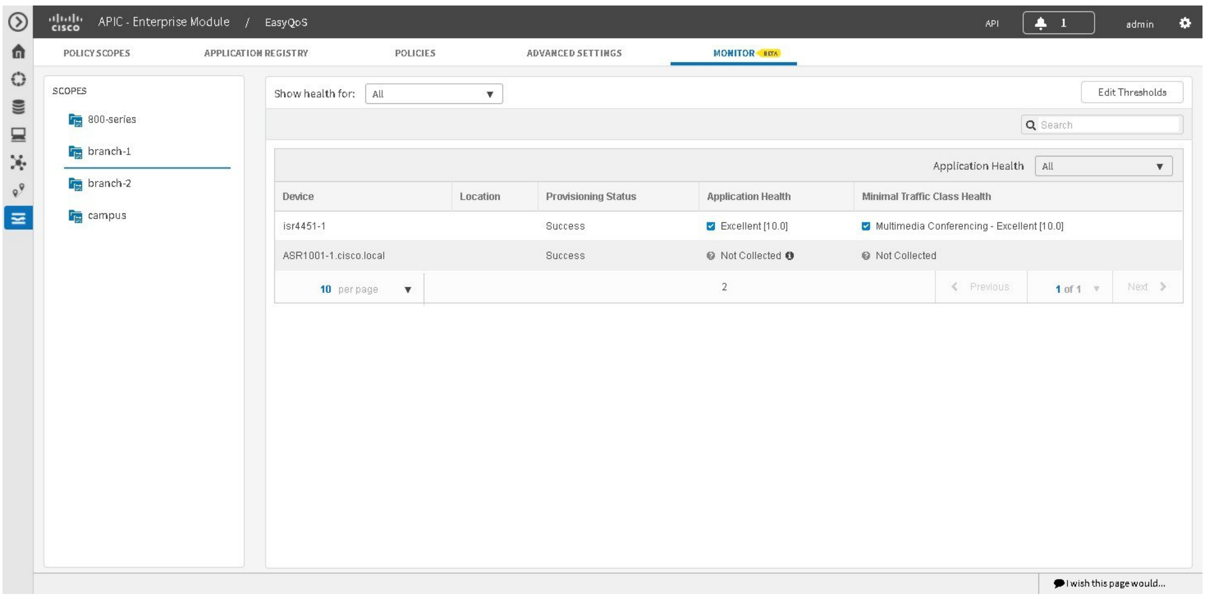
What to Do Next

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

Filtering for the Device and its Application Health

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

Figure 4: Monitoring Window



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

- The device is a router. Only Cisco router data appears in the **Monitoring** window.
- The device has an active NBAR license.
- The device's interface is a WAN interface.
- Monitoring has been enabled for the scope. For information about this procedure, see Enabling Monitoring for EasyQoS, on page 3.

Before You Begin

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

Make sure that you have discovered your complete network topology.

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

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

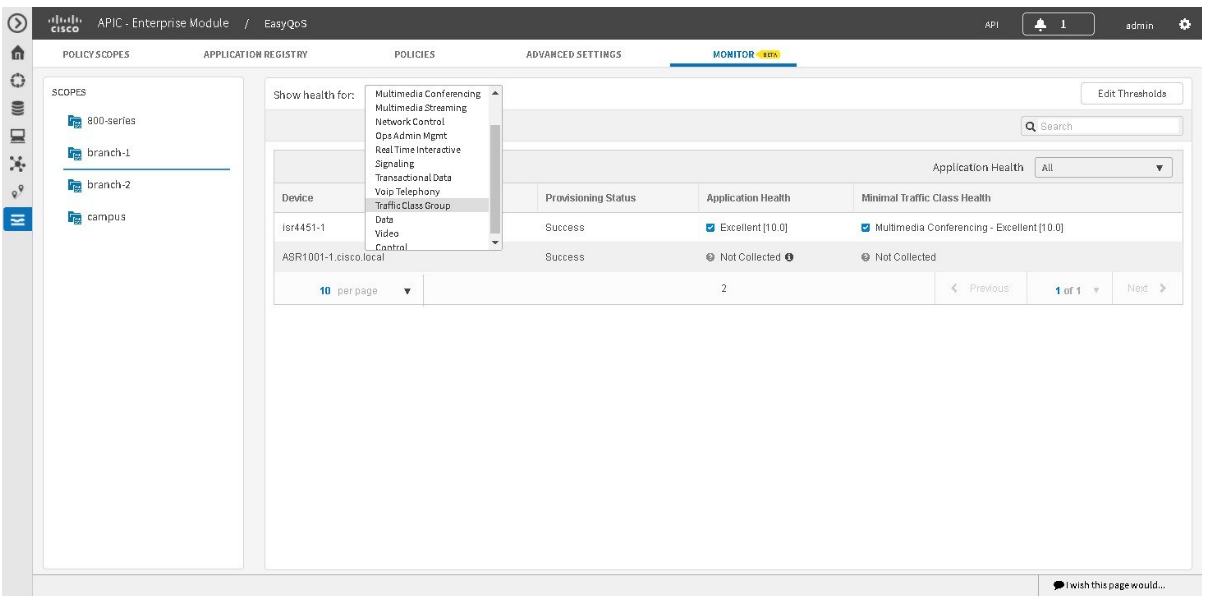
Step 1 From the **Navigation** pane, click **EasyQoS**.

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

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

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

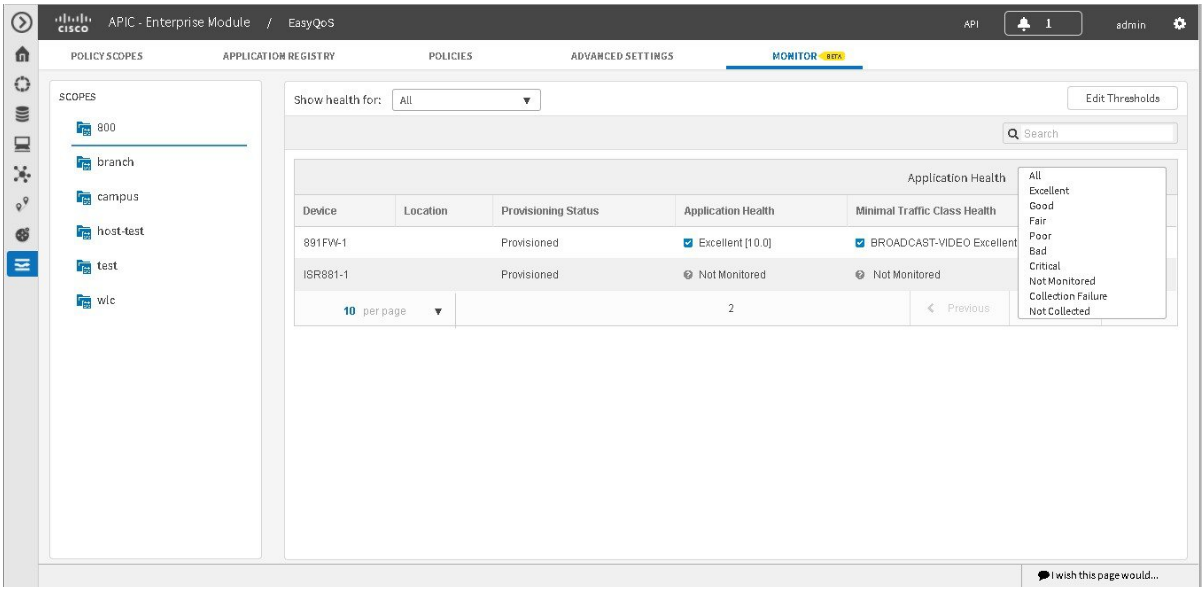
Figure 5: Option for Traffic Class Selection



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

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

Figure 6: Option for Application Health Selection



The following application health filters are available:

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

The application health filters (and values) are determined by pre-configured thresholds for packet sensitivity. You can reconfigure these pre-configured thresholds. For information about this procedure, see Changing Sensitivity Factor for the Traffic Class, on page 10.

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

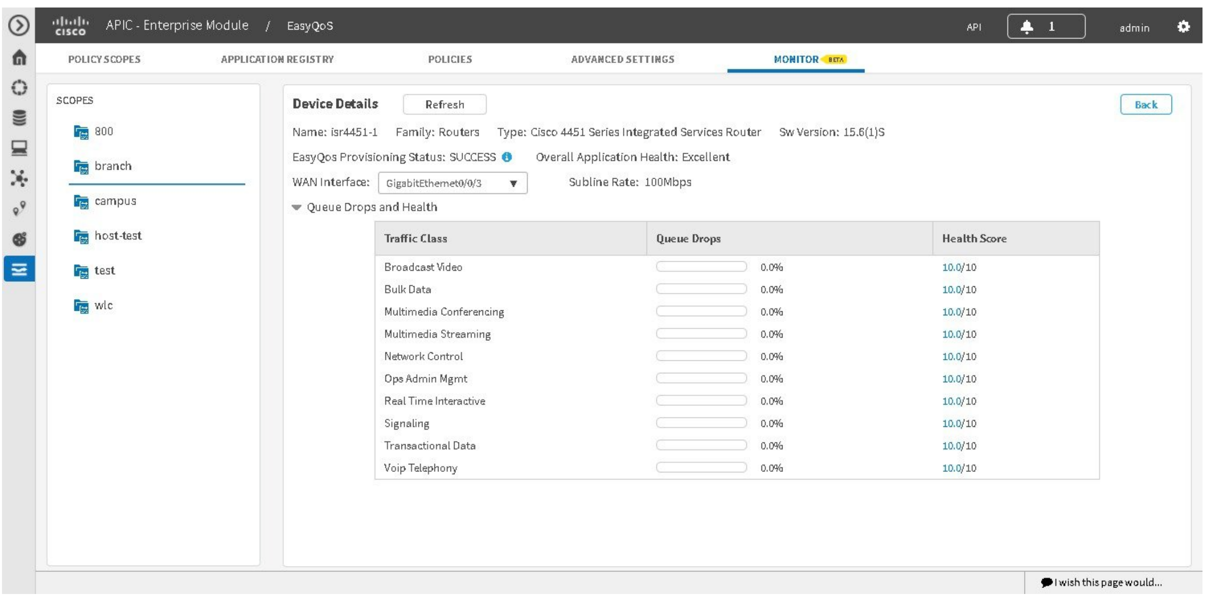
- **Device**
- **Location**
- **Provisioning Status**

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

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

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

Figure 7: Device Details



The following device data appears:

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

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

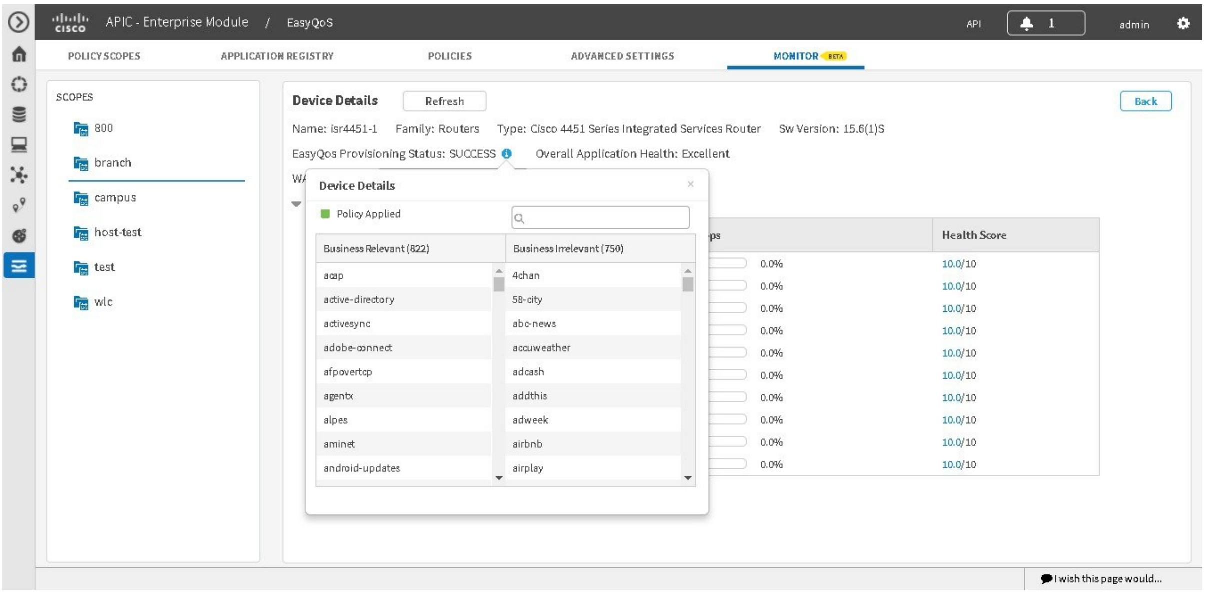
  Based on the health score values, the progress bar displays the appropriate color.

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

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

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

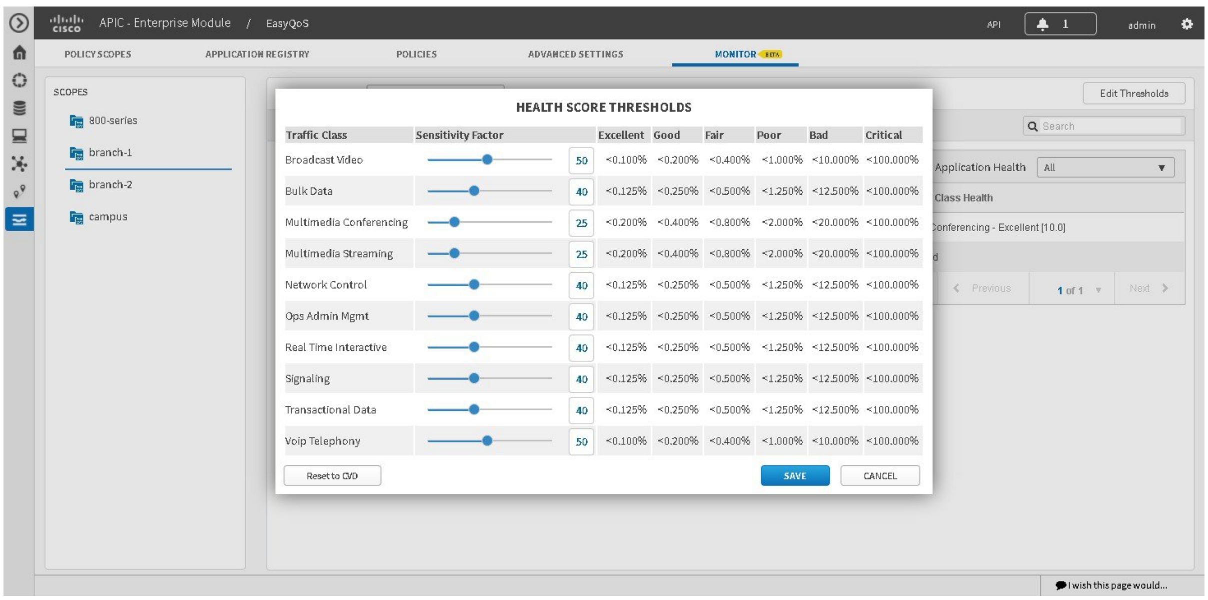
Figure 8: Device Details - Policy Applied



Changing Sensitivity Factor for the Traffic Class

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

Figure 9: Health Score Thresholds



Before You Begin

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

Make sure that you have discovered your complete network topology.

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

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

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

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

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

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

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

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

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

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