
Configure CoS for SD-LAN



For supported software information, click [here](#).

When a network experiences congestion and delay, you can use class of service (CoS), also known as quality of service (QoS), to prioritize traffic so that more important traffic is handled with a higher priority. CoS examines and classifies all incoming (ingress) traffic on a Versa Operating System™ (VOS™) device, and it then schedules the outgoing (egress) traffic so that it is transmitted out the VOS device's interfaces. CoS classifies all ingress traffic packets based on their importance and places related packets into their own forwarding class. For ingress traffic, you define policies that accept or deny Layer 2 and application-specific traffic. For both ingress and egress traffic, you can rewrite the Differentiated Service Code Points (DSCP) and IEEE 802.1p bits in the packet headers.

This article describes how to configure CoS for SD-LAN networks.

Configure Classifier Profiles

CoS classification is the process of analyzing ingress traffic packets and sorting them into categories called forwarding classes. Each forwarding class represents a level of importance that determines how the traffic should be prioritized. You create classifier rules to assign incoming packets to a forwarding class based on information in the packet header fields.

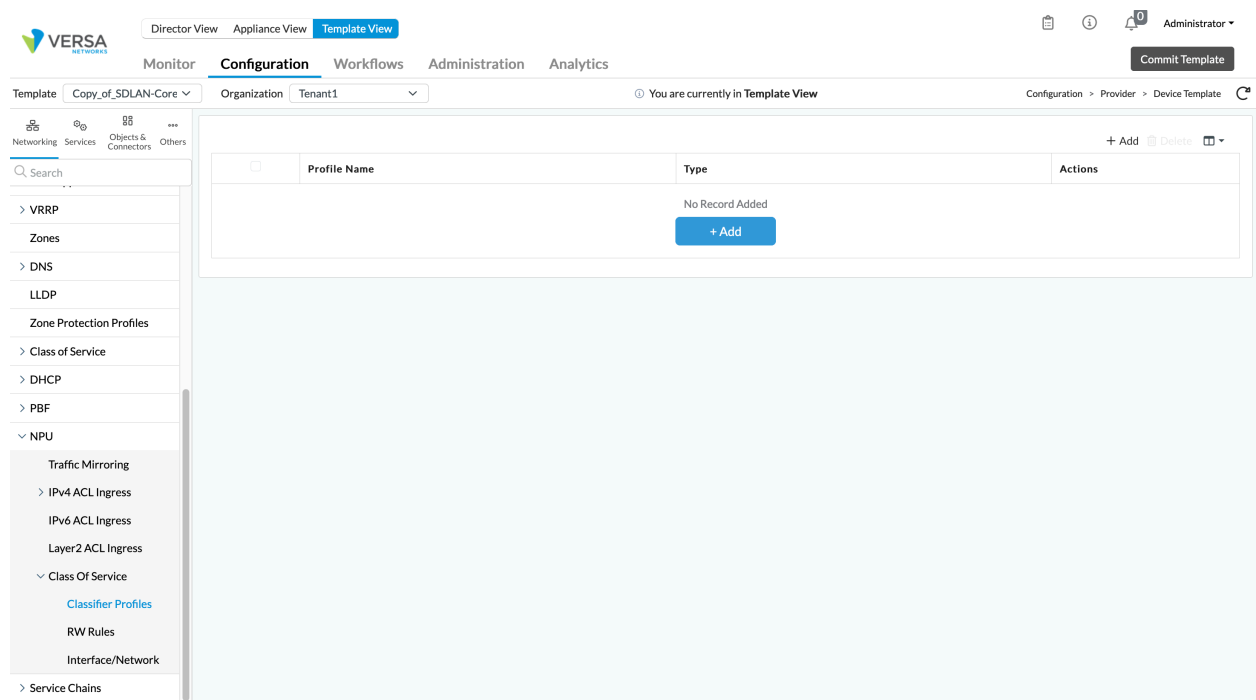
You can use default classifier rules for DSCP and 802.1p. For more information about the default classifier rules, see [Associate QoS Rules with Interfaces or Networks](#), below.

You can also configure a classifier profile. To do this, in the classifier profile, you create classifier rules with match conditions for either DSCP or 802.1p field values. You can also configure the loss priority for each classification. After traffic is classified, the classifier profile sets the values of fields in the Ethernet or IP header to indicate the required level of QoS service for that traffic.

To configure a classifier profile:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices from the horizontal menu bar.
 - c. Select an organization in the left menu bar.
 - d. Select a branch, hub, or Controller from the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.

3. Select Networking > NPU > Class of Service > Classifier Profiles in the left menu bar.



4. Click the + Add icon. In the Add Classifier Profile popup window, enter information for the following fields.

Add Classifier Profile

Profile Name *

Type *

DSCP

Rules

+ Add

	Rule Name	Actions
No Record Added		

OK

Cancel

Field	Description
Profile Name	Enter a name for the rewrite table to contain the assigned forwarding class, loss priority, and DSCP or IEEE 802.1p value.
Type	Select the type of header values to use for classification: <ul style="list-style-type: none"> ◦ DSCP—Use the DSCP value in the IP header. ◦ IEEE 802.1p—Use the 802.1p value in the Ethernet header.

- To add a rule to the profile, click + Add. The Add Rule popup window displays.

Add Rule



Rule Name *

Match Set

☒ Code Points

☐ Code Values

Code Point ▾

Please Select---

▼

+


No Records to Display

OK

Cancel

- In the Rule Name field, enter a name for the classifier rule.
- Select the Match tab to specify the match criteria for the classifier rule, and then enter information for the following

fields. You must configure at least one match condition.

Field	Description
Code Points	Select the DSCP or 802.1p code point names to match.
Code Values	If you select the DSCP code point, enter the DSCP code point values to match. <i>Range: 0 through 63</i>
 Add icon	Click the Add icon to add a code point or code value.

8. Select the Set tab to set or modify attributes for matching traffic, and then enter information for the following fields.

Add Rule



Rule Name *

Match Set

Forwarding Class

Loss Priority

DSCP

☒ Code Point

☐ Code Value

Code Point

OK

Cancel

Field	Description
Forwarding Class	<p>Select a forwarding class to which you want to assign the packets:</p> <ul style="list-style-type: none"> Forwarding Class 0 through Forwarding Class 3—Network Control Forwarding Class 4 through Forwarding Class 7—Expedited Forwarding Class 8 through Forwarding Class 11—Assured Forwarding Class 12 through Forwarding Class 15—Best Effort
Loss Priority	<p>Select a loss priority:</p> <ul style="list-style-type: none"> High Low Medium
Code Points	Select the DSCP code point names to set.
Code Values	<p>Enter the DSCP code point values to set.</p> <p><i>Range:</i> 0 through 63</p>

9. Click OK to add the Rule.
10. Click OK to add the Classifier Profile.

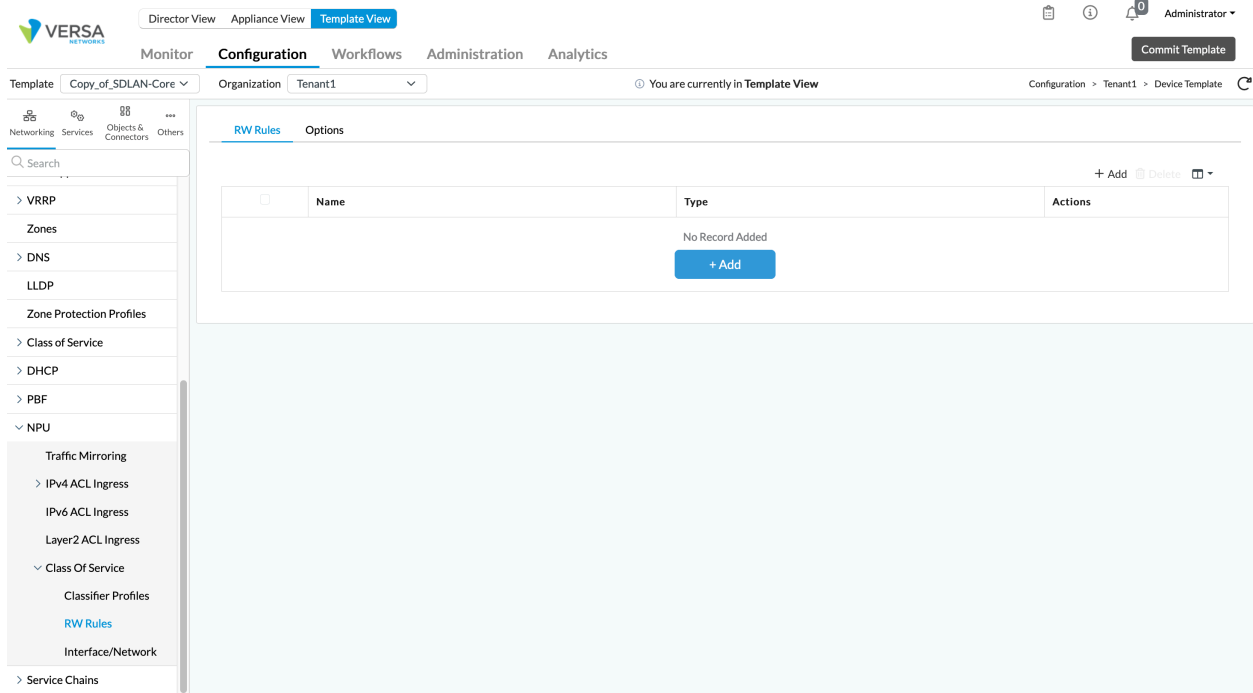
Configure Rewrite Rules

Rewrite rules allow you to remark, or change, the DSCP and 802.1p values in the headers of outbound traffic. This helps other devices in the network apply the correct QoS policies to the traffic. A rewrite rule examines a packet's forwarding class and loss priority and sets the QoS bits to the value defined in the rule. Depending on where you apply the rewrite policy, it modifies the QoS bits of either the inner or outer header.

To configure rewrite rules:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices from the horizontal menu bar.

- c. Select an organization in the left menu bar.
- d. Select a branch, hub, or Controller from the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Class of Service > RW Rules in the left menu bar.



4. Select the RW Rules tab, and then click + Add. In the Add RW Rule popup window, enter information for the following fields.

Add RW Rule



Rewrite Table Name *

Type *

Configuration

+ Add

<input type="checkbox"/>	Forwarding Class	Actions
No Record Added		

OK

Cancel

Field	Description
Rewrite Table Name	Enter a name for the rewrite table to contain the assigned forwarding class, loss priority, and DSCP or IEEE 802.1p value.
Type	Select the rewrite table type: <ul style="list-style-type: none"> ◦ DSCP ◦ IEEE 802.1p

5. To add the forwarding class, click the + Add icon. In the Add Configuration popup window, enter information for the following fields.

Add Configuration




Forwarding Class *

---Please Select---

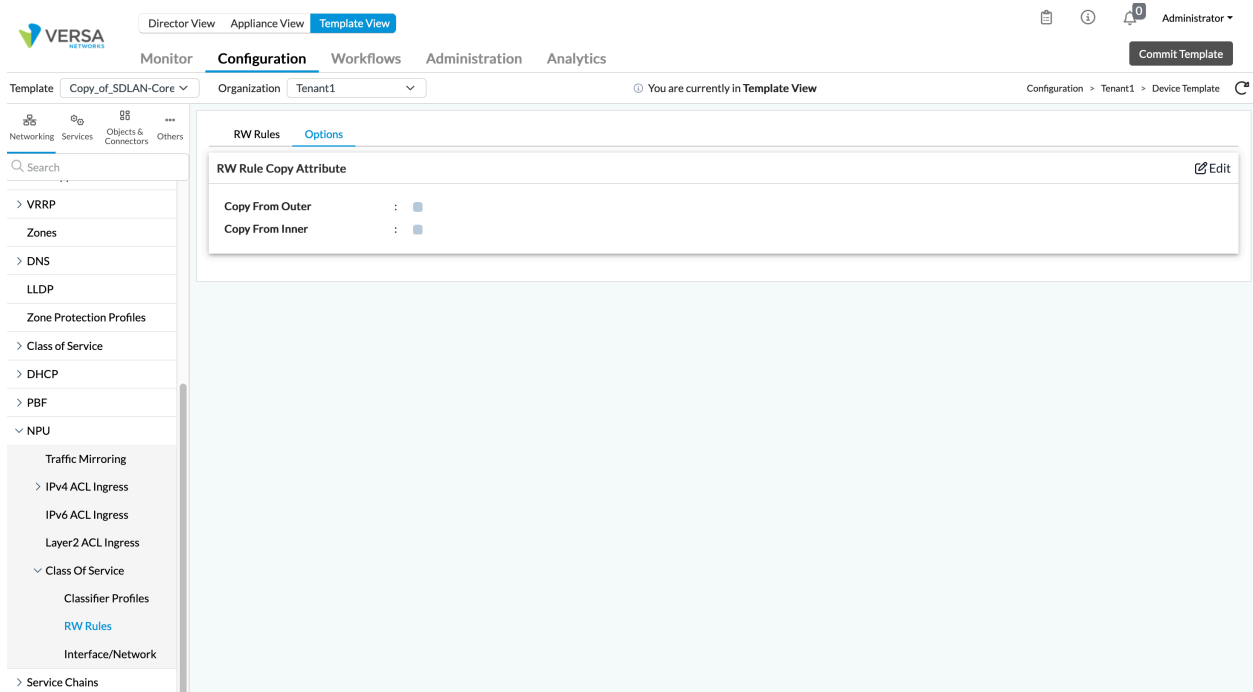
Loss Priority *	Code Point	Code Value	
<div> ---Please Select </div>	<div> ---Please Select </div>	<div>0...63</div>	<div>+</div>
No Records to Display			

OK

Cancel

Field	Description
Forwarding Class	Select the forwarding class to which to apply the rewrite rule.
Loss Priority	Select the drop loss priority at which the DSCP or IEEE 802.1p value should be rewritten: <ul style="list-style-type: none"> ◦ High ◦ Low ◦ Medium
Code Point	Select the DSCP or 802.1p code point names to associate with the forwarding class and the drop loss priority.
Code Value	If you select DSCP, enter the DSCP code point values to associate with the forwarding class and the drop loss priority. <i>Range: 0 through 63</i>
 Add Icon	Click the Add icon to add a forwarding class.

6. Click OK.
7. Click OK to add the rewrite rule.
8. Select the Options tab to configure rewrite options to copy the header markings from the inner header to the outer header, or vice versa.



- Click Edit. In the Edit RW Rule Copy Attribute popup window, enter information for the following fields.

Edit RW Rule Copy Attribute

✕

☐ Copy From Outer
 ☐ Copy From Inner

OK
Cancel

Field	Description
Copy From Outer	Copy the outer header markings to the inner header.
Copy From Inner	Copy the inner header markings to the outer header.

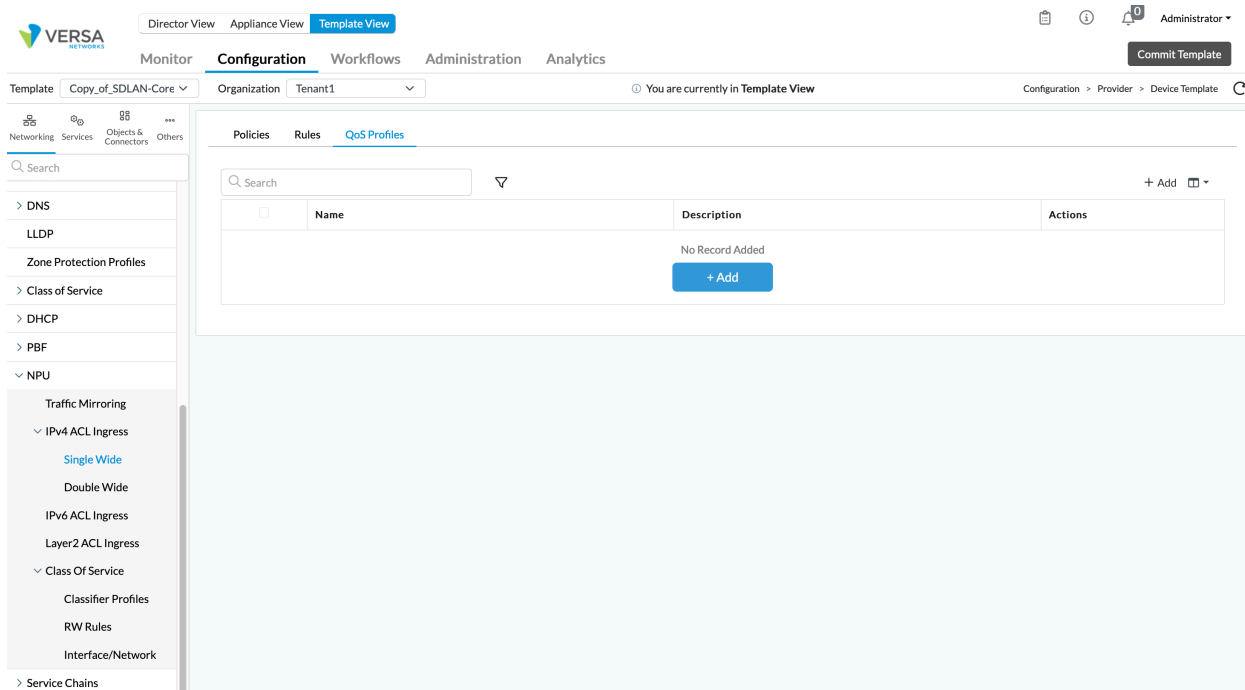
- Click OK.

Configure a QoS Profile for an ACL

You can associate a QoS profile to an access control list (ACL) to apply QoS policies to specific inbound traffic flows. In the QoS profile, you can configure a traffic policer to control the amount of traffic allowed by the ACL to prevent ingress traffic from overloading an egress port or the VOS device itself.

To configure a QoS profile for an ACL:

1. In Director View:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Click the name of an appliance. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > NPU in the left menu bar.
4. Select the type of NPU ACL policy:
 - IPv4 ACL Ingress, Single Wide
 - IPv4 ACL Ingress, Double Wide
 - IPv6 ACL Ingress
 - Layer 2 ACL Ingress
5. Click the QoS Profiles tab, and then click the + Add icon or the + Add button.



6. In the Add QoS Profiles popup window, enter information for the following fields.

Add QOS Profiles



Name *

Description

☒ Forwarding Class

☐ Per User Policer

Forwarding Class *

Loss Priority *

OK

Cancel

Field	Description
Name (Required)	Enter a name for the profile.
Description	Enter a text description the QoS profile.

- To assign ingress traffic to a forwarding class, click Forwarding Class, and then enter information for the following fields.

Field	Description
Forwarding Class	<p>Select the forwarding class to associate with the profile.</p> <ul style="list-style-type: none"> ◦ Forwarding Class 0 through Forwarding Class 3—Network Control ◦ Forwarding Class 4 through Forwarding Class 7—Expedited ◦ Forwarding Class 8 through Forwarding Class 11—Assured ◦ Forwarding Class 12 through Forwarding Class 15—Best Effort
Loss Priority	<p>Select the loss priority for the forwarding class.</p> <ul style="list-style-type: none"> ◦ Low ◦ Medium ◦ High

8. To configure a per-user policer, click Per-User Policer, and then enter information for the following fields.

Field	Description
Profile Choice	<p>Select the type of profile to use to limit traffic on the interface:</p> <ul style="list-style-type: none"> ◦ Single-Rate, Two-Color Policer—Configure a policer that consider the committed information rate (CIR) and committed burst size (CBS) values when limiting traffic flow. If the traffic rate falls below both values, the packets are marked as green. If the packet rate exceeds both the CIR and CBS thresholds, the packets are marked as red. By default, packets that are marked as green are allowed to pass, and those marked as red are dropped. ◦ Single-Rate, Three-Color Policer—Configure a policer that considers the CIR, CBS, and peak burst size (PBS) values when limiting traffic flow. If the traffic rate falls below the CIR, CBS, and PBS values, the packets are marked as green. If the traffic rate falls between the CBS and PBS thresholds, the packets are marked as yellow. If the packet rate exceeds either the CIR, CBS, or PBS values, the packets are marked as red. By default, packets that are marked as green or yellow are allowed to pass, and those marked as red are dropped. ◦ Two-Rate, Three-Color Policer—Configure a policer that considers the CIR, CBS, peak information rate (PIR), and PBS values when limiting traffic flow. If the traffic rate falls below the CIR, CBS, PIR, and PBS values, the packets are marked as green. If the packet rate is between CIR/CBS and PIR/PBS thresholds, the packets are marked as yellow. If the packet rate exceeds the both CIR/CBS and PIR/PBS threshold, the packets are marked as red. By default, packets that are marked as green or yellow are allowed to pass, and those marked as red are dropped.
Committed Burst Size	<p>Enter the CBS value, in bytes per second (Bps). This is the average volume of burst traffic that can pass through an interface.</p> <p><i>Range:</i> 125 through 4294967295 Bps <i>Default:</i> 125 Bps</p>

Committed Information Rate	<p>Enter the CIR value, in kilobits per second (Kbps). The CIR is the average rate of traffic that can pass through an interface.</p> <p><i>Range:</i> 64 through 4294967295 Bps <i>Default:</i> 64 Kbps</p>
Peak Information Rate	<p>For two-rate, three-color policers, enter the PIR value, in Kbps. The PIR is the maximum rate of traffic that can pass through an interface. The PIR value must be equal to or greater than the CIR value.</p> <p><i>Range:</i> 64 through 4294967295 Bps <i>Default:</i> 64 Kbps</p>
Peak Burst Size	<p>For three-color policer, enter the PBS value, in bytes per second. The PBS is the maximum volume of burst traffic that can pass through an interface. The PBS value must be equal to or greater than the CBS value.</p> <p><i>Range:</i> 125 through 4294967295 Bps <i>Default:</i> 125 bps</p>
Action	<p>Select the action to take when packets match the configured policer properties:</p> <ul style="list-style-type: none"> ◦ Drop Excess Traffic ◦ Exceed Loss Priority
Exceed Loss Priority	<p>For Exceed Loss Priority action, configure the exceed loss priority:</p> <ul style="list-style-type: none"> ◦ Low ◦ High ◦ Medium

9. Click OK.

Associate QoS Rules with Interfaces or Networks

You must associate classifier and rewrite rules with interfaces or networks. You use classifier rules to mark incoming packets on the ingress interface, and you then use rewrite rules to mark packets again when they exit on the egress interface.

Default Classifier Rules

When you associate classifier rules with an interface or network, you can select the classifier rules that you configured, or you can select default DSCP or 802.1p classifier rules. The following tables show the default mappings between DSCP and 802.1p values and the forwarding class and loss priority.

802.1p Value	Forwarding Class	Loss Priority
0	fc14	Low
1	fc_be	Low
2	fc10	Low
3	fc_af	Low
4	fc6	Low
5	fc_ef	Low
6	fc2	Low
7	fc_nc	Low

DSCP Value	Forwarding Class	Loss Priority
0-3	fc15	Low
4-7	fc14	Low
8-11	fc13	Low
12-15	fc_be	Low
16-19	fc11	Low
20-23	fc10	Low
24-27	fc9	Low
28-31	fc_af	Low
32-35	fc7	Low
36-39	fc6	Low
40-43	fc5	Low
44-47	fc_ef	Low
48-51	fc3	Low
52-55	fc2	Low
56-59	fc1	Low
60-63	fc_nc	Low

Configure Classifier and Rewrite Rules on Interfaces or Networks

- In Director view:
 - Select the Configuration tab in the top menu bar.
 - Select Devices > Devices from the horizontal menu bar.
 - Select an organization in the left menu bar.
 - Select a branch, hub, or Controller from the main pane. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select Networking > Class of Service > Interface/Network in the left menu bar.

The screenshot shows the Versa Networks Director View Template configuration page. The 'Interface' tab is selected in the 'Network' section. The table shows 'No Record Added' with a '+ Add' button. The left sidebar shows the navigation menu with 'Interface/Network' highlighted.

4. Select the Interface tab, and then click + Add to apply a QoS classifier or rewrite rule to an interface.
5. In the Add Interface popup window, enter information for the following fields.

Add Interface



<p>Name *</p> <div>---Please Select---</div>	<p>Description</p> <div></div>
<p>DSCP Rewrite Rule</p> <div>---Please Select---</div>	<p>802.1p Rewrite Rule</p> <div>---Please Select---</div>
<p>DSCP Classifier Rule</p> <div>---Please Select---</div>	<p>802.1p Classifier Rule</p> <div>---Please Select---</div>

Field	Description
Name (Required)	Select the name of an interface.
Description	Enter a text description for the interface.
DSCP Rewrite Rule	Select the DSCP rewrite rule to use for the egress traffic.
802.1p Rewrite Rule	Select the 8021p rule to use for the egress traffic.
DSCP Classifier Rule	Select the DSCP classifier rule to use for the egress traffic.
802.1p Classifier Rule	Select the 8021p classifier to use for the egress traffic.

6. Click OK.
7. Select the Network tab, and then click + Add to apply a QoS classifier or rewrite rule to a network.
8. In the Add Network popup window, enter information for the following fields.

Add Network



Name *

---Please Select---

Description

DSCP Rewrite Rule

---Please Select---

802.1p Rewrite Rule

---Please Select---

DSCP Classifier Rule

---Please Select---

802.1p Classifier Rule

---Please Select---

OK

Cancel

Field	Description
Name (Required)	Select the name of a network
Description	Enter a text description for the network.
DSCP Rewrite Rule	Select the DSCP rewrite rule to use for the egress traffic.
802.1p Rewrite Rule	Select the 8021p rule to use for the egress traffic.
DSCP Classifier Rule	Select the DSCP classifier rule to use for the egress traffic.
802.1p Classifier Rule	Select the 8021p classifier to use for the egress traffic.

9. Click OK.

Supported Software Information

Releases 22.1.4 and later support all content described in this article.

Additional Information

[Configure CoS](#)