Configure CoS

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 allows you to do the following:

- Prioritize network and application traffic so that you can ensure high priority for essential traffic and limit traffic for non-essential activities.
- Control how to share a link's bandwidth among different classes, subnetworks, and users in the network.
- Allocate bandwidth to internal and external traffic, and to upload and download traffic.
- Ensure low latency for network traffic involved in generating enterprise revenue.
- Implement application traffic profiling to ensure bandwidth usage.

CoS examines and classifies all incoming (ingress) traffic on a Versa Operating System^{TM} (VOS^{TM}) 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 egress traffic, CoS distributes the forwarding classes across interface queues and schedules the transmission for each queue. 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 DSCP and 802.1p bits in the packet headers.

To define how CoS handles ingress traffic, you do the following:

- Configure QoS profiles—QoS profiles define how to police ingress traffic, they assign the ingress traffic to a forwarding class, and they define whether to rewrite the DSCP or 802.1p header bits. For Releases 21.2.2 and later, a QoS profile can define a per-user policer, based either on IP address or user ID, to police the traffic for individual users, restrict the total number of concurrent users on the device, and restrict the number of sessions allowed for each user. For example, you can restrict YouTube traffic to 10 concurrent users, with 5 Mbps per user, and you can allow 100 concurrent users for voice traffic, with 100 Mbps and two active sessions for each user. You associate a QoS profile with a QoS policy.
- Define QoS policies—QoS policies define how to process ingress traffic, including match parameters and actions to take on matching traffic.
- Define application QoS policies—Application QoS policies define how to process ingress traffic based on the application or URL from which the traffic originates. When you define both QoS and application QoS policies, the QoS policy is applied first and the application QoS policy is applied second. This means that the application QoS policy overwrites the QoS policy.

To define how CoS handles egress traffic, you do the following:

- Define rewrite rules—Rewrite rules modify the DSCP and 802.1p bits in the headers of outbound traffic.
- Define drop profiles—Drop profiles define how to handle congestion on outbound queues when these queues are near or at their capacity. QoS supports weighted random early detection (WRED) and tail drops.
- Create schedulers and assign them to scheduler maps—Schedulers assign different types of traffic to different outbound queues. They associate drop profiles with a high and a low drop-low priority. Schedulers are grouped into a scheduler map, which assigns the schedulers to a traffic class.
- Associate the CoS egress configuration with interfaces and networks—For an interface or network, you define traffic shaping for the egress traffic, and you associate rewrite rules and schedule maps with the interface or network.

Hardware-Based Shapers

For Releases 22.1.1 and later.

CSG5000 series appliances support hardware-based egress CoS and shaping for Intel E810-based NICs, which support interfaces with data rates of 100 Gbps. The hardware-based shapers differ from the software-based VOS shapers, as described in this section.

For hardware-based shapers, you can configure four traffic classes and at most two queues per traffic class, for a maximum of eight scheduler queues. These eight queues are scheduled by a single parent scheduler node. This scheme differs from software shaper implementation, in which the queues are scheduled using a two-level scheduler in which the traffic class–level scheduler schedules only the traffic classes and the queues in each traffic class are scheduled using a second-level scheduler.

To map the forwarding classes (queues), the default mapping is done for two forwarding classes (out of the four) to a single queue as follows:

Software-Based Shaping Queue	Hardware-Based Shaping Queue
TC0	
• FC0, FC1	TC0_0
• FC2, FC3	TC0_1
TC1	
• FC4, FC5	TC1_0
• FC6, FC7	TC1_1

Software-Based Shaping Queue	Hardware-Based Shaping Queue
TC2	
• FC8, FC9	TC2_0
• FC10, FC11	TC2_1
TC3	
• FC12, FC13	TC3_0
• FC14, FC15	TC3_1

If you enable shaping and scheduling for traffic egressing an interface, you must configure all four traffic classes.

The two queues in a traffic class are scheduled at the same priority level as that of the traffic class to which they belong. The four traffic classes are scheduled in a strict priority, but the two queues within each are at the same priority level as that of its traffic class.

The Intel E810 scheduler does not support priority scheduling in the expected manner. To account for this, weighted round-robin (WRR) weights are added to the traffic classes to mimic a pseudo priority scheduling for sharing bandwidth that exceeds the queue's committed information rate (CIR). This mechanism provide sa rough strict priority scheduling, but it is not ideal and does not guarantee very low latency for the highest-priority traffic.

The CIR is guaranteed for each traffic class, and any extra bandwidth is distributed as per the priority.

If you configure a traffic class but do not configure a queue for the traffic class, a single default queue, queue-0, is instantiated, and the traffic for all four forwarding classes for the traffic class are queued to this single queue. Also, in absence of a forwarding class to {traffic class, queue} mapping configuration, for a traffic class configured with a single queue, traffic for all forward classes that are, by default, mapped to the traffic queue is queued to this single queue, the one configured or the default queue-0 if no queue is configured.

If you configure two queues for the traffic class, and if you also configure the CIR or priority information rate (PIR) for the traffic class, each configured queue is assigned a CIR and PIR proportional to the WRR weight for the queue. If you do not configure configure any weights for the queues, the CIR and PIR weights are split evenly (50 percent each) and traffic is forwarded in a round-robin fashion within the class. When the committed rate for a queue is met, any extra bandwidth is distributed equally between the two queues for the traffic class.

If you do not configure two queues for a traffic class, only one queue is instantiated, and it is assigned the traffic specifications for the traffic class. This behavior prevents unnecessary fragmentation of traffic rates across unused queues.

In contrast to software-based shapers, hardware-based shapers do not support the following:

- Pipe-level shaping—The only shaping that that hardware-based shapers support are port-level and interface-level scheduling and shaping for the traffic classes with two queues within the traffic classes, and port-level shaping.
- Adaptive shaping.
- Per-tenant shaping.
- Weighted random early detection (WRED) drops—Only tail drops are performed.

If you configure hardware-based shapers, it is recommended that you implement CoS on 100-Gbps ports.

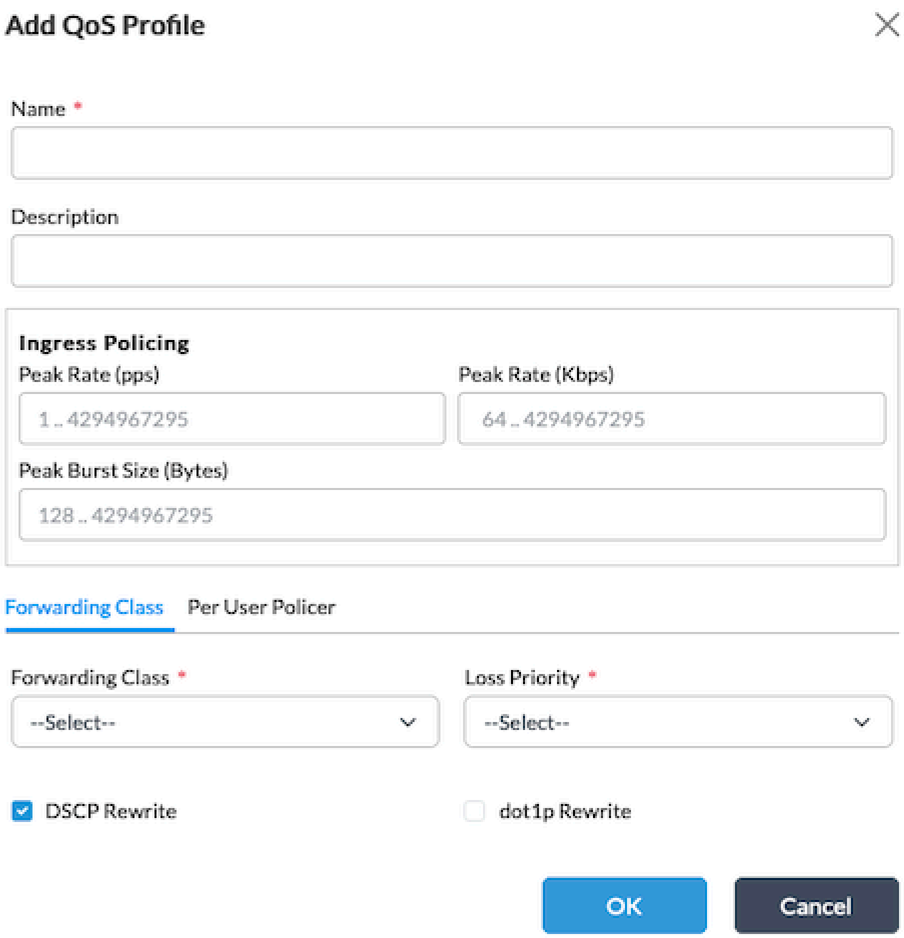
At the platform level, to enable hardware-based Cos on an interface, the interface must be configured with at most eight transmit poller threads (that is, at most eight TSS queues).

Configure QoS Profiles

You create QoS profile rules to configure bandwidth and priority settings for a forwarding class. You then associate one or more QoS profile rules with a QoS policy to apply the defined priority and bandwidth settings to a traffic flow. You can configure a maximum of 255 QoS profiles per tenant.

To configure a QoS 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 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 > QoS Profiles in the left menu bar.
4. Click the ⊞ Add icon to add a QoS profile. Enter information for the following fields.



Add QoS Profile

Name *

Description

Ingress Policing

Peak Rate (pps)

1..4294967295

Peak Rate (Kbps)

64..4294967295

Peak Burst Size (Bytes)

128..4294967295

Forwarding Class *

--Select--

Loss Priority *

--Select--

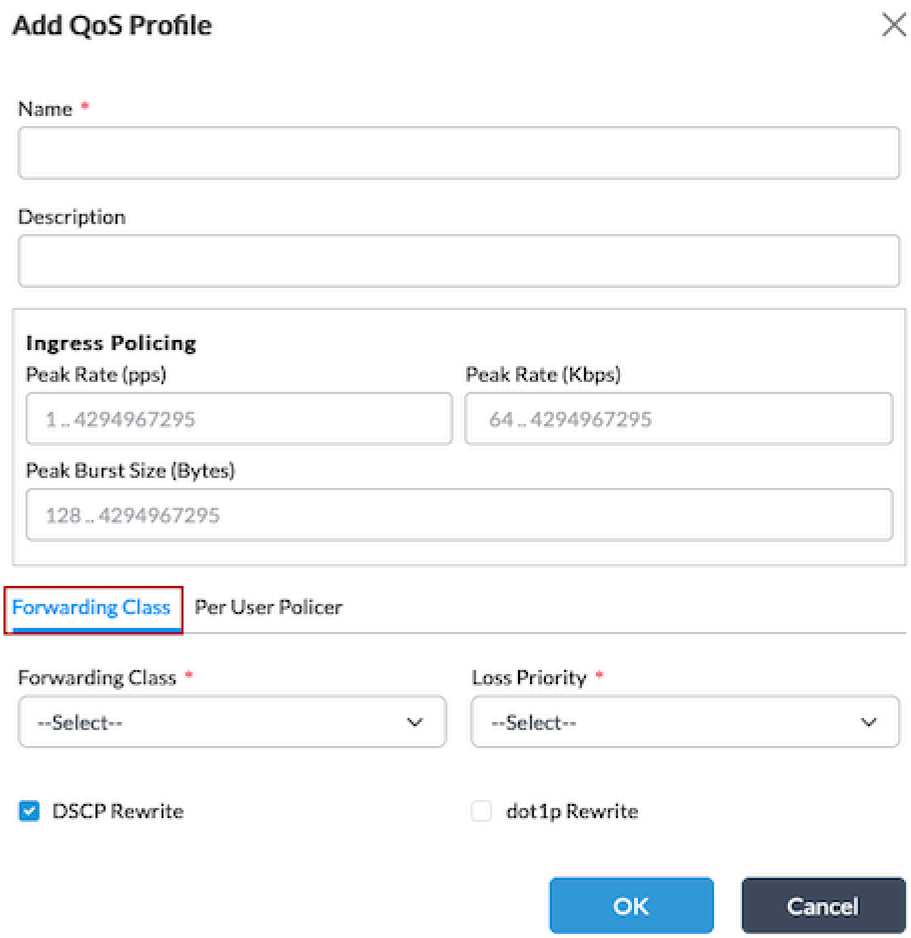
☑ DSCP Rewrite

□ dot1p Rewrite

Field	Description
Name (Required)	Enter a name for the profile.
Description	Enter a text description the profile.
Ingress Policing (Group of Fields)	
◦ Peak Rate	Enter how many data packets to allow, in packets per second (pps). All packets that exceed this value are dropped. Entering a peak rate value enables the policer. *Range*: 1 through 4294967295 pps *Default*: None

Field	Description
◦ Peak Rate	Enter the maximum ingress rate, in kilobits per second (Kbps). For Releases 21.2.2 and later, if you enter a peak rate value, the fields on the Per-User Policer tab display. For more information, see Step 6. *Range*: 64 through 4294967295 Kbps *Default*: None
◦ Peak Burst Size	Enter the packet burst size, in bytes. *Range*: 128 through 4294967295 bytes *Default*: None

5. Select the Forwarding Class tab, and enter information for the following fields.



Add QoS Profile

Name *

Description

Ingress Policing

Peak Rate (pps): 1 .. 4294967295

Peak Rate (Kbps): 64 .. 4294967295

Peak Burst Size (Bytes): 128 .. 4294967295

Forwarding Class *: --Select--

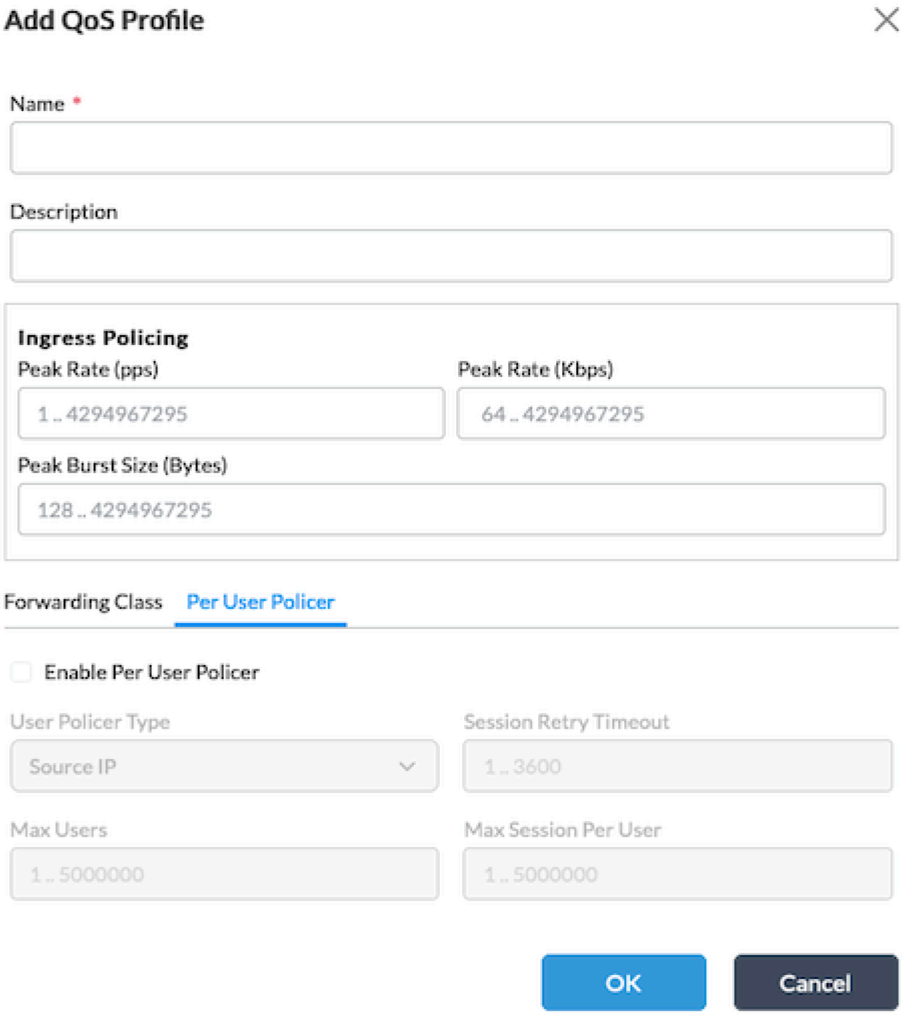
Loss Priority *: --Select--

☑ DSCP Rewrite

□ dot1p Rewrite

Field	Description
Forwarding Class (Required)	Select the forwarding class to associate with the profile.
Loss Priority (Required)	Select the loss priority for the forwarding class.
DSCP Rewrite	Click to change the DSCP value in the header of incoming IP packets. The value can be changed to predefined values.
Dot IP Rewrite	Click to rewrite the IEEE 802.1p value of outgoing Ethernet packets. The value can be changed to predefined values.

6. (For Releases 21.2.2 and later.) Select the Per-User Policer tab, and enter information for the following fields. Note that for the fields on the Per-User Policer tab to display, you must enter a value in the Peak Rate (Kbps) field. For more information about per-user policer statistics, see Monitor Per-User Policers, below.



Add QoS Profile

Name *

Description

Ingress Policing

Peak Rate (pps): 1 .. 4294967295

Peak Rate (Kbps): 64 .. 4294967295

Peak Burst Size (Bytes): 128 .. 4294967295

□ Enable Per User Policer

User Policer Type: Source IP

Session Retry Timeout: 1 .. 3600

Max Users: 1 .. 5000000

Max Session Per User: 1 .. 5000000

Field	Description
Enable Per-User Policer	Click to enable per-user policers. When you enable per-user policers, the policer allocates bandwidth to each user, aggregating bandwidth across all the user's sessions. For example, suppose you configure a QoS profile that has a peak Kbps rate of 10 Mbps, a maximum of 5 users, and a maximum of 4 sessions per user. If the QoS profile is associated with a policy that matches an application, the profile allows a maximum of 5 concurrent users to access the application, and each user can have a maximum of 4 sessions. The aggregate bandwidth limit that you define in the profile is applied on a per-user basis of 10 Mbps for all application traffic that matches the QoS or application QoS (App QoS) policy.
User Policer Type	Select the type of user for the policer: ◦ Source IP address. This is the default. ◦ User ID.
Session Retry Timeout	Enter the time, in seconds, after which user sessions can try to reconnect after a session timeout on exceeding the limit for maximum users or sessions per user. *Range*: 1 through 3600 seconds *Default*: 5 seconds
Maximum Users	Enter the maximum number of concurrent users allowed. *Range*: 1 through 5000000 *Default*: None
Maximum Sessions Per User	Enter the maximum number of concurrent sessions allowed for each user.

	Range: 1 through 5000000 *Default*: None

7. Click OK.

Configure Rewrite Rules

Rewrite rules allow you to remark, or change, bits in the header of outgoing packets. A rewrite rule examines a packet's forwarding class and loss priority and set the CoS bits to the value defined in the rule.

You use a classifier to mark packets or streams that arrive on the input interface, and you then use rewrite rules to mark packets or streams again when they exit on the egress interface. Rewrite rules apply the packet loss priority and forwarding class information to determine the Differentiated Services Code Point (DSCP) on outbound packets or streams.

VOS devices support the following types of remarking:

- DSCP for IPv4
- DSCP for IPv6
- IEEE 802.1p (not available on tvi tunnel interfaces)

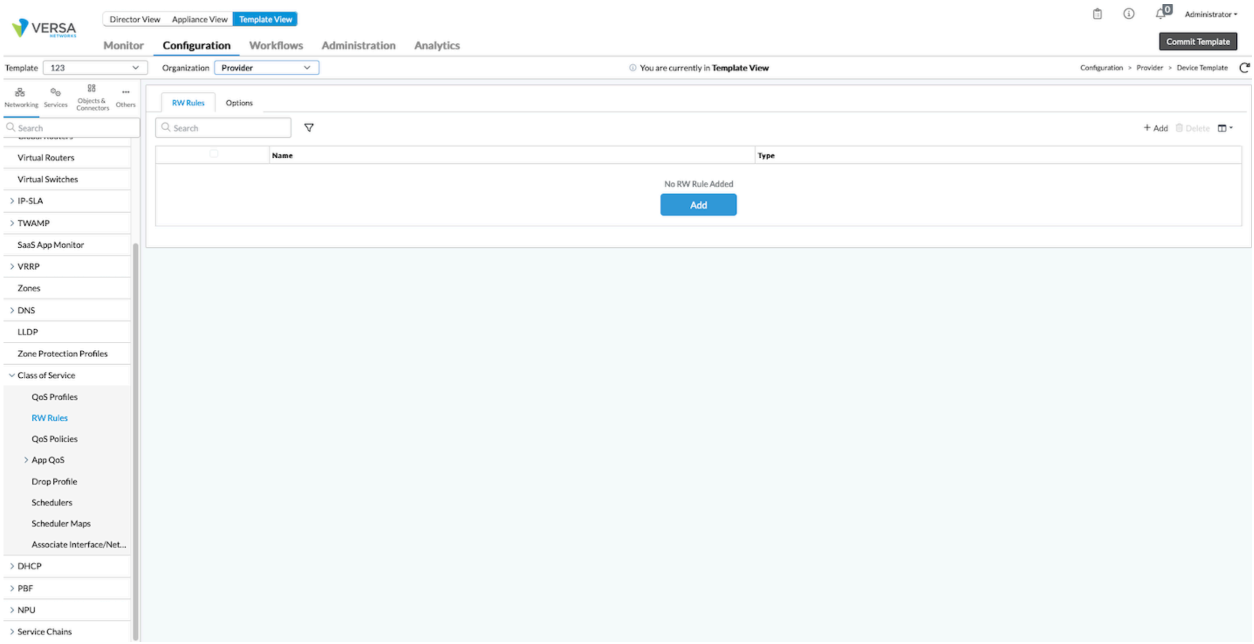
You can specify different rewrite rules for DSCP and IEEE 802.1p for each tenant (organization).

The Versa Networks technology uses an overlay to transport packets from one branch to another. The packets are encapsulated in a VXLAN header and then transported to the remote branch. Hence, the packets have two headers, referred to as the inner header and the outer header. You can use two methods to change the QoS markings on the inner and outer headers:

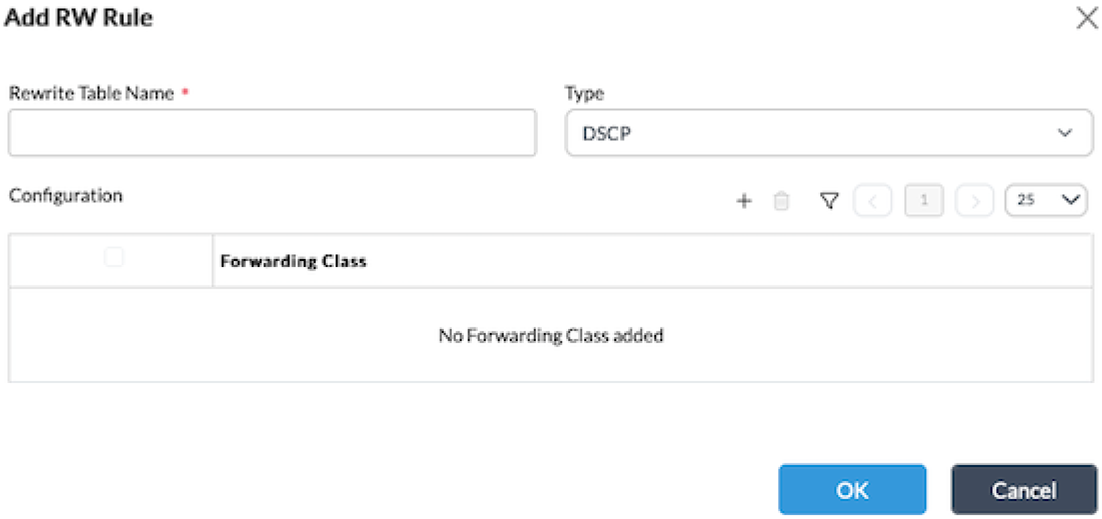
- Use a rewrite policy to classify traffic and set the QoS bits.
- Use rewrite options to copy the inner header markings to the outer header, and vice versa.

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 in the horizontal menu bar.



5. Click the ⊞ Add icon. In the Add RW Rule popup window, enter information for the following fields.



Add RW Rule

Rewrite Table Name *

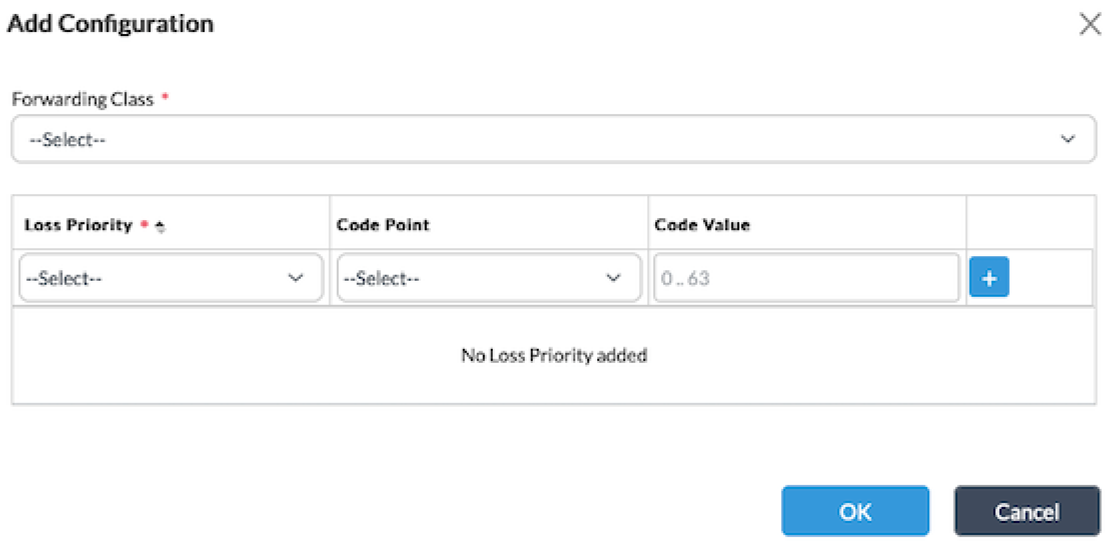
Type: DSCP

Configuration

□	Forwarding Class
	No Forwarding Class added

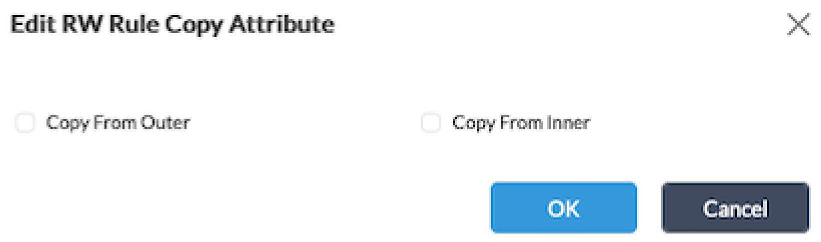
Field	Description
Rewrite Table Name	Enter a name for the rewrite table to contain the assigned forwarding class, loss priority, and DSCP, DSCPv6 or IEEE 802.1p value.
Type	Select the rewrite table type: ◦ DSCP ◦ DSCPv6 ◦ IEEE 802.1p (not available on tvi tunnel interfaces)
Configuration	Select the forwarding class: ◦ Assured forwarding ◦ Best effort ◦ Expedited forwarding ◦ Network control

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



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, DSCPv6, or IEEE 802.1p value should be rewritten: ◦ Low ◦ High
Code Point	Select the standard code point to associate with the forwarding class and the drop loss priority.
+ Add Icon	Click the Add icon to add a forwarding class.

7. Select the Options tab in the horizontal menu bar to use rewrite options to copy the inner header markings to the outer header. In the Edit RW Rule Copy Attribute popup window, enter information for the following fields.



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.

8. Click OK.

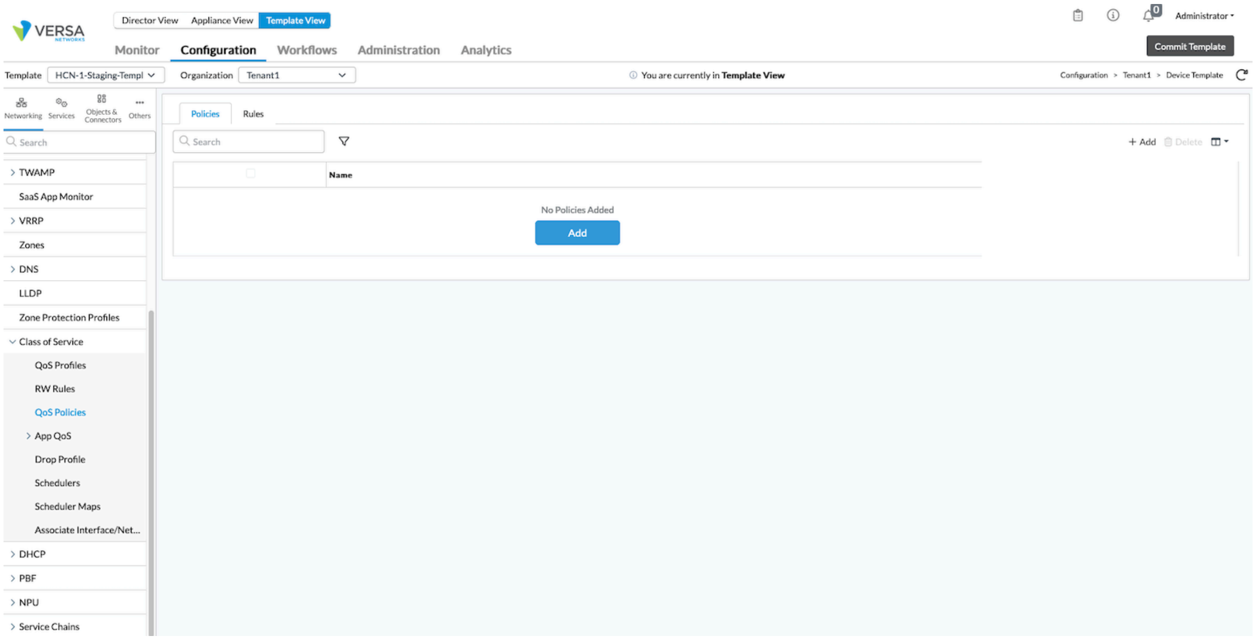
Configure QoS Policies

QoS policies define how to handle traffic when a network becomes congested. In the policies, you define rules for processing mission-critical and latency-sensitive application traffic as well as for processing lower-priority traffic. QoS policies are enforced on traffic flows. In a QoS policy, you associate QoS classes with specific types of traffic, and then you define how to classify traffic for treatment when it transits a QoS-enabled interface.

The rules in a policy are evaluated starting with the first rule, that is, from top to bottom in the order in which the rules are displayed in the Director rules table. When a packet matches the criteria defined in a rule, that rule is enforced and all subsequent rules in the policy are ignored. Therefore, to enforce the most specific match, place the more specific rules above the more generic rules, and place generic rules that can match any packets, such as wildcard rules, at the end. After you create policy rules, you can re-order them.

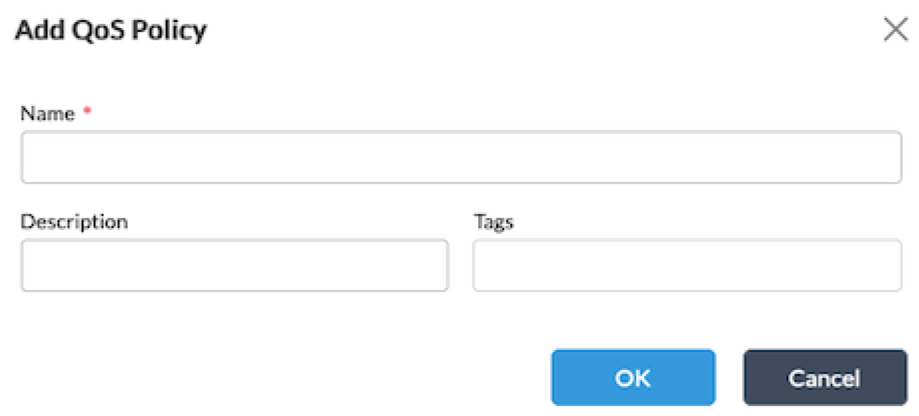
To configure a QoS policy:

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 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 > QoS Policies in the left menu bar.



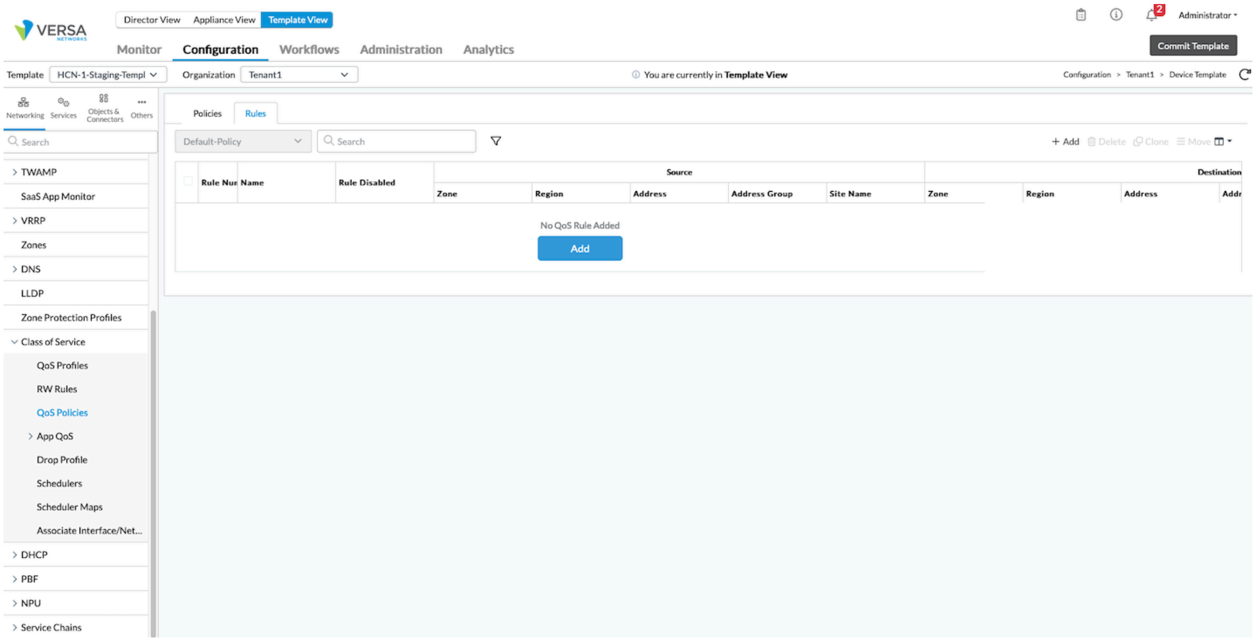
4. Select the Policies tab in the horizontal menu bar.

5. Click the ⊞ Add icon. In the Add QoS Policy popup window, enter information for the following fields.



Field	Description
Name (Required)	Enter a name for the policy.
Description	Enter a text description of the policy.
Tags	Enter tags to associate with the policy.

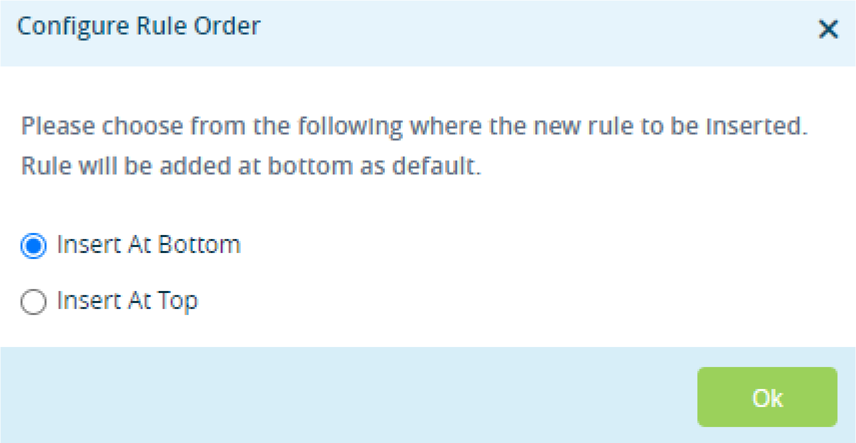
5. Click OK.
6. Select the Rules tab in the horizontal menu bar to define the matching criteria to select the incoming packets to which to apply the QoS policy.



7. Click the Add icon to define rules for the policy. The Add Rule popup window displays.
8. (For Releases 21.2.1 and later.) If you have already added one or more rules, the Configure Rule Order popup

window displays. The rules in a policy are evaluated from top to bottom as they are displayed in the Rules table, and when a packet matches, subsequent rules are ignored, so ensure that the policy rules are ordered with the most specific rules first.

a. Select where you want to insert the policy rule, either at the beginning or end of the existing rules.



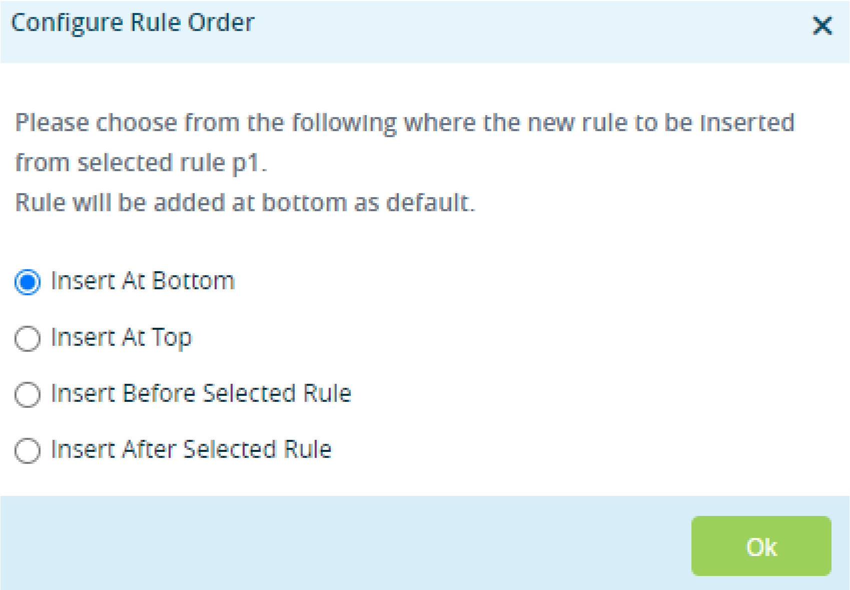
Configure Rule Order

Please choose from the following where the new rule to be inserted.
Rule will be added at bottom as default.

● Insert At Bottom

○ Insert At Top

b. If you select a rule and then click the Add icon, the Configure Rule Order popup window displays the following options:



Configure Rule Order

Please choose from the following where the new rule to be inserted from selected rule p1.
Rule will be added at bottom as default.

● Insert At Bottom

○ Insert At Top

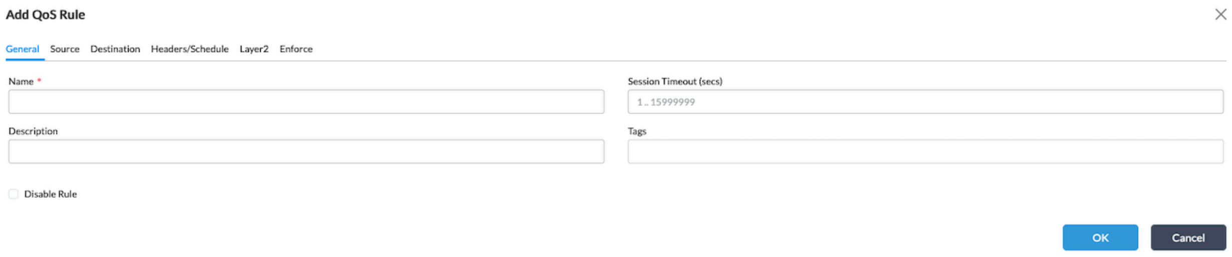
○ Insert Before Selected Rule

○ Insert After Selected Rule

c. Select the order to insert the rule (at the beginning or end bottom of the existing rules, or before or after the selected rule).

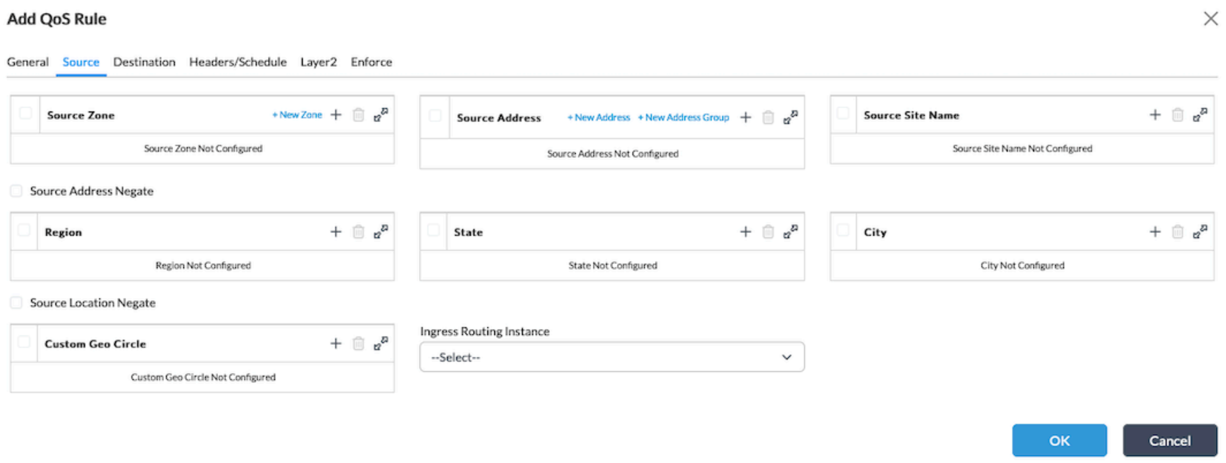
d. Click OK. The Add Rule popup window displays.

9. Select the General tab, and enter information for the following fields.



Field	Description
Name (Required)	Enter a name for the rule.
Session Timeout	Enter how long to wait before the session times out. *Range*: 1 through 15999999 seconds
Description	Enter a text description of the rule.
Tags	Enter tags to associate with the rule.
Disable Rule	Click to not activate the rule.

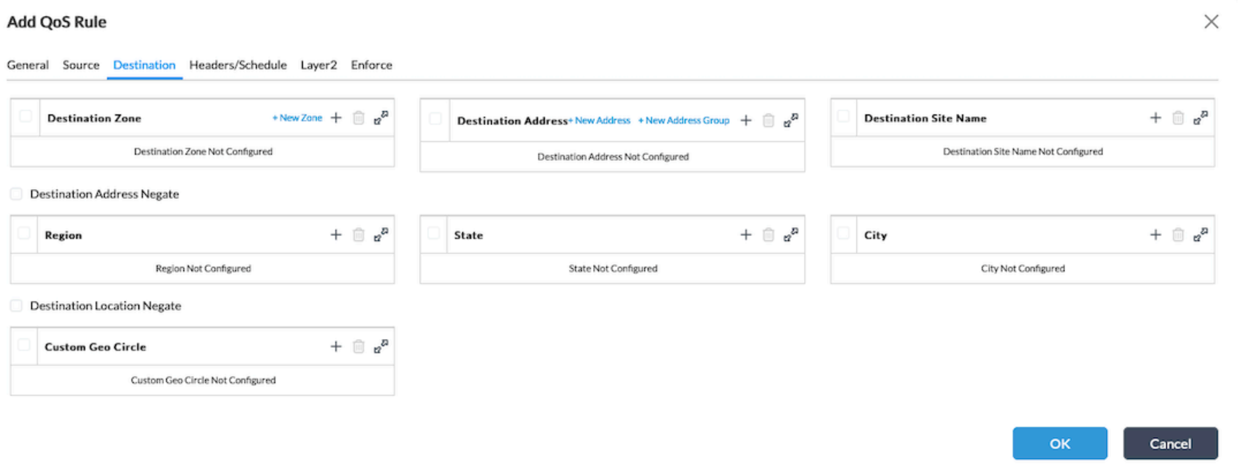
10. Select the Source tab to define match criteria based on the the source IP addresses, sites, and zones of the incoming packets. Enter information for the following fields.



Field	Description
Source Zone	For zones that you have configured for interfaces and networks, select the source zone to apply the rule to traffic coming from any interfaces or networks in the zone. Click the ⊞ Add icon to add an already configured zone to the list in the source zone table. Click + New Zone to configure a new zone. Note that

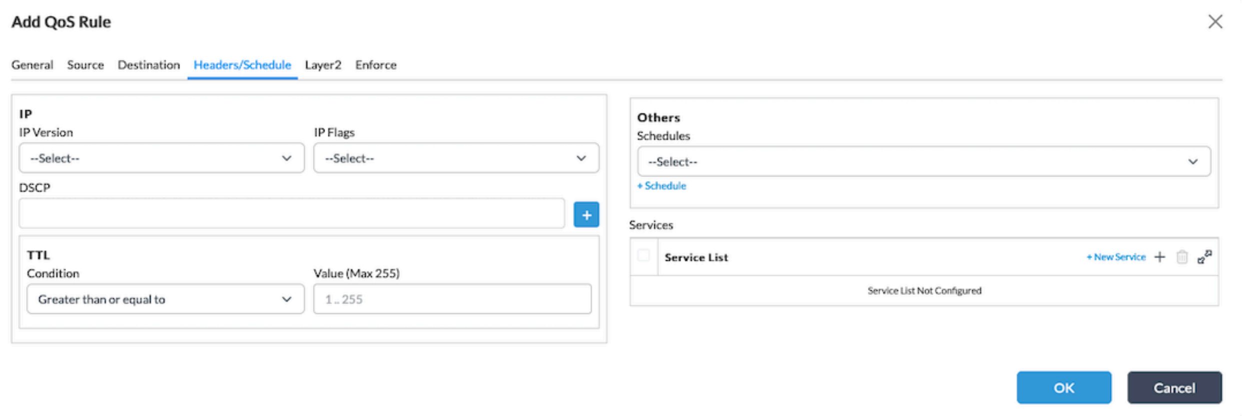
Field	Description
	you cannot configure source zones for zones that you have configured for routing instances or for organizations. For information about configuring zones, see Configure Zones and Zone Protection Profiles.
Source Address	Select the address from which the traffic originates. Click the ⊞ Add icon to add an already configured address to the list in the source address table. Click + New Address to configure a new address. For information about configuring a new address, see the Configure Policy Rules section in Configure Policy-Based Forwarding. Note that for IPv4 addresses, you cannot enter a wildcard mask. For more information, see Configure Address Objects.
Source Site Name	Select the name of the site from which the traffic originates. Click the ⊞ Add icon to add an already site to the list in the source site name table.
Ingress Routing Instance	Select the routing instance from which the traffic originates
Source Address Negate	Click to block traffic from the selected source addresses.

11. Select the Destination tab to define match criteria based on the the destination IP addresses and zones of the incoming packets. Enter information for the following fields.


Add QoS Rule
General
Source
Destination
Headers/Schedule
Layer2
Enforce
Destination Zone
+ New Zone
Destination Zone Not Configured
Destination Address
+ New Address
+ New Address Group
Destination Address Not Configured
Destination Site Name
Destination Site Name Not Configured
□ Destination Address Negate
Region
Region Not Configured
State
State Not Configured
City
City Not Configured
□ Destination Location Negate
Custom Geo Circle
Custom Geo Circle Not Configured
OK
Cancel

Field	Description
Destination Zone	For zones that you have configured for interfaces and networks, select the destination zone to apply the rule to traffic going to any interfaces or networks in the zone. Click the ⊞ Add icon to add an already configured zone to the list in the destination zone table. Click + New Zone to configure a new zone. Note that you cannot configure source zones for zones that you have configured for routing instances or for organizations. For information about configuring zones, see Configure Zones and Zone Protection Profiles.
Destination Address	Select the address to which the traffic is directed. Click the ⊞ Add icon to add an already configure address to the list in the destination address table. Click + New Address to configure a new address. For information about configuring a new address, see the Configure Policy Rules section in Configure Policy-Based Forwarding. Note that for IPv4 addresses, you cannot enter a wildcard mask. For more information, see Configure Address Objects.
Destination Site Name	Select the name of the site to which the traffic is directory. Click the ⊞ Add icon to add an already site to the list in the destination site name table.
Destination Address Negate	Click to block traffic destined to the selected addresses.

12. Select the Headers/Schedule tab to define match criteria based on the IP packet header information and to define schedules. Enter information for the following fields.


Add QoS Rule

General | Source | Destination | Headers/Schedule | Layer2 | Enforce

IP

IP Version: --Select--

IP Flags: --Select--

DSCP

TTL

Condition: Greater than or equal to

Value (Max 255): 1..255

Others

Schedules: --Select--

+ Schedule

Services

Service List

+ New Service

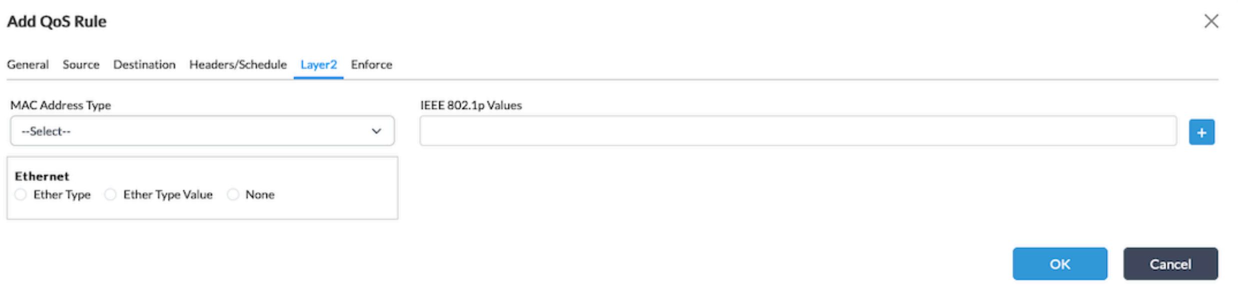
Service List Not Configured

OK Cancel

Field	Description
IP (Group of Fields)	
◦ IP Version	Select the IP version.
◦ IP Flags	Select the IP flags to set: ◦ More Fragments—Fragment incoming data packets. ◦ Don’t Fragment—Don't fragment incoming data packets.
◦ DSCP	Select the Differentiated Services Code Point (DSCP), which is the value or cost of
TTL (Group of Fields)	Set time-to-live information. ime to ive (TTL) Condition is the number of hops that a discarded by a router.
◦ Condition	Select the condition to apply to the TTL value: ◦ Greater than or Equal to ◦ Less than or Equal to ◦ Equal to
◦ Value	Enter a numeric value for the TTL, which is the number of hops that a packet can tr discarded. *Range:* 1 through 255
Others	
◦ Schedules	Select the schedule to apply to the rule. Schedules define rules for day-of the-week time-of-day actions to apply to the rule.
Services	Select the predefined and user-defined services to allow or block. Services are defi

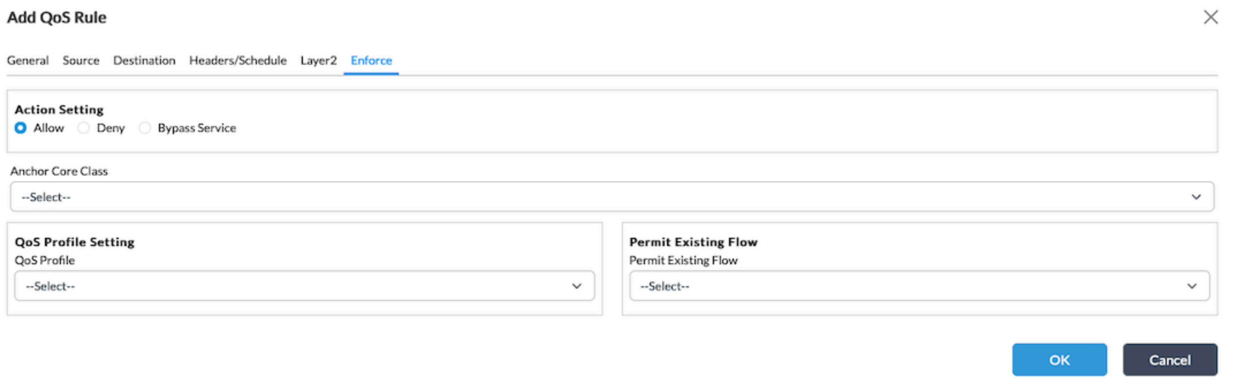
Field	Description
	address and port. Click the Add icon to add a service to the list.

13. Select the Layer 2 tab to classify the packets received on an interface. Enter information for the following fields.



Field	Description
MAC Address Type	Select a MAC address type to classify incoming packets: ◦ Broadcast ◦ Multicast
IEEE 802.1p Values	Enter the IEEE 802.1p priority value.
Ethernet (Group of Fields)	
◦ Ether Type	Click, and then select the type of incoming packet: ◦ IPv4 ◦ ARP
◦ Ether Type Value	Click, and then enter the value of the EtherType field in the Ethernet frame. *Range:* 1536 through 65535
◦ None	Click to not classify incoming packets based on Layer 2 criteria.

14. Select the Enforce tab to configure the action to take on the traffic. Enter information for the following fields.



Add QoS Rule

Action Setting
● Allow ○ Deny ○ Bypass Service

Anchor Core Class
--Select--

QoS Profile Setting
QoS Profile
--Select--

Permit Existing Flow
Permit Existing Flow
--Select--

Field	Description
Action Setting	Click the action to take on traffic that matches the rule: ◦ Allow—Permit traffic that matches the rule. ◦ Deny—Do not permit traffic that matches the rule. ◦ Bypass Service—Route traffic that matches without performing any service-related processing and without creating a session for this traffic.
QoS Profile Setting (Group of Fields)	
◦ QoS Profile	Select a QoS profile to associate with the QoS rule. The traffic peak rate, burst rate, forwarding class, and loss priority are applied to traffic that matches the rule. For more information, see Configure QoS Profiles, above.
Anchor Core Class	Select a core class to associate with the QoS rule. Core anchoring allow you to fine-tune performance on VOS devices for latency-sensitive applications. Setting an anchor core class overrides the Flow default Core Class allocation to Traffic Core Class (0 through 3) or User Core Class (4 through 7) so that you can configure more detailed flow anchoring to specific worker threads only. For more information, see Configure Core Profiles.
Permit Existing Flow	Select how to apply the rule to an existing flow for TCP sessions created by a non-SYN TCP packet. By default, system-level checking for TCP SYN packets is enabled, and all non-SYN TCP flows are dropped. For trusted TCP flows (that is, flows that match the rule) after a switchover or restart, you can allow them

Field	Description
	as follows: ◦ Allow—Allow the existing TCP flows with minimal services. This option allows trusted TCP flows (that is, flows that match the QoS rule) to continue after a switchover or restart. ◦ Validate—Allow the existing TCP flows with all services applicable in the service chain (that is, for all services applicable for the configured service set) to continue after a switchover or restart.

15. Click OK.

Configure Application QoS Policies

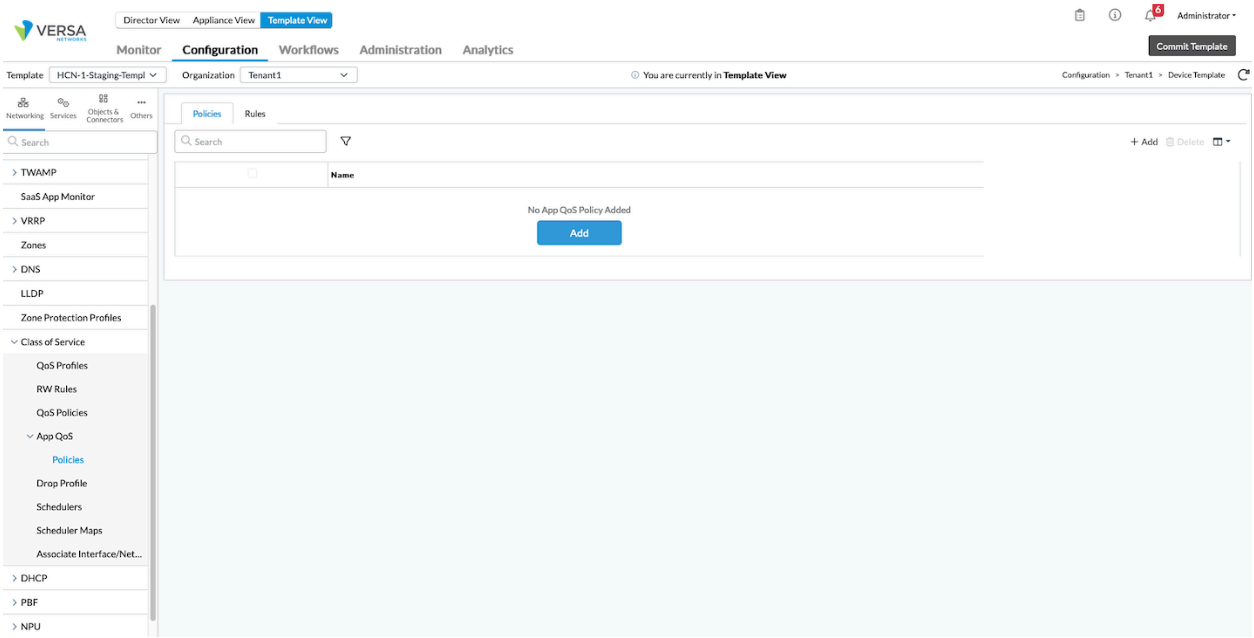
As with QoS policies, application quality of service, or App QoS, policies define how to handle traffic when a network becomes congested. You define rules for processing mission-critical and latency-sensitive application traffic as well as for processing lower-priority traffic. App QoS policies are based on Layer 7 protocols, and they are enforced on a per-session basis. In an App QoS policy, you associate QoS classes with specific types of Layer 7 applications, and then you define how to classify traffic for treatment when it transits a QoS-enabled interface.

The rules in a policy are evaluated starting with the first rule, that is, from top to bottom in the order in which the rules are displayed in the Director rules table. When a packet matches the criteria defined in a rule, that rule is enforced and all subsequent rules in the policy are ignored. Therefore, to enforce the most specific match, place the more specific rules above the more generic rules, and place generic rules that can match any packets, such as wildcard rules, at the end. After you create policy rules, you can re-order them.

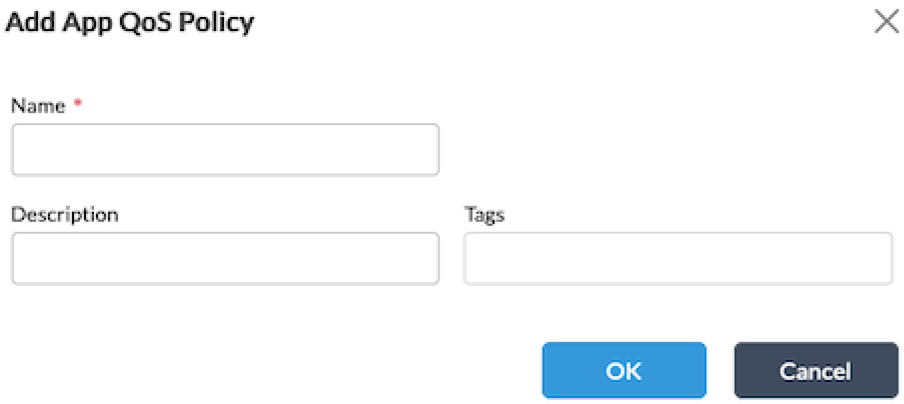
When you configure both QoS and App QoS policies, the QoS policy is evaluated first and then the App QoS policy is evaluated. Because the App QoS policy evaluation occurs after the QoS policy evaluation, the forwarding class assigned in the App QoS policy overwrites the one assigned in the QoS policy.

To configure an App QoS policy:

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 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 > App QoS > Policies in the left menu bar.



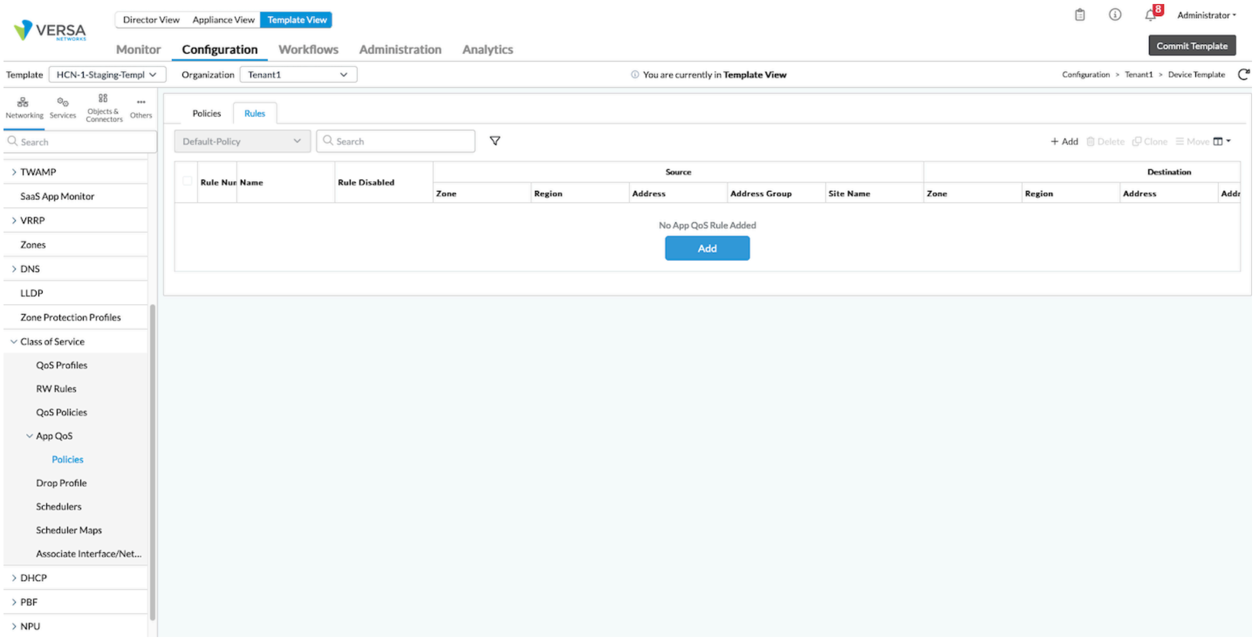
4. Click the ⊞ Add icon. In the Add App QoS Policy popup window, enter information for the following fields.



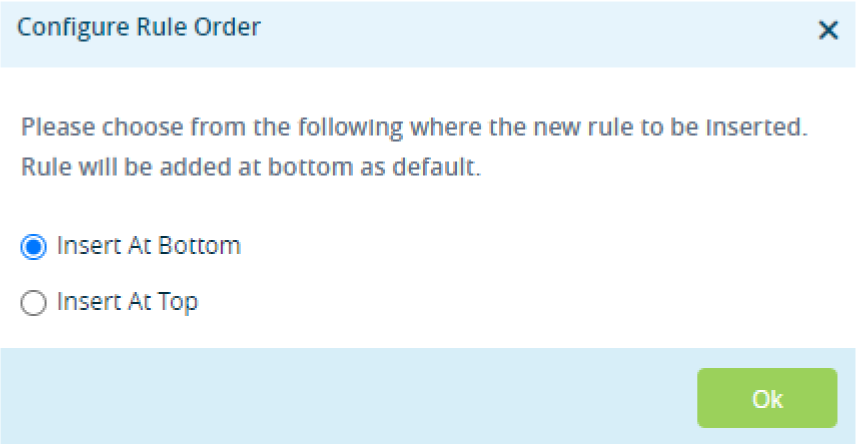
Field	Description
Name (Required)	Enter a name for the policy.
Description	Enter a text description of the policy.
Tags	Enter tags to associate with the policy.

5. Click OK. The main pane displays the new policy.
6. Select the Rules tab in the horizontal menu bar, to define the matching criteria to select the incoming packets to

which to apply the App QoS policy.



7. Click the Add icon to define rules for the policy. The Add Rule popup window displays.
8. (For Releases 21.2.1 and later.) If you already added one or more rules, the Configure Rule Order popup window displays. The rules in a policy are evaluated from top to bottom as they are displayed in the Rules table, and when a packet matches, subsequent rules are ignored, so ensure that the policy rules are ordered with the most specific rules first.
   a. Select where you want to insert the policy rule, either at the beginning or end of the existing rules.

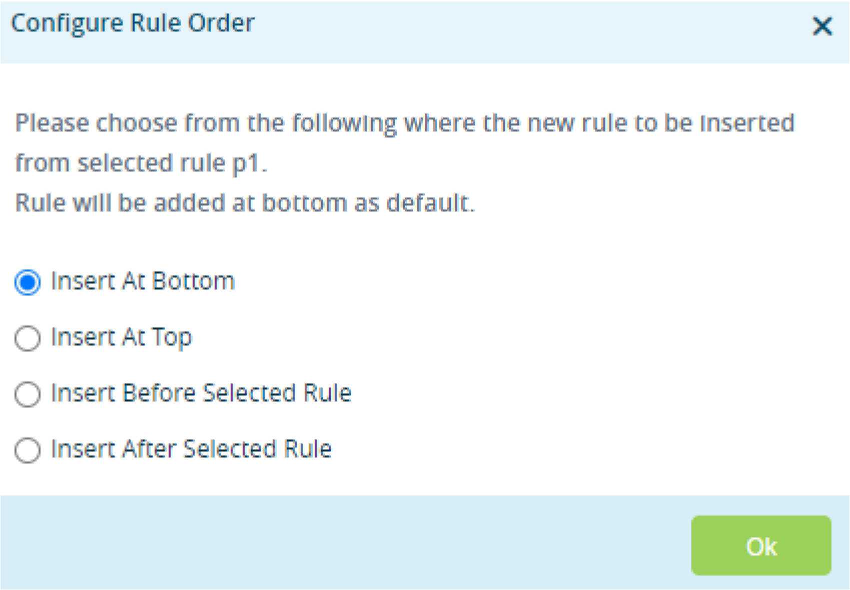

Configure Rule Order

Please choose from the following where the new rule to be inserted.
Rule will be added at bottom as default.

● Insert At Bottom

○ Insert At Top

   b. If you select a rule and then click the Add icon, the Configure Rule Order popup window displays the following options:



Configure Rule Order

Please choose from the following where the new rule to be inserted from selected rule p1.
Rule will be added at bottom as default.

● Insert At Bottom

○ Insert At Top

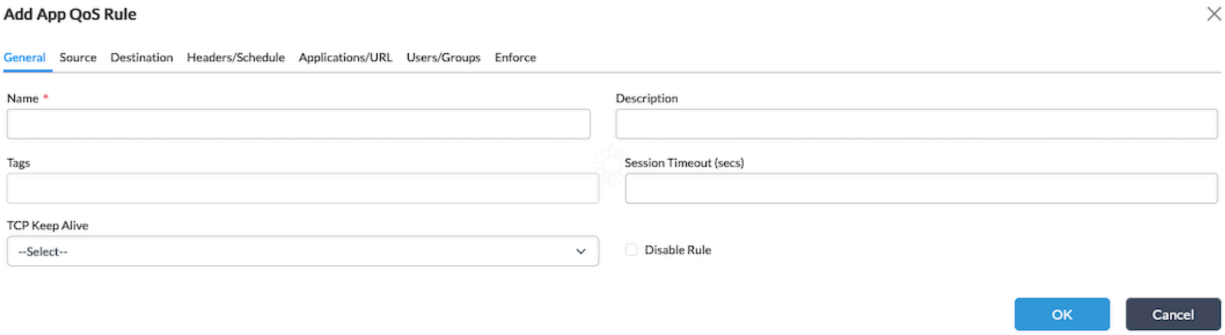
○ Insert Before Selected Rule

○ Insert After Selected Rule

c. Select the order to insert the rule (at the beginning or end bottom of the existing rules, or before or after the selected rule).

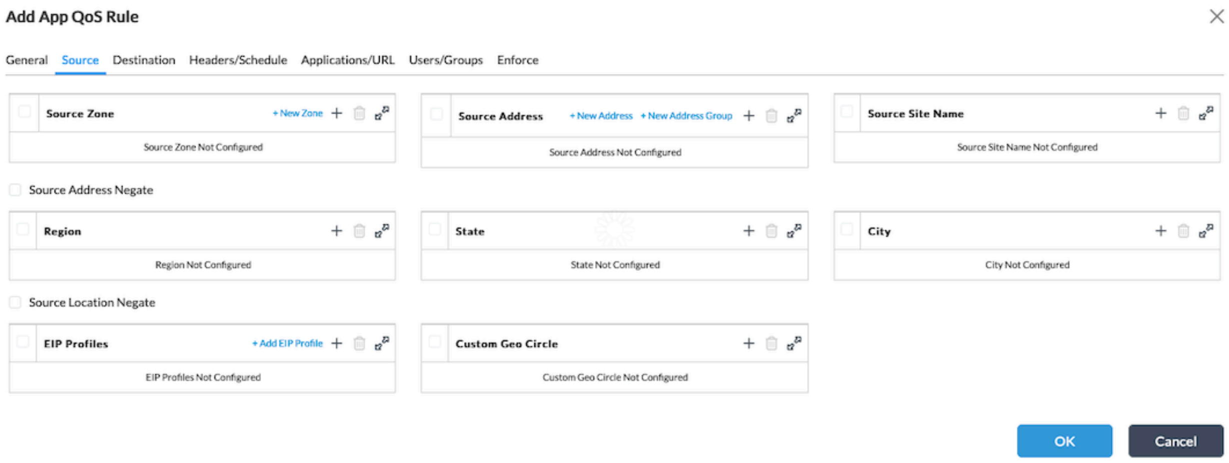
d. Click OK. The Add Rule popup window displays.

9. Select the General tab, and enter information for the following fields.



Field	Description
Name (Required)	Enter a name for the rule.
Description	Enter a text description of the rule.
Tags	Enter tags to associate with the rule.
Session Timeout	Enter how long to wait before the session times out. *Range*: 1 through 15999999 seconds
TCP Keepalive	Select whether to enable TCP keepalives.
Disable Rule	Click to not activate the rule.

8. Select the Source tab to define match criteria based on the source IP addresses, site names, and zones of the incoming packets. Enter information for the following fields.



Add App QoS Rule

General | Source | Destination | Headers/Schedule | Applications/URL | Users/Groups | Enforce

□ Source Zone + New Zone
Source Zone Not Configured

□ Source Address + New Address + New Address Group
Source Address Not Configured

□ Source Site Name
Source Site Name Not Configured

□ Source Address Negate

□ Region
Region Not Configured

□ State
State Not Configured

□ City
City Not Configured

□ Source Location Negate

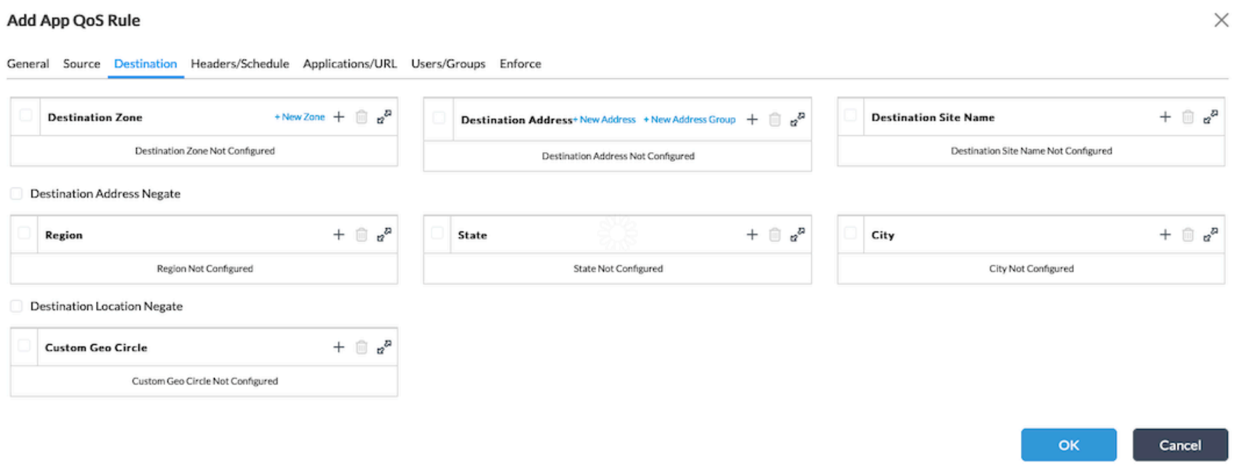
□ EIP Profiles + Add EIP Profile
EIP Profiles Not Configured

□ Custom Geo Circle
Custom Geo Circle Not Configured

Field	**Description**
Source Zone	For zones that you have configured for interfaces and networks, select the source zone to apply the rule to traffic coming from any interfaces or networks in the zone. Click the ⊞ Add icon to add an already configured zone to the list in the source zone table. Click + New Zone to configure a new zone. Note that you cannot configure source zones for zones that you have configured for routing instances or for organizations. For information about configuring zones, see Configure Zones and Zone Protection Profiles.
Source Address	Select the address from which the traffic originates. Click the ⊞ Add icon to add an already configure address to the list in the source address table. Click + New Address to configure a new address. For information about configuring a new address, see the Configure Policy Rules section in Configure Policy-Based Forwarding. (For Releases 20.2.2 and later.) For IPv4 addresses, you can enter a wildcard mask. The bits in the mask can be on (1) or off (0). Only the bits that are enabled in the mask are used to determine whether an IPv4 address matches. When a bit in a wildcard mask is

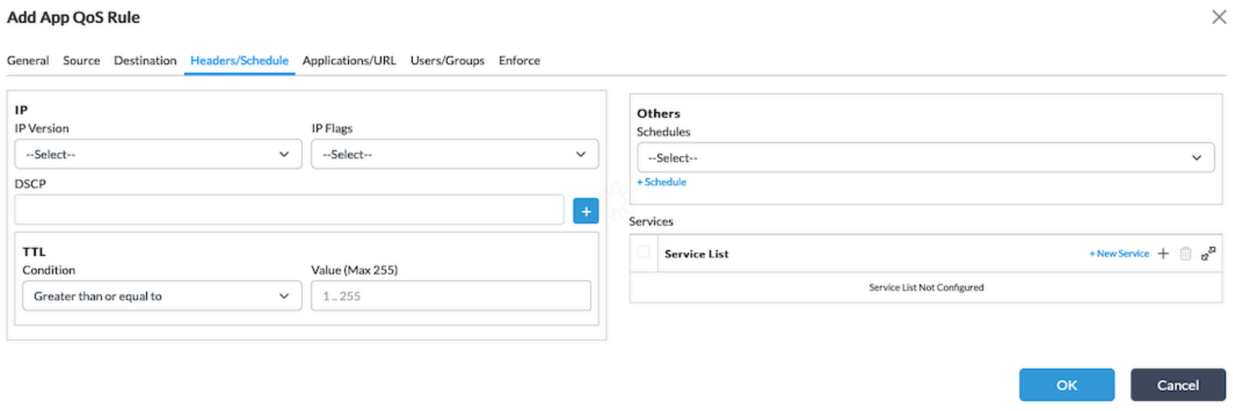
Field	Description
	on, that bit must match. When a bit in a wildcard mask is off, it is considered as a "don't care" bit and is disregarded for purposes of address matching. For example, the IPv4 address and mask 192.168.3.100/ 255.255.3.255 matches any IPv4 address 192.168.x.100, where, for x, the first 6 bits can be on (1) or off (0) and the last two bits must be on (11). Note that in a wildcard mask, at least one bit must be on. You can configure overlapping wildcard addresses. A single session can match a maximum of 16 wildcard addresses. For more information, see Configure Address Objects.
Source Site Name	Select the name of the site from which the traffic originates. Click the ⊞ Add icon to add an already site to the list in the source site name table.
Source Address Negate	Click to block traffic from the selected source addresses.

9. Select the Destination tab to define match criteria based on the destination IP addresses, site names, and zones of the outgoing packets. Enter information for the following fields.



Field	Description
Destination Zone	Select the name of the zone to which the traffic is directed. Click the ⊞ Add icon to add an already configured zone to the list in the destination zone table. Click + New Zone to configure a new zone. Note that you cannot configure destination zones for zones that you have configured for routing instances or for organizations. For information about configuring zones, see [Configure Zones and Zone Protection Profiles]().
Destination Address	For zones that you have configured for interfaces and networks, select the destination zone to apply the rule to traffic going to any interfaces or networks in the zone. Click the ⊞ Add icon to add an already configure address to the list in the destination address table. Click + New Address to configure a new address. For information about configuring a new address, see the Configure Policy Rules section in [Configure Policy-Based Forwarding]().
Destination Site Name	Select the name of the site to which the traffic is directed. Click the ⊞ Add icon to add an already site to the list in the source site name table.
Destination Address Negate	Click to block traffic to the selected destination addresses.

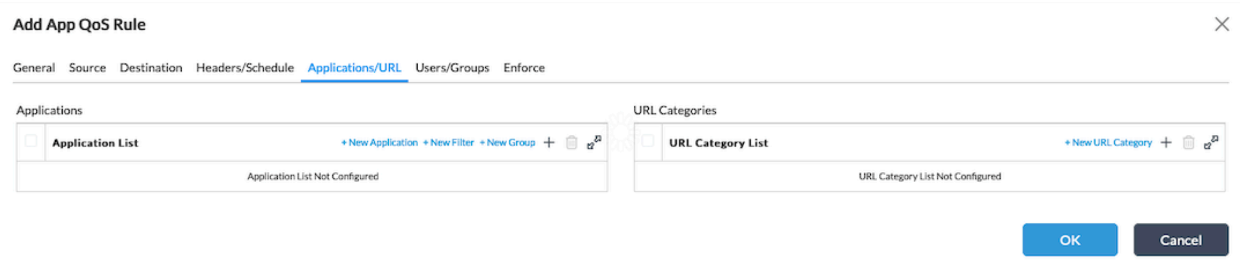
10. Select the Headers/Schedule tab to define match criteria based on the IP packet header information and to define schedules. Enter information for the following fields.



Condition: Greater than or equal to

Field	Description
IP (Group of Fields)	
◦ IP Version	Select the IP version.
◦ IP Flags	Select the IP flags to set: ◦ More Fragments—Fragment incoming data packets. ◦ Don’t Fragment—Don't fragment incoming data packets.
◦ DSCP	Select the Differentiated Services Code Point (DSCP), which is the value or cost
TTL (Group of Fields)	Set time-to-live information. ime to ive (TTL) Condition is the number of hops that discarded by a router.
◦ Condition	Select the condition to apply to the TTL value: ◦ Greater than or Equal to ◦ Less than or Equal to ◦ Equal to
◦ Value	Enter a numeric value for the TTL, which is the number of hops that a packet can being discarded.
Others	
◦ Schedules	Select the schedule to apply to the rule. Schedules define rules for day-of the-wee and time-of-day actions to apply to the rule.
Services	Select the predefined and user-defined services to allow or block. Services are de address and port. Click the Add icon to add a service to the list.

11. Select the Applications/URL tab to define matching criteria based on the source application or source URL category. A URL category is a group of related URLs. Enter information for the following fields.


Add App QoS Rule

General Source Destination Headers/Schedule Applications/URL Users/Groups Enforce

Applications

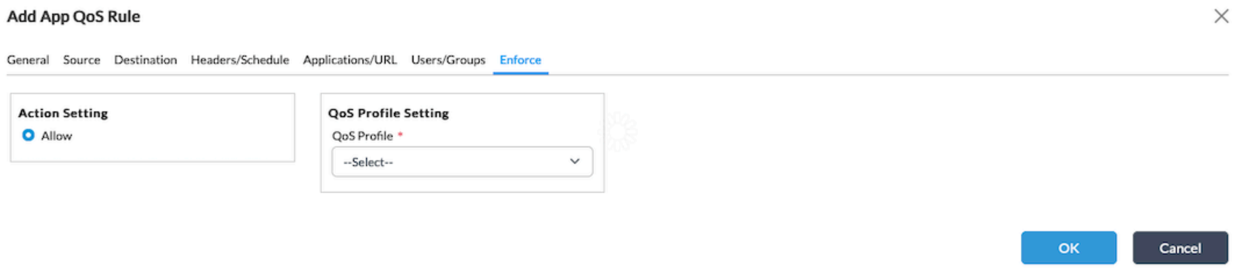
☐	Application List
Application List Not Configured	

URL Categories

☐	URL Category List
URL Category List Not Configured	

Field	Description
Applications	Select the application to match. Click the ⊞ Add icon to add an application to the list. Click + New Group to create an application group. For information about configuring a new application group, see the Configure Policy Rules section in [Configure Policy-Based Forwarding](#). Click + New Filter to create an application filter. Click + New Application to create an application list. For information about configuring a new application list, see the Configure Policy Rules section in [Configure Policy-Based Forwarding](#).
URL Categories	Select the URL category to match. Click the ⊞ Add icon to add a URL category to the list. Click + New URL Category to create a URL category.

12. Select the Enforce tab to configure the action to take on the traffic. Enter information for the following fields.



Action Setting
● Allow

QoS Profile Setting
QoS Profile *
--Select--

Field	Description
Action Setting	Select the action to take on traffic that matches this rule: ◦ Allow—Permit traffic that matches this rule.
QoS Profile Setting	

Field	Description
◦ QoS Profile	Select the QoS profile to associate with the App QoS rule. The traffic peak rate, burst rate, forwarding class, and loss priority are applied to traffic that matches the rule.

13. Click OK.

Configure Drop Profiles

Congestion occurs when there are more packets to send than the interface can handle. Drop profiles define how to handle congestion on outbound queues when these queues are near or at their capacity. You associate drop profiles with the two drop-loss priorities in a scheduler, and you then group schedulers into a scheduler map, which assigns the schedulers to a traffic class.

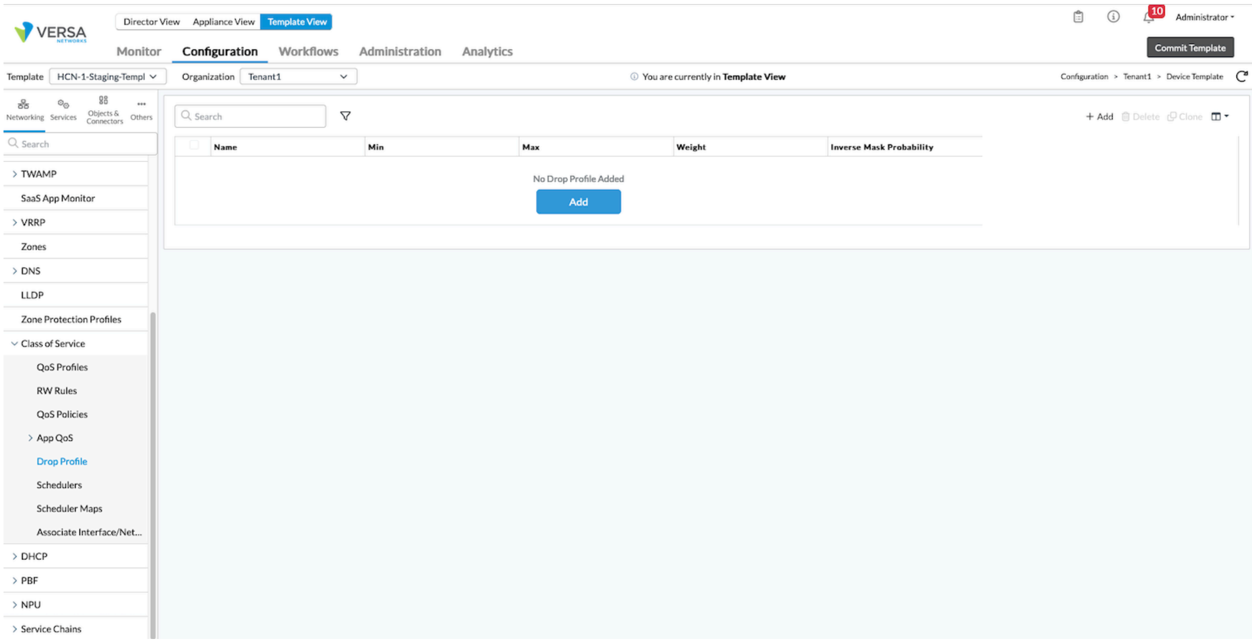
QoS supports the following ways to drop packets in outbound queues:

- Weighed random early detection (WRED)—Track the average queue length and drop packets randomly before the queue becomes full. WRED allows you to set the threshold at which packets with different priorities are placed in the outbound queue.
- Tail drops—Drop packets when the outbound queue is full.

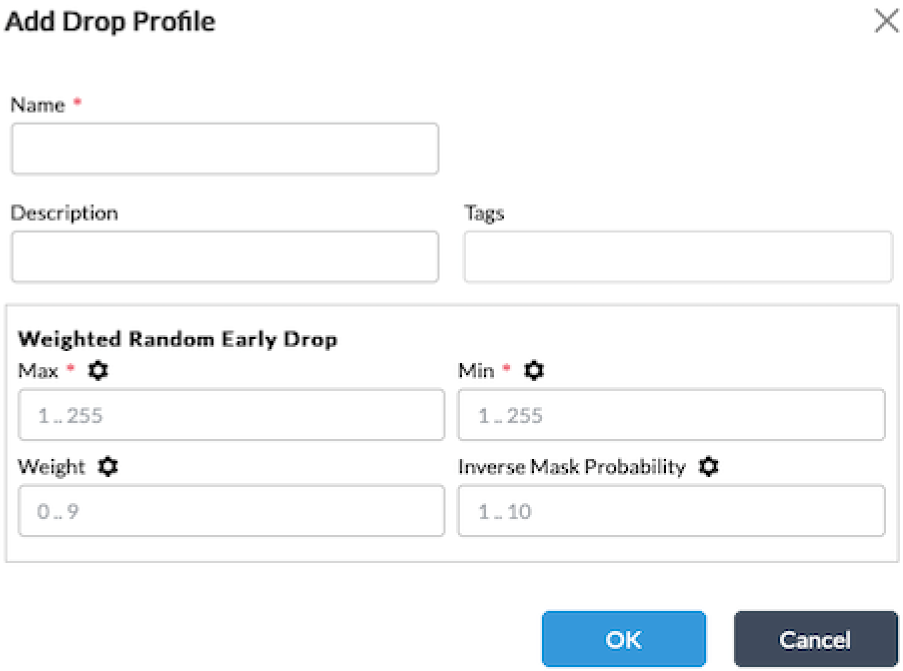
Configuring a drop profile is optional. If you do not configure one, by default, the VOS software sets a minimum value of 48 and a maximum value of 64 for WRED low loss priority, and a minimum value of 32 and a maximum value of 64 for WRED high loss priority. To use different values, create a drop profile.

To configure a drop 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 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 > Drop Profile in the left menu bar.



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



Field	Description
Name (Required)	Enter a name for the drop profile.

Field	Description
Description	Enter a text description of the drop profile.
Tags	Enter tags to associate with the drop profile.
Weighted Random Early Drop (Group of Fields)	
◦ Maximum	Enter a value for the high loss priority, which is the maximum number of data packets that the outbound queue can accept. When the average number of data packets in a traffic queue equals or exceeds this value, all the data packets are dropped. *Range*: 1 through 255 *Default*: None
◦ Minimum	Enter a value for the low loss priority, which is the minimum number of data packets that the outbound queue can accept. When the average number of data packets in a traffic queue equals or is greater than this value, data packets are randomly dropped. *Range*: 1 through 255 *Default*: None
◦ Weight	Enter a value for the exponentially weighted moving average (EWMA) filter weight. This weight is represented as an inverse log value. A lower value causes WRED to react more quickly, and a higher value causes it to react more slowly. *Range*: 0 through 9 *Default*: None
◦ Inverse-Mask Probability	Enter a value for the number of packets to drop in a group of packets. Put another way, one packet is dropped for every *x* number of packets, where *x* is the value you enter in this field. For example, if the value is 10, 1 packet out of every 10 packets is dropped. Note that use of this field is deprecated. It is recommended that you use the default values. *Range*: 1 through 10 *Default*: None

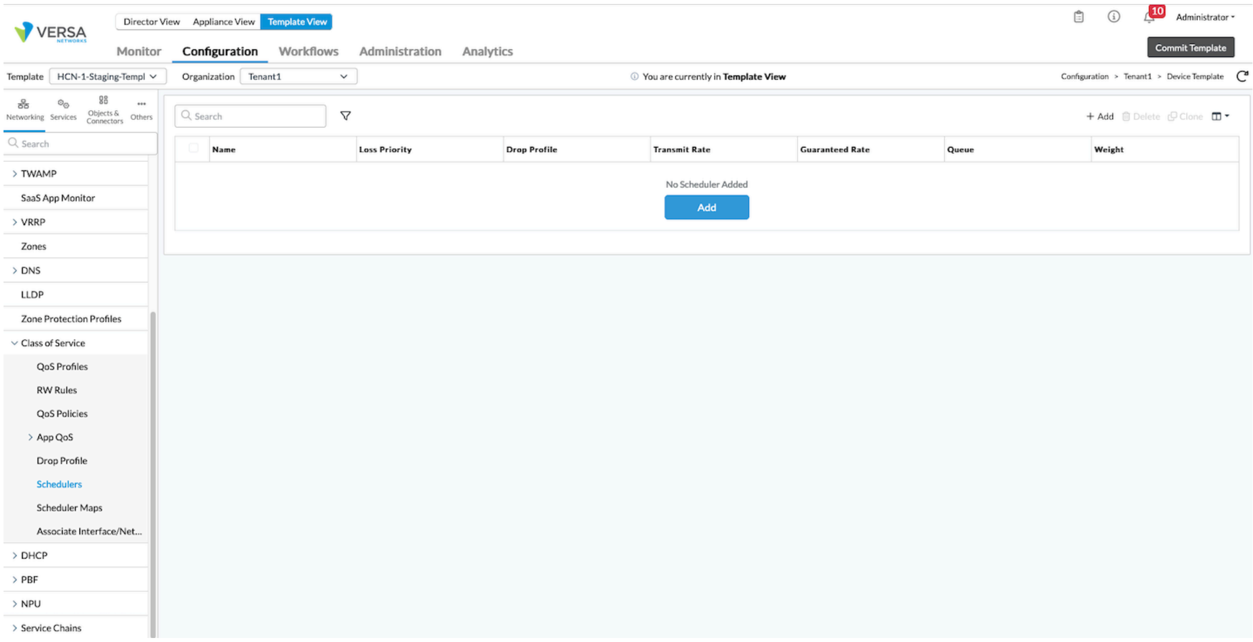
5. Click OK.

Configure Schedulers

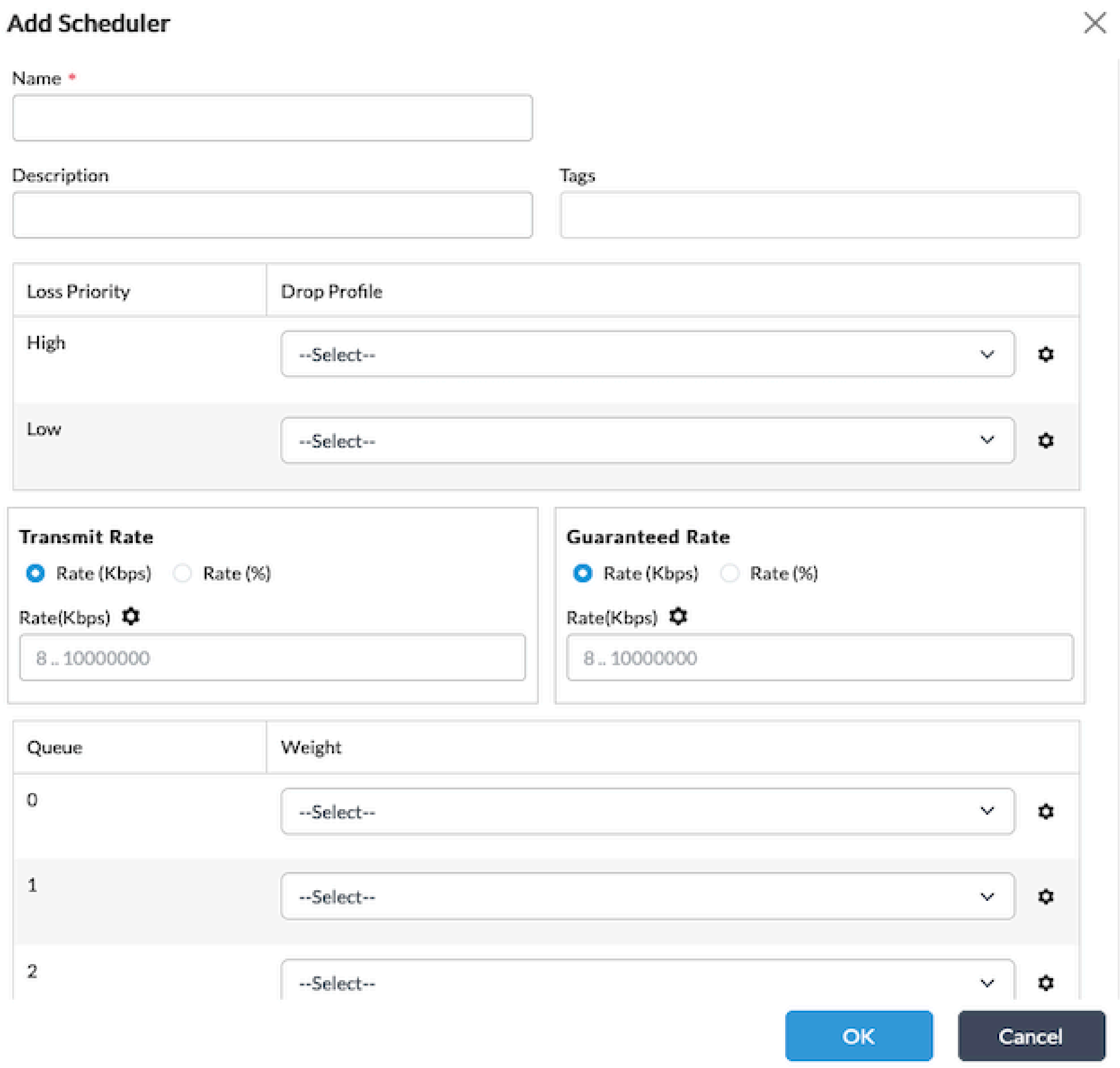
Schedulers assign traffic with different drop-loss priority levels to different outbound queues. Each scheduler has two drop loss priorities, high and low, and you can associate a different drop profile with each drop loss priority. You group schedulers into a scheduler map, which assigns the schedulers to a traffic class.

To configure a scheduler:

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 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 > Schedulers in the left menu bar.



4. Click the ⊞ Add icon. In the Add Scheduler popup window, enter information for the following fields.



Field	Description
Name (Required)	Enter a name for the scheduler.
Description	Enter a text description of the scheduler.
Tags	Enter tags to associate with the scheduler.
Loss Priority and Drop Profile	Select a drop profile to associate with traffic: ◦ High—Select a drop profile to associate with high-loss or lower-priority traffic.

Field	Description
	◦ Low—Select a drop profile to associate with low-loss or higher-priority traffic.
Transmit Rate (Group of Fields)	Set the transmission rate of data packets.
◦ Rate (Kbps)	Click, and then enter the transmission rate of data packets in kilobits per second (Kbps). *Range*: 8 through 100000000 Kbps *Default*: None
◦ Rate (%)	Click, and then enter the transmission rate of data packets as a percentage of the line bandwidth rate or of the parent interface's shaping rate. *Range*: 1 through 100 percent *Default*: None
Guaranteed Rate (Group of Fields)	Set the guaranteed transmission rate of data packets.
◦ Rate (Kbps)	Click, and then enter the guaranteed transmission rate of data packets in kilobits per second (Kbps). *Range*: 8 through 100000000 Kbps *Default*: None
◦ Guaranteed Rate (%)	Click, and then enter the guaranteed transmission rate of data packets as a percentage of the line bandwidth rate or of the parent interface's shaping rate. *Range*: 1 through 100 percent *Default*: None
Queue and Weight	For each queue, assign a weight for the queue.Traffic can be assigned to different queues.

5. Click OK.

Configure Scheduler Maps

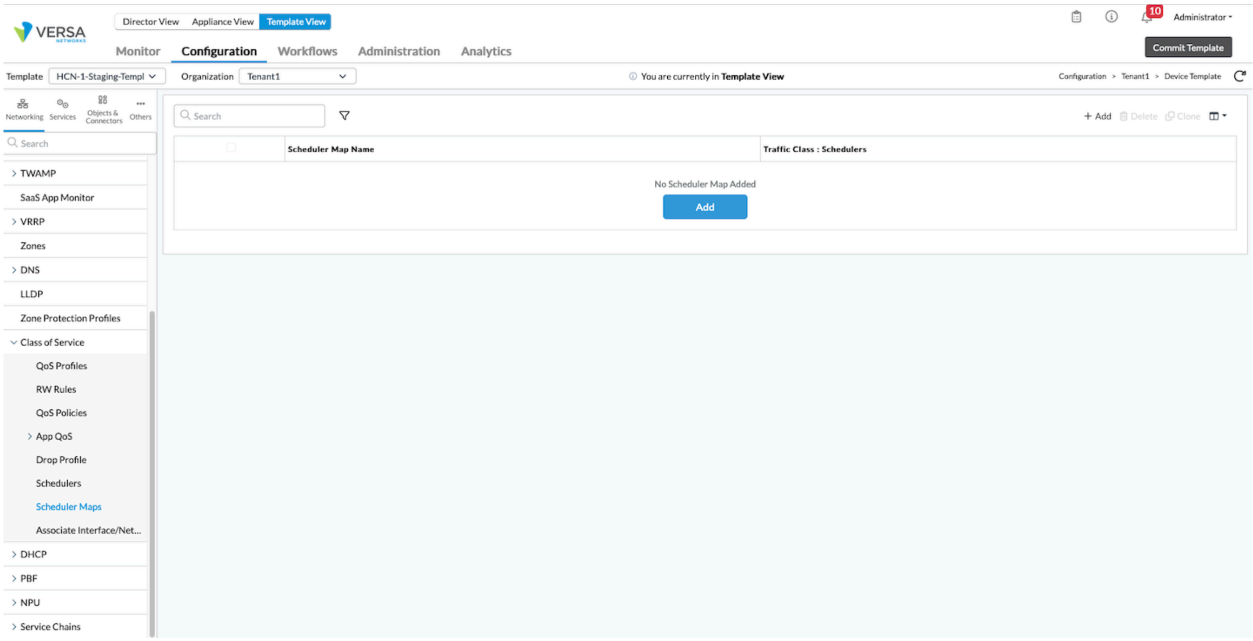
You group schedulers into a scheduler map, which assigns each scheduler to a traffic class. You apply scheduler maps to the egress interface to control and manage outgoing traffic.

To configure a scheduler map:

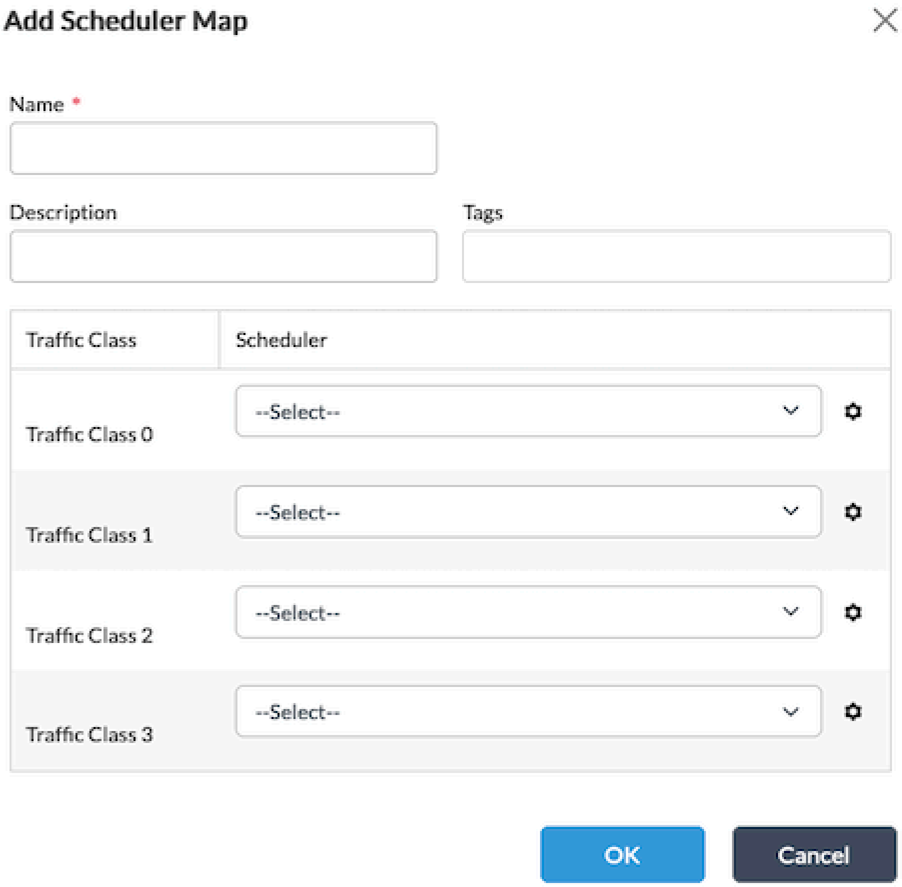
1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Devices > Devices from the horizontal menu bar.
   c. Select an organization in the left menu bar.

d. Select a 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 > Scheduler Maps in the left menu bar.



4. Click the ⊞ Add icon. In the Add Scheduler Map popup window, enter information for the following fields.



Add Scheduler Map

Name *

Description

Tags

Traffic Class	Scheduler
Traffic Class 0	--Select--
Traffic Class 1	--Select--
Traffic Class 2	--Select--
Traffic Class 3	--Select--

Field	Description
Name (Required)	Enter a name for the scheduler map.
Description	Enter a text description of the scheduler map.
Tags	Enter tags to associate with the scheduler map.
Traffic Class and Scheduler	For each traffic class, assign a scheduler based on the priority of the traffic. There are four traffic classes, 0 through 3, with Traffic Class 0 having the highest priority and Traffic Class 3 having the lowest.

5. Click OK.

Associate Egress Traffic with Interfaces and Networks

As the final step in configuring CoS, you associate the egress traffic with an interface or with a network. In this process, you associate a scheduler map and rewrite rules with the interface or network, and you define shaping parameters (burst size and peak traffic rate) for the egress traffic. Note that when you associate the egress traffic with an interface, the interface must be a whole interface, not a subinterface.

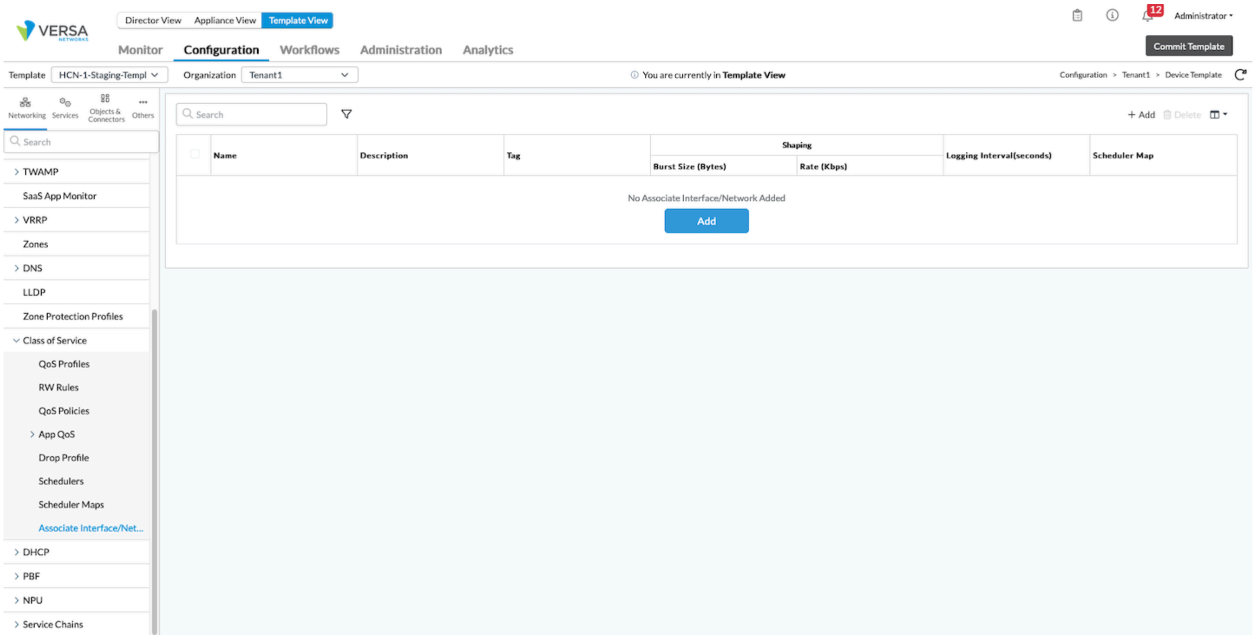
The following table describes which CoS features you can associate with different interface types. The information in this table has been verified against Release 21.2.

CoS Feature	**vni-*x*/*x* Interface**	**tvi Interface**	**Tunnel Interface**	**Network (Logical Interface)**
DSCP rewrite rule	No	Yes	Yes	Yes
802.1P rewrite rule	No	No	No	Yes
Drop profile (in scheduler)	Yes	No	No	No
Scheduler	Yes	No	Yes	Yes
Static shaping	Yes	No	No	Yes
Logging interval	Yes	No	No	Yes
Bandwidth sharing	Yes	No	No	No

Note that you cannot configure traffic shaping on TVI interfaces or on networks associated with any TVI interfaces. To associate a scheduler map with an adaptive shaping pipe (that is, an SD-WAN pipe), configure it under the tunnel interface (for Releases 21.2.1 and later).

To associate egress traffic with interfaces and networks:

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 Controller node in 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 > Associate Interface/Network in the left menu bar.

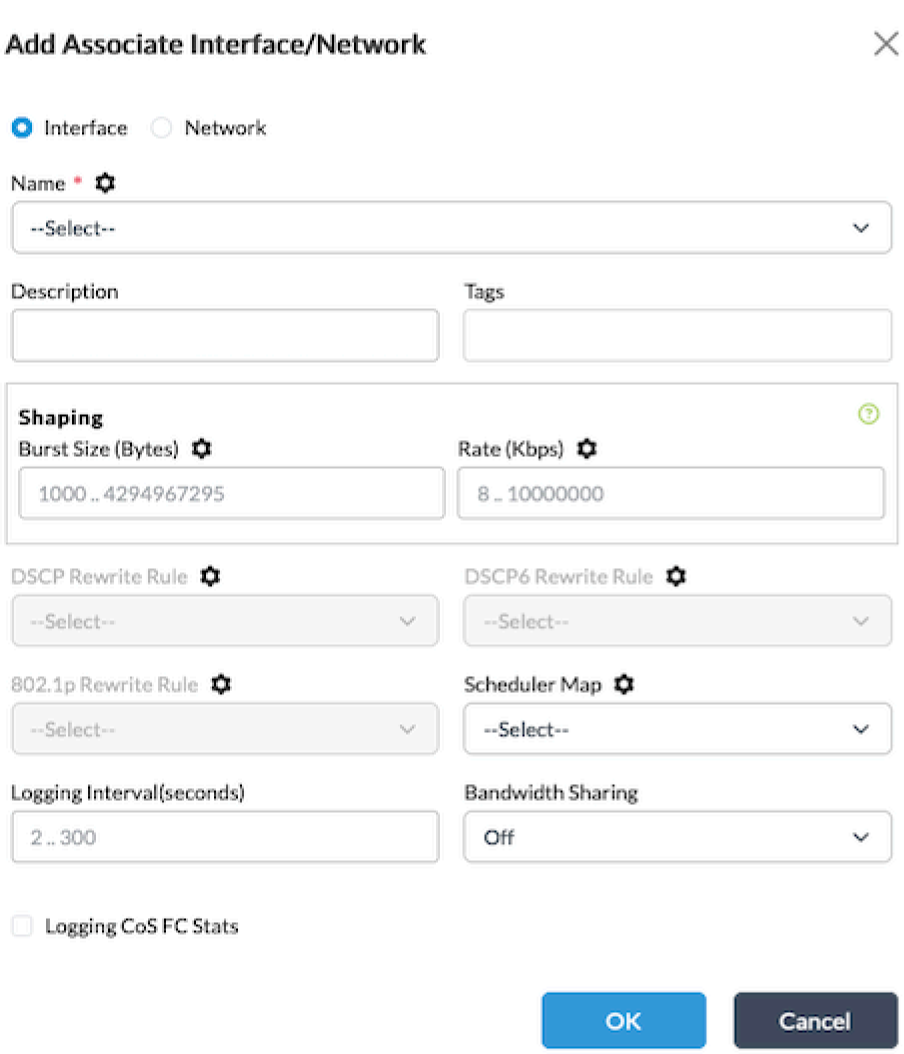


	Name	Description	Tag	Shaping		Logging Interval(seconds)	Scheduler Map
				Burst Size (Bytes)	Rate (Kbps)		

No Associate Interface/Network Added

Add

4. Click the ⊞ Add icon, and enter information for the following fields.



Add Associate Interface/Network

● Interface ○ Network

Name *

--Select--

Description

Tags

Shaping

Burst Size (Bytes): 1000 .. 4294967295

Rate (Kbps): 8 .. 10000000

DSCP Rewrite Rule: --Select--

DSCP6 Rewrite Rule: --Select--

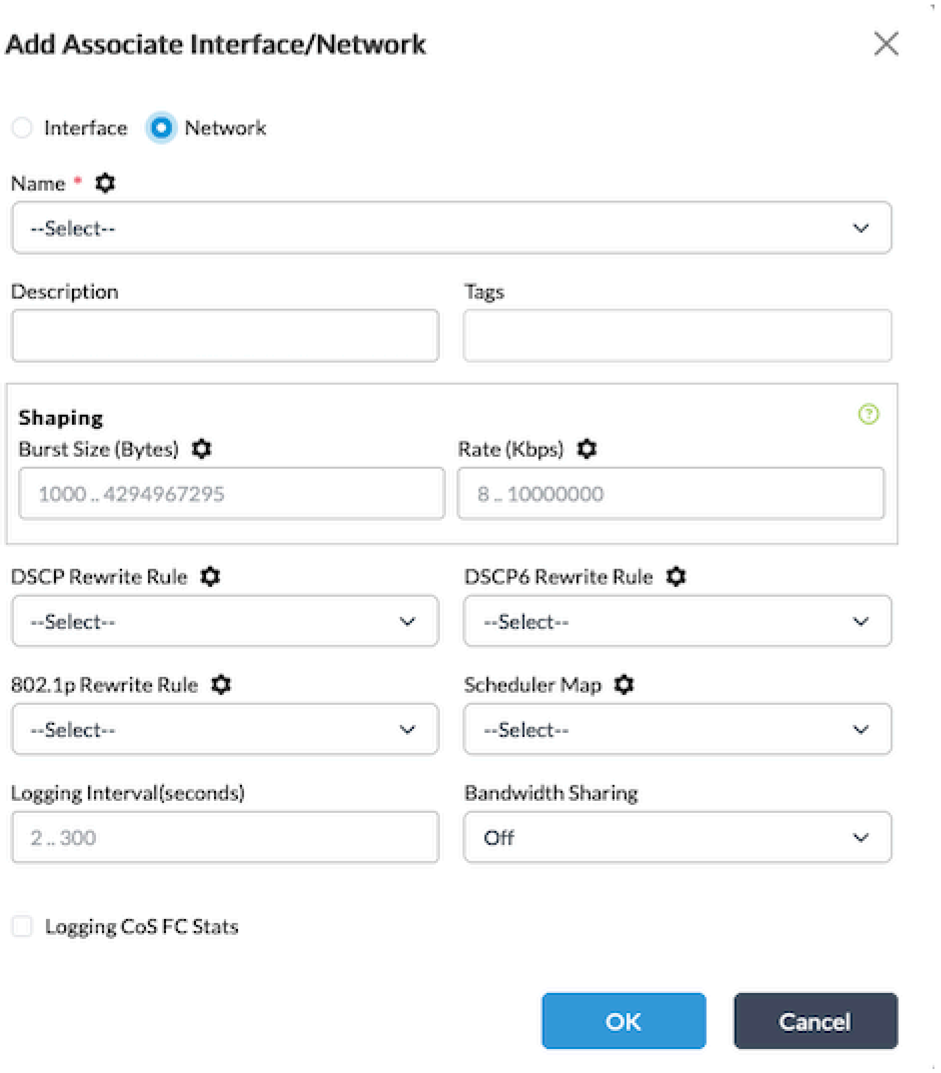
802.1p Rewrite Rule: --Select--

Scheduler Map: --Select--

Logging Interval(seconds): 2 .. 300

Bandwidth Sharing: Off

□ Logging CoS FC Stats



Add Associate Interface/Network

○ Interface ● Network

Name *

--Select--

Description

Tags

Shaping

Burst Size (Bytes): 1000 .. 4294967295

Rate (Kbps): 8 .. 10000000

DSCP Rewrite Rule: --Select--

DSCP6 Rewrite Rule: --Select--

802.1p Rewrite Rule: --Select--

Scheduler Map: --Select--

Logging Interval(seconds): 2 .. 300

Bandwidth Sharing: Off

□ Logging CoS FC Stats

Field	Description
Interface	Click to configure an interface association.
Network	Click to configure a network association.
Name (Required)	Select the name of an interface (when you select Interface) or a network (when you select the Network).
Description	Enter a text description for the interface or network.
Tags	Enter tags to identify the interface or network.
Shaping (Group of Fields)	Available when you select Network.
◦ Burst Size	Enter the burst size, in bytes.

Field	Description
	Range: 1000 through 4294967295 bytes *Default:* Depends on the link speed of the underlying interface. For example, if you connect two 1-GB interfaces, the burst size is 125000 bytes. If you connect a 1-GB interface to a 100-MB interface, the link speed is autonegotiated to 100 MB and the burst size is automatically set to 12500 bytes, and if you connect a 1-GB to a 10-MB interface, the burst size is automatically set to 1250 bytes. For most cases, it is recommended that you do not change the interface's burst size. However, you might consider changing it when the interface has autonegotiated a smaller burst size, but you know that the link can handle a larger higher burst. For example, if a 1-GB interface has autonegotiated to 10 MB, and if you know that the hardware can handle a burst of 125000 bytes and that the other side of the line can handle that much incoming burst, you could configure a larger burst.
◦ Rate	Enter the shaping rate, in Kbps. *Range*: 8 through 10000000 Kbps *Default:* None
DSCP Rewrite Rule	Select the DSCP rewrite rule to use for the egress traffic.
DSCP6 Rewrite Rule	Select the DSCP6 rewrite rule to use for the egress traffic.
802.1p Rewrite Rule	Select the 8021p rule to use for the egress traffic.
Scheduler Map	Select the scheduler map to use for the egress traffic.
Logging Interval	Enter a value for how often to log egress traffic, in seconds. Logs are forwarded to the active collector of the default LEF profile. For more information about configuring QoS logging, see section Configure SD-WAN QoS Logging in Apply Log Export Functionality.

Field	Description
Bandwidth Sharing	(For Releases 20.2 and later.) Select On to allow traffic distribution across units (pipes) in a single port. Note that within a particular unit, traffic distribution is governed by the guaranteed rate or transmit rate and weights allotted per traffic class. However, if traffic is distributed across units on a port, the behavior varies, depending on the configuration and the traffic pattern. To determine the effect of bandwidth sharing, consider the following scenarios: ◦ Non-oversubscription and bandwidth sharing are Off—Consider an example in which three units—units 10, 20, and 30—are allocated bandwidths of 10 Mbps, 20 Mbps, and 30 Mbps, respectively, and collectively, the bandwidth of the three units cannot exceed the total port bandwidth of 60 Mbps. If the units are overloaded, they do not use bandwidth of any of the other units. However, if one unit does not use its share of bandwidth, other units are not allowed to use that bandwidth. So, if unit 30 stops sending traffic, units 10 and 20 can still send only 10 Mbps and 20 Mbps, respectively, even though the port can send a maximum of 60 Mbps. This is the default and preferred mode of operation. ◦ Oversubscription—Consider an example in which which the three units—units 10, 20, and 30—can each send a maximum of 60 Mbps, and collectively, they cannot send more than the total port bandwidth of 60 Mbps. If all three units are overloaded and the traffic is relatively interleaved, the traffic is equally distributed across the three pipes. However, under unfavorable traffic conditions, significant deviations can be observed from an equitable distribution. ◦ Non-oversubscription and bandwidth sharing are On—Unused bandwidth can be shared between different units. The unused bandwidth is redistributed among the units that need them in the ratio of their configured bandwidths. For example, if unit 30, whose allotted bandwidth is 30 Mbps, stops sending traffic, the 30 Mbps of bandwidth is redistributed between the other units on the port.

4. Click OK.

Configure Traffic Shapers for Provider Organizations and Tenants

A provider organization can allocate the amount of WAN-facing bandwidth for each tenant in its organization. In this way, an appliance owner (that is, a provider organization) can control the bandwidth allocated to tenants. Tenants can view the amount of bandwidth allocated to them and can configure traffic shaping by creating schedulers to handle the traffic based on the allocated bandwidth (they do this in Versa Director), but they cannot change the amount of allocated bandwidth. The appliance owner (provider organization) can configure traffic shaping on physical interfaces.

The Director node automatically identifies the appliance owner as the organization that was used to onboard the appliance.

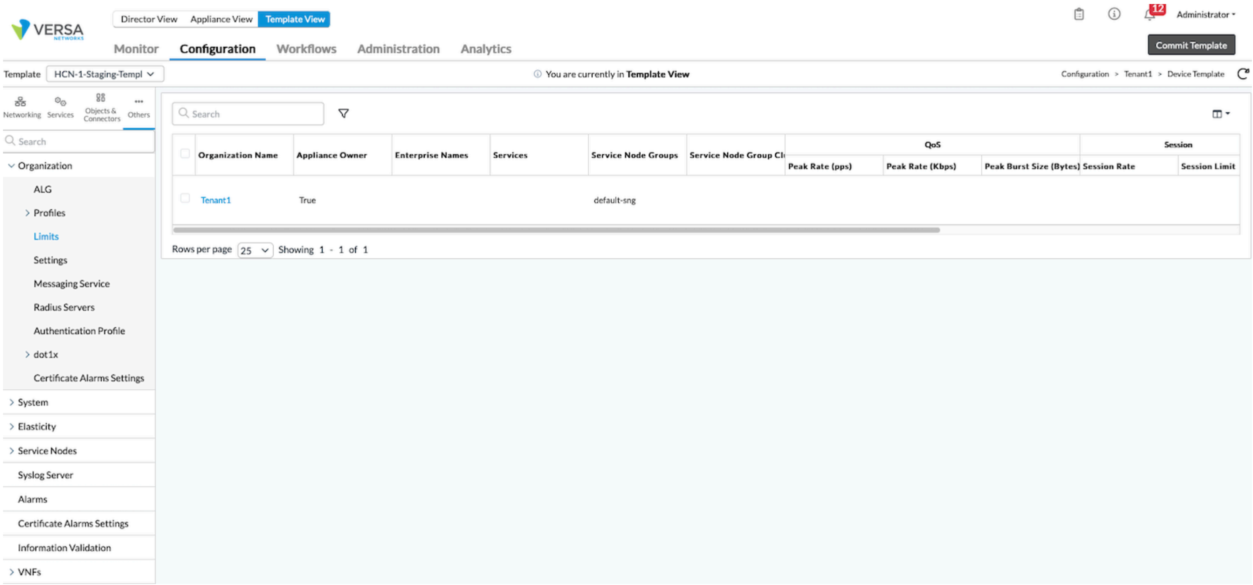
When you upgrade from an earlier software release, the VOS device automatically copies the existing configuration to the appliance owner's organization.

Note that you cannot configure traffic shapers on TVI tunnel interfaces or on networks associated with any TVI interfaces.

Configure a Traffic Shaper for a Provider Organization

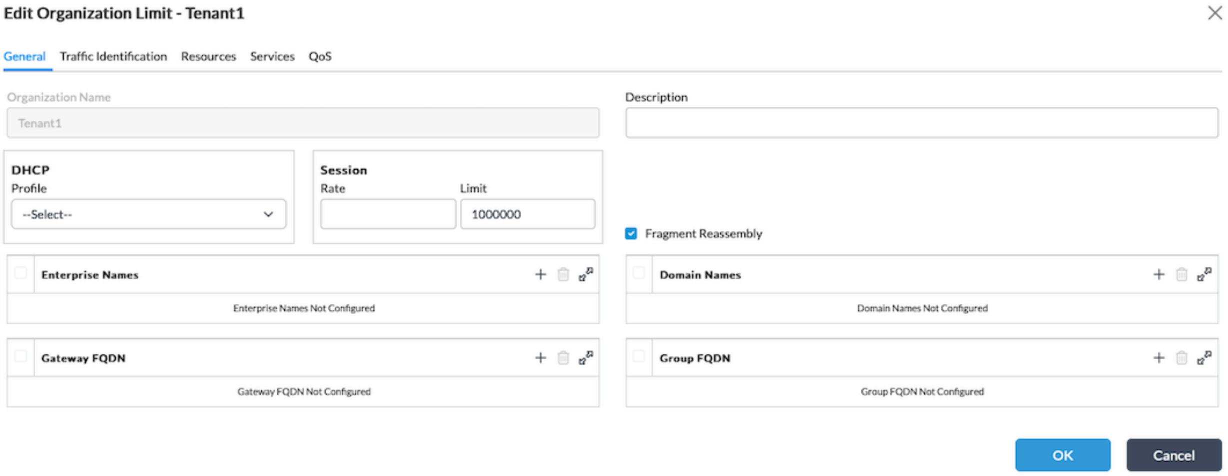
To configure a traffic shaper for an appliance owner organization:

1. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliances in the left menu bar.
    c. Select an appliance in the main pane. The view changes to Appliance View.
2. Select the Configuration tab in the top menu bar.
3. Select Others > Organization > Limits in the left menu bar.



Organization Name	Appliance Owner	Enterprise Names	Services	Service Node Groups	Service Node Group Cl	QoS			Session	
						Peak Rate (pps)	Peak Rate (Kbps)	Peak Burst Size (Bytes)	Session Rate	Session Limit
Tenant1	True			default-sng						

4. Select an organization in the main panel. In the Edit Organization Limit popup window, select the General tab to configure QoS information for all the organization's interfaces. Enter information for the following fields in the QoS group of fields.

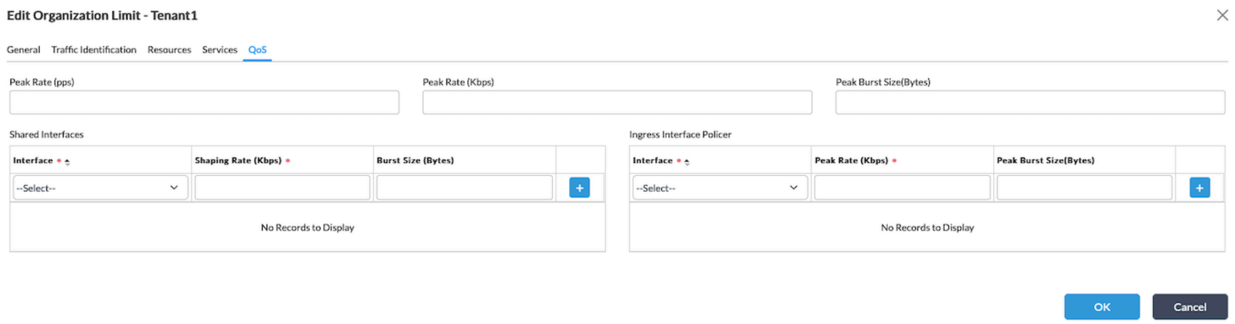

Edit Organization Limit - Tenant1
General
Traffic Identification
Resources
Services
QoS
Enterprise Names
Enterprise Names Not Configured
Domain Names
Domain Names Not Configured
Gateway FQDN
Gateway FQDN Not Configured
Group FQDN
Group FQDN Not Configured
OK
Cancel

Organization Name	Tenant1
Description	
DHCP Profile	--Select--
Session Rate	
Session Limit	1000000
☑ Fragment Reassembly	

Field	Description
Peak Rate (packets)	Enter the peak shaping rate, in packets per second (pps). *Range*: 1 through 4294967295 pps *Default*: None

Field	Description
Peak Rate (bandwidth)	Enter the peak shaping rate, in Kbps. *Range*: 64 through 4294967295 Kbps *Default*: None
Peak Burst Size	Enter the peak burst size, in bytes. *Range*: 128 through 4294967295 bytes *Default*: None

5. Select the QoS tab to configure QoS information for individual interfaces. Enter information for the following fields.



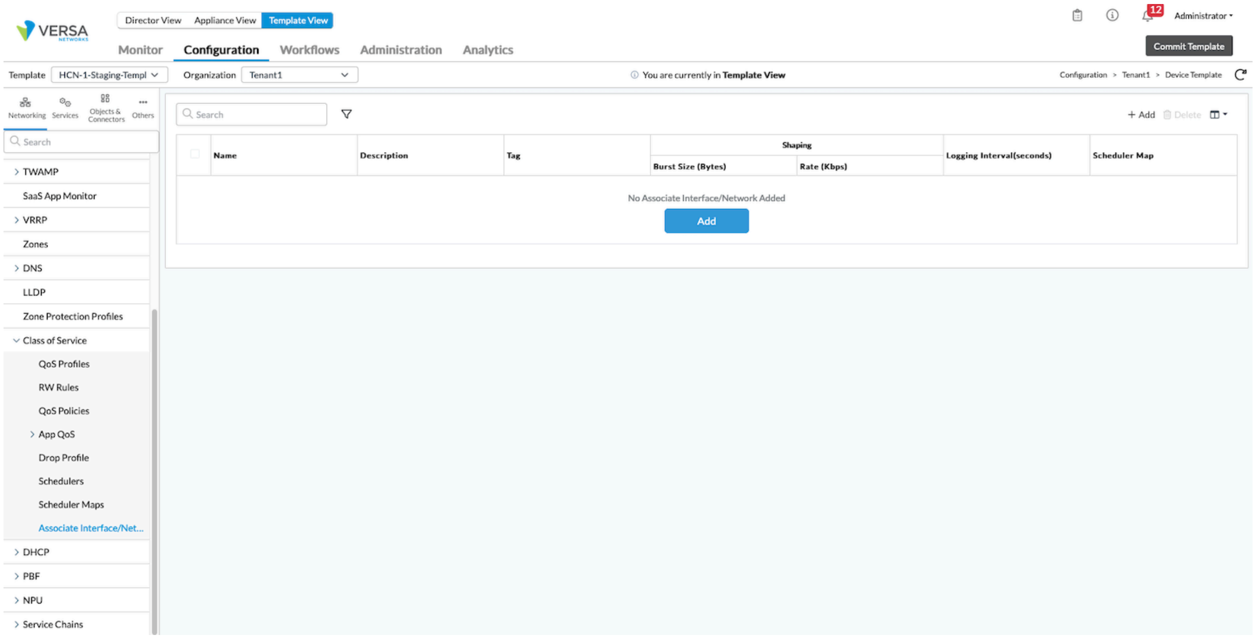
Field	Description
Interface	Select the interface.
Shaping Rate	Enter the shaping rate, in packets per second (pps). *Range*: 1 through 4294967295 pps *Default*: None
Burst Size	Enter the burst size, in bytes. *Range*: 128 through 4294967295 bytes *Default*: None

6. Click OK.

Rate-Limit a Tenant's Bandwidth

After the appliance owner has created a traffic shaper for its provider organization, a tenant can rate-limit its allocated bandwidth:

1. In Director view:
    a. Select the Configuration tab in the top menu bar.
    b. Select an organization in the left menu bar.
    c. Select Templates > Device Templates in the horizontal menu bar.
    d. Select a post-staging template in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Class of Service > Associate Interface/Network in the left menu bar.



Template HCN-1-Staging-Templ

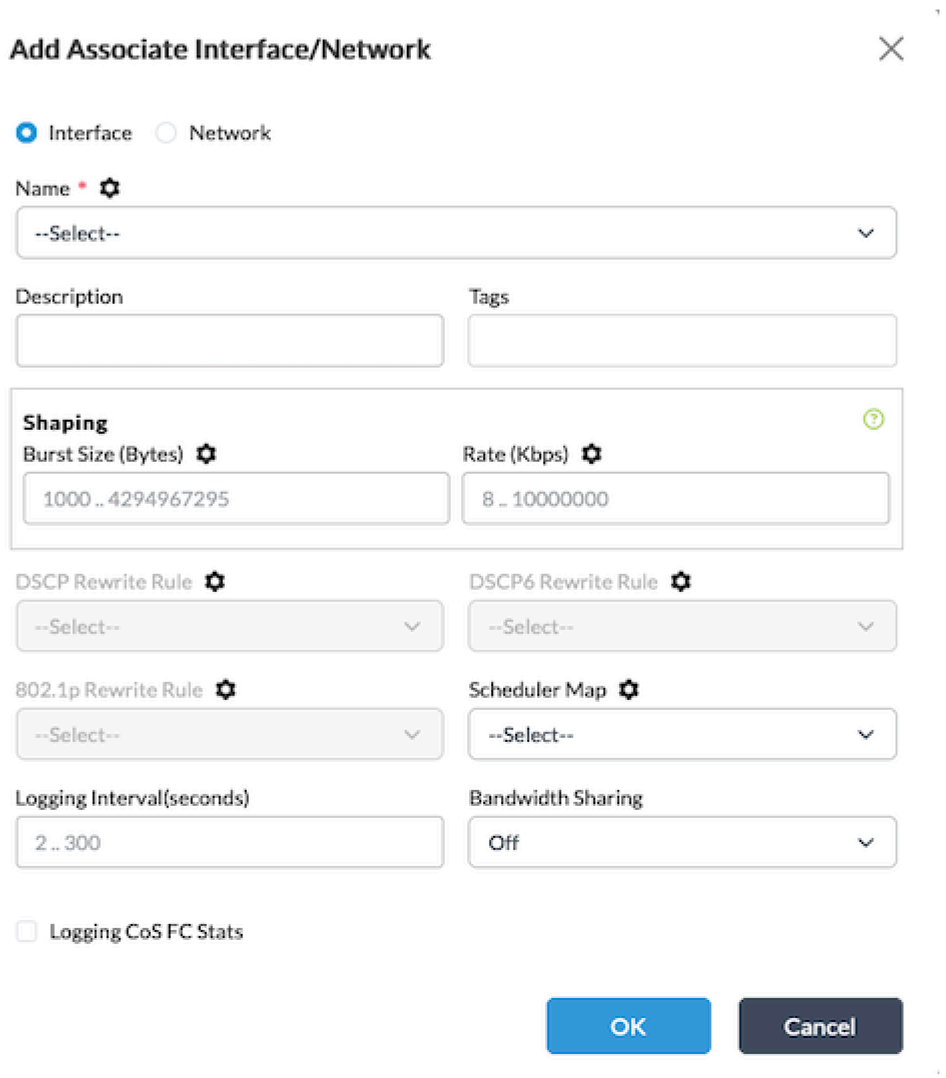
Organization Tenant1

You are currently in **Template View**

□	Name	Description	Tag	Shaping		Logging Interval(seconds)	Scheduler Map
				Burst Size (Bytes)	Rate (Kbps)		

No Associate Interface/Network Added

4. Click the ⊞ Add icon. In the Associate Interface/Network popup window, enter information for the following fields.



Add Associate Interface/Network

● Interface ○ Network

Name *

--Select--

Description

Tags

Shaping

Burst Size (Bytes): 1000 .. 4294967295

Rate (Kbps): 8 .. 10000000

DSCP Rewrite Rule: --Select--

DSCP6 Rewrite Rule: --Select--

802.1p Rewrite Rule: --Select--

Scheduler Map: --Select--

Logging Interval(seconds): 2 .. 300

Bandwidth Sharing: Off

□ Logging CoS FC Stats

Field	Description
Interface	Click to configure an interface association.
Network	Click to configure a network association.
Name (Required)	Select an interface (when you click Interface) or network name (when you click Network).
Description	Enter a text description for the interface or network.
Tags	Enter tags to identify with the interface or network.
Shaping (Group of Fields)	Available when you select Network.
◦ Burst Size	Enter the burst size, in bytes.

Field	Description
	Range: 1000 through 4294967295 bytes *Default:* Depends on the link speed of the underlying interface. For example, if you connect two 1-GB interfaces, the burst size is 125000 bytes. If you connect a 1-GB interface to a 100-MB interface, the link speed is autonegotiated to 100 MB and the burst size is automatically set to 12500 bytes, and if you connect a 1-GB to a 10-MB interface, the burst size is automatically set to 1250 bytes. For most cases, it is recommended that you do not change the interface's burst size. However, you might consider changing it when the interface has autonegotiated a smaller burst size, but you know that the link can handle a larger higher burst. For example, if a 1-GB interface has autonegotiated to 10 MB, and if you know that the hardware can handle a burst of 125000 bytes and that the other side of the line can handle that much incoming burst, you could configure a larger burst.
◦ Rate	Enter the shaping rate, in Kbps. *Range*: 8 through 10000000 Kbps *Default:* None
DSCP Rewrite Rule	Select a DSCP rewrite rule.
DSCP6 Rewrite Rule	Select a DSCP6 rewrite rule.
802.1p Rewrite Rule	Select an 802.1p rewrite rule.
Scheduler Map	Select a scheduler map.
Logging Interval	a value for how often to log egress traffic, in seconds.
Bandwidth Sharing	(For Releases 20.2 and later.) Select On to allow traffic distribution across units (pipes) in a single port. For more information, see Associate Egress Traffic with Interfaces and Networks, above.

5. Click OK.

The tenant organization can now assign schedulers to its interface. For more information, see Configure Schedulers.

Verify the Configuration

To verify the configuration on the interface and display all the related counters using the following **show** commands:

```
(config)% run show class-of-services interfaces extensive vni-0/1
  ...
  Pipe ID      : 1
     Users        : [ vni-0/1-custorg ]
     Type         : Access circuit
     Configuration :
       Burst Size : 50000 bytes
       Rate       : 2000 kbps
         TC0: Network-Control      : 2000-2000 kbps
         TC1: Expedited-Forwarding : 2000-2000 kbps
         TC2: Assured-Forwarding   : 2000-2000 kbps
         TC3: Best-Effort          : 1000-2000 kbps
     Traffic Stats:
       Queues Cfg       Inferred      TX        TX        TX       Bytes         Avg       Avg Drop
              Wt        BW kbps       Pkts      Dropped   Bytes     Dropped Qlen  Rate bps    Rate bps
    tc0 network-control:
      q0: fc_nc   1       500-2000       0         0        0         0    0        0          0
      q1: fc1     1       500-2000       0         0        0         0    0        0          0
      q2: fc2     1       500-2000       0         0        0         0    0        0          0
      q3: fc3     1       500-2000       0         0        0         0    0        0          0
    tc1   expedited-fwd:
      q0: fc_ef   1       500-2000       0         0        0         0    0        0          0
      q1: fc5     1       500-2000       0         0        0         0    0        0          0
      q2: fc6     1       500-2000       0         0        0         0    0        0          0
      q3: fc7     1       500-2000       0         0        0         0    0        0          0
    tc2     assured-fwd:
      q0: fc_af   1       500-2000       0         0        0         0    0        0          0
      q1: fc9     1       500-2000       0         0        0         0    0        0          0
      q2: fc10    1       500-2000       0         0        0         0    0        0          0
      q3: fc11    1       500-2000       0         0        0         0    0        0          0
    tc3     best-effort:
      q0: fc_be   5       500-2000       0         0        0         0    0        0          0
      q1: fc13    3       300-2000       0         0        0         0    0        0          0
      q2: fc14    1       100-2000       0         0        0         0    0        0          0
      q3: fc15    1       100-2000       0         0        0         0    0        0          0
```

Adjust the QoS Frame Overhead

When a client sends a packet from one SD-WAN branch device to another SD-WAN branch device, the VOS software adds to the packet QoS header information about the link between the two branches. The amount of header information added to each packet depends on the configuration. Adding the header information increases the overhead incurred and increases the transmission rate the branches require to transmit QoS frames. (Note that if a policy specifies that a VOS device should send traffic from an SD-WAN branch directly to the internet without going through another SD-WAN branch, the VOS device does not add QoS header information to the packets.)

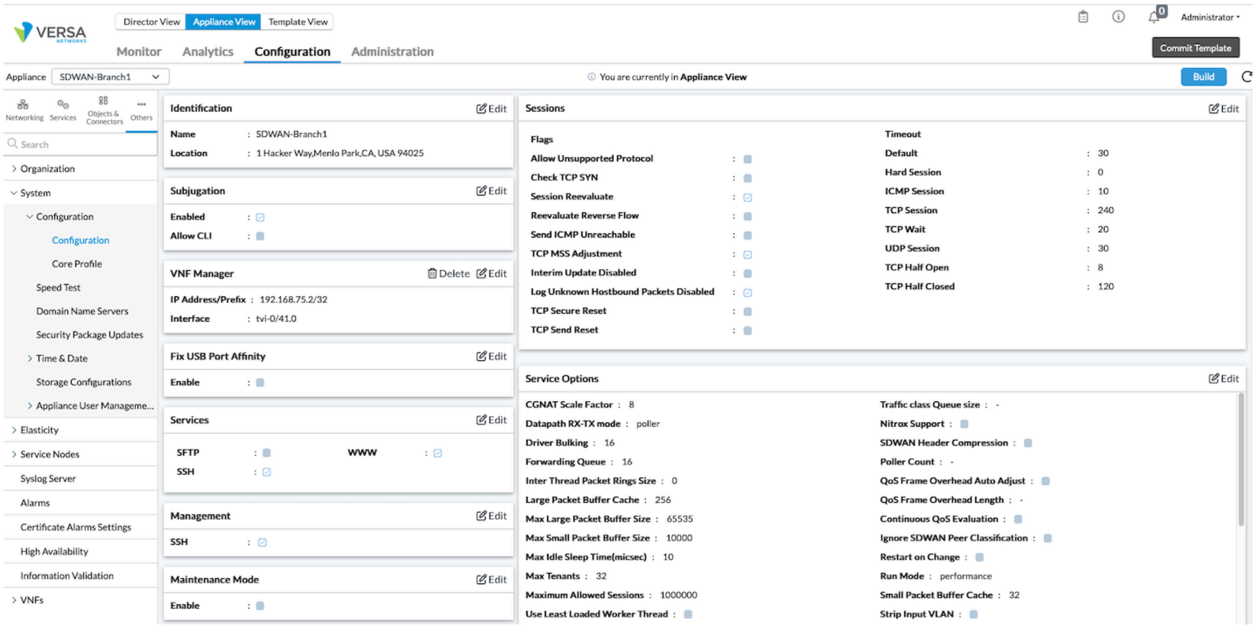
You can configure an SD-WAN branch device to automatically adjust the data transmission rate of QoS frames based on the amount of information that is added to the packet headers. If you configure a shaping rate and enable automatic adjustment of the QoS frame overhead, the VOS software discounts the amount of additional header information and sends the full amount of data specified by the shaping rate. You can also enable manual adjustment of the QoS frame overhead.

Service providers, who typically absorb the cost of the increased transmission rate, might want to enable automatic adjustment of the QoS frame overhead to help reduce the cost of providing SD-WAN services. Enterprises, who typically buy bandwidth from a service provider, might want to enable automatic adjustment of the QoS frame overhead to keep the traffic rate between their branches at or below the amount of bandwidth they purchased from the service provider.

By default, automatic adjustment of the QoS frame overhead is disabled, so each WAN interface transmits the full amount of data for which it was configured.

To adjust the QoS frame overhead:

1. In Director view:
    a. Select the Configuration tab in the top menu bar.
    b. Select Devices > Devices in the horizontal menu bar.
    c. Select an organization in the left menu bar.
    d. Click a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Others > System > Configuration > Configuration in the left menu bar.



Appliance SDWAN-Branch1

You are currently in **Appliance View**

Identification

Name : SDWAN-Branch1
Location : 1 Hacker Way,Menlo Park,CA, USA 94025

Subjugation

Enabled : ☑
Allow CLI : □

VNF Manager

IP Address/Prefix : 192.168.75.2/32
Interface : tvi-0/41.0

Fix USB Port Affinity

Enable : □

Services

SFTP : □
SSH : ☑
WWW : ☑

Management

SSH : ☑

Maintenance Mode

Enable : □

Sessions

Flags
Allow Unsupported Protocol : □
Check TCP SYN : □
Session Reevaluate : ☑
Reevaluate Reverse Flow : □
Send ICMP Unreachable : □
TCP MSS Adjustment : ☑
Interim Update Disabled : □
Log Unknown Hostbound Packets Disabled : ☑
TCP Secure Reset : □
TCP Send Reset : □

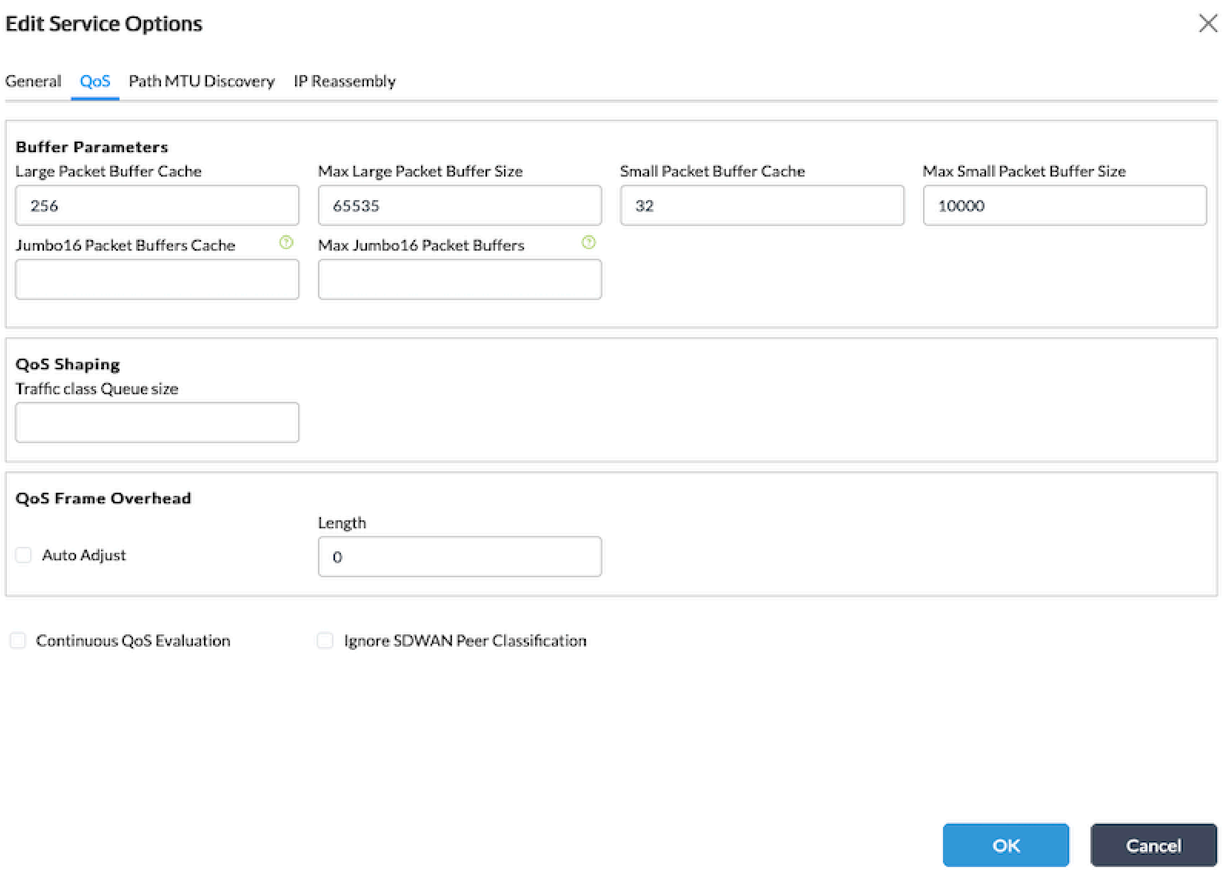
Timeout
Default : 30
Hard Session : 0
ICMP Session : 10
TCP Session : 240
TCP Wait : 20
UDP Session : 30
TCP Half Open : 8
TCP Half Closed : 120

Service Options

CGNAT Scale Factor : 8
Datapath RX-TX mode : poller
Driver Bulking : 16
Forwarding Queue : 16
Inter Thread Packet Rings Size : 0
Large Packet Buffer Cache : 256
Max Large Packet Buffer Size : 65535
Max Small Packet Buffer Size : 10000
Max Idle Sleep Time(micsec) : 10
Max Tenants : 32
Maximum Allowed Sessions : 1000000
Use Least Loaded Worker Thread : □

Traffic class Queue size : -
Nitrox Support : □
SDWAN Header Compression : □
Poller Count : -
QoS Frame Overhead Auto Adjust : □
QoS Frame Overhead Length : -
Continuous QoS Evaluation : □
Ignore SDWAN Peer Classification : □
Restart on Change : □
Run Mode : performance
Small Packet Buffer Cache : 32
Strip Input VLAN : □

4. In the Service Options pane, click the ✎ Edit icon. In the Edit Service Options popup window, select the QoS tab and enter information for the following fields.



Edit Service Options

General | QoS | Path MTU Discovery | IP Reassembly

Buffer Parameters

Large Packet Buffer Cache: 256

Max Large Packet Buffer Size: 65535

Small Packet Buffer Cache: 32

Max Small Packet Buffer Size: 10000

Jumbo16 Packet Buffers Cache:

Max Jumbo16 Packet Buffers:

QoS Shaping

Traffic class Queue size:

QoS Frame Overhead

□ Auto Adjust

Length: 0

□ Continuous QoS Evaluation

□ Ignore SDWAN Peer Classification

Field	Description
QoS Frame Overhead (Group of Fields)	
◦ Auto Adjust	Click to have the VOS software automatically adjust the length of the QoS frame overhead for each packet.
◦ Length	Enter a value to manually set the length of the QoS frame overhead for each packet. *Range:* –128 through 128 bytes

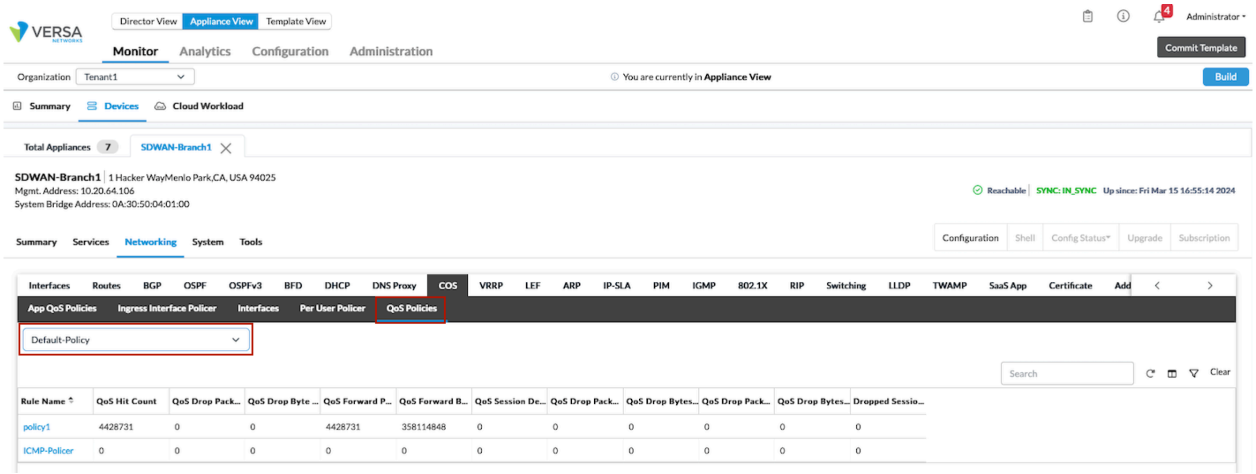
5. Click OK.

Monitor QoS Policies

You can monitor QoS policies to view the traffic flow details when a policy is used.

To monitor QoS policies:

1. In Director view, select the Administration tab in the top menu bar.
2. Select Appliances in the left menu bar.
3. Select a device name in the main panel. The view changes to Appliance view.
4. Select the Monitor tab in the top menu bar.
5. Select the organization or tenant in the left menu bar.
6. Select Networking > CoS, and click the QoS Policies tab.
7. Select a policy from the drop-down list. Statistics about the QoS policy display. The following table describes each of the fields in the QoS policy statistics output



SDWAN-Branch1 | 1 Hacker WayMenlo Park,CA, USA 94025
Mgmt. Address: 10.20.64.106
System Bridge Address: 0A:30:50:04:01:00

Reachable | SYNC: IN_SYNC Up since: Fri Mar 15 16:55:14 2024

Default-Policy

Rule Name	QoS Hit Count	QoS Drop Pack...	QoS Drop Byte ...	QoS Forward P...	QoS Forward B...	QoS Session De...	QoS Drop Pack...	QoS Drop Bytes...	QoS Drop Pack...	QoS Drop Bytes...	Dropped Sessio...
policy1	4428731	0	0	4428731	358114848	0	0	0	0	0	0
ICMP-Policer	0	0	0	0	0	0	0	0	0	0	0

Field	Description
Rule Name	Name of the QoS policy.
QoS Hit Count	Total number of traffic flows that matched the QoS policy and were evaluated by the policy.
QoS Drop Packet Count	Packets that were dropped because of the policy.
QoS Drop Byte Count	Bytes that were dropped because of the policy.
QoS Forward Packet Count	Packets that were forwarded because of the policy.
QoS Forward Byte Count	Bytes that were forwarded because of the policy.
QoS Session Deny Count	Total number of sessions that were denied because of the policy.
QoS Drop Packets Count by PPS	Packets that were dropped, in PPS, because of the policy.
QoS Drop Bytes Count by PPS	Bytes that were dropped, in PPS, because of the

Field	Description
	policy.
QoS Drop Packets Count by Kbps	Packets that were dropped, in Kbps, because of the policy.
QoS Drop Bytes Count by Kbps	Bytes that were dropped, in Kbps, because of the policy.
Dropped Sessions By Per-User Policer	Total number of sessions dropped because of a per-user policer in the policy.

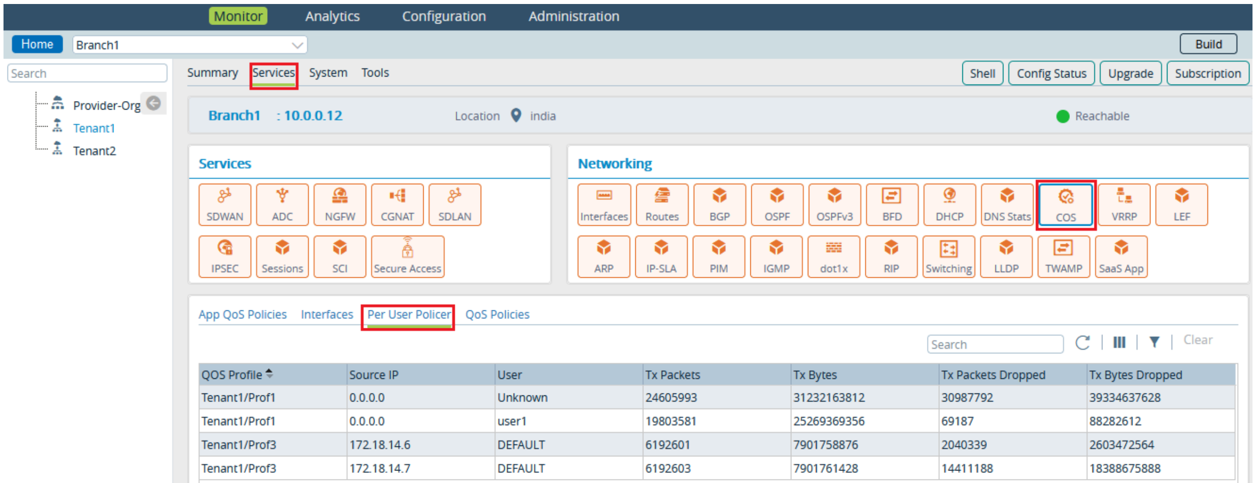
Monitor Per-User Policers

For Releases 21.2.2 and later.

You can monitor per-user policers to view the number of users and information about users who were restricted because of a user policer in a QoS profile.

To monitor per-user policers:

1. In Director view, select the Administration tab in the top menu bar.
2. Select Appliances in the left menu bar.
3. Select a device name in the main panel. The view changes to Appliance view.
4. Select the Monitor tab in the top menu bar.
5. Select the organization or tenant in the left menu bar.
6. Select Networking > COS CoS and click the Per-User Policer tab. The per-user policer statistics display. These statistics include the QoS profile associated with the user policer, source IP address of the user, user ID, total number of transaction packets and bytes for each user, and number of dropped packets and bytes for each user. If the per-user policer is based on a source IP address, the User column displays Default, and if the per-user policer is based on a user ID, the Source IP column displays 0.0.0.0. The QoS Policies tab displays the number of session that have been dropped because of user or session limit violations. For more information, see Monitor QoS Policies, above.



QOS Profile	Source IP	User	Tx Packets	Tx Bytes	Tx Packets Dropped	Tx Bytes Dropped
Tenant1/Prof1	0.0.0.0	Unknown	24605993	31232163812	30987792	39334637628
Tenant1/Prof1	0.0.0.0	user1	19803581	25269369356	69187	88282612
Tenant1/Prof3	172.18.14.6	DEFAULT	6192601	7901758876	2040339	2603472564
Tenant1/Prof3	172.18.14.7	DEFAULT	6192603	7901761428	14411188	18388675888

Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Release 20.2.1 adds the ability to configure traffic shapers for provider organizations and tenants.
- Release 21.2.1 adds support for configuring traffic shaping for tunnel interfaces and configuring rule order for QoS and application QoS policy rules.
- Release 21.2.2 adds support for configuring and monitoring per-user policers for QoS profiles.
- Releases 22.1.1 adds support for hardware-based shapers.

Additional Information

Apply Log Export Functionality
Configure Adaptive Shaping
Configure Address Objects
Configure Control and Management Plane Protection
Configure Core Profiles
Configure Log Export Functionality
Configure Organization Limits
Configure Policy-Based Forwarding
Monitor Device Services
Monitor VOS Devices in Real Time