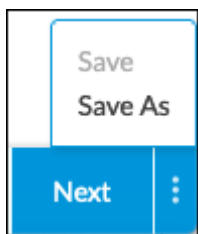

Configure QoS Policies and Rules

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

To add QoS policies and rules, you first create an application policy to classify incoming traffic based on match criteria, such as application, source IP address, destination IP address, and incoming zone. Then, you specify the action to take when traffic matches the configured criteria.

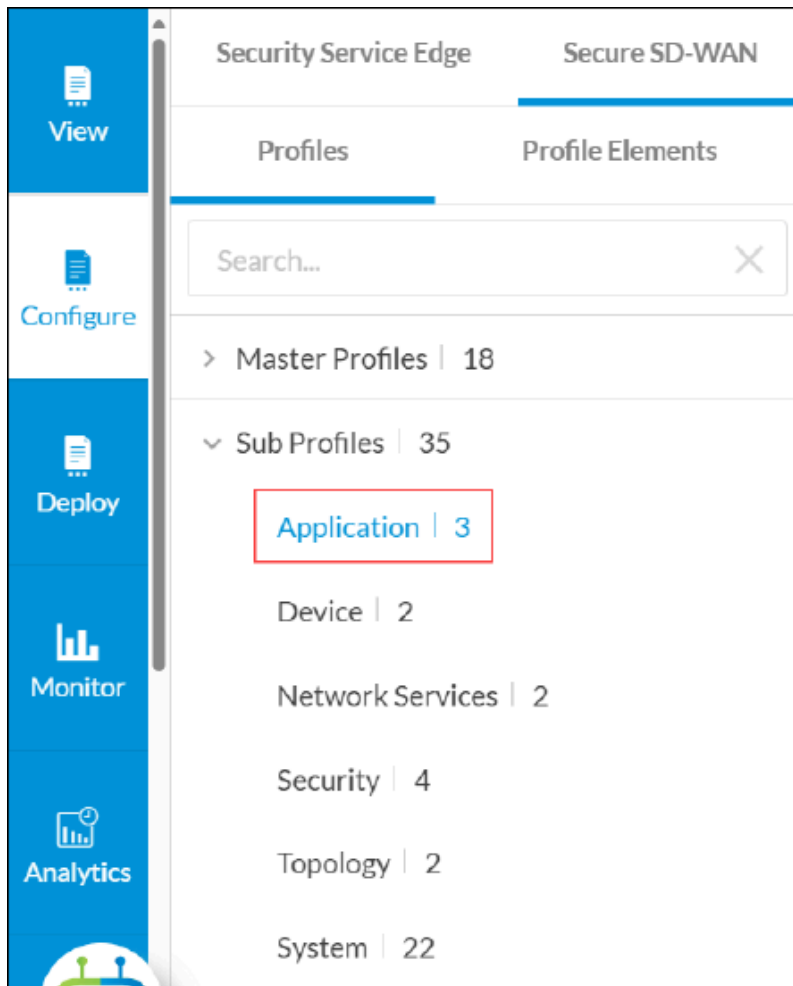
QoS policies and rules belong to the Application subprofile type. To provide flexibility, you can attach one or more QoS policies to an Application subprofile, which allows you to create a group of QoS tools with different rules to reuse in different QoS subprofiles. You can add a QoS policy to an existing Application subprofile, or you can add it when you create a new subprofile. For more information, see [Create a New Subprofile](#). You can add a QoS policy as a profile element that can then be used in one or more Application subprofiles. For more information, see [Add New Application Elements](#).

You can build reusable application policies by navigating to the Policies > Application > QoS folder. You can also build policies and rules inline. These inline rules apply only to the policies currently being configured. You cannot reuse them in other subprofiles until you add them to the reusable Subprofiles folder by clicking the ellipsis to the right of Next and then selecting Save As.

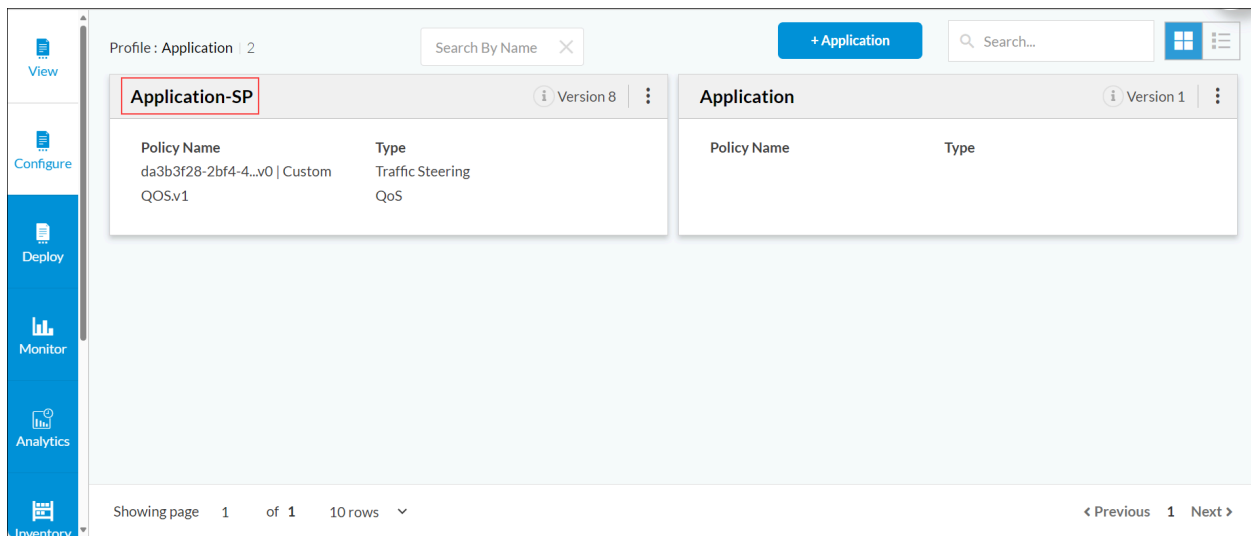




Add a QoS Policy to an Existing Application Subprofile

1. Go to Configure > Secure SD-WAN > Profiles > Sub Profiles > Application.



The screen displays the existing Application profiles.



2. To add a QoS policy, click an application subprofile (Application-SP in the screenshot above), or click the  Ellipsis icon, and then click the  Edit icon in the popup menu. The Edit Application Subprofile screen displays.

Edit Application Sub Profile

Configure > Profiles > Sub Profiles > Application : Application-SP

General

Policy

Permissions

Name

Application-SP

Version 8

Description

Type

Application

Variables | 0

No variables present

Policies | 2

Name	Version	Type	# Rules
da3b3f28-2bf4-4a07-b5f5-93a...	0 Custom	Traffic Ste...	0
QOS	1	QoS	0

Tags

Press Enter to add

Close

Next

3. Select the Policy tab, and then click + Policy.

Edit Application Sub Profile

Configure > Profiles > Sub Profiles > Application : Application-SP

General

Policy

Permissions

Traffic Steering Policy | 1

1 :: da3b3f28-2bf4-4a07...

0 Rules

Variables | 0

QoS Policy | 1

1 :: QOS.v1

0 Rules

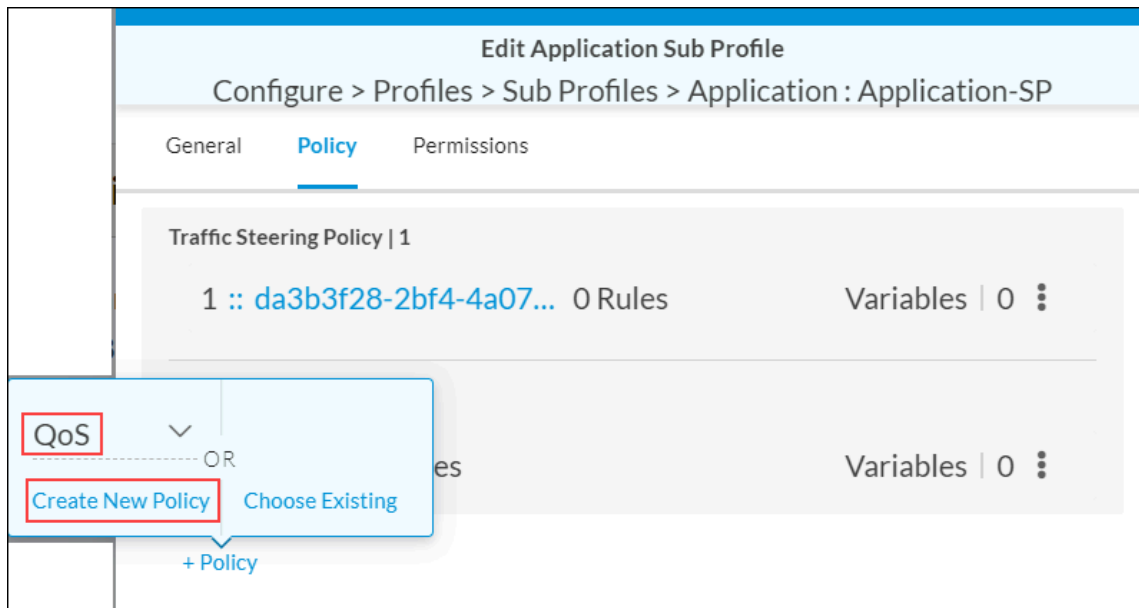
Variables | 0

+ Policy

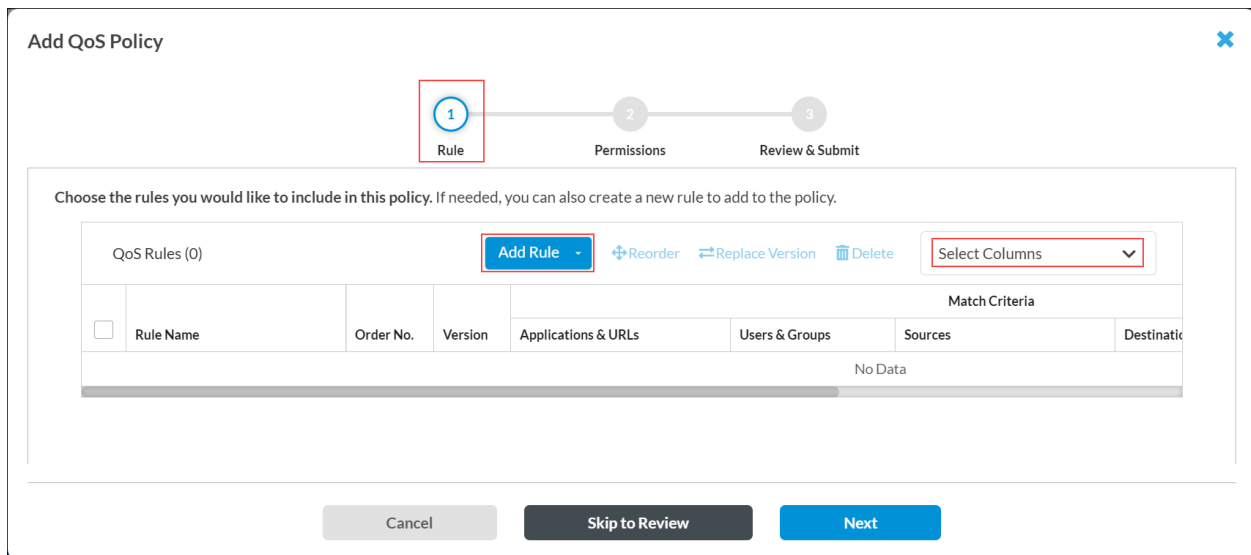
Close

Next

- In the popup menu, select QoS. To create a new policy, click Create New Policy. To use an existing policy, click Choose Existing, and then select a policy from the list.



The Add QoS Policy screen displays, and Step 1, Rules is selected.



5. To change the columns displayed on the screen, click the Select Columns down arrow, and then select or deselect columns to choose the ones you want to display. To restore the default column settings, click Reset.

Select Columns

☒ Order No.
 ☒ Version
 ☒ Applications & URLs
 ☒ Users & Groups
 ☒ Sources
 ☒ Destinations
 ☒ Services
 ☐ Schedule
 ☐ DSCP
 ☒ Classification
 ☐ Variables
 ☒ Status

Reset

6. In the Add QoS Policy screen, click Add Rule. The following screen displays.

Add Rule

Reorder

Add Existing Rule

Create Rule only for this policy

7. To create a new rule for the application policy, continue to Step 8. To add an existing rule:
- a. Click Add Existing Rule. The Add Existing QoS Rules screen displays the existing QoS rules.

Add Existing QoS Rules

Select one or more rules to add to the QoS Policy

Available Rules: 25
☐ Select All

<input type="checkbox"/>	noClassificationTest	Version 1	⚙ Disabled
<input type="checkbox"/>	kasunTestDisableAutoDelete	Version 1	✅ Enabled
<input type="checkbox"/>	kasunTest45	Version 1	✅ Enabled
<input type="checkbox"/>	kasunTest4	Version 1	✅ Enabled
<input type="checkbox"/>	kasunTest3	Version 1	✅ Enabled
<input type="checkbox"/>	kasunTest	Version 1	✅ Enabled

QoS Rules Selected: 0

No rules selected

- b. Select one or more rules. The selected rules move to the QoS Rules Selected pane.

Add Existing QoS Rules

Select one or more rules to add to the QoS Policy

Available Rules: 25
☐ Select All

<input checked="" type="checkbox"/>	noClassificationTest	Version 1	⚙ Disabled
<input type="checkbox"/>	kasunTestDisableAutoDelete	Version 1	✅ Enabled
<input type="checkbox"/>	kasunTest45	Version 1	✅ Enabled
<input type="checkbox"/>	kasunTest4	Version 1	✅ Enabled
<input type="checkbox"/>	kasunTest3	Version 1	✅ Enabled
<input type="checkbox"/>	kasunTest	Version 1	✅ Enabled

QoS Rules Selected: 1

☒ noClassificationTest 1

Applications or URLs Network Layer 3-4 Classification

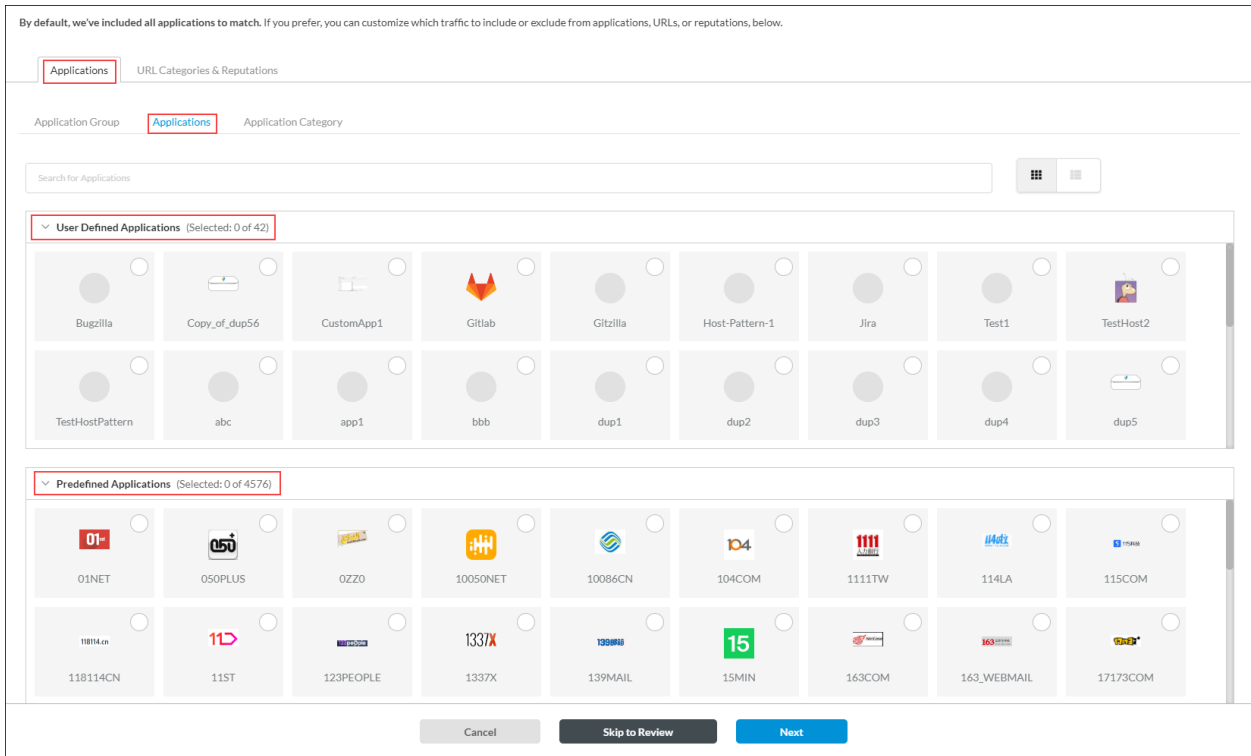
Variable Types

✅ All Applications

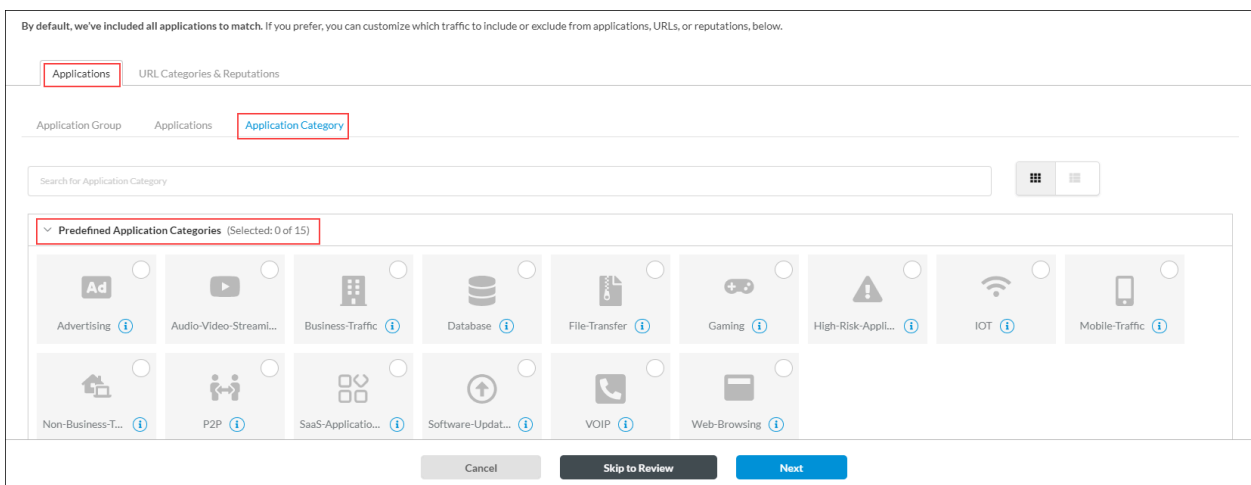
- c. To view the configuration elements for a selected rule, click the down arrow next to the rule, and then select a category to display the configuration elements for that category:
- Applications or URLs
 - Classification
 - Network Layer 3-4
 - Variable Types
- d. Click Add Rules to add the QoS rules to the application policy.
8. To create a new rule for the application policy, select Create Rule only for this Policy. The Add QoS Rule screen displays, and the Step 1, Applications & URLs and the Applications > Application Group tab is selected.

9. On the Applications tab, you can select specific applications, application groups, or application categories to include in the match criteria. All applications are included by default. You can use this screen to customize which applications to include in the match criteria.
 - To select application groups for the rule to match, on the Applications > Application Group tab, click the group category (User Defined Application Groups or Predefined Application Groups), and then select the application groups for the rule to match. You can also use the Search bar to find specific application groups.

- To select applications for the rule to match, select the Applications > Applications tab, click the group category (User-Defined Applications or Predefined Applications), and then select the applications. You can also use the Search bar to find specific applications.



- To select predefined application categories for the rule to match, select the Applications > Application Category tab, and then select one or more predefined application categories. You can also use the Search bar to find specific application categories.



10. Select the URL Categories and Reputations tab. The following screen displays.

By default, we've included all applications to match. If you prefer, you can customize which traffic to include or exclude from applications, URLs, or reputations, below.

Applications **URL Categories & Reputations**

URL Categories

Search or select from list

Reputations

Add Reputation

Cancel Skip to Review Next

11. In the URL Categories field, click the down arrow, and then select one or more URL categories for the rule to match.
12. In the Reputations field, click the down arrow, and then select one or more reputations to include in the rule:
 - High risk
 - Low risk
 - Moderate risk
 - Suspicious
 - Trustworthy
 - Undefined
13. Click Next or select Step 2, Users & Groups.

Add QoS Rule

Applications & URLs **Users & Groups** Match Criteria Service & DSCP Classification Permissions Review & Submit

By default we have chosen all users and groups to apply your security enforcements If you prefer, you can select the specific users or groups for the security posture.

Users & Groups

Enable QoS Rule for the following matched users or user groups

User Type

☒ All Users ☐ Known Users ☐ Unknown Users ☐ Selected Users

Cancel Back Skip to Review Next

14. Select the user type to match with the QoS policy:

- All Users
- Known Users
- Selected Users
- Unknown Users

15. To add an existing user group, click Selected Users and click the name of one or more user groups (Group in the screenshot below).

16. To add a new user group, click + Add New User Group. The following screen displays.

- Enter a user group name and a distinguished name (DN).
- Click Add.

17. Select the Users tab. To add existing users, click Selected Users, and then click the name of one or more users.

Users & Groups

Enable QoS Rule for the following matched users or user groups

User Type

☐ All Users
 ☐ Known Users
 ☐ Unknown Users
 ☒ Selected Users

ACME-Group

User Groups **Users**

Search for Users

Users (0) **+ Add New User**

User Name	Work Email
<input type="checkbox"/> Ramanjana Reddy Ram@versa-qa-lab.local	Ram@versa-qa-lab.local
<input type="checkbox"/> Venki One.venki1@versa-qa-lab.local	venki1@versa-qa-lab.local
<input type="checkbox"/> Venki Two.venki2@versa-qa-lab.local	venki2@versa-qa-lab.local

18. To add a new user, click + Add New User. The following screen displays.

×

Add User

User Name*

Work Email *

- a. Enter a user name and a work email address.
 - b. Click Add.
19. Click Next or select Step 3, Source & Destination Traffic. The following screen displays. By default, all source and destination traffic is included in the match criteria. You can use this screen to customize the source and destination traffic to include in the match criteria.

Add QoS Rule

Applications & URLs Users & Groups **Source & Destination Traffic** Service & DSCP Classification Permissions Review & Submit

By default, all source & destination traffic have been included. If you prefer, you can customize which source & destination traffic to include or exclude below.

Source Address Destination Address Source Zone & Sites Destination Zone & Sites

☐ Negate Source Address [+ Add Variable](#)

Search or select from list

Name	Addresses
<input type="checkbox"/> Copy_hbjh	192.168.0.56/255.255.0.255, 192.168.0.1/255.255.0.255, 192.168.0.2/255.255.0.255, 192.168.3.0/255.255.0.255, 0012::/23, 11::/23, 14::/23, 18::/23, 5.5.5.5-5.5.10.5, 5.5.15.5-5.5.15.15, 5.5.15.115-5.5.15.215
<input type="checkbox"/> Copy_of_Copy_of_Copy_of_Jan2192	192.168.0.56/255.255.0.255, 192.168.0.1/255.255.0.255, 192.168.0.2/255.255.0.255, 192.168.3.0/255.255.0.255, 0012::/23, 11::/23, 14::/23, 18::/23, 5.5.5.5-5.5.10.5, 5.5.15.5-5.5.15.15, 5.5.15.115-5.5.15.215
<input type="checkbox"/> Copy_of_Copy_of_Jan2192	192.168.0.56/255.255.0.255, 192.168.0.1/255.255.0.255, 192.168.0.2/255.255.0.255, 192.168.3.0/255.255.0.255, 0012::/23, 11::/23, 14::/23, 18::/23, 5.5.5.5-5.5.10.5, 5.5.15.5-5.5.15.15, 5.5.15.115-5.5.15.215
<input type="checkbox"/> Copy_of_Copy_of_Jan	1.2.3.4-1.2.3.10, 10.2.3.0/24, 192.168.0.56/255.255.0.255, 0012::/23
<input type="checkbox"/> Copy_of_VeryLONGNAMETOTRUNCATEDATAHERE	
<input type="checkbox"/> Copy_of_Jan2192	192.168.0.56/255.255.0.255, 192.168.0.1/255.255.0.255, 192.168.0.2/255.255.0.255, 192.168.3.0/255.255.0.255, 0012::/23, 11::/23, 14::/23, 18::/23, 5.5.5.5-5.5.10.5, 5.5.15.5-5.5.15.15, 5.5.15.115-5.5.15.215
<input type="checkbox"/> Copy_of_Jan	1.2.3.4-1.2.3.10, 10.2.3.0/24, 192.168.0.56/255.255.0.255, 0012::/23
<input type="checkbox"/> VeryLONGNAMETOTRUNCATEDATAHERE	
<input type="checkbox"/> Jan2192	192.168.0.56/255.255.0.255, 192.168.0.1/255.255.0.255, 192.168.0.2/255.255.0.255, 192.168.3.0/255.255.0.255, 0012::/23, 11::/23, 14::/23, 18::/23, 5.5.5.5-5.5.10.5, 5.5.15.5-5.5.15.15, 5.5.15.115-5.5.15.215
<input type="checkbox"/> Jan	1.2.3.4-1.2.3.10, 10.2.3.0/24, 192.168.0.56/255.255.0.255, 0012::/23


Showing 1-10 of results 10 Rows per Page Go to page 1 < Previous 1 2 Next >

IP Address or IP Range [+ Add Variable](#) IP Subnet [+ Add Variable](#) IP WildCard [+ Add Variable](#)


Enter IP address or range Enter a list of IPv4/IPv6 Subnet values Enter a list of wildcard values


Cancel Back Skip to Review Next


20. To customize the source traffic, on the Source Address tab, use one of the following methods:
 - To specify source addresses to include in the match criteria, continue with Step 21.
 - To specify source addresses to exclude from the match criteria, select Negate Source Address to match all source addresses except the source addresses that you specify, and then continue with Step 21.
21. To specify a source address to include or exclude in the match criteria, you can select a source address from the list or use the search box to find a source address. To create a variable for the source address, click + Add

Variable to the right of the source address list. Enter a name for the variable, click the  Plus icon, and then click Add. You can add multiple variables.

You can also enter values for the fields IP Address or IP Range, IP Subnet, or IP Wildcard as part of the match criteria. To create variables for these values, click + Add Variable for that field.

- To add a variable for the IP address or IP range, select IPv4 Address, IPv4 Range, or IPv6 Address from the drop-down list, click the  Plus icon, and then click Add. You can add multiple variables.

- To add a variable for the IP subnet, select IP Subnet or IPv6 Subnet, click the  Plus icon, and then click Add. You can add multiple variables.

- To add a variable for the IP wildcard, enter a name for the variable, click the  Plus icon, and then click Add. You can add multiple variables.

22. Click the Destination Address tab. The following screen displays.

Add QoS Rule

Match Criteria

Applications & URLs Users & Groups **Source & Destination Traffic** Service & DSCP Action Classification Permissions Review & Submit

By default, all source & destination traffic have been included. If you prefer, you can customize which source & destination traffic to include or exclude below.

Source Address **Destination Address** Source Zone & Sites Destination Zone & Sites

☐ Negate Destination Address [+ Add Variable](#)

Search or select from list

Name	Addresses
<input type="checkbox"/> Copy_hbqh	192.168.0.56/255.255.0.255, 192.168.0.1/255.255.0.255, 192.168.0.2/255.255.0.255, 192.168.3.0/255.255.0.255, 0012::/23, 11::/23, 14::/23, 18::/23, 5.5.5.5-5.5.10.5, 5.5.15.5-5.5.15.15, 5.5.15.115-5.5.15.215
<input type="checkbox"/> Copy_of_Copy_of_Copy_of_lan2192	192.168.0.56/255.255.0.255, 192.168.0.1/255.255.0.255, 192.168.0.2/255.255.0.255, 192.168.3.0/255.255.0.255, 0012::/23, 11::/23, 14::/23, 18::/23, 5.5.5.5-5.5.10.5, 5.5.15.5-5.5.15.15, 5.5.15.115-5.5.15.215
<input type="checkbox"/> Copy_of_Copy_of_lan2192	192.168.0.56/255.255.0.255, 192.168.0.1/255.255.0.255, 192.168.0.2/255.255.0.255, 192.168.3.0/255.255.0.255, 0012::/23, 11::/23, 14::/23, 18::/23, 5.5.5.5-5.5.10.5, 5.5.15.5-5.5.15.15, 5.5.15.115-5.5.15.215
<input type="checkbox"/> Copy_of_Copy_of_lan	1.2.3.4-1.2.3.10, 10.2.3.0/24, 192.168.0.56/255.255.0.255, 0012::/23
<input type="checkbox"/> Copy_of_VeryLONGNAMETOTRUNCATEDATAHERE	
<input type="checkbox"/> Copy_of_lan2192	192.168.0.56/255.255.0.255, 192.168.0.1/255.255.0.255, 192.168.0.2/255.255.0.255, 192.168.3.0/255.255.0.255, 0012::/23, 11::/23, 14::/23, 18::/23, 5.5.5.5-5.5.10.5, 5.5.15.5-5.5.15.15, 5.5.15.115-5.5.15.215
<input type="checkbox"/> Copy_of_lan	1.2.3.4-1.2.3.10, 10.2.3.0/24, 192.168.0.56/255.255.0.255, 0012::/23
<input type="checkbox"/> VeryLONGNAMETOTRUNCATEDATAHERE	
<input type="checkbox"/> lan2192	192.168.0.56/255.255.0.255, 192.168.0.1/255.255.0.255, 192.168.0.2/255.255.0.255, 192.168.3.0/255.255.0.255, 0012::/23, 11::/23, 14::/23, 18::/23, 5.5.5.5-5.5.10.5, 5.5.15.5-5.5.15.15, 5.5.15.115-5.5.15.215
<input type="checkbox"/> lan	1.2.3.4-1.2.3.10, 10.2.3.0/24, 192.168.0.56/255.255.0.255, 0012::/23

Showing 1-10 of results 10 Rows per Page

Go to page 1 < Previous 1 2 Next >

IP Address or IP Range [+ Add Variable](#) IP Subnet [+ Add Variable](#) IP WildCard [+ Add Variable](#)

Enter IP address or range Enter a list of IPv4/IPv6 Subnet values Enter a list of wildcard values

Cancel Back Skip to Review Next

23. To customize the destination traffic, use one of the following methods:

- To specify destination addresses to include in the match criteria, continue to Step 24 to select addresses.
- To specify destination addresses to exclude from the match criteria, select Negate Source Address to match all destination addresses except the addresses that you specify, and then continue to Step 24 to select addresses.

24. To specify a destination address to include or exclude in the match criteria, you can select a destination address from the list or use the search box to find a destination address. To create a variable for the destination address, click + Add Variable to the right of the destination address list. You can also enter values for the fields IP Address or IP range, IP Subnet, or IP Wildcard as part of the match criteria. To create variables for these values, click + Add Variable for that field. For more information on adding variables, see step 21.

25. Select the Source Zone and Sites tab. The following screen displays. All source zones and source sites are included in the match criteria by default. To customize the source zones and source sites to be included in the match criteria, enter information for the following fields.

Add QoS Rule

Match Criteria

Applications & URLs Users & Groups **Source & Destination Traffic** Service & DSCP

Action

Classification Permissions Review & Submit

By default, all source & destination traffic have been included. If you prefer, you can customize which source & destination traffic to include or exclude below.

Source Address Destination Address **Source Zone & Sites** Destination Zone & Sites

Source Zones **+ Add Variable**

Search or select from list

Source Sites **+ Add Variable**

Search or select from list

Cancel Back Skip to Review Next

Field	Description
Source Zones	Click the down arrow, and then select one or more zones. To create a variable for the source zone, click + Add Variable .
Source Sites	Click the down arrow, and then select one or more sites. To create a variable for the source zone, click + Add Variable .

26. Select the Destination Zone and Sites tab. By default, all destination zones and destination sites are included in the match criteria. To customize the destination zones and destination sites to be included in the match criteria, enter information for the following fields.

Add QoS Rule

Applications & URLs Users & Groups **Source & Destination Traffic** Service & DSCP Classification Permissions Review & Submit

By default, all source & destination traffic have been included. If you prefer, you can customize which source & destination traffic to include or exclude below.

Source Address Destination Address Source Zone & Sites **Destination Zone & Sites**

Destination Zones **+ Add Variable**

Search or select from list

Destination Sites **+ Add Variable**

Search or select from list

Cancel Back Skip to Review Next

Field	Description
Destination Zones	Click the down arrow, and then select one or more zones. To create a variable for the source zone, click + Add Variable .
Destination Sites	Click the down arrow, and then select one or more sites. To create a variable for the source zone, click + Add Variable .

- Click Next or select Step 4, Service & DSCP. The following screen displays. All services, service groups, and differentiated services code points (DSCPs) are included in the match criteria by default. On this screen you can specify the services, service groups, and DSCPs to include in the match criteria.

Add QoS Rule

Applications & URLs Users & Groups Source & Destination Traffic **Service & DSCP** Classification Permissions Review & Submit

By default, all services, service groups & DSCP have been include If you prefer, you can customize which traffic to include or exclude from service, service groups & DSCP below.

Services Service Groups DSCP

Services

Search or select from list

Services(User Defined: 27 | Predefined: 741) All Services


	Name	Type	Protocol	Source Port	Destination Port	Source or Destination Port
<input type="checkbox"/>	TCPCheck	User Defined	TCP			500, 234
<input type="checkbox"/>	CheckForDifferentValues	User Defined	TCP	55	666	
<input type="checkbox"/>	ServiceCheck	User Defined	TCP	123,45	123,45	
<input type="checkbox"/>	test	User Defined	TCP	1213-1345, 3000		
<input type="checkbox"/>	Copy_of_Copy_of_kasunTest30	User Defined	TCP_OR_UDP	90	99	

Cancel Back Skip to Review Next

28. To specify the services to include, do one or both of the following:

- In the search box under Services, enter the service name.
- Select one or more services from the list below the search box. Click All Services to select a category to filter the list:
 - Predefined
 - User Defined

29. Select the Service Groups tab, then select the service group to which you want to apply security access control

rules. You can select User-Defined, Predefined, or both. Click the  Toggle Row Expand icon next to the service group name to view the details for each service group.

Add QoS Rule

Applications & URLs Users & Groups Source & Destination Traffic **Service & DSCP** Classification Permissions Review & Submit

By default, all services, service groups & DSCP have been include If you prefer, you can customize which traffic to include or exclude from service, service groups & DSCP below.

Services **Service Groups** DSCP

Service Groups

Test_SG Search or select from list

Service Groups

	Name	User Defined	Predefined
<input checked="" type="checkbox"/> >	Test_SG		1

Showing 1-1 of 1 results 10 Rows per Page Go to page 1 < Previous 1 Next >

Cancel Back Skip to Review Next

30. Select one or more service groups to include in the match criteria. The service groups are added to the Services

list.

31. Select the DSCP tab. All DSCP decimal values are included by default. You can specify which DSCP decimal values to include in the match criteria.

Add QoS Rule

Applications & URLs Users & Groups Source & Destination Traffic **Service & DSCP** Classification Permissions Review & Submit

By default, all services, service groups & DSCP have been include If you prefer, you can customize which traffic to include or exclude from service, service groups & DSCP below.

Services Service Groups **DSCP**

DSCP Decimal
Select one or more DSCP decimal to apply the QoS Rule. Range is from 0 to 63.

Search or select from list

0
1
2
3
4
5
6

Cancel Back Skip to Review Next

32. Select one or more DSCP decimal values, or use search to locate one or more values.
33. Click Next to go to Step 5, Classification. In the Classification field, select a classification criteria to classify the traffic. The list shows the classifications defined in the Profile Elements > Elements > QoS > Classification folder of reusable objects. For information about configuring QoS classifications, see [Configure QoS Classification Elements](#).

Add QoS Rule

Applications & URLs Users & Groups Source & Destination Traffic Service & DSCP **Classification** Permissions Review & Submit

You can classify traffic based on the following criteria

Classification *

lan

Cancel Back Skip to Review Next

34. Click Next to go to Step 6, Permissions, and revise the permissions, if needed.

Add QoS Rule

Applications & URLs Users & Groups Source & Destination Traffic Service & DSCP Classification **Permissions** Review & Submit


We have preselected the permissions for the roles, below You can change the permission for each of the roles.

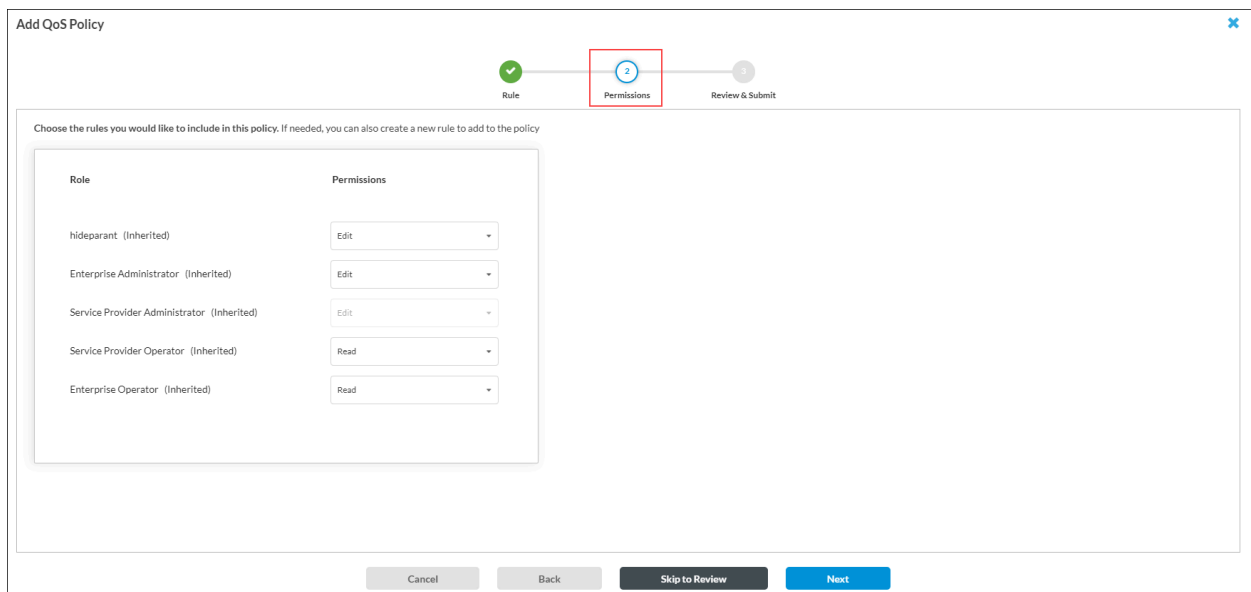
Role	Permissions
hideparant (Inherited)	Edit
Enterprise Administrator (Inherited)	Edit
Service Provider Administrator (Inherited)	Edit
Service Provider Operator (Inherited)	Read
Enterprise Operator (Inherited)	Read

Cancel Back Skip to Review Next

35. Click Next to go to Step 7, Review and Submit and then enter information for the following fields.

Field	Description
◦ Schedule	Select a schedule to set the time and frequency at which the rule is in effect.
◦ Rule Enabled	Click to disable the rule once it is saved. By default, the rule is enabled.

36. Review the selected settings. Click the  Edit icon to change a setting, as needed.
37. Click Save to save the rule.
38. In the Add QoS Policy screen, click Step 2, Permissions. The following screen displays.



Add QoS Policy

Progress: Rule (1) → **Permissions (2)** → Review & Submit (3)

Choose the rules you would like to include in this policy. If needed, you can also create a new rule to add to the policy

Role	Permissions
hideparant (Inherited)	Edit
Enterprise Administrator (Inherited)	Edit
Service Provider Administrator (Inherited)	Edit
Service Provider Operator (Inherited)	Read
Enterprise Operator (Inherited)	Read

Buttons: Cancel, Back, Skip to Review, Next

39. To change the permissions for a role, select Edit, Hide, or Read in the Permissions column.
40. Click Next to go to Step 3, Review and Submit.

Add QoS Policy ✕

✓ Rule
✓ Permissions
⚙ Review & Submit

Choose the rules you would like to include in this policy. If needed, you can also create a new rule to add to the policy

General

Name

Description

Tags

Rules ✎ Edit

QoS Rules (0)


Rule Name	Version	Match Criteria					Action			Status	Last Modified
		Applications & URLs	Users & Groups	Sources	Destinations	Services	Classification				
No Data											

Permissions ✎ Edit

hideparant	Edit
Enterprise Administrator	Edit

Cancel
Back
Save

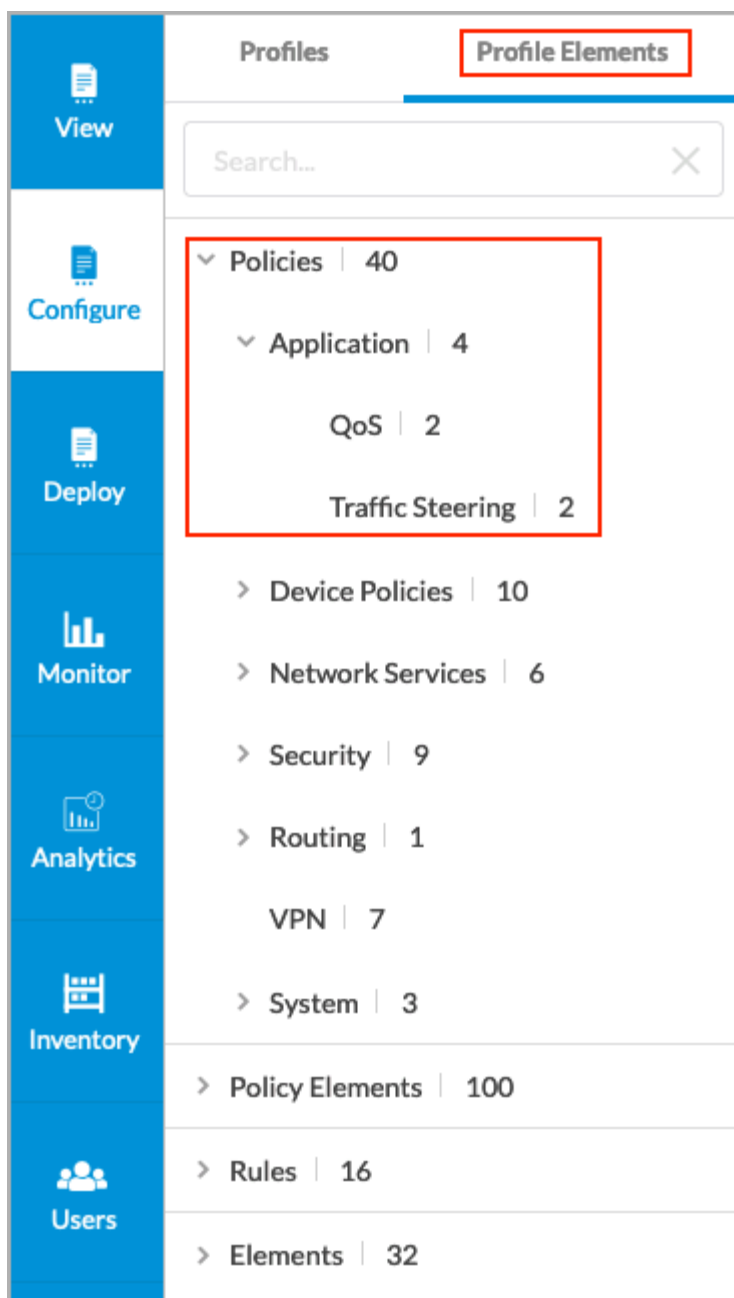
41. In the General box, enter a name for the QoS policy, and optionally enter a text description for the policy and one or more tags. A tag is an alphanumeric text descriptor with no spaces or special characters. You can specify multiple tags added for the same object. The tags are used for searching the objects.

42. Review the settings you have selected. Click the  Edit icon to change a setting, as needed.

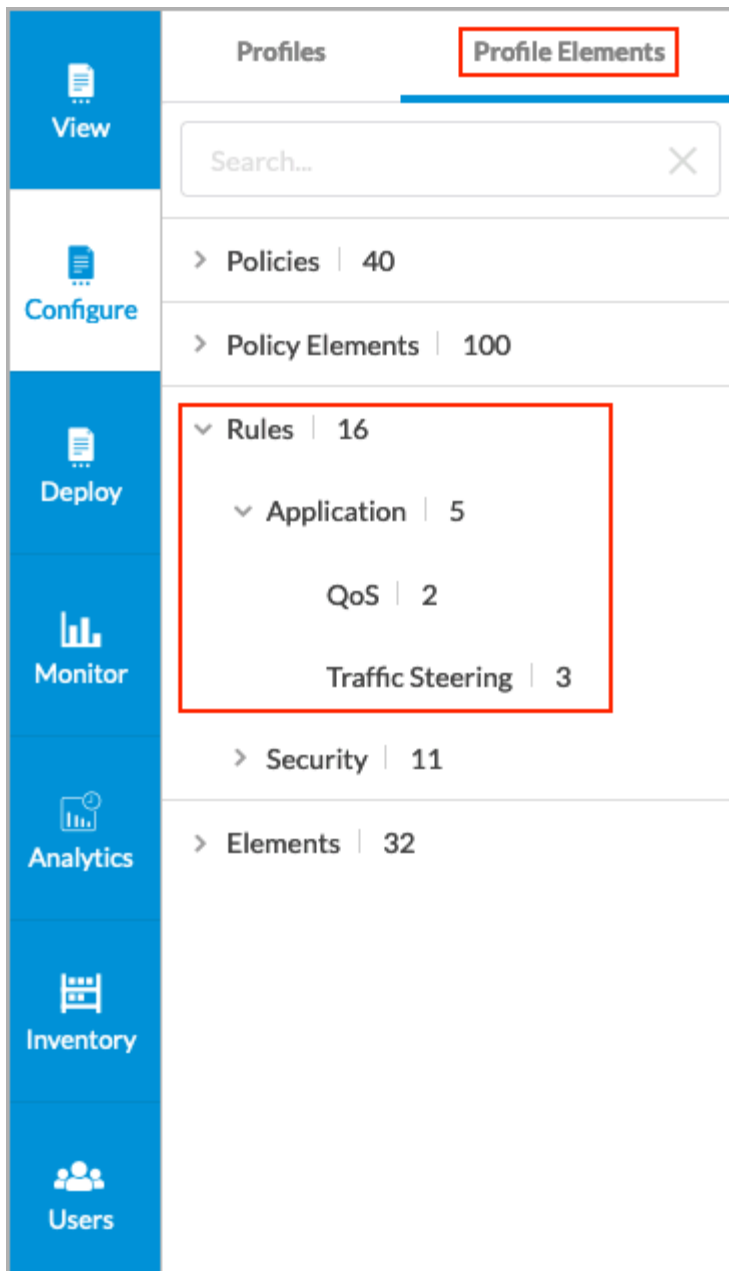
43. Click Save to create the QoS policy.

Note that you can create QoS policy rules in the Profile Elements also, in two places:

- To create a QoS rule in the Profile Elements > Policies > Application folder, click QoS and then follow step 6 through step 43, above.



- To create a QoS rule in the Profile Elements > Rules > Application folder, click QoS and then follow Step 8 through 37, above.

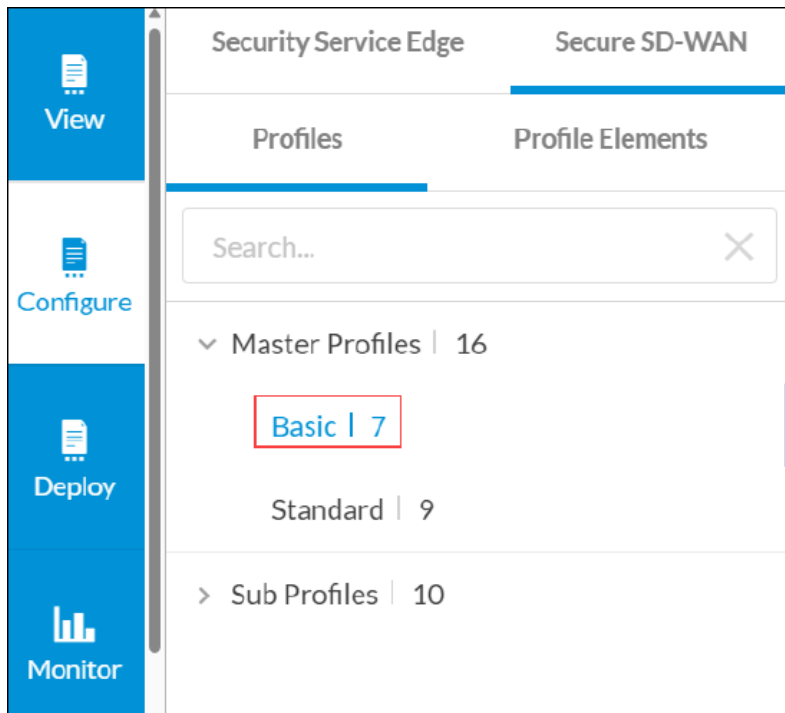


Attach QoS Policies to a Basic Master Profile

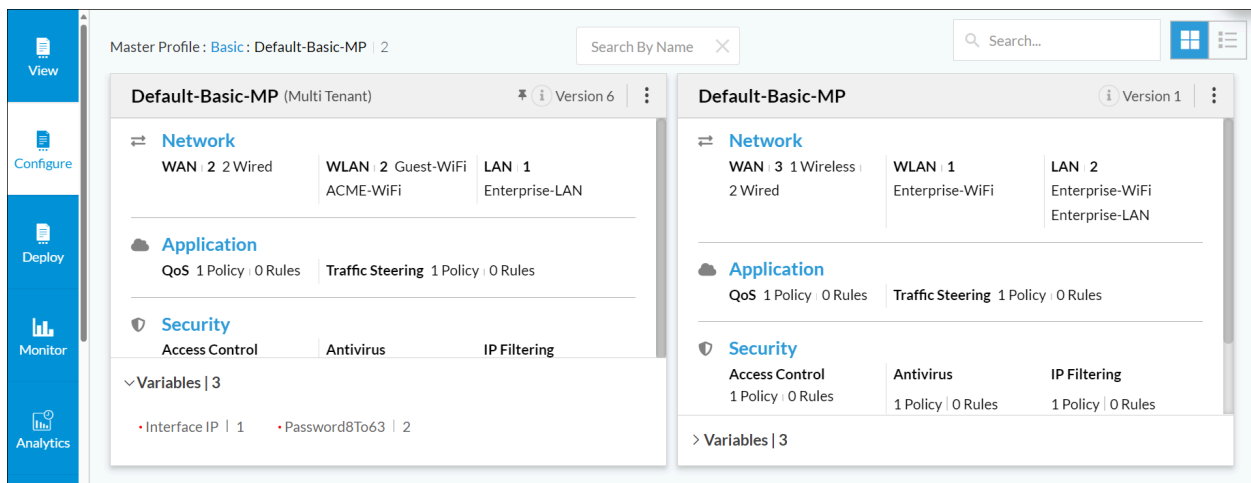
After you create a QoS policy, you can attach it to a basic master profile.

To attach QoS policies to a basic master profile:

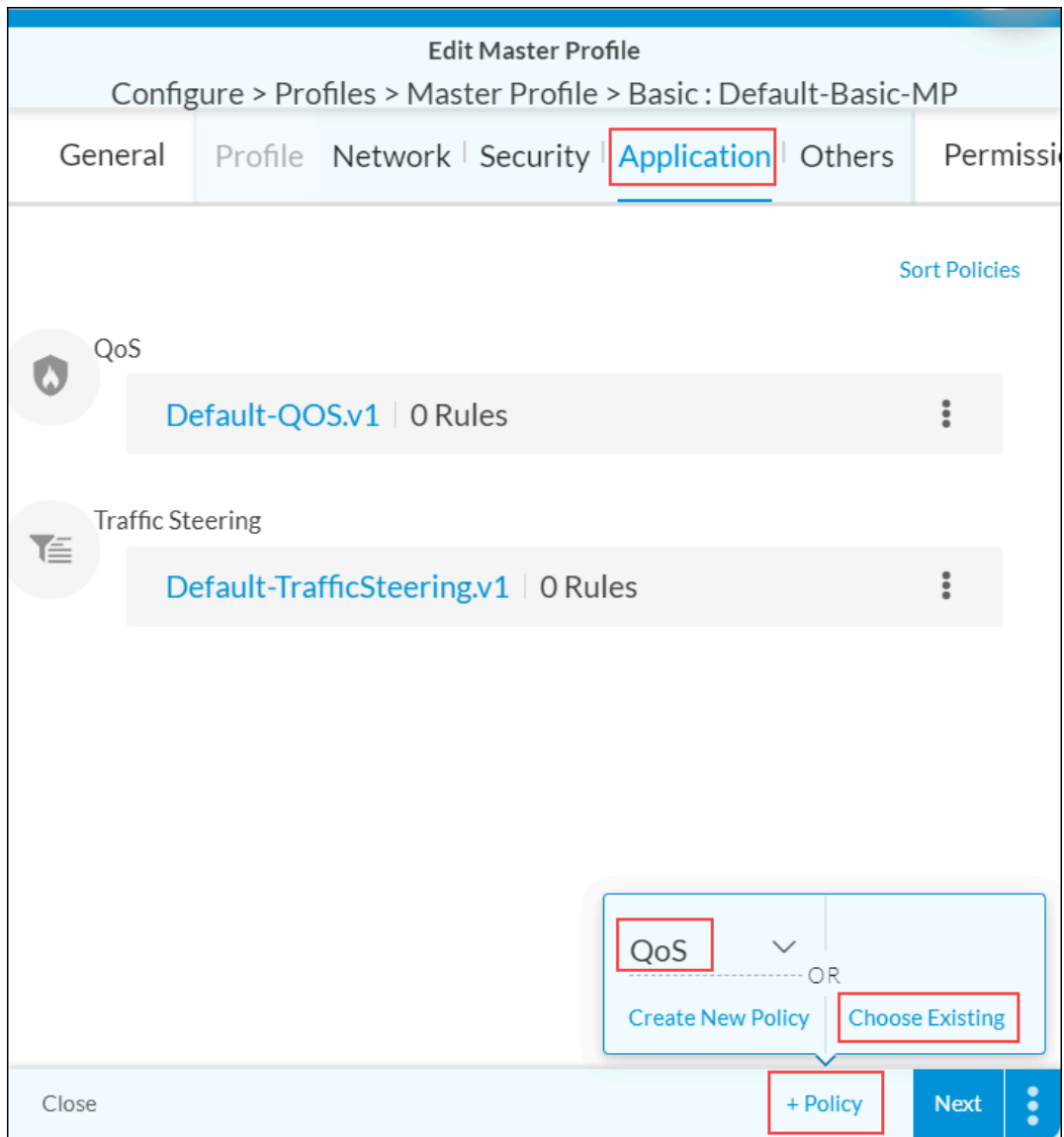
1. Go to Configure > Secure SD-WAN > Profiles > Master Profiles > Basic.



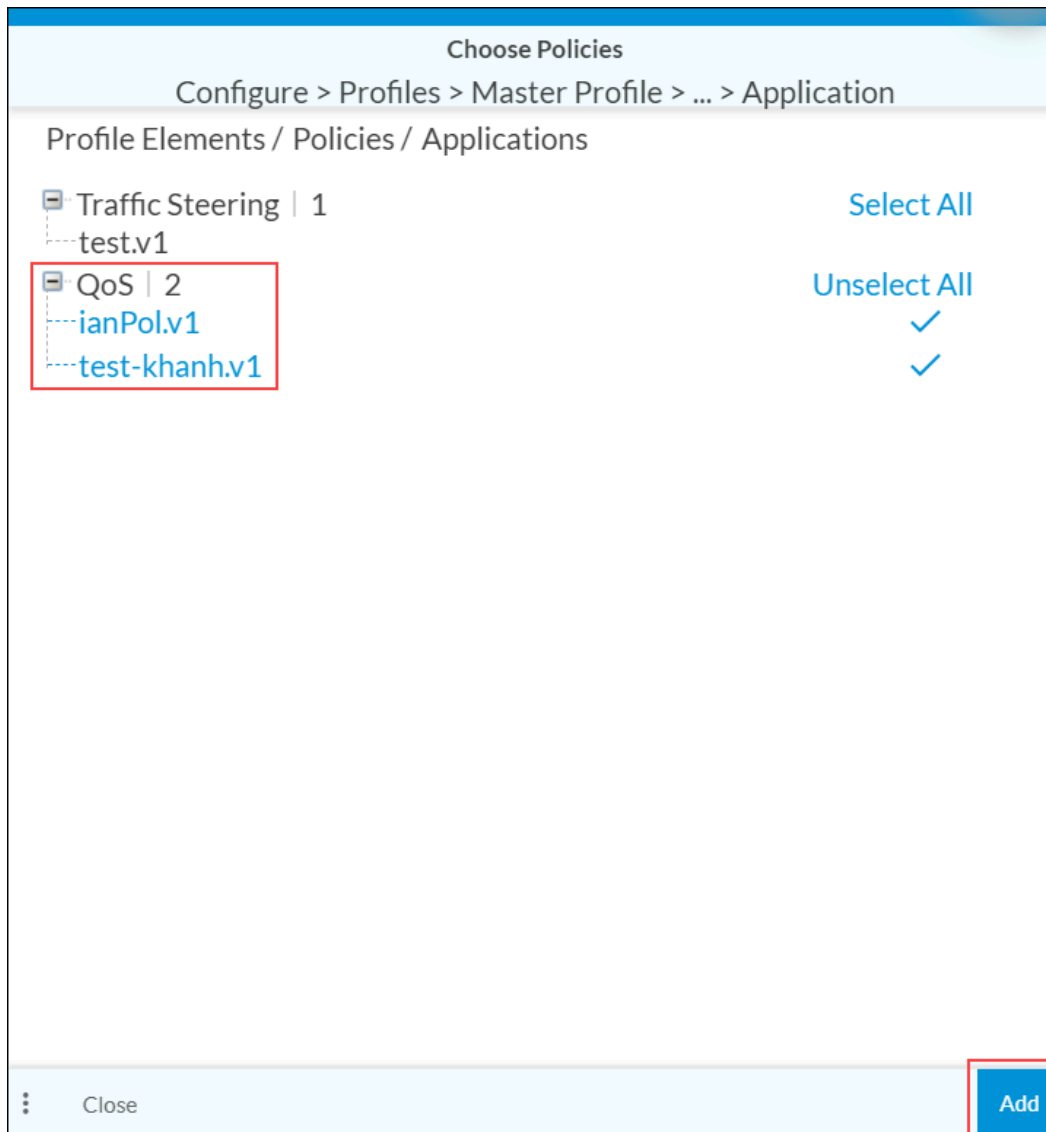
The screen displays the configured basic master profiles.



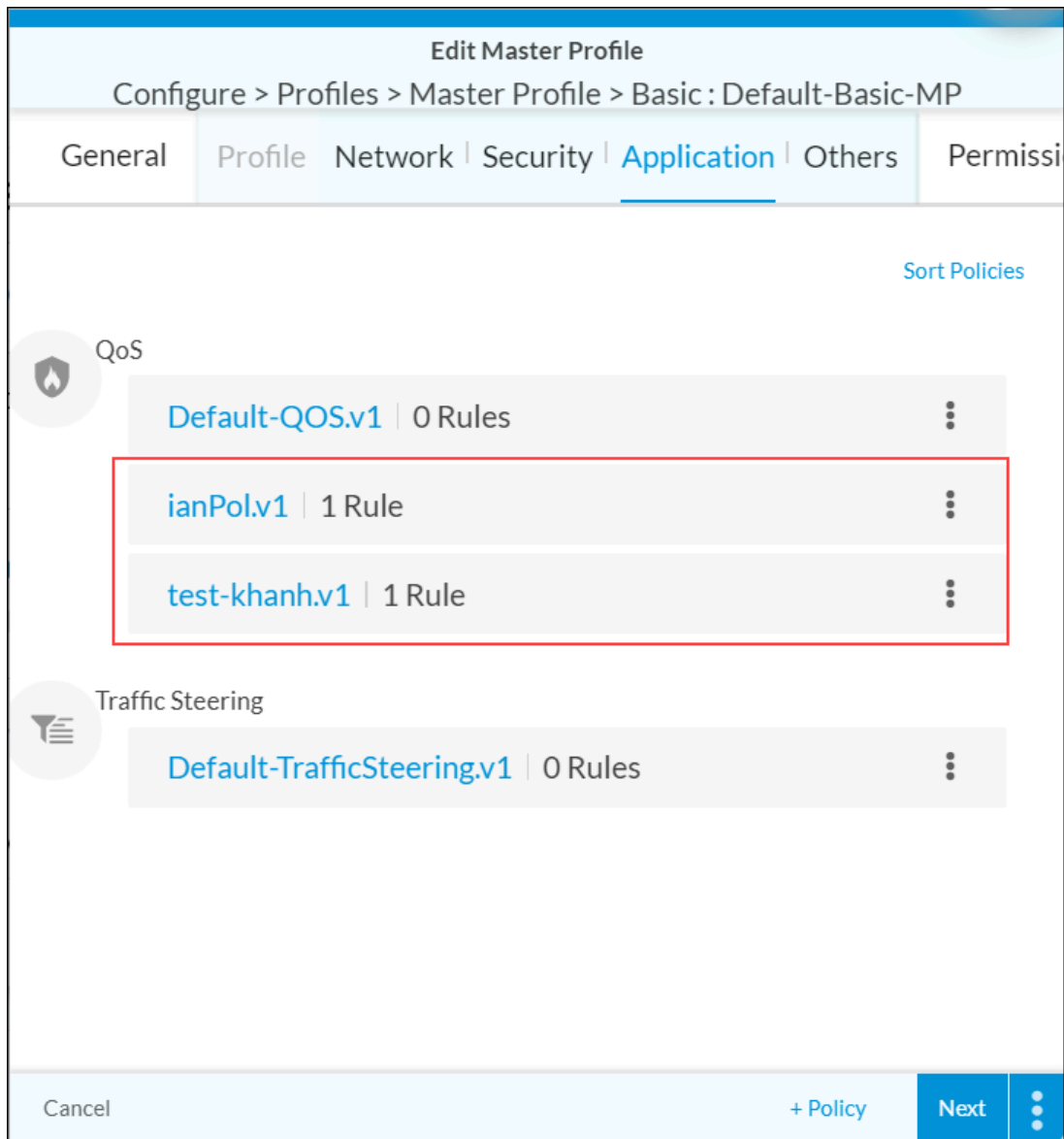
2. Click the master profile to which you want to attach the QoS policy. The Edit Master Profile screen displays.
3. Select the Profile > Application tab. Click +Policy, click the down arrow and select QoS, and then select Choose Existing.



4. In the Choose Policies screen, select the QoS policy from the list, and then click Add.



The Edit Master Profile screen displays the QoS policies added.



Supported Software Information

Releases 10.2.1 and later support all content described in this article, except:

- Release 12.1.1 adds support for the Negate Source Address and Negate Destination Address options when configuring a QoS rule.

Additional Information

[Configure Profiles](#)

https://docs.versa-networks.com/Secure_SD-WAN/02_Configuration_from_Concerto/Secure_SD-WAN_Configuration/Config...

Updated: Wed, 23 Oct 2024 08:04:33 GMT

Copyright © 2024, Versa Networks, Inc.

