

---

## Configure Profile Elements

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

You use the Configure lifecycle to create all configuration objects for Secure SD-WAN deployments. The Concerto configuration objects are hierarchical. For more information, see [Configuration Hierarchies](#).

The top level of the hierarchy consists of Profiles and Profile Elements. The Profiles hierarchy consists of Master Profiles and Subprofiles. For information about configuring profiles, see [Configure Profiles](#).

Profile elements are reusable configuration objects that are part of all profiles. There are four types of profile elements:

- Policies—You can configure the following types of policies for a profile element:
  - Application
  - Device Policies
  - Network Services
  - Security
  - User and Device Authentication
  - Routing
  - VPN
  - System
- Policy elements—You can configure the following types of policy elements for a profile element:
  - Device
  - Network services
  - VPN elements
- Rules—You can configure the following types of rules for a profile element:
  - Application
  - Security
- Elements—You can configure the following types of elements for a profile element:
  - Application
  - Certificates
  - Endpoint
  - Monitor
  - Security (for Releases 12.1.1 and later)

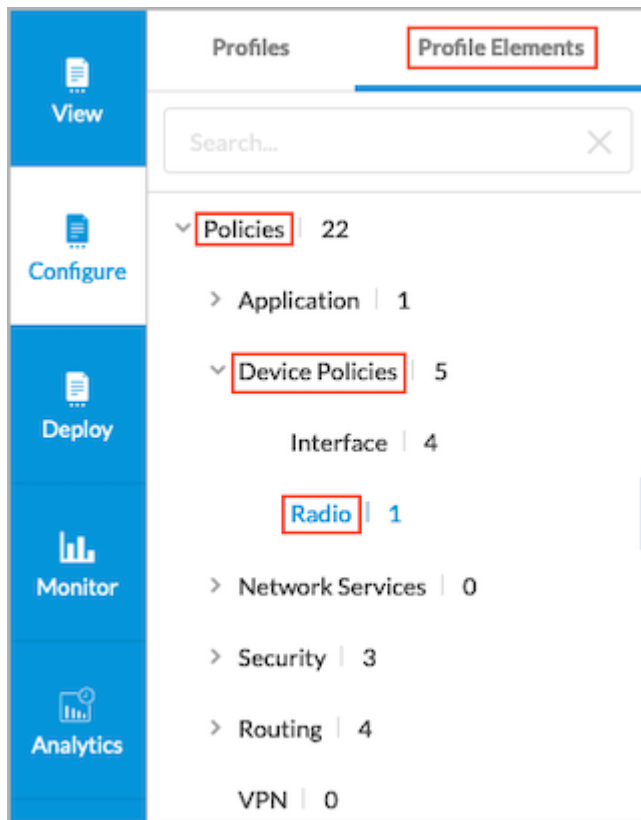
- QoS
- Servers
- VPN name

---

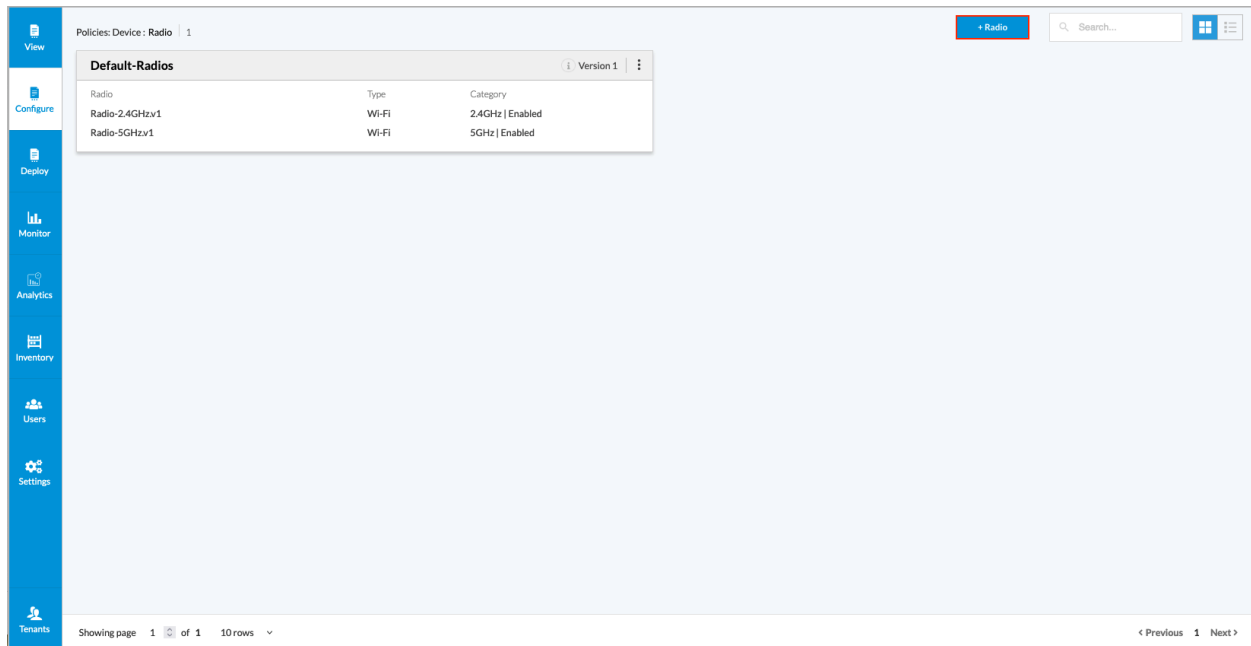
## Add a New Profile Element

To add a new profile element:

1. In Tenants view, select the tenant name. The configured landing page for the tenant displays.
2. In the left menu bar, click Configure. The Configure screen displays, and the Profiles tab is selected.
3. Select the Profile Elements tab, and then navigate to the type of profile element that you want to create. For example, to create a new Radio device policy, you would navigate as follows: Configure > Profile Elements > Policies > Device Policies > Radio.



The following screen displays.



4. Click + Radio. The Create Radio Policy screen displays.

Create Radio Policy

General

Radio

Permissions

Name

Version 1

Type

Radio

Variables | 0

No variables present

Radio | 0

No Radio Present

Tags

Close

Next

- 5. Enter the required information in the General, Radio, and Permissions tabs.
- 6. Click Save.

---

## Add New Application Elements

You can configure the following types of new application elements to use in higher-level policies and subprofiles:

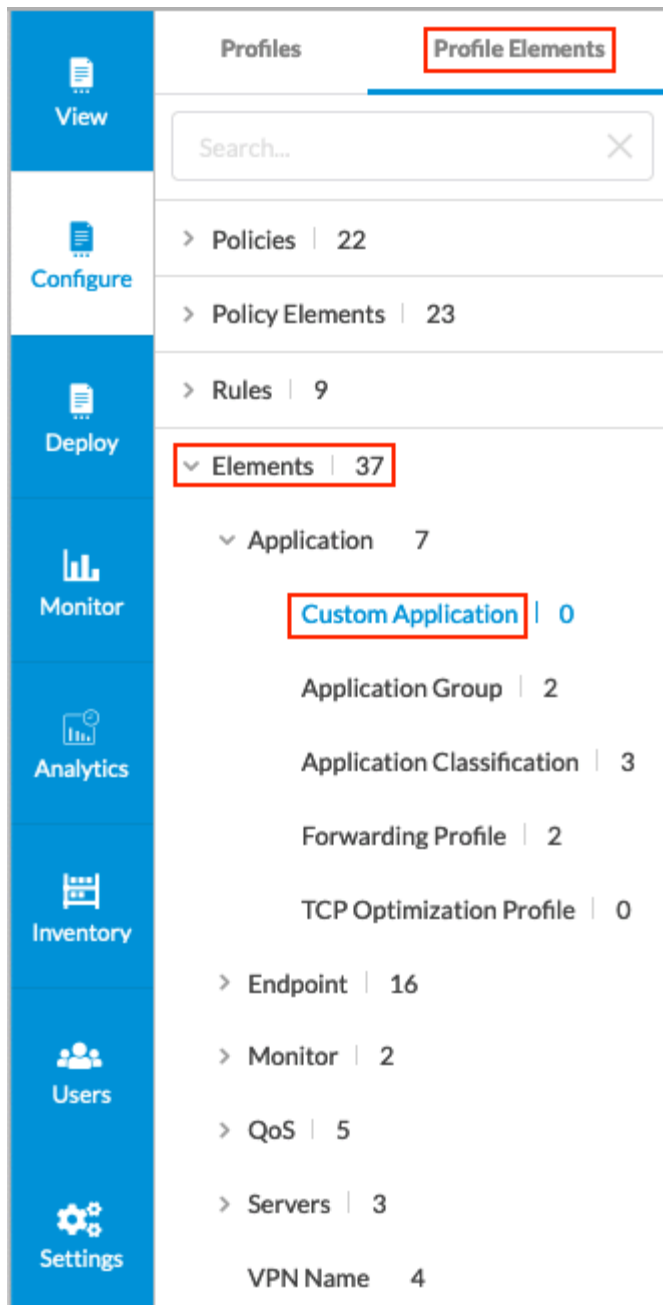
- Custom Application
- Application Group
- Application Classification
- Forwarding Profile
- TCP Optimizations

---

## Add a Custom Application Element

To add a custom application element:

1. Go to Configure > Profile Elements > Elements > Application > Custom Application.



The following screen displays.

View

Configure

Deploy

Monitor

Analytics

Inventory

Security Service Edge

Secure SD-WAN

7

Search By Name

+ Custom Applications

Search...

Profiles

Profile Elements

Search...

> Policies | 3

> Policy Elements | 2

> Rules | 5

> Elements | 39

> Application | 12

Custom Application | 7

Application Group | 1

Application Classification | 4

Forwarding Profile | 0

ables	Image	Last Modified	
refix / Host Pattern: 1.0.0.0/24 ocol: TCP		6/16/2023, 5:19:15 PM Administrator	
refix / Host Pattern: abcd.com ocol: TCP		6/12/2023, 9:39:02 AM Administrator	
refix / Host Pattern: 1.1.1.0/24 ocol: TCP		6/12/2023, 9:38:09 AM Administrator	
refix / Host Pattern: abcd.com ocol: TCP		6/7/2023, 10:25:19 AM Administrator	
refix / Host Pattern: abcd.com ocol: TCP		6/7/2023, 10:23:49 AM Administrator	
refix / Host Pattern: /host/versa ocol: TCP		5/29/2023, 11:18:23 AM Administrator	
refix / Host Pattern: 1.1.1.0/24 ocol: TCP		5/23/2023, 1:33:33 AM Administrator	

- Click + Custom Application. The Create Custom Applications screen displays. Enter information for the following fields.

Create Custom Applications

General

Advanced

Permissions

Name

Type

Internet
▼

Logo

+

Add

Files supported: PNG or SVG only.

Tags

Press Enter to add

Close

Next

⋮

Field	Description
Name	Enter a name for the custom application.
Type	Select the application type. Internet is the only available custom application type.
Logo	Add a logo for the custom application. Click the + Add icon to upload an application image, and then select an image and upload it. The image must be in .png or .svg format.
Tags	Enter one or more tags. A tag is an alphanumeric descriptor, with no white spaces or special characters, that you can use to search the objects.

3. Select the Advanced tab, and then enter information for the following fields.

[https://docs.versa-networks.com/Secure\\_SD-WAN/02\\_Configuration\\_from\\_Concerto/Secure\\_SD-WAN\\_Configuration/Config...](https://docs.versa-networks.com/Secure_SD-WAN/02_Configuration_from_Concerto/Secure_SD-WAN_Configuration/Config...)

Updated: Wed, 23 Oct 2024 08:03:10 GMT

Copyright © 2024, Versa Networks, Inc.



Create Custom Applications

General

Advanced

Permissions

☒ IP Prefix

☐ Host Pattern

Protocol

TCP

Source Port

Port number between 0-65535 or range

Destination Port

Port number between 0-65535 or range

Family

Sub-Family

Risk

Productivity

Precedence

Precedence number between 0-65535

Cancel

Next

Field	Description
IP Prefix	Click to use an IP prefix. Then enter a valid IP prefix and subnet. Note that if you select IP Prefix, you cannot also select Host Pattern.
Host Pattern	Click to use a host pattern. Then enter a host pattern to detect. Note that if you select Host Pattern, you cannot also select IP Prefix.
Protocol	Select a protocol. If you selected Host Pattern, TCP is the only protocol available.
Source Port	<p>If you select IP Prefix and either TCP or UDP, enter the source port number. You can enter a single port value or a range of value,; for example, 500 and 1-100.</p> <p><i>Range:</i> 0 through 65535</p> <p><i>Default:</i> None</p>
Destination Port	<p>If you select IP Prefix and either TCP or UDP, enter the destination port number. You can enter a single port value or a range of values, for example, 500 and 1-100.</p> <p><i>Range:</i> 0 through 65535</p> <p><i>Default:</i> None</p>
Family	<p>(For Releases 11.4.1 and later.) Select the application's family type:</p> <ul style="list-style-type: none"> <li>◦ business-system</li> <li>◦ collaboration</li> <li>◦ general-internet</li> <li>◦ media networking</li> </ul>
Subfamily	<p>(For Releases 11.4.1 and later.) Select the application's subfamily type:</p> <ul style="list-style-type: none"> <li>◦ antivirus</li> </ul>

	<ul style="list-style-type: none"> <li>◦ application-service</li> <li>◦ audio-video</li> <li>◦ authentication</li> <li>◦ behavioral</li> <li>◦ compression</li> <li>◦ database</li> <li>◦ encrypted</li> <li>◦ encrypted-tunnel</li> <li>◦ erp</li> <li>◦ file-server</li> <li>◦ file-transfer</li> <li>◦ forum</li> <li>◦ game</li> <li>◦ instant-messaging</li> <li>◦ internet-utility</li> <li>◦ mail</li> <li>◦ microsoft-office</li> <li>◦ middleware</li> <li>◦ network-management</li> <li>◦ network-service</li> <li>◦ peer-to-peer</li> <li>◦ printer</li> <li>◦ routing</li> <li>◦ security-service</li> <li>◦ standard</li> <li>◦ telephony</li> <li>◦ terminal</li> <li>◦ thin-client</li> <li>◦ tunneling</li> <li>◦ unknown</li> <li>◦ wap</li> <li>◦ web</li> <li>◦ webmail</li> </ul>
Risk	(For Releases 11.4.1 and later.) Select a risk level to assign to the application.

	<i>Value:</i> 1 through 5
Productivity	(For Releases 11.4.1 and later.) Select a productivity value to assign the application.  <i>Value:</i> 1 through 5
Precedence	(For Releases 11.4.1 and later.) Enter a unique priority number to use when multiple applications match the traffic. The application with a higher precedence value is matched first.  <i>Range:</i> 0 through 65535

4. Select the Permissions tab, and then revise the permissions if necessary.

Create Custom Applications

General

Advanced

Permissions

US-Hide (Inherited)	Read	⌵
US_Read (Inherited)	<div> <div>Edit</div> <div>Read</div> <div>Hide</div> </div>	
Audit-Hide (Inherited)		
ACL_Hide (Inherited)	Edit	⌵
SPO-Copy (Inherited)	Read	⌵
EO_AuditEDit (Inherited)	Read	⌵
RR1 (Inherited)	Edit	⌵
Test1 (Inherited)	Edit	⌵
US_Hide (Inherited)	Edit	⌵
Enterprise Administrator (Inherited)	Edit	⌵

Cancel

Save

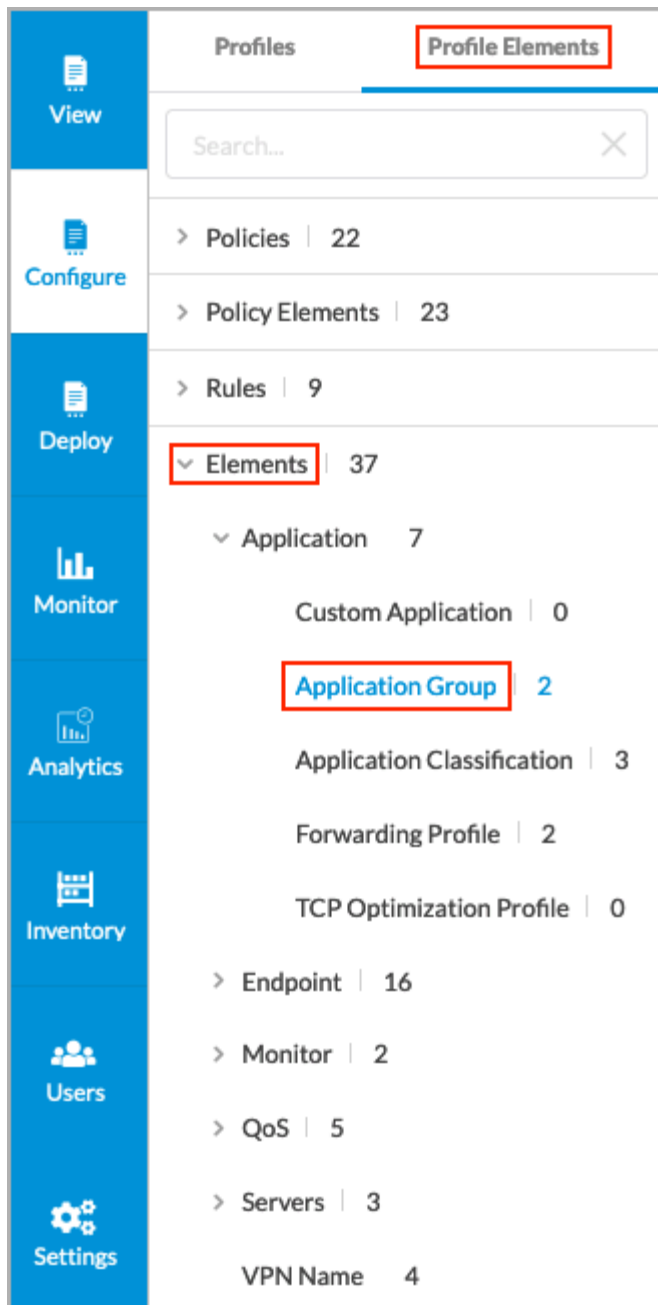
⋮

5. Click Save to create the custom application.

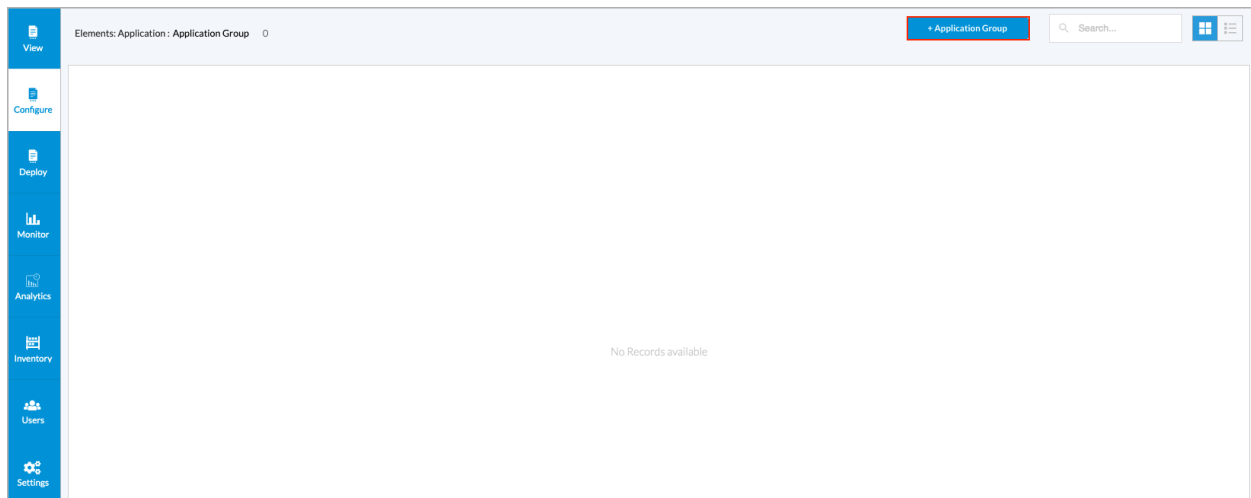
## Add an Application Group Element

To add a new application group:

1. Go to Configure > Profile Elements > Elements > Application > Application Group.



The following screen displays.



2. Click + Application Group. The Create Application Group screen displays. Enter information for the following fields.

Create Application Group

V1

General

Applications

Permissions

Name

Type

Internet

Logo

Add

Files supported: PNG or SVG only.

Summary

None

Tags

Close

Next



Field	Description
Name	Enter a name for the custom application.
Type	Select the custom application type. Internet is the only available type.
Logo	Add a logo for the custom application. Click the + Add icon to upload an application image, and then select an image and upload it. The image must be in .png or .svg format.
Tags	Enter one or more tags. A tag is an alphanumeric descriptor, with no white spaces or special characters that you can use to search the objects.

3. Select the Applications tab, click in the Search for Applications field, and then select the applications to include in the group.

Note: You can select only internet and predefined applications.

Create Application Group

V1

General

Applications

Permissions

Search for Applications

Predefined

01NET

050PLUS

0ZZ0

10050NET

10086CN

104COM

1111TW

114LA

115COM

118114CN

11ST

123PEOPLE

1337X

139MAIL

15MIN

163\_WEBMAIL

163COM

17173COM

Select All

Cancel

Next

4. Select the Permissions tab, and then revise the permissions if necessary.

Create Application Group

General

Applications

Permissions

Enterprise Administrator (Inherited)	<div>Edit</div> <div> <div>Edit</div> <div>Read</div> <div>Hide</div> </div>
Service Provider Administrator (Inherited)	
Service Provider Operator (Inherited)	
Enterprise Operator (Inherited)	<div>Read</div> <div></div>

Cancel

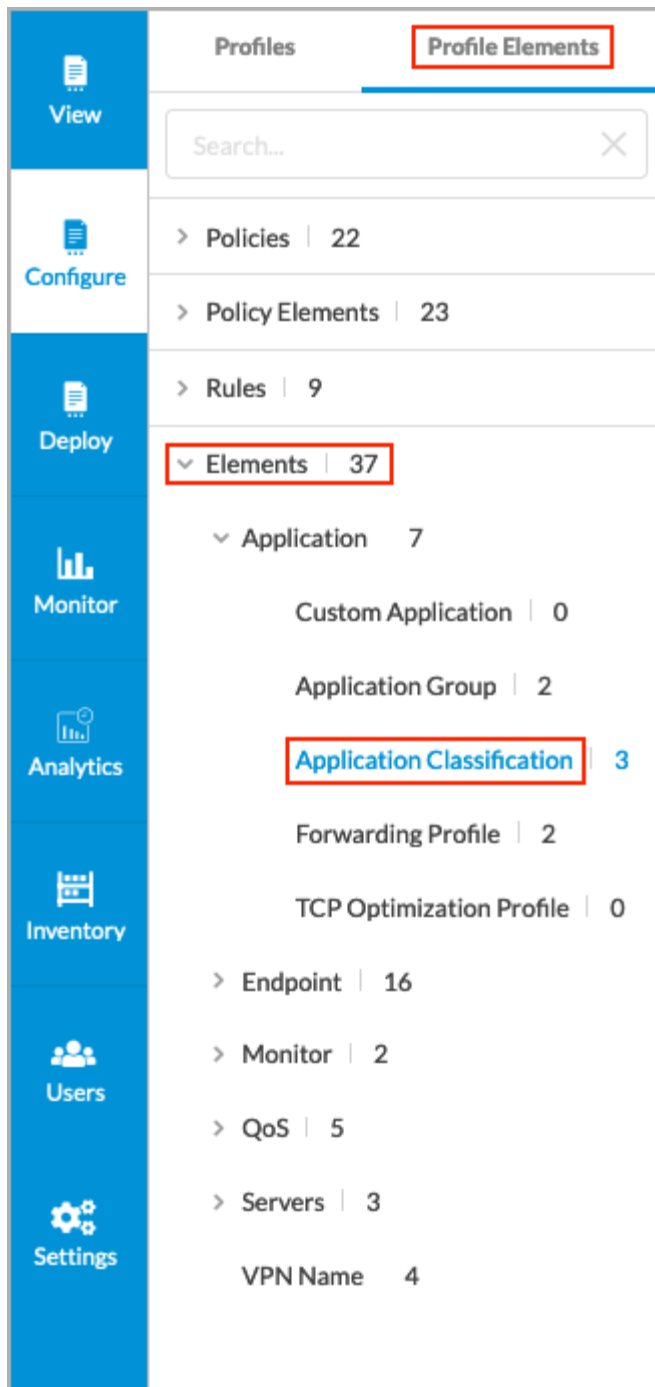
Save

- Click Save to create the application group.

## Add an Application Classification Element

To add a new application classification element:

- Go to Configure > Profile Elements > Elements > Application > Application Classification.



2. Select Application Classification. The screen displays the application classifications that are already configured.

View

Configure

Deploy

Monitor

Analytics

Inventory

Users

Settings

Tenants

Elements: Application : Application Classification 3

+ Application Classification

Search...

Real-Time

Category	Expedited	Forwarding Class
Application Category	VOIP Audio-Video-Streaming	Forwarding Class 4

Business-Critical

Category	Assured	Forwarding Class
Application Category	ADP-Apps Amazon-Apps Box-Apps Citrix-Apps Concur-Apps DocuSign-Apps Dropbox-Apps IBM-Apps Intuit-Apps Jira-Apps Office365-Apps Oracle-Apps SAP-Apps Salesforce-Apps	Forwarding Class 8

Default

Category	Best Effort	Forwarding Class
Application Category	Google-Apps Conferencing-Apps SoftwareUpdates File-Transfer Adobe-Apps	Forwarding Class 12

Showing page 1 of 1 10 rows

< Previous 1 Next >

- Click + Application Classification. The Create Application Classification screen displays.
- Enter information for the following fields.

Create Application Classification

V1

General

Application Category

Permissions

Name

Version 1

Type

Classification

Forwarding Class

Category

Network Control

Class

Forwarding Class 0

Advanced

Close

Next

Field	Description
Name	Enter a name for the application classification.

Field	Description
Forwarding Class (Group of Fields)	
<ul style="list-style-type: none"> <li>Category</li> </ul>	Select a category: <ul style="list-style-type: none"> <li>Assured</li> <li>Best Effort</li> <li>Expedited</li> <li>Network</li> </ul>
<ul style="list-style-type: none"> <li>Class</li> </ul>	Select a class. The classes listed depend on the category you select. <ul style="list-style-type: none"> <li>0 through 3 (for Network category)</li> <li>4 through 7 (for Expedited category)</li> <li>8 through 11 (for Assured category)</li> <li>12 through 15 (for Best Effort category)</li> </ul>

5. Click Advanced to configure advanced options.

Advanced

Loss Priority

▼

Low


▼

×

Add Term

6. Select a term, and then enter information for the following fields. Available terms are Loss Priority, Traffic Conditioning, SLA Metrics, and Connection Priority.

Field	Description
Connection Priority	Select a connection type: <ul style="list-style-type: none"> <li>Internet</li> <li>LTE</li> <li>MPLS</li> </ul> <p>Click Avoid to avoid using the selected connections when forwarding traffic.</p>

Field	Description
	Click Add to add the term, or click cancel to cancel the selected connection type.
Loss Priority	Select the loss priority: <ul style="list-style-type: none"> <li>◦ High</li> <li>◦ Low</li> </ul>
SLA Metrics	Select an SLA metric: <ul style="list-style-type: none"> <li>◦ Low Latency</li> <li>◦ Low Packet Loss</li> <li>◦ Low Delay Variation</li> </ul>
Traffic Conditioning	Select one or more traffic conditions: <ul style="list-style-type: none"> <li>◦ FEC (forward error correction)</li> <li>◦ Load Balance—Click the  slider to select per-flow or per-packet load balancing.</li> <li>◦ Replication</li> </ul>

- Click Advanced again, or click Add Term to add more terms.
- Select the Application Category tab.

Create Application Classification

V1

General

**Application Category**

Permissions

Add Category

- Click Add Category to add more categories.



<

New Application Category

General

Members

Name

AppCategory1

Application Forwarding

Traffic Conditioning

✓ FEC

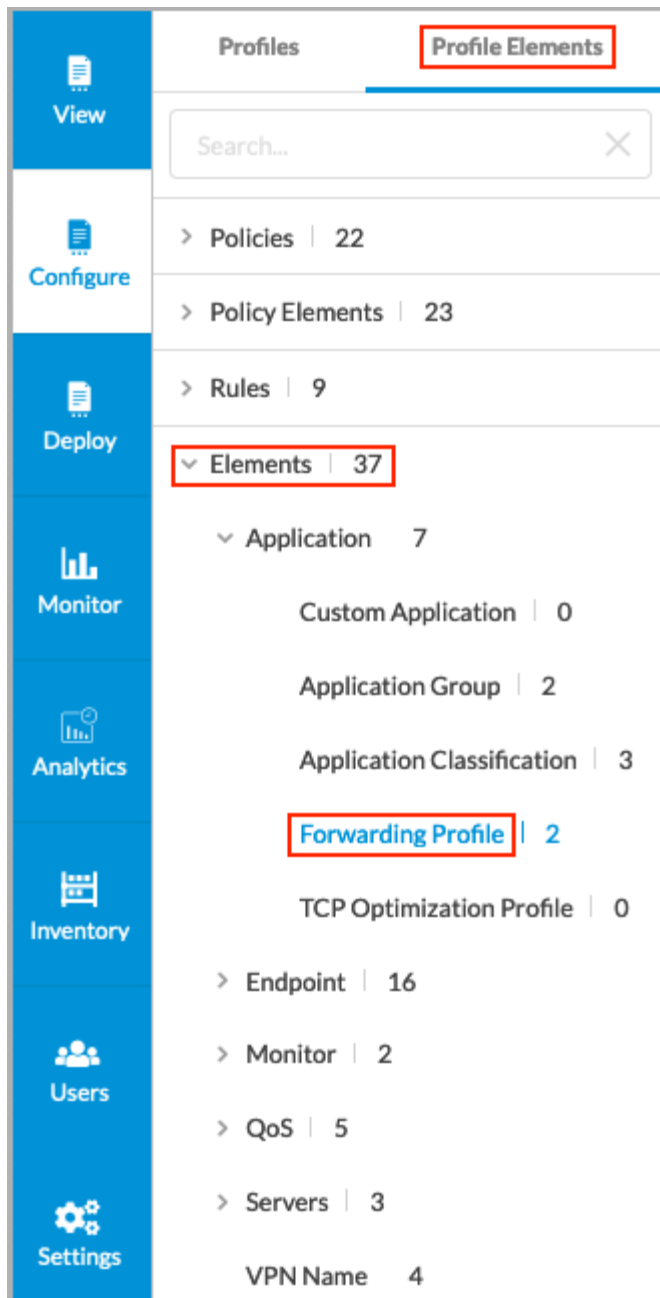
✓ Replication

✓ Load Balance

Add Term

10. In the Name field, enter a name for the application category.
11. Click Add Term.
12. Add Traffic Conditioning, SLA Metrics, and Connection Priority terms, as described in [Step 5](#) above.
13. Select the Members tab.





The Forwarding Profile screen displays all the configured forwarding profiles.

Configure > Profile Elements > Elements > Application

### Forwarding Profile

Below are all the Forwarding Profiles

Forwarding Profiles (1) [+ Add Forwarding Profile](#) [Clone](#) [Delete](#) [Refresh](#) [Select Columns](#)

	Name	Path Selection		Service Level Agreement(SLA)		Path Conditioning		Last Modified
		Path Type	No. Of Priorities			Forward Error Correction	Packet Replication	
<input type="checkbox"/>	<a href="#">FWP-SDWAN-Path-Priority-SLA-FEC-TC-01</a>	SDWAN	2	Maximum Latency	642	<a href="#">Enabled</a>	<a href="#">Enabled</a>	7/7/2023, 12:30:40 PM Ramanjan
				Low Latency	Enabled			
				Max Jitter	90			

[More Details](#)

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

- To customize which columns to display, click Select Columns and then click the columns to display or hide. Click Reset to return to the default column settings.

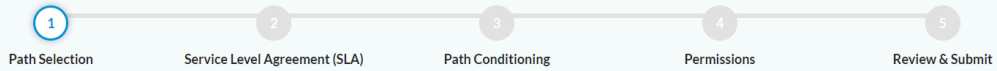
Select Columns

- ☒ Path Type
- ☒ No. of Priorities
- ☒ Service Level Agreement(SLA)
- ☒ Forward Error Correction
- ☒ Packet Replication
- ☒ Last Modified

[Reset](#)

- To create a forwarding profile, click +Add Forwarding Profile. In the Step 1, Path Selection screen, select a route path type.
  - SD-WAN (see steps 4 through 6)
  - Direct Internet and/or Preferred Exit Location (see steps 9 through 13)
- Click SD-WAN to select the SD-WAN route path for forwarding traffic, and then enter information for the following fields. Note that in Releases 11.3.2 and earlier, you configure the forwarding profile on a single screen.

## Forwarding Profile



## Configure Path Selection

Select the path for forwarding traffic by choosing an appropriate Route Path Type.

Choose Route Path Type. The Route Path Type refers to how the next hop is calculated when forwarding the traffic. It can either be a routing lookup or be decided by an SD-WAN policy rule.

☒ SDWAN ☐ Direct Internet and/or Preferred SD-WAN Exit Location

For WAN path selection where the next hop is a Branch, Hub, DC or Gateway in the SD-WAN VPN network. The next-hop for the traffic is decided by a routing table lookup.

Priority	Connection Mode	Local	Remote	
1	Name	--Select--	--Select--	

Add Priority

Select Connection Priority for Unconfigured Paths

--Select--

Cancel

Skip to Review

Next

Field	Description
Priority	<p>Select the path priorities based on WAN connection names, types, or remote site names:</p> <ul style="list-style-type: none"> <li>◦ 1 through 8</li> <li>◦ Avoid—Configure the path as one to avoid. An avoided path is not used even if it is the only available path. If the only available paths are configured as avoid, traffic is dropped.</li> <li>◦ Last Resort—Use the when all other paths are down. As an example, you can configure a last resort so as not to use LTE paths when other paths are available.</li> </ul>
Connection Mode	<p>Select the connection mode:</p> <ul style="list-style-type: none"> <li>◦ Name</li> <li>◦ Type</li> </ul>
Local	<p>If you select the Name WAN connection mode, select a WAN connection name on the local branch:</p> <ul style="list-style-type: none"> <li>◦ Internet-1</li> <li>◦ Internet-2</li> </ul> <p>If you select the Type WAN connection mode, select a WAN connection type on the local branch:</p> <ul style="list-style-type: none"> <li>◦ Broadband</li> <li>◦ LTE</li> <li>◦ MPLS</li> </ul>
Remote	<p>If you select the Name WAN connection mode, select a WAN connection name on the remote branch:</p> <ul style="list-style-type: none"> <li>◦ Internet-1</li> <li>◦ Internet-2</li> </ul> <p>If you select the Type WAN connection mode, select a WAN connection type on the remote branch:</p> <ul style="list-style-type: none"> <li>◦ Broadband</li> <li>◦ LTE</li> </ul>

	<ul style="list-style-type: none"> <li>◦ MPLS</li> </ul>
--	--

- To add another path with the same priority value, click the Plus icon. To remove a path within the same priority value, click the Minus icon.
- To add a path with a different priority value, click Add Priority, and perform Steps 4 and 5.
- Select Connection Priority for Unconfigured Paths.
- Click Direct Internet and/or Preferred SD-WAN Exit Location to select a direct internet preferred exit location route type, and then enter information for the following fields.

Configure > Profile Elements > Elements > Application

### Forwarding Profile

1 Path Selection
 2 Service Level Agreement (SLA)
 3 Path Conditioning
 4 Permissions
 5 Review & Submit

## Configure Path Selection

Select the path for forwarding traffic by choosing an appropriate Route Path Type.

Choose Route Path Type. The Route Path Type refers to how the next hop is calculated when forwarding the traffic. It can either be a routing lookup or be decided by an SD-WAN policy rule.

☐ SDWAN
 ☒ Direct Internet and/or Preferred SD-WAN Exit Location

Direct Internet refers to the WAN Circuit selection for Internet breakout traffic at the Branch. The Preferred SD-WAN Exit Location refers to the traffic path in the SD-WAN VPN network where the next hop or exit location is a Branch, Hub, DC or Gateway. This exit location is decided by the SD-WAN Policy Rule configuration and overrides the routing table lookup at the branch.

Nexthop Selection Method: Load Balance  
 Nexthop Failure Action: Wait Recover  
 Session Pinning to DNS Path: ☒

> NEXT HOP PRIORITY

> SD-WAN PATH PRIORITY

Cancel Skip to Review Next

Field	Description
Next-Hop Selection Method	<p>Select how to choose the next hop for DIA traffic:</p> <ul style="list-style-type: none"> <li>◦ Automatic—Select the next hop that provides the best performance based on passively collected performance metrics.</li> <li>◦ High-Available Bandwidth—Use high-available bandwidth to load-balance DIA traffic among equal priority next hops.</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>◦ Load Balance—Perform equal-cost load balancing among all active next hops at the highest priority level using SLA monitoring and SLA-based path selection metrics.</li> <li>◦ Weighted Round-Robin—Use WRR to load-balance DIA traffic between equal priority next-hops.</li> </ul>
Next-Hop Failure Action	<p>Select the action to take when none of the configured next hops is deemed reachable:</p> <ul style="list-style-type: none"> <li>◦ Failover—Fall back to routing-based path selection.</li> <li>◦ Next Rule—Fail over to the next matching rule.</li> <li>◦ Wait Recover—Wait for this rule to recover at least one next hop.</li> </ul>
Session Pinning to DNS Path	Slide the toggle button to pin all sessions between a client and server to the path of the DNS query that resolved the server.

9. Click Next-Hop Priority, and then click Add Route Path. Enter information for the following fields.



Configure > Profile Elements > Elements > Application

Forwarding Profile

1

2

3

4

5

Path Selection

Service Level Agreement(SLA)

Path Conditioning

Permissions

Review & Submit

Configure Path Selection

Select the path for forwarding traffic by choosing an appropriate Route Path Type.

Choose Route Path Type. The Route Path Type refers to how the next hop is calculated when forwarding the traffic. It can either be a routing lookup or be decided by an SD-WAN policy rule.

☐ SDWAN
 ☒ Direct Internet and/or Preferred SD-WAN Exit Location

Direct Internet refers to the WAN Circuit selection for Internet breakout traffic at the Branch. The Preferred SD-WAN Exit Location refers to the traffic path in the SD-WAN VPN network where the next hop or exit location is a Branch, Hub, DC or Gateway. This exit location is decided by the SD-WAN Policy Rule configuration and overrides the routing table lookup at the branch.

Nexthop Selection Method: 
 Nexthop Failure Action: 
 Session Pinning to DNS Path ? ☒

▼ NEXT HOP PRIORITY

Priority	Path Type	Exit Location	SLA Monitor	Max Latency(ms)	Max Packet Loss(%)	
<input type="text" value="1"/>	<input type="text" value="Preferred SD-WAN ..."/>	<input type="text" value="--Select--"/>	<input type="text" value="--Select--"/>	<input type="text"/>	<input type="text"/>	

Add Route Path

> SD-WAN PATH PRIORITY

Cancel

Skip to Review

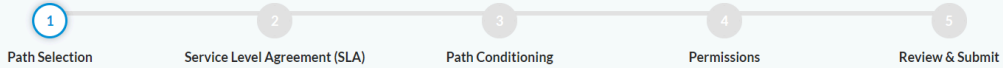
Next

Field	Description
Priority	Select a next-hop priority value. <i>Range:</i> 1 through 15
Path Type	Select a path type: <ul style="list-style-type: none"> <li>Preferred SD-WAN Exit Location—Select the traffic path in the SD-WAN VPN network where the next hop or exit location is a branch, gateway, or hub.</li> <li>Direct Internet—Select the WAN circuit for internet breakout traffic at the branch.</li> </ul>
Preferred SD-WAN Exit Location (Group of Fields)	
<ul style="list-style-type: none"> <li>Exit Location</li> </ul>	Select the branch as an exit location.

Field	Description
◦ SLA Monitor	Select the SLA Monitor created under the Monitor. See <a href="#">Configure SaaS Application Monitors</a> .
◦ Maximum Latency	Enter a value for the maximum traffic latency, in milliseconds.
◦ Maximum Packet Loss	Enter a percentage value for the total combined forward and reverse packet loss.
Direct Internet (Group of Fields)	
◦ WAN Connection	Select the WAN connection.
◦ Next-Hop Address	Enter the next-hop address.
◦ Reachability Monitor	Select the reachability monitor.
◦ SLA Monitor	Select an SLA monitor that you created under the Monitor. See <a href="#">Configure SaaS Application Monitors</a> .
◦ Maximum Latency	Enter a value for the maximum traffic latency, in milliseconds.
◦ Maximum Packet Loss	Enter a percentage value for the total combined forward and reverse packet loss.

10. Click SD-WAN Path Priority, and then click Add Priority. Enter information for the following fields.

## Forwarding Profile



## Configure Path Selection

Select the path for forwarding traffic by choosing an appropriate Route Path Type.

Choose Route Path Type. The Route Path Type refers to how the next hop is calculated when forwarding the traffic. It can either be a routing lookup or be decided by an SD-WAN policy rule.

☐ SDWAN    ☒ Direct Internet and/or Preferred SD-WAN Exit Location



Direct Internet refers to the WAN Circuit selection for Internet breakout traffic at the Branch. The Preferred SD-WAN Exit Location refers to the traffic path in the SD-WAN VPN network where the next hop or exit location is a Branch, Hub, DC or Gateway. This exit location is decided by the SD-WAN Policy Rule configuration and overrides the routing table lookup at the branch.

Nexthop Selection Method    Nexthop Failure Action    Session Pinning to DNS Path ?

Load Balance    Wait Recover    ☐

> NEXT HOP PRIORITY

SD-WAN PATH PRIORITY

Priority	Connection Mode	Local	Remote	
1	Name	--Select--	--Select--	 

Add Priority

Cancel

Skip to Review

Next

Field	Description
Priority	<p>Select the path priorities based on WAN connection names, types, or remote site names:</p> <ul style="list-style-type: none"> <li>◦ 1 through 8</li> <li>◦ Avoid—Configure the path as one to avoid. An avoided path is not used even if it is the only available path. If the only available paths are configured as avoid, traffic is dropped.</li> <li>◦ Last Resort—Use the when all other paths are down. As an example, you can configure a last resort so as not to use LTE paths when other paths are available.</li> </ul>
Connection Mode	<p>Select the connection mode:</p> <ul style="list-style-type: none"> <li>◦ Name</li> <li>◦ Type</li> </ul>
Local	<p>If you select the Name WAN connection mode, select a WAN connection name on the local branch:</p> <ul style="list-style-type: none"> <li>◦ Internet-1</li> <li>◦ Internet-2</li> </ul> <p>If you select the Type WAN connection mode, select a WAN connection type on the local branch:</p> <ul style="list-style-type: none"> <li>◦ Broadband</li> <li>◦ LTE</li> <li>◦ MPLS</li> </ul>
Remote	<p>If you select the Name WAN connection mode, select a WAN connection name on the remote branch:</p> <ul style="list-style-type: none"> <li>◦ Internet-1</li> <li>◦ Internet-2</li> </ul> <p>If you select the Type WAN connection mode, select a WAN connection type on the remote branch:</p> <ul style="list-style-type: none"> <li>◦ Broadband</li> <li>◦ LT</li> </ul>

◦ MPLS

11. To add another path with the same priority value, click the Plus icon. To remove a path within the same priority value, click the Minus icon.
12. To add a path with a different priority value, click Add Priority, and perform steps 3 and 4.
13. Click Next. In the Step 2, Service Level Agreement (SLA) screen, enter information for the following fields.

Configure > Profile Elements > Elements > Application

**Forwarding Profile**

✓

2

3

4

5

Path SelectionService Level Agreement (SLA)Path ConditioningPermissionsReview & Submit

### Configure Service Level Agreement (SLA)

Define SLA link-performance parameters to consider when making the final decision which WAN link to use for forward outgoing traffic.

Maximum Latency

ms

☒ Low Latency

Max Jitter

ms

☒ Low Jitter

Max Packet Loss

%

☒ Low Packet Loss

Maximum Transmit Utilization

%

Maximum Receive Utilization

%

Connection Selection Method

Weighted Round Robin

▼

Recompute Timer

sec

Mean Opinion Score (MOS)

☒ Enable Gradual Migration

☒ Enable SLA Smoothing

☒ Enable SLA Violation Damping

SLA Smoothing Interval

sec

SLA Violation Damping Interval

sec



Cancel

Back

Skip to Review

Next

Field	Description
Maximum Latency	Enter a value for the maximum traffic latency (delay). The link latency is a two-way measurement. <i>Range:</i> 1 to 1000 milliseconds <i>Default:</i> None
Low Latency	Slide the toggle button to select a path based on the lowest latency.
Maximum Jitter	Enter a value for the forward and reverse delay variation (jitter). <i>Range:</i> 1 to 100 milliseconds <i>Default:</i> None
Low Jitter	Slide the toggle button to select a path based on the lowest delay variation (jitter).
Maximum Packet Loss	Enter a percentage value for the total combined forward and reverse packet loss. <i>Range:</i> 1 to 100 percent <i>Default:</i> None
Low Packet Loss	Slide the toggle button to select a path based on the lowest packet loss.
Maximum Transmit Utilization	Enter the percentage of a circuit's available bandwidth to use to transmit traffic. <i>Range:</i> 1 to 100 percent <i>Default:</i> None
Maximum Receive Utilization	Enter the percentage of a circuit's available bandwidth to use to receive traffic. < <i>Range:</i> 1 to 100 percent <i>Default:</i> None
Connection Selection Method	Select how to forward a traffic flow when multiple available WAN paths have the highest priority. For example, if there are two paths at priority 1 and one path at priority 2, one of the priority 1 paths is chosen. <ul style="list-style-type: none"> <li>◦ High available bandwidth—Use the circuit with the highest available bandwidth. Continuing with the example in the previous bullet, because the available bandwidth on WAN2 is higher, this link would be used.</li> <li>◦ Path high available bandwidth</li> <li>◦ Path weighted round-robin</li> <li>◦ Weighted round-robin—Use WRR, which</li> </ul>

Field	Description
	<p>balances flows across paths proportional to their available bandwidth. This is the default connection selection method.</p> <p><i>Default:</i> WRR</p>
Recompute Timer	<p>Enter how often to re-evaluate the SLA-compliance state of all paths. If the re-evaluation identifies an SLA violation on a circuit, the traffic is switched to a different circuit.</p> <p><i>Range:</i> 5 through 1800 seconds <i>Default:</i> 300 seconds</p>
Mean Opinion Score (MOS)	<p>Enter a mean opinion score for audio, video, and voice traffic. Mean opinion score is a measure of the quality of voice data traffic, and it represents the user experience of audio, video, and voice applications. Voice data is always compressed using a codec before it is transmitted, and so the MOS score can vary for the voice data on the same link depending on the codec.</p> <p><i>Range:</i> 0 to 5, where 5 represents the best traffic quality <i>Default:</i> None</p>
Enable Gradual Migration	<p>Click the  toggle button to enable gradual migration.</p>
Enable SLA Violation Damping	<p>Click the  toggle button to enable gradual migration. Select this option to associate the recompute interval value with the damping interval value. If you do not enable SLA violation damping, the SLA compliance of a path is checked every recompute interval.</p>
SLA Smoothing Interval	<p>Enter the SLA smoothing interval, in seconds.</p> <p><i>Range:</i> 10 through 300 seconds</p>

Field	Description
	<i>Default:</i> 120 seconds
SLA Violation Damping Interval	Enter the SLA violation damping interval, in seconds.  <i>Range:</i> 10 through 300 seconds

14. Click Next. In the Step 3, Path Conditioning screen, enter information for the following fields.



Configure > Profile Elements > Elements > Application

Forwarding Profile

✓

Path Selection

✓

Service Level Agreement (SLA)

3

Path Conditioning

4

Permissions

5

Review & Submit

Configure Path Conditioning

Define SD-WAN traffic-steering mechanism that allows you to control errors in data transmission flows when the communication channels are unreliable or noisy

✓

FORWARD ERROR CORRECTION (FEC)

✓

Enable FEC

Send FEC Packet To

Alternate Circuit

Duplicate FEC Packet

Disable

Number of Data Packets per FEC Packets

4

Start When

Always

✓

Stop When

Circuit Utilization

%

✓

PACKET REPLICATION

✓

Enable Packet Replication

Replication Factor

Start When

--Select--

✓

Stop When

Circuit Utilization


%

Cancel

Back

Skip to Review

Next

Field	Description
Forwarding Error Correction (FEC) (Group of Fields)	
<ul style="list-style-type: none"> <li>Enable FEC</li> </ul>	Click the  toggle button to enable FEC. <i>Default:</i> Disabled


[https://docs.versa-networks.com/Secure\\_SD-WAN/02\\_Configuration\\_from\\_Concerto/Secure\\_SD-WAN\\_Configuration/Config...](https://docs.versa-networks.com/Secure_SD-WAN/02_Configuration_from_Concerto/Secure_SD-WAN_Configuration/Config...)

Updated: Wed, 23 Oct 2024 08:03:10 GMT

Copyright © 2024, Versa Networks, Inc.

41

Field	Description
<ul style="list-style-type: none"> <li>Send FEC Packet To</li> </ul>	<p>Select the circuit on which to send FEC parity packets:</p> <ul style="list-style-type: none"> <li>Alternate circuit—Send FEC parity packets on a WAN interface that is not an interface on which data packets are transmitted. This is the default. If an alternate circuit is unavailable, FEC parity packets are sent on the same circuit as data packets.</li> <li>Same circuit—Send FEC parity packets on the same WAN interface used to transmit data packets.</li> </ul> <p><i>Default:</i> Alternate circuit</p>
<ul style="list-style-type: none"> <li>Duplicate FEC Packet</li> </ul>	<p>Select how to duplicate FEC parity packets:</p> <ul style="list-style-type: none"> <li>Alternate circuit—Duplicate FEC parity packets and send them on a WAN interface that is not an interface on which data packets are transmitted.</li> <li>Disable—Do not duplicate FEC parity packets. This is the default.</li> <li>Same circuit—Duplicate FEC parity packets and send them on the same WAN interface used to transmit data packets.</li> </ul> <p><i>Default:</i> Disable</p>
<ul style="list-style-type: none"> <li>Number of Data Packets per FEC Packets</li> </ul>	<p>Enter the number of data packets after which an FEC packet is generated and sent to the peer branch. The generated FEC parity packet can recover a packet on the peer branch only if there is one lost packet in the specified number of packets per FEC.</p> <p><i>Range:</i> 1 through 32 <i>Default:</i> 4</p>
<ul style="list-style-type: none"> <li>Start When</li> </ul>	<p>Select when to start sending FEC parity packets:</p> <ul style="list-style-type: none"> <li>Always</li> <li>SLA violated—When all available paths are SLA violated</li> </ul>

Field	Description
◦ Stop When	Click to set the circuit utilization threshold at which to stop sending FEC parity packets.
◦ Circuit Utilization	<p>When you enable Stop When, enter the utilization threshold at which replication stops automatically. Specify this as a percentage of the total circuit bandwidth. When the circuit utilization of the links used for data packets or FEC parity packet transmission exceeds this threshold, FEC stops.</p> <p><i>Range:</i> 1 through 100 percent <i>Default:</i> None</p>
Packet Replication (Group of Fields)	
◦ Enable Packet Replication	<p>Click the  toggle button to enable packet replication.</p> <p><i>Default:</i> Disabled</p>
◦ Replication Factor	<p>For each ingress packet, define the number of egress packets to send.</p> <p><i>Range:</i> 2 through 4</p>
◦ Start When	<p>Select when to start replication automatically:</p> <ul style="list-style-type: none"> <li>◦ Always</li> <li>◦ SLA violated—When all available paths do not meet configured SLA threshold</li> </ul>
Stop When	Click to enable using a circuit utilization threshold value to stop packet replication.
Circuit Utilization	When you enable Stop When, enter the circuit utilization threshold at which replication stops automatically. Specify this as a percentage of the total circuit bandwidth. When the circuit utilization exceeds this threshold value, packet replication stops automatically.

Field	Description
	<i>Range:</i> 1 through 100 percent <i>Default:</i> None

15. Click Next. In Step 4, Permissions screen displays, showing the default roles and their inherited permissions.

Configure > Profile Elements > Elements > Application

**Forwarding Profile**

✓

✓

✓

4

5

Path Selection    Service Level Agreement(SLA)    Path Conditioning    Permissions    Review & Submit

We have preselected the permissions for the roles, below

You can change the permission for each of the roles.

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

Cancel    Back    Skip to Review    Next

16. If desired, change the permissions by selecting a new permission level for each role.
17. Click Next to go to Step 5, Review and Submit screen.

Configure > Profile Elements > Elements > Application

### Forwarding Profile

✓ Path Selection
✓ Service Level Agreement (SLA)
✓ Path Conditioning
✓ Permissions
5 Review & Submit

[Review & Submit](#)

#### General

Name  Description

Tags

Press Enter to add

#### Path Selection [Edit](#)

Route Path Type SDWAN

Connection Priority for Unconfigured Paths 1

#### Service Level Agreement (SLA) [Edit](#)

Maximum Latency (ms)

Low Latency Enabled

Maximum Jitter (ms)

Low Jitter Enabled

Maximum Packet Loss (%)

Low Packet Loss Enabled

Maximum Transmit Utilization

Maximum Receive Utilization

Connection Selection Method weighted-round-robin

Recompute Timer (sec) 300

Mean Opinion Score (MOS)

Gradual Migration Enabled

SLA Smoothing Enabled

SLA Smoothing Interval (sec)

SLA Violation Damping Enabled

SLA Damping Interval (sec)

#### Path Conditioning [Edit](#)

Forward Error Correction Enabled

Send FEC Packet To alternate-circuit

Duplicate FEC Packet disable

No. of Data Packets per FEC Packets 4

Start When always

Stop When Enabled

Circuit Utilization

Packet Replication Enabled

Start When

Replication Factor

Stop When Enabled

Circuit Utilization

#### Permissions [Edit](#)

Enterprise Administrator	Edit
Enterprise Operator	Read

Cancel
Back
Save

18. In the General section, enter a name for the forwarding profile. Optionally, enter a description and add tags for the profile.
19. Click Edit next to any section to make changes.

20. Click Save.

---

## Add a TCP Optimization Application Element

*For Releases 11.3.1 and later.*

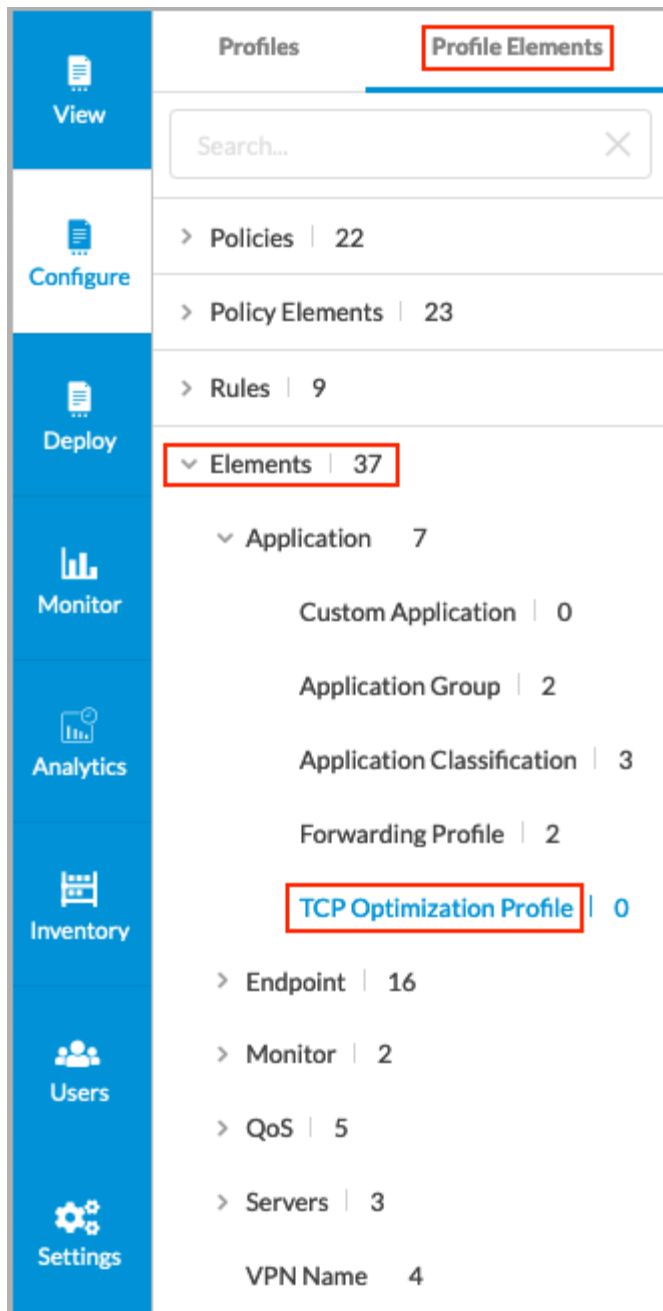
TCP optimizations mitigate the effects of high latency and packet loss on the performance of TCP-based applications. The optimizations are based on a TCP proxy architecture in which one or more VOS devices in a network path between a client and server split the TCP connection into two. One connection faces the client and one faces the server, with the VOS devices acting as TCP proxies for each of the split network segments. The optimizations can be done in one of the following modes:

- Dual-ended mode—TCP connection is split between two peer VOS devices in the network path
- Single-ended mode—TCP connection is split independently on one or more VOS devices in the network path

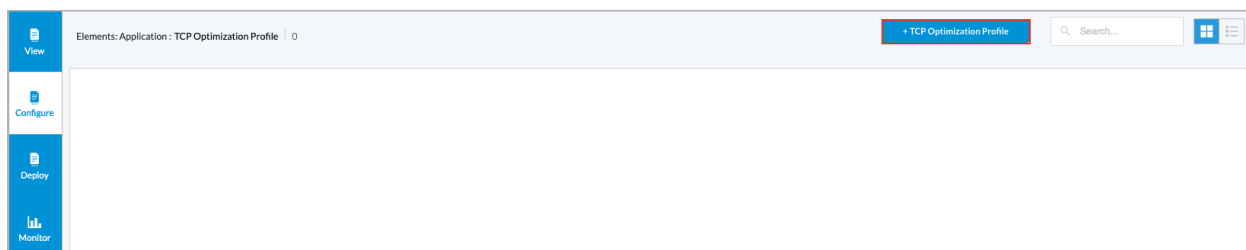
After you create a new TCP optimization application element, you can use it when configuring traffic-steering rules.

To add a TCP optimization application forwarding profile element:

1. Go to Configure > Profile Elements > Elements > Application.



2. Select TCP Optimization Profile. The screen displays already configured TCP optimization profiles.



[https://docs.versa-networks.com/Secure\\_SD-WAN/02\\_Configuration\\_from\\_Concerto/Secure\\_SD-WAN\\_Configuration/Config...](https://docs.versa-networks.com/Secure_SD-WAN/02_Configuration_from_Concerto/Secure_SD-WAN_Configuration/Config...)

Updated: Wed, 23 Oct 2024 08:03:10 GMT

Copyright © 2024, Versa Networks, Inc.

3. Click + TCP Optimization Profile. In the Create TCP Optimization Profile screen, enter information for the following fields.

Create TCP Optimization Profile

V1

General

Permissions

Name

Description

Max TCP Send Buffer (KB)

4096

Max TCP Receive Buffer (KB)

4096

TCP Congestion Control

Cubic congestion control algorithm

TCP Loss Detection

Duplicate ACKs

TCP Loss Recovery

Pipe algorithm - RFC 6675

☐ TCP Hybrid Slow/Start

☐ Rate Pacing

☐ Auto Rate Pacing Limit

Tags

Press Enter to add

Close

Next



Field	Description
Name	Enter a name for the TCP optimization profile.
Maximum TCP Send Buffer	<p>Enter the maximum size of the TCP send buffer. Setting the buffer size limits TCP memory consumption.</p> <p><i>Range:</i> 64 through 16384 KB <i>Default:</i> 4096 KB</p>
Maximum TCP Received Buffer	<p>Enter the maximum size of the TCP receive buffer. Setting the buffer size limits TCP memory consumption.</p> <p><i>Range:</i> 64 through 16384 KB <i>Default:</i> 4096 KB</p>
TCP Congestion Control	<p>Select the congestion control algorithm to use:</p> <ul style="list-style-type: none"> <li>BBR congestion control algorithm—Bottleneck bandwidth and round-trip propagation time measures both the largest amount of recent bandwidth available to a connection and the connection's smallest recent round-trip delay. BBR then uses these metrics to control how fast it sends data and how much data it allows to be sent at any given time.</li> <li>Cubic congestion control algorithm—An algorithm that uses a cubic function instead of a linear window increase function to improve scalability and stability for fast and long-distance networks. This is the default.</li> <li>New Reno congestion control algorithm—An algorithm that responds to partial acknowledgments.</li> </ul> <p><i>Default:</i> Cubic congestion control algorithm.</p>
TCP Loss Detection	<p>Select the method to use to detect TCP packet loss:</p> <ul style="list-style-type: none"> <li>Duplicate ACKs—Loss detection based on duplicate acknowledgements. Duplicate acknowledgements mean that one or more</li> </ul>

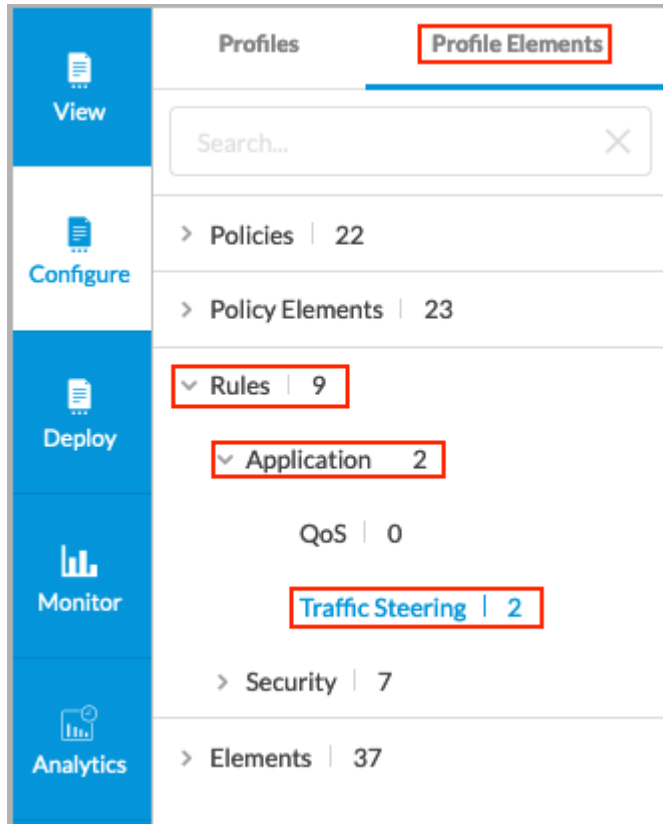
Field	Description
	<p>packets have been lost in a TCP stream and the connection is attempting to recover them. They are a common symptom of packet loss.</p> <ul style="list-style-type: none"> <li>Recent acknowledgment (RACK). RACK uses the notion of time, instead of packet or sequence counts, to detect losses.</li> </ul> <p><i>Default:</i> Duplicate ACKs</p>
TCP Loss Recovery	<p>Select the method to use to recover lost TCP packets:</p> <ul style="list-style-type: none"> <li>Pipe algorithm—Perform TCP loss recovery as described in <a href="#">RFC 6675</a>. This is the default.</li> <li>Proportional rate reduction—Perform TCP loss recovery as described in <a href="#">RFC 6937</a>.</li> </ul> <p><i>Default:</i> Pipe algorithm</p>
TCP Hybrid Slow/Start	<p>Click to enable TCP hybrid slow start. Hybrid slow start maintains the TCP slow-start mechanism, which probes network bandwidth and gradually increases the amount of data transmitted until it finds the network's maximum carrying capacity. It also provides a mechanism to help TCP slow-start to exit without incurring a large number of lost packets. By default, hybrid slow start is disabled.</p> <p><i>Default:</i> Disabled</p>
Rate Pacing	<p>Click to enable rate pacing. Rate pacing injects packets smoothly into the network, thereby avoiding transmission bursts, which could lead to packet loss. By default, rate pacing is disabled.</p> <p><i>Default:</i> Disabled</p>
Automatic Rate-Pacing Limit	<p>Click to enable rate pacing. Rate pacing injects packets smoothly into the network, thereby avoiding transmission bursts, which could lead to packet loss. By default, rate pacing is disabled.</p> <p><i>Default:</i> Disabled</p>
Tags	<p>Enter one or more tags. A tag is an alphanumeric descriptor, with no white spaces or special characters, that you can use to search the objects.</p>

- Click Next, or select the Permissions tab and update the permissions as needed.
- Click Save.

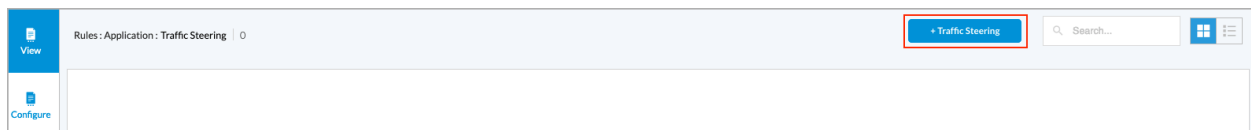
## Reference a TCP Optimization Application Element in a Traffic-Steering Rule

For Releases 11.3.1 and later.

1. Go to Configure > Profile Elements > Rules > Applications > Traffic Steering.



2. Click + Traffic Steering.



3. In the Create Traffic Steering Rule screen, enter a name for the rule.

Create Traffic Steering Rule

General

Criteria

Actions

Permissions

Version 1

Rule Name

Type

Traffic Steering

Enabled

Tags

Press Enter to add

Summary

Variables | 0

No variables present

Close

Next

4. Select the Criteria tab, and the add the desired criteria. For more information, see [Configure Traffic-Steering Policies and Rules](#), above.

Create Traffic Steering Rule

General

Criteria

Actions

Permissions

Rule: TS-rule1

Add Criteria

Cancel

Next

- Click the Actions tab, and then enter information for the following fields.

Create Traffic Steering Rule

General

Criteria

Actions

Permissions

Rule: TS-rule1

Type

Flow

Allow

Type

Log

Events

Never

Forwarding Profile

Name

v1

[ Select Existing ]

Term Type ?

Connection Priority

Path Type

Enterprise

Connection Mode

Name

Any

Add Connection Mode

☐ Avoid ?

Cancel

Add

[https://docs.versa-networks.com/Secure\\_SD-WAN/02\\_Configuration\\_from\\_Concerto/Secure\\_SD-WAN\\_Configuration/Config...](https://docs.versa-networks.com/Secure_SD-WAN/02_Configuration_from_Concerto/Secure_SD-WAN_Configuration/Config...)  
Updated: Wed, 23 Oct 2024 08:03:10 GMT  
Copyright © 2024, Versa Networks, Inc.

54

## Add Term

### TCP Optimization Profile

Mode	Bypass Latency Threshold(msec)
-- Select --	Enter Threshold
LAN Profile	
WAN Profile	

Cancel

Next

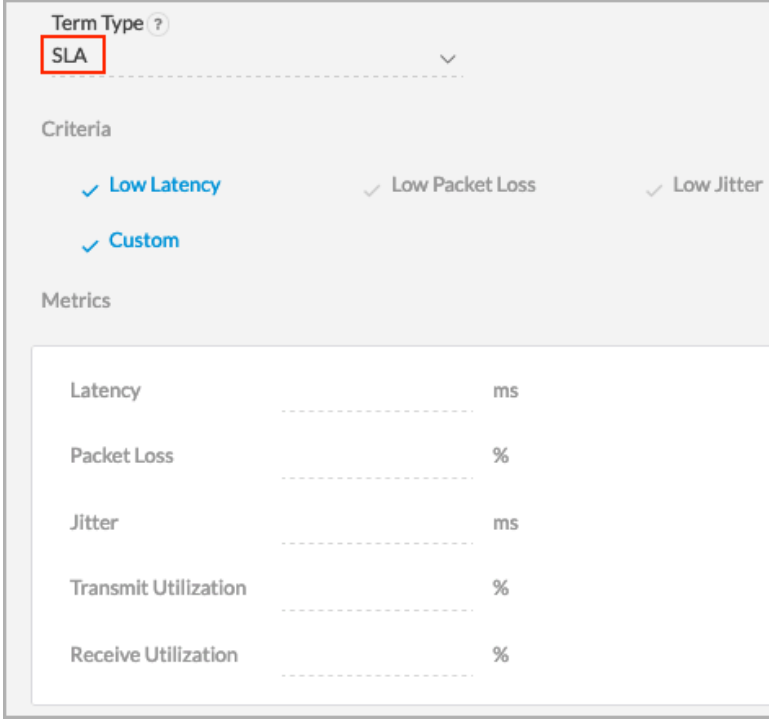


Field	Description
Type Flow	Select the flow type action: <ul style="list-style-type: none"><li>◦ Allow</li><li>◦ Drop. If you select Drop, no other actions can be taken.</li></ul>
Type Log	Under Events, select one of the following: <ul style="list-style-type: none"><li>◦ Never—Do not send logs.</li><li>◦ Priority Change—Send logs only when the traffic priority changes.</li><li>◦ SLA Violated—Send logs only when the traffic violates the SLA.</li></ul>
Forwarding Profile (Group of Fields)	
◦ Name	Enter a name for the forwarding profile.
◦ Term Type	Select a term type: <ul style="list-style-type: none"><li>◦ Connection Priority</li><li>◦ Path Conditioning</li><li>◦ SLA</li></ul>

Field	Description
<ul style="list-style-type: none"> <li>◦ Connection Priority</li> </ul>	<p>Create path priorities based on WAN connection names, types, or remote site names. The WAN connection name and type can be local, remote, or both.</p> <div> <div>Term Type ?</div> <div>Connection Priority</div> <div>Path Type</div> <div>Enterprise</div> <div>Connection Mode</div> <div>Name</div> <div>Add Connection Mode</div> <div><input checked="" type="checkbox"/> Avoid ?</div> </div> <ul style="list-style-type: none"> <li>◦ For Path Type Enterprise: <ul style="list-style-type: none"> <li>▪ Connection Mode <ul style="list-style-type: none"> <li>▪ Name—Select Internet-1 or Internet-2 from the first drop-down list, and then select Any (default), Local, or Remote from the second drop-down list.</li> <li>▪ Type—Select Broadband, MPLS, or LTE, and then select Any (default), Local, or Remote from the second drop-down list.</li> <li>▪ Exit Location—Currently not supported.</li> </ul> </li> </ul> </li> </ul>



Field	Description
	<div> <div> Term Type ?  Connection Priority </div> <div> Path Type  <b>Direct Internet</b> </div> <div> Connection Mode  Name </div> <div> Application Monitor </div> </div> <ul style="list-style-type: none"> <li>For Path Type Direct Internet: <ul style="list-style-type: none"> <li>Name—Select Internet-1 or Internet-2.</li> <li>Application Monitor—Select an application monitor.</li> </ul> </li> <li>Add Connection Mode—Click to add an additional connection mode.</li> <li>Avoid—If Guest is enabled, this VPN does not participate in the SD-WAN topology and only Direct Internet Access is provisioned.</li> </ul>
<ul style="list-style-type: none"> <li>Path Conditioning</li> </ul>	<p>Set level of FEC and packet replication:</p> <ul style="list-style-type: none"> <li>Aggressive</li> <li>Moderate</li> <li>Standard</li> </ul> <div> <div> Term Type ?  <b>Path Conditioning</b> </div> <div> Mode  Select </div> </div>

Field	Description
<ul style="list-style-type: none"> <li>SLA</li> </ul>	<p>SLA—Select the SLA by criteria or based on absolute metrics.</p>  <p>If you select Custom, enter information for the following fields:</p> <ul style="list-style-type: none"> <li>Latency—Enter the amount of latency in milliseconds (ms). <i>Range:</i> 1 through 1000 milliseconds</li> <li>Packet Loss—Enter the percentage of packet loss allowed.</li> <li>Jitter—Enter the amount of jitter allowed, in milliseconds. <i>Range:</i> 1 through 100 milliseconds</li> <li>Transmit Utilization—Enter the percentage of transit traffic.</li> <li>Receive Utilization—Enter the percentage of received traffic.</li> </ul>
Add Term	Click to add additional forwarding profile terms.

Field	Description
TCP Optimization Profile (Group of Fields)	
<ul style="list-style-type: none"> <li>Mode</li> </ul>	<p>Select the TCP optimization mode:</p> <ul style="list-style-type: none"> <li>Auto—Detect which VOS device is closest to the client and which is closest to the server (peer discovery)</li> <li>Bypass—Disable TCP optimizations.</li> <li>Forward proxy—Optimize data being sent from clients to servers. You configure this option on the VOS device closer to the client.</li> <li>Proxy—Configure a single VOS device to be a proxy for the TCP connection instead of performing end-to-end peer discovery.</li> <li>Reverse proxy—Optimizes data being sent from servers to clients. You configure this option on the VOS device closer to the server.</li> <li>Splice—Split the TCP connection locally after an application or URL category is identified or when the VOS device receives the first data packet after the three-way handshake completes.</li> </ul>
<ul style="list-style-type: none"> <li>Bypass Latency Threshold</li> </ul>	<p>If you select TCP Auto or Splice mode, enter how much latency must be measured before TCP optimizations begin.</p> <p><i>Range:</i> 0 through 60000 milliseconds  <i>Default:</i> 10 milliseconds</p>
<ul style="list-style-type: none"> <li>LAN Profile</li> </ul>	<p>Select a LAN profile.</p> <p>For proxy mode, you must configure a TCP profile.</p> <p>Note that you can select the same TCP profile for LAN profiles and WAN profiles.</p> <p>If you do not select TCP profiles, a system default LAN profile is applied that uses the cubic congestion control algorithm and duplicate ACK loss detection.</p>
<ul style="list-style-type: none"> <li>WAN Profile</li> </ul>	<p>Select a WAN profile.</p>

Field	Description
	<p>For proxy mode, you must configure a TCP profile.</p> <p>Note that you can select the same TCP profile for WAN profiles and LAN profiles.</p> <p>If you do not select TCP profiles, a system default WAN profile is applied that uses the BBR congestion control algorithm and RACK loss detection.</p>

6. Click Next, or select the Permissions tab and update the permissions as desired.
7. Click Save.

---

## Configure Custom SD-WAN Security Profile Elements

*For Releases 12.1.1 and later.*

You can configure two types of custom SD-WAN profile elements:

- Security actions—Allows you to choose the type of security action (such as cloud access security broker (CASB), decryption, and DNS) and the action to take on that type.
- URL categories—Allows you to create a custom URL category by specifying a URL pattern and reputation, a URL string and reputation, and by uploading files in .csv format.

Note: You can configure URL categories and security actions as part of both SSE and SD-WAN services in Concerto. The configurations are common between the two services. If you configure URL categories and security actions for an SSE service, the same configuration appears in the SD-WAN service, and vice versa.

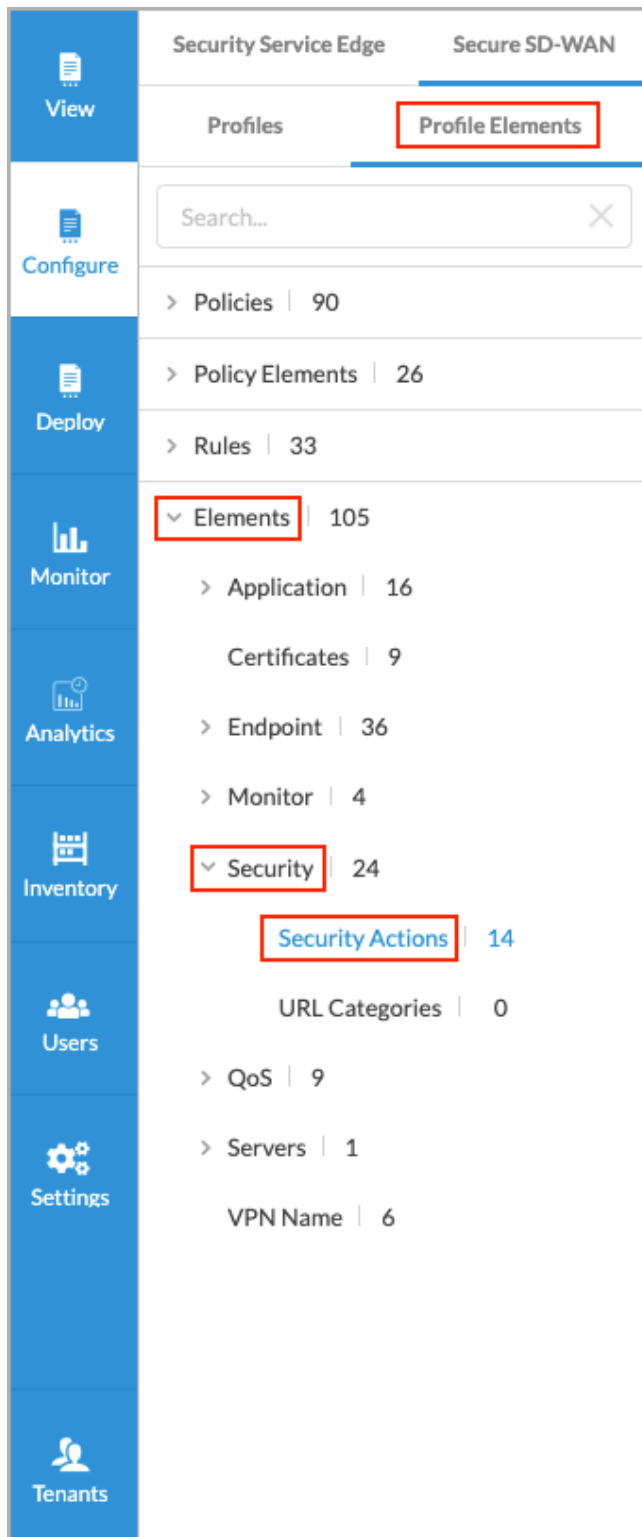
You can then use the security actions and URL categories when you configure security policies under Configure > Profile Elements > Policies > Security.

---

## Configure Security Actions

To configure a security actions profile element:

1. Go to Configure > Profile Elements > Elements > Security > Security Actions.



The following screen displays.

View

Configure

Deploy

Monitor

Analytics

Inventory

Users

Settings

Configure > Profile Elements > Elements > Security Actions

Security Actions

Below are all the Security Actions

Security Actions

Search

+ Add Security Actions

Clone

Delete

Refresh

Select Columns

<input type="checkbox"/>	NAME	SECURITY ACTION TYPE	ACTION	MESSAGE	EXPIRATION TIME (MIN)
<input type="checkbox"/>	customCASBAction1	CASB	Allow	-	-
<input type="checkbox"/>	dns-type	DNS	Allow	-	-
<input type="checkbox"/>	IP-Rep	IP Reputation	Reset Client and Server	-	-
<input type="checkbox"/>	IPS-Action	Intrusion Prevention System (IPS)	Drop Session	-	-
<input type="checkbox"/>	IPS-Custom	Intrusion Prevention System (IPS)	Allow	-	-
<input type="checkbox"/>	My-Action-1	All	Reset Client	-	10 mins
<input type="checkbox"/>	My-IP-Action1	IP Reputation	Inform	-	-
<input type="checkbox"/>	Olive-action	IP Reputation	Drop Session	-	-
<input type="checkbox"/>	Olive-iprep	Decryption	Allow	-	-
<input type="checkbox"/>	Sink-Hole	All	Sinkhole	-	-

Showing 1-10 of 14 results

10 Rows per Page

Go to page 1 < > Previous 1 2 Next >

- Click + Add Security Actions. The Add Security Actions screen displays.
- Select Step 1, Define Security Action, and then enter information for the following fields.

Configure > Profile Elements > Elements > Security Actions

Add Security Actions

1 DEFINE SECURITY ACTION

Security Action Type

All

Action

Allow

Decrypt Bypass

This disables SSL encryption for matching traffic, to allow you to define websites that are not subject to decryption.

Log Captive Portal Actions

Expiration Time

Enter Value

Min

Message

Enter message to display on the captive portal page

Cancel

Next

2 NAME, DESCRIPTION & TAGS

Field	Description
Security Action Type	<div>Select a security action type:</div> <ul style="list-style-type: none"> <li>All</li> <li>CASB</li> <li>Decryption</li> <li>DNS</li> <li>Intrusion Prevention System (IPS)</li> <li>IP Filtering</li> </ul>

[https://docs.versa-networks.com/Secure\\_SD-WAN/02\\_Configuration\\_from\\_Concerto/Secure\\_SD-WAN\\_Configuration/Config...](https://docs.versa-networks.com/Secure_SD-WAN/02_Configuration_from_Concerto/Secure_SD-WAN_Configuration/Config...)  
Updated: Wed, 23 Oct 2024 08:03:10 GMT  
Copyright © 2024, Versa Networks, Inc.

62

Field	Description
	<ul style="list-style-type: none"> <li>◦ URL Filtering (URLF)</li> </ul>
Action	<p>Select an action:</p> <ul style="list-style-type: none"> <li>◦ Allow—Forward the current packet without generating an entry in the log.</li> <li>◦ Drop Packet—Browser waits for a response from the server and then drops the packets.</li> <li>◦ Drop Sessions—Browser waits for a response from the server and then drops the session.</li> <li>◦ Reset Client—TCP Reset packet is sent to the client and the browser displays an error message indicating that the connection has been reset.</li> <li>◦ Reset Client and Server—TCP Reset packet is sent to the server. The browser waits for a response from the server and then drops the session.</li> <li>◦ Block—Present an alert page to the user and block the user from continuing, in case of HTTP/HTTPS.</li> <li>◦ Inform—Browser presents an information page that allows the user to continue with the operation by clicking OK.</li> <li>◦ Ask—Browser presents an information page that allows the user to either cancel the operation by clicking Cancel, or continue with the operation by clicking OK.</li> <li>◦ Justify—Browser presents an information page that allows the user to either cancel the operation by clicking Cancel, or continue with the operation after entering a justification message and clicking OK.</li> <li>◦ Override—Browser prompts the user to enter a PIN (4 to 6 digits).</li> <li>◦ Custom Redirection—Browser redirects the user to the URL configured in the Redirection URL field.</li> <li>◦ Sinkhole—A DNS sinkhole spoofs DNS servers to prevent the resolution of the host names associated with URLs. And returns a false IP address to the URL, thus blocking a DNS sinkhole.</li> </ul>
Decrypt Bypass	(For all security types except CASB.) Click the slider

Field	Description
	bar to disable SSL encryption for matching traffic, to allow you to define web sites that are not subject to decryption. SSL encryption for matching traffic is enabled by default.
Log Captive Portal Actions	(For all security types except CASB.) Click the slider bar to enable the logging of captive portal actions. Logging of captive portal actions is disabled by default.
Expiration Time	(For the security types IP Reputation and URL Filtering.) Enter how often to redirect a user to the URL, in minutes.
Message	(For the security types IP Reputation and URL Filtering.) Enter a message to display on the captive portal page.

4. Click Next to go to Step 2, Name, Description, and Tags, and then enter information for the following fields.

Field	Description
Name (Required)	Enter a name for the security action.
Description	Enter a text description.
Tags	Enter one or more tags. A tag is an alphanumeric text descriptor with no for searching tunnels.

5. Click Save.

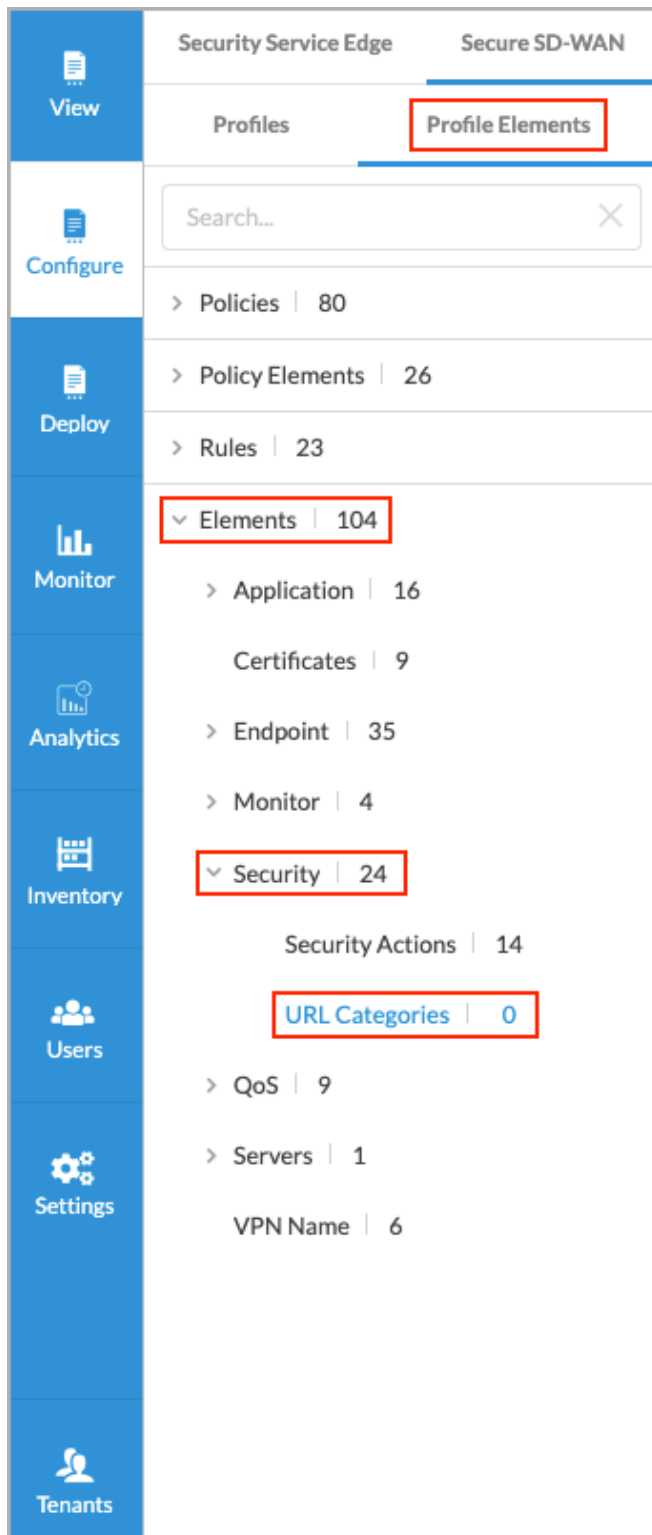


---

## Configure URL Categories

To configure a URL categories profile element:

1. Go to Configure > Profile Elements > Elements > Security > URL Categories.



The following screen displays.

Configure > Profile Elements > Elements > URL Categories

### URL Categories

Below are all the URL Categories

+ Add URL Categories
Clone
Delete
Refresh
Select Columns

NAME	URL PATTERN		URL STRING	
	PATTERN	PATTERN REPUTATION	STRING	STRING REPUTATION
No Data				

- Click + Add URL Categories.
- In the Add URL Categories screen, select Step 1, URL Patterns, and then enter information for the following fields.

Configure > Profile Elements > Elements > URL Categories

### Add URL Categories

1 URL PATTERNS

Enter a RegEx pattern and reputation to match the URLs.

Patterns ⓘ

Example: \*.versa-networks\*

Reputation

Select

Cancel

Next

2 URL STRINGS

+

3 URL FILES

+

4 ENTER NAME, DESCRIPTIONS & TAGS

+

Field	Description
Patterns	Enter a URL pattern to match and group the URLs. You can include regex pattern <code>www.versa-networks.com</code> , or you can use a wildcard such as <code>*.versa-r</code> regex pattern, escape it by preceding it with a backslash.
Reputation	Select a predefined reputation, and then assign it to the URL match pattern.

- Click Next. In Step 2, URL Strings, enter information for the following fields.

Configure > Profile Elements > Elements > URL Categories

**Add URL Categories**

1

URL PATTERNS

+

2

URL STRINGS

-

Enter a URL string and reputation to match the URLs.

String

Enter a URL string

Example: www.versa-networks.com/

Reputation

Select

Cancel Next

3

URL FILES

+

4

ENTER NAME, DESCRIPTIONS & TAGS

+

Field	Description
String	Enter a URL string to match the URL, for example, www.versa-networks.com
Reputation	Select a predefined reputation, and then assign it to the URL string.

- Click Next. In Step 3, URL Files, enter information for the following fields.

Configure > Profile Elements > Elements > URL Categories

**Add URL Categories**

1

URL PATTERNS

+

2

URL STRINGS

+

3

URL FILES

-

Select URL file and reputation to match the URLs.

URL Files

Select

Add new file

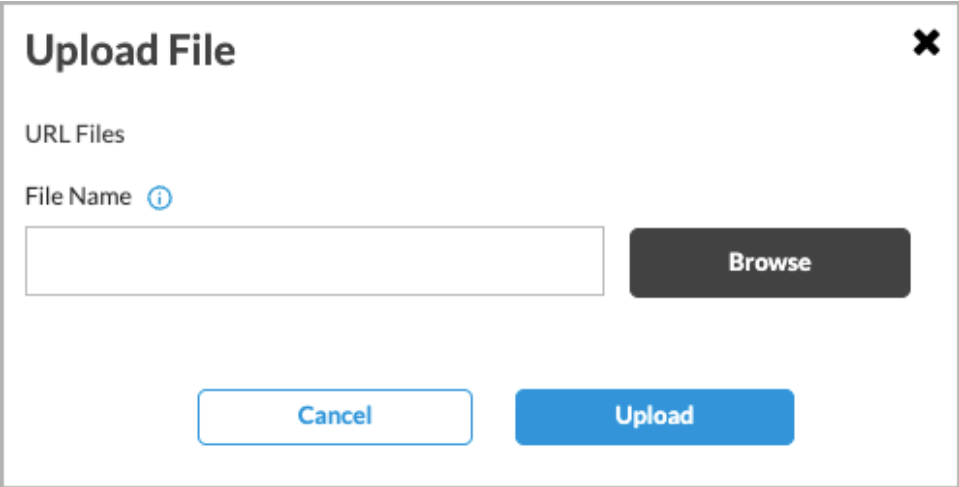
Cancel Next

4

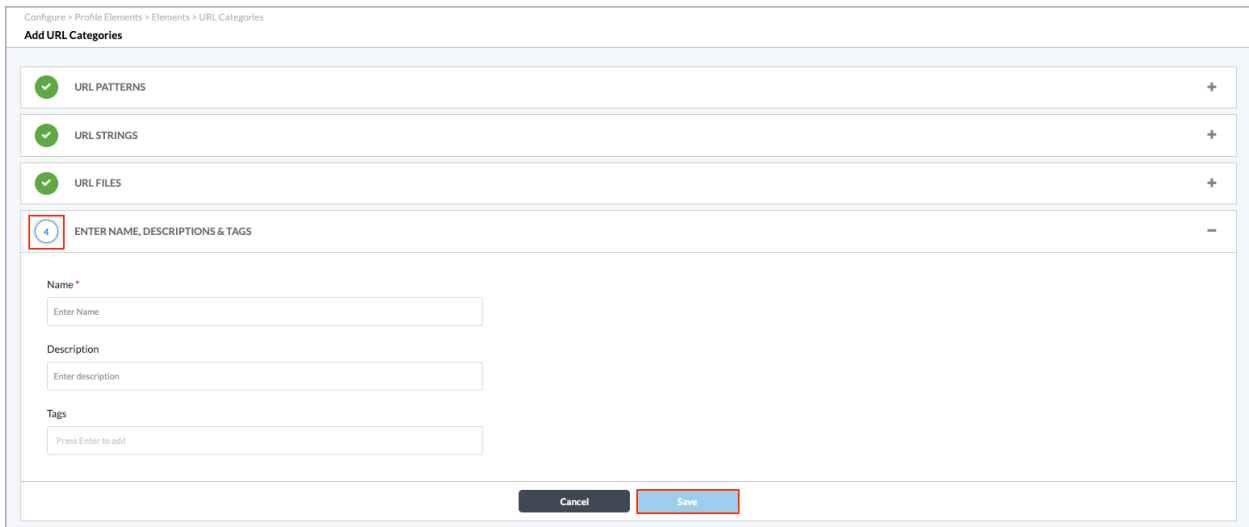
ENTER NAME, DESCRIPTIONS & TAGS

+

Field	Description
URL Files	Select a URL file.
Add New File	Click to add a new URL file. The Upload File popup window displays.

Field	Description
	 <ol style="list-style-type: none"> <li>1. Enter the name of the file to upload or click Browse to select the file. The file</li> <li>2. Click Upload.</li> </ol>

6. Click Next. In Step 4, Enter Name, Description, and Tags, enter information for the following fields.



Field	Description
Name (Required)	Enter a name for the URL category. This name is displayed in the category list when the match criteria for URL categories in policy rules.
Description	Enter a text description for the URL category.
Tags	Enter one or more tags for the URL category. A tag is an alphanumeric text description.

[https://docs.versa-networks.com/Secure\\_SD-WAN/02\\_Configuration\\_from\\_Concerto/Secure\\_SD-WAN\\_Configuration/Config...](https://docs.versa-networks.com/Secure_SD-WAN/02_Configuration_from_Concerto/Secure_SD-WAN_Configuration/Config...)

Updated: Wed, 23 Oct 2024 08:03:10 GMT

Copyright © 2024, Versa Networks, Inc.

Field	Description
	that you use for searching URL categories.

7. Click Save.

---

## Supported Software Information

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

- Release 11.1.1 adds support for the Custom Application and Application Group application elements.
- Release 11.2.1 adds support for multitenancy configuration in Default-Active-Active and Default-Basic-MP basic master profiles, and for a new default basic master subtenant profile, Default-Basic-MP-Sub-Tenant.
- Release 11.3.1 adds support for the TCP optimizations application element and the ability to add service templates to individual devices in a redundant master profile.
- Release 11.4.1 adds support for a configuration wizard for configuring access control policies and rules; the creation of CGNAT rules for subtenants in addition to provider tenants in multitenant master profiles; custom applications support family, subfamily, risk, productivity and precedence; enhanced forwarding profiles and IP SLA profiles.
- Release 12.1.1 adds support for the custom SD-WAN security profile elements Security Actions and URL Categories.

---

## Additional Information

[Configuration Hierarchies](#)

[Configure Profiles](#)

[Configure SaaS Application Monitors](#)

[Configure TCP Optimizations](#)