

---

## Configure SD-WAN TLS Decryption in Concerto

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

Transport Layer Security (TLS) is a widely-adopted security protocol that provides privacy and data security for communications over the internet. A primary use case for TLS is encrypting the communications between web applications and servers, such as web browsers loading a website. TLS can also be used to encrypt other communications, such as email, messaging, and voice over IP (VoIP).

TLS decryption uses two mechanisms to secure traffic:

- Handshake protocol—Authenticates the client and server devices at both ends of a secure communications channel, negotiates cryptographic modes and parameters, and establishes shared keying material to negotiate the security parameters of a connection. The handshake protocol then sends messages to the TLS record protocol.
- Record protocol—Takes transmitted messages from the handshake protocol, fragments the data into manageable blocks, protects the records, and transmits the result. The data received is verified, decrypted, reassembled, and then delivered to higher-level clients.

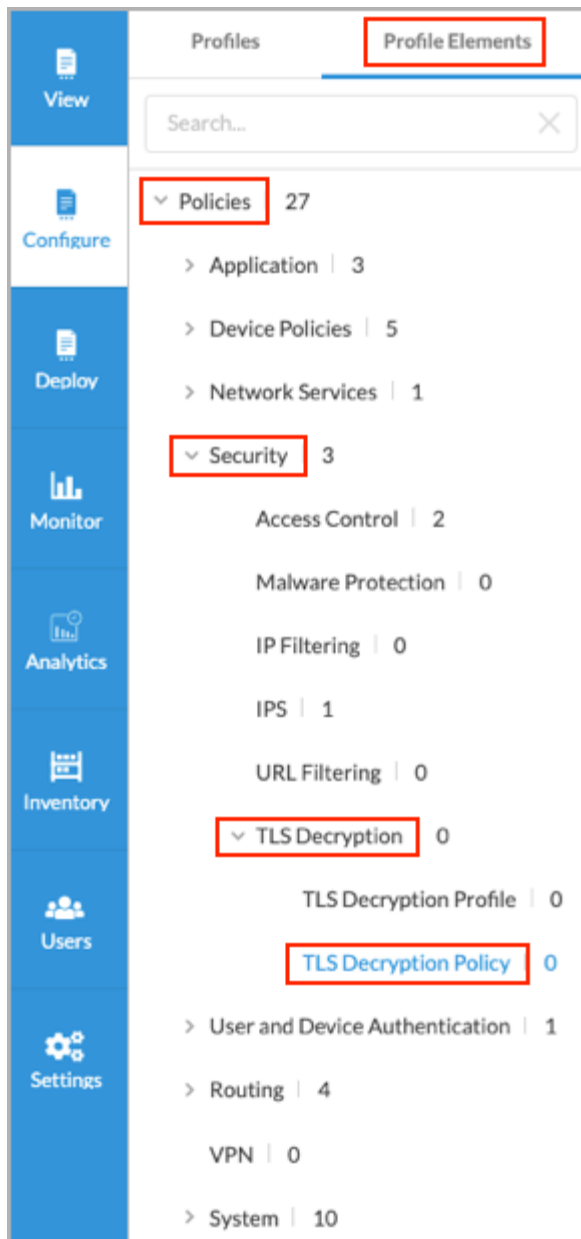
To configure SD-WAN TLS decryption, you create TLS decryption policies and profiles. Decryption enforces security policies on encrypted traffic to help prevent malicious content from entering the network and to protect sensitive data disguised as encrypted traffic from leaving the network. You can configure a decryption profile with SSL inspection and policy enforcement information. The following sections describe the procedures to configure the decryption policies and profiles.

---

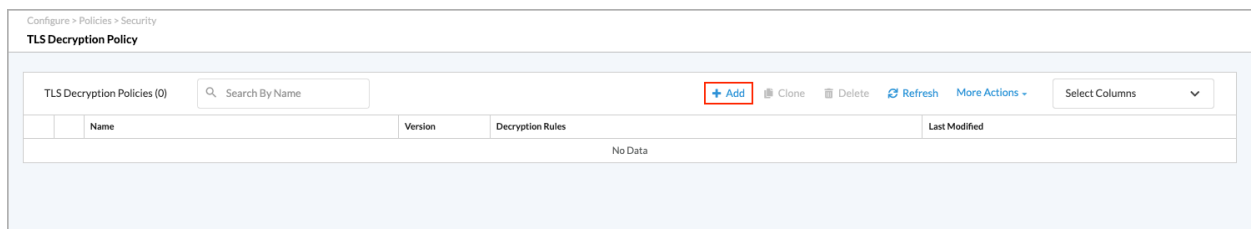
## Configure SD-WAN TLS Decryption Policies

To configure SD-WAN TLS decryption policies:

1. Go to Configure > Profile Elements > Policies > Security > TLS Decryption > TLS Decryption Policy.



The following screen displays.



2. Click + Add. The Add Decryption Policy screen displays.

[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 08:02:43 GMT

Copyright © 2024, Versa Networks, Inc.

**Add TLS Decryption Policy**

1 **Decryption Rules** 2 Permissions 3 Review & Submit

Add one or more Decryption rules to the TLS Decryption policy.

Decryption Rules (0) + Add + Reorder Delete Select Columns

Name	Order	Decryption Profile	URL Categories & Reputations	Users & Groups	Sources	Destinations	Services
No Data							

Cancel Skip to Review Next

- In Step 1, Decryption Rules, click the + Add icon. The Add TLS Decryption Policy Rule screen displays. In Step 1, Decryption Enforcement, to select the type of policy to create, enter information for the following fields.

**Add TLS Decryption Policy Rule**

1 **Decryption Enforcement** 2 URL Categories & Reputations 3 Users & Groups 4 Source & Destination Traffic 5 Service & DSCP 6 Permissions 7 Review & Submit

Select the type of policy that you would like to create. You can customize either configuration you'd like to enforce.

**Decrypt and Inspect the Traffic** ✓

Normally, encrypted traffic is not blocked. Decryption enforces security policies on encrypted traffic to help prevent malicious content from entering the network and to protect sensitive data disguised as encrypted traffic from leaving the network.

Use the following decryption profile

▼

URL Filtering Action Override(optional)

-- Select --

**Do Not Decrypt** ✓

This option does not decrypt and enforce security rules on traffic because the traffic remains encrypted. This option should be used on sites, applications or services you need for your organization.

☐ Do not decrypt but do inspect the traffic

Encryption does not necessarily mean that content is safe. Gain visibility into the hidden traffic within your network and identify, classify, and inspect the packets for threats. Know what is being intentionally or accidentally sent outside of your organization.

Select Profile

☐ Do not decrypt and do not inspect the traffic

Allow traffic from certain trusted sites to go un-inspected. Keep in mind, this can be risky because webpages are not static.

Cancel Skip to Review Next

Field	Description
Decrypt and Inspect the Traffic (Group of Fields)	Select to decrypt and inspect all traffic. Decryption enfor

[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 08:02:43 GMT

Copyright © 2024, Versa Networks, Inc.

Field	Description
	entering the network and to protect sensitive data disgu
<ul style="list-style-type: none"> <li>Use the following decryption profile</li> </ul>	Select a TLS decryption profile to use in the rule. To cre
<ul style="list-style-type: none"> <li>URL Filtering Action Override</li> </ul>	Select a URL-filtering profile to bypass the decryption a
Do Not Decrypt (Group of Fields)	Select to bypass decryption of the traffic. Selecting the l the traffic remains encrypted. This option should be use
<ul style="list-style-type: none"> <li>Do not decrypt but do inspect the traffic</li> </ul>	Do not decrypt the traffic but inspect the traffic to identifi
<ul style="list-style-type: none"> <li>Do not decrypt and do not inspect the traffic</li> </ul>	Click to allow traffic from certain trusted sites to pass wi

4. Click Next to go to Step 2, URL Categories and Reputations. By default, all URL categories and reputations are included in the match criteria. To specify the URL categories and reputations to which the rule applies, enter the following information.

- a. Select one or more URL categories in the URL Categories field to specify the URL categories to which the rule applies.
  - b. Select one or more reputations in the Reputations field to specify the reputations to which the rule applies.
5. Click Next to go to Step 3, Users & Groups. The User Groups tab displays a list of existing user groups, if any. By default, all users and groups are included. You can specify the specific users or groups to be included.

**Add TLS Decryption Policy Rule**

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 Access Control Rule for the following matched users or user groups

Select Users & Groups Profile

**User Groups** Users

Search for User Groups

User Groups (0) [+ Add New User Group](#)

Name	Distinguished Name (DN)
------	-------------------------

Cancel Back Skip to Review Next

6. On the User Groups tab, select one or more existing user groups, or click + Add New User Group to add a new user group.
  - a. If you click + Add New User Group, the following popup window displays.

**Add User Group**

User Group\*

Distinguished Name (DN)\*

Cancel Add

- b. Enter a user group name and a distinguished name (DN).
  - c. Click Add.
7. Select the Users tab.

**Add TLS Decryption Policy Rule**

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 Access Control Rule for the following matched users or user groups

Select Users & Groups Profile

User Groups **Users**

Search for Users

Users 0 **+ Add New User**

User Name	Work Email
-----------	------------

Cancel Back Skip to Review Next

8. Select one or more existing users, or click + Add New User to add a new user.
  - a. If you click + Add New User, the following popup window displays.


**Add User**

User Name \*


Work Email \*

Cancel Add

- b. Enter a user name and a work email address.
  - c. Click Add.
9. Click Next to go to Step 4, Source & Destination Traffic. The following screen displays. By default, all source and destination traffic is included. You can specify which source and destination traffic to include.

10. 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 11.
  - 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 11.
11. On the Source Address tab, 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.. You can click + Add Variable to create a variable for the source address. Enter a name for the variable, click the  Plus icon, then click Add. You can add multiple variables before clicking the Add button.

You can also enter for the fields IP Address or IP Range, IP Subnet, or IP Wildcard as part of the match criteria. You can click + Add Variable to create variables for these values, and you can add multiple variables for each one.

- 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, the click Add.

**Add Variable**

IPv4 Address \$ - +

IPv4 Address  
IPv4 Range  
IPv6 Address

Cancel Add

- To add a variable for the IP subnet, select IP Subnet or IPv6 Subnet from the drop-down list, click the + Plus icon, then click Add.

**Add Variable**

IP Subnet \$ - +

IP Subnet  
IPv6 Subnet

Cancel Add

- To add a variable for the IP wildcard, enter a name for the variable, click the + Plus icon, then click Add.

**Add Variable**

\$ - +

Cancel Add

12. Click the Destination Address tab.

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

- To specify destination addresses to include in the match criteria, continue to Step 14 to select addresses.



- To specify destination addresses to exclude from the match criteria, select Negate Destination Address to match all destination addresses except the addresses that you specify, and then continue to Step 14 to select addresses.
- 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 11.
  - Select the Source Zone and Sites tab, and then enter information for the following fields.

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 <a href="#">+ Add Variable</a>	Source Sites <a href="#">+ Add Variable</a>	<input type="text" value="Search or select from list"/>	<input type="text" value="Search or select from list"/>

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

- Select the Destination Zone and Sites tab, and then enter the information for the destination zone and destination site. The fields are the same as for the Source Zone and Sites shown above.
- Click Next to go to Step 5, Service & Differentiated Services Code Point (DSCP). By default, all services, service groups, and DSCP's are included in the match criteria.

**Add TLS Decryption Policy Rule**

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**

Search or select from list

Services(User Defined: 2 | Predefined: 741)

Name	Type	Protocol	Source Port	Destination Port	Source or Destination Port
<input type="checkbox"/> n2	User Defined	18			
<input type="checkbox"/> nn	User Defined	AH			
<input type="checkbox"/> 3com-amp3	Predefined	TCP	any	629	
<input type="checkbox"/> 3com-tsmux	Predefined	UDP	any	629	
<input type="checkbox"/> 914c-g	Predefined	TCP	any	106	
<input type="checkbox"/> 914c-g	Predefined	UDP	any	106	
<input type="checkbox"/> 914c-g	Predefined	TCP	any	211	
<input type="checkbox"/> 914c-g	Predefined	UDP	any	211	
<input type="checkbox"/> 9pfs	Predefined	TCP	any	564	

Cancel Back Skip to Review Next

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

- In the search box under Services, enter the service name.
- Click All Services and one of the following categories to filter using the drop-down list:
  - Predefined
  - User Defined

19. Select the Service Groups tab, then select the user-defined or predefined service groups to which to apply security access control rules. Click the > Toggle Row Expand icon next to the service group name to view the details for each service group.

**Services**

SG\_00R ng04 Search or select from list

**Service Groups**

	Name	User Defined	Predefined
<input checked="" type="checkbox"/> >	ng04	1	
<input checked="" type="checkbox"/> >	SG_00R	1	
<input type="checkbox"/> >	ng003	2	
<input type="checkbox"/> >	newSG_01	2	
<input type="checkbox"/> >	My-Group	2	2
<input type="checkbox"/> >	SG01	4	

20. Select one or more service groups to add to the rule. The service groups are added to the Services list.

21. Select the DSCP tab. All DSCP decimal values are included by default. You can specify which DSCP decimal values to include. The range is from 0 through 63.

Services Service Groups **DSCP**

### DSCP Decimal

Select one or more DSCP decimal to apply the access control 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

22. Click Next to go to Step 6, Permissions. To revise the permissions for a role, select Edit, Hide, or Read in the Permissions column.

Add TLS Decryption Policy Rule

Decryption Enforcement URL Categories & Reputations Users & Groups Source & Destination Traffic Service & DSCP **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

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

**Add TLS Decryption Policy Rule**

Action: Decryption Enforcement URL Categories & Reputations Users & Groups Source & Destination Traffic Service & DSCP Permissions **Review & Submit**

Review your configurations. Before submitting, review and edit any steps of your configuration below.

**General**

Name

Description

Tags

Press Enter to add

**Schedule**

Select a schedule to set the time and frequency at which the rule is in effect.

Search or select from list

☒ Rule Enabled ☐ Logging Disabled


**Decryption Enforcement** Edit

Rule Type: ☐ Do Not Decrypt ☒ Do Not Inspect the Traffic

Inspect Traffic Enabled ☐ Do not Inspect the Traffic ☒

Cancel Back Save

Field	Description
General (Group of Fields)	
◦ Name	Enter a name or the rule.
◦ Description	(Optional) Enter a description for the rule.
◦ Tags	(Optional) Enter one or more tags. A tag is an alphanumeric text descriptor with no s tags are used for searching the objects.
◦ 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.
◦ Logging Disabled	Click to the slider bar to enable logging for the rule. By default, logging is disabled.

24. Review the selected settings. Click the  Edit icon to change a setting, if needed.
25. Click Save to save the rule. The Add TLS Decryption Policy screen displays with the new rule listed.

Add TLS Decryption Policy

1 2 3  
Decryption Rules Permissions Review & Submit

Add one or more Decryption rules to the TLS Decryption policy.

Decryption Rule [1] +Add +Reorder Delete Select Columns

	Name	Order	Decryption Profile	URL Categories & Reputations	Users & Groups	Sources	Destinations	Services
<input type="checkbox"/>	TLS-decryption-R1	1	Do not decrypt and do not inspect the traffic	> URL Categories > Reputations	All Users	All Sources	All Destinations	All layer 4 services

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

Cancel Skip to Review Next

26. Click Next to go to Step 2, Permissions.

Add TLS Decryption Policy

1 2 3  
Decryption Rules 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

27. To revise the permissions for a role, select Edit, Hide, or Read in the Permissions column.

28. Click Next to go to Step 3, Review & Submit, then enter the following information.

Add TLS Decryption Policy

Decryption Rules Permissions **Review & Submit**

Review your configurations. Before submitting, review and edit any steps of your configuration below.

**General**

Name Description

Tags

Press Enter to add

**Decryption Rules** [Edit](#)

Decryption Rule (1)

Name	Order	Decryption Profile	URL Categories & Reputations	Users & Groups	Sources	Destinations	Services
TLS-decryption-R1	1	Do not decrypt and do not inspect the traffic	<a href="#">URL Categories</a> <a href="#">Reputations</a>	All Users	All Sources	All Destinations	All layer 4 services

Showing 1-1 of 1 results 10 Rows per Page

Go to page 1 < Previous 1 Next >

**Permissions** [Edit](#)

Cancel Back Save

Field	Description
General (Group of Fields)	
◦ Name	Enter a name or the rule.
◦ Description	(Optional) Enter a description for the rule.
◦ Tags	(Optional) Enter one or more tags. A tag is an alphanumeric text descriptor with no spaces. Tags are used for searching the objects.

29. Review the selected settings. Click the [Edit](#) icon to change a setting, as needed.
30. Click Save to save the new TLS policy.

## Configure SD-WAN TLS Decryption Profiles

You can configure two types of SD-WAN TLS decryption profiles:

- Decryption Profile—Applies both decryption and inspection protocols that you can associate with decryption rules.
- Inspection Profile—Applies only inspection protocols that you can associate with decryption rules.

To configure SD-WAN TLS decryption profiles:

1. Go to Configure > Profile Elements > Policies > Security > TLS Decryption > TLS Decryption Profile.

[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 08:02:43 GMT

Copyright © 2024, Versa Networks, Inc.




The following screen displays with Decryption Profile selected by default.

Add TLS Decryption Profile

1 Profile Type 2 Certificate Setup 3 Inspection Options 4 Decryption Options 5 Permissions 6 Review & Submit

Select which mode to use to check the availability of the server. Decryption enforces security policies on encrypted traffic to help prevent malicious content from entering the network and to protect sensitive data disguised as encrypted traffic from leaving the network. You can configure a decryption profile with SSL inspection and policy enforcement information. This section will guide you through the process of configuring the decryption profiles.



**Decryption Profile**

This profile applies both decryption and inspection protocols that you can associate with your decryption rules.



**Inspection Profile**

This profile applies only inspection protocols that you can associate with your decryption rules.

Cancel Skip to Review Next

2. Select the type of decryption profile to configure. The options are:

- Decryption Profile
- Inspection Profile

Note: If you select Inspection Profile, go to [Step 7](#) below. The workflow steps for an inspection profile do not include the Certification Setup or Decryption Profile steps.

Add TLS Decryption Profile

1 Profile Type 2 Inspection Options 3 Permissions 4 Review & Submit

3. Click Next to go to Step 2, Certificate Setup (for a decryption profile only).




Add TLS Decryption Profile


Profile Type **2** Certificate Setup Inspection Options Decryption Options Permissions Review & Submit

By default, we've selected a certificate authority for you. A certificate authority (CA) is an entity that issues digital certificates to verify the ownership of a public key. Only one certificate can be selected. If you prefer, you can choose another CA to use.


Previously Uploaded Certificates

--Select--  [+ Add New](#)

Cancel Back Skip to Review Next


4. Select a previously-uploaded certificate from the drop-down list. The certificate information displays. Click the  Download icon to download the certificate.

Previously Uploaded Certificates

ACME  [+ Add New](#)

**Details**

Name: ACME  
 File Name: ACME.zip  
 Key: ACME.key  
 Certificate: ACME.crt  
 Issued To: ACME  
 Issued By: Versa Networks Inc.  
 Validity: 2022-01-12 07:31:54 to 2027-01-11 07:31:54

 [Download Certificate](#)

5. Click + Add New to upload a new CA certificate. In the Add CA Certificate popup window, enter information for the following fields.

**Note:** The file to be uploaded must be in .zip format. The .zip file must consist of two files: a key file and a certificate file. The key file must have a .key extension. There is no restriction on the extension of the certificate file.

Add CA Certificate

Certificate Type
CA Certificate

The file to be uploaded needs to be in .zip format. They will consist of 2 files: a key and a certificate. The key file needs to have .key extension. There is no restriction on the extension of the certificate file.

Certificate Name \*

CA-Chain Name\*

Select

Pass-Phrase

Upload File

Cancel

Add

Field	Description
Certificate Name (Required)	Enter a name for the certificate.
CA-Chain Name (Required)	Select a CA chain.
Pass-Phrase	Enter a pass phrase of 1 through 15 characters.
Upload File	Click to upload the .zip file.

- Click Add to add the CA certificate.
- Click Next to go to Step 3, Inspection Options, then enter information for the following fields. Note that if you are configuring an Inspection Profile, this step is Step 2, Inspection Options.

TLS inspection is the process of intercepting and reviewing SSL or TLS encrypted internet communication between the client and the server. The inspection of SSL or TLS encrypted traffic has become critically important because the vast majority of internet traffic is SSL or TLS encrypted, including malicious traffic.



Based on the most common secure enterprise settings, we've chosen the inspection options, below. If you prefer, you can customize which inspection options you'd like to enable.

TLS inspection is the process of intercepting and reviewing SSL or TLS encrypted internet communication between the client and the server. The inspection of SSL or TLS encrypted traffic has become critically important because the vast majority of internet traffic is SSL or TLS encrypted, including malicious traffic.

[More Information](#) 

## t ⓘ

Select the minimum and maximum version of TLS that is supported. When you select a version that is not TLS 1.3, select one or more key exchange algorithms for the SSL connection.



This is the Internet protocol used by web browsers to determine the revocation status of SSL/TLS certificates supplied by HTTPS websites.

Verify with OCSP ⓘ

Enable server certificate verification using the Online Certificate Status Protocol (OCSP).

Block Unknown Certificates ⓘ

Block SSL sessions whose certificate status is unknown.

Response timeout(seconds) for an OCSP request

**S** ⓘ

Choose what actions should occur for the following server certificate checks. When the certificate expires, do the following:

When the certificate is received from an untrusted issuer, do the following:

Choose whether to restrict the certificate key usage extensions to either digital signature or key encipherment.

☐ Restrict Certificate Extension

**S** ⓘ

Choose what actions should occur for the following SSL or TLS protocol checks.

When the negotiated SSL or TLS protocol between the Client and Server uses an unsupported key length, do the following:

Minimum Supported RSA Key Length

Enter a value of 512 bits or higher

When the negotiated SSL or TLS protocol between the Client and Server uses an unsupported cipher, do the following:

When the negotiated SSL or TLS protocol between the Client and Server uses an unsupported protocol version, do the following:

Next

Field	Description
Transport Layer Security (TLS) Version Support	Use the slider to select the minimum version supported. Default is 1.3, select one or both key exchange methods.
Certificate Validation (Group of Fields)	
◦ Verify with OCSP	Select to use the Online Certificate Status Protocol (OCSP) to verify certificates.
◦ Block Unknown Certificates	Select to block SSL sessions whose certificates are not in the trusted certificate store.
◦ Response timeout (seconds) for an OCSP request	Enter how long, in seconds, before a timeout occurs. <i>Default: 5 seconds</i> <i>Range: 1 to 255 seconds</i>
Server Certificate Actions (Group of Fields)	
◦ When the certificate expires, do the following:	Select a predefined or user-defined action. <ul style="list-style-type: none"> <li>◦ Alert</li> <li>◦ Allow</li> <li>◦ Drop Packet</li> <li>◦ Drop Session</li> <li>◦ Reject</li> </ul>
◦ When the certificate is received from an untrusted issuer, do the following	Select an action to take when a certificate is received from an untrusted issuer. The predefined actions are: <ul style="list-style-type: none"> <li>◦ Alert</li> <li>◦ Allow</li> <li>◦ Drop Packet</li> <li>◦ Drop Session</li> <li>◦ Reject</li> </ul>
◦ Restrict Certificate Extension	Click to choose whether to restrict the certificate extension.
SSL or TLS Protocol Checks (Group of Fields)	
◦ When the negotiated SSL or TLS protocol between the client and server uses	Select a predefined or user-defined action.

Field	Description
an unsupported key length, do the following:	<p>key length.</p> <p>The predefined actions are:</p> <ul style="list-style-type: none"> <li>◦ Alert</li> <li>◦ Allow</li> <li>◦ Drop Packet</li> <li>◦ Drop Session</li> <li>◦ Reject</li> </ul>
◦ Minimum Supported RSA Key Length	<p>Enter the minimum supported RSA key length.</p> <p><i>Default:</i> 1024 bit</p> <p><i>Range:</i> 512 bits or longer</p>
◦ When the negotiated SSL or TLS protocol between the client and server uses an unsupported cipher, do the following:	<p>Select a predefined or user-defined cipher.</p> <p>The predefined actions are:</p> <ul style="list-style-type: none"> <li>◦ Alert</li> <li>◦ Allow</li> <li>◦ Drop Packet</li> <li>◦ Drop Session</li> <li>◦ Reject</li> </ul>
◦ When the negotiated SSL or TLS protocol between the client and server uses an unsupported protocol version, do the following:	<p>Select a predefined or user-defined protocol version.</p> <p>The predefined actions are:</p> <ul style="list-style-type: none"> <li>◦ Alert</li> <li>◦ Allow</li> <li>◦ Drop Packet</li> <li>◦ Drop Session</li> <li>◦ Reject</li> </ul>

8. Click Next. If you selected Decryption Profile as the profile type, the Step 4, Decryption Options screen displays. 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 08:02:43 GMT

Copyright © 2024, Versa Networks, Inc.

If you selected Inspection Profile as the profile type, the Decryption Options screen is not visible. Continue to [Step 9](#).

Add TLS Decryption Profile

Profile Type

Certificate Setup

Inspection Options

Decryption Options

Permissions

Review & Submit

Based on the most common secure enterprise settings, we've chosen the protocol options, below. If you prefer, you can customize which protocol options you'd like to enable for your decryption.

Transport Layer Security (TLS) Version Support

Select the minimum and maximum version of TLS that is supported. When you select a version that is not TLS 1.3, select one or more key exchange algorithms for the SSL connection.

TLS 1.0

TLS 1.1

TLS 1.2

TLS 1.3

Key Exchange Algorithms

☐ ECDHE--Elliptic-Curve Diffie--Hellman Key Exchange

☐ RSA--Rivest--Shamir--Adleman algorithm

Advanced

Algorithms

Select which encryption and authentication algorithms to use.

Encryption Algorithms

☐ AES-128-CBC

☐ AES-128-GCM

☐ AES-256-CBC

☐ AES-256-GCM

☐ CAMELLIA-256-CBC

☐ CHACHA20-POLY1305

☐ SEED-CBC

Authentication Algorithms

☐ SHA

☐ SHA256

☐ SHA384

TLS Cipher Suites

The following TLS cipher suites are automatically selected based on your algorithms above.

☐ TLS-AES-128-GCM-SHA256

☐ TLS-CHACHA20-POLY1305-SHA256

☐ TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256

☐ TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA

☐ TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384

☐ TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256

☐ TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA

☐ TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384

☐ TLS-RSA-WITH-AES-128-CBC-SHA256

☐ TLS-RSA-WITH-AES-256-CBC-SHA

☐ TLS-RSA-WITH-AES-256-GCM-SHA384

☐ TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256

☐ TLS-RSA-WITH-SEED-CBC-SHA

☐ TLS-AES-256-GCM-SHA384

☐ TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA

☐ TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256

☐ TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384

☐ TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA

☐ TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256

☐ TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384

☐ TLS-RSA-WITH-AES-128-CBC-SHA

☐ TLS-RSA-WITH-AES-128-GCM-SHA256

☐ TLS-RSA-WITH-AES-256-CBC-SHA256

☐ TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256

☐ TLS-RSA-WITH-CAMELLIA-256-CBC-SHA

Cancel

Back

Skip to Review

Next

Field	Description
Transport Layer Security (TLS) Version Support (Group of 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 08:02:43 GMT

Copyright © 2024, Versa Networks, Inc.

22

Field	Description
<ul style="list-style-type: none"> <li>Minimum and maximum version of TLS that is supported</li> </ul>	Use the slider to select the minimum and maximum TLS version that is supported. If you select a version that is not TLS 1.3, select one or both key exchange algorithms for the SSL connection.
<ul style="list-style-type: none"> <li>Key Exchange Algorithms</li> </ul>	<p>If you selected a version that is not TLS 1.3, select one or both key exchange algorithms:</p> <ul style="list-style-type: none"> <li>ECDHE—Elliptic-Curve Diffie-Hellman Key Exchange</li> <li>RSA—Rivest-Shamir-Adleman algorithm.</li> </ul>
Advanced	Click to configure algorithms and TLS cipher suites.
Algorithms	Select which encryption and authentication algorithms to use. The encryption algorithms that you choose determine which authentication algorithms are available.
TLS Cipher Suites	Displays the TLS cipher suites selected depending on the algorithms.

9. Click Next to go to the Permissions screen.

Add TLS Decryption Profile

Profile Type Certificate Setup Inspection Options Decryption Options **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

10. You can change the permissions for the roles listed, or you can click Next to go to the Review & Submit screen.



Add TLS Decryption Profile

Profile Type

Certificate Setup

Inspection Options

Decryption Options

Permissions

Review & Submit

Review your configurations. Before submitting, review and edit any steps of your configuration below.

General

Name

Description

Tags

Press Enter to add

Profile Type

Edit

Profile Type
Decryption Profile

Certificate Setup

Edit

Certificate Authority
Issued For
Issued By

Inspection Options

Edit

When the certificate expires, do the following:
When the certificate is received from an untrusted issuer, do the following:
Restrict Certificate Extension: Disabled
SSL or TLS Protocol Checks
When the negotiated SSL or TLS protocol between the Client and Server uses an unsupported key length, do the following: 1024 bits
Minimum Supported RSA Key Length
When the decryption encounters an unsupported protocol version, do the following:
When the decryption encounters an unsupported cipher, do the following:

Decryption Options

Edit

Minimum TLS-1.1
Maximum TLS-1.2
Key Exchange Algorithms:
Algorithms
Encryption Algorithms
Authentication Algorithms
TLS Cipher Suites
Encryption Algorithms

Permissions


Edit

Enterprise Administrator Edit
Service Provider Administrator Edit
Service Provider Operator Read
Enterprise Operator Read

Cancel

Back

Save

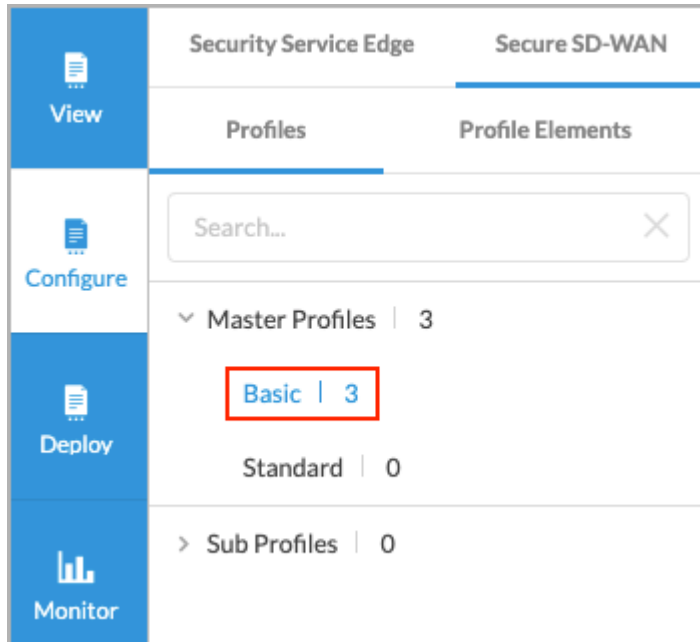
11. To change any of the information, click the  Edit icon in the section and then make the required changes.
12. Click Save to save the new TLS decryption profile.

After you create a TLS decryption profile, you can attach it to a TLS policy rule. See [Step 3](#) in [Configure SD-WAN TLS Decryption Policies](#).

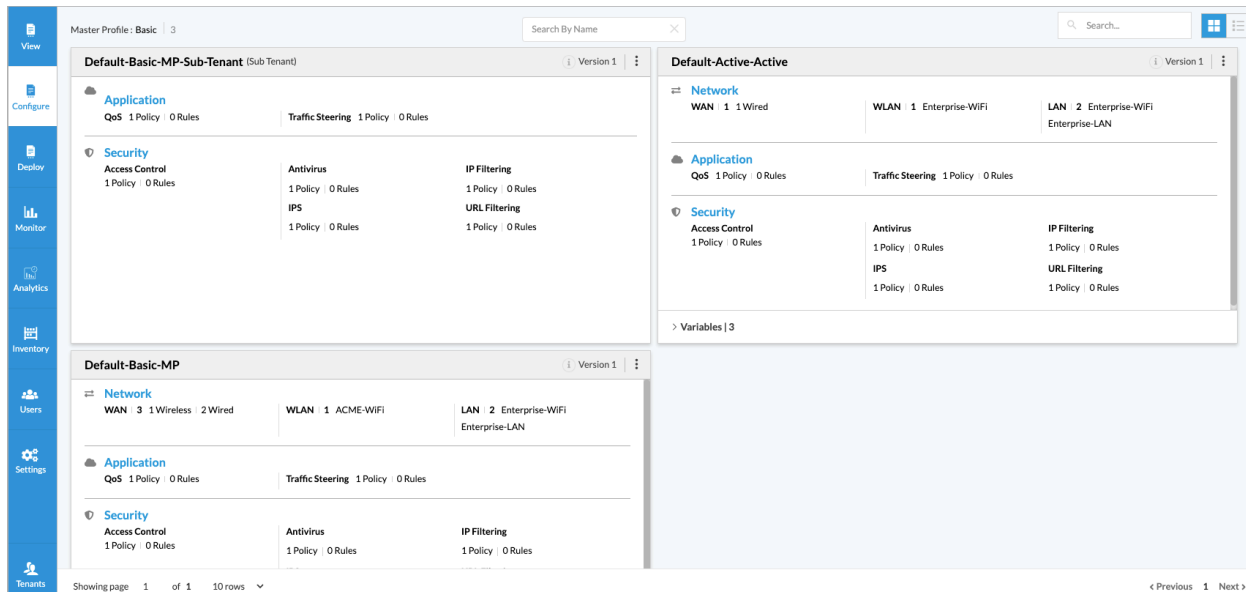
# Attach TLS Decryption Profiles and Policies to a Basic Master Profile

To attach TLS decryption profiles and policies to a basic master profile:

1. Go to Profiles > Master Profiles > Basic.



The screen displays the configured basic master profiles.



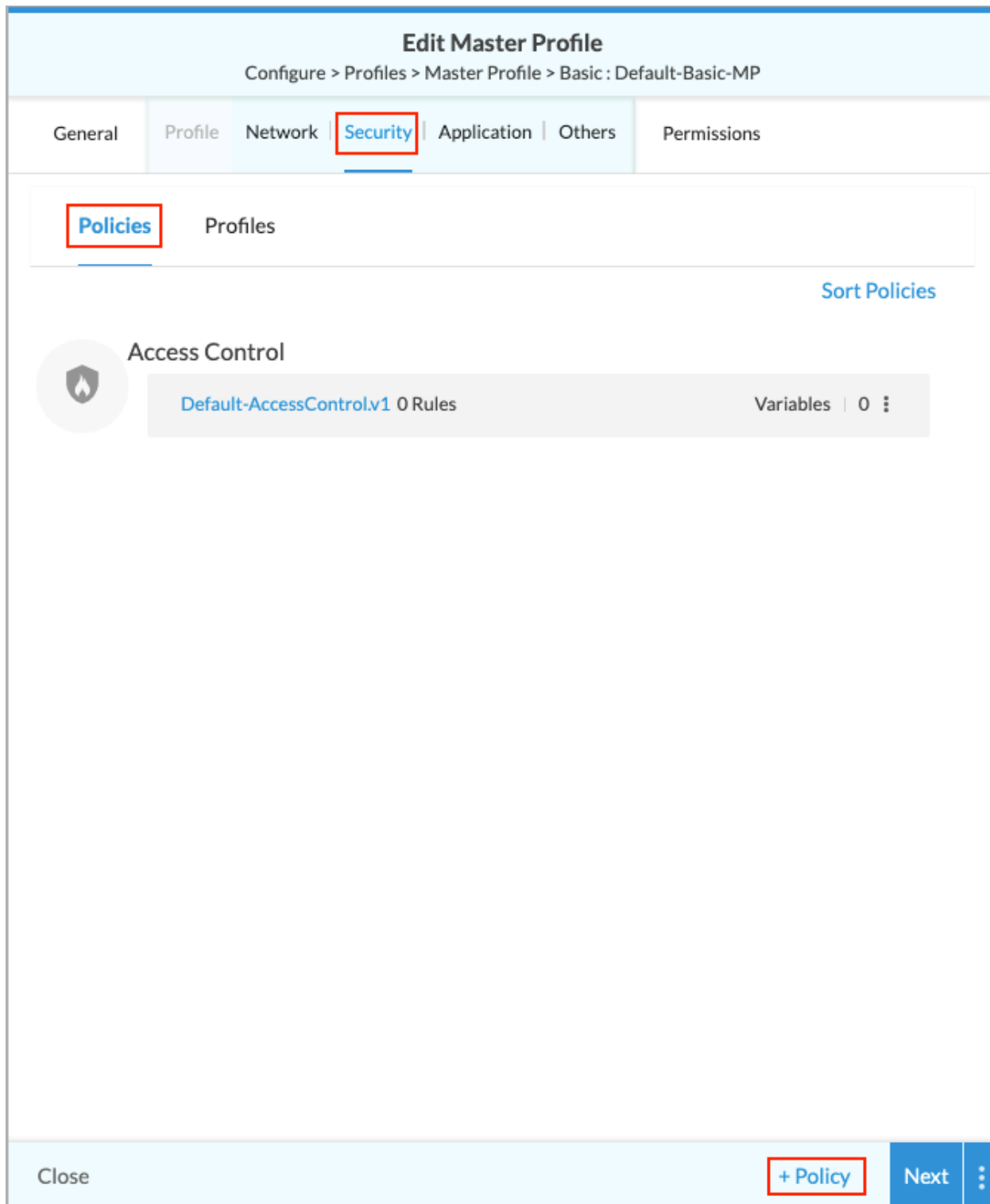
2. Click the master profile to which you will add the TLS decryption policy or rule. The Edit Master Profile screen displays.

[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 08:02:43 GMT

Copyright © 2024, Versa Networks, Inc.

3. Click Profile > Security in the menu bar. The following screen displays.

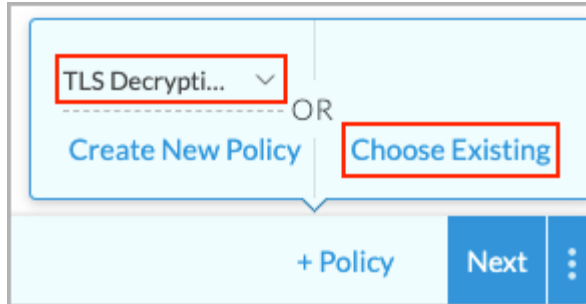


4. To attach a TLS decryption policy to the basic master profile, select the Policies tab and then click +Policy. The following pop-up window displays.

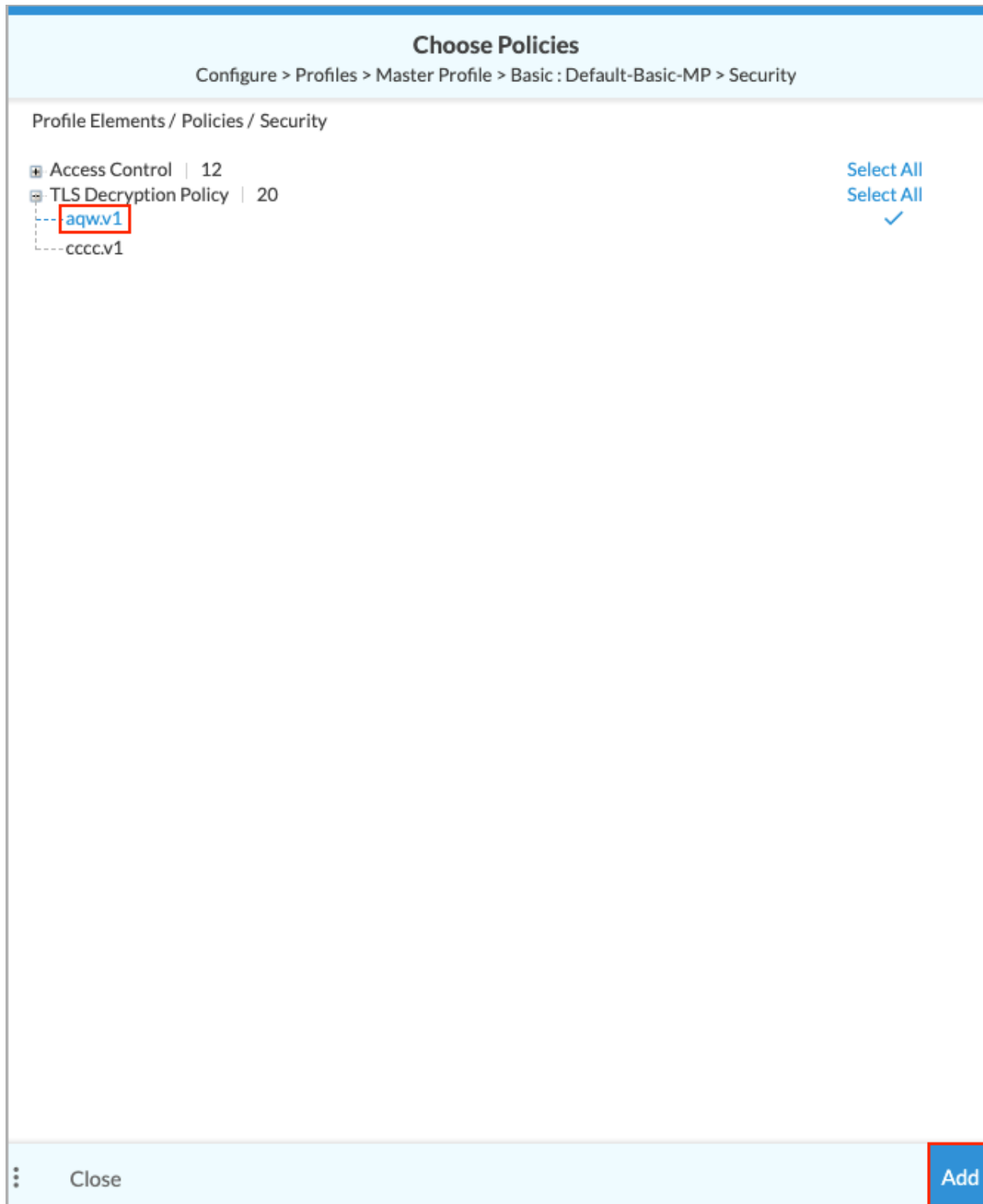
[https://docs.versa-networks.com/Secure\\_SD-WAN/02\\_Configuration\\_from\\_Concerto/Secure\\_SD-WAN\\_Configuration/Config...](https://docs.versa-networks.com/Secure_SD-WAN/02_Configuration_from_Concerto/Secure_SD-WAN_Configuration/Config...)

Updated: Wed, 23 Oct 2024 08:02:43 GMT

Copyright © 2024, Versa Networks, Inc.



5. Click the down arrow and select TLS Decryption Policy, then click Choose Existing. The Choose Policies screen displays.



6. Select a TLS decryption policy from the list (aqw.v1 in the example above), then click Add.
7. To attach a TLS decryption profile to the basic master profile, select the Profile tab in the Edit Master Profile > Profiles > Security screen.

Edit Master Profile

Configure > Profiles > Master Profile > Basic : Default-Basic-MP

General

Profile

Network

Security

Application

Others

Permissions

Policies

Profiles

Antivirus

Default-AntiVirus.v1

IP Filtering

Default-IPFiltering.v1

IPS

Default-IPS.v1

URL Filtering

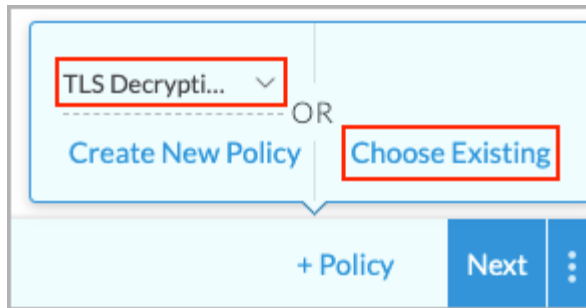
Default-URLFiltering.v1

Close

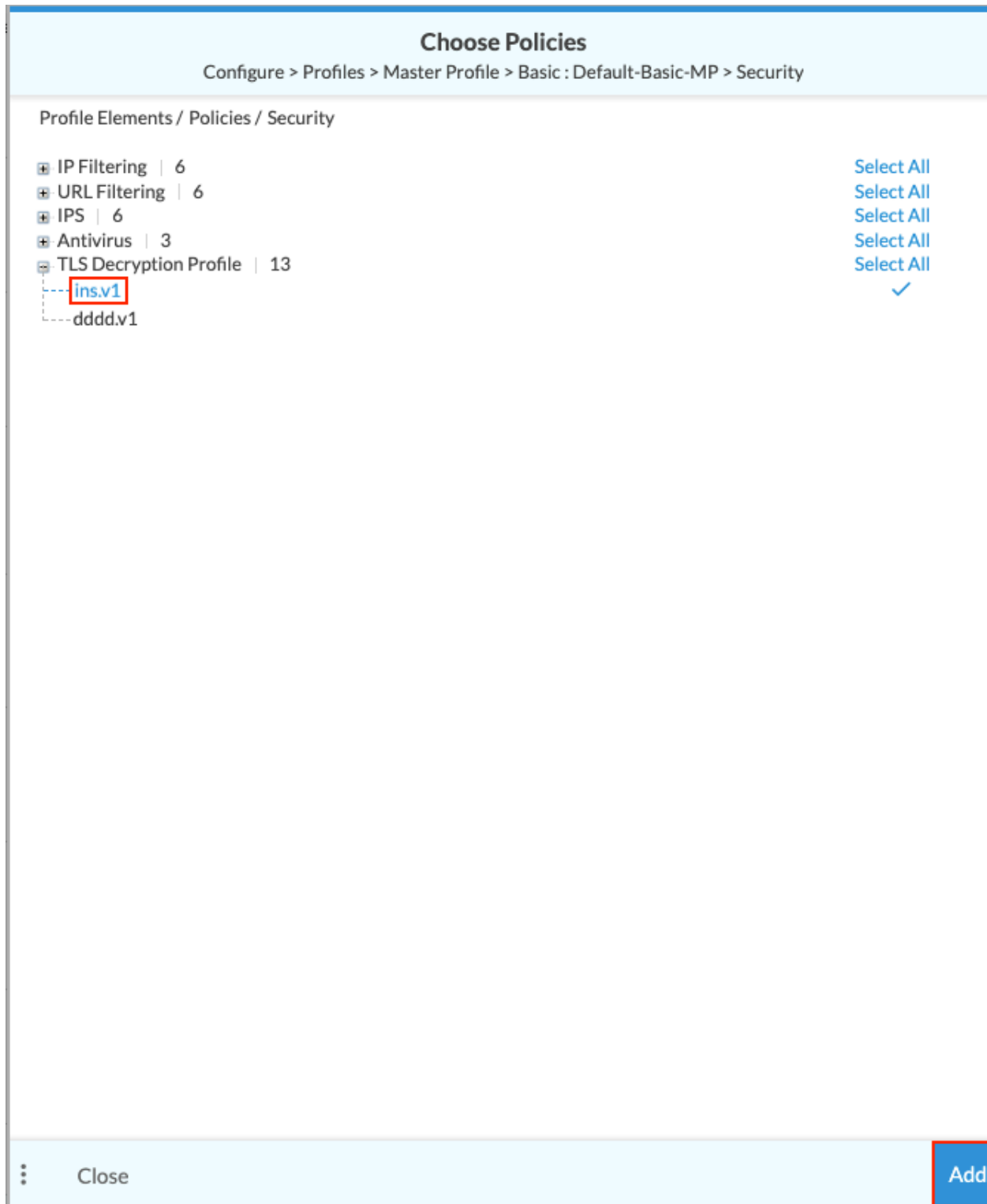
+ Policy

Next

8. Click +Policy. The following pop-up window displays.



9. Click the down arrow and select TLS Decryption Profile, then click Choose Existing. The Choose Policies screen displays.



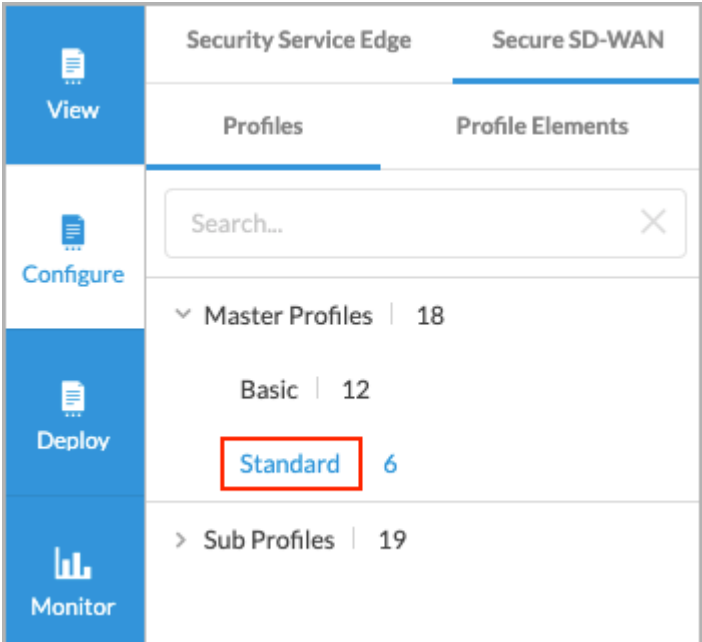
10. Select the new TLS decryption profile from the list (ins.v1 in the example above), then click Add.



# Attach TLS Decryption Profiles and Policies to a Standard Master Profile

To attach TLS decryption profiles and policies to a standard master profile:

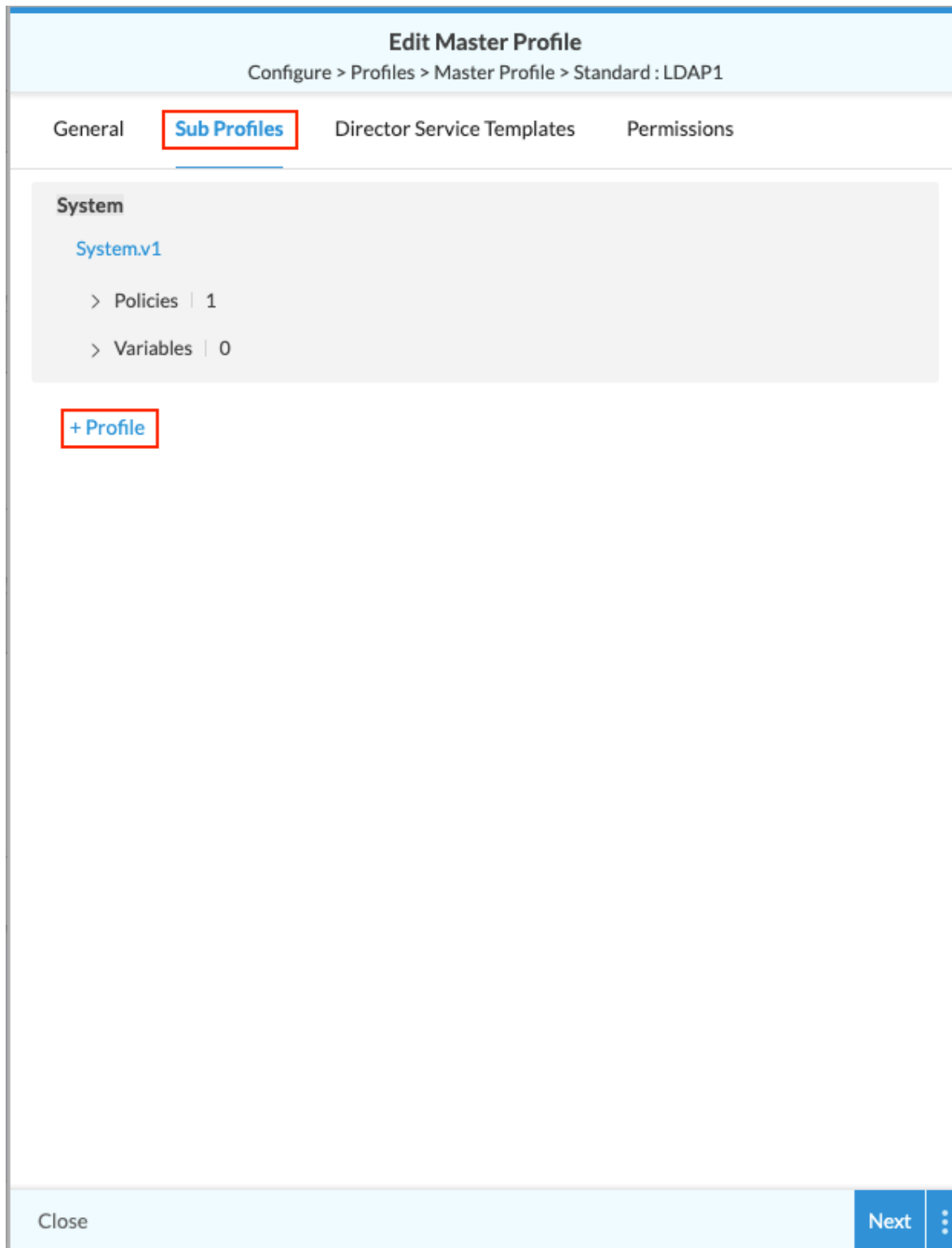
1. Go to Profiles > Master Profiles > Standard.



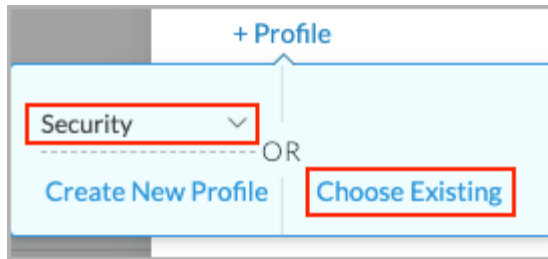
The screen displays the configured standard master profiles. Note that you can have only one instance of each profile type for each standard master profile. If a standard master profile already has a security profile attached to it, you cannot add another security profile. You can, however, create a new standard master profile and attach a TLS decryption profile to it.

View	Master Profile: Standard   6	Search By Name	+ Standard	Search...
Configure	LDAPDeploy		LDAP1	
Deploy	Version 1		Version 1	
Monitor	Profile Name	Type	Profile Name	Type
Analytics	Systemv1	System	Systemv1	System
Inventory	#Policies		#Policies	
Users	1		1	
Settings	LDAP		212	
Tenants	Version 1		Version 1	
	Profile Name	Type	Profile Name	Type
	ap-2v1	Security	ap-2v1	Security
	Systemv5	System	Systemv5	System
	#Policies		#Policies	
	8		8	
	7		7	
	> Variables   1		> Variables   1	
	Copy_of_TE		TE	
	Version 1		Version 1	
	Profile Name	Type	Profile Name	Type
	TLSPProfv1	Security	Devicev8	Device
	Topologyv2	Topology	testv2	System
	Devicev8	Device		
	testv2	System		
	#Policies		#Policies	
	14		1	
	1		1	
	1		1	
	> Variables   37		> Variables   35	
	Showing page 1 of 1 10 rows		< Previous 1 Next >	

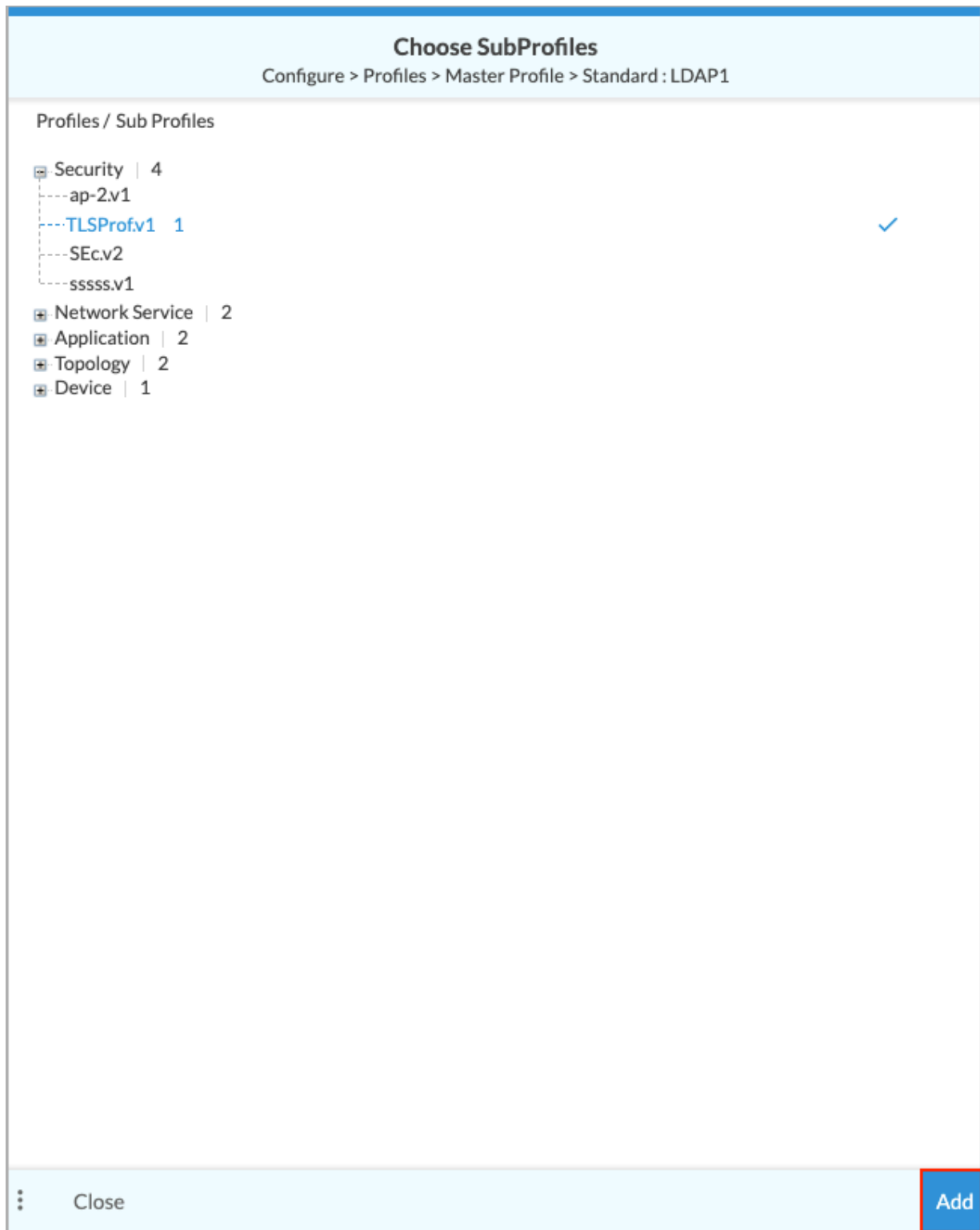
2. Click the standard master profile to which you will add the security TLS decryption policy or rule. The Edit Master Profile screen displays.
3. Click Sub Profiles in the menu bar. The following screen displays.



4. Click +Profile. The following pop-up window displays.



5. Click the down arrow and select Security, then click Choose Existing. The Choose SubProfiles screen displays.



6. Select the new TLS decryption profile under Security (TLSPProf.v1 in the example above), then click Add.

---

## Supported Software Information

Releases 12.1.1 and later support all content described in this article.

---

## Additional Information

[Configure Profiles](#)