
Configure SD-WAN User and Device Authentication

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

You can create policies and rules to authenticate both the users and the devices that enter a secure SD-WAN network. You can authenticate the users and devices before the gateways route the traffic to internet or private applications.

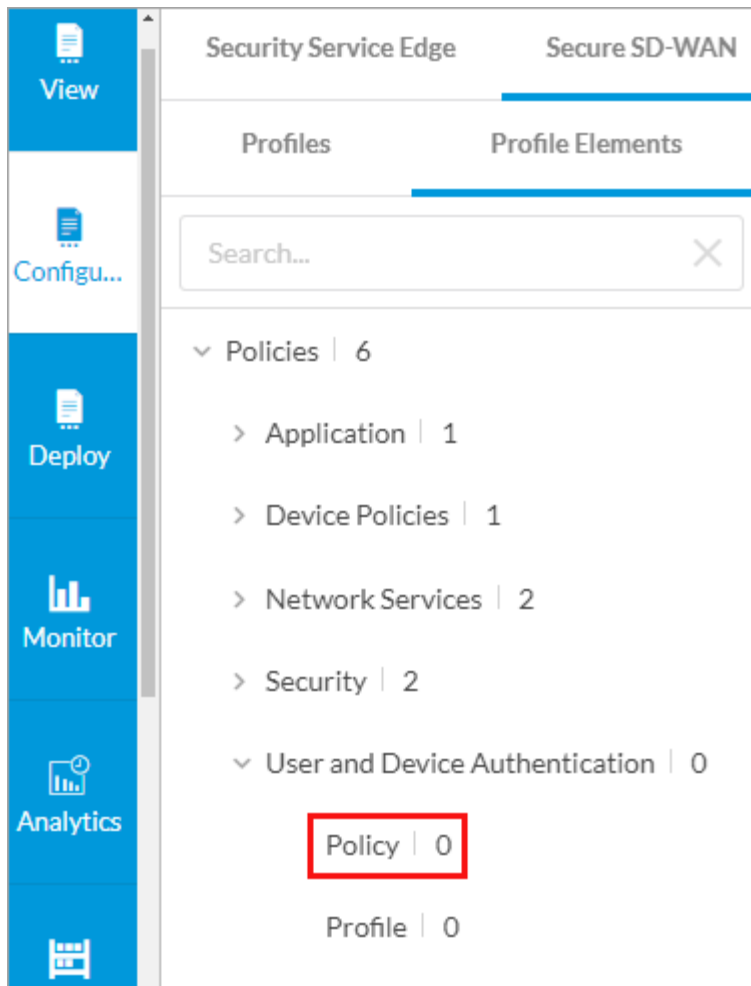
To define rules for user and device authentication, you can select applications and URLs, source and destination traffic, IP addresses, and services as match criteria to decide when to authenticate users. You can also create rules with match criteria for users who you do not want to authenticate.

You configure user and device authentication profiles to specify the authentication type for user authentication. You use the authentication profiles in user and authentication rules to specify the method to authenticate users who match the authentication rule criteria.

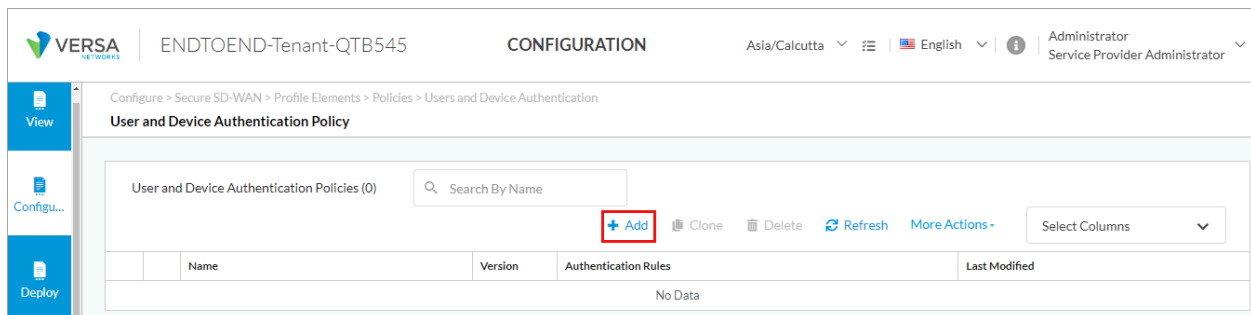
Configure User and Device Authentication Policies

To configure a user and device authentication policy for secure SD-WAN users and groups:

1. Go to Configure > Secure SD-WAN > Profile Elements > Policies > User and Device Authentication > Policy.



The User and Device Authentication Policy screen displays.



2. To create a new user and device authentication policy, click + Add. The Add User and Device Authentication Rule displays the first step of the workflow.
3. In Step 1, Applications and URLs, the Applications tab and the Application Group tab are selected. By default, all applications, URLs, and reputations are included in the match criteria.

Add User and Device Authentication Rule

1 Applications & URLs 2 Source & Destination Traffic 3 Service & DSCP 4 Action 5 Permissions 6 Review & Submit

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

Applications URL Categories & Reputations

Application Group Applications Application Category

Search for Application Group

> User Defined Application Groups (Selected: 0 of 10)

Predefined Application Groups (Selected: 0 of 23)

DocuSign Docusign-Apps

Dropbox-Apps

Google-Apps

GotoMeeting-A...

IBM-Apps

Intuit-Apps

Cancel Skip to Review Next

- To select specific application groups to include in the match criteria, click User-Defined Application Groups, Predefined Application Groups, or both. Then select the application groups for the rule to match. Use the Search bar to find specific application groups.
- Select the Applications > Applications tab, and then select one or more user-defined or predefined applications for the rule to match. Use the Search bar to find specific applications.

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

Applications URL Categories & Reputations

Application Group Applications Application Category

Search for Applications

> User Defined Applications (Selected: 0 of 43)

Predefined Applications (Selected: 0 of 4576)

01NET

050PLUS

0ZZ0

10050NET

10086CN

104COM

- Select the Applications > Application Category tab, and then select one or more predefined application categories for the rule to match.

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

Applications URL Categories & Reputations

Application Group Applications **Application Category**

Search for Application Category

▼ **Predefined Application Categories** Selected: 0 of 15)

Advertising ⓘ	Audio-Video-Stream...	Business-Traffic ⓘ	Database ⓘ	File-Transfer ⓘ	Gaming ⓘ

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

Add User and Device Authentication Rule

1 2 3 4 5 6

Applications & URLs Source & Destination Traffic Service & DSCP Action Permissions Review & Submit

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

Applications **URL Categories & Reputations**

URL Categories

Search or select from list

Reputations

Add Reputation

Cancel Skip to Review Next

8. In the URL Categories field, click the down arrow, and then select one or more URL categories for the rule to match.
9. In the Reputations field, click the down arrow, and then select one or more reputations for the rule to match:
 - High risk
 - Low risk
 - Moderate risk
 - Suspicious
 - Trustworthy
 - Undefined
10. Click Next or select Step 2, Source and Destination Traffic. The following screen displays, and the Source Address tab is selected. By default, all source and destination traffic is included. You can specify which source and destination traffic to include in the match criteria.

Add User and Device Authentication Rule

Match Criteria: 1. Applications & URLs, 2. **Source & Destination Traffic**, 3. Service & DSCP, 4. Action, 5. Permissions, 6. Review & Submit

Source Address | Destination Address | Source Zones | Destination Zones

+ Add Variable

Search or select from list

	Name	Addresses
<input type="checkbox"/>	Copy_of_kasunTest1	1.1.1.0/24, 1.1.1.1-1.1.1.111
<input type="checkbox"/>	kasunTest1	1.1.1.0/24, 1.1.1.1-1.1.1.111
<input type="checkbox"/>	test	1.2.3.0/24
<input type="checkbox"/>	Copy_of_testFiles_kasun_test	testversa, b7b64a5a-feb6-475c-a8cd-8d064f3b0cfe, 10.2.3.1-10.2.3.5, 192.168.0.56/0.0.0.255, test
<input type="checkbox"/>	Copy_of_testFile01	10.1.1.0/24, ee176d27-fdd1-4086-87b6-11070db7b81f
<input type="checkbox"/>	testFile01	10.1.1.0/24, ee176d27-fdd1-4086-87b6-11070db7b81f
<input type="checkbox"/>	ComplexAddress Group	192.168.0.56/0.0.0.255, 192.168.0.55/0.0.0.255, 192.168.0.54/0.0.0.255, 192.168.0.53/0.0.0.255, 192.168.0.52/0.0.0.255, 192.168.0.51/0.0.0.255, 192.168.0.50/0.0.0.255, 192.168.0.49/0.0.0.255, 192.168.0.48/0.0.0.255, 192.168.0.47/0.0.0.255, 192.168.0.46/0.0.0.255, b7b64a5a-feb6-475c-a8cd-8d064f3b0cfe
<input type="checkbox"/>	testFiles	testversa, b7b64a5a-feb6-475c-a8cd-8d064f3b0cfe, 10.2.3.1-10.2.3.5, 192.168.0.56/0.0.0.255, test
<input type="checkbox"/>	RIYADH	10.0.0.0/23
<input type="checkbox"/>	riyadh	10.0.0.0/24

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

IP Address or IP Range + Add Variable IP Subnet + Add Variable IP WildCard + Add Variable

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

Cancel Back Skip to Review Next

11. Select a source address group for the rule to match, or use the search box to find a source address group. 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.

Add Variable


\$

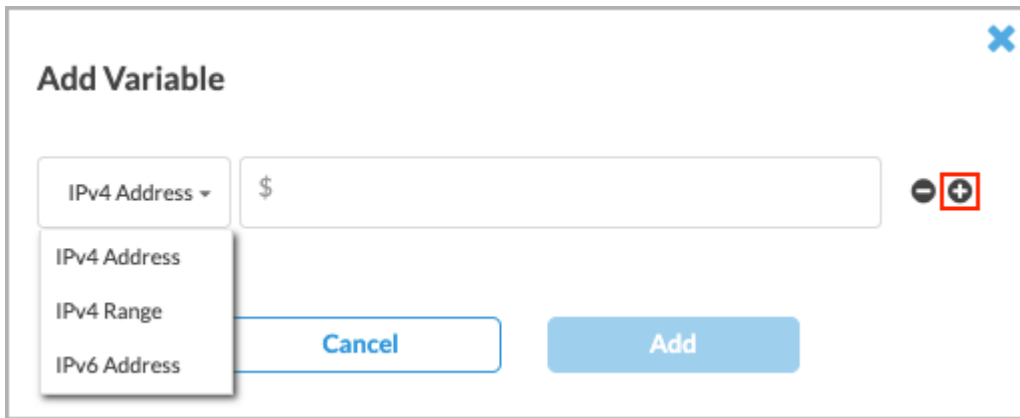
+ -

Cancel Add


You can also enter values in any of the following fields for the rule to match: IP Address or IP Range, IP Subnet, or IP Wildcard. You can click + Add Variable to create variables for these values, and you can add multiple variables

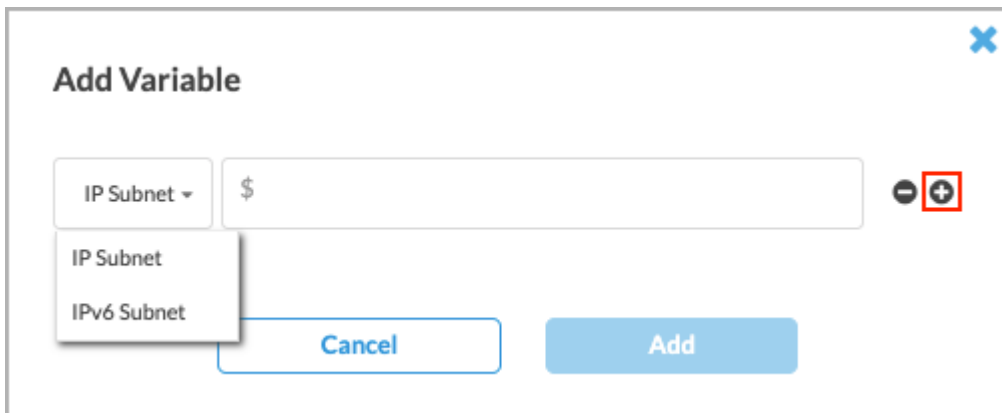
for each one.

- To add a variable for the IP address or IP range, select IPv4 Address, IPv4 Range, or IPv6 Address, click the  Plus icon, and then click Add.




The 'Add Variable' dialog box shows a dropdown menu with 'IPv4 Address' selected. The input field contains a dollar sign '\$'. To the right of the input field are minus and plus icons, with the plus icon highlighted by a red square. Below the input field are 'Cancel' and 'Add' buttons.

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



The 'Add Variable' dialog box shows a dropdown menu with 'IP Subnet' selected. The input field contains a dollar sign '\$'. To the right of the input field are minus and plus icons, with the plus icon highlighted by a red square. Below the input field are 'Cancel' and 'Add' buttons.

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

×

Add Variable

\$

−

+

Cancel

Add

12. Click the Destination Address tab, and then select a destination address group for the rule to match or use the search box to find a source address. Then, enter values in any of the following fields for the rule to match: IP Address or IP Range, IP Subnet, or IP wildcard. You can click + Add Variable to create variables for these values. For more information about adding variables, see Steps 13 and 14.

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 Zones

Destination Zones

+

 Add Variable

Search or select from list

	Name	Addresses
<input type="checkbox"/>	Copy_of_kasunTest1	1.1.1.0/24, 1.1.1.1-1.1.1.111
<input type="checkbox"/>	kasunTest1	1.1.1.0/24, 1.1.1.1-1.1.1.111
<input type="checkbox"/>	test	1.2.3.0/24
<input type="checkbox"/>	Copy_of_testFiles_kasun_test	test.versa, b7b64a5a-feb6-475c-a8cd-8d064f3b0cfe, 10.2.3.1-10.2.3.5, 192.168.0.56/0.0.0.255, test
<input type="checkbox"/>	Copy_of_testFile01	10.1.1.0/24, ee176d27-fdd1-4086-87b6-11070db7b81f
<input type="checkbox"/>	testFile01	10.1.1.0/24, ee176d27-fdd1-4086-87b6-11070db7b81f
<input type="checkbox"/>	ComplexAddress Group	192.168.0.56/0.0.0.255, 192.168.0.55/0.0.0.255, 192.168.0.54/0.0.0.255, 192.168.0.53/0.0.0.255, 192.168.0.52/0.0.0.255, 192.168.0.51/0.0.0.255, 192.168.0.50/0.0.0.255, 192.168.0.49/0.0.0.255, 192.168.0.48/0.0.0.255, 192.168.0.47/0.0.0.255, 192.168.0.46/0.0.0.255, b7b64a5a-feb6-475c-a8cd-8d064f3b0cfe
<input type="checkbox"/>	testFiles	test.versa, b7b64a5a-feb6-475c-a8cd-8d064f3b0cfe, 10.2.3.1-10.2.3.5, 192.168.0.56/0.0.0.255, test
<input type="checkbox"/>	RIYADH	10.0.0.0/23
<input type="checkbox"/>	riyadh	10.0.0.0/24

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

IP Address or IP Range
+ Add Variable

Enter IP address or range

IP Subnet
+ Add Variable

Enter a list of IPv4/IPv6 Subnet values

IP WildCard
+ Add Variable

Enter a list of wildcard values

13. Select the Source Zones tab to specify source zones to include in the match criteria. Select one or more source zones from the list, or use the search box to find source zones. To create a variable for the source zone, click + Add Variable.

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 Zones** Destination Zones

Source Zones [+ Add Variable](#)

Search or select from list ▼

14. Select the Destination Zones tab to specify destination zones to include in the match criteria. Select one or more destination zones from the list, or use the search box to find destination zones. To create a variable for the source zone, click [+ Add Variable](#).

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 Zones **Destination Zones**

Destination Zones [+ Add Variable](#)

Search or select from list ▼

15. Click Next or select Step 3, Service and DSCP. The following screen displays, and the Services tab selected. By default, all services, service groups, and DSCPs are included in the match criteria. You can specify the services, service groups, and Differentiated Services Code Points (DSCPs) for the rule to match.

Add User and Device Authentication Rule

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

Services Service Groups DSCP

Search or select from list

Services(User Defined: 31 | Predefined: 741) All Services

	Name	Type	Protocol	Source Port	Destination Port	Source Or Destination Port
<input type="checkbox"/>	Copy_of_Copy_of_TCPCheck	User Defined	TCP			123,125
<input type="checkbox"/>	Copy_of_Copy_of_TCPCheck1	User Defined	TCP			123,125
<input type="checkbox"/>	Copy_of_TCPCheck1	User Defined	TCP			123,125
<input type="checkbox"/>	Copy_of_TCPCheck	User Defined	TCP			123,125

Showing 1-10 of 772 results 10 Rows per Page Go to page 1 < Previous 1 2 ... Next >

Cancel Back Skip to Review Next

16. 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 then select one of the following categories to filter the list:
 - Predefined
 - User Defined
17. Select the Service Groups tab, and then select the user-defined and predefined service groups to which to apply security access control rules. Click the ➤ Row Expand icon next to the service group name to view the details for each service group.

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

Services **Service Groups** DSCP

Service Groups

Search or select from list

Service Groups

	Name	User Defined	Predefined
<input type="checkbox"/> >	lan2_of_Copy_of_Copy_of_tstGG01	1	2
<input type="checkbox"/> >	Copy_of_Copy_of_Copy_of_tstGG01	1	2
<input type="checkbox"/> >	Copy_of_Copy_of_tstGG01	1	2
<input type="checkbox"/> >	Copy_of_tstGG01	1	2
<input type="checkbox"/> >	tstGG01	1	2
<input type="checkbox"/> >	ng04	1	
<input type="checkbox"/> >	SG_00R	1	
<input type="checkbox"/> >	ng003	2	
<input type="checkbox"/> >	newSG_01	2	
<input type="checkbox"/> >	My-Group	2	2

Showing 1-10 of 11 results 10 ▾ Rows per Page Go to page 1 ▾ < Previous 1 2 Next >

18. Select the DSCP tab. By default, all DSCP decimal values are included in the match criteria. You can specify which DSCP decimal values to include.

Services Service Groups **DSCP**

DSCP Decimal

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

Search or select from list

- 0
- 1
- 5
- 6
- 7
- 8
- 9

19. Select one or more DSCP decimal values, or use the search to locate one or more values.
20. Click Next to go to Step 4, Action.

Add User and Device Authentication Rule

Match Criteria

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

By default, no Authentication is impose Select the action to impose on the traffic for applications and URLs.

Do Not Authentication (No Authentication) ☒

Authenticate Using Users & User Groups Profile ☐

Select

Cancel Back Skip to Review Next

21. If you do not want to authenticate users for the match criteria that you selected in Step 1, click Do Not Authenticate.
22. If you want to use a profile to specify the authentication type, click Authenticate Using User and Group Profile, and then select a profile that you configured in [Configure User and Device Authentication Profiles](#), below.

Add User and Device Authentication Rule

Match Criteria

Applications & URLs Source & Destination Traffic Service & DSCP Action Permissions Review & Submit

By default, no Authentication is impose Select the action to impose on the traffic for applications and URLs.

Do Not Authentication (No Authentication)

Authenticate Using Users & User Groups Profile

ACME-Group

Cancel Back Skip to Review Next

23. Click Next to go to Step 5, Permissions.

Add User and Device Authentication Rule

Match Criteria

Applications & URLs Source & Destination Traffic Service & DSCP Action 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

Cancel Back Skip to Review Next

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

25. Click Next to go to Step 3, Review and Submit.

Add User and Device Authentication Rule

Match Criteria

Applications & URLs Source & Destination Traffic Service & DSCP Action 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 Enabled

Applications & URLs Edit

✓ All Applications

Source & Destination Traffic Edit

Service & DSCP Edit

Action Edit

Authenticate Using Users & User Groups Profile ACME-Group

Permissions Edit

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

Cancel Back **Save**

26. In the General section, enter a name for the rule. Optionally, enter a description and add tags for the rule.
27. By default, the rule is enabled. Toggle to disable the rule.
28. To enable logging for the rule, slide the toggle to Enabled.
29. Click the Edit icon next to any section to make changes.

30. Click Save.

Configure User and Device Authentication Profiles

To specify the authentication type to use for user authentication, you configure user and device authentication profiles. For each enterprise, you can configure profiles for Lightweight Directory Access Protocol (LDAP), RADIUS, Security Assertion Markup Language (SAML), and Versa Directory. You can configure both an LDAP and a SAML profile for an enterprise, but for RADIUS and Versa Directory profile, you can configure only one for each enterprise. You can configure user and device certificate-based profiles with each other, or with LDAP or SAML authentication profiles.

LDAP is a client-server protocol that allows a network device to access an LDAP server, which provides directory services that store descriptive attribute-based information. When an end user sends a request to access a webpage, the Versa Operating System™ (VOS™) device accesses the LDAP server to validate the user. Based on the authentication result, the user is either authenticated or their authentication request is denied. You can configure either a user-based or group-based policy to allow or deny traffic.

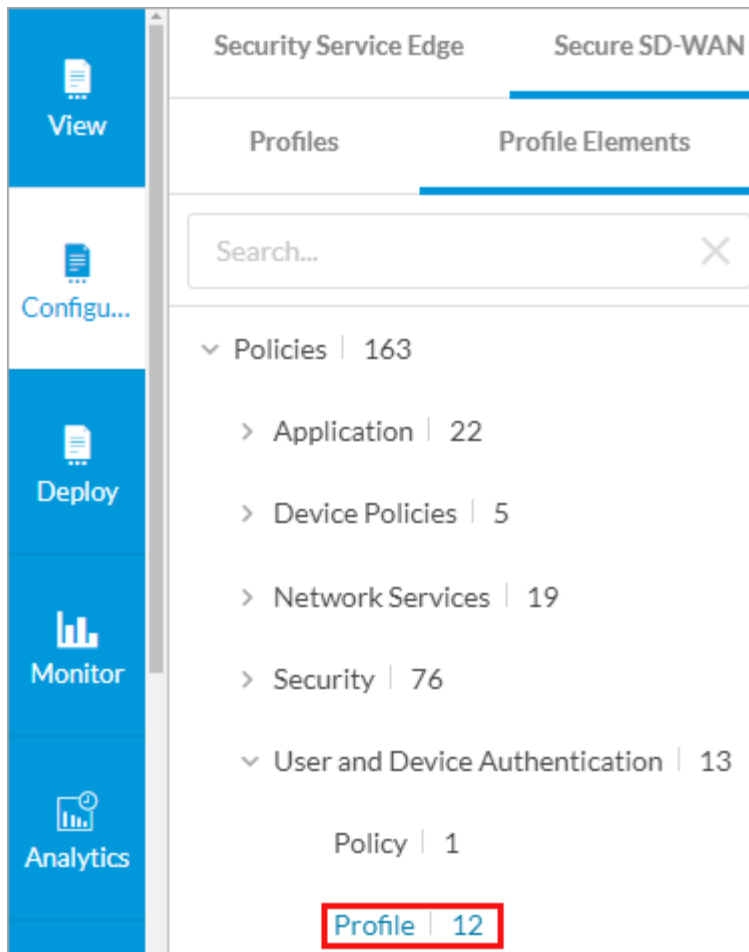
RADIUS is a distributed client-server system that secures networks against unauthorized access. A RADIUS server provides an external database that you can use to authenticate users before allowing them to access a network, a device, or related services.

SAML authenticates users so that they can access multiple services and applications. SAML is useful when you want to access multiple services or applications and have authentication for each service or application, for example, Google and its related services. SAML is a common standard for exchanging authentication between parties and is most commonly used for web browser-based single sign-on (SSO).

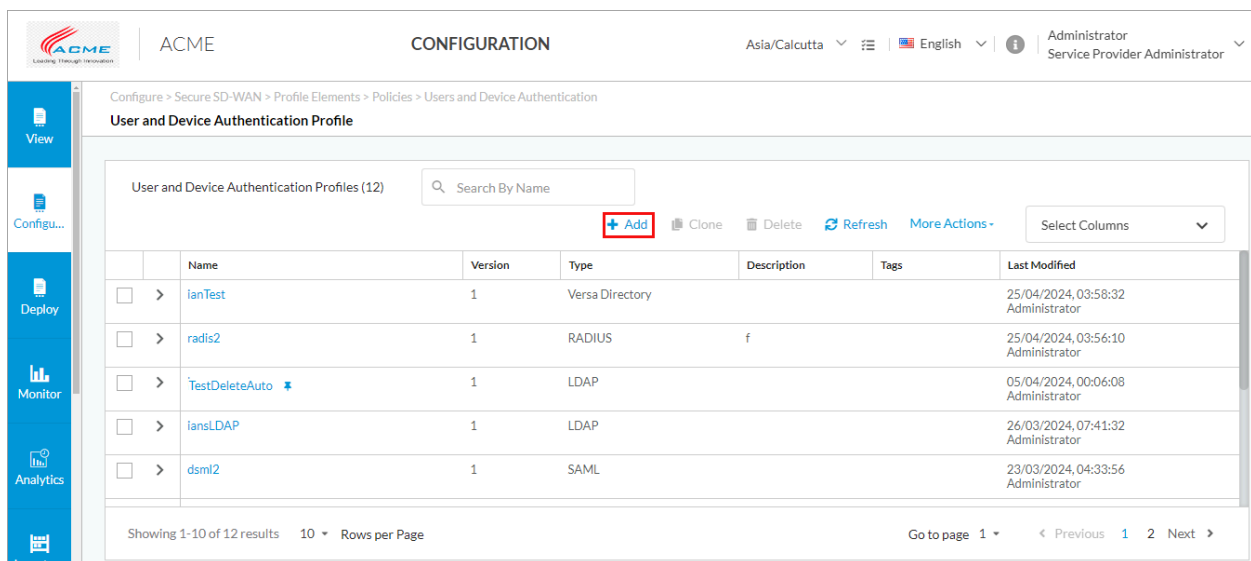
With Versa directory authentication, you upload lists of users and groups for authentication purposes. You can also add individual users and groups using the GUI.

To configure user and device authentication profiles:

1. Configure > Secure SD-WAN > Profile Elements > Policies > User and Device Authentication > Profile.



The User and Device Authentication Profile screen displays.



2. To create a new profile, click + Add. The Add User and Device Authentication Profile screen displays.

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

Updated: Wed, 23 Oct 2024 08:02:38 GMT

Copyright © 2024, Versa Networks, Inc.

Add User and Device Authentication Profile ✕

Select which authentication profile you would like to configure.

LDAP

LDAP is a client-server protocol that enables a network device to access an LDAP server, which provides directory services that store descriptive attribute-based information.

SAML

SAML is a common standard for authenticating users so that they can access multiple services and applications. SAML is most commonly used for web browser-based single sign-on (SSO)

RADIUS

RADIUS server provides an external database that you can use to authenticate users before allowing them to access a network, a device, or related services.

Versa Directory

With Versa directory authentication, you upload lists of users and groups for authentication purposes, as well as add individual users and user groups.

Cancel

Get Started

3. Select the type of authentication to configure from these options: LDAP, RADIUS, SAML, or Versa Directory.
4. Click Get Started.
5. In Step 1, Settings, configure the settings for the selected authentication type:
 - For the LDAP authentication type, enter information for the following fields.

Add LDAP Authentication Profile

1
Settings
2
User And Group Profile
3
Permissions
4
Review & Submit

Server Type

Active Directory

Select either FQDN or IP Address *

☒ FQDN

+ Add Variable

www.text.com

☐ IP Address

+ Add Secondary Server

VPN Name *

ACME-LAN-VR

Port *
+ Add Variable

389

☒ Enable SSL

SSL Mode

STARTTLS

CA Certificate

default

+ Add New

Details

Bind DN *

123

Bind Password *
+ Add Variable

Bind Timeout (sec)
+ Add Variable

30

Base DN *

1313

Domain Name *
+ Add Variable

domain1

Base Domain

Search Timeout (sec)
+ Add Variable

30

Cache Expiry Time
+ Add Variable

10

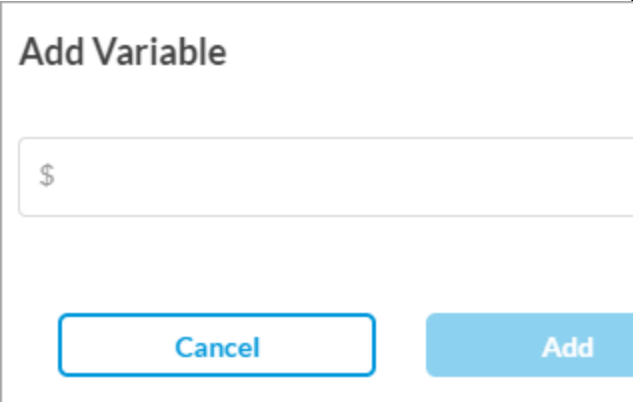
mins


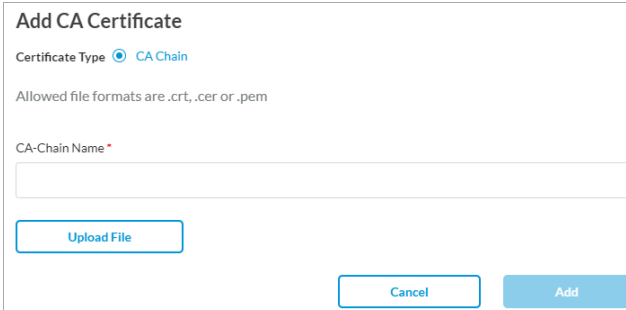
Cancel

Skip to Review

Next

Field	Description
Server Type	Select the server type: <ul style="list-style-type: none"> Active Directory Open LDAP
+ Add Variable	Click to create a variable for parameters. Enter a name for the variable, and then click Add. You can add multiple variables. The Add Variable screen is the same for all parameters.

	
Select Either FQDN or IP Address	<p>Click FQDN or IP Address, and then enter the FQDN or IP address of the Active Directory or LDAP server.</p> <p>Click + Add Secondary Server to add another server of the same type. In the Add Secondary Server popup window, enter the required information, and then click Add.</p>

	<p>Click the slider again to disable SSL for the LDAP session.</p> 
SSL Mode	<p>If you enable SSL, select the SSL mode for the LDAP session:</p> <ul style="list-style-type: none"> ▪ LDAPS—Use secure LDAP (LDAP over SSL) ▪ STARTTLS—Use LDAP over TLS
CA Certificate	<p>If you enable SSL, select the certificate authority (CA) certificate to use for the secure LDAP connection. To add a new CA certificate, click + Add New, and then enter the required information.</p> 
Bind DN	Enter the bind distinguished name (DN) to use when logging in to the LDAP server.
Bind Password	Enter the password that the bind DN uses when logging in to the LDAP server.
Base DN	Enter the base DN to use when an LDAP client initiates a search.
Domain Name	Enter the domain name to use for LDAP searches, for example, versa-networks.com.
Domain Base	Enter the name of the base domain.

- For the SAML authentication type, enter information for the following fields.

Add SAML Authentication Profile

1
Settings
2
Users And User Groups
3
Permissions
4
Review & Submit

Select SAML Type

okta
OKTA

PingIdentity
Ping Identity

Office 365
Office 365

Azure Active Directory
Azure Active Directory

Google IAM
Google IAM

Other
Other

Device Host FQDN
Add Variable

Single Sign-on URL
Add Variable

Service Provider Entity ID
Add Variable

Identity Provider Entity ID
Add Variable

Prefix ID
Add Variable

Group Attribute
Add Variable

Single Sign-out URL
Add Variable

Service Provider Certificate
--Select--
Add New

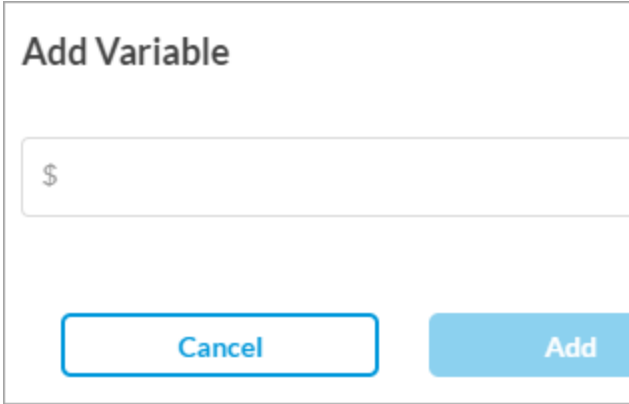
Identity Provider Certificate
asdasdasd
Add New

Details
Name: asdasdasd
File Name: ACME.crt
Issued To: ACME
Issued By: Versa Networks Inc.
Validity: 2022-01-12 07:31:54 to 2027-01-11 07:31:54

Cache Expiry Time
Add Variable
10 mins

Cancel
Skip to Review
Next

Field	Description
Select SAML Type	Select the SAML type: <ul style="list-style-type: none"> Azure Active Directory Google IAM Office 365 Okta Other PingIdentity

Field	Description
+ Add Variable	<p>Click to create a variable for parameters. Enter a name for the variable, and click Add. You can add multiple variables. The Add Variable screen is the same for all parameters.</p>  <p>The dialog box titled 'Add Variable' contains a text input field with a dollar sign (\$) as a placeholder. Below the input field are two buttons: 'Cancel' and 'Add'.</p>
Device Host FQDN	Enter the host FQDN of the user device.
Single Sign-on URL (Required)	Enter the URL of the identify provider (IdP) to use for single sign-on.
Single Sign-out URL	Enter the URL to point to for single sign-out.
Service Provider Entity ID (Required)	Enter the entity ID of the service provider.
Service Provider Certificate	Select the certificate that the service provider uses to authenticate.
Identity Provider Entity ID (Required)	Enter the entity ID that uniquely identifies the SAML IdP.
Identity Provider Certificate (Required)	Select the authentication certificate issued by the IdP.
Prefix ID	Enter the name of the external IdP.
Cache Expiry Time	<p>Enter the time, in minutes, for cache expiry, after which the live user record expires. On reaching the cache expiry time, the user record expires and the user gets logged out.</p> <p><i>Default: 10 minutes</i></p>
Group Attribute	Enter the SAML group attribute to identify group

Field	Description
	value from the SAML response.

- For the RADIUS authentication type, enter information for the following fields.

Field	Description
IP Address (Required)	Enter the IP address of the RADIUS server.
Port (Required)	Enter the port number to use on the RADIUS server.
VPN Name	Select the VPN instance to use to connect to the RADIUS server.
Shared Secret	Enter the RADIUS shared secret (password) string.
Cache Expiry Time	<p>Enter the time, in minutes, after which cache for the authentication profile expires.</p> <p><i>Default:</i> 10 minutes</p>

- For the Versa Directory authentication type, enter the time, in minutes, for cache expiry, after which the live user record expires. On reaching the cache expiry time, the user record expires and the user gets logged out. The default is 10 minutes.

Add Versa Directory Authentication Profile

1 Settings 2 Users And User Groups 3 Permissions 4 Review & Submit

Cache Expiry Time [+ Add Variable](#)

10 mins

Cancel Skip to Review Next

6. Click Next.
7. In Step 2, User and Group Profile, configure the users and groups for the selected authentication type.
 - For LDAP authentication, enter information for the following fields.

Add LDAP Authentication Profile

Settings 2 User And Group Profile 3 Permissions 4 Review & Submit

Group Object Class * [+ Add Variable](#)

Group Name * [+ Add Variable](#)

Group Member * [+ Add Variable](#)

User Object Class * [+ Add Variable](#)

User Name * [+ Add Variable](#)

Refresh Interval (seconds) [+ Add Variable](#)

Password Last Set [+ Add Variable](#)

Password Max Age [+ Add Variable](#)

21600

Cancel Back Skip to Review Next

Field	Description
+ Add Variable	Click to create a variable for parameters. Enter a name for the variable, and click Add. You can add multiple variables. The Add Variable screen is the same for all parameters.

	<div> <div>Add Variable</div> <div> <div>\$</div> </div> <div> <div>Cancel</div> <div>Add</div> </div> </div>
Group Object Class (Required)	Enter the group object class provided by your administrator.
Group Name (Required)	Enter the group name provided by your administrator.
Group Member (Required)	Enter the group member provided by your administrator.
User Object Class (Required)	Enter the user object class provided by your administrator.
User Name (Required)	Enter the format of the username, for example, User Principal Name.
Refresh Interval	Enter how often to refresh the LDAP profile information, in seconds. <i>Range:</i> 60 through 86400 seconds <i>Default:</i> 21600 seconds
Password Last Set	Enter the time when the user password was last set or updated.
Password Max Ageimum	Enter the validity period of the password.

- For SAML, RADIUS, and Versa Directory authentication, enter information for the following fields.

	<div><div><div>Add User</div><div><div>User Name*</div><div></div><div>First Name</div><div></div><div>Last Name</div><div></div><div><div>Cancel</div><div>Add</div></div></div></div></div>
	<p>For Versa Directory, the following screen displays when you click + Add to add a user:</p>

Add User

User Name*

Password*

First Name

Last Name

Email*

Phone Number



Description

Group Name [+ Add New](#)

Cancel

Add

Click + Add New to add a new user group, as shown below in the Groups List tab.

Group List Tab

Select the Group List tab and click Browse. In the popup window, select a user group file in CSV format to upload. Each line in the CSV file must be in the following format:

- Group Name*, Description

	<div data-bbox="885 210 1615 451"> <div> <div>User List</div> <div>Group List</div> </div> <p>Upload group list in the following format: csv</p> <div> <input type="text"/> <div>Browse</div> </div> <p>Note: CSV file should be in the following format: Group Name, and Description.</p> <p>Groups (0)</p> <table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th>Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td>No Data</td> </tr> </tbody> </table> </div>	<input type="checkbox"/>	Name	Description			No Data
<input type="checkbox"/>	Name	Description					
		No Data					
<div data-bbox="240 871 311 898">+ Add</div>	<p>Click + Add to add a new user group. In the Add User Group screen, enter the required information.</p> <div data-bbox="885 693 1615 1260"> <div> <div>Add User Group</div> <div>×</div> </div> <div>Name*</div> <div><input type="text"/></div> <div>Description</div> <div><input type="text"/></div> <div> <div>Cancel</div> <div>Add</div> </div> </div>						

8. Click Next.
9. In Step 3, Permissions, set or update the permission for each role. The roles are Enterprise Administrator, Enterprise Operator, Service Provider Administrator, and Service Provider Operator. The permission for each role is selected by default, and you can update it. The role permissions are Edit, Hide, and Read. This screen is common for all authentication types.

Add LDAP Authentication Profile

Settings ✓ User And Group Profile ✓ **3 Permissions** 4 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. Click Next to go to Step 4, Review and Submit. The following screen is common for all authentication types.

Add Versa Directory Authentication Profile

Settings ✓ Users And User Groups ✓ Permissions ✓ **4 Review & Submit**

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

General

Name Description

Tags

Press Enter to add

Settings [Edit](#)

Cache Expiry Time (mins) 10

Users & User Groups [Edit](#)

Users(0) User Groups(0)

No users No user groups

Permissions [Edit](#)

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

Cancel Back **Save**


11. In the General box, enter a name for the rule, and optionally, enter a text description for the rule and one or more

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

Updated: Wed, 23 Oct 2024 08:02:38 GMT

Copyright © 2024, Versa Networks, Inc.

tags.

12. Review the selected settings. Click the  Edit icon to change a setting, as needed.
13. Click Save to create the authentication profile.

Supported Software Information

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

Additional Information

[Configure User and Device Authentication](#)