
Configure User and Device Authentication

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

For users who are using an SD-WAN device to connect to a SASE gateway over an IPsec tunnel, you can create rules to authenticate both the user and the device. You can use user and device authentication to authenticate traffic that enters through Versa SASE gateways to access security services using a non-Versa SASE client. For example, you can authenticate users who connect from a remote location using a site-to-site tunnel to the SASE cloud gateway. You can authenticate these users and devices before SASE gateways route the traffic to internet or private applications.

To authenticate users and devices, you create authentication profiles and create rules to filter users.

To define rules for user and device authentication, you can select destination zones, IP addresses, SASE services, and schedules 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.

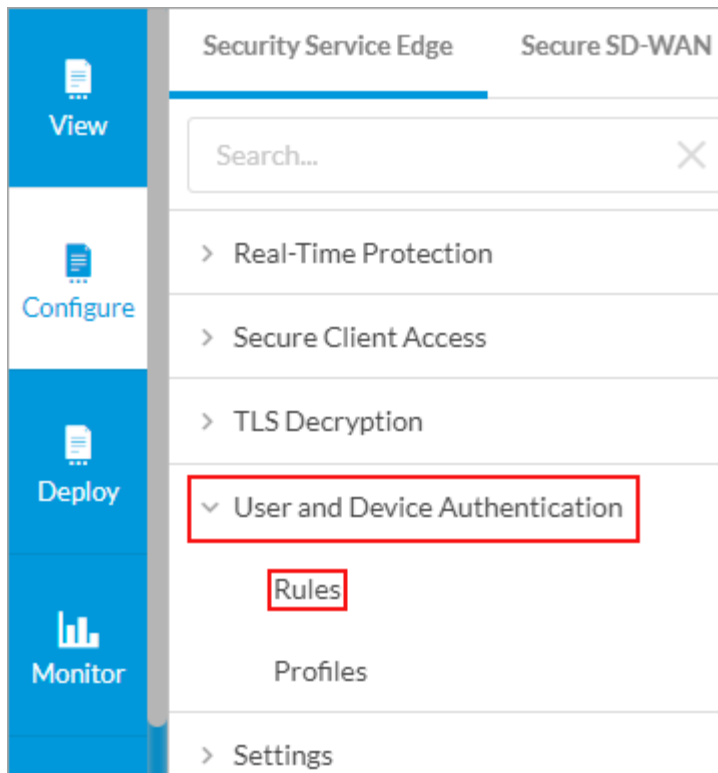
You configure user and device authentication profiles to specify the authentication type for user authentication. You use these authentication profiles in user and authentication rules to specify the method to authenticate users who match the authentication rule criteria.

For information about configuring user and group authentication for Releases 11.3.1 and earlier, see [Configure User and Device Authentication](#).

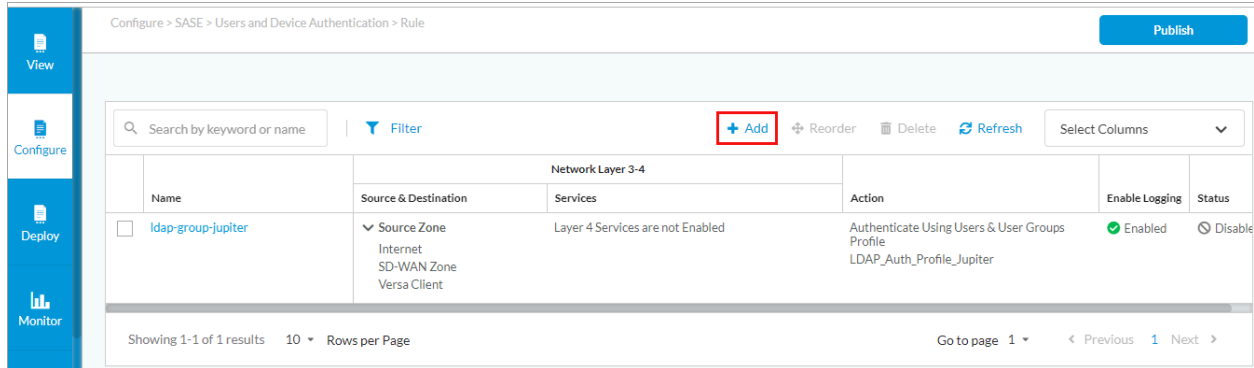
Configure User and Device Authentication Rules

To configure user and device authentication rules for SASE users and groups:

1. Go to Configure > Security Service Edge > User and Device Authentication > Rules.



The Rule screen displays.



2. To create a new users and groups profile, click + Add. The Create Users and Device Authentication Rule window displays the first step of the workflow:
 - For Releases 12.1.1 and later, the first step is Applications and URLs.
 - For Releases 11.4.1 and earlier, the first step is Network Layer 3-4. Skip to Step 11 of this procedure to continue.
3. For Releases 12.1.1 and later, in Step 1, Applications and URLs, select the match criteria for applications, reputations, and URLs. By default, all applications, URLs, and reputations are included in the match criteria.

Configure > SASE > Users and Device Authentication > Rule

Create Users and Device Authentication Rule

1

2

3

4

Applications & URLs Network Layer 3-4 Action 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 below.

Applications

URL Categories & Reputations

Applications

Application Group

Applications

Application Category

App-Group-1

Search for Application Group

+ Add New Clear All

✓ User Defined Application Groups

Selected: 1 of 1

App-Group-1

✓ Predefined Application Groups

Selected: 0 of 23

ADP-Apps

Adobe-Apps

Amazon-Apps

Box-Apps

Citrix-Apps

Concur-Apps

Docusign-Apps

Dropbox-Apps

Google-Apps

GotoMeeting-A...

IBM-Apps

Intuit-Apps

Jira-Apps

LinkedIn-Apps

Office365-Apps

Oracle-Apps

SAP-Apps

Salesforce-Apps

Social-Media

Twitter-Apps

Webex-Apps

Zendesk-Apps

Zoho-Apps

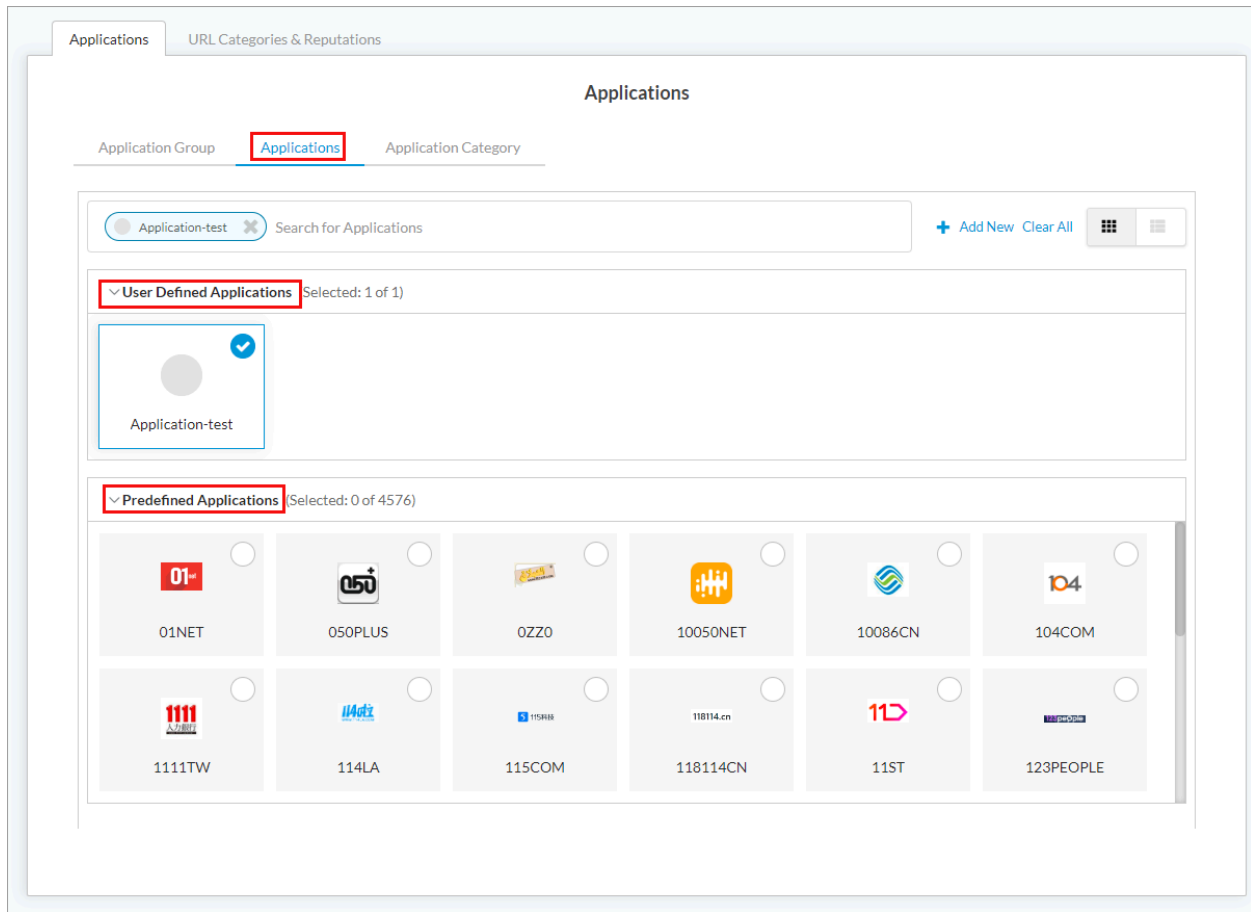
Cancel

Back

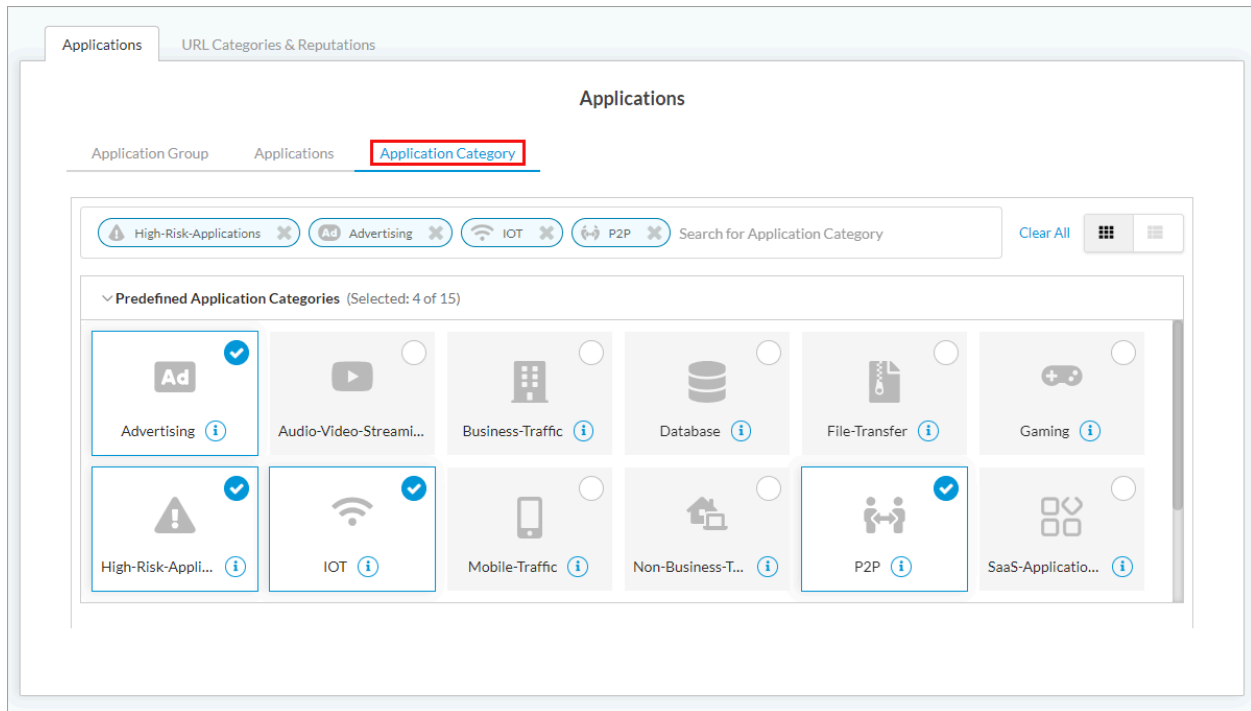
Skip to Review

Next

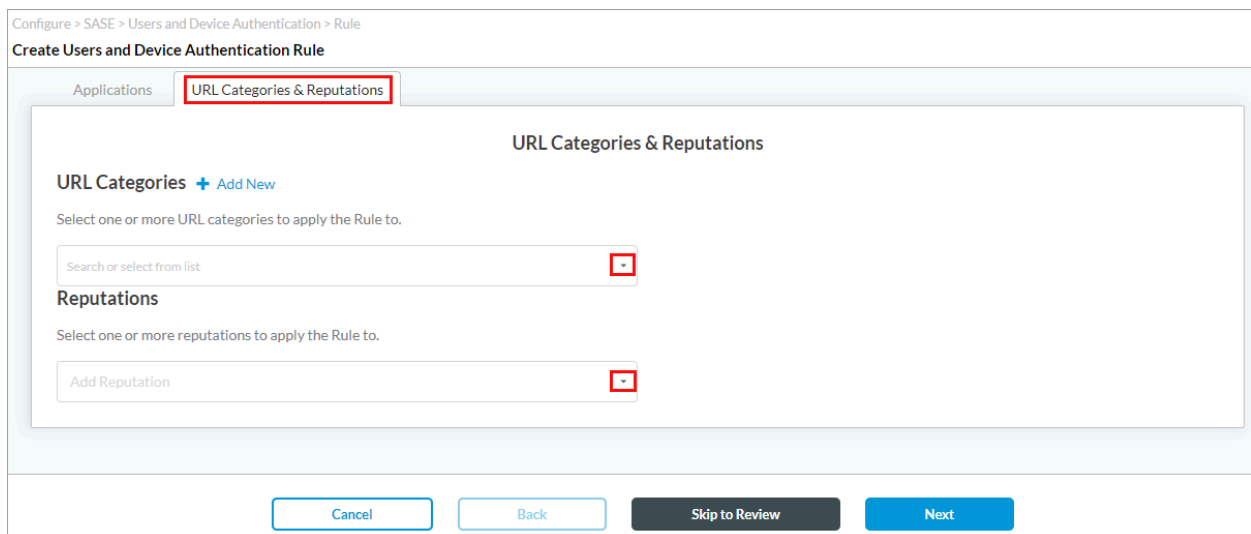
4. Select the Applications > Application Group tab, and then select one or more user-defined and predefined application groups for the rule to match.
5. Select the Applications > Applications tab, and then select one or more user-defined and predefined applications for the rule to match.



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



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



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.

11. In Step 1, Network Layer 3-4 (for Release 11.4.1) or in Step 2, Network Layer 3-4 (for Releases 12.1.1 and later), you can customize the Layer 4 services, Layer 3 source and destination information, and schedules to which the previously selected security enforcements should apply. By default, all traffic receives the previously selected security enforcements.

Configure > SASE > Users and Device Authentication > Rule

Create Users and Device Authentication Rule

1 Network Layer 3-4 2 Action 3 Review & Submit

All traffic is selected, and it will receive the previously selected security enforcements

If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

Services ☒ All layer 4 services Customize

Source & Destination (Layer 3) Customize

Schedule ☒ None Selected Customize

Cancel Back Skip to Review Next

12. To customize the Layer 4 services, click Customize in the Services pane.

1 Network Layer 3-4 2 Action 3 Review & Submit

All traffic is selected, and it will receive the previously selected security enforcements

If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

Services ☒ All layer 4 services Customize

Source & Destination (Layer 3) Customize

Schedule ☒ None Selected Customize

The Services window displays.

Configure > SASE > Users and Device Authentication > Rule

Create Users and Device Authentication Rule

1

2

3

Network Layer 3-4

Action

Review & Submit

All traffic is selected, and it will receive the previously selected security enforcements

If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

← Back

Services

Services refer to matching traffic based on IP protocol number or TCP/UDP port numbers. Versa has a predefined list of well known services (e.g. ESP,SSH, HTTP etc) that the user can select from. If a custom service has been created before then it can be selected here.

Services

Search or select from list

Services(User Defined: 1 | Predefined: 741)

All Services

+ Add UserDefined

	Name	Type	Protocol	Source Port	Destination Port	Source Or Destination Port
<input type="checkbox"/>	rish	User Defined	AH			
<input type="checkbox"/>	3com-amp3	Predefined	TCP	any	629	
			UDP	any	629	
<input type="checkbox"/>	3com-tsmux	Predefined	TCP	any	106	
			UDP	any	106	
<input type="checkbox"/>	914c-g	Predefined	TCP	any	211	
			UDP	any	211	
<input type="checkbox"/>	914c/g	Predefined	TCP	any	211	
			UDP	any	211	
<input type="checkbox"/>	9pfs	Predefined	TCP	any	564	
			UDP	any	564	
<input type="checkbox"/>	BFD-CONTROL	Predefined	TCP	any	3784	
			UDP	any	3784	
<input type="checkbox"/>	BFD-ECHO	Predefined	TCP	any	3785	
			UDP	any	3785	
<input type="checkbox"/>	BFD-MULTI-CTL	Predefined	TCP	any	4784	
			UDP	any	4784	
<input type="checkbox"/>	CAIlic	Predefined	TCP	any	216	
			UDP	any	216	

Showing 1-10 of 742 results

10 Rows per Page

Go to page 1

< Previous

1

2

...

Next >

Cancel

Back

Skip to Review

Next


13. To find a service, enter the name of the service in the Services field, and then press Enter, or click All Services and then select User-defined Services or Predefined Services to filter the list of service objects.
14. To add a custom service object, click + Add User-Defined. The Service window displays. For more information, see [Configure SASE Services](#).


15. To customize the source and destination information for a rule, in Network Layer 3-4 screen, click Customize in the Source and Destination Layer box.


Configure > SASE > Users and Device Authentication > Rule
Create Users and Device Authentication Rule

1 2 3
Network Layer 3-4 Action Review & Submit

All traffic is selected, and it will receive the previously selected security enforcements
If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

**Services** ⓘ
☒ All layer 4 services
[Customize](#)

**Source & Destination (Layer 3)** ⓘ
[Customize](#)

**Schedule** ⓘ
✓ None Selected
[Customize](#)

Cancel Back Skip to Review Next

16. The Source and Destination (Layer 3) window displays. Select the Source Address tab, and then enter information for the following fields.

1

2

3

Network Layer 3-4ActionReview & Submit

All traffic is selected, and it will receive the previously selected security enforcements

If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

← Back

Source & Destination (Layer 3)

The Source Destination section represents Layer 3 of the network layer traffic. Layer 3 transmits data segments between networks in the form of packets. When you message your friend, this layer assigns source and destination IP addresses to the data segments. Your IP address is the source, and your friend's is the destination.

[More Information](#)

Source Address

Destination Address

Source Zones

Destination Zones

☐ Negate Source Address

[+ Add Address Group](#)

<input type="checkbox"/>	Name	Total	IP Addresses
<input type="checkbox"/>	Addressgroup-SASE	5	23.4.5.0/24, 23.4.5.34-23.4.5.64, google.com, ab, 45.6.7.0/0.0.34.45
<input type="checkbox"/>	AG1	1	1.1.1.1-1.1.1.11
<input type="checkbox"/>	AG10	1	uuu
<input type="checkbox"/>	AG100	2	*vera.com, abcd
<input type="checkbox"/>	Ag3	1	*abcd.com

Showing 1-5 of 5 results10Rows per PageGo to page 1Previous1Next

IP Subnet ⓘ

IP Range ⓘ

IP WildCard ⓘ

Field	Description
Negate Source Address	Click to match any source addresses except the configured addresses.
Address Group	Select an address group to match. To add a source address group, click + Add Address Group. The Address Group screen displays. For more information, see Configure Address Group Objects .
IP Subnet	Enter an IPv4 or IPv6 subnet.
IP Range	Enter an IP address range.
IP Wildcard	Enter a list of wildcard IP addresses.

17. Select the Destination Address tab, and then enter information for the following fields.

1

2

3

Network Layer 3-4ActionReview & Submit

All traffic is selected, and it will receive the previously selected security enforcements

If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

← Back

Source & Destination (Layer 3)

The Source Destination section represents Layer 3 of the network layer traffic. Layer 3 transmits data segments between networks in the form of packets. When you message your friend, this layer assigns source and destination IP addresses to the data segments. Your IP address is the source, and your friend's is the destination.

[More Information](#)

Source Address

Destination Address

Source Zones

Destination Zones

☐ Negate Destination Address

Search

☐

Name

Total

IP Addresses

☐

Addressgroup-SASE

5

23.4.5.0/24, 23.4.5.34-23.4.5.64, google.com, ab, 45.6.7.0/0.0.34.45

☐

AG1

1

1.1.1.1-1.1.1.11

☐

AG10

1

uuu

☐

AG100

2

*vera.com, abcd

☐

Ag3

1

*abcd.com

Showing 1-5 of 5 results

10

Rows per Page

Go to page 1

< Previous

1

Next >

IP Subnet ⓘ

IP Range ⓘ

IP WildCard ⓘ

Enter a list of IPv4/IPv6 Subnet values

Enter a list of IP Range values

Enter a list of wildcard values

Field	Description
Negate Destination Address	Click to match any destination addresses except the configured addresses.
Address Group	Select an address group to match. To add a source address group, click + Add Address Group. The Address Group screen displays. For more information, see Configure Address Group Objects .
IP Subnet	Enter an IPv4 or IPv6 subnet.
IP Range	Enter an IP address range.
IP Wildcard	Enter a list of wildcard IP addresses.

18. Select the Source Zone tab, the and select the user source zone for which to create authentication rule. You must configure a source zone.

19. Select the Destination Zone tab, and then select the user destination zone for which to create authentication rule.

1 Network Layer 3-4 2 Action 3 Review & Submit

All traffic is selected, and it will receive the previously selected security enforcements
If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

← Back Source & Destination (Layer 3)

The Source Destination section represents Layer 3 of the network layer traffic. Layer 3 transmits data segments between networks in the form of packets. When you message your friend, this layer assigns source and destination IP addresses to the data segments. Your IP address is the source, and your friend's is the destination.

[More Information](#)

Source Address Destination Address Source Zones **Destination Zones**

Destination Zones(0)

20. To customize the schedule for when the rule is in effect, in Network Layer 3-4 screen, click Customize in the Schedule box.

Configure > SASE > Users and Device Authentication > Rule

Create Users and Device Authentication Rule

1 Network Layer 3-4 2 Action 3 Review & Submit

All traffic is selected, and it will receive the previously selected security enforcements
If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

Services ⓘ
All layer 4 services
[Customize](#)

Source & Destination (Layer 3) ⓘ
[Customize](#)

Schedule ⓘ
✓ None Selected
[Customize](#)

Cancel Back Skip to Review Next

The Schedule window displays.

Configure > SASE > Users and Device Authentication > Rule

Create Users and Device Authentication Rule

1
2
3

Network Layer 3-4 Action Review & Submit

All traffic is selected, and it will receive the previously selected security enforcements
If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

← Back
Schedule

Schedule Hours

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

+ Add New

Cancel
Back
Skip to Review
Next

21. Select a schedule object to set the time and frequency when the rule to take effect.
22. Click + Add New to add a new schedule. The Schedule window displays. For more information, see [Configure SASE Schedules](#).
23. Click Next. The Step 2, Action (for Release 11.4.1) or Step 3, Action (for Releases 12.1.1 and later) displays.

Configure > SASE > Users and Device Authentication > Rule

Create Users and Device Authentication Rule

✓
2
3

Network Layer 3-4 Action Review & Submit

Select Rule Action

Select the action to impose on the traffic for applications and URLs.

Do Not Authentication
(No Authentication)

Authenticate Using Users & User Groups Profile

Cancel
Back
Skip to Review
Next

24. If you do not want to authenticate users for the match criteria you selected above, click Do Not Authenticate.
25. 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.

Configure > SASE > Users and Device Authentication > Rule

Create Users and Device Authentication Rule

✓

2

✓

Network Layer 3-4

Action

Review & Submit

Select Rule Action

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

- Click Next. The Step 3, Review and Submit (for Release 11.4.1) or Step 4, Review and Submit (for Releases 12.1.1 and later) displays.

Configure > SASE > Users and Device Authentication > Rule

Create Users and Device Authentication Rule

✓ Network Layer 3-4
 ✓ Action
 3 Review & Submit

Please give your rule a name:

General

Name * ⓘ

Rule Name

Description

Enter description name

Tags

Press Enter to add

☐ Logging is Disabled
 ☒ Rule is Enabled

Network Layer 3-4

[Edit](#)

Services

✓ All Services

Source

Zones

✓ SD-WAN Zone

Action

[Edit](#)

Do Not Authentication

Cancel
Back
Save

27. In the General section enter a name for the rule. Optionally, enter a description and add tags for the rule.
28. To enable logging for the rule, slide the toggle to Enabled.
29. The rule is enabled by default. Slide the Rule is Enabled toggle to disable the rule.
30. Click Edit next to any section to make changes.
31. Click Save.

Configure User and Device Authentication Profiles

To specify the authentication type 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. For Releases 12.1.1 and later, you can also configure user and device certificate-based profiles. You can configure both an LDAP and a SAML profile for an enterprise, but for RADIUS and Versa Directory profiles types, you can configure only one per enterprise. You can configure user and device certificate-based profiles with each other, or with LDAP or SAML authentication profiles.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_User_and_Device_...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_User_and_Device_...)

Updated: Wed, 23 Oct 2024 08:38:04 GMT

Copyright © 2024, Versa Networks, Inc.

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.

Certificate-based authentication is a secure method to validate the identity of users and devices. For Releases 12.1.1 and later, Versa SASE supports user and device certificate-based authentication. When you enable certificate-based authentication, the gateway initiates a request to the SASE client for users to provide their certificates during client portal registration and gateway connection.

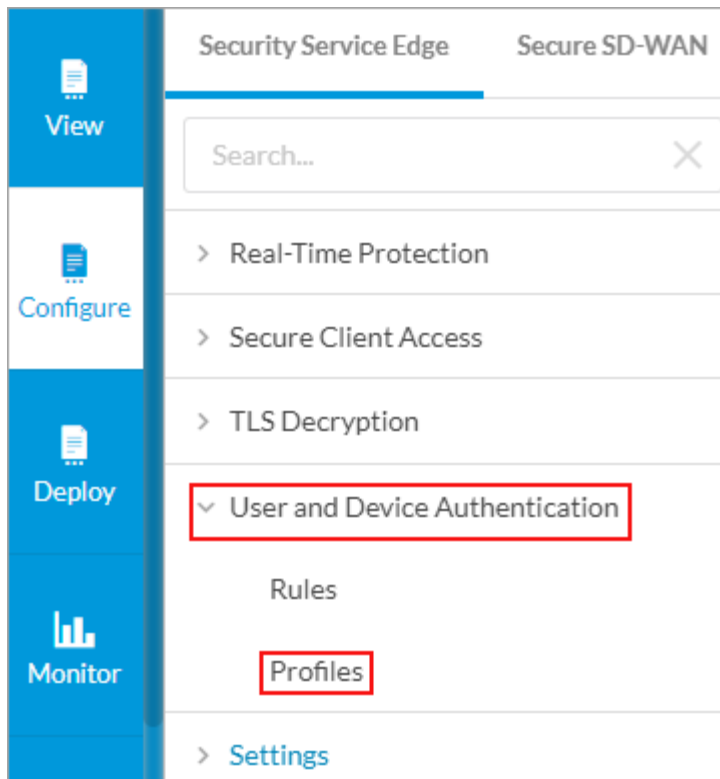
Note: You must configure the following SASE rules, profiles, and settings in a specific order:

1. Configure users and groups, and then publish them to the gateway, as described in this article.
2. Configure site-to-site tunnels. For more information, see [Configure SASE Site-to-Site Tunnels](#).
3. Configure secure client access profiles and rules. For more information, see [Configure SASE Secure Client Access Rules](#).

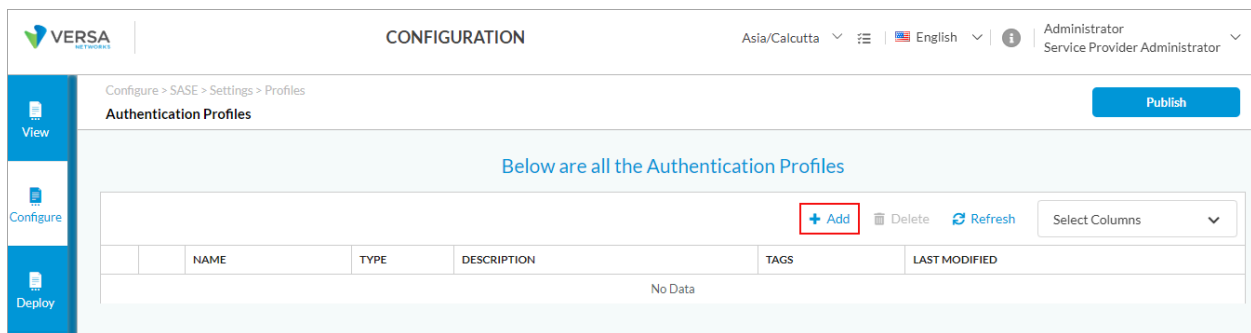
You do not need to configure the remaining SASE rules, profiles, and settings in a specific order.

To configure user and device authentication profiles:

1. Go to Configure > Security Service Edge > User and Device Authentication > Profiles.



The Authentication Profiles screen displays.



2. To create a new profile, click + Add.
 - For Releases 12.1.1 and later, the Add User and Device Authentication Profile screen displays.

Add User and Device Authentication Profile

Select which user / device 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.

Note: LDAP authentication profile can be combined with SAML, User Certificate Based and Device Certificate Based authentication profiles.

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).

Note: SAML authentication profile can be combined with LDAP, User Certificate Based and Device Certificate Based authentication profiles.

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.

Note: RADIUS authentication profile can not be combined with other authentication profiles.

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.

Note: Versa Directory authentication profile can not be combined with other authentication profiles.

User Certificate Based

Note: User certificate based authentication profile can be combined with LDAP, SAML and device certificate based authentication profiles.

Device Certificate Based

Note: Device certificate based authentication profile can be combined with LDAP, SAML and user certificate based authentication profiles.

Cancel Get Started

- For Releases 11.4.1 and earlier, the Add Profile screen displays.

Configure > SASE > Users and Device Authentication > Profiles

Add Profile Publish

Choose which authentication type you wish to use and complete it's settings. Once the authentication has been configured, you'll be able to make changes later.

Select Type

☒ LDAP ☐ SAML ☐ RADIUS ☐ Versa Directory

Cancel Next

3. Select the type of authentication to configure:
 - (For Releases 12.1.1 and later.) Select one of the following options: Device Certificate Based, LDAP, RADIUS, SAML, User Certificate Based, or Versa Directory.
 - (For Releases 11.4.1 and earlier.) In the Select Type field, click one of the following options: LDAP, RADIUS, SAML, or Versa Directory.
4. Click Next (or Get Started for Releases 12.1.1 and later).
5. For the LDAP authentication type, the following screen displays. Enter information for the following fields.

Configure > SASE > Users and Device Authentication > Profiles

Publish

Add Profile

Define Settings

Server Type

Active Directory

Select either FQDN or IP Address *

☒ FQDN

☐ IP Address

VPN Name *

Tenant1000-Enterprise

Port *

389

☒ Enable SSL

SSL Mode

CA Certificate

--Select--

+ Add New

Bind DN *

Bind Password *

Base DN *

Domain Name *

Domain Base



Add Another Server

Cancel

Back

Next

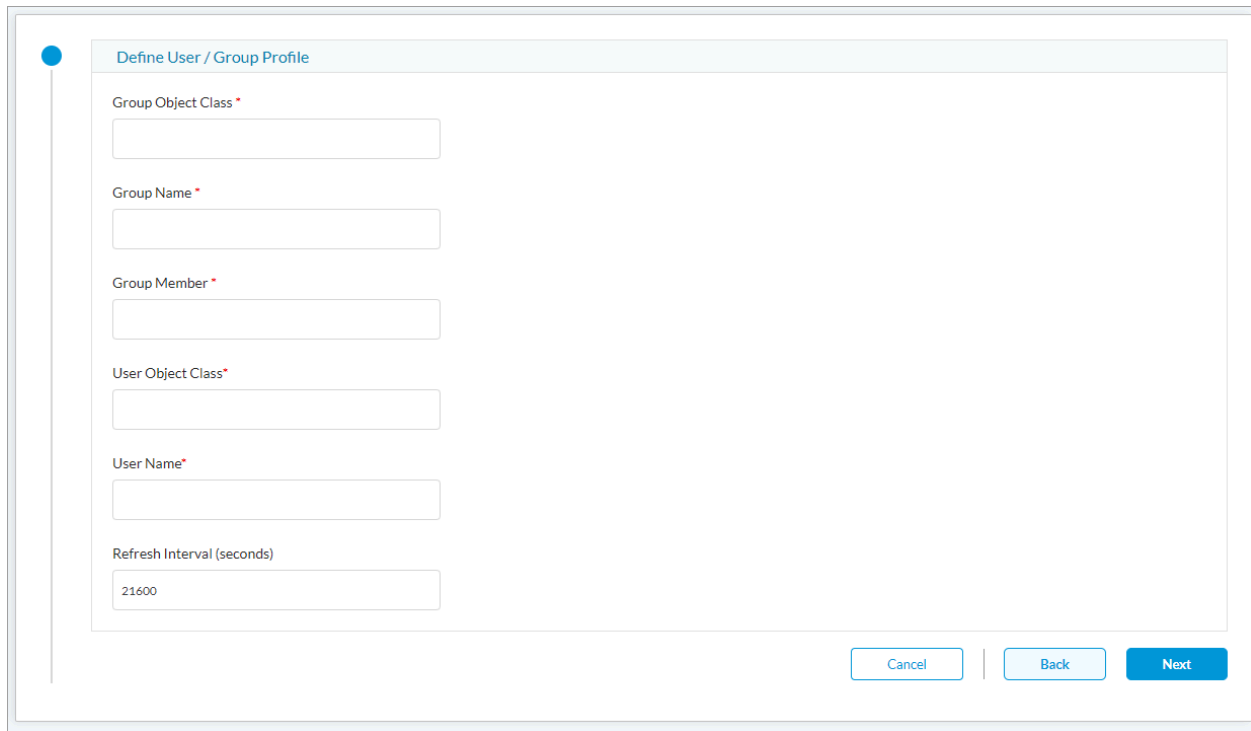
Field	Description
Server Type	Select the server type:

Field	Description
	<ul style="list-style-type: none"> ◦ Active Directory ◦ Open LDAP
Select Either FQDN or IP Address	Click FQDN or IP Address, and then enter the FQDN or IP address of the Active Directory or LDAP server.
VPN Name	Select the name of the tenant VPN to use to reach the LDAP server.
Port	<p>Enter the listening port number on the LDAP server, which allows you to communicate with the LDAP directory service.</p> <p><i>Range:</i> 0 through 65535</p> <p><i>Default:</i> None</p>
Enable SSL	<p>Click the slider to enable SSL for the LDAP session.</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	If you enable SSL, select the CA certificate to use for the secure LDAP connection. To add a new CA

Field	Description
	<p>certificate, click + Add New, and then enter the required information.</p> <div> <div>Add CA Certificate</div> <div> <div>Certificate Type</div> <div> <input checked="" type="checkbox"/> Ca Chain </div> </div> <p>Allowed file formats are .crt, .cer or .pem</p> <p>CA-Chain Name *</p> <input type="text"/> <div> <div>Upload File</div> <div> <div>Cancel</div> <div>Add</div> </div> </div> </div>
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 distinguished name 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.
Add Another Server	Click to add another server of the same type. In the Add Another Server popup window, enter the required information, and then click Add.

Field	Description
	<div><div>Add Another Server</div><div>Select either FQDN or IP Address *</div><div><div><input checked="" type="radio"/> FQDN</div><div></div></div><div><div><input type="radio"/> IP Address</div><div></div></div><div>Port *</div><div>389</div><div>VPN Name*</div><div>Tenant1000-Enterprise</div><div><div>Cancel</div><div>Add</div></div></div>

- 6. Click Next.
- 7. The Define User/Group Profile screen displays. Enter information for the following fields.



Field	Description
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	<p>Enter how often to refresh the LDAP profile information, in seconds.</p> <p><i>Range:</i> 60 through 86400 seconds</p> <p><i>Default:</i> 21600 seconds</p>

- Click Next. The Provide Information screen displays. This screen is common for all authentication types. Enter the required information, as described in Step 16.

9. For the SAML authentication type, the following screen displays. Enter information for the following fields.

Configure > SASE > Users and Device Authentication > Profiles

Add Profile

Publish

Define Settings

Select SAML Type

☐

Okta

☐

PingIdentity

☐

Office 365

☐

Azure Active Directory☐

Single Sign-on URL *

Single Sign-out URL

Service Provider Entity ID * ?

Service Provider Certificate

--Select--

+ Add New

Identity Provider Entity ID * ?

Identity Provider Certificate *

--Select--

+ Add New

Prefix ID

Reply URL (Assertion Consumer Reply URL)

https://tenant1000-b1-gw.versa-test.net/secure-access/services/saml/login-consumer

Cancel

Back

Next

Field	Description
Select SAML Type	Select the SAML type: <ul style="list-style-type: none">Azure Active DirectoryOffice 365OktaOtherPingIdentity
Single Sign-on URL (Required)	Enter the URL of the identify provider (IdP) to use for

Field	Description
	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.
Reply URL (Assertion Consumer Reply URL)	Enter the assertion consumer reply URL from which the application receives the authentication token. SAML also refers to this to as the Assertion Consumer Service (ACS).

10. Click Next. The Location of Users and User Groups screen displays. Enter information for the following fields.

For Releases 12.1.1 and later, the following screen displays.

Add User Certificate Authentication Profile

Settings

Additional Authentication Method

Users And User Groups

Review & Submit

User ListGroup List

Upload user list in the following format: csv

Browse

Note: CSV file should be in the following format: UserName*, First Name, and Last Name.

Users (0)

+Add

Delete

User Name

First Name

Last Name

No Data

Cancel

Back

Skip to Review

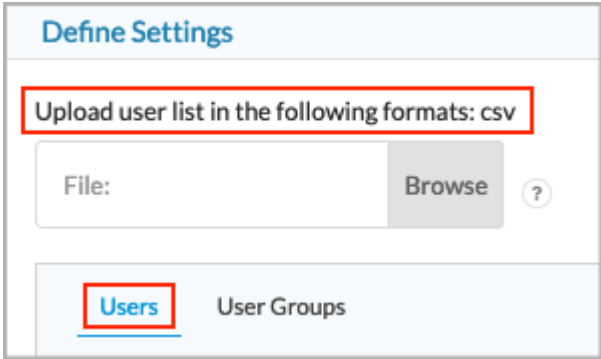
Next

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_User_and_Device_...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_User_and_Device_...)

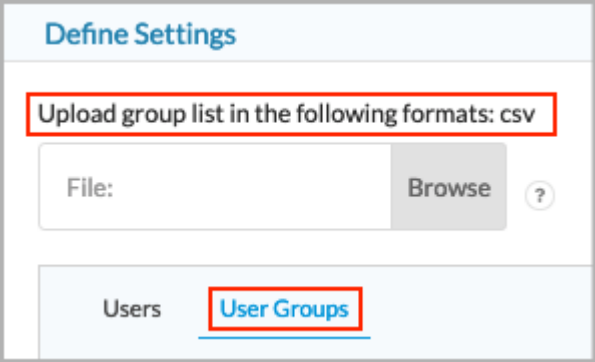
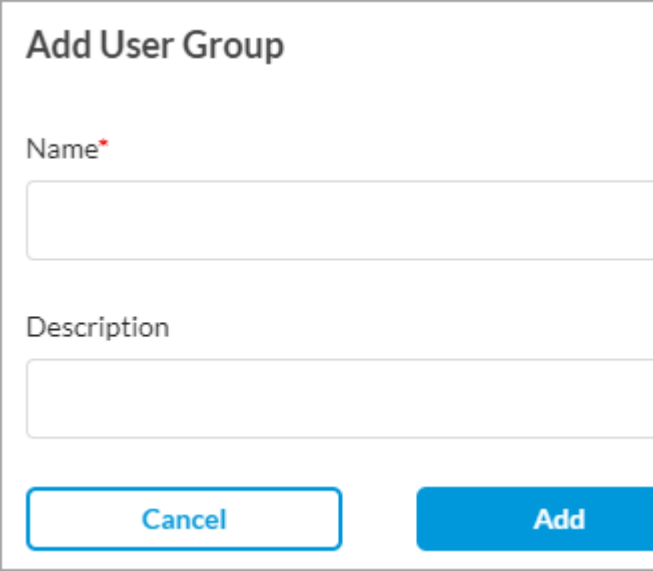
Updated: Wed, 23 Oct 2024 08:38:04 GMT

Copyright © 2024, Versa Networks, Inc.

27

Field	Description
Upload user list in the following formats: csv	<p>If you select the Users tab in the Define Settings section, click File: Browse. In the popup window, select a user list file in CSV format to upload. Each line in the CSV file must be in the following format:</p> <ul style="list-style-type: none"> ◦ User Name*, First Name, Last Name, Password*, Email*, Phone, Description, Group Name. (Note that fields marked with an asterisk (*) are mandatory.) 
Users tab	<p>Click + Add to add a new user. In the Add User screen, enter the required information. When you select LDAP or SAML as the authentication type, the following screen displays:</p>

	<div data-bbox="860 210 1604 955"><div>Add User ✕</div><div>User Name*</div><div></div><div>First Name</div><div></div><div>Last Name</div><div></div><div>Cancel</div><div>Add</div></div> <p>For Versa Directory, the following screen displays when you click + Add to add a user:</p> <div data-bbox="860 1186 1604 1612"><div>Add User</div><div>User Name(Email)*</div><div></div><div>First Name</div><div></div><div>Last Name</div><div></div><div>Phone Number</div><div></div><div>Description</div><div></div><div>Group Name + Add New</div><div></div><div>Cancel</div><div>Add</div></div> <p>Click + Add New to add a new user group, as shown below in the User Groups tab.</p>
Upload group list in the following formats: csv	If you select the User Groups tab in the Define

	<p>Settings section, click File: 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:</p> <ul style="list-style-type: none"> ◦ Group Name*, Description 
<p>User Groups tab</p>	<p>Click + Add to add a new user group. In the Add User Group screen, enter the required information.</p> 

11. Click Next. The Provide Information screen displays. This screen is common for all authentication types. Enter the information as described in Step 16.
12. If you select RADIUS as the authentication type, the following screen displays. Enter information for the following fields.

Configure > SASE > Users and Device Authentication > Profiles

Add Profile Publish

Define Settings

IP Address *

Port *

VPN Name

Tenant1000-Enterprise ▼

Shared Secret *

Cancel Back Next

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.

13. Click Next. The Location of Users and User Groups screen displays. Enter the information as described in Step 10.
14. Click Next. The Provide Information screen displays. This screen is common for all authentication types. Enter the information as described in Step 16.
15. If you select Versa Directory as the authentication type, the Location of Users and User Groups screen displays. Enter the information as described in Step 10.
16. (For Releases 12.1.1 and later.) If you select User Certificate Based as the authentication type, the Add User Certificate Authentication Type screen displays. In the Settings screen, enter information for the following fields.

Add User Certificate Authentication Profile

1

Settings

2

Additional Authentication Method

3

Users And User Groups

4

Review & Submit

Client CA Chain*

--Select--

+ Add New

Username Identifying Field in Certificate *

--Select--

Cache Expiry Time

10mins

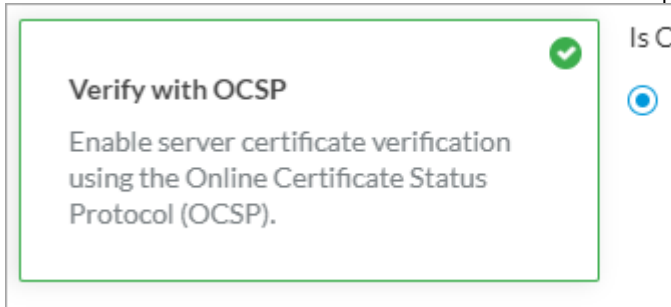
Verify with OCSP

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

Cancel

Skip to Review

Next

Field	Description
Client CA Chain (Required)	Select the client CA certificate chain to authenticate the user. To add a new CA certificate, click + Add New. The Add CA Certificate window displays. For more information, see Configure SASE Certificates .
Username Identifying field in Certificate (Required)	<p>Select the field that Concerto uses to validate a name match in the client certificate:</p> <ul style="list-style-type: none"> ◦ Subject-Alternative-name Email ◦ Subject Alternative-name Principal Name ◦ Subject Common-name
Cache Expiry Time	<p>Enter the time in minutes after which the cache expires.</p> <p><i>Default:</i> 10 minutes</p>
Verify with OSCP	<p>Click to enable verification of server certificate using Online Certificate Status Protocol (OCSP). The following fields display:</p>  <p>Yes is selected by default and if you select Yes, Concerto uses the CA server on the internet for OCSP verification.</p> <p>If you select No, enter the VPN name to check for to server certificate.</p>

17. Click Next or select Step 2, Additional Authentication Method. The following screen displays.

Add User Certificate Authentication Profile

Settings **2 Additional Authentication Method** Users And User Groups Review & Submit

By enabling multi-factor authentication, you can include an additional authentication method such as LDAP, SAML, RADIUS and Versa Directory.

☐ Multi-factor Authentication Disabled

Cancel Back Skip to Review Next

18. To enable multi-factor authentication using LDAP or SAML profiles, slide the Multi-factor Authentication Disabled toggle. This is disabled by default.

☒ Multi-factor Authentication Enabled

Below are your available options:

No profile has been added [Add Profile](#)

19. If LDAP and SAML profiles are configured, the profiles display.
20. Click Add Profile to add a profile. For adding LDAP profiles, follow Step 5 through 7 and for SAML profile, follow Steps 9 through 11.
21. Click Next. The Users and User Groups screen displays. Enter the information as described in Step 10.
22. (For Releases 12.1.1 and later.) If you select Device Certificate Based as the authentication type, the Add Device Certificate Authentication Type screen displays. In the Settings screen, enter information as described in Step 16.

Add Device Certificate Authentication Profile

1 Settings 2 Authentication Order 3 Review & Submit

Client CA Chain*
--Select--
[+ Add New](#)

Username Identifying Field in Certificate*
--Select--

Cache Expiry Time
10 mins

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

Cancel Skip to Review Next

23. Click Next or select Step 2, Authentication Order. The following screen displays.

Add Device Certificate Authentication Profile

1 Settings 2 Authentication Order 3 Review & Submit

Select which profile would you like to authenticate first?

☒ Device Authentication ☐ User Authentication

Cancel Back Skip to Review Next

24. If you have configured a user certificate-based authentication profile, select Device Authentication or User Authentication to specify which profile to use first for authentication. Device Authentication is select by default.
25. (For Releases 11.4.1 and earlier.) Click Next. In the Provide information screen, enter information for the following fields

Configure > SASE > Users and Device Authentication > Profiles

Add Profile Publish

●

Provide Information

Name *

Description (Optional)

Tags (Optional)

Press Enter to add

Cancel

Back

Save

Field	Description
Name	Enter a name for the authentication profile, for example, ACME-SAML-Profile or ACME-LDAP-Profile.
Description	Enter a text description for the text authentication profile.
Tags	Enter tags to associate with the authentication profile.

26. Click Save.
27. (For Releases 12.1.1.) Click Next. The Review and Submit screen displays. This screen is common for all authentication types.

Settings Additional Authentication Method Users And User Groups **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](#)

Client CA Chain	default
Username Identifying Field in Certificate	subject
Verify with OCSP	Disabled
Is CA Server on Internet?	disabled
VPN Name	Test-tenant-Enterprise
Cache Expiry Time (mins)	10

Additional Authentication Method [Edit](#)

Multi-factor Authentication	Disabled
Profile to authenticate first	
Cache Expiry Time (mins)	10

Users & User Groups [Edit](#)

Users(0)	User Groups(0)
No users	No user groups

Cancel Back Save

28. In the General box, enter a name for the rule, and optionally, enter a text description for the rule and one or more tags.
29. Review the selected settings. Click the [Edit](#) icon to change a setting, as needed.
30. Click Save to create the authentication profile.

Configure Versa Directory Authentication Using an IAM Server

You can use an identity and access management (IAM) server to store local-user data and to send activation emails to local users. Concerto uses the users and groups profile to store user data and then uses IAM user APIs to store user data on the IAM server. IAM user API calls are asynchronous. You can track these calls in the Concerto Tasks screen,

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_User_and_Device_...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_User_and_Device_...)

Updated: Wed, 23 Oct 2024 08:38:04 GMT

Copyright © 2024, Versa Networks, Inc.

which opens after you complete and save the User and Groups configuration screen.

Tasks

All

Search

Auto Refresh every 15 secs

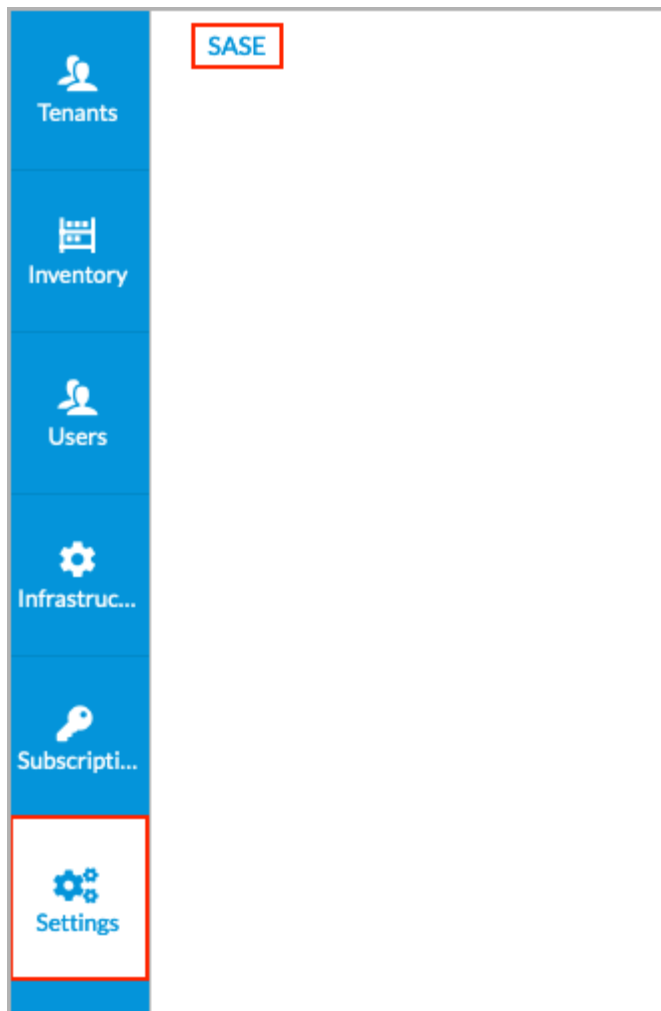
Refresh now

USER	NAME	DESCRIPTION	START TIME	END TIME	PROGRESS
▼ Administrator	IAM Server user(s) sync	Create SASE user(s) in IAM Server for tenant SASE-SDWAN-T003	1/17/2023 4:29:48 PM	1/17/2023 4:30:12 PM	✓
<div> <div>Task ID: 00041b36-e7c4-4908-b857-eeee962c73</div> <div> <div>Messages:</div> <ul style="list-style-type: none"> • Fetching users from IAM server • Constructing IAM server user payload • Creating users [user1@gmail.com, user2@gmail.com] on IAM server • IAM task UUID 8cab2262-bec5-439d-8ed2-cbd8016cd805 • Waiting for IAM task 8cab2262-bec5-439d-8ed2-cbd8016cd805 to be completed • Waiting for IAM task 8cab2262-bec5-439d-8ed2-cbd8016cd805 to be completed • IAM task 8cab2262-bec5-439d-8ed2-cbd8016cd805 status completed • Success Users [user1@gmail.com, user2@gmail.com] • Successfully synced SASE local users to IAM Server </div> </div>					
▶ Administrator	IAM Server user(s) sync	Delete SASE user(s) on IAM Server for tenant SASE-SDWAN-T003	1/17/2023 4:23:52 PM	1/17/2023 4:23:53 PM	✓
▶ Administrator	IAM Server user(s) sync	Update SASE user(s) in IAM Server for tenant SASE-SDWAN-T003	1/17/2023 4:23:15 PM	1/17/2023 4:23:30 PM	✓
▶ Administrator	IAM Server user(s) sync	Update SASE user(s) in IAM Server for tenant SASE-SDWAN-T003	1/17/2023 4:22:21 PM	1/17/2023 4:22:22 PM	✓
▶ Administrator	IAM Server user(s) sync	Create SASE user(s) in IAM Server for tenant SASE-SDWAN-T003	1/17/2023 4:20:13 PM	1/17/2023 4:20:37 PM	✓

Note: Only newly created Users and Groups profiles use the IAM server.

To configure SASE IAM server information:

1. Log in as a service provider system administrator.
2. Go to Settings > SASE.



3. In the SASE Infrastructure Settings screen, enter information for the following fields.

Settings > SASE

SASE Infrastructure Settings

Below are your SASE Infrastructure Settings

Root Domain

versanow.net

☐ Use Tenant Name in GW FQDNs

SASE Client Software Location

URL

User Name

Password

SASE IAM Server Detail

FQDN/IP*

URL*

User Name*

Password*

LDAP Configuration

Domain Name*

LDAP Base*

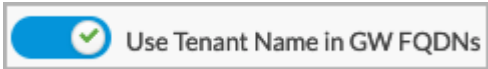
Bind DN*

Password*

Certificate Name*

Cancel

Save

Field	Description
Root Domain	Enter the root domain, for example, versanow.net.
Use Tenant Name in GW FQDNs	<p>Click the slider to use the tenant name in the SASE gateway FQDNs.</p> 
SASE IAM Server Detail (Group of Fields)	
◦ FQDN/IP	Enter the FQDN of the SASE IAM server.
◦ URL	Enter the URL of the SASE IAM server.
◦ Username	Enter the username to use for the SASE IAM server.
◦ Password	Enter the password to use for the SASE IAM server.
SASE Client Software Location (Group of Fields)	
◦ URL	Enter the URL where the SASE client software is

Field	Description
	located.
◦ Username	Enter the username to use to access the SASE client software location.
◦ Password	Enter the password to use to access the SASE client software location.
LDAP Configuration (Group of Fields)	
◦ Domain Name	Enter the LDAP domain name.
◦ LDAP Base	Enter the LDAP base domain name.
◦ Bind DN	Enter the bind distinguished name (DN) to use when logging in to the LDAP server.
◦ Password	Enter the password that the bind DN uses when logging in to the LDAP server.
◦ Certification Name	Enter the name of the certificate to use for the LDAP connection.

4. Click Save.

Supported Software Information

Releases 11.4.1 and later support all content described in this article, except:

- Release 12.1.1 adds support for device certificate and user certificate-based authentication profiles.

Additional Information

[Configure SASE User-Defined Objects](#)

[Configure User and Device Authentication](#)