
Configure User and Group Policy



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

You create user and user group security policies to detect the users and user groups who are using applications on your network. The security policies help to identify who may have transferred files or transmitted threats. User and user group policies identify users based on their name or role rather than their IP address.

Creating user group policies simplifies firewall administration, because you do not have to update the rules whenever a group's membership changes.

For Releases 21.2.2 and earlier, NGFW supports LDAP and SAML authentication. For Releases 22.1.3 and later, NGFW can use certificate, LDAP, local profile, Kerberos, RADIUS, and SAML for user and group authentication.

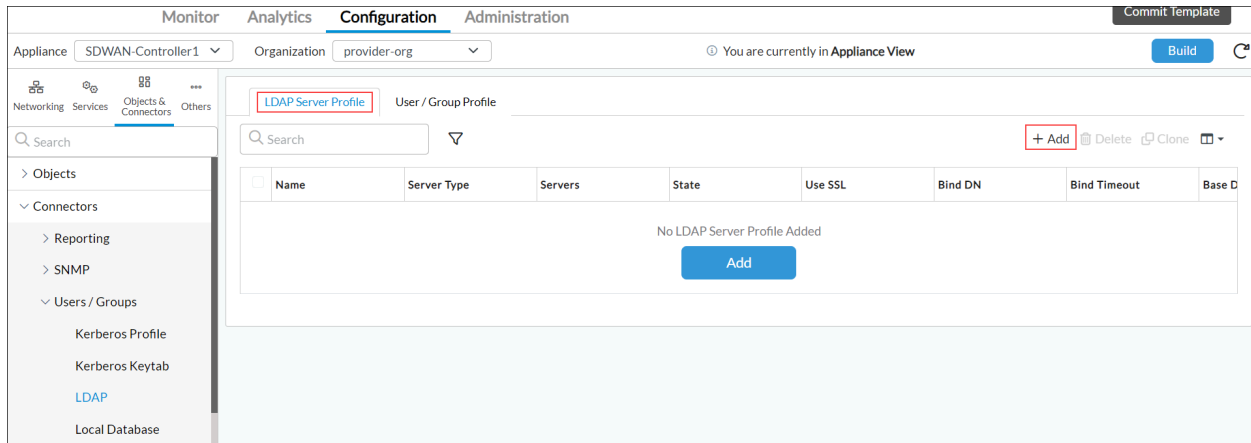
Configure an LDAP Server Profile

You configure an LDAP server profile to define how NGFW connects to and authenticates the Active Directory server and how it searches the Active Directory and retrieves the group list and associated list members.

Before you begin the configuration process, ensure that you have the bind distinguished name (DN) authentication credentials and the bind password. You can get this information from the LDAP administrator.

To configure an LDAP server for Active Directory authentication:

1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select a device name in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects and Connectors > Connectors > Users/Groups > LDAP in the left menu bar.
4. Select the LDAP Server Profile tab, and then click the **+** Add icon.



5. In the Add LDAP Server Profile popup window, select the General tab and enter information for the following fields.


The screenshot shows the 'Add LDAP Server Profile' popup window. The 'General' tab is selected. The form contains the following fields and controls:

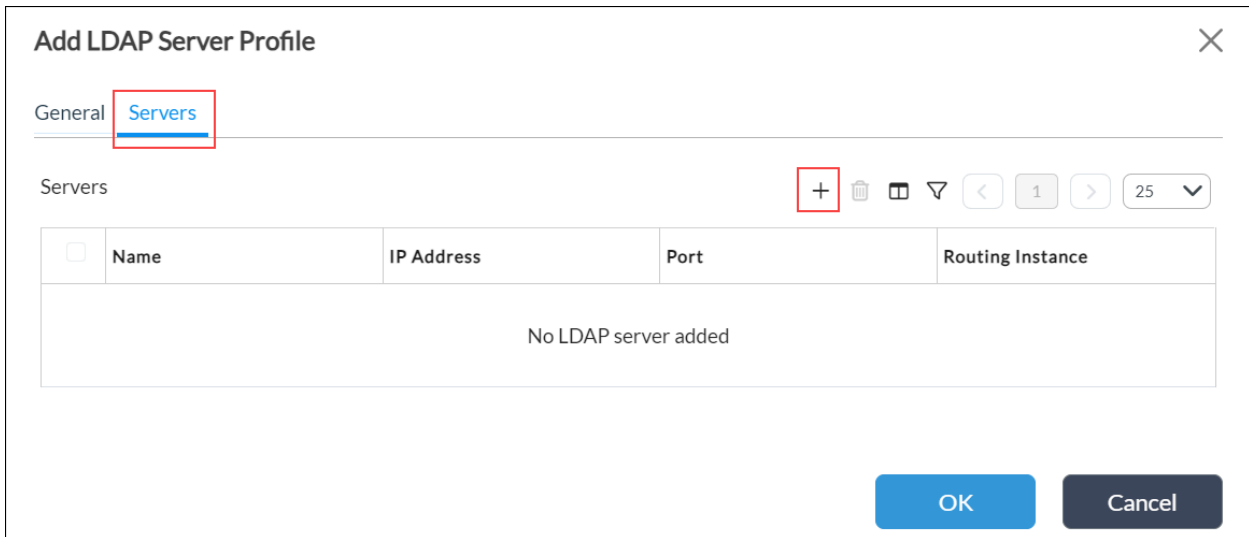
- Name ***: Text input field.
- Description**: Text input field.
- Tags**: Text input field.
- Server Type ***: Dropdown menu with 'Active Directory' selected.
- Domain Base**: Text input field.
- Domain Name ***: Text input field.
- Base DN ***: Text input field.
- Bind DN ***: Text input field.
- Bind Password ***: Text input field with a visibility toggle icon.
- Bind Timeout ***: Text input field with value '30'.
- Search Timeout ***: Text input field with value '30'.
- Use SSL**: Radio buttons for 'Enable' and 'Disable' (selected).
- State**: Radio buttons for 'Enable' (selected) and 'Disable'.
- SSL Mode**: Dropdown menu with 'LDAPS' selected.
- CA Certificate**: Dropdown menu with '--Select--' selected.

At the bottom right, there are 'OK' and 'Cancel' buttons.

Field	Description
Name	Enter a name for the LDAP server profile. NGFW uses this name to connect to the LDAP directory to retrieve group mapping information and to select the usernames and group names for the profile.
Description	Enter a text description for the LDAP server profile.
Tags	Enter a keyword or phrase that allows you to filter the profile name. This is useful when you have many profiles and want to view those that are tagged with a particular keyword.
Server Type	Select Active Directory as the location of the LDAP server. NGFW populates the LDAP attributes in the group mapping settings on this server.
Domain Base	Enter the domain base of the LDAP directory to fetch domain attributes.
Domain Name (Required)	Enter the domain name in which the LDAP server resides.
Base DN (Required)	Enter the base DN of the LDAP directory location. NGFW initiates a search for user and group information at this location.
Bind DN (Required)	Enter the bind distinguished name (DN) authentication credentials for binding to the LDAP tree.
Bind Password (Required)	Enter the bind password.
Bind Timeout (Required)	Enter the bind timeout period, in seconds. <i>Default: 30 seconds</i>
Search Timeout (Required)	Enter the search timeout period, in seconds.
Use SSL (Group of Fields)	Click enable to use SSL for the LDAP session. Click disable not to use SSL for the LDAP session.
<ul style="list-style-type: none"> SSL Mode 	Select the SSL mode for the LDAP session: <ul style="list-style-type: none"> LDAPS—Use secure LDAP (LDAP over SSL). Start TLS—Use LDAP over TLS.








◦ CA Certificate	Select the Certificate Authority (CA) to use for the secure LDAP connection.
State	Click enable to use the LDAP server. Click disable not to use the LDAP server.

6. Select the Servers tab and then click the  Add icon. (Note that for Releases 21.1 and earlier, the General tab and Servers tab fields are on a single tab.)



Add LDAP Server Profile

General **Servers**

Servers      1  25 

<input type="checkbox"/>	Name	IP Address	Port	Routing Instance
No LDAP server added				

OK Cancel

7. In the Add Servers popup window, enter information for the following fields.

Add Servers

×

Name *

IP Address

Port *

Routing Instance

--Select--

FQDN

OK

Cancel

Field	Description
Name (Required)	Enter the hostname of the device hosting the LDAP directory service.
IP Address	Enter the IP address of the LDAP server.
Port (Required)	Enter the number of the listening port on the LDAP server. This is the port that communicates with the LDAP directory service.
Routing Instance	Select the routing instance to use to reach the LDAP server.
FQDN	Enter the full domain name of the LDAP server.

8. Click OK.

Configure Appliance Proxy To Fetch the LDAP User and Group Profile

If a Director node is directly connected to the LDAP server, the Director node can fetch the user and group profile. If the Director node is not connected to the LDAP server, you can configure appliance proxy, which allows a Versa Operating

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_User_a...

Updated: Wed, 23 Oct 2024 08:17:27 GMT

Copyright © 2024, Versa Networks, Inc.

System™ (VOS™) device to act as an LDAP proxy.

To configure an appliance proxy:

1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Organizations in the left menu bar.
 - c. Select an organization In the main pane, and then click the Appliance Proxy icon.

The screenshot shows the Versa Networks Director View interface. The top navigation bar includes tabs for Director View, Appliance View, and Template View. Below this is a secondary navigation bar with Monitor, Configuration, Workflows, Administration (selected), and Analytics. A left sidebar contains a search bar and a list of menu items: Organizations, Appliances, Connectors, System, VMS Services, Scheduled Tasks, Notification Configuration, Entitlement Manager, Director User Management, Inventory, SDWAN, Support, and Files and Folders. The main content area displays a table of organizations. The table has columns for Organization Name, Description, Tags, Parent Organization, CMS Connectors, Global Organization ID, and Configured Appliance LDAP. The first row, 'provider-org', is selected. Below the table, there are controls for rows per page (set to 25) and a status bar indicating 'Showing 1 - 11 of 11'. In the top right corner of the main content area, there is a red box highlighting the 'Appliance Proxy' icon.

Organization Name	Description	Tags	Parent Organization	CMS Connectors	Global Organization ID	Configured Appliance LDAP
<input checked="" type="checkbox"/> provider-org	-	-	none	-	20	View More...
<input type="checkbox"/> Tenant1	-	-	provider-org	-	1	View More...
<input type="checkbox"/> Tenant10	-	-	provider-org	-	10	View More...
<input type="checkbox"/> Tenant2	-	-	provider-org	-	2	View More...
<input type="checkbox"/> Tenant3	-	-	provider-org	-	3	View More...
<input type="checkbox"/> Tenant4	-	-	provider-org	-	4	View More...
<input type="checkbox"/> Tenant5	-	-	provider-org	-	5	View More...
<input type="checkbox"/> Tenant6	-	-	provider-org	-	6	View More...
<input type="checkbox"/> Tenant7	-	-	provider-org	-	7	View More...

2. In the Edit Appliance Proxy popup window, enter information for the following fields.

Edit Appliance Proxy

Organization *

provider-org

Appliances *

CASB-DEVICE

LDAP Server Profile *

☐ Deconfigure Appliance Proxy

Existing Appliance Proxy

Appliance	LDAP Server Profile
-----------	---------------------

OK

Cancel

Field	Description
Organization (Required)	Displays the organization.
Appliances (Required)	Select the VOS device. The drop-down list lists all VOS devices associated w
LDAP Server Profile (Required)	Select the LDAP server profile.
Deconfigure Appliance Proxy	Click to disable the appliance proxy.

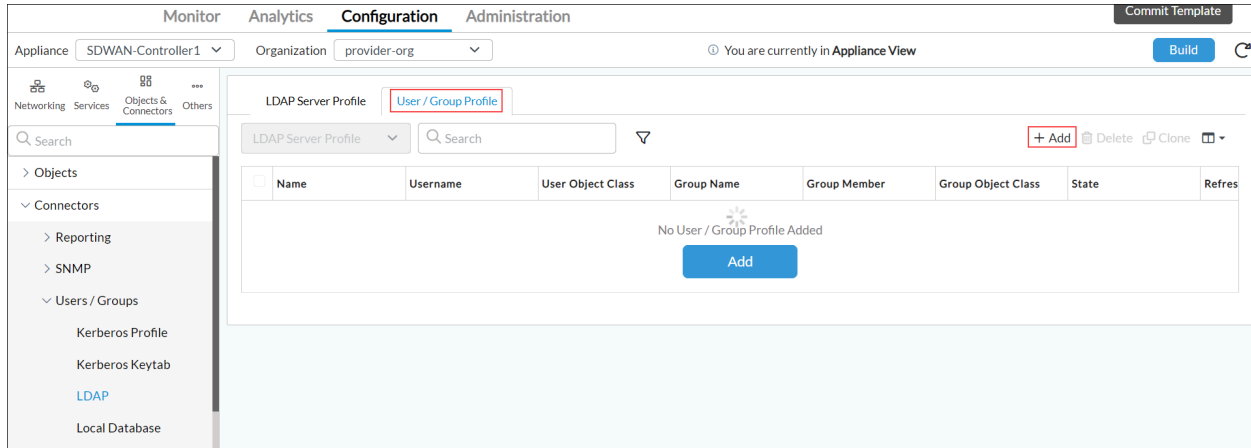
- Click OK.

Configure a User and Group Mapping Profile

To configure a user and group mapping profile:

- In Director view:
 - Select the Administration tab in the top menu bar.

- b. Select Appliances in the left menu bar.
 - c. Select a device name in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects and Connectors > Connectors> Users/Groups > LDAP in the left menu bar.
4. Select the User/Group Profile tab, and then click the **+** Add icon.



5. In the Add User/Group Profile popup window, enter information for the following fields.

Add User / Group Profile

Name *

Description

Tags

Group Object Class *

Group Name *

Group Member *

User Object Class *

Username *

Refresh Interval *

Password Max Age

Password Last Set

Email

Mobile

Custom Filter

User

Group

State

☒ Enable
 ☐ Disable

OK

Cancel

Field	Description
Name (Required)	Enter a name for the user and user group profile.
Description	Enter a text description for the user and user group profile.
Tags	Enter a keyword or phrase that allows you to filter the profile name. This is useful when you have many profiles and want to view those that are tagged with a particular keyword.
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.
Username (Required)	Enter the format of the username. An example is User Principal Name.
Refresh Interval (Required)	<p>Enter the time period to refresh the profile.</p> <p><i>Range:</i> 60 through 86400 seconds</p> <p><i>Default:</i> 60 seconds</p>
Password Max Age	Enter the password maximum age provided by your administrator. An example is maxPwdAge.
Password Last Set	Enter the password last set provided by your administrator. An example is pwdLastSet.
Email	Enter the email address provided by your administrator.
Mobile	Enter the mobile provided by your administrator.
Custom Filter (Group of Fields)	
◦ User	Enter the custom filter to query LDAP server for a user belonging to a group. An example is (o=ORG1).
◦ Group	Enter the custom filter to query LDAP server for a group. An example is (o=ORG1).

State	Select to either enable or disable the user/group profile.
-------	--

6. Click OK.

Search User and Group Information

The Director node periodically retrieves the entire listing for users and user groups from the LDAP server, either directly or through an LDAP proxy, and it stores the information in an internal cache. Updating the cache in this way ensures that the listing remains current.

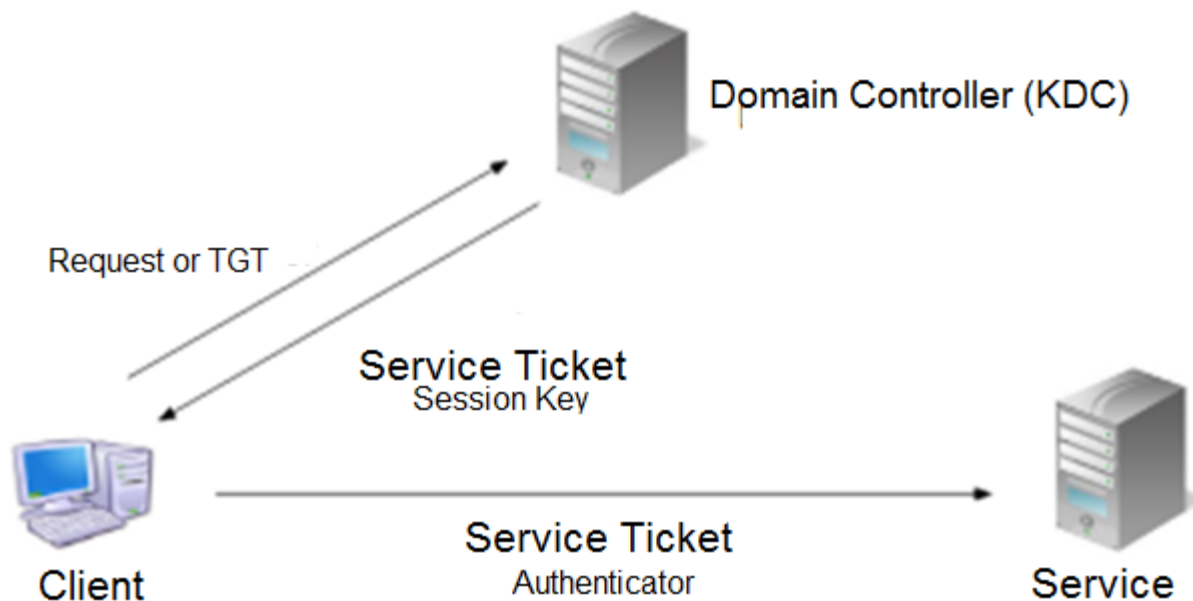
By default, the Director periodically fetches the LDAP user and user group information every 60 minutes, updating the cache after it successfully retrieves the information.

The Director nodes lists the users and user groups that are in the cache. If, at any time, the Director node is unable to fetch the user and user group information from the LDAP server, it lists the information from the previously cached data.

To configure an LDAP proxy, see [Configure Appliance Proxy To Fetch the LDAP User and Group Profile](#), above. For information about configuring security policy, see [Configure NGFW](#).

Define Kerberos for User and Group Authentication

Kerberos provides strong authentication for users and groups, an authentication that is stronger than LDAP. Kerberos uses secret key cryptography, so it never transmits the actual user credentials over the network. The following figure illustrates how Kerberos authentication works.



The client, here, the VOS device, authenticates itself to the authentication server, which forwards the username to the key distribution center (KDC). The KDC issues a ticket-granting ticket (TGT) with a timestamp, encrypts it using the ticket-granting service (TGS) secret key, and returns the encrypted result to the user. After the user verifies the validity of the TGT, the user is granted access to the requested service. The TGS issues a service ticket and a session key to the client. The client then sends the ticket to the service server along with its service request.

To configure Kerberos for user and group authentication, you upload a Kerberos keytab file to the Director node and then you define a Kerberos profile for authenticating users and groups.


Upload the Kerberos Keytab File

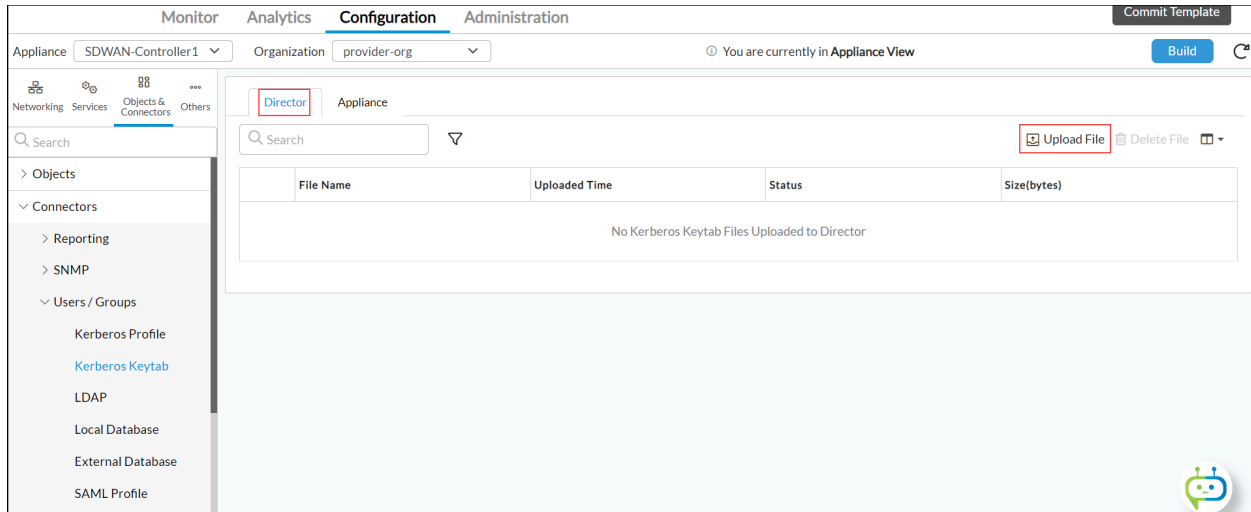
The Kerberos keytab file contains pairs of Kerberos principals and encrypted keys, which are derived from the Kerberos password. You use the Kerberos keytab file to authenticate the systems that use Kerberos without entering the password.

Note: If you change the Kerberos password, you must recreate all the keytabs.

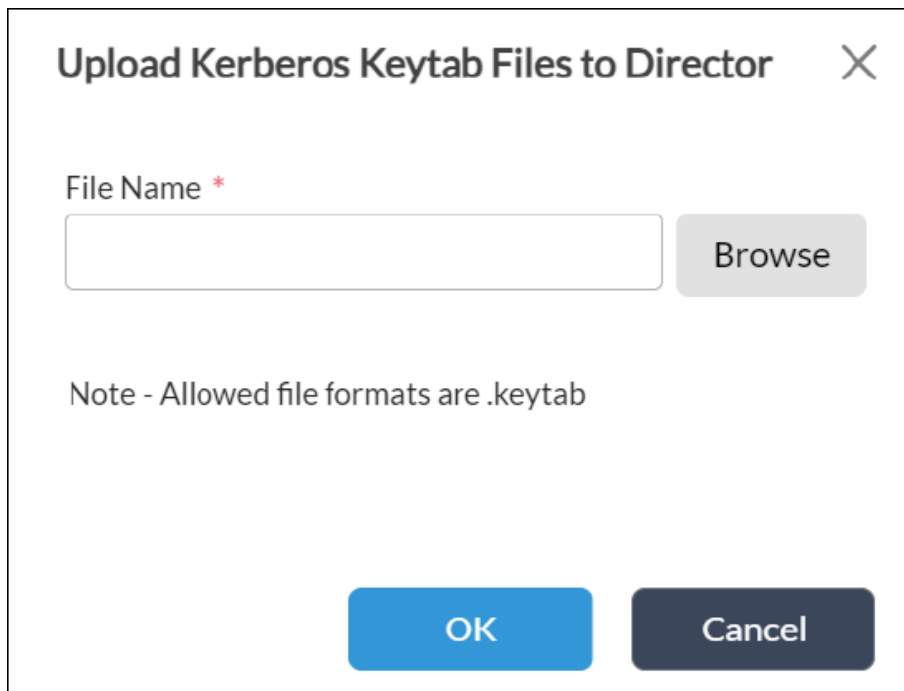
To upload a Kerberos keytab file to the Director node:


1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects and Connectors > Connectors > Users/Groups > Kerberos Keytab in the left menu bar.

4. Select the Director tab, and then click the  Upload File icon to upload the keytab file to the Director node.



5. The Upload Kerberos Keytab Files to Director popup window displays.



6. Click the Browse button, and then select the keytab file.
7. Click OK to upload the keytab file to the Director node.
8. Select the Appliance tab, and then click the  Upload File icon to map the Kerberos keytab file to the VOS device. The Upload Kerberos Keytab Files to Appliance popup window displays.

Upload Kerberos Keytab Files to Appliance

File Name *

Appliance

SDWAN-Controller1

OK

Cancel

9. In the Filename field, select the Kerberos keytab file. The Appliance field is populated by default.
10. Click OK.

Configure a Kerberos Profile

To define a Kerberos profile for authenticating a user and group:

1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects and Connectors > Connectors > Users/Groups > Kerberos Profile in the left menu bar.

Monitor Analytics **Configuration** Administration

Appliance SDWAN-Controller1

Organization provider-org

You are currently in Appliance View

Build

Networking Services **Objects & Connectors** Others

Search

+ Add

Delete

Clone

Search

> Objects

> Connectors

> Reporting

> SNMP

> Users / Groups

Kerberos Profile

Kerberos Keytab

Name

Keytab File

SPN

No Kerberos Profile Added

Add

3. Click the **+** Add icon. In the Add Kerberos Profile popup window, enter information for the following fields.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_User_a...

Updated: Wed, 23 Oct 2024 08:17:27 GMT

Copyright © 2024, Versa Networks, Inc.

13

Add Kerberos Profile

Name *

Description

Keytab File

--Select--

SPN

Virtual URL

OK

Cancel

Field	Description
Name (Required)	Enter a name for the Kerberos profile.
Description	Enter a text description for the Kerberos profile.
Keytab File	Select the keytab file that you uploaded in Upload the Kerberos Keytab File , above.
SPN	Enter the value for the service principal name.
Virtual URL	Enter the Kerberos virtual URL.

- Click OK.


Configure a Local Database

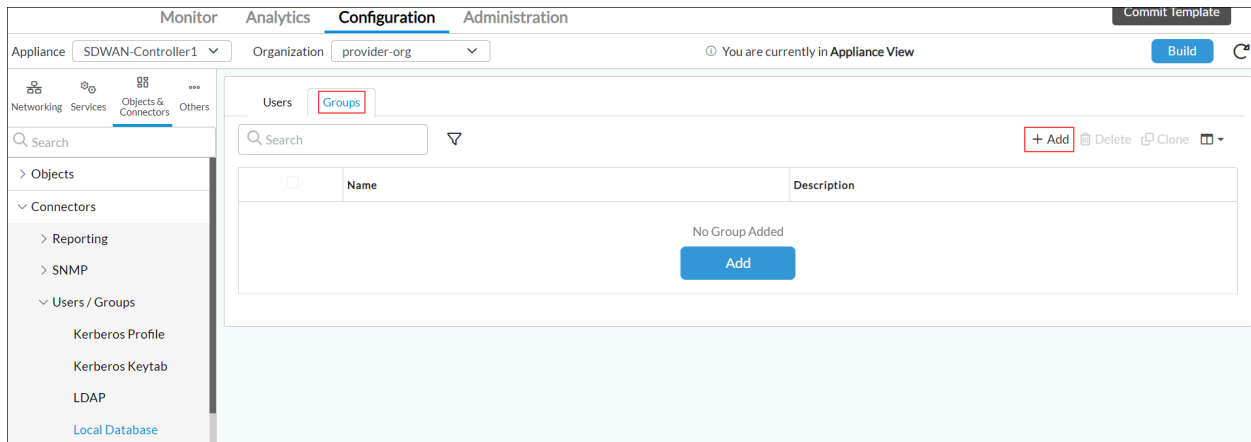
You can store user and group information in a local database on a VOS device, and the VOS device then uses the local database to authenticate, search for, and retrieve users and group membership information. This section describes how to configure local database users and groups.

Note: Configure and use a local database only for small set of users and groups, up to a maximum of 50 to 100. For a larger set of users and groups, it is recommended that you use a third-party user authentication solution, such as LDAP or Kerberos.

Configure Local Database Groups

To configure groups in the local authentication database:

1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects and Connectors > Connectors > Users/Groups > Local Database in the left menu bar.
4. Select the Groups tab, and then click the  Add icon.



5. In the Add Group popup window, enter information for the following fields.

Add Group

×

Name *

Description

OK


Cancel

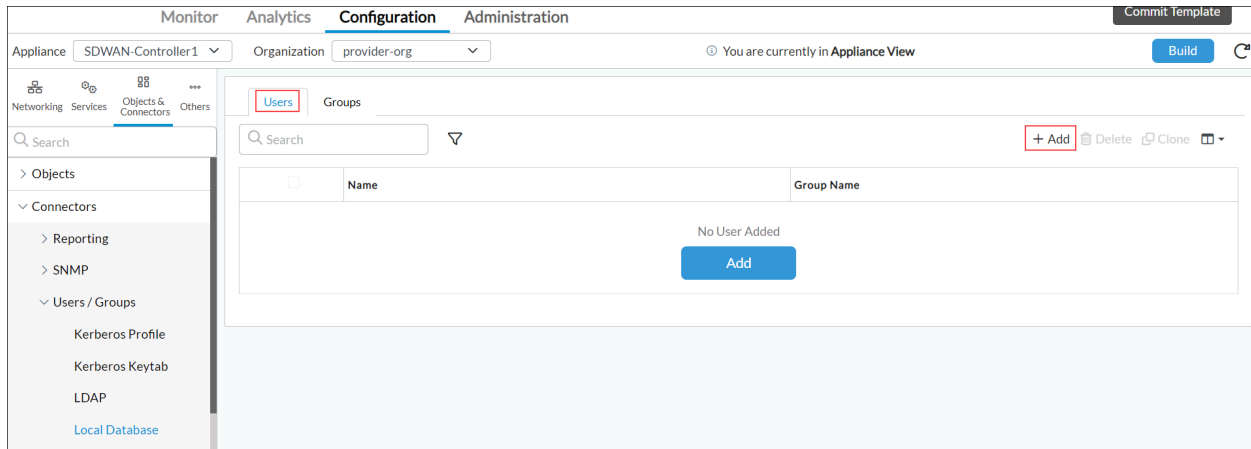
Field	Description
Name (Required)	Enter a name for the local database group.
Description	Enter a text description for the group.

- Click OK.

Configure Local Database Users

To configure users in the local authentication database:

- In Director view:
 - Select the Administration tab in the top menu bar.
 - Select Appliances in the left menu bar.
 - Select a device name in the main panel. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select Objects and Connectors > Connectors > Users/Groups > Local Database in the left menu bar.
- Select the Users tab in the horizontal menu bar, and then click the  Add icon.



5. In the Add User popup window, enter information for the following fields.

×

Add User

Username *

Password *

👁

First Name

Last Name

Email ID

Phone Number

🇺🇸 (201) 555-0123

Description

Group Name

0 selected ▼

OK

Cancel


Field	Description
Username (Required)	Enter a username for the local user.
Password (Required)	Enter the password to authenticate the user.
First Name	Enter the first name of the user.
Last Name	Enter the last name of the user.
Email ID	Enter an email address that can be used for two-factor authentication and to register the user with the system.
Phone Number	Enter a phone number that can be used for two-factor authentication and to register the user with the system.
Description	Enter a text description for the user.
Group Name	Select the group to which the user belongs.

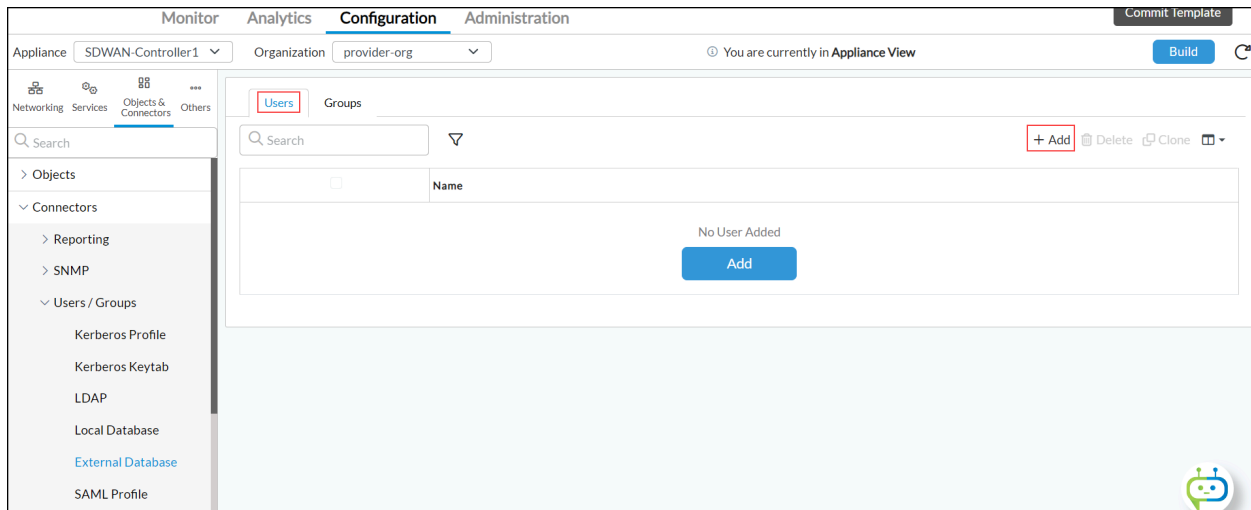
6. Click OK.

Add External Database Users

VOS devices do not load the full database of users into its RAM because it may be too large. Therefore, when you use external authentication, through Kerberos, LDAP, SAML, or TACACS+, you may want to match a specific user or group in the policy. To do this, you define external users that you use in the match condition for CoS (QoS), NGFW, SD-WAN, and UTM policy rules.

To add an external database user:

- In Director view:
 - Select the Administration tab in the top menu bar.
 - Select Appliances in the left menu bar.
 - Select a device name in the main panel. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select Objects and Connectors > Connectors > Users/Groups > External Database in the left menu bar.
- Select the Users tab in the horizontal menu bar, and then click the  Add icon.



5. In the Add User popup window, enter information for the following fields.

Add User

×

Name *

Description

First Name

Last Name

Email ID

Phone Number

🇺🇸 ▼

OK

Cancel

Field	Description
Name (Required)	Enter the name of the external user. This is usually the user's email address.
Description	Enter a text description for the user.
First Name	Enter the first name of the user.
Last Name	Enter the last name of the user.
Email ID	Enter an email address that can be used for two-factor authentication and to register the user with the system.
Phone Number	Enter a phone number that can be used for two-factor authentication and to register the user with the system.

6. Click OK.

Configure SAML Profiles

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

You can configure SAML SSO to log in using a single sign-on and then access multiple services and applications. Similarly, you can configure SAML single sign-out to end sessions for multiple services and applications and then log out from only one session. You can use SAML authentication for services and applications that are external or internal to your organization.

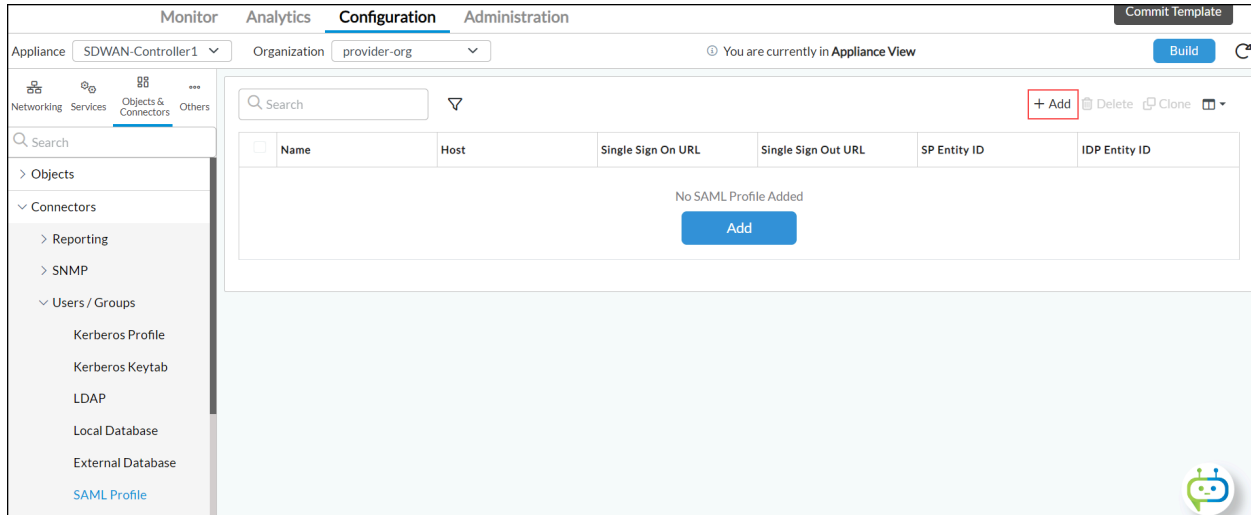
VOS devices use SAML to support user-identification from external identity providers (IdP). You can use any third-party IdP to authenticate users, and you then apply the users, groups, roles, and location security policies on these users. Multiple VOS branch devices can use SAML to authenticate users from a single centrally located authentication server. User authentication is done by the IdP, and the VOS device is aware only of the users. A captive portal is used to send redirections.

To configure SAML, you configure a SAML profile, which contains information about the third-party SAML IDP and other protocol information.

To configure a SAML profile:

1. In Director view:
 - a. Select the Administration tab in the top menu bar.

- b. Select Appliances in the left menu bar.
 - c. Select a device name in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Object and Connectors > Connectors > Users/Groups > SAML Profile in the left menu bar.



4. Click the  Add icon. In the Add SAML Profile popup window, enter information for the following fields.

Add SAML Profile ✕

Name *

Description

Host

Prefix ID

Single Sign On URL

Single Sign Out URL

SP Entity ID

IDP Entity ID

SP Certificate

--Select--

IDP Certificate

--Select--

Group Attribute

OK

Cancel

Field	Description
Name (Required)	Enter a name for the SAML profile.
Description	Enter a text description for the SAML profile.
Host	Enter the name of the host to which to apply the SAML profile.
Prefix ID	Enter the name of the external IdP.
Single Sign-on URL	Enter the URL of the IdP to use for single sign-on.
Single Sign-out URL	Enter the URL to point to for single sign-out.
SP Entity ID	Enter the entity ID of the service provider (that is, the VOS device).
IdP Entity ID	Enter the entity ID that uniquely identifies the SAML identity provider.
SP Certificate	Select the certificate that the service provider uses to authenticate and send a message to NGFW. NGFW uses this authentication information and provides access to the applications and services.
IdP Certificate	Select the authentication certificate issued by the identity provider. The IdP and NGFW use this certificate to sign SAML messages.
Group Attribute	Enter the SAML group attribute to identify group value from the SAML response.

5. Click OK.

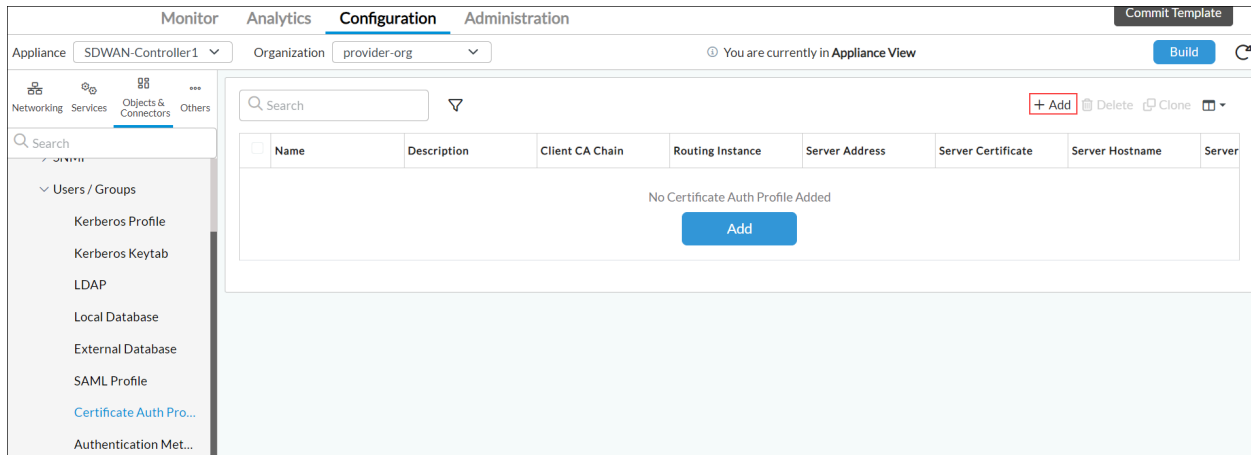
Configure a Certificate Authentication Profile

You configure a certificate authentication profile to use when you configure an authentication profile. For more information, see [Configure an Authentication Method](#), below.

To define a certificate authentication profile:

1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select a device name in the main pane. The view changes to Appliance view.

2. Select the Configuration tab in the top menu bar.
3. Select Object and Connectors > Connectors > Users/Groups > Certificate Authentication Profile in the left menu bar.



4. Click the **+** Add icon. In the Add Certificate Authentication Profile popup window, enter information for the following fields.

Add Certificate Auth Profile

Name *

Description

Server Certificate *

--Select--

Server Hostname *

Server Port *

Client CA Chain *

--Select--

UserName Field

Subject Common-name

SNAT Pool

--Select--

Routing Instances *

☐

+

⌵

Routing Instances Not Configured

Server Addresses

☐

+


⌵

Server Addresses Not Configured

☐ Verify OCSP

OK

Cancel

Field	Description
Name (Required)	Enter a name for the certificate authentication profile.
Description	Enter a description for the certificate authentication profile.
Server Certificate (Required)	Select the server certificate for certificate authentication.
Server Hostname (Required)	Enter a hostname to start certificate authentication service.
Server Address (Required)	Enter the server address to start certificate authentication service.
Server Port (Required)	Enter the port number to start certificate authentication service.
Client CA Chain (Required)	Select the CA chain to authenticate client certificate.
Username Field	<p>Select the field that the VOS software uses to validate a name match in the client certificate:</p> <ul style="list-style-type: none"> ◦ Alternative-name Email ◦ Subject Alternative-name Principal Name ◦ Subject Common-nameSubject
SNAT Pool	Select an SNAT pool. To create an SNAT pool, click +SNAT Pool. For more information, see Configure SNAT Pools .
Routing Instances (Required)	Click the  Add icon and select the routing instances to reach the certificate authentication server.
Server Addresses	Enter the WAN-VR IP address to start certificate authentication service.
Verify OCSP	Click to use the Online Certificate Status Protocol (OCSP) to verify a certificate authentication.

5. Click OK.

Configure SMTP Server Settings

For Releases 21.2.1 and later.

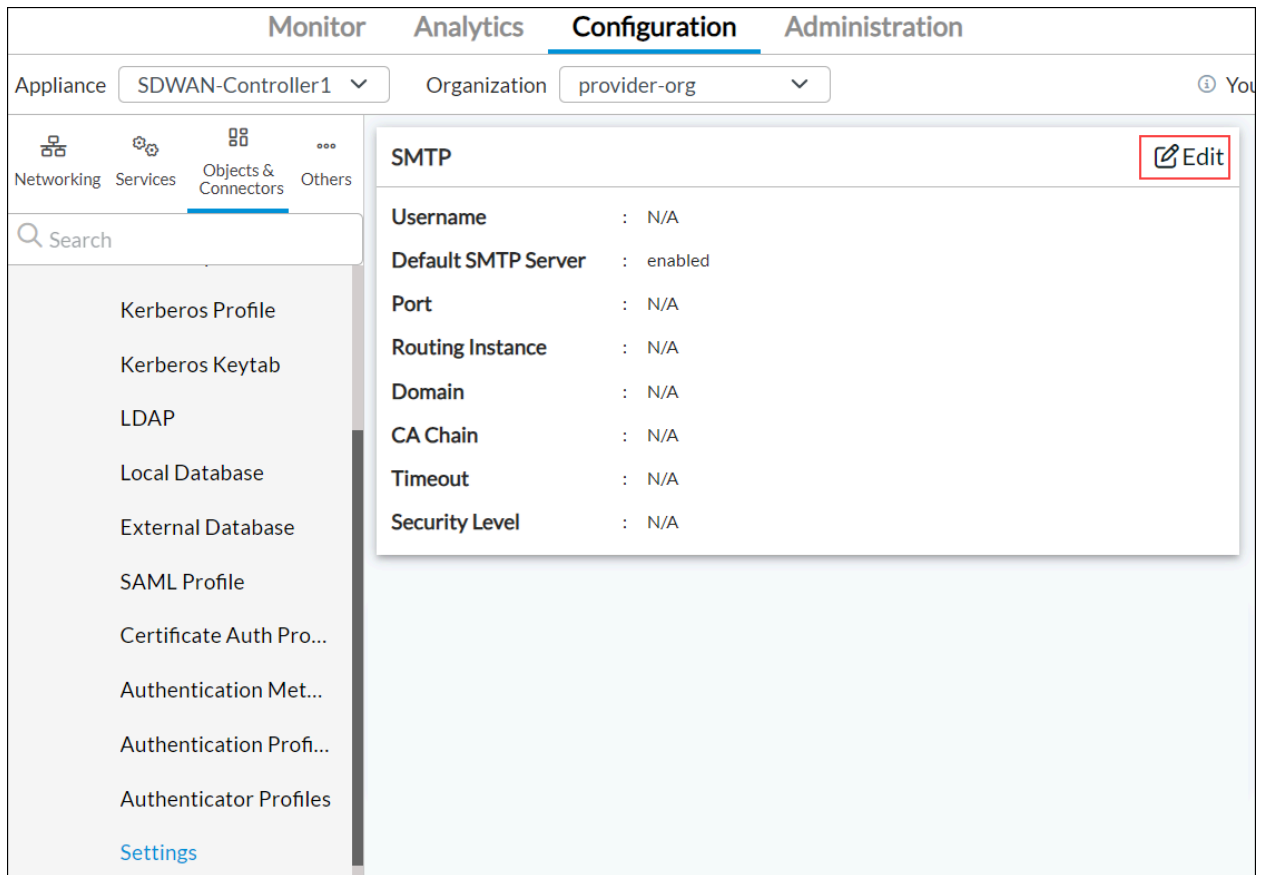
For Versa secure access (VSA), you configure SMTP server settings to support two-factor authentication (2FA). For more information about VSA, see [Configure the Versa Secure Access Service](#) and [Use the Versa SASE Client Application](#).


With VSA, you can generate a one-time password (OTP) that is shared using SMS or email. When the OTP is shared by email, it is sent using the SMTP server details that you set in the SMTP server settings. The dynamically generated authentication code that a user enters allows you to verify the user's enterprise credentials and to determine whether they are using a cell phone or email.

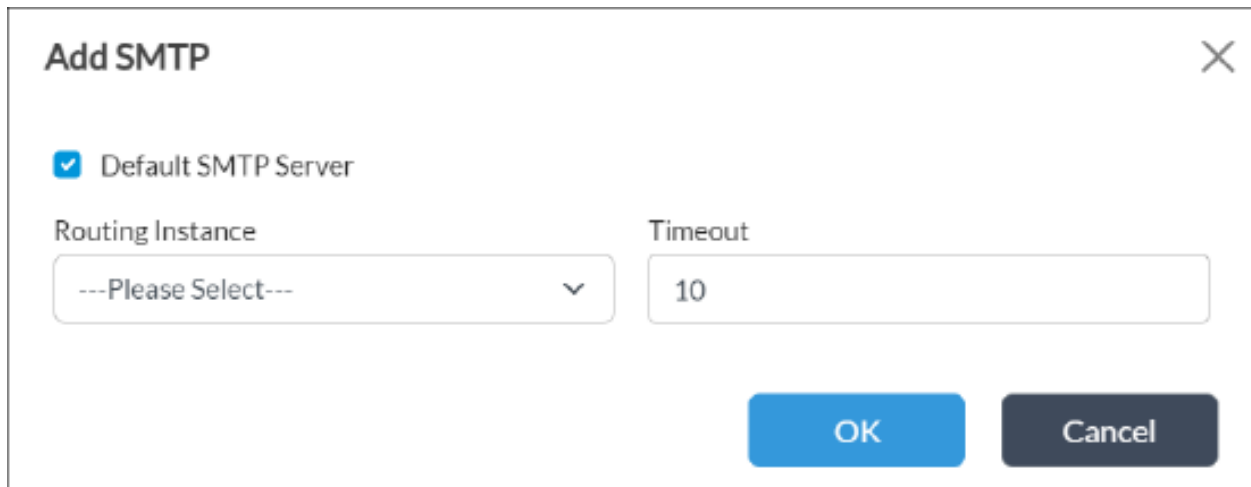
By default, SMTP server settings are enabled and they use the default SMTP server. You can customize the SMTP server configuration.

To configure SMTP server settings:

1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Object and Connectors > Connectors > Users/Groups > Settings > in the left menu bar. The main pane displays the SMTP settings pane.



- Click the  Edit icon. The Add SMTP popup window displays.



- Clear the Default SMTP Server checkbox, and then enter information for the following fields.

Add SMTP

☐ Default SMTP Server

Routing Instance

---Please Select---

▼

Timeout

10

Host

Port

Username

Password

👁

Security Level

---Please Select---

▼

CA Chain

---Please Select---

▼

OK

Cancel

Field	Description
Routing Instance	Select the routing instance to use for the SMTP server.
Timeout	Enter the time, in seconds, after which the connection request to the SMTP server times out. <i>Default:</i> 10 seconds
Host	Enter the FQDN or IP address of the SMTP server.
Port	Enter the port number to use on the SMTP server. <i>Range:</i> 0 to 65353
Username	Enter the username to use to connect to the SMTP server.
Password	Enter the password of the user to connect to the SMTP server.
Security Level	Select the security level to use to connect to the SMTP server: <ul style="list-style-type: none"> ◦ Plain text ◦ SMTPS ◦ StartTLS
CA Chain	Select the CA chain to use to validate the x509 certificate.

6. Click OK.

Configure Active User Distribution for VMS

For Releases 22.1 and later.

You use active user distribution to apply uniform user or group-based policies for user traffic across gateways. When you enable active user distribution, when a user connects to a gateway or branch, the user login or logout information is shared across all branches or gateways using a Versa Messaging Server (VMS).

To configure active user distribution:

1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Object and Connectors > Connectors > Users/Groups > Settings in the left menu bar.
4. In the main pane, click the Edit icon in the Active User Distribution section. In the Manage Active User Distribution popup window, enter information for the following fields.

Manage Active User Distribution ✕

Send
☒ Enable ☐ Disable

Receive
☒ Enable ☐ Disable

Messaging Server
☒ Profile ☐ Provider

Key

Profile Name

Field	Description
Send	<ul style="list-style-type: none"> ◦ Disable—Click to disable the sending of user login and logout events to VMS. This is the default. ◦ Enable—Click to enable the sending of user login and logout events to VMS.
Receive	<ul style="list-style-type: none"> ◦ Disable—Click to disable the receiving of user traffic information. This is the default. ◦ Enable—Click to enable the receiving of user traffic information.
Messaging Server (Group of Fields)	Configure the VMS messaging server.
<ul style="list-style-type: none"> ◦ Profile 	<p>Configure a VMS profile. Enter information for the following fields.</p> <ul style="list-style-type: none"> ◦ Key—Enter the authentication key for the VMS that shares user information. ◦ Profile Name—Enter the name of the profile VMS profile to share user information.
<ul style="list-style-type: none"> ◦ Provider 	<div data-bbox="873 1094 1624 1411"> <p>Messaging Server</p> <p> <input type="radio"/> Profile <input checked="" type="radio"/> Provider </p> <p>Key <input type="text"/></p> <p> Provider Profile <input type="text"/> Provider Tenant Name <input type="text"/> </p> </div> <p>Configure a VMS provider. Enter information for the following fields.</p> <ul style="list-style-type: none"> ◦ Key—Enter the authentication key for the VMS server that shares user information. ◦ Provider Profile—Enter the name of VMS profile for which to share user information. ◦ Provider Tenant Name—Enter the provider tenant name for which to share user information.

5. Click OK.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_User_a...

Updated: Wed, 23 Oct 2024 08:17:27 GMT

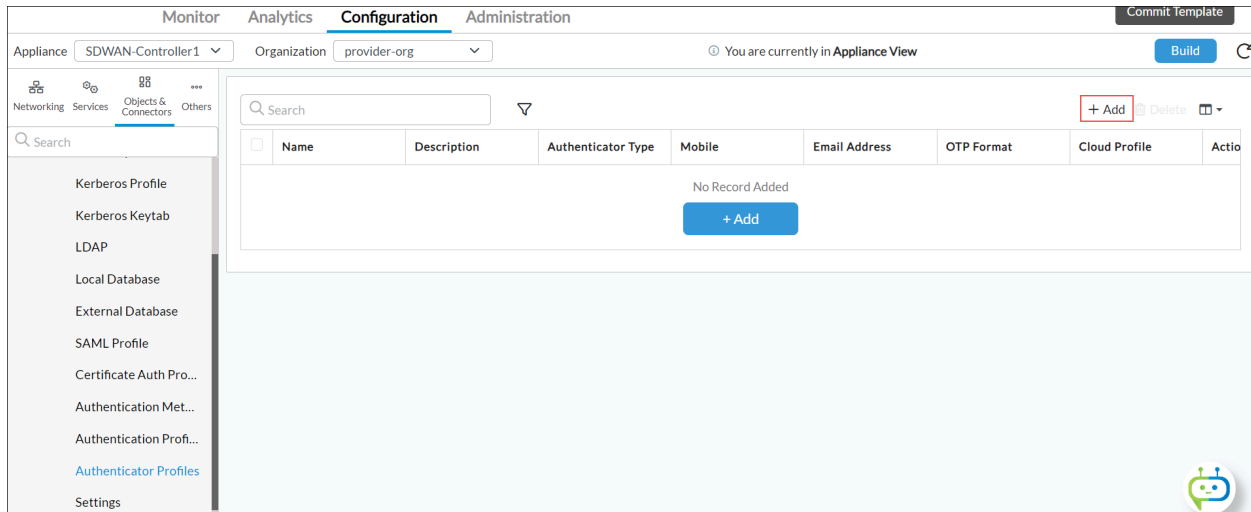
Copyright © 2024, Versa Networks, Inc.

Configure an Authenticator Profile

Before you configure an authenticator profile, ensure that SMTP server settings are enabled, to support two-factor authentication using OTP. For more information about receiving an OTP through email, see [Configure SMTP Server Settings](#), above.

To define an authenticator profile to use in the authentication profile:

1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Connectors > Users/Groups > Authenticator Profiles in the left menu bar.



4. Click the **+** Add icon. In the Add Authenticator Profiles popup window, enter information for the following fields.

Add Authenticator Profiles

Name *

Description

Authenticator Type

REST based authenticator service

One Time Password

☐ Mobile

Mobile Message Format

☐ Email Address

Mail Message Format

OTP Format

Cloud Profile

Length

Time To Live

---Please Selec

---Please Selec

30

OK

Cancel

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_User_a...
Updated: Wed, 23 Oct 2024 08:17:27 GMT
Copyright © 2024, Versa Networks, Inc.

32

Field	Description
Name (Required)	Enter a name for the authenticator profile.
Description	Enter a text description for the authenticator profile.
Authenticator Type	<p>Select an authenticator type:</p> <ul style="list-style-type: none"> ◦ REST-based Authenticator Service—Select to configure a one-time password in the One-Time Password group of fields. ◦ Time-based OTP Authenticator Service
One-Time Password (Group of Fields)	
◦ Mobile	Click to send a one-time password (OTP) to a mobile device.
◦ Mobile Message Format	Enter the format for the mobile message.
◦ Email Address	Click to send the one-time password using email and to share a QR code to use to register the SASE client to the user's email address. Note that if the email address of the user is not configured or if the user is not available through LDAP or SAML, the authentication fails and the user cannot register the client. For more information, see Enable a Time-Based One-Time Password .
◦ Mail Message Format	Enter the format for the email.
◦ OTP Format	<p>Select the format for the one-time password:</p> <ul style="list-style-type: none"> ◦ Alphabetic ◦ Alphanumeric ◦ Numeric—Note that for Release 21.2.1, only Numeric is supported.
◦ Cloud Profile	Select a cloud profile to use for one-time password-based authentication. For more information, see Configure a Cloud Profile .
◦ Length	Enter the length of the one-time password.

◦ Time To Live	Enter how long the one-time password is valid.
----------------	--

5. Click OK.

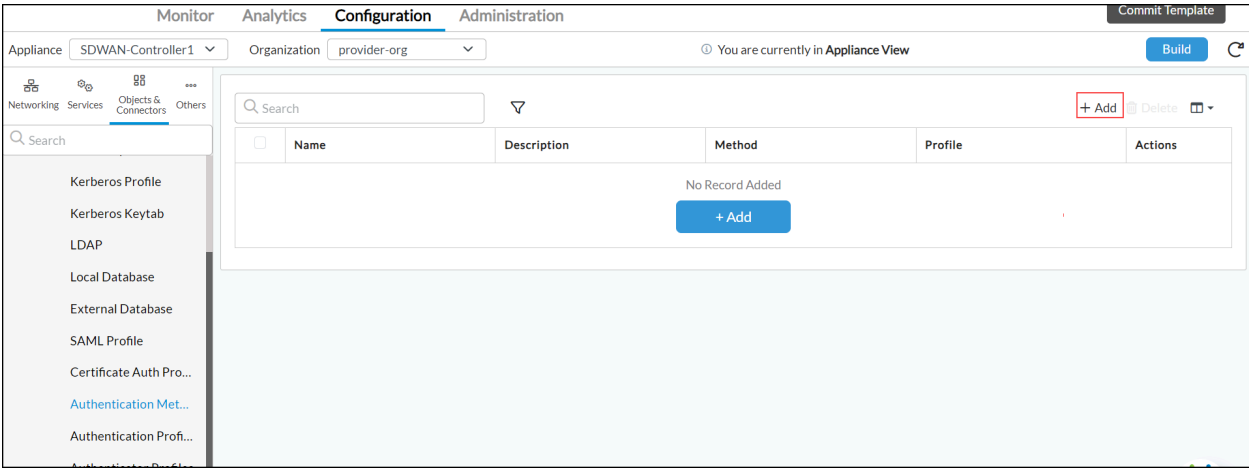
Configure an Authentication Method

For Releases 22.1.3 and later.

You configure the authentication method to use for certificate authentication, Kerberos, LDAP, local, RADIUS, or SAML profiles, and you then use this method when you configure an authentication profile for user authentication.

To configure an authentication method:

- In Director view:
 - Select the Administration tab in the top menu bar.
 - Select Appliances in the left menu bar.
 - Select a device name in the main panel. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select Object and Connectors > Connectors > Users/Groups > Authentication Methods in the left menu bar.



- Click the **+** Add icon. In the Add Authentication Methods popup window, enter information for the following fields.

Add Authentication Methods

✕

Name *

Description

Authentication Method

Method

Kerberos Profile

Kerberos Profile

---Please Select---

OK

Cancel

Field	Description
Name (Required)	Enter a name for the authentication method.
Description	Enter a text description for the authentication method.
Authentication Method (Group of Fields)	
<ul style="list-style-type: none"> Methods 	<p>Select the authentication method, and then, in the field on the right, select a configured profile to associate with the authentication method:</p> <ul style="list-style-type: none"> Certificate Authentication Profile—Select, and then select a certificate authentication profile. For more information, see Configure Certificate Authentication Profile, above. Kerberos Profile—Select, and then select a Kerberos profile. For more information, see Define Kerberos for User and Group Authentication, above. LDAP Profile—Select, and then select an LDAP profile. For more information, see Configure an LDAP Server Profile, above. Local Profile—Select to use the local database on the VOS device for user authentication. Do not enter any information in the field on the right. RADIUS Profile—Select, and then select a RADIUS server. For more information, see Configure RADIUS Servers, below. SAML Profile—Select, and then select a SAML profile. For more information, see Configure SAML Profiles, above.

5. Click OK.

To associate an authentication method with an authentication profile, see [Configure an Authentication Profile](#), below.

Configure an Authentication Profile

To define an authentication profile to use in the user and group authentication policy:

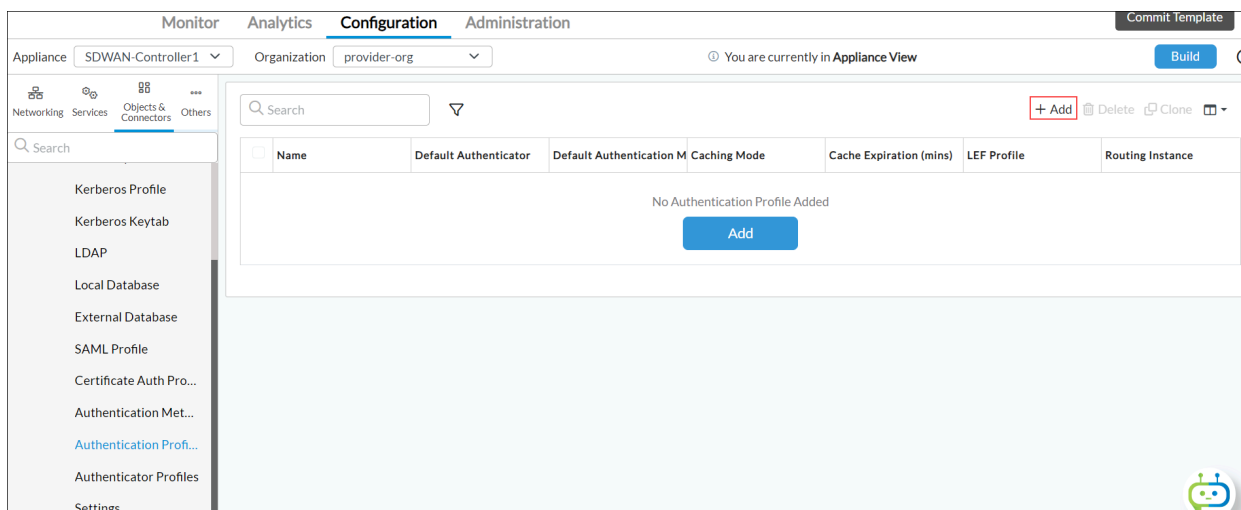
- In Director view:
 - Select the Administration tab in the top menu bar.
 - Select Appliances in the left menu bar.
 - Select a device name in the main panel. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_User_a...

Updated: Wed, 23 Oct 2024 08:17:27 GMT

Copyright © 2024, Versa Networks, Inc.

3. Select Object and Connectors > Connectors > Users/Groups > Authentication Profiles in the left menu bar.



4. Click the **+** Add icon. The Add Authentication Profile popup window displays. For Releases 21.2.1 and earlier, the popup window has one tab, General. For Releases 22.1.3 and later, the popup window has two tabs, General and Rules.

The screenshot shows the 'Add Authentication Profile' popup window. It has two tabs: 'General' (selected) and 'Rules'. The 'General' tab contains the following fields:


- Name ***: A text input field.
- Description**: A text input field.
- Authentication Type**: A dropdown menu with 'Active' selected.
- VMS Profile**: A dropdown menu with '--Select--' selected.
- Caching Mode**: A dropdown menu with 'IP Based' selected.
- Cache Expiration (mins)**: A text input field with '10' entered.
- Cookie Name**: A text input field.
- Concurrent Login**: A text input field with '1' entered.
- Expiration Mode**: A dropdown menu with '--Select--' selected.
- Default Authenticator**: A dropdown menu with '--Select--' selected.
- Proactive-Reauth**: A checkbox that is unchecked.
- Default Authentication Method ***: A section with a '+', a trash icon, and a refresh icon. Below it, a message says 'Default Authentication Method Not Configured'.
- LEF Profile**: A dropdown menu with '--Select--' selected.
- Default Profile**: A checkbox that is checked.

At the bottom right, there are 'OK' and 'Cancel' buttons.

5. Select the General tab, and enter information for the following fields.

Field	Description
Name (Required)	Enter a name for the authentication profile name.
Description	Enter a text description for the authentication profile.
Tags	Enter a keyword or phrase that allows you to filter the authentication profile. Tagging is useful when you have many profiles and want to view those that are tagged with a particular keyword.
Authentication Type	<p>(For Releases 22.1.3 and later.) Select the type of authentication to use:</p> <ul style="list-style-type: none"> ◦ Active—Use active authentication by using one or more Kerberos, LDAP, and SAML profiles. ◦ Passive—Use passive authentication using a Versa message service (VMS) profile.
VMS Profile	<p>(For Releases 22.1.3 and later.) If you select passive authentication, select a VMS profile to use for passive authentication. For more information, see Configure Passive Authentication for VMS.</p>
Local Database	<p>(For Releases 22.1.3 and later.) Click to use the database on the local VOS device for storing the user and group authentication information on the local server. It is recommended that you use the local database only for user groups no larger than 50 to 100 users.</p>
Caching Mode	<p>Select the caching mode:</p> <ul style="list-style-type: none"> ◦ Cookie Based—Set the cookie in the user's browser, and do not store the user information on the device. ◦ IP Based—Map users using their IP address as the key.
Cache Expiration	<p>Enter the time, in minutes, after which cache for the authentication profile expires.</p> <p><i>Default:</i> 10 minutes</p>
Cookie Name	If you select cookie-based caching, enter the authentication cookie name.

Concurrent Login	If you select IP-based caching, enter the number of concurrent logins a user can perform from different devices.
Routing Instance	If you select an LDAP provider, select the routing instance to use to reach the LDAP server.
Expiration Mode	<p>Select the mode to use to end a session:</p> <ul style="list-style-type: none"> ◦ Fixed Interval—Use the time specified in the cache expiration as the time interval to end a session. ◦ Inactivity—Use the time specified in the cache expiration as the interval of inactivity after which to end a session.
LEF Profile	Select a LEF profile to use to register logs for the profile.
Default Profile	Click to mark the LEF profile as the default profile.
Kerberos Profile	(For Releases 21.2.2 and earlier.) If you select Kerberos authentication, select a Kerberos profile to associate with the authentication profile. Click + Create Kerberos Profile to add a new Kerberos profile. For more information, see Create a Kerberos Profile , above.
LDAP Profile	(For Releases 21.2.2 and earlier.) If you select LDAP authentication, select an LDAP profile to associate with this authentication profile. Click + Create LDAP Profile to add a new LDAP profile. For more information, see Configure an LDAP Server Profile , above.
SAML Profile	(For Releases 21.2.2 and earlier.) If you select SAML authentication, select a SAML profile to associate with this authentication profile. Click + Create SAML Profile to add a new SAML profile. For more information, see Configure SAML Profiles , above.
Certificate Authentication Profile	(For Releases 21.2.1 and earlier.) Select a certificate

	<p>authentication profile to associate with this authentication profile. Click + Create Cert Authentication Profile to add a new certificate authentication profile. For more information, see Configure a Certificate Authentication Profile, above.</p>
Proactive Reauthentication	<p>(For Releases 21.1.1 and later.) If you select a Kerberos profile and set Expiration Mode as Fixed Interval, click to proactively reauthenticate midway through the expiration interval. For example, if the expiration interval is set to 10 minutes, one of the TCP sessions is selected for Kerberos authentication when the expiration time reaches 5 minutes (the halfway point). If the domain client browser follows the redirection for Kerberos, the user session is automatically authenticated. If the response for a TCP session authentication is not received within 30 seconds or if the reauthentication fails, another TCP session is selected for redirection until the reauthentication is successful. After a TCP session is reauthenticated, the expiration interval is reset to the configured interval (in this example, 10 minutes). This mechanism ensures that all the traffic is not redirected and that the user is not logged out at the end of the expiration interval.</p>
Default Authenticator	<p>Select a default authenticator profile.</p> <p>Note that for Releases 21.2.1 and earlier, this field is called Authentication Profiles</p>
Default Authentication Method	<p>(For Releases 22.1.3 and later.) Select an authentication method to associate with the authentication profile.</p> <p>Click the  Add icon to add more authentication methods. For more information, see Configure an Authentication Method, above.</p>

6. For Releases 21.2.1 and earlier, click OK.
7. For Releases 22.1.3 and later, select the Rules tab.

Add Authentication Profile

×

General

Rules

+

🗑️

↕️

↑

↓

⌵

📅

🔍

⏪

1

⏩


25

▼

<input type="checkbox"/>	Name	Description
No Rules Added		

OK

Cancel

8. Click the  Add icon. The Add Rules Popup window displays. Select the General tab, and enter information for the following fields.

Add Rules

✕

General

Match

Set

Name *

Description

OK

Cancel

Field	Description
Name (Required)	Enter a name for the authentication profile rule.
Description	Enter a text description for the authentication profile rule.

9. Select the Match tab, and enter information for the following fields.

Add Rules

×

General Match Set

Domains

☐ Domains

+

🗑️

↗️

Domains Not Configured

OK

Cancel

Field	Description
Domains	Click the + Add icon, and then enter a domain name to use as match filter in the rule. Click the + Add icon to add more domains.

10. Select the Set tab, and enter information for the following fields.

Add Rules

×

General Match Set

☐ Authentication Methods

+

🗑️

↗️

☐

▼

☐ Authenticator Profiles

+

🗑️

↗️

☐

▼

OK

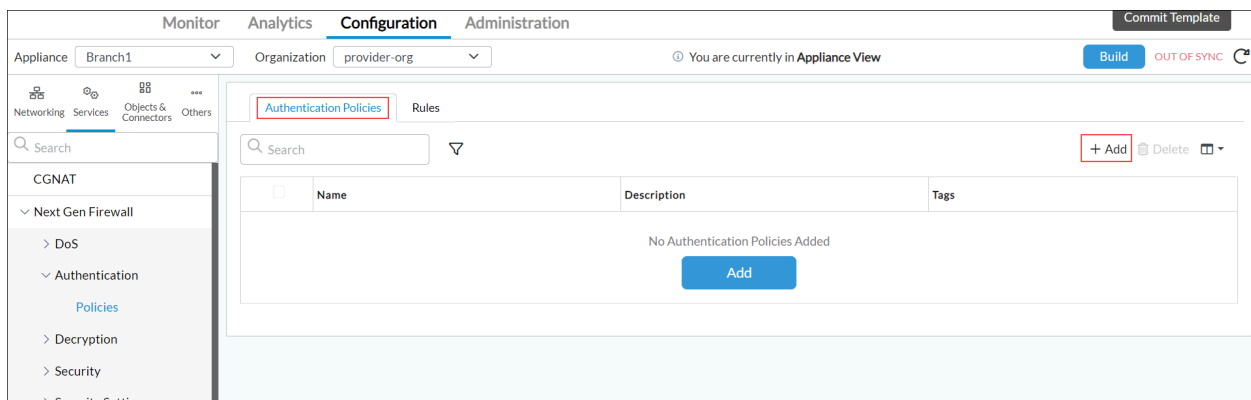
Cancel

Field	Description
Authentication Methods	Click the + Add icon and select an authentication method to associate with the rule. Click the + Add icon to add more authentication methods. For more information, see Configure an Authentication Method , above.
Authenticator Profiles	Click the + Add icon and select an authenticator profile to associate with the rule. Click the + Add icon to add more authenticator profiles. For more information, see Configure an Authenticator Profile , above.

11. Click OK.

Configure Authentication Policies

- In Director view:
 - Select the Administration tab in the top menu bar.
 - Select Appliances in the left menu bar.
 - Select a device name in the main panel. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select Services > Next-Gen Firewall > Authentication > Policies in the left menu bar.
- Select the Authentication Policies tab, and then click the **+** Add icon.



- In the Add Policies popup window, enter information for the following fields.

Add Policies

×

Name *

Description

Tags

OK

Cancel

Field	Description
Name (Required)	Enter a name for the authentication policy.
Description	Enter a text description for the policy.
Tags	Enter a keyword or phrase that allows you to filter the policy name. This is useful when you have many policies and want to view those that are tagged with a particular keyword.

6. Click OK.

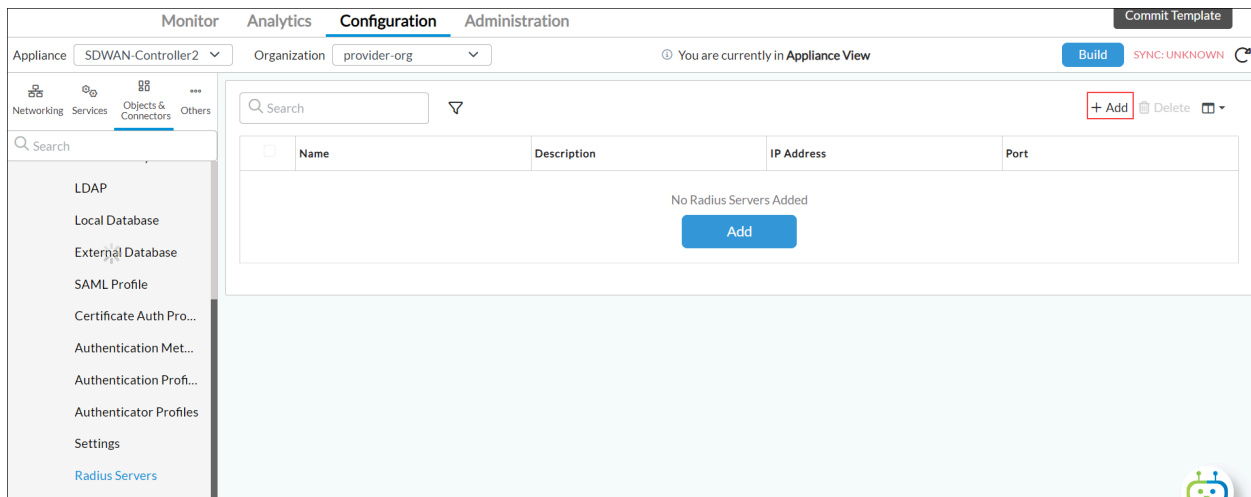
Configure RADIUS Servers


For Releases 22.1.3 and later.

To configure RADIUS servers to use for user authentication:


1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select a device name in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.

3. Select Object and Connectors > Connectors > Users/Groups > RADIUS Servers in the left menu bar.






4. Click the  Add icon. In the Add RADIUS Servers popup window, enter information for the following fields.


Add Radius Servers

Name 

Description

IP Address  Port  Routing Instance

Shared Secret 

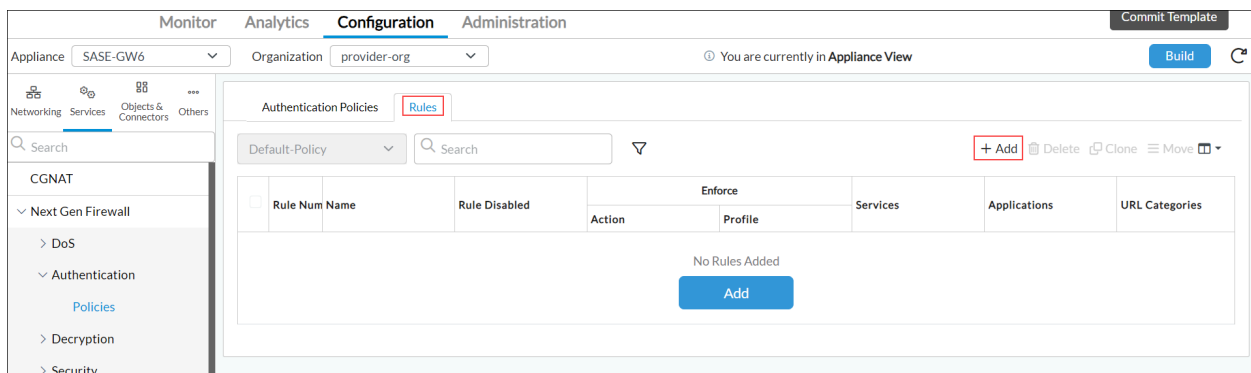


Field	Description
Name (Required)	Enter a name for the RADIUS server.
Description	Enter a text description for the RADIUS server.
IP Address (Required)	Enter the IP address of the RADIUS server.
Port (Required)	Enter the port number to use on the RADIUS server.
Routing Instance	Enter the routing instance to use to reach the RADIUS server.
Shared Secret (Required)	Enter the RADIUS shared secret (password) string.

- Click OK.

Configure Rules for Authentication Policies

- In Director view:
 - Select the Administration tab in the top menu bar.
 - Select Appliances in the left menu bar.
 - Select a device name in the main panel. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select Services > Next-Gen Firewall > Authentication > Policies in the left menu bar.
- Select Rules tab, and then click the **+** Add icon in the dashboard to add a new authentication policy. The Add Rules popup window displays.




- (For Releases 21.2.1 and later.) If you have already added one or more rules, the Configure Rule Order popup window displays.
 - Select where you want to insert the policy rule, either at the beginning or end of the existing rules.

Configure Rule Order

Please choose from the following where the new rule to be inserted.
Rule will be added at bottom as default.

☒ Insert At Bottom
☐ Insert At Top

Ok

- b. If you select a rule and then click the  Add icon, the Configure Rule Order popup window displays the following options:

Configure Rule Order

Please choose from the following where the new rule to be inserted
from selected rule p1.
Rule will be added at bottom as default.

☒ Insert At Bottom
☐ Insert At Top
☐ Insert Before Selected Rule
☐ Insert After Selected Rule

Ok

- c. Select the order to insert the rule (at the beginning or end bottom of the existing rules, or before or after the selected rule).
- d. Click OK. The Add Rule popup window displays.
6. Select the General tab, and enter information for the following fields.

Add Rules
✕

General
Source
Destination
Applications/URL
Headers/Schedule
Enforce

Name *

Description

Tags
☐ Disable Rule

OK
Cancel

Field	Description
Name (Required)	Enter a name for the authentication policy rule.
Description	Enter a text description for the rule.
Tags	Enter a keyword or phrase that allows you to filter the rule name. This is useful when you have many policies and want to view those that are tagged with a particular keyword.
Disable Rule	Click to not activate the access policy rule after you configure it.

- Select the Source tab to define the source zone and the source address of the incoming (source) traffic to which the authentication policy rule applies. Enter information for the following fields. (Note that for Releases 21.1 and earlier, the Source and Destination rule fields are on a single tab.)

Add Rules

General

Source

Destination

Applications/URL

Headers/Schedule

Enforce

Source Zone

+ New Zone +

Source Zone Not Configured

Source Address

+ New Address + New Address Group +

Source Address Not Configured

Source Address Negate

Region

+

Region Not Configured

State

+

State Not Configured

City

+

City Not Configured

Source Location Negate

Custom Geo Circle

+

Custom Geo Circle Not Configured

OK







Cancel

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_User_a...

Updated: Wed, 23 Oct 2024 08:17:27 GMT

Copyright © 2024, Versa Networks, Inc.

49

Field	Description
Source Zone	Select the source zone to apply the rule to traffic coming from any interface in the specified zone. Click the  Add icon to add more security zones.
Source Address	Select and specify one or more source address to which the rule applies. Click the  Add icon to add more source addresses.
Source Address Negate	Enable this to select any address except the configured addresses.
Region	Click the  Add icon to select a region.
State	Click the  Add icon to select a state.
City	Click the  Add icon to select a city.
Source Location Negate	Click to have the rule select any location except the configured locations.
Custom Geo Circle	Click the  Add icon to select a custom geographic circle, which consists of a point and the area enclosed by a circle drawn around that point. You specify the point by its latitude and longitude coordinates, and you specify the size of the circle by a distance. For more information, see Configure Geolocation Objects .

8. Select the Destination tab to define the destination zone and the destination address of the outgoing (destination) traffic to which the authentication policy rule applies. Enter information for the following fields. (Note that for Releases 21.1 and earlier, the Source and Destination rule fields are on a single tab.)

Add Rules

General

Source

Destination



Applications/URL

Headers/Schedule

Enforce

☐



Destination Zone

+ New Zone +  

Destination Zone Not Configured

☐

Destination Address



+ New Address + New Address Group +  

Destination Address Not Configured

☐ Destination Address Negate

☐



Region

+  

Region Not Configured

☐



State

+  

State Not Configured

☐

City



+  

City Not Configured

☐ Destination Location Negate

☐

Custom Geo Circle

+  

Custom Geo Circle Not Configured

OK







Cancel

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_User_a...

Updated: Wed, 23 Oct 2024 08:17:27 GMT

Copyright © 2024, Versa Networks, Inc.

51

Field	Description
Destination Zone	Select the destination zone to apply the rule to traffic coming from all interfaces into a given zone. Click the  Add icon to add more security zones.
Destination Address	Select and specify one or more destination address to apply the rule to the traffic marked to the specific destination. Note that for an explicit proxy, the destination address is the address on which the explicit proxy is configured, so configuring this option with explicit proxy is not effective. Click the  Add icon to add more destination addresses.
Destination Address Negate	Enable this to specify any address except the configured addresses. For explicit proxy, the destination address is the address on which the explicit proxy is configured. Configuring this option with explicit proxy is not effective.
Region	Click the  Add icon to select a region.
City	Click the  Add icon to select a city.
State	Click the  Add icon to select a state.
Destination Location Negate	Click to have the rule select any location except the configured locations.
Custom Geo Circle	Click the  Add icon to select a custom geographic circle, which consists of a point and the area enclosed by a circle drawn around that point. You specify the point by its latitude and longitude coordinates, and you specify the size of the circle by a distance. For more information, see Configure Geolocation Objects .

9. Select the Application/URL tab to select the applications and URLs to which the security access rule applies. Enter information for the following fields.

Add Rules

General

Source

Destination

Applications/URL

Headers/Schedule

Enforce

☐ Application List

[+ New Application](#)
[+ New Filter](#)
[+ New Group](#)

+

Application List Not Configured

☐ URL Category List

[+ New URL Category](#)

+

URL Category List Not Configured




☐ URL Reputations

+

Predefined Reputations Not Configured

OK

Cancel

Field	Description
Applications	Click the  Add icon and then select one or more predefined or custom application signature and apply the authentication policy rule to the application. For more information, see Configure Application Objects .
URL Categories	Click the  Add icon and then select one or more predefined/custom URL categories and apply the authentication policy rule to the URL. For more information, see Configure URL Category Objects .
Reputations	(For Releases 21.2.1 and later.) Click the  Add icon and then select one or more predefined URL reputations and apply the security access rule to the URL. For more information, see View a Predefined URL Reputation .

- Select the Header/Schedule tab to define the IP header, services and schedule to which the authentication policy rule applies. Enter information for the following fields.

Add Rules

General

Source

Destination

Applications/URL

Headers/Schedule

Enforce

IP

IP Version

--Select--

IP Flags

--Select--

DSCP

0 .. 63

+

TTL

Condition

--Select--

Value (Max 255)

Others

Schedules

--Select--

+ Schedule

☐



Services

+ New Service +

Services Not Configured

OK

Cancel

Field	Description
IP (Group of Fields)	
◦ IP Version	Select the IP version.
◦ IP Flags	For IPv4, select the IP flag: <ul style="list-style-type: none"> ◦ Don't Fragment ◦ More Fragment
◦ DSCP	Enter a differentiated service code point value to classify the way the IP packet is queued to get forward, then click the  Add icon.
TTL (Group of Fields)	
◦ Condition	Select the TTL condition of the IP packet that the security access policy rule verifies: <ul style="list-style-type: none"> ◦ Greater than or equal to—TTL value must be greater than or equal to the specified value for the security access rule to trigger. ◦ Less than or equal to—TTL value must be less than or equal to the specified value for the security access rule to trigger. ◦ Equal to—TTL value must be equal to the specified value for the security access rule to trigger.
◦ Value	Enter the TTL value to match with the TTL condition.
Others (Group of Fields)	
◦ Schedules	Select a schedule to specify when the security access rule is in effect. You can also create and add a new schedule. For more information, see Configure Schedule Objects .
Services table	Click the  Add icon then select one or more services to apply the security access rule to the configured services.

11. Select the Enforce tab to specify the applications and URLs to which the authentication policy rule applies. Enter information for the following fields.

Add Rules [Close]

General Source Destination Applications/URL Headers/Schedule **Enforce**

Action

☒ Do not Authenticate ☐ Authenticate using Profile

--Select-- [v]

Log

☒ Do not Log ☐ Log using Profile

--Select-- [v] ☐ Default Profile

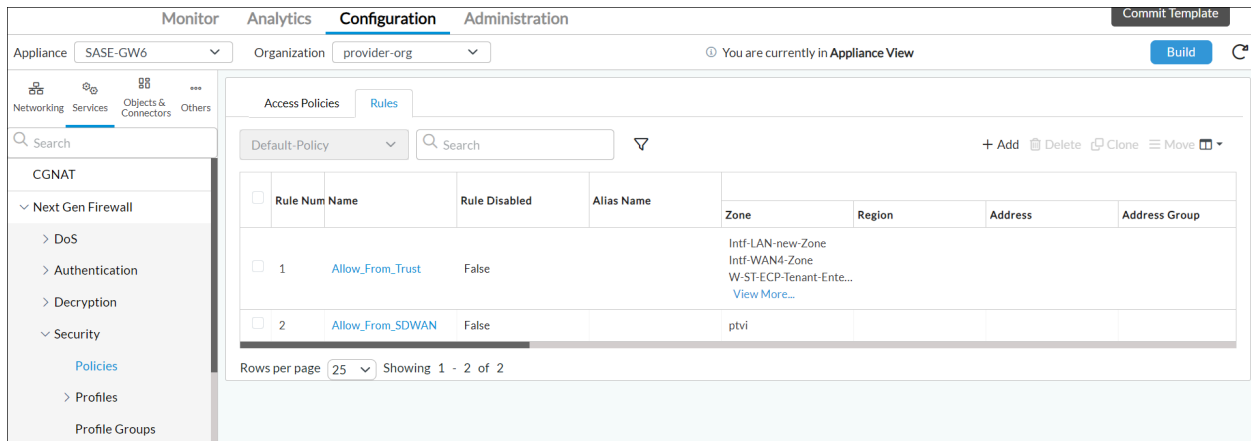
OK Cancel

Field	Description
Actions	Select the action to impose on the traffic: <ul style="list-style-type: none">◦ Do Not Authenticate—Select to not authenticate the profile.◦ Authenticate Using Profile—Select, then select an authentication profile.
Log	Select how to log the data: <ul style="list-style-type: none">◦ Do Not Log—Do not log the authentication profile information.◦ Log Using Profile—Select, and then select a LEF profile from the list, or click Default Profile to use the default LEF.

12. Click OK.

Match Users and Groups in Access Policy

1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Next-Gen Firewall > Security > Policies in the left menu bar.



4. Select the Rules tab, and click a security rule in the main pane to make changes to it. The Edit Rule popup window displays.
5. Select the Users/Groups tab, and enter information for the following fields.

Edit Rule - Allow_From_Trust

General
Source
Destination
Headers/Schedule
Applications/URL
IoT Security
Users/Groups
Enforce

Match Users

Any

User Group Profile

--Select--

☐ Local Database

Users

+ New Custom User +

Users Not Configured

☐ External Database

Groups

+ New Custom Group +

Groups Not Configured

OK
Cancel

Field	Description
Match Users	<p>Select the user to match with the access policy:</p> <ul style="list-style-type: none"> Any Known Unknown Selected—Click the + Add icon and select users from the drop-down list.
User Group Profile	<p>If the match is for selected users, select the user group profile to access the network in the security policy.</p>

Field	Description
Local Database	Click to use local database to store the user and group authentication information on the local server. It is recommended that you use a local database only when the number of user sand groups does not exceed 50 to 100.
External Database	Click to use an external database to store user authentication information.

6. Click OK.

Supported Authentication Protocols

For NGFW, VOS devices support various protocols, including LDAP, SAML, and Kerberos (in both HTTP and HTTPS modes).

End clients use captive portal autodetection to attempt to fetch a preconfigured HTTP URL. If the path includes a captive portal, the client redirects with its own response page. This is different from what the device expects to see from the server. Thus, the device pops up an application to follow the link that the captive portal would have sent in the redirect request. Because the generated traffic is plain text, it does not require an SSL proxy. For a captive portal to redirect a request, the captive portal must understand that it is an HTTP request. In response to that HTTP request, the captive portal must redirect with an appropriate response code. This can be done only if the captive portal sees an HTTP request in clear text. The entire response to an HTTPS request cannot be in clear text, because the SSL layer at the client would discard it as a malformed SSL record. Also, without decryption, the system cannot send an encrypted response to the client.

The following table describes the supported authentication protocols.

Authentication Protocol	Session Protocol	Session Type	Supported	SSL Decryption Required	Notes
Kerberos	HTTP	No Proxy	No	Not applicable	None
		Forward Proxy	No	Not applicable	None
		Transparent Full Proxy	Yes	Not applicable	None
		Explicit Full Proxy	Yes	Not applicable	None
	HTTPS	No Proxy	No	Not applicable	None

Authentication Protocol	Session Protocol	Session Type	Supported	SSL Decryption Required	Notes
		Forward Proxy	No	Not applicable	None
		Transparent Full Proxy	Yes	Yes	Decryption required to redirect session to virtual URL to get Kerberos token
		Explicit Full Proxy	Yes	No	Kerberos token is received from CONNECT HTTP method and hence does not require decryption
LDAP	HTTP	No Proxy	Yes	Not applicable	None
		Forward Proxy	Yes	Not applicable	None
		Transparent Full Proxy	Yes	Not applicable	None
		Explicit Full Proxy	Yes	Not applicable	None
	HTTPS	No Proxy	Yes	Yes	Decryption required to redirect session to authentication page
		Forward Proxy	Yes	Yes	Decryption required to redirect session to authentication page
		Transparent Full Proxy	Yes	Yes	Decryption required to redirect session to authentication page
		Explicit Full Proxy	Yes	Yes	Decryption required to redirect session

Authentication Protocol	Session Protocol	Session Type	Supported	SSL Decryption Required	Notes
					to authentication page
Local	HTTP	No Proxy	Yes	Not applicable	None
		Forward Proxy	Yes	Not applicable	None
		Explicit Full Proxy	Yes	Not applicable	None
	HTTPS	No Proxy	Yes	Yes	Decryption required to redirect session to authentication page
		Forward Proxy	Yes	Yes	Decryption required to redirect session to authentication page
		Transparent Full Proxy	Yes	Yes	Decryption required to redirect session to authentication page
		Explicit Full Proxy	Yes	Yes	Decryption required to redirect session to authentication page
SAML	HTTP	No Proxy	Yes	Not applicable	None
		Forward Proxy	Yes	Not applicable	None
		Transparent Full Proxy	Yes	Not applicable	None
		Explicit Full Proxy	Yes	Not applicable	None
	HTTPS	No Proxy	Yes	Yes	Decryption required to redirect session to IdP

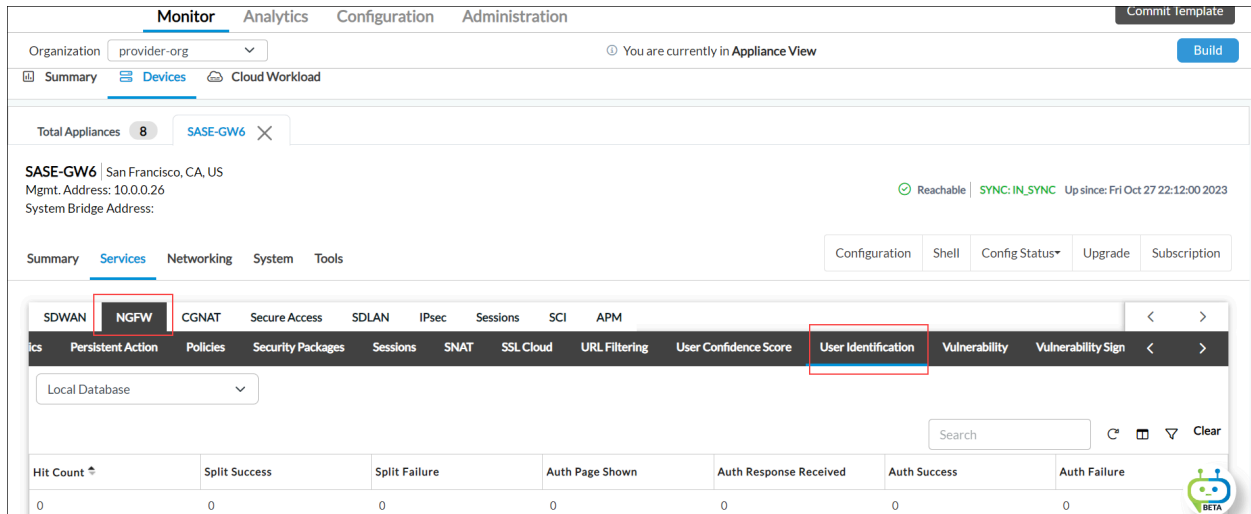
Authentication Protocol	Session Protocol	Session Type	Supported	SSL Decryption Required	Notes
		Forward Proxy	Yes	Yes	Decryption required to redirect session to IdP
		Transparent Full Proxy	Yes	Yes	Decryption required to redirect session to IdP
		Explicit Full Proxy	Yes	Yes	Decryption required to redirect session to IdP

Monitor User Identification Statistics

You monitor user ID statistics to view the reports for profiles associated with a user ID. For more information, see [Monitor Device Services](#).

To monitor user identification statistics:

1. Select the Administration tab in the top menu bar.
 - a. Select Appliances in the left menu bar.
 - b. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Monitor tab in the top menu bar.
3. Select the Provider Organization > Services tab.
4. Select NGFW > User Identification, and then select one of the following options from the drop-down list: Authentication Profile, Local Database, LDAP Profile, Kerberos Profile, SAML Profile, or Live Users. The user ID statistics display.



Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Release 20.2.2 adds support for authenticator profiles.
- Release 21.2.1 adds support for certificate authentication profile and SMTP server settings, and configuring rule order for authentication policy rules.
- Release 22.1 adds support for configuration of active user distribution for VMS.
- Release 22.1.3 adds support for configuration of additional authentication methods, associating authentication profiles with authentication methods, configuring authentication profile rules, and configuring RADIUS servers.

Additional Information

[Configure CA Certificates, Key File, and CA Chains](#)

[Configure File Filtering](#)

[Configure IEEE 802.1X Device Authentication](#)

[Configure Kerberos Authentication](#)

[Configure Layer 7 Objects](#)

[Configure NGFW](#)

[Configure Passive Authentication for VMS](#)

[Configure Policy-Based Forwarding](#)

[Configure Schedule Objects](#)

[Configure SD-WAN Policy](#)

[Configure URL Filtering](#)

[Configure the Versa Secure Access Service](#)

[Configure Versa SASE Clients](#)

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_User_a...

Updated: Wed, 23 Oct 2024 08:17:27 GMT

Copyright © 2024, Versa Networks, Inc.

