

Configuring Authentication Profiles on the SSE Gateway

About This Document

This guide provides a comprehensive, step-by-step configuration process for setting up and preparing your organization for the Authentication Methods supported on the VOS.

Authentication serves as a mechanism for verifying users' identities to ensure that only authorised individuals gain access to applications. Multiple authentication methods can be configured to authenticate end users, including the use of a local database, a Lightweight Directory Access Protocol (LDAP) server, Security Assertion Markup Language (SAML), and Kerberos. This document outlines the procedures for configuring an Open-LDAP server, Active Directory (AD) LDAP server, SAML, device and user certificates for end-user authentication. Additionally, administrators can configure either user-based or group-based policies to determine whether access is permitted or denied.

Document Information

Title	Configuring Authentication Profiles on the SSE Gateway
Author	Versa Professional Services
Version	V 1.0

Disclaimer

Information contained in this document regarding Versa Networks (the Company) is considered proprietary.

Before you begin

Before you proceed with the steps outlined in this document, please ensure you've met the following prerequisites.

- The provider administrator must complete your tenant configuration. If you haven't received this information, please contact your Managed Service Provider or Account Manager for assistance.
- You have the Enterprise Administrator (Tenant Admin) credentials for the Versa SASE portal, also called the Concerto User Interface.

LDAP Active-Directory	4
Scenario	4
SAML Authentication	12
OKTA	12
Microsoft Entra ID	28
Versa Directory	51
Device Certificate Authentication	51
User Certificate	71
Appendix A: LDAP	79
How to Find Base DN and Bind DN in Active Directory for Versa Integration	79

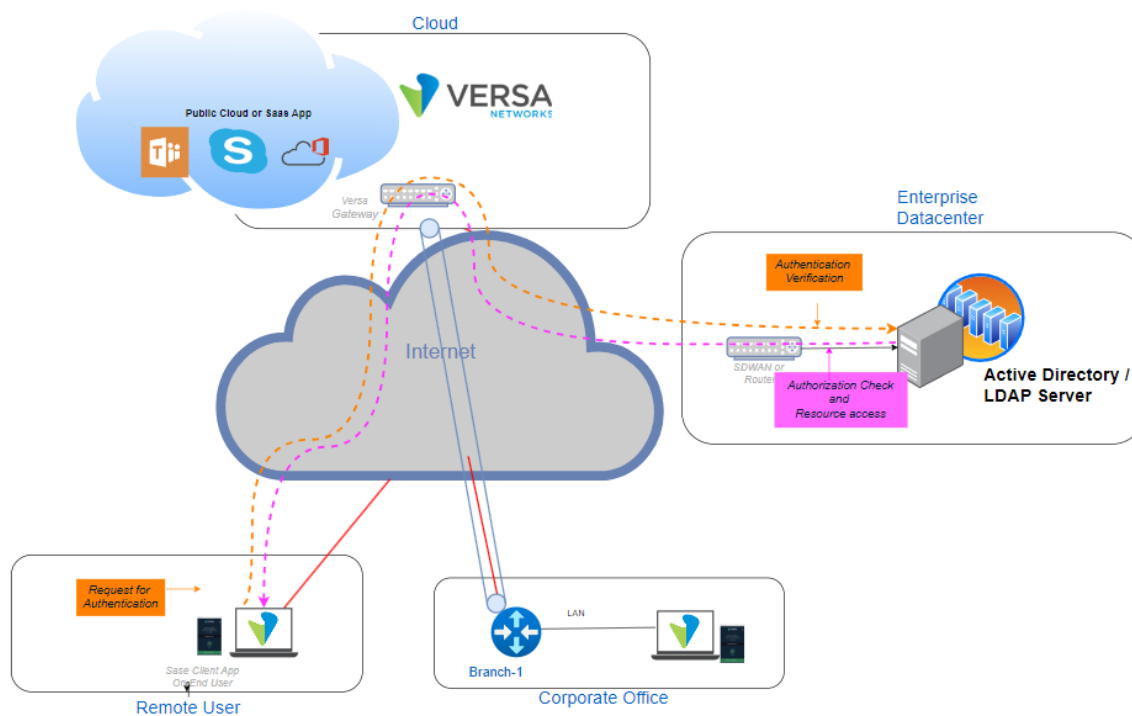
LDAP Active-Directory

LDAP is a client-server protocol that enables network devices to access directory services storing attribute-based information, allowing for user authentication through querying a directory server. The SSE gateway queries the LDAP server to validate the user, granting or denying access based on the authentication result. Users can be validated individually or within groups, and the configuration involves specifying server details, SSL settings, and profiles.

Scenario

In most enterprise environments, user authentication is centralized through AD/LDAP servers in the data centre. In cases of VSPA or VISA, users securely connect to the SSE gateways using the Versa SASE Client from remote locations, branches, or corporate offices. Authentication requests from the SASE client are directed to the Versa Secure Access Gateway, which communicates with AD/LDAP over IPsec tunnels to validate credentials and retrieve group or role attributes for policy enforcement.

Upon successful authentication, users are granted secure access to resources hosted within data centres and to SaaS/cloud applications such as Microsoft Teams, Skype, and Office 365. This configuration ensures consistent, identity-based access for both remote and on-premises users, thereby facilitating streamlined policy enforcement based on identity enforcement.



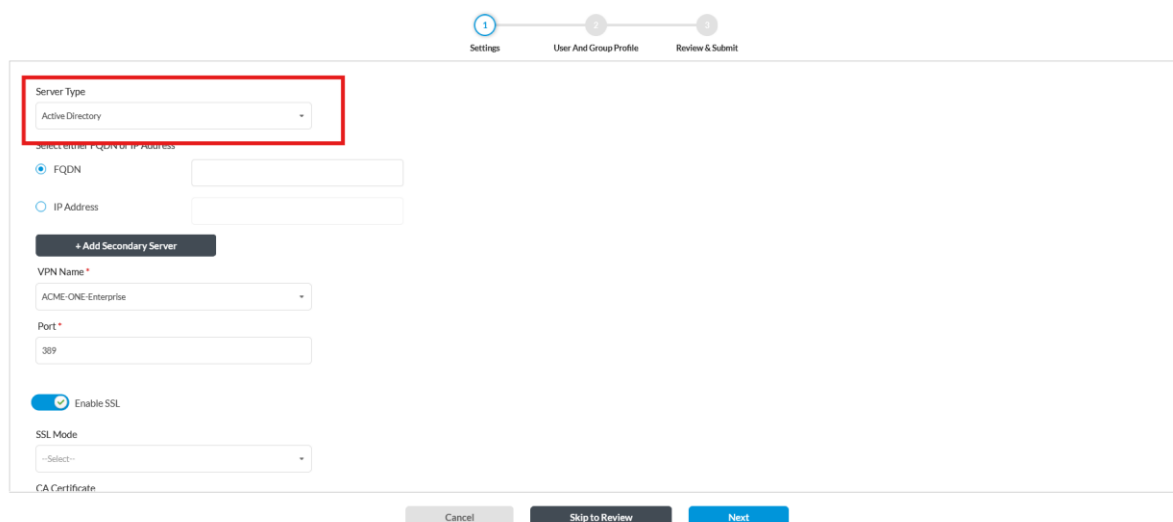
Navigate to User and Device Authentication Configuration

Go to: Configure > Security Service Edge > User and Device Authentication > Profiles then "+ Add"

Select **LDAP** as Authentication Method then Click **Get Started**

From the Server Type dropdown, select Active Directory

Add LDAP Authentication Profile



The following section explains all parameters for LDAP Authentication Profile configuration.

LDAP Authentication Profile – Parameters		
Parameter	Description	Current Use Case
Server Type	It indicates that the authentication source is Microsoft Active Directory or Open-LDAP.	active directory
FQDN or IP Address	The Fully Qualified Domain Name (FQDN) or IP address of the AD/LDAP server.	10.163.106.33 or ad-server.company.local
VPN Name	Defines which VPN instance or network segment this authentication profile applies to.	ACME-ONE-Enterprise
Port	Port used for LDAP/AD communication. Possible options: 389: Default LDAP port & 636: Default LDAPS (LDAP over SSL)	389 TCP
SSL Status	Enabled/Disabled: Determines if the connection between Versa and the AD server uses SSL/TLS for security. If enabled , you must also specify the CA certificate details (trusted CA/chain) that will be used for TLS communication verification.	Disabled
Bind DN	Bind Distinguished Name (DN): This is the "service account" that Versa will use to connect and query the LDAP/AD directory. Bind DN allows Versa to authenticate itself to the AD server, enabling it to search for users and groups.	cn=Administrator, cn=users, dc=versa,dc=com cn = Common Name dc = Domain Component
Bind Password	The password for the Bind DN account.	Service account password
Base DN	Base Distinguished Name (DN): This is the starting point in the LDAP directory tree from which searches will begin. It defines the organisational scope of the LDAP search.	Example: cn=users,dc=versa,dc=com
Domain Name	The name of the AD domain.	versa.com
Search Timeout (sec)	Maximum time (in seconds) Versa will wait for a response from the LDAP server during a query.	30

Cache Expiry Time (mins)	How long (in minutes) user/group information retrieved from LDAP will be cached before refreshing.	10
Concurrent Logins	The maximum number of concurrent sessions allowed for the same user.	3

NOTE: Refer Appendix A to understand how to get the Base DN and Bind DN

Add LDAP Authentication Profile

Settings User And Group Profile Review & Submit

1 Server Type: Active Directory

2 Select either FQDN or IP Address*: IP Address: 10.163.106.33

3 VPN Name*: ACME-ONE-Enterprise

4 Port*: 389

Enable SSL

SSL Mode: Select

CA Certificate

Cancel Skip to Review Next

Next, complete the required fields: specify the **Bind DN** (Distinguished Name of the user account used to bind to the LDAP/AD server), enter the **Bind Password** for that account, set the **Base DN** (the starting point in the directory tree for LDAP searches), and provide the **Domain Name**. Once all values are filled in, click **Next** to proceed Next

Add LDAP Authentication Profile

Settings User And Group Profile Review & Submit

VPN Name: ACME-ONE-Enterprise

Port*: 389

Enable SSL

SSL Mode: Select

CA Certificate: Select Add New

Bind DN*: cn=Administrator,cn=users,dc=acme-one,dc=com

Bind Password*: *****

Bind Timeout (sec): 30

Base DN*: cn=users,dc=acme-one,dc=com

Domain Name*: acme-one.com

Base Domain:

Search Timeout (sec): 30

Cache Expiry Time (mins): 10

Concurrent Logins: 3

Cancel Skip to Review Next

Next, complete the required fields:

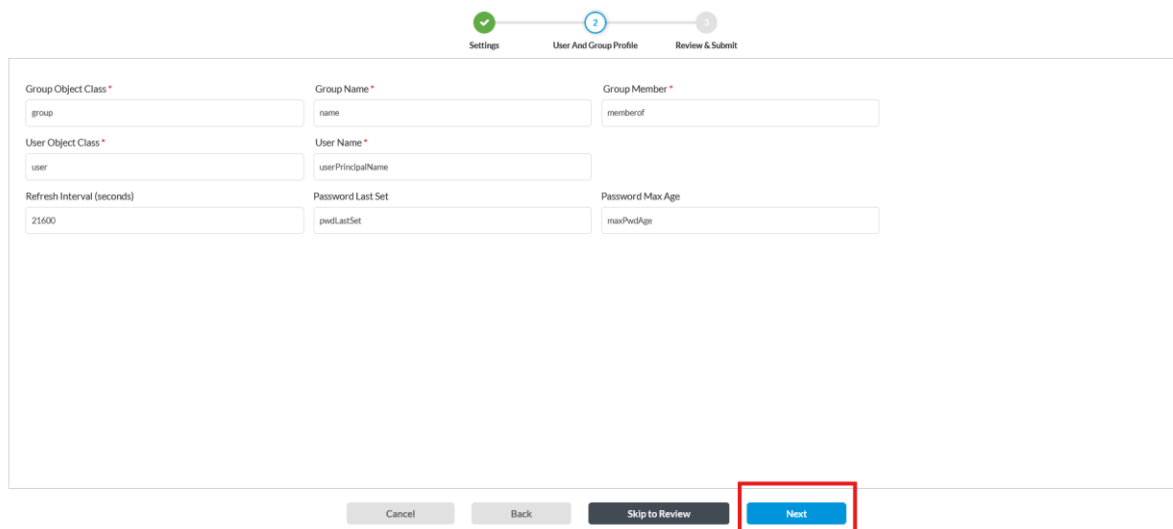
LDAP Object and User Attributes

Parameter	Value / Default	Description
Group Object Class	group	Standard AD object class for security and distribution groups. Required to identify groups in the directory.

Group Name	name	Attribute that defines the display name of a group. Used by Versa to match groups during policy evaluation.
Group Member	memberOf	Attribute that lists group memberships for a user object. Ensures Versa can apply policies based on AD group membership.
User Object Class	user	Standard AD object class for user accounts. Required for identifying users in the directory.
User Name	userPrincipalName (recommended) or sAMAccountName	Attribute used for login. userPrincipalName (e.g., user@versanet-works.com) is modern and preferred. sAMAccountName is legacy but still supported.
Password Last Set	pwdLastSet	Attribute showing when a user's password was last changed. Useful for enforcing password expiration policies.
Password Max Age	maxPwdAge	Attribute defining the maximum password lifetime. Derived from the AD domain password policy.
Refresh Interval (sec)	21600 (default = 6 hours)	Determines how often Versa refreshes user and group information from LDAP. Can be tuned based on the frequency of directory changes.

click **Next** to proceed.

Add LDAP Authentication Profile



Next, fill in the **Name** field with a descriptive reference, such as *AD_Server_ACME-ONE*, and review all parameters to ensure they are correctly configured.

Add LDAP Authentication Profile



General

AD_Server_Acme_One

Description

Tags

Settings

Server Type

active-directory

FQDN or IP Address

10.163.306.33

VPN Name

ACME-ONE-Enterprise

Port

389

SSL Status

Disabled

SSL Mode

CA Certificate

File Name

Issued To

Issued By

Validity

Bind DN

cn=Administrator,cn=users,dc=acme-one,dc=com

Bind Password

***** @

Bind Timeout (sec)

30

Base DN

cn=users,dc=acme-one,dc=com

Domain Name

acme-one.com

Base Domain

Search Timeout (sec)

30

Cache Expiry Time (mins)

10

Concurrent Logins

3

Cancel

Back

Save

Then **Save**.

Add LDAP Authentication Profile



FQDN or IP Address

10.163.306.33

VPN Name

ACME-ONE-Enterprise

Port

389

SSL Status

Disabled

SSL Mode

CA Certificate

File Name

Issued To

Issued By

Validity

Bind DN

cn=Administrator,cn=users,dc=acme-one,dc=com

Bind Password

***** @

Bind Timeout (sec)

30

Base DN

cn=users,dc=acme-one,dc=com

Domain Name

acme-one.com

Base Domain

Search Timeout (sec)

30

Cache Expiry Time (mins)

10

Concurrent Logins

3

User and Group Profile

Group Object Class

group

Group Name

name

Group Member

membersOf

User Object Class

user

User Name

userPrincipalName

Refresh Interval (seconds)

21600

Password Last Set

pwdLastSet

Password Max Age

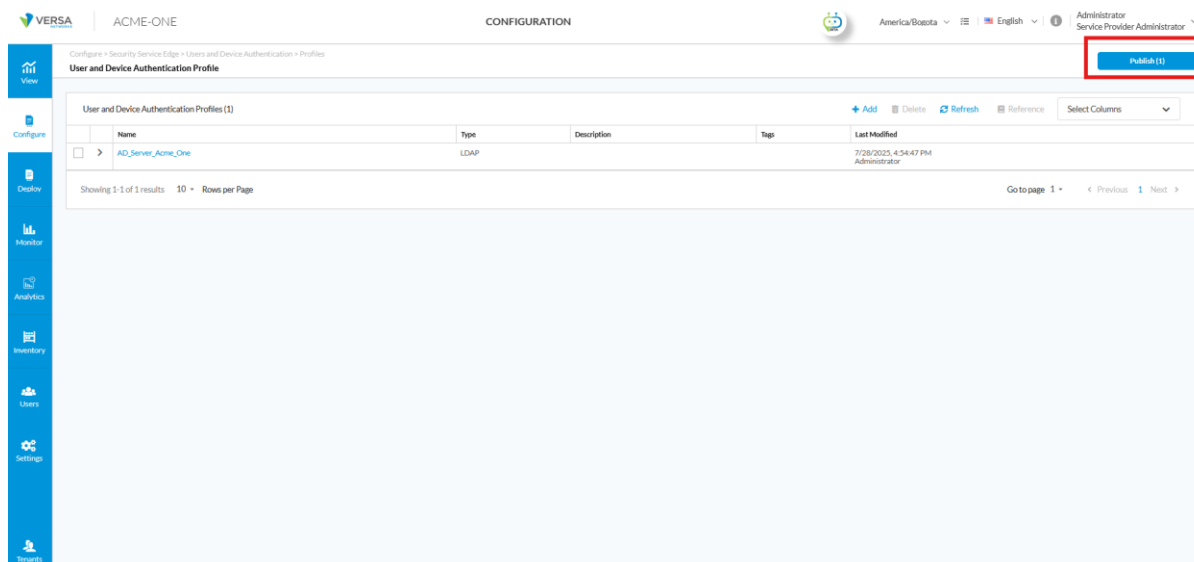
maxPwdAge

Cancel

Back

Save

Go to **Publish**.



The screenshot shows the Versa Configuration interface. At the top, the breadcrumb trail is 'Configure > Security Service Edge > Users and Device Authentication > Profiles'. The main heading is 'User and Device Authentication Profile'. A red box highlights the 'Publish (1)' button in the top right corner. Below this, a table titled 'User and Device Authentication Profiles (1)' contains one entry: 'AD_Server_Acme_One' of type 'LDAP'. The table has columns for Name, Type, Description, Tags, and Last Modified. At the bottom of the table, it says 'Showing 1-1 of 1 results' and '10 Rows per Page'.

After creating an Authentication Profile, you need to publish it to take effect.

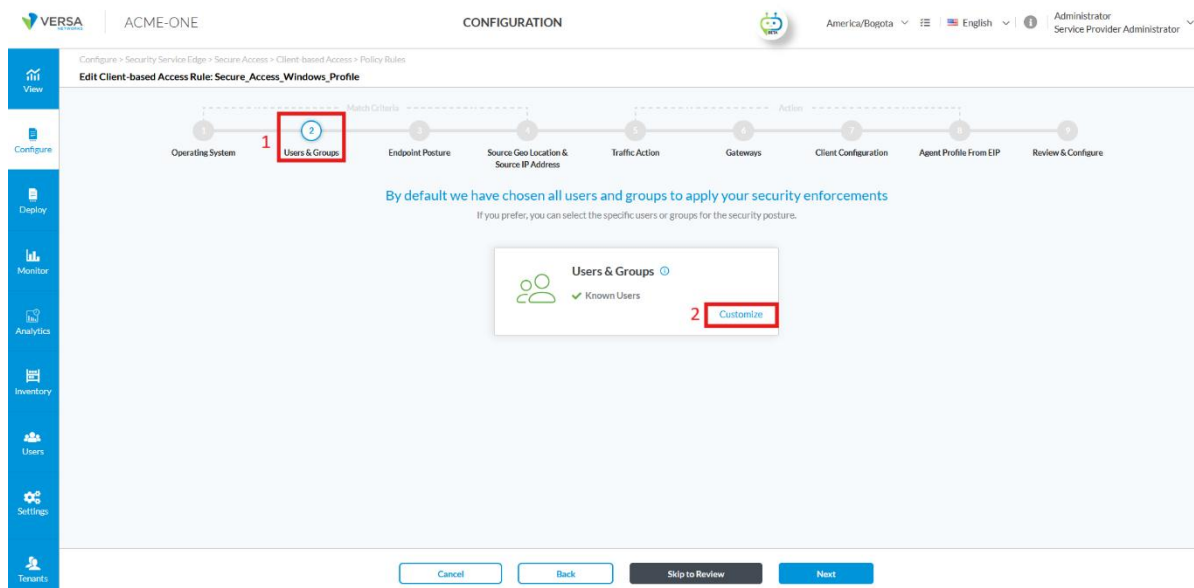
Verification

To verify that LDAP authentication is working, we can create a dummy Secure Access rule and check if the User or Group list is being populated.

Navigate to: **Configure > Security Service Edge > Secure Access > Client-based Access > Rules.**

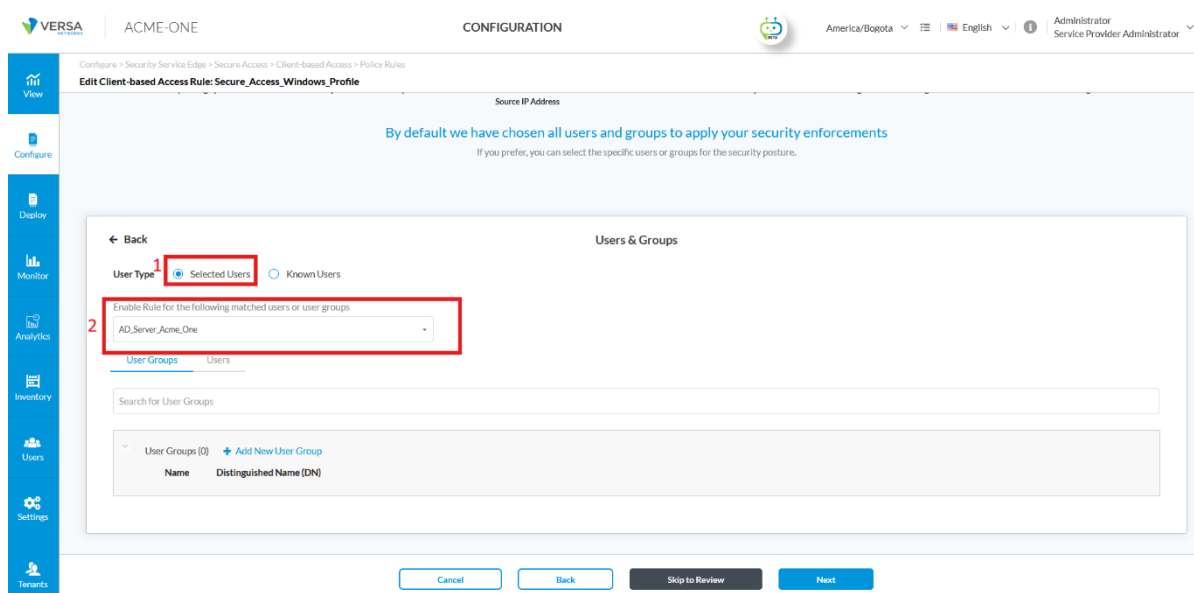
Click “+ **Add**” to create a new Secure Access Client rule or edit an existing rule.

In the **Match Criteria** configuration, navigate to the **Users & Groups** section. Under the **Users & Groups** panel, click on **Customize** to begin specifying user-based access rules using the authentication profile you previously created.



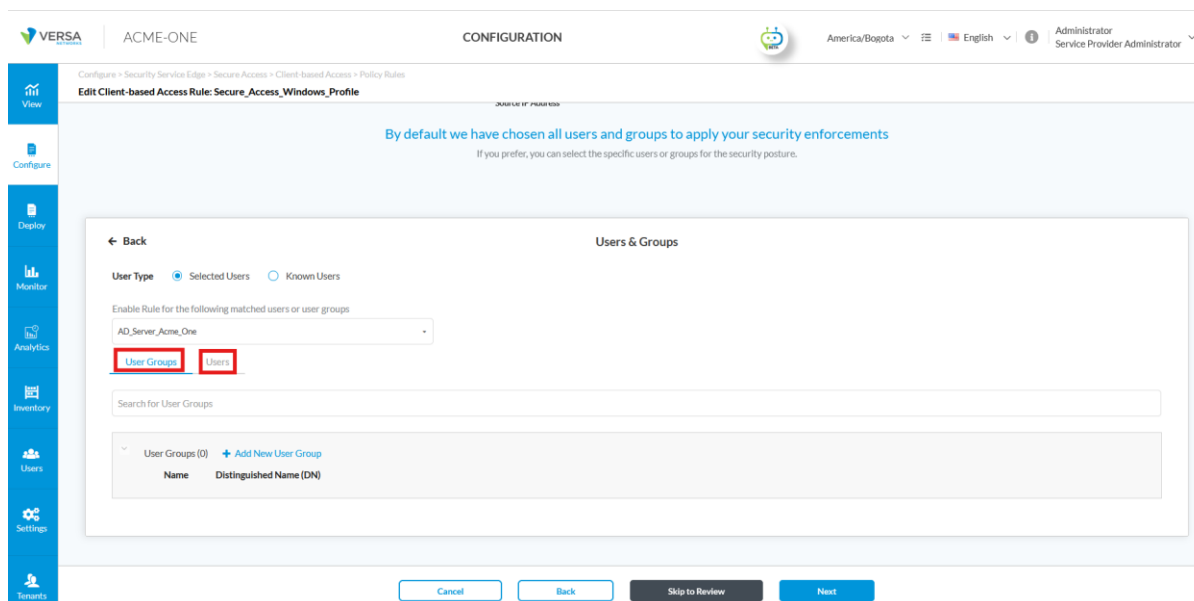
In the **Users & Groups** customization panel, select **Selected Users** as the user type. Then, under **Enable Rule for the following matched users or user groups**, choose the appropriate authentication profile (Example., AD_Server_Acme_One). This allows the policy to enforce access control based on Active Directory user group membership.

Note: When you choose an LDAP/AD server profile, you are able to list users and groups directly and select them for Secure Access rule configuration.



In this step, you can choose to add specific **users** or **groups** to enforce security policies.

Use the **User Groups** or **Users** tabs to select the desired entries.



After reviewing all configuration sections, click **Save** to apply the settings to the current Secure Access Profile. Then go to the **Publish** section at the top-right corner of the screen and click **Publish**.

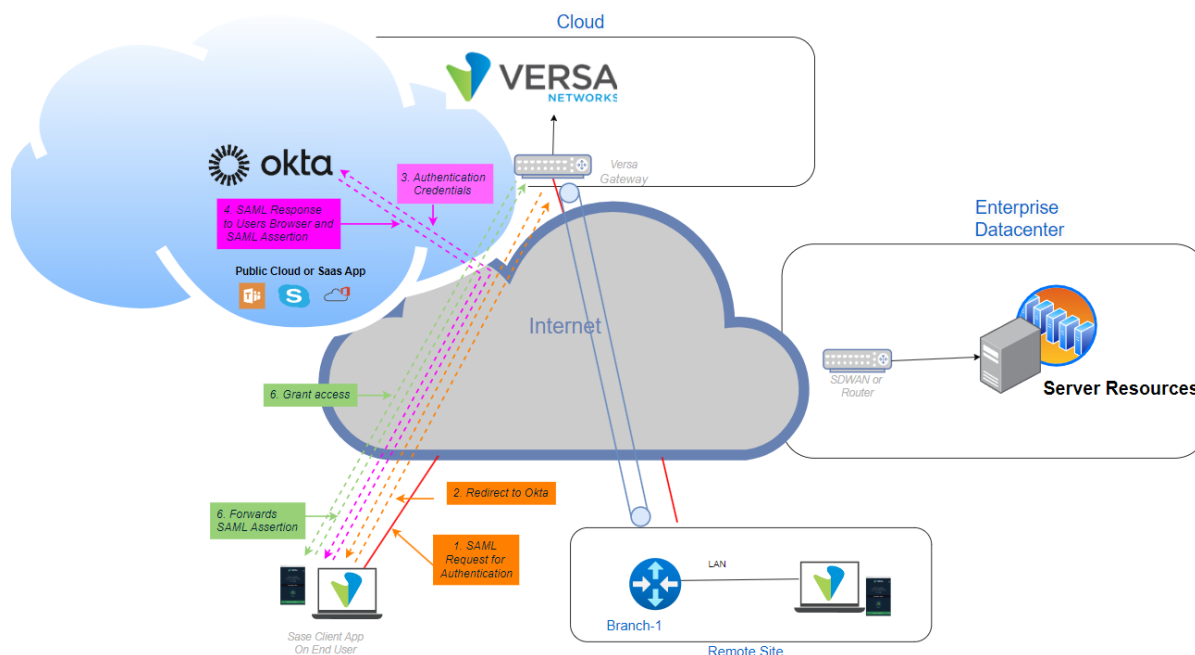
SAML Authentication

Security Assertion Markup Language (SAML) is an open standard for secure authentication and authorisation between an Identity Provider (IdP) and Service Providers (SPs), allowing users to authenticate once with the IdP and then seamlessly access multiple applications without re-entering credentials. It uses XML-based assertions to securely pass identity and authorisation data between parties, enabling web-based single sign-on (SSO) to services like Salesforce, Office 365, or Slack. In this workflow, platforms like Okta act as the IdP, verifying the user's identity and issuing a SAML assertion (secure token) to the SP, which grants access based on the trusted authentication. (SP), granting access without additional logins. Okta's SAML implementation is widely used for integrating third-party apps and simplifying enterprise authentication.

OKTA

Scenario

Within the enterprise context, Okta functions as the centralized Identity Provider (IdP) responsible for managing user identities and will be integrated with Versa SASE. When a user initiates a connection, the Versa SSE Gateway redirects the login request to Okta, which performs identity validation and returns a SAML assertion. This process grants access based on the User or group.



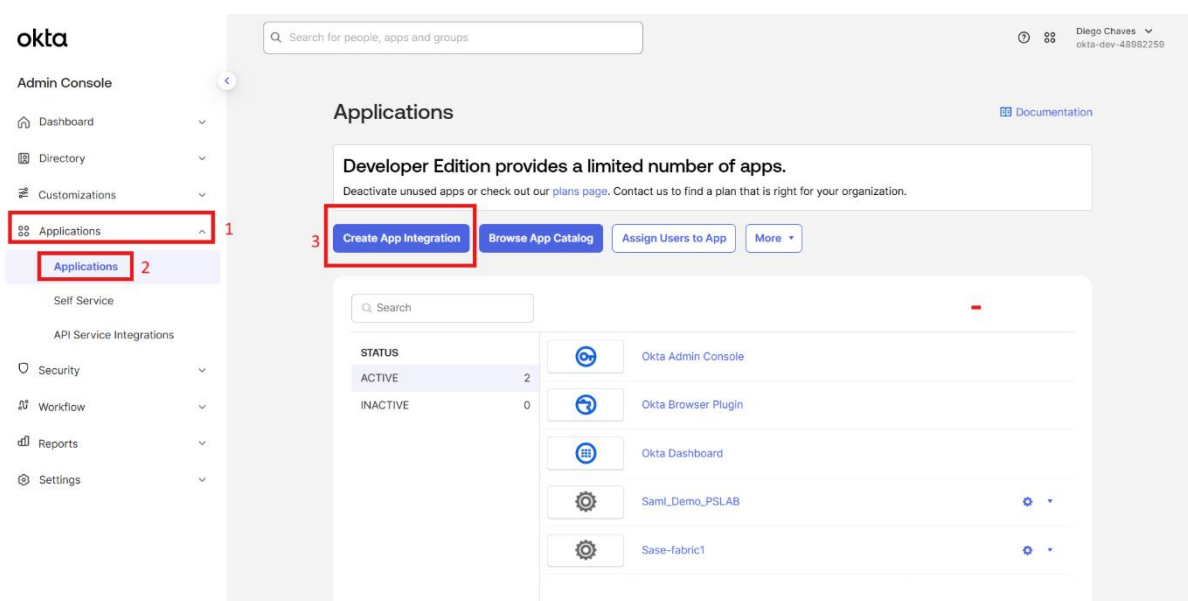
OKTA Portal Configuration

Create an Application in the OKTA portal.

- Create an application on Okta.
- Add users to the application.

1. login to your OKTA admin console.

Navigate to: Application then Click on Applications >> Create App Integration.



2. In the Create a **New App Integration** window, click SAML 2.0, and then click **Next**.

Create a new app integration

Sign-in method

[Learn More](#)

- ☐ **OIDC - OpenID Connect**
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- ☒ **SAML 2.0**
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- ☐ **SWA - Secure Web Authentication**
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- ☐ **API Services**
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Cancel

Next

- In the **General Settings > App name** field, enter an application name, and then click **Next**.

okta

Admin Console

Dashboard

Directory

Customizations

Applications

Security

Workflow

Reports

Settings

Search for people, apps and groups

Diego Chaves
okta-dev-48982259

Create SAML Integration

1 General Settings 2 Configure SAML 3 Feedback

1 General Settings

App name ACME-ONE-SAML

App logo (optional)

App visibility ☐ Do not display application icon to users

Cancel Next

© 2025 Okta, Inc. Privacy Status site OK12 Cell (US) Version 2025.07.3 E Feedback

- Define custom attributes.

- In the SAML settings, enter information for the indicates fields.

Field	Description
Single Sign-On URL	<p>URL where Okta sends SAML responses.</p> <p>Format: https://<SASE-GW-FQDN>/versa-flexvnf/saml/login-consumer.</p> <p>Example: https://acme-one-sasegwdiegos-lab.versanow.net/versa-flexvnf/saml/login-consumer</p>
Audience URI (SP Entity ID)	<p>Service Provider (SP) entity ID:</p> <p>Format: https://<SASE-GW-FQDN>/metadata.</p> <p>Example: https://acme-one-sasegwdiegos-lab.versanow.net/metadata</p>
Default Relay State	<p>Used for IdP-initiated SSO:-</p> <p>System user: vd-ui::system</p> <p>Tenant user: vd-ui::<organization-name></p>
Attribute Statements	Define attributes such as role, organisation, and idle timeout. (<i>Case-sensitive</i>)
Group Attribute Statements (optional)	<p>Enables Versa to import user-to-group mappings from Okta Configuration: -</p> <p>Name: https://schemas.microsoft.com/ws/2008/06/identity/claims/groups</p> <p>Name format: <i>Unspecified</i></p> <p>Filter: Regex (.*)</p> <p>This ensures all groups a user belongs to are included in the SAML assertion, enabling group-based policies (Internet Protection, Private App Protection, etc.).</p>
Preview the SAML Assertion	Use this option to preview. Copy the metadata and save as an XML file for Versa configuration.

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion ID="id-5773745532411060288246009139" IssueInstant="2025-08-08T17:10:21.828Z" Version="2.0"
  xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"/>
  <saml2:Subject>
    <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">userName</saml2:NameID>
    <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      <saml2:SubjectConfirmationData NotOnOrAfter="2025-08-08T17:15:22.008Z" Recipient="https://acme-one-sasegwdiegos-lab.versanow.net/versa-flexvnf/saml/login-consumer"/>
    </saml2:SubjectConfirmation>
  </saml2:Subject>
  <saml2:Conditions NotBefore="2025-08-08T17:05:22.008Z" NotOnOrAfter="2025-08-08T17:15:22.008Z">
    <saml2:AudienceRestriction>
      <saml2:Audience>https://acme-one-sasegwdiegos-lab.versanow.net/metadata</saml2:Audience>
    </saml2:AudienceRestriction>
  </saml2:Conditions>
  <saml2:AuthnStatement AuthnInstant="2025-08-08T17:10:21.828Z">
    <saml2:AuthnContext>
      <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClassRef>
    </saml2:AuthnContext>
  </saml2:AuthnStatement>
  <saml2:AttributeStatement>
    <saml2:Attribute Name="https://schemas.microsoft.com/ws/2008/06/identity/claims/groups" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml2:AttributeValue>
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">GroupName Match Starts with ".*" (ignores case)
      </saml2:AttributeValue>
    </saml2:Attribute>
  </saml2:AttributeStatement>
</saml2:Assertion>
```

Configure the parameters as shown in the previous table, and then click **Next**.

Create SAML Integration

1 General Settings
2 **Configure SAML**
3 Feedback

A SAML Settings

General

Single sign-on URL

https://acme-one-sasegwdiegios-lab.versanow.net/vers

Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID)

https://acme-one-sasegwdiegios-lab.versanow.net/met

Default RelayState

If no value is set, a blank RelayState is sent

Name ID format

Unspecified

Application username

Okta username

Update application username on

Create and update

Show Advanced Settings

Attribute Statements (optional)

LEARN MORE

Name	Name format (optional)	Value
	Unspecified	

Add Another

Group Attribute Statements (optional)

Name	Name format (optional)	Filter
https://schemas.mic	Unspecified	Matches regex .*

Add Another

What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.


5. In the Help Okta Support understand how you configured this application section, you can provide optional information for Okta Support.
 - Under App type, check This is an internal app that we have created (recommended for internal SSO integrations like Versa).
 - Click Finish to complete the SAML integration setup.
6. Retrieve SAML Integration Details

After completing the previous steps, Okta displays the SAML configuration details required to set up the SAML profile in Versa Concerto. Copy the Sign on URL, the Issuer value and Download the Signing Certificate file, CHANGE.


SAML 2.0


Default Relay State


Metadata details



Metadata URL `https://dev-48982259.okta.com/app/exkpzj71tIng6xg675d7/sso/saml/metadata`
 Copy

▼ Hide details

Sign on URL `https://dev-48982259.okta.com/app/dev-48982259_acmeonesaml_1/exkpzj71tIng6xg675d7/sso/saml`
 Copy

Sign out URL `https://dev-48982259.okta.com`
 Copy

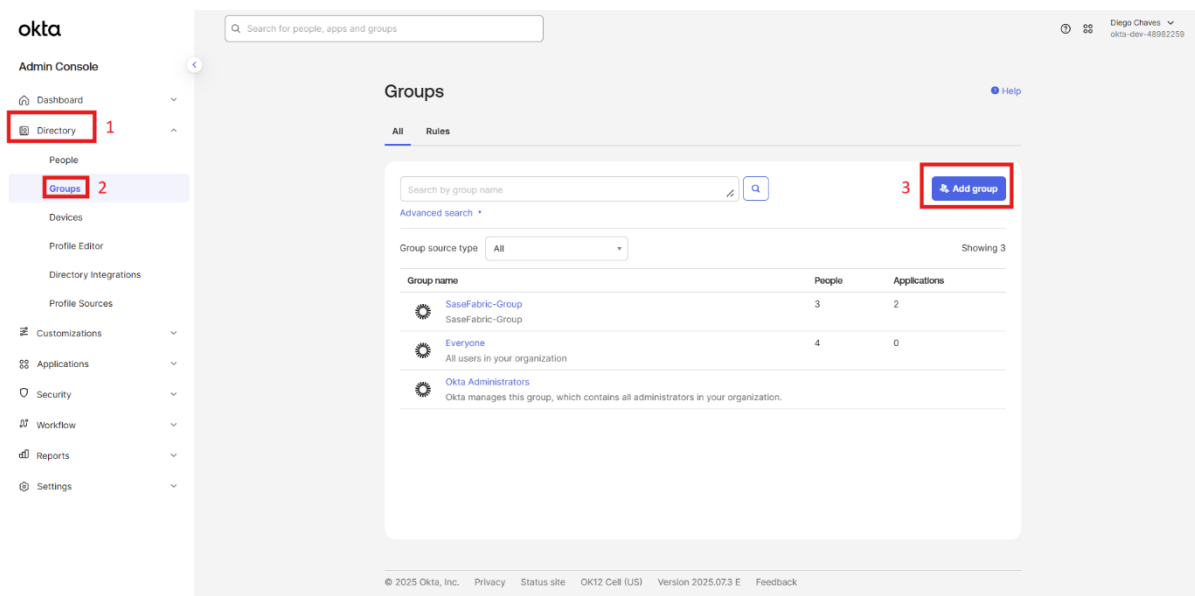
Issuer `http://www.okta.com/exkpzj71tIng6xg675d7`
 Copy

Signing Certificate  Download  Copy

▶ Certificate fingerprint

Note: Rename the downloaded certificate file from .cert to .crt before use

7. Create the Groups and Users. **Navigate** to **Directory>Groups** then Click **Add group**



In the name field, enter a group name

Add group

Name

Engineering-Group

Description (optional)

Engineering-Group

Save

Cancel

Refresh the page and click to the newly created group “**Engineering-Group**”.

After opening the group, go to the **Applications** tab and Click Assing Applications To assign the newly created SAML application to the group.

Engineering-Group

1

Actions

Engineering-Group

Created: 8/8/2025

Last modified: 8/8/2025

View logs

People

Applications

2 Profile

Directories

Admin roles

Applications

3

Assign applications

01101110

01101111

01101100

01101000

01101001

01101110

01100111

No applications assigned to this group

Use Assign applications to assign apps to this group

Group Members

People, apps and directories can be members of a group. People are automatically assigned any apps that are members of a group.

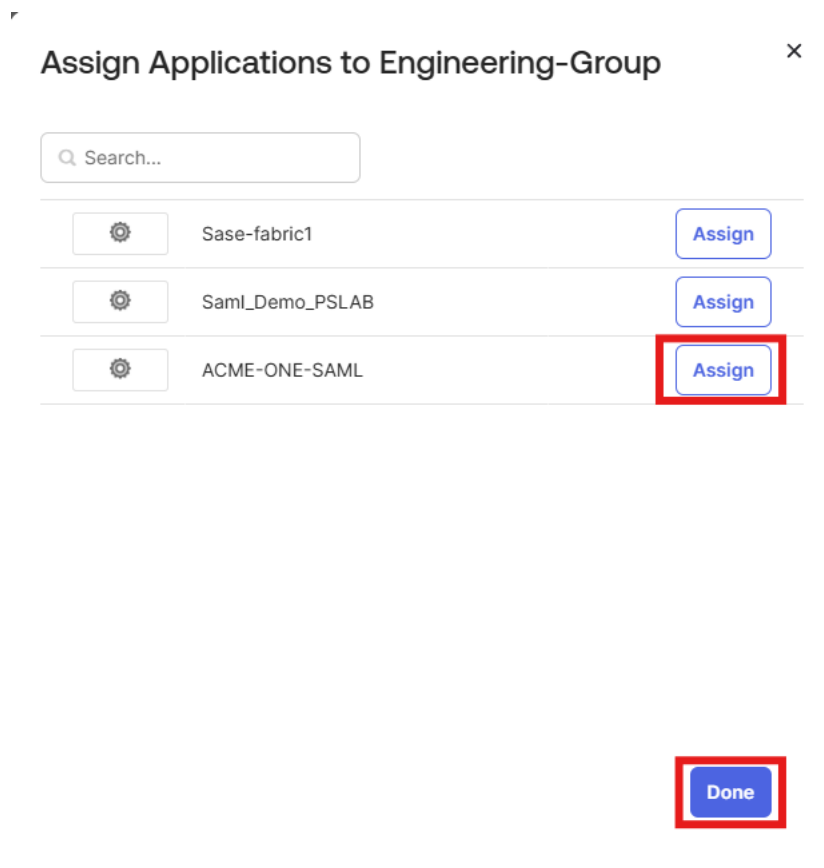
Directories, like Active Directory or Workday with profile management enabled, will manage user profiles when they are members of a group.

Use **Assign People** to add people to this group. Use **Assign applications** to do the equivalent for applications.

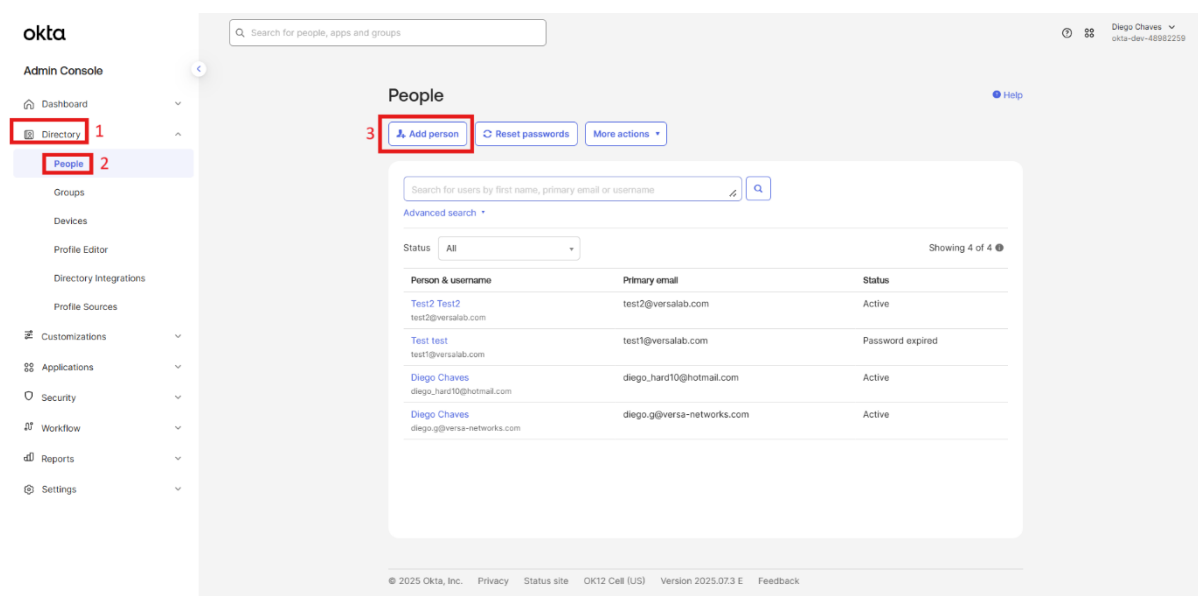
How do I edit the group name and description?

Hover your mouse over the group name or description to edit them inline.

Select newly created SAML application



To create users, Navigate to **Directory>People**, click **Add Person**, fill in the required user details in the pop-up, assign the necessary groups, and save.



In the **Add Person** window, set **User** type to User, enter the **first name**, last name, **username**, and primary email, select the required group (Example Engineering-Group), choose **Activate now**, set a password, and ensure User must change password on first login is checked before saving.

Add Person

User type ?

User ▼

First name

VIP1

Last name

VIP


Username

vip1@acme-one.com

Primary email

vip1@acme-one.com

Groups (optional)

 Engineering-Group x

Activation

Activate now ▼

☒ I will set password

.....

☒ User must change password on first login

Do not send unsolicited or unauthorized activation emails. [Read more](#)

Save

Save and Add Another

Cancel

Concerto OKTA Authentication Profiles

Navigate to User and Device Authentication Profiles

Go to: Configure > Security Service Edge > Users and Device Authentication > Profiles then "+ Add"

Configure > Security Service Edge > Users and Device Authentication > Profiles

User and Device Authentication Profile

Publish(1)

User and Device Authentication Profiles (1)

+ Add Delete Refresh Reference Select Columns

Name	Type	Description	Tags	Last Modified
AD_Server_Acme_One	LDAP			7/28/2025, 4:54:47 PM Administrator

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

Select **SAML**, Click Get Started

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.

SAML

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

RADIUS

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

Versa Directory

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

Note: Only one Versa Directory authentication profile can be added.

User Certificate Based

Certificate-based authentication is a secure method to validate the identity of users. 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.

Device Certificate Based

Certificate-based authentication is a secure method to validate the identity of devices. 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.

Cancel Get Started

Select **OKTA**

To configure the settings, use the information collected in **Step 6** from Okta SAML app created. In the Okta admin console, go to **Applications**, open the created app, click **Sign On**, and scroll down to view the **SAML setup instructions**.

SAML 2.0

Default Relay State

Metadata details

Metadata URL
https://dev-48982259.okta.com/app/exkpzj71tINg6xg675d7/sso/saml/metadata
Copy

Hide details

Sign on URL
https://dev-48982259.okta.com/app/dev-48982259_acmeonesaml_1/exkpzj71tINg6xg675d7/sso/saml
Copy

Sign out URL
https://dev-48982259.okta.com
Copy

Issuer
http://www.okta.com/exkpzj71tINg6xg675d7
Copy

Signing Certificate
Download Copy

Certificate fingerprint


The information collected from the Okta SAML application created in **Step 6** (In this example, ACME-ONE-SAML) is used here to complete the configuration. **Single Sign-on URL**, **Service Provider Entity ID** and **Identity Provider Entity ID** are mandatory fields and the signing certificate from Okta must be uploaded. This information should be gathered beforehand to set up the authentication profile correctly.


Add SAML Authentication Profile


✕


1 2 3
 Settings Users And User Groups Review & Submit


Select SAML Type



 OKTA


 Ping Identity


 Office 365


 Microsoft Entra ID


 Google IAM


 Cisco Duo

Other

Single Sign-on URL *

Service Provider Entity ID *

Identity Provider Entity ID *

Prefix ID

Group Attribute

Reply URL (Assertion Consumer Reply URL)

- https://acme-one-sasegwldiegos-lab.versanow.net/versa-flexvrf/saml/login-consumer

Single Sign-out URL

Service Provider Certificate

~Select~ + Add New

Identity Provider Certificate * + Add New

Cache Expiry Time (mins)

Concurrent Logins

Cancel
Skip to Review
Next

Complete the parameters using the values from the Okta app:

Example:

Single Sign-on URL: https://dev-48982259.okta.com/app/dev-48982259_ac-meonesaml_1/exkpzj71tINg6xg675d7/sso/saml

Service Provider Entity ID: <https://acme-one-sasegwldiegos-lab.versanow.net/metadata>

Identity Provider Issuer: <http://www.okta.com/exkpzj71tINg6xg675d7>

In the **Prefix ID** field fill it as OKTA

24

Add SAML Authentication Profile

1
2
3

Settings
Users And User Groups
Review & Submit

Select SAML Type

okta
OKTA

Pingidentity
Ping Identity

Office365
Office 365

Microsoft Entra ID

Google IAM

Cisco Duo

Other

Single Sign-on URL *

https://dev-48982259.okta.com/app/dev-48982259_acmeone-saml_1/okta/711hgngt75d7/so/saml

Service Provider Entity ID *

https://acme-one-sasgwldiegos-labversanow.net/metadata

Identity Provider Entity ID *

http://www.okta.com/okta/711hgngt75d7

Prefix ID

OKTA

Group Attribute
Reply URL (Assertion Consumer Reply URL)

https://acme-one-sasgwldiegos-labversanow.net/versa-flexvnf/saml/login-consumer

Single Sign-out URL
Service Provider Certificate

~Select~
Add New

Identity Provider Certificate *

~Select~
Add New

Cache Expiry Time (mins)

10

Concurrent Logins

1

Cancel
Skip to Review
Next

Then Upload the **Identity Provider Certificate** by clicking on the **Add New** button. Rename the downloaded certificate file from .cert to .crt before use on concerto.

Add SAML Authentication Profile

1
2
3

Settings
Users And User Groups
Review & Submit

Select SAML Type

okta
OKTA

Pingidentity
Ping Identity

Office365
Office 365

Microsoft Entra ID

Google IAM

Cisco Duo

Other

Single Sign-on URL *

https://dev-48982259.okta.com/app/dev-48982259_acmeone-saml_1/okta/711hgngt75d7/so/saml

Service Provider Entity ID *

https://acme-one-sasgwldiegos-labversanow.net/metadata

Identity Provider Entity ID *

http://www.okta.com/okta/711hgngt75d7

Prefix ID

OKTA

Group Attribute
Reply URL (Assertion Consumer Reply URL)

https://acme-one-sasgwldiegos-labversanow.net/versa-flexvnf/saml/login-consumer

Single Sign-out URL
Service Provider Certificate

~Select~
Add New

Identity Provider Certificate *

~Select~
Add New

Cache Expiry Time (mins)

10

Concurrent Logins

1

Cancel
Skip to Review
Next

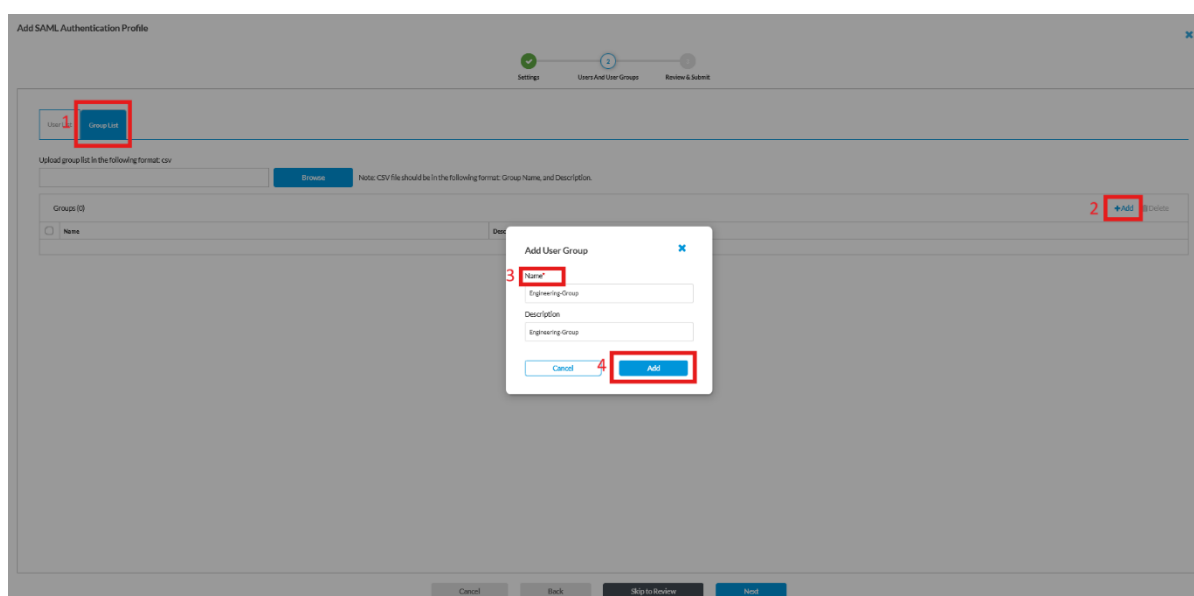
Name to **CA-Chain Name** upload certificate issue by clicking on the Upload File.

Then **Next**

On the **Users and User Groups** page, you can associate either an individual **user list** or a complete **group list** with the SAML authentication profile. The advantage of this approach is that a group or

user list can be adjusted and applied within the authentication profile, allowing you to enforce a specific Secure Access rule for those users. You can define **users and groups** in two different ways:

- **User List:** upload a CSV file or manually add users one by one.
- **Group List:** upload a CSV file or manually add a user group. In this example, we will use the group created earlier in the Okta portal (for example, **Engineering-Group**). Add the group, click Add, and then click Next to continue.



The screenshot shows the 'Add SAML Authentication Profile' wizard, Step 2: Users And User Groups. The 'Group List' tab is selected. A modal 'Add User Group' dialog is open, showing fields for Name, Description, and a list of groups. The 'Add' button in the modal is highlighted with a red box and the number 4. The 'Add' button in the main dialog is highlighted with a red box and the number 2. The 'Group List' tab is highlighted with a red box and the number 1. The 'Add' button in the modal is highlighted with a red box and the number 4.

On the **Review & Submit** page, enter a **Name** and **Description** for the profile, then review all configuration details including general information, SAML settings, and assigned users or groups. Once confirmed, click **Save** to complete the profile creation.

Settings Users And User Groups Review & Submit

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

General

Name:

Description:

Tag:

Settings [Edit](#)

SAML Type: OKTA

Single Sign-on URL: https://dev-48962259.okta.com/app/dev-48962259_acmeonesaml_1/okta/718hgmg73d7/sso/saml

Single Sign-out URL: https://dev-48962259.okta.com/app/dev-48962259_acmeonesaml_1/okta/718hgmg73d7/sso/saml

Service Provider Entity ID: <https://acme-one-sasgwedlgo-lab-versanox.net/metadata>

Service Provider Certificate: <https://www.okta.com/okta/718hgmg73d7>

Identity Provider Entity ID: OKTA-ACME

Identity Provider Certificate: OKTA

Prefix ID: 30

Cache Expiry Time (mins): 1

Concurrent Logins: 1

Group Attribute: <https://acme-one-sasgwedlgo-lab-versanox.net/versa-flexont/iam/login-consumer>

Reply URL (Assertion Consumer Reply URL): <https://acme-one-sasgwedlgo-lab-versanox.net/versa-flexont/iam/login-consumer>

Users & User Groups [Edit](#)

Users(0):

User Groups(1):

Cancel Back Save

After creating and Publishing the Authentication Profile, you must apply them to the Secure Access Client policy to enforce authentication and apply the corresponding security policies.

Microsoft Entra ID

Microsoft Entra ID is a cloud-based identity and access management service that provides secure single sign-on (SSO) to Microsoft 365, SaaS apps, and on-premises resources using standards like SAML, OAuth, and OpenID Connect.

Scenario

The same scenario described above also applies when using Entra ID as the Identity Provider. Because it is a cloud-based IdP, Entra ID can seamlessly integrate with Versa SASE via SAML, validating user identities and issuing assertions that grant access to both cloud services and enterprise applications under consistent policy enforcement.

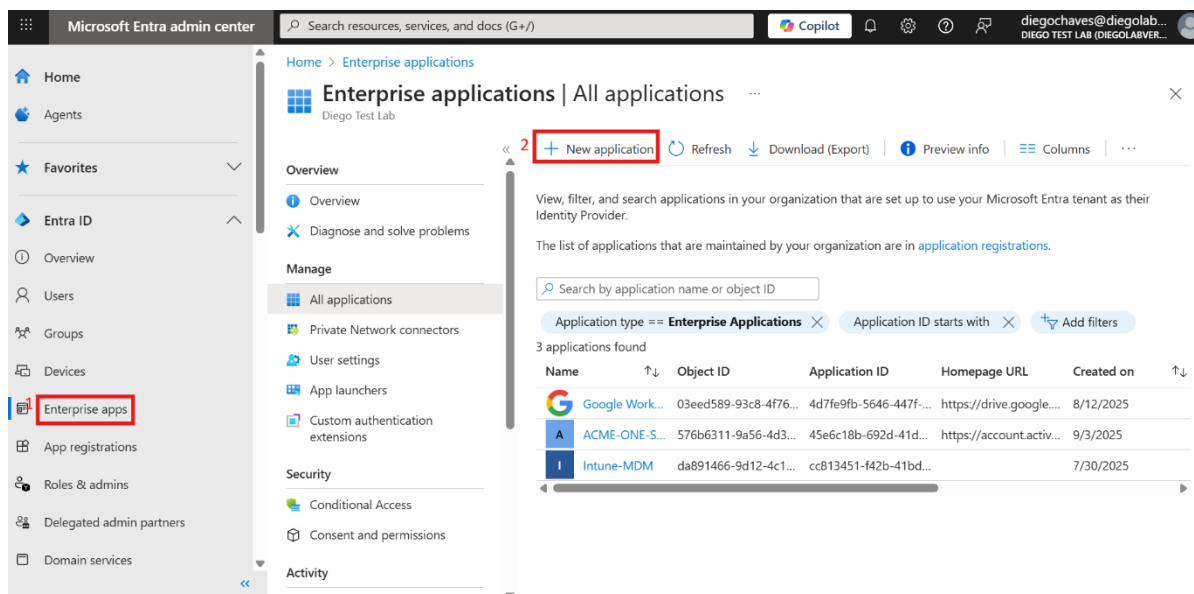
Entra ID Configuration

Create an Enterprise Application in the Entra ID portal.

- Create a new application in Entra ID.
- Assign users or groups to the application.

1. Log in to your **Entra ID / Azure portal**.

Navigate to: **Enterprise apps > New application**.



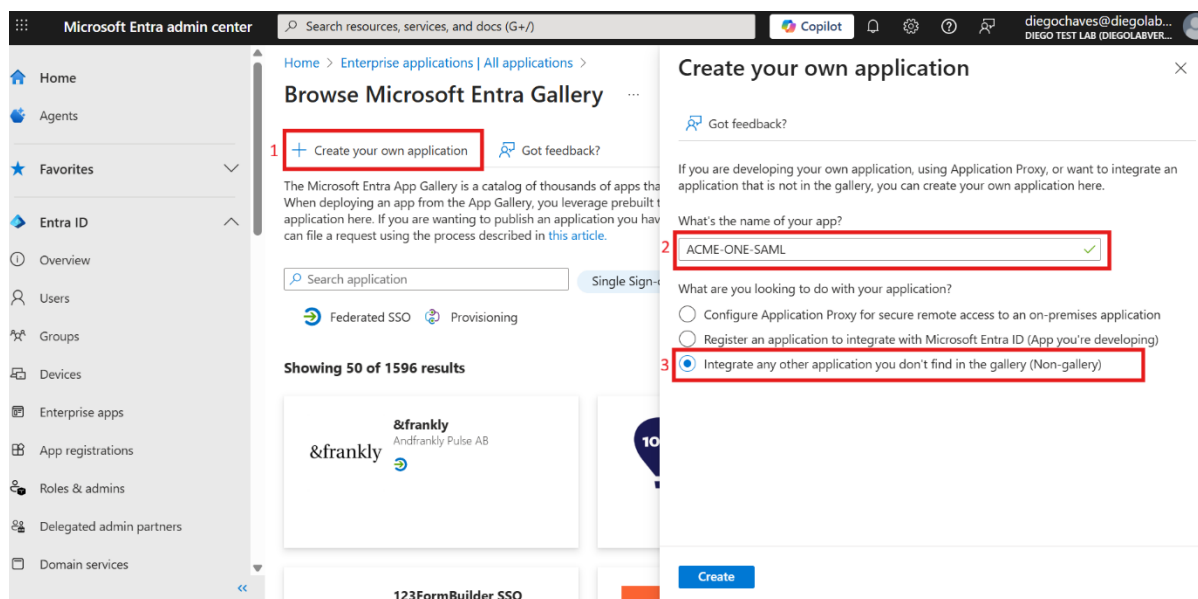
2. Select **Create a new application**

Click + **Create your own application**.

Enter the application name (Example, **ACME-ONE-SAML**).

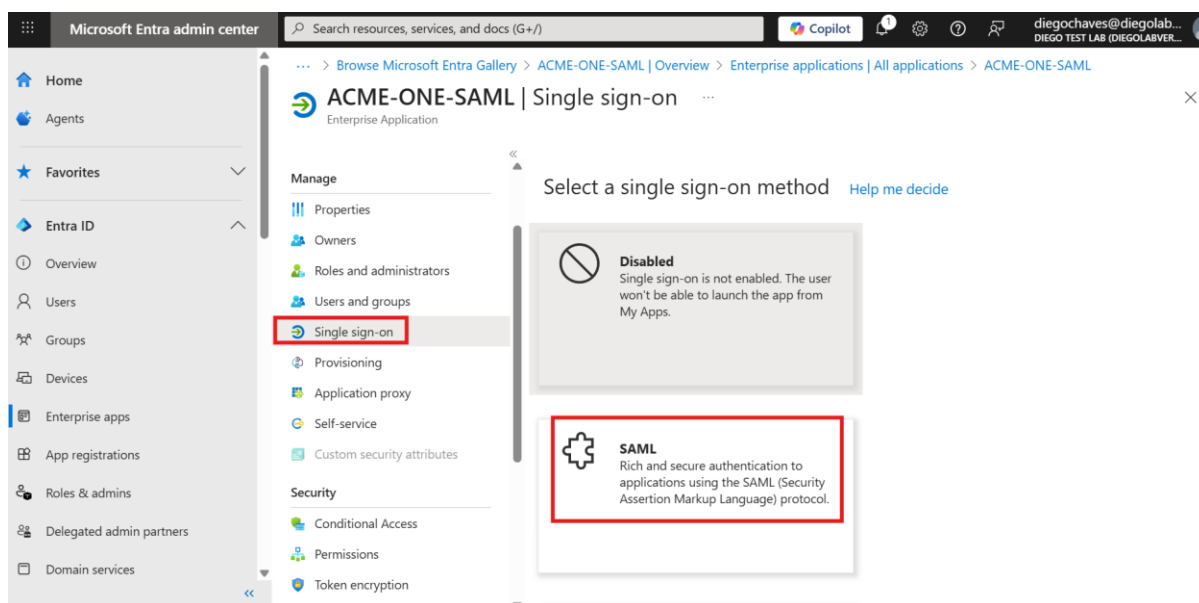
Select **Integrate any other application you don't find in the gallery (Non-gallery)**.

Click **Create**.



3. Set up **SAML-based** SSO

- Open the newly created application.
- Go to **Single sign-on** and select **SAML** as the method.

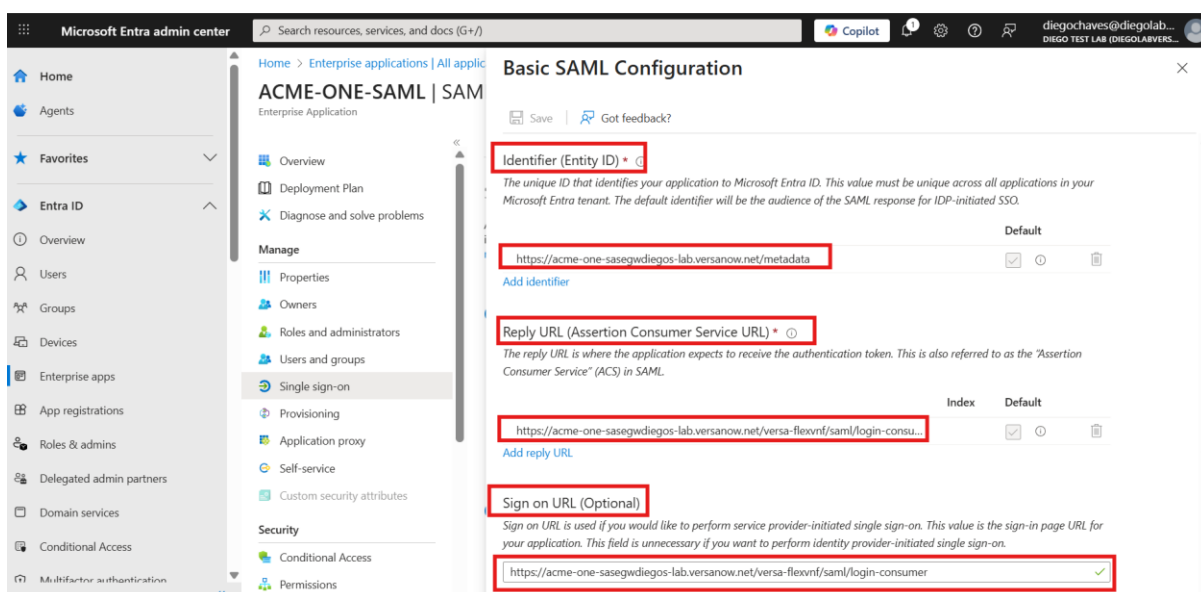


4. In the SAML settings, enter information for the indicates fields.

Field	Description
Reply URL (Assertion Consumer Service URL) and Sign on URL (Optional)	Enter the URL to which Okta sends OAuth responses. The responses are sent in the format https://saseGw-FQDN/versa-flexvnf/saml/login-consumer . (Here the Gateway's FQDN is used as the main URL +/versa-flexvnf/saml/login-consumer). In the example https://acme-one-sasegwdiegos-lab.versanow.net/versa-flexvnf/saml/login-consumer
Identifier (Entity ID)	Enter the service provider entity ID, which is https://saseGw-FQDNt/metadata . In the example https://acme-one-sasegwdiegos-lab.versanow.net/metadata
Attribute Statements	Enter the role, organization, and idle timeout attributes. The attribute strings are case sensitive.
Group Attribute Statements (optional)	<p>To allow Versa to receive all user-to-group mappings from Okta, configure a group attribute statement as follows:</p> <p>Name: https://schemas.microsoft.com/ws/2008/06/identity/claims/groups</p> <p>Name format: Unspecified</p> <p>Filter: Select Regex (or equivalent option) and enter .*</p> <p>This configuration ensures that all groups a user belongs to are included in the SAML assertion. Versa uses this information to apply group-based mappings for Internet Protection rules, Private App Protection, and other user-based policies.</p>
Preview the SAML Assertion	Click to preview the SAML assertion . Copy the metadata, and save it as an XML file.

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion ID="id-5773745532411060288246009139" IssueInstant="2025-08-08T17:10:21.828Z" Version="2.0"
  xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"/>
  <saml2:Subject>
    <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified" userName="/saml2:NameID">
    <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      <saml2:SubjectConfirmationData NotOnOrAfter="2025-08-08T17:15:22.008Z" Recipient="https://acme-one-sasegwdiegolab-versanow.net/versa-flexvnt/saml/login-consumer"/>
    </saml2:SubjectConfirmation>
  </saml2:Subject>
  <saml2:Conditions NotBefore="2025-08-08T17:05:22.008Z" NotOnOrAfter="2025-08-08T17:15:22.008Z">
    <saml2:AudienceRestriction>
      <saml2:Audience>https://acme-one-sasegwdiegolab-versanow.net/metadata/</saml2:Audience>
    </saml2:AudienceRestriction>
  </saml2:Conditions>
  <saml2:AuthnStatement AuthnInstant="2025-08-08T17:10:21.828Z">
    <saml2:AuthnContext>
      <saml2:AuthnContextClassRef urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport/</saml2:AuthnContextClassRef>
    </saml2:AuthnContext>
  </saml2:AuthnStatement>
  <saml2:AttributeStatement>
    <saml2:Attribute Name="https://schemas.microsoft.com/ws/2008/06/identity/claims/groups" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml2:AttributeValue>
        xmlns:xsi="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">GroupName Match Starts with ".*" (ignores case)
      </saml2:AttributeValue>
    </saml2:Attribute>
  </saml2:AttributeStatement>
</saml2:Assertion>
```

- Configure the parameters as shown in the previous table, in Basic SAML Configuration and then click **Save**.



- Define **Attributes & Claims**.




Add the following mappings, click **+Add new claim**:

- `user.userprincipalname` > name
- "ACME-ONE" > organization
- `user.assignedroles` > role

[Home](#) > [Enterprise applications | All applications](#) > [ACME-ONE-SAML | SAML-based Sign-on](#) > [SAML-based Sign-on](#) > [Attributes & Claims](#) >

Manage claim ...

×

 Save
  Discard changes
  Got feedback?

Name * ✓

Namespace ✓

Choose name format

Source * ☒ Attribute ☐ Transformation ☐ Directory schema extension

Source attribute * ✓


Claim conditions

Advanced SAML claims options

[Home](#) > [Enterprise applications | All applications](#) > [ACME-ONE-SAML | SAML-based Sign-on](#) > [SAML-based Sign-on](#) > [Attributes & Claims](#) >

Manage claim ...

×

 Save
  Discard changes
  Got feedback?

Name * ✓

Namespace ✓

Choose name format

Source * ☒ Attribute ☐ Transformation ☐ Directory schema extension

Source attribute * ✓

Claim conditions

Advanced SAML claims options

[Home](#) > [Enterprise applications | All applications](#) > [ACME-ONE-SAML | SAML-based Sign-on](#) > [SAML-based Sign-on](#) > [Attributes & Claims](#) >

Manage claim ...

×

 Save
  Discard changes
  Got feedback?

Name * ✓

Namespace ✓

Choose name format

Source * ☒ Attribute ☐ Transformation ☐ Directory schema extension

Source attribute * ✓

Claim conditions

Advanced SAML claims options

- Configure **Group Claims referring to previous table Group Attribute Statements**.

Click + Add a group Claim

Home > App registrations > Enterprise applications | All applications > ACME-ONE-SAML | SAML-based Sign-on > SAML-based Sign-on >

Attributes & Claims ...

×

+ Add new claim + Add a group claim Columns | Got feedback?

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...] ***

Additional claims

Claim name	Type	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname ***

✓ Advanced settings

- Under **Group Claims**, choose **All groups**.
- Set **Source attribute** to *Group ID*.

Group Claims

Manage the group claims used by Microsoft Entra ID to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

☐ None
☒ All groups
☐ Security groups
☐ Directory roles
☐ Groups assigned to the application

Source attribute *

Group ID

☐ Emit group name for cloud-only groups

Advanced options

Save

- Click **Advance options** then Enable **Customize the name of the group claim** > set name as groups.

Group Claims

Manage the group claims used by Microsoft Entra ID to populate SAML tokens issued to your app

☐ Emit group name for cloud-only groups ⓘ

Advanced options

☐ Filter groups

Attribute to match

Match with

String

☒ Customize the name of the group claim

Name (required)

groups

Namespace (optional)

☐ Emit groups as role claims ⓘ

Save

- Click on **Apply regex replace to groups claim content** then set **Regex replace**:

- Pattern: .*
- Replacement: \$0

Group Claims

Manage the group claims used by Microsoft Entra ID to populate SAML tokens issued to your app

String

☒ Customize the name of the group claim

Name (required)

groups

Namespace (optional)

☐ Emit groups as role claims ⓘ

☒ Apply regex replace to groups claim content

Regex pattern * ⓘ

.*

Regex replacement pattern * ⓘ

\$0

☐ Expose claim in JWT tokens in addition to SAML tokens

Save

- Retrieve SAML Integration Details

After completing the previous steps, Entra-id displays the SAML configuration details required to set up the SAML profile in Versa Concerto. Copy the Sign on URL, the Issuer value and Download the Signing Certificate file.

The screenshot shows the 'ACME-ONE-SAML | SAML-based Sign-on' page in the Microsoft Entra admin center. The left sidebar contains navigation options like Overview, Deployment Plan, and Manage. The main content area is divided into two sections: 'SAML Certificates' and 'Set up ACME-ONE-SAML'. In the 'SAML Certificates' section, the 'Token signing certificate' is listed with details like Status (Active), Thumbprint, Expiration, and Notification Email. Below this, there are links to download the 'Certificate (Base64)', 'Certificate (Raw)', and 'Federation Metadata XML'. In the 'Set up ACME-ONE-SAML' section, there are fields for 'Login URL', 'Microsoft Entra Identifier', and 'Logout URL', each with a corresponding URL value and a download icon. Red boxes highlight the 'Certificate (Base64)' download link and the 'Login URL' field.

- Create the Groups and Users.


Navigate to Microsoft Entra admin **Center user > Group** then Click New Group

The screenshot shows the 'Groups | Overview' page in the Microsoft Entra admin center. The left sidebar contains navigation options like Home, Agents, Favorites, and Entra ID. The main content area shows the 'Groups | Overview' page with a 'New group' button highlighted in red. Below this, there are sections for 'Basic information' (Total groups: 4, Dynamic groups: 1, M365 groups: 3, Cloud groups: 4, Security groups: 1, On-premises groups: 0), 'Alerts', and 'Feature highlights' (Access reviews, Conditional Access). The 'Groups' link in the left sidebar is also highlighted in red.

In the name field, enter an **group** name

[Home](#) > [Groups | Overview](#) > [Users](#) > [Groups | Overview](#) > [New Group](#) > [Groups | Overview](#) >

New Group ...

 Got feedback?

Group type * ⓘ
Security

Group name * ⓘ
VIP_Group

Group description ⓘ
Enter a description for the group

Microsoft Entra roles can be assigned to the group ⓘ
Yes No

Membership type * ⓘ
Assigned

Owners
No owners selected

Members
No members selected

Create

Refresh the page and click to the newly created group **"VIP_Group"**.

To create users Navigate to Microsoft Entra admin Center > user, click New User.

In the Basics tab, define the User Principal Name (UPN) and Display Name.

Example:

UPN → vip@acme-one.onmicrosoft.com

Display Name → vip

Home > Groups | Overview > Users > Groups | Overview > New Group > Groups | All groups > VIP_Group | Roles and administrators > Users >

Create new user

Create a new internal user in your organization

Basics Properties Assignments Review + create

Create a new user in your organization. This user will have a user name like alice@contoso.com. [Learn more](#)

Identity

User principal name * vip @ diegolabversa.onmicos... [Domain not listed? Learn more](#)

Mail nickname * vip ☒ Derive from user principal name

Display name * vip

Password * ☒ Auto-generate password

Account enabled ☒

[Review + create](#)

[< Previous](#)

[Next: Properties >](#)

[Give feedback](#)

In the **Properties** tab, add first name, last name, and user type (Example, **Member**).

Other fields such as job title or department are optional but can be filled for organizational use.

Home > Groups | Overview > Users > Groups | Overview > New Group > Groups | All groups > VIP_Group | Roles and administrators > Users >

Create new user

Create a new internal user in your organization

Basics **Properties** Assignments Review + create

Identity

First name VIP1

Last name VIP1

User type Member

Authorization info [+ Edit Certificate user IDs](#)

Job Information

Job title

Company name

Department

Employee ID

Employee type

Employee hire date

Office location

[Review + create](#)

[< Previous](#)

[Next: Assignments >](#)

[Give feedback](#)

In the **Assignments** tab, click **Add Group**.

- Select the previously created **VIP_Group** (or any other relevant group).

This ensures the user inherits group-based claims when authenticating via SAML.

[Home](#) > [Groups | Overview](#) > [Users](#) > [Groups | Overview](#) > [New Group](#) > [Groups | All groups](#) > [VIP_Group | Roles and administrators](#) > [Users](#) >

Create new user

Create a new internal user in your organization

[Basics](#)
[Properties](#)
[Assignments](#)
[Review + create](#)

Make up to 20 group or role assignments. You can only add a user to a maximum of 1 administrative unit.

[+ Add administrative unit](#)
[+ Add group](#)
[+ Add role](#)

No assignments to display.

[Review + create](#)
[< Previous](#)
[Next: Review + create >](#)
[Give feedback](#)






Select group

Try changing or adding filters if you don't see what you're looking for.

Search


5 results found

All Groups

	Name	Type	Details
<input type="checkbox"/>	 All Company	Group	allcompany@diegolabversa.onmicrosoft.com
	 All Users	Group	Dynamic groups are not allowed.
<input type="checkbox"/>	 Diego Test Lab	Group	DiegoTestLab@diegolabversa.onmicrosoft.com
<input type="checkbox"/>	 Group for Answers in Viva Engag...	Group	groupforanswersinvivaengagedonotdelete162
<input checked="" type="checkbox"/>	 VIP_Group	Group	

Selected (1)

Reset

 VIP_Group

Select

- Still under **Assignments**, click **Add Role**.
 - From the directory roles list, assign security-related roles as required. For example:
 - **Security Reader** – allows read access to security reports.
 - **Security Administrator** – manages security configuration.
 - Roles are optional for SAML authentication itself but useful if role claims are mapped into SAML tokens for authorization in downstream apps.

Home > Groups | Overview > Users > Groups | Overview > New Group

Create new user

Create a new internal user in your organization

Basics Properties **Assignments** Review + create

Make up to 20 group or role assignments. You can only add a user to a maximum of 20 groups or roles.

+ Add administrative unit + Add group **+ Add role**

Type	Name
Group	VIP_Group

Directory roles

Choose admin roles that you want to assign to this user. [Learn more](#)

securi

Role	Description
<input type="checkbox"/> Attribute Assignment Administrator	Assign custom security attribute keys and values to supported Microsoft Entra objects.
<input type="checkbox"/> Attribute Assignment Reader	Read custom security attribute keys and values for supported Microsoft Entra objects.
<input type="checkbox"/> Attribute Definition Administrator	Define and manage the definition of custom security attributes.
<input type="checkbox"/> Attribute Definition Reader	Read the definition of custom security attributes.
<input type="checkbox"/> Attribute Log Administrator	Read audit logs and configure diagnostic settings for events related to custom security attributes.
<input type="checkbox"/> Attribute Log Reader	Read audit logs related to custom security attributes.
<input type="checkbox"/> Attribute Provisioning Administrator	Read and edit the provisioning configuration of all active custom security attributes for an application.
<input type="checkbox"/> Attribute Provisioning Reader	Read the provisioning configuration of all active custom security attributes for an application.
<input type="checkbox"/> Cloud App Security Administrator	Can manage all aspects of the Cloud App Security product.
<input type="checkbox"/> Global Secure Access Log Reader	Provides designated security personnel with read-only access to network traffic logs in Microsoft Entra Internet Access and Microsoft Entra Private Access for detailed analysis.
<input type="checkbox"/> Message Center Privacy Reader	Can read security messages and updates in Office 365 Message Center only.
<input checked="" type="checkbox"/> Security Administrator	Can read security information and reports, and manage configuration in Microsoft Entra ID and Office 365.
<input type="checkbox"/> Security Operator	Creates and manages security events.
<input type="checkbox"/> Security Reader	Can read security information and reports in Microsoft Entra ID and Microsoft

Select

Review + create < Previous Next: Review + create

Review & Create

Confirm the user configuration in the **Review + create** tab.

Assigning Groups to the SAML Application in Entra ID

Once the group and users are created, the final step is to assign them to the SAML application so they can authenticate.

1. Navigate to the **Enterprise Apps** (Example., ACME-ONE-SAML) > **Users and groups**.

Microsoft Entra admin center

Search resources, services, and docs (G+/I)

diegochaves@diegolab... DIEGO TEST LAB (DIEGOLABVER...)

Home Agents Favorites

Entra ID

Overview

Users

Groups

Enterprise apps

App registrations

Roles & admins

Delegated admin partners

Domain services

Conditional Access

Multifactor authentication

ACME-ONE-SAML | Overview

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Custom security attributes

Security

Conditional Access

Permissions

Properties

Name ACME-ONE-SAML

Application ID 45e6c18b-692d-41d2-8f61-...

Object ID 576b6311-9a56-4d32-8011-...

Getting Started

1. Assign users and groups

Provide specific users and groups access to the applications

[Assign users and groups](#)

2. Set up single sign on

Enable users to sign into their application using their Microsoft Entra credentials

[Get started](#)

3. Provision User Accounts

Automatically create and delete user accounts in the application

4. Conditional Access

Secure access to this application with a customizable access policy.

- Click **Add user/group**, search for the group (Example, VIP_Group), select it, and assign it to the application.

... > Users > Enterprise applications | All applications > ACME-ONE-SAML | Users and groups > Enterprise applications | All applications > ACME-ONE-SAML

ACME-ONE-SAML | Users and groups ...

Enterprise Application

Overview
Deployment Plan
Diagnose and solve problems

Manage
Properties
Owners
Roles and administrators
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service
Custom security attributes

Security
Conditional Access
Permissions

+ Add user/group Edit assignment Remove assignment Update credential Refresh Manage view ...

The application will appear for assigned users within My Apps. Set "visible to users?" to no in properties to prevent this.

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the [application registration](#)

First 200 shown, search all users & groups

Display name	Object type
No application assignments found	

- Confirm the assignment, and the group will appear under the application's **Users and groups** tab.

... > ACME-ONE-SAML | Users and groups > Enterprise applications | All applications > ACME-ONE-SAML | Users and groups >

Add Assignment ...

Diego Test Lab

Users and groups

None Selected

Select a role

User

Users and groups

Try changing or adding filters if you don't see what you're looking for.

Search

9 results found

All Users Groups

	Name	Type	Details
<input type="checkbox"/>	Diego Test Lab	Group	DiegoTestLab@diegolabversa.onmicrosoft.com
<input type="checkbox"/>	vip	User	vip@diegolabversa.onmicrosoft.com
<input type="checkbox"/>	Group for Answers in Viva Engage...	Group	groupforanswersinivaengagedonotdelete1
<input type="checkbox"/>	VIP	User	vip1@diegolabversa.onmicrosoft.com
<input type="checkbox"/>	VIP_Group	Group	

Selected (0)
Reset
No items selected

Select

Then click **Assign**, This ensures all members of the assigned group inherit SAML access to the application without needing individual assignments.

... > ACME-ONE-SAML | Users and groups > Enterprise applications | All applications > ACME-ONE-SAML | Users and groups >

Add Assignment

Diego Test Lab

⚠ When you assign a group to an application, only users directly in the group will have access. The assignment does not cascade to nested groups.

Users and groups
1 group selected.

Select a role
User

Assign

Concerto configuration for ENTRA-ID SAML Authentication Profiles

Navigate to User and Device Authentication Profiles

Go to:

Configure > Security Service Edge > Users and Device Authentication > Profiles then "+ Add"

VERSA | ACME-ONE | CONFIGURATION

America/Bogota | English | Administrator Service Provider Administrator

Configure > Security Service Edge > Users and Device Authentication > Profiles

User and Device Authentication Profile

Publish(1)

User and Device Authentication Profiles (1)

+ Add Delete Refresh Reference Select Columns

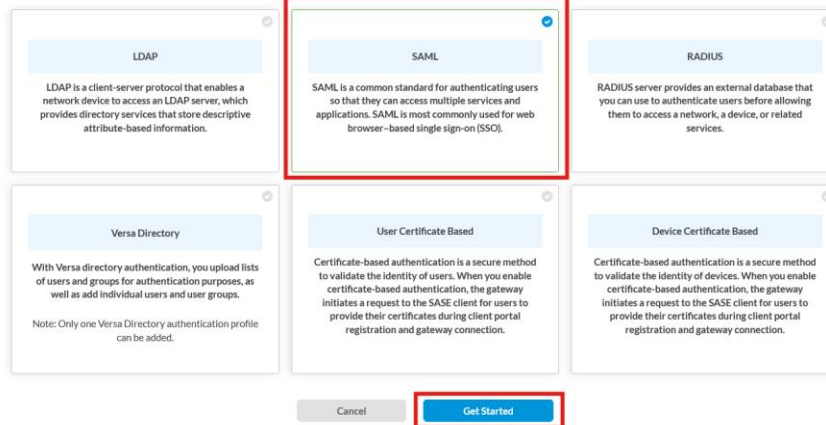
Name	Type	Description	Tags	Last Modified
AD_Server_Acme_One	LDAP			7/28/2025, 4:54:47 PM Administrator

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

Select **SAML**, Click Get Started

Add User and Device Authentication Profile

Select which user / device authentication profile you would like to configure.



The dialog shows six authentication profile options:

- LDAP**: LDAP is a client-server protocol that enables a network device to access an LDAP server, which provides directory services that store descriptive attribute-based information.
- SAML** (Selected): SAML is a common standard for authenticating users so that they can access multiple services and applications. SAML is most commonly used for web browser-based single sign-on (SSO).
- RADIUS**: RADIUS server provides an external database that you can use to authenticate users before allowing them to access a network, a device, or related services.
- Versa Directory**: With Versa directory authentication, you upload lists of users and groups for authentication purposes, as well as add individual users and user groups. Note: Only one Versa Directory authentication profile can be added.
- User Certificate Based**: Certificate-based authentication is a secure method to validate the identity of users. 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.
- Device Certificate Based**: Certificate-based authentication is a secure method to validate the identity of devices. 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.

Buttons: Cancel, Get Started

Select **ENTRA-ID**

To configure the settings, use the information collected in **Step 8** from the Microsoft ENTRA ID. Go to Entra ID > Enterprise apps > All applications > *ACME-ONE-SAML* > Single sign-on (SAML).

From this page, copy/download the values required :

- Certificate (Base64) – Download.
- Login URL – Copy.
- Microsoft Entra Identifier (Entity ID) – Copy.
- Logout URL – Copy.

Home > App registrations > Enterprise applications | All applications > ACME-ONE-SAML >

ACME-ONE-SAML | SAML-based Sign-on

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Custom security attributes

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-in logs

Upload metadata file

Change single sign-on mode

Test this application

Got feedback?

3

SAML Certificates

Token signing certificate

Status

Active

Edit

Thumbprint

0382CE5329AACF016A20F1C7419EBF0E150D786

Expiration

9/4/2028, 10:34:51 AM

Notification Email

diegochaves@diegolabversa.onmicrosoft.com

App Federation Metadata Url

https://login.microsoftonline.com/a08ab2d2-a5df-...

Certificate (Base64)

Download

Certificate (Raw)

Download

Federation Metadata XML

Download

Verification certificates (optional)

Required

No

Edit

Active

0

Expired

0

4

Set up ACME-ONE-SAML

You'll need to configure the application to link with Microsoft Entra ID.

Login URL

https://login.microsoftonline.com/a08ab2d2-a5df-...

Microsoft Entra Identifier

https://sts.windows.net/a08ab2d2-a5df-481b-9ffa-...

Logout URL

https://login.microsoftonline.com/a08ab2d2-a5df-...

Single Sign-on URL, Service Provider Entity ID and Identity Provider Entity ID are mandatory fields to be configured and you must upload certificate issued by Microsoft Entra ID.

Add SAML Authentication Profile

1

2

3

Settings

Users And User Groups

Review & Submit

Select SAML Type

Okta

Ping Identity

Office 365

Microsoft Entra ID

Google IAM

Cisco Duo

Other

Single Sign-on URL *

Service Provider Entity ID *

Identity Provider Entity ID *

Prefix ID

Group Attribute

Reply URL (Assertion Consumer Reply URL)

https://acme-one-samlgwdiego-labversanow.net/versa-flexvnt/saml/login-consumer

Single Sign-out URL

Service Provider Certificate

Identity Provider Certificate *

Cache Expiry Time (mins)

Concurrent Logins

Cancel

Skip to Review

Next

Complete the parameters using the values from the Microsoft Entra id

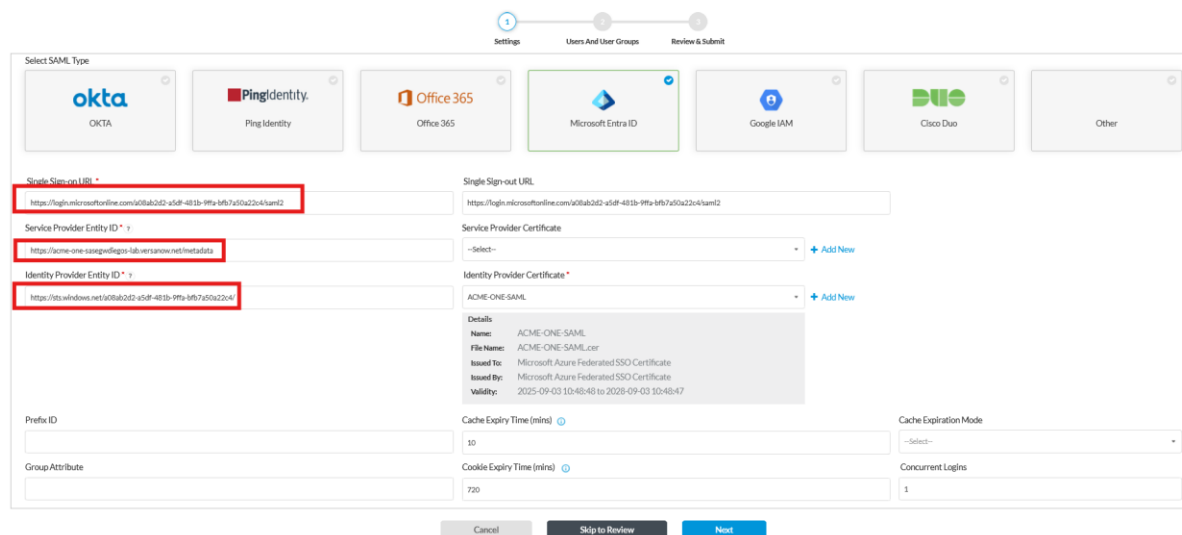
Example:

Single Sign-on URL: <https://login.microsoftonline.com/a08ab2d2-a5df-481b-9ffa-bfb7a50a22c4/saml2>

Service Provider Entity ID: <https://acme-one-sasegwldiegos-lab.versanow.net/metadata>

Identity Provider Issuer: <https://sts.windows.net/a08ab2d2-a5df-481b-9ffa-bfb7a50a22c4/>

Edit SAML Authentication Profile: ENTRA-ID-SAML



1 2 3
Settings Users And User Groups Review & Submit

Select SAML Type

Single Sign-on URL *

Service Provider Entity ID *

Identity Provider Entity ID *

Prefix ID

Group Attribute

Single Sign-out URL

Service Provider Certificate

Identity Provider Certificate *

Details

Name: ACME-ONE-SAML

File Name: ACME-ONE-SAML.cer

Issued To: Microsoft Azure Federated SSO Certificate

Issued By: Microsoft Azure Federated SSO Certificate

Validity: 2025-09-03 10:48:48 to 2028-09-03 10:48:47

Cache Expiry Time (mins)

Cache Expiration Mode

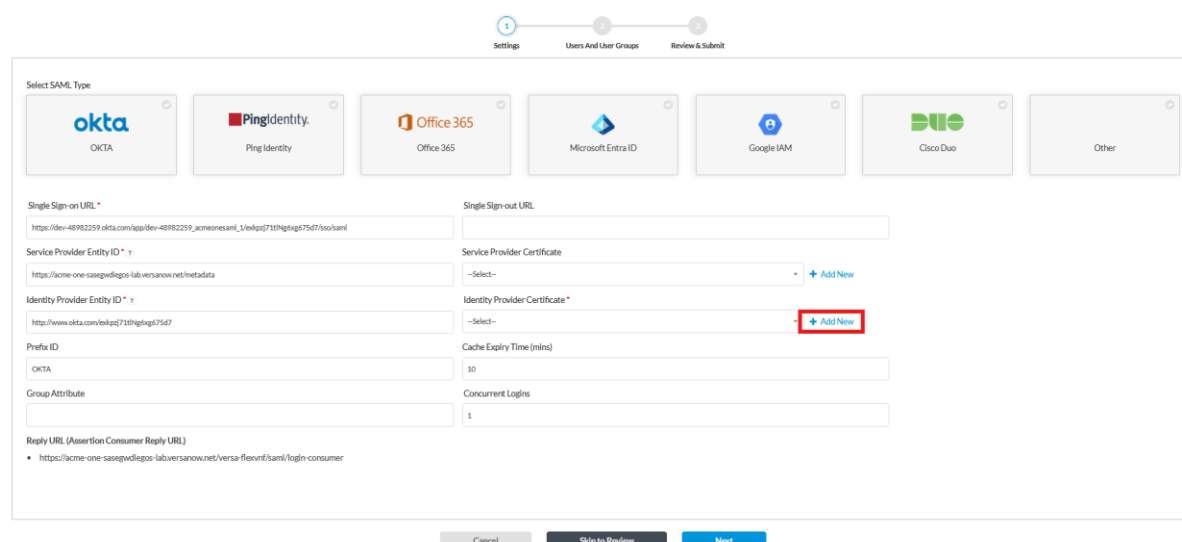
Cookie Expiry Time (mins)

Concurrent Logins

Cancel Skip to Review Next

Then Upload the **Identity Provider Certificate** by clicking on the Add New button.

Add SAML Authentication Profile



1 2 3
Settings Users And User Groups Review & Submit

Select SAML Type

Single Sign-on URL *

Service Provider Entity ID *

Identity Provider Entity ID *

Prefix ID

Group Attribute

Single Sign-out URL

Service Provider Certificate

Identity Provider Certificate *

Cache Expiry Time (mins)

Cache Expiration Mode

Cookie Expiry Time (mins)

Concurrent Logins

Reply URL (Assertion Consumer Reply URL)

• <https://acme-one-sasegwldiegos-lab.versanow.net/versa-flexv/saml/login-consumer>

Cancel Skip to Review Next

On the **Users and User Groups** page, you can add individual users or entire groups. Click **User Groups** and add the **VIP1_Group** created in the Okta app. Click **Add**, then click **Next** to continue.

The screenshot shows the 'Edit SAML Authentication Profile: ENTRA-ID-SAML' interface. At the top, there are three steps: 'Settings', 'Users and User Groups' (active), and 'Review & Submit'. Below the steps, there's a 'Group List' button highlighted with a red box. A modal window titled 'Add User Group' is open, showing a 'Name' field with 'VIP_Group' and a 'Description' field. The 'Add' button at the bottom right of the modal is highlighted with a red box. The background shows a table with columns for 'Name' and 'Description'.

On the **Review & Submit** page, enter a **Name** and **Description** for the profile, then review all configuration details including general information, SAML settings, and assigned users or groups. Once confirmed, click **Save** to complete the profile creation.

The screenshot shows the 'Add SAML Authentication Profile' interface. At the top, there are three steps: 'Settings', 'Users and User Groups', and 'Review & Submit' (active). Below the steps, there's a 'Review your configurations. Before submitting, review and edit any steps of your configuration below.' section. The 'General' section has 'Name' as 'ACHIE_SAML_ACHIE_One' and 'Description' as an empty field. The 'Settings' section shows SAML configuration details like 'SAML Type' (OKTA), 'Single Sign-on URL', 'Service Provider Entity ID', 'Identity Provider Entity ID', 'Identity Provider Certificate', 'Prefix ID', 'Cache Expiry Time (mins)', 'Concurrent Logins', 'Group Attribute', and 'Reply URL (Assertion Consumer Reply URL)'. The 'Users & User Groups' section shows 'Users' as 'No users' and 'User Groups' as 'Engineering-Group'. The 'Save' button at the bottom right is highlighted.

After creating and Publishin the Authentication Profile, you must apply them to the Secure Access Client policy to enforce authentication and apply the corresponding security policies.

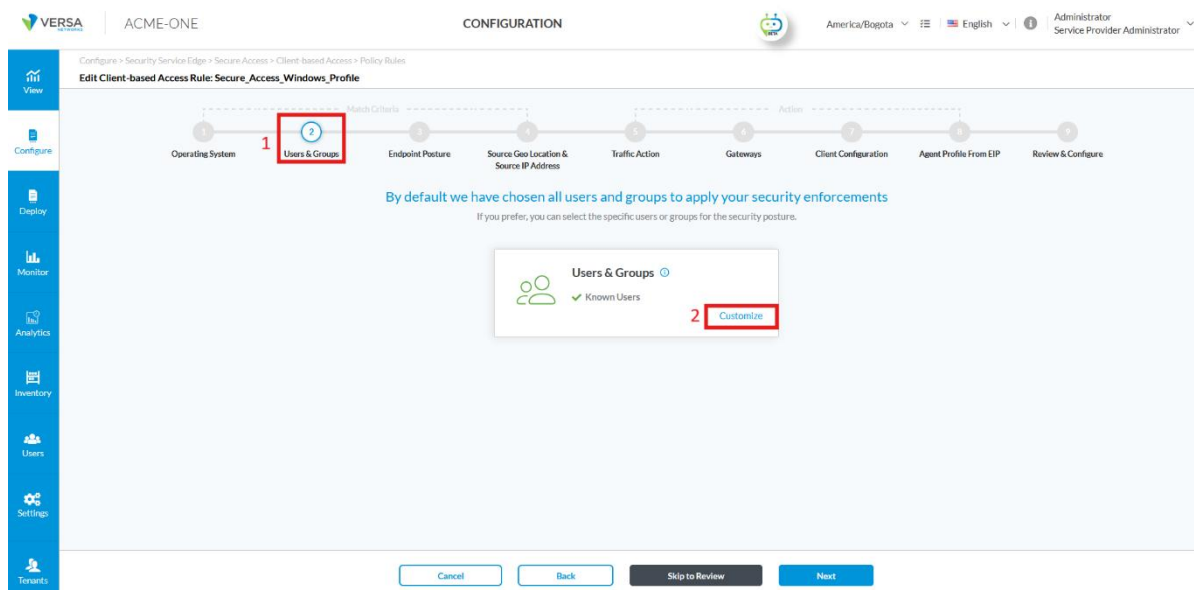
Navigate

to:

Configure > Security Service Edge > Secure Access > Client-based Access > Rules.

Click “+ **Add**” to create a new Secure Access Client rule or edit an existing rule.

In the **Match Criteria** configuration, navigate to the **Users & Groups** section. Under the **Users & Groups** panel, click on **Customize** to begin specifying user-based access rules using the authentication profile you previously created.



In the **Users & Groups** customization panel, select **Selected Users** as the user type. Then, under **Enable Rule for the following matched users or user groups**, choose the appropriate authentication profile (Example., ENTRA-ID-SAML). This allows the policy to enforce access control based on Active Directory user group membership.

Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules

Edit Client-based Access Rule: Secure_Access_Windows_Profile

By default we have chosen all users and groups to apply your security enforcements
If you prefer, you can select the specific users or groups for the security posture.

← Back

Users & Groups

User Type ☒ Selected Users ☐ Known Users

Enable Rule for the following matched users or user groups

2

User Groups Users

Search for Users

User Name	First Name	Last Name
<input checked="" type="checkbox"/> vip1@diglobalversa.onmicrosoft.com	VIP1	VIP

Cancel Back Skip to Review Next

In this step, you can choose to add specific **users** or **groups** to enforce security policies. Use the **User Groups** or **Users** tabs to select the desired entries.

Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules

Edit Client-based Access Rule: Secure_Access_Windows_Profile

By default we have chosen all users and groups to apply your security enforcements
If you prefer, you can select the specific users or groups for the security posture.

← Back

Users & Groups

User Type ☒ Selected Users ☐ Known Users

Enable Rule for the following matched users or user groups

User Groups Users

Search for Users

User Name	First Name	Last Name
<input checked="" type="checkbox"/> vip1@diglobalversa.onmicrosoft.com	VIP1	VIP

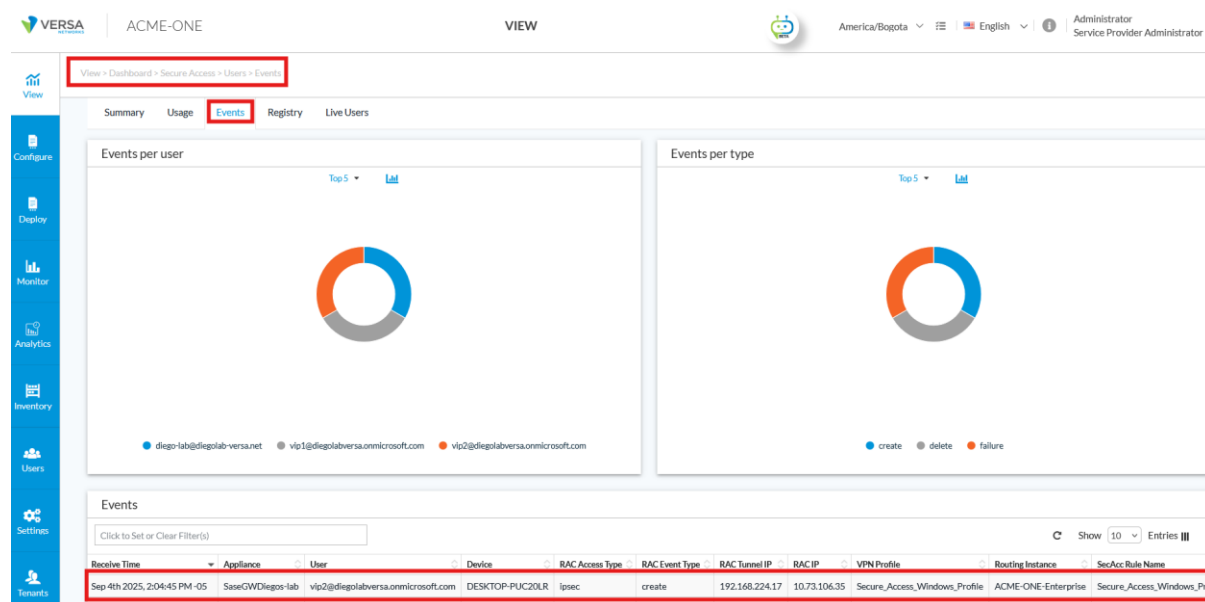
Cancel Back Skip to Review Next

After reviewing all configuration sections, click **Save** to apply the settings to the current Secure Access Profile. Then go to the **Publish** section at the top-right corner of the screen and click **Publish**.

Verification

When a user connects to the Gateway and SAML is enabled, the Gateway redirects the login to the configured IdP (Example., Okta or Entra ID). After the user completes credentials/MFA, the IdP returns a **signed SAML assertion** to the Gateway. The Gateway validates the signature and audience, extracts the **NameID** and any mapped attributes (email,

groups/roles), and—if successful—establishes the session and applies the matching Secure Access policy. Authentication events can be verified in Concerto under **View > Dashboard > Secure Access > Users > Event**, where successful and failed attempts are logged with details such as username, tunnel IP, and applied profile.



You would see the method used and the authenticated user in the Authentication Logs under **View > Dashboard > Secure Access > Logs > Authentication > Events**.

Authentication events										
Click to Set or Clear Filter(s)										
Receive Time	Appliance	Auth Profile	Method	Status	Status Message	Time Taken	User	Source Address	Destination Address	Source Port
Sep 4th 2025, 2:04:18 PM -05	SaseGWDiegolab	Default-Auth-Profile	ENTRA-ID-SAML	success	VSA : SAML : Authenticated successfully.	0ms	vip2@diegolab-versa.onmicrosoft.com	10.73.106.35	10.73.106.18	59925
Sep 4th 2025, 1:38:17 PM -05	SaseGWDiegolab	Default-Auth-Profile	AD_Server_Acme_One	success	VSA : LDAP : Authenticated successfully.	138ms	diego-lab@diegolab-versa.net	10.73.106.36	10.73.106.18	62080

Additionally, administrators can confirm active sessions and mapped users via CLI commands on SaseGateway typing command **show orgs org-services <ORG-NAME> user-identification live-users list brief**.

```
admin@SaseGWDiego-lab-cli> show orgs org-services ACME-ONE user-identification live-users list
-----^
syntax error: incomplete path
[error][2025-09-04 12:11:46]
admin@SaseGWDiego-lab-cli> show orgs org-services ACME-ONE user-identification live-users list brief
-----^
IP ADDRESS      NAME                                     STATUS  SESSION  TIME  EXPIRATION
                vip2@diegolabversa.onmicrosoft.com  Live    17        60    inactivity
-----^
[ok][2025-09-04 12:11:50]
admin@SaseGWDiego-lab-cli>
```

Versa Directory

Versa Directory is a Versa-hosted IDP service based on LDAP, available for Versa-hosted SSE Services. The prerequisite to use this service for you tenant is that enabled on Headend at infrasture level by Versa or MSP(if using thirdparty hosted headend): [https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_User_and_Device_Authentication#Configure_Versa_Directory_Authentication_Using_an_IAM_Server](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_User_and_Device_Authentication#Configure_Versa_Directory_Authentication_Using_an_IAM_Server)

Now to use Versa Directory and create users refer the following document: [https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/002_Versa_SSE_Quick_Start_Guide#Step_3:_Configure_User_Authentication](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/002_Versa_SSE_Quick_Start_Guide#Step_3:_Configure_User_Authentication)

Device Certificate Authentication

Device certificate-based authentication strengthens enterprise security by validating not just user credentials but also the identity of endpoint devices before granting access to corporate networks and applications. Unlike traditional password-based mechanisms, this method leverages digital certificates issued by a trusted Certificate Authority (CA). During authentication, the device must present a valid certificate that is signed by the trusted CA and has not expired or been revoked. This ensures a strong CA trust relationship, guaranteeing that only devices with properly issued and trusted certificates are allowed to connect.

Common Use Cases

1. **Corporate Laptops in BYOD Environments:** Even in bring-your-own-device scenarios, only corporate-issued laptops with valid certificates can establish VPN tunnels, enforcing Zero Trust by validating both the user and the device.
2. **Regulated Industries (Banking, Healthcare, Government):** Compliance frameworks like PCI-DSS, HIPAA, and GDPR mandate strong access controls. Device certificates provide tamper-resistant proof of device identity, safeguarding sensitive systems against unauthorised access.
3. **Remote Workforces with Layered Authentication:** Users log in via SAML (e.g., Okta, Azure AD), while their devices authenticate using certificates. This layered approach ensures stolen credentials alone cannot grant access from untrusted devices.
4. **Pre-Logon VPN for Domain Services:** Certificates enable VPN connectivity before user login on Windows/macOS, allowing Group Policies, scripts, and security updates from Active Directory to be applied seamlessly at login.

Configuration Workflow

1. Step to Generate Device Certificate:

If you are using a self-signed certificate, follow the official guide in the documentation. You can find the detailed procedure under the section *"Generate the CA Key, CA Certificate, and Device Certificate"* in the following link:

[https://docs.versa-networks.com/Security Service Edge \(SSE\)/Configuration from Concerto/Configure Certificate-Based Device Authentication for Secure Access](https://docs.versa-networks.com/Security Service Edge (SSE)/Configuration from Concerto/Configure Certificate-Based Device Authentication for Secure Access)

If you are using an enterprise Certificate you would follow the next guide:

To validate possible link with Sudhir

2. **Upload the CA Chain:** Import the root and intermediate CA certificates that will be used to validate client device certificates.
3. **Configure Identity Mapping:** Select the username identifying field from the certificate (e.g., CN, UPN, or SAN).
4. **Enable Validation:** Optionally enable OSCP (Online Certificate Status Protocol) checks for real-time certificate revocation verification and select the source VR for the query.
5. **Pre-Logon Stage:** Toggle the option to enable device certificate-based authentication during pre-logon if required.

6. **Multi-Factor Support:** When combining device certificate authentication with user-based authentication methods (e.g., SAML, LDAP), define the order of authentication to align with security policies.
7. **Finalize:** Assign a profile name and save the configuration.

Ensure the Root CA is uploaded to Gateways from Concerto and reflected correctly in the Device:
 Navigate to Certificates Go to: Configure > Security Service Edge > Settings > Certificates then "+ Add"

The screenshot shows the VERSA configuration interface. On the left sidebar, the 'Configure' menu is expanded, and 'Settings' is selected. Under 'Settings', 'Certificates' is highlighted. The main content area shows the 'Certificates' page with a table of existing certificates. The table has columns: File, Type, Issued To, Issued By, Valid, Expires, and Actions. There are three certificates listed. An '+ Add' button is visible in the top right of the table area.

In Add Certificate/CA-Chain/Private Key, select the Certificate Type you need:

- CA Chain, or Cert/Key bundle, or Private Key.

Add Certificate/CA-Chain/Private Key

Certificate Type ☒ Cert/Key bundle ☐ CA Chain ☐ Private Key

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

Certificate Name *

CA-Chain Name *

 + Add

Pass-Phrase

Upload File

Cancel

Add

As an Example, Add a **CA Chain**

CA-Chain Name: enter the name (Example, device-auth-ca-chain).

- Click **Upload File** and select the CA chain file.
- Click **Add**.

Add Certificate/CA-Chain/Private Key

Certificate Type ☐ Cert/Key bundle ☒ CAChain ☐ Private Key

Allowed file formats are .crt, .cer or .pem

CA-Chain Name *

device-auth-ca-chain

Upload File

device-auth-ca-chain.crt

Cancel Add

Now check CA Chain (device-auth-ca-chain) is successfully uploaded and listed under Configure > Security Service Edge > Settings > Certificates :

ACME-ONE
CONFIGURATION
America/Bogota
English
Administrator
Service Provider Administrator

View
Configure
Deploy
Monitor
Analytics
Inventory
Users
Settings

Configure > Security Service Edge > Settings > Certificates

Certificates

Below are all the Certificates

Name	File	Type	Issued To	Issued By	Valid	Expires	Actions
ACME-ONE	ACME-ONE.zip	CA Certificate	VOS Certificate	Versa Concerto Certificate Authority	From: 7/22/2025, 9:51:35 AM To: 7/21/2030, 9:51:35 AM	1825 days	
ACME-ONE	concerto_ca_chain.pem	CA-Chain	Versa Concerto Certificate Authority	Versa Networks Root Certificate Authority	From: 11/19/2021, 6:49:31 AM To: 9/28/2031, 7:49:31 AM	3600 days	
device-auth-ca-chain	device-auth-ca-chain.crt	CA-Chain	RAS-CA	RAS-CA	From: 5/21/2025, 8:43:12 AM To: 5/19/2035, 8:43:12 AM	3650 days	
OKTA-ACME	OKTA-ACME.crt	CA-Chain	dev-48982259	dev-48982259	From: 8/8/2025, 12:23:19 PM To: 8/8/2035, 12:24:18 PM	3652 days	
PrivateKey							

Navigate to User and Device Authentication Configuration

Go to:

Configure > Security Service Edge > User and Device Authentication > Profiles then "+ Add"

Select **Device Certificate Based** as Authentication Method then Click **Get Started**

Add User and Device Authentication Profile

Select which user / device authentication profile you would like to configure.

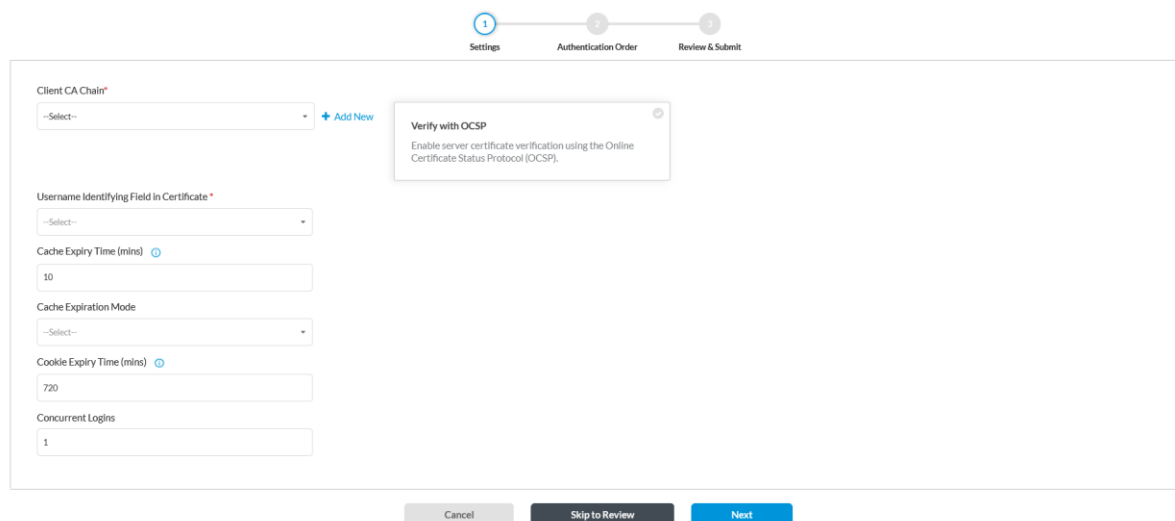
In Add Device Certificate Authentication Profile > Settings:

- **Client CA Chain** > Select the certificate you uploaded (Example device-auth-ca-chain.crt).
- Username Identifying Field in Certificate > choose the correct option (Example Subject common-name).
- Cache Expiry Time (mins) > 10, (Default Value).
- Cookie Expiry Time (mins) > 720, (Default Value).

- Concurrent Logins > 1.
- Leave **Verify with OCSP** disabled (optional unless required).

Then Click **Next** to continue

Add Device Certificate Authentication Profile



Settings Authentication Order Review & Submit

Client CA Chain*
--Select-- + Add New

Username Identifying Field in Certificate*
--Select--

Cache Expiry Time (mins) ⓘ
10

Cache Expiration Mode
--Select--

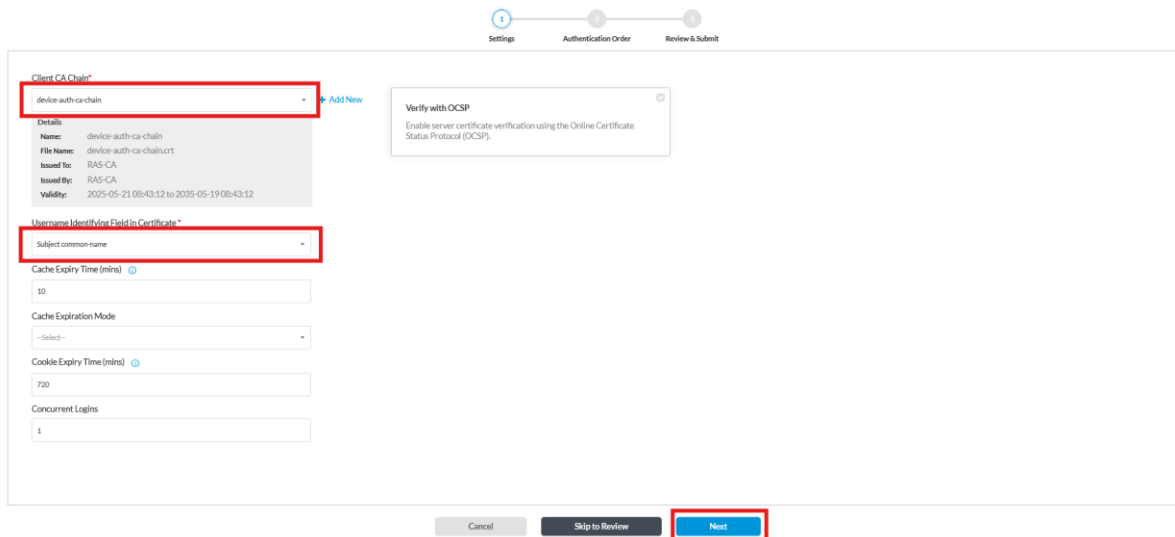
Cookie Expiry Time (mins) ⓘ
720

Concurrent Logins
1

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

Cancel Skip to Review Next

Add Device Certificate Authentication Profile



Settings Authentication Order Review & Submit

Client CA Chain*
device-auth-ca-chain + Add New

Details
Name: device-auth-ca-chain
File Name: device-auth-ca-chain.crt
Issued To: RAS-CA
Issued By: RAS-CA
Validity: 2025-05-21 08:43:12 to 2035-05-19 08:43:12

Username Identifying Field in Certificate*
Subject common name

Cache Expiry Time (mins) ⓘ
10

Cache Expiration Mode
--Select--

Cookie Expiry Time (mins) ⓘ
720

Concurrent Logins
1

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

Cancel Skip to Review Next

In Authentication Order, you can optionally enable Pre-login devices to authenticate before user login. If you do not need this feature, leave it as **Disabled**.

Enable Device Authentication.

In the authentication order selection, you will see two options: Device Authentication or User Authentication. Choose Device Authentication to ensure the device authenticates first.

Add Device Certificate Authentication Profile



Prelogon Device Authentication

Enable prelogon Device Authentication to login in prelogon using device certificate authentication.

☐ Prelogon Disabled

Device Authentication

Enable Device Authentication to authenticate in Postlogon with MFA using device certificate authentication and user credentials.

☐ Device Authentication Disabled

Cancel
Back
Skip to Review
Next

Add Device Certificate Authentication Profile



Prelogon Device Authentication

Enable prelogon Device Authentication to login in prelogon using device certificate authentication.

☐ Prelogon Disabled

Device Authentication

Enable Device Authentication to authenticate in Postlogon with MFA using device certificate authentication and user credentials.

☒ Device Authentication Enabled

Select which profile would you like to authenticate first?

☒ Device Authentication ☐ User Authentication

Cancel
Back
Skip to Review
Next

Then Click **Next** to continue

In the Review & Submit page:

Confirm the Client CA Chain = device-auth-ca-chain.

Confirm Username Identifying Field = subject.

Verify Authentication Order = **Device**.

Click **Save** then **Publish**.

Add Device Certificate Authentication Profile

Settings Authentication Order Review & Submit

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

General

Name: Description:

Tags:

Settings [Edit](#)

Client CA Chain	device-auth-ca-chain
Username Identifying Field in Certificate	subject
Verify with OCSP	Disabled
Is CA Server on Internet?	
VPN Name	ACME-ONE-Enterprise
Cache Expiry Time (mins)	30
Cache Expiration Mode	
Concurrent Logins	1
Cookie Expiry Time (mins)	720

Authentication Order [Edit](#)

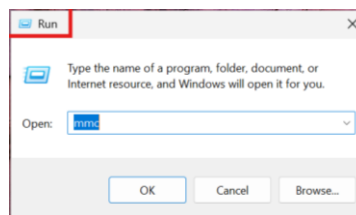
Prelogin	Disabled
Profile to authenticate first	Device

Cancel Back Save

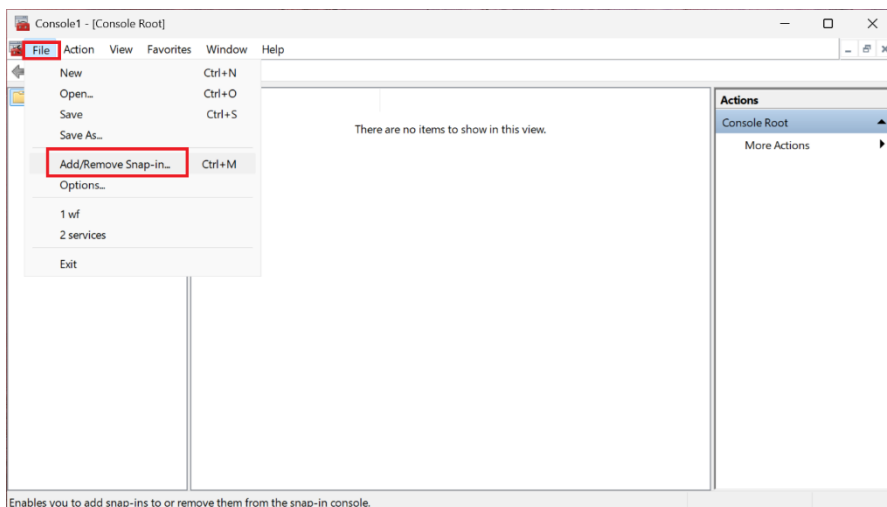
Installing Certificates on the Client Device:

Download the certificate file onto the client machine (for example, the .pfx file signed by the same CA authority used for the CA chain upload in the previous section)

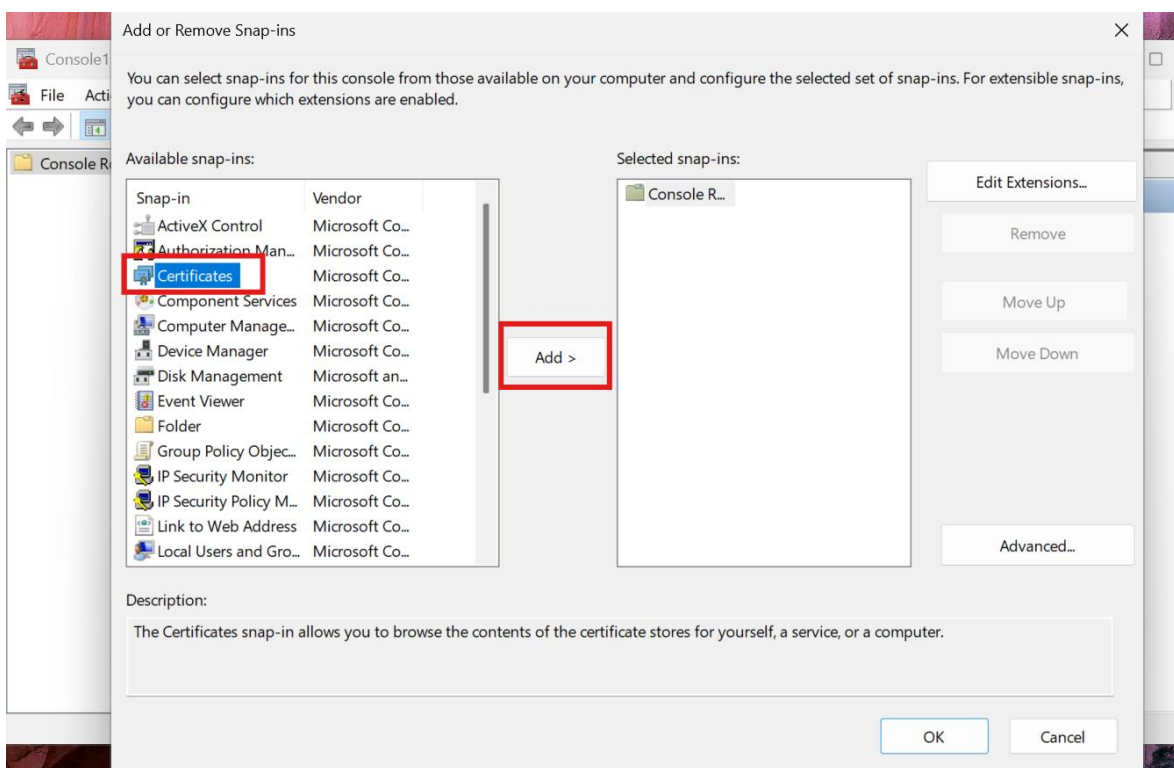
For Windows open the Run dialog, type mmc, and press Enter.

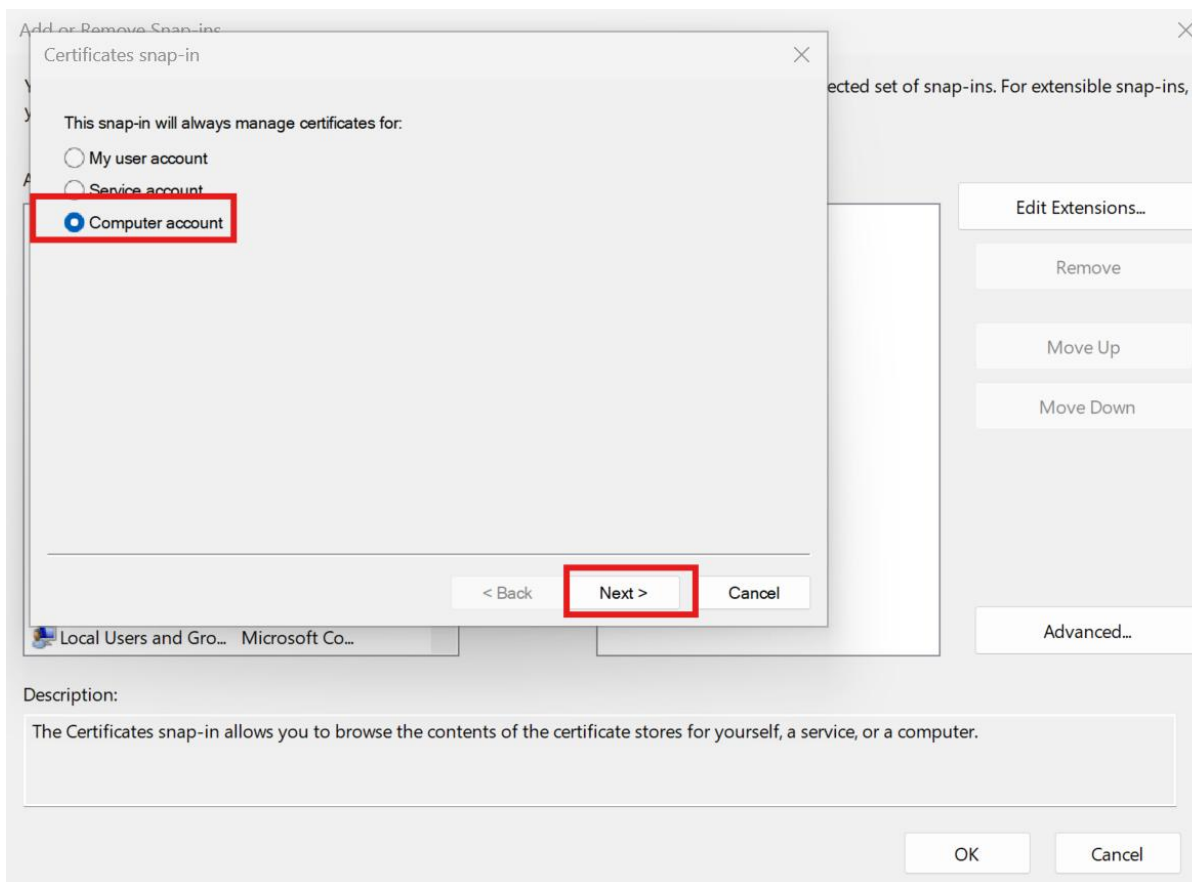


In the MMC console, go to File → Add/Remove Snap-in.

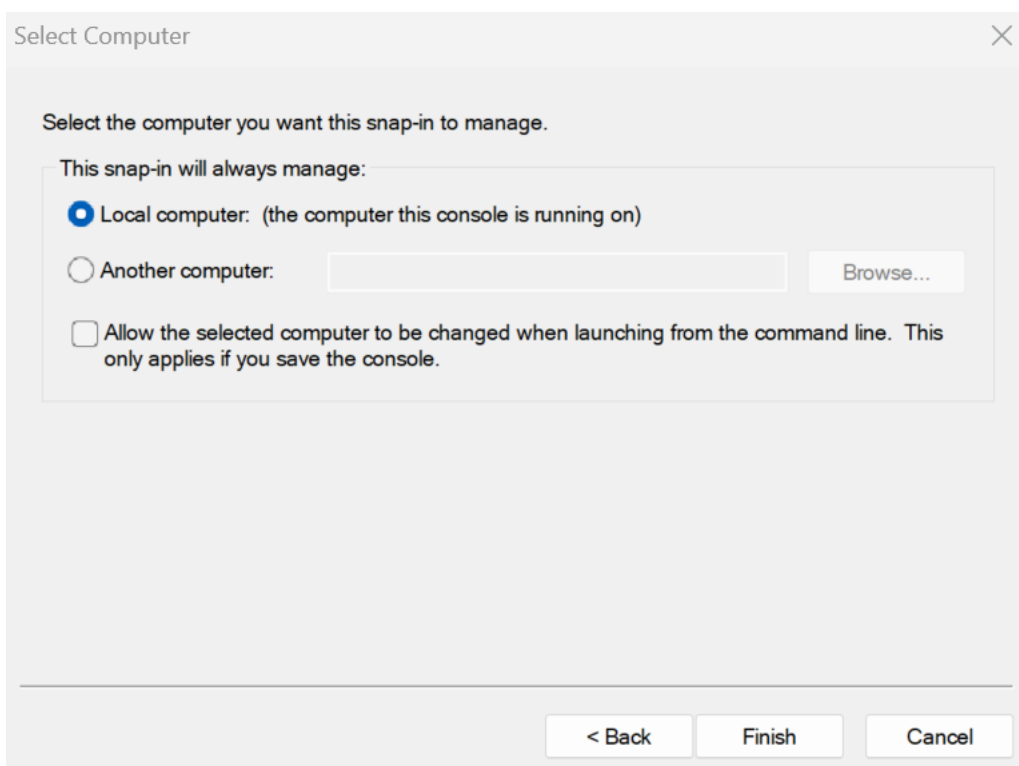


Select Certificates, click Add, and choose Computer Account to manage device-level certificates.

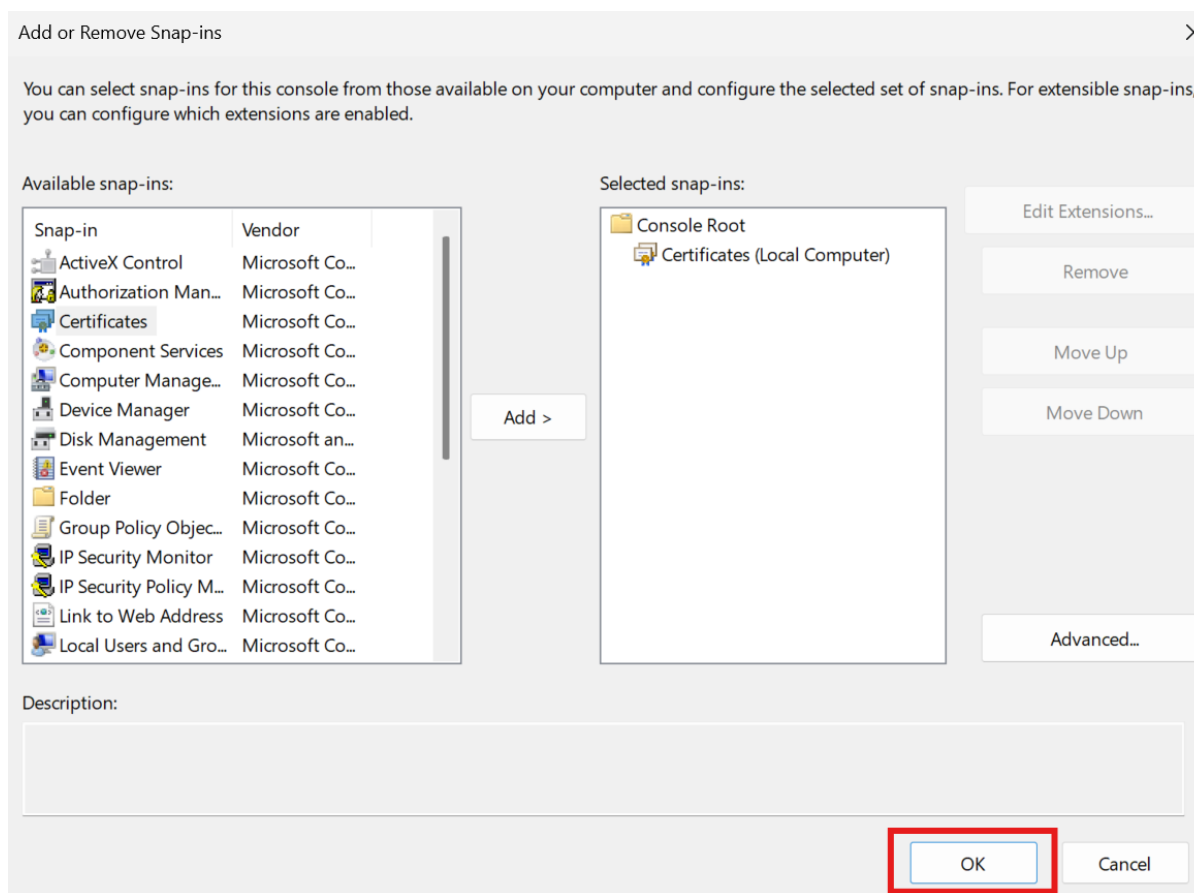




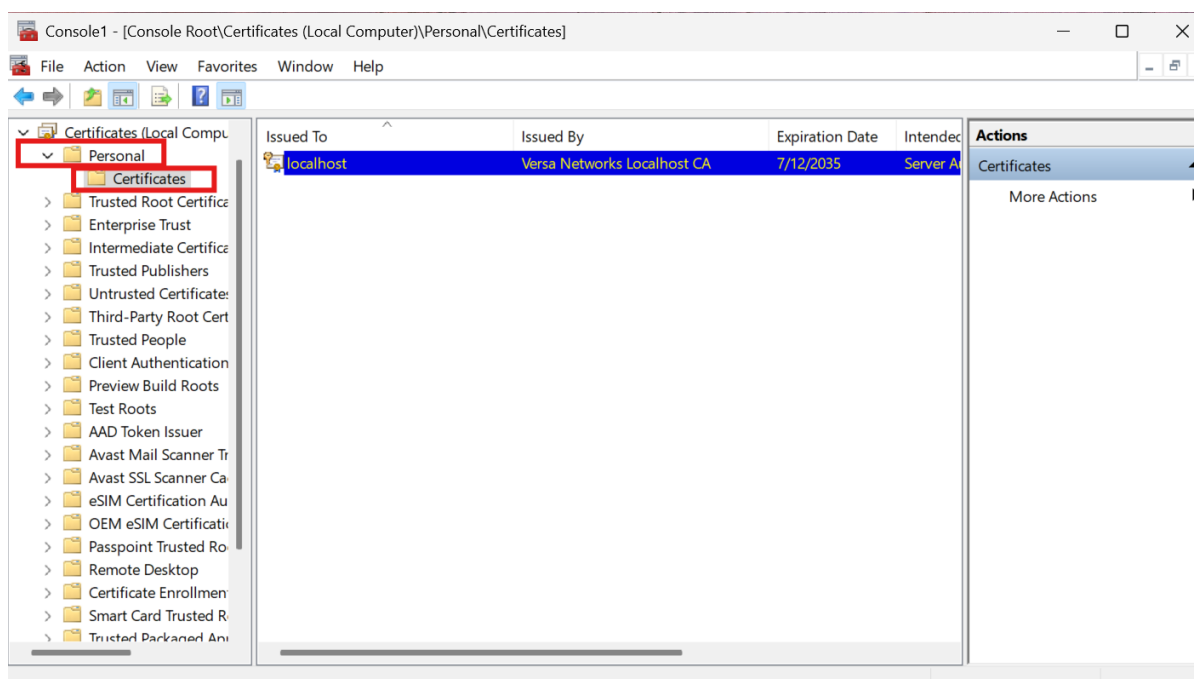
Choose Local Computer and Finish.



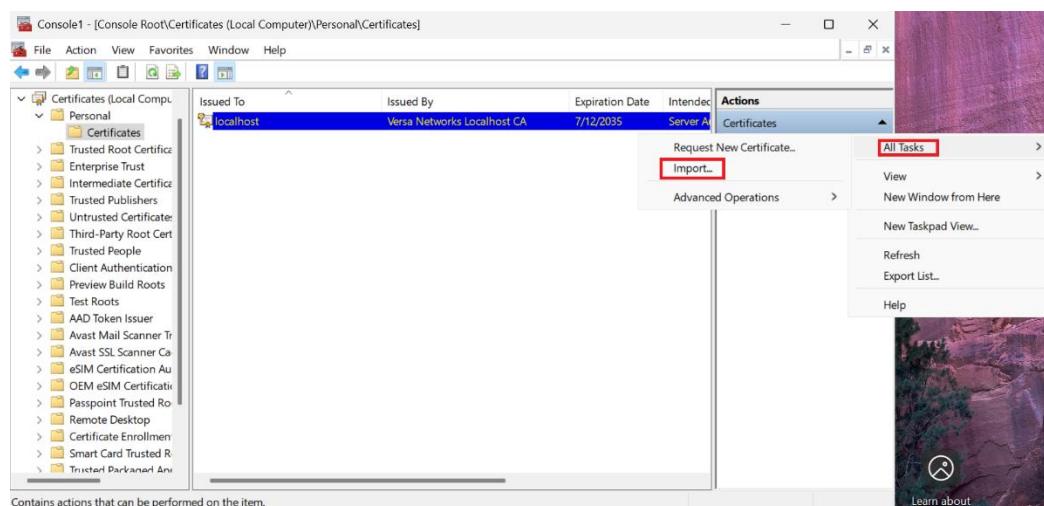
Then OK.



Right-click on the **Certificates** folder under **Personal**.



go to More Actions then **All Tasks > Import**.



The **Certificate Import Wizard** will open. Ensure **Local Machine** is selected as the store location, then click **Next**.



←  Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

- ☐ Current User
- ☒ Local Machine


To continue, click Next.

Next

Cancel

Browse to the location of the certificate file (for example user1-cert.pfx), select it, and click **Open**

×

←  Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:


Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)
 Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
 Microsoft Serialized Certificate Store (.SST)

Enter the certificate's private key password.

- Optionally, you may check **Mark this key as exportable** if you want to re-use it later.
 - Ensure Include all extended properties is checked.
- Click Next.

×

←  Certificate Import Wizard

Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

.....

☐ Display Password

Import options:

☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☐ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☐ Protect private key using virtualized-based security(Non-exportable)

☒ Include all extended properties.

Next
Cancel

On the **Certificate Store** screen, select **Place all certificates in the following store**, ensure it is set to **Personal**, and click **Next**.



←  Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

☐ Automatically select the certificate store based on the type of certificate

☒ Place all certificates in the following store

Certificate store:

Personal

Browse...

Next

Cancel

Click **Finish** to complete the import. A confirmation message should appear:
"The import was successful."



←  Certificate Import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

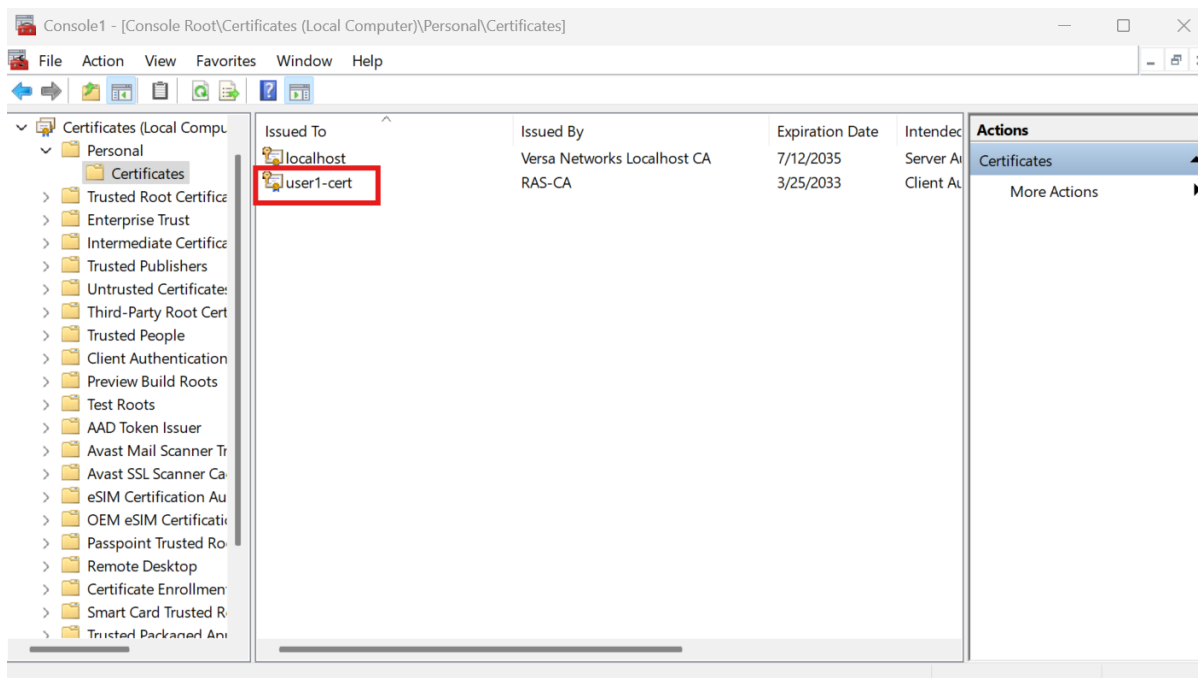
You have specified the following settings:

Certificate Store Selected by User	Personal
Content	PFX
File Name	C:\Users\admin\Desktop\user1-cert.pfx

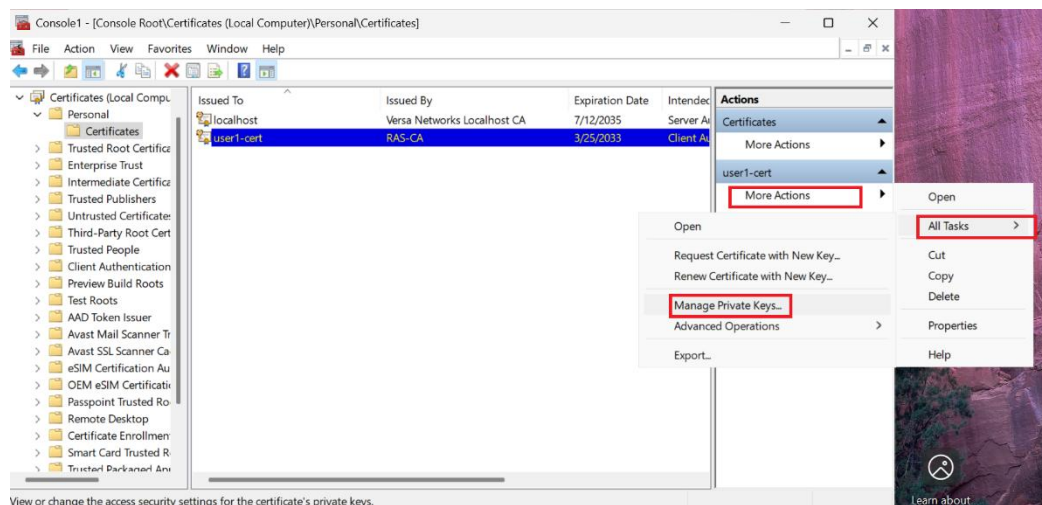
Finish

Cancel

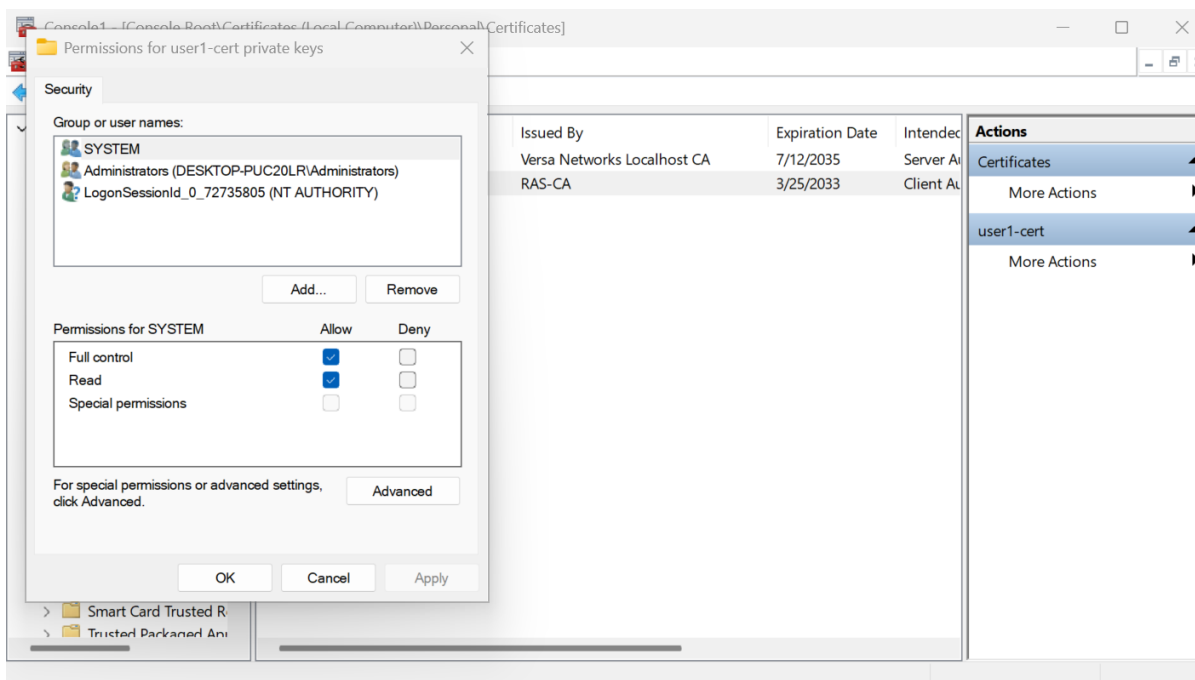
Verify that the imported certificate is visible under:
Certificates (Local Computer) > Personal > Certificates.



Next, ensure the user has access to the private keys assigned at the device level. Click on the particular device **certificate** > **More Actions** > **All Tasks** > **Manage Private Keys**.



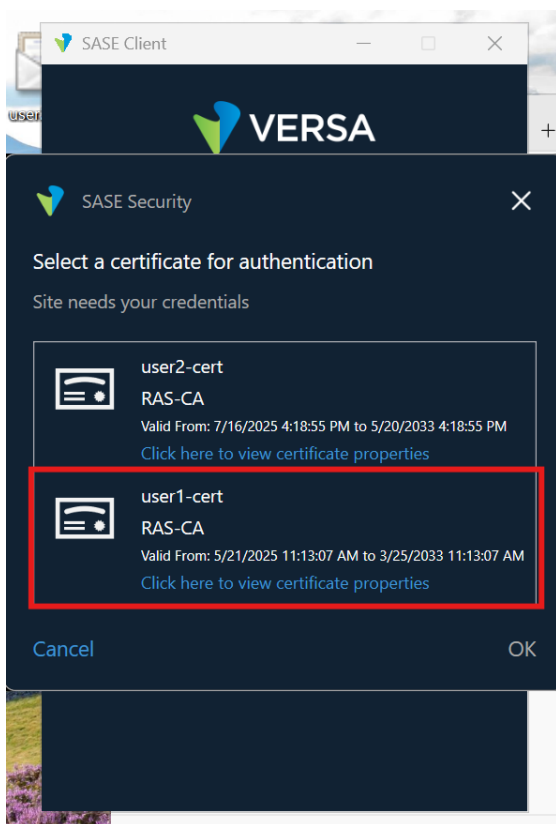
Assign permissions for users.



Verification

When a user connects to the Gateway and the Device Certificate Authentication profile is enabled, the authentication order is processed as Device first, followed by User (SSO/LDAP). The user would be prompted with a certificate selection pop-up to choose the correct device certificate. On subsequent connections, the same certificate would be auto-selected **as long as no other device certificate is installed on the endpoint**; if another device certificate is present, the client would prompt for selection again.

If the certificate validation succeeds, the connection proceeds to the next stage where the user is authenticated through SAML/SSO (or LDAP, depending on configuration), This ensures that both the device and the user identity are verified before access is granted.



User Certificate

User Certificate Authentication enhances enterprise security by validating the identity of individual users through digital certificates issued by a trusted Certificate Authority (CA). Unlike device certificates, which identify and authenticate endpoint hardware, user certificates are bound to a specific user identity and installed within their personal profile.

Client certificate authentication from end devices relies on digital certificates to authenticate both users and systems before granting access to the gateway, in addition to existing SAML or LDAP authentication mechanisms. In user certificate authentication, the focus is on verifying individual users across the same device, using a unique certificate configured within each user's profile. This method is particularly valuable in shared-device environments, as it prevents user spoofing by ensuring that the Common Name (CN) in the certificate matches the username defined in LDAP or SAML.

During authentication, the system validates that the presented certificate is signed by a trusted CA, has not expired or been revoked, and that its CN or Subject Alternative Name (SAN) aligns with the username provided during login. This process provides a secure, certificate-driven layer of identity verification that complements existing SSO and directory-based authentication mechanisms.

Common Use Cases

1. **Shared Workstations or Multi-User Systems:**

In environments where multiple users share the same endpoint (for example, kiosks, customer-service terminals, or lab systems), user certificates ensure that each session is authenticated to the correct individual.

The system verifies that the Common Name (CN) in the certificate matches the username provided in SAML or LDAP, preventing user spoofing and enforcing accountability for every login.

2. **Regulated Industries (Banking, Healthcare, Government):**

Compliance frameworks like PCI-DSS, HIPAA, and GDPR mandate strong access controls. User certificates provide identity-bound proof of authentication, ensuring that each login is cryptographically linked to a verified individual, reducing the risk of credential misuse or impersonation.

3. **Remote Workforces with Layered Authentication:**

Users authenticate through SAML (e.g., Okta, Azure AD), while their certificates validate their personal identity at the gateway. This layered approach enforces Zero Trust principles by ensuring that both the user credentials and the associated certificate match before access is granted.

4. **Dual Validation with Device Certificates:**

User and device certificates can be combined for layered authentication. The device certificate confirms the integrity and trust level of the hardware, while the user certificate validates the person operating it. This two-tier validation ensures that both the endpoint and the user meet the organization's access control requirements.

The steps to configure are like the device certificate (Refer to the section before this one). We also have the option to use the LDAP/SAML profile in conjunction with user certificate authentication.

Navigate to User and Device Authentication Configuration

Go to:

Configure > Security Service Edge > User and Device Authentication > Profiles then "+ Add"

The screenshot shows the VERSA ONE configuration interface. The left sidebar has a 'Configure' button highlighted with a red circle. The main area displays the 'User and Device Authentication' configuration page. A table lists existing authentication profiles:

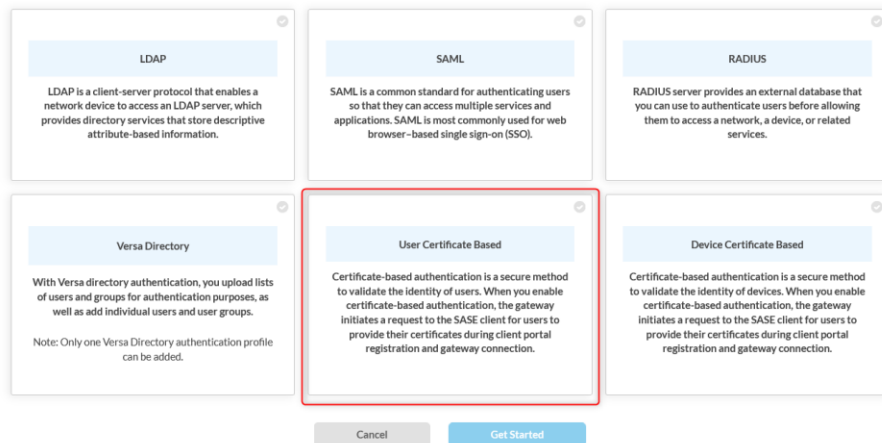
Type	Description	Tags	Last Modified
LDAP			8/28/2025, 10:24:08 AM Administrator
User Certificate			9/13/2025, 11:54:01 AM Administrator
SAML			9/4/2025, 20:18 PM Administrator
SAML			8/8/2025, 4:51:03 PM Administrator

A red circle highlights the '+ Add' button in the top right of the table. Another red circle highlights the 'Profiles' option in the left sidebar under 'User and Device Authentication'.

Select **User Certificate Based** as Authentication Method then Click **Get Started**

Add User and Device Authentication Profile

Select which user / device authentication profile you would like to configure.



The dialog displays five authentication profile options:

- LDAP**: LDAP is a client-server protocol that enables a network device to access an LDAP server, which provides directory services that store descriptive attribute-based information.
- SAML**: SAML is a common standard for authenticating users so that they can access multiple services and applications. SAML is most commonly used for web browser-based single sign-on (SSO).
- RADIUS**: RADIUS server provides an external database that you can use to authenticate users before allowing them to access a network, a device, or related services.
- Versa Directory**: With Versa directory authentication, you upload lists of users and groups for authentication purposes, as well as add individual users and user groups. Note: Only one Versa Directory authentication profile can be added.
- User Certificate Based**: Certificate-based authentication is a secure method to validate the identity of users. 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. (This option is highlighted with a red border in the image).
- Device Certificate Based**: Certificate-based authentication is a secure method to validate the identity of devices. 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.

Buttons at the bottom: Cancel, Get Started

In Add User Certificate Authentication Profile > Settings:

- **Client CA Chain** > Select the certificate you uploaded (Example ROOT-ACME-ONE.crt).
- Username Identifying Field in Certificate > choose the correct option (Example Subject common-name).
- Cache Expiry Time (mins) > 10, (Default Value).
- Cookie Expiry Time (mins) > 720, (Default Value).
- Concurrent Logins > 1.
- Leave **Verify with OCSP** disabled (optional unless required).

Then Click **Next** to continue

Add User Certificate Authentication Profile

✕

1 2 3 4
 Settings Additional Authentication Method Users Review & Submit

Client CA Chain*

--Select--

+ Add New

Username Identifying Field in Certificate *

Subject common-name

Cache Expiry Time (mins) ⓘ

10

Cache Expiration Mode

--Select--

Cookie Expiry Time (mins) ⓘ

720

Concurrent Logins

1

Verify with OCSP ✓

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

Cancel

Skip to Review

Next

Add User Certificate Authentication Profile

✕

1 2 3 4
 Settings Additional Authentication Method Users Review & Submit

Client CA Chain*

ROOT-ACME-ONE

+ Add New

Details

Name: ROOT-ACME-ONE

File Name: root-acme-one.pem

Issued To: root-acme-one-cert

Issued By: root-acme-one-cert

Validity: 2025-09-12 08:32:18 to 2035-09-10 08:32:18

Username Identifying Field in Certificate *

Subject common-name

Cache Expiry Time (mins) ⓘ

10

Cache Expiration Mode

--Select--

Cookie Expiry Time (mins) ⓘ

720

Concurrent Logins

1

Verify with OCSP ✓

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

Cancel

Skip to Review

Next

In **Additional Authentication Method**, you can enable **Multi-factor Authentication**. If left **Disabled**, only the user certificate is used for authentication.

When **Multi-factor Authentication** is enabled, you can select an additional method such as **LDAP** or **SAML**, and the associated profile will be displayed.

Then, under Select which profile would you like to authenticate first? You can choose either the LDAP Profile or the User Certificate Based Profile.

Add User Certificate Authentication Profile



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

☐ Multi-factor Authentication Disabled

Add User Certificate Authentication Profile



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

☒ Multi-factor Authentication Enabled

Below are your available options:

☒ LDAP ☐ SAML

LDAP Profile available: AD_Server_Acme_One

Select which profile would you like to authenticate first?

☐ LDAP Profile ☒ User Certificate Based Profile

Then click **Next** to continue.

In the **Users** step, you have the option to upload or manually add user entries. This is not mandatory and is only required if you explicitly want to match certificates to specific users.

- You can upload a user list in CSV format using the fields: **UserName**, **First Name**, and **Last Name**.
- Alternatively, you can manually add a user by providing the same details.

If no users are added, the authentication profile will still work without explicit user-to-certificate mapping.

Then Click **Next** to continue

In the **Review & Submit** page: you can provide a **Name** and an optional **Description** for the profile. Use these fields to clearly identify the purpose of the configuration.

Confirm the Client CA Chain = device-auth-ca-chain.

Confirm Username Identifying Field = subject.

Verify Additional Authentication Method.

Click **Save** then **Publish**.

Add User Certificate Authentication Profile

Settings Additional Authentication Method Users Review & Submit

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

General

Name: User_Certificate Description:

Tags:

Settings [Edit](#)

Client CA Chain	ROOT-ACME-ONE
Username Identifying Field in Certificate	subject
Verify with OCSP	Disabled
Is CA Server on Internet?	
VPN Name	ACME-ONE-Enterprise
Cache Expiry Time (mins)	10
Cache Expiration Mode	
Concurrent Logins	1
Cookie Expiry Time (mins)	720

Additional Authentication Method [Edit](#)

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

Cancel Back **Save**

Add Device Certificate Authentication Profile

Settings Authentication Order Review & Submit

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

General

Name: Device_Authentication Description:

Tags:

Settings [Edit](#)

Client CA Chain	device-auth-ca-chain
Username Identifying Field in Certificate	subject
Verify with OCSP	Disabled
Is CA Server on Internet?	
VPN Name	ACME-ONE-Enterprise
Cache Expiry Time (mins)	10
Cache Expiration Mode	
Concurrent Logins	1
Cookie Expiry Time (mins)	720

Authentication Order [Edit](#)

Prelogin	Disabled
Profile to authenticate first	Device

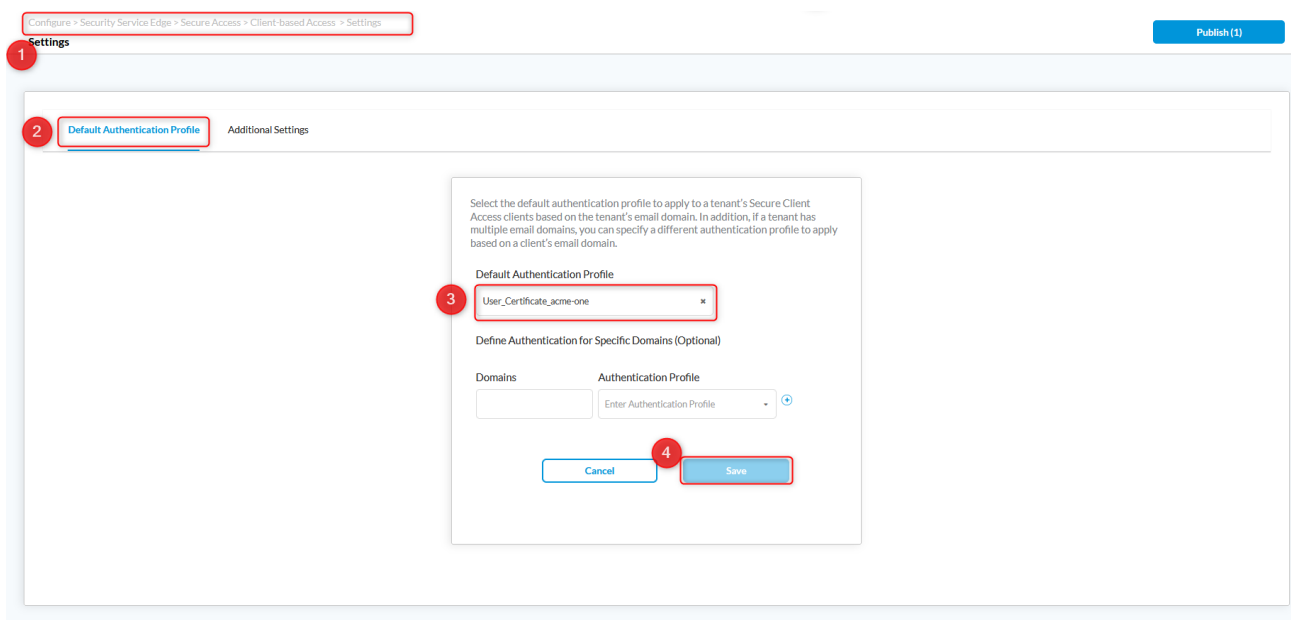
Cancel Back **Save**

Additional Requirements for Client Certificate Authentication

- Concerto generates a unique hostname for each SASE Gateway, which is referenced in the **cert-auth-profiles**.

```
admin@SaseGWDiegos-lab-cli(config)% show orgs org-services ACME-ONE user-identification cert-auth-profiles
User_Certificate_acme-one {
  server-hostname      acme-one-sasegwdiegos-lab-cert.versanow.net;
  server-addresses     [ 10.73.106.18 192.168.210.18 192.168.224.0 ];
  server-port          443;
  routing-instance     [ ACME-ONE-Enterprise Internet2-Transport-VR MPLS-Transport-VR ];
  client-ca-chain       ACME-ONE;
  server-certificate    SaseGWDiegos-lab.crt;
  username-field       subject;
}
[ok][2025-10-14 10:39:33]
```

- Ensure this hostname resolves correctly to the corresponding Gateway IP address from the end user's PC or endpoint.
- Verify that the same **End-Entity Certificate** used for client authentication is also configured on the server side under the **server-certificate** field to maintain a valid certificate trust relationship.
- Mandatory Requirement:** The *User Certificate Authentication Profile* cannot be mapped directly to a *Secure Access Rule*. It must be assigned as the **Default Authentication Profile** under **Configure > Security Service Edge > Secure Access > Client-based Access > Settings**, as illustrated below. This configuration ensures that user certificate validation is applied globally for all client-based access sessions.



Configure > Security Service Edge > Secure Access > Client-based Access > Settings

Settings Publish (1)

1

2 Default Authentication Profile Additional Settings

3 Select the default authentication profile to apply to a tenant's Secure Client Access clients based on the tenant's email domain. In addition, if a tenant has multiple email domains, you can specify a different authentication profile to apply based on a client's email domain.

Default Authentication Profile

User_Certificate_acme-one

Define Authentication for Specific Domains (Optional)

Domains Authentication Profile

Enter Authentication Profile

4 Cancel Save

Installing Certificates on the Client Device:

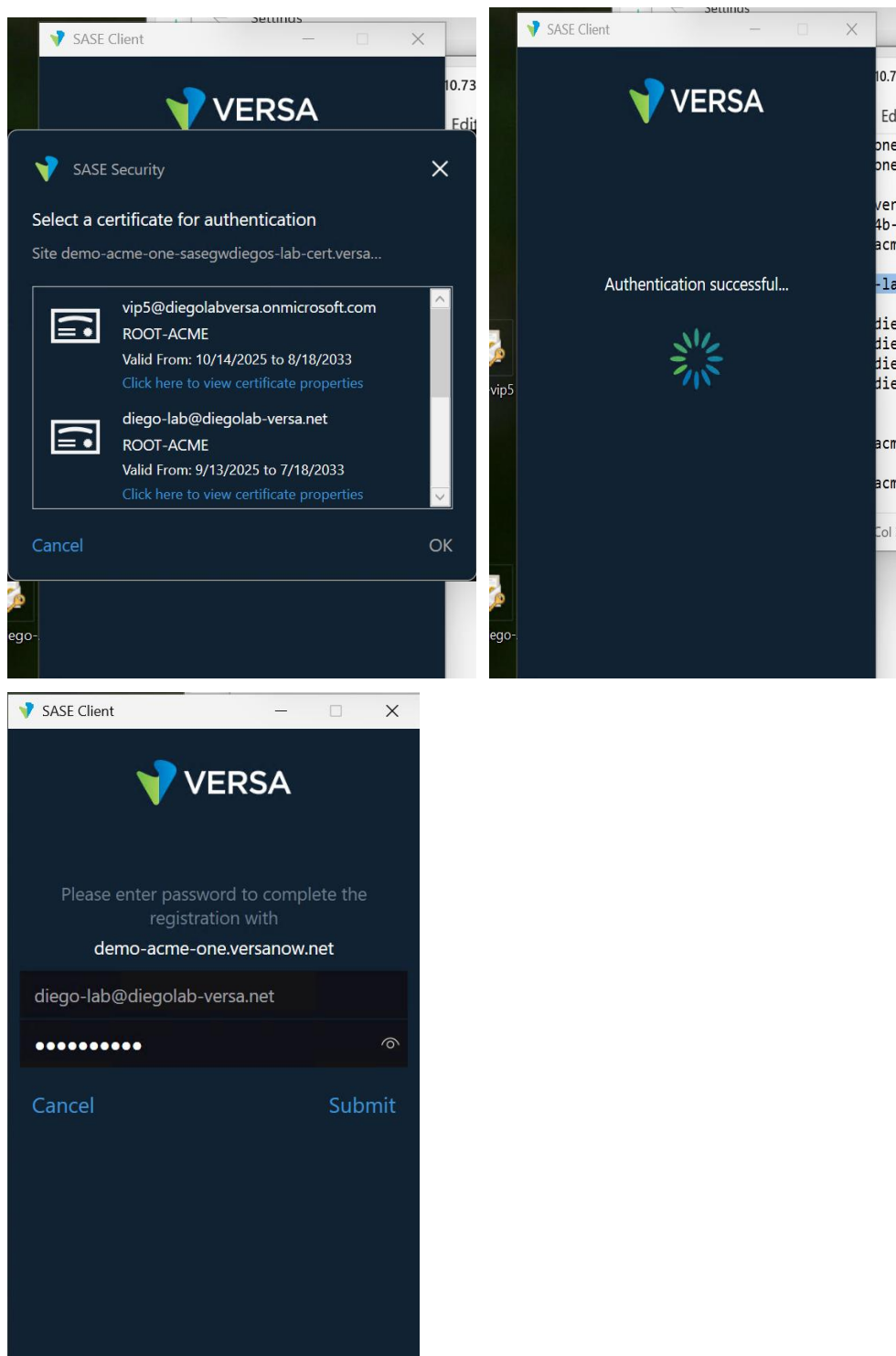
The installation process for user certificates on client devices follows the same procedure described in the **Device Certificate Authentication** section. The certificate must be imported into the appropriate certificate store on the client machine.

Verification

When a user connects to the Gateway and the **User Certificate Authentication** profile is enabled, the authentication process begins by validating the user's digital certificate before proceeding to directory-based authentication (SAML or LDAP). The client prompts the user with a certificate selection pop-up to choose the appropriate **user certificate** from their local certificate store.

During the first connection, the user must manually select the correct certificate corresponding to their identity. This selection prompt appears only when multiple certificates issued by the **same Certificate Authority (CA)** are present on the endpoint. In such cases, the user is required to choose the appropriate certificate that matches their user identity to ensure proper validation. For subsequent sessions, the same certificate is automatically selected as long as no new user certificates from the same CA are added to the device.

If the certificate validation is successful, the authentication continues to the next stage, where the user's credentials are verified through SAML/SSO or LDAP, depending on the configured profile. This sequence ensures that the user identity is validated cryptographically before directory authentication occurs, providing a layered and secure login process.



Appendix A: LDAP

How to Find Base DN and Bind DN in Active Directory for Versa Integration

Summary

When configuring Versa Security to integrate with Microsoft Active Directory (AD) using LDAP, you need to provide:

1. Base DN – the starting point in the AD hierarchy where searches begin.
2. Bind DN – the service account distinguished name (DN) Versa uses to query and authenticate against AD.

This article explains how to locate both values and provides ready-to-use examples.

Procedure

Step 1: Find the Base DN

The Base DN is derived from your AD domain.

1. Open Active Directory Users and Computers (ADUC).
2. Identify the domain name (e.g., versanetworks.com).
3. Convert the domain name into DN format:

DC=versanetworks,DC=com

Tip: The Base DN can be scoped to a specific OU if you want to restrict searches. Example:

OU=Engineering,DC=versanetworks,DC=com

Step 2: Find the Bind DN

The Bind DN corresponds to the account Versa will use for authentication and directory searches.

To retrieve it:

Command Line (dsquery):

dsquery user -name test1

Example output:

CN=test1,OU=OUtest2,OU=OUtest,DC=versanetworks,DC=com

Step 3: Understand CN vs OU

- CN (Container): Default AD containers, e.g. CN=Users.
- OU (Organizational Unit): Custom organizational units, e.g. OU=OUtest2.

Examples

Scenario	DN Example	Notes
Base DN – Domain Root	DC=versanetworks,DC=com	Search starts at the domain root.
Bind DN – Admin in Users container	CN=admin,CN=Users,DC=versanetworks,DC=com	Service account located in the built-in Users container.
Bind DN – User in nested OUs	CN=test1,OU=OUtest2,OU=OUtest,DC=versanetworks,DC=com	User object located in OUtest2, which is inside OUtest.

Quick Reference

Use the following commands and templates to retrieve and configure LDAP DN values quickly.

1. Find Base DN (Domain Root)

- Command (run on AD server):
`dsquery * domainroot -scope base`
- Output Example:
`DC=versanetworks,DC=com`
- Configure in Versa:
Base DN = `DC=versanetworks,DC=com`

2. Find a User's Bind DN

- Command (example for user test1):
`dsquery user -name test1`
- Output Example:
`CN=test1,OU=OUtest2,OU=OUtest,DC=versanetworks,DC=com`
- Configure in Versa:
Bind DN = `CN=test1,OU=OUtest2,OU=OUtest,DC=versanetworks,DC=com`

3. Find an Admin Account in Users Container

- Command (example for admin):
`dsquery user -name admin`
- Output Example:
`CN=admin,CN=Users,DC=versanetworks,DC=com`
- Configure in Versa:
Bind DN = `CN=admin,CN=Users,DC=versanetworks,DC=com`

4. Find OU-Specific Base DN

- Command (example for OU "Engineering"):
`dsquery ou -name Engineering`
- Output Example:
`OU=Engineering,DC=versanetworks,DC=com`
- Configure in Versa:
Base DN = `OU=Engineering,DC=versanetworks,DC=com`

About Versa

Versa, the global leader in SASE, enables organizations to create self-protecting networks that radically simplify and automate their network and security infrastructure. Powered by AI, the [VersaONE Universal SASE Platform](#) delivers converged SSE, SD-WAN, and SD-LAN solutions that protect data and defend against cyberthreats while delivering a superior digital experience. Thousands of customers globally, with hundreds of thousands of sites and millions of users, trust Versa with their mission critical networks and security. Versa is privately held and funded by investors such as Sequoia Capital, Mayfield, and BlackRock. For more information, visit <https://www.versa-networks.com> and follow Versa on [LinkedIn](#) and X (Twitter) [@versanetworks](#).