

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.

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

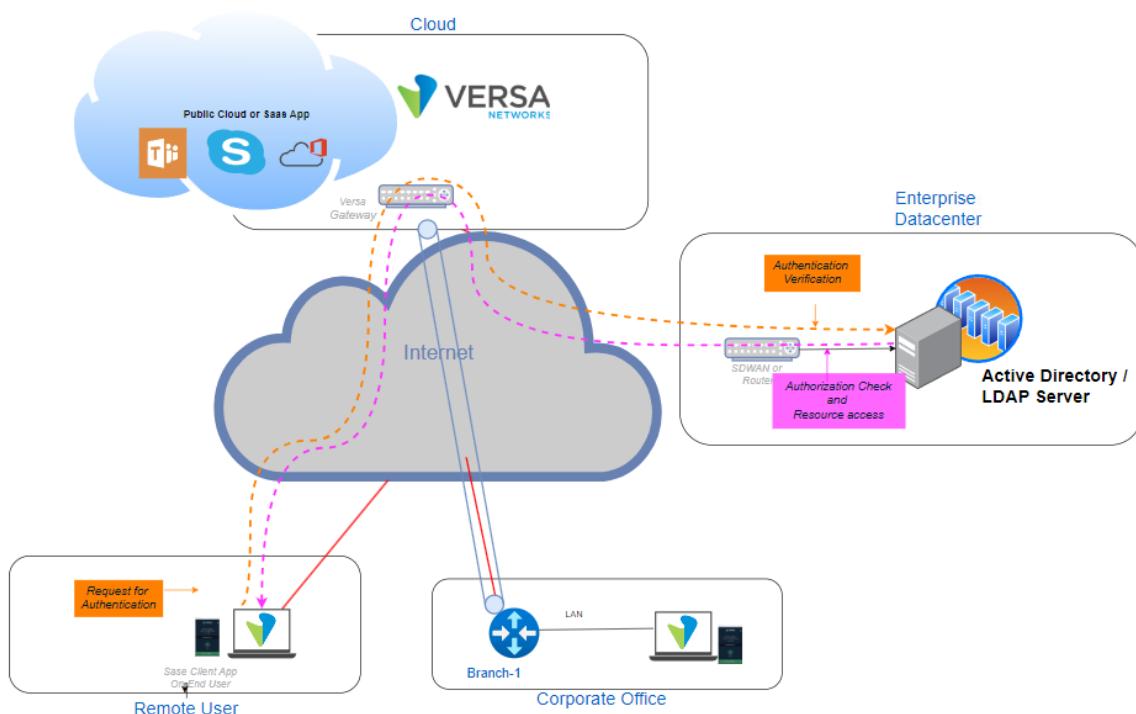
LDAP Active-Directory

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

Add User and Device Authentication Profile

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

| | | |
|--|---|---|
| LDAP | SAML | RADIUS |
| 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 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 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 | User Certificate Based | Device Certificate Based |
| 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. | 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. | 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**

From the Server Type dropdown, select Active Directory

Add LDAP Authentication Profile

The screenshot shows the 'Add LDAP Authentication Profile' wizard in progress. The 'Server Type' dropdown is set to 'Active Directory' and is highlighted with a red box. Other fields include 'FQDN' (radio button selected), 'IP Address', 'VPN Name' (ACME-ONE-Enterprise), 'Port' (389), 'Enable SSL' (checkbox checked), 'SSL Mode' (dropdown set to 'Select'), and 'CA Certificate' (dropdown set to 'Select'). Buttons at the bottom are 'Cancel', 'Skip to Review', and 'Next'.

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. | <p>cn=Administrator, cn=users, dc=versa,dc=com</p> <p>cn = Common Name</p> <p>dc = Domain Component</p> |
| 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

Server Type: Active Directory (1)

Select either FQDN or IP Address.*
 FQDN
 IP Address (2)
 10.163.106.33

+ Add Secondary Server

VPN Name* (3)
 ACME-ONE-Enterprise

Port*
 389

Enable SSL (4)

SSL Mode
 --Select--

CA Certificate
 --Select--

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

Bind DN* (1)
 cn=Administrator,cn=users,dc=acme-one,dc=com

Bind Password* (2)

Bind Timeout (sec) (3)
 30

Base DN* (4)
 cn=users,dc=acme-one,dc=com

Domain Name* (5)
 acme-one.com

Base Domain
 --Select--

Search Timeout (sec)
 30

Cache Expiry Time (mins)
 10

Concurrent Logins
 3

Cancel Skip to Review Next (red box)

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@versanetworks.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

Settings 2 User And Group Profile 3 Review & Submit

| | | |
|----------------------------|-------------------|------------------|
| Group Object Class * | Group Name * | Group Member * |
| group | name | memberOf |
| User Object Class * | User Name * | |
| user | userPrincipalName | |
| Refresh Interval (seconds) | Password Last Set | Password Max Age |
| 21600 | pwdLastSet | maxPwdAge |

Cancel Back Skip to Review **Next**

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

Settings 

| | |
|-------------------------|--|
| Server Type | active-directory |
| FQDN or IP Address | 10.163.106.33 |
| 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 (min) | 10 |
| Concurrent Logins | 3 |

Description

Cancel  Save

Then **Save**.

Add LDAP Authentication Profile

General

FQDN or IP Address: 10.163.106.33

Settings 

| | |
|-------------------------|--|
| FQDN or IP Address | 10.163.106.33 |
| 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 (min) | 10 |
| Concurrent Logins | 3 |

User and Group Profile 

| | |
|----------------------------|-------------------|
| Group Object Class | group |
| Group Name | name |
| Group Member | member |
| User Object Class | user |
| User Name | userPrincipalName |
| Refresh Interval (seconds) | 21600 |
| Password Last Set | pwdLastSet |
| Password Max Age | maxPwdAge |

Cancel  Save

Go to **Publish**.

The screenshot shows the VERSA Configuration interface with the following details:

- Header:** ACME-ONE, CONFIGURATION, America/Bozota, English, Administrator, Service Provider Administrator.
- Left Sidebar:** View, Configure, Deploy, Monitor, Analytics, Inventory, Users, Settings, Tenants.
- Current Path:** Configure > Security Service Edge > Users and Device Authentication > Profiles > User and Device Authentication Profile.
- Table:** User and Device Authentication Profiles (1)

| | Name | Type | Description | Tags | Last Modified |
|--------------------------|--------------------|------|-------------|------|--|
| <input type="checkbox"/> | AD_Server_Acme_One | LDAP | | | 7/28/2025, 4:54:47 PM Administrator |
- Buttons:** Publish (1) (highlighted with a red box), Add, Delete, Refresh, Reference, Select Columns.
- Page Navigation:** Showing 1 of 1 results, 10 rows per page, Go to page 1, Previous, Next.

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.

ACME-ONE

CONFIGURATION

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

Edit Client-based Access Rule: Secure_Access_Windows_Profile

Match Criteria

Action

Operating System 1 Users & Groups 2 Endpoint Posture 3 Source Geo Location & Source IP Address 4 Traffic Action 5 Gateways 6 Client Configuration 7 Agent Profile From EIP 8 Review & Configure

By default we have chosen all users and groups to apply your security enforcements

If you prefer, you can select the specific users or groups for the security posture.

Users & Groups

Known Users

Customize

Cancel Back Skip to Review Next

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.

ACME-ONE

CONFIGURATION

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

Edit Client-based Access Rule: Secure_Access_Windows_Profile

Source IP Address

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.

User Type 1 Selected Users Known Users

Enable Rule for the following matched users or user groups

AD_Server_Acme_One

User Groups 2 User Groups [0] + Add New User Group

Name Distinguished Name (DN)

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.

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**.

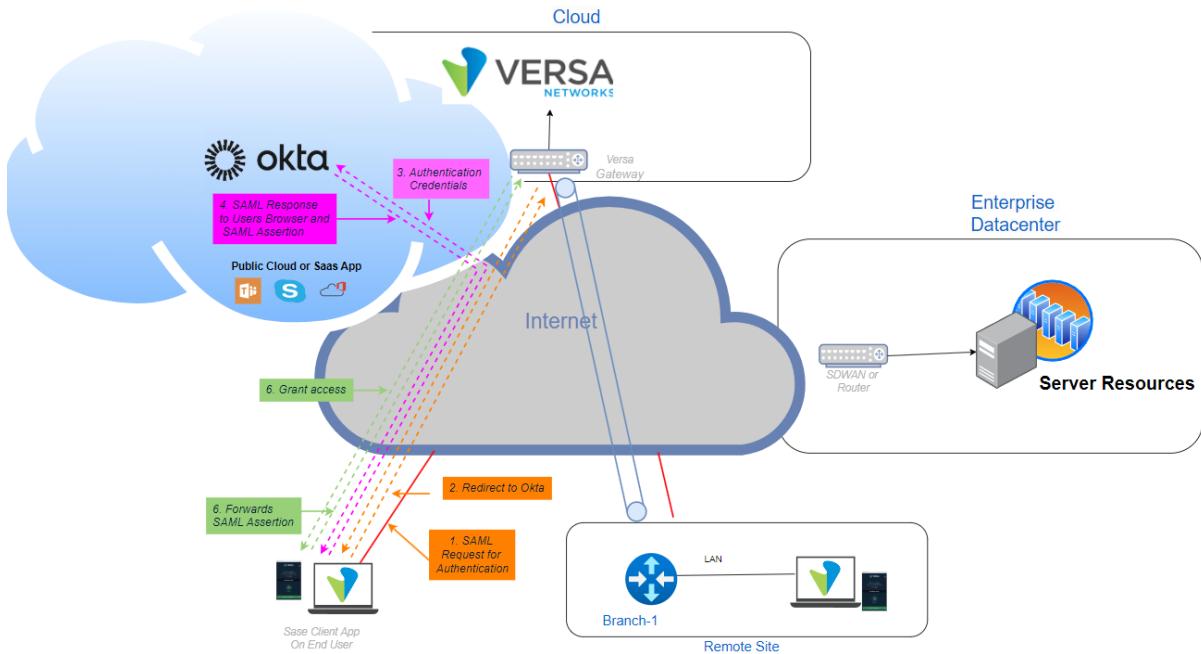
SAML Authentication

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.



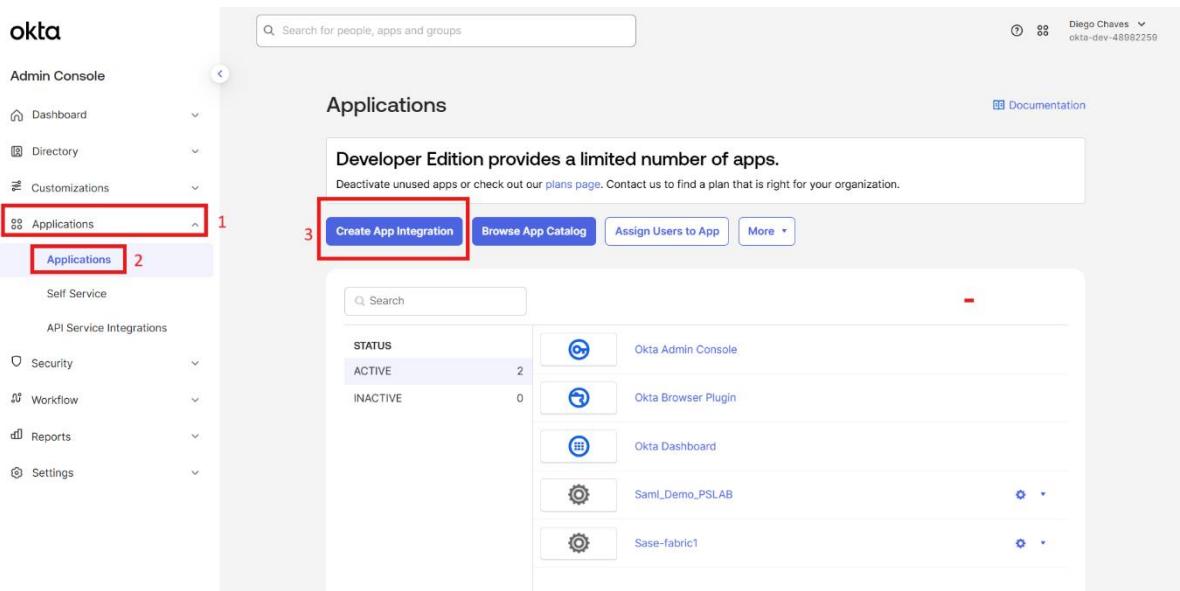
OKTA Portal Configuration

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.



The screenshot shows the Okta Admin Console interface. The left sidebar is titled "Admin Console" and includes "Dashboard", "Directory", "Customizations", "Applications" (which is highlighted with a red box and has a red number "1" next to it), "Self Service", "API Service Integrations", "Security", "Workflow", "Reports", and "Settings". The main content area is titled "Applications" and contains the following text: "Developer Edition provides a limited number of apps. Deactivate unused apps or check out our [plans page](#). Contact us to find a plan that is right for your organization." Below this is a button labeled "Create App Integration" (which is highlighted with a red box and has a red number "3" next to it). Other buttons include "Browse App Catalog", "Assign Users to App", and "More". A search bar is at the top of the main content area. Below the search bar is a table with columns "STATUS", "ACTIVE" (with a value of 2), and "INACTIVE" (with a value of 0). The table lists several applications: "Okta Admin Console" (ACTIVE), "Okta Browser Plugin" (ACTIVE), "Okta Dashboard" (ACTIVE), "Saml_Demo_PSLAB" (ACTIVE), and "Sase-fabric1" (ACTIVE). Each application has a gear icon for settings.

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.

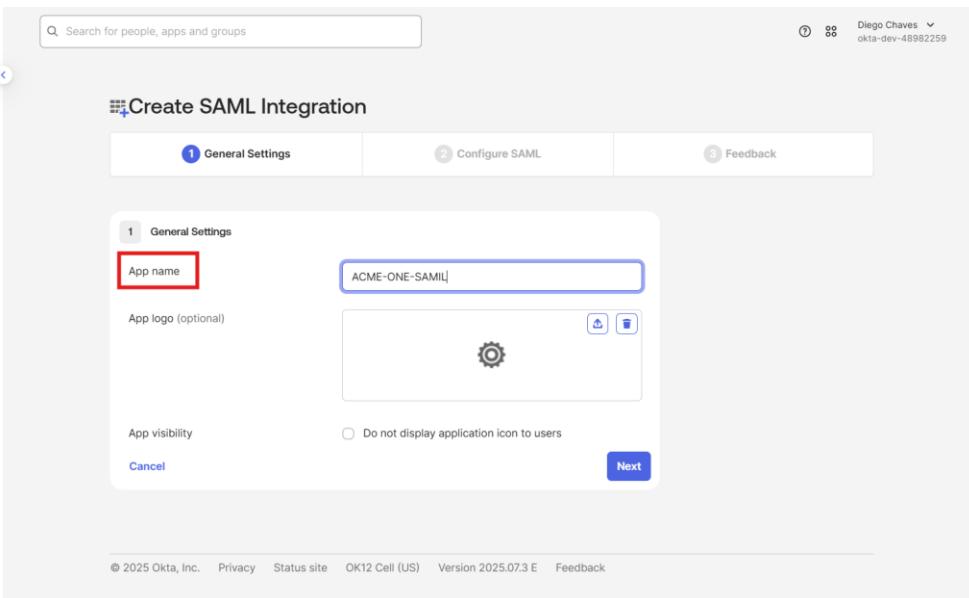
API Services

Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

[Cancel](#)

[Next](#)

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



The screenshot shows the Okta Admin Console interface. The left sidebar lists various admin sections like Dashboard, Directory, Customizations, Applications, Security, Workflow, Reports, and Settings. The main area is titled 'Create SAML Integration' and is on the 'General Settings' step. It has three tabs: 'General Settings' (selected), 'Configure SAML', and 'Feedback'. Under 'General Settings', there is a 'App name' field containing 'ACME-ONE-SAML' (which is highlighted with a red box), an 'App logo (optional)' section with a placeholder image, and an 'App visibility' section with a checkbox for 'Do not display application icon to users'. At the bottom are 'Cancel' and 'Next' buttons, with 'Next' also highlighted with a red box. The top right corner shows the user 'Diego Chaves' and the Okta instance 'okta-dev-48982259'.

- Define custom attributes.

4. 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: <code>https://<SASE-GW-FQDN>/versa-flexvnf/saml/login-consumer</code>.</p> <p>Example: <code>https://acme-one-sasegwdiegos-lab.versanow.net/versa-flexvnf/saml/login-consumer</code></p> |
| Audience URI (SP Entity ID) | <p>Service Provider (SP) entity ID:</p> <p>Format: <code>https://<SASE-GW-FQDN>/metadata</code>.</p> <p>Example: <code>https://acme-one-sasegwdiegos-lab.versanow.net/metadata</code></p> |
| Default Relay State | <p>Used for IdP-initiated SSO:-</p> <p>System user: <code>vd-ui::system</code></p> <p>Tenant user: <code>vd-ui::<organization-name></code></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: <code>https://schemas.microsoft.com/ws/2008/06/identity/claims/groups</code></p> <p>Name format: <i>Unspecified</i></p> <p>Filter: Regex <code>(.*)</code></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-5773745532411860288246009139" 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 href="https://acme-one-sasegwdiegos-lab.versanow.net/metadata"/>
      </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">
            <AttributeValue>
              <xsi:type="http://www.w3.org/2001/XMLSchema">
                <xsi:type="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">GroupName Match Starts with ".*" (ignores case)
              </AttributeValue>
            </saml2:Attribute>
          </saml2:AttributeStatement>
        </saml2:AttributeStatement>
      </saml2:AuthnStatement>
    </saml2:AuthnStatement>
  </saml2:Assertion>

```

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

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/exkpzj71t!Ng6xg675d7/sso/saml/metadata> 

Hide details

Sign on URL https://dev-48982259.okta.com/app/dev-48982259_acmeonesaml_1/exkpzj71t!Ng6xg675d7/sso/saml 

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

Issuer <http://www.okta.com/exkpzj71t!Ng6xg675d7> 

Signing Certificate  

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**

Groups

| Group name | People | Applications |
|---------------------|--|--------------|
| SaseFabric-Group | 3 | 2 |
| Everyone | 4 | 0 |
| Okta Administrators | Okta manages this group, which contains all administrators in your organization. | |

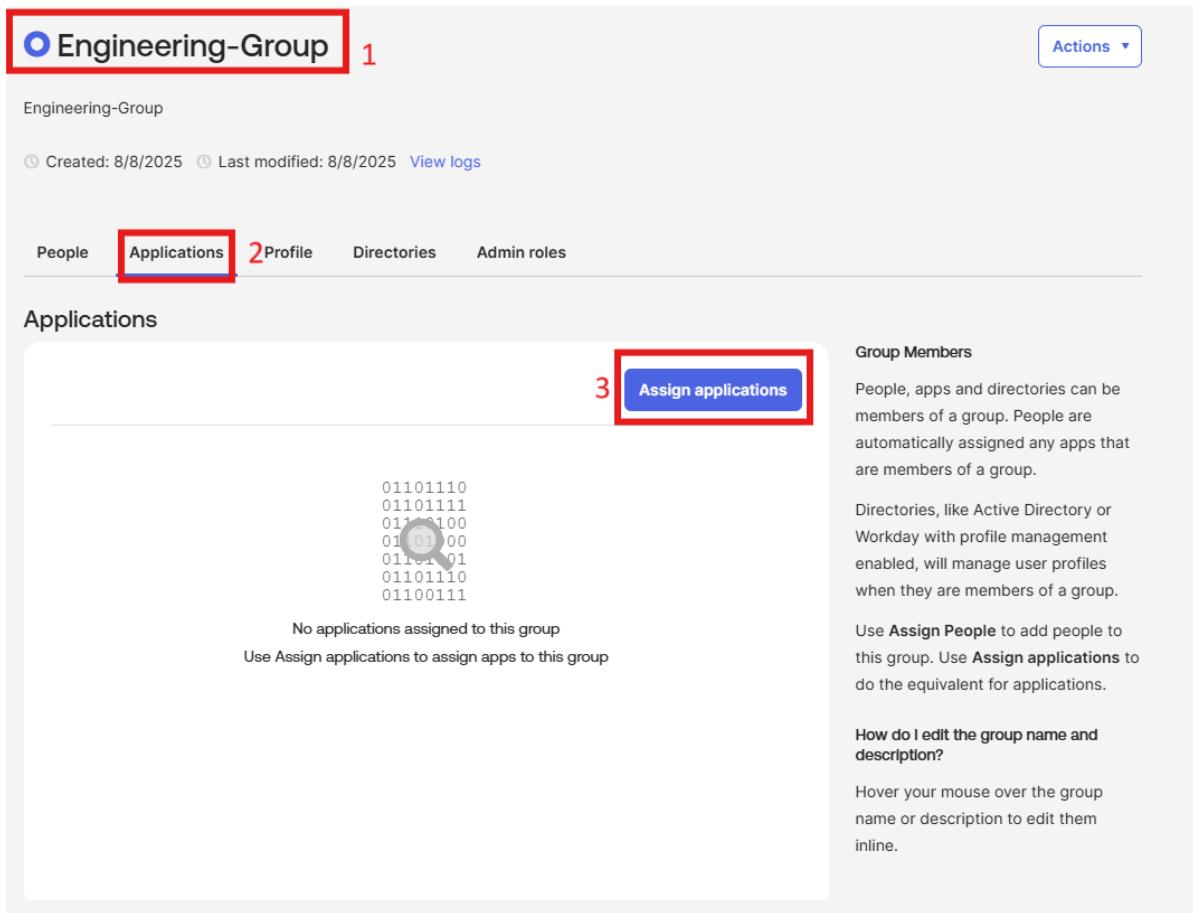
In the name field, enter a group name

Add group

| | |
|---|--|
| Name | <input type="text" value="Engineering-Group"/> |
| Description (optional) | <input type="text" value="Engineering-Group"/> |
| <input type="button" value="Save"/> <input type="button" value="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

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
01101100
01101101
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 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?

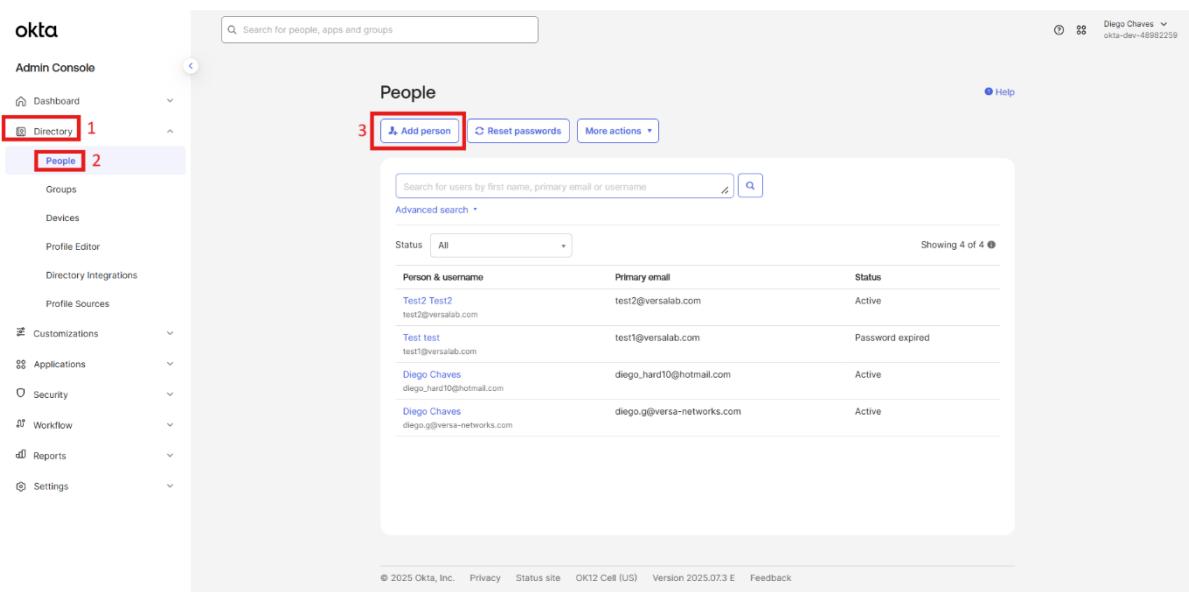
Hover your mouse over the group name or description to edit them inline.

Select newly created SAML application

Assign Applications to Engineering-Group

| | | |
|--|-----------------|--|
| | Sase-fabric1 | <input style="border: 1px solid #0072BD; border-radius: 5px; padding: 2px 10px; background-color: #0072BD; color: white;" type="button" value="Assign"/> |
| | Saml_Demo_PSLAB | <input style="border: 1px solid #0072BD; border-radius: 5px; padding: 2px 10px; background-color: #0072BD; color: white;" type="button" value="Assign"/> |
| | ACME-ONE-SAML | <input style="border: 1px solid #0072BD; border-radius: 5px; padding: 2px 10px; background-color: #0072BD; color: white;" type="button" value="Assign"/> |

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.



okta

Admin Console

1 [Directory](#)

2 [People](#)

3 [Add person](#)

People

Search for users by first name, primary email or username

| Person & username | Primary email | Status |
|--|----------------------------|------------------|
| Test2 Test2 test2@versalab.com | test2@versalab.com | Active |
| Test test test1@versalab.com | test1@versalab.com | Password expired |
| Diego Chaves diego_hard10@hotmail.com | diego_hard10@hotmail.com | Active |
| Diego Chaves diego.g@versa-networks.com | diego.g@versa-networks.com | Active |

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

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"

Select **SAML**, Click Get Started

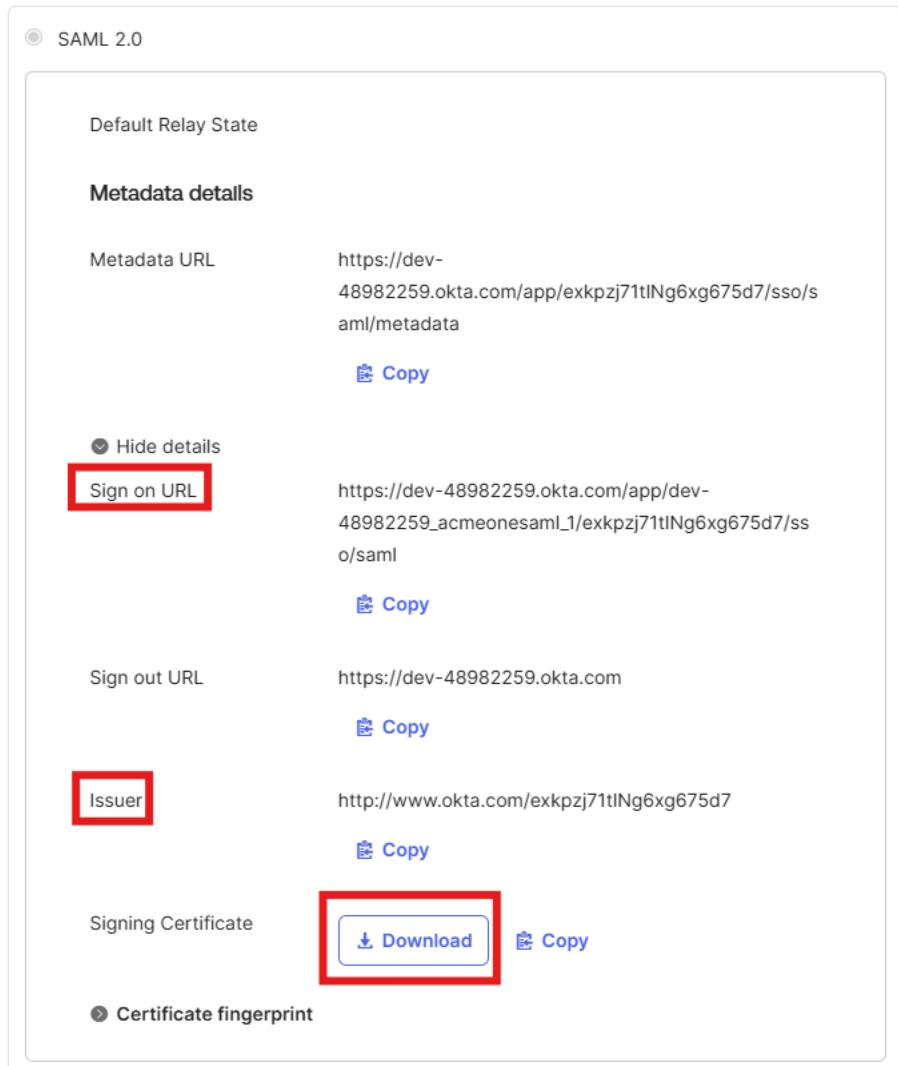
Select which user / device authentication profile you would like to configure.

- LDAP**: LDAPS 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**.



The screenshot shows the 'SAML 2.0' configuration page in the Okta admin console. The 'Metadata details' section is expanded, displaying the following information:

- Metadata URL:** https://dev-48982259.okta.com/app/dev-48982259_acmeonesaml_1/exkpzj71tINg6xg675d7/sso/saml/metadata (with a **Copy** button)
- Sign on URL:** https://dev-48982259.okta.com/app/dev-48982259_acmeonesaml_1/exkpzj71tINg6xg675d7/sso/saml (with a **Copy** button)
- Sign out URL:** <https://dev-48982259.okta.com> (with a **Copy** button)
- Issuer:** <http://www.okta.com/exkpzj71tINg6xg675d7> (with a **Copy** button)
- Signing Certificate:** A download button labeled **Download** (with a red box around it) and a **Copy** button.
- Certificate fingerprint:** (link)

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 PingIdentity 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

Single Sign-out URL

Service Provider Certificate

Identity Provider Certificate*

Cache Expiry Time (mins)

Concurrent Logins

Reply URL (Assertion Consumer Reply URL)

- https://acme-one-sasegwdiegos-lab.versanow.net/versa-flexvnt/saml/login-consumer

Cancel Skip to Review Next

Complete the parameters using the values from the Okta app:

Example:

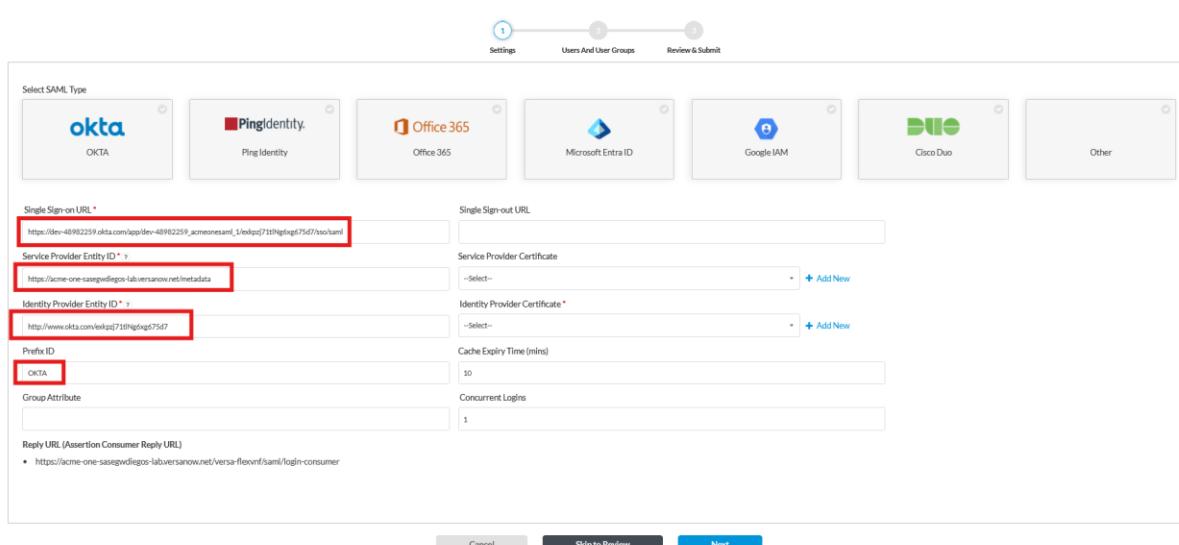
Single Sign-on URL: https://dev-48982259.okta.com/app/dev-48982259_acmeonesaml_1/exkpzj71tINg6xg675d7/sso/saml

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

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

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

Add SAML Authentication Profile



Single Sign-on URL *

https://dev-40982259.okta.com/app/dev-40982259_acmeonesaml_1/oxisp/71tngxg675d7/soi/saml

Service Provider Entity ID * ↴

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

Identity Provider Entity ID * ↴

http://www.okta.com/oxisp/71tngxg675d7

Prefix ID

OKTA

Group Attribute

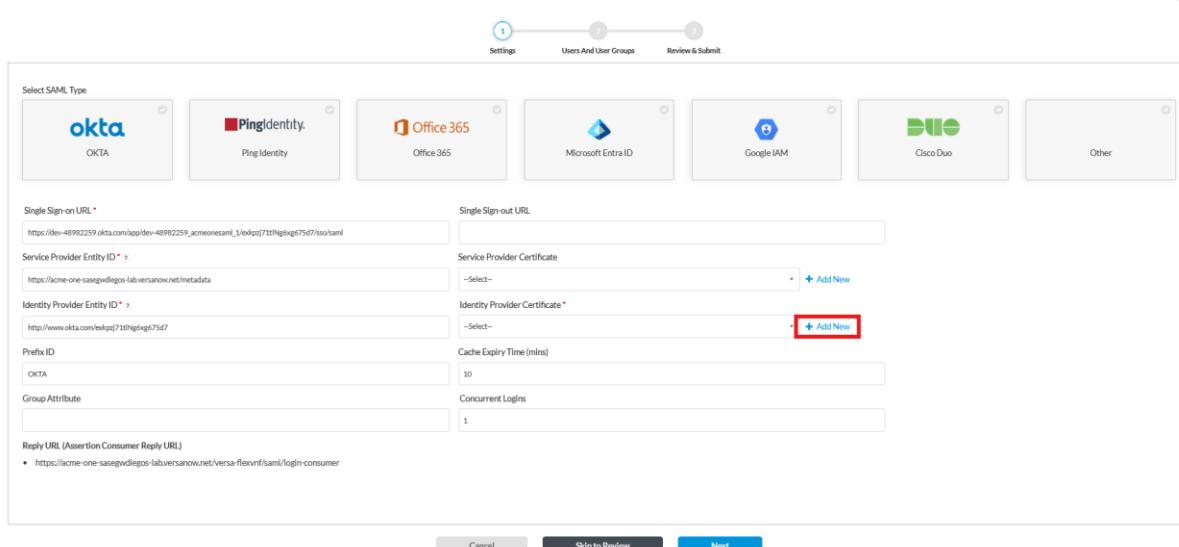
Reply URL (Assertion Consumer Reply URL)

- https://acme-one-sasagwdelego-labversanow.net/versa-flexvrf/saml/login-consumer

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



Single Sign-on URL *

https://dev-40982259.okta.com/app/dev-40982259_acmeonesaml_1/oxisp/71tngxg675d7/soi/saml

Service Provider Entity ID * ↴

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

Identity Provider Entity ID * ↴

http://www.okta.com/oxisp/71tngxg675d7

Prefix ID

OKTA

Group Attribute

Reply URL (Assertion Consumer Reply URL)

- https://acme-one-sasagwdelego-labversanow.net/versa-flexvrf/saml/login-consumer

Cancel Skip to Review Next

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

Add Certificate/CA-Chain/Private Key

Certificate Type CA Chain

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

CA-Chain Name *

OKTA_ACME

Upload File

Cancel

Add

Then Add

Add Certificate/CA-Chain/Private Key

Certificate Type CA Chain

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

CA-Chain Name *

OKTA-ACME

Upload File

OKTA-ACME.crt 

Cancel

Add

If certificate was uploaded successful, the certificate details will be displayed

Add SAML Authentication Profile

1 Settings 2 Users And User Groups 3 Review & Submit

Select SAML Type



Single Sign-on URL*

https://www.okta.com/app/0002259_acme/restart_1_welpp710hbgp75d7s0/saml

Service Provider Entity ID *

<https://acme-one-sso-bridge-lab.versanow.net/metadata>

Identity Provider Entity ID *

<http://www.okta.com/rekip710hbgp75d7>

Single Sign-out URL

Service Provider Certificate

-Select-  

Identity Provider Certificate*

OKTA-ACME  

Details
Name: OKTA-ACME
File Name: OKTA-ACME.crt
Issuer ID: 0e-4002259
Issued By: 3025-08-08 12:23:19 to 2035-08-08 12:24:10

Cache Expiry Time (mins)

10

Concurrent Logins

1

Prefix ID

OKTA

Group Attribute

Reply URL (Assertion Consumer Reply URL)

<https://acme-one-sso-bridge-lab.versanow.net/versa-florent/saml/login-consumer>

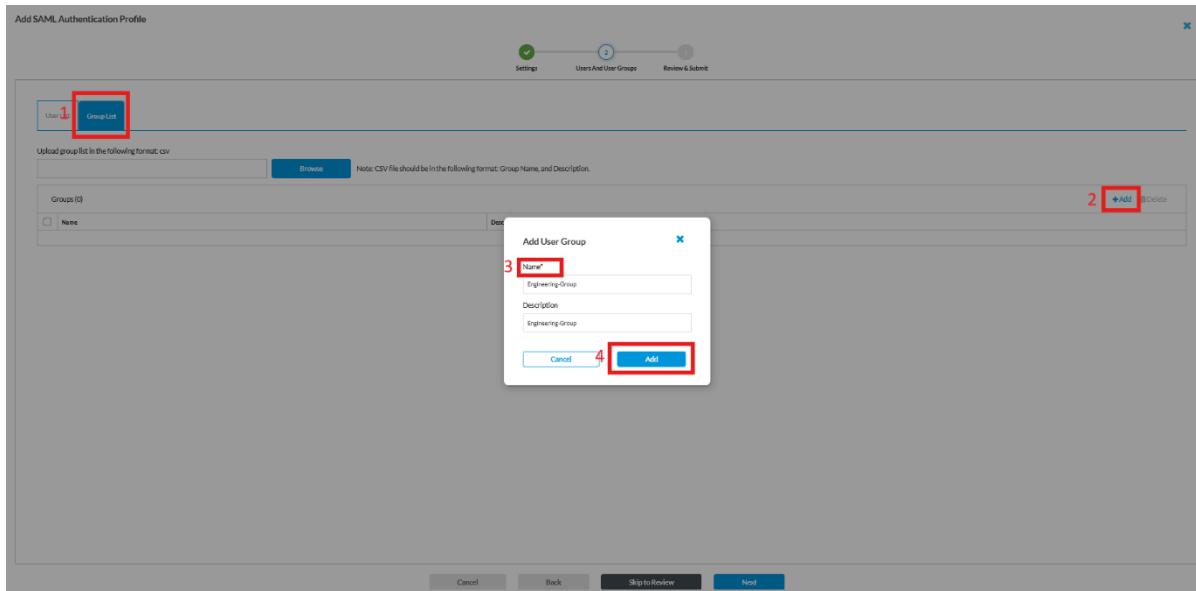
Cancel **Skip to Review** **Next**

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.



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.

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**.

Microsoft Entra admin center

Enterprise applications | All applications

Overview

Manage

Security

Activity

Application type == Enterprise Applications

| Name | Object ID | Application ID | Homepage URL | Created on |
|----------------|-----------------------|-----------------------|--------------------------|------------|
| Google Work... | 03eed589-93c8-4f76... | 4d7fe9fb-5646-447f... | https://drive.google... | 8/12/2025 |
| ACME-ONE-S... | 576b6311-9a56-4d3... | 45e6c18b-692d-41d... | https://account.activ... | 9/3/2025 |
| Intune-MDM | da891466-9d12-4c1... | cc813451-f42b-41bd... | | 7/30/2025 |

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**.

Microsoft Entra admin center

Enterprise applications | All applications

Browse Microsoft Entra Gallery

+ Create your own application

Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

ACME-ONE-SAML

What are you looking to do with your application?

Configure Application Proxy for secure remote access to an on-premises application

Register an application to integrate with Microsoft Entra ID (App you're developing)

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

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

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

The screenshot shows the Microsoft Entra admin center interface. On the left, the navigation menu includes Home, Agents, Favorites, Entra ID, Overview, Users, Groups, Devices, Enterprise apps, App registrations, Roles & admins, Delegated admin partners, and Domain services. The 'Enterprise apps' section is selected. In the center, the 'ACME-ONE-SAML | Single sign-on' page is displayed. The 'Manage' section on the left lists Properties, Owners, Roles and administrators, Users and groups, Single sign-on (which is selected and highlighted with a red box), Provisioning, Application proxy, Self-service, Custom security attributes, Security, Conditional Access, Permissions, and Token encryption. The main content area is titled 'Select a single sign-on method' and shows two options: 'Disabled' (with a note that single sign-on is not enabled and users won't be able to launch the app from My Apps) and 'SAML' (with a note that it provides rich and secure authentication using the SAML protocol). The 'SAML' option is also highlighted with a red box.

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: <code>https://schemas.microsoft.com/ws/2008/06/identity/claims/groups</code></p> <p>Name format: Unspecified</p> <p>Filter: Select Regex (or equivalent option) and enter <code>*</code></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:c: 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 href="https://acme-one-sasegwdiegos-lab.versanow.net/metadata"/>
      </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: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>

```

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

The screenshot shows the Microsoft Entra admin center interface. On the left, the navigation menu is visible with sections like Home, Agents, Favorites, Entra ID, Overview, Users, Groups, Devices, Enterprise apps, App registrations, Roles & admins, Delegated admin partners, Domain services, Conditional Access, and Multifactor authentication. The main content area is titled "Basic SAML Configuration" for the "ACME-ONE-SAML | SAM" enterprise application. The "Identifier (Entity ID)" field contains "https://acme-one-sasegwdiegos-lab.versanow.net/metadata". The "Reply URL (Assertion Consumer Service URL)" field contains "https://acme-one-sasegwdiegos-lab.versanow.net/versa-flexvnf/saml/login-consu...". The "Sign on URL (Optional)" field also contains "https://acme-one-sasegwdiegos-lab.versanow.net/versa-flexvnf/saml/login-consumer". The "Save" button is located at the top right of the configuration form.

6. Define **Attributes & Claims**.

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

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

Manage claim ...

X

Save X Discard changes | Got feedback?

| | | |
|---|--|---|
| Name * | <input type="text" value="givenname"/> | ✓ |
| Namespace | <input type="text" value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"/> | ✓ |
| ▼ Choose name format | | |
| Source * | <input checked="" type="radio"/> Attribute <input type="radio"/> Transformation <input type="radio"/> Directory schema extension | |
| Source attribute * | <input type="text" value="user.givenname"/> | |
| ▼ Claim conditions | | |
| ▼ Advanced SAML claims options | | |

Manage claim ...

X

Save X Discard changes | Got feedback?

| | | |
|---|--|---|
| Name * | <input type="text" value="organization"/> | ✓ |
| Namespace | <input type="text" value="Enter a namespace URI"/> | ✓ |
| ▼ Choose name format | | |
| Source * | <input checked="" type="radio"/> Attribute <input type="radio"/> Transformation <input type="radio"/> Directory schema extension | |
| Source attribute * | <input acme-one\""="" type="text" value="\"/> | |
| ▼ Claim conditions | | |
| ▼ Advanced SAML claims options | | |

Manage claim ...

X

Save X Discard changes | Got feedback?

| | | |
|---|--|---|
| Name * | <input type="text" value="role"/> | ✓ |
| Namespace | <input type="text" value="Enter a namespace URI"/> | ✓ |
| ▼ Choose name format | | |
| Source * | <input checked="" type="radio"/> Attribute <input type="radio"/> Transformation <input type="radio"/> Directory schema extension | |
| Source attribute * | <input type="text" value="user.assignedroles"/> | |
| ▼ Claim conditions | | |
| ▼ Advanced SAML claims options | | |

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

Click + Add a group Claim

Attributes & Claims X

[+ 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 X

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 *

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) ✓

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) ✓

Namespace (optional)

Emit groups as role claims ⓘ

Apply regex replace to groups claim content

Regex pattern * ⓘ

Regex replacement pattern * ⓘ

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.

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 **3**

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

Thumbprint: 0382CE53329AACF016A20F1C7419EBF0E150D786

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

Notification Email: diegohaves@diegolabversa.onmicrosoft.com

App Federation Metadata Url: <https://login.microsoftonline.com/a08ab2d2-a5df-481b-9ffa-13a2a2a2a2a2>

Certificate (Base64) [Download](#)

Certificate (Raw) [Download](#)

Federation Metadata XML [Download](#)

Verification certificates (optional)

Required: No

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-481b-9ffa-13a2a2a2a2a2>

Microsoft Entra Identifier: <https://sts.windows.net/a08ab2d2-a5df-481b-9ffa-13a2a2a2a2a2>

Logout URL: <https://login.microsoftonline.com/a08ab2d2-a5df-481b-9ffa-13a2a2a2a2a2>

- Create the Groups and Users.

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

Microsoft Entra admin center

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

Groups | Overview

Diego Test Lab

New group

Download groups

Preview features

Overview

All groups

Deleted groups

Diagnose and solve problems

Settings

General

Expiration

Naming policy

Activity

Privileged Identity Management

Access reviews

Audit logs

Bulk operation results

Troubleshooting + Support

New support request

Basic information

Total groups: 4

Dynamic groups: 1

M365 groups: 3

Cloud groups: 4

Security groups: 1

On-premises groups: 0

Feature highlights

Access reviews: Make sure only the right people have continued access.

Conditional Access: Control user access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.

Quick actions

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

Create new user ...

X

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.onmicrosoft.com

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.

Create new user ...

X

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 ...

X

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.

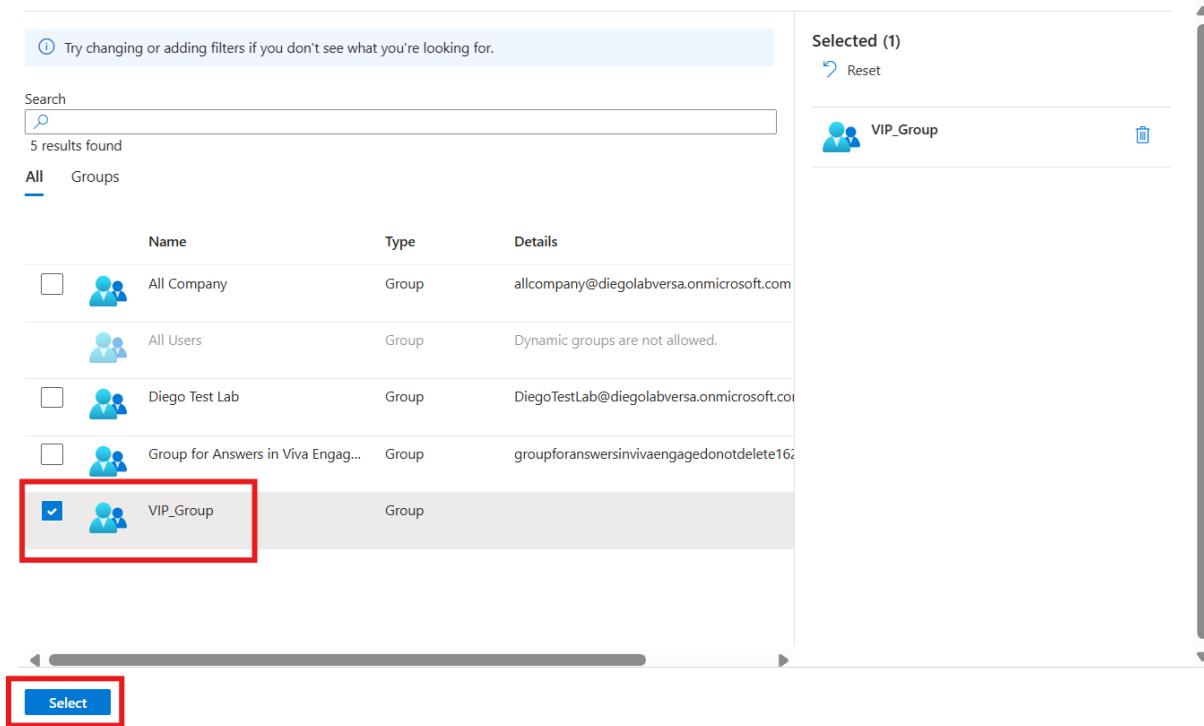
Review + create

< 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 |
| <input type="checkbox"/> | 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 | |

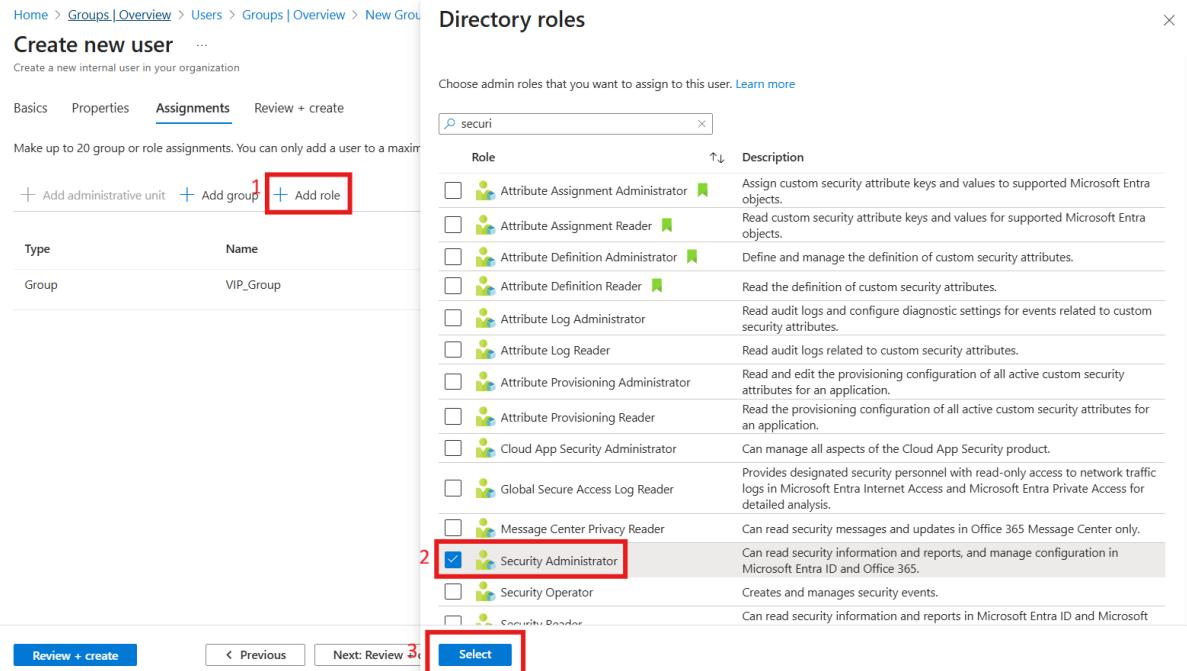
Selected (1)

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 1 + Add role

| Type | Name |
|-------|-----------|
| Group | VIP_Group |

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

Role Description

- Attribute Assignment Administrator Assign custom security attribute keys and values to supported Microsoft Entra objects.
- Attribute Assignment Reader Read custom security attribute keys and values for supported Microsoft Entra objects.
- Attribute Definition Administrator Define and manage the definition of custom security attributes.
- Attribute Definition Reader Read the definition of custom security attributes.
- Attribute Log Administrator Read audit logs and configure diagnostic settings for events related to custom security attributes.
- Attribute Log Reader Read audit logs related to custom security attributes.
- Attribute Provisioning Administrator Read and edit the provisioning configuration of all active custom security attributes for an application.
- Attribute Provisioning Reader Read the provisioning configuration of all active custom security attributes for an application.
- Cloud App Security Administrator Can manage all aspects of the Cloud App Security product.
- 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.
- Message Center Privacy Reader Can read security messages and updates in Office 365 Message Center only.
- Security Administrator 2 Can read security information and reports, and manage configuration in Microsoft Entra ID and Office 365.
- Security Operator Creates and manages security events.
- Security Reader 3 Can read security information and reports in Microsoft Entra ID and Microsoft

Review + create < Previous Next: Review 3 Select

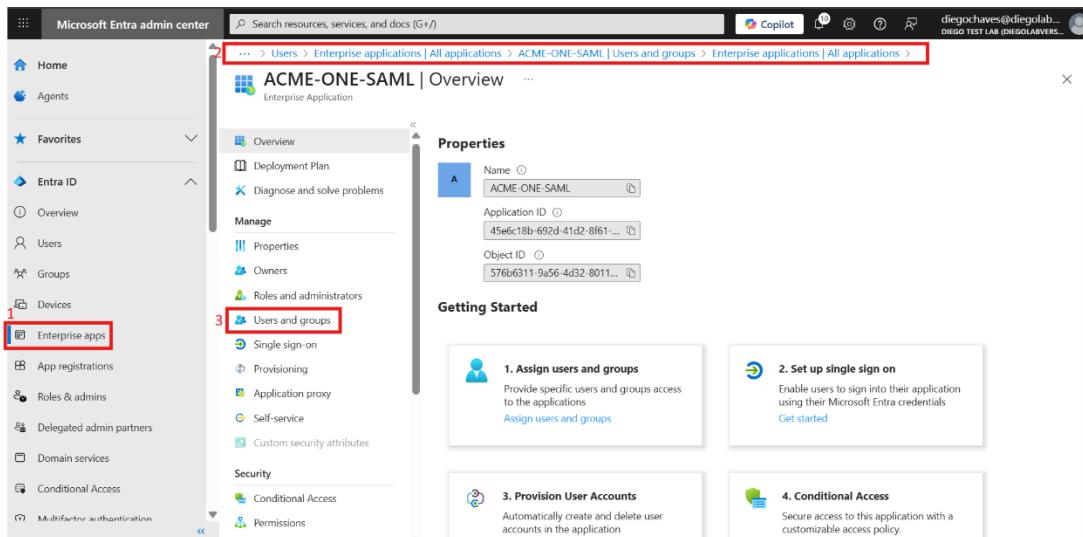
Review & Create

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

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

ACME-ONE-SAML | Overview

Properties

Name: ACME-ONE-SAML

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

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

Getting Started

- 1. Assign users and groups
- 2. Set up single sign on
- 3. Provision User Accounts
- 4. Conditional Access

1 Enterprise apps

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

3 Users and groups

2. 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

Manage

- + 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 | |

Security

- Conditional Access
- Permissions

3. 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

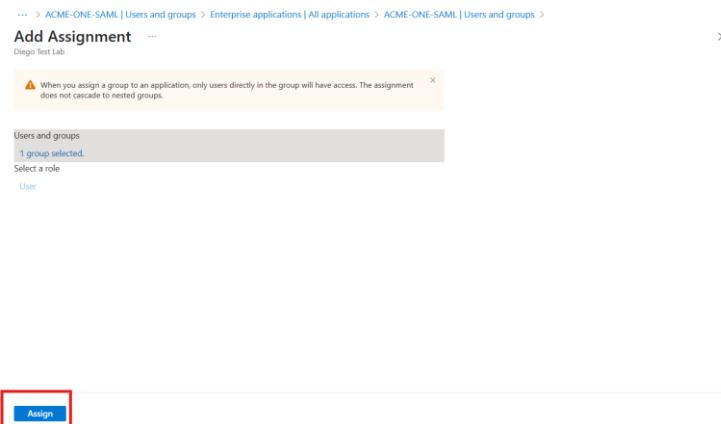
9 results found

All Users Groups

| Name | Type | Details |
|------------------------------------|-------|--|
| Diego Test Lab | Group | DiegoTestLab@diegolabversa.onmicrosoft.com |
| vip | User | vip@diegolabversa.onmicrosoft.com |
| Group for Answers in Viva Engag... | Group | groupforanswersinvivaengagedonotdelete1 |
| VIP | User | vip1@diegolabversa.onmicrosoft.com |
| VIP_Group | Group | |

Select

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



Concerto configuration for ENTRA-ID SAML Authentication Profiles

Navigate to User and Device Authentication Profiles

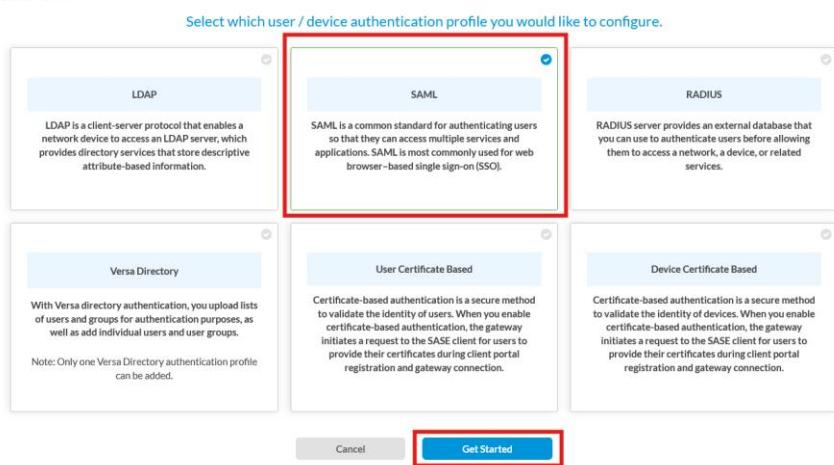
Go to:

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

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

Select **SAML**, Click Get Started

Add User and Device Authentication Profile

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

Conditional Access Permissions Token encryption

Activity

Sign-in logs

3 SAML Certificates

Token signing certificate

| | |
|-----------------------------|---|
| Status | Active |
| Thumbprint | 0382CE53329AACF016A20F1C7419EBF0E150D786 |
| Expiration | 9/4/2028, 10:34:51 AM |
| Notification Email | diegochaves@diegolabversa.onmicrosoft.com |
| App Federation Metadata Url | https://login.microsoftonline.com/a08ab2d2-a5df-481b-9ffa-000000000000 |
| Certificate (Base64) | Download |
| Certificate (Raw) | Download |
| Federation Metadata XML | Download |

Verification certificates (optional)

| | |
|----------|----|
| Required | No |
| 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-481b-9ffa-000000000000 |
| Microsoft Entra Identifier | https://sts.windows.net/a08ab2d2-a5df-481b-9ffa-000000000000 |
| Logout URL | https://login.microsoftonline.com/a08ab2d2-a5df-481b-9ffa-000000000000 |

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 Settings 2 Users And User Groups 3 Review & Submit

Select SAML Type

- okta
- PingIdentity
- Office 365
- Microsoft Entra ID
- Google IAM
- Duo
- Other

Single Sign-on URL *

Service Provider Entity ID *

Identity Provider Entity ID *

Single Sign-out URL

Service Provider Certificate

Identity Provider Certificate *

Cache Expiry Time (mins)

Concurrent Logins

Reply URL (Assertion Consumer Reply URL)

- <https://acme-one-sasegvdiegos-labversanow.net/versa-flexonf/saml/login-consumer>

Cancel Skip to Review Next

Complete the parameters using the values from the Microsoft Entra id

Example:

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

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

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

Edit SAML Authentication Profile: ENTRA-ID-SAML

1 Settings 2 Users And User Groups 3 Review & Submit

Select SAML Type

- OKTA
- PingIdentity
- Office 365
- Microsoft Entra ID
- Google IAM
- Duo
- Other

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

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

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

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 10:48:40 to 2028-09-03 10:48:47

Prefix ID

Cache Expiry Time (mins) Cache Expiration Mode

Group Attribute

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 Settings 2 Users And User Groups 3 Review & Submit

Select SAML Type

- OKTA
- PingIdentity
- Office 365
- Microsoft Entra ID
- Google IAM
- Duo
- Other

Single Sign-on URL * https://dev-48982259.okta.com/api/dev-48982259_acmeonesaml_1/expsj7tthq6sg67sd7sso/saml

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

Identity Provider Entity ID * <http://www.okta.com/expsj7tthq6sg67sd7>

Prefix ID

Reply URL (Assertion Consumer Reply URL) <https://acme-one-sasegwdiegos-lab.versanow.net/versa-flexvnt/saml/login-consumer>

Service Provider Certificate

Identity Provider Certificate *

Cache Expiry Time (mins) Concurrent Logins

Group Attribute

Cancel Skip to Review Next

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

Add Certificate/CA-Chain/Private Key

Certificate Type **CAChain**

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

CA-Chain Name *

ACME-ONE-SAML

Upload File

Cancel

Add

Then **Add**

Add Certificate/CA-Chain/Private Key

Certificate Type **CA Chain**

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

CA-Chain Name *

ACME-ONE-SAML

Upload File

ACME-ONE-SAML.cer 

Cancel

Add

If certificate was uploaded successful, the certificate details will be displayed

Edit SAML Authentication Profile: ENTRA-ID-SAML

Settings  Users And User Groups  Review & Submit 

Select SAML Type

okta

OKTA

PingIdentity

PingIdentity

Office 365

Office 365

Microsoft Entra ID

Microsoft Entra ID

Google IAM

Google IAM

Duo

Duo

Other

Single Sign-on URL *

<https://login.microsoftonline.com/00b82c22-5d5f-481b-9f9b-750a22e4a512>

Service Provider Entity ID * *

<https://acme-one-saml.svc.ingress.letsversa.net/metadata>

Identity Provider Entity ID *

<https://sts.windows.net/00b82c22-5d5f-481b-9f9b-750a22e4a512/>

Single Sign-out URL

<https://login.microsoftonline.com/00b82c22-5d5f-481b-9f9b-750a22e4a512>

Service Provider Certificate

-Select-

Add New

Identity Provider Certificate *

ACME-ONE-SAML

Add New

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

Prefix ID

Cache Expiry Time (min)

10

Cache Expiry Mode

-Select-

Group Attribute

Cookie Expiry Time (min)

720

Concurrent Logins

1

Reply URL (Assertion Consumer Reply URL)

<https://acme-one-saml.svc.ingress.letsversa.net/versa-floent/saml/login-consumer>

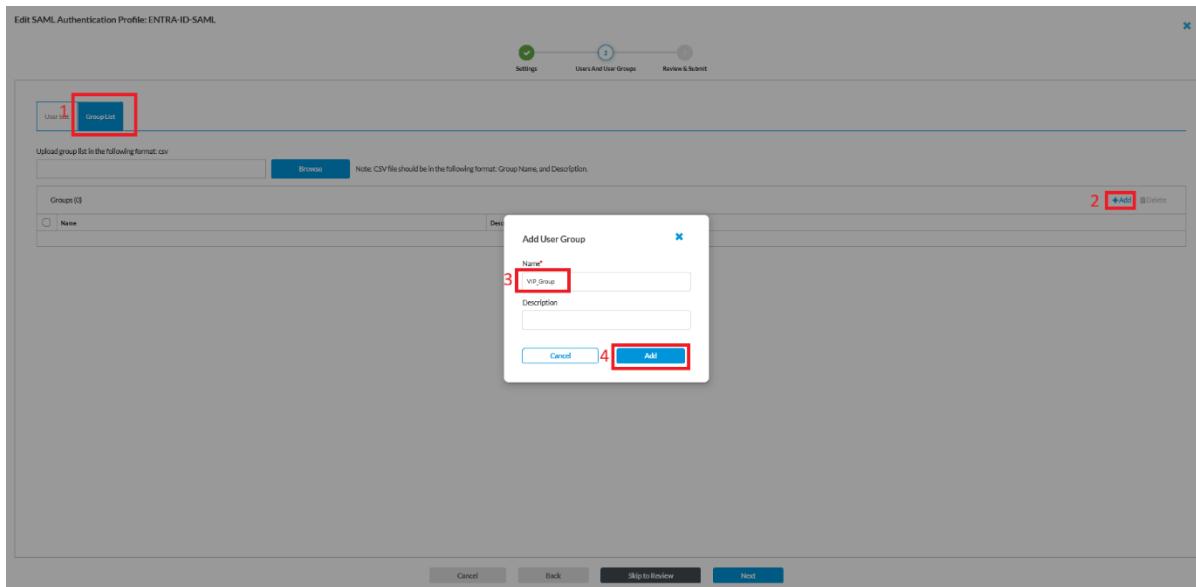
Cancel

Skip to Review

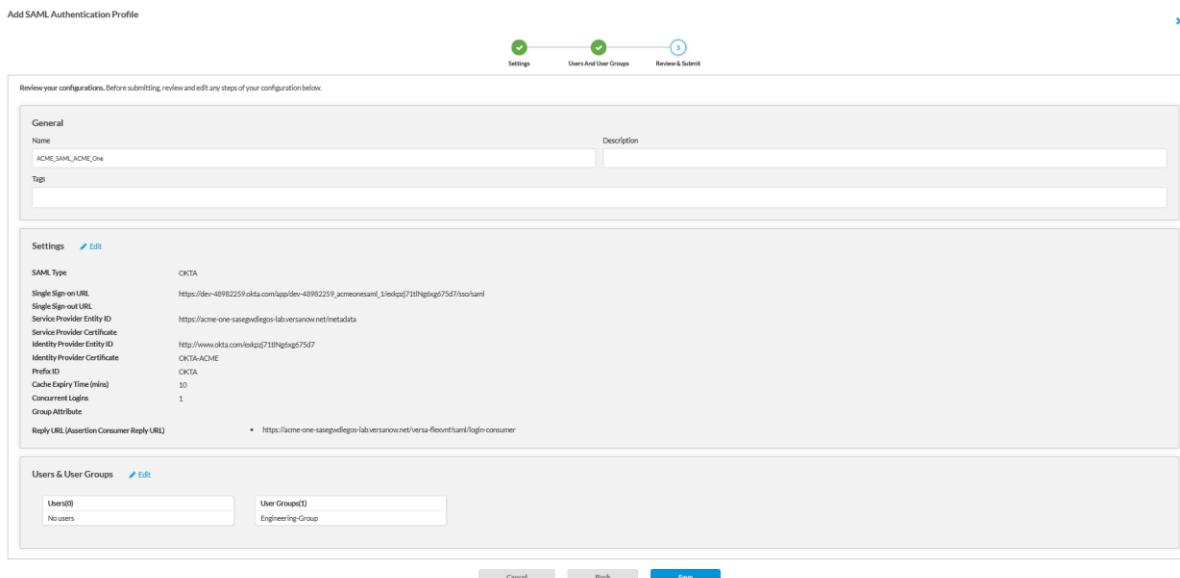
Next

Then **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.



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.



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.

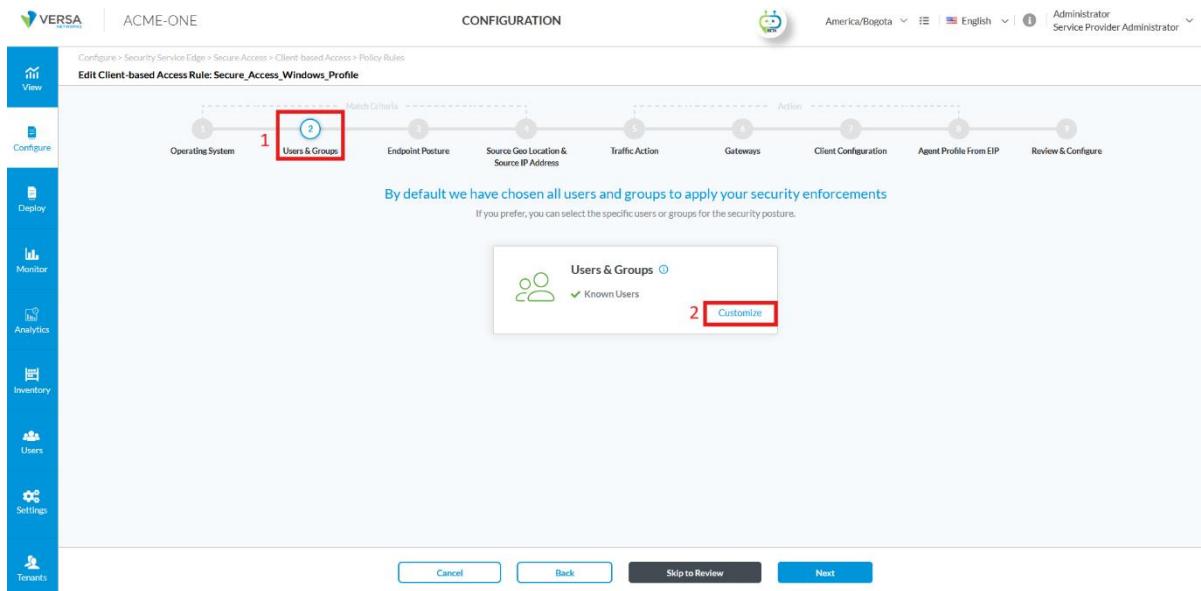
Navigate

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.



The screenshot shows the VERSA Configuration interface for editing a client-based access rule. The left sidebar has icons for View, Configure, Deploy, Monitor, Analytics, Inventory, Users, Settings, and Tenants. The main header shows 'ACME-ONE' and 'CONFIGURATION'. The top navigation bar includes 'Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules', 'Edit Client-based Access Rule: Secure_Access_Windows_Profile', 'Administrator', 'Service Provider Administrator', and language settings. The main content area is titled 'Edit Client-based Access Rule: Secure_Access_Windows_Profile'. It shows a flowchart with steps: Match Criteria (Operating System, 1), Endpoint Posture, Source Geo Location & Source IP Address, Traffic Action, Gateways, Client Configuration, Agent Profile From EIP, and Review & Configure. Step 1 (Operating System) is highlighted with a red box and labeled '1'. A callout box shows the 'Users & Groups' customization panel with the 'Customize' button highlighted with a red box and labeled '2'. The customization panel also shows 'Known Users'.

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.

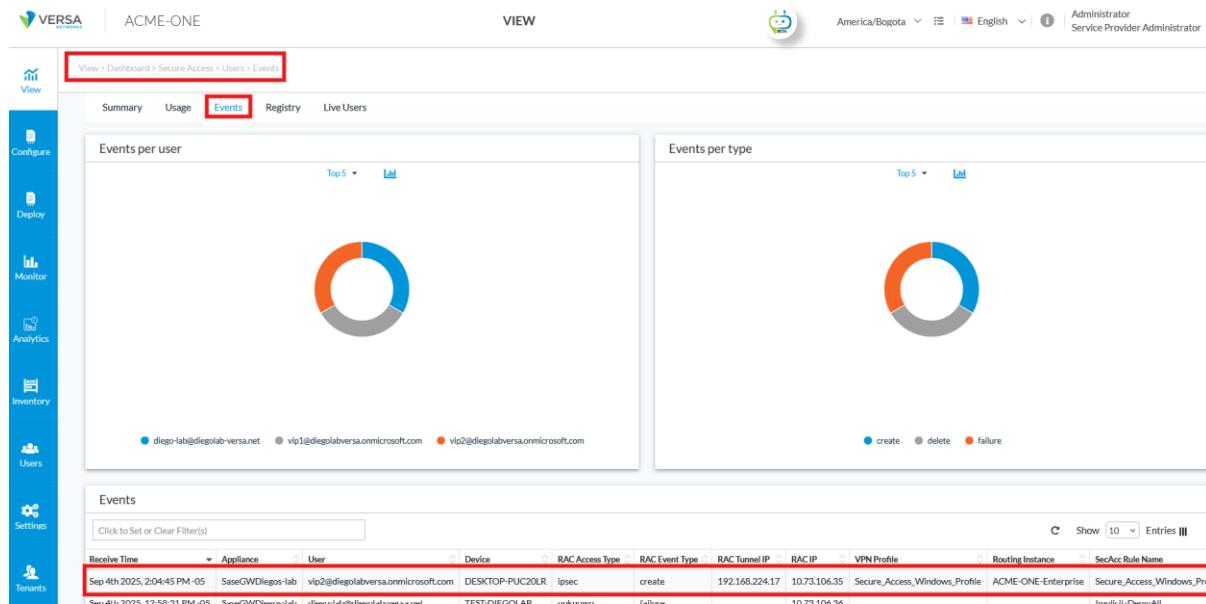
In this step, you can choose to add specific **users** or **groups** to enforce security policies. Use the **User Groups** or **Users** tabs to select the desired entries.

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**.

Verification

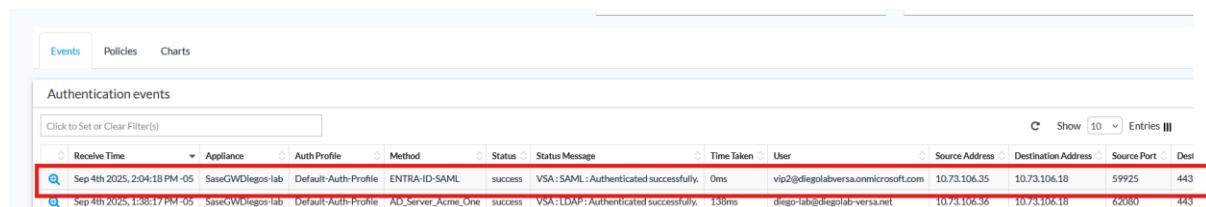
When a user connects to the Gateway and SAML is enabled, the Gateway redirects the login to the configured IdP (Example., Okta or Entra ID). After the user completes credentials/MFA, the IdP returns a **signed SAML assertion** to the Gateway. The Gateway validates the signature and audience, extracts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



| Receive Time | Appliance | User | Method | Status | Time Taken | User | Source Address | Destination Address | Source Port | Dest |
|------------------------------|------------------|------------------------------------|-----------------|---------|------------|----------------|----------------|-------------------------------|---------------------|-------------------------------|
| Sep 4th 2025, 2:04:45 PM -05 | SaseGWDiegos-lab | vip2@diegolabversa.onmicrosoft.com | DESKTOP-PUC20LR | ipsec | create | 192.168.224.17 | 10.73.106.35 | Secure_Access_Windows_Profile | ACME-ONE-Enterprise | Secure_Access_Windows_Profile |
| Sep 4th 2025, 2:04:51 PM -05 | SaseGWDiegos-lab | diego-lab@diegolab-versa.net | TEST-DEVICE-AB | failure | | 10.73.106.34 | | | | |

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



| Receive Time | Appliance | Auth Profile | Method | Status | Status Message | Time Taken | User | Source Address | Destination Address | Source Port | Dest |
|------------------------------|------------------|----------------------|--------------------|---------|--|------------|------------------------------------|----------------|---------------------|-------------|------|
| Sep 4th 2025, 2:04:18 PM -05 | SaseGWDiegos-lab | Default-Auth-Profile | ENTRA-ID-SAML | success | VSA : SAML : Authenticated successfully. | 0ms | vip2@diegolabversa.onmicrosoft.com | 10.73.106.35 | 10.73.106.18 | 59925 | 443 |
| Sep 4th 2025, 1:38:17 PM -05 | SaseGWDiegos-lab | Default-Auth-Profile | AD_Server_Acme_One | success | VSA : LDAP : Authenticated successfully. | 130ms | diego-lab@diegolab-versa.net | 10.73.106.36 | 10.73.106.18 | 62080 | 443 |

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@saseGWDiegos-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@saseGWDiegos-lab-cli> show orgs org-services ACME-ONE user-identification live-users list brief
          TIME
          SESSION TO EXPIRATION
IP ADDRESS      NAME      STATUS HITS EXPIRY MODE
-----
192.168.224.17  vip2@diegolabversa.onmicrosoft.com  Live   17    60  inactivity
[ok][2025-09-04 12:11:50]
admin@saseGWDiegos-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 your tenant is that it is enabled on Headend at infrastructure level by Versa or MSP (if using third-party 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 a 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 OCSP (Online Certificate Status Protocol) checks for real-time certificate revocation verification and selects 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"

| Name | Type | Issued To | Issued By | Valid | Expires | Actions |
|-----------------------|----------------|--------------------------------------|---|---|-----------|---------|
| 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 | ⋮ |
| 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 | ⋮ |
| XKTA-ACME.crt | CA-Chain | dev-48982259 | dev-48982259 | From: 8/8/2025, 12:22:19 PM To: 8/8/2035, 12:24:18 PM | 3652 days | ⋮ |

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*

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 CA Chain Private Key

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

CA-Chain Name *

Upload File

Cancel **Add**

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

| Name | File | Type | Issued To | Expires |
|----------------------|--------------------------|----------------|-----------|-----------|
| device-auth-ca-chain | device-auth-ca-chain.crt | CA Certificate | RAS-CA | 3650 days |

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.

| Profile Type | Description |
|--------------------------|---|
| 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. |
| 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. |

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

Client CA Chain*

Verify with OCSP

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

Username Identifying Field in Certificate*

Cache Expiry Time (mins)

Cookie Expiry Time (mins)

Concurrent Logins

Cancel Skip to Review Next

Add Device Certificate Authentication Profile

Client CA Chain*

Verify with OCSP

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

Username Identifying Field in Certificate*

Cache Expiry Time (mins)

Cookie Expiry Time (mins)

Concurrent Logins

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.

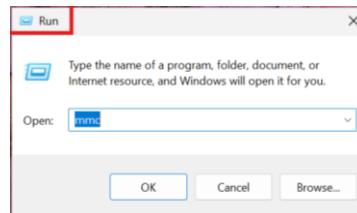
Verify Authentication Order = **Device**.Click **Save** then **Publish**.

Add Device Certificate Authentication Profile

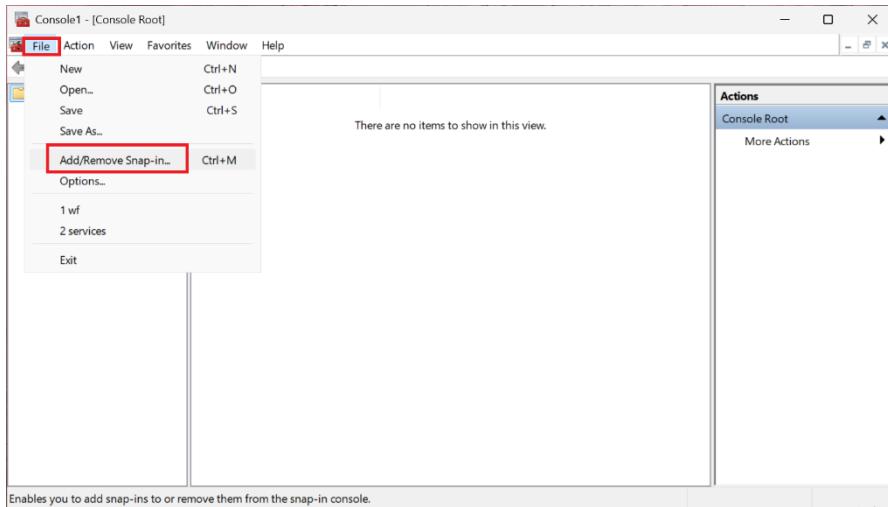
Installing Certificates on the Client Device:

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)

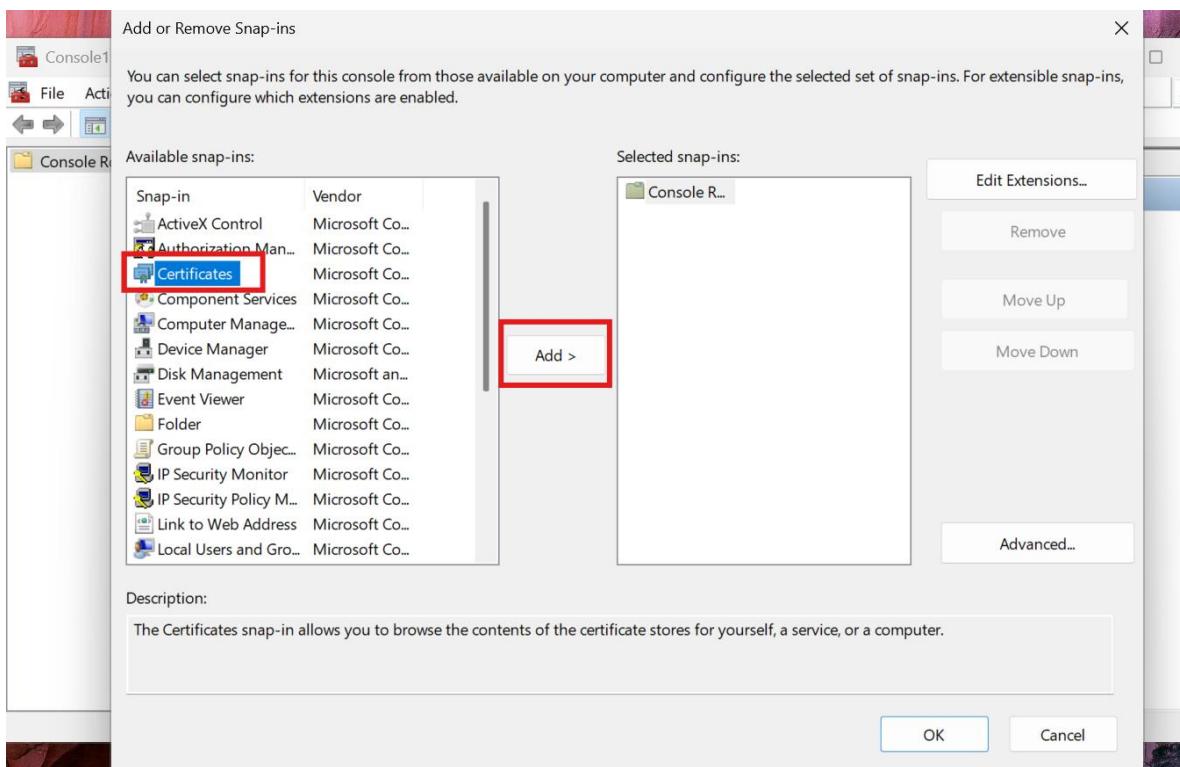
For Windows open the Run dialog, type mmc, and press Enter.

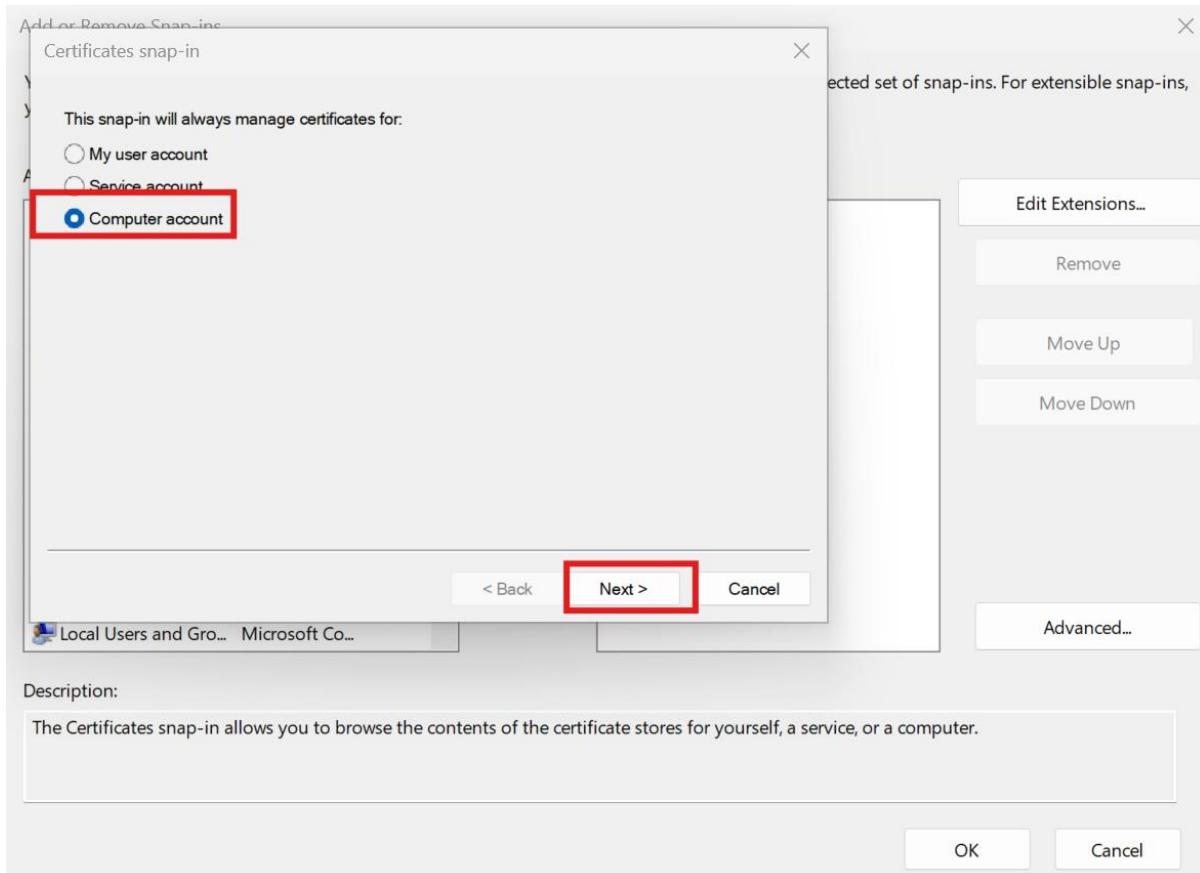


In the MMC console, go to File → Add/Remove Snap-in.

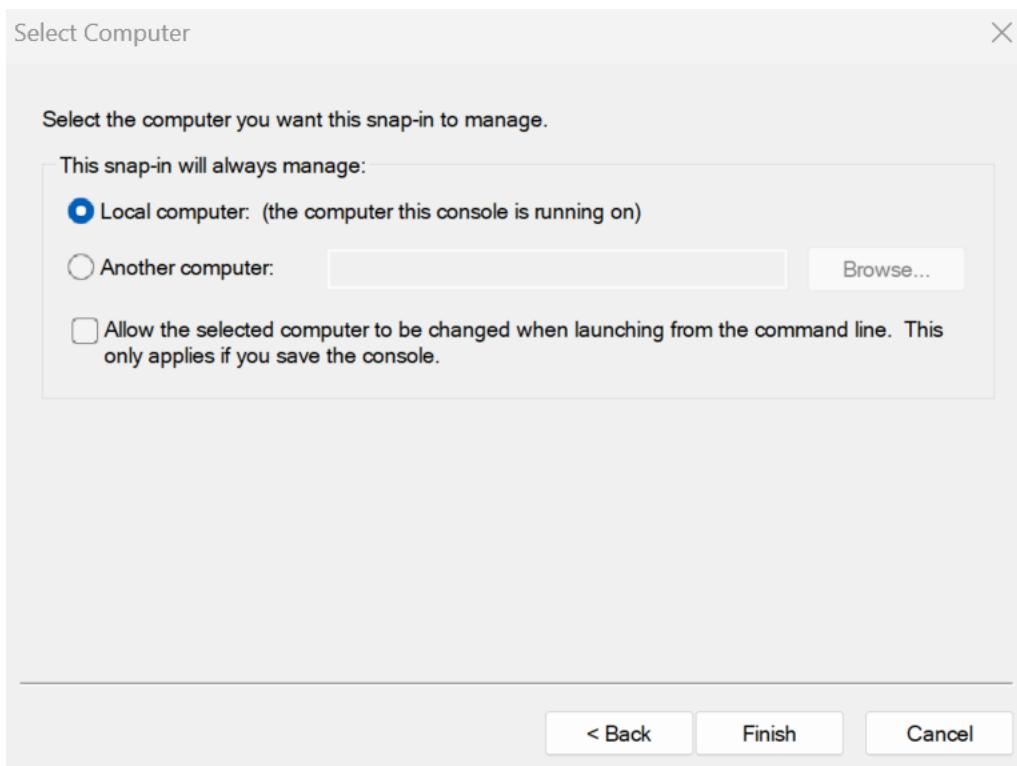


Select Certificates, click Add, and choose Computer Account to manage device-level certificates.

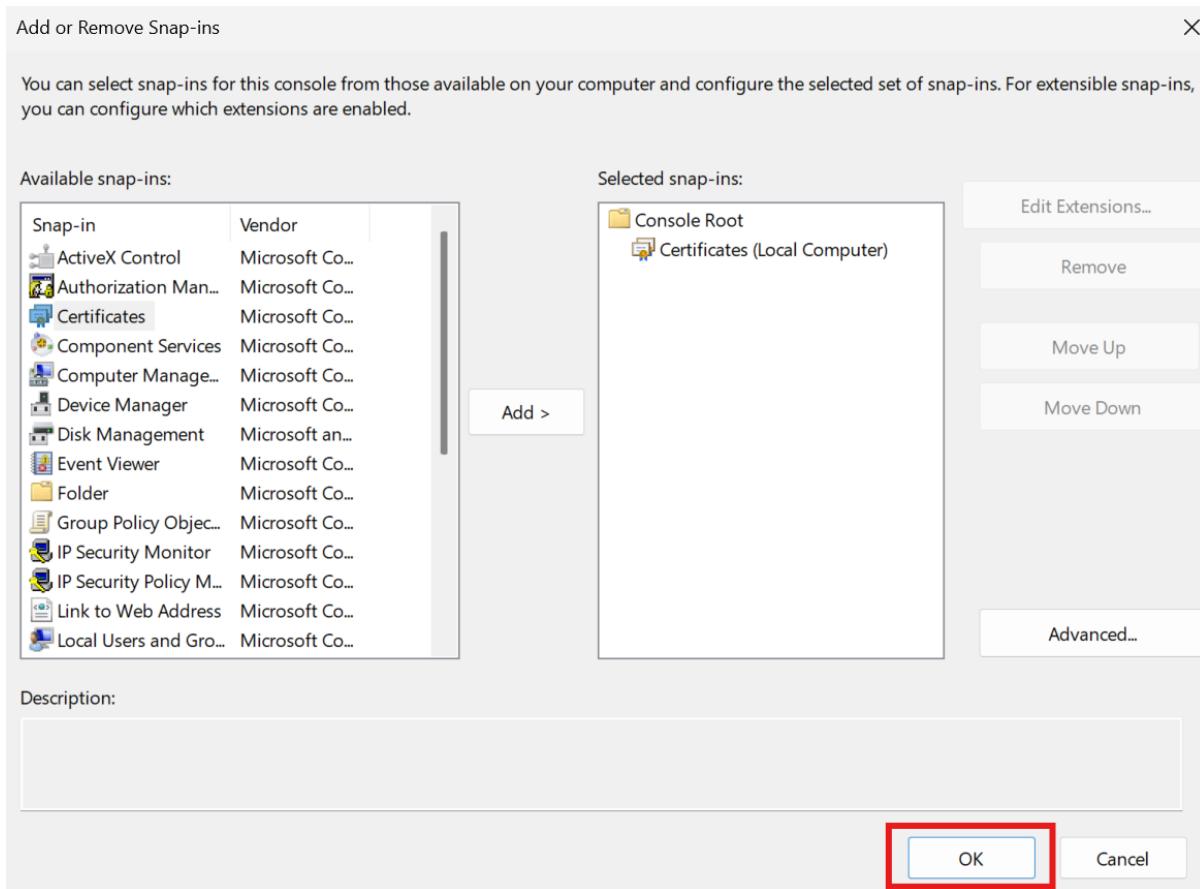




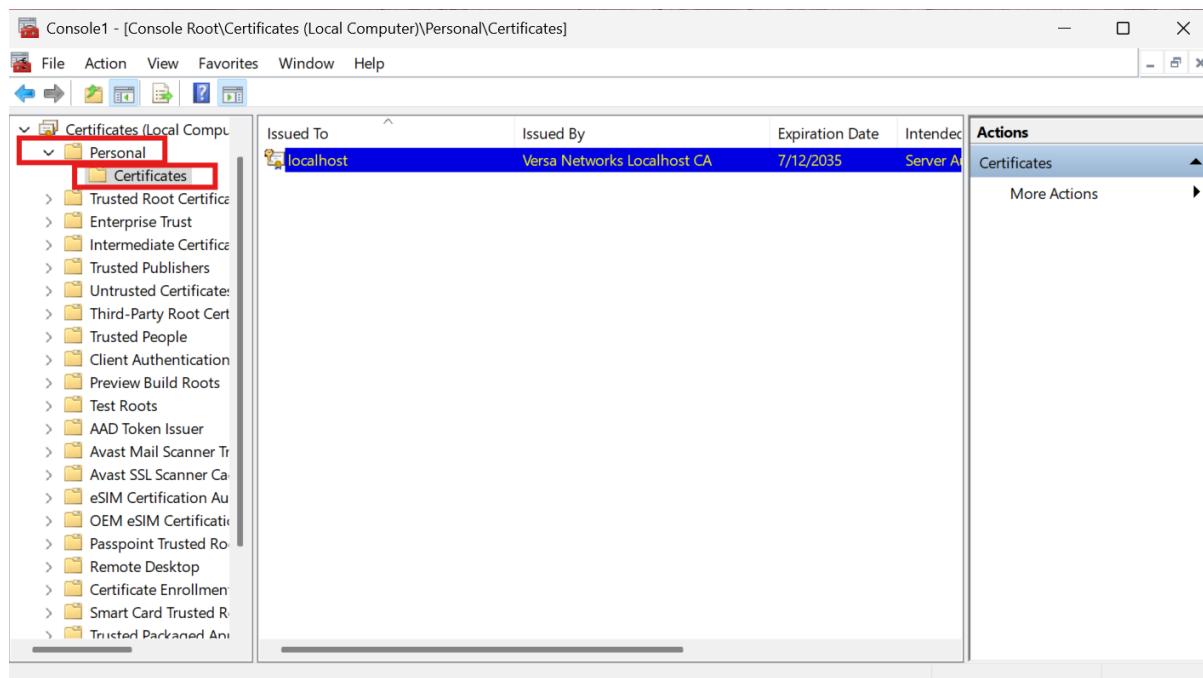
Choose Local Computer and Finish.



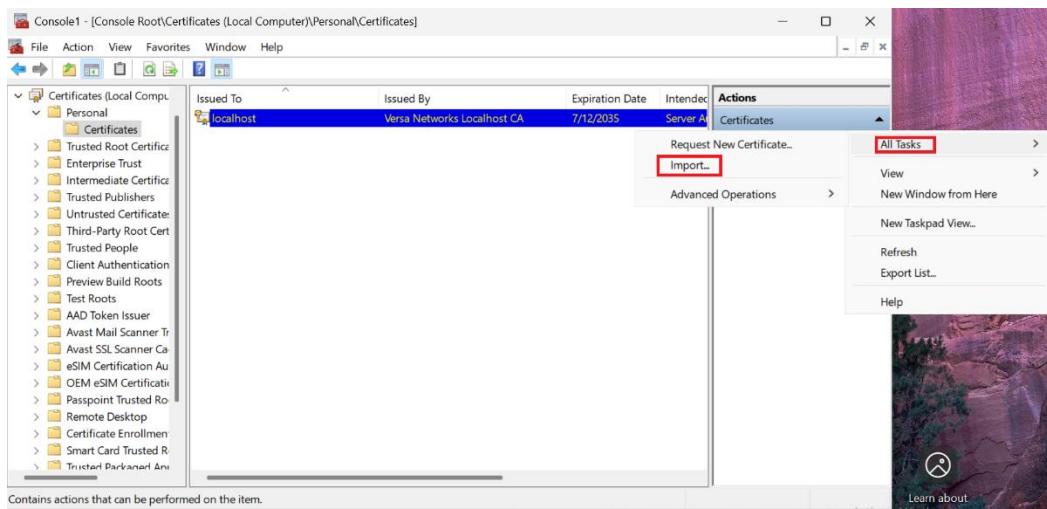
Then OK.



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**.

X

 Certificate Import Wizard

Welcome to the Certificate Import Wizard

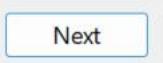
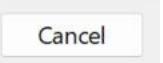
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

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.

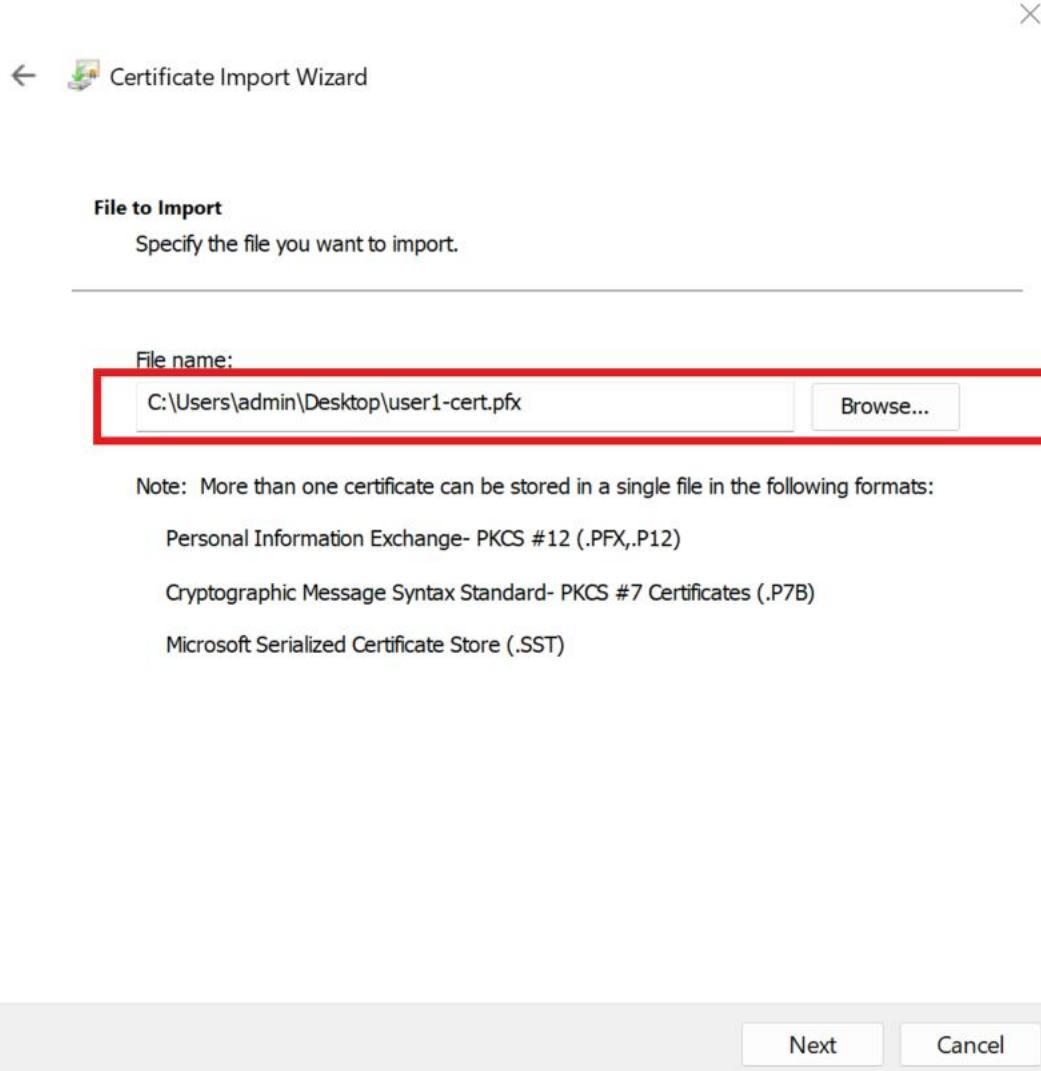
Store Location

Current User
 Local Machine

To continue, click **Next**.

 Next Cancel

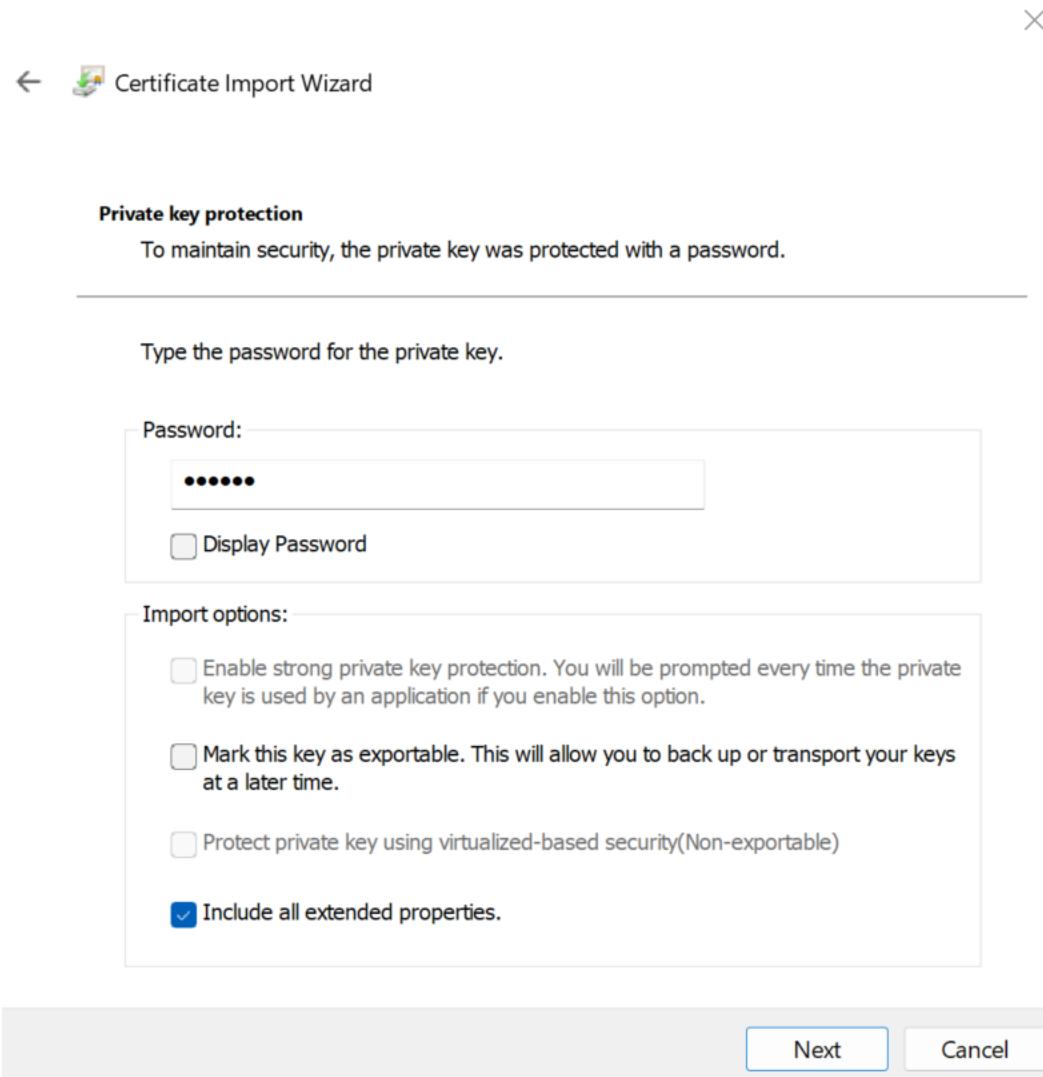
Browse to the location of the certificate file (for example user1-cert.pfx), select it, and click **Open**



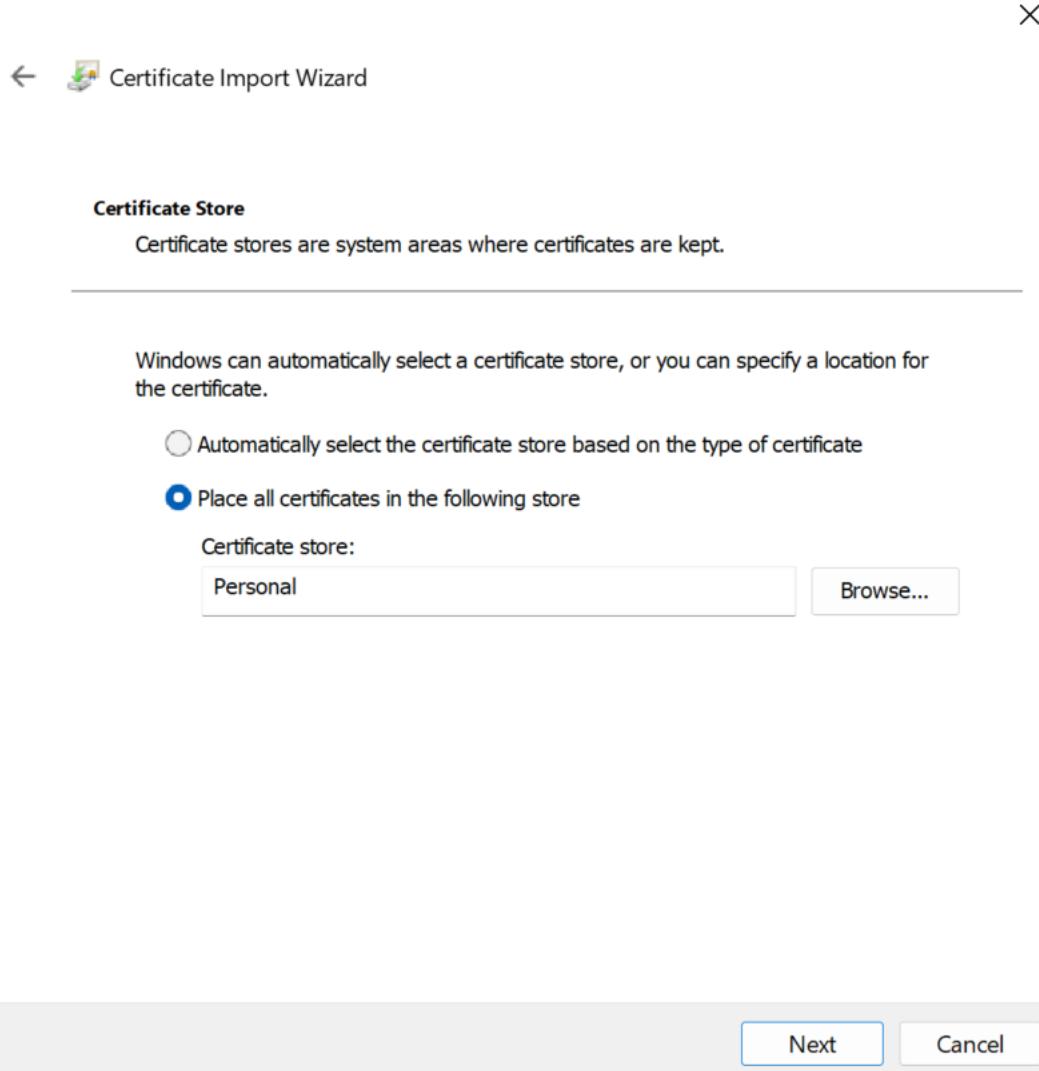
Enter the certificate's private key password.

- 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.



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



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



Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

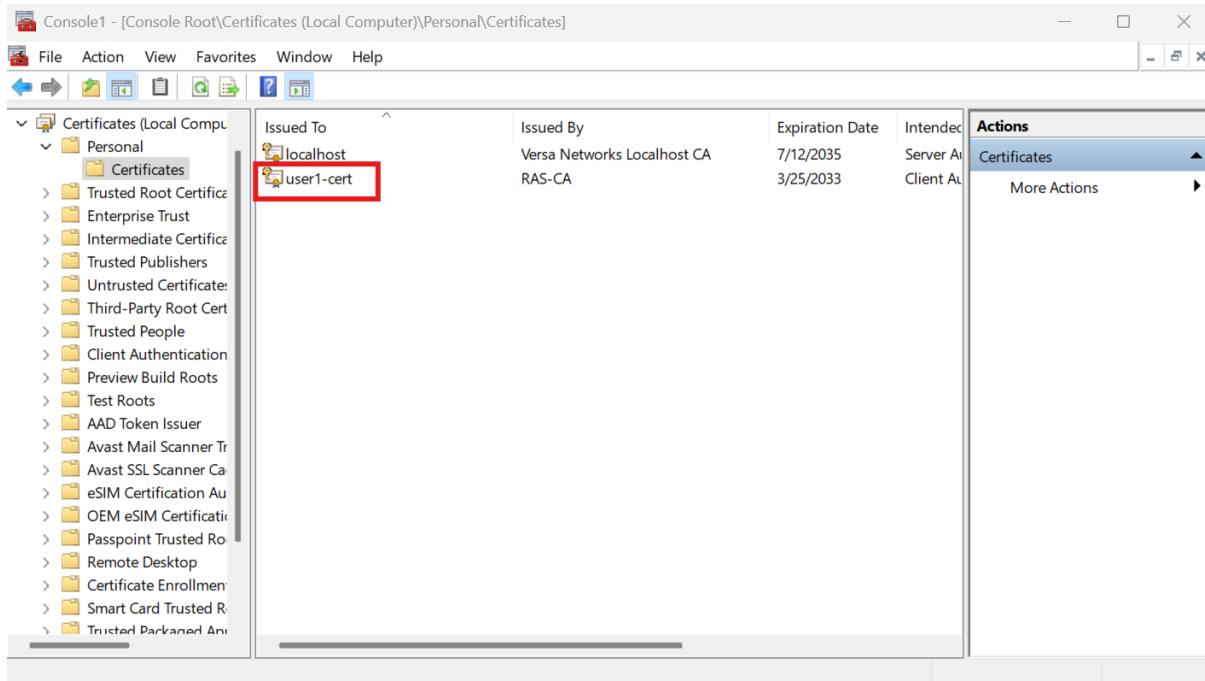
| | |
|------------------------------------|---------------------------------------|
| Certificate Store Selected by User | Personal |
| Content | PFX |
| File Name | C:\Users\admin\Desktop\user1-cert.pfx |

Finish

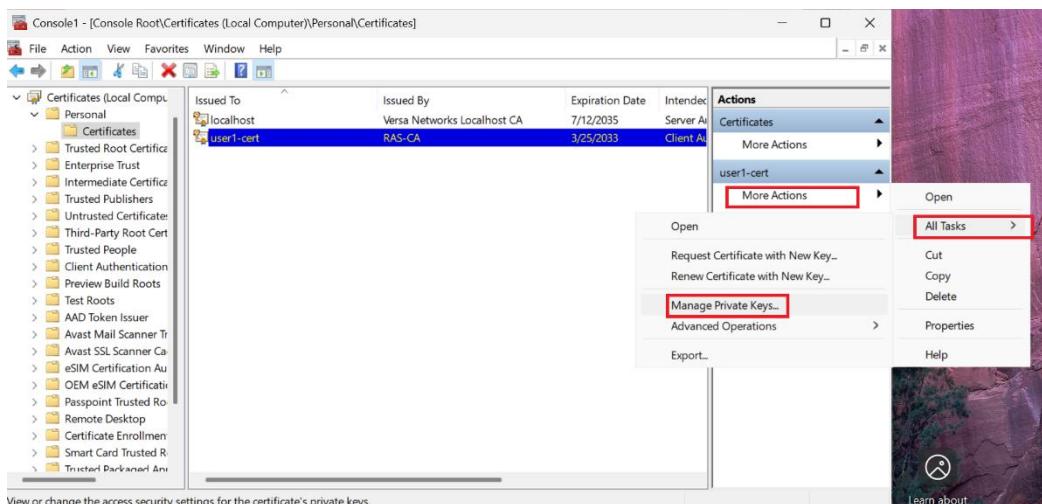
Cancel

Verify that the imported certificate is visible under:

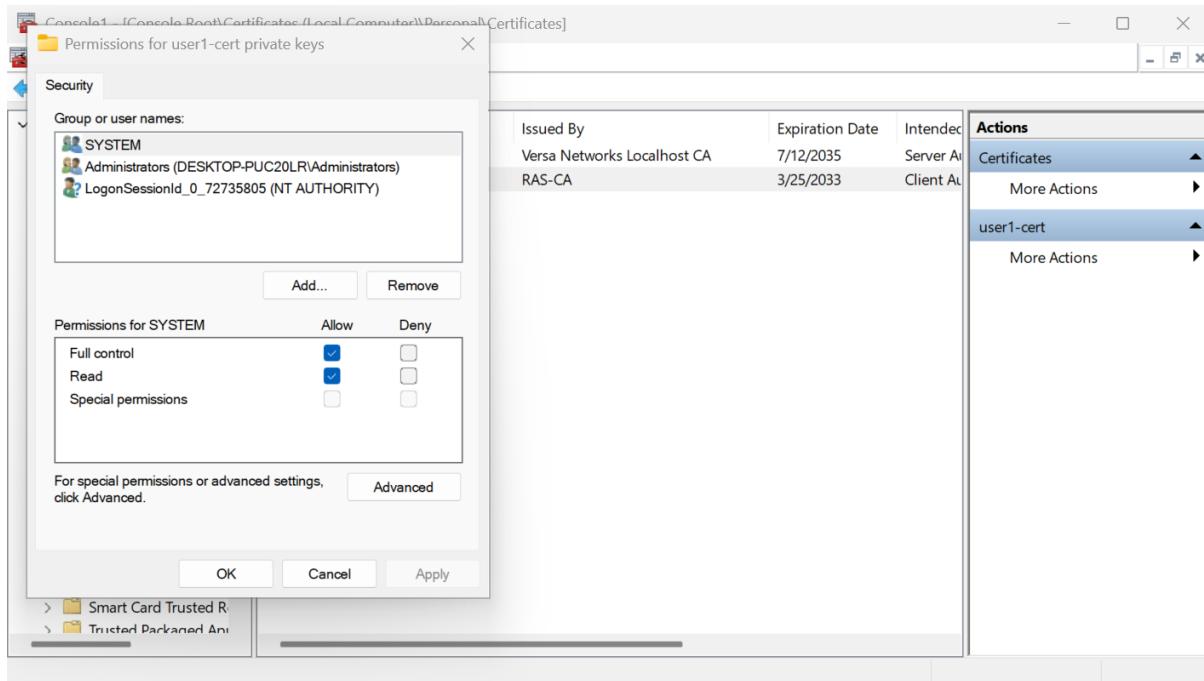
Certificates (Local Computer) > Personal > Certificates.



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**.



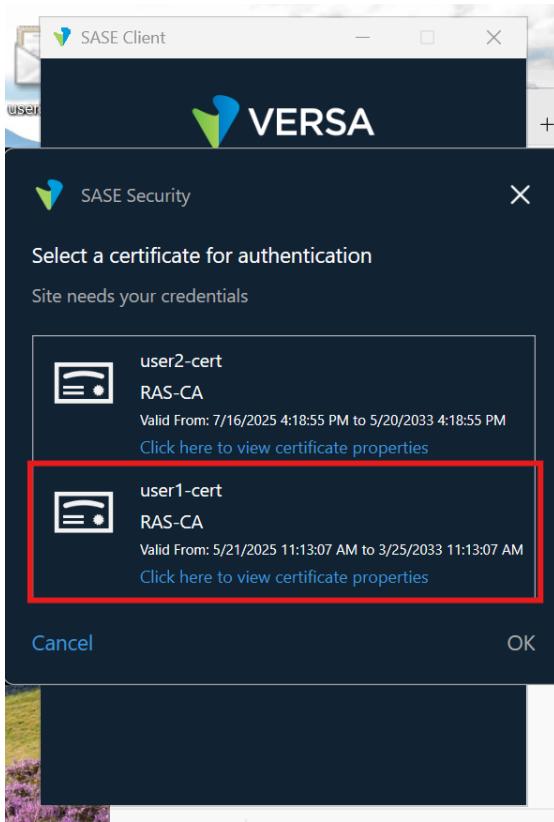
Assign permissions for users.



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:

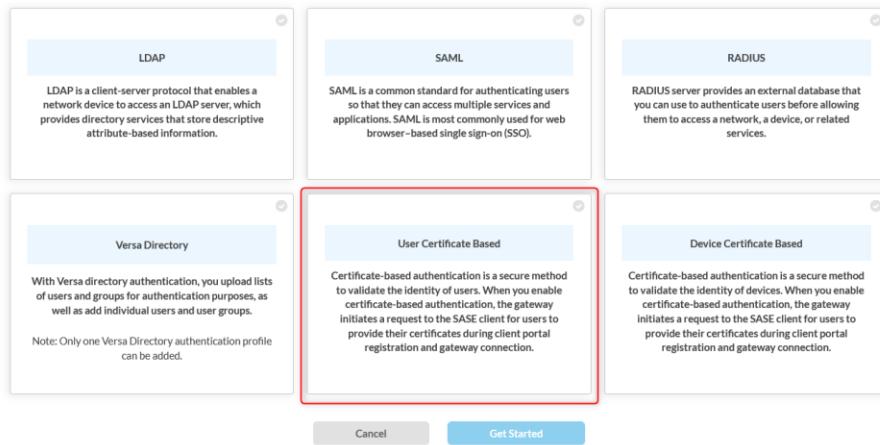
Configure > Security Service Edge > User and Device Authentication > Profiles then "+ Add"

| 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, 2:01:18 PM Administrator |
| SAML | | | 8/8/2025, 4:51:03 PM Administrator |

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.

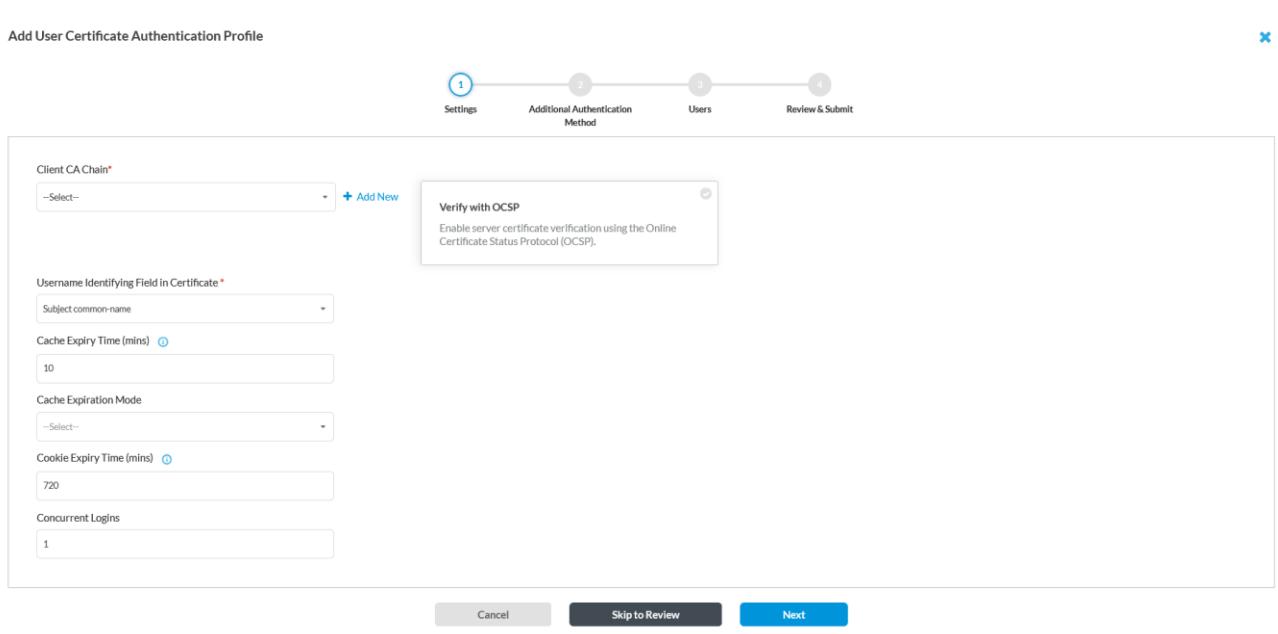


In Add User Certificate Authentication Profile > Settings:

- **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



Client CA Chain*

Verify with OCSP

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

Username Identifying Field in Certificate*

Subject common-name

Cache Expiry Time (mins)

10

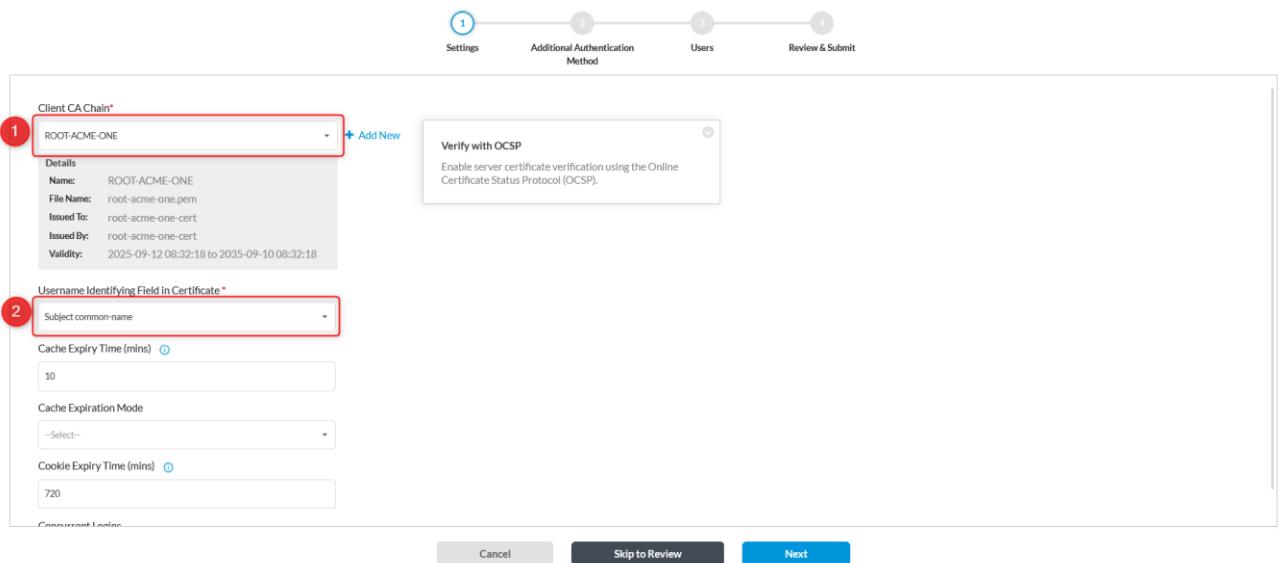
Cache Expiration Mode

Concurrent Logins

1

Cancel Skip to Review Next

Add User Certificate Authentication Profile



Client CA Chain*

1 ROOT-ACME-ONE

Verify with OCSP

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

Username Identifying Field in Certificate*

2 Subject common-name

Cache Expiry Time (mins)

10

Cache Expiration Mode

Concurrent Logins

1

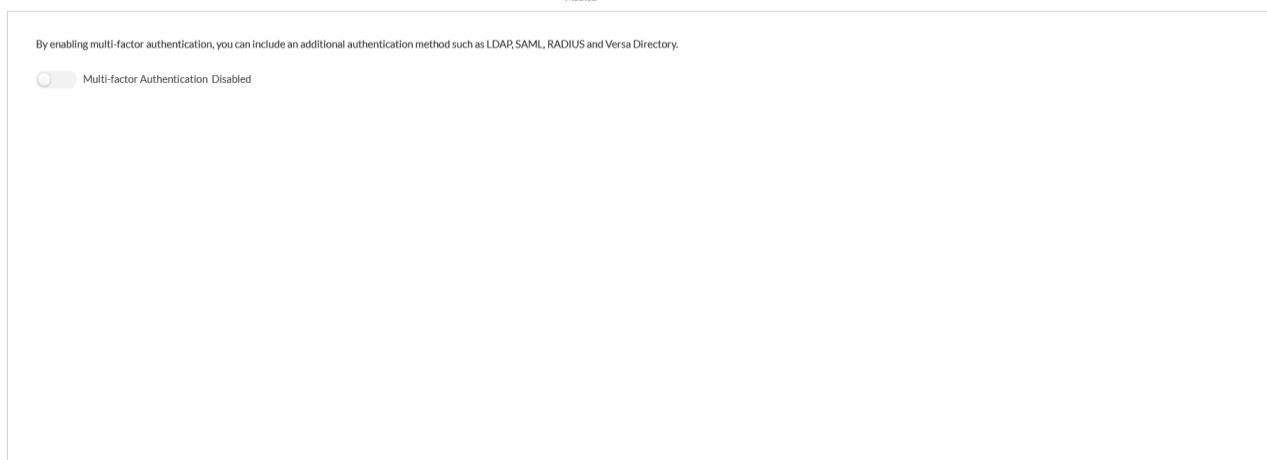
Cancel Skip to Review Next

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

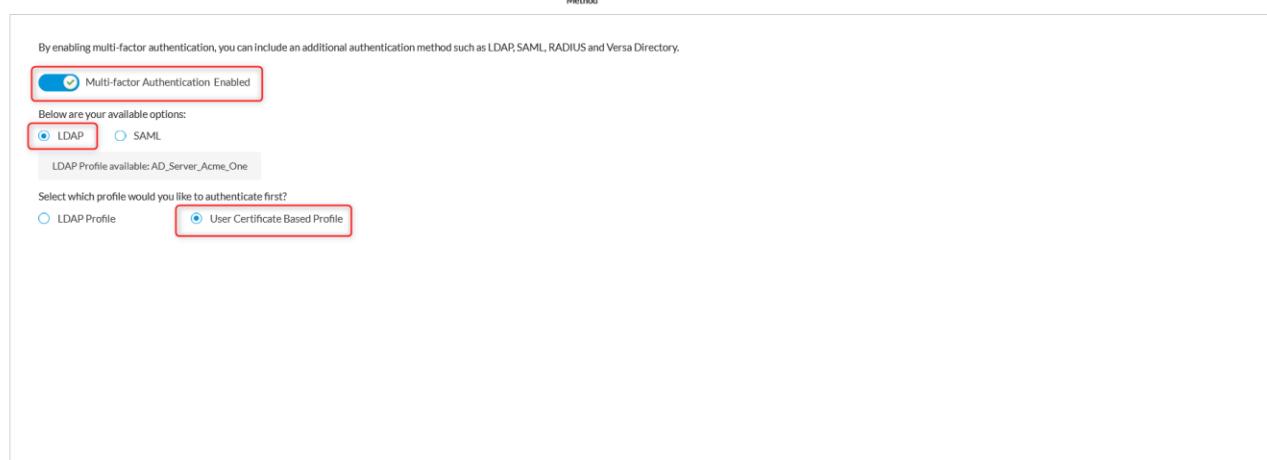


By enabling multi-factor authentication, you can include an additional authentication method such as LDAP, SAML, RADIUS and Versa Directory.

Multi-factor Authentication Disabled

[Cancel](#) [Back](#) [Skip to Review](#) [Next](#)

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

[Cancel](#) [Back](#) [Skip to Review](#) [Next](#)

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

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

General

Name: **User_Certificate**

Tags: Press Enter to add

Settings

Client CA Chain: device-auth-ca-chain

Username Identifying Field in Certificate: subject

Verify with OCSP: Disabled

Is CA Server on Internet?: No

VPN Name: ACME-ONE-Enterprise

Cache Expiry Time (mins): 10

Cache Expiration Mode: Standard

Concurrent Logins: 1

Cookie Expiry Time (mins): 720

Additional Authentication Method

Multi-factor Authentication: Enabled

Profile to authenticate first: Ldap Profile

Cache Expiry Time (mins): 10

Cancel Back **Save**

Add Device Certificate Authentication Profile

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

General

Name: **Device_Authentication**

Tags: Press Enter to add

Settings

Client CA Chain: device auth-ca-chain

Username Identifying Field in Certificate: subject

Verify with OCSP: Disabled

Is CA Server on Internet?: No

VPN Name: ACME-ONE-Enterprise

Cache Expiry Time (mins): 10

Cache Expiration Mode: Standard

Concurrent Logins: 1

Cookie Expiry Time (mins): 720

Authentication Order

Profile to authenticate first: Device

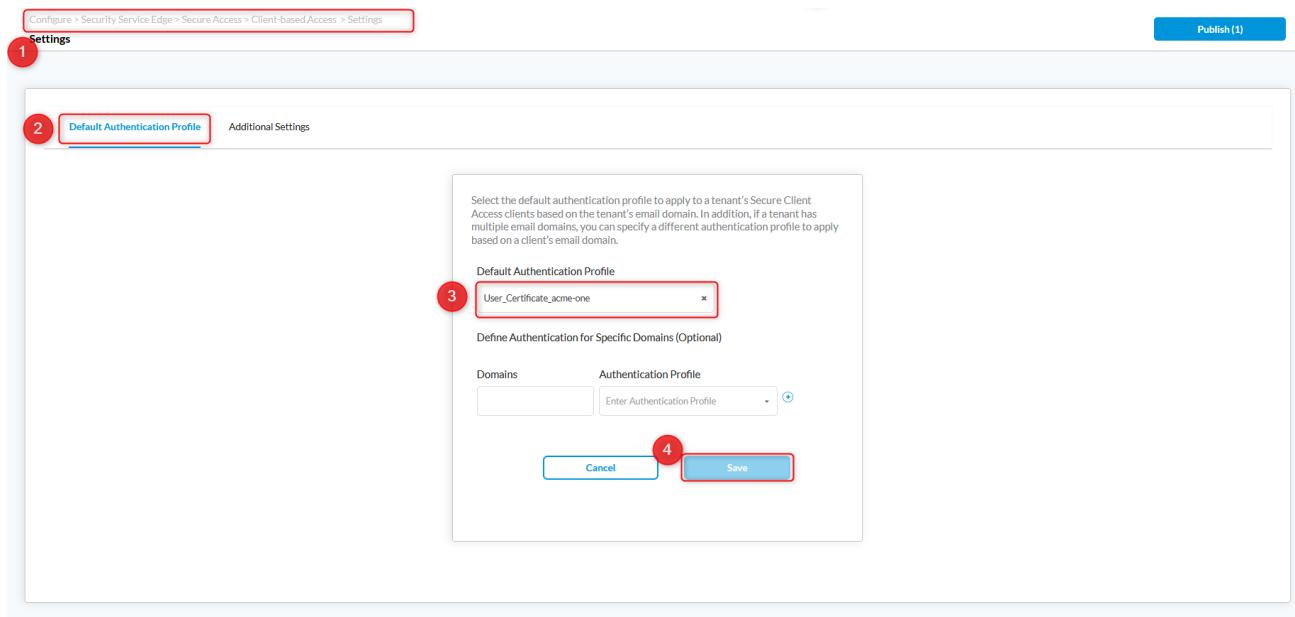
Cancel Back **Save**

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.



Installing Certificates on the Client Device:

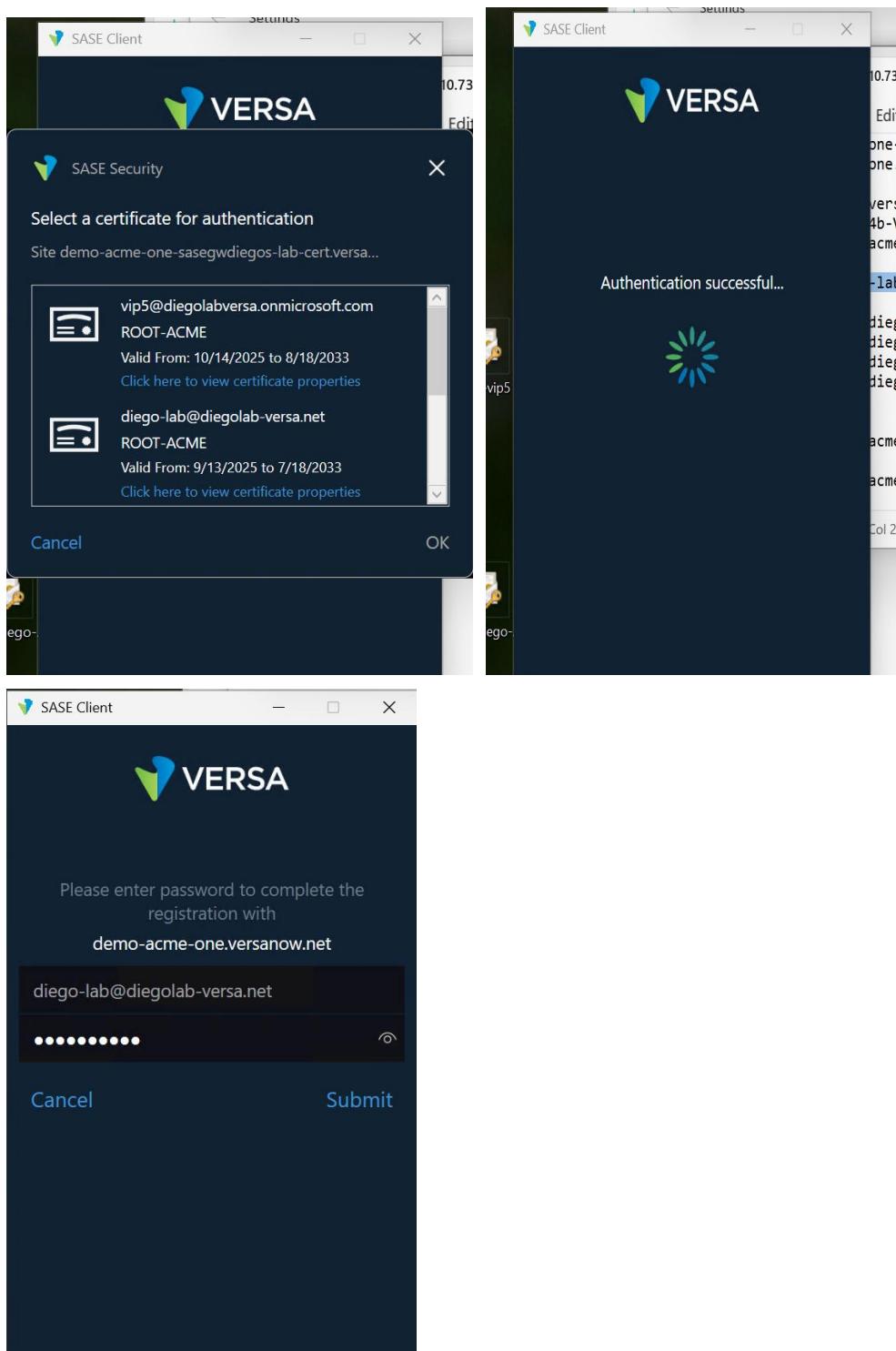
The installation process for user certificates on client devices follows the same procedure described in the **Device Certificate Authentication** section. The certificate must be imported into the appropriate certificate store on the client machine.

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](#).