Configuring Authentication Profiles on the SSE Gateway

About This Document

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

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

Document Information

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

Disclaimer

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

Before you begin

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

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

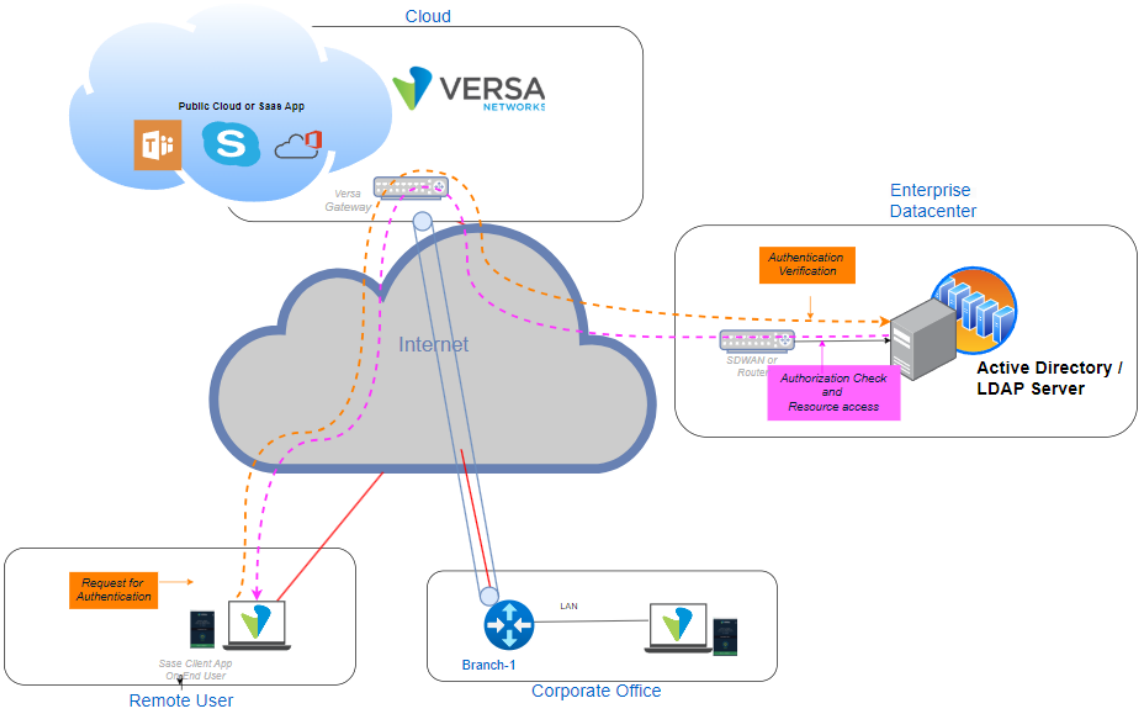
LDAP Active-Directory

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

Scenario

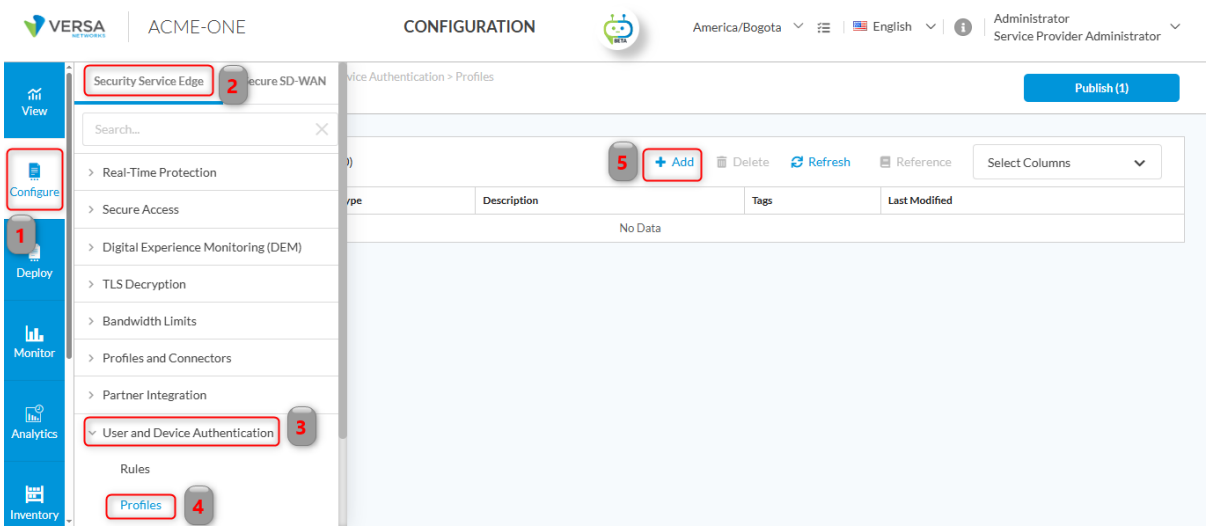
In most enterprise environments, user authentication is centralized through AD/LDAP servers in the data centre. In cases of VSPA or VISA, users securely connect to the SSE gateways using the Versa SASE Client from remote locations, branches, or corporate offices. Authentication requests from the SASE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

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

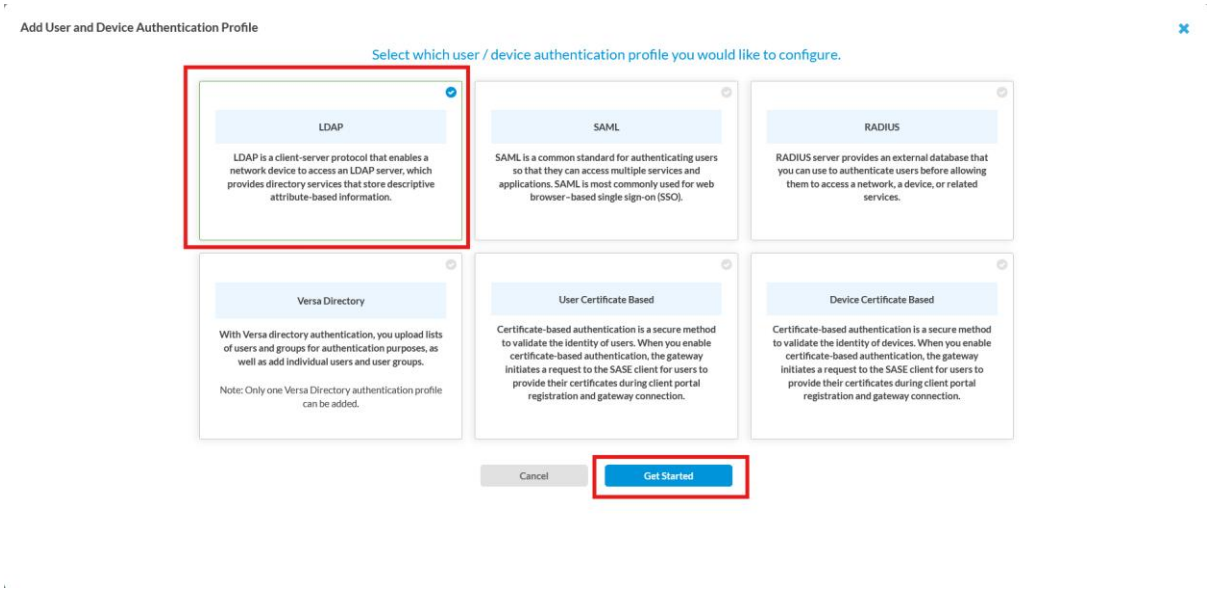


Navigate to User and Device Authentication Configuration

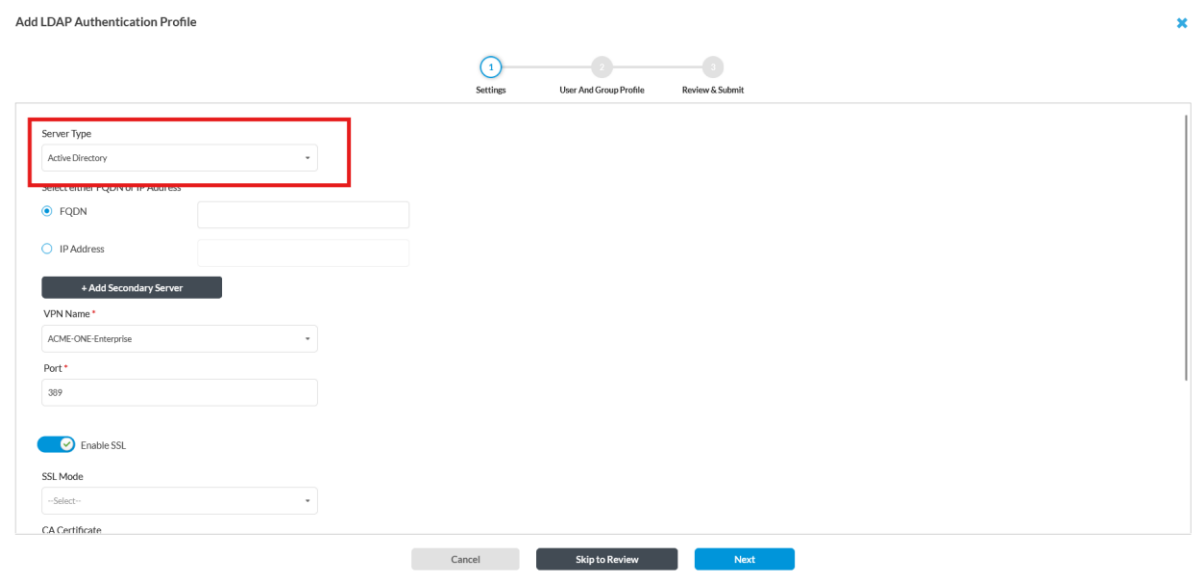
Go to: Configure > Security Service Edge > User and Device Authentication > Profiles then "+ Add"



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



From the Server Type dropdown, select Active Directory

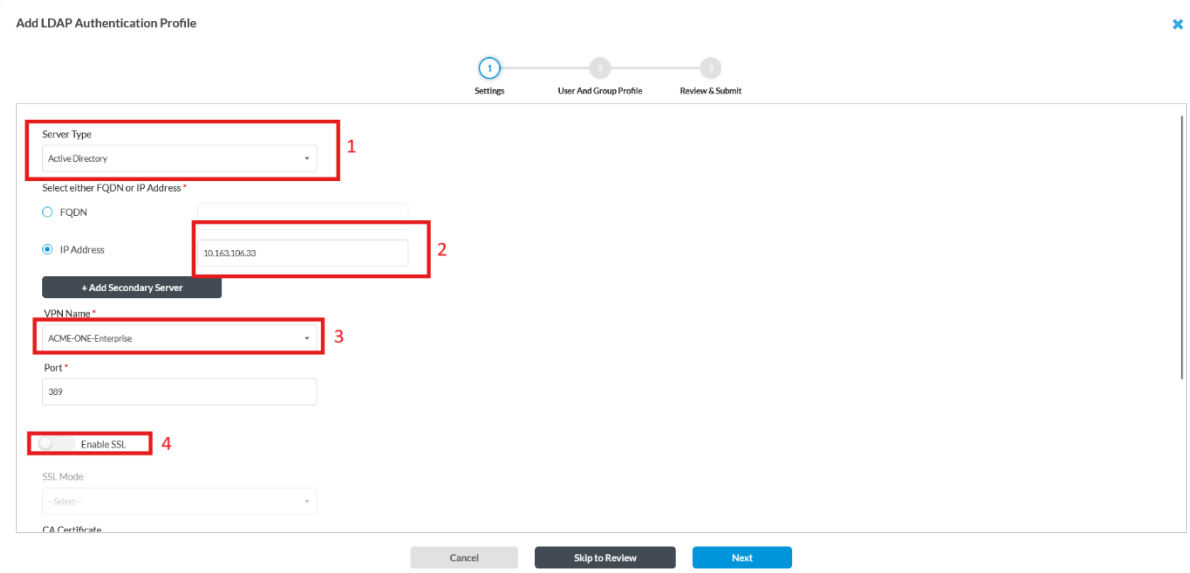


The following section explains all parameters for LDAP Authentication Profile configuration.

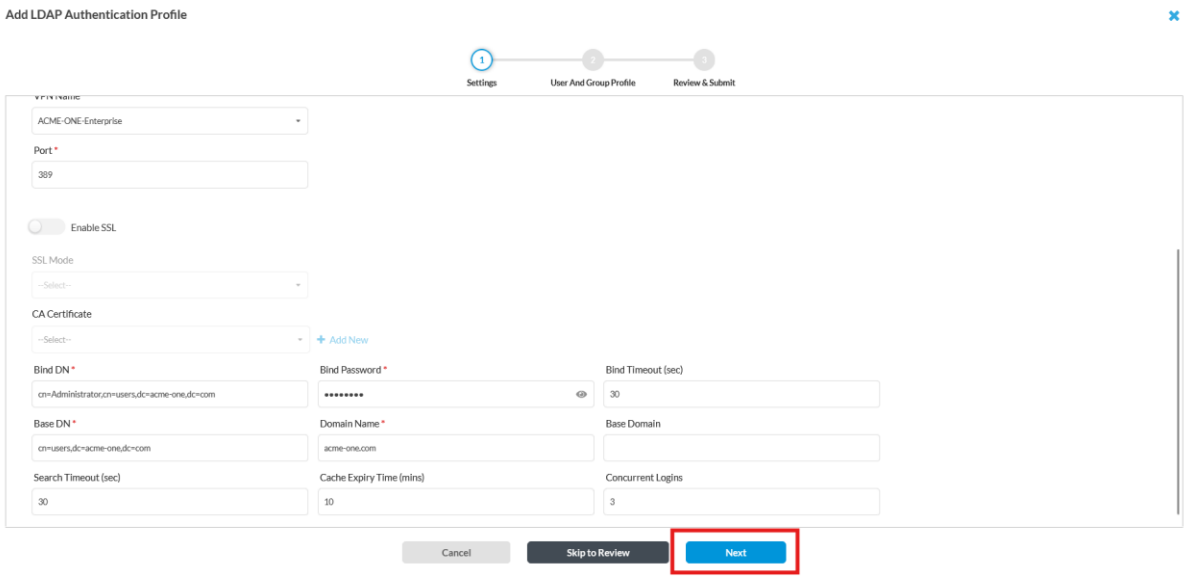
LDAP Authentication Profile – Parameters		
Parameter	**Description**	**Current Use Case**
Server Type	It indicates that the authentication source is Microsoft Active Directory or Open-LDAP.	active directory
FQDN or IP Address	The Fully Qualified Domain Name (FQDN) or IP address of the AD/LDAP server.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

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

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



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



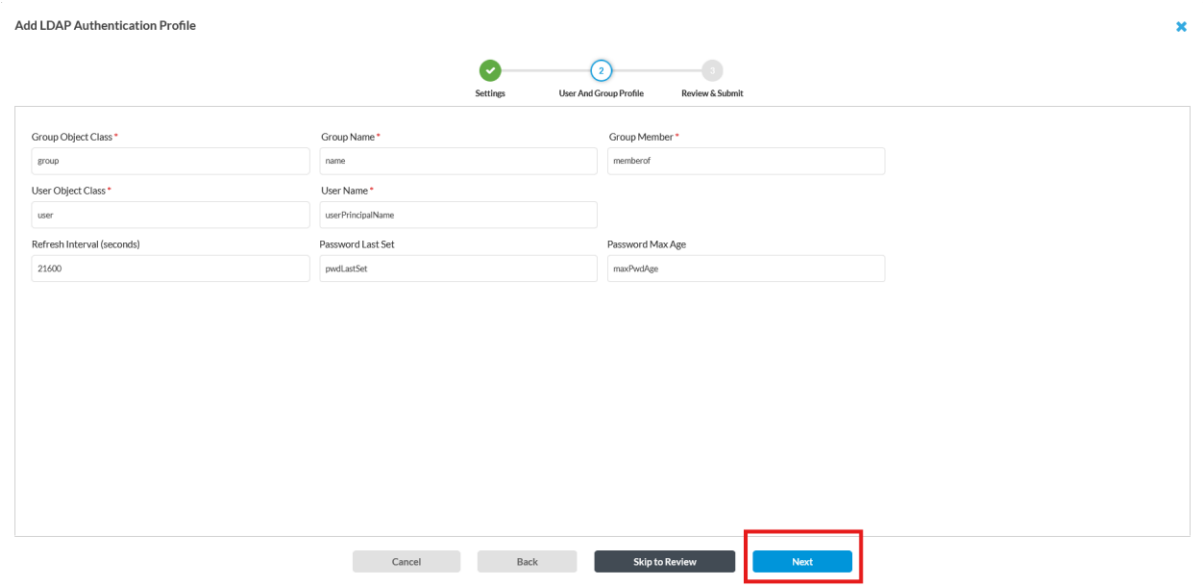
Next, complete the required fields:

LDAP Object and User Attributes

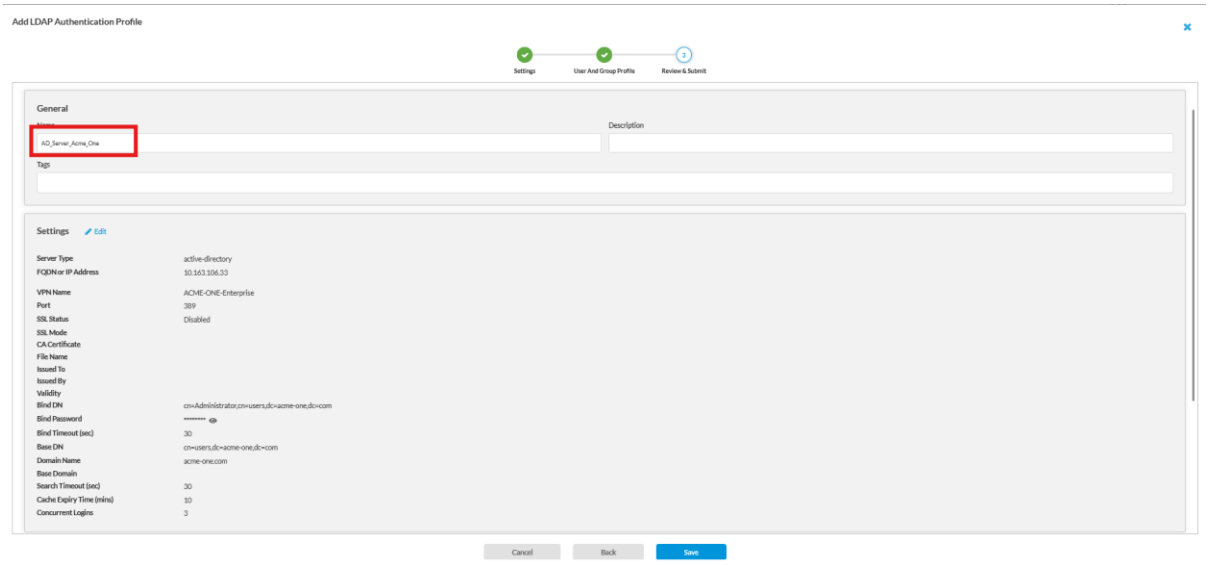
Parameter	Value / Default	Description
Group Object Class	group	Standard AD object class for security and distribution groups. Required to identify groups in the directory.

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.

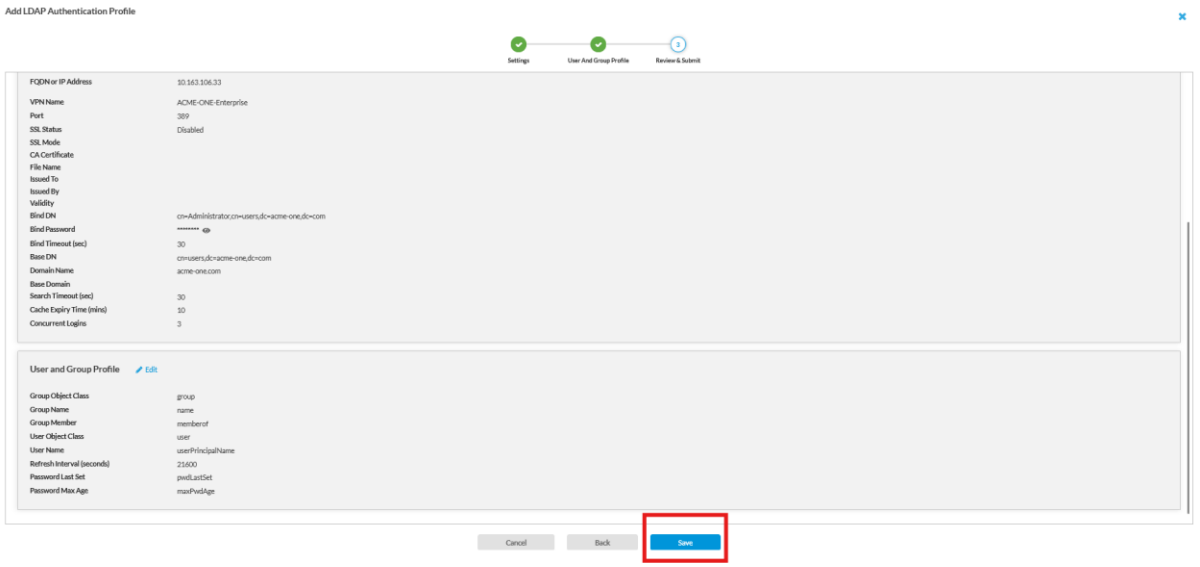
click **Next** to proceed.



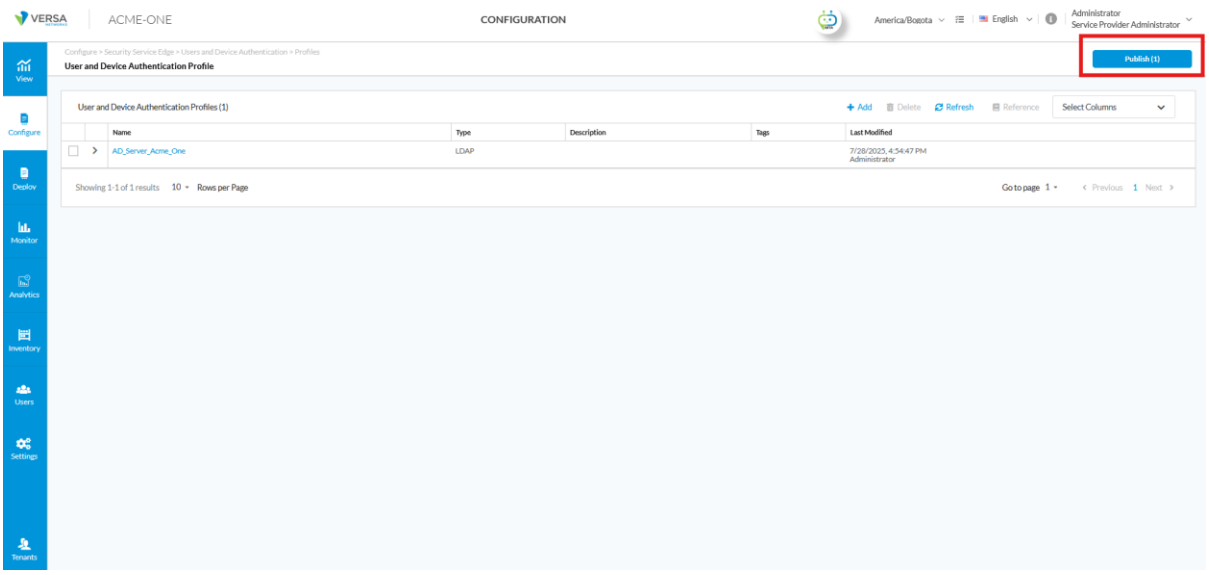
Next, fill in the **Name** field with a descriptive reference, such as *AD_Server_ACME-ONE*, and review all parameters to ensure they are correctly configured.



Then **Save.**



Go to **Publish**.



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

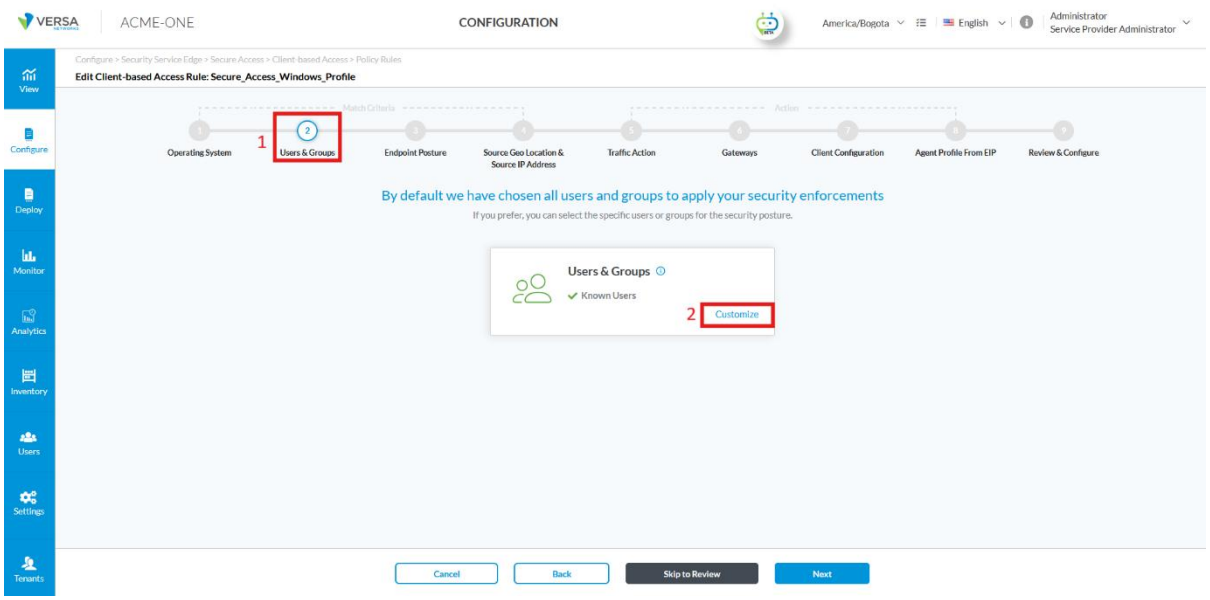
Verification

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

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

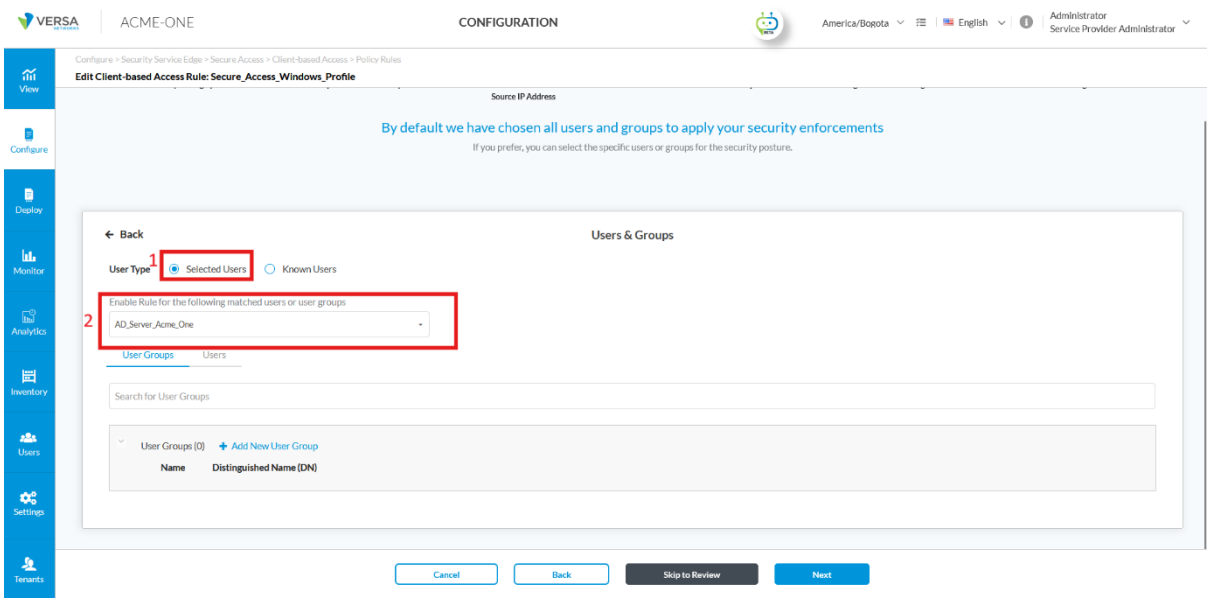
Click "**+ Add**" to create a new Secure Access Client rule or edit an existing rule.

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

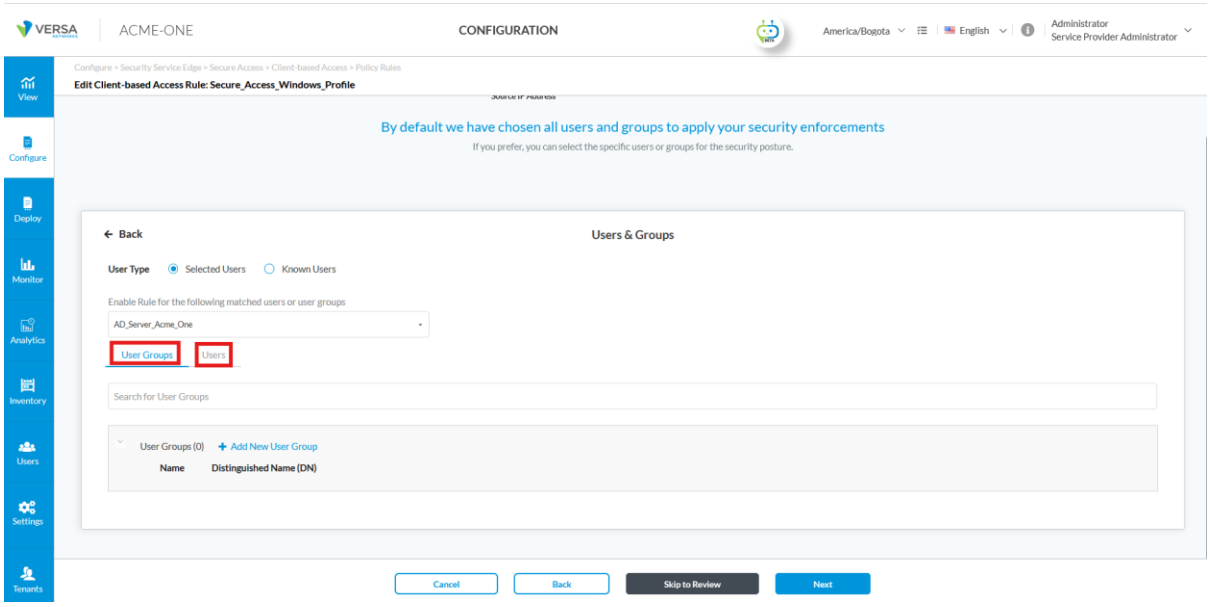


In the **Users & Groups** customization panel, select **Selected Users** as the user type. Then, under **Enable Rule for the following matched users or user groups**, choose the appropriate authentication profile (Example., AD_Server_Acme_One). This allows the policy to enforce access control based on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

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



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



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

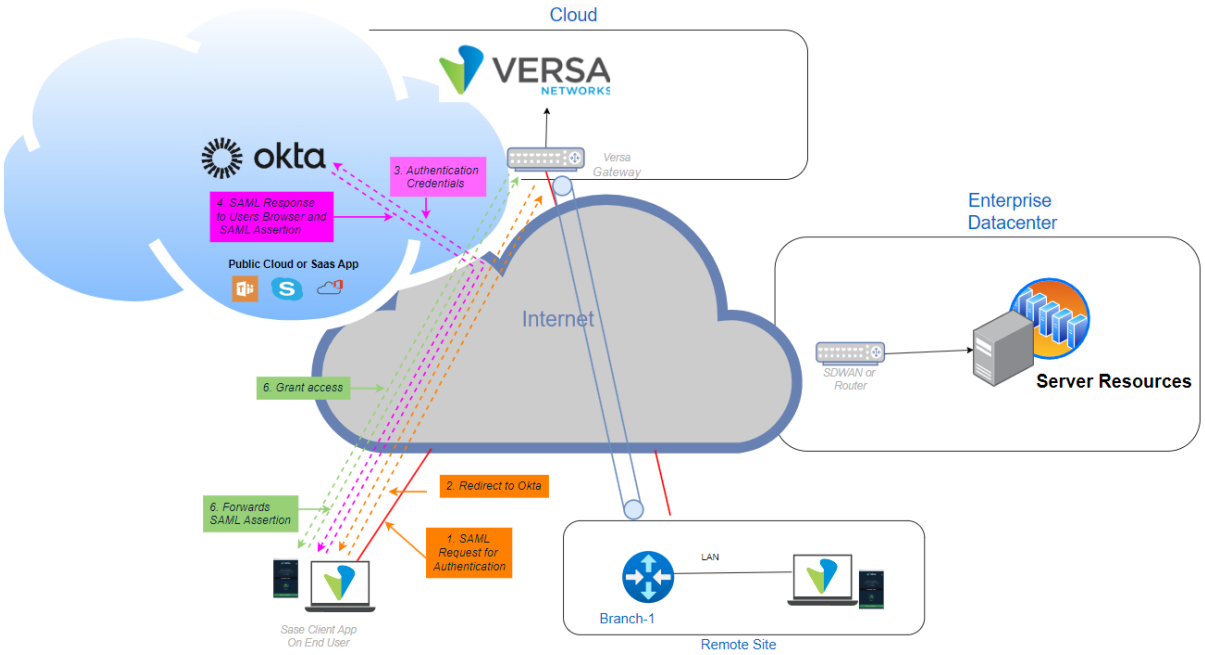
SAML Authentication

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

OKTA

Scenario

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



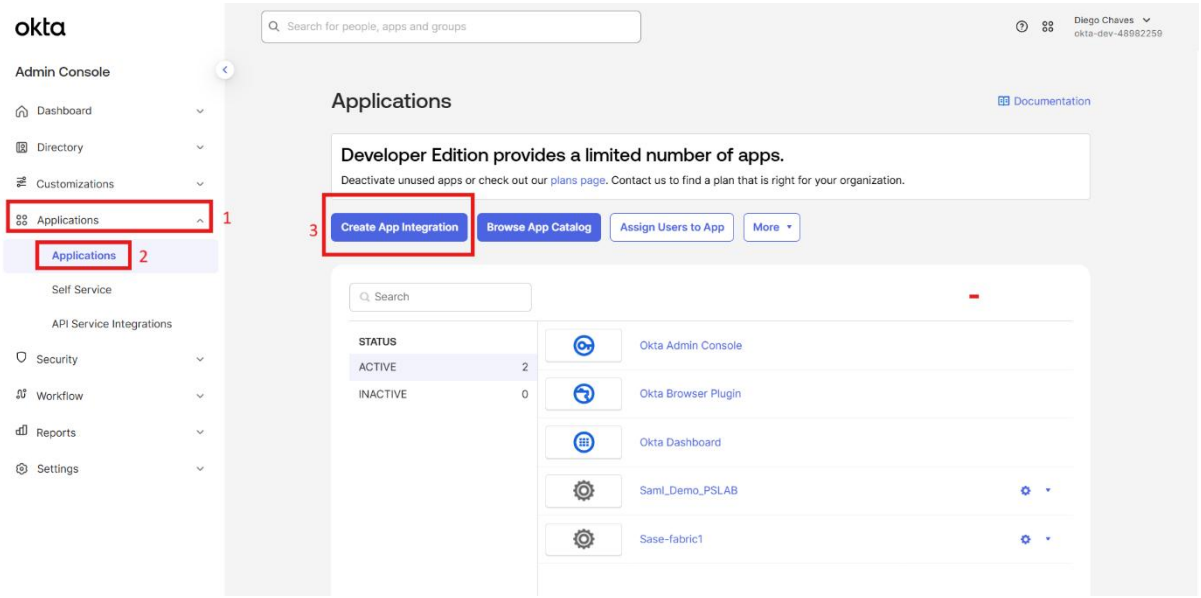
OKTA Portal Configuration

Create an Application in the OKTA portal.

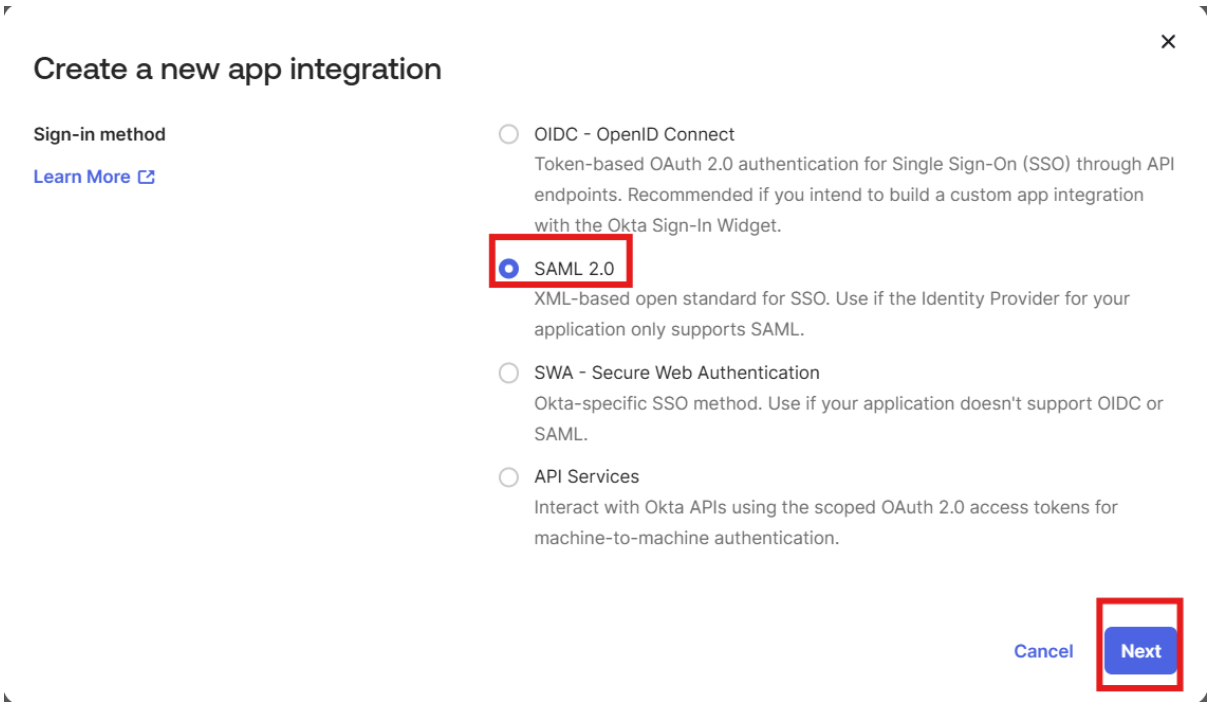
- Create an application on Okta.
- Add users to the application.

1. login to your OKTA admin console.

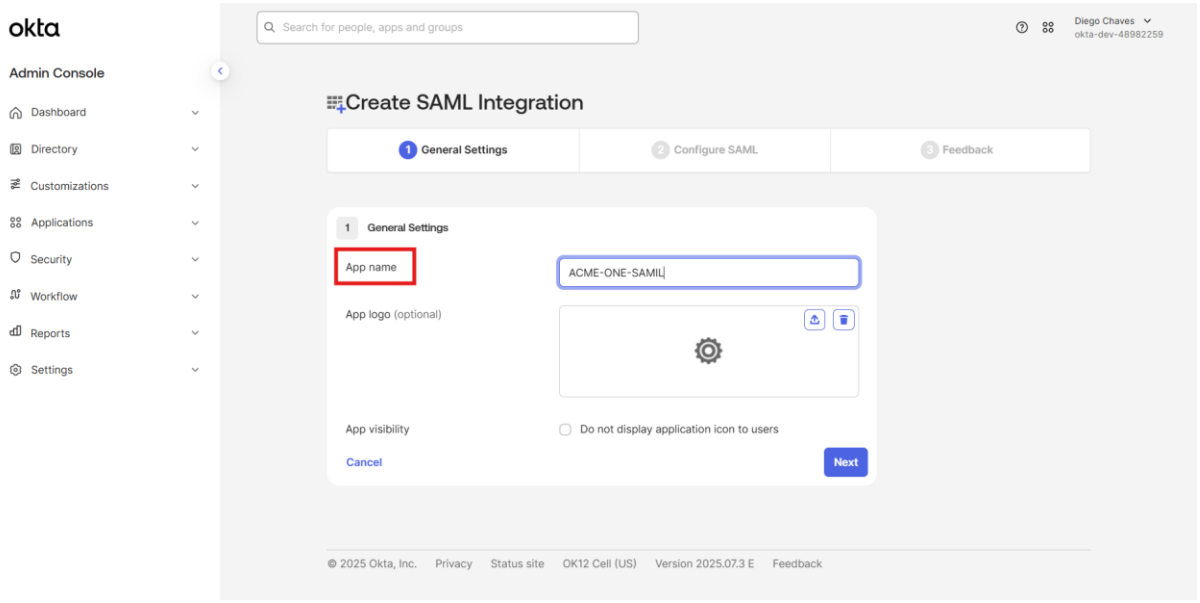
   Navigate to: Application then Click on Applications >> Create App Integration.



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



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



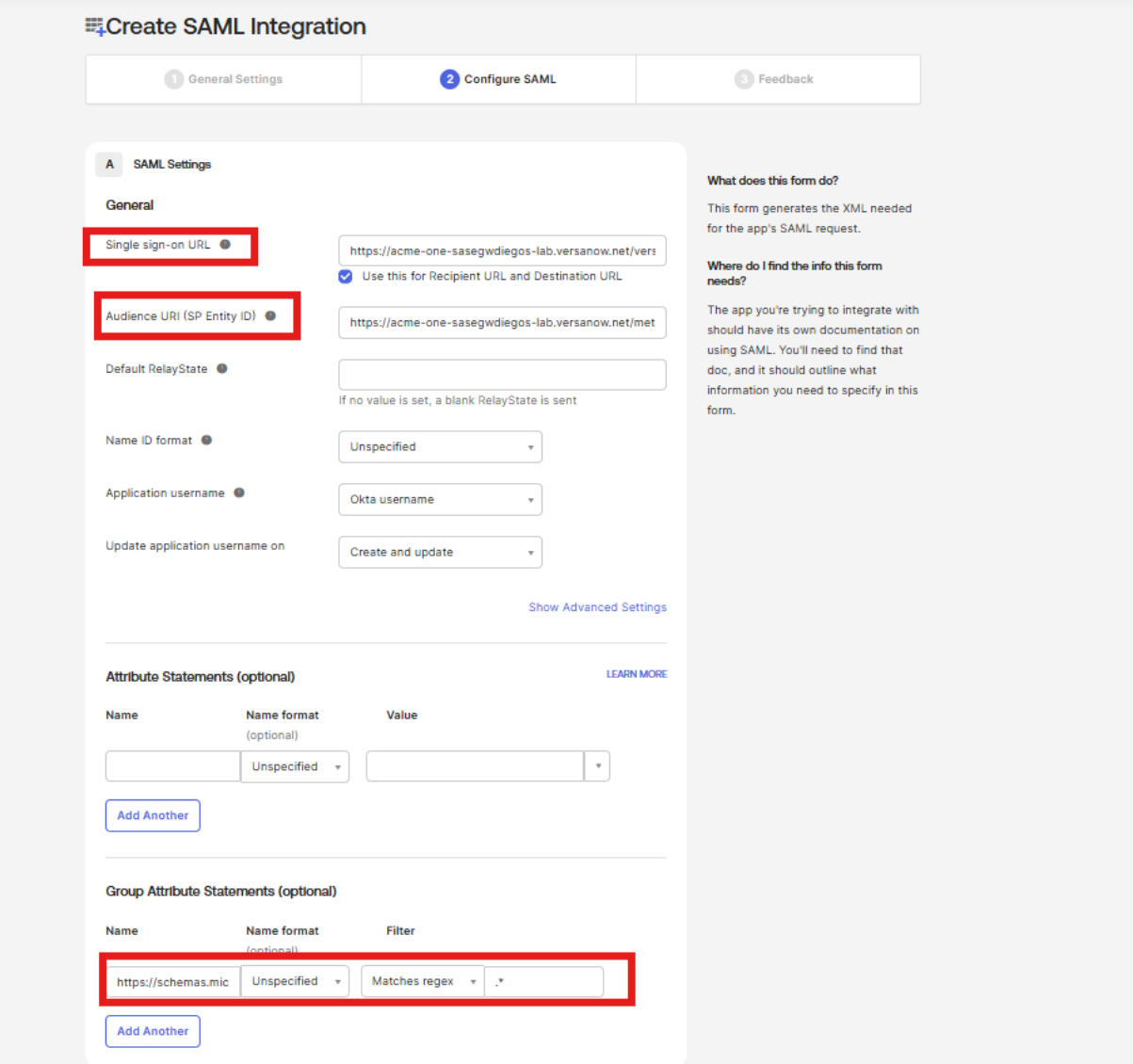
- Define custom attributes.

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

Field	Description
Single Sign-On URL	URL where Okta sends SAML responses. Format: https://<SASE-GW-FQDN>/versa-flexvnf/saml/login-consumer. Example: https://acme-one-sasegwdiegos-lab.versanow.net/versa-flexvnf/saml/login-consumer
Audience URI (SP Entity ID)	Service Provider (SP) entity ID: Format: https://<SASE-GW-FQDN>/metadata. Example: https://acme-one-sasegwdiegos-lab.versanow.net/metadata
Default Relay State	Used for IdP-initiated SSO:- System user: vd-ui::system Tenant user: vd-ui::<organization-name>
Attribute Statements	Define attributes such as role, organisation, and idle timeout. *(Case-sensitive)*
Group Attribute Statements (optional)	Enables Versa to import user-to-group mappings from Okta Configuration: - Name: https://schemas.microsoft.com/ws/2008/06/identity/claims/groups Name format: *Unspecified* Filter: Regex (.*) This ensures all groups a user belongs to are included in the SAML assertion, enabling group-based policies (Internet Protection, Private App Protection, etc.).
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-577374553241106028824600913 9" IssueInstant="2025-08-08T17:10:21.828Z" Version="2.0"
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
    <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"/>
    <saml2:Subject>
        <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">userName</saml2:NameID>
        <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml2:SubjectConfirmationData NotOnOrAfter="2025-08-08T17:15:22.008Z" Recipient="https://acme-one-sasegwdiegos-lab.versanow.net/versa-flexvnf/saml/login-consumer"/>
        </saml2:SubjectConfirmation>
    </saml2:Subject>
    <saml2:Conditions NotBefore="2025-08-08T17:05:22.008Z" NotOnOrAfter="2025-08-08T17:15:22.008Z">
        <saml2:AudienceRestriction>
            <saml2:Audience>https://acme-one-sasegwdiegos-lab.versanow.net/metadata</saml2:Audience>
        </saml2:AudienceRestriction>
    </saml2:Conditions>
    <saml2:AuthnStatement AuthnInstant="2025-08-08T17:10:21.828Z">
        <saml2:AuthnContext>
            <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClassRef>
        </saml2:AuthnContext>
    </saml2:AuthnStatement>
    <saml2:AttributeStatement>
        <saml2:Attribute Name="https://schemas.microsoft.com/ws/2008/06/identity/claims/groups" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
            <saml2:AttributeValue
                xmlns:xs="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">GroupName Match Starts with ".*" (ignores case)
            </saml2:AttributeValue>
        </saml2:Attribute>
    </saml2:AttributeStatement>
</saml2:Assertion>
```

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

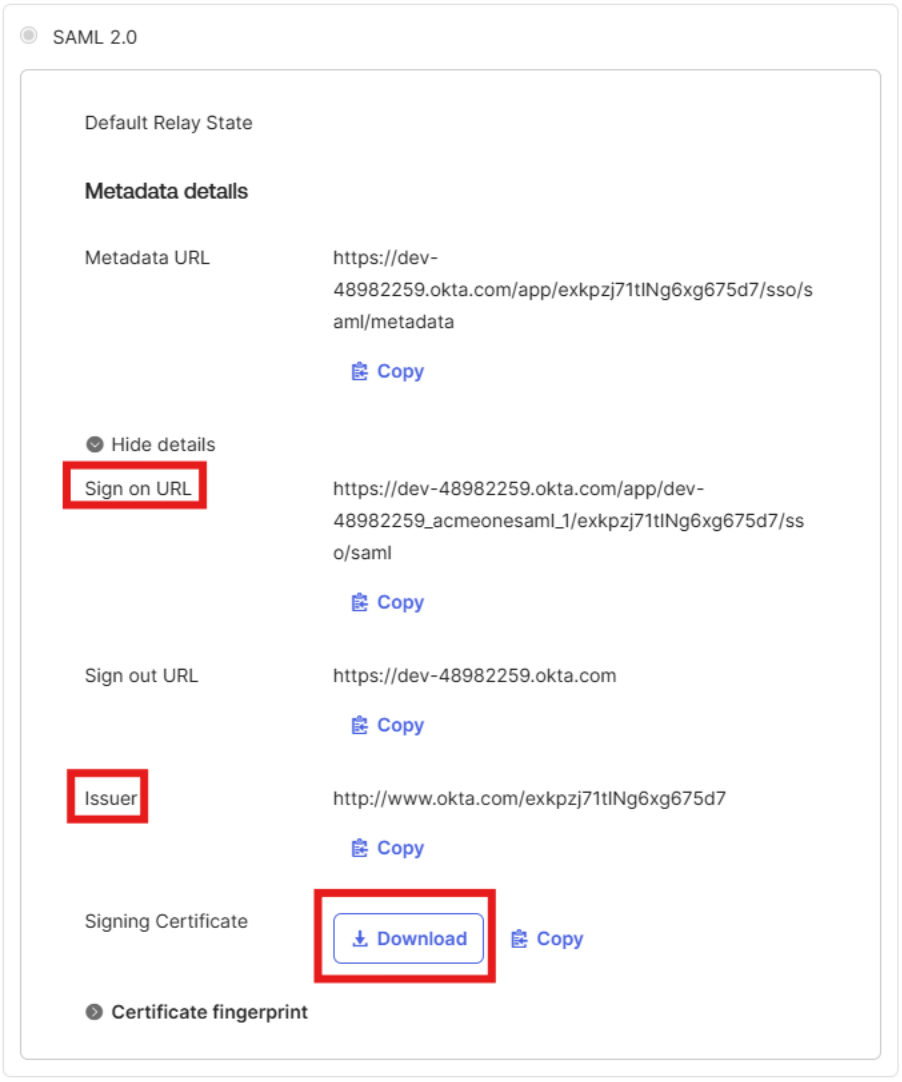


5. In the Help Okta Support understand how you configured this application section, you can provide optional information for Okta Support.

    - 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.

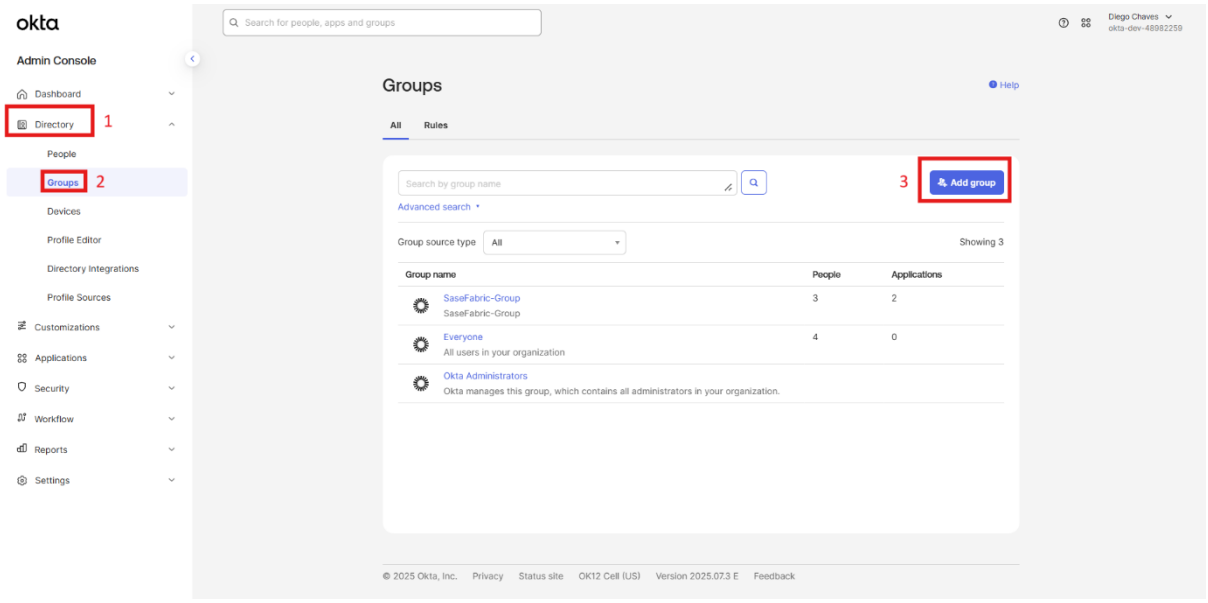
6. Retrieve SAML Integration Details

    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.

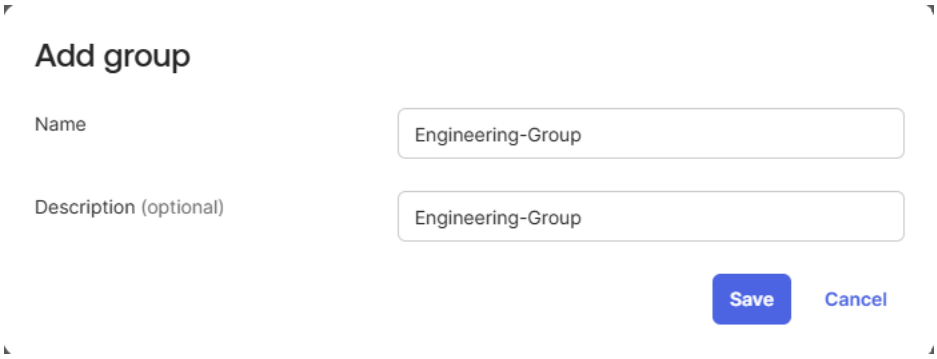


Note: Rename the downloaded certificate file from .cert to .crt before use

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

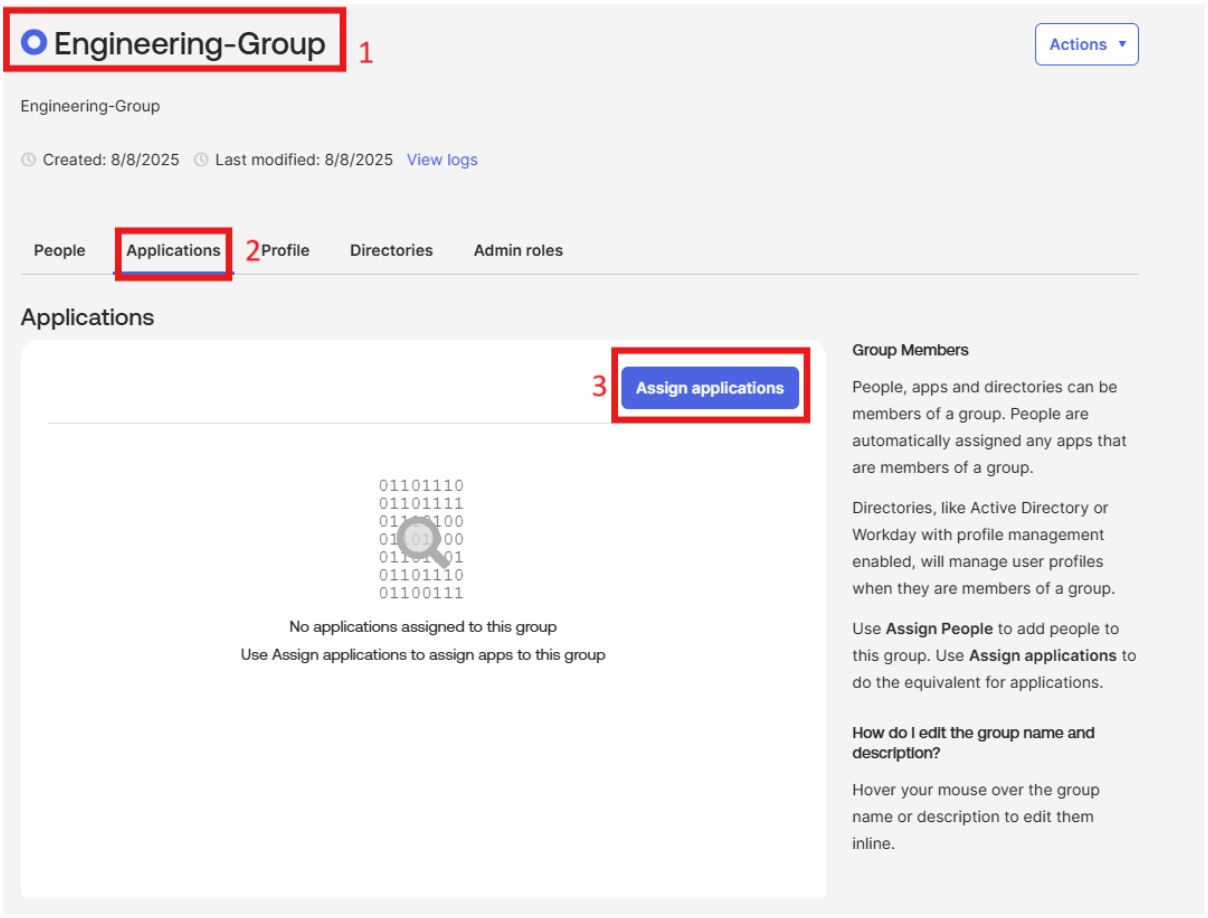


In the name field, enter a group name

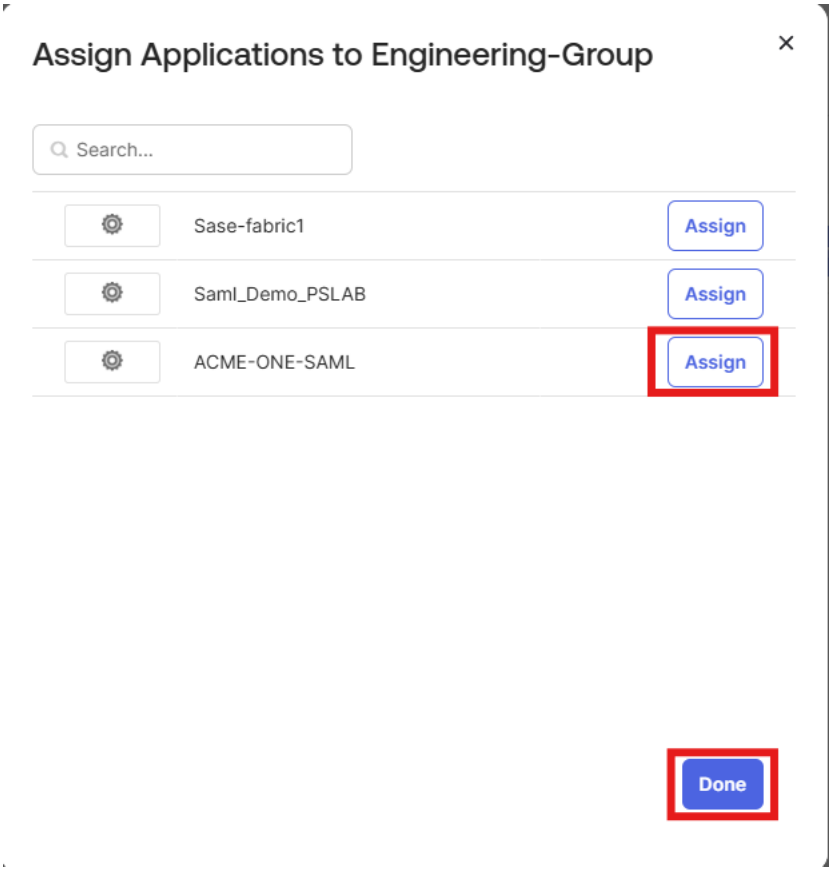


Refresh the page and click to the newly created group "**Engineering-Group".**

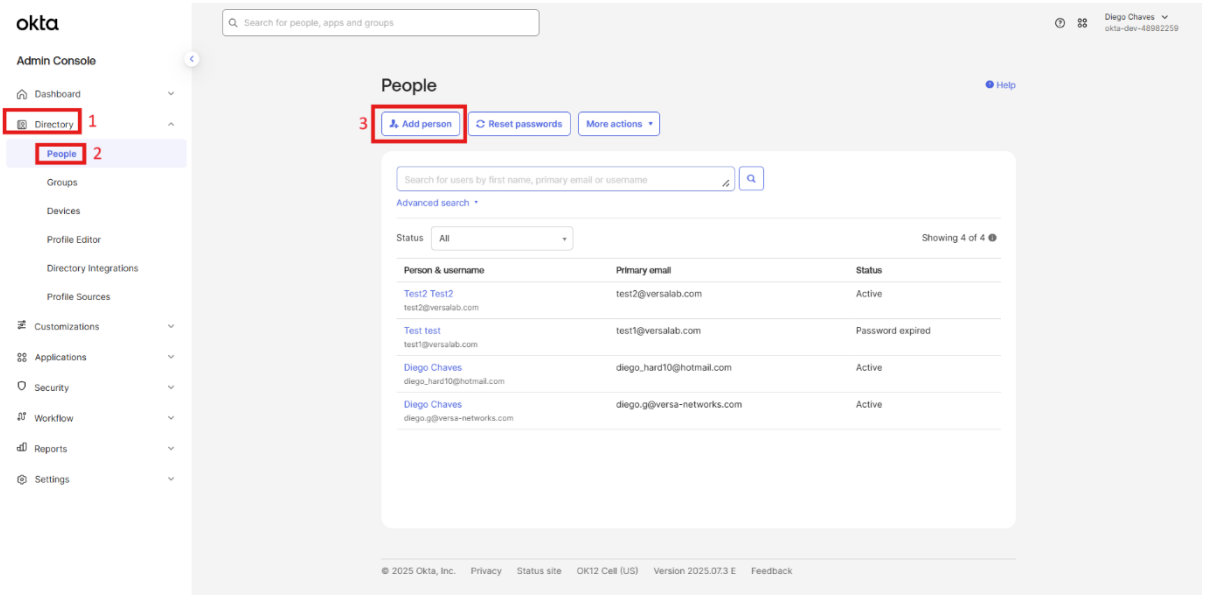
After opening the group, go to the **Applications** tab and Click Assing Applications To assign the newly created SAML application to the group.



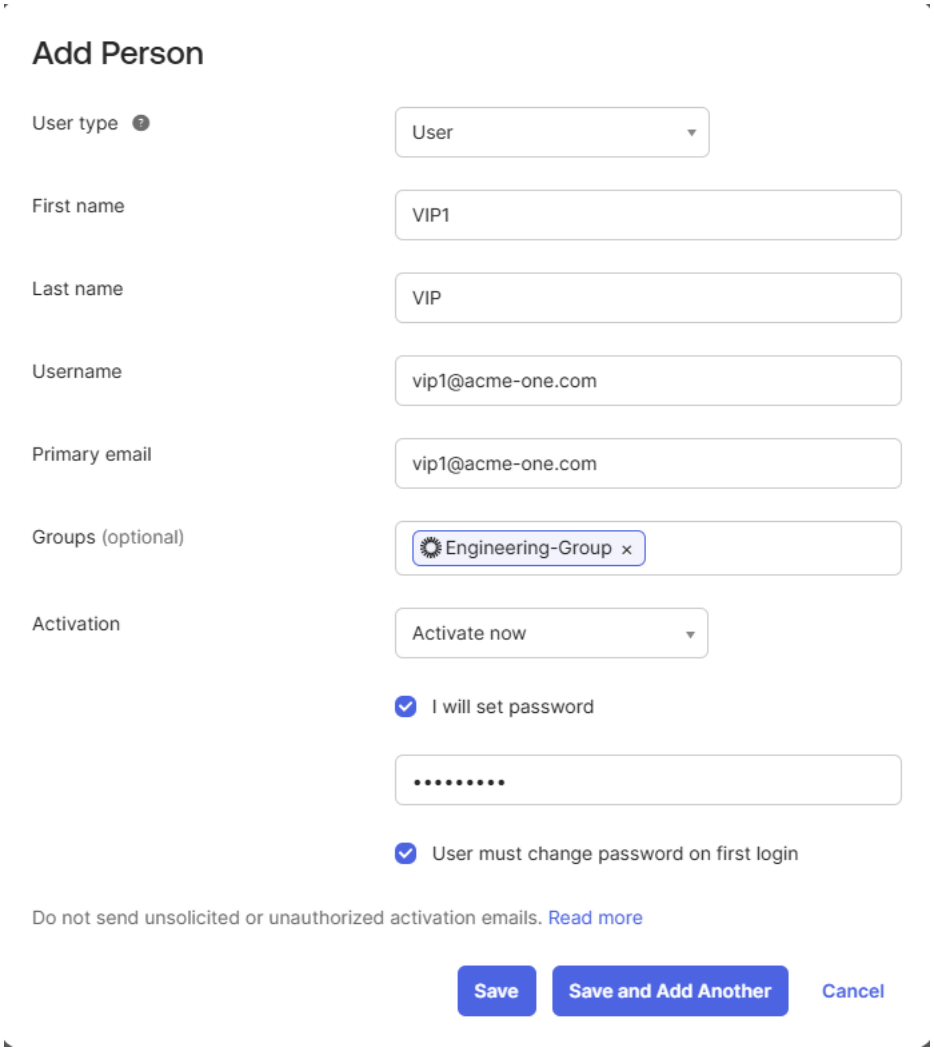
Select newly created SAML application



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



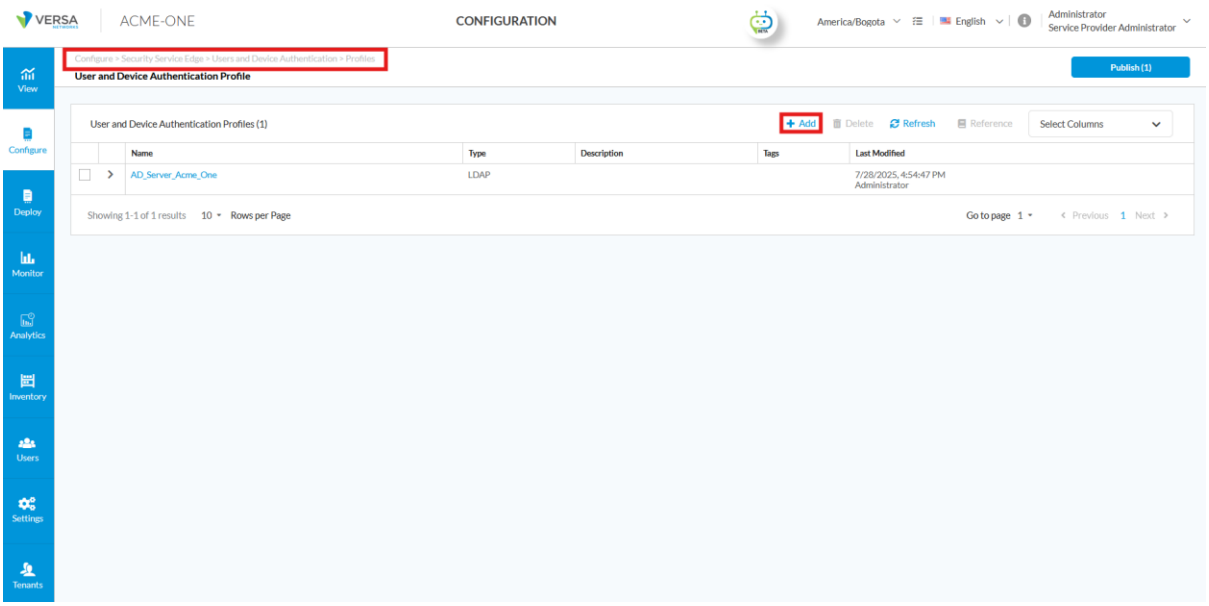
In the **Add Person** window, set **User** type to User, enter the **first name**, last name, **username**, and primary email, select the required group (Example Engineering-Group), choose **Activate now**, set a password, and ensure User must change password on first login is checked before saving.



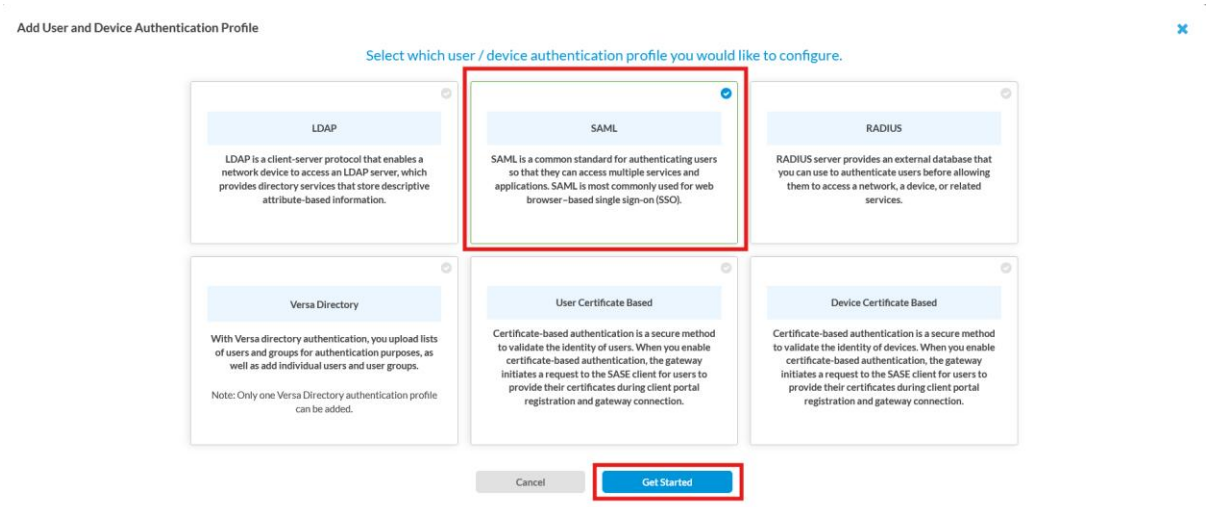
Concerto OKTA Authentication Profiles

Navigate to User and Device Authentication Profiles

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

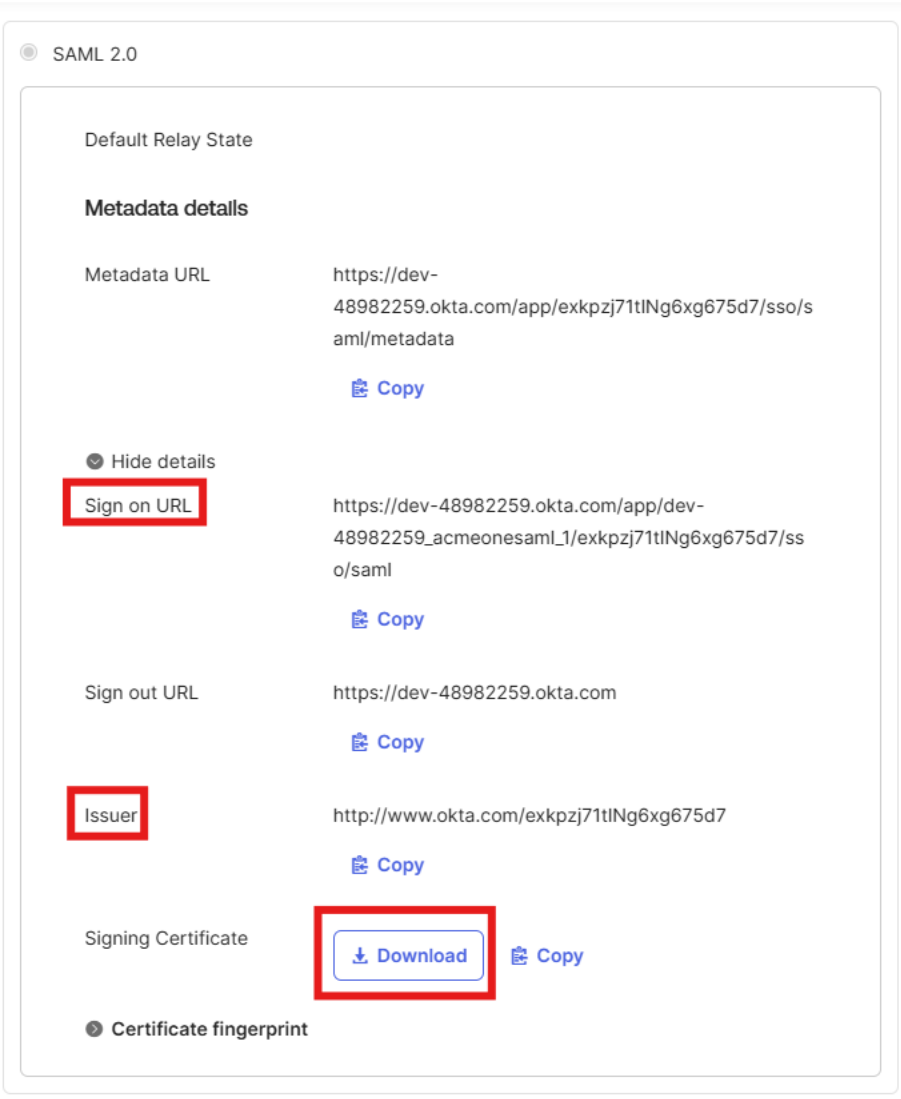


Select **SAML,** Click Get Started

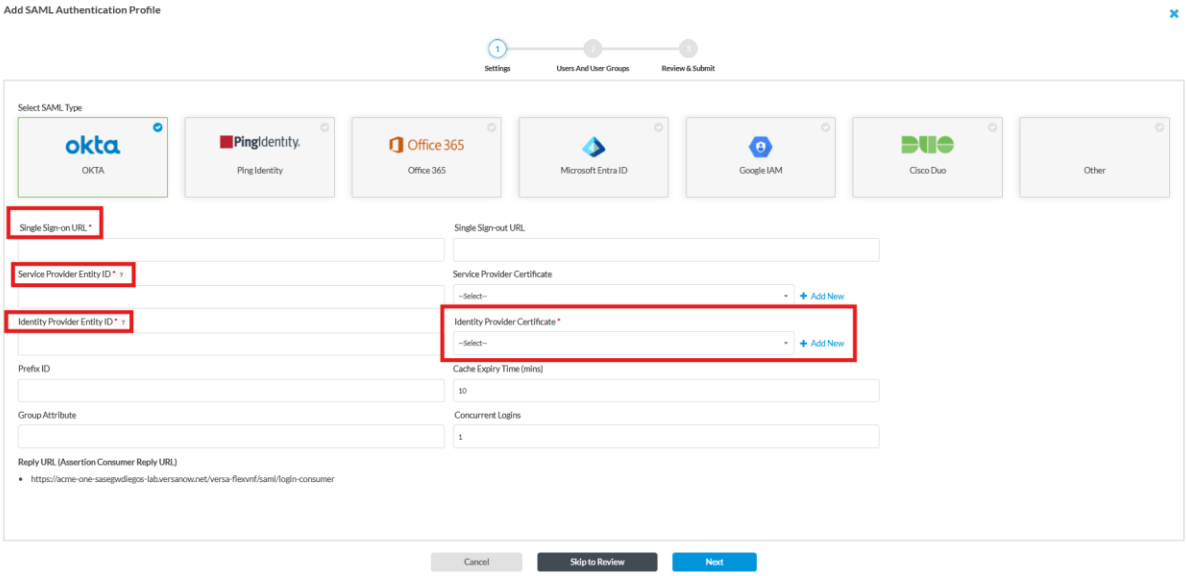


Select **OKTA**

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 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.



Complete the parameters using the values from the Okta app:

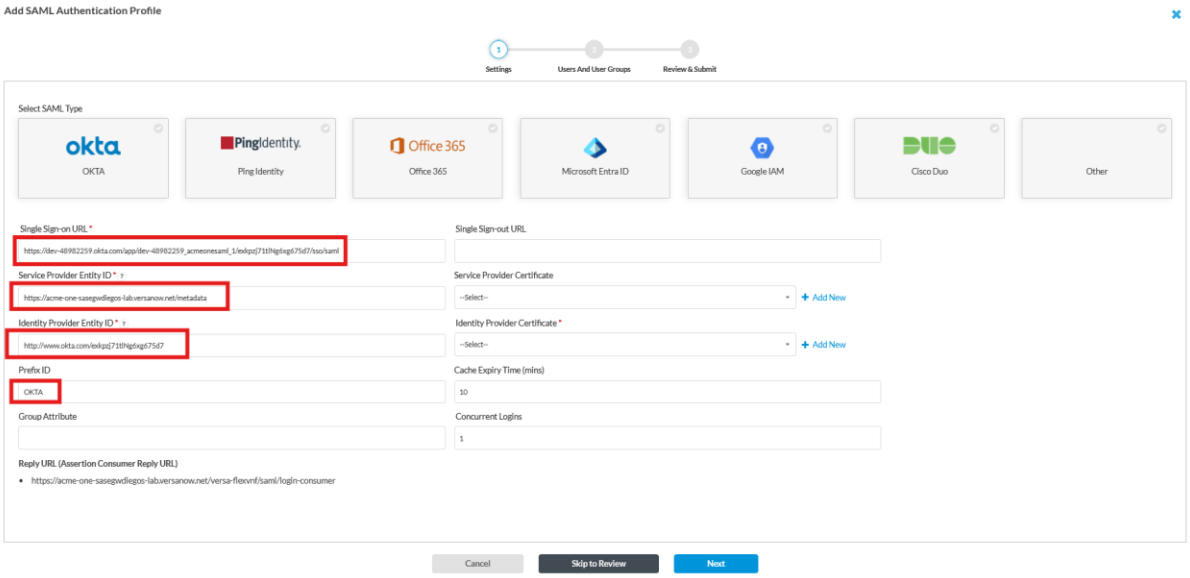
Example:

Single Sign-on URL: https://dev-48982259.okta.com/app/dev-48982259_ac-meonesaml_1/exkpzj71tlNg6xg675d7/sso/saml

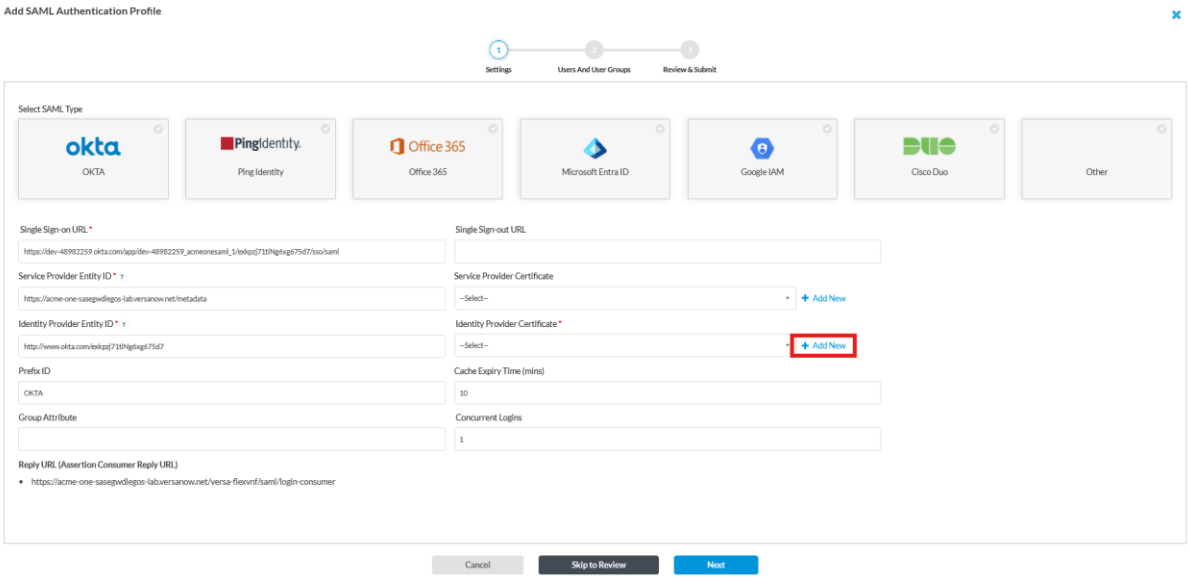
Service Provider Entity ID: https://acme-one-sasegwdiegos-lab.versanow.net/metadata

Identity Provider Issuer: http://www.okta.com/exkpzj71tlNg6xg675d7

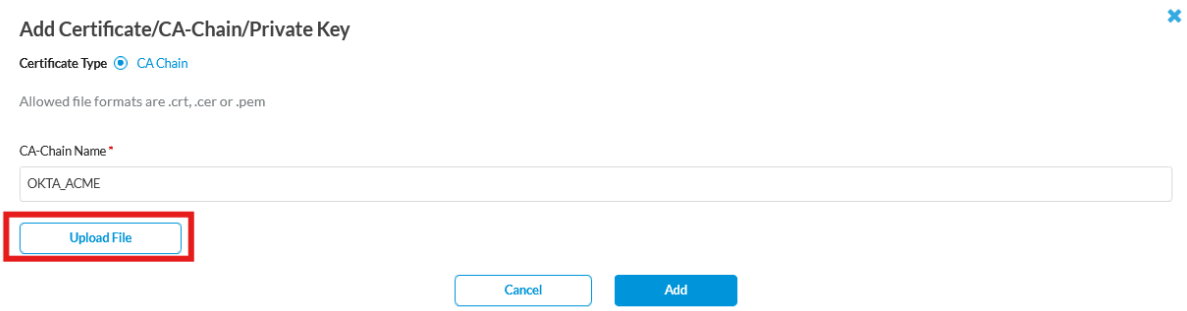
In the **Prefix ID** field fill it as OKTA



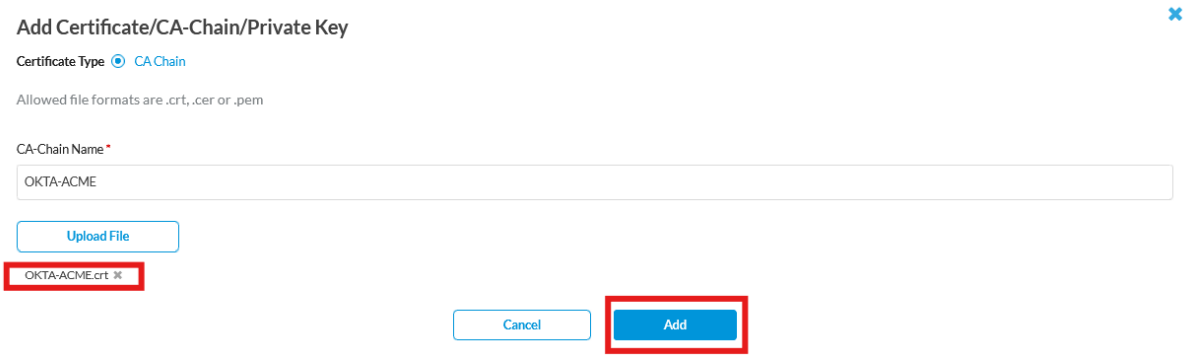
Then Upload the **Identity Provider Certificate** by clicking on the **Add** New button. Rename the downloaded certificate file from .cert to .crt before use on concerto.



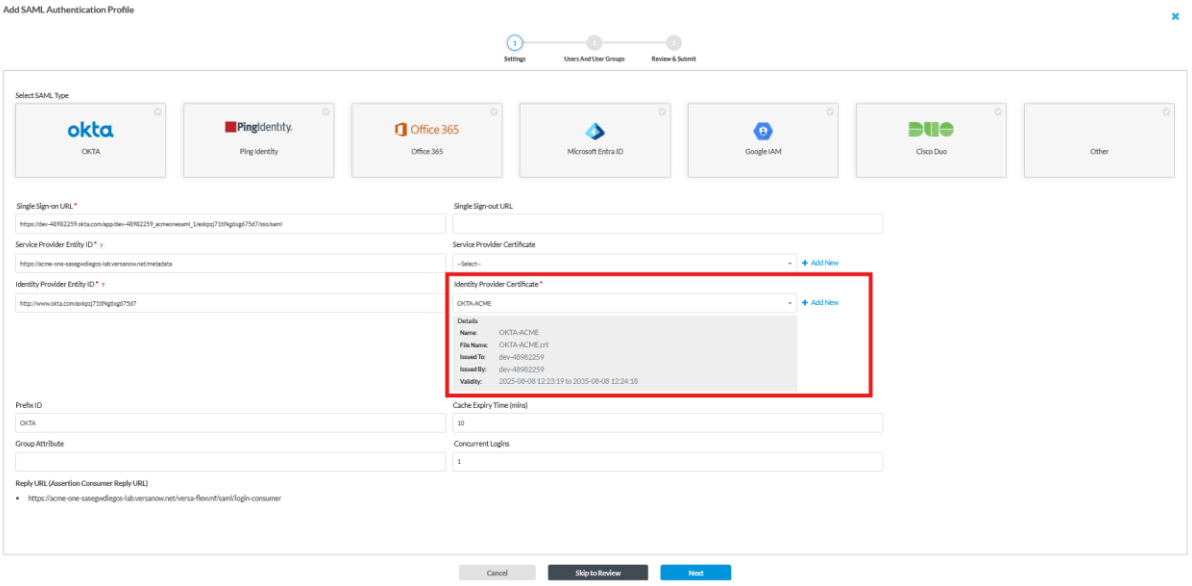
Name to **CA-Chain Name** upload certificate issue by clicking on the Upload File.



Then Add



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

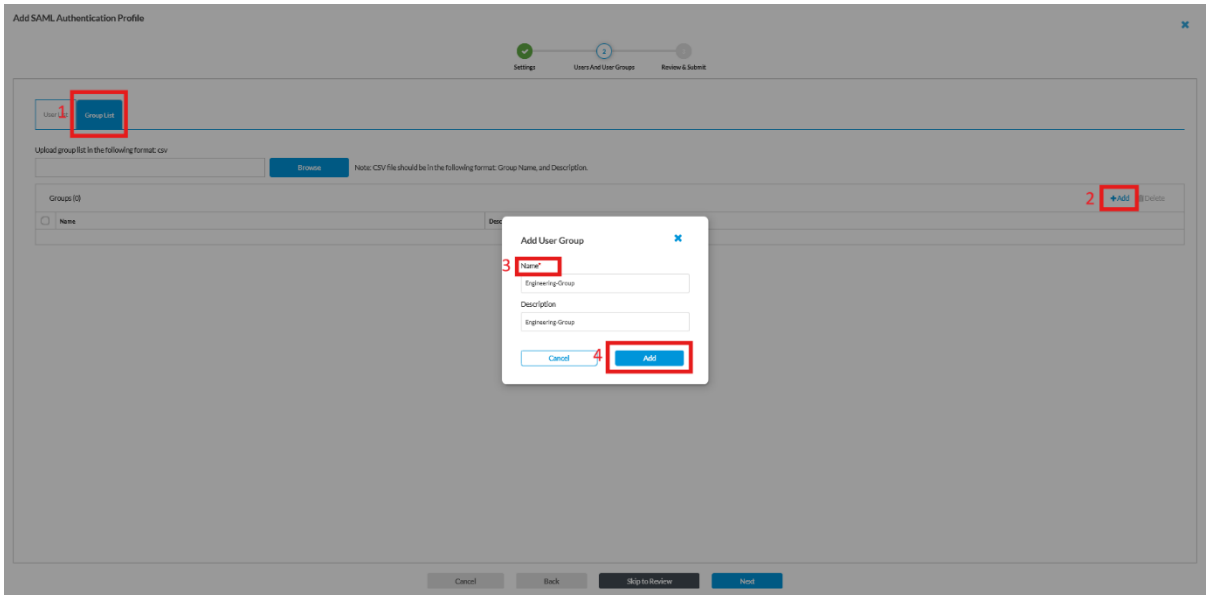


Then **Next**

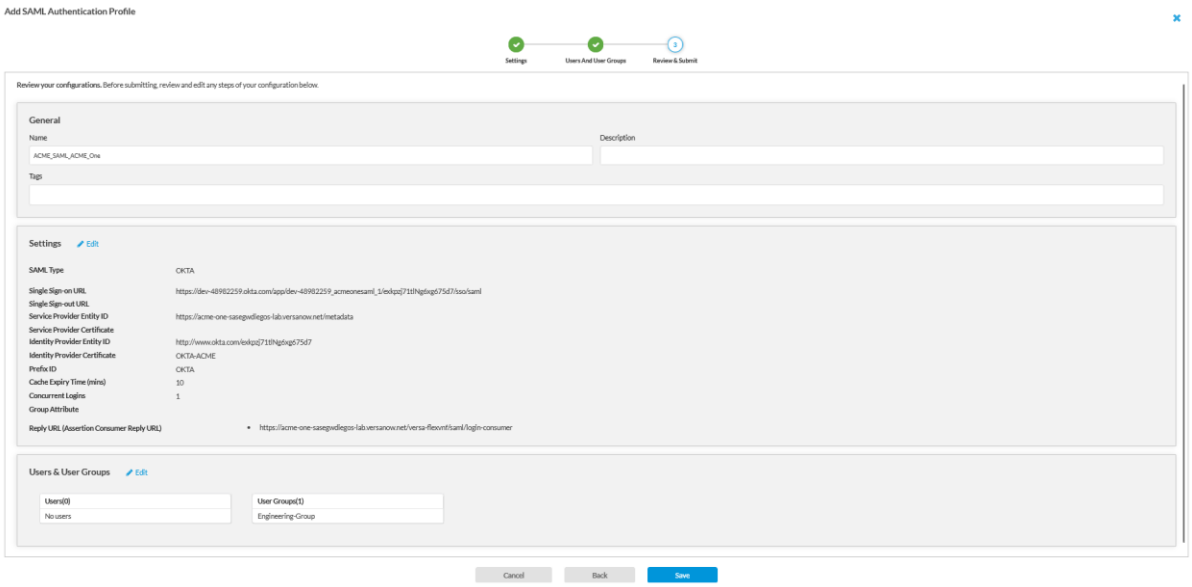
On the **Users and User Groups** page, you can associate either an individual **user list** or a complete **group list** with the SAML authentication profile. The advantage of this approach is that a group or

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.

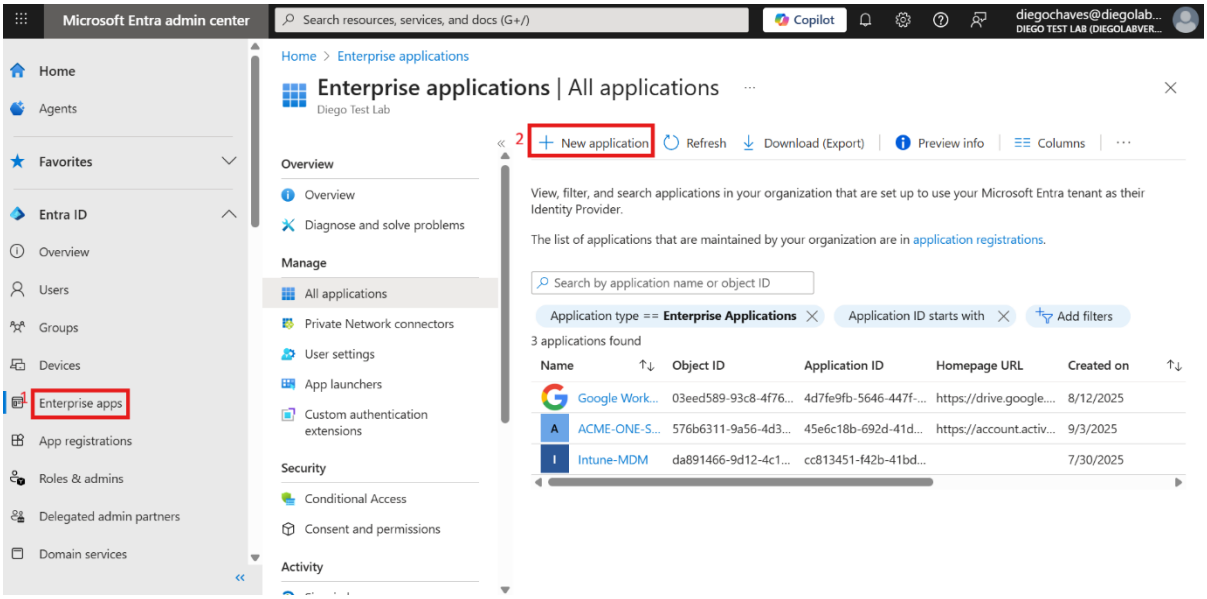
Entra ID Configuration

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**.



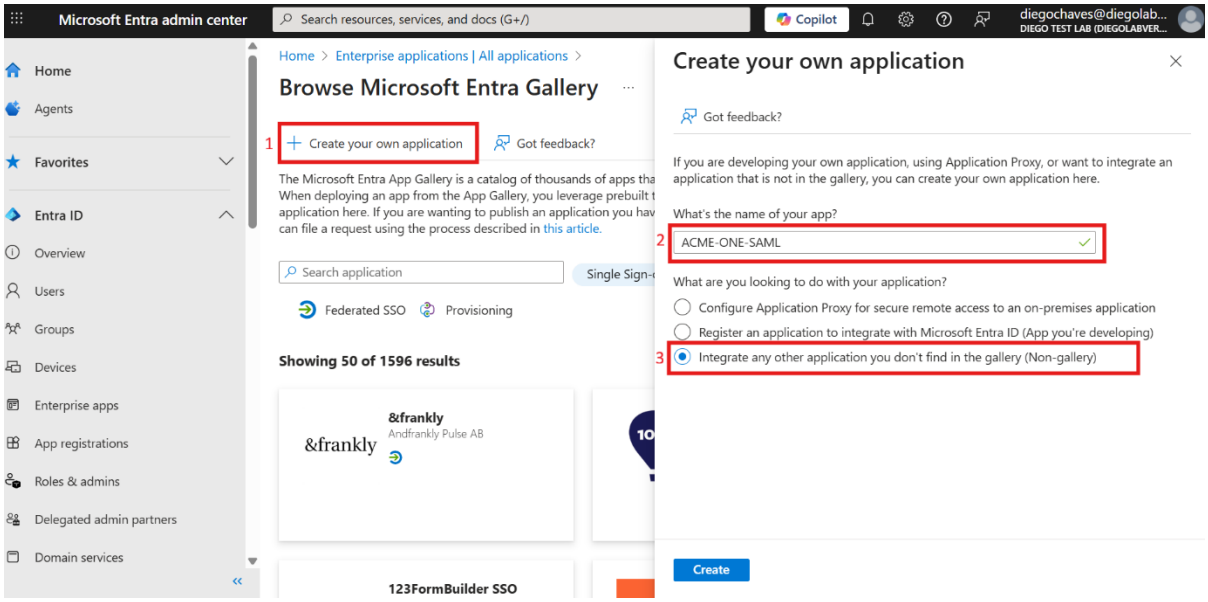
2. Select **Create a new application**

Click **+ Create your own application**.

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

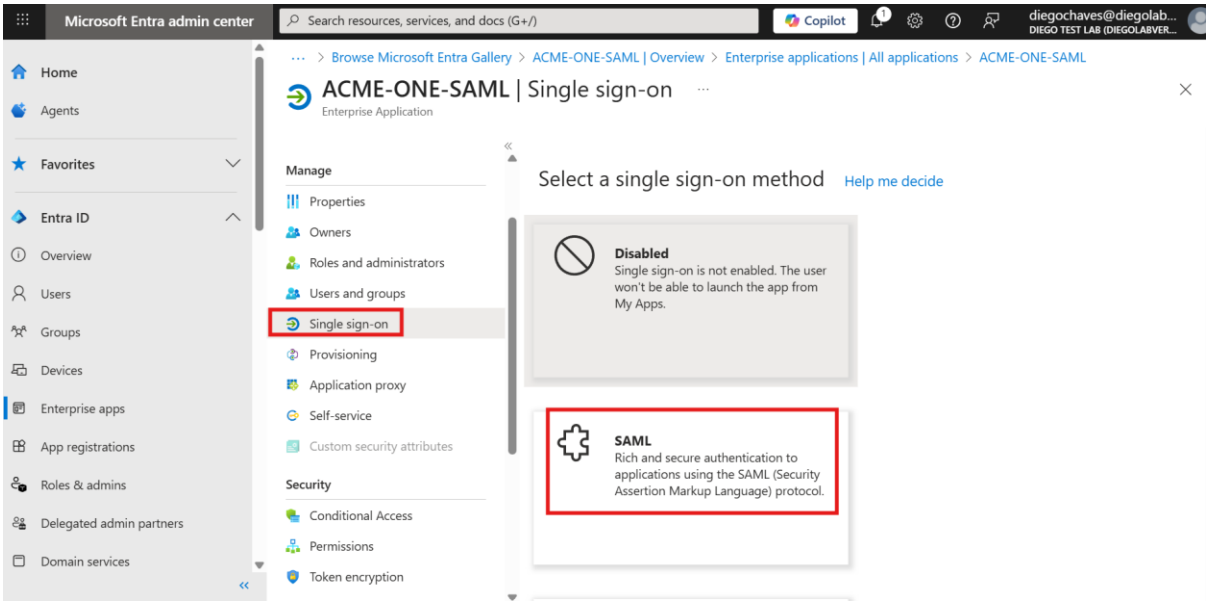
Select **Integrate any other application you don't find in the gallery (Non-gallery)**.

Click **Create**.



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

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

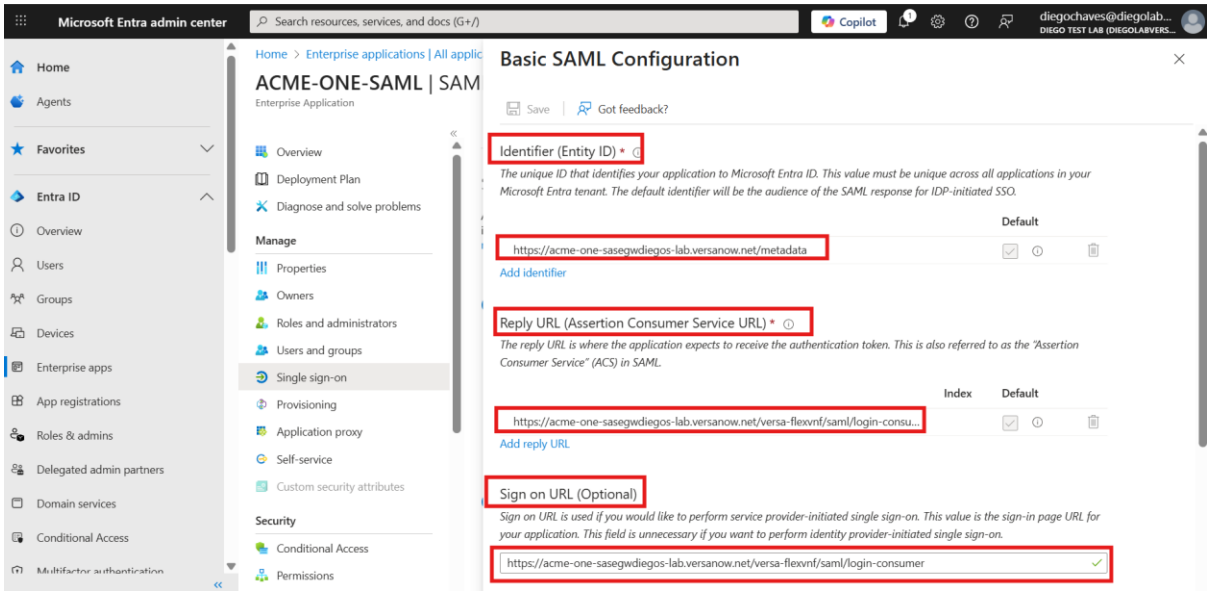


4. In the SAML settings, enter information for the indicates fields.

Field	Description
Reply URL (Assertion Consumer Service URL) and Sign on URL (Optional)	Enter the URL to which Okta sends OAuth responses. The responses are sent in the format . **https://saseGw-FQDN/versa-flexvnf/saml/login-consumer**. (Here the Gateway's FQDN is used as the main URL +/versa-flexvnf/saml/login-consumer). In the exampe **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)	To allow Versa to receive all user-to-group mappings from Okta, configure a group attribute statement as follows: **Name:** https://schemas.microsoft.com/ws/2008/06/identity/claims/groups **Name format:** Unspecified **Filter:** Select **Regex** (or equivalent option) and enter **.*** 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.
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-577374553241106028824609139" IssueInstant="2025-08-08T17:10:21.828Z" Version="2.0"
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
    <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"/>
    <saml2:Subject>
        <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">userName</saml2:NameID>
        <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml2:SubjectConfirmationData NotOnOrAfter="2025-08-08T17:15:22.008Z" Recipient="https://acme-one-sasegwdiegos-lab.versanow.net/versa-flexvnf/saml/login-consumer"/>
        </saml2:SubjectConfirmation>
    </saml2:Subject>
    <saml2:Conditions NotBefore="2025-08-08T17:05:22.008Z" NotOnOrAfter="2025-08-08T17:15:22.008Z">
        <saml2:AudienceRestriction>
            <saml2:Audience>https://acme-one-sasegwdiegos-lab.versanow.net/metadata</saml2:Audience>
        </saml2:AudienceRestriction>
    </saml2:Conditions>
    <saml2:AuthnStatement AuthnInstant="2025-08-08T17:10:21.828Z">
        <saml2:AuthnContext>
            <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClassRef>
        </saml2:AuthnContext>
    </saml2:AuthnStatement>
    <saml2:AttributeStatement>
        <saml2:Attribute Name="https://schemas.microsoft.com/ws/2008/06/identity/claims/groups" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
            <saml2:AttributeValue
                xmlns:xs="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">GroupName Match Starts with ".*" (ignores case)
            </saml2:AttributeValue>
        </saml2:Attribute>
    </saml2:AttributeStatement>
</saml2:Assertion>
```

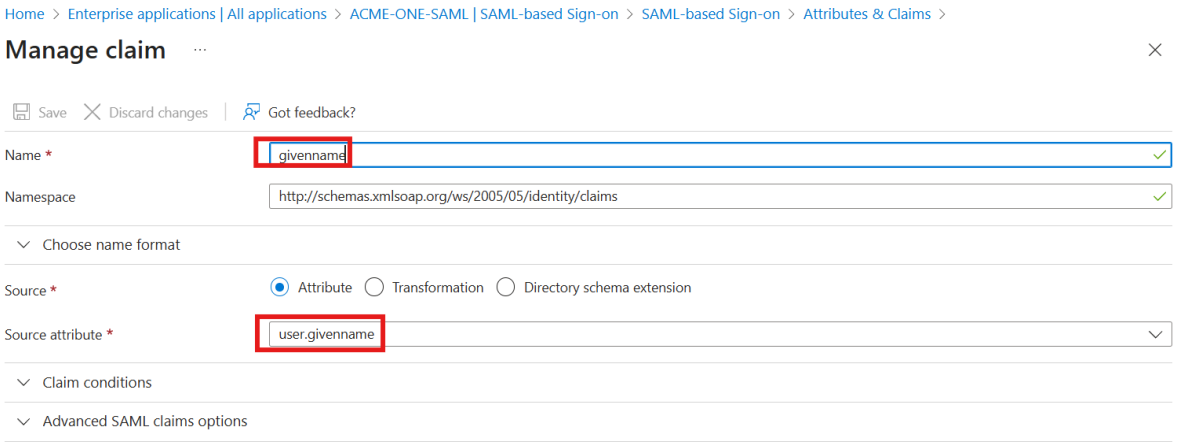

5. Configure the parameters as shown in the previous table, in Basic SAML Configuration and then click **Save**.

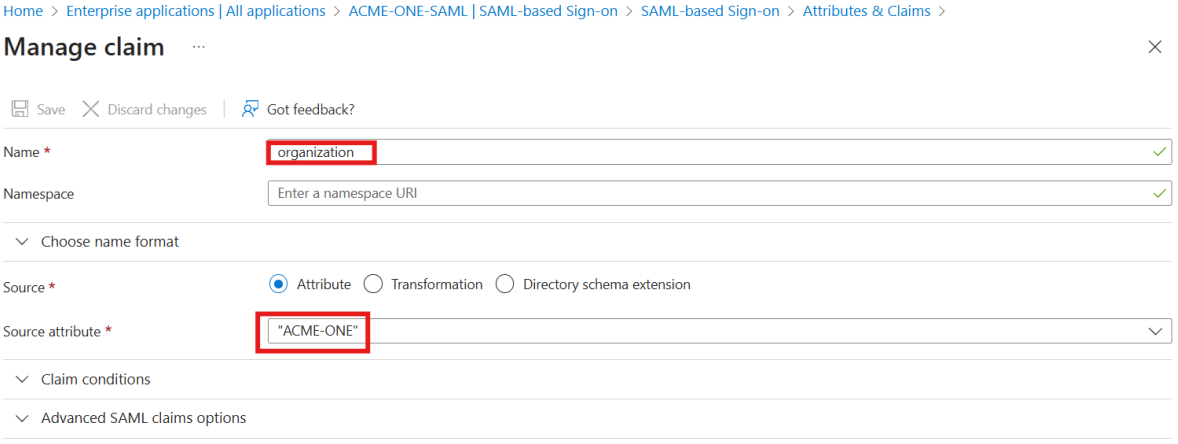


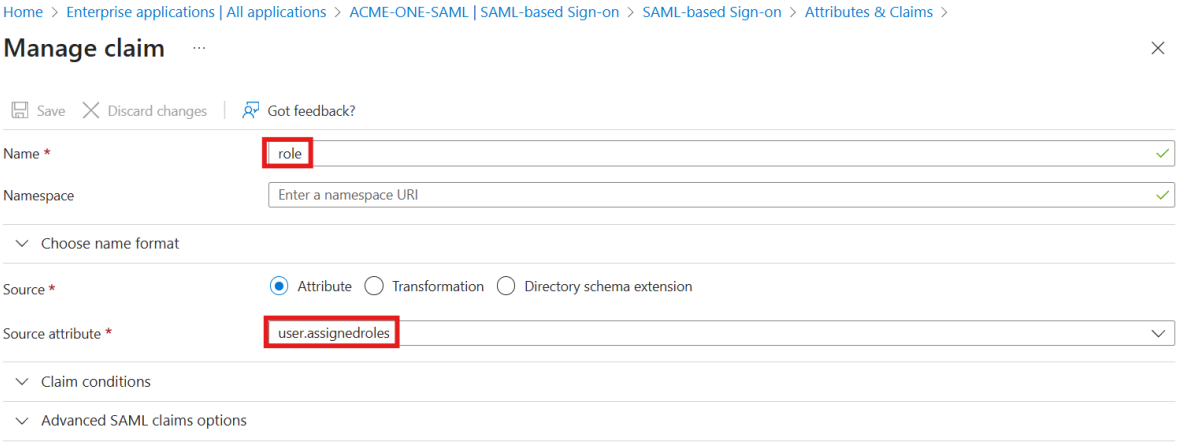
6. Define **Attributes & Claims**.

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

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

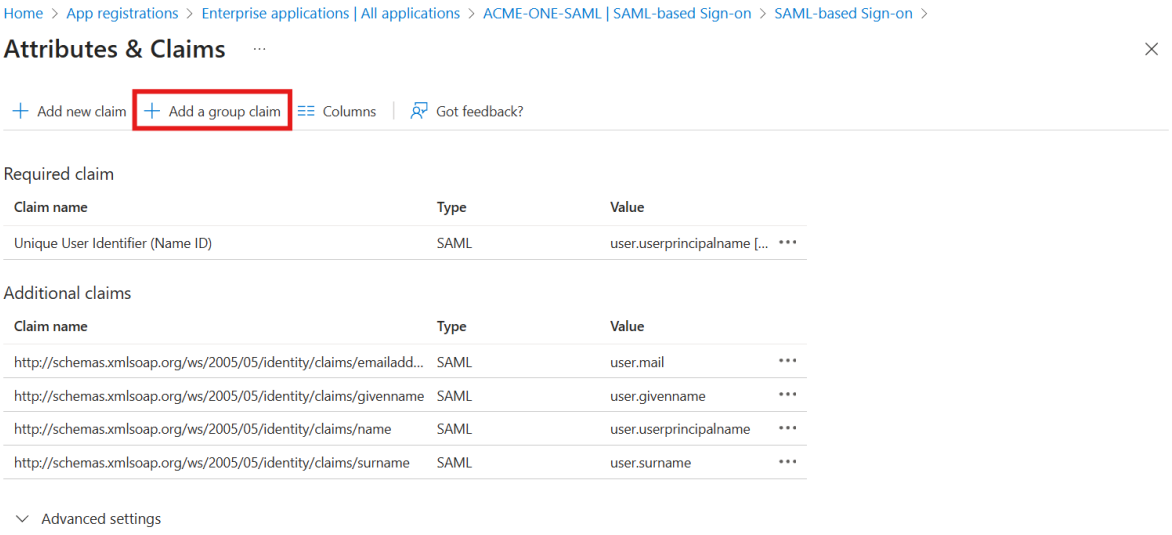




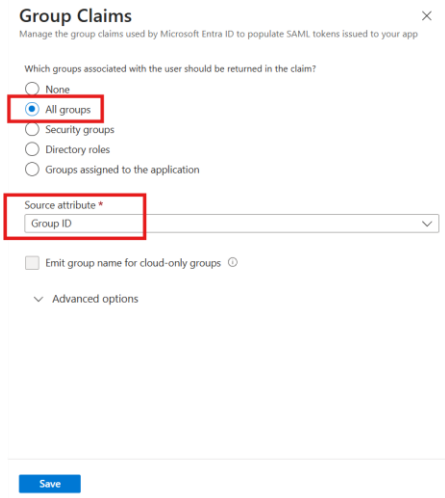


- Configure **Group Claims referring to previous table Group Attribute Statements**.

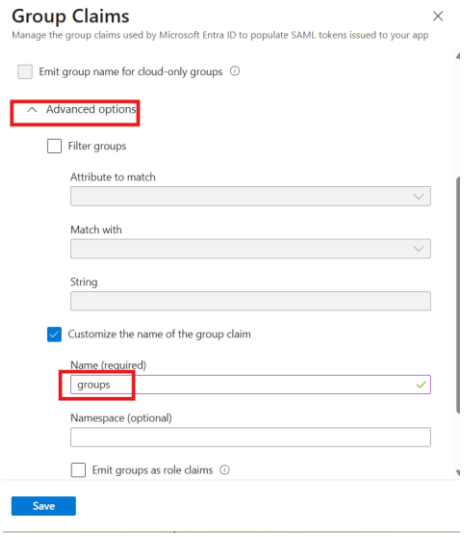
Click + Add a group Claim



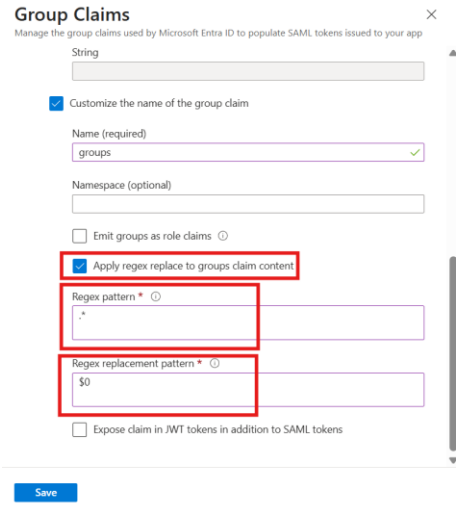
- Under **Group Claims**, choose **All groups**.
- Set **Source attribute** to *Group ID*.



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

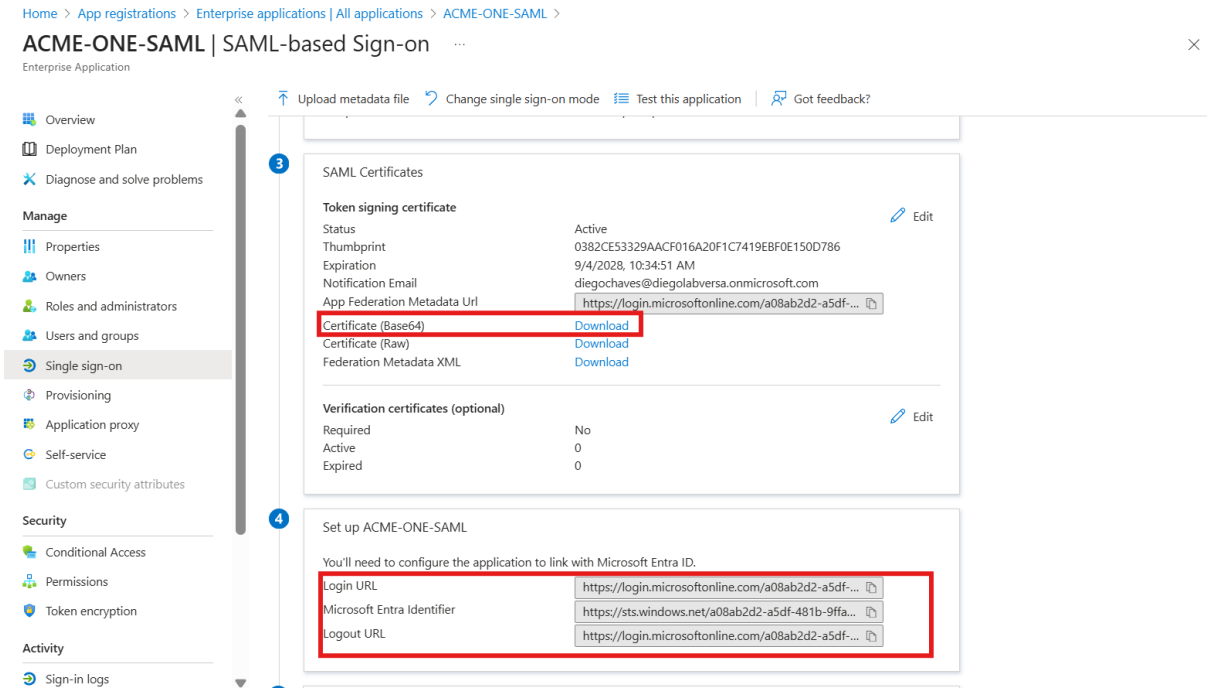


- Click on **Apply regex replace to groups claim content** then set **Regex replace**:
    - Pattern: `.*`
    - Replacement: `$0`



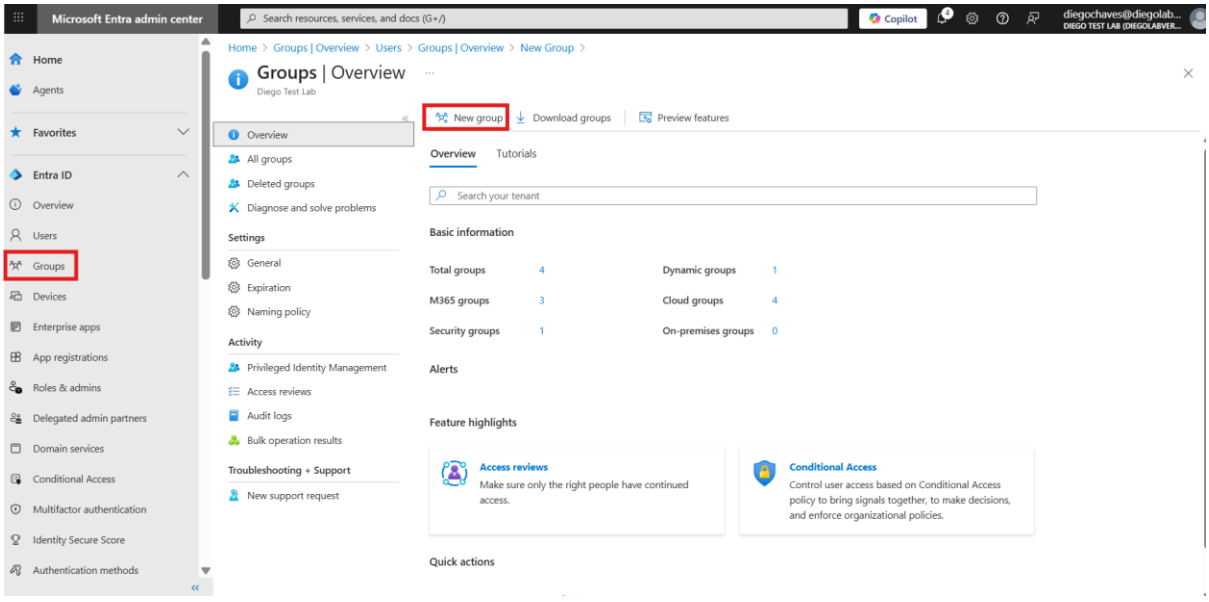
- Retrieve SAML Integration Details

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.

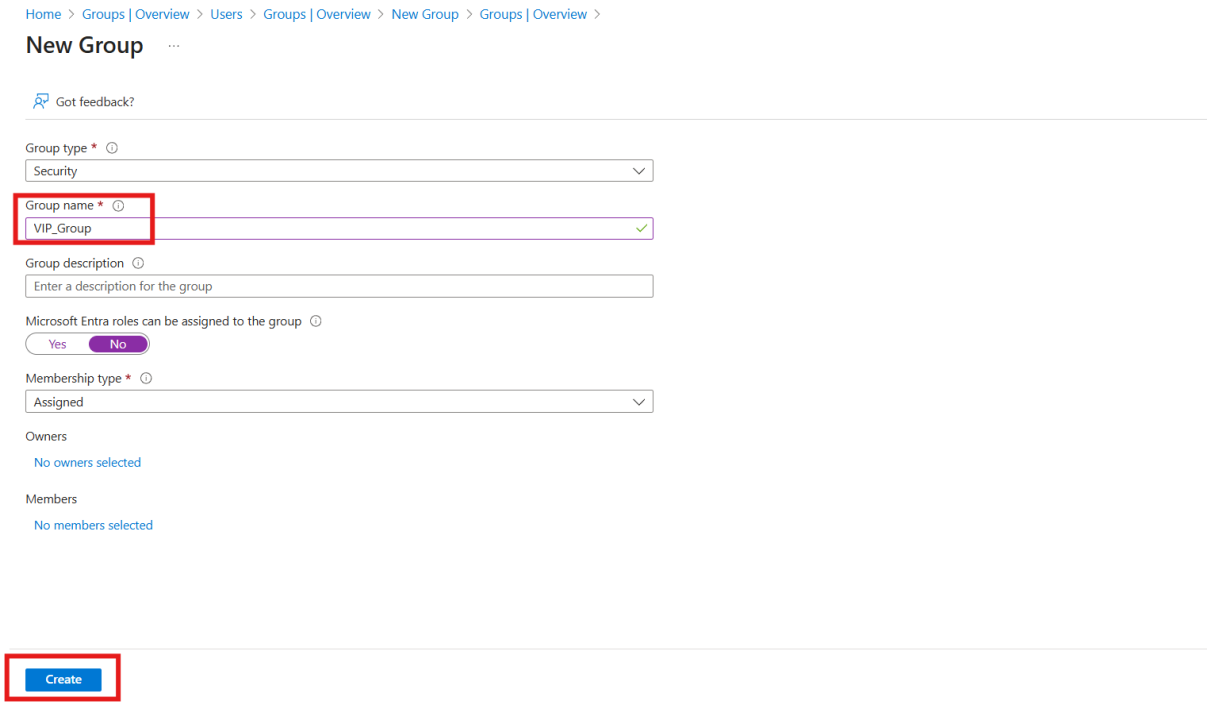


- Create the Groups and Users.

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



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



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

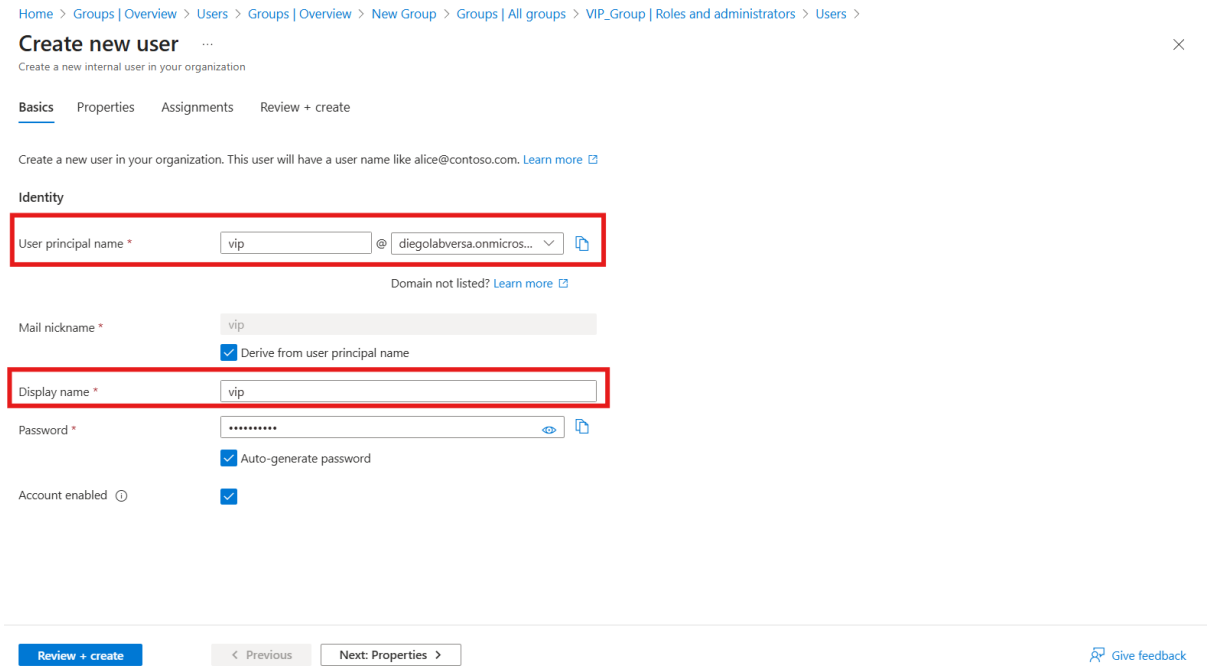
To create users Navigate to Navigate to Microsoft Entra admin Center > user, click New User.

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

Example:

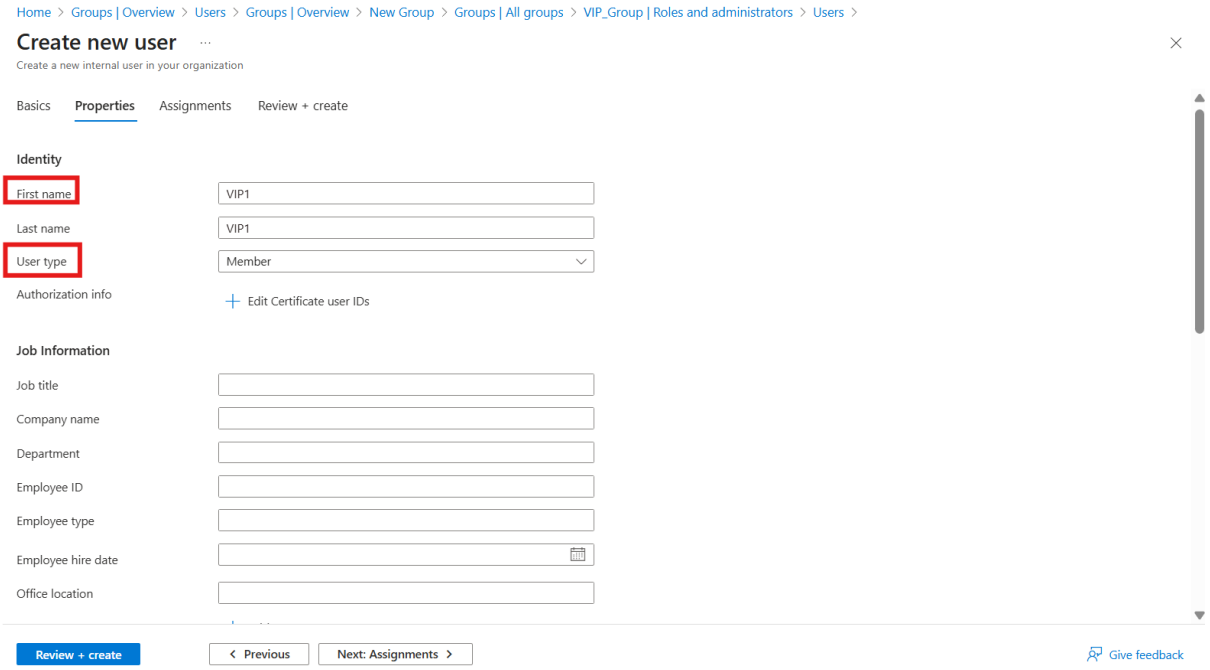
UPN → vip@acme-one.onmicrosoft.com

Display Name → vip



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

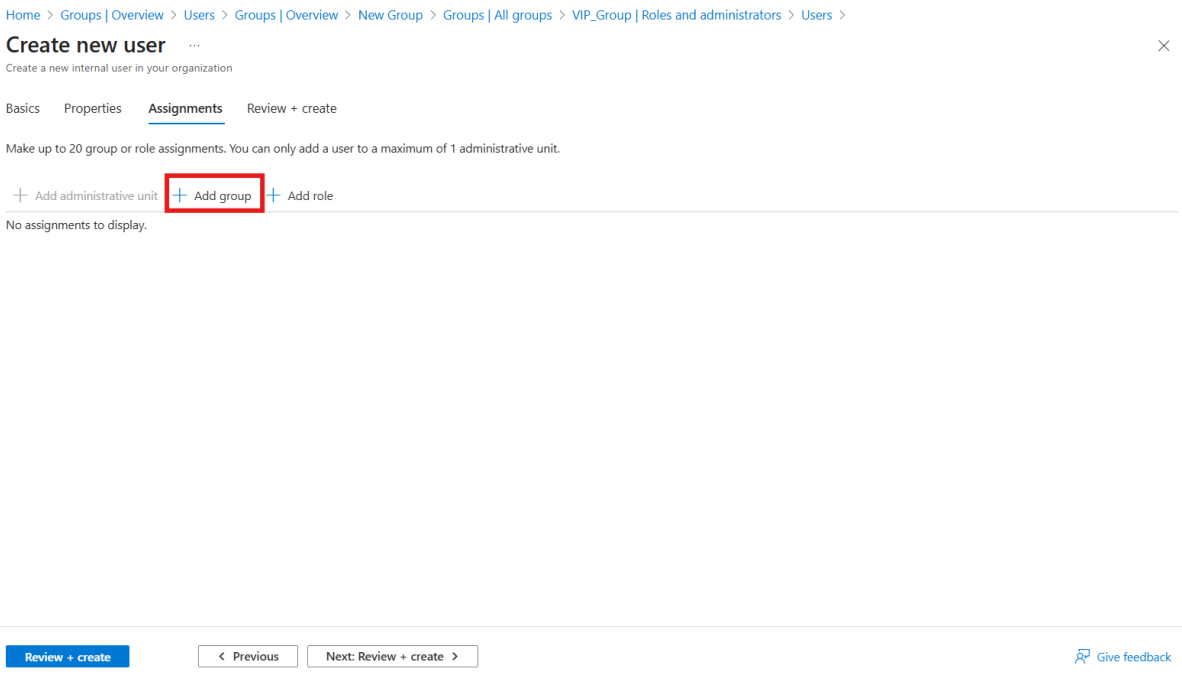
Other fields such as job title or department are optional but can be filled for organizational use.

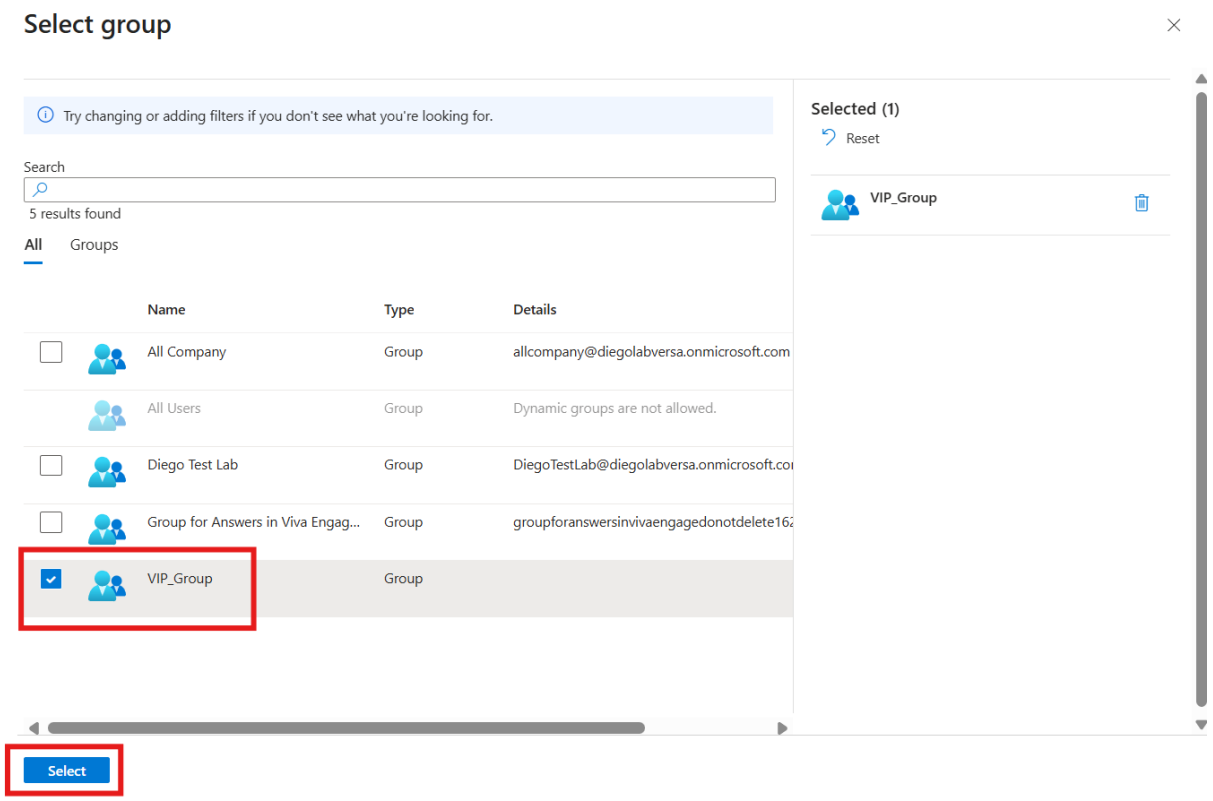


In the **Assignments** tab, click **Add Group**.

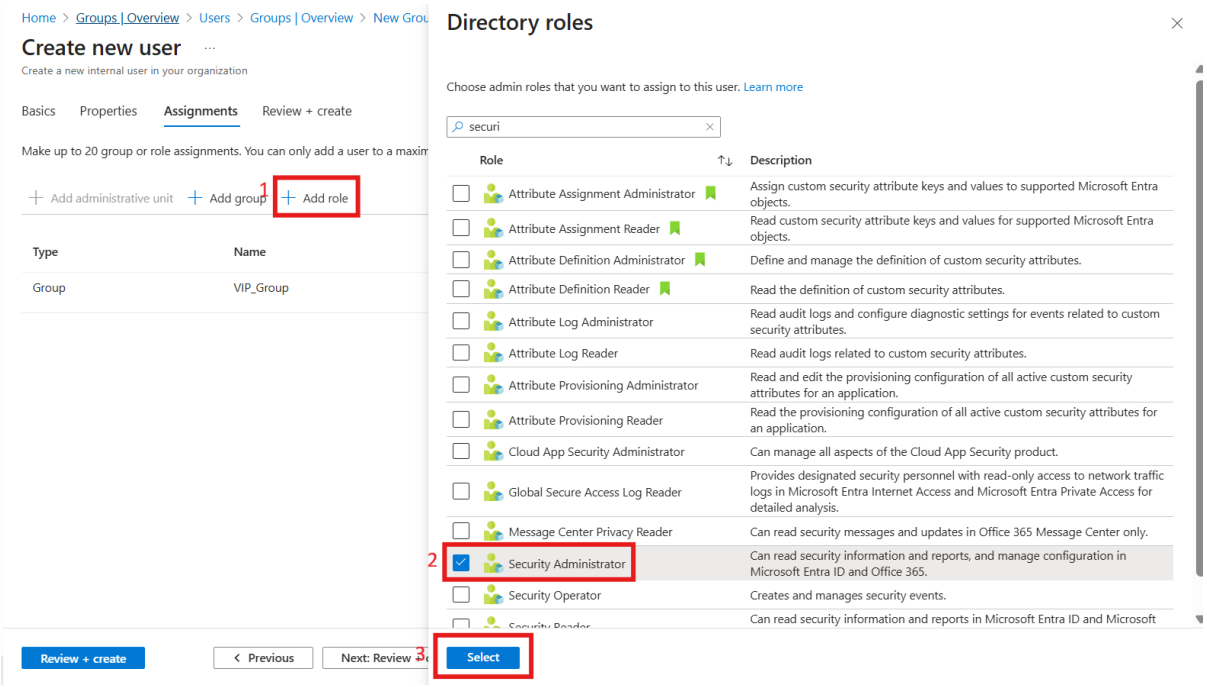
- Select the previously created **VIP_Group** (or any other relevant group).

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





- 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.



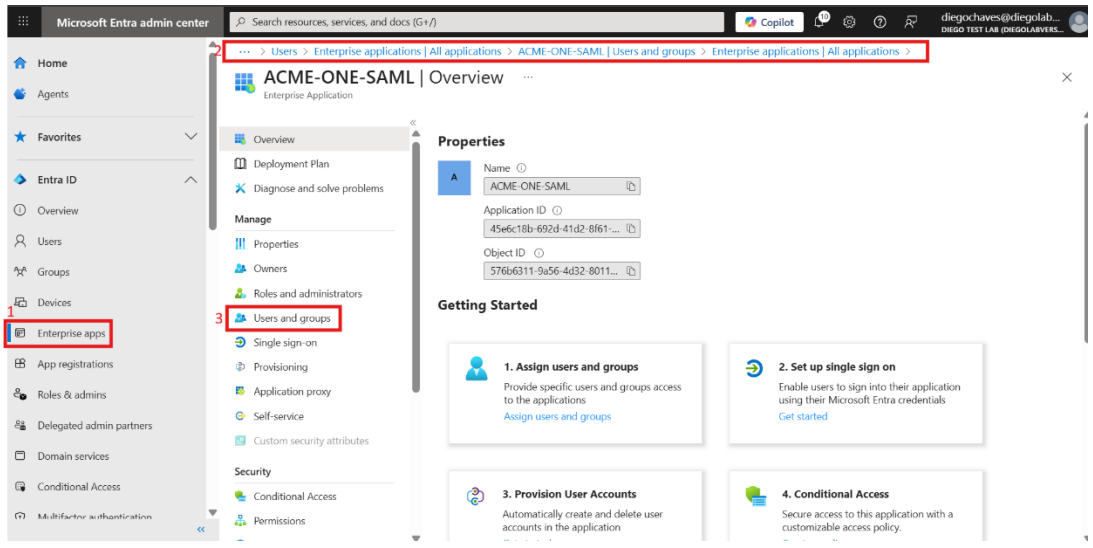
Review & Create

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

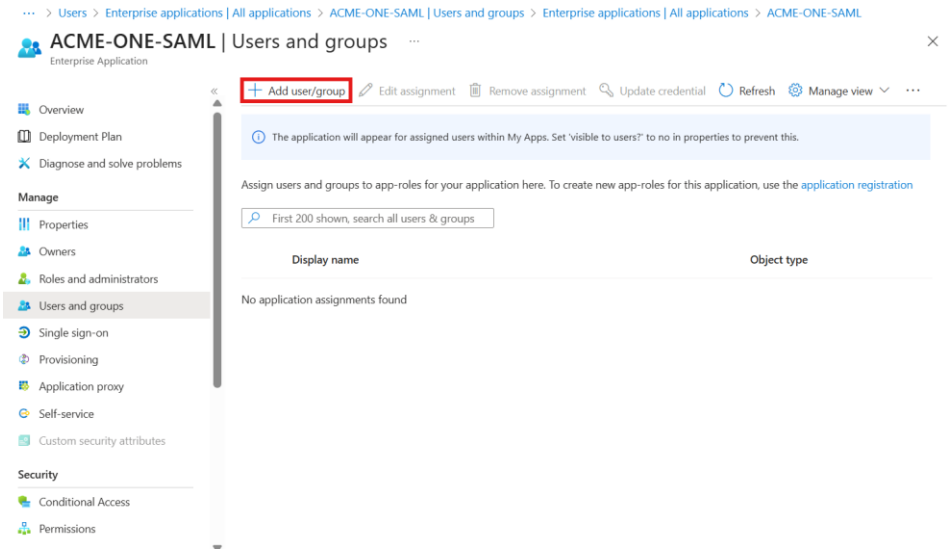
Assigning Groups to the SAML Application in Entra ID

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

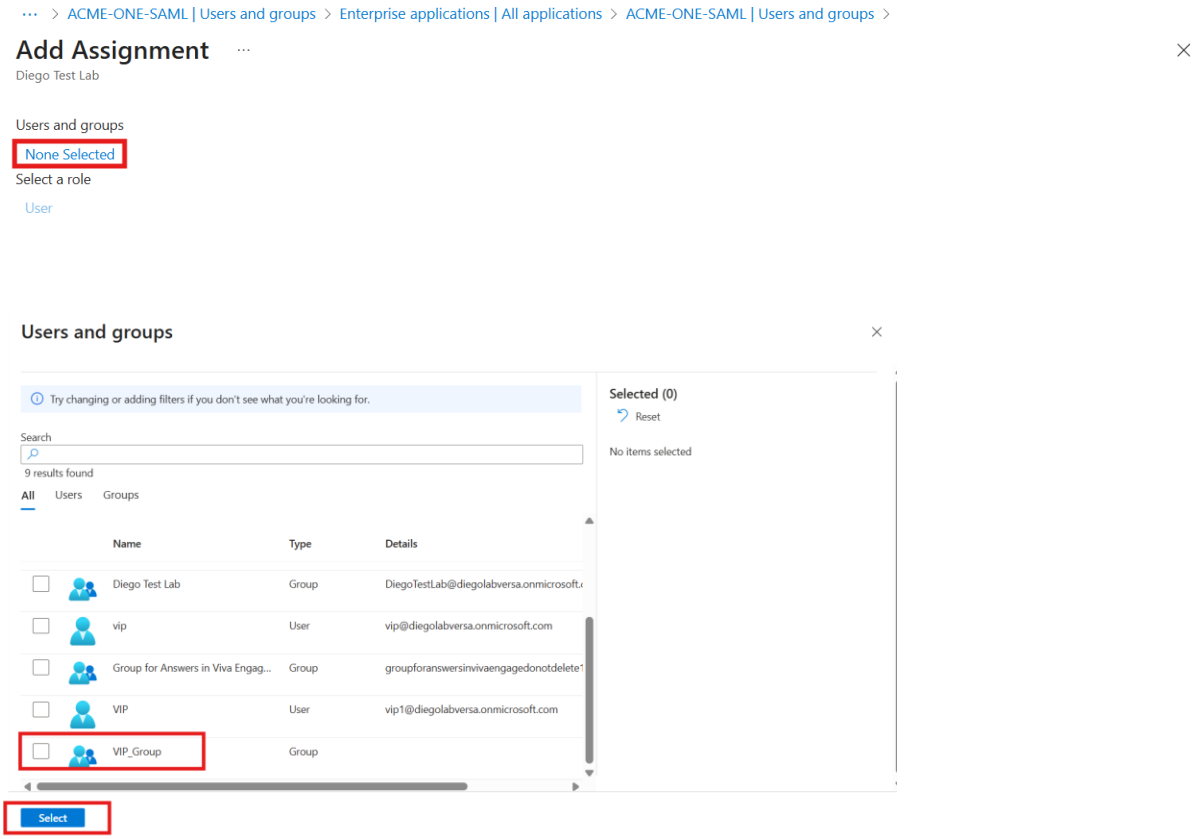
1. Navigate to the **Enterprise Apps** (Example., ACME-ONE-SAML) > **Users and groups**.



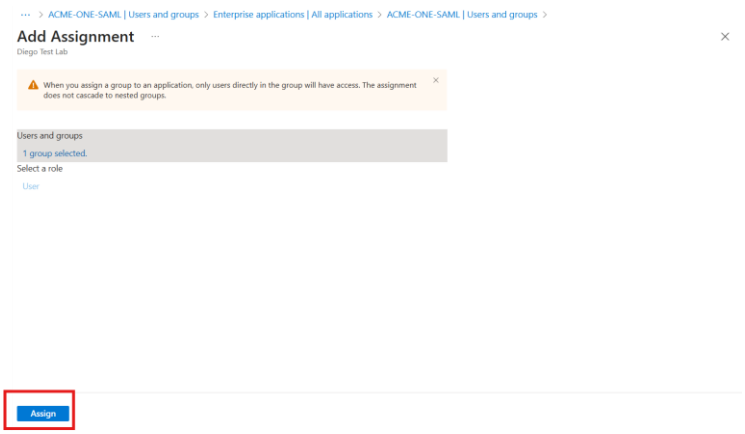
2. Click **Add user/group**, search for the group (Example, VIP_Group), select it, and assign it to the application.



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

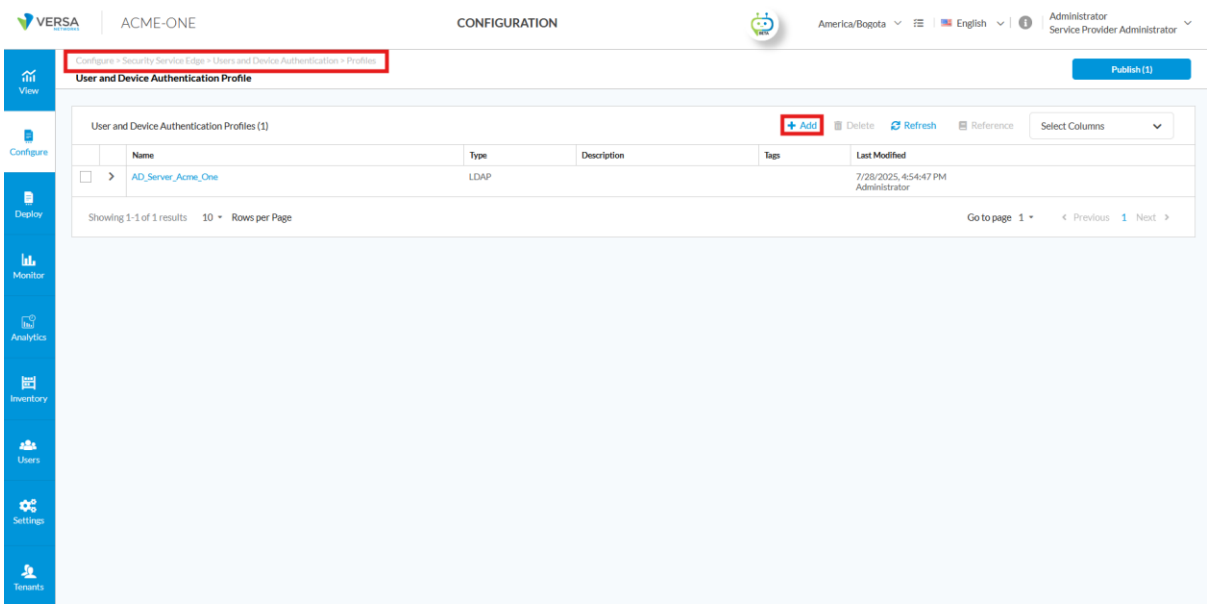


Then click **Assign**, This ensures all members of the assigned group inherit SAML access to the application without needing individual assignments.

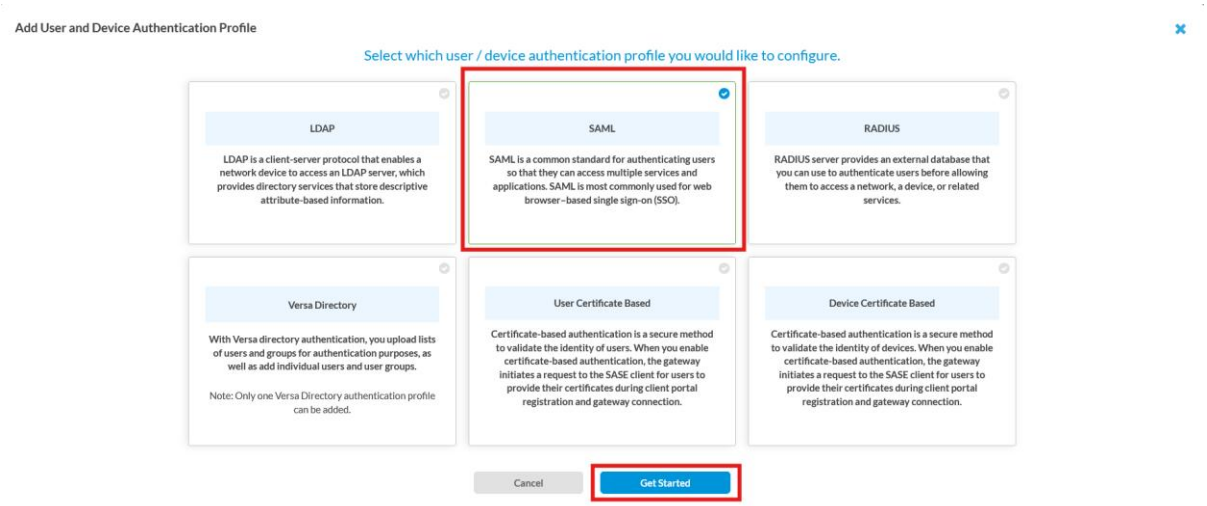


Concerto configuration for ENTRA-ID SAML Authentication Profiles

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



Select **SAML,** Click Get Started

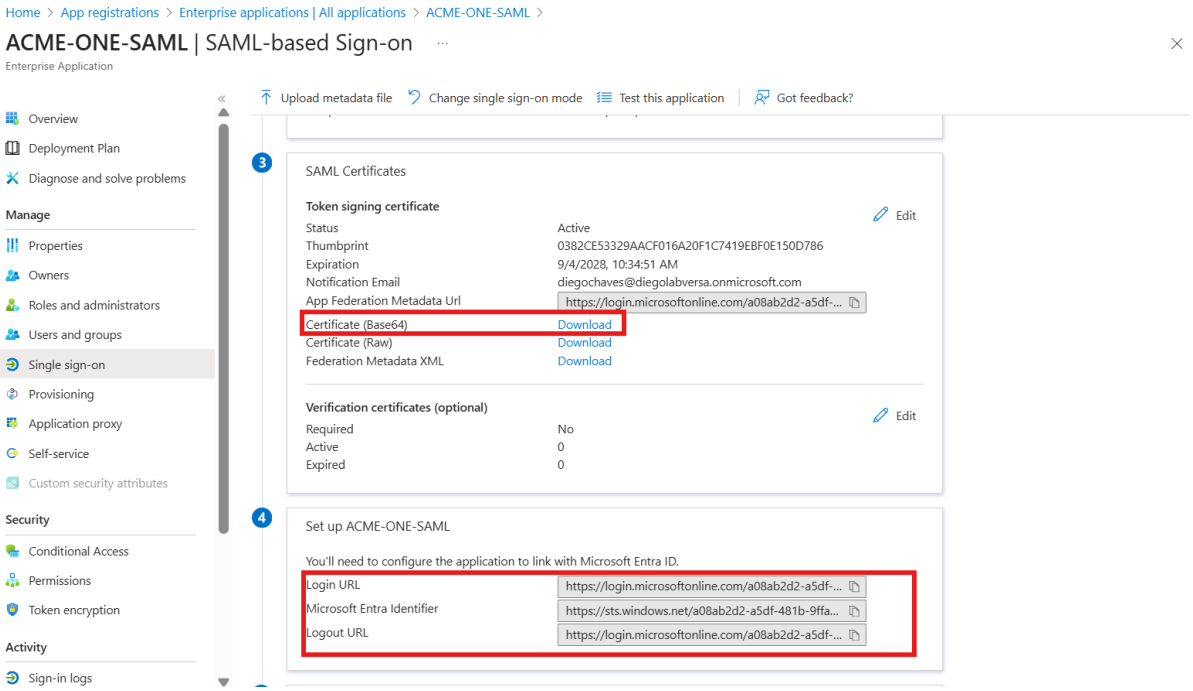


Select **ENTRA-ID**

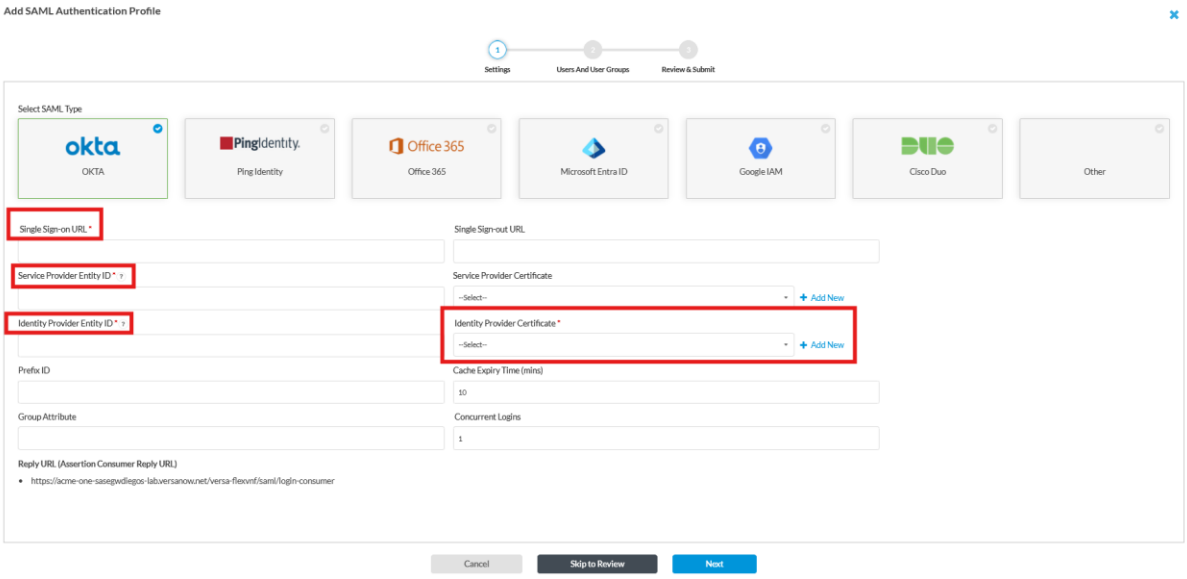
To configure the settings, use the information collected in **Step 8** from the Microsoft ENTRA ID. Go to Entra ID > Enterprise apps > All applications > *ACME-ONE-SAML* > Single sign-on (SAML).

From this page, copy/download the values required :

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



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.



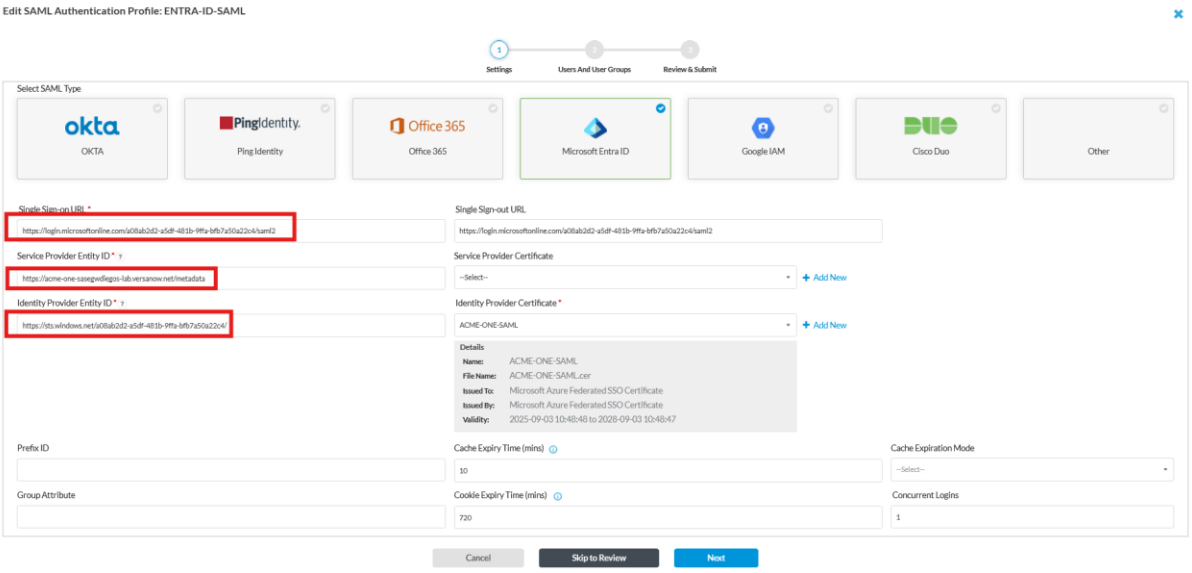
Complete the parameters using the values from the Microsoft Entra id

Example:

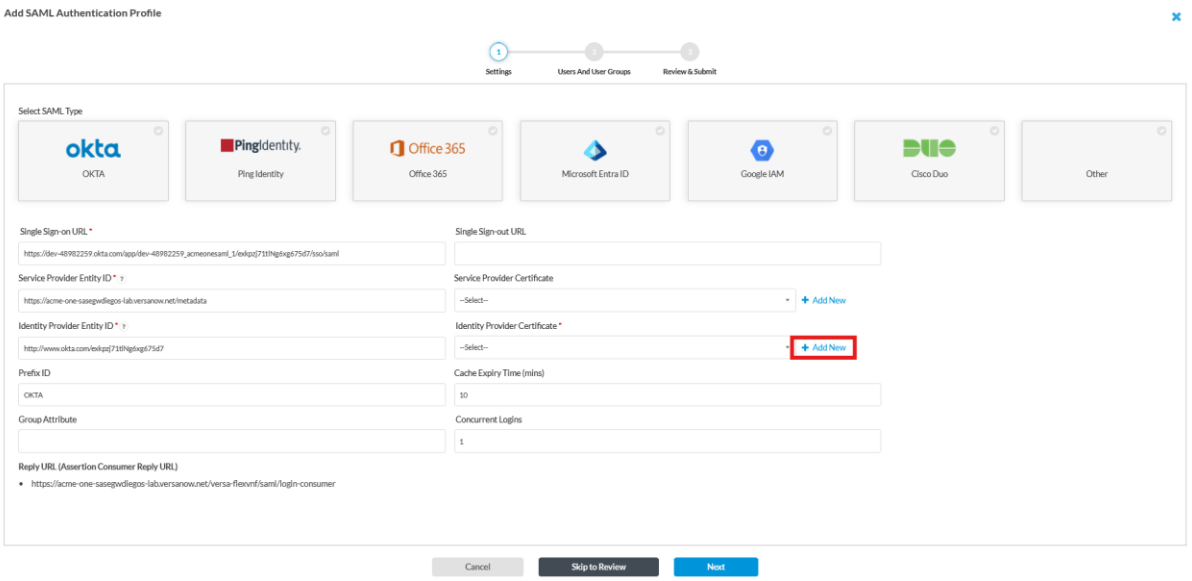
Single Sign-on an out URL: https://login.microsoftonline.com/a08ab2d2-a5df-481b-9ffa-bfb7a50a22c4/saml2

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

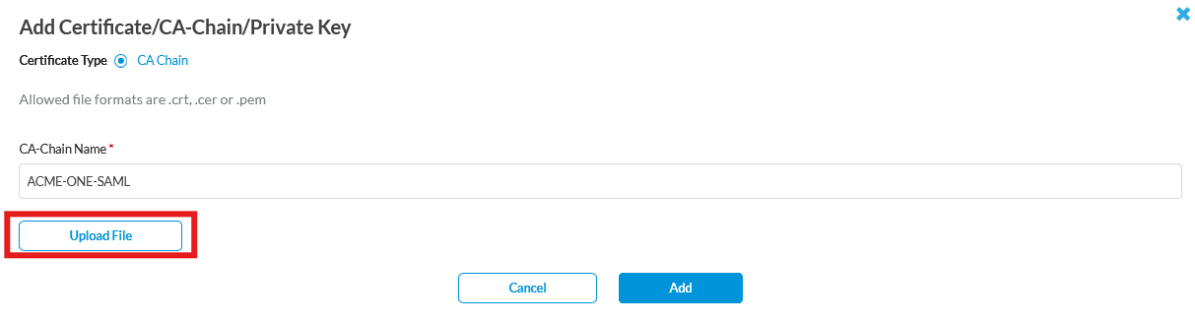
Identity Provider Issuer: https://sts.windows.net/a08ab2d2-a5df-481b-9ffa-bfb7a50a22c4/



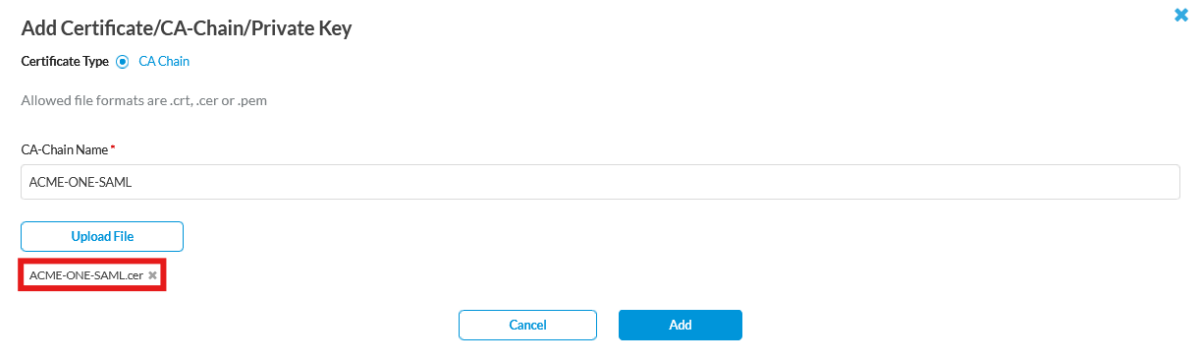
Then Upload the **Identity Provider Certificate** by clicking on the Add New button.



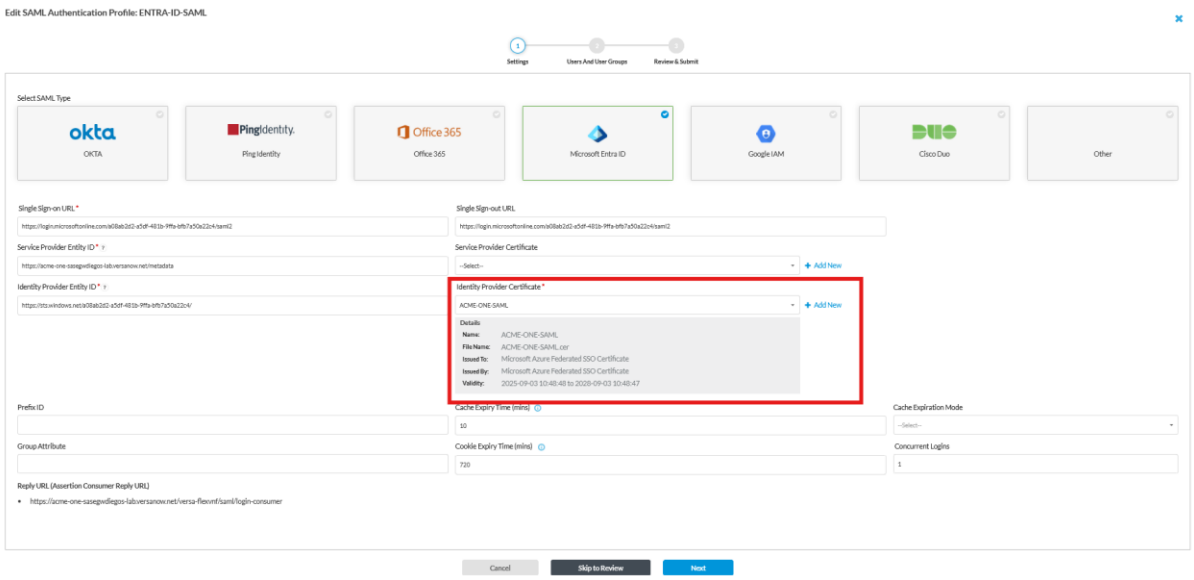
Name to **CA-Chain** Name upload certificate issue by clicking on the Upload File.



Then Add

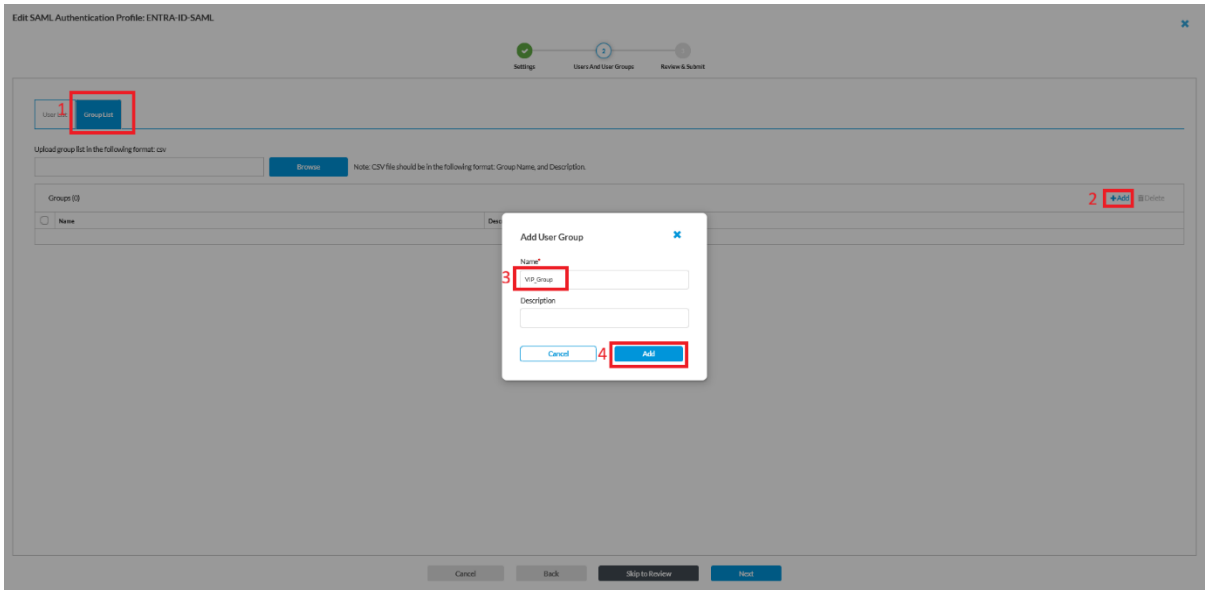


If certificate was uploaded successful, the certificate details will be displayed

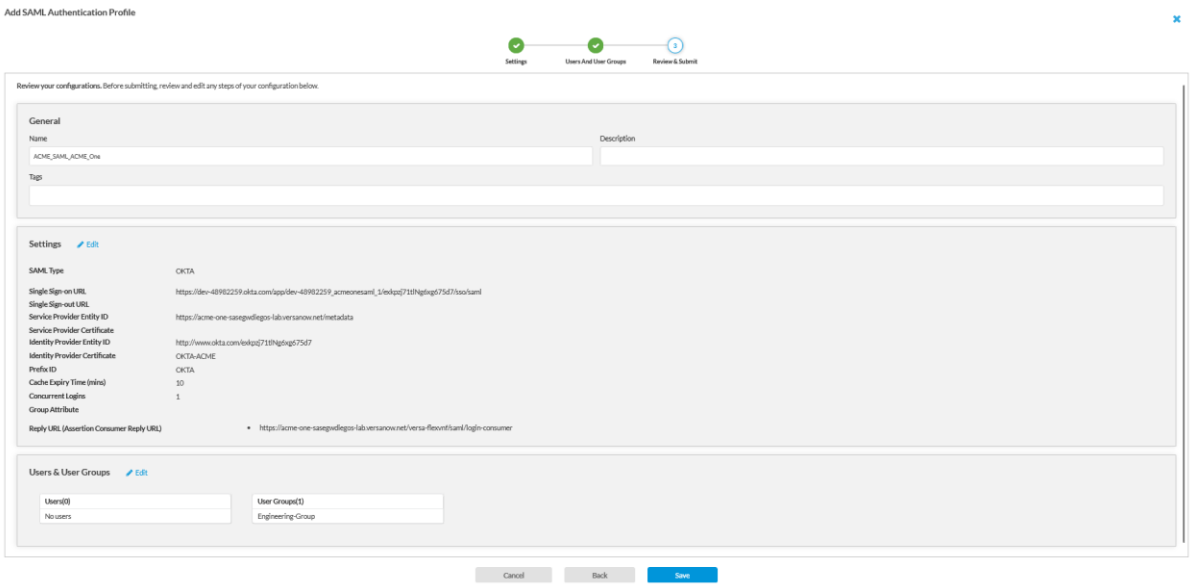


Then **Next**

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.



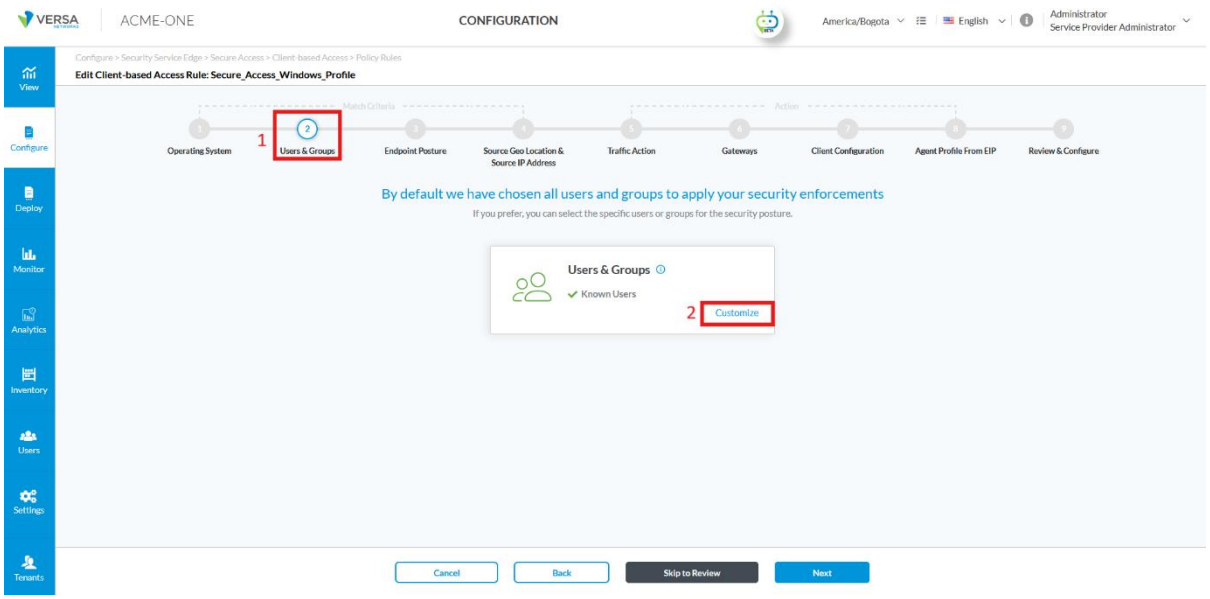
After creating and Publishin the Authentication Profile, you must apply them to the Secure Access Client policy to enforce authentication and apply the corresponding security policies.

Navigate to:

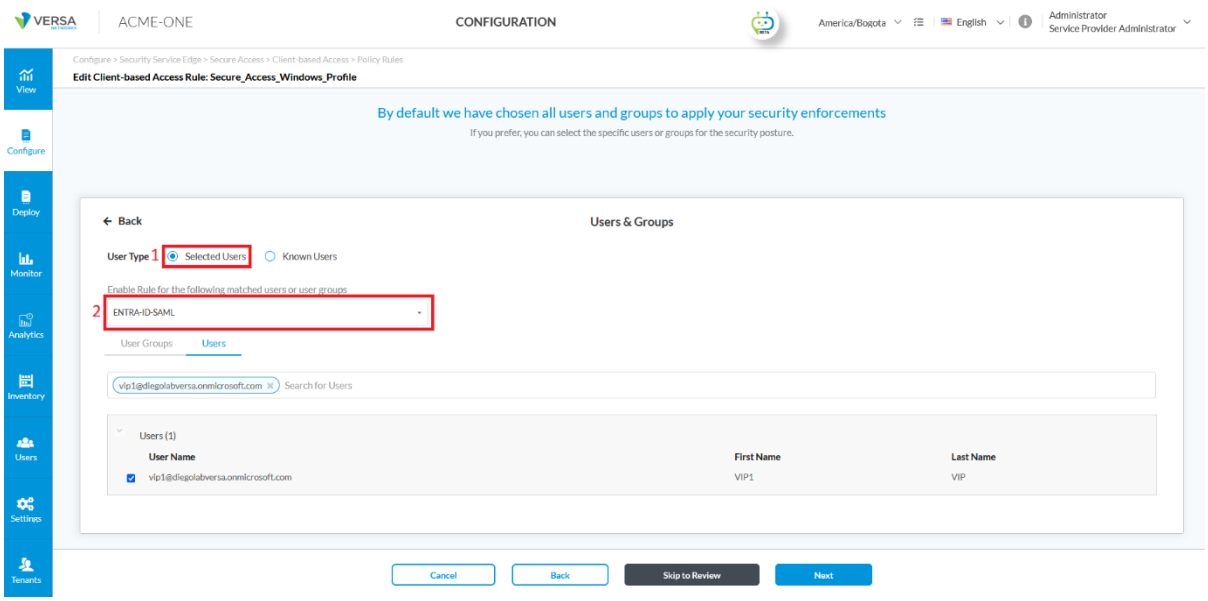
Configure > Security Service Edge > Secure Access > Client-based Access > Rules.

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

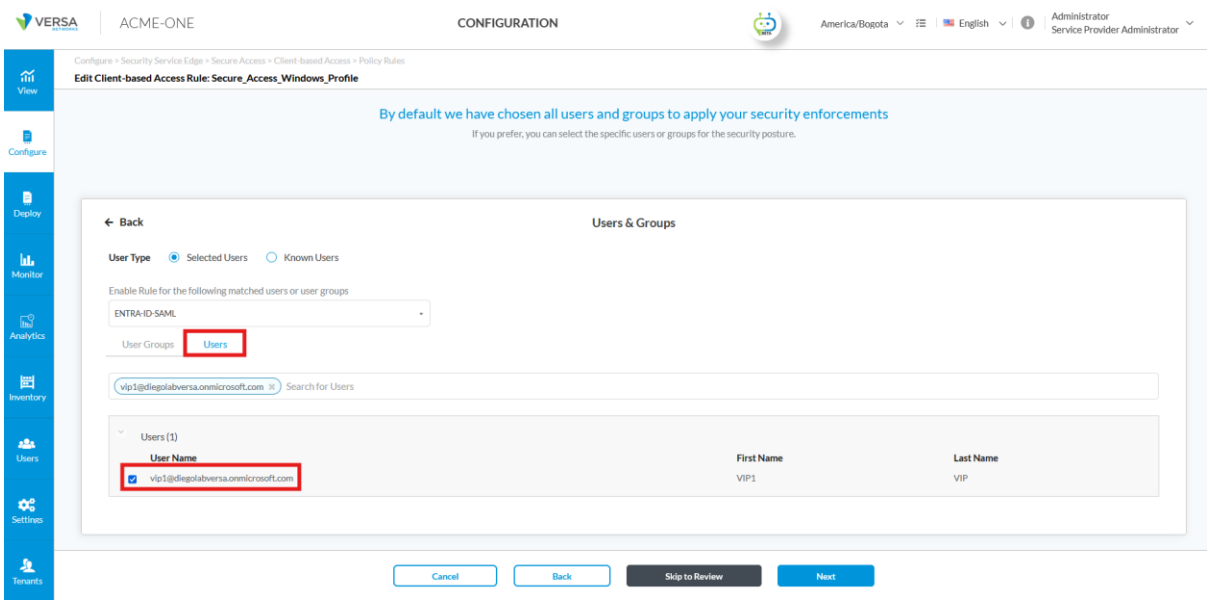
In the **Match Criteria** configuration, navigate to the **Users & Groups** section. Under the **Users & Groups** panel, click on **Customize** to begin specifying user-based access rules using the authentication profile you previously created.



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



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.

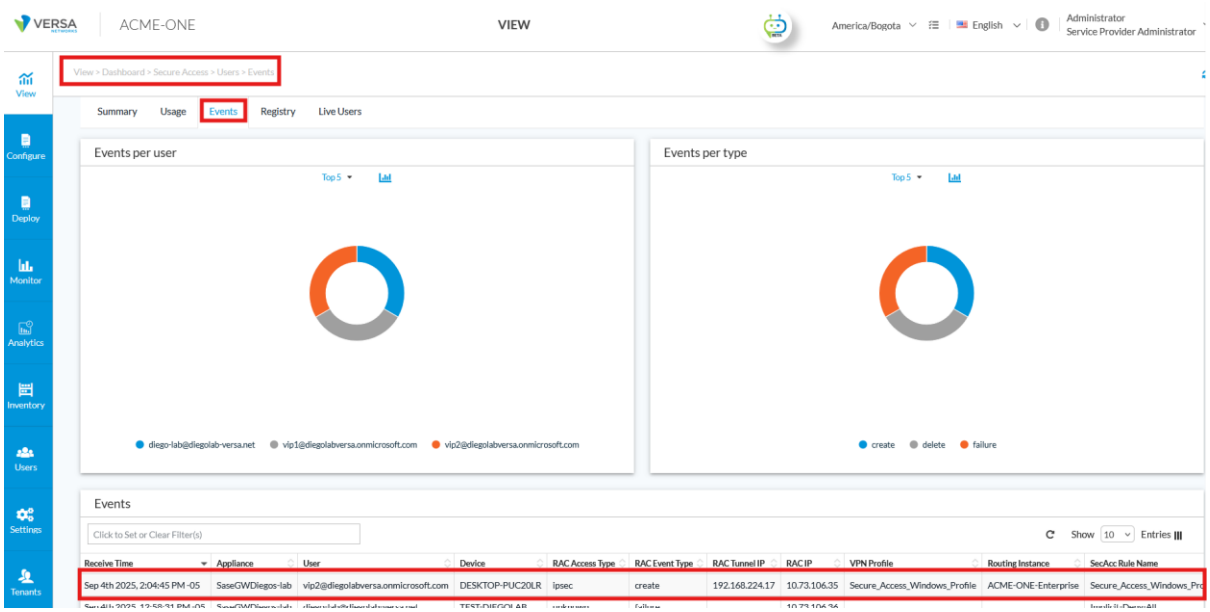


After reviewing all configuration sections, click **Save** to apply the settings to the current Secure Access Profile. Then go to the **Publish** section at the top-right corner of the screen and click **Publish**.

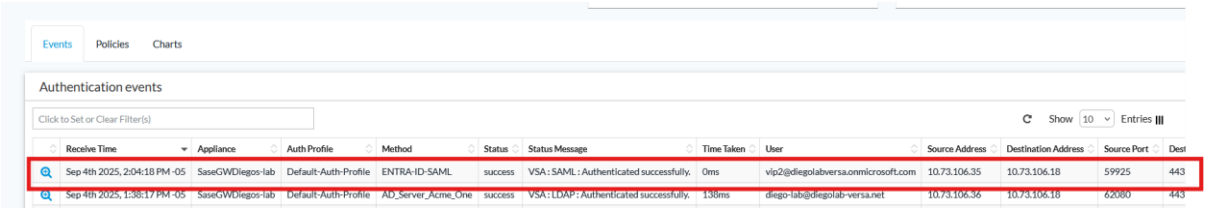
Verification

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.



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



Additionally, administrators can confirm active sessions and mapped users via CLI commands on SaseGateway typping 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 you tenant is that enabled on Headend at infrasture level by Versa or MSP(if using thirdparty hosted headend): https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_User_and_Device_Authentication#Configure_Versa_Directory_Authentication_Using_an_IAM_Server

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

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

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.

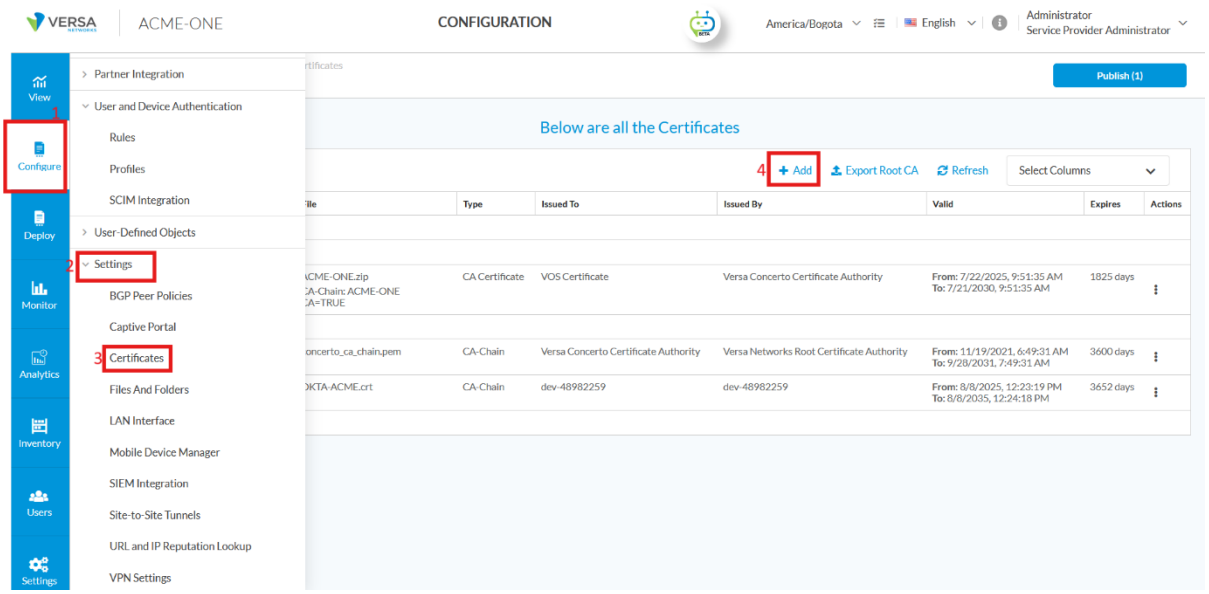
5. **Pre-Logon Stage**: Toggle the option to enable device certificate-based authentication during pre-logon if required.

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.

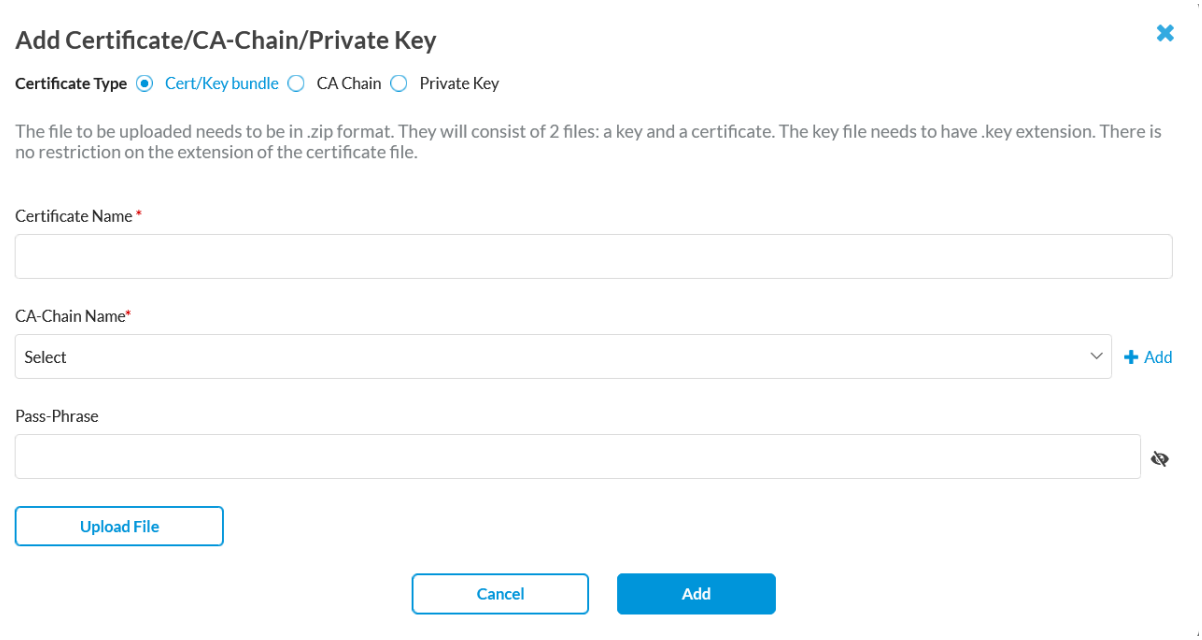
Ensure the Root CA is uploaded to Gateways from Concerto and reflected correctly in the Device:

Navigate to Certificates Go to: Configure > Security Service Edge > Settings > Certificates then "+ Add"



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

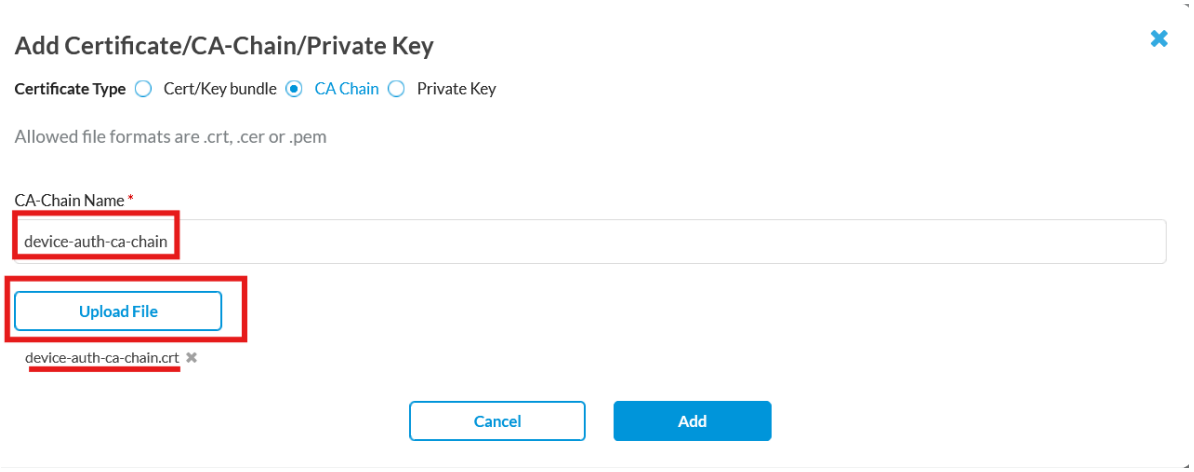
- CA Chain, or Cert/Key bundle, or Private Key.



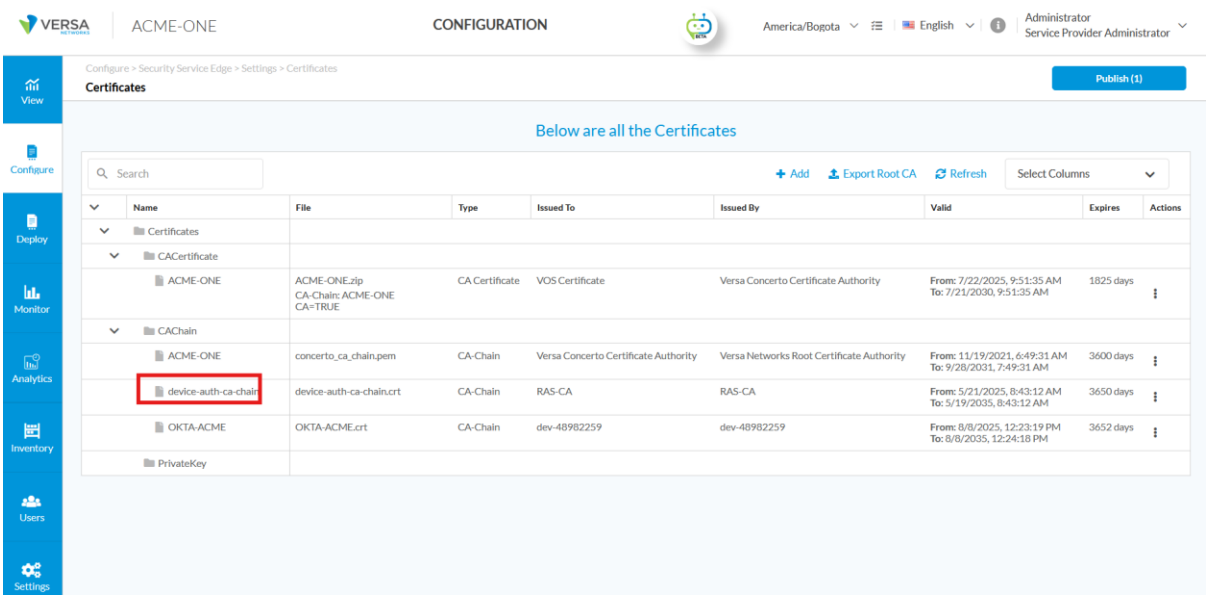
As an Example, Add a **CA Chain**

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

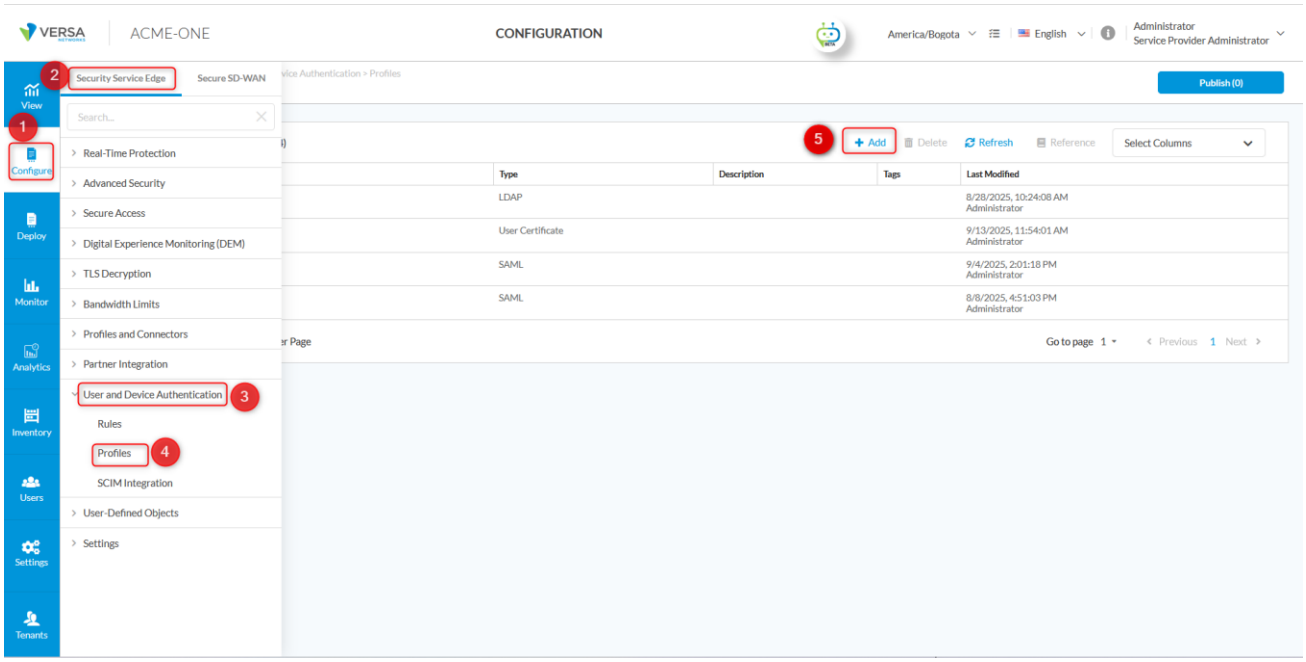
- Click **Upload File** and select the CA chain file.
- Click **Add**.



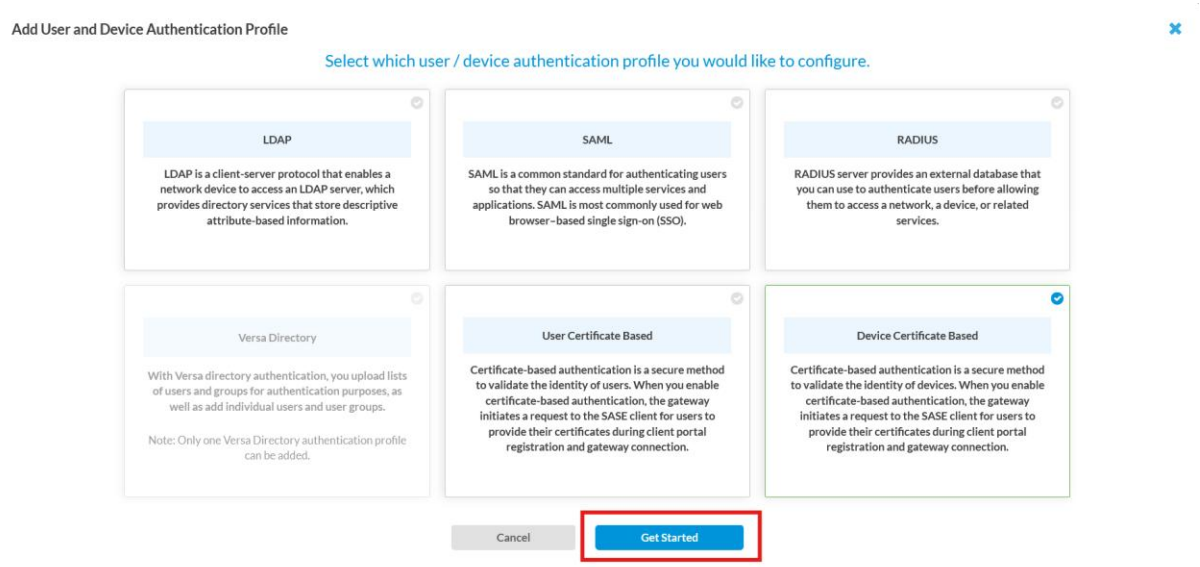
Now check CA Chain (device-auth-ca-chain) is successfully uploaded and listed under Configure > Security Service Edge > Settings > Certificates :



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**

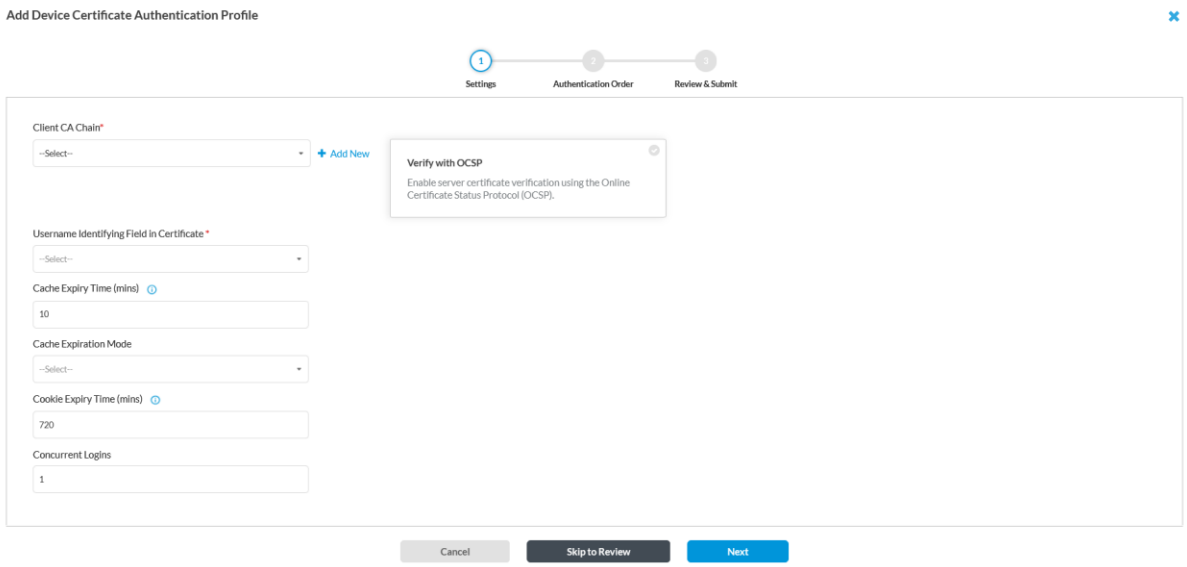


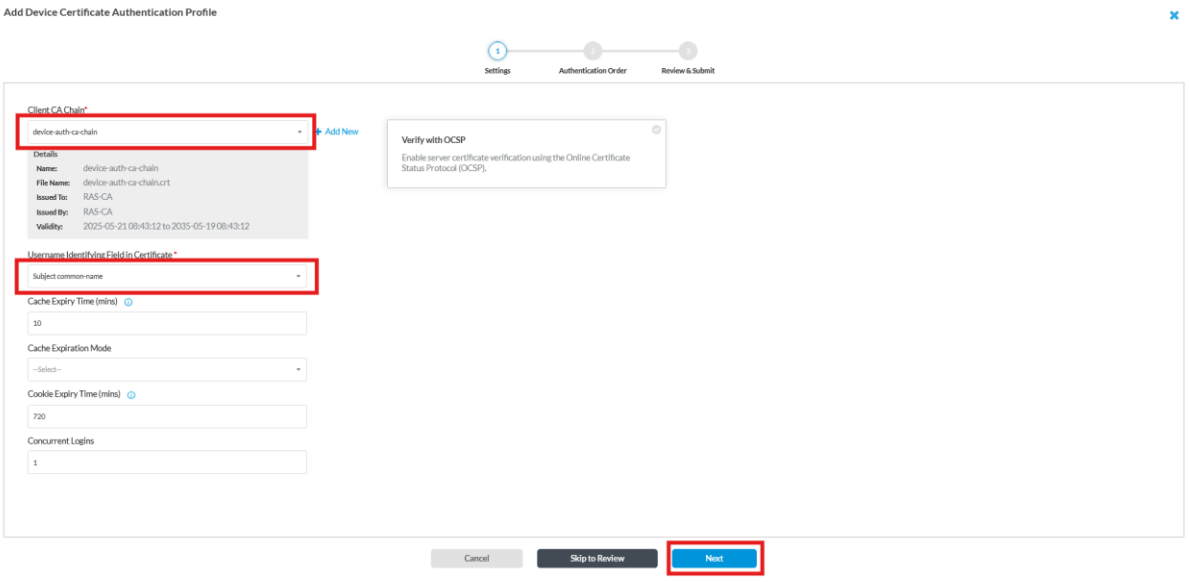
In Add Device Certificate Authentication Profile > Settings:

- **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

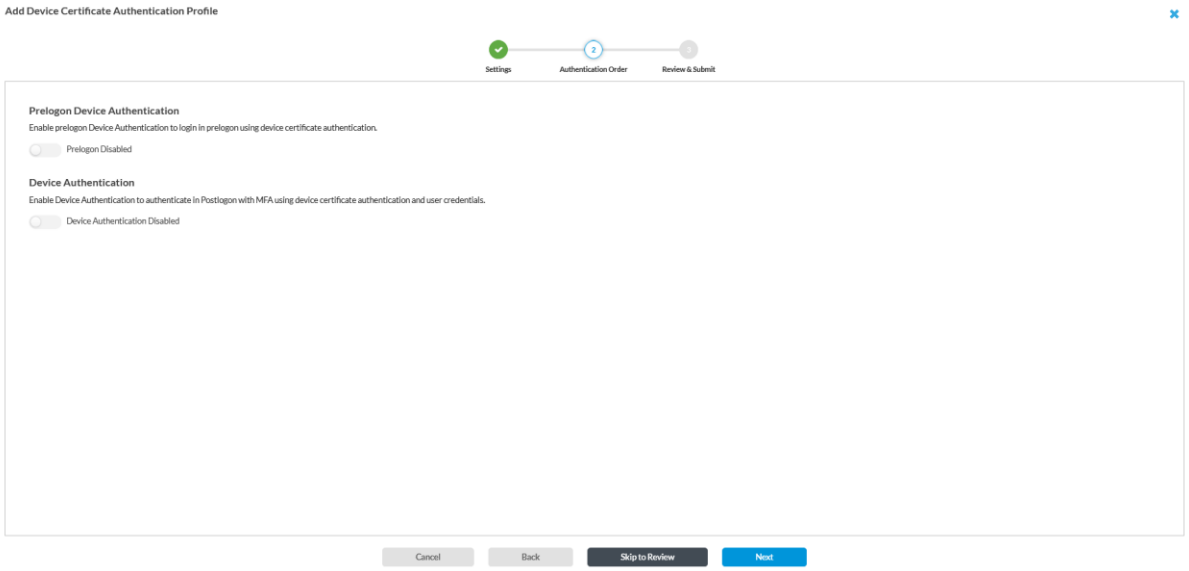


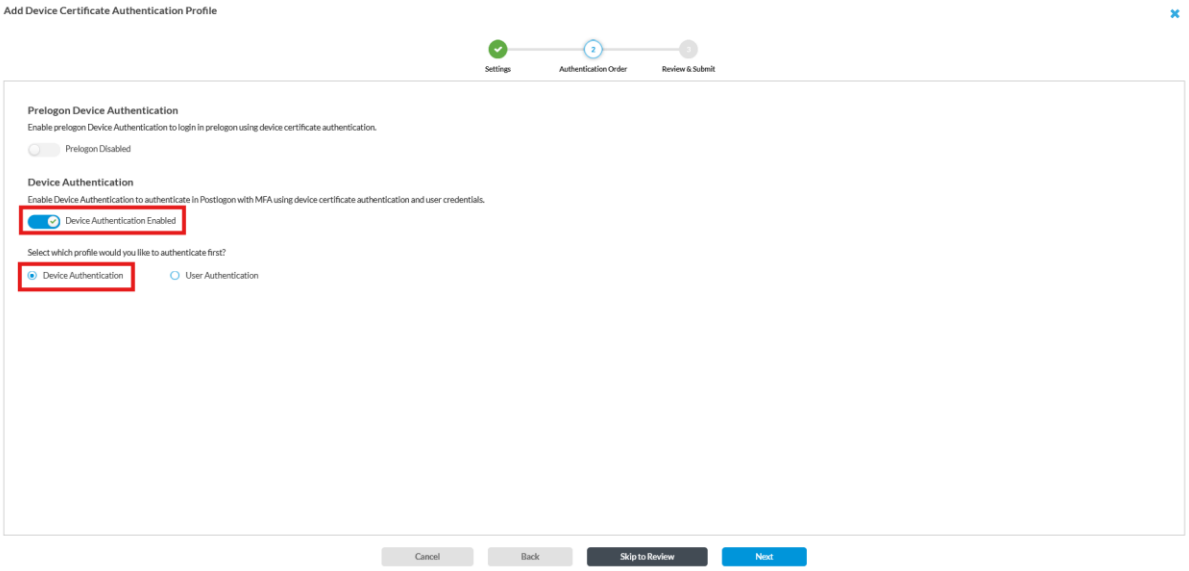


In Authentication Order, you can optionally enable Pre-login devices to authenticate before user login. If you do not need this feature, leave it as **Disabled**.

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.





Then Click **Next** to continue

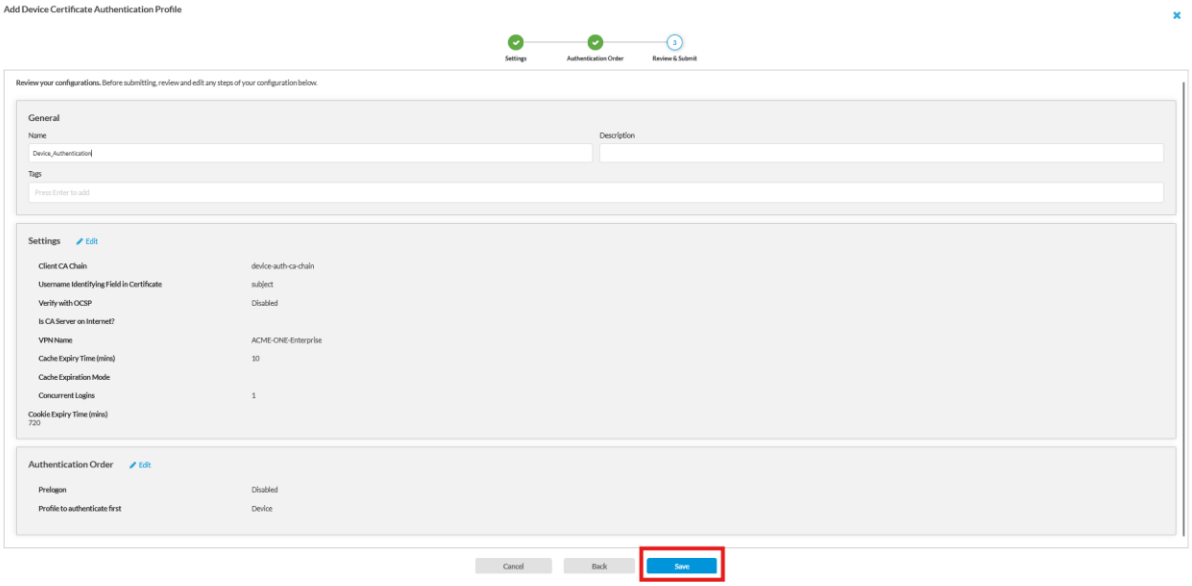
In the Review & Submit page:

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

Confirm Username Identifying Field = subject.

Verify Authentication Order = **Device**.

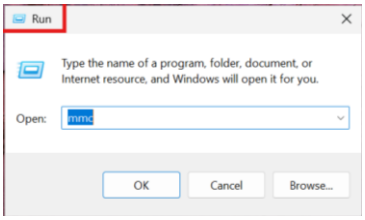
Click **Save** then **Publish**.



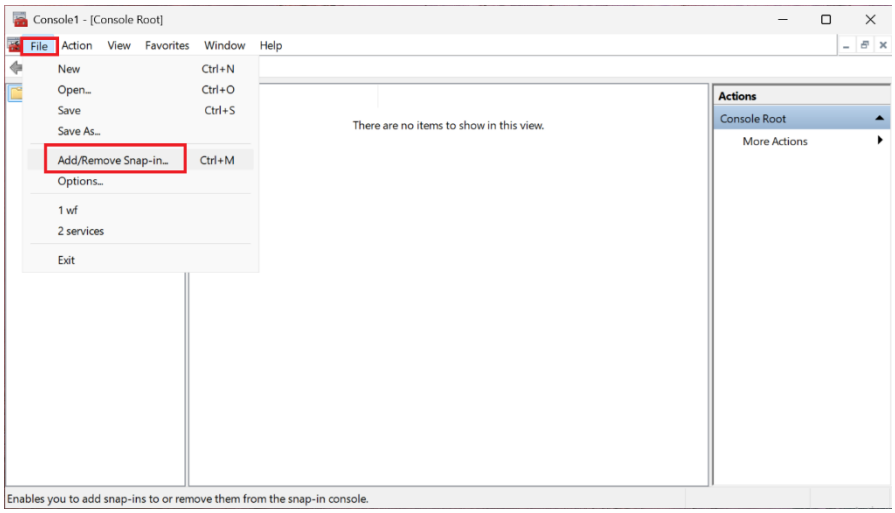
Installing Certificates on the Client Device:

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)

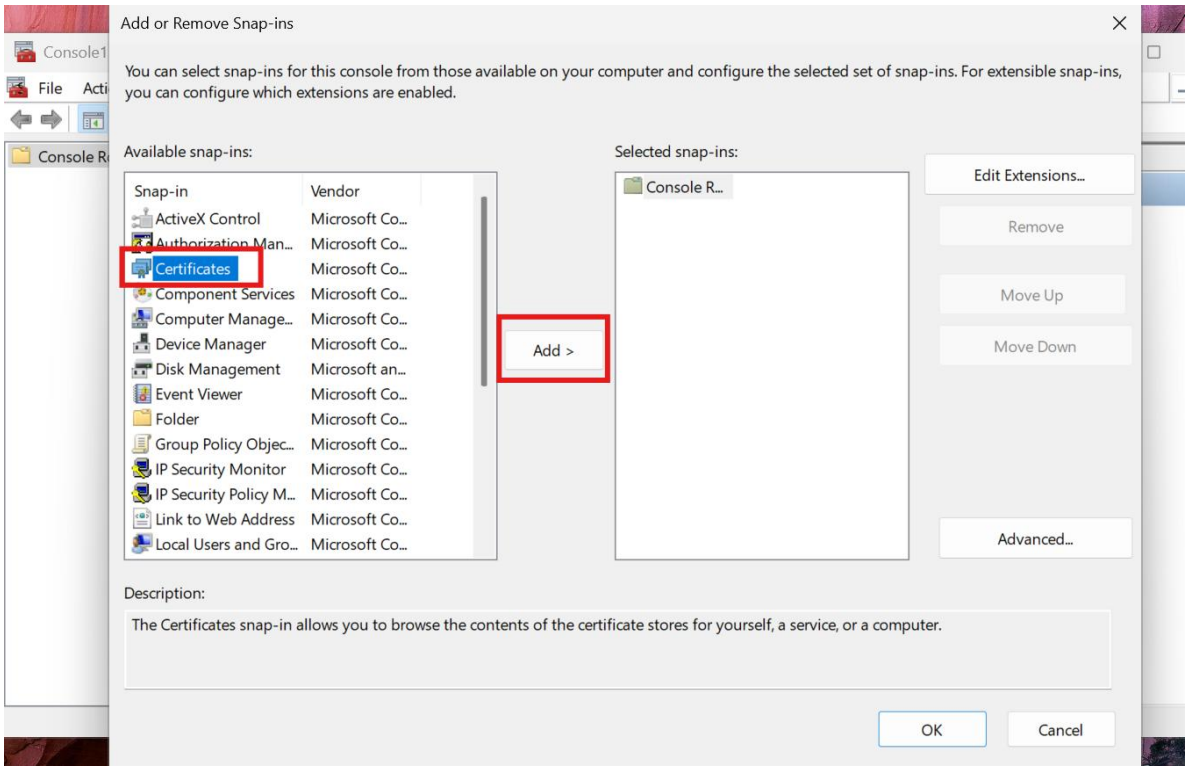
For Windows open the Run dialog, type mmc, and press Enter.

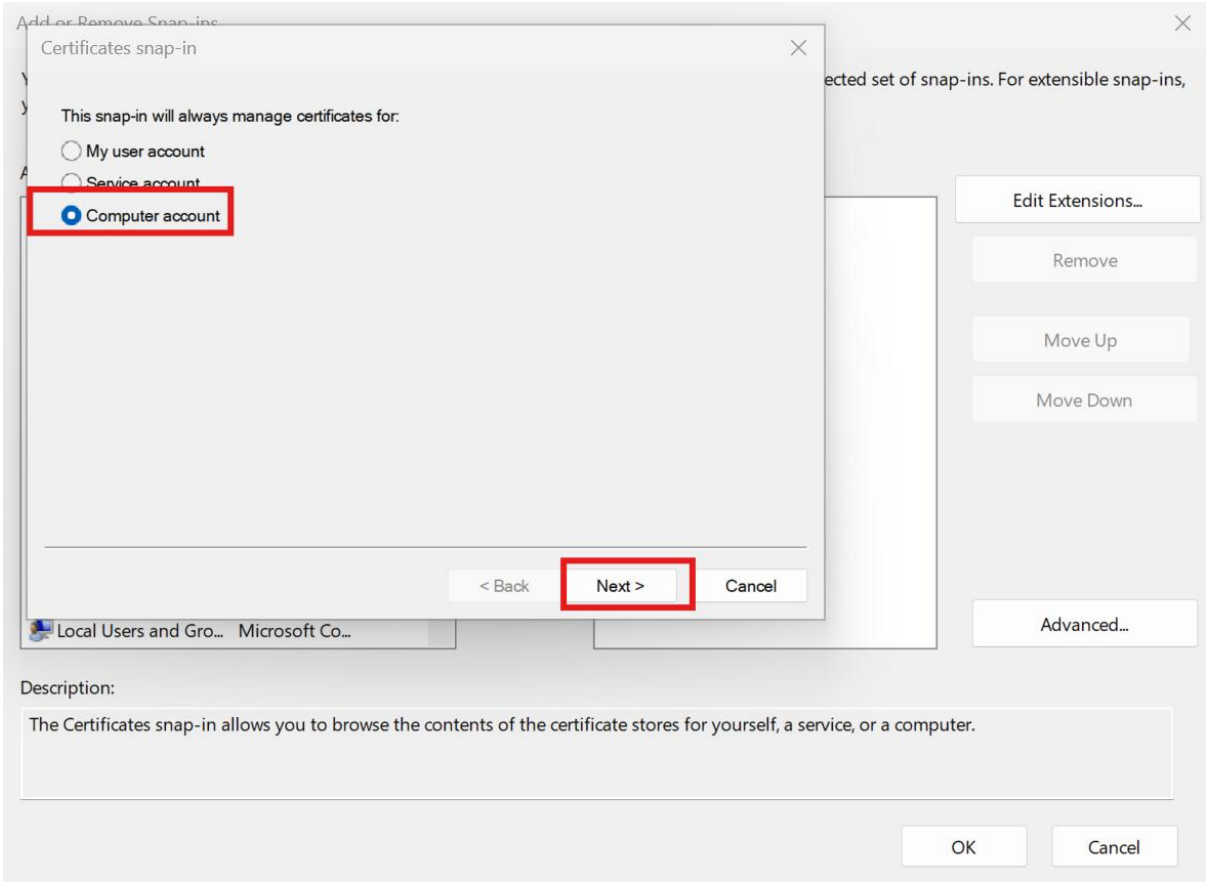


In the MMC console, go to File → Add/Remove Snap-in.

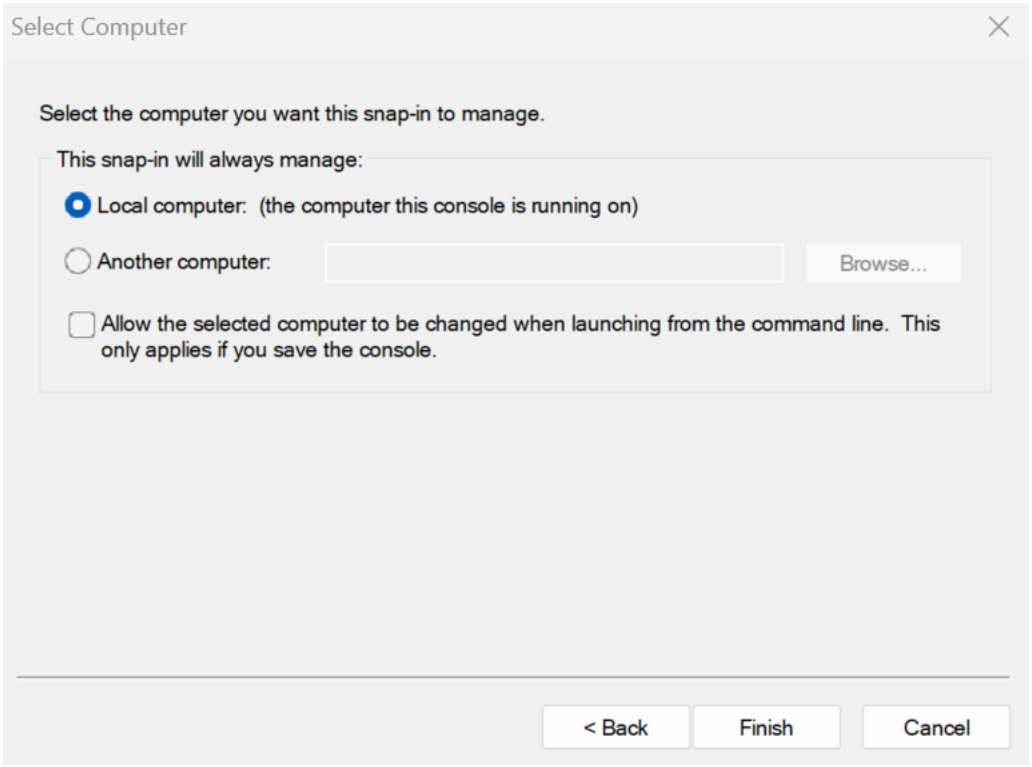


Select Certificates, click Add, and choose Computer Account to manage device-level certifi-
cates.

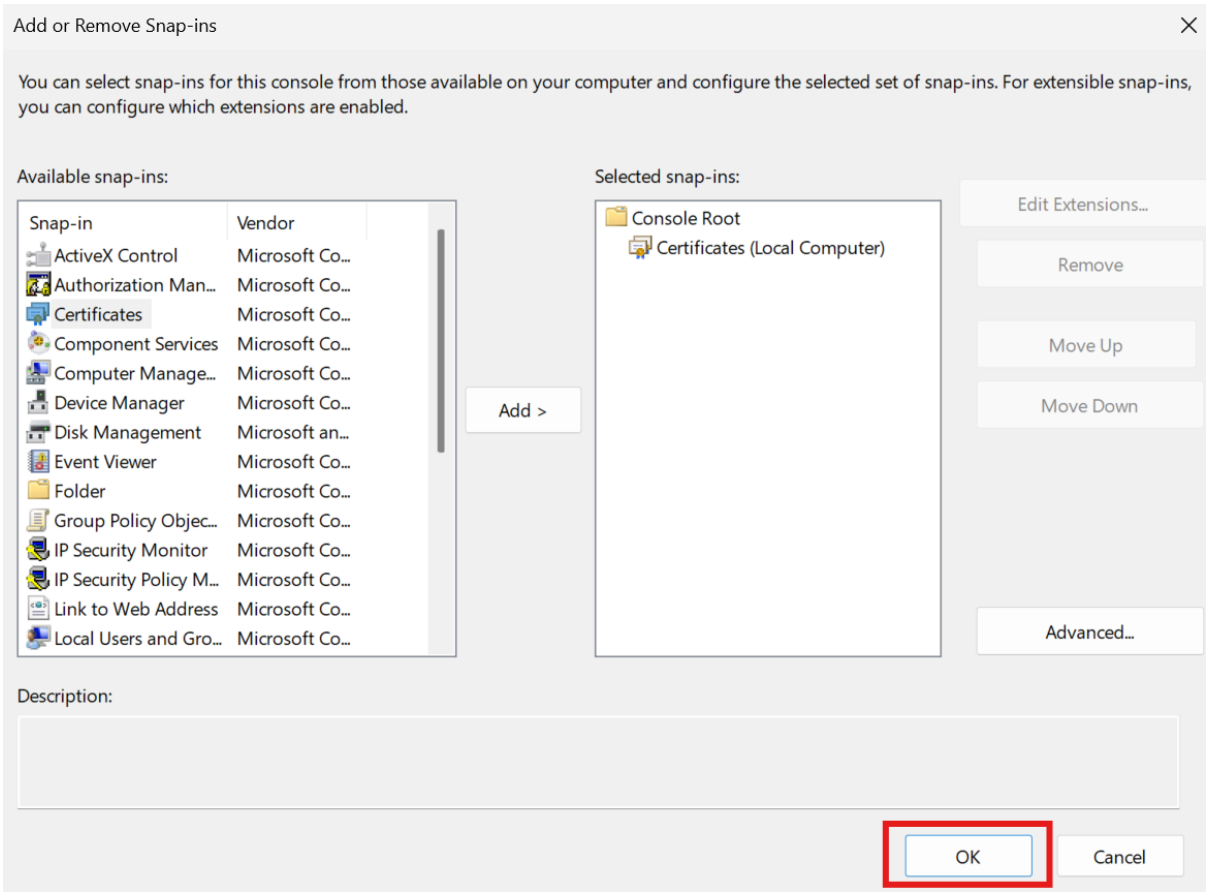




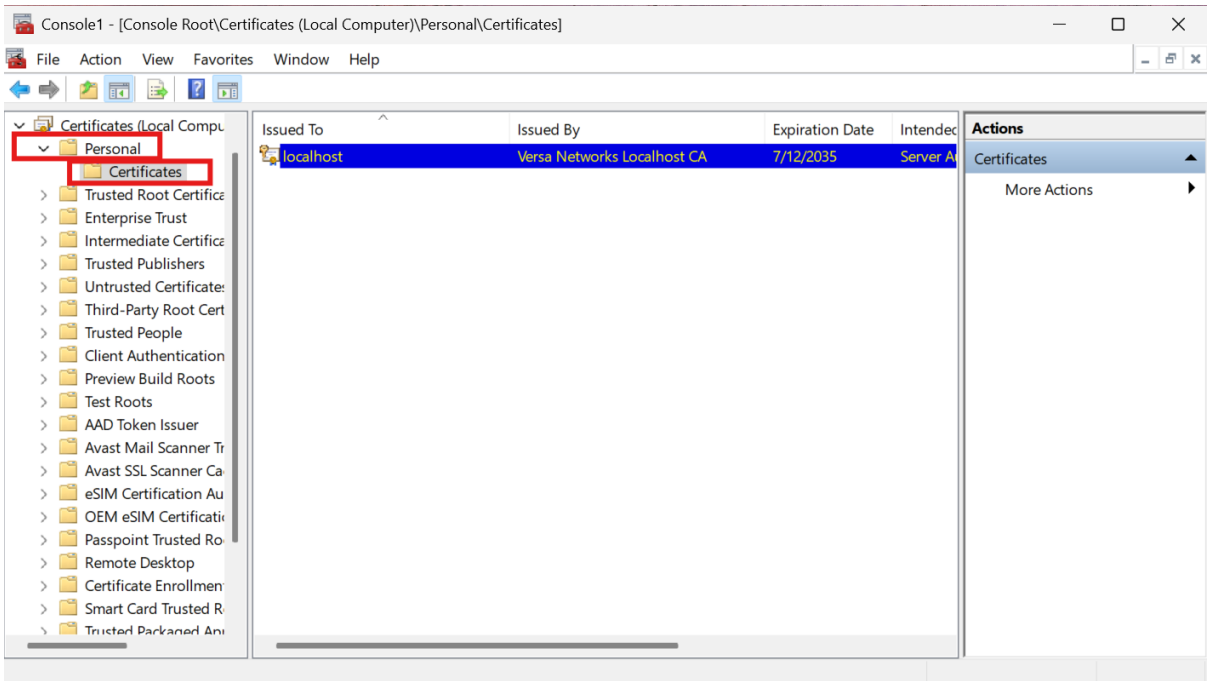
Choose Local Computer and Finish.



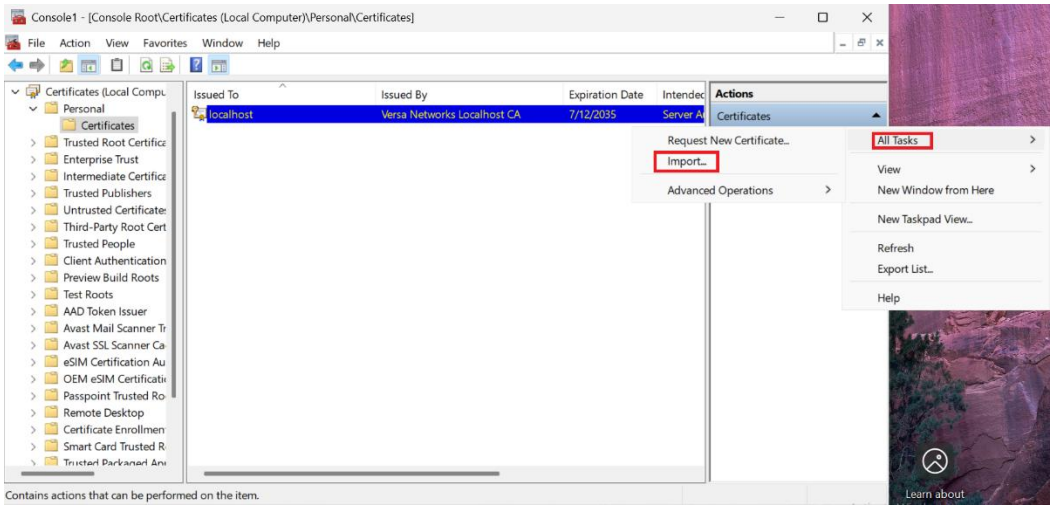
Then OK.



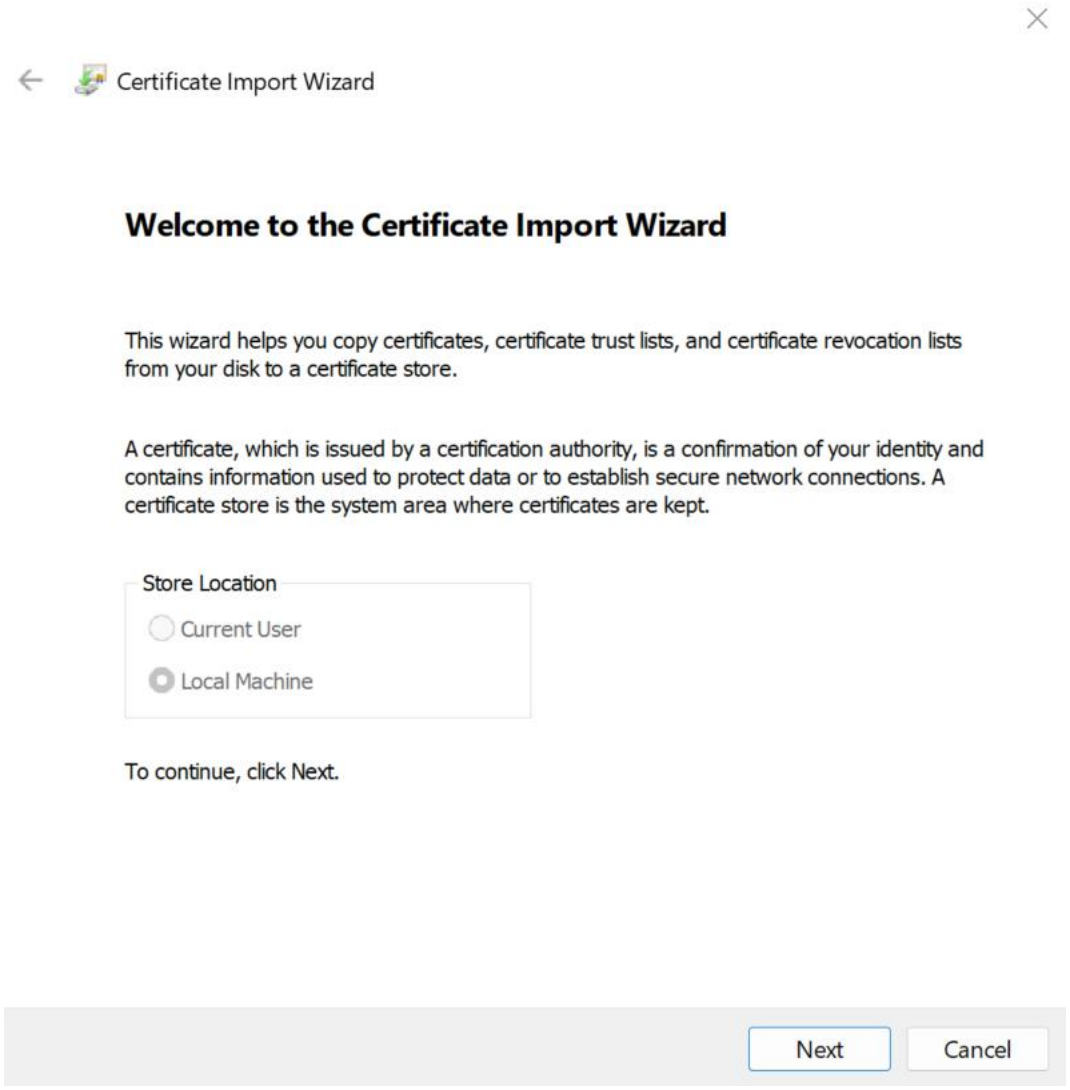
Right-click on the **Certificates** folder under **Personal.**



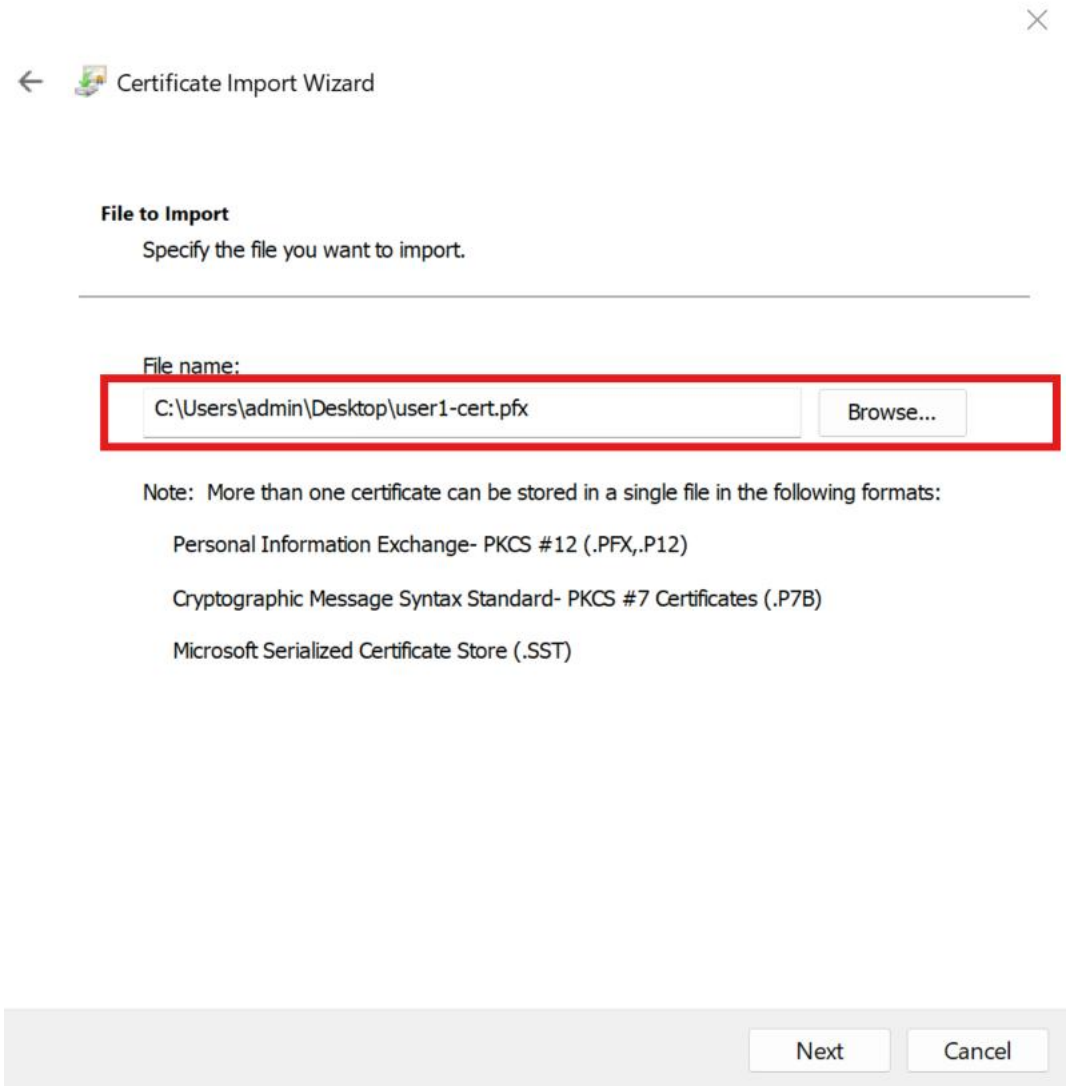
go to More Actions then **All Tasks > Import**.



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



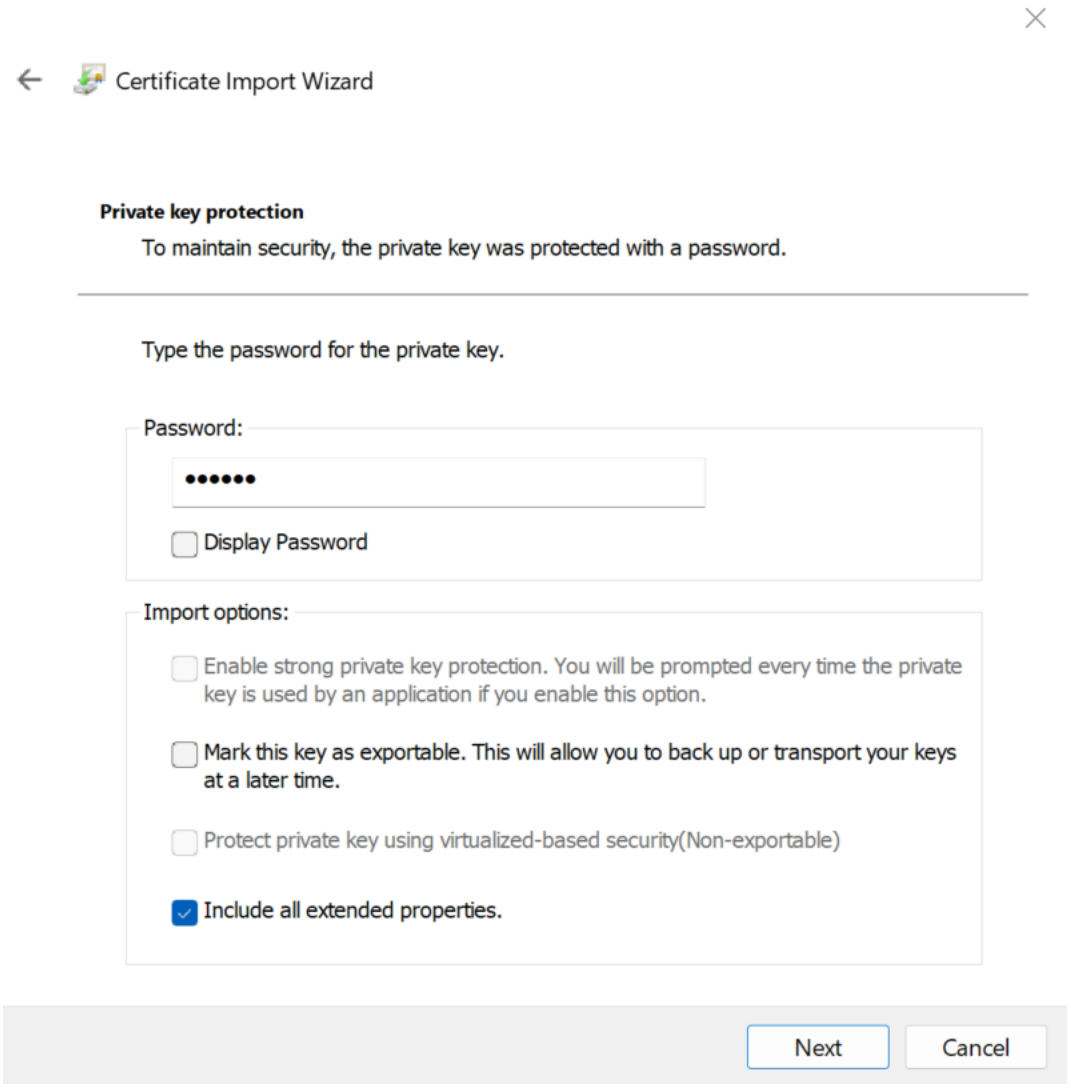
Browse to the location of the certificate file (for example user1-cert.pfx), select it, and click **Open**



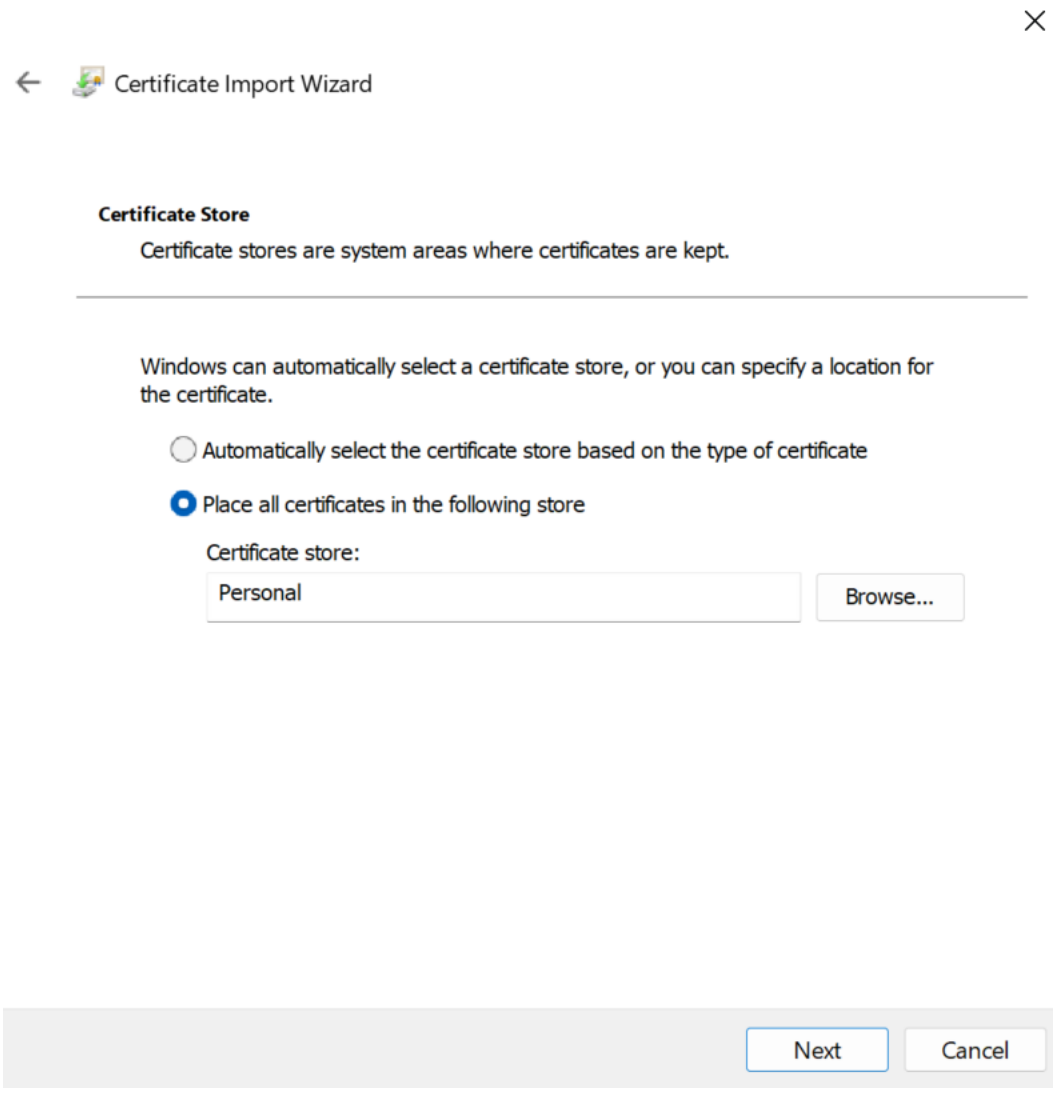
Enter the certificate's private key password.

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

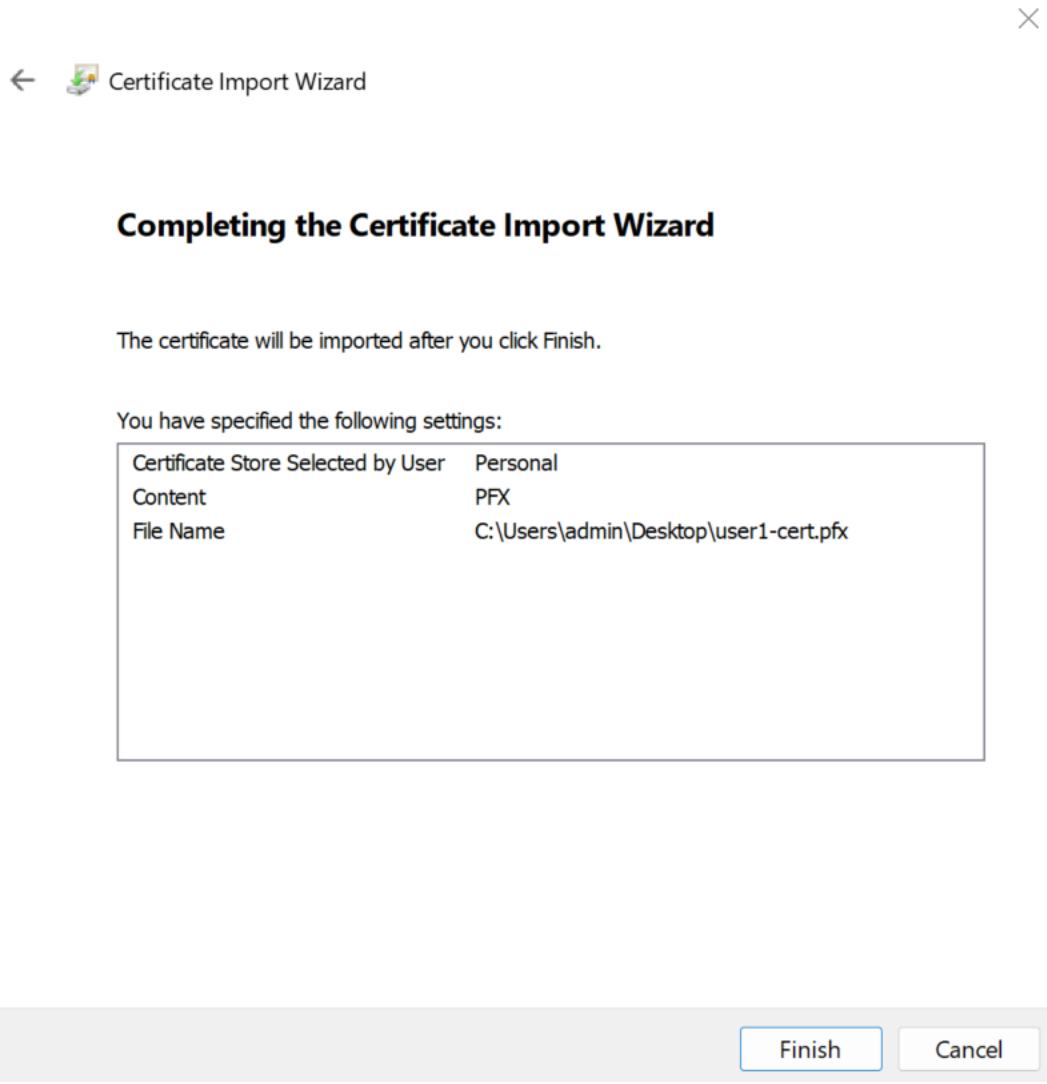
  Click Next.



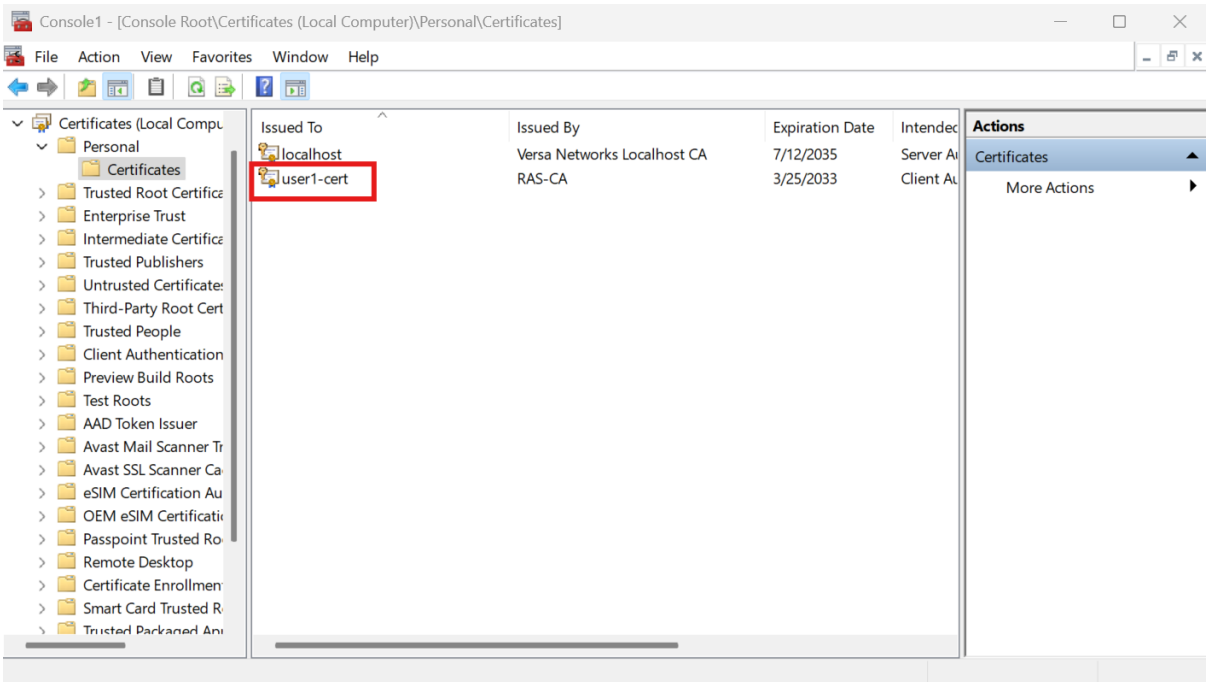
On the **Certificate Store** screen, select **Place all certificates in the following store**, ensure it is set to **Personal**, and click **Next**.



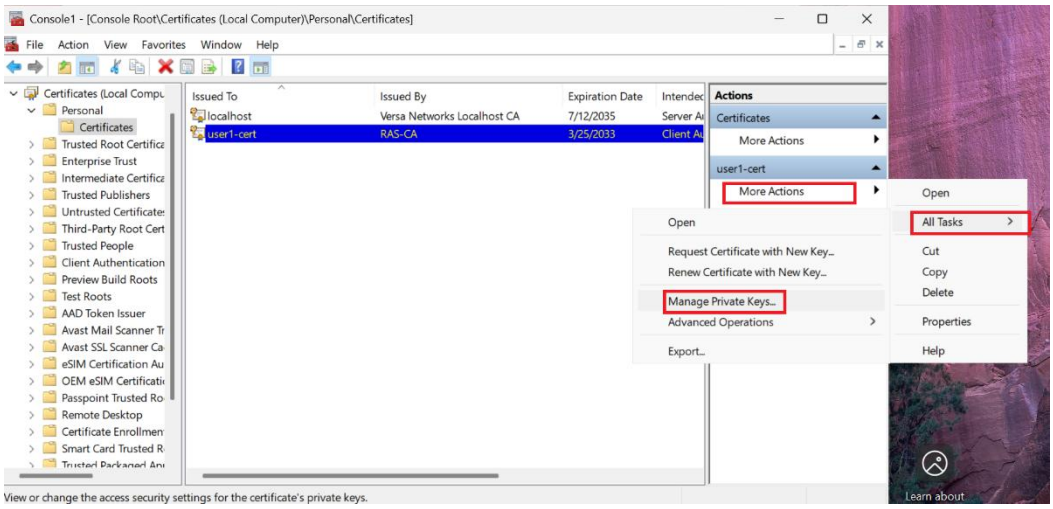
Click **Finish** to complete the import. A confirmation message should appear: **"The import was successful.**"



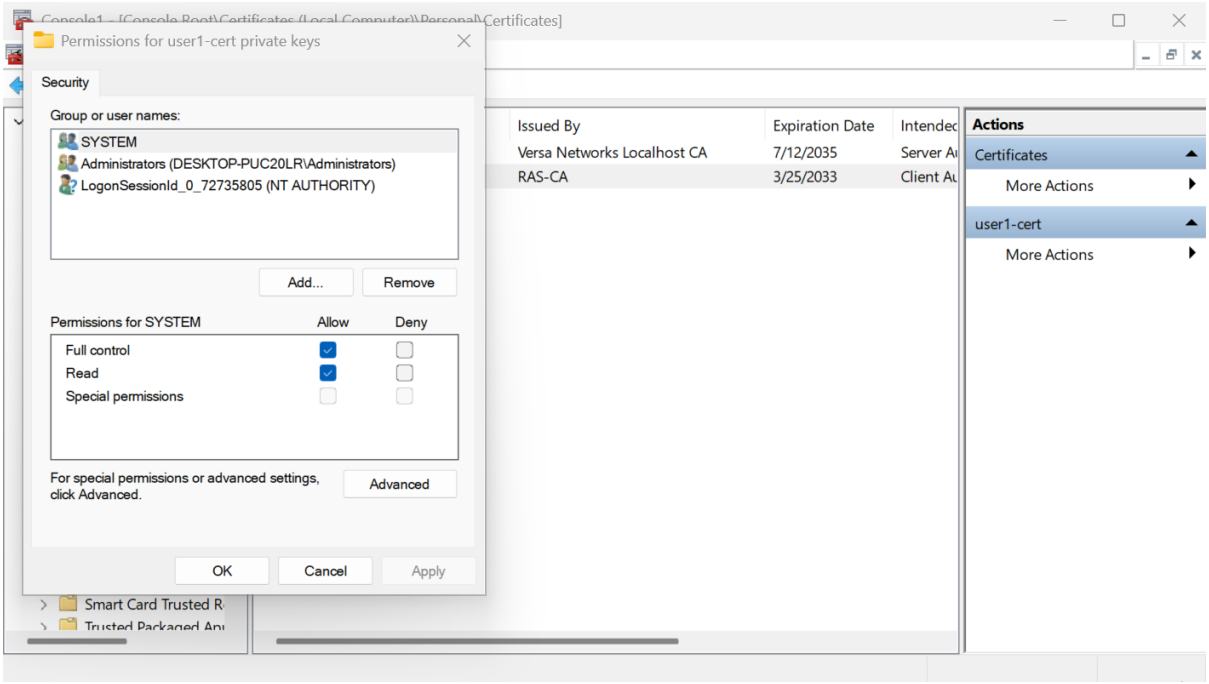
Verify that the imported certificate is visible under: **Certificates (Local Computer) > Personal > Certificates.**



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**.



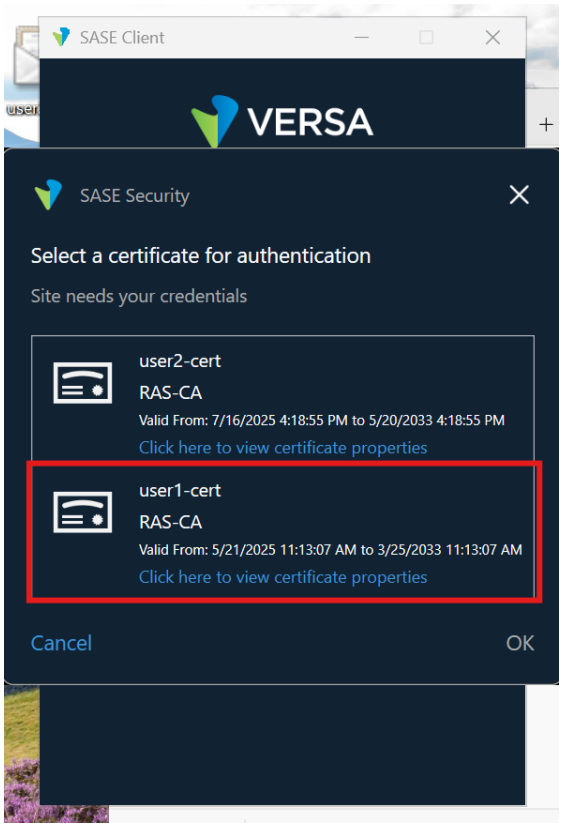
Assign permissions for users.



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.


SASE Client
VERSA
SASE Security
Select a certificate for authentication
Site needs your credentials
user2-cert
RAS-CA
Valid From: 7/16/2025 4:18:55 PM to 5/20/2033 4:18:55 PM
Click here to view certificate properties
user1-cert
RAS-CA
Valid From: 5/21/2025 11:13:07 AM to 3/25/2033 11:13:07 AM
Click here to view certificate properties
Cancel
OK

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.

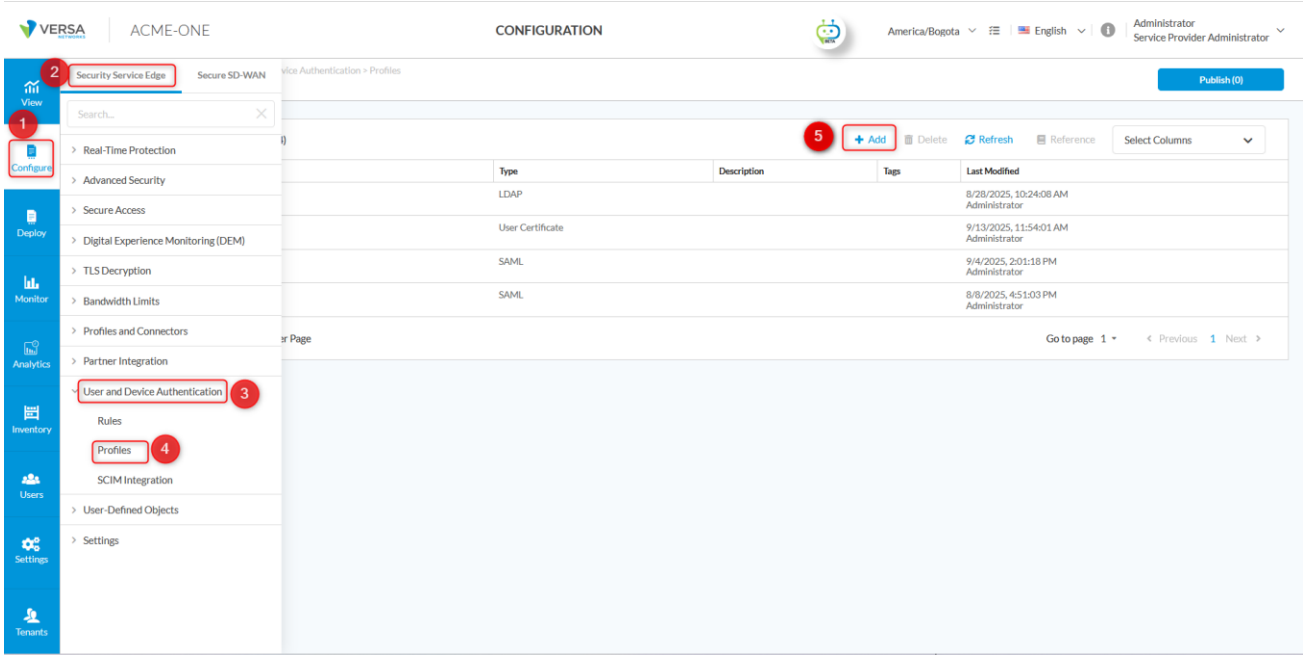
3. **Remote Workforces with Layered Authentication:** Users authenticate through SAML (e.g., Okta, Azure AD), while their certificates validate their personal identity at the gateway. This layered approach enforces Zero Trust principles by ensuring that both the user credentials and the associated certificate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

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

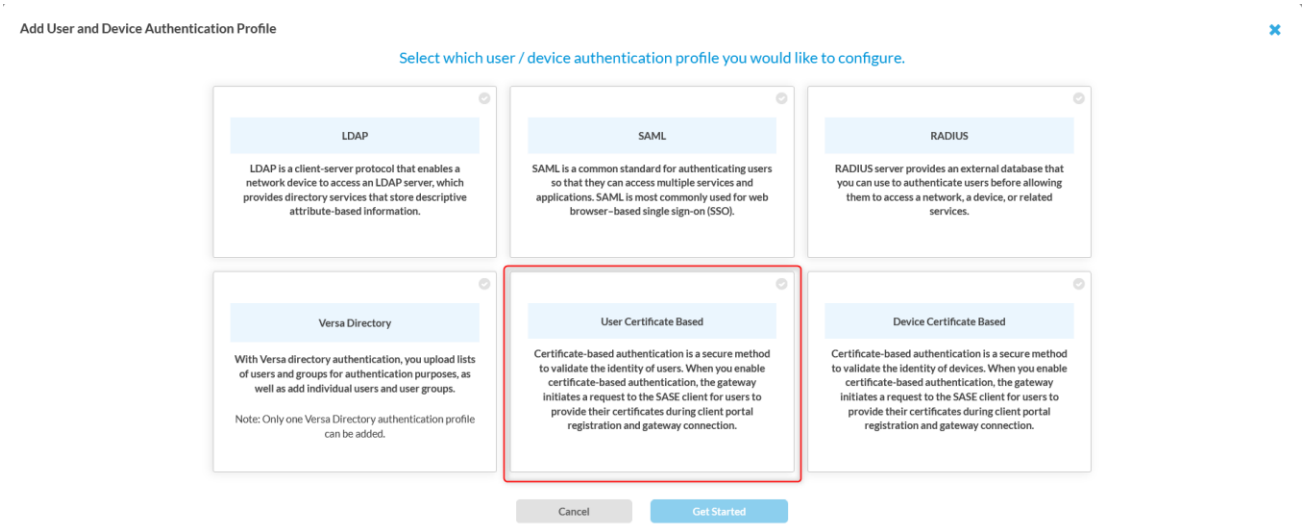
   User and device certificates can be combined for layered authentication. The device certificate confirms the integrity and trust level of the hardware, while the user certificate validates the person operating it. This two-tier validation ensures that both the endpoint and the user meet the organization's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



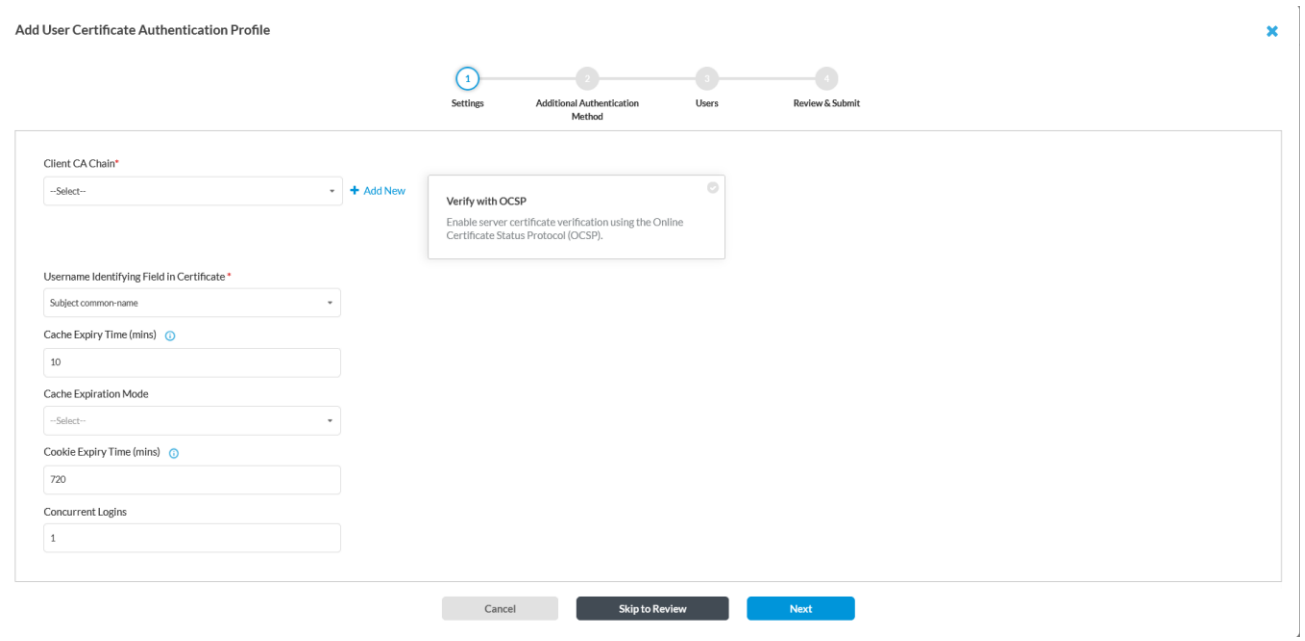
Select **User Certificate Based** as Authentication Method then Click **Get Started**

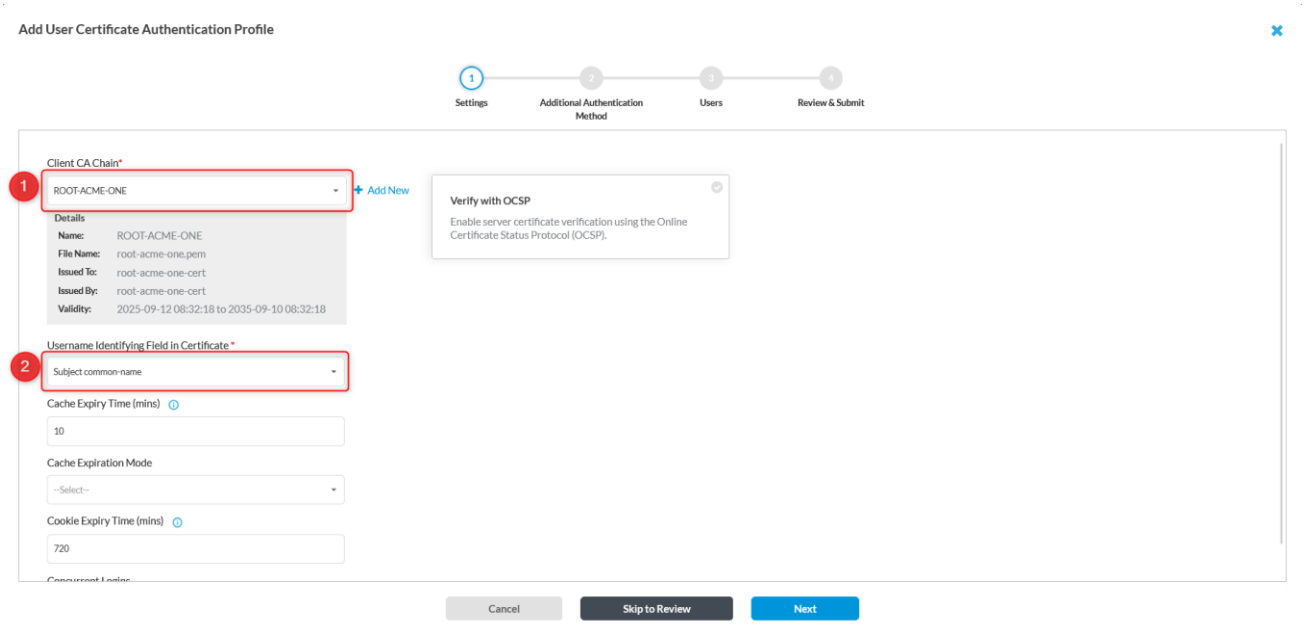


In Add User Certificate Authentication Profile > Settings:

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

Then Click **Next** to continue

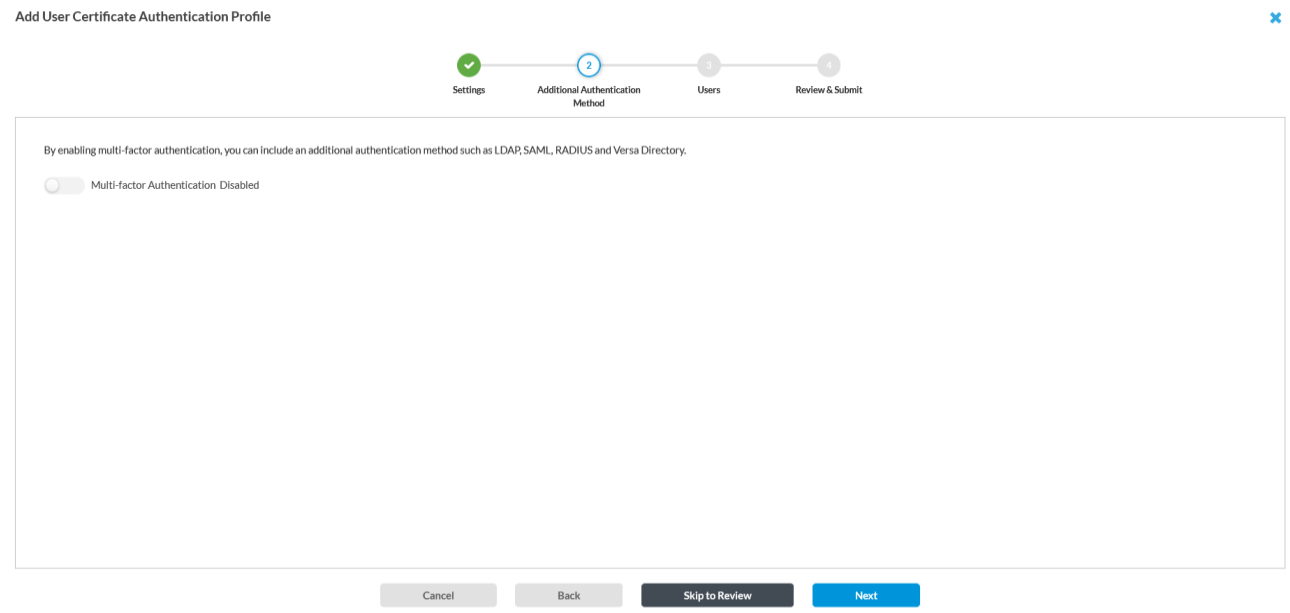


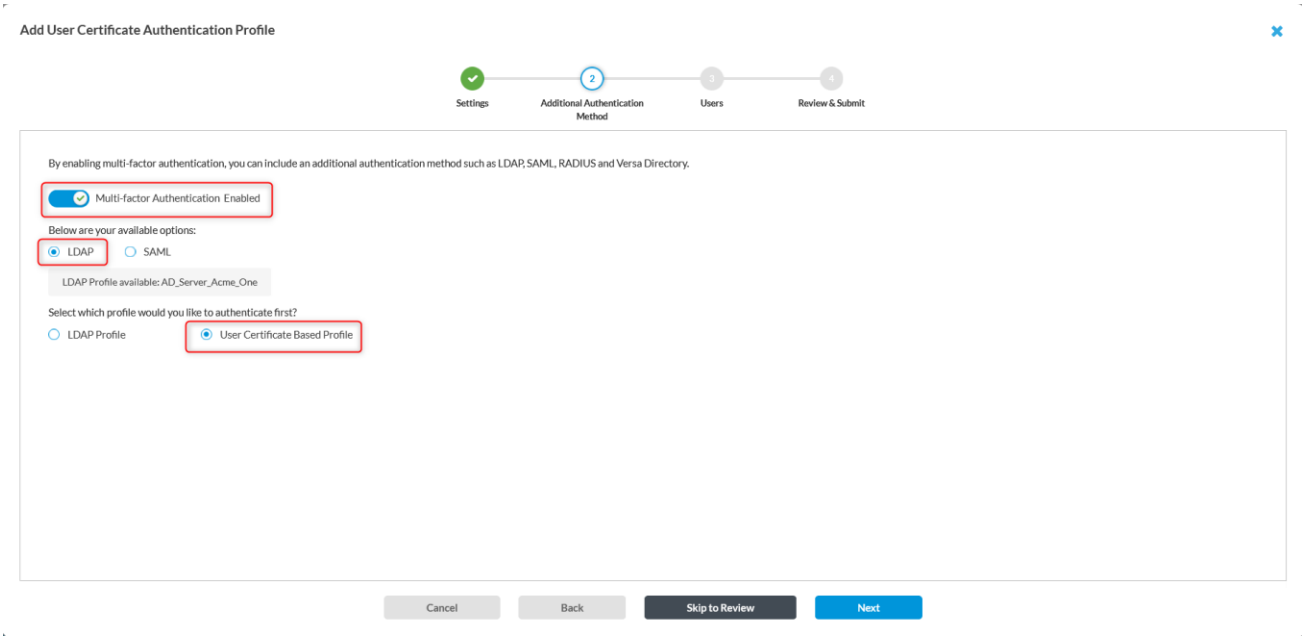


In **Additional Authentication Method**, you can enable **Multi-factor Authentication**. If left **Disabled**, only the user certificate is used for authentication.

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.





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

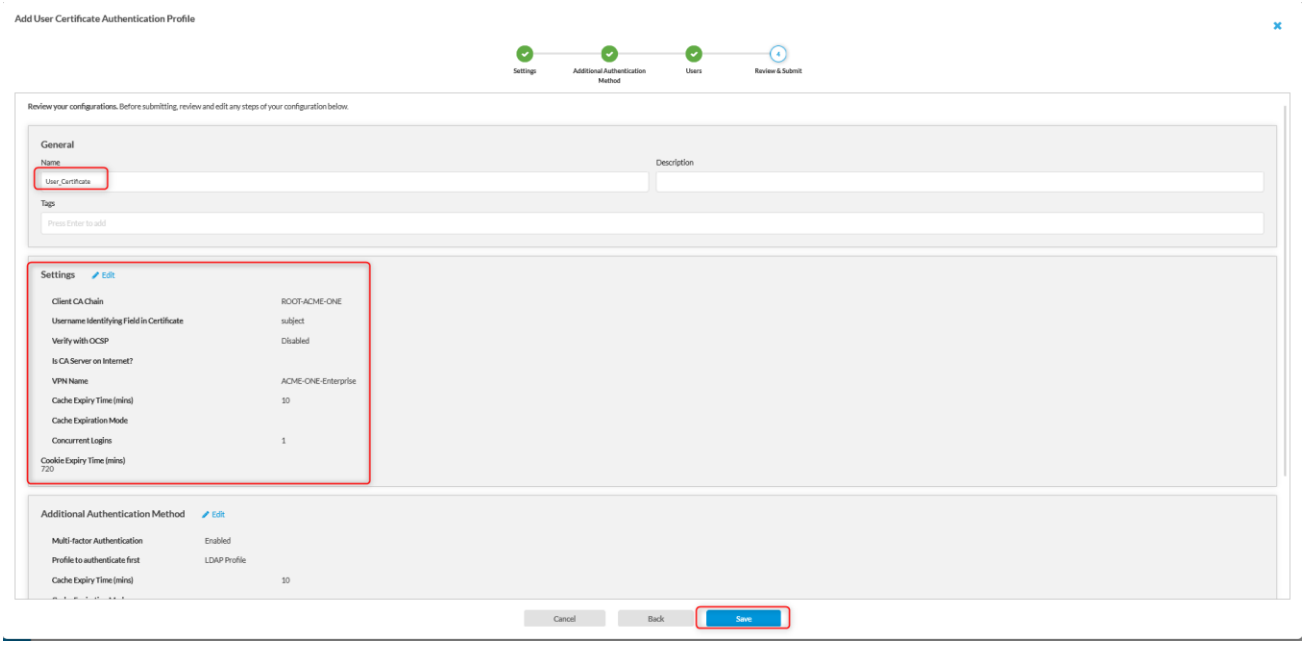
In the **Review & Submit** page: you can provide a **Name** and an optional **Description** for the profile. Use these fields to clearly identify the purpose of the configuration.

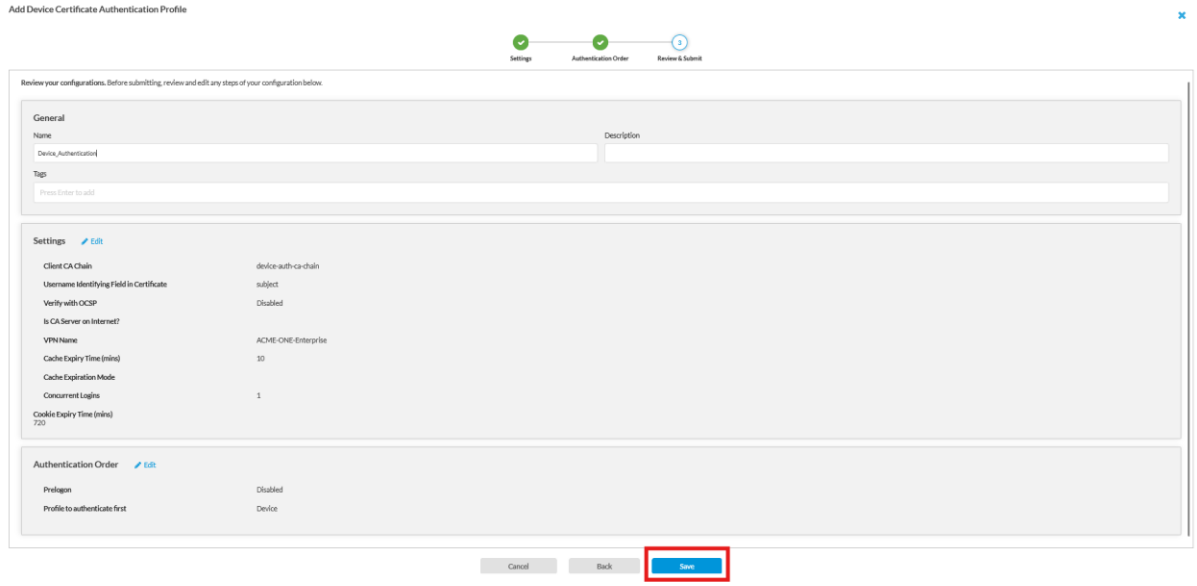
Confirm the Client CA Chain = device-auth-ca-chain.

Confirm Username Identifying Field = subject.

Verify Additional Authentication Method.

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





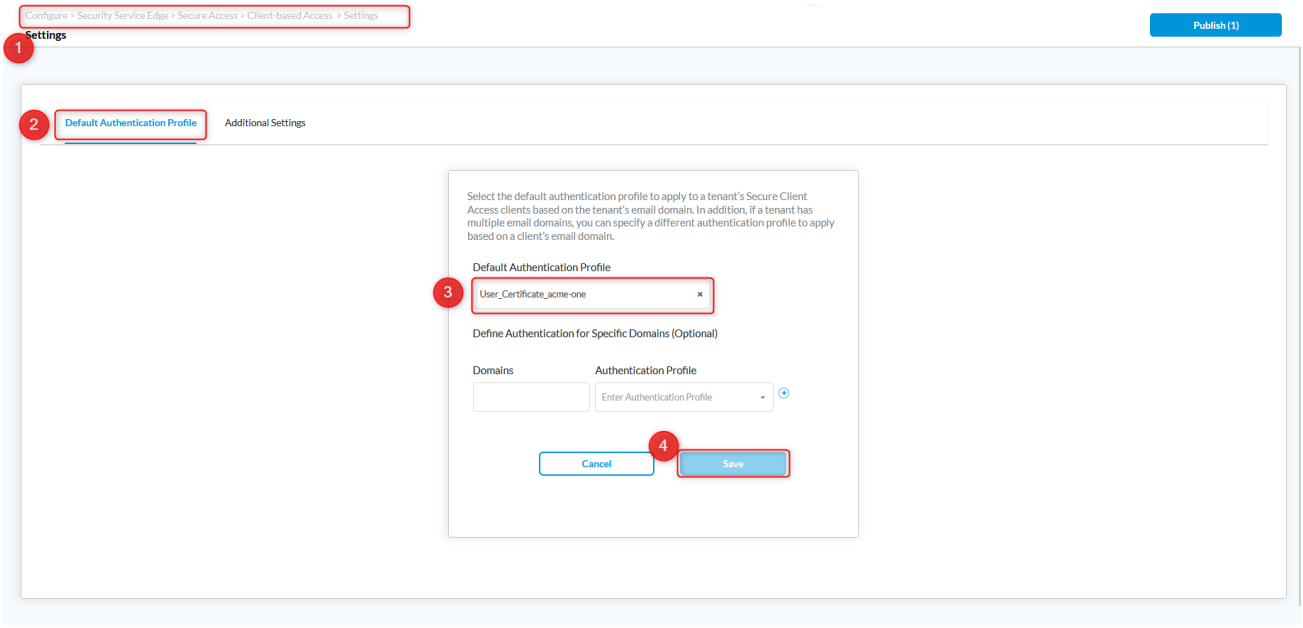
Additional Requirements for Client Certificate Authentication

- 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:

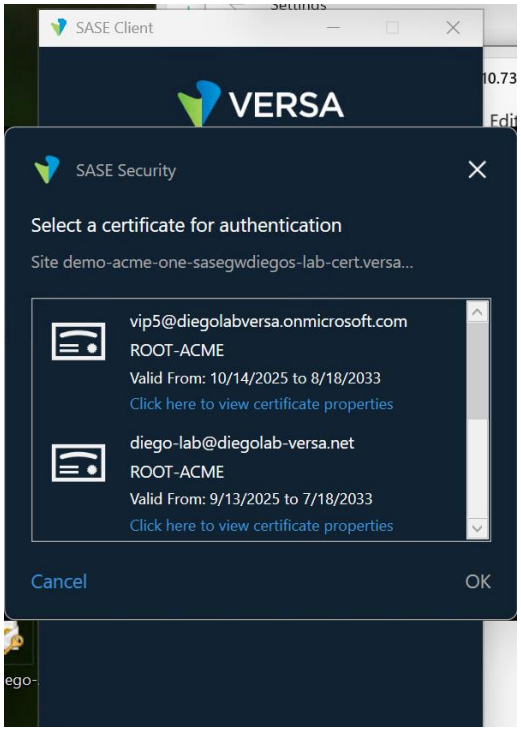
The installation process for user certificates on client devices follows the same procedure described in the **Device Certificate Authentication** section. The certificate must be imported into the appropriate certificate store on the client machine.

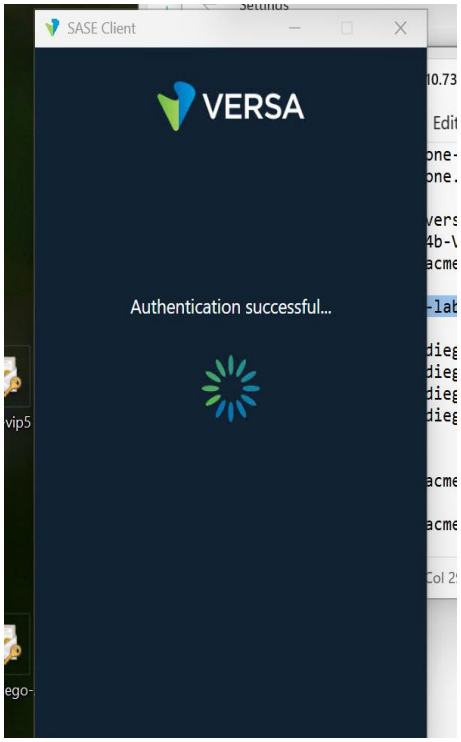
Verification

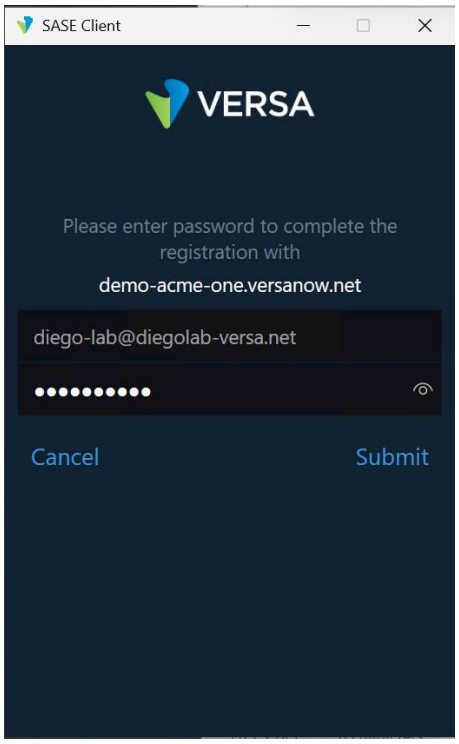
When a user connects to the Gateway and the **User Certificate Authentication** profile is enabled, the authentication process begins by validating the user's digital certificate before proceeding to directory-based authentication (SAML or LDAP). The client prompts the user with a certificate selection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