VERSA

IMPLEMENTATION GUIDE

Step-By-Step Configuration Guide for Versa Secure Internet Access (VSIA)

About This Document

This guide provides a comprehensive, step-by-step configuration process for setting up and preparing your organization's Versa Secure Internet Access (VSIA).

Versa Secure Internet Access (VSIA) is a software-defined solution that securely connects employees to the internet with advanced security features from anywhere. It safeguards devices, information, applications, and users using on-premises or cloud services. The VSIA consolidates security features including Secure Web Gateway (SWG), Next-Gen Firewall-as-a-Service (NGFWaaS), Cloud Access Security Broker (CASB)_, and Data Loss Prevention (DLP) on the SASE Platform to secure headquarters, branches, remote sites, home offices, travelling users, and "client-less" devices accessing distributed applications.

Document Information

Title	**Step-By-Step Configuration Guide for Versa Secure Internet Access (VSIA)**
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 get in touch with 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.

Scenario

This use case describes a Versa Secure Internet Access (VSIA)–only deployment for ACME-ONE. This global enterprise requires secure and seamless Internet access for both remote and roaming users. The objective is to deliver strong security controls without compromising user experience.

User Categories:

- Contractors distributed globally.
- IT role users located in Colombia.

Both categories demand:

- Strong authentication
- Device posture validation
- User-based access control
- Advanced security enforcement via the SSE Gateway (TLS inspection, SaaS Tenant, DNS filtering and URL Filtering).

Key Configuration Steps

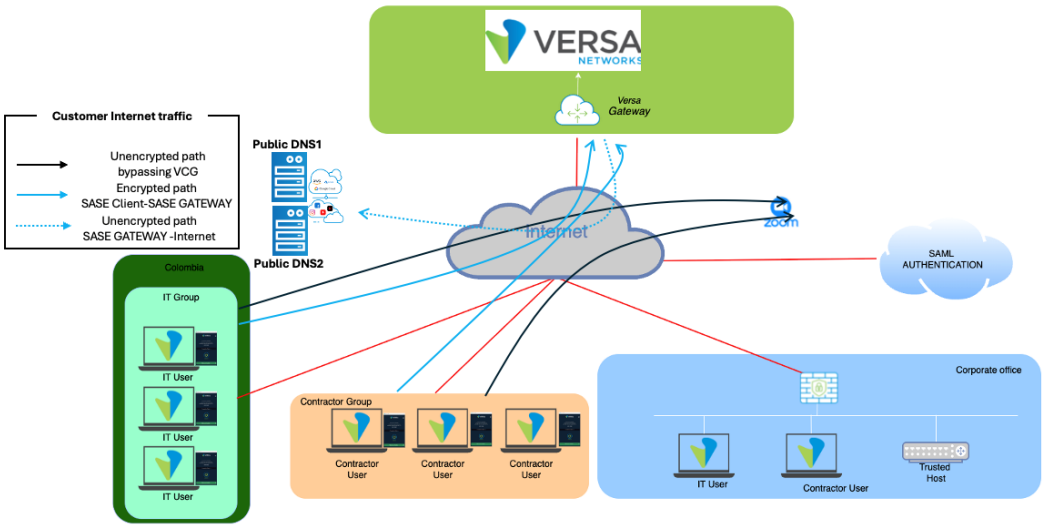
- SSE Gateway: Deploy with VSIA enabled.
- DNS & Monitoring: Configure two public DNS servers and enable Digital Experience Monitoring (DEM) for Office 365.
- SASE Client:
    - Enable Always-On with Trusted Network Detection.
    - Block all traffic if the gateway connection fails.
    - In corporate offices, Trusted Network Detection ensures traffic is handled by local security instead of tunnel redirection.
    - Enable tamper protection for all users.
- Geo-Location Controls:
    - IT users: restricted to connections originating in Colombia.
    - Contractors: allowed to connect from anywhere.
- Authentication:
    - SAML integration with two groups (IT and Contractors).
    - Example accounts:
        - ituser1@acme-one.com
        - contractor1@acme-one.com
- Device Posture Validation: Allow access only from devices running an approved endpoint security application.
- Local Breakout: Exclude Zoom traffic from secure tunnels; all other traffic is sent to the SSE gateways.
- Internet Protection Policies:

  - IT users: apply the Versa recommended URL filtering profile.
  - Contractors: restrict access to categories including Adult, Sports, Gambling, Firearms, and Violence.
  - Block AAAA DNS queries.
- SaaS Tenant Control: Restrict Office 365 access to corporate accounts only.
- Data Protection: Block sharing of compressed (.zip/.rar) and .exe files through personal email or file-sharing apps.

Topology

The deployment implements a secure remote Internet access architecture, where users connect over encrypted tunnels to the Versa SASE gateways.

- IT Group
  - Access restricted to connections originating from **Colombia**.
  - Any attempt from other geographies is blocked.
- Contractors Group
  - Global access permitted with no geolocation restrictions.
- Okta SAML
  - Authentication for both groups handled through Okta SAML identity provider over the Internet.
- Corporate Office
  - On-prem security stack protects Internet access locally.
  - Trusted Network Detection ensures no tunnels are established when users are inside corporate facilities.
- Trusted Host
  - A specific corporate-reachable host validates **Trusted Network Detection**.
  - When detected, tunnels to the gateway are bypassed.
- Zoom
  - Zoom traffic is explicitly excluded from gateway inspection.
  - It breaks out locally to preserve quality and reduce latency.



Configuration steps

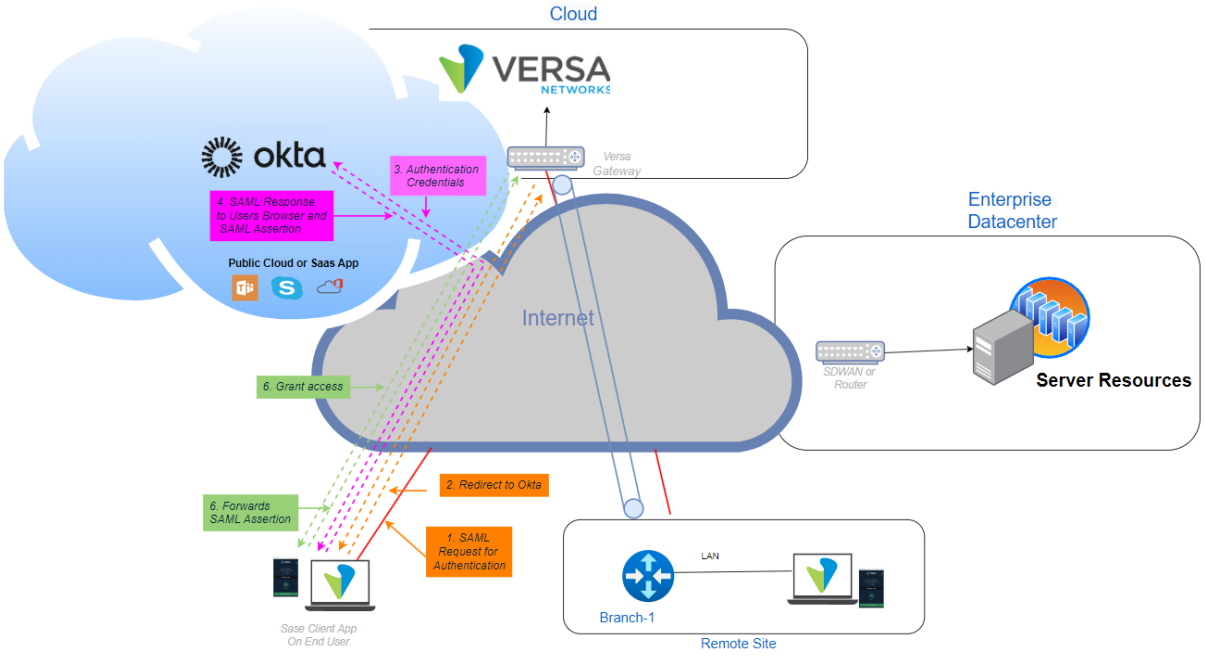
The VSIA configuration consists of the following steps:

- Step 1: Configure SAML Authentication method. Two groups (IT and Contractors) will be active.
- Step 2: Configure DNS under secure Access Profile.
- Step 3: Configure Secure Access client rules with geo-Location, always On, tamper protection Trusted Network Hostname, tunnel monitoring and Customer Logo.
- Step 4: Configure DNS Filtering to Block DNS AAAA Queries.
- Step 5: Configure Profile for SaaS Tenant Control.
- Step 6: Configure TLS decryption and bypass. Health and financial sites should not be decrypted.
- Step 7: Configure File Filtering Profile Rules to deny .exe files and compressed files.
- Step 8: Configure URL Filtering Profile.
- Step 9: Configure Internet Protection Policy Rules

Step 1. Configure Authentication method - SAML (Okta)

Overview

Within the enterprise context, Okta functions as the centralised 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 using the SAML protocol, which performs identity validation and returns a SAML assertion. This process grants access based on the user or group.



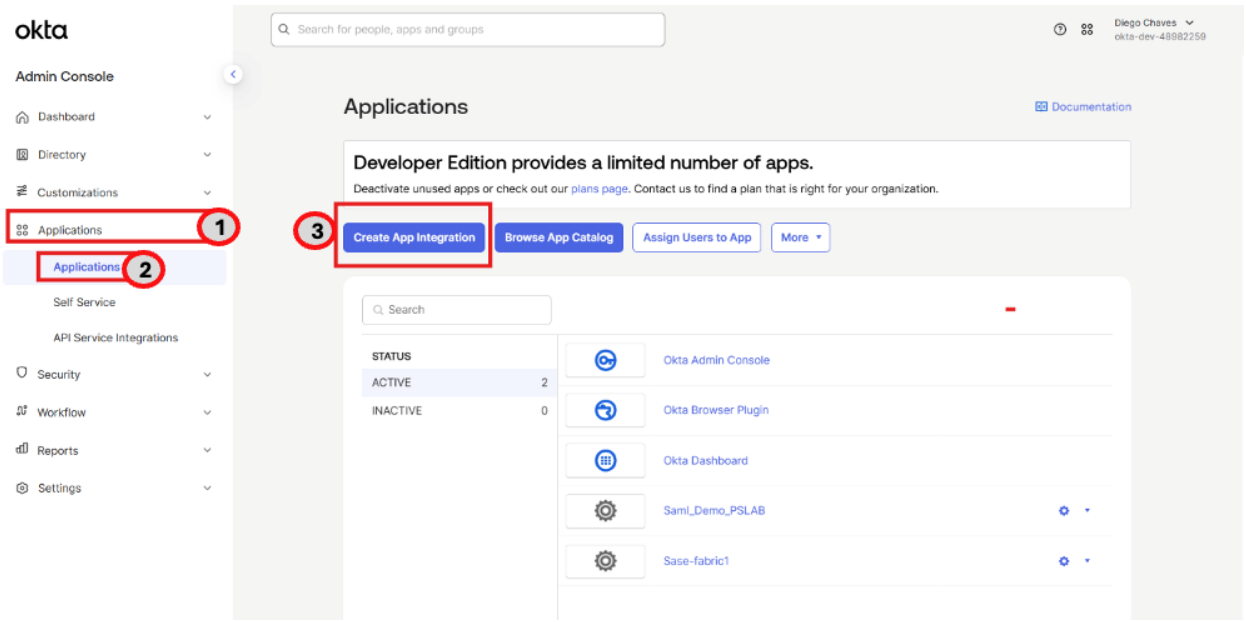
Okta SAML Configuration

In the Okta Portal, create an Application and add groups/users to the it.

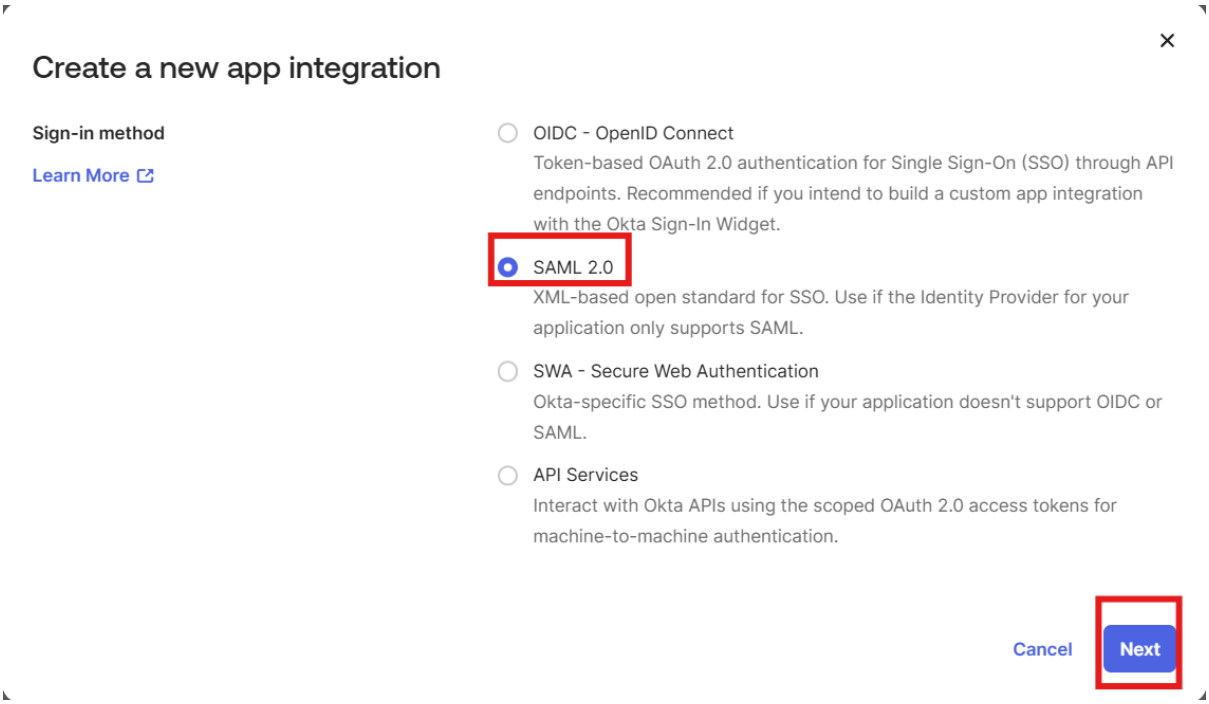
Create an application on Okta

1. Log in to your Okta admin console.

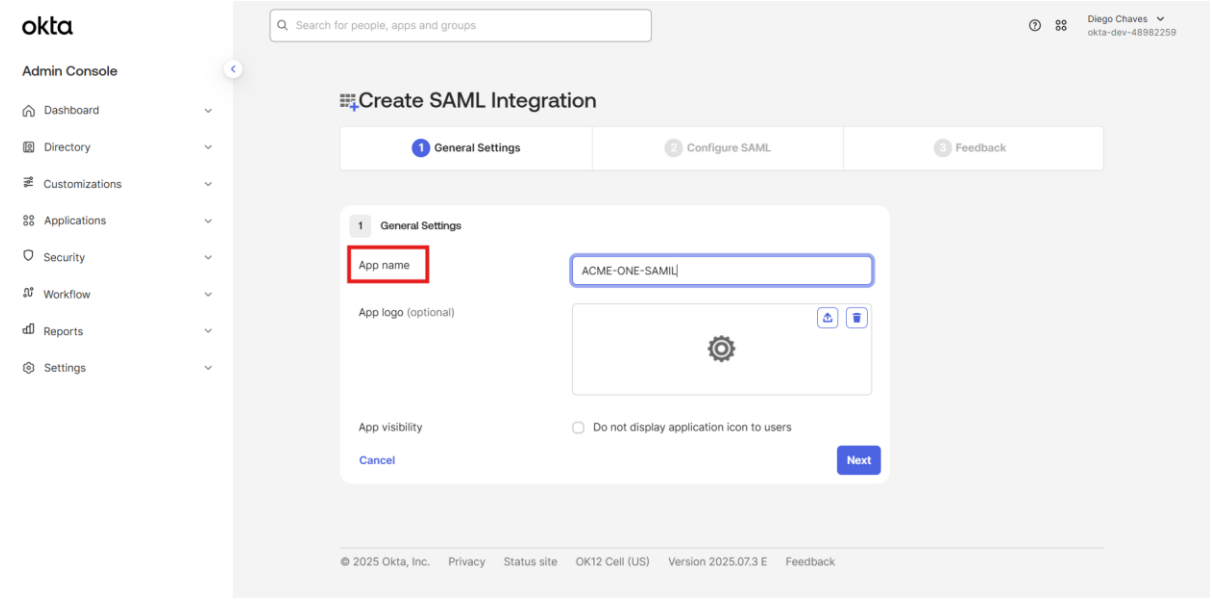
Navigate to: Application (1), then click on Applications (2) >> Create App Integration (3).



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**.



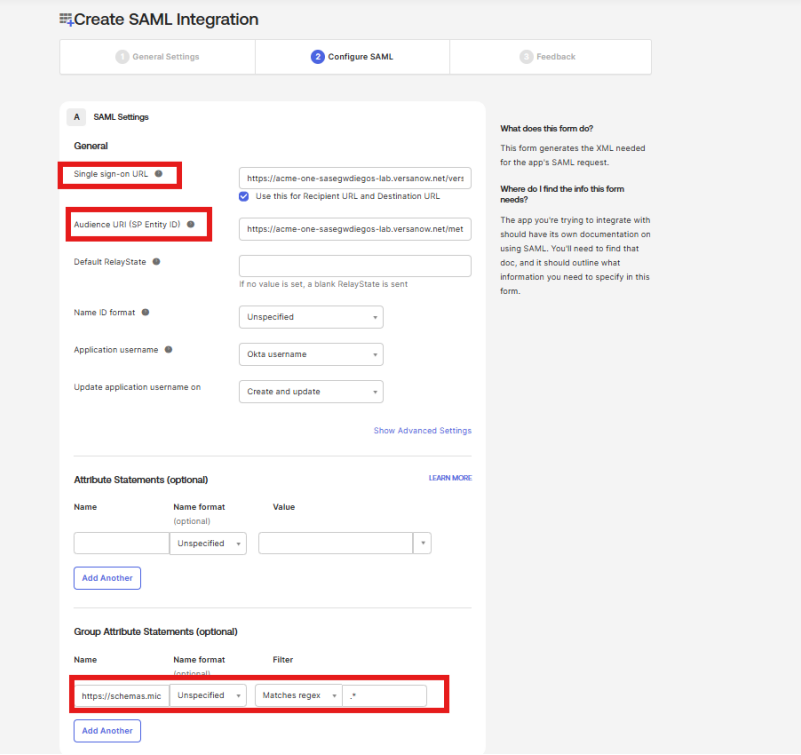
4. Define custom attributes.

In **Configure SAML > SAML settings**, enter information for the indicated fields as shown in the table below, then click **Next**.

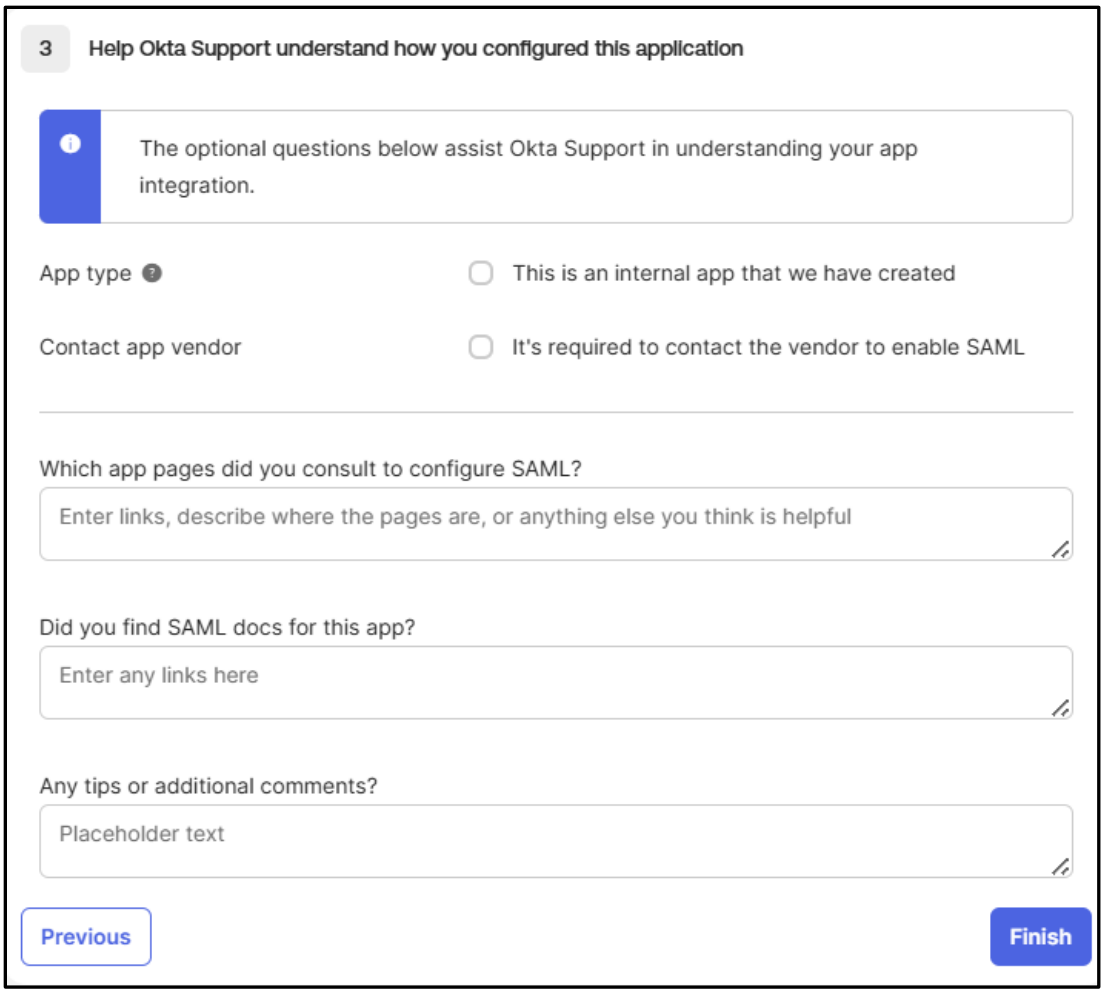
Field	Description
Single Sign-On URL	URL where Okta sends SAML responses. Format: https://<SASE-GW-FQDN>/versa-flexvnf/saml/login-consumer. Example: https://acme-one-sasegwdiegos-lab.versanow.net/versa-flexvnf/saml/login-consumer
Audience URI (SP Entity ID)	Service Provider (SP) entity ID: Format: https://<SASE-GW-FQDN>/metadata. Example: https://acme-one-sasegwdiegos-lab.versanow.net/metadata
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 output from the SAML Assertion preview:

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion ID="id-577374555241106028824600913 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>
```

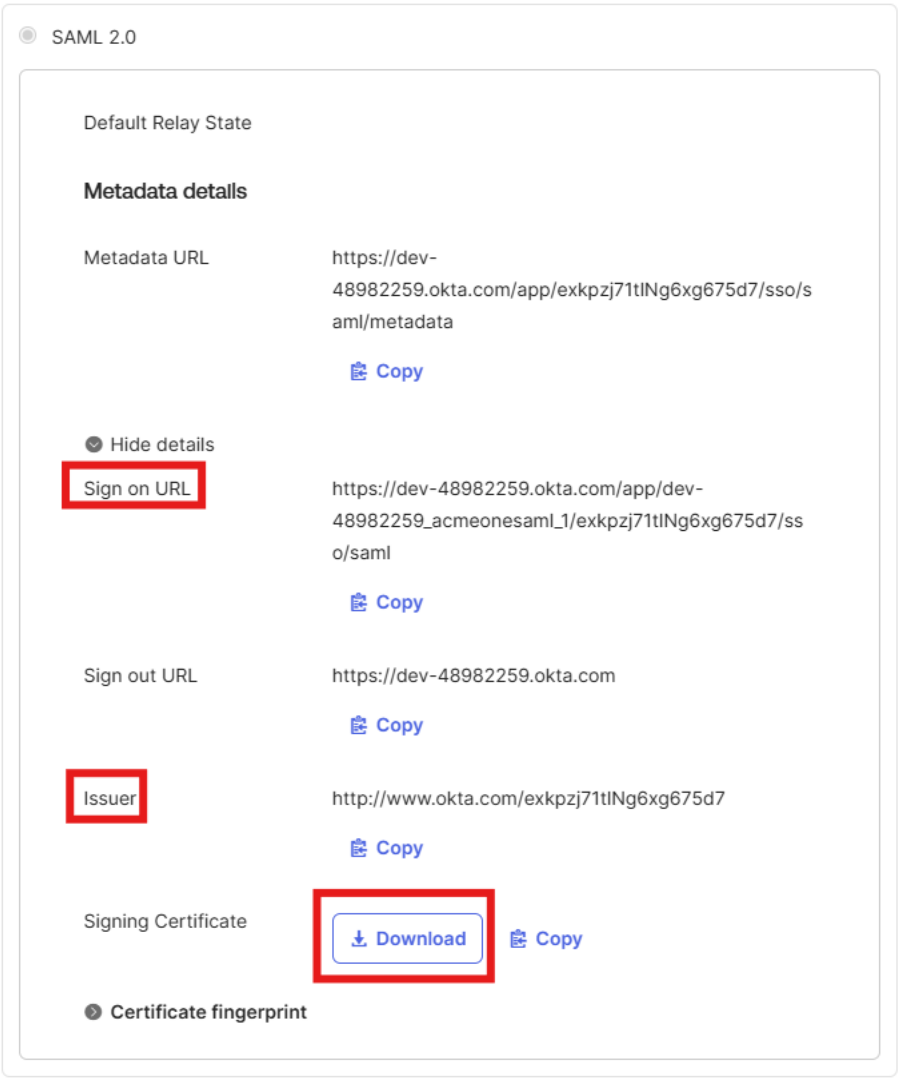


5. Click Next
6. In the **Help Okta Support understand how you configured this application section**, you can provide optional information for Okta Support.
    - Under **App type**, check **This is an internal app** that we have created (recommended for internal SSO integrations like Versa).
    - Click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



7. Retrieve SAML Integration Details

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



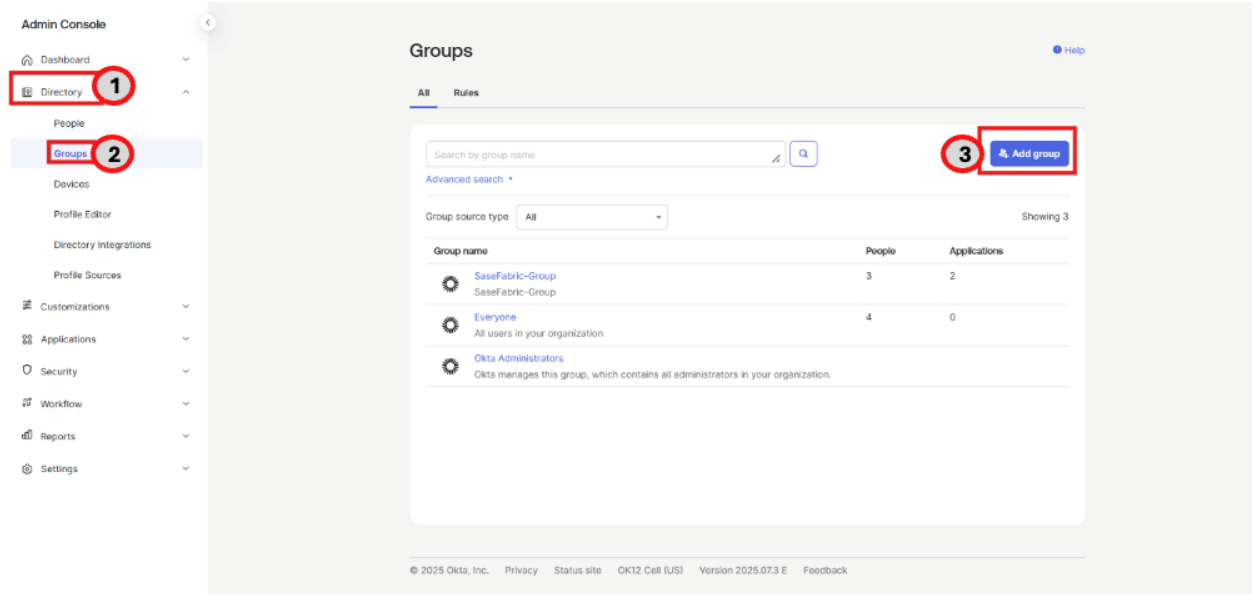
Note: Rename the file extension of the downloaded certificate file from. cert to .crt before use.

Add Groups and Users to the application

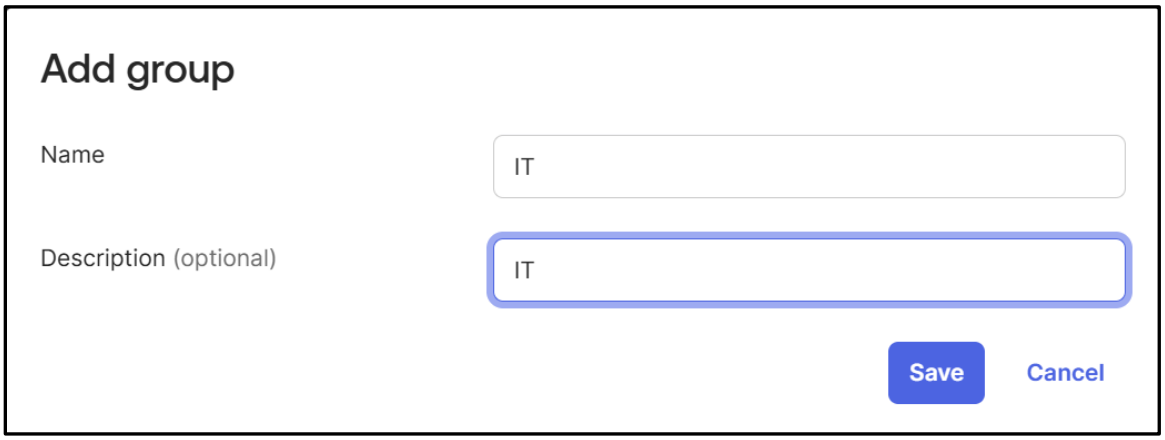
In this step create the Users and Groups as per the Scenario which will be used for authentication and identity-based access control.

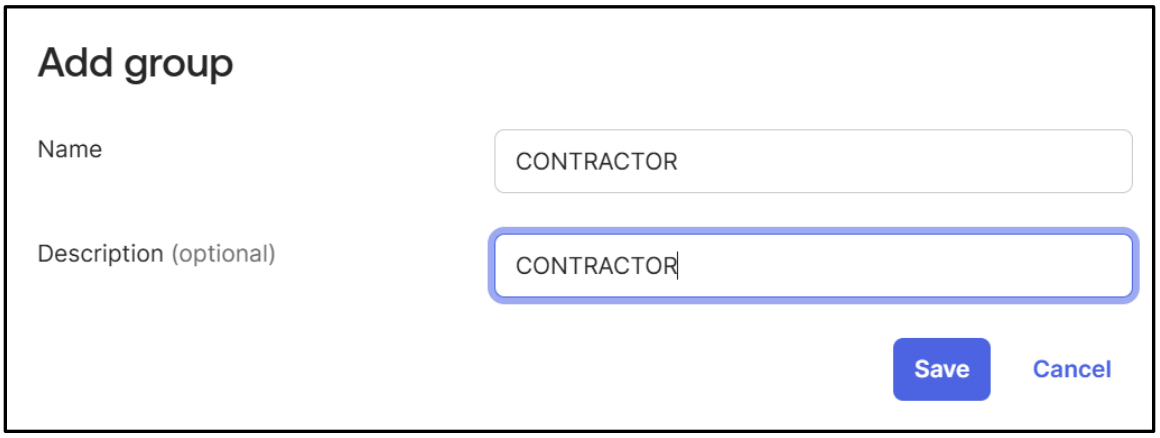
User	Group
ituser1@acme-one.com	IT
contractor1@acme-one.com	CONTRACTOR

In the Okta portal, navigate to **Directory (1) > Groups (2),** then click on **Add group (3).**

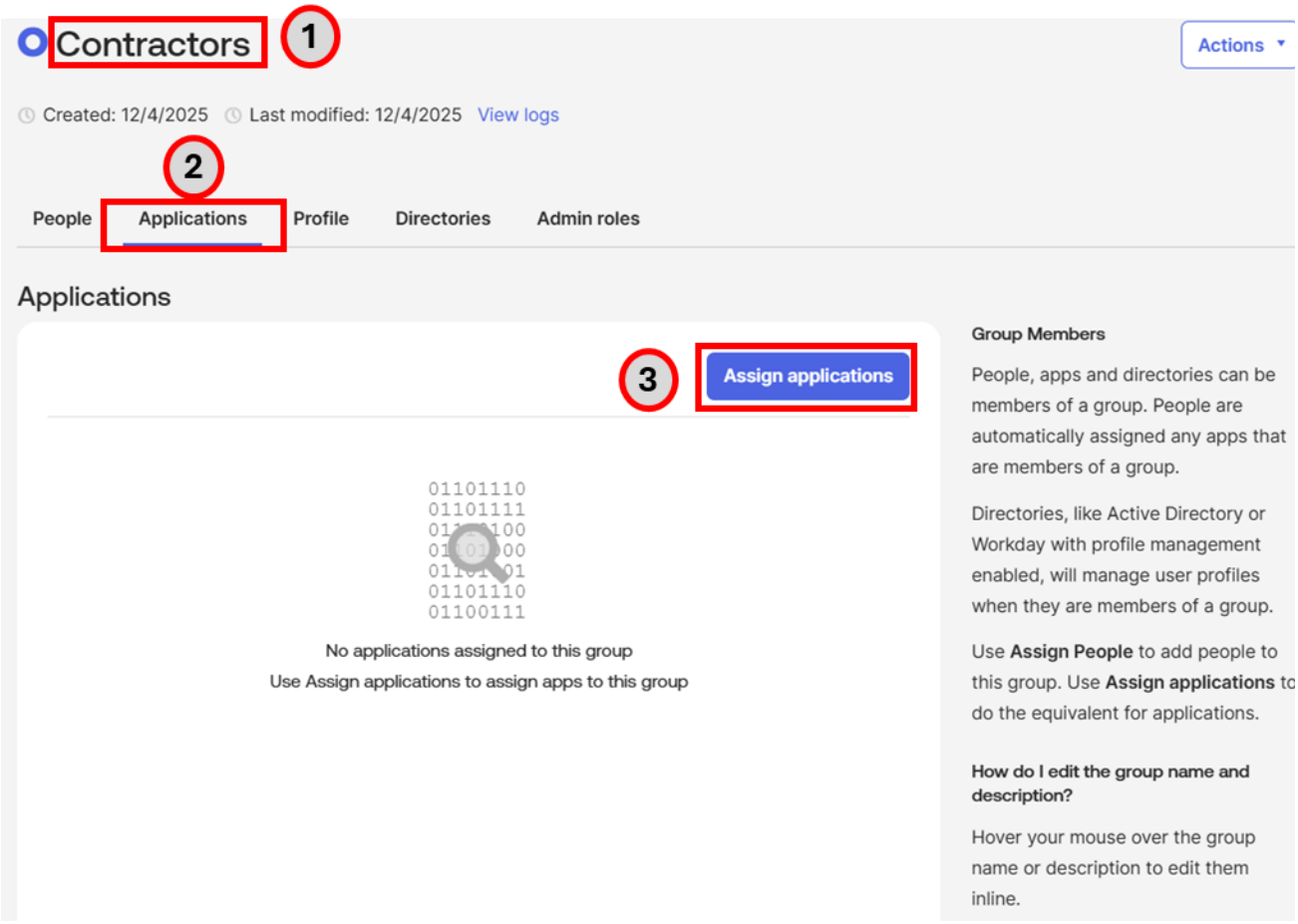


In the name field, enter a group name and click **Save**.

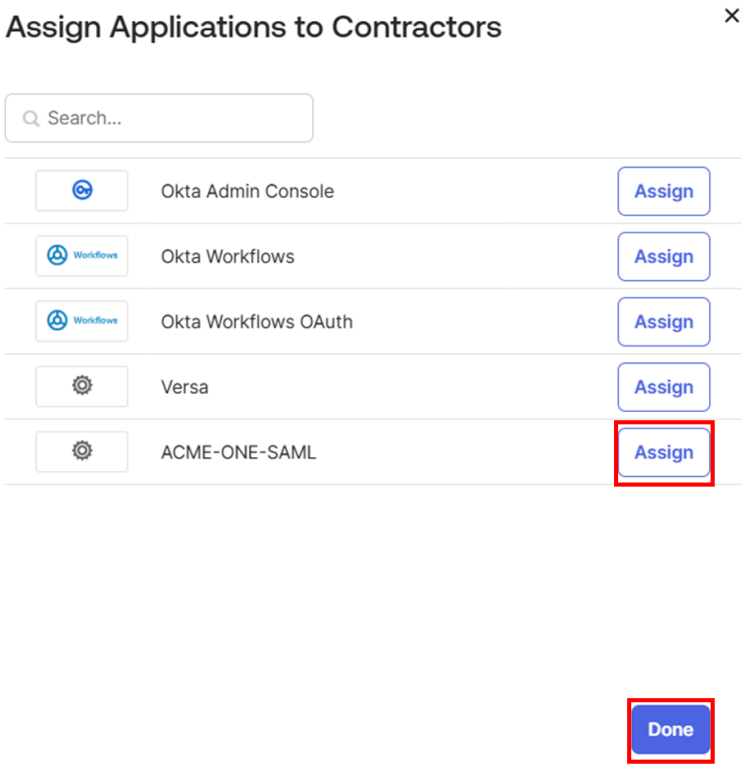




Refresh the page and click to the newly created group **Contractors group (1).** After opening the group, go to the **Applications (2)** tab and click **Assign Applications (3)** to assign the newly created SAML application to the group.

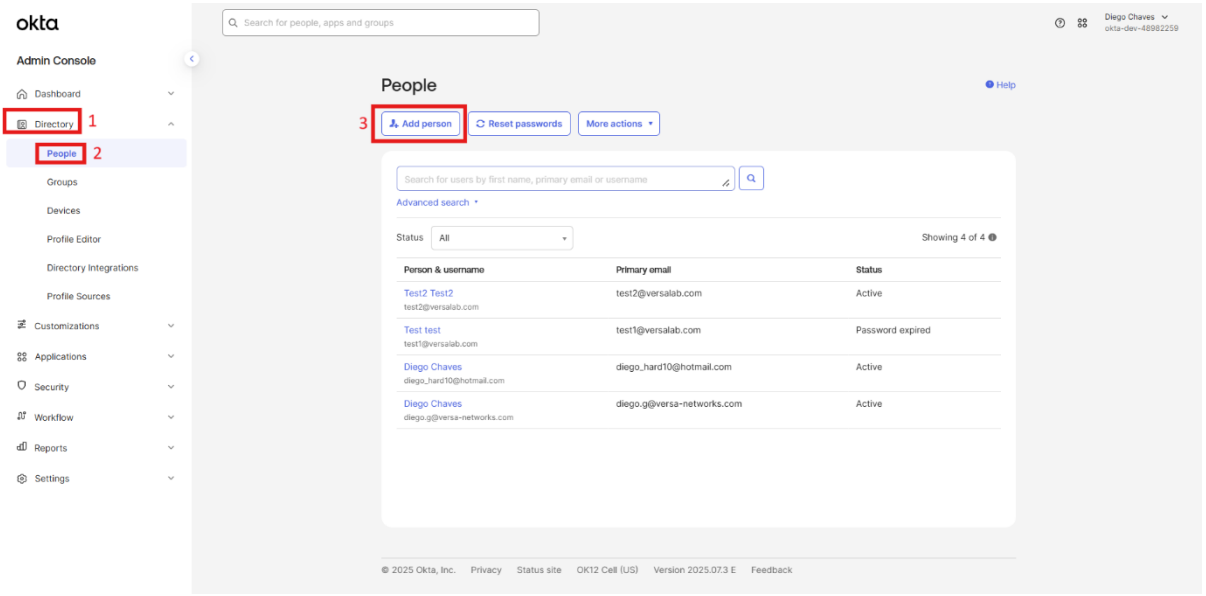


Select newly created SAML application and click **Done**.

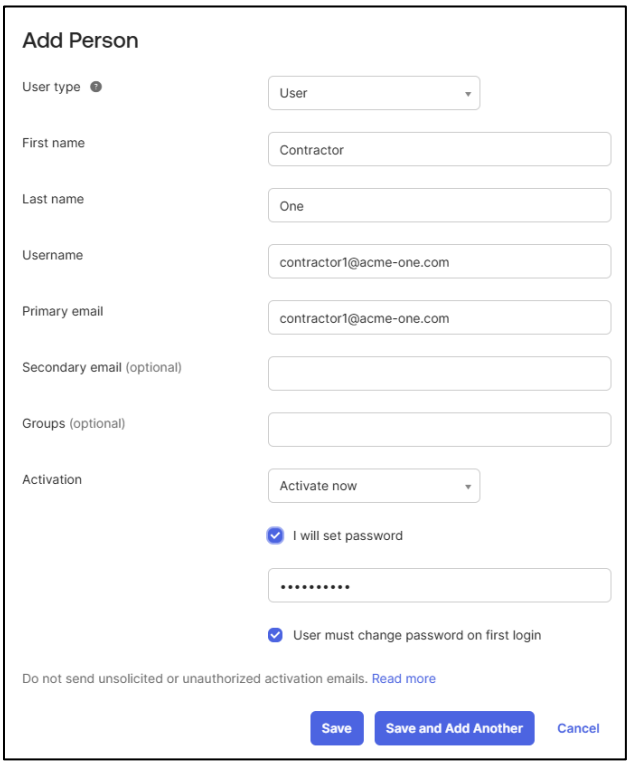


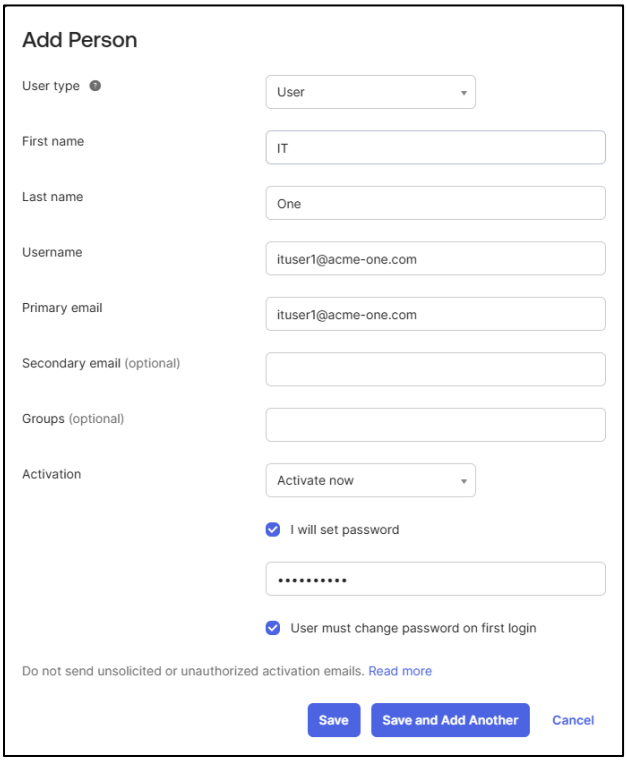
Repeat the same steps for the IT group.

Next to create users navigate to **Directory > People**, click **Add Person** for ituser1@acme-one.com and contractor1@acme-one.com

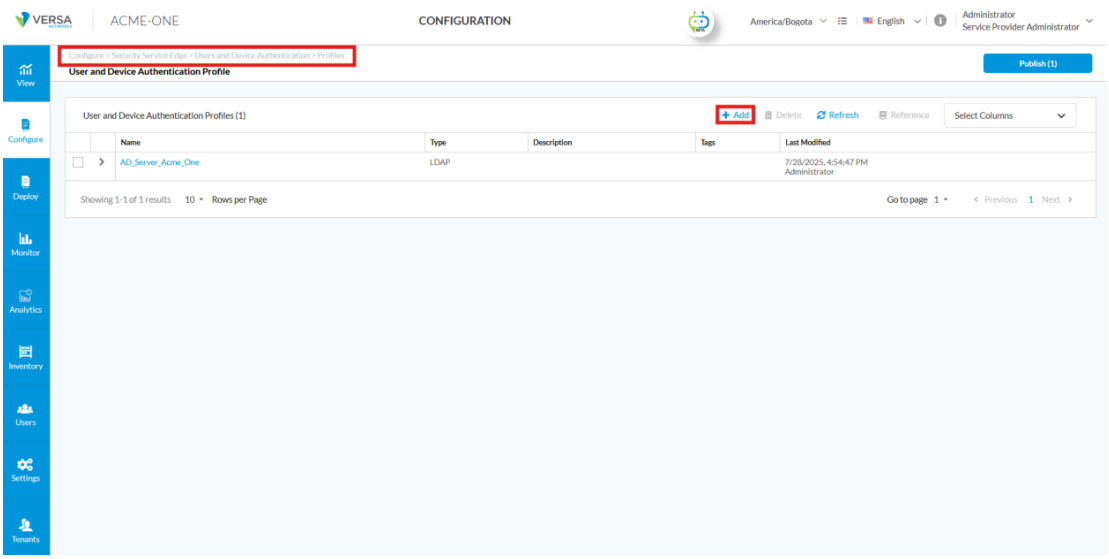


In the **Add Person** window, set **User** type to User, enter the **first name**, **last name**, **username**, and **primary email**, select the required group (Example Engineering-Group), choose **Activate now**, set a **password**, and select the check-box **User must change password on first login.**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

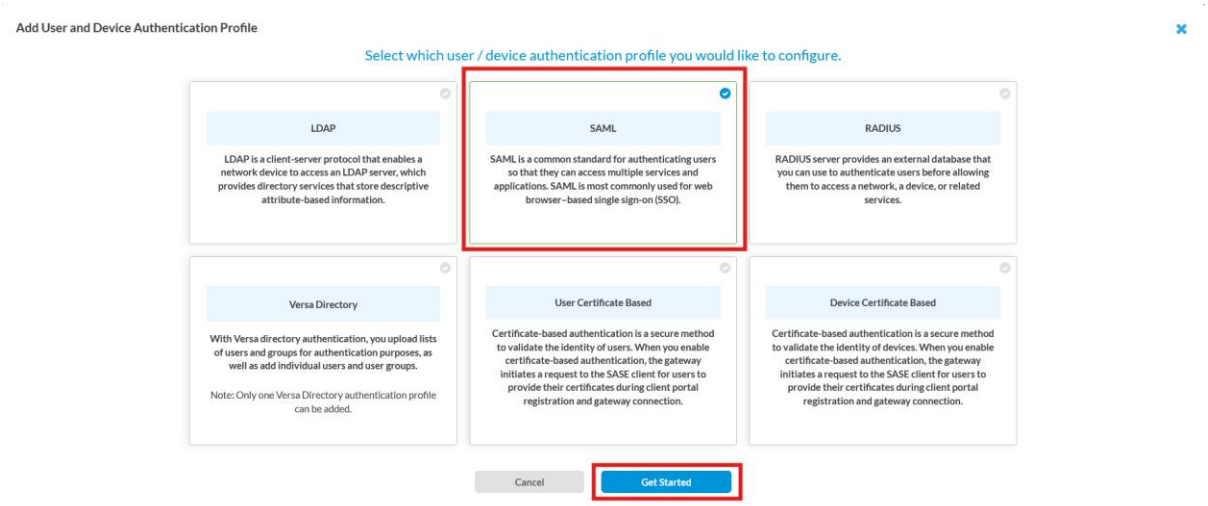

Add Person
User type
User
First name
Contractor
Last name
One
Username
contractor1@acme-one.com
Primary email
contractor1@acme-one.com
Secondary email (optional)
Groups (optional)
Activation
Activate now
I will set password
User must change password on first login
Do not send unsolicited or unauthorized activation emails. Read more
Save
Save and Add Another
Cancel


Add Person
User type
User
First name
IT
Last name
One
Username
ituser1@acme-one.com
Primary email
ituser1@acme-one.com
Secondary email (optional)
Groups (optional)
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

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



Select **SAML,** then click **Get Started**



Select **Okta**. To configure the authentication settings, use the information collected in **Step 6** from the Okta SAML application.

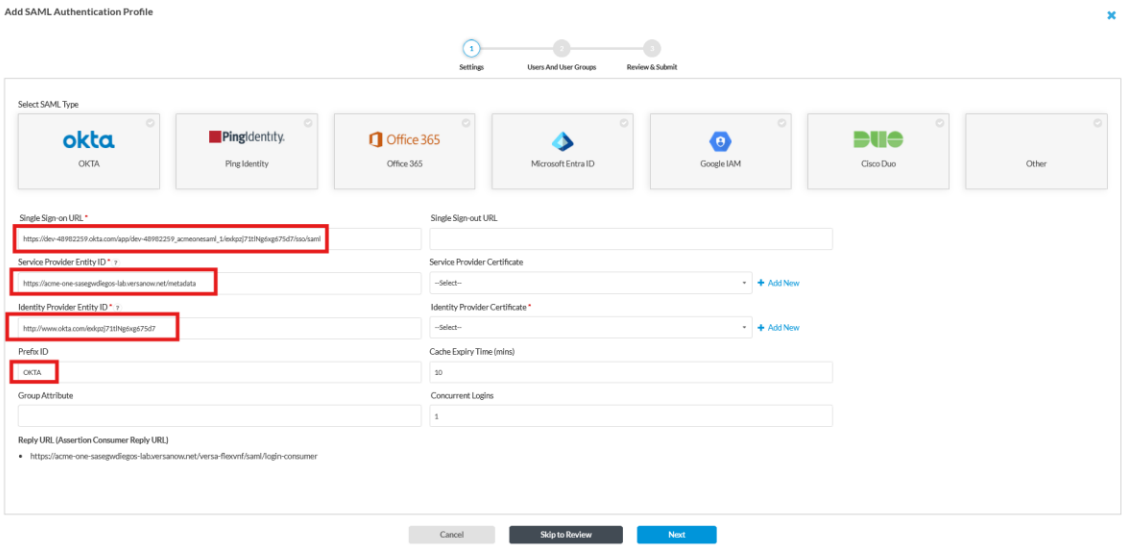
Single Sign-on URL, **Service Provider Entity ID** and **Identity Provider Entity ID** are mandatory fields to be configured, and you must upload the signing certificate file issued by Okta.

Complete the parameters using the values from the Okta app:

Example:

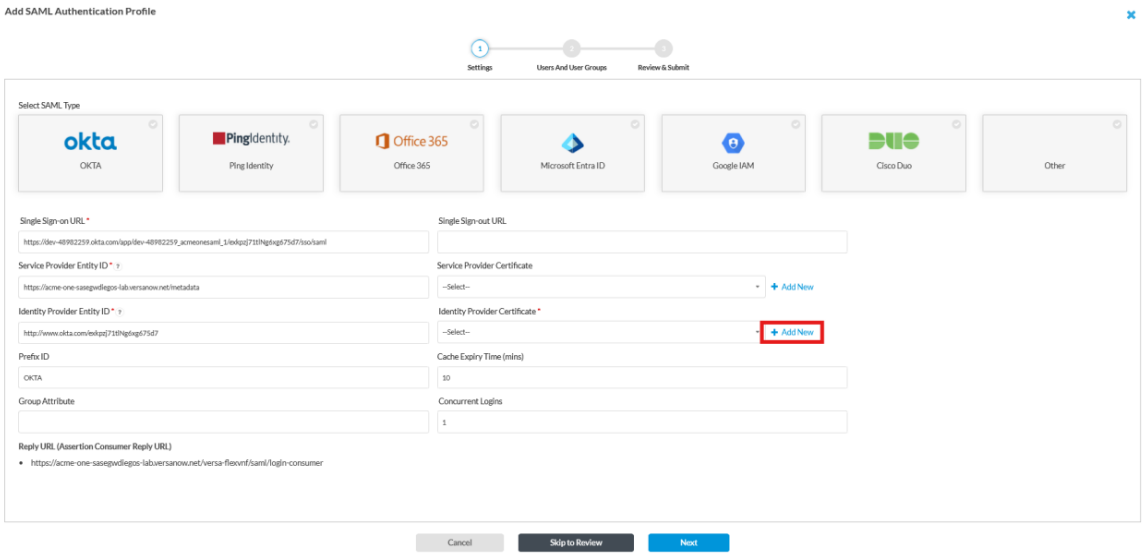
- **Single Sign-on URL:** https://dev-48982259.okta.com/app/dev-48982259_ac-meonesaml_1/exkpzj71tlNg6xg675d7/sso/saml
- **Service Provider Entity ID:** https://acme-one-sasegwdiegos-lab.versanow.net/metadata
- **Identity Provider Issuer**: http://www.okta.com/exkpzj71tlNg6xg675d7

Prefix ID: Okta

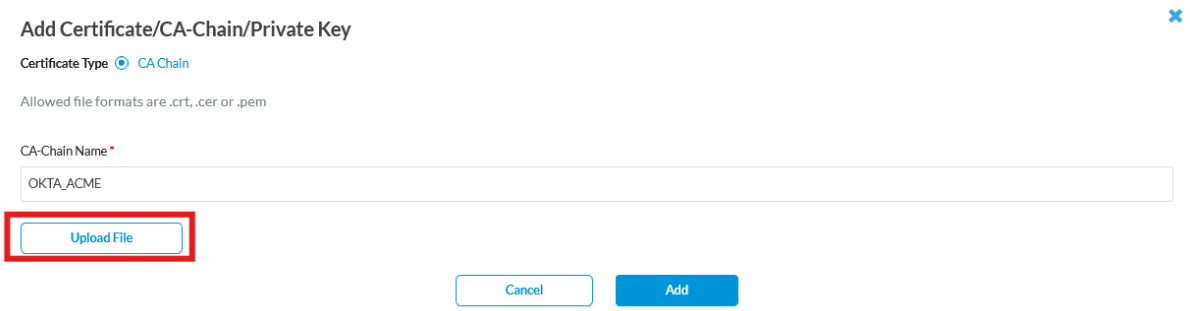


Then upload the **Identity Provider Certificate** by clicking on the **Add New** button.

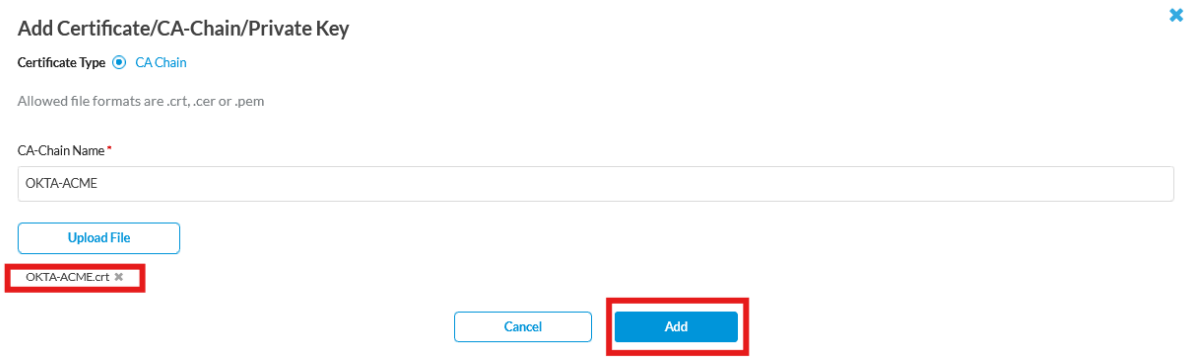
Note: Rename the downloaded certificate file from .cert to .crt before uploading.



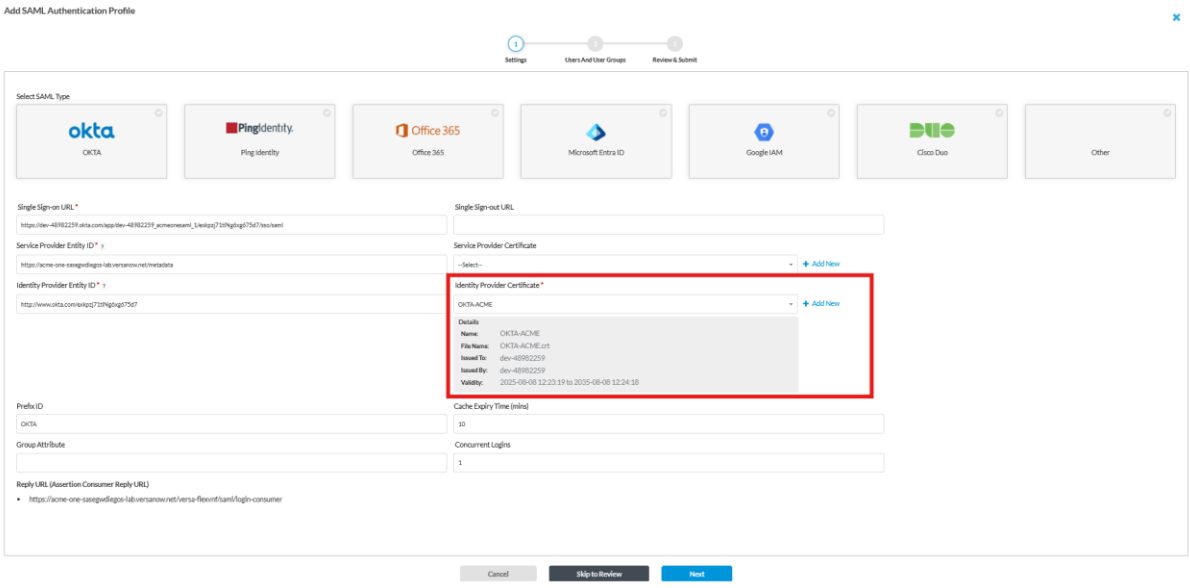
Assign a descriptive name for **CA-Chain Name**, then upload the certificate file by clicking **Upload File**.



The file uploaded will be confirmed below the Upload File button. Click **Add** to close the window.



If the certificate was uploaded successfully, the certificate details will be displayed. Click **Next.**

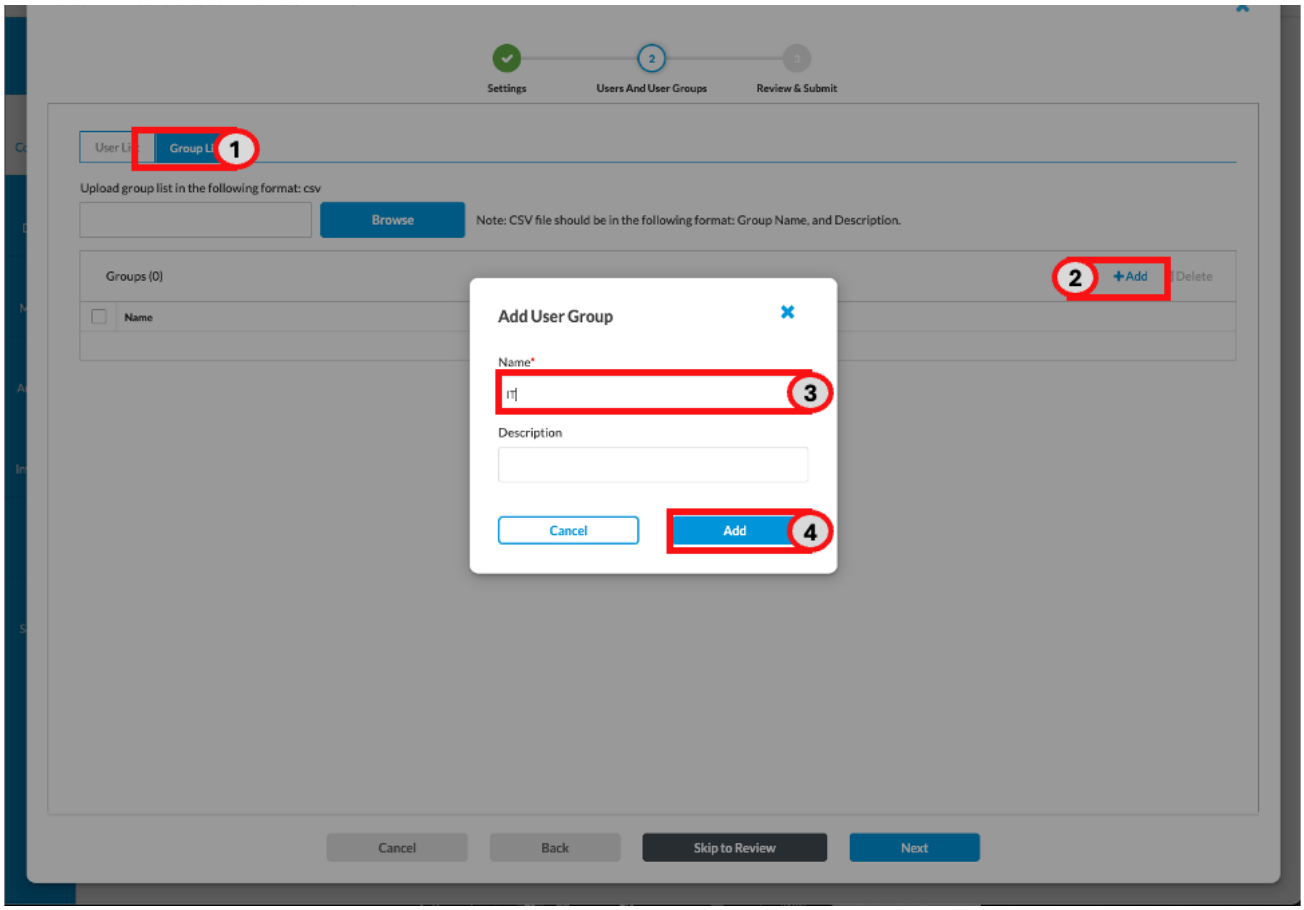


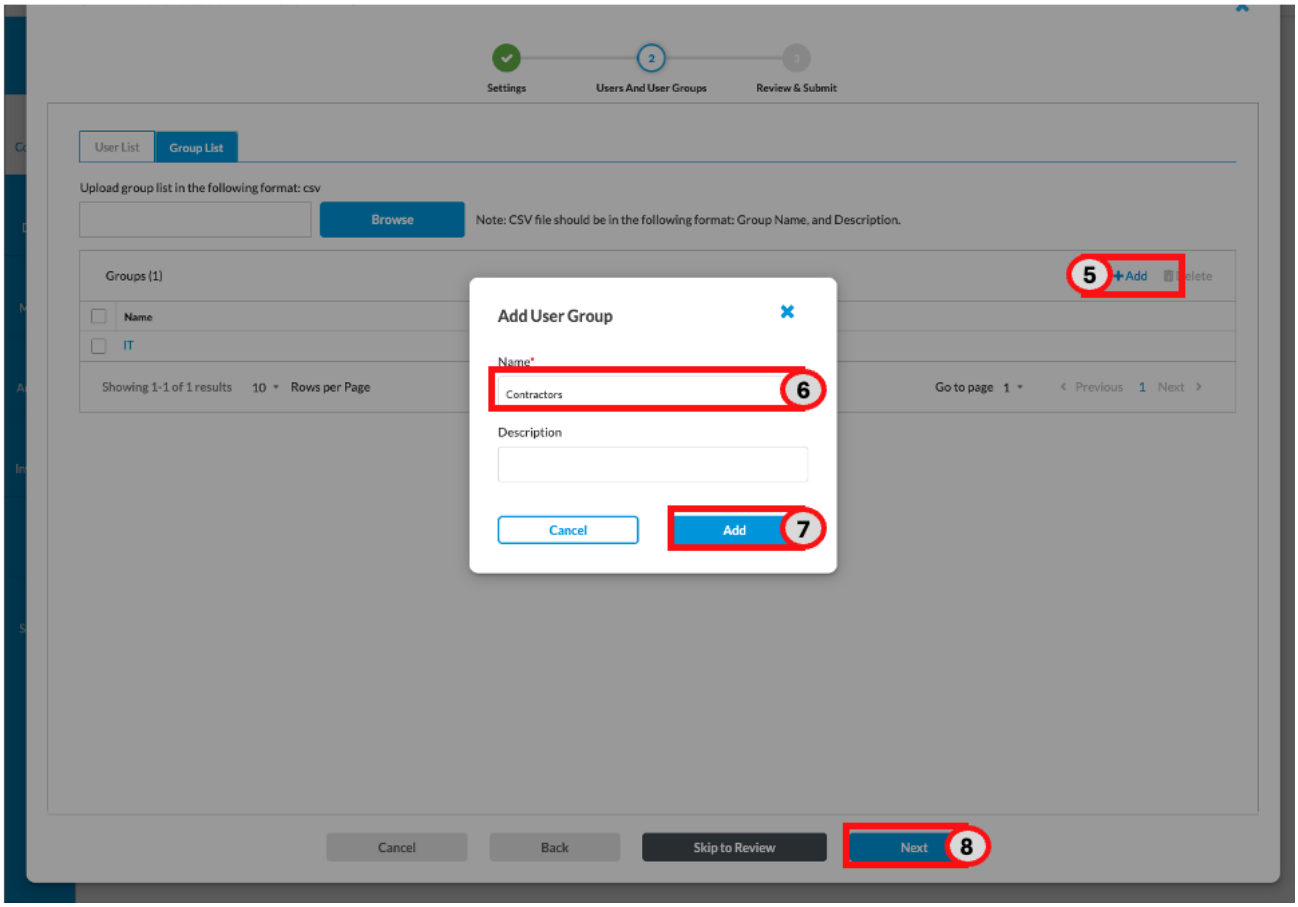
On the **Users and User Groups** page, you can add either individual users or entire groups. Unlike LDAP, SAML-based users and groups do not auto-populate; they must be created manually. These groups can then be referenced when configuring Secure Access Rules and Real-Time Protection Rules.

As an alternative, you can enable SCIM integration, which automates user and group provisioning. (Note: SCIM requires additional components. For details, see **Provision SCIM Service on Versa SASE**)

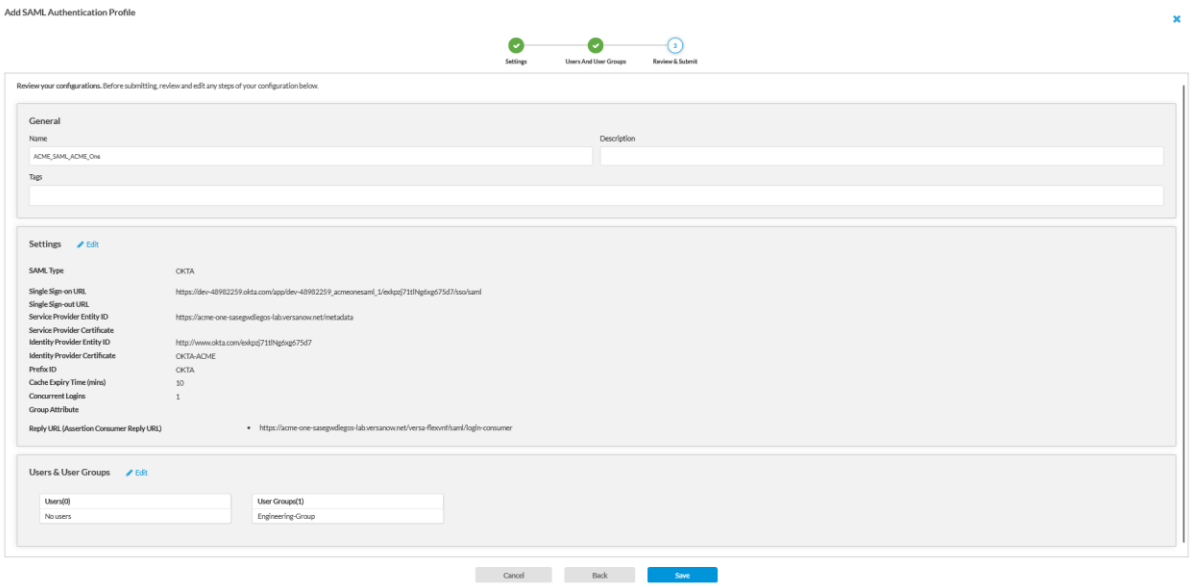
Click **User Groups** and **+ Add** to add the groups created in the Okta App. Provide the name for each group, click **Add**, then click **Next** to continue after both groups are added.

Group
IT
CONTRACTOR





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.



Step 2: Configure Secure Client Access Profile

Secure Access Profiles define the configuration applied to a user's device when the Versa SASE Client establishes a connection to the Gateway. These profiles may include Application Monitors, DNS Resolvers, and Private Routes.

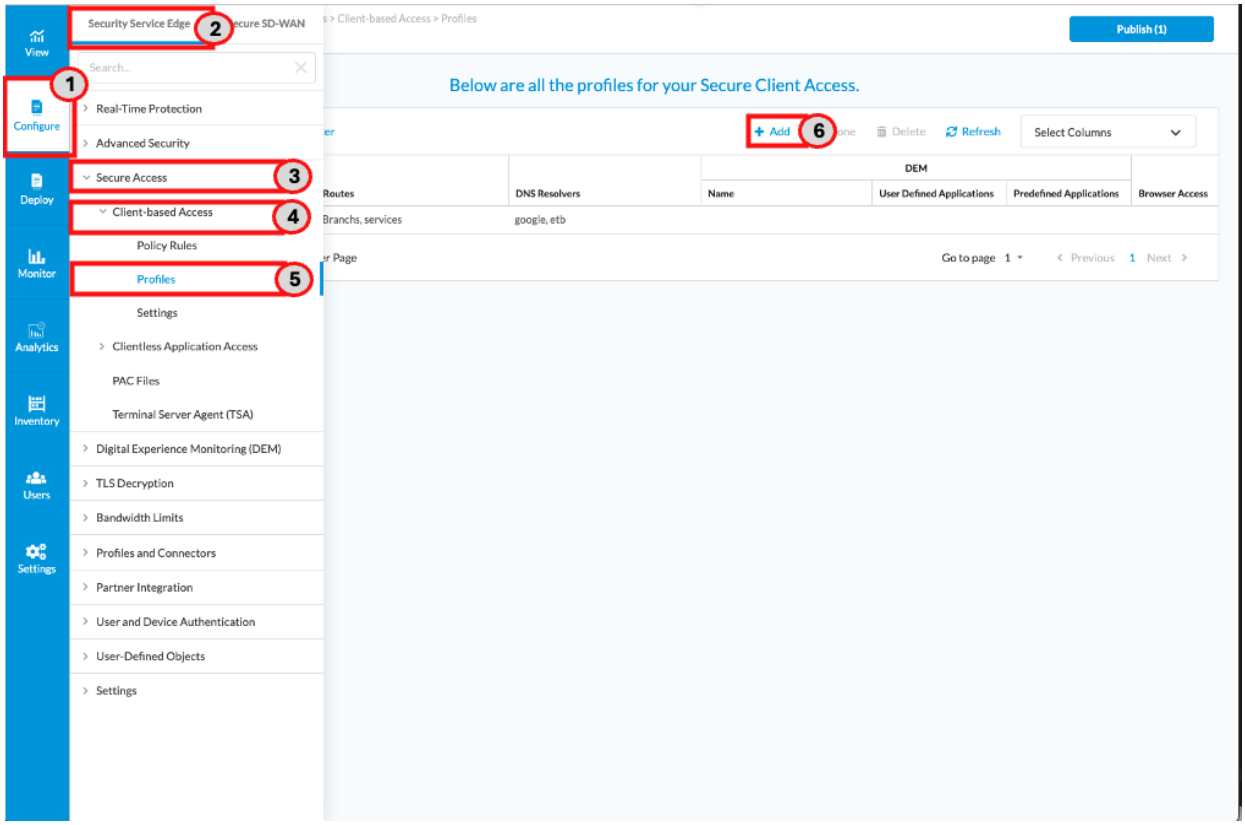
In this Use case:

- The Gateway is used only for securing Internet traffic.
- Two public DNS resolvers will be configured as only Internet Traffic will be serviced
- Since no private resources are accessed through the Gateway, no private DNS resolvers are required.
- Office 365 will be monitored with Digital Experience Monitoring (DEM) to capture performance metrics and ensure better user experience.

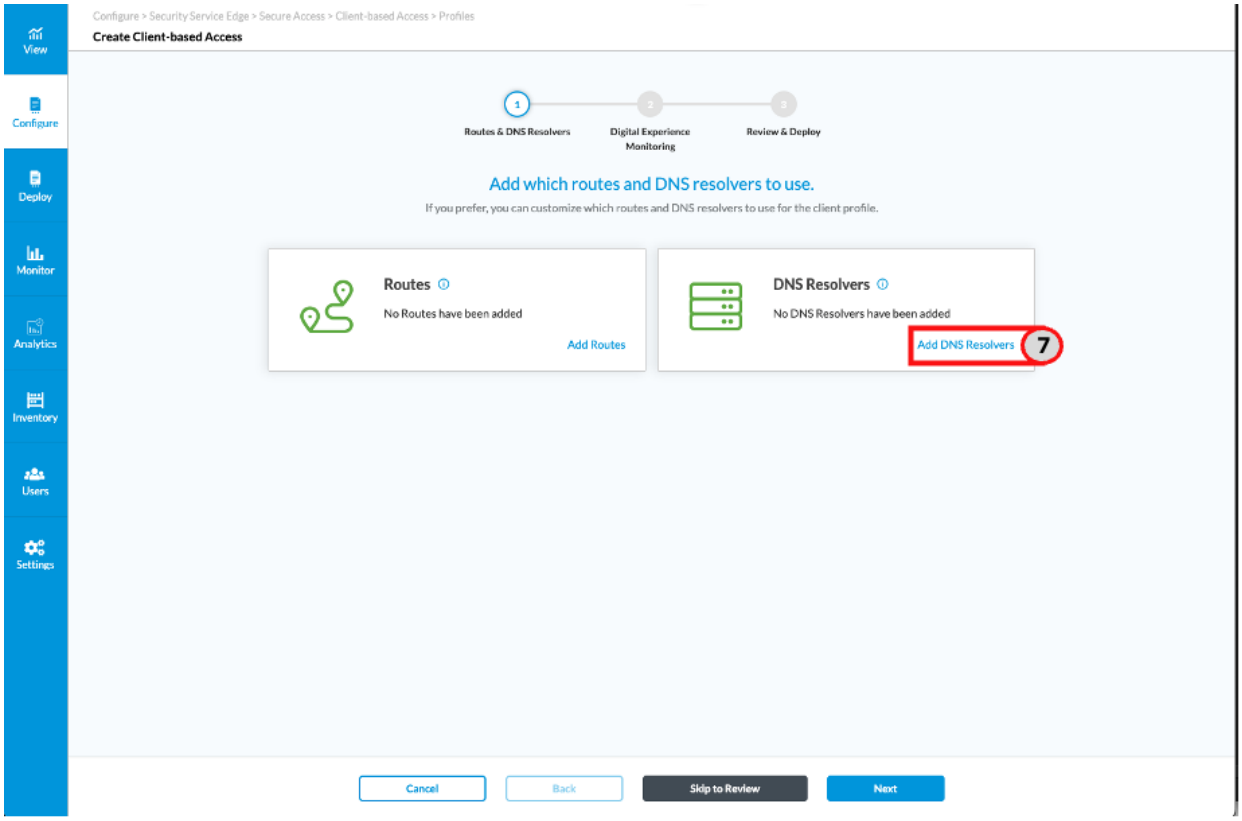
The following Information is required to complete the configuration.

Parameter	Description
DNS Record Name	Reference name for the Primary DNS in Concerto
Primary DNS IP	IP address of the primary public DNS server
Secondary DNS IP	IP address of the secondary public DNS server (for redundancy)
DEM Application	Application to be monitored (e.g., Office 365)
DEM Profile Name	Friendly name for the DEM profile
Secure Access Profile Name	Friendly name for the Secure Access Profile

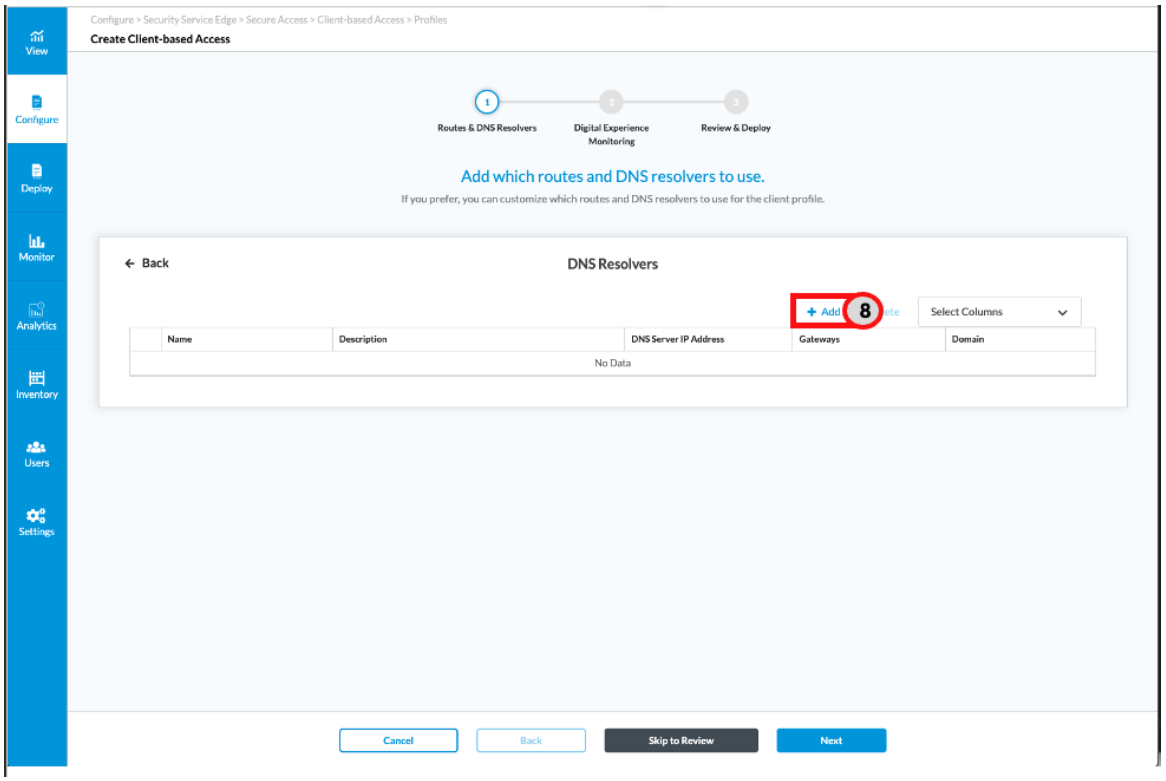
Navigate to **Configure > Security Service Edge > Secure Access > Client-based Access > Profiles and click on +Add** as shown in the figure below.



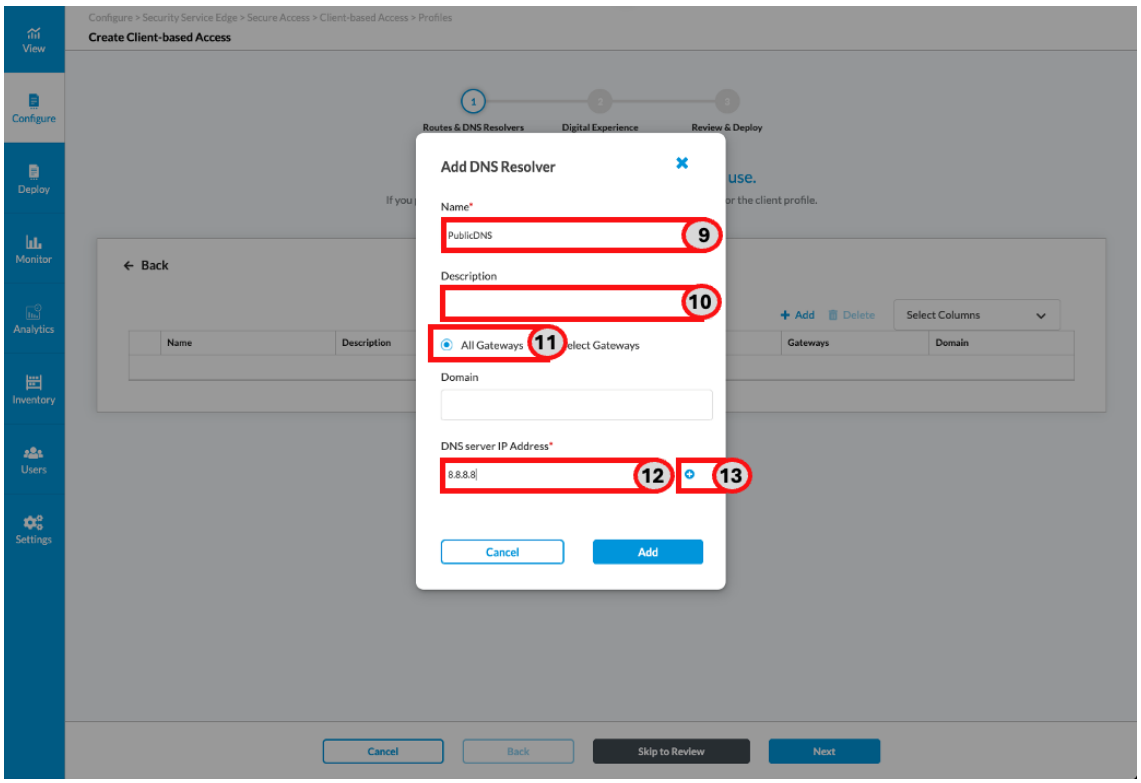
In the DNS resolvers section click **Add DNS Resolvers**.



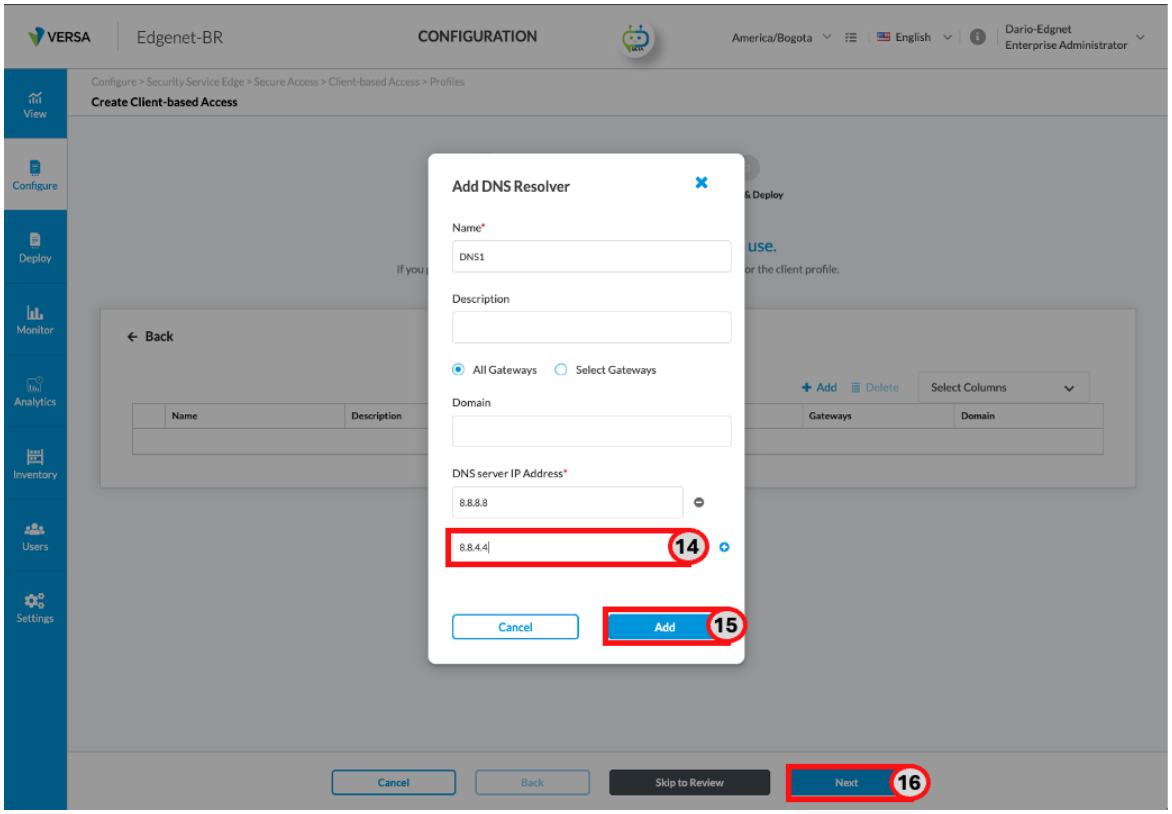
Click **+ *Add*** (8) to include a new DNS entry.



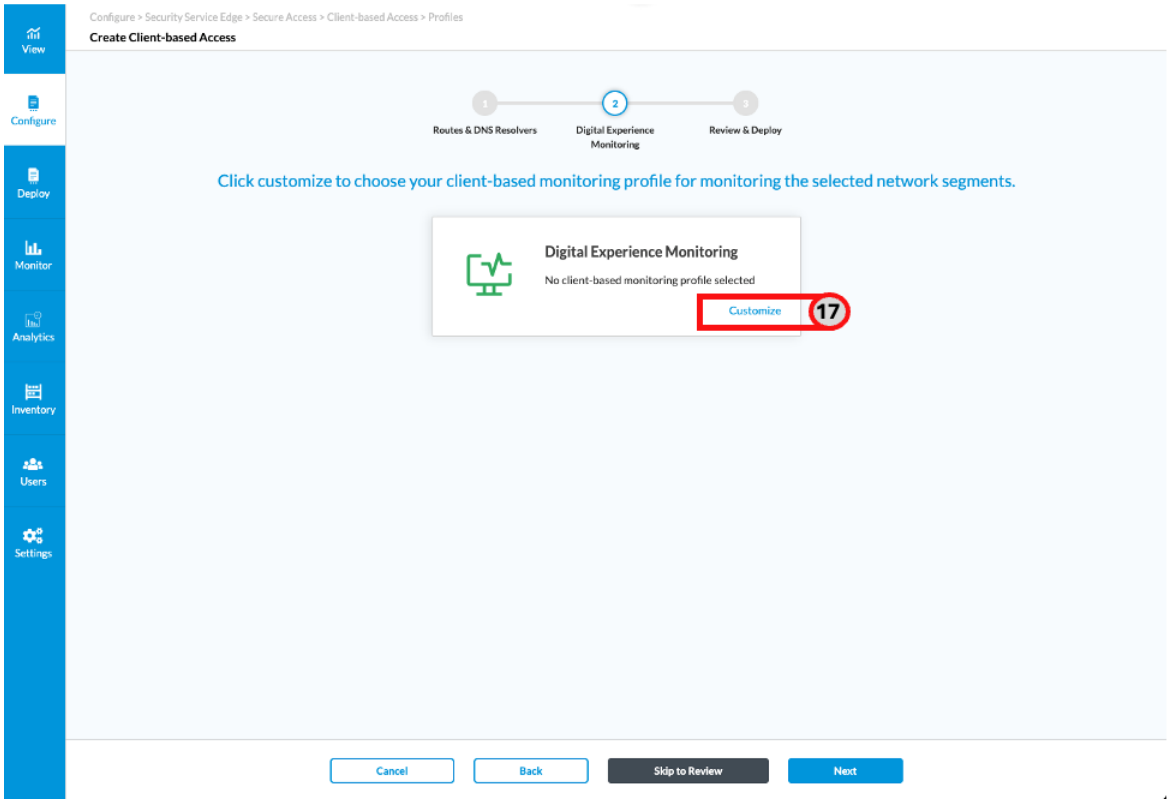
Configure the **Name** for the DNS Record entry, a **Description** can be included (optional), select the **All Gateways** option and define the **IP address** for the DNS. Click **+** to include the DNS resolver entry.



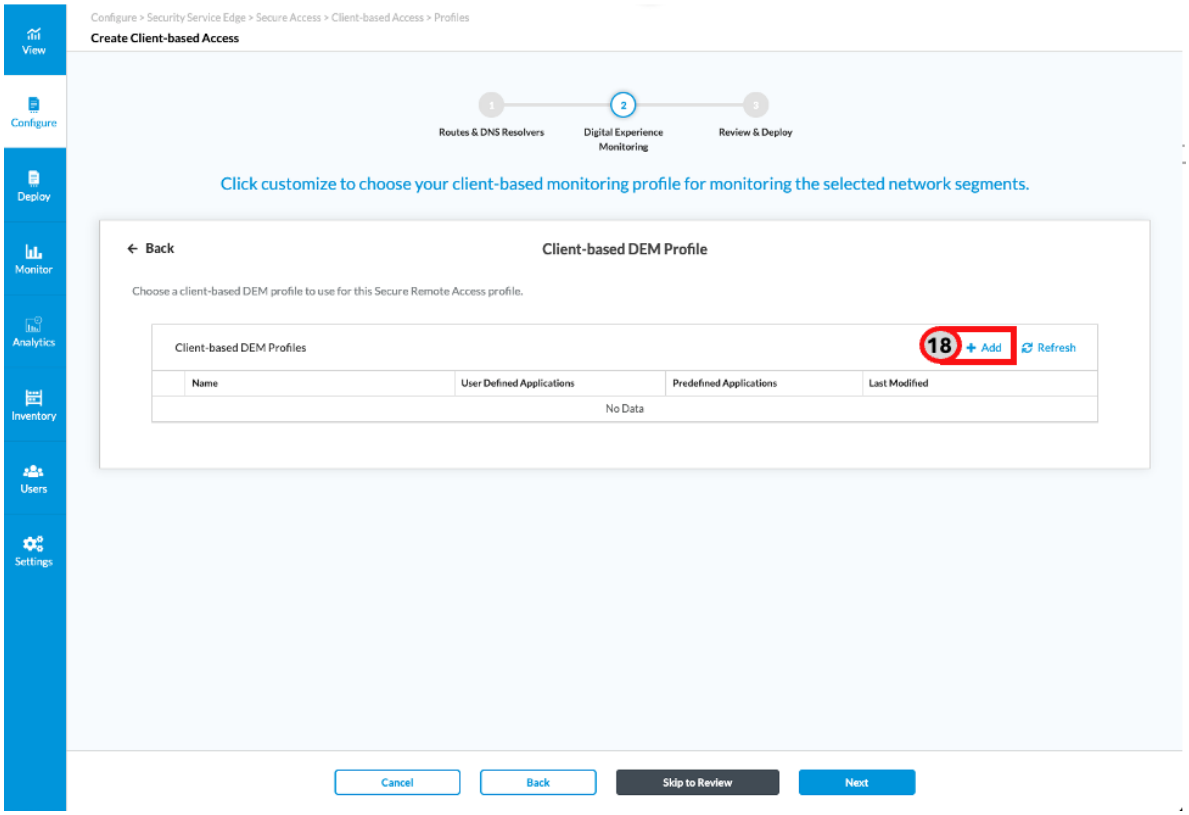
Configure a second DNS IP Address as shown and click **Add**. Then Click **Next** to continue.



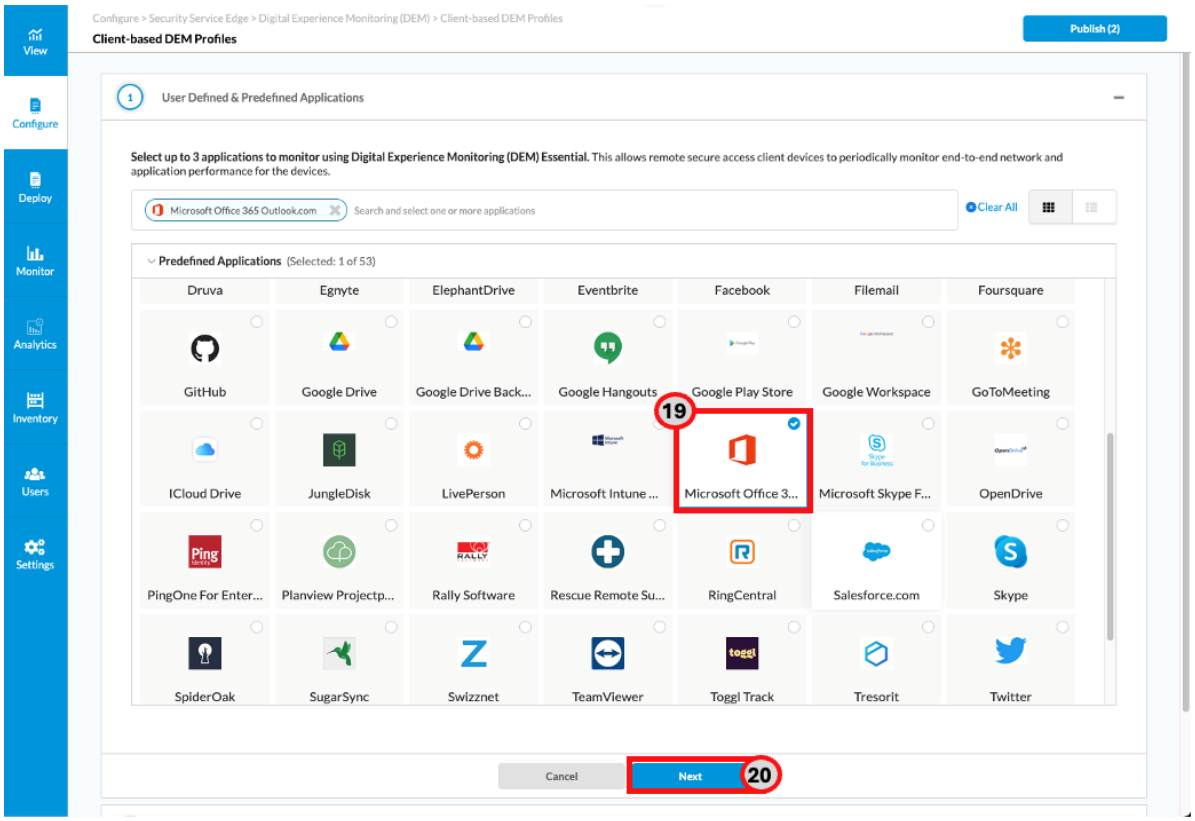
Now create a Digital Experience Monitor by clicking in **Customize**.



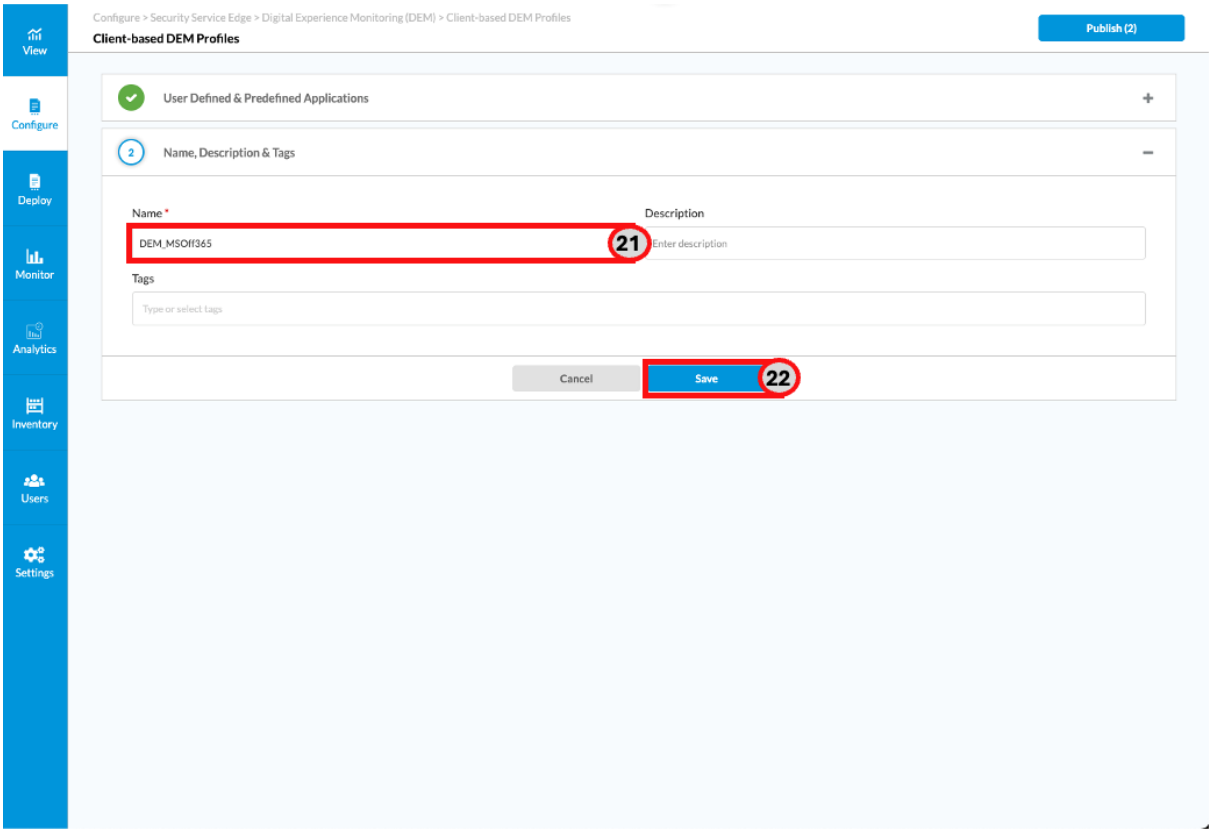
Click **+ Add**.



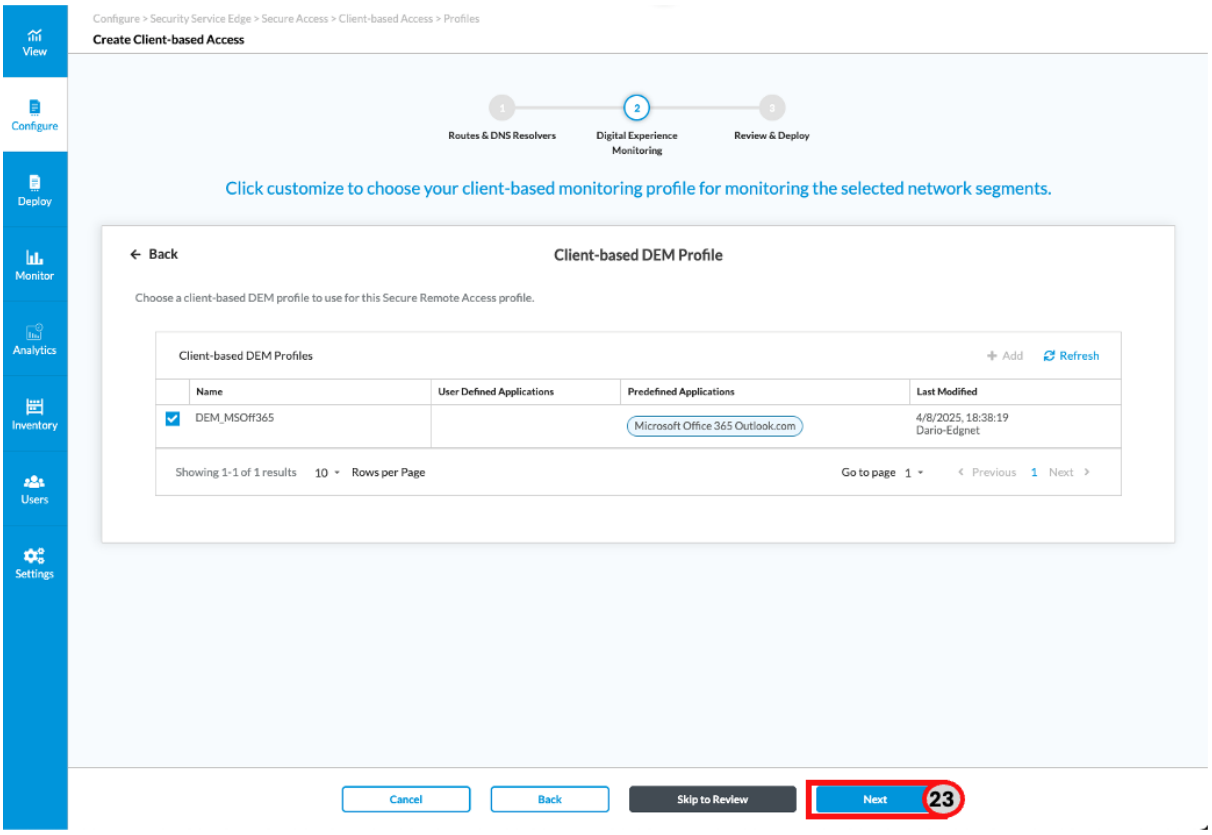
Scroll down and select **Microsoft Office 365**, then click **Next**.



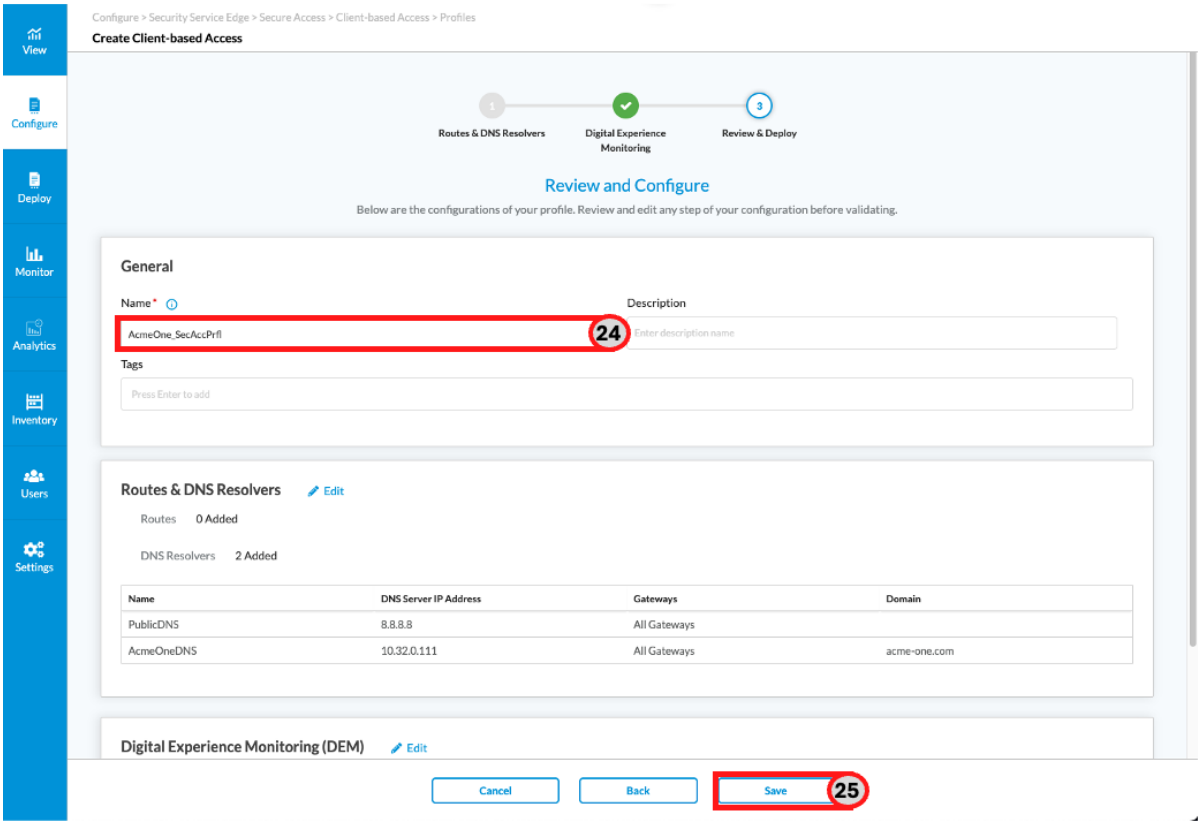
Use a descriptive **Name** for the DEM entry and the click **Save**.



Click **Next**.



Provide a descriptive name for the secure access profile and finally click **Save**).



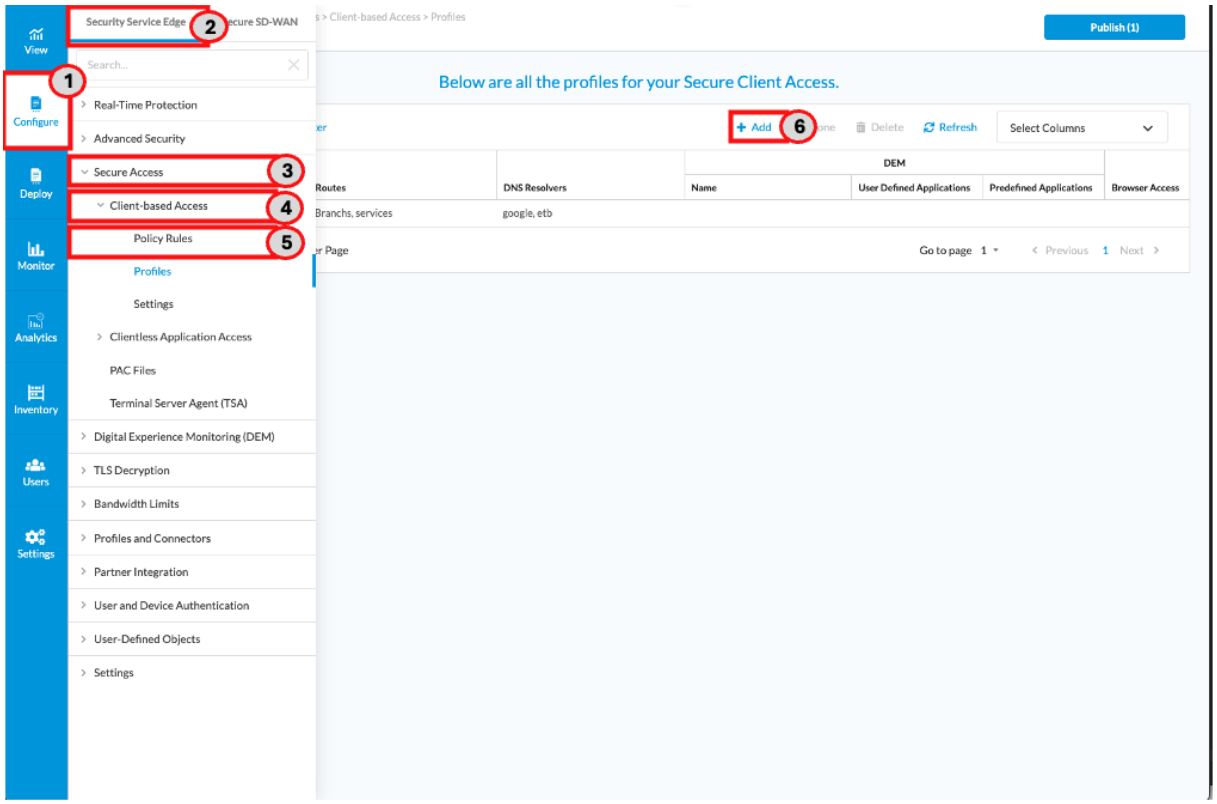
Step 3: Configure Secure Client Access Policy Rules

Secure Access Policy rRles define the connection parameters between the SASE client on the end user device and the SASE gateway. Two access policy rules are required for this use case, one for users in the IT group with the Colombia Geolocation constraint, and the other one for users in the Contractors group allowed worldwide. For both profiles, only Windows devices running any endpoint security application will be allowed; Zoom will bypass the tunnel and go directly to the Internet (DIA – Direct Internet Access). Always On with Fail Close, Trusted Host Name, tamper protection and tunnel monitoring will be configured for both profiles.

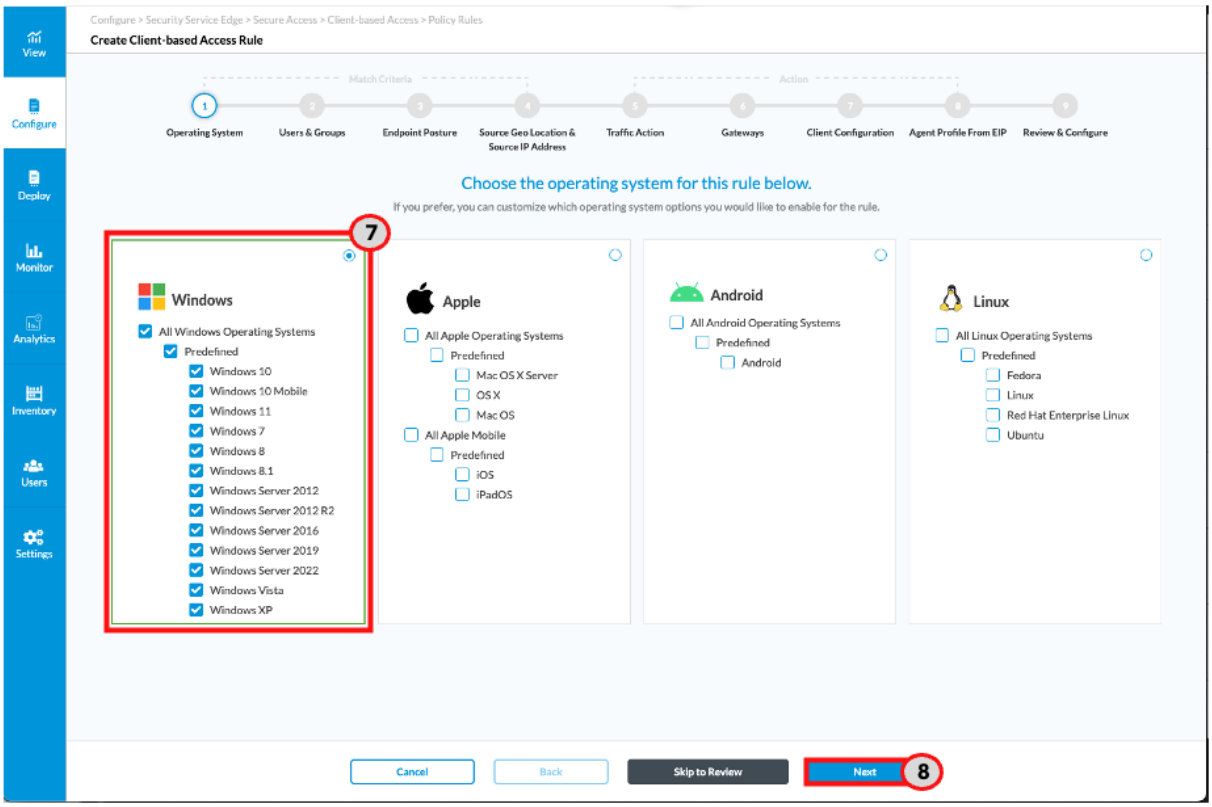
The parameters listed in next table are required to complete the configuration.

Parameter	Description
GeoLocation constrain	Region to apply filtering, Colombia
App to bypass Tunnel(use DIA)	Zoom
Trusted Host Name	Device to be reached to detect the Trusted Network IP/FQDN
Tunnel Monitoring Host	Host to Monitor the tunnel
Access Rule Name	Name for the rule

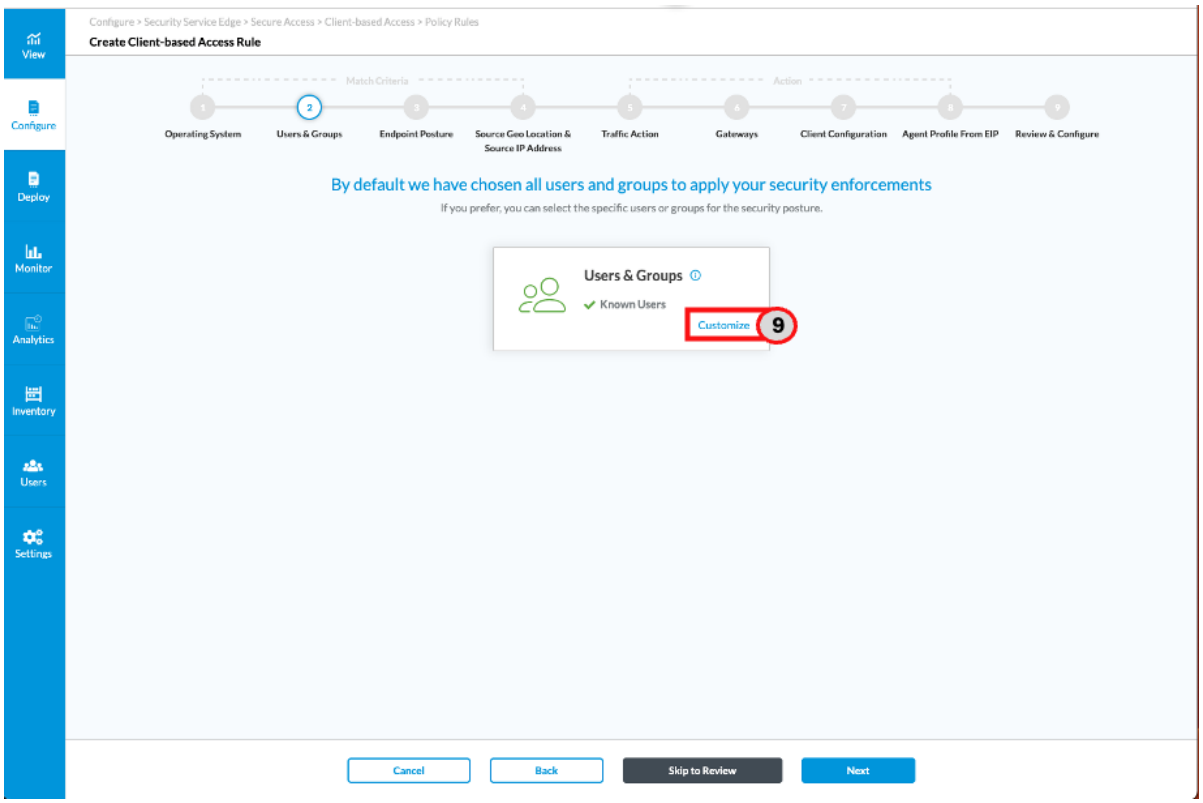
To configure the first secure client access rule for the IT group (Colombia GeoLocation constraint), Navigate to **Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules** and click on **+Add**.



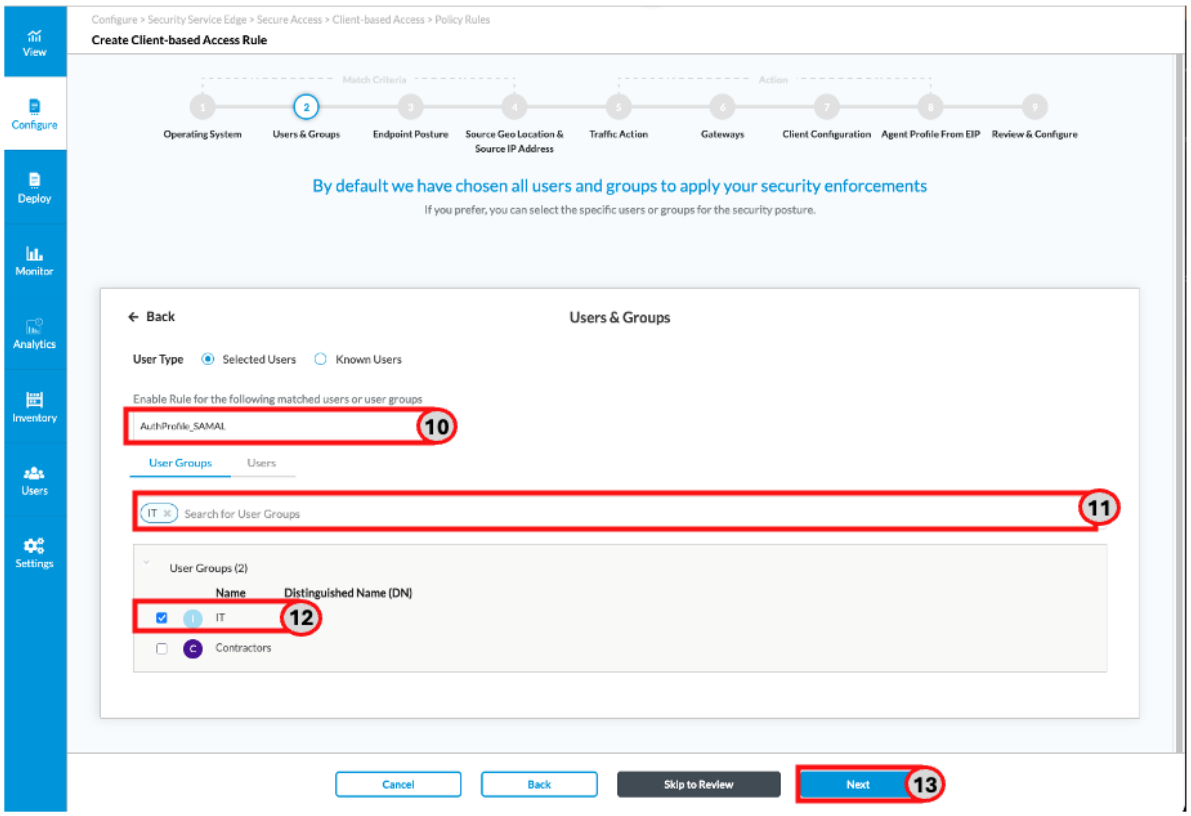
For this use case select **All Windows Operating Systems** and then click **Next**.



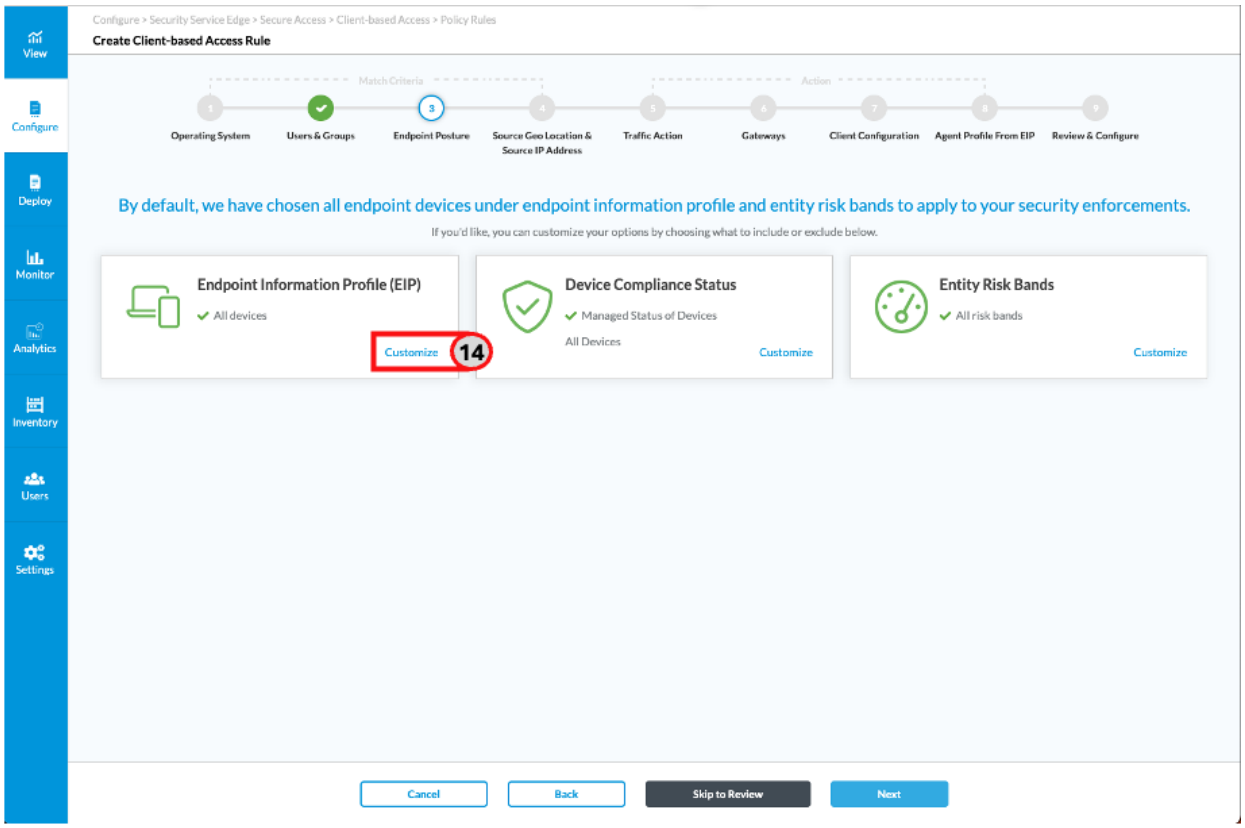
In the users and group section click in **Customize**.



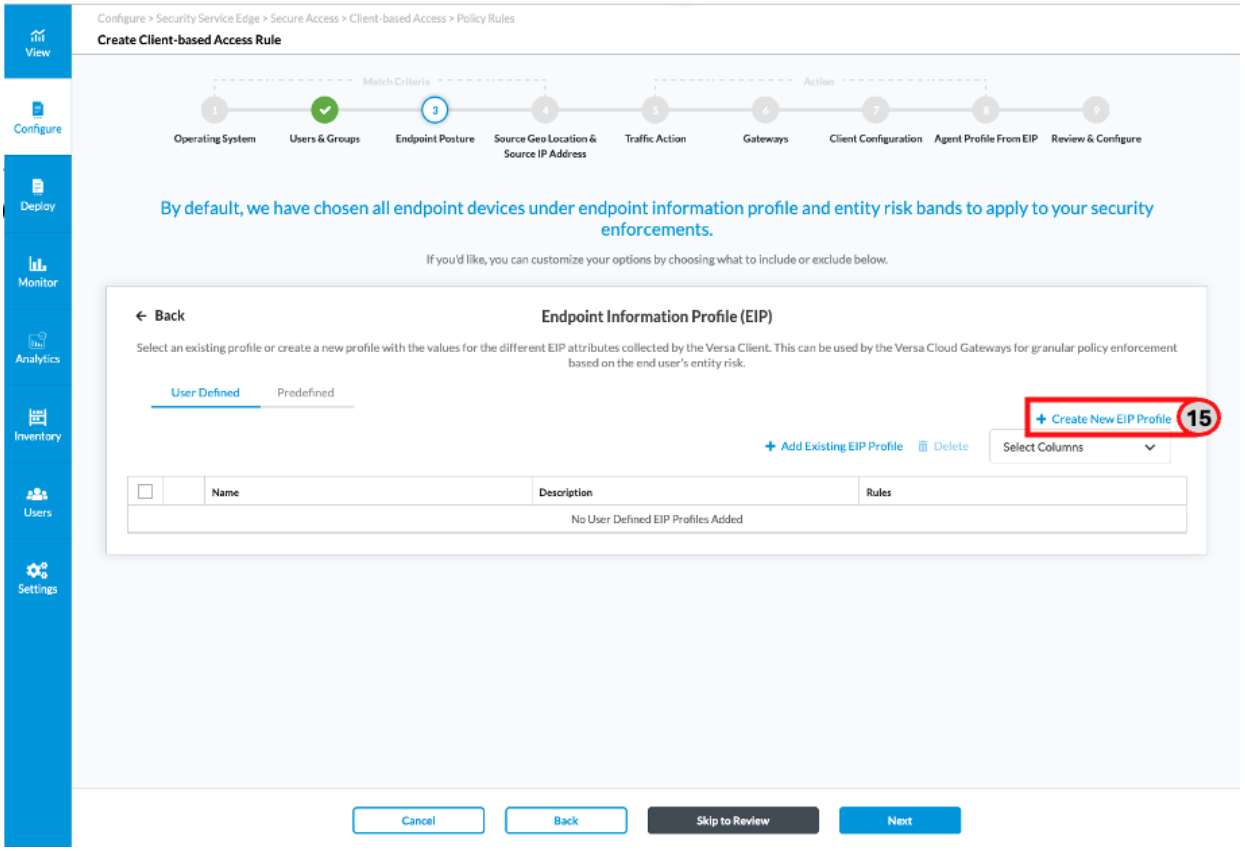
In the users and groups configuration select the SAML authentication profile created before, enter the name of group in the search text box, select the appropriate group and then click **Next**.



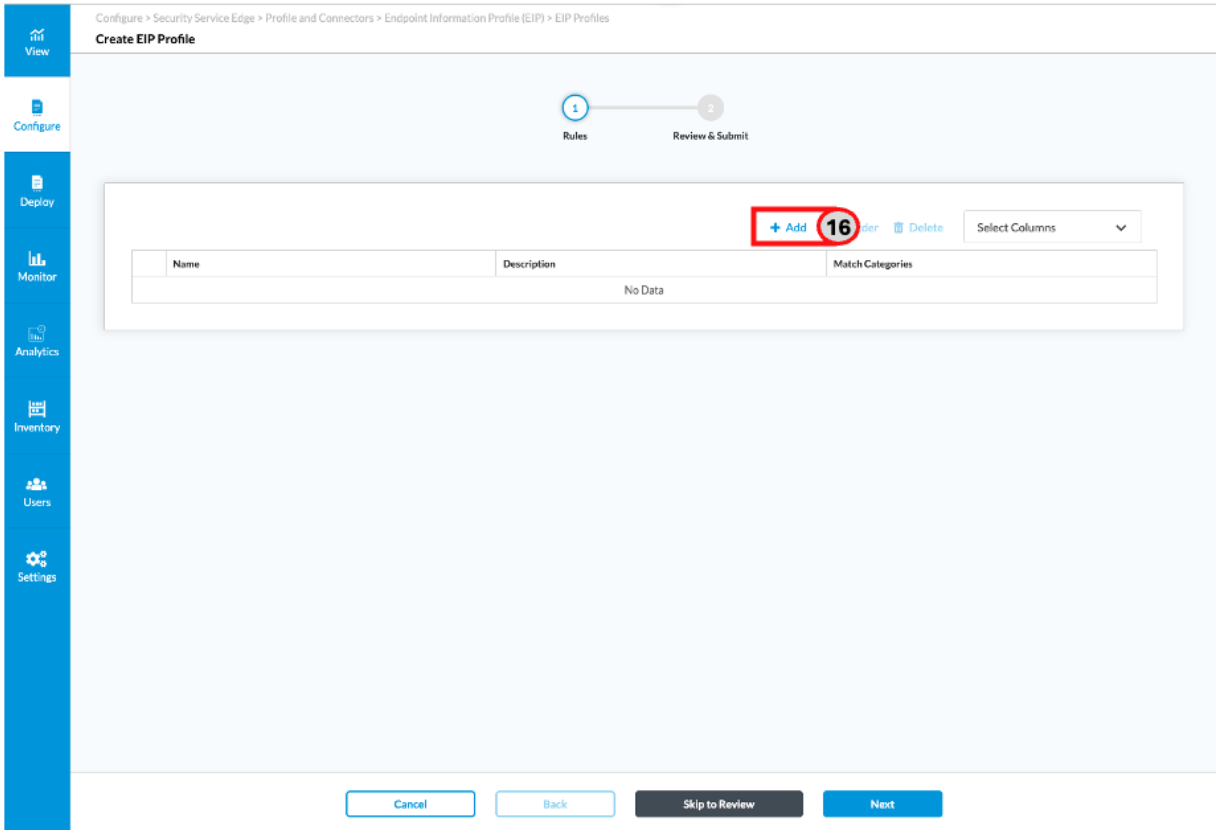
In Endpoint Posture, click **Customize** under the Endpoint Information Profile (EIP) box.



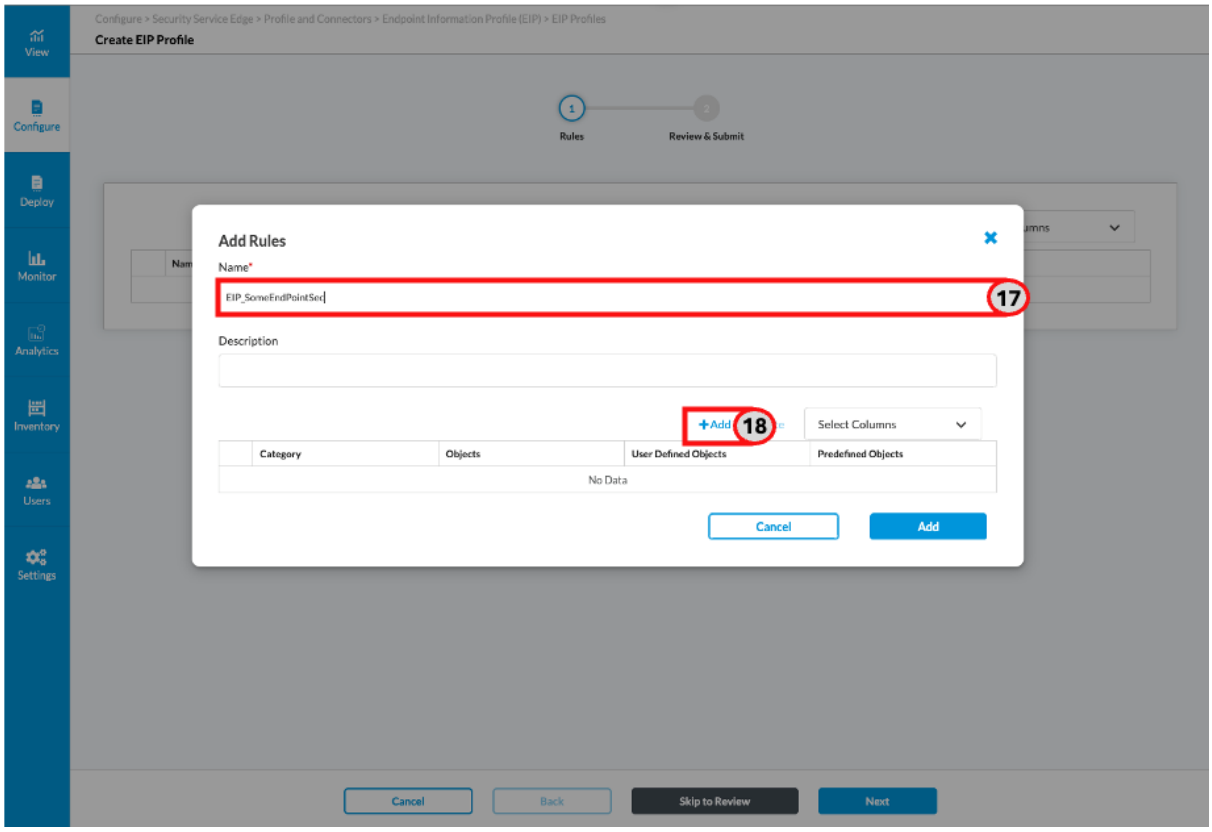
Click **+ Create New EIP Profile**.



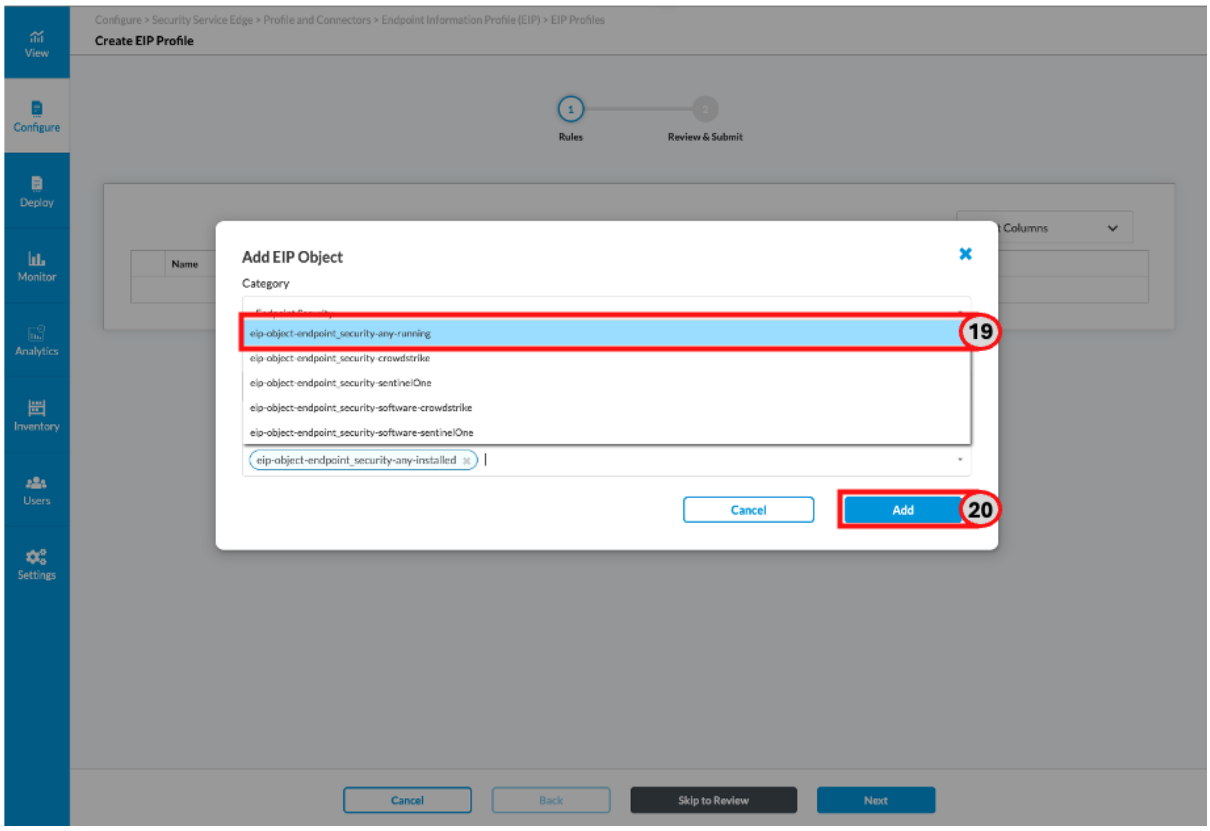
In the page that appears, click **Add**.



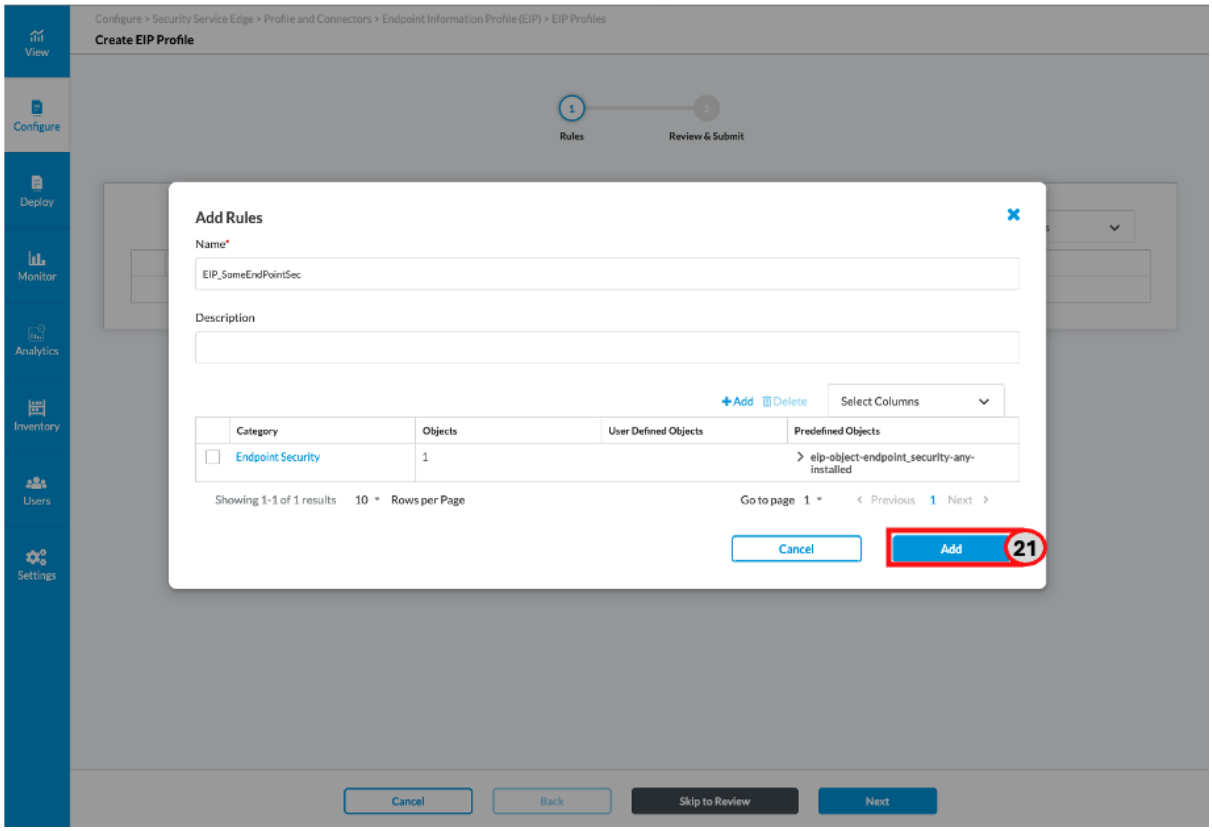
Assign a descriptive **Name**, then click **Add**.



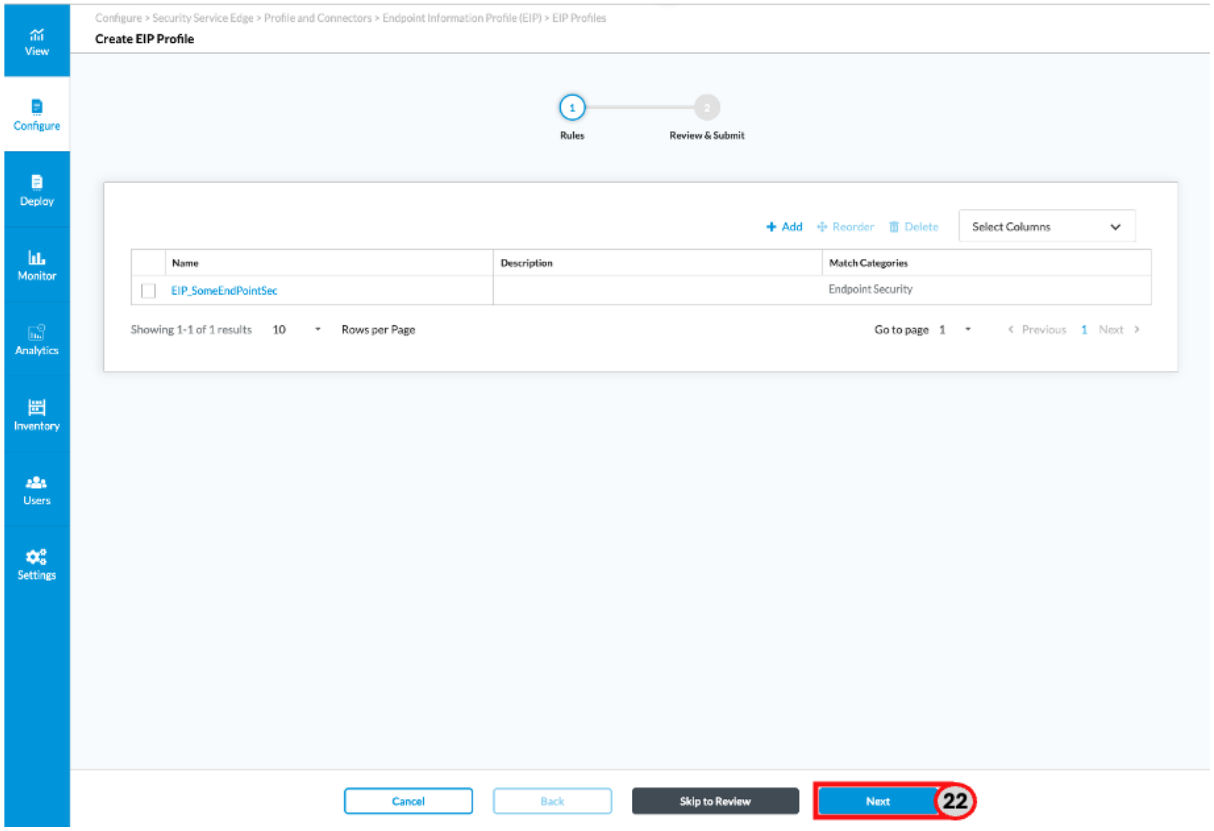
In the Add EIP Object pop up, select **eip-object-endpoint-security-any-running**, then click **Add**.



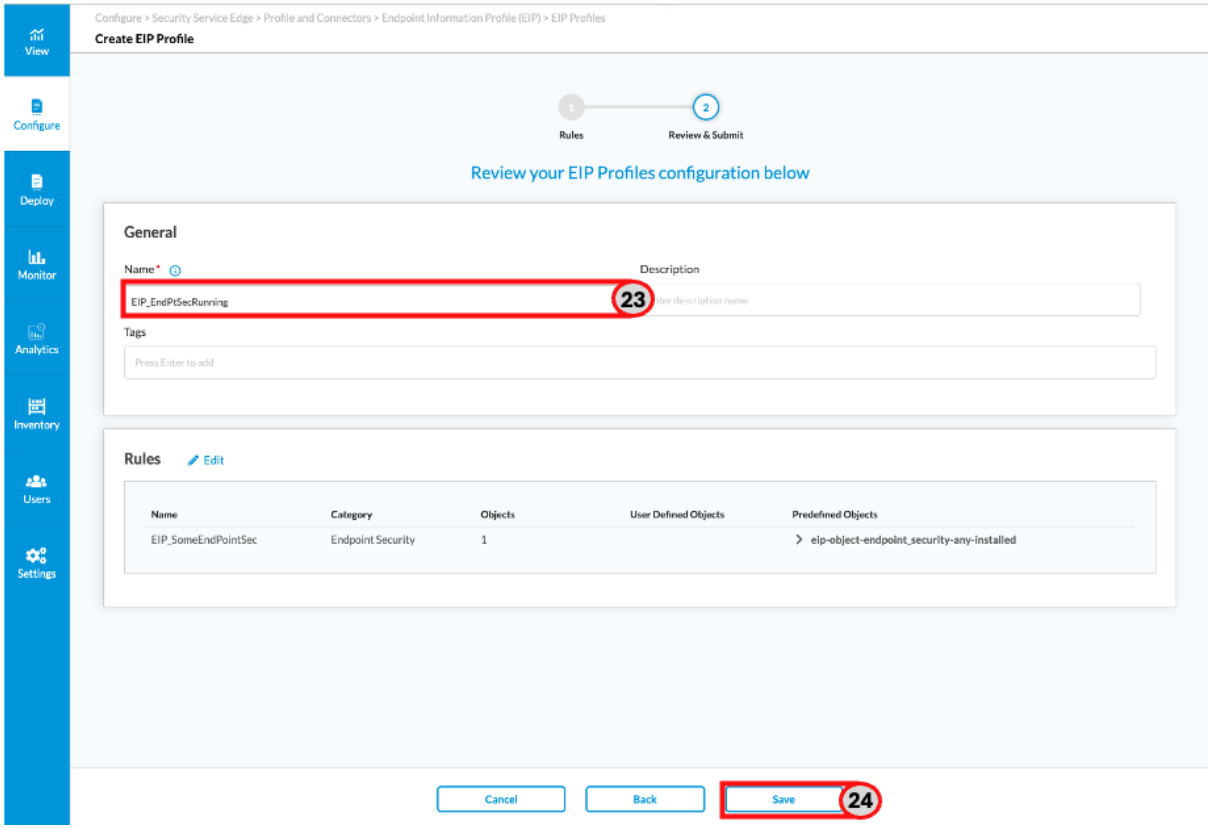
Click **Add** again.



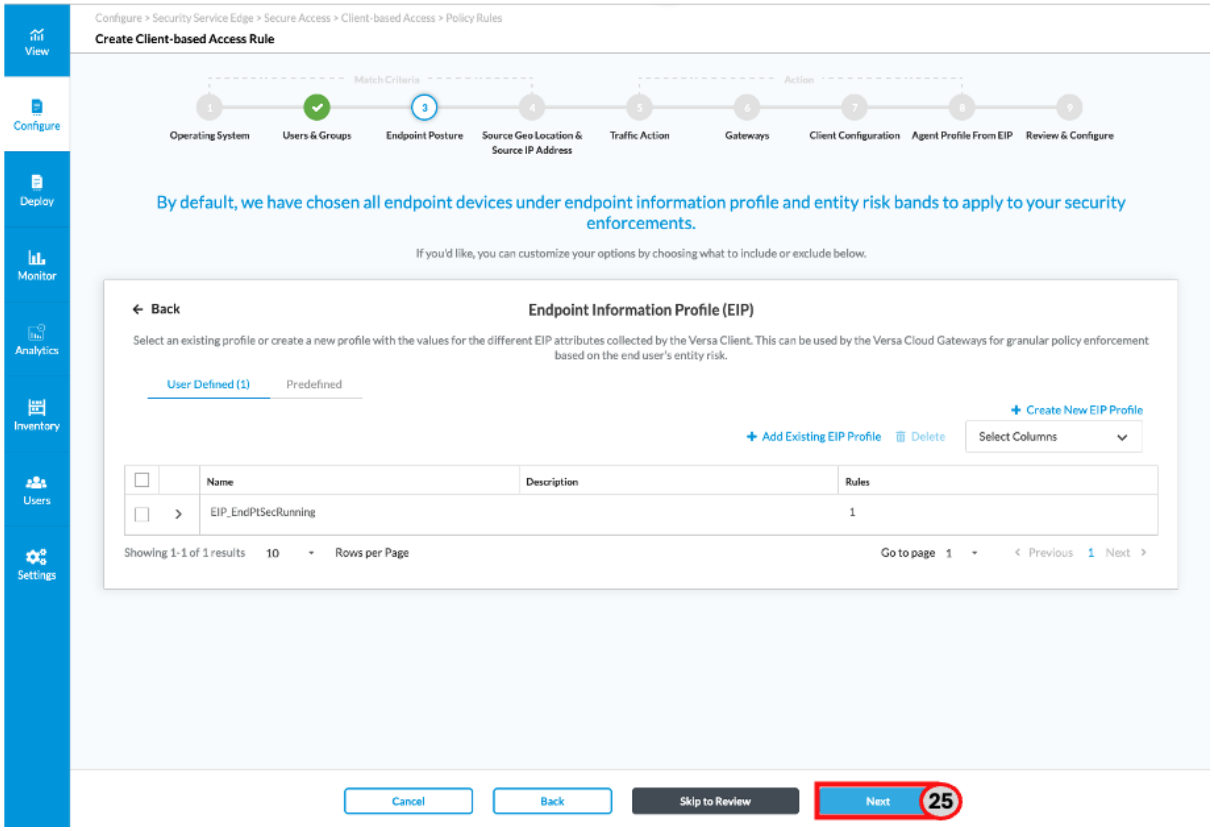
Click Next.



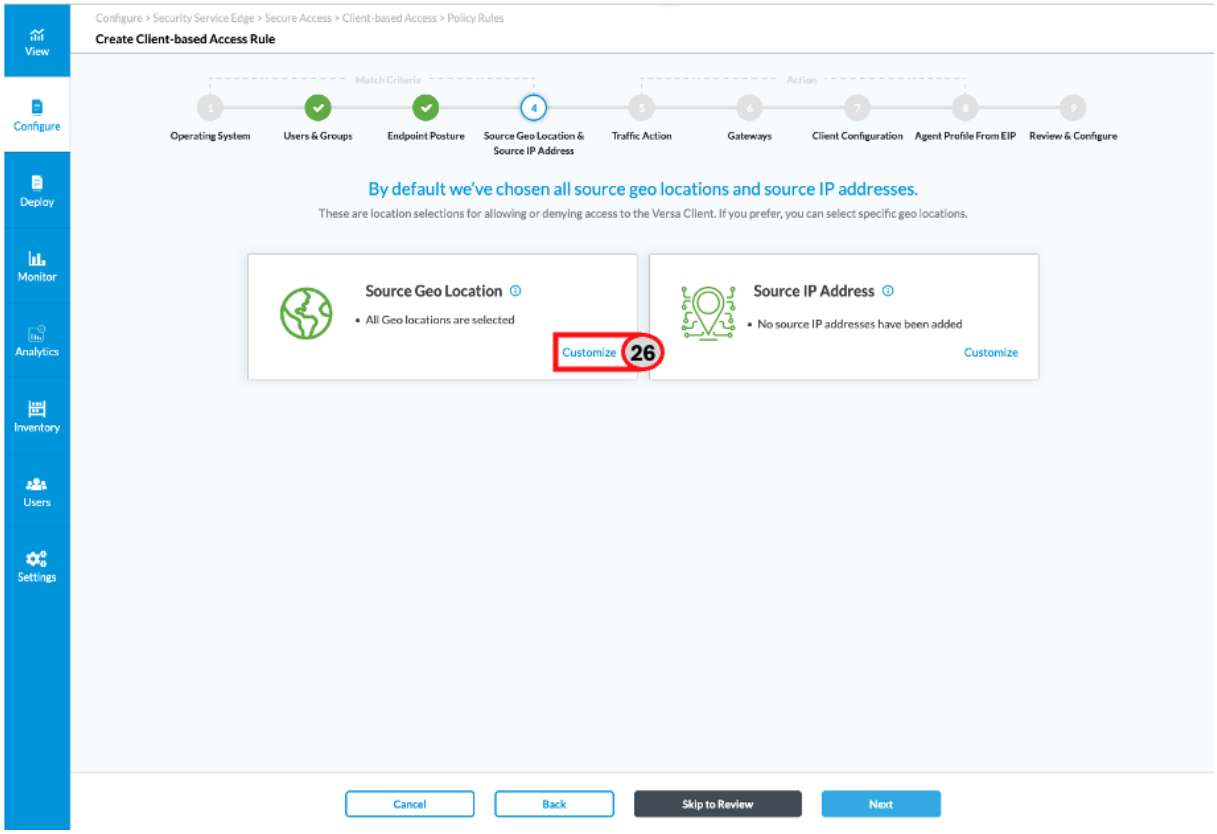
Assign a descriptive **Name** for the EIP Profile and **Save**.



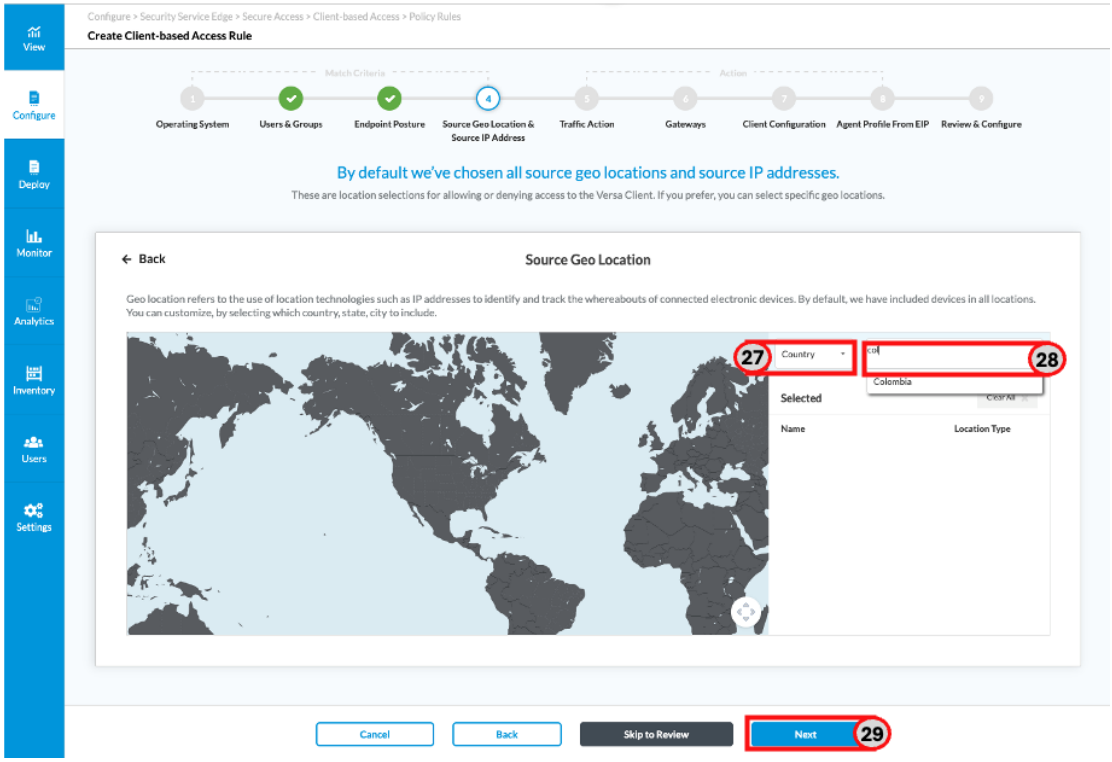
With the Endpoint Information Profile added, click **Next**.



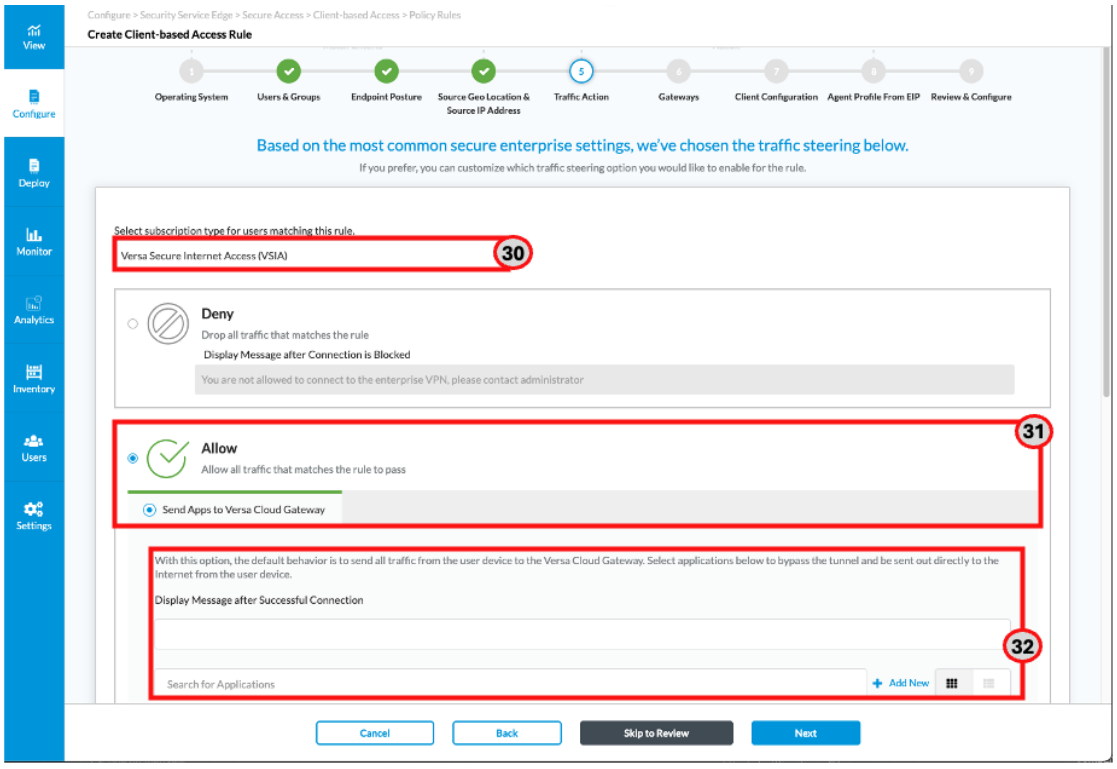
Click **Customize** in the Source Geo Location box.



Select the *Country* option from the dropdown and search and select **Colombia**, then click ***Next***.

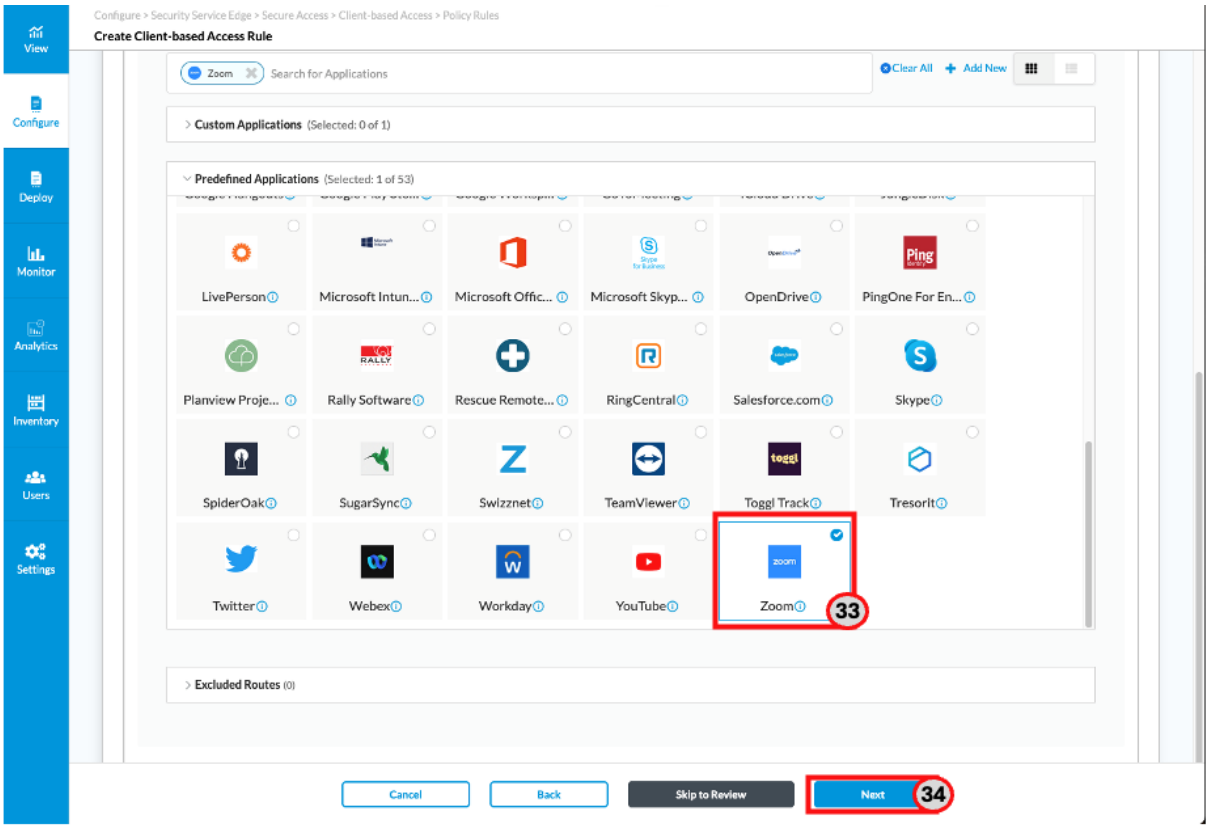


For the traffic action configuration first select the Subscription type corresponding to your License, in this case **VSIA** . Note: there are another two possible traffic actions: VSPA and VSIA & VASPA. Select **Allow** (31), which sends all matching traffic to the gateway, except the Zoom application selected in the list bellow.

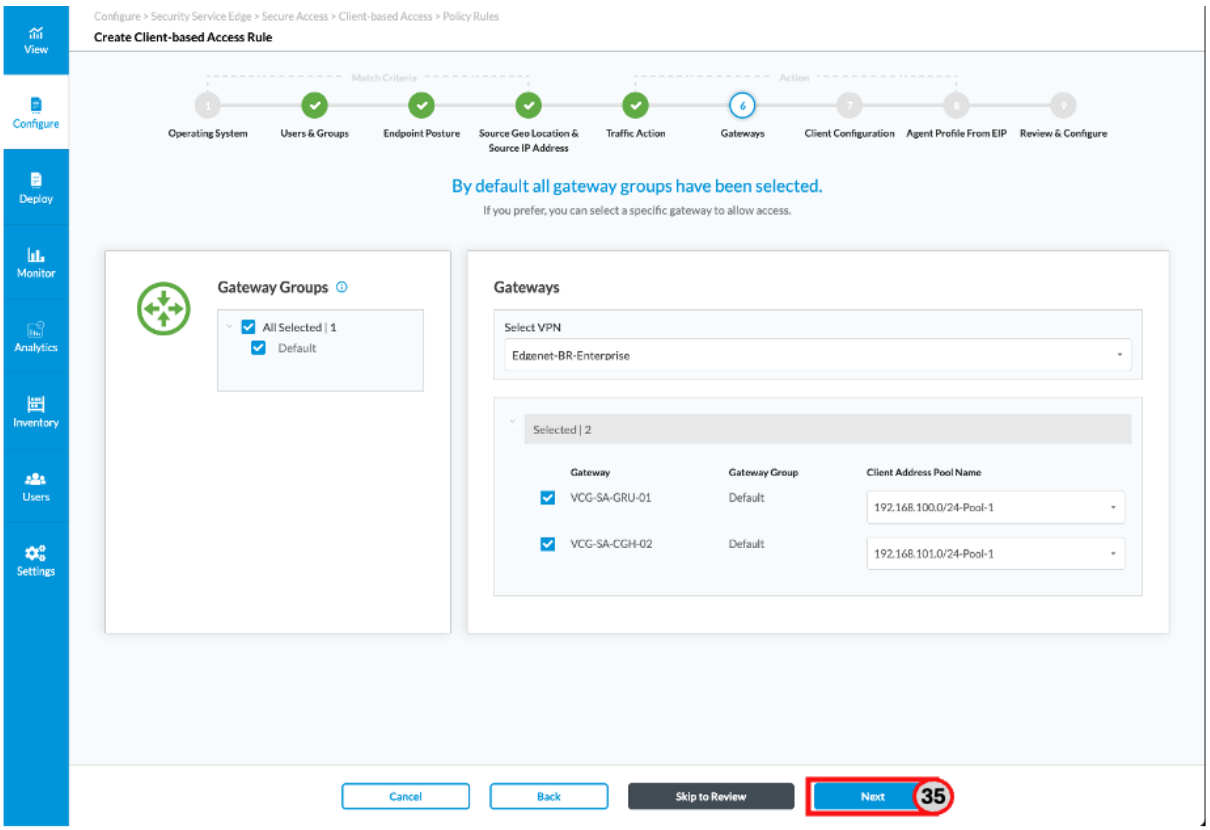


You can bypass the Gateway for custom or *predefined applications*. Scroll down and select **Zoom** from the Predefined

Applications list, then click **Next**.

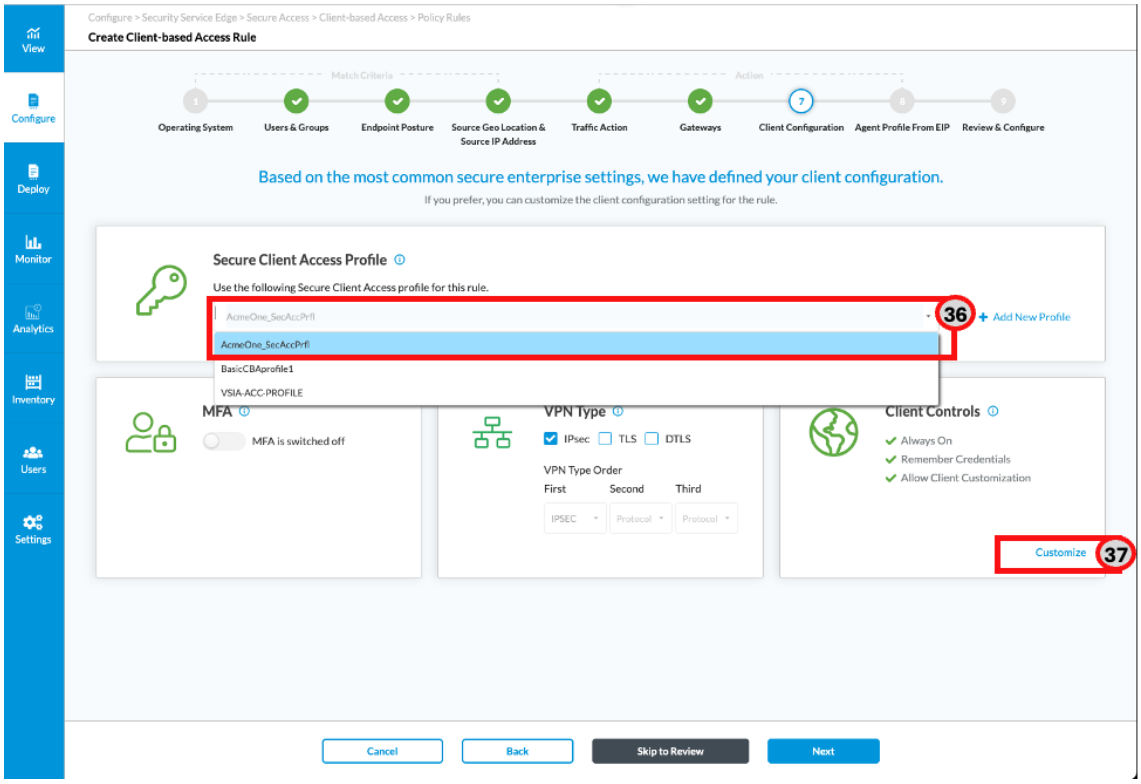


Let the default gateways configuration and click **Next**.

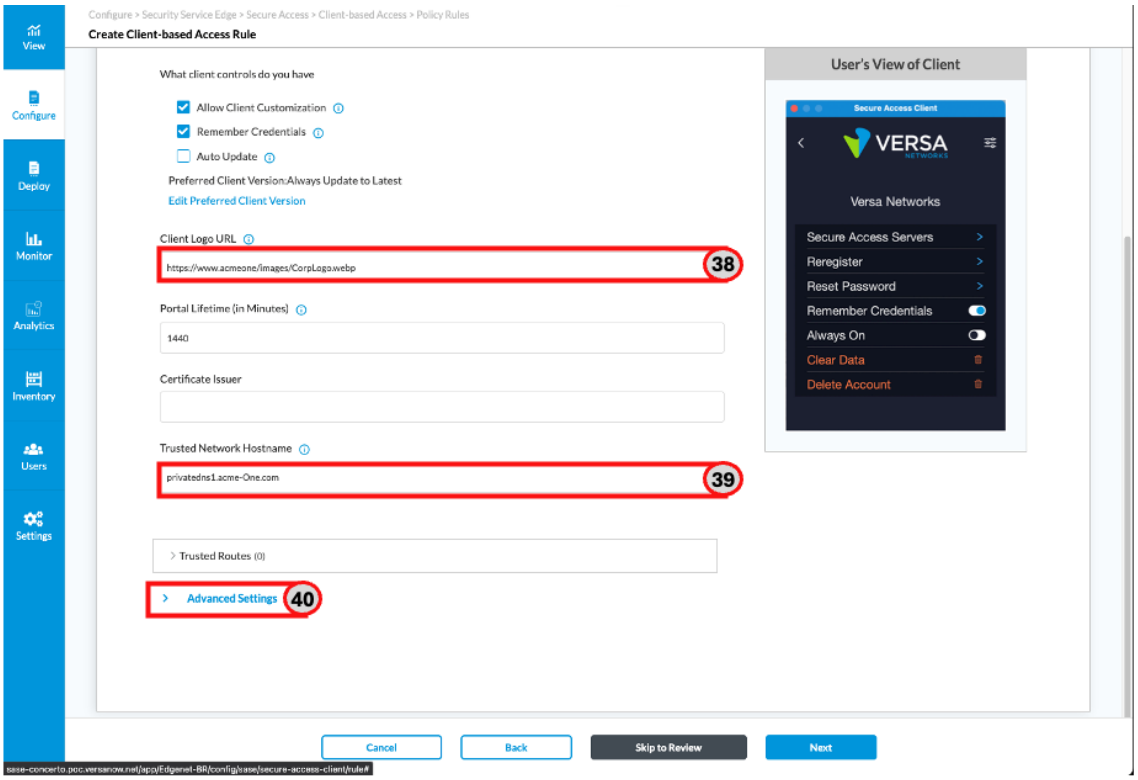


Select the Secure Client Access Profile configured previously to be used with this policy rule the click **Customize** in the

Client Controls box.

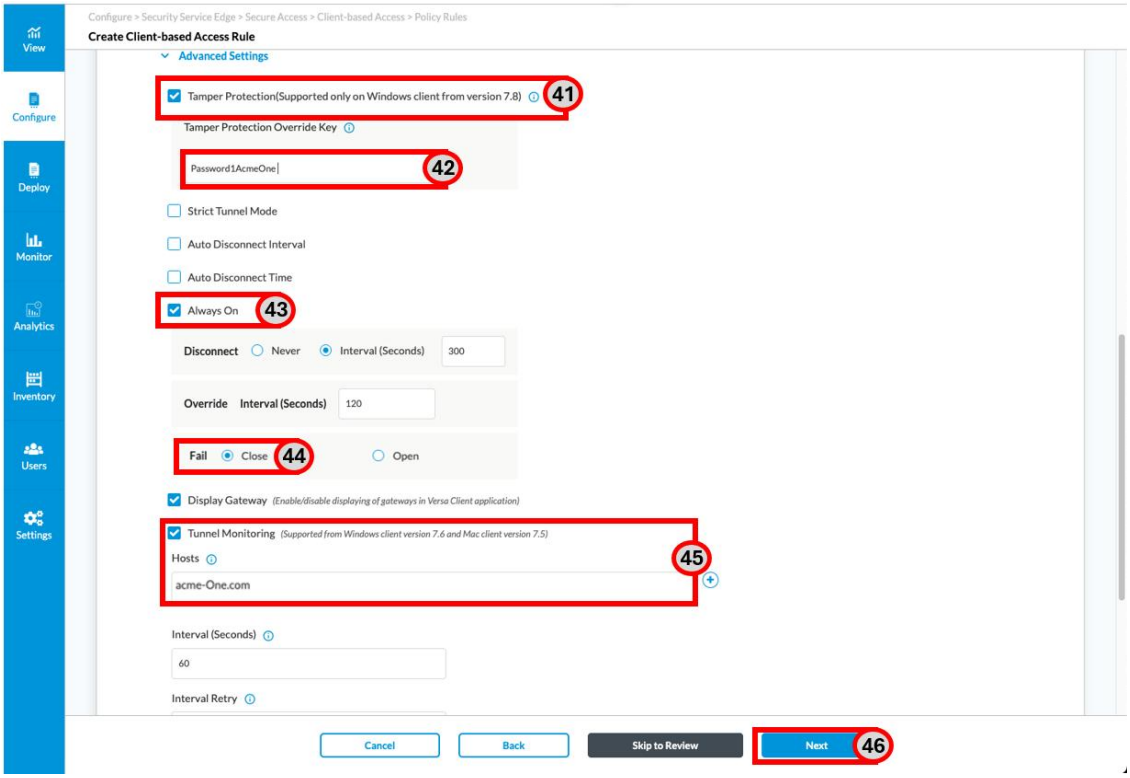


For Client Configuration, fill the **Client Logo URL** information to USE the logo in the Client, define the **Trusted Network Hostname** and click the **Advanced Settings** arrow .

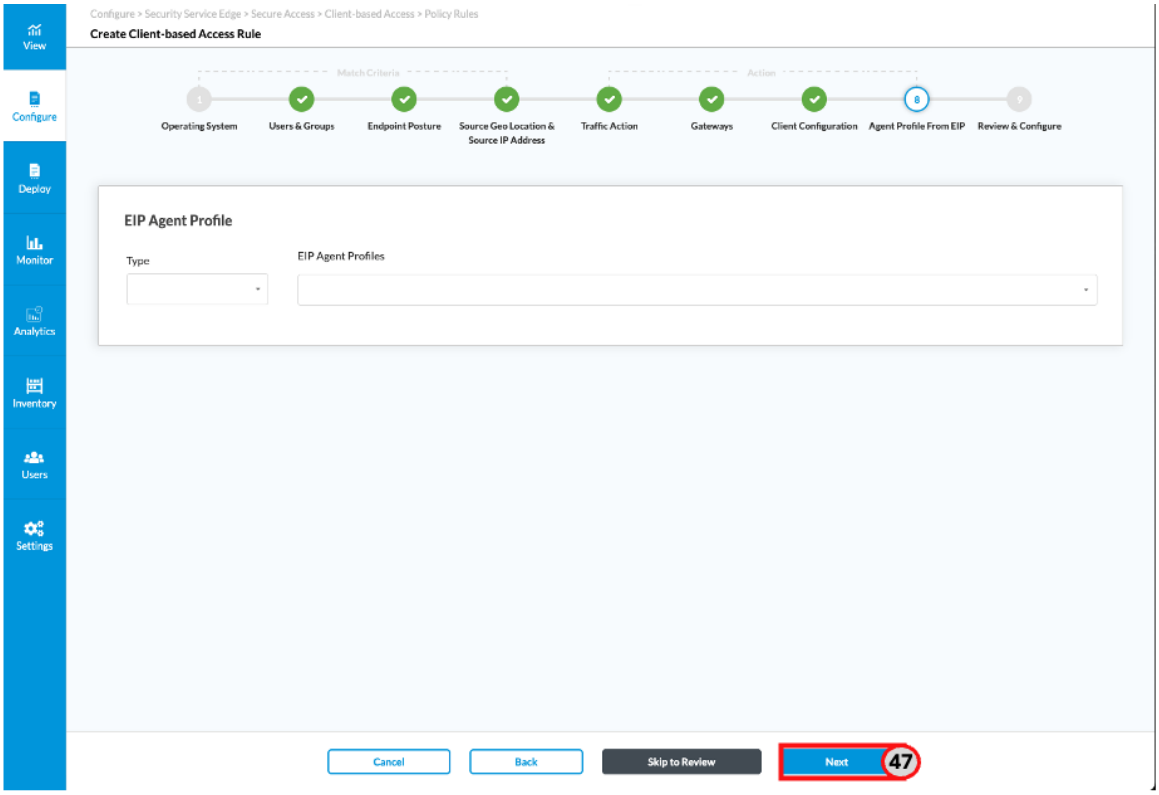


In the Advanced Settings section, select the Tamper Protection checkbox and provide the Tamper Protection Override

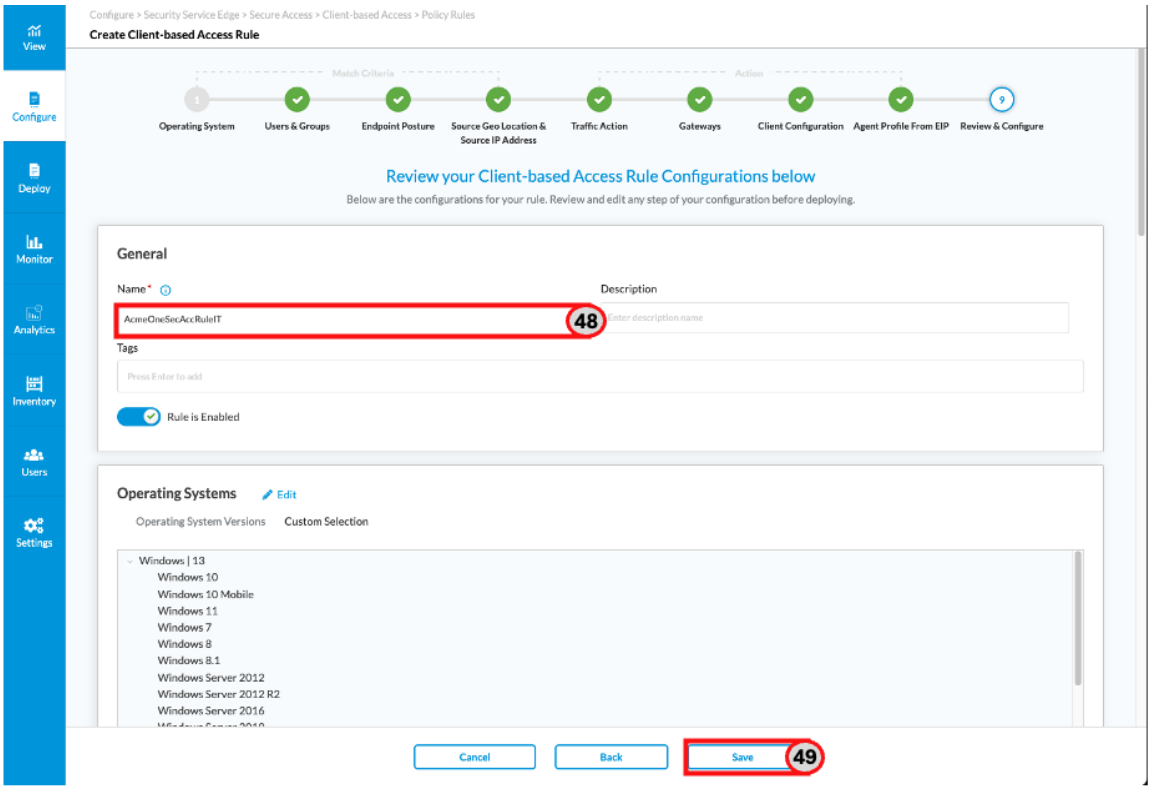
Key password. Select the checkbox **Always On** and the **Close** radio button which closes the tunnel if there is a failure., Select the checkbox **Tunnel Monitoring** with the Hosts information as shown below. Click **Next**.



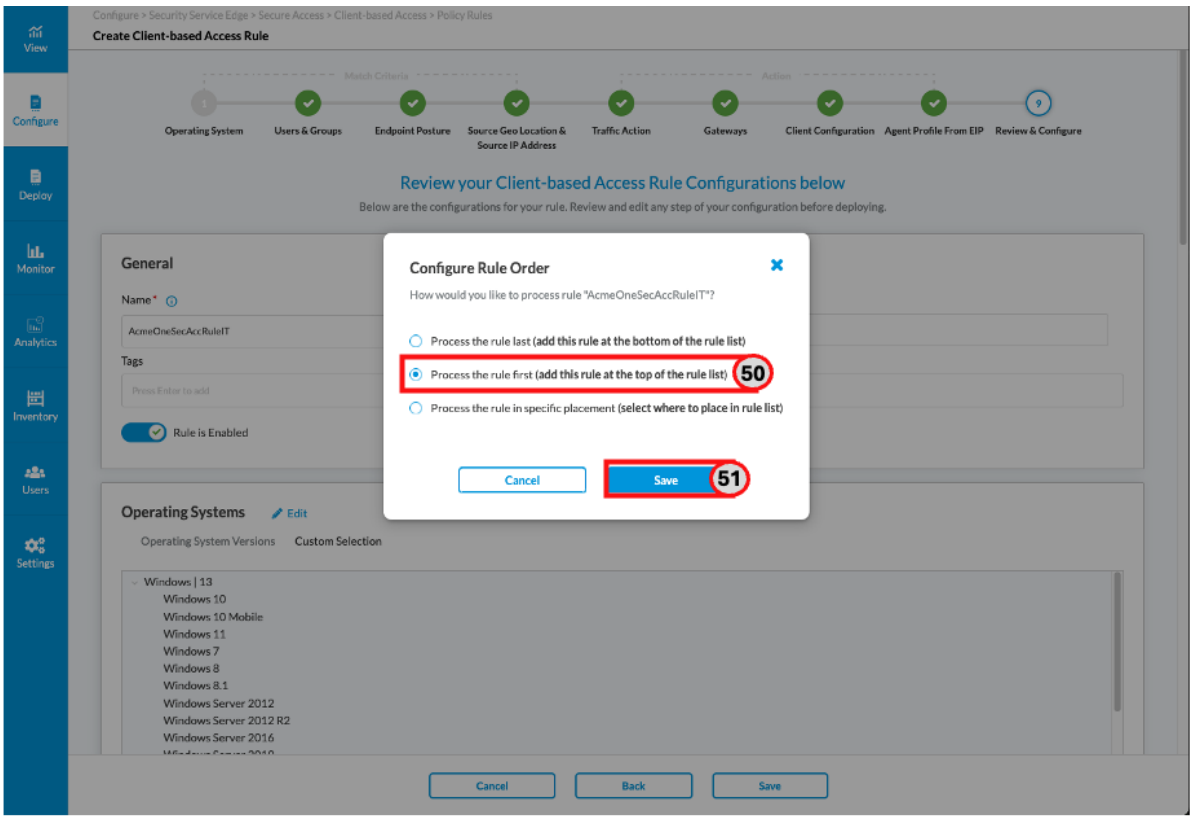
In the Agent Profile from EIP step, click **Next**.



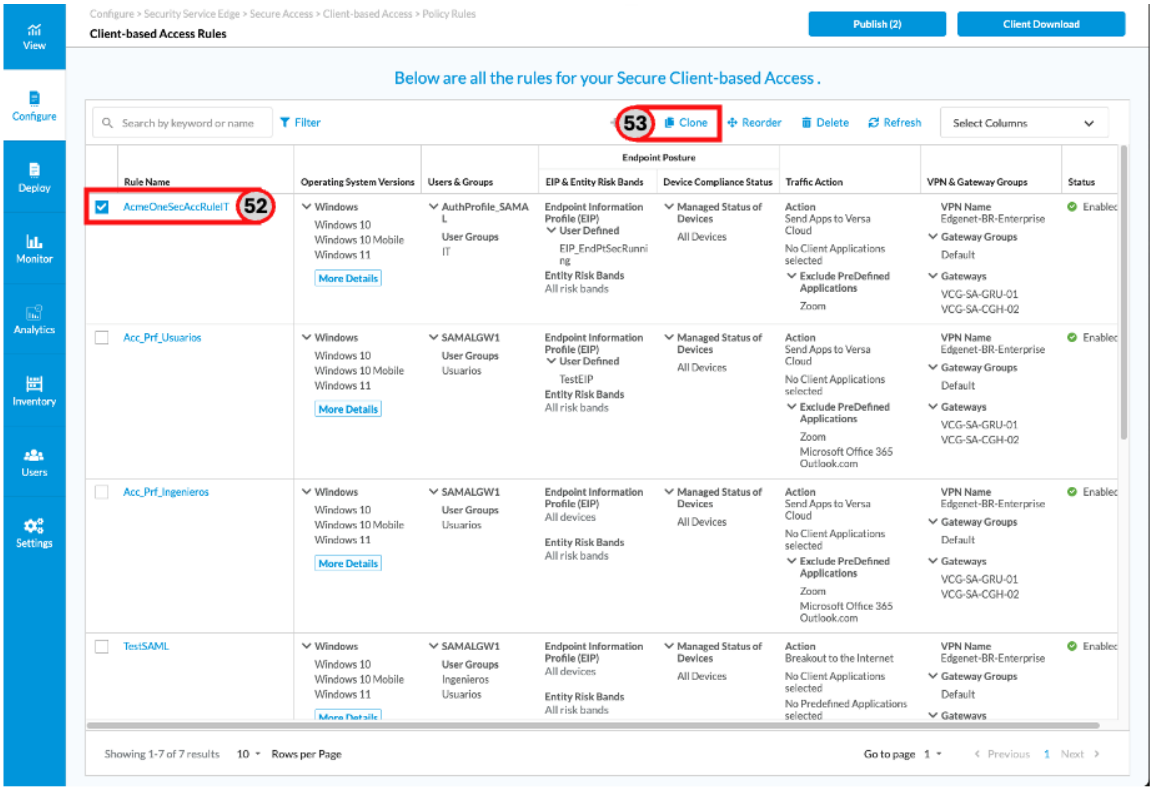
On the **Review & Submit** page, assign a descriptive **Name** for the Secure Access Policy Rule.. Confirm the configuration, then click **Save**.



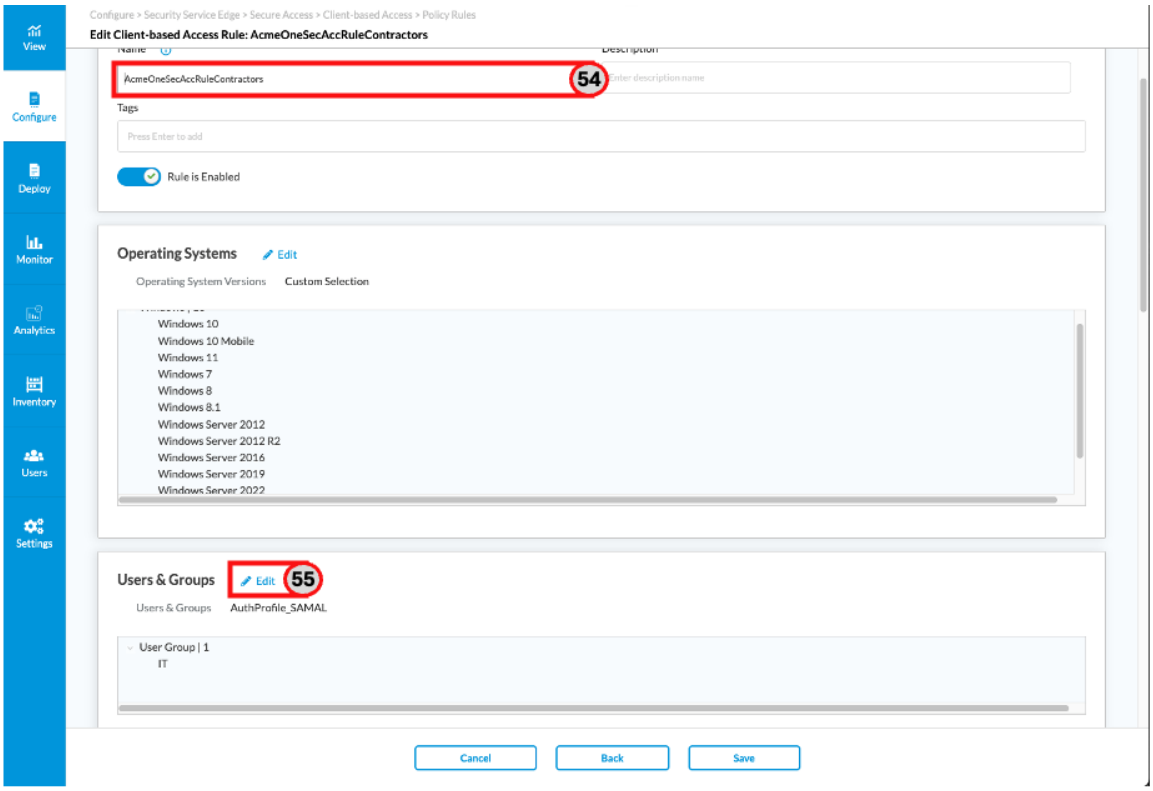
Configure the rule to be evaluated first and click **Save**.



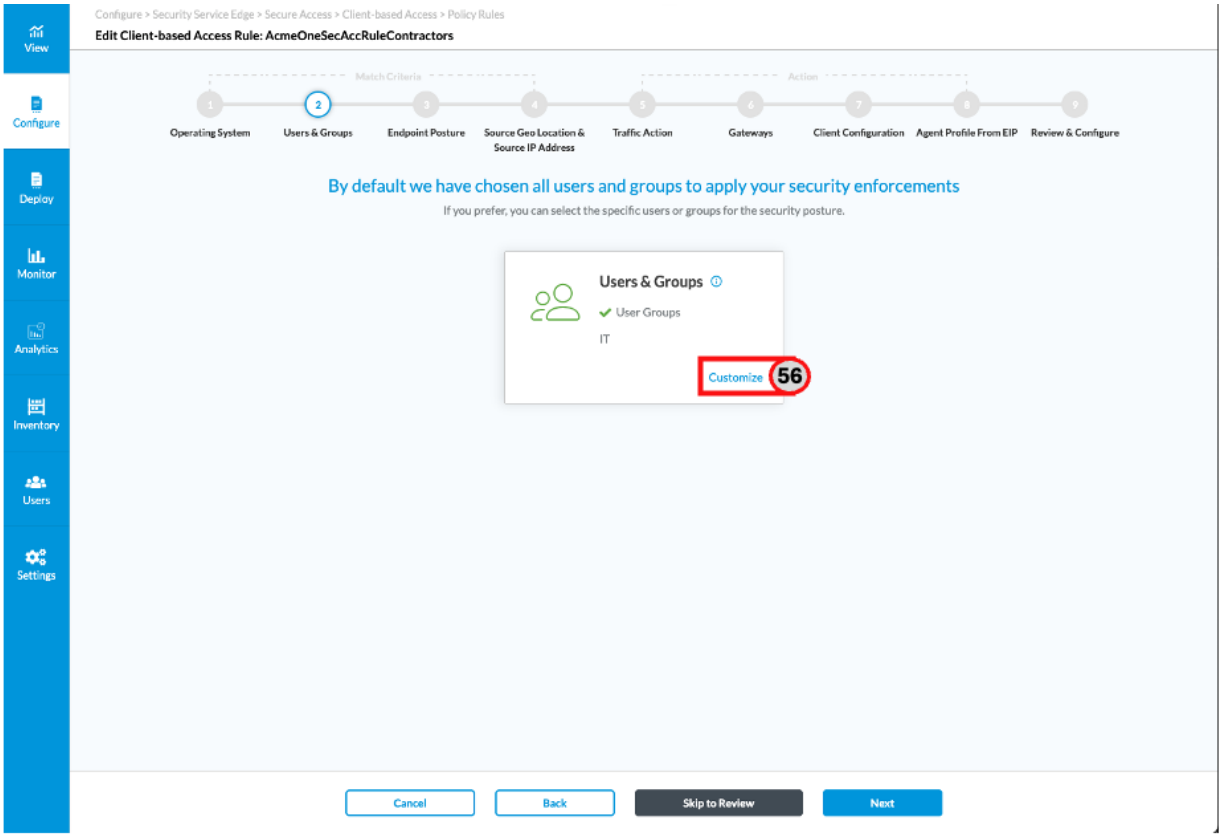
To create the second rule for Contractors group (without Geolocation constraints), the same rule can be used with modified settings. Select the rule you just created and click **Clone** to copy it.



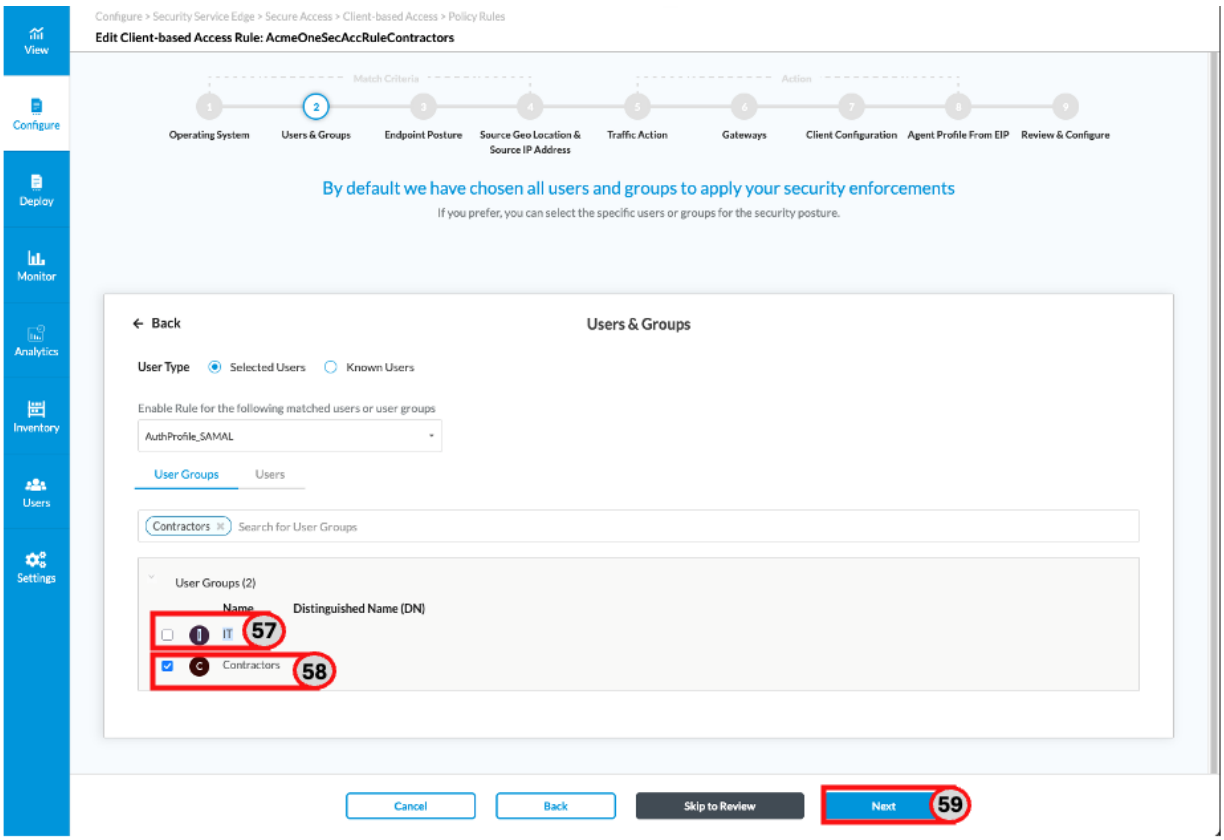
Provide a descriptive **Name** for the new Secure Access Policy Rule and selec **Edit** in the *Users & Groups section*.



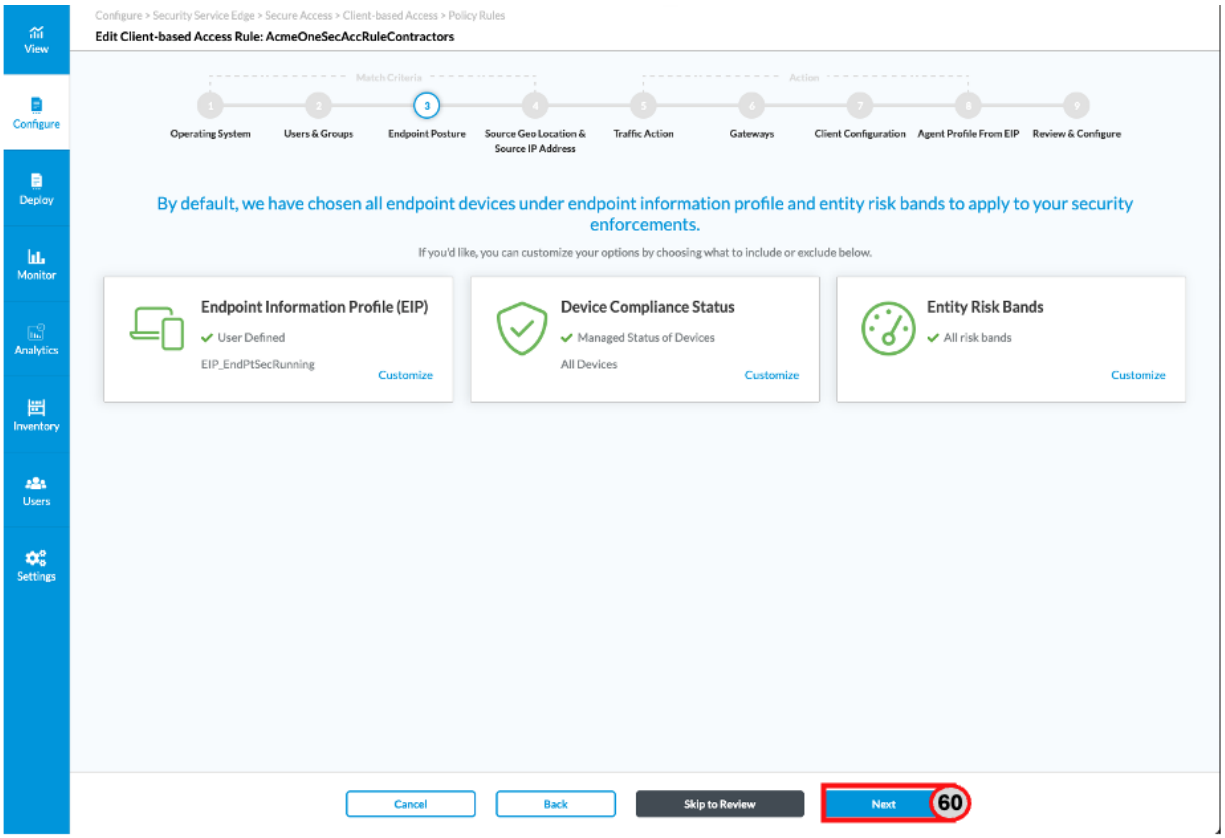
Click **Customize** for Users & Groups.



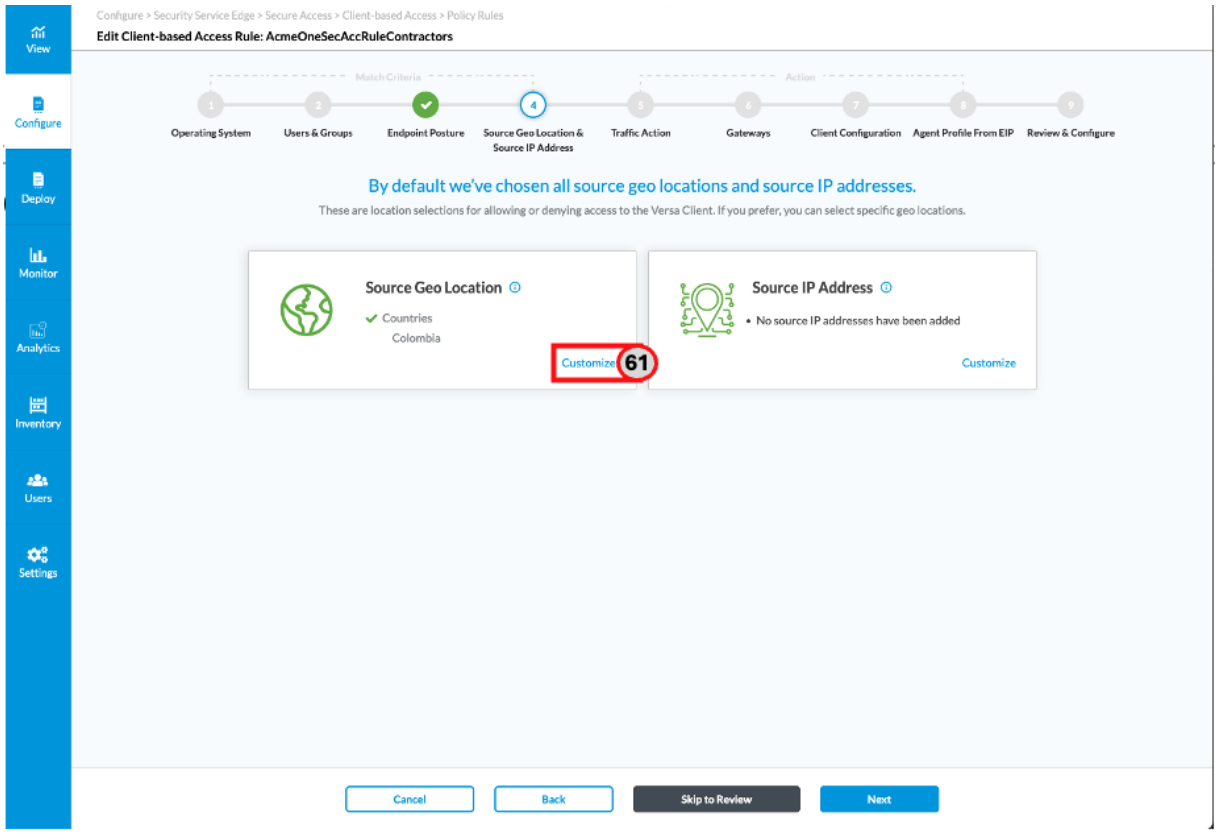
Uncheck the *IT* group and check the Contractors group to be used in this rule. Now click **Next**.



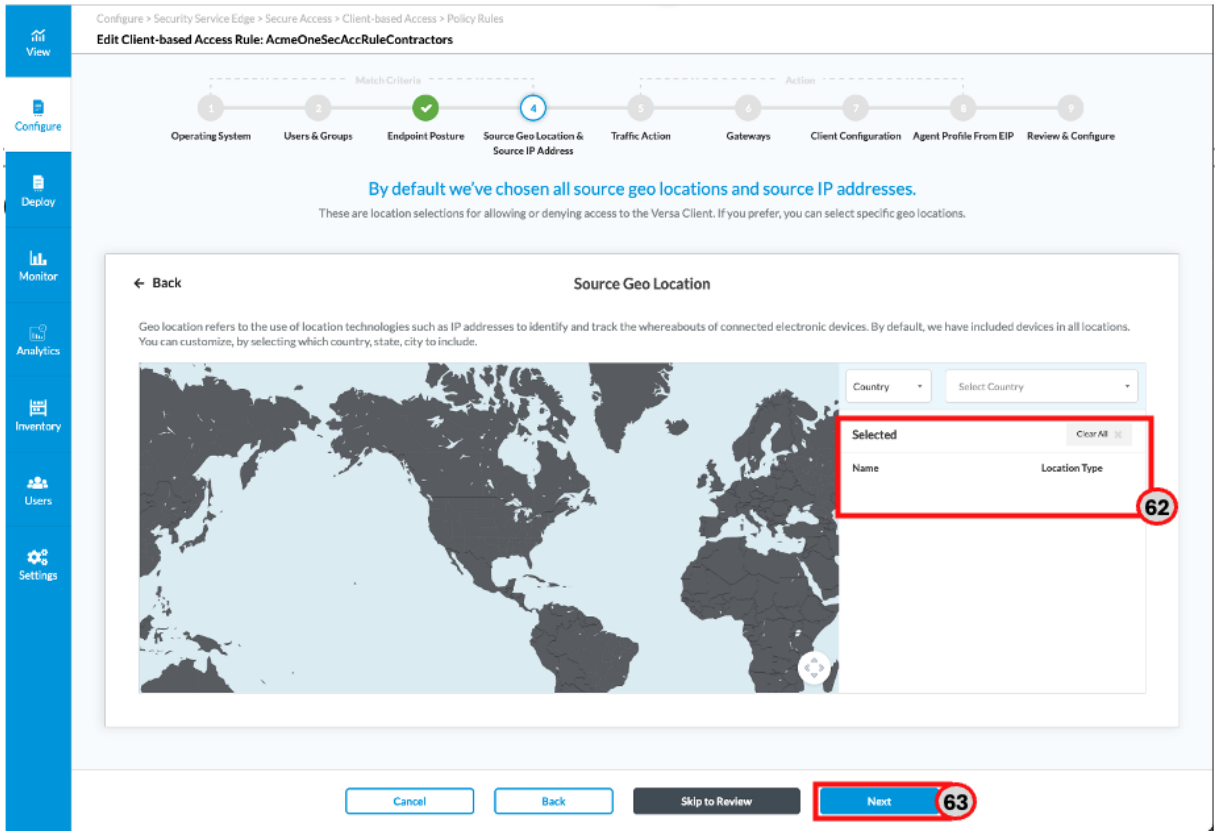
There are no changes to the Endpoint Posture , so click **Next**.



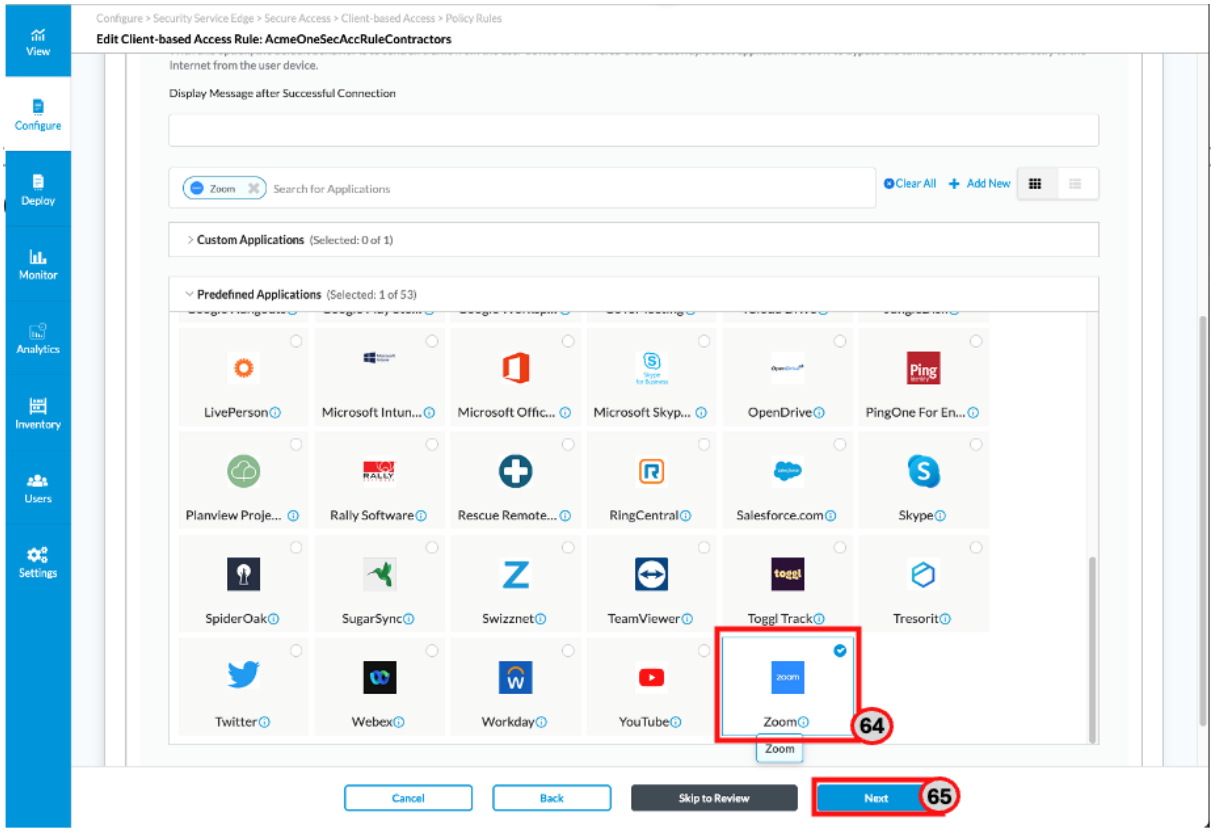
Change the country in the Source Geo Location box by clicking **Customize**.



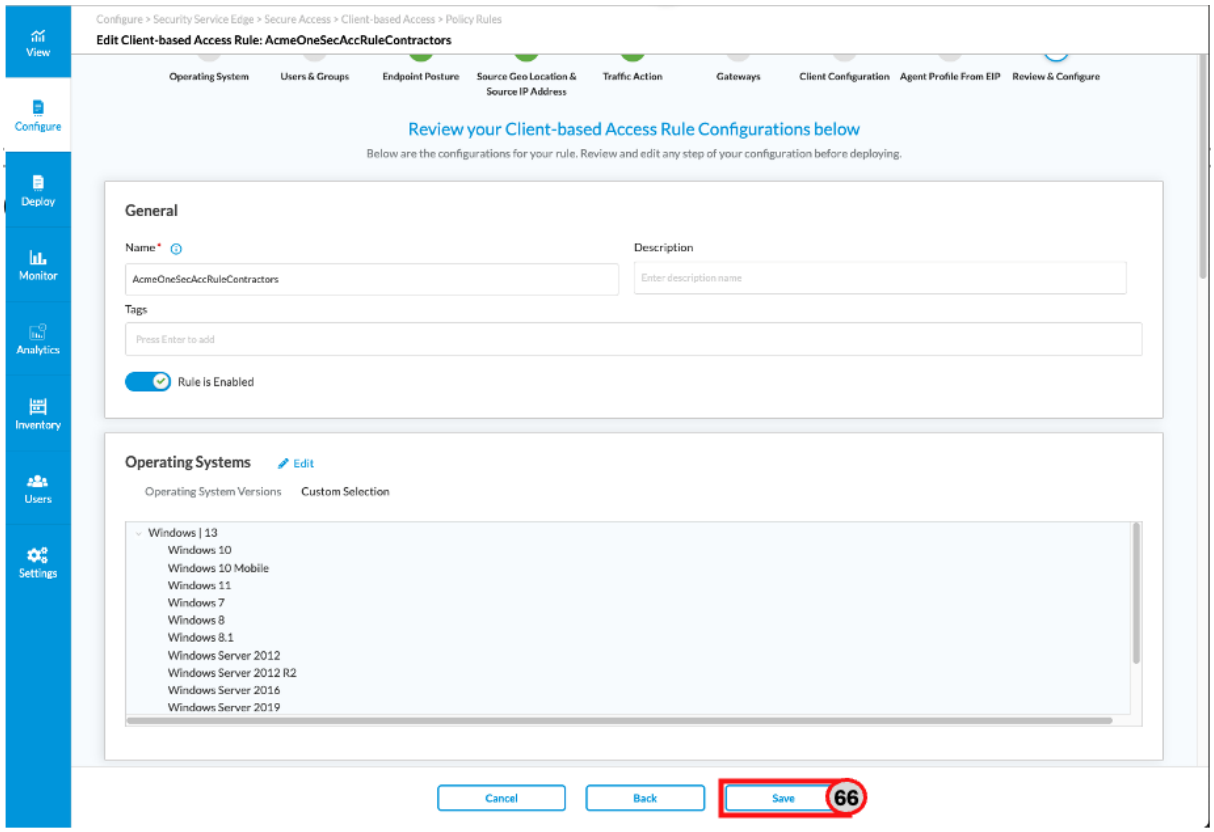
Clear All countries from the site list , then click **Next**.



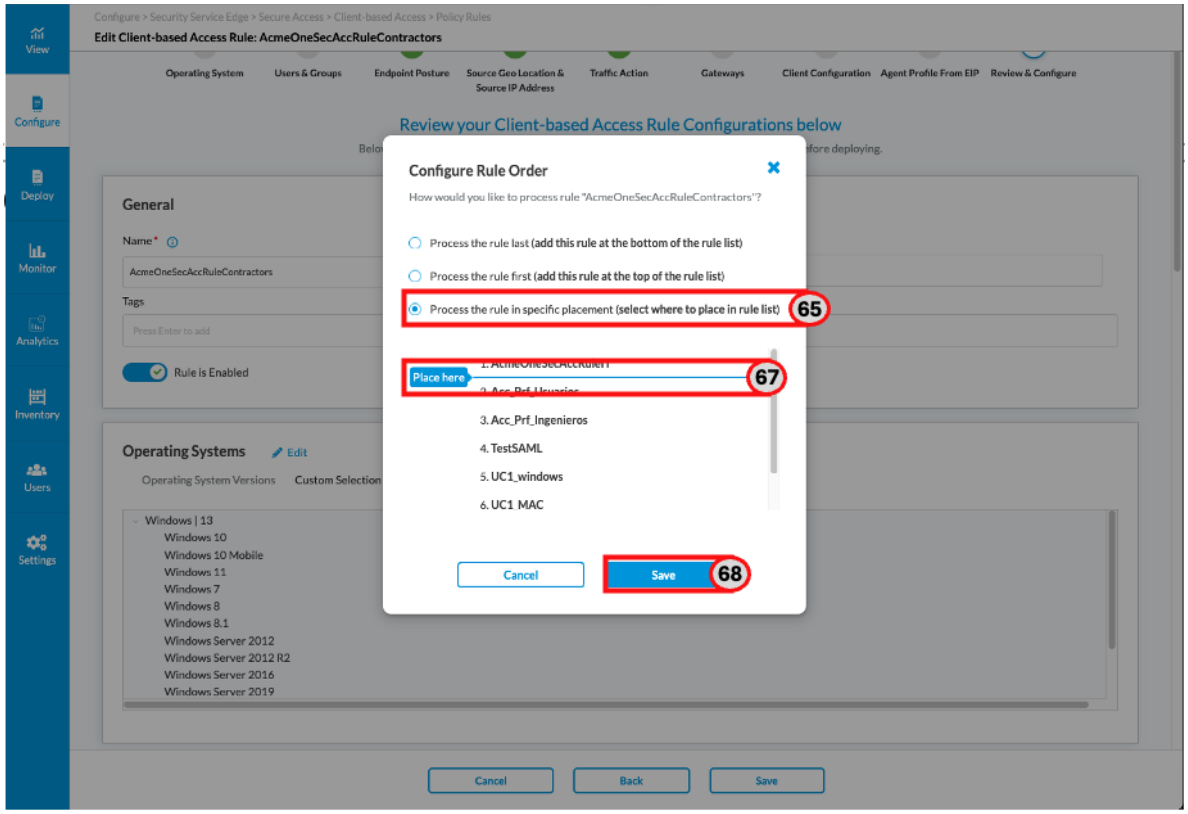
Last, verify the Predefined Application previously defined, *Zoom*, is selected. Then click **Next**.



On the **Review & Submit** page, verify the configuration and then click **Save**.



In the Configure Rule Order screen, select **Process the rule in specific placement**, then drag the rule to place it 2nd, then click **Save**.



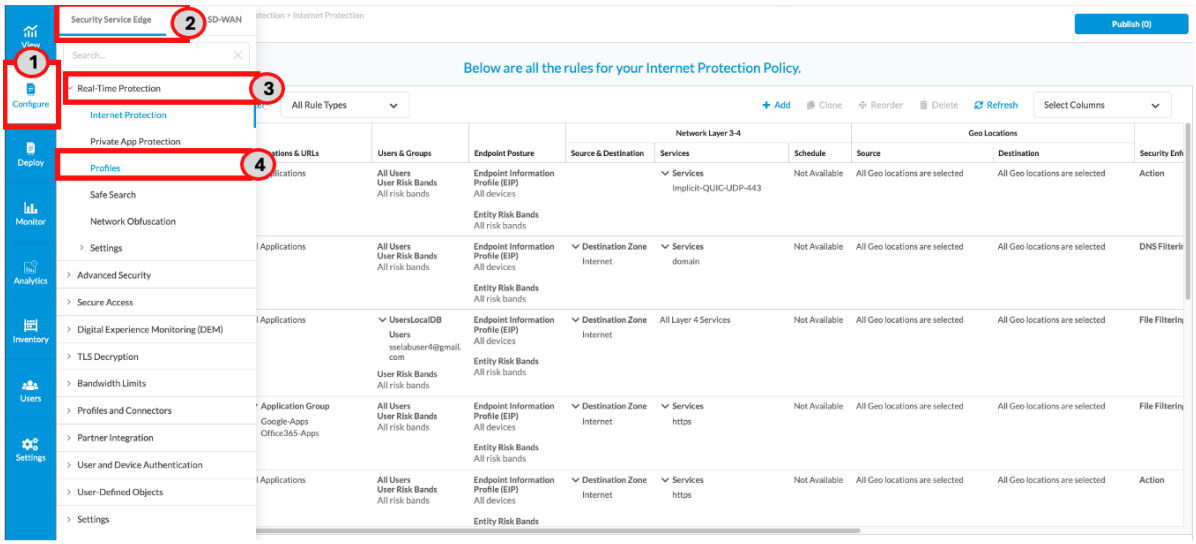
Step 4: Configure DNS Filtering to Block AAAA Queries

In some IPv4-Only or IPv4/IPv6 mixed environments, customers using IPv4 might receive AAAA records pointing to IPv6 addresses, potentially causing issues to the connection. So, in IPv4-only networks, it's a good practice to block IPv6 AAAA DNS queries. This is accomplished by creating a DNS Filtering Profile.

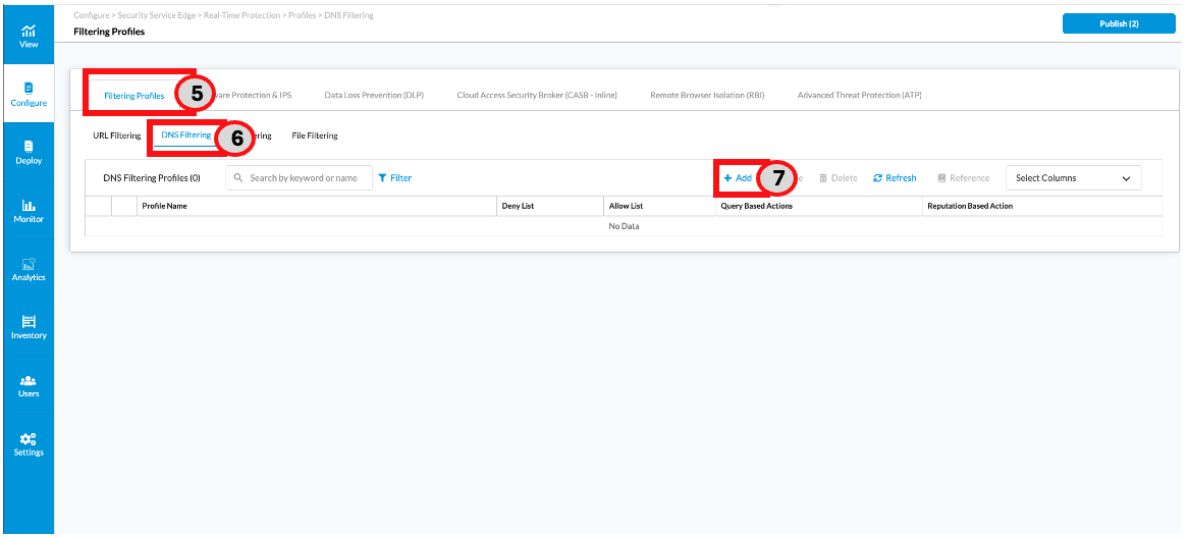
The required information to configure DNS filtering is listed in the following table.

Parameter	Description
Profile Name	Descriptive name for the DNS Filtering Profile
Query Base Action Rule Name	Descriptive name for the Query Base Action Rule
Request Type	Define Query as Request Type
Query Type	Define AAAA as Query Type
Domain Name	Use .* to block all AAAA queries

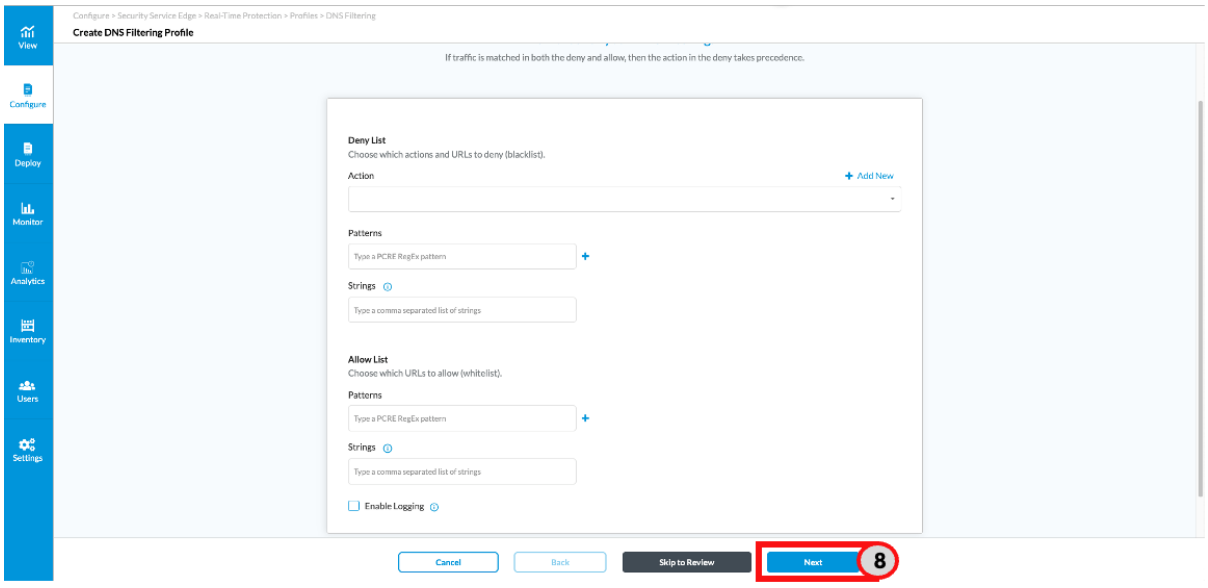
To create the DNS Filtering Profile go to **Configure >> Security Service Edge >> Real Time Protection >> Profiles**.



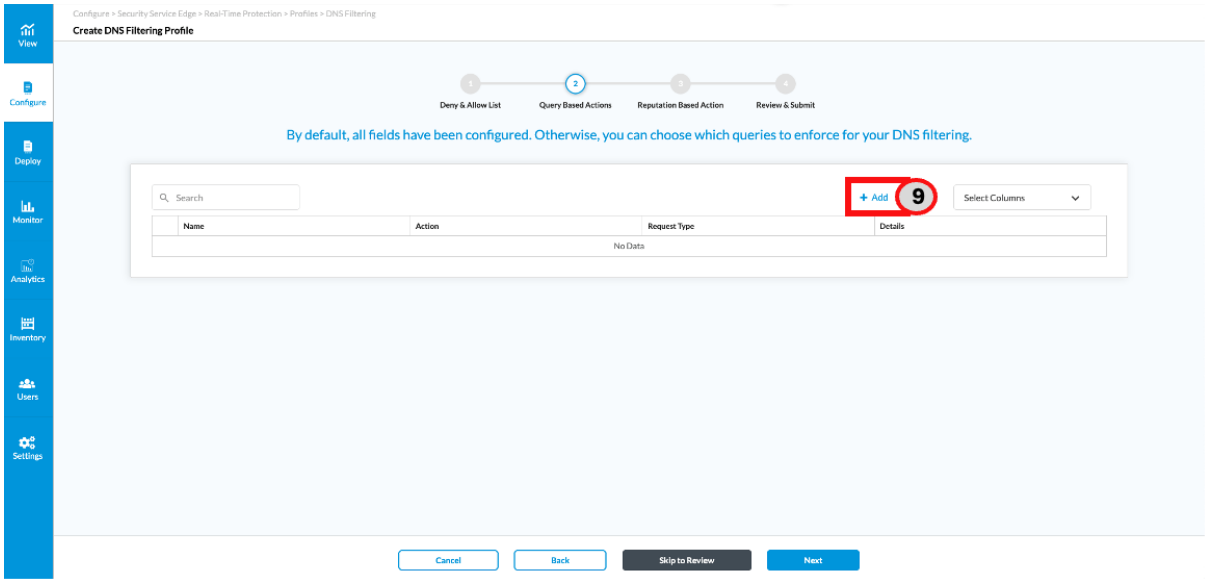
Select **Filtering Profiles**, click in **DNS Filtering** then click **+ Add**.



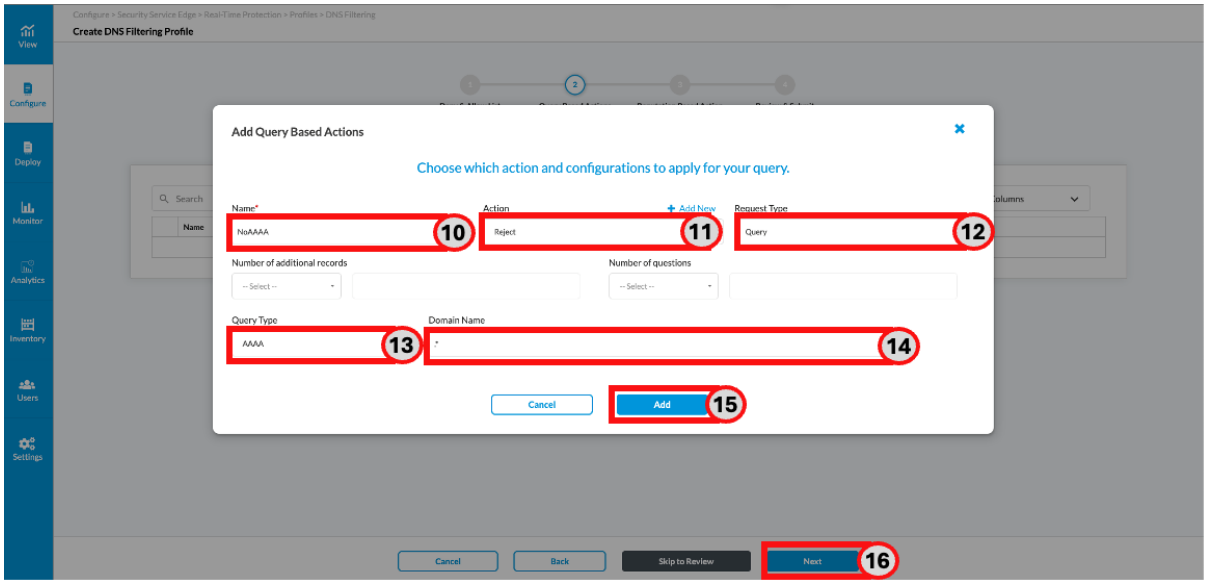
No White or Black list will be created for this example so click **Next**.



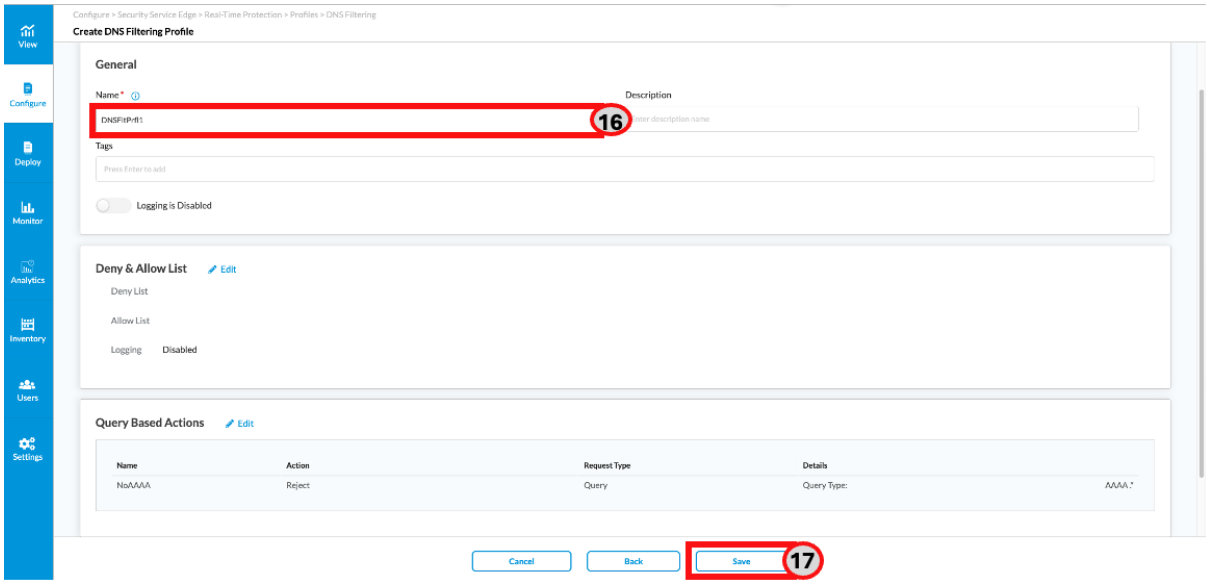
Click **+ Add** to create a new Query Based Action Rule.



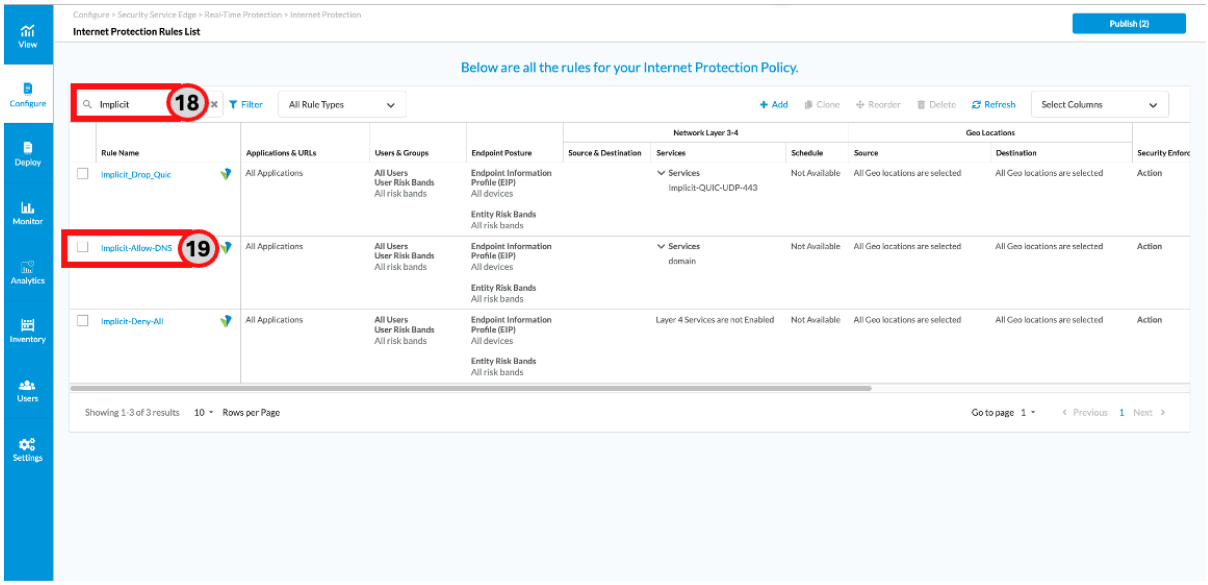
Assign a descriptive **Name** for the rule, select the Reject **Action**, and Query for the **Request Type**. Select "AAAA" as the **Query Type** and ".*..*" in the **Domain Name Field**. Click **Add** to save the action rule and then click **Next**.



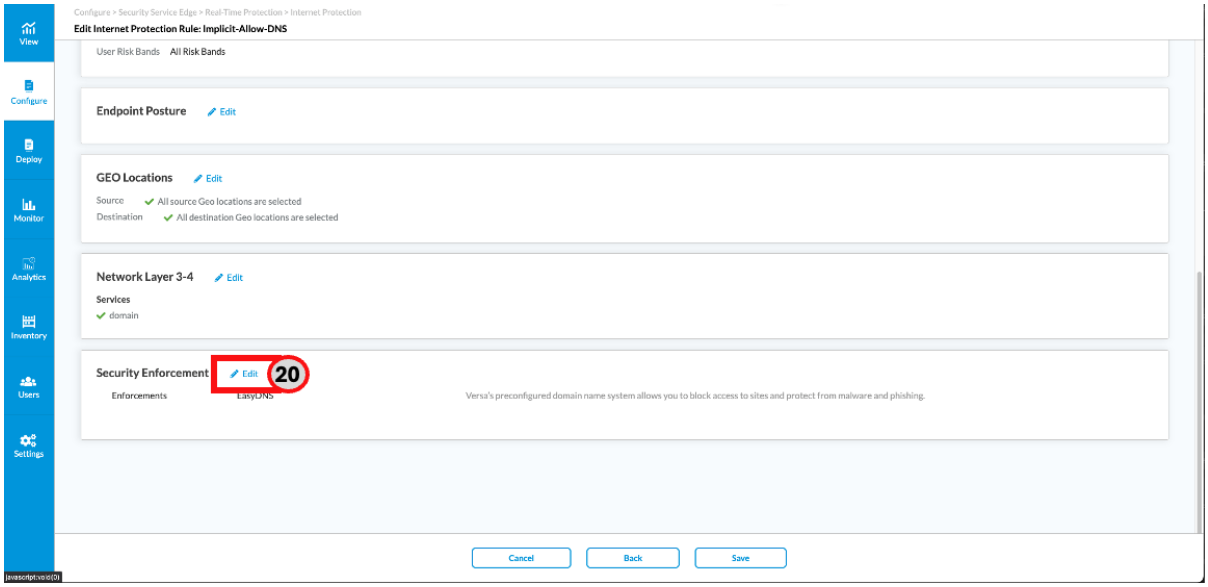
Assign a descriptive **Name** for the DNS Filtering Profile and click **Save**.



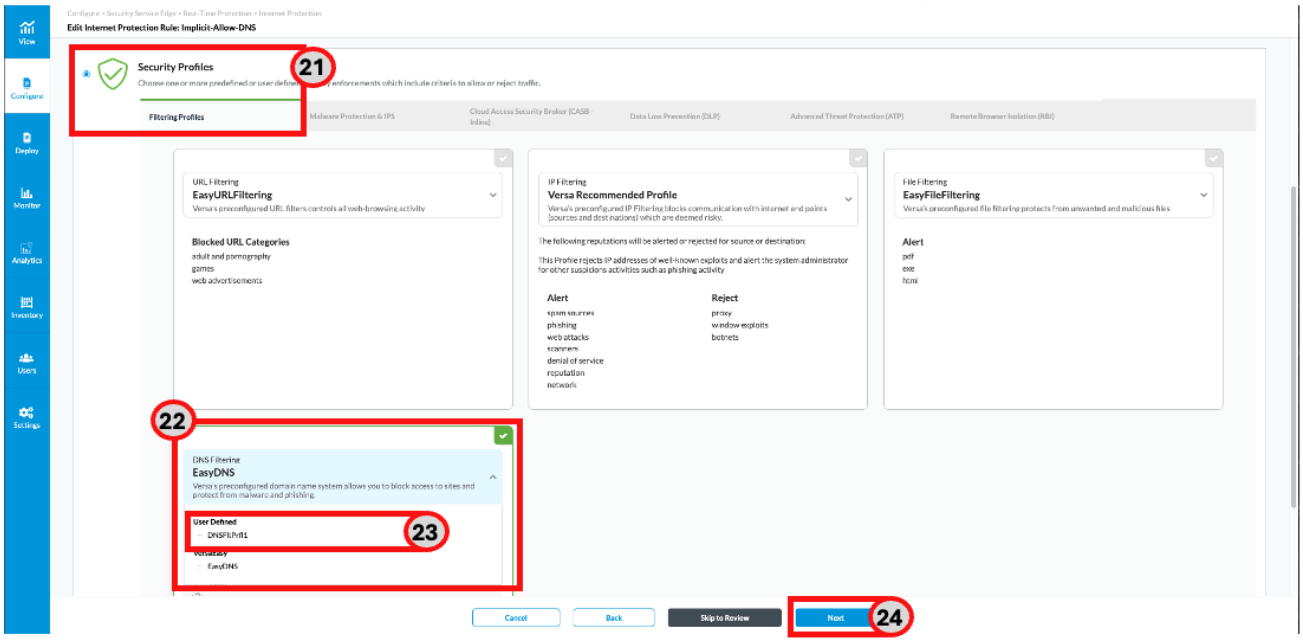
In the Internet Protection Rules List table, use the search tool to find rules matching the term “implicit”. The rules with the implicit string used in the name will be listed. Edit the Implicit-Allow-DNS rule by clicking the rule name.



Scroll down to the Security Enforcement section. Click **Edit**.



Change the enforcement action from Allow to **Security Profiles**.Select the **Filtering Profiles** tab, and in the **DNS filtering** sectio select the DNSFltPrf1 rule created earlier. Click **Save**.



Step 5: Configure Saas Tenant Control

In this scenario, SaaS Tenant Control will be configured to ensure that users access Office 365 only with corporate domain accounts. This prevents logins with personal or third-party accounts, which could lead to data leakage or use of unmanaged, non-compliant environments. Enforcing tenant restrictions aligns with corporate security and compliance policies, while still allowing seamless access to business-critical Office 365 services.

The required information to complete the configuration is listed in the following table.

Parameter	Description
Application Rule Name	Name assigned to the SaaS tenant control rule.
Application	Application to control: - -Office 365 block Consumer Account -Microsoft Office365 Tenant-Restrictions
Profile Name	Name for the SaaS Control Profile where the rule is applied.

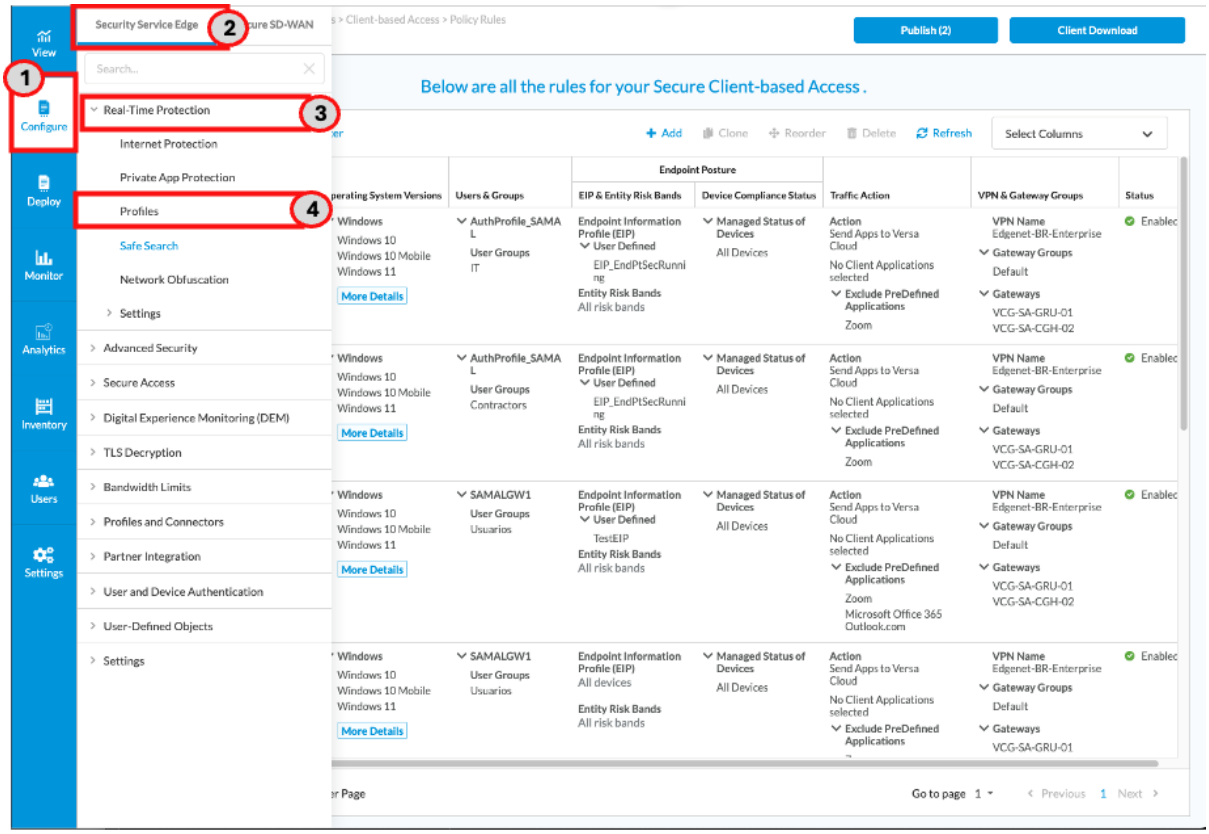
Why Two Controls Are Required

- **Office 365 Block Consumer Account:** This control prevents users from signing in with personal Microsoft accounts (e.g., *@outlook.com*, *@hotmail.com*, *@live.com*). Without this restriction, users could bypass corporate monitoring and store or share sensitive data in unmanaged personal accounts.
- **Microsoft-Office365-Tenant-Restrictions:** This control enforces access to a **specific corporate tenant** (e.g., *acme-one.com*). Even if a user tries to log in with another company's Office 365 tenant or a third-party organizational account, the connection will be blocked. This ensures all traffic is tied to the customer's authorized tenant only.

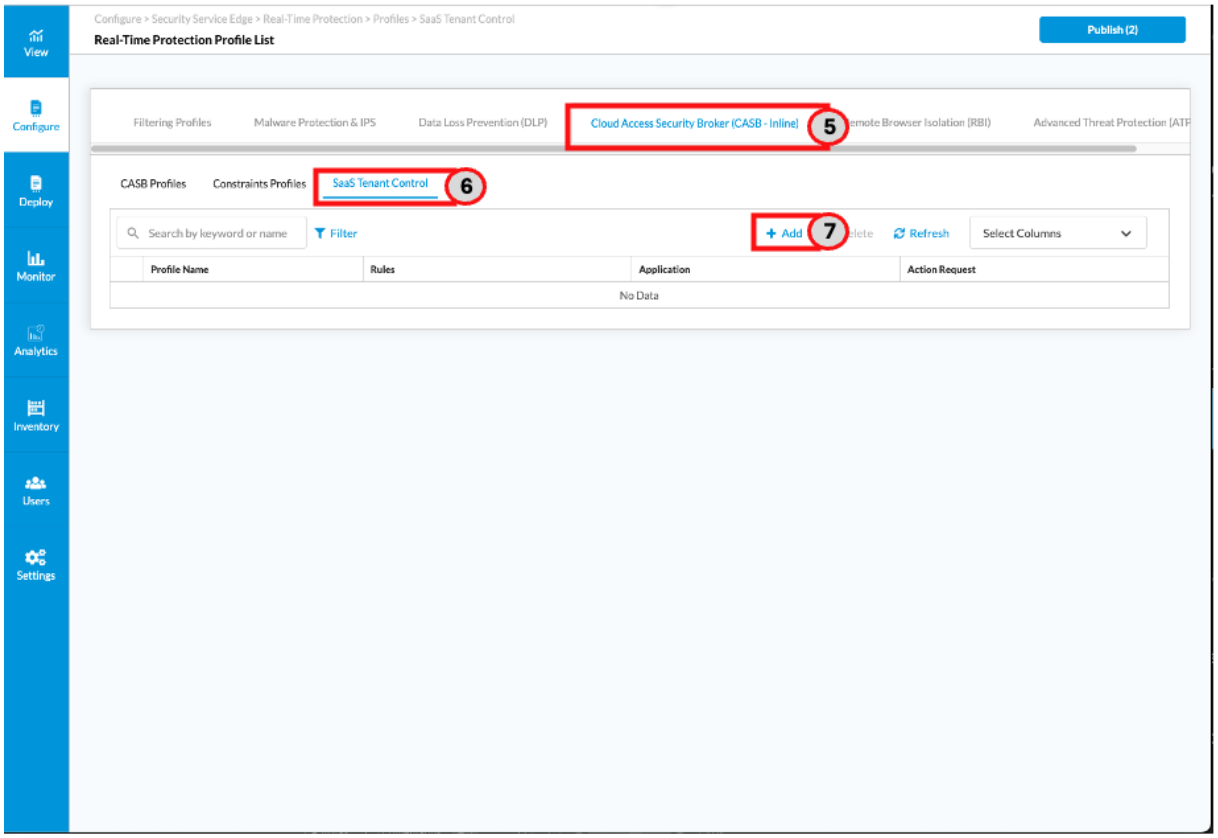
Together, these rules ensure that:

1. Users cannot use **personal accounts** for Office 365.
2. Users cannot use other organizations' tenants.
3. Only the **corporate Office 365 tenant** is accessible, closing both major loopholes for data leakage.

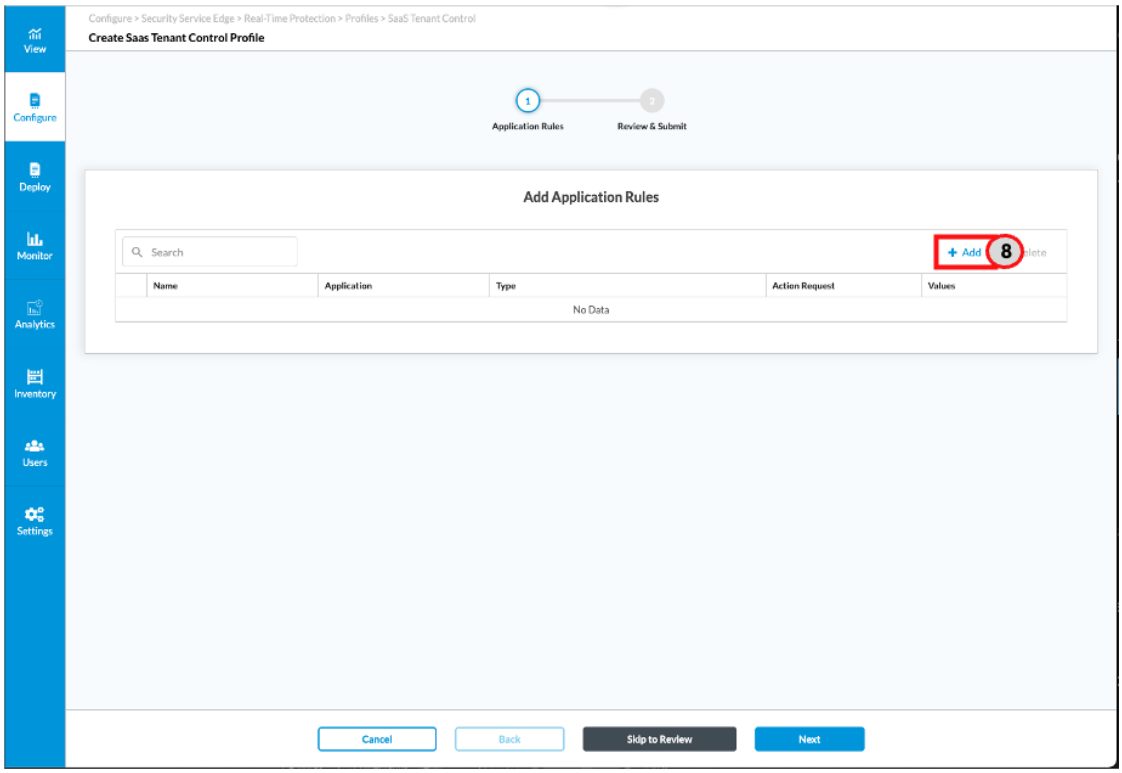
To configure SaaS Tenant Control, go to **Configure > Security Service Edge > Real Time Protection > Profiles**.



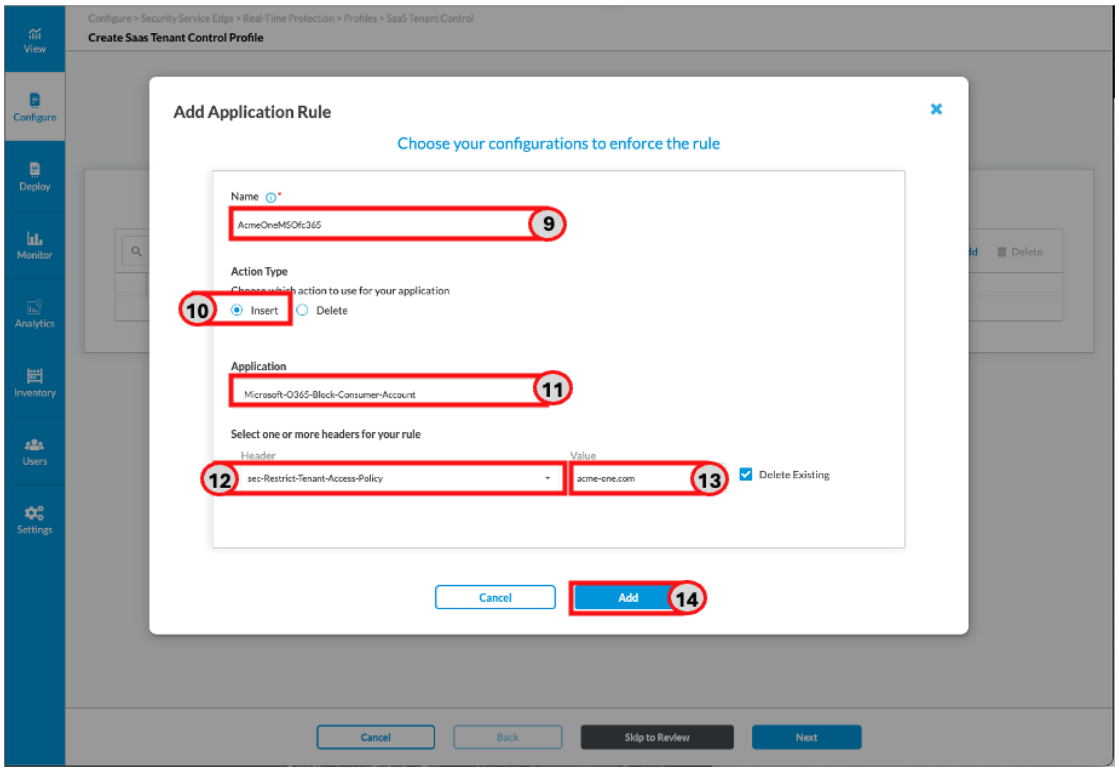
Next, go to **Cloud Access Security Broker CASB > SaaS Tenant Control > Add**.


Configure > Security Service Edge > Real-Time Protection > Profiles > SaaS Tenant Control
Real-Time Protection Profile List
Publish (2)
View
Configure
Deploy
Monitor
Analytics
Inventory
Users
Settings
Filtering Profiles
Malware Protection & IPS
Data Loss Prevention (DLP)
Cloud Access Security Broker (CASB - Inline)
5
Remote Browser Isolation (RBI)
Advanced Threat Protection (ATP
CASB Profiles
Constraints Profiles
SaaS Tenant Control
6
Search by keyword or name
Filter
+ Add
7
Delete
Refresh
Select Columns
Profile Name
Rules
Application
Action Request
No Data

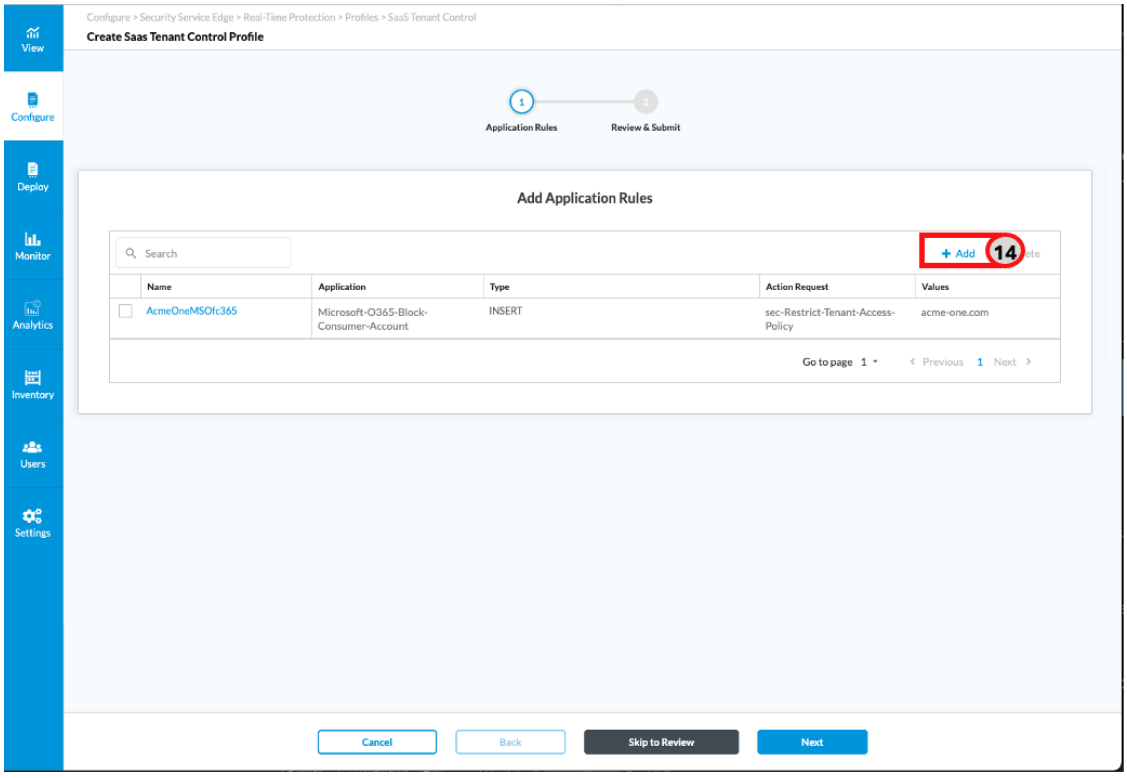
Click **+ Add**.


Configure > Security Service Edge > Real-Time Protection > Profiles > SaaS Tenant Control
Create Saas Tenant Control Profile
View
Configure
Deploy
Monitor
Analytics
Inventory
Users
Settings
1
Application Rules
2
Review & Submit
Add Application Rules
Search
+ Add
8
Delete
Name
Application
Type
Action Request
Values
No Data
Cancel
Back
Skip to Review
Next

Assign a descriptive **Name**, and select the **Insert** radio button for Action Type. In the Application dropdown select **Microsoft Office 365 Block Consumer Account** to filter consumer/public domains. In the Header dropdown select **Sec-Restrict-Tenant-Access-policy** and specify the Value **acme-one.com**. Click **Add**.

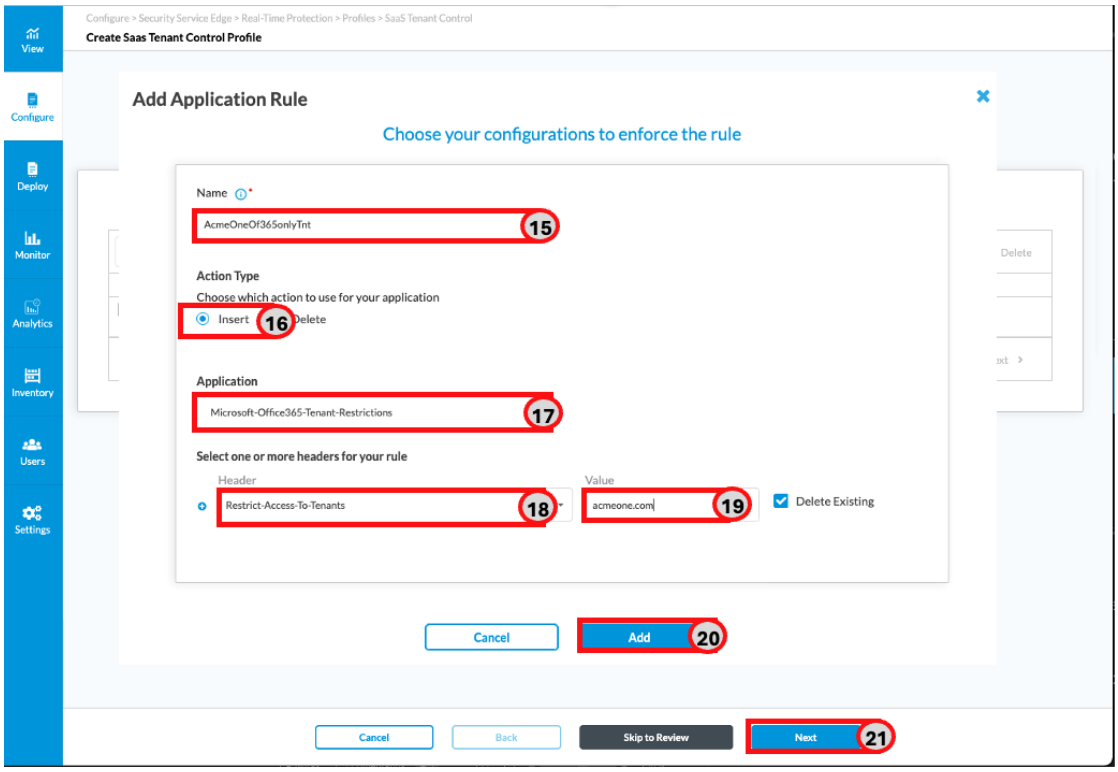


Select **Add** again to create a restriction for Corporate domains that are not acme-one.com.

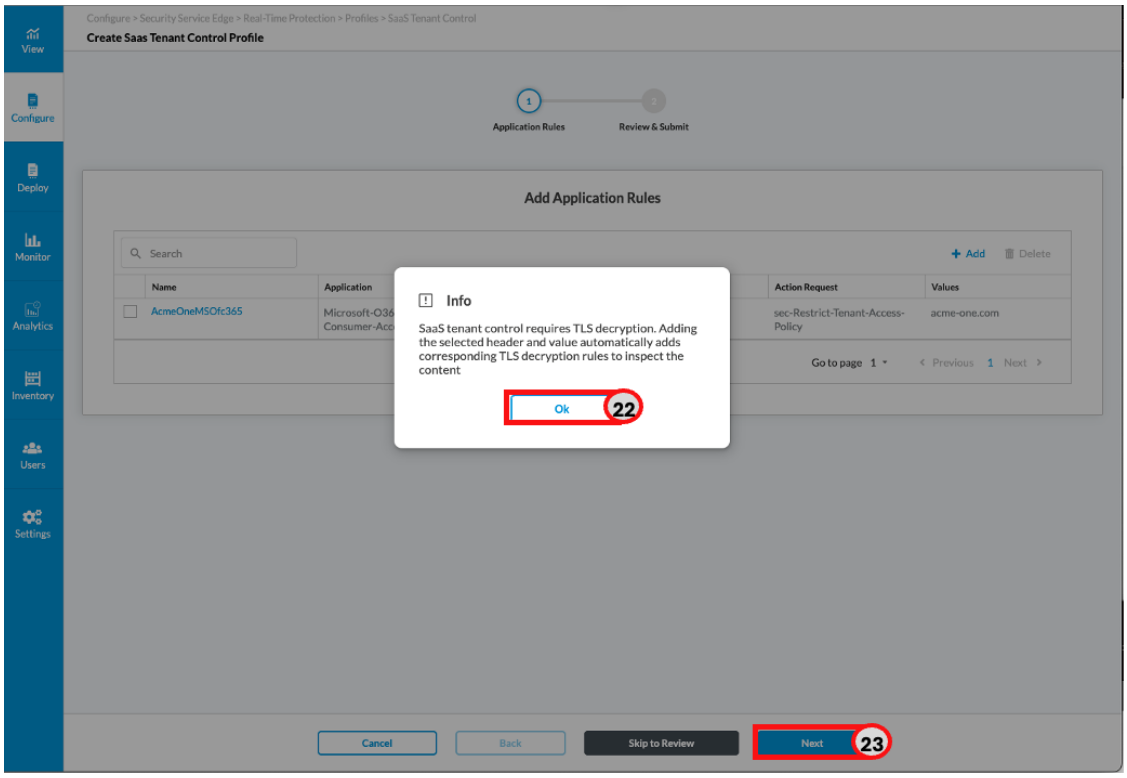


Assign a descriptive **Name**, and select the **Insert** radio button for Action Type. In the Application dropdown select **Microsoft Office 365 Block tenant restriction** to filter corporate domains. In the Header dropdown use **Restrict-**

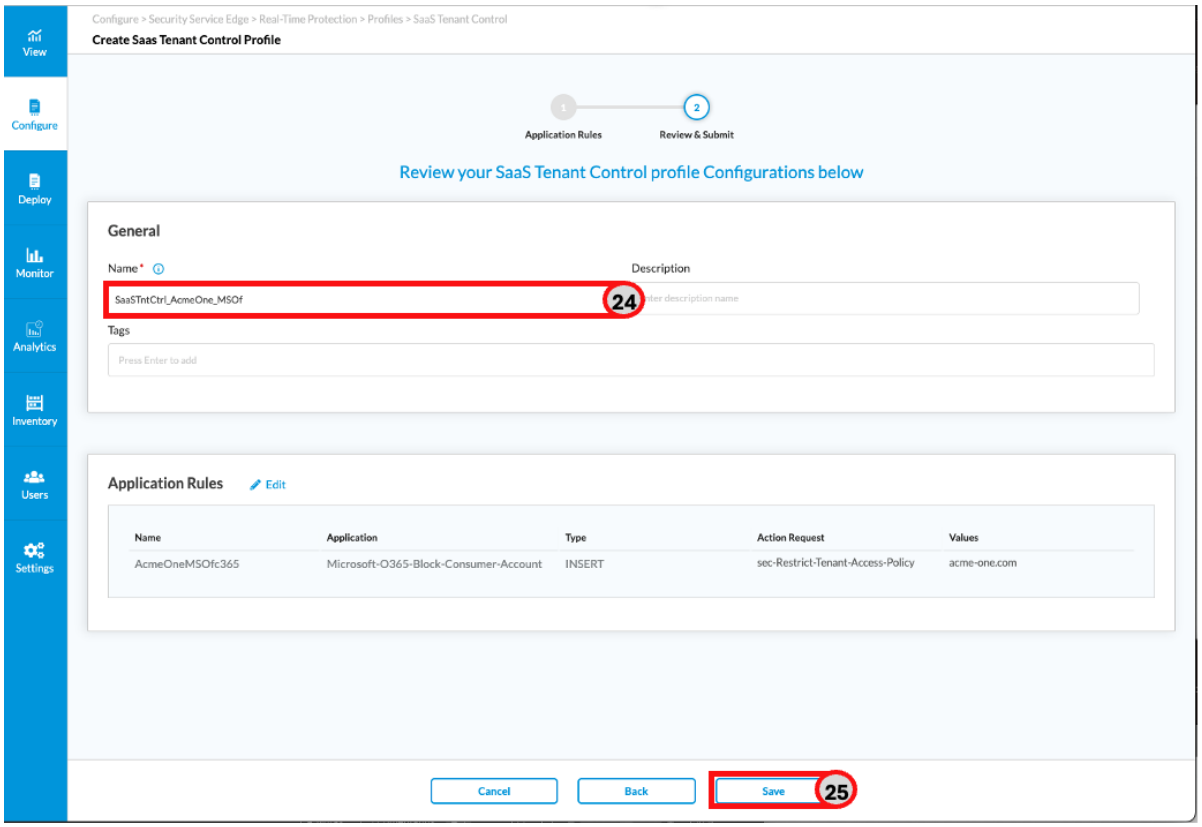
Access-To-Tenant and specify the Value **acme-one.com**. Click **Add** and then click **Next**.



Click **Ok** to dismiss the information window regarding the TLS decryption requirement, then Click **Next**.



To complete the configuration, assign a descriptive **Name** and click **Save**.



Step 6: Configure TLS Decryption

Most web traffic today is secured with SSL/TLS encryption, which protects data between the user device and the web server. However, this also prevents security controls from inspecting the content of those data flows.

By configuring TLS Decryption, the Versa SSE Gateway can intercept and decrypt HTTPS traffic, enabling the use of advanced security features such as Cloud Access Security Broker (CASB), Anti-Malware, and Data Loss Prevention (DLP).

To maintain user privacy and comply with regulations:

- Financial services and healthcare-related websites should be explicitly excluded from decryption.
- All other traffic will be decrypted, allowing sensitive flows to be inspected and protected by Versa's security stack.

The required information to complete the configuration is in the next list.

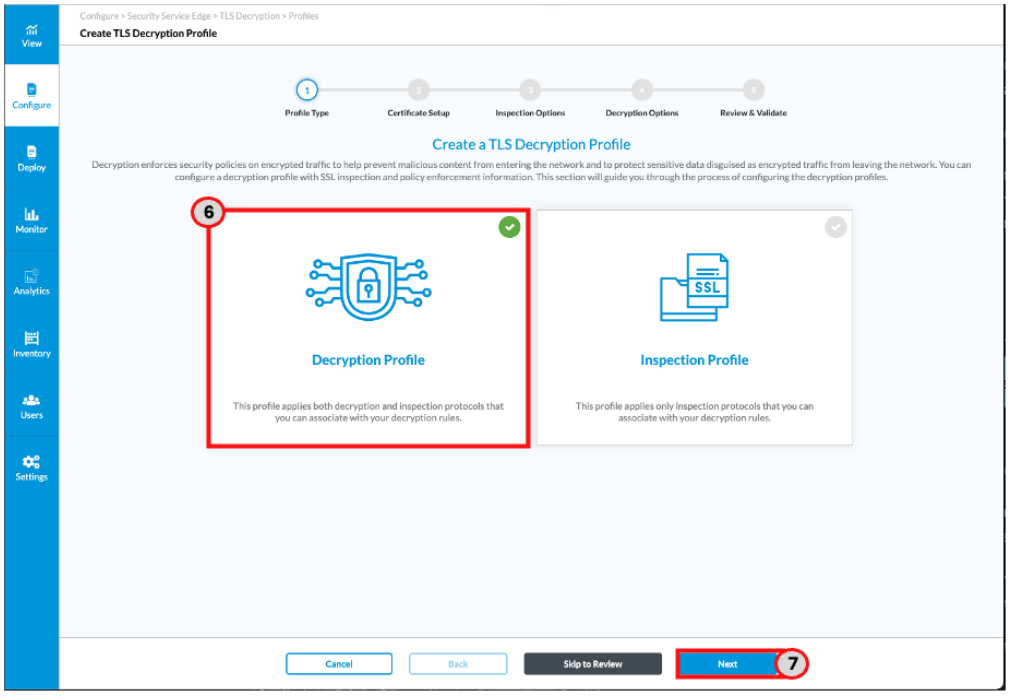
Parameter	**Description**
Profiles Name	Name for Decryption Profiles
Certificate	Certificate to be used for TLS Decryption
Key Exchange Algorithms	Key Exchange Algorithms allowed to be used for TLS
Encryption Algorithms	Encryption Algorithms allowed to be used for TLS
Authentication Algorithms	Authentication Algorithms allowed to be used for TLS
TLS Cipher Suites	TLS Cipher Suites allowed to be used for r TLS

Versa include some predefined profiles you can use, but if a specific/custom profile is required, please follow the steps listed below to create a new one.

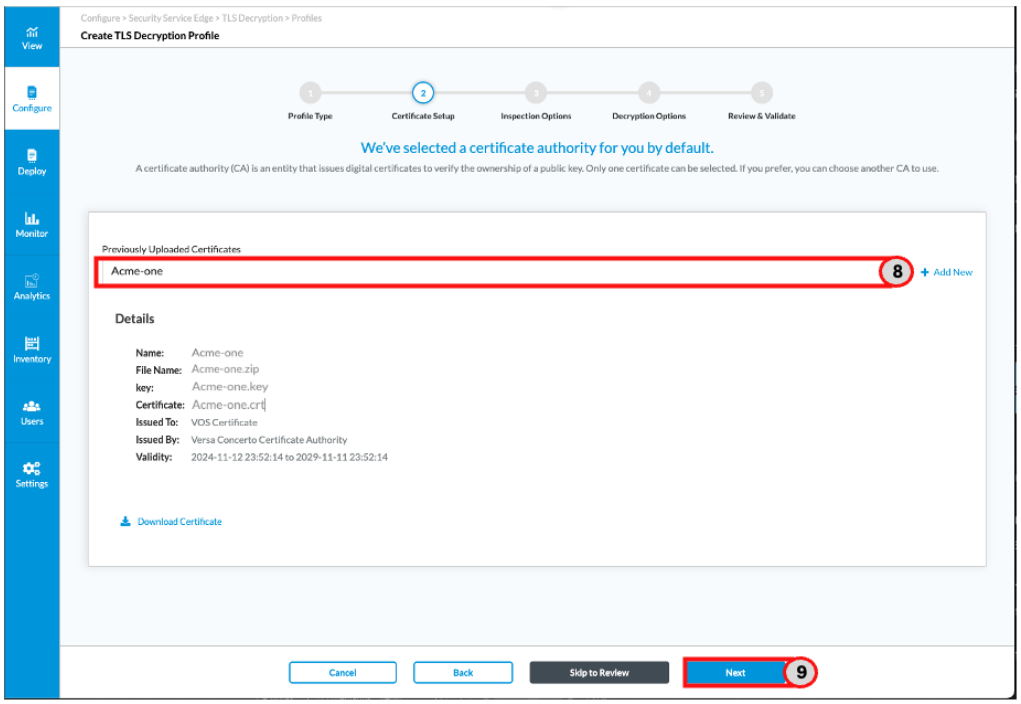
Create a TLS Decryption Profile

To configure TLS decryption, create a TLS decryption profile. Go to **Configure > Security Service Edge > TLS Decryption > Profiles**.

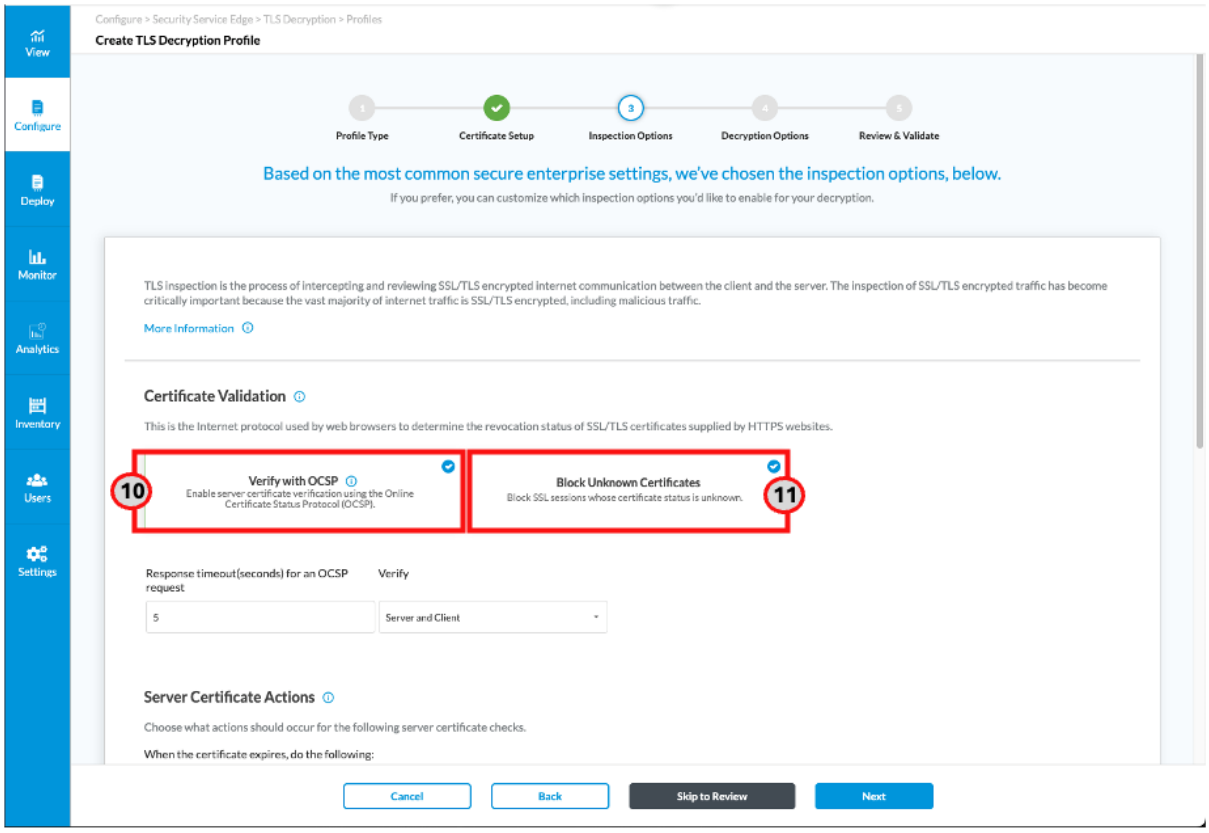
Select **Decryption Profile** and click **Next**.



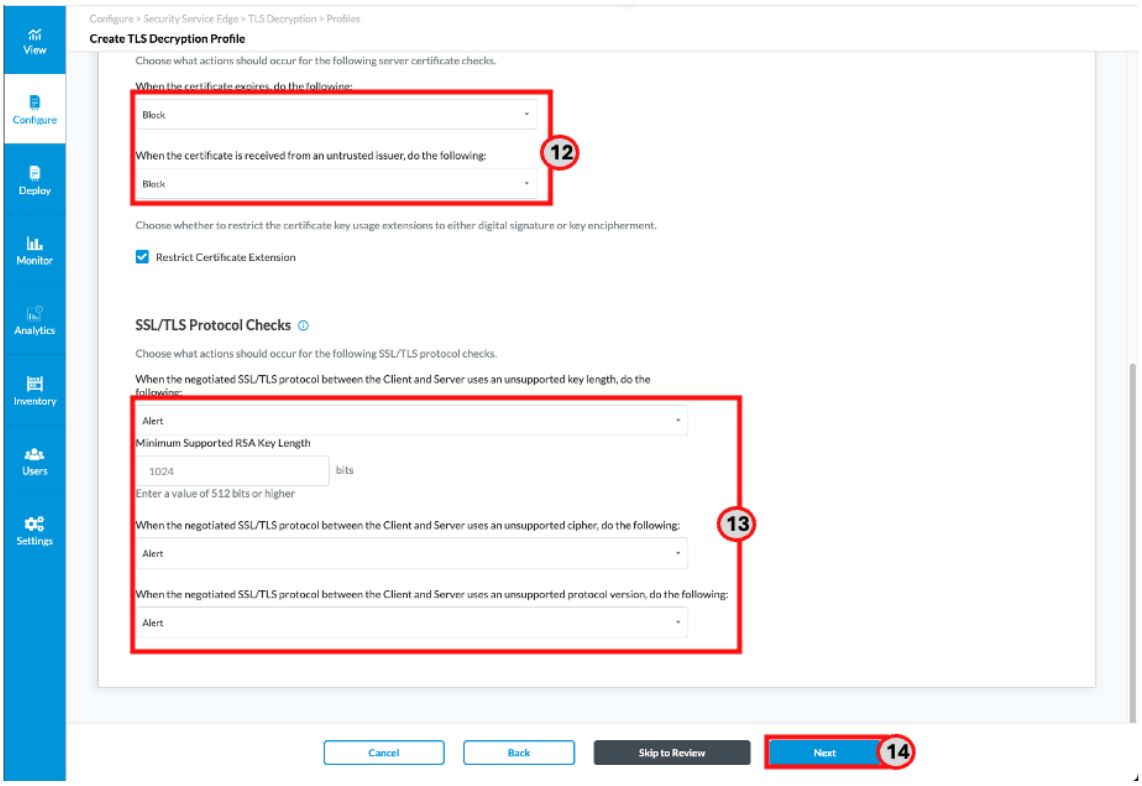
Choose the **Certificate**, then click **Next**.



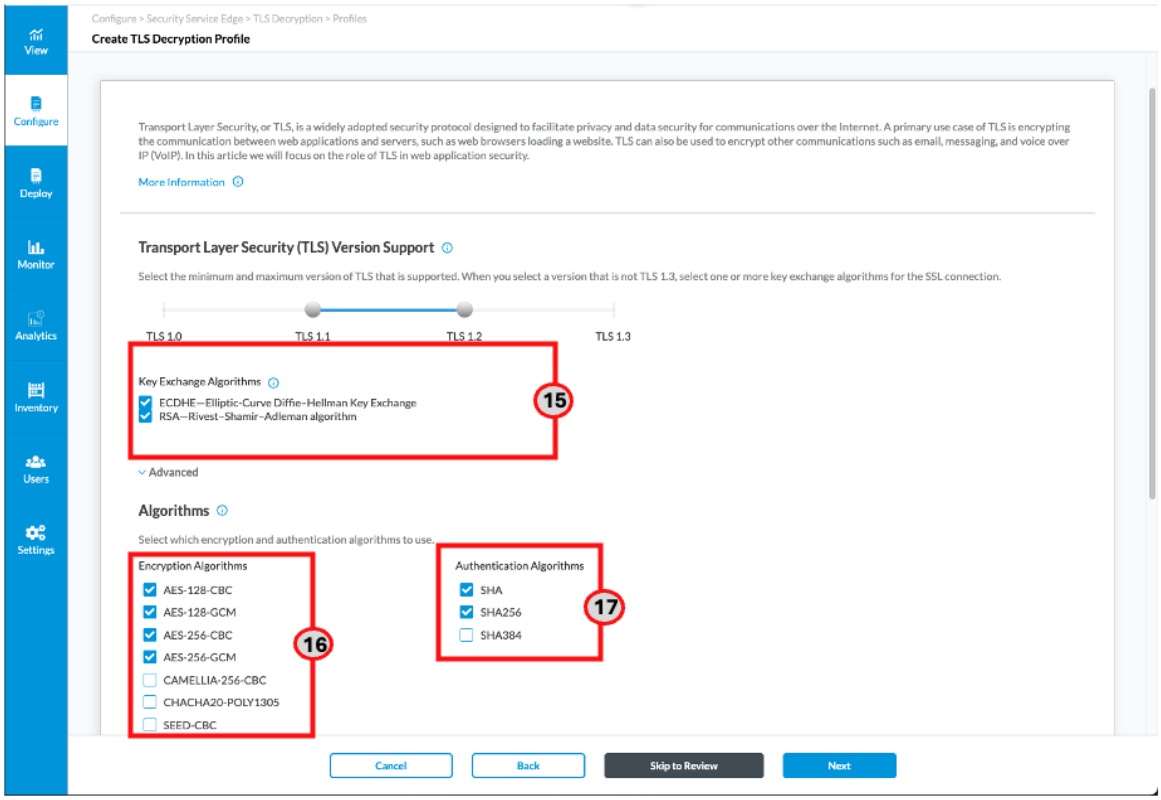
Select **Verify with OSCP** and **Block Unknown Certificates**, then scroll down.



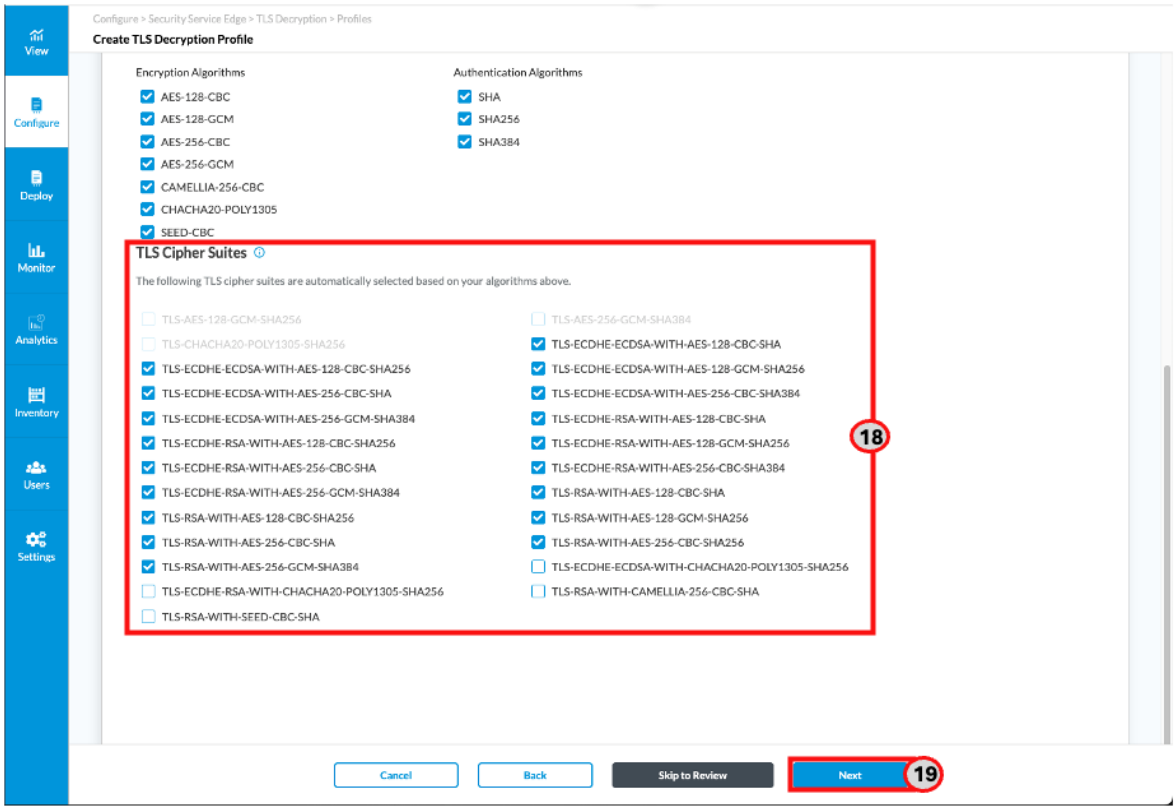
Select the **Block** dropdown for Expired and Untrusted Certificates and select the **Alert** dropdown for Unsupported Key Lengths, Unsupported Ciphers and Unsupported Protocol Versions. Click **Next**.



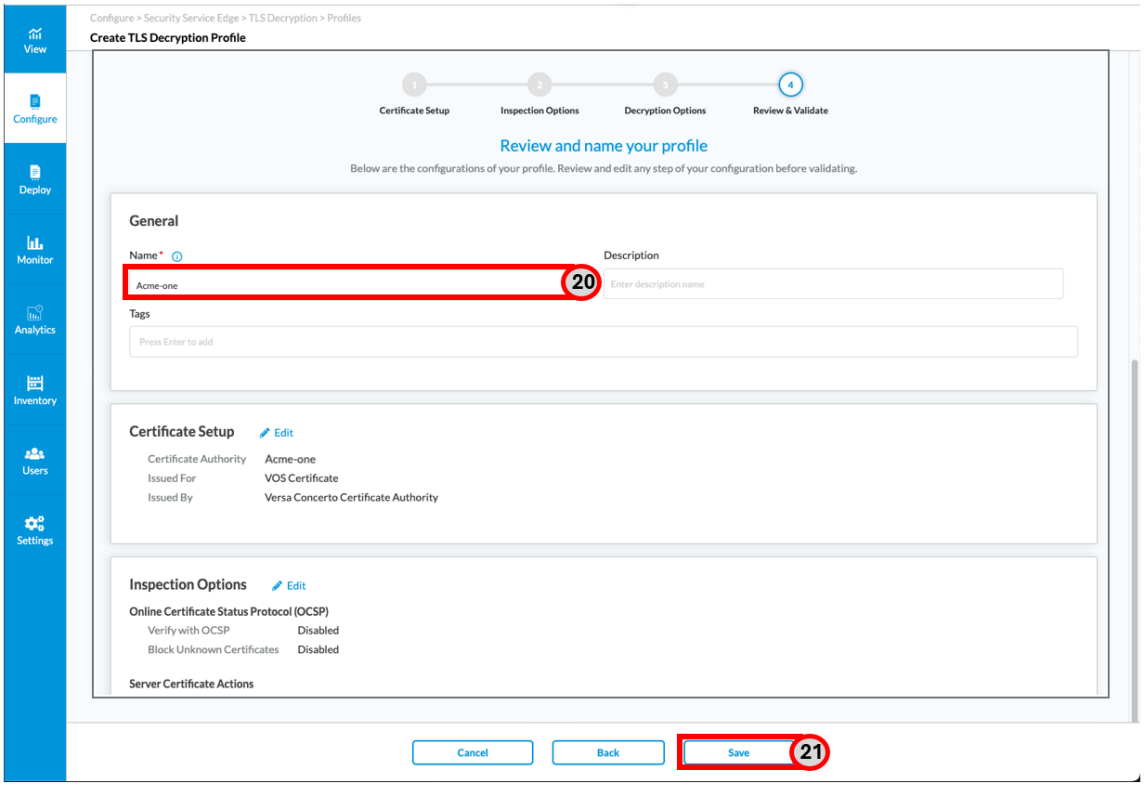
Select both **Key Exchange Algorithms**, select the necessary **Encryption Agorithms** and **Authentication Algorithms**, then scroll down.



Select the desired **TLS Cipher Suites**, then click **Next**.



Assign a descriptive **Name** then click **Save**.

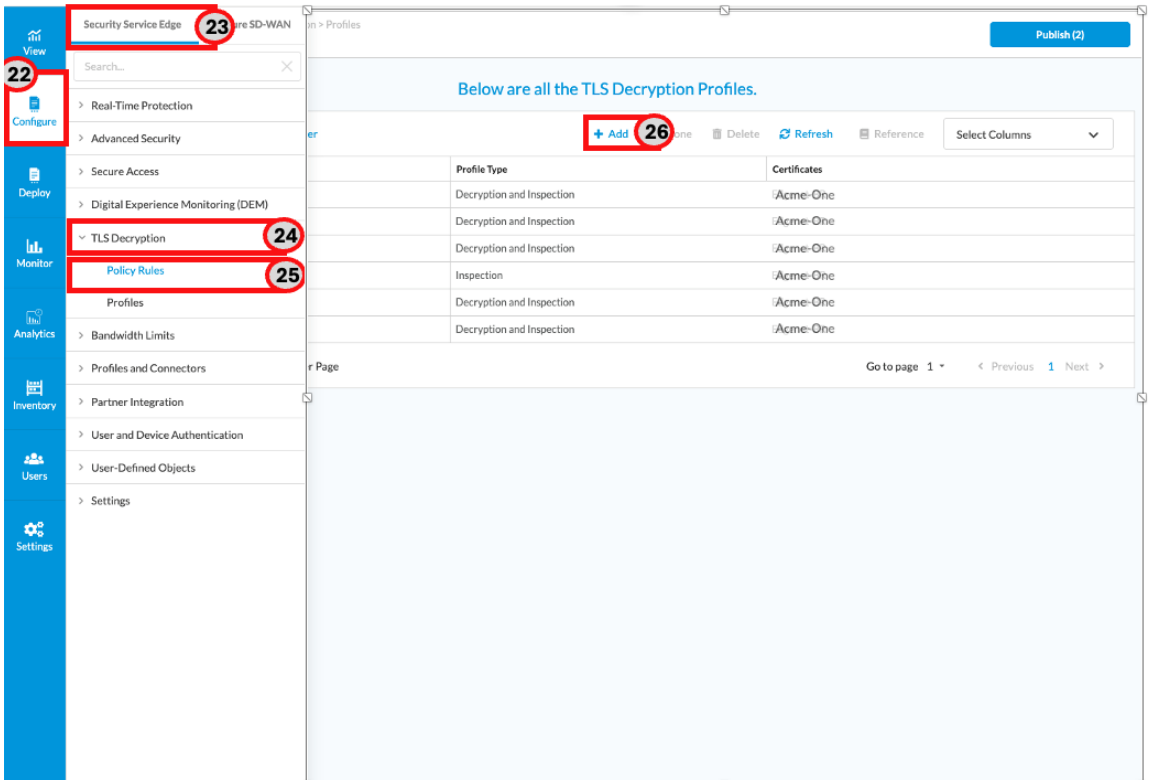


Create TLS Decryption Policy Rules

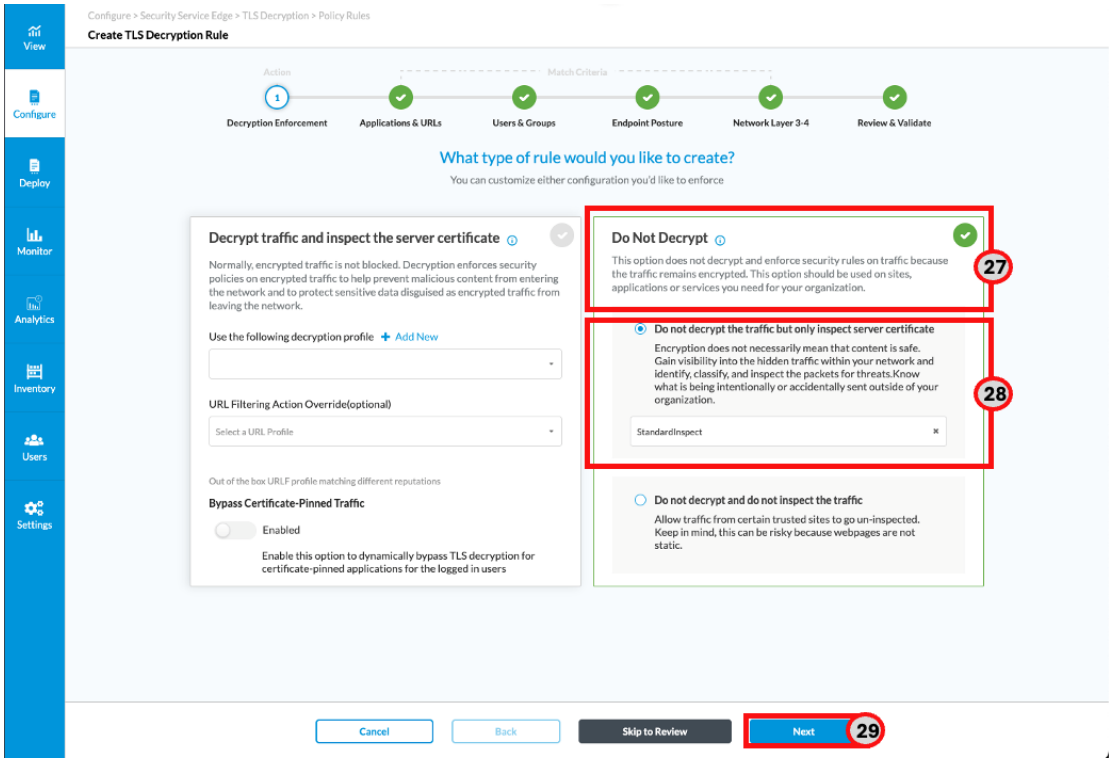
As specified in the use case, two decryption policy rules are needed. The first rule maintains privacy for certain types of regulated traffic, while the second decrypts all remaining traffic.

TLS Decryption Policy Rule 1

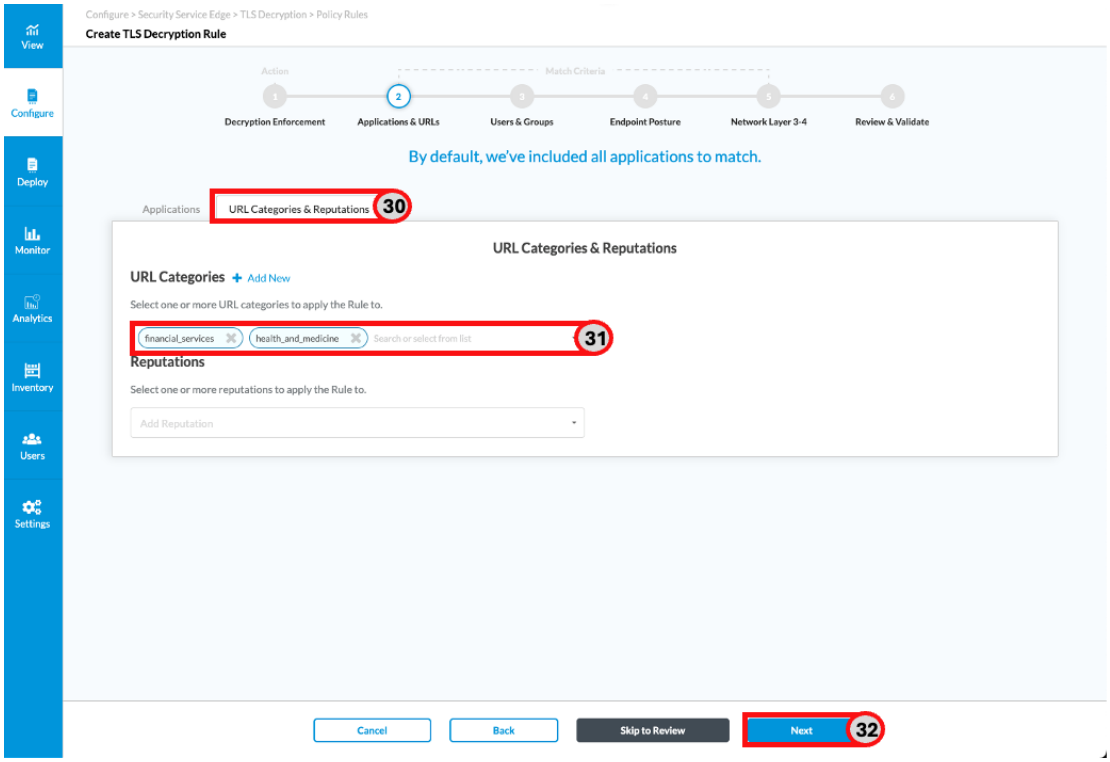
To create the rule to avoid Health and Financial URLs from being decrypted, go to **Configure > Security Service Edge > TLS Decryption > Policy Rules**, then click **Add** to create a new TLS Decryption Policy Rule.



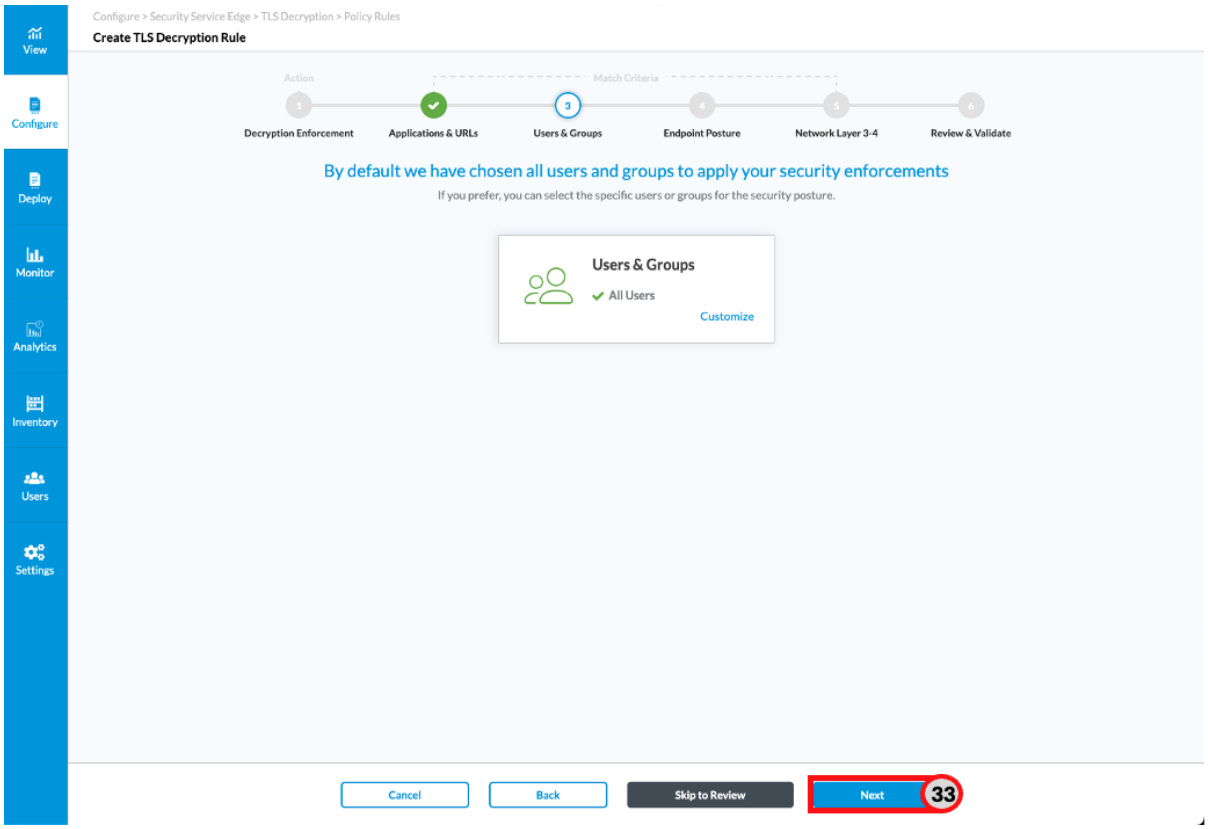
Select **Do Not Decrypt** box and the radio button to only inspect certificates with the **Standard Inspect** profile, then click **Next**.



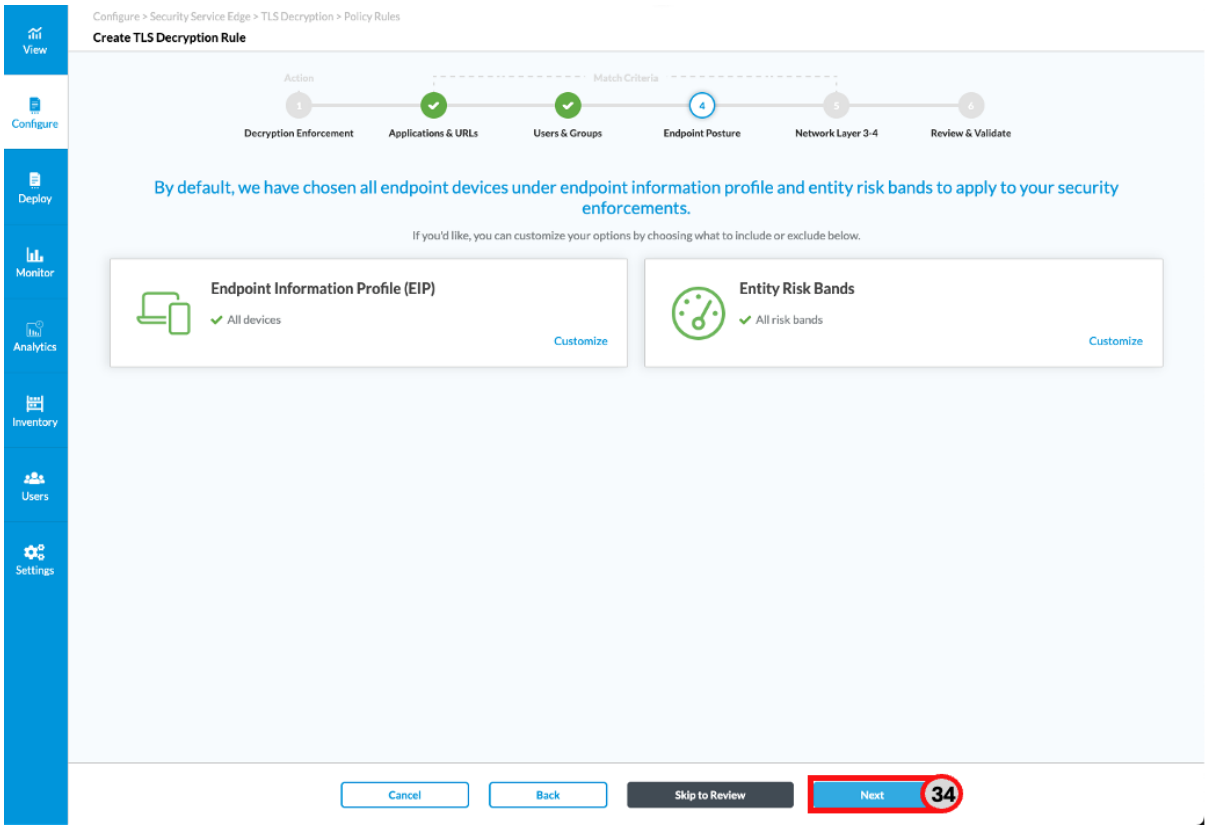
From **URLs Categories and Reputations** tab , search for **financial_services** and **health_and_medicine** categories. Press enter to add each category, then click **Next**.



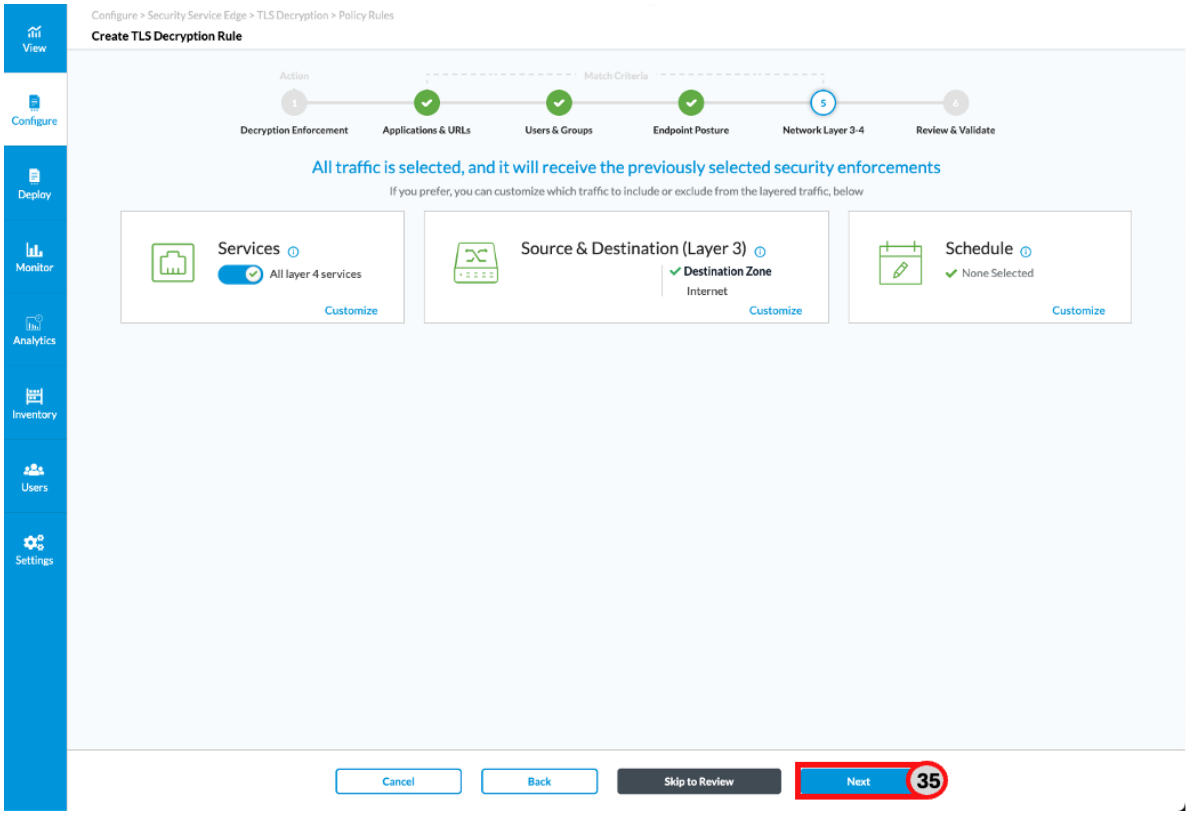
Click **Next** in Users & Groups configuration.



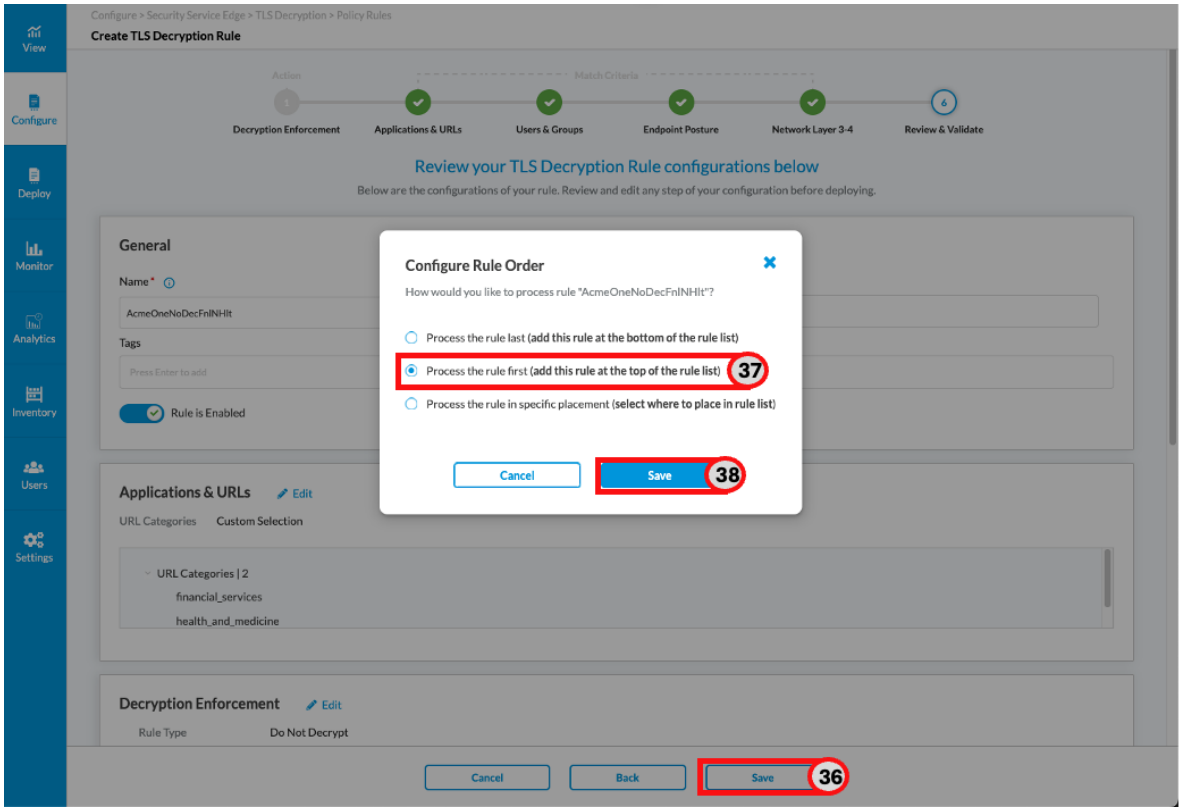
Click **Next** in Endpoint Posture configuration.



Click **Next** in Network Layer 3-4 configuration.

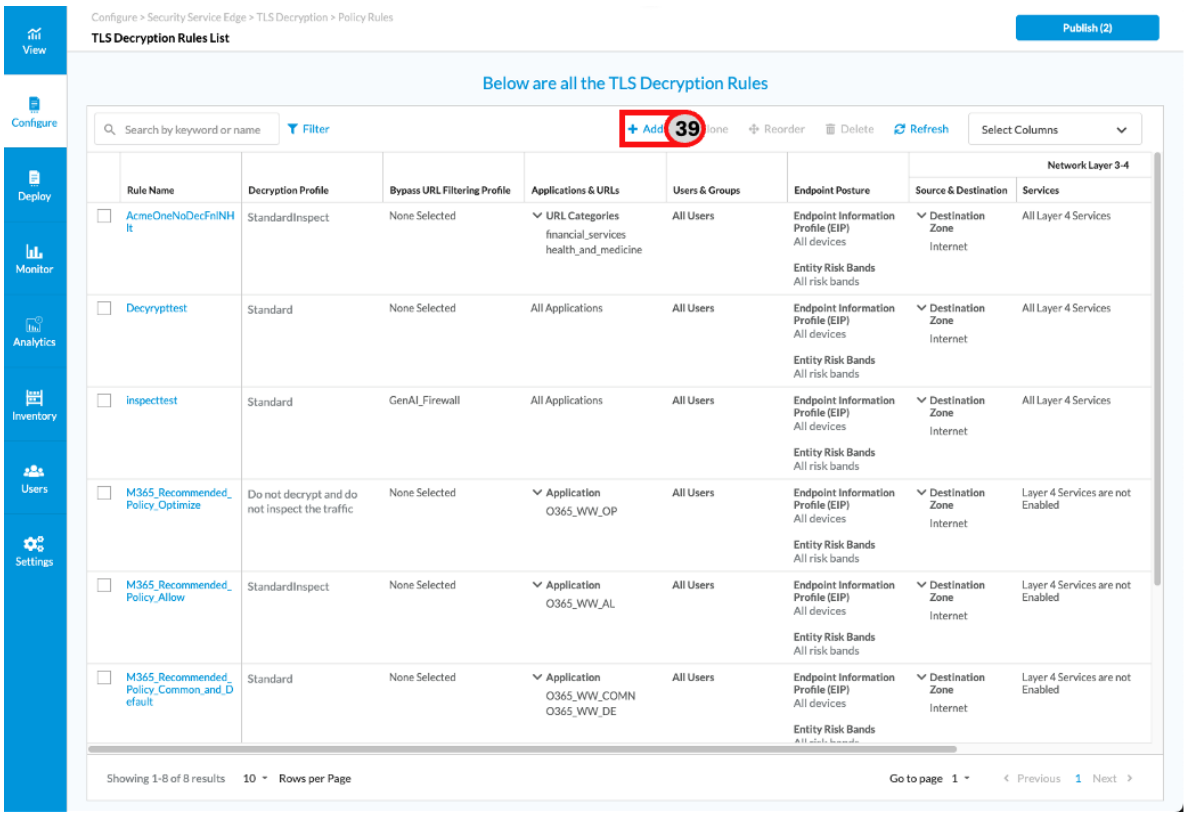


Click **Save** to finish. In the Configure Rule Order window select **Process the rule first** and then click **Save**..



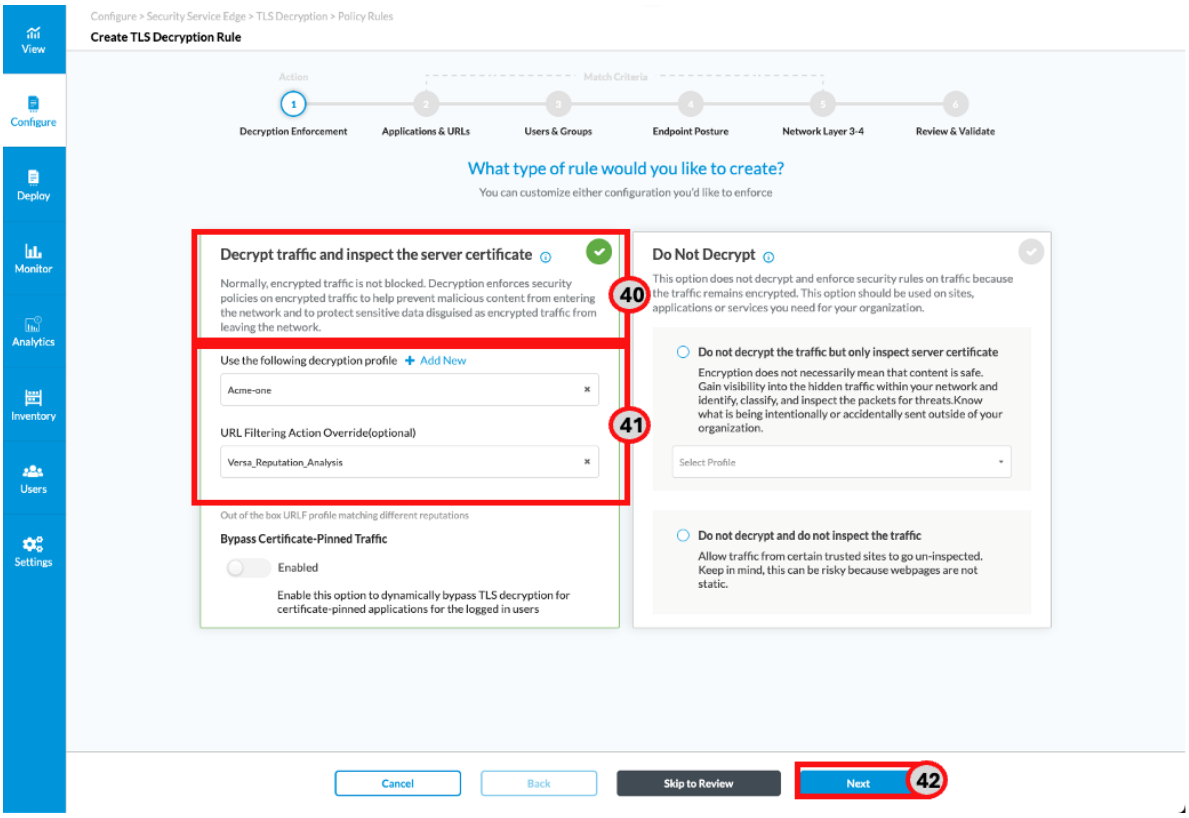
TLS Decryption Policy Rule 2

To create the second rule allowing decryption of all other traffic, click **Add**.

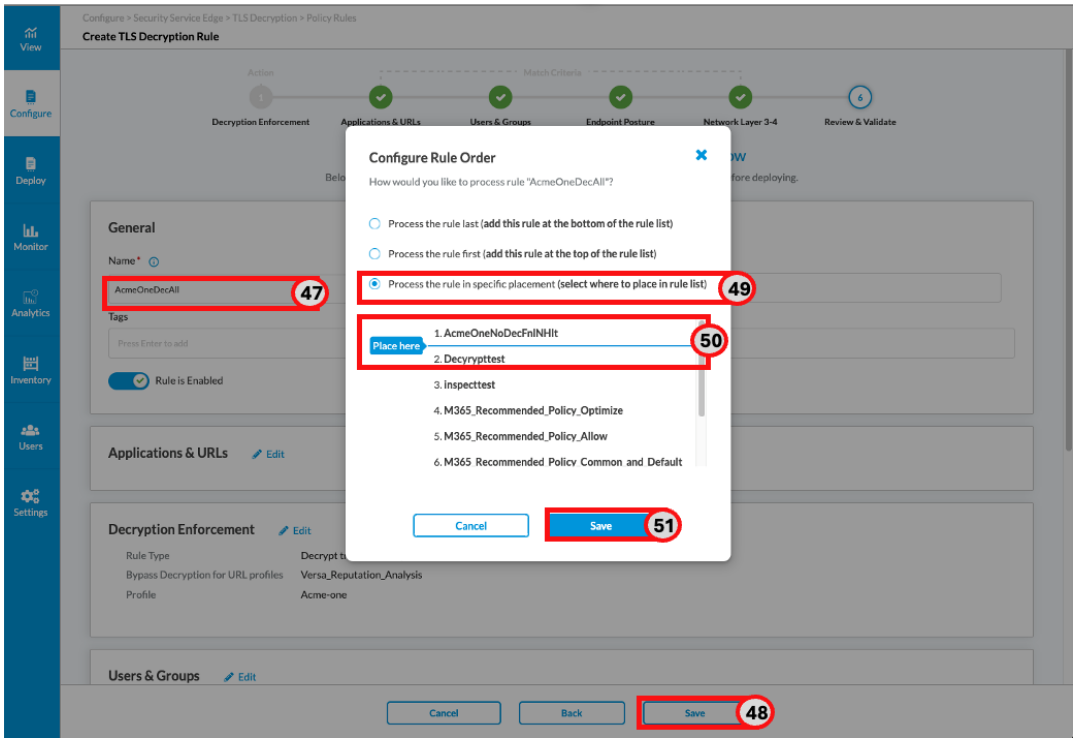


Select **Decrypt Traffic and Inspect server Certificate**, then select the decryption profile created previously, and URL

Filtering Action Override, then click **Skip to Review**.



Assign a descriptive **Name** and click **Save**., In the Configure Rule Order window select **Process Rule in specific placement**, move the rule to 2nd place, then click **Save**.



Step 7: Configure The File Filtering Profile

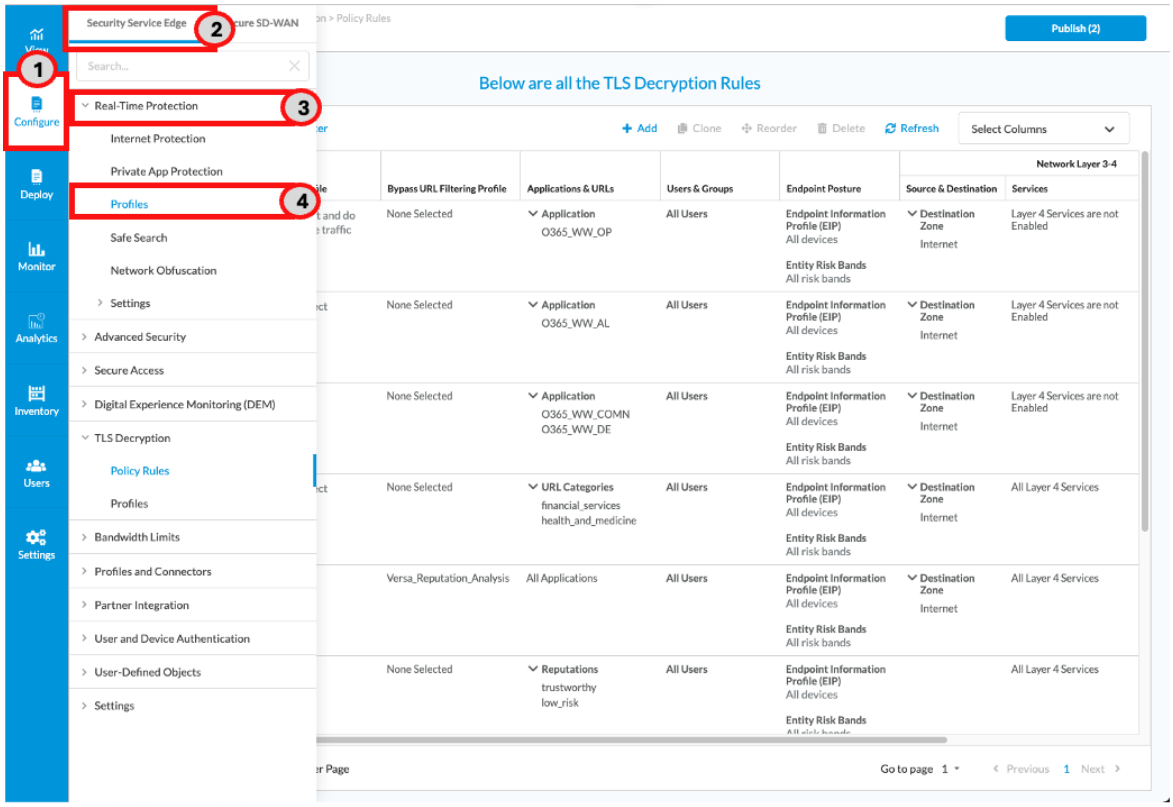
To meet the customer's requirement, a File Filtering profile will be configured to block the download and upload of archive files (e.g., ZIP, RAR) and executable files (.exe) over SaaS App and Personal emails, as these file types may represent a security threat.

Unlike simple extension-based blocking, File Filtering in Versa performs content-based inspection to identify files by their actual type (MIME/content header) across supported protocols. This ensures that renamed or disguised files (e.g., an .exe renamed as .txt) are still detected and blocked.

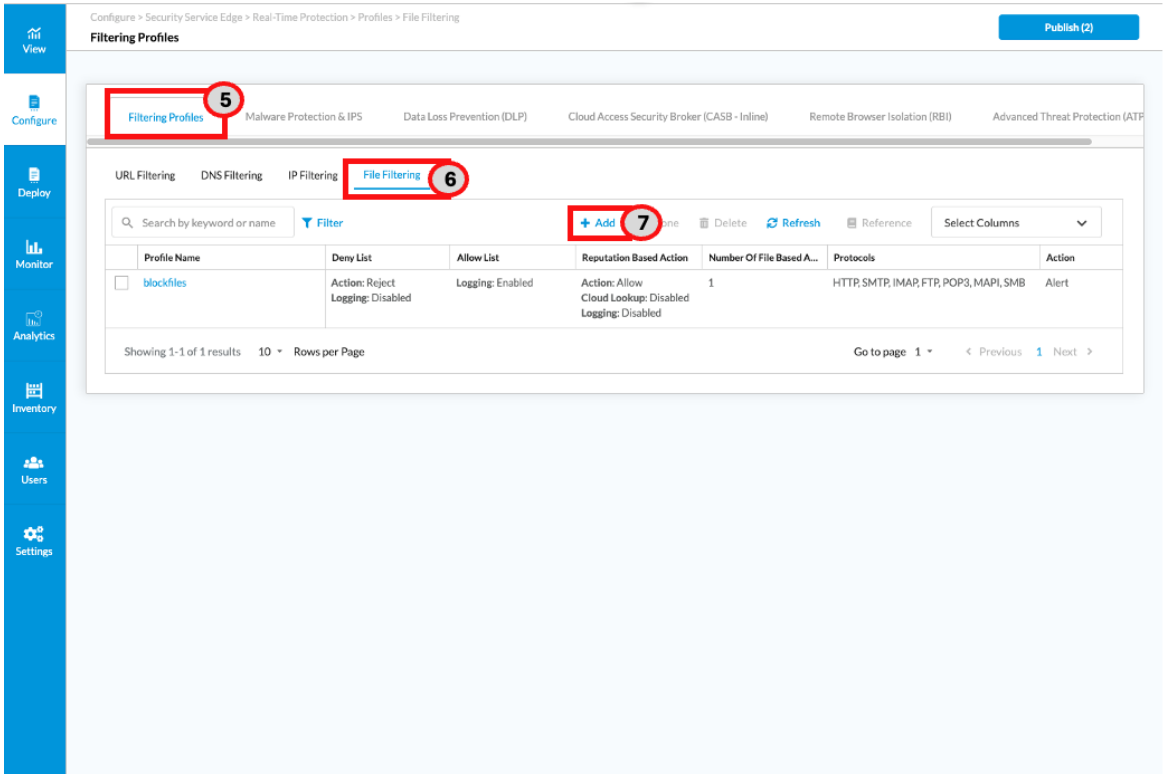
The required information to configure File filtering is listed in the following table.

Parameter	Description
Profile Name	File Filtering profile name
File Type	File type or Extension to block (exe, rar, zip, gzip, 7zip and bzip2)
Protocol	Protocol to analyze looking for file type to block (http)
File Base Action Name	Name for the File filter Action rule

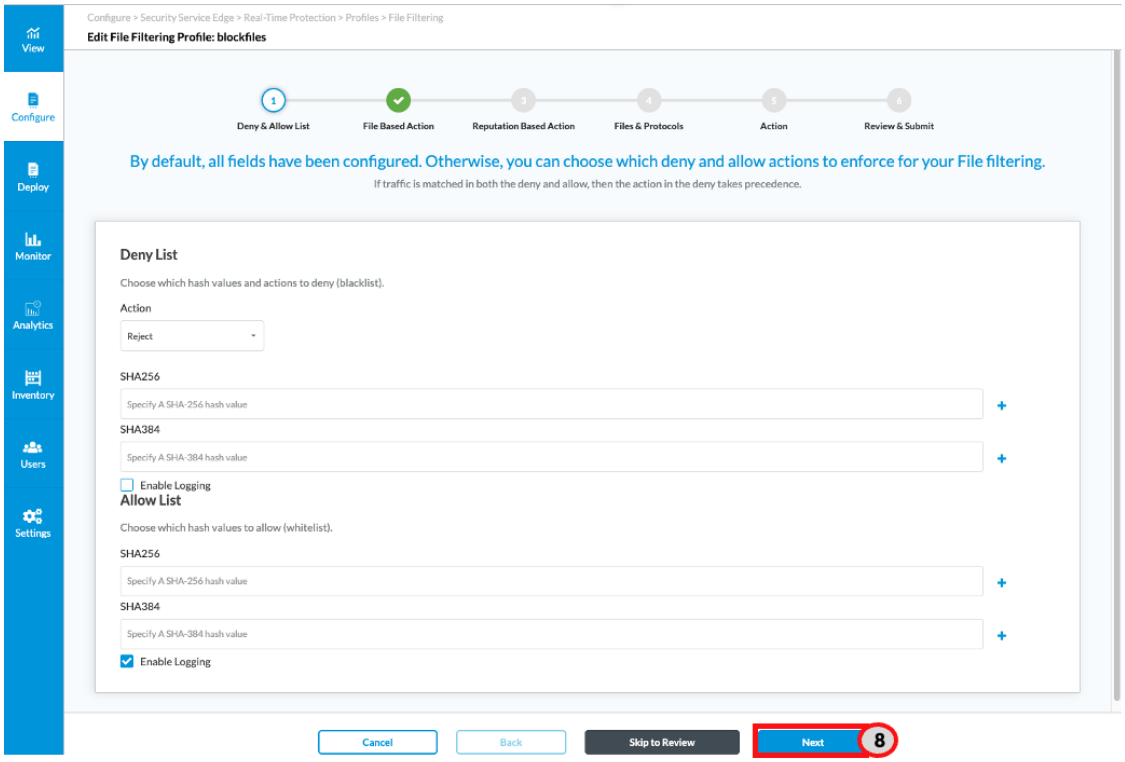
To Configure File Filtering, create a Profile. Go to **Configure> Security Service Edge > Real Time Protection > Profiles** to access the Profiles configuration section.



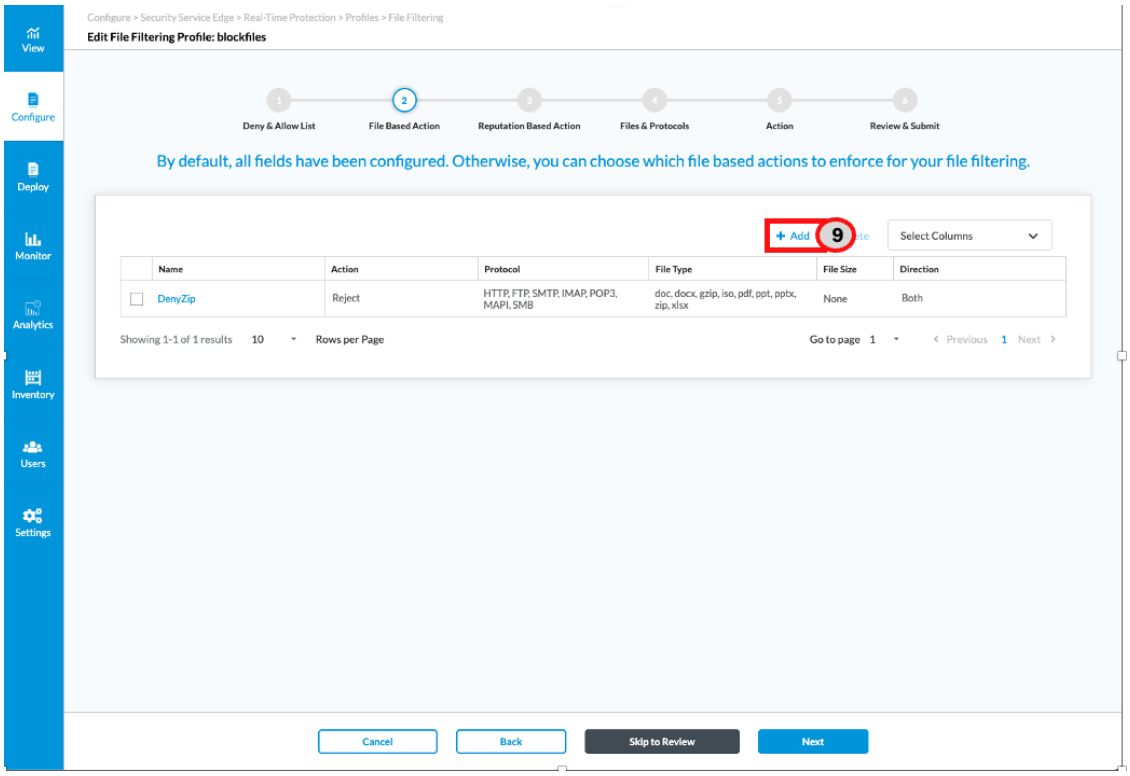
Go to the **Filtering Profiles** tab, then the **File Filtering** tab, then click **+ Add** .



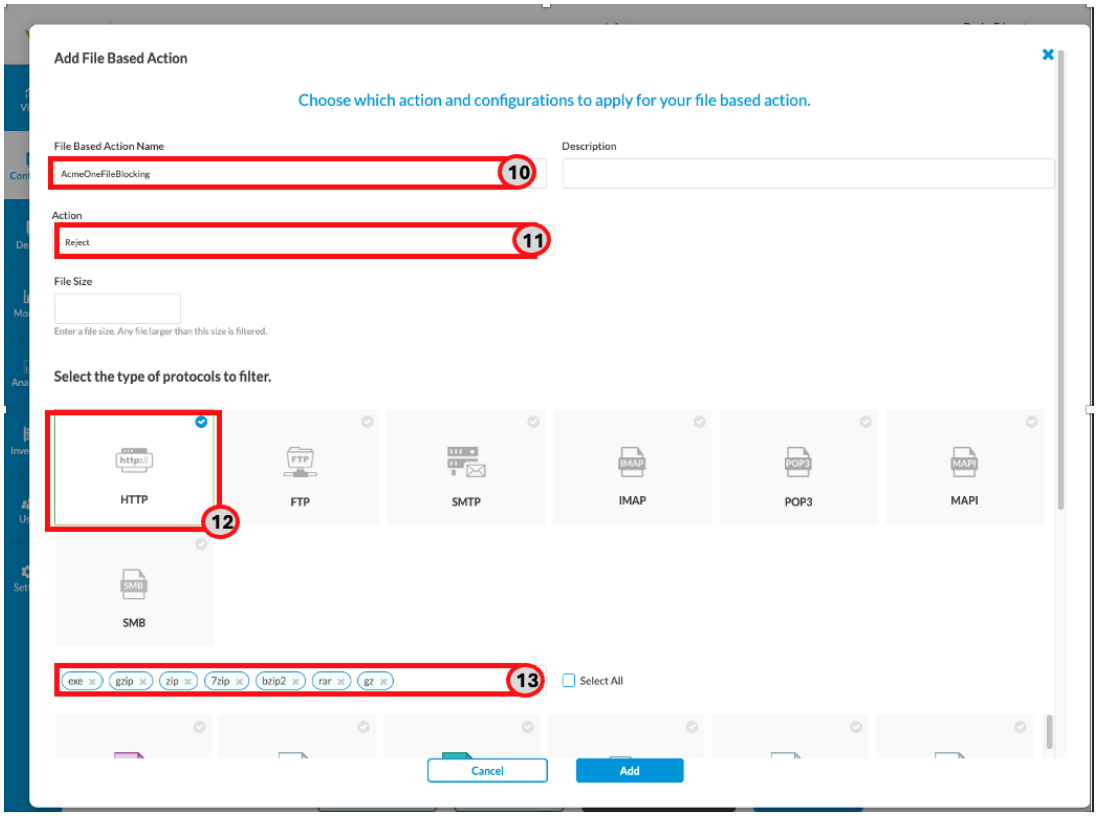
In Deny & Allow List you can optionally create a Deny List (aka black list) or Allow List (aka white list) with file hash to control specific file transfers. If that is not required for the use case, then click **Next**.



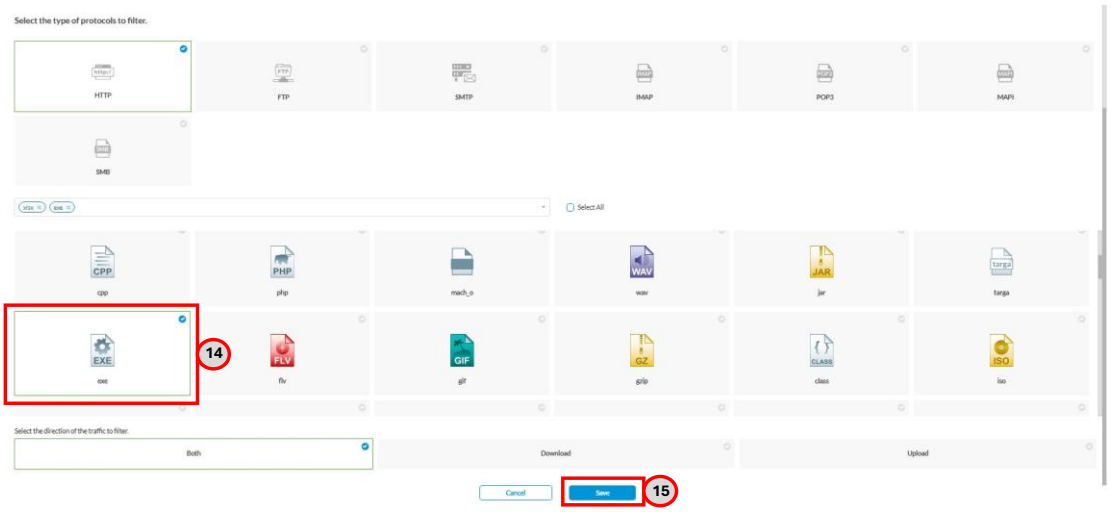
Click **Add** to create a File-based Action based on the file types you want to prevent users from downloading.



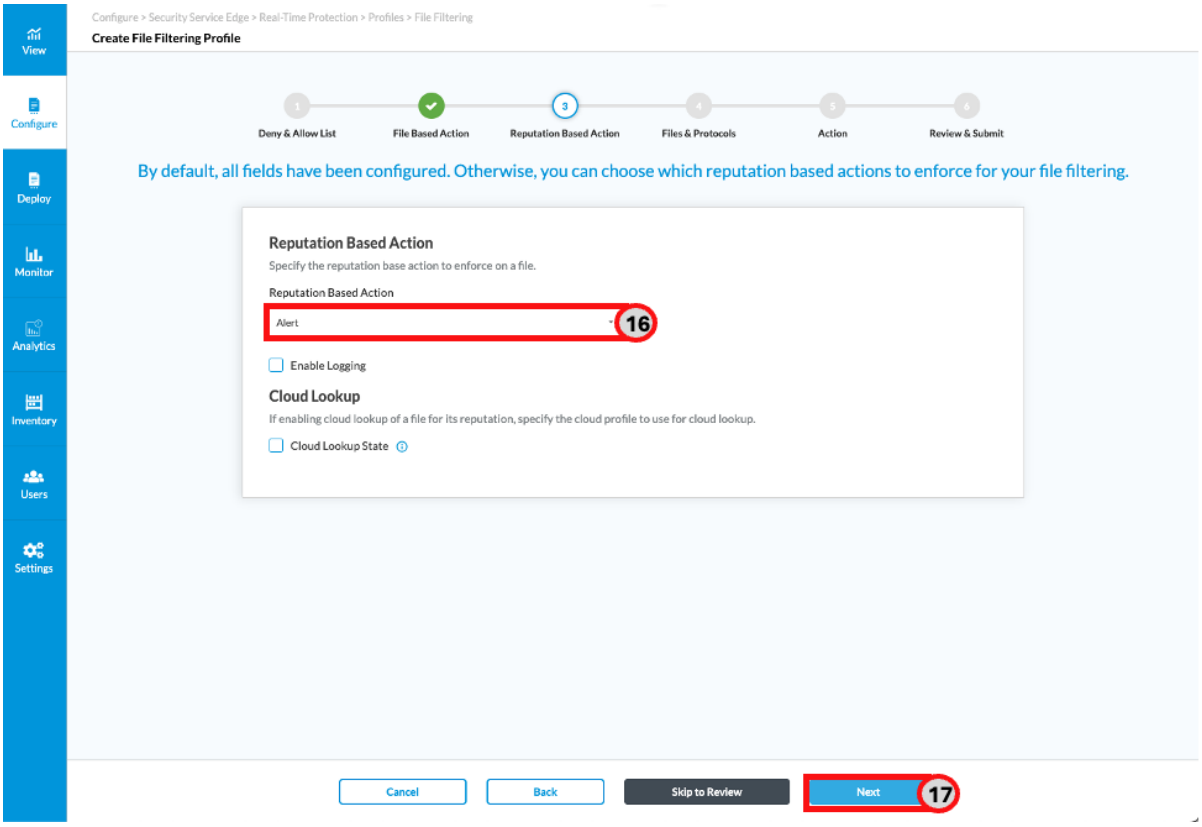
Assign a descriptive **Name**, choose the **Reject** action for the match criteria, select **HTTP** as the protocol to monitor and add the exe, zip, gzip, 7zip, bzip2, rar and exe file types to match.



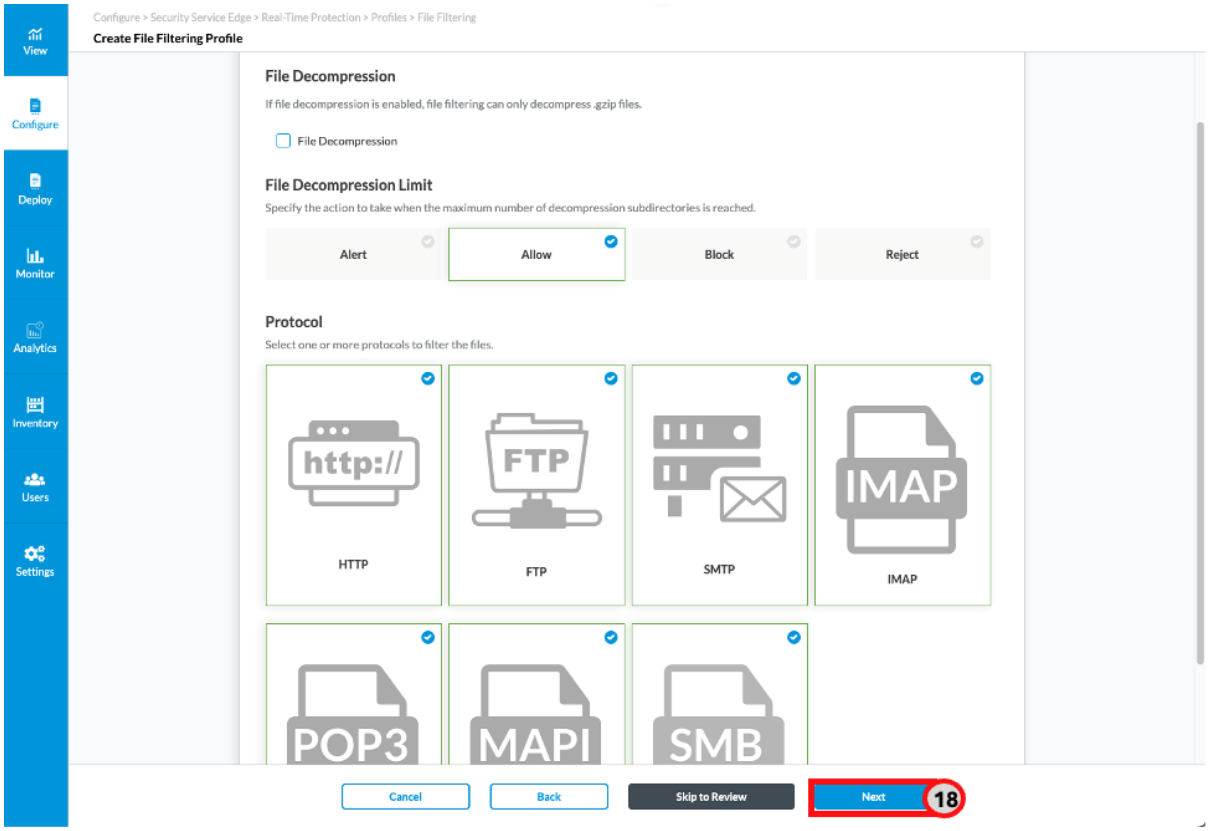
Scroll down and select **Download (14)**, then click **Save (15)** followed by **Next**.



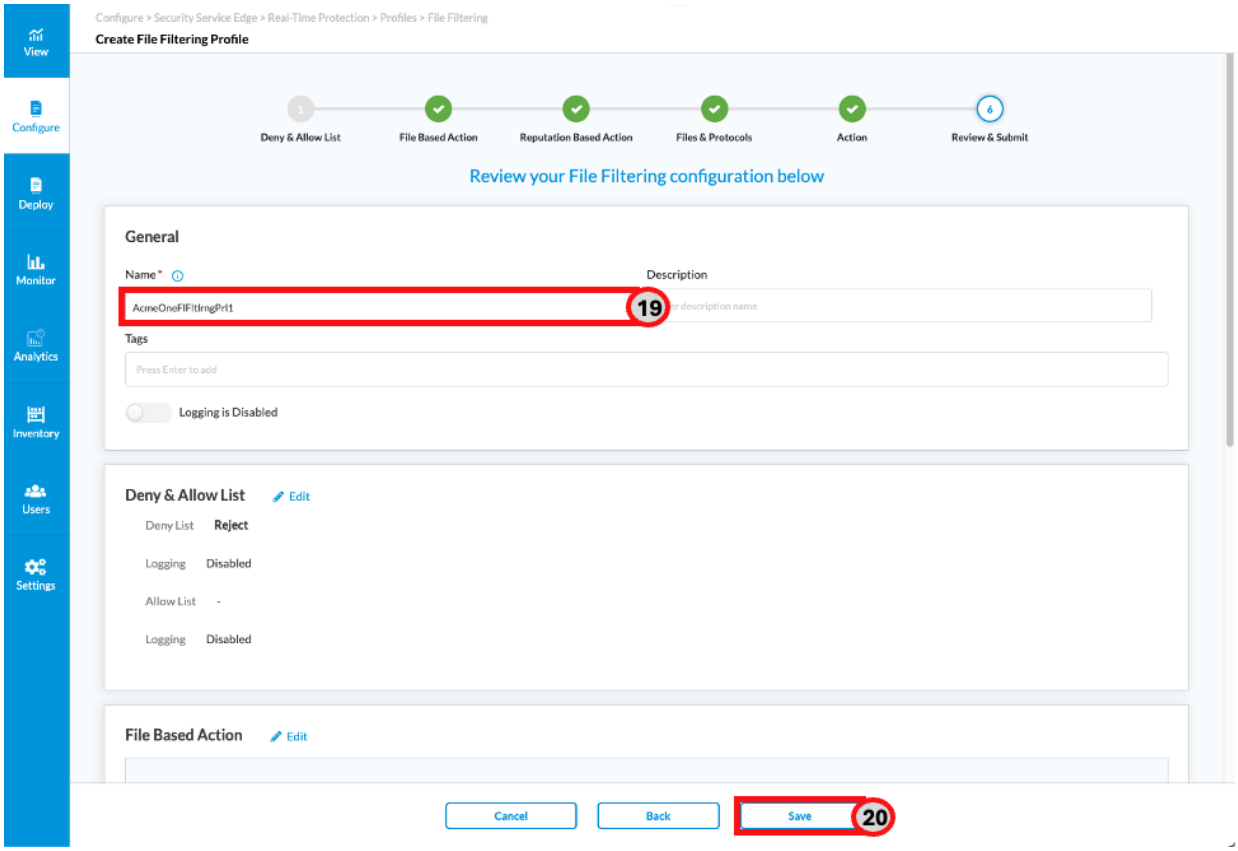
No action is required based related to file reputation so just configure the **Alert (16)** action and click **Next (17)**.



Compress files are not allowed so you can scroll down and click **Next**.



Assign a descriptive **Name** then click **Save**.



Step 8: Configure URL filtering Profile

URL Filtering ensures that user access to web resources is controlled based on corporate security and compliance requirements. Profiles can be applied to specific user groups to restrict risky or non-business-related content.

In this use case:

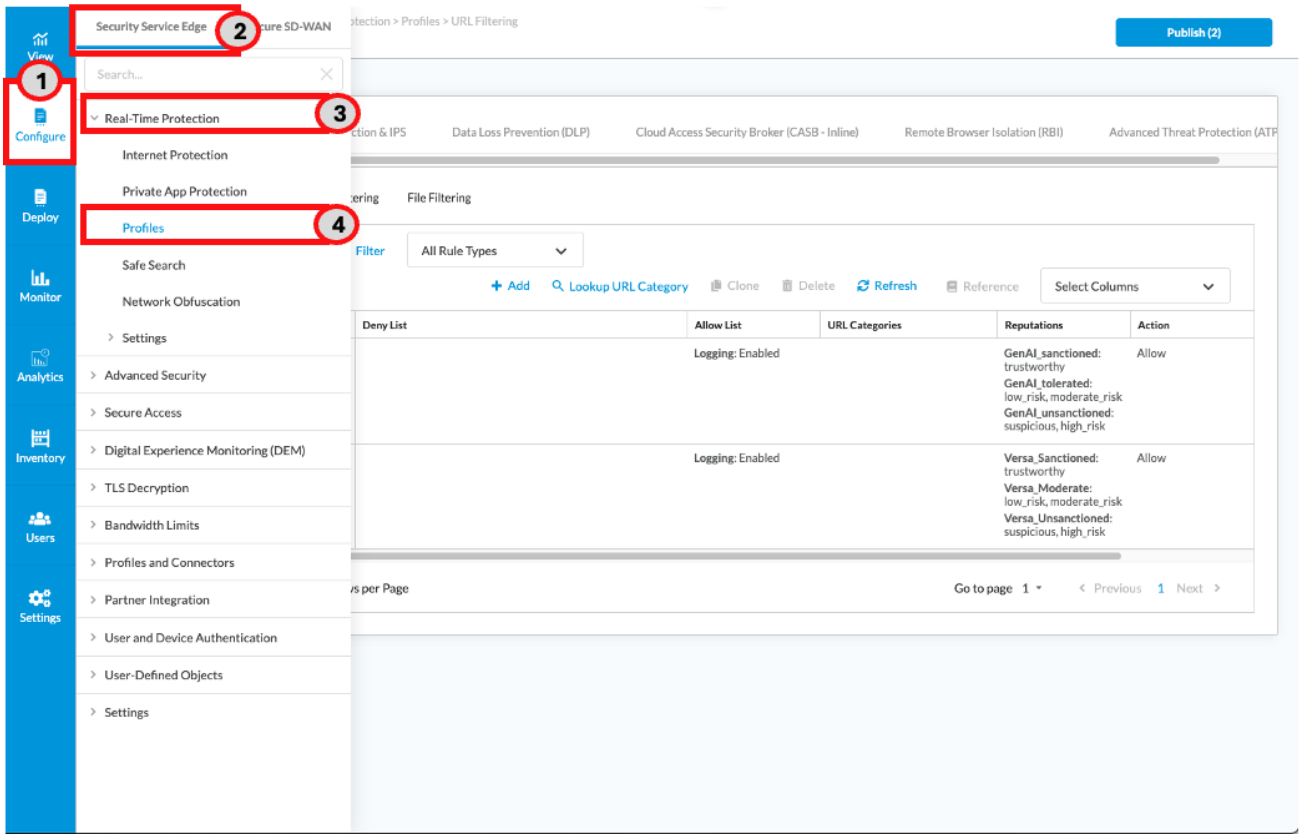
- IT Users: Apply the Versa Recommended URL Filtering Profile.
    - This profile is preconfigured by Versa with a balanced set of controls designed to protect against common threats and enforce corporate-appropriate browsing.
    - It covers high-risk categories such as malware, phishing, botnets, and anonymizers, while still allowing access to legitimate business and productivity resources.
    - It is considered a **best-practice baseline** and reduces the need for extensive manual tuning.
- Contractor Users: Apply a Custom URL Filtering Profile.
    - This profile will be created specifically to block categories inappropriate or unnecessary for contractors, such as:
        - Adult content
        - Sports
        - Gambling
        - Firearms
        - Violence

- By tailoring this profile, contractors have access only to business-related websites while ensuring compliance and minimizing distractions.

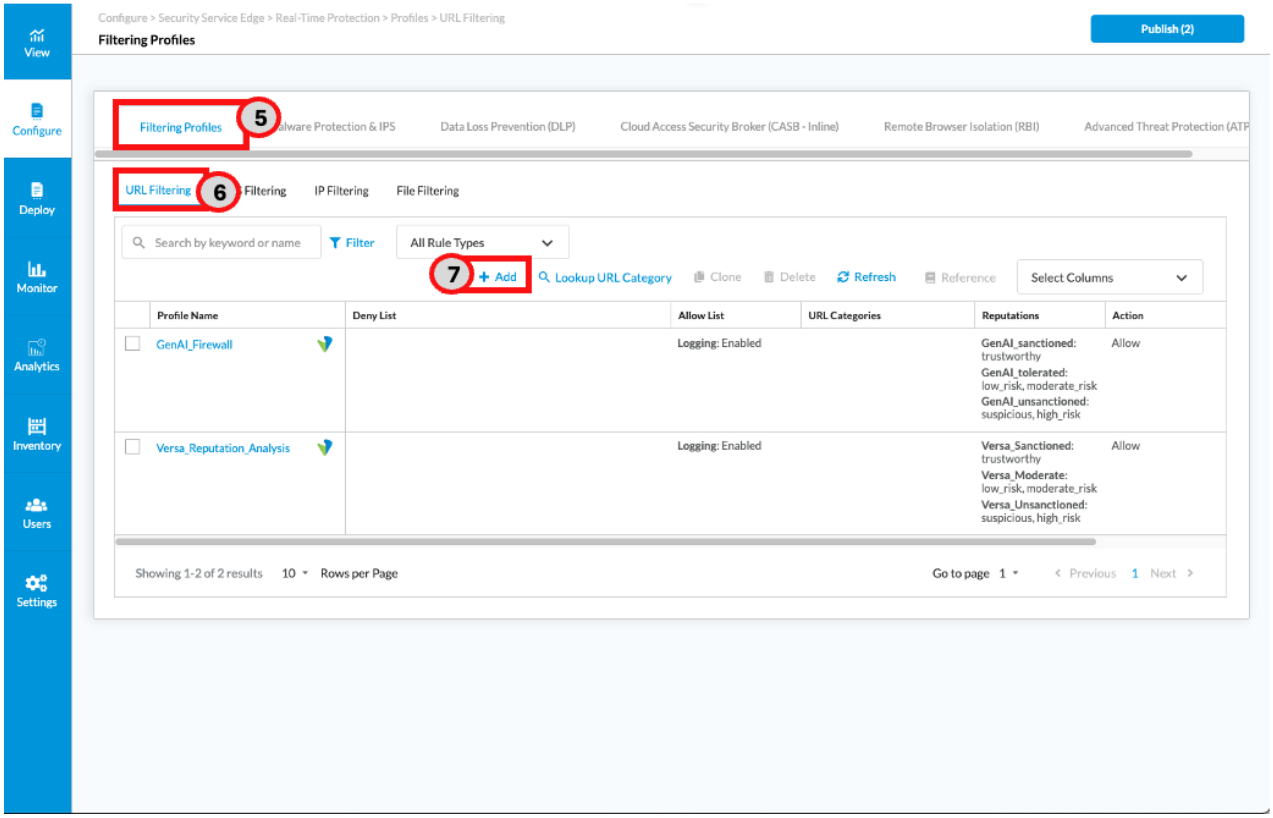
We will now create a custom URL filtering profile for contractor users

Parameter	Description
Profile Name	URL Filtering profile name
URL Categories	URL categories to match

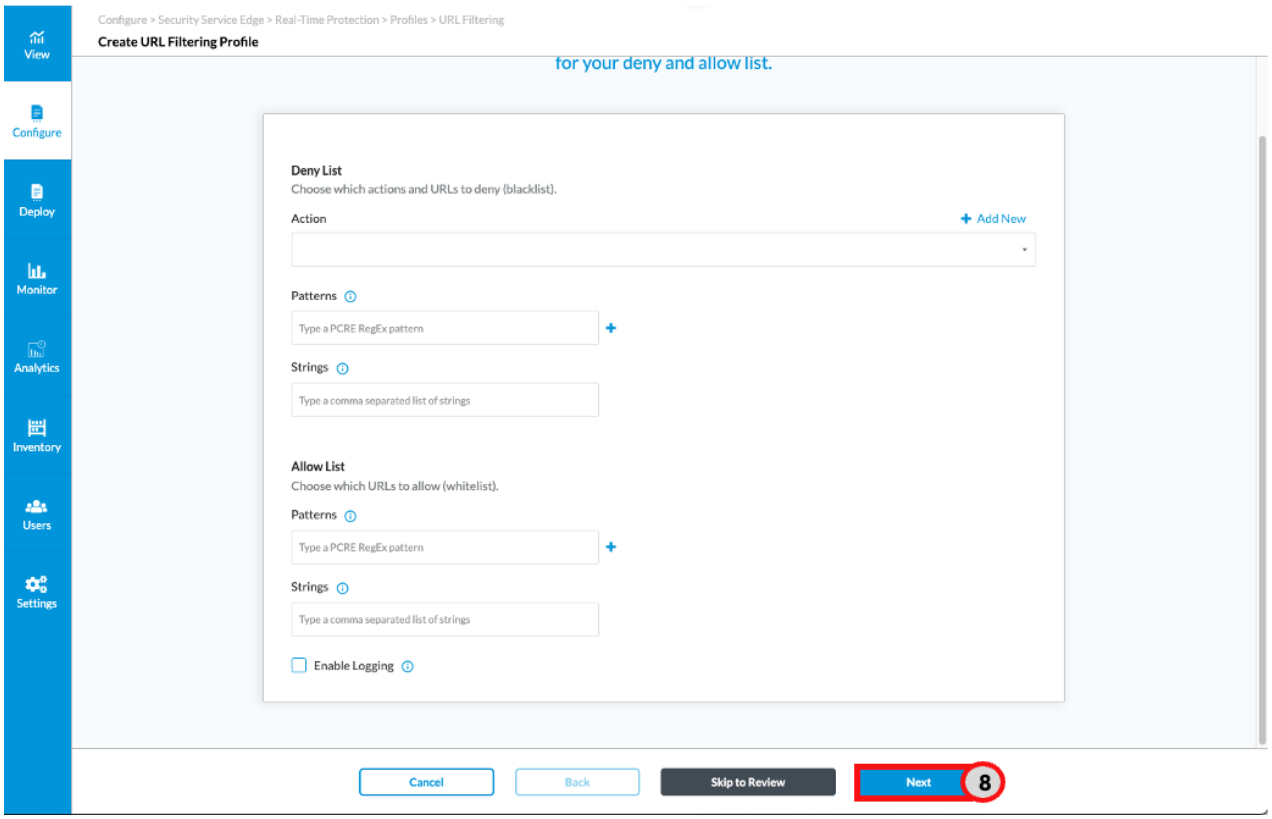
To Configure a URL Filtering Profile, go to **Configure > Security Service Edge > Real Time Protection > Profiles**.



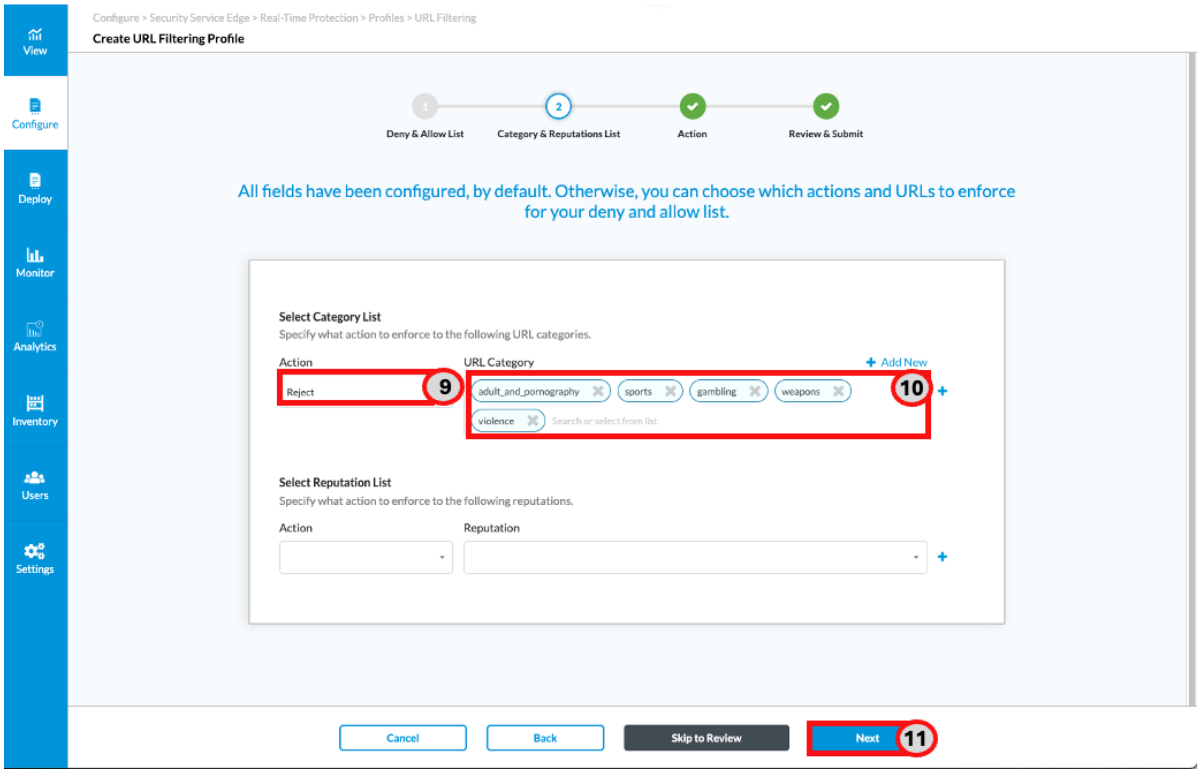
Go to filtering **Profiles**, select **URL Filtering**, then click **+ Add**.



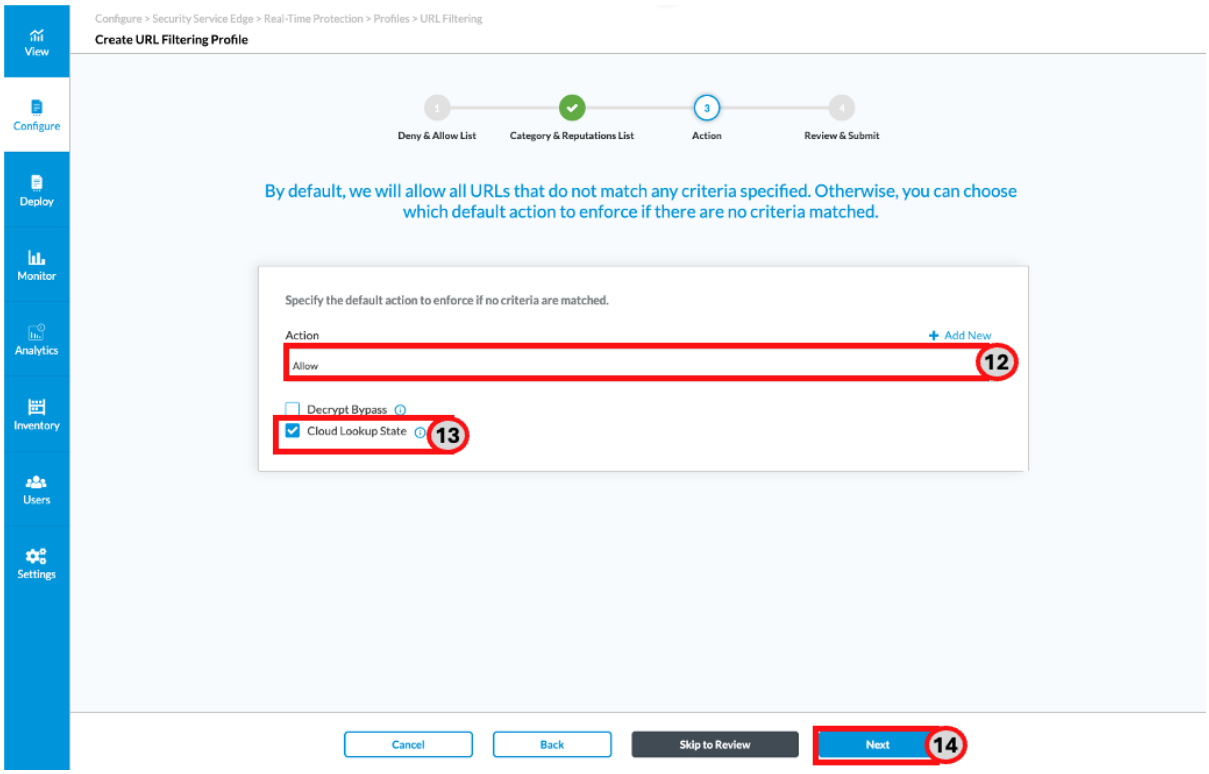
In Deny & Allow List there are no specific URLS to allow or deny, so click **Next** .



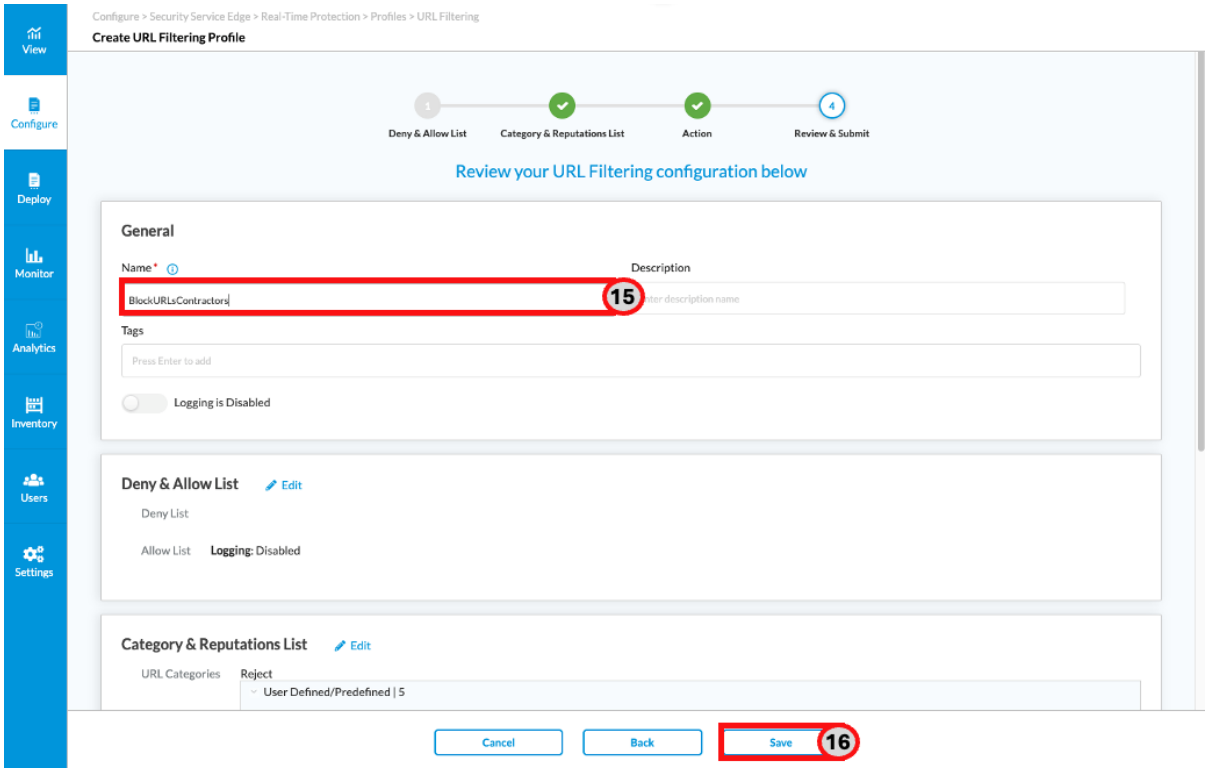
Under Select Category List select **Reject** in the Action dropdown, then search and select the names of the URL categories for which this action applies: **adult_and_pornography, sports, gambling, weapons and violence**. When the list is complete click **Next** to continue.



Select **Allow** as default action if the URL does not match any URL category being enforced from the previous step. Select the checkbox **Cloud lookup State**. This helps provide visibility into millions of URLs and categories beyond what can be stored locally. Click **Next** to continue.



Assign a descriptive **Name** for the profile and then click on **Save**.



Step 9: Configure Internet Protection Policy Rules

All the elements needed to create the policies enforcing the security requirements of the use case have already been made. The next step is to create rules that align with the traffic and apply the previously developed elements to enforce the expected behaviour. To meet the customer's requirements, two rules will be created, one for Contractor and other for IT users.

Internet Protection Policy Rule for Contractor Users

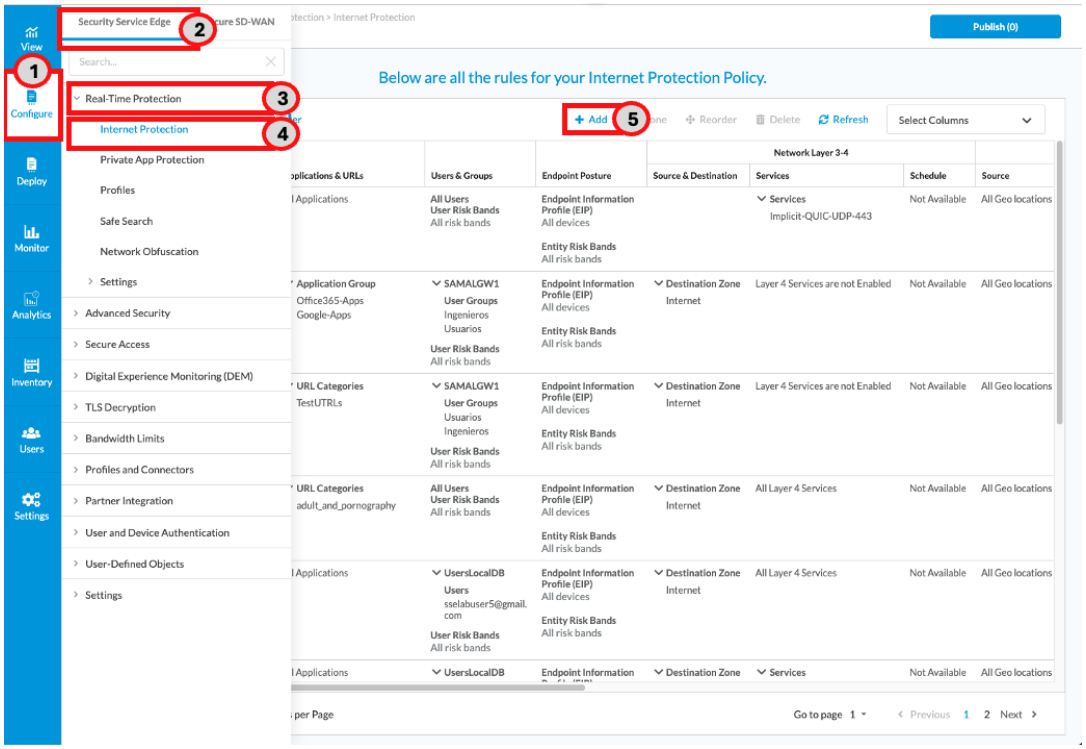
For the first rule, the required information to configure the Internet Protection Rules for Contractor Users is listed below.

Parameter	Description
Rule Name	Name to identify the Internet Protection Rule
Profile Type	Type of profile to enforce a specific rule (File Filtering and URL Filtering Profile)
Profile Name	Name of the profile to enforce a specific rule (blockfiles and BlockURLsContractors)
Match Criteria	Criteria to match or isolate specific traffic for a Rule (user Group =Contractors)

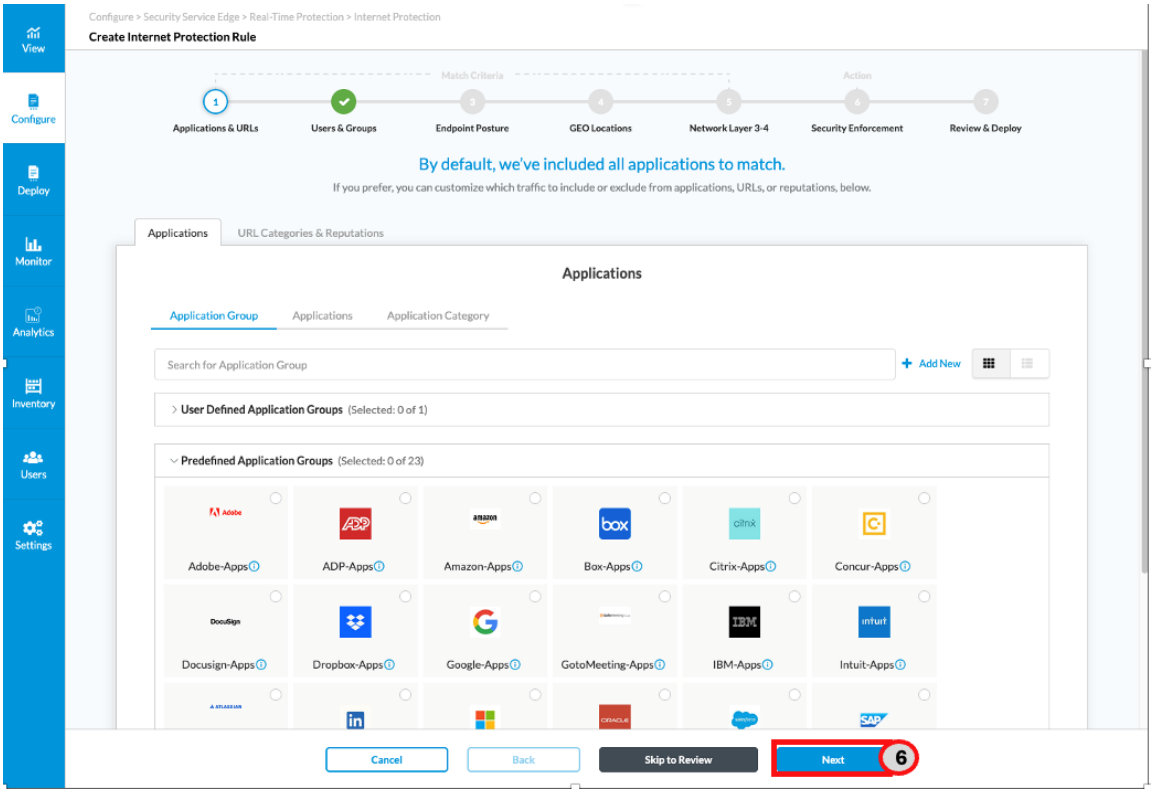
The policy allows traffic for the Contractor users but enforces security for files and URLs constraints.

To create the rule, go to **Configure > Security Service Edge > Real Time Protection > Internet Protection**. Click **+**

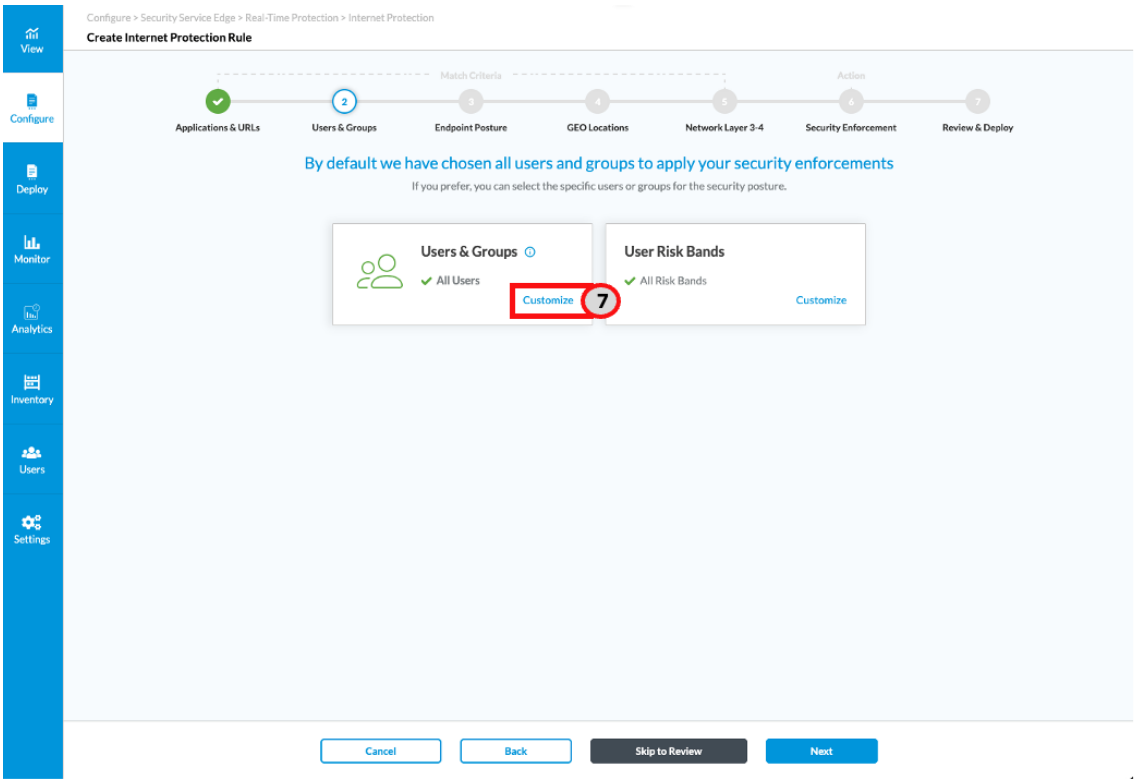
Add .



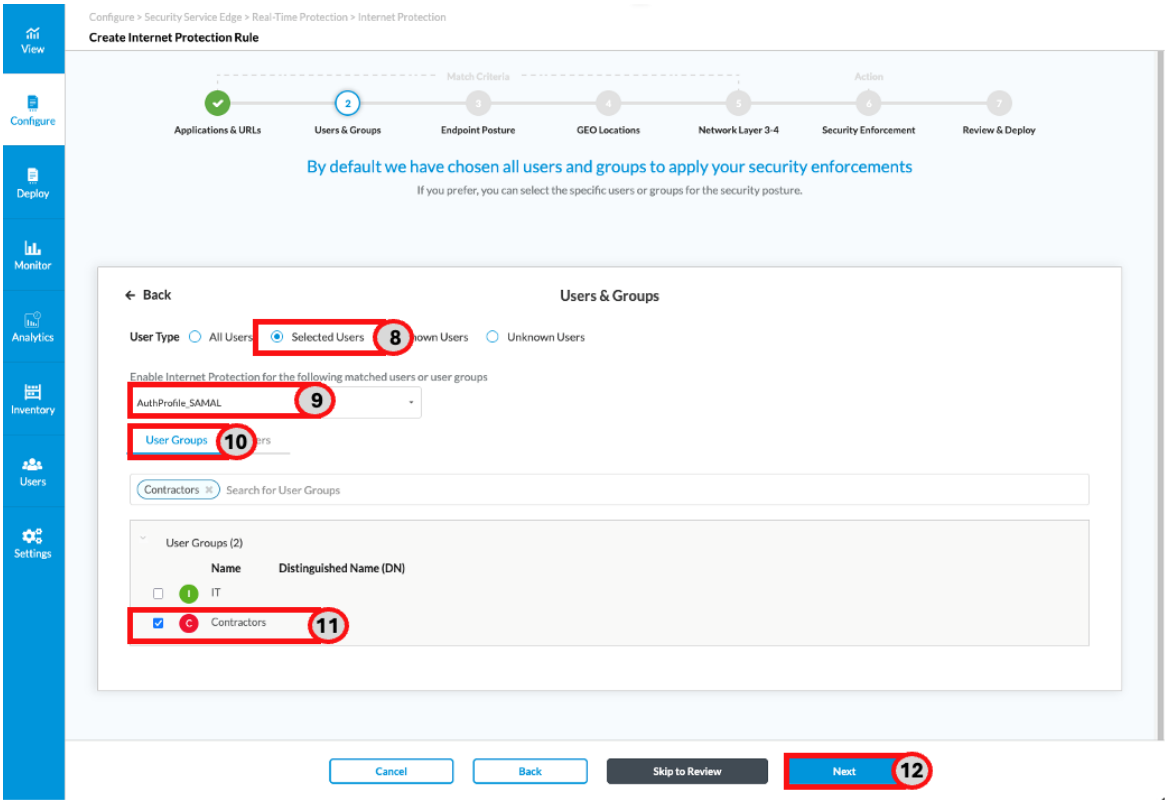
In Applications & URLs, click **Next** without making any changes. URL filtering will be performed using a profile later on in Security Enforcement, so no matching applications or URLs are required here.



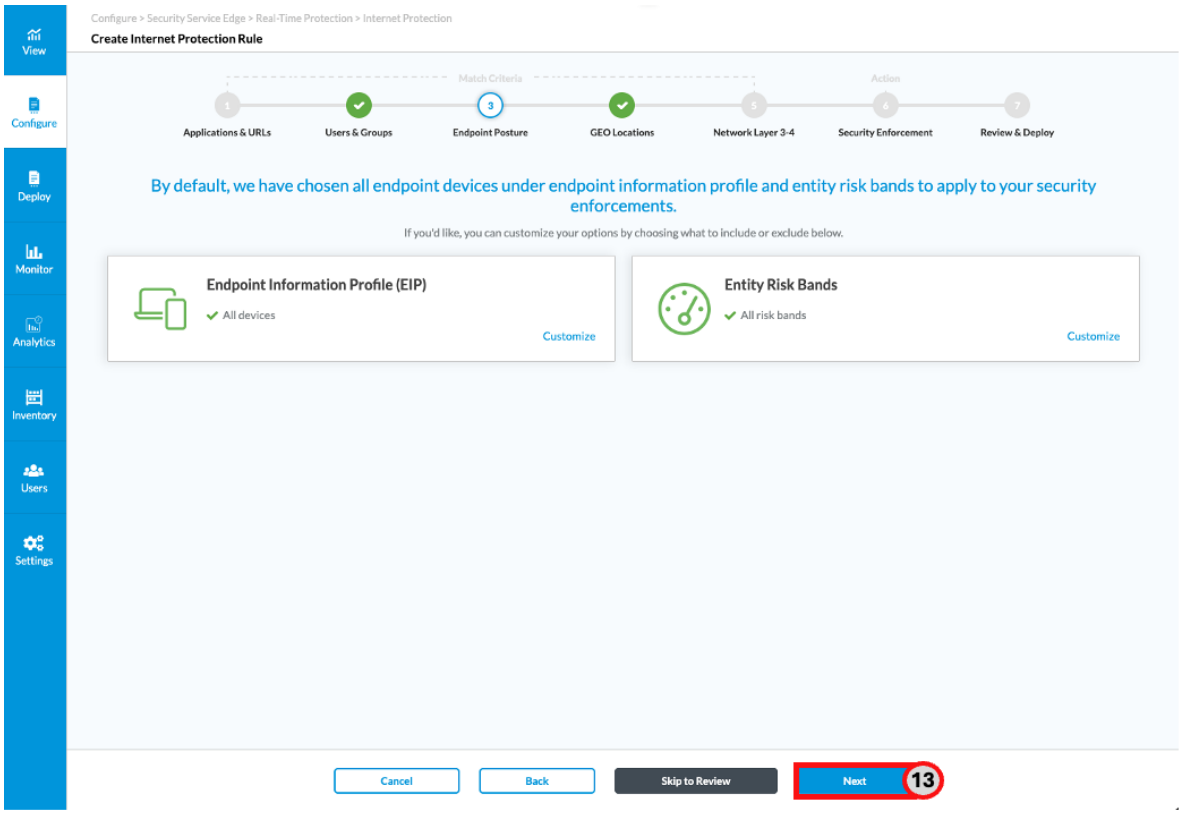
Click **Customize** under Users & Groups.



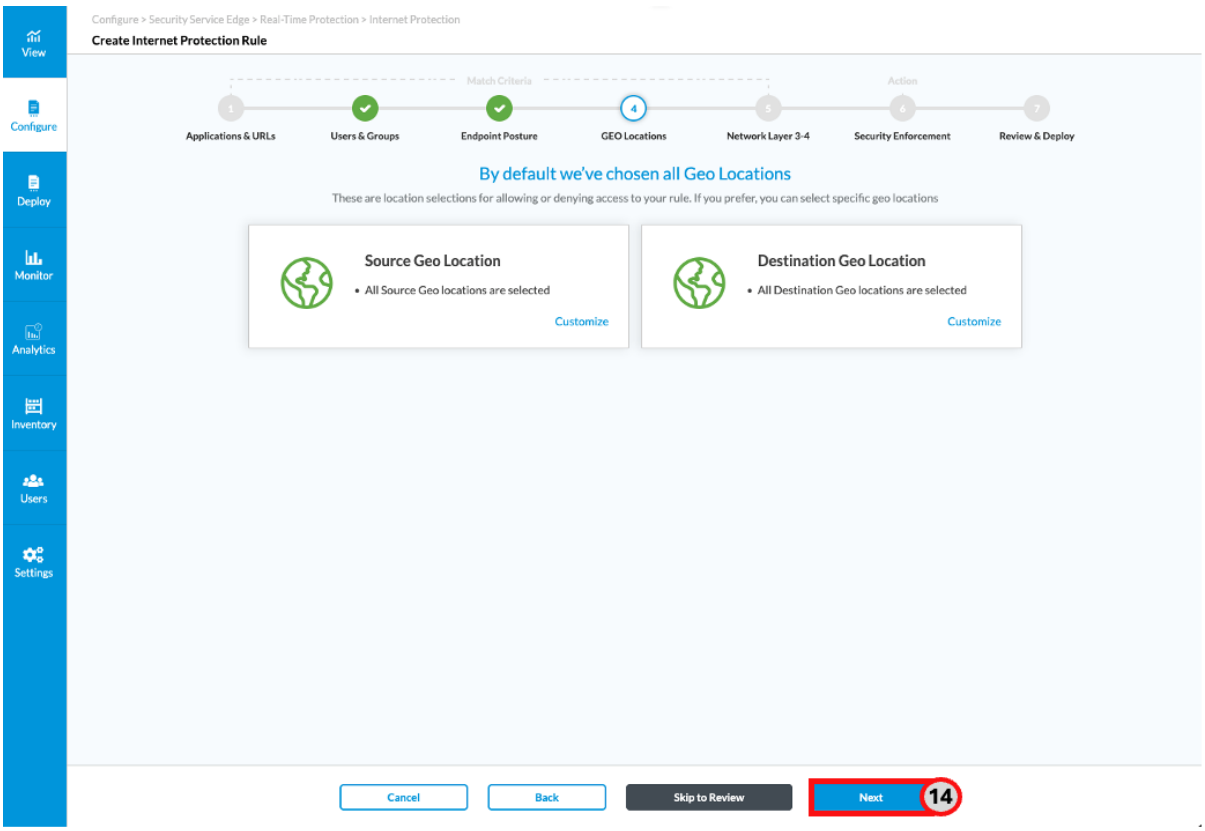
Select the radio button **Selected Users** , select the SAML authentication profile created from step 1, select **User Groups**, then search and check **Contractors**. Click **Next**.



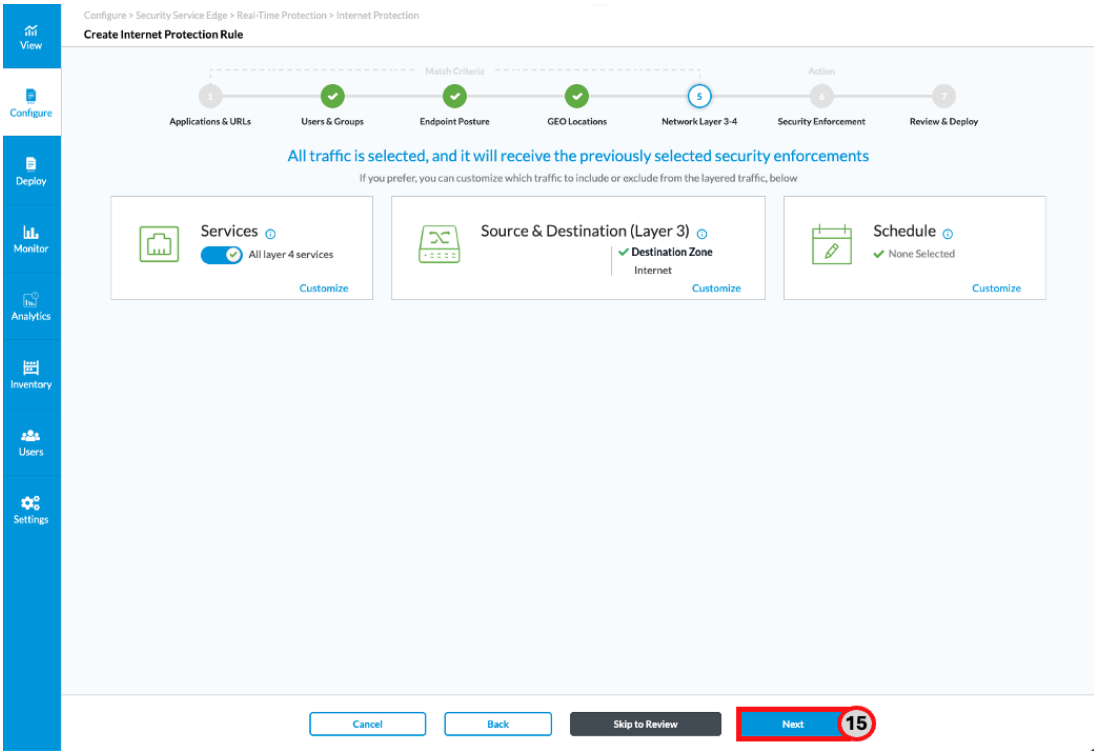
Click **Next** in Endpoint Posture as no EIP or Entity Risk criteria will be used as match criteria .



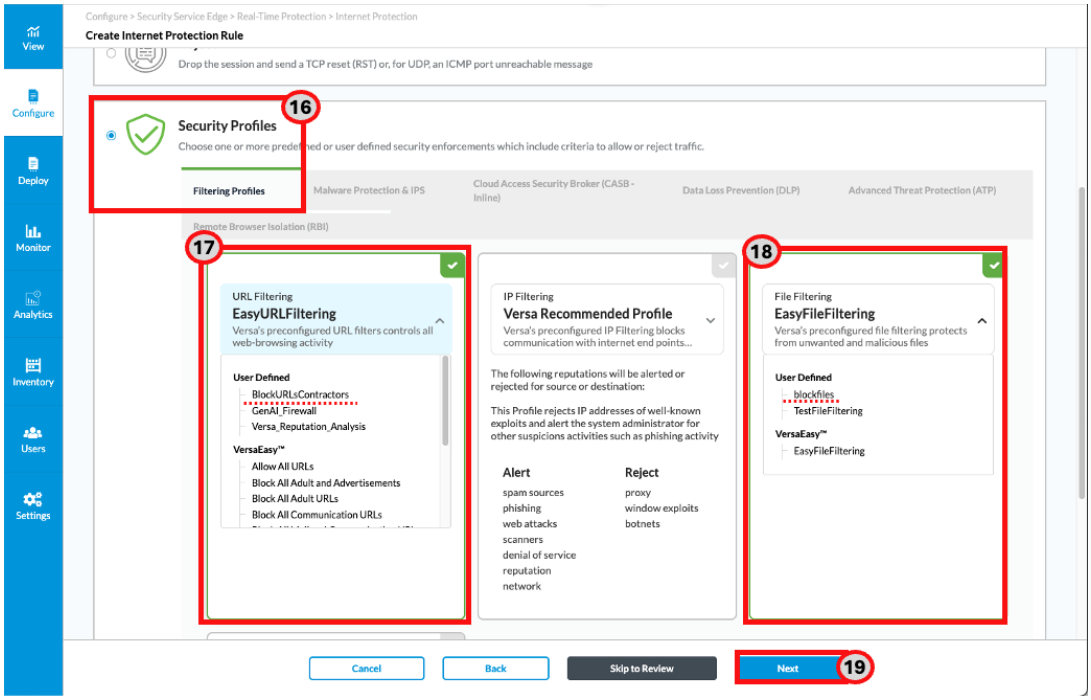
Click **Next** in Geo Locations section, as no match criteria is required for contractor users traffic.



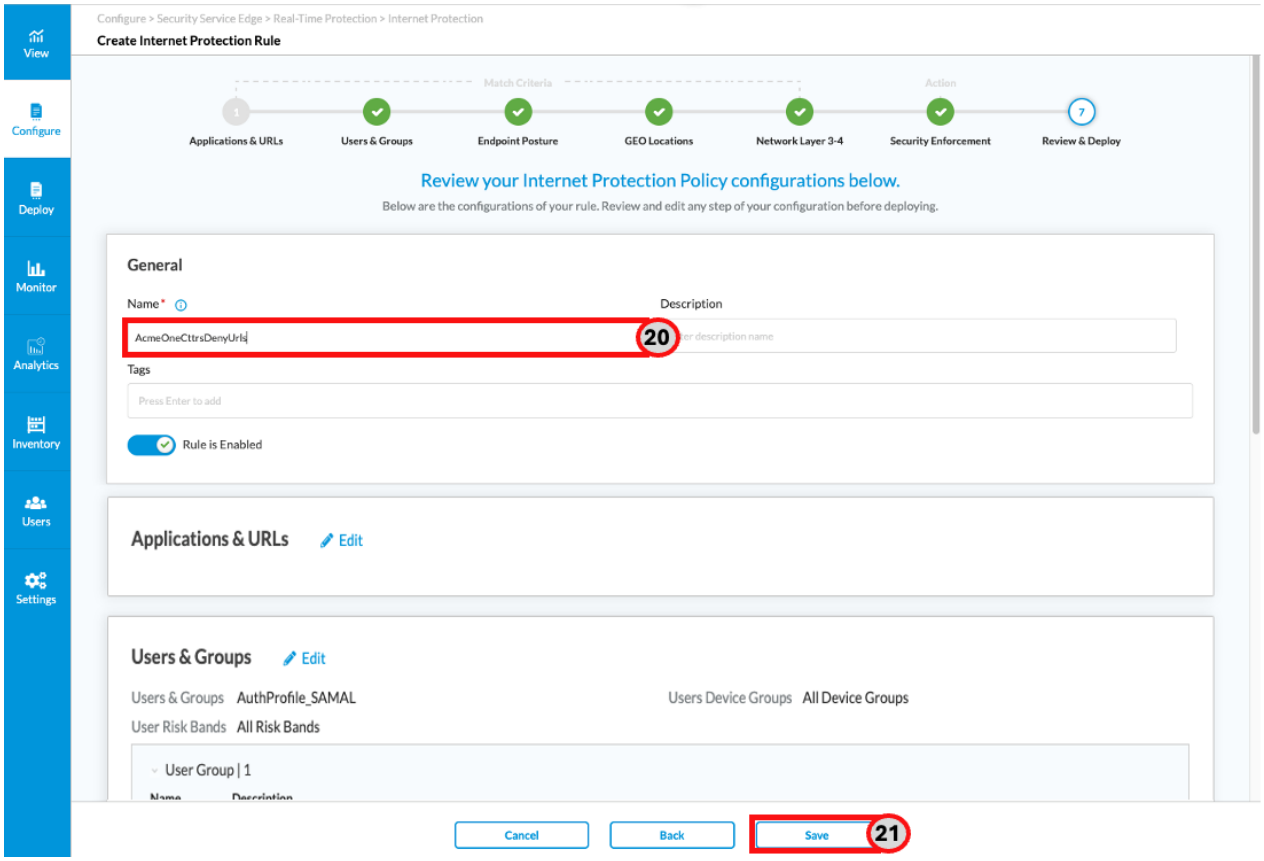
Click **Next** in Network Layer 3-4 section.



In Security Enforcement, scroll down and select the **Security Profile** radio button and select the **Filtering Profiles** tab. Check the **URL Filtering** box and from the list select the **BlockURLContractors** user defined profile. Check the **File Filtering** box and from the list select the **blockfiles** user defined profile. Click **Next**.



Use a descriptive **Name** and click **Save** to create the Rule. In the Configure Rule Order screen, select **Process the rule in specific placement**, then drag the rule to place it after the Implicit-Allow-DNS rule.



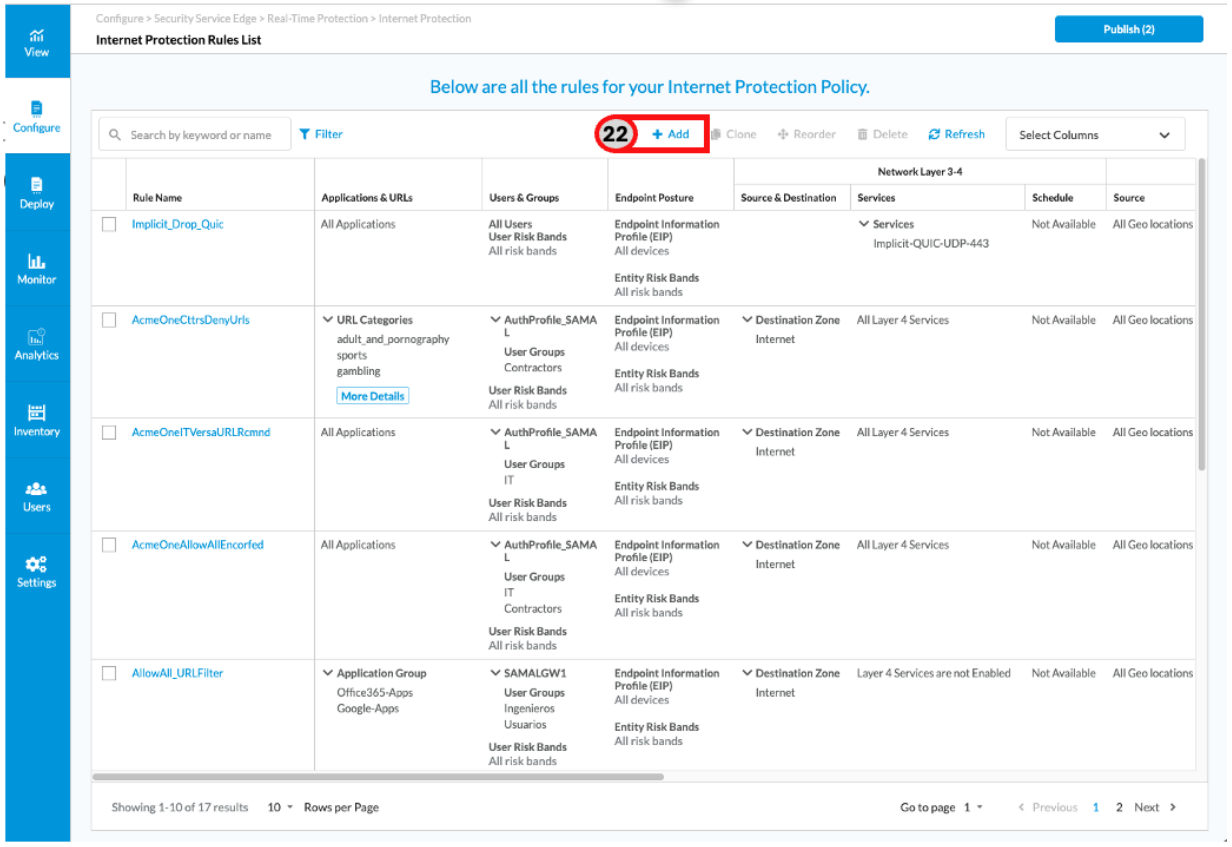
Internet Protection Policy Rule for IT Users

The second rule will allow traffic for IT Users, enforcing the URL and files constraints.

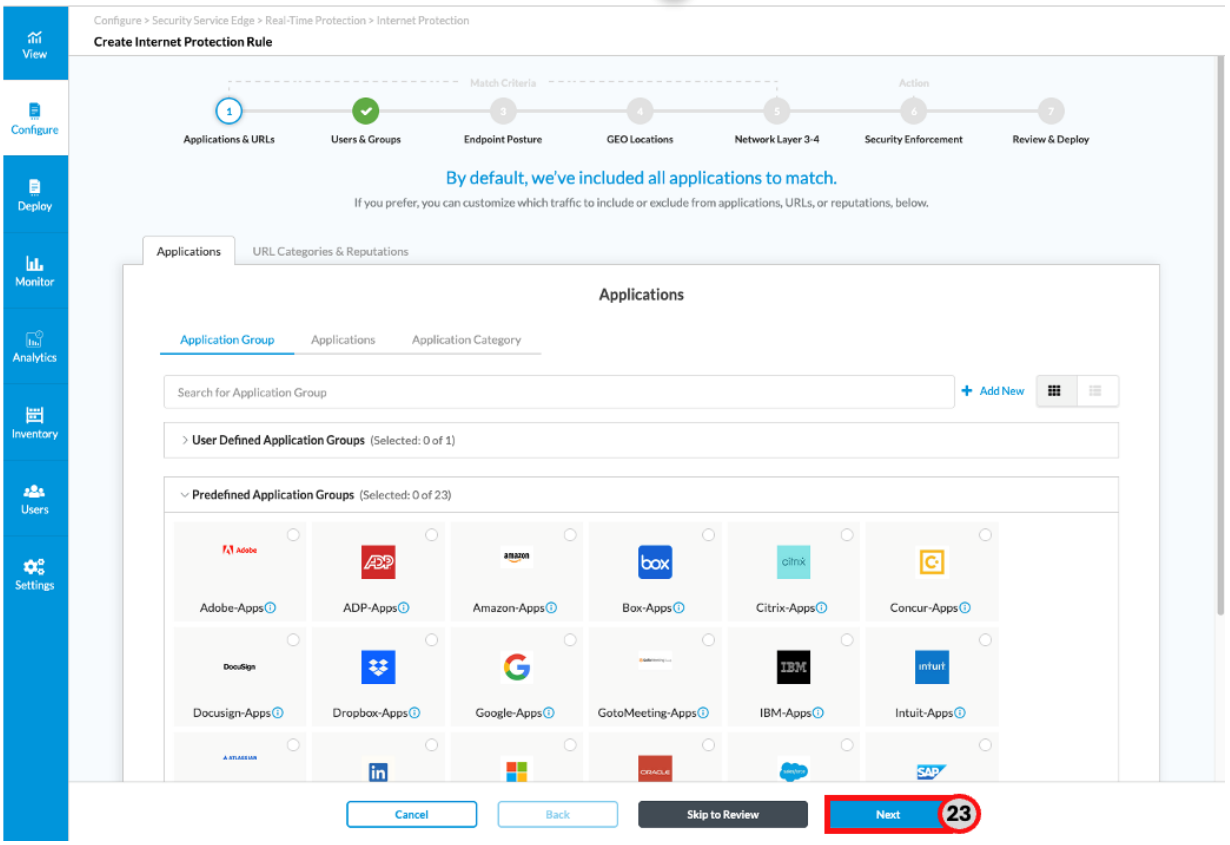
The required information to configure the Internet Protection Rules for IT Users are listed below.

Parameter	Description
Rule Name	Name to identify the Internet Protection Rule
Profile Type	Type of profile to enforce a specific rule (File Filtering and URL Filtering Profile)
Profile Name	Name of the profile to enforce a specific rule (block-files and EasyURLFiltering)
Match Criteria	Criteria to match or isolate specific traffic for a Rule (Group=IT)

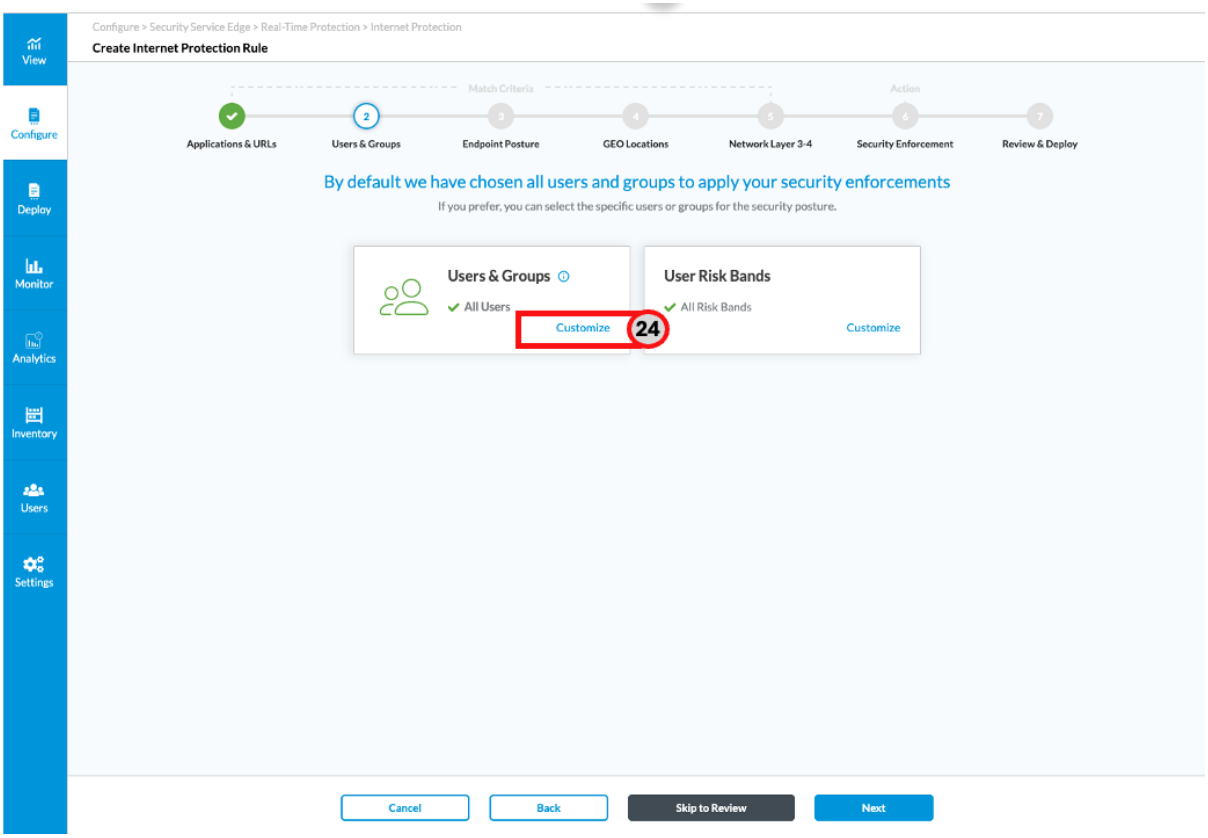
To create the rule for IT users, Click **+ Add** .



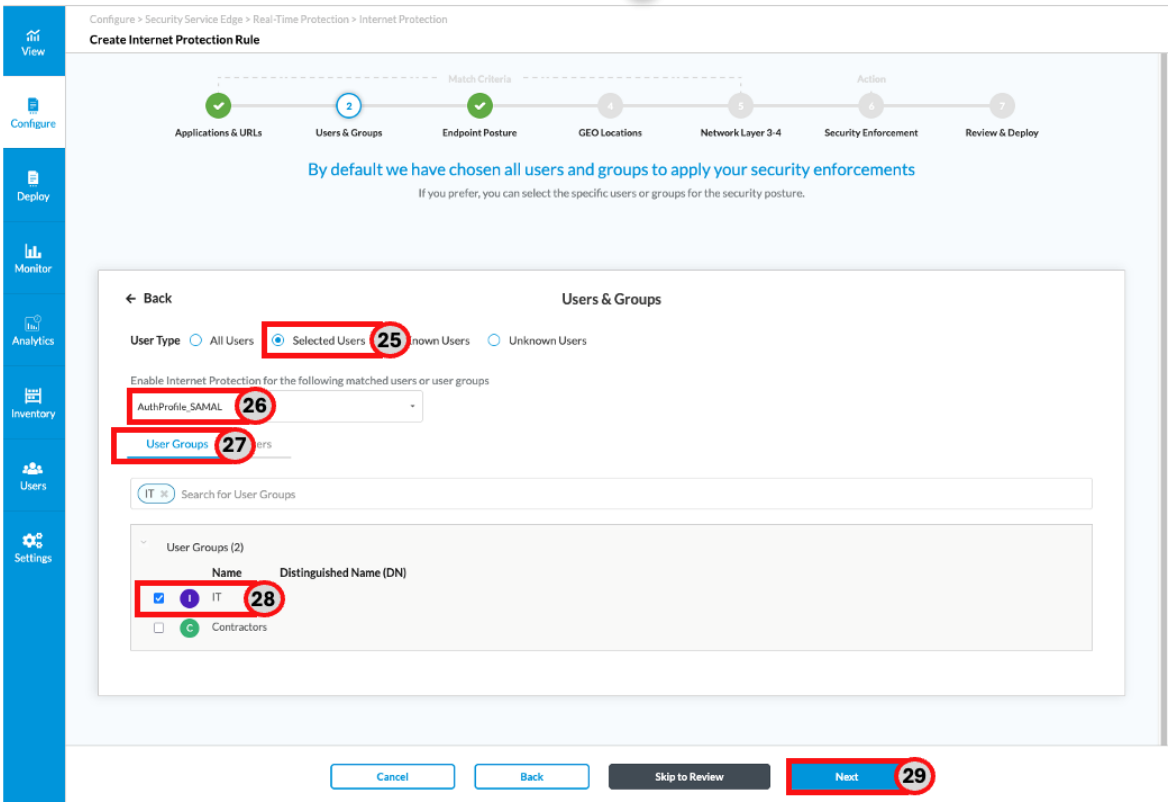
In Applications & URLs, click **Next** without making any changes. URL filtering will be performed using a profile later on in Security Enforcement, so no matching applications or URLs are required here.



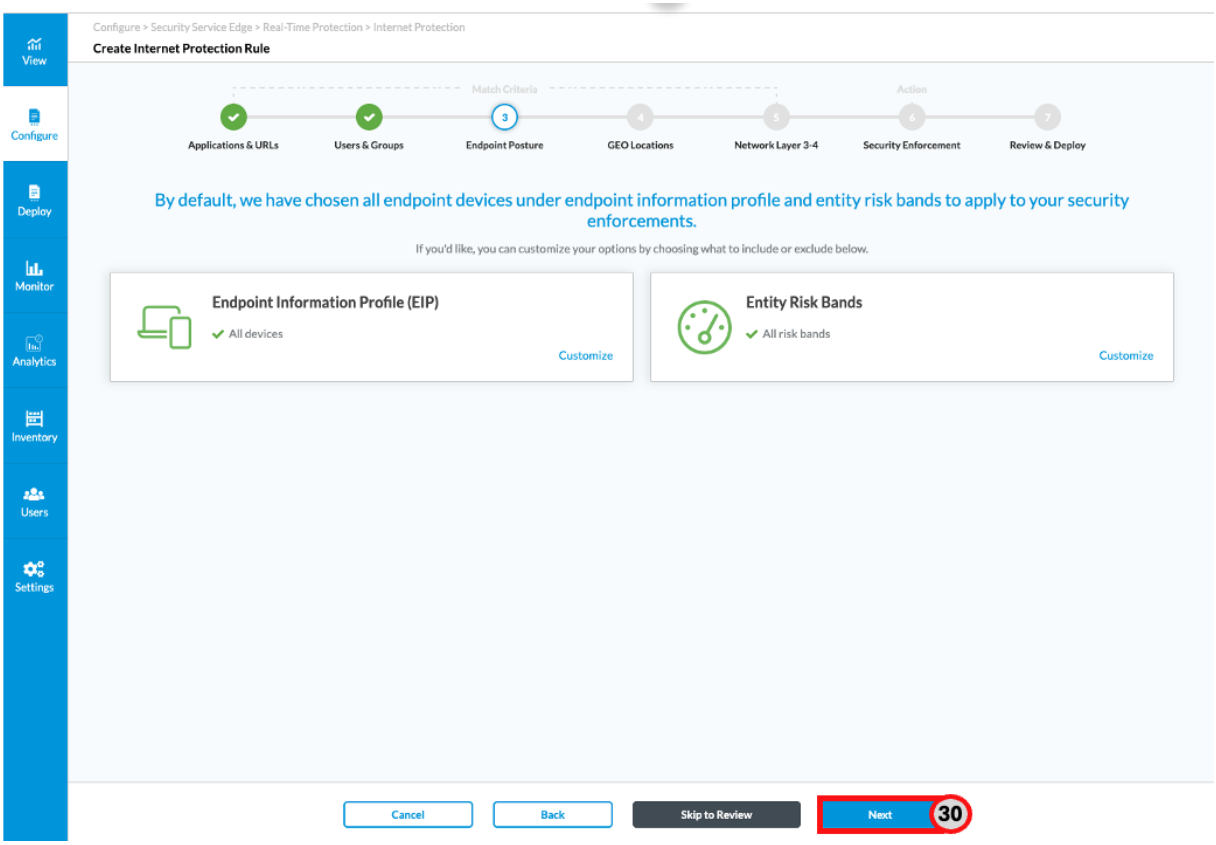
Click **Customize** under Users & Groups.



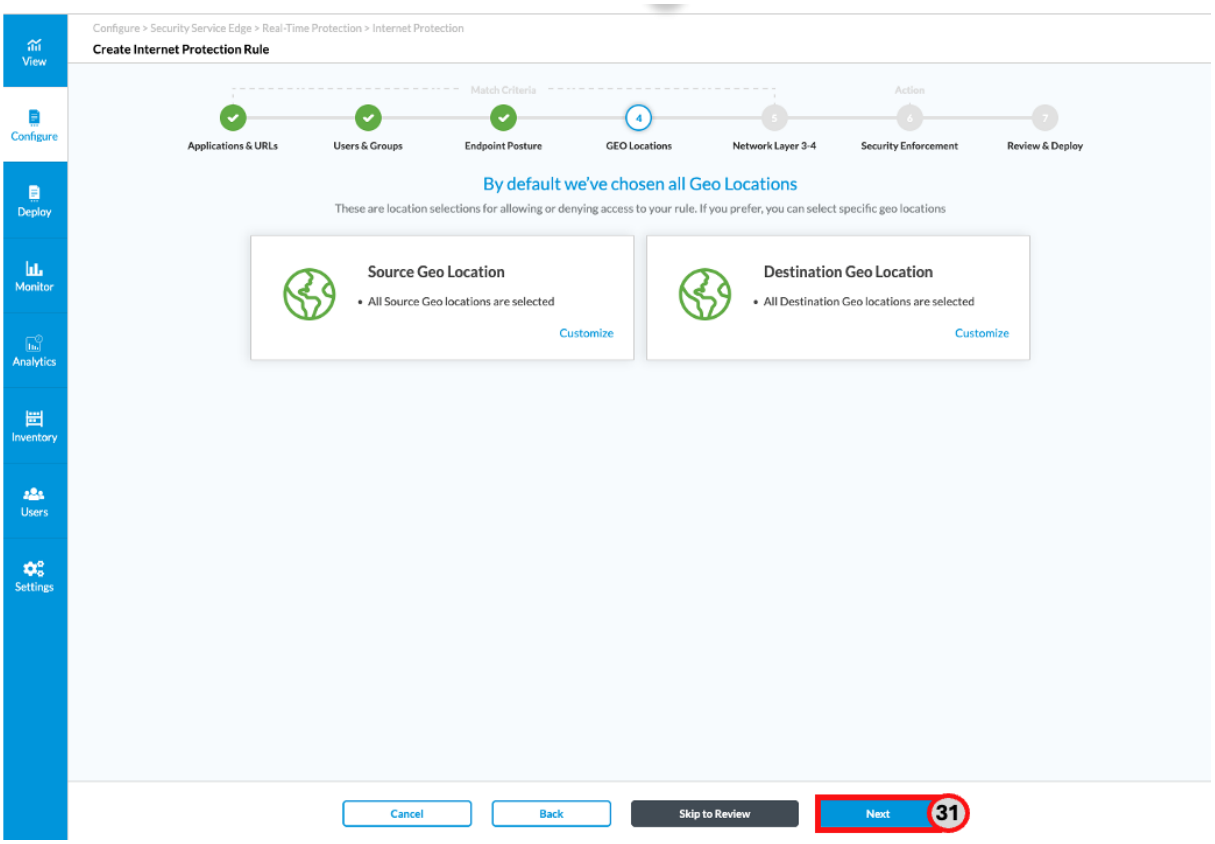
Select the radio button **Selected Users**, select the SAML authentication profile created from step 1, select **User Groups**, then search and check **IT**. Click **Next**.



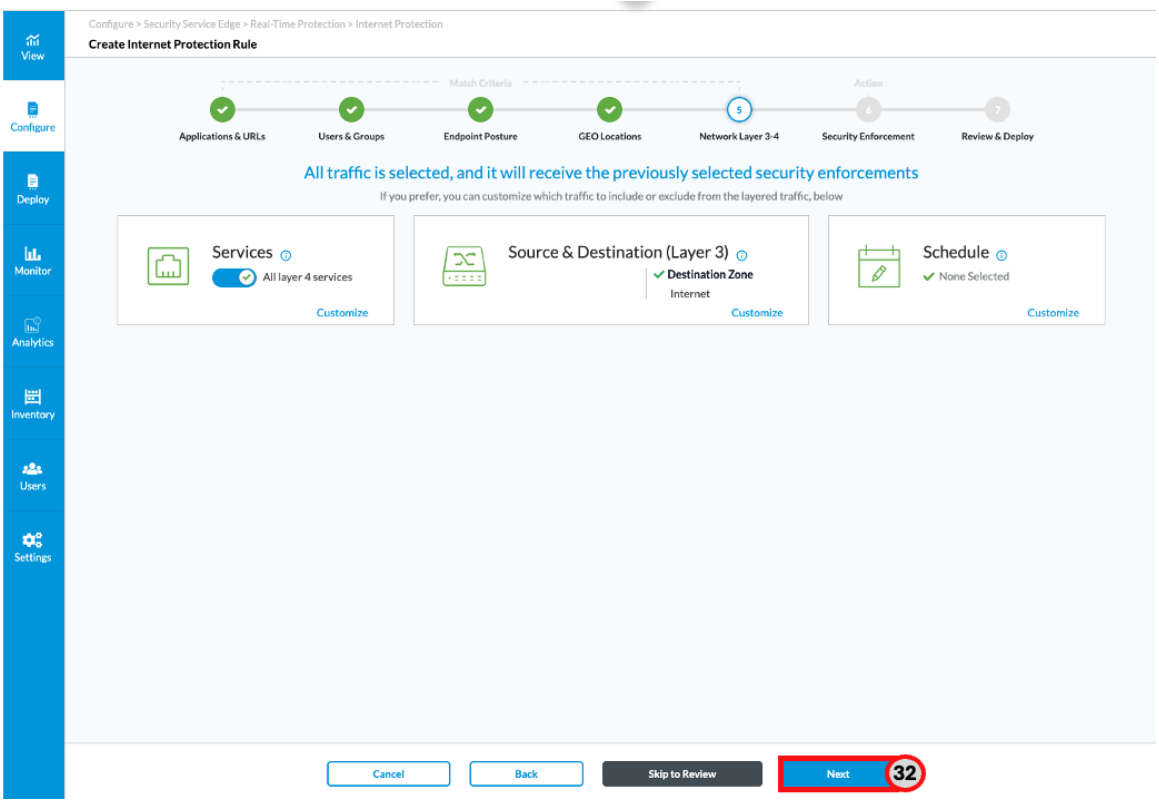
Click **Next** in Endpoint Posture section as no EIP or Entity Risk criteria will be used as match criteria.



Click **Next** in Geo Locations section, as no match criteria is required for IT users traffic. This is enforced from Secure Client Access configured in step 3.

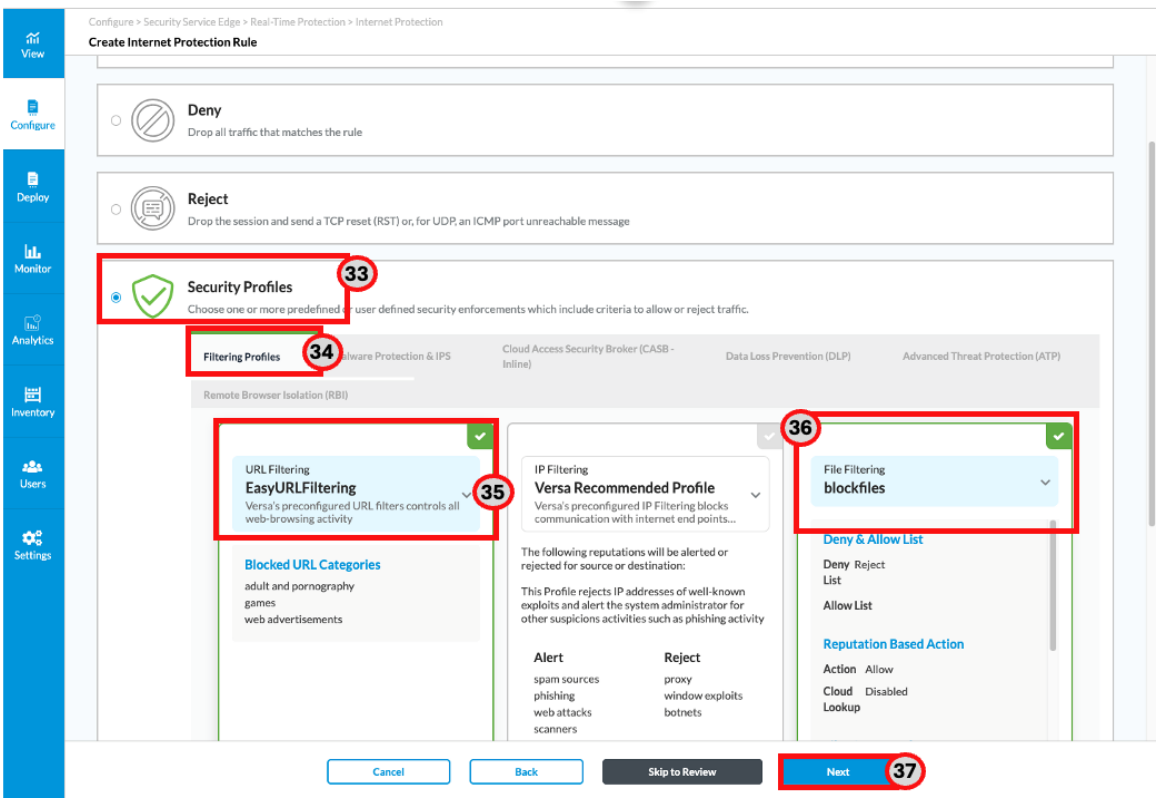


Click **Next** in the Network Layer 3-4 section.

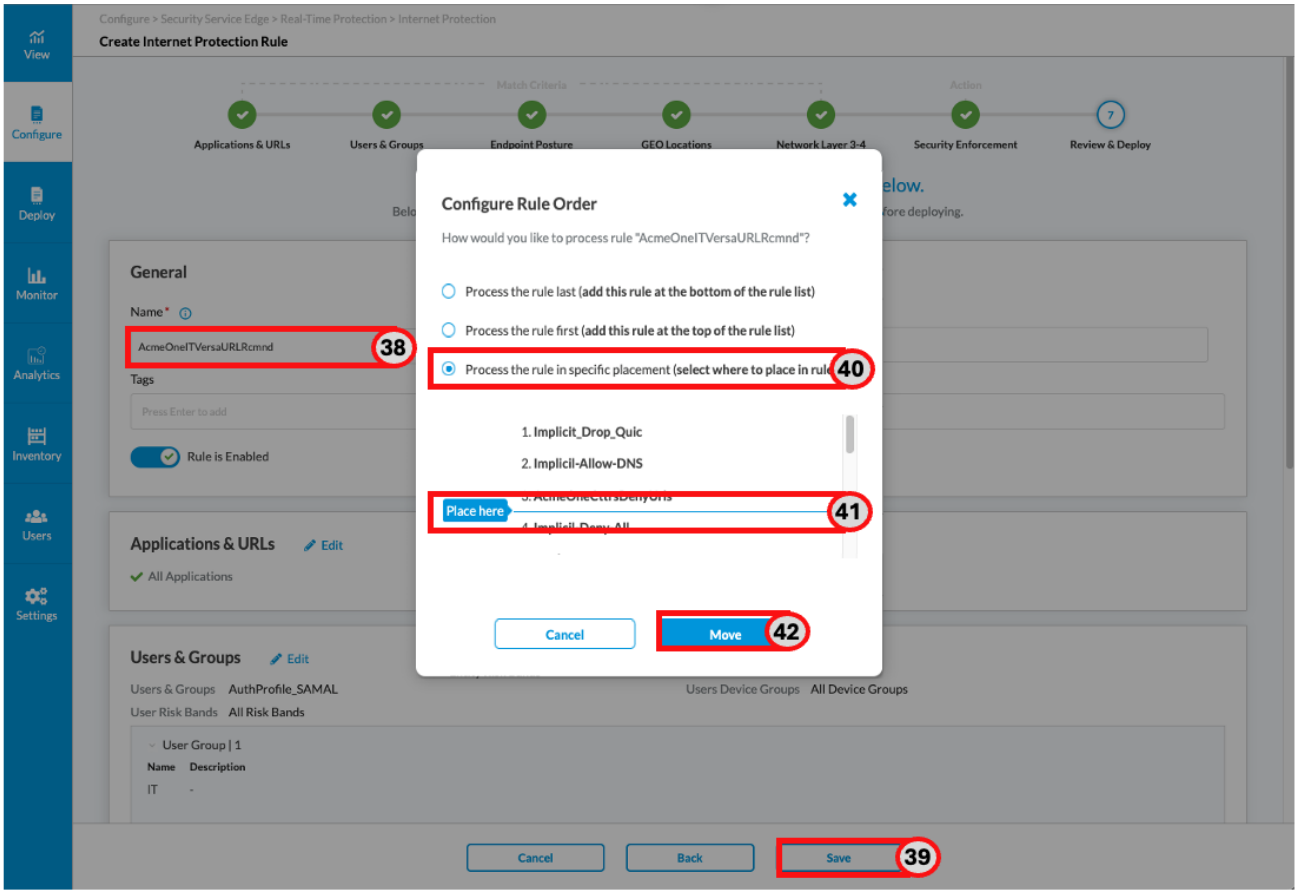


In Security Enforcement, scroll down and select the **Security Profile** radio button and select the **Filtering Profiles**

tab. Check the **URL Filtering** box and from the list select the EasyURLfiltering profile. Check the **File Filtering** box and from the list select the **blockfiles** user defined profile. Click **Next**.



Assign a descriptive **Name** and click in **Save**. In the Configure Rule Order screen, select **Process the rule in specific placement**, then drag the rule to place it before the Implicit Deny All rule and click **Save** .


Configure > Security Service Edge > Real-Time Protection > Internet Protection
Create Internet Protection Rule
Match Criteria
Action
Applications & URLs
Users & Groups
Endpoint Posture
GEO Locations
Network Layer 3-4
Security Enforcement
Review & Deploy
General
Name *
AcmeOneITVersaURLRcmnd
38
Tags
Press Enter to add
Rule is Enabled
Applications & URLs
Edit
All Applications
Users & Groups
Edit
Users & Groups AuthProfile_SAMAL
User Risk Bands All Risk Bands
Users Device Groups All Device Groups
User Group | 1
Name Description
IT -
Cancel
Back
Save
39
Configure Rule Order
How would you like to process rule "AcmeOneITVersaURLRcmnd"?
Process the rule last (add this rule at the bottom of the rule list)
Process the rule first (add this rule at the top of the rule list)
Process the rule in specific placement (select where to place in rule
40
1. Implicit_Drop_Quic
2. Implicil-Allow-DNS
Place here
41
Cancel
Move
42

Appendix A – Authentication Methods Configuration

LDAP Active-Directory

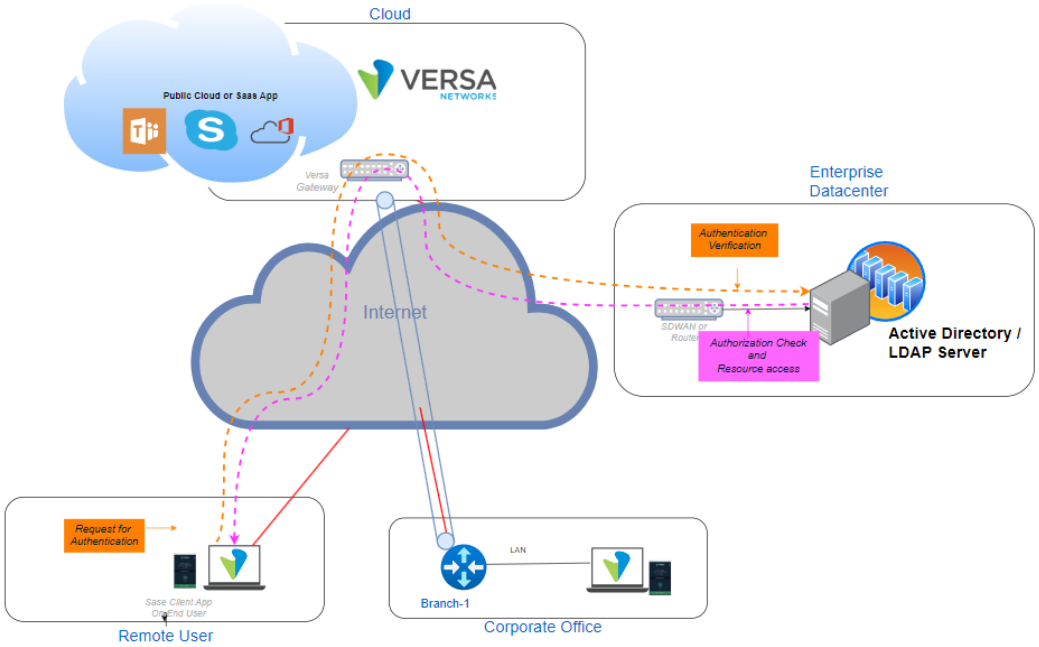
LDAP is a client-server protocol that enables network devices to access directory services storing attribute-based information, allowing for user authentication through querying a directory server. The SSE gateway queries the LDAP server to validate the user, granting or denying access based on the authentication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

Scenario

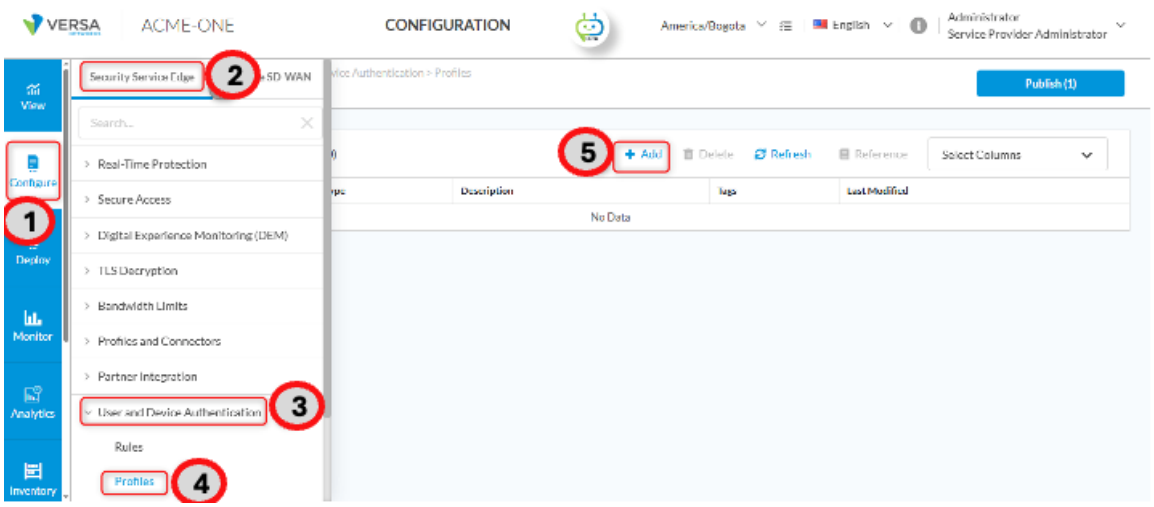
In most enterprise environments, user authentication is centralized through AD/LDAP servers in the data centre. In cases of VSPA or VISA, users securely connect to the SSE gateways using the Versa SASE Client from remote locations, branches, or corporate offices. Authentication requests from the SASE 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.

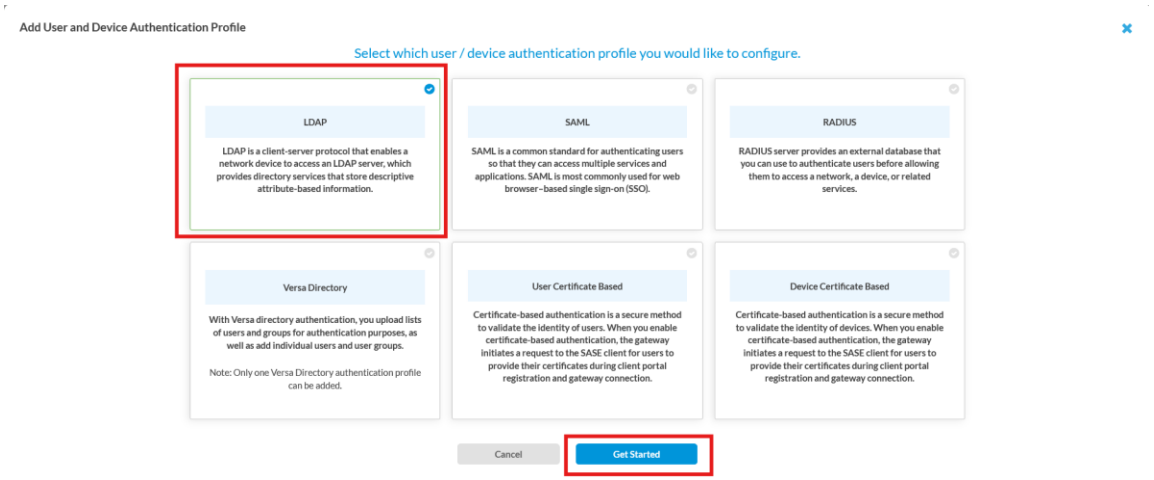
This configuration ensures consistent, identity-based access for both remote and on-premises users, thereby facilitating streamlined policy enforcement based on identity enforcement.



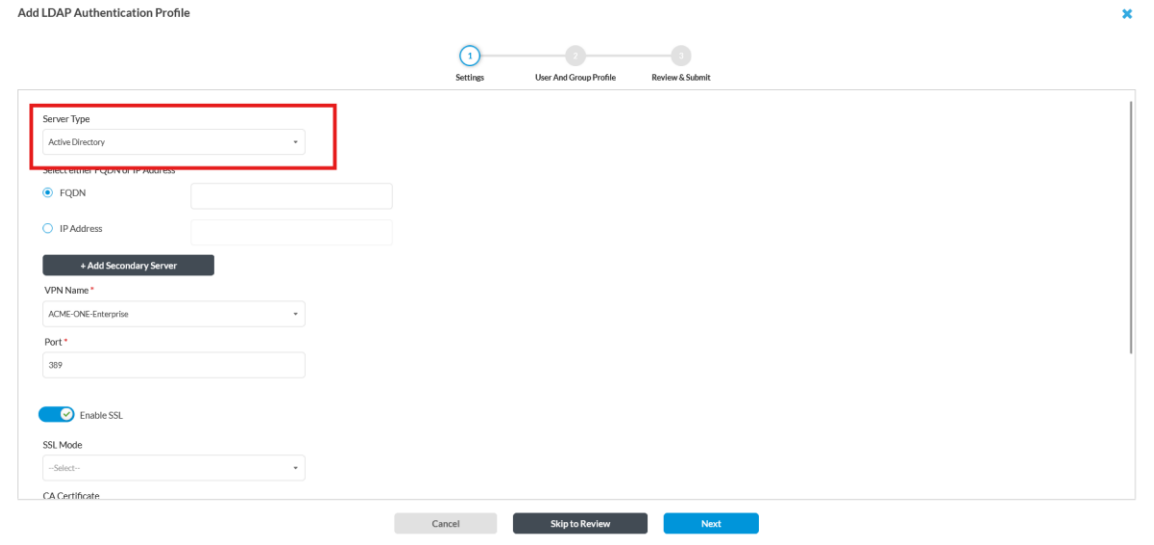
Navigate to User and Device Authentication Configuration Go to: Configure (1)> Security Service Edge (2) > User and Device Authentication (3) > Profiles (4) then "+ Add" (5)



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



From the Server Type dropdown, select Active Directory

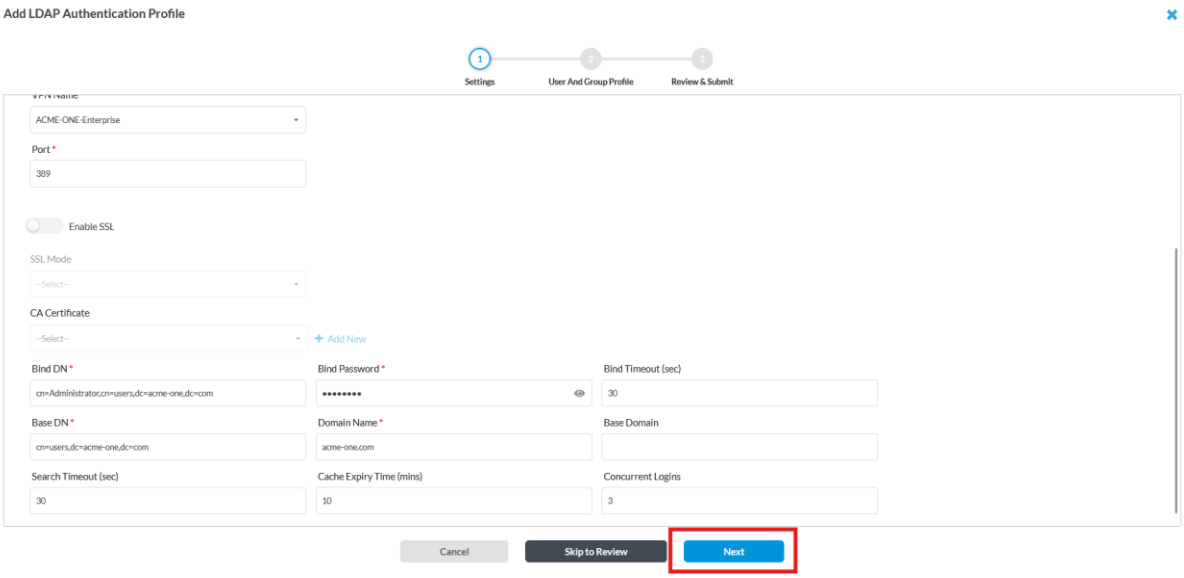


The following section explains all parameters for LDAP Authentication Profile configuration.

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 organizational 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



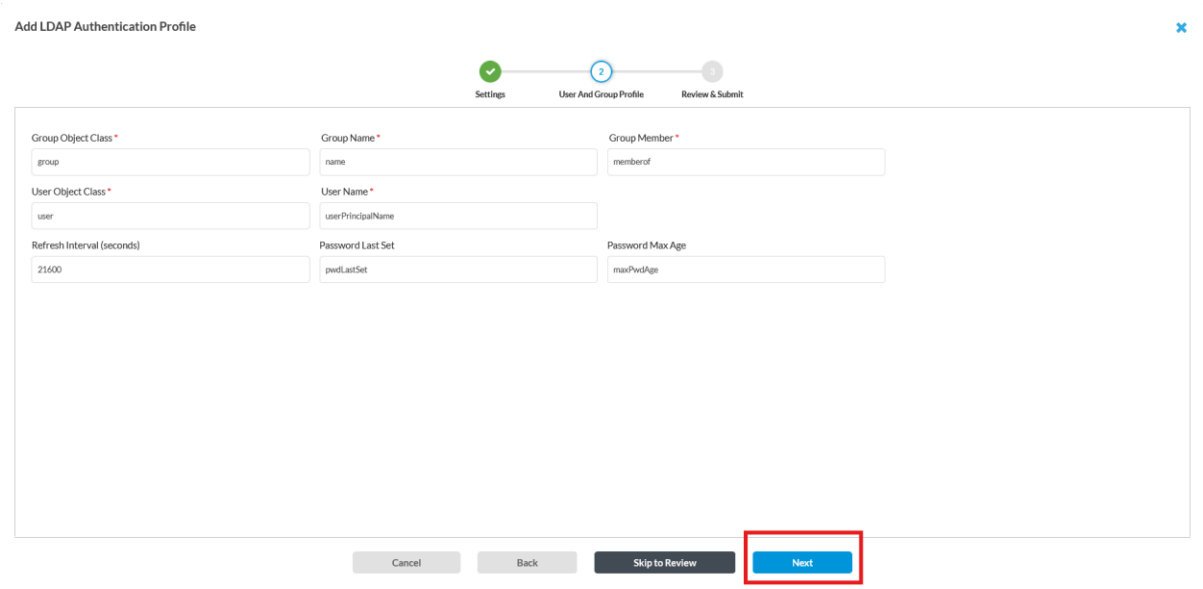
Next, complete the required fields:

LDAP Object and User Attributes

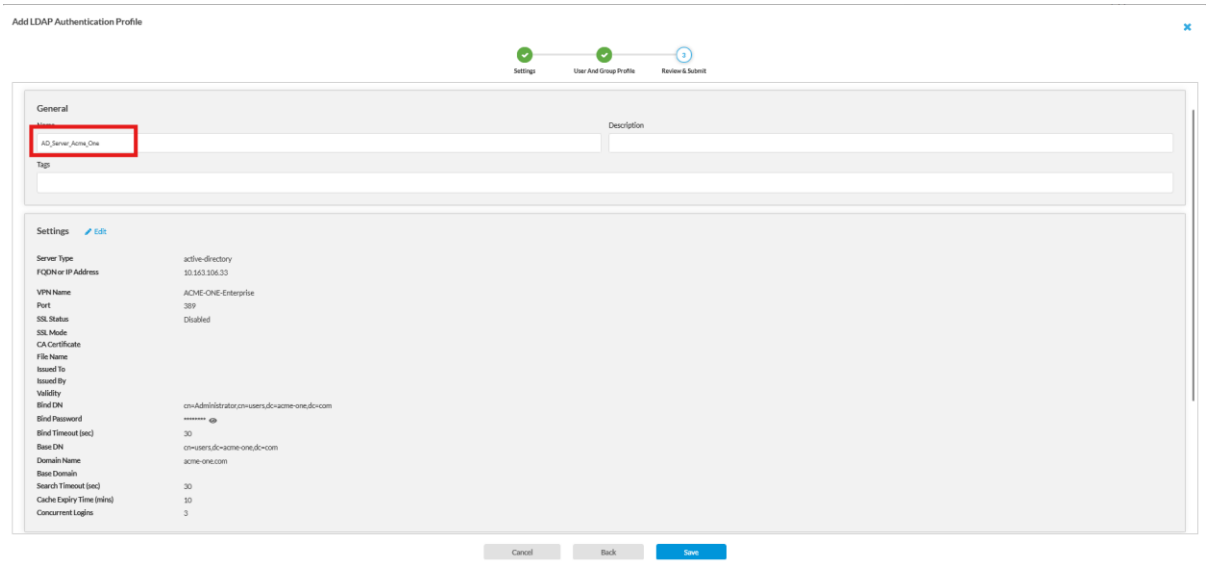
Parameter	Value / Default	Description
Group Object Class	group	Standard AD object class for security and distribution groups. Required to identify groups in the directory.
Group Name	name	Attribute that defines the display name of a group. Used by Versa to match groups during policy evaluation.
Group 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.

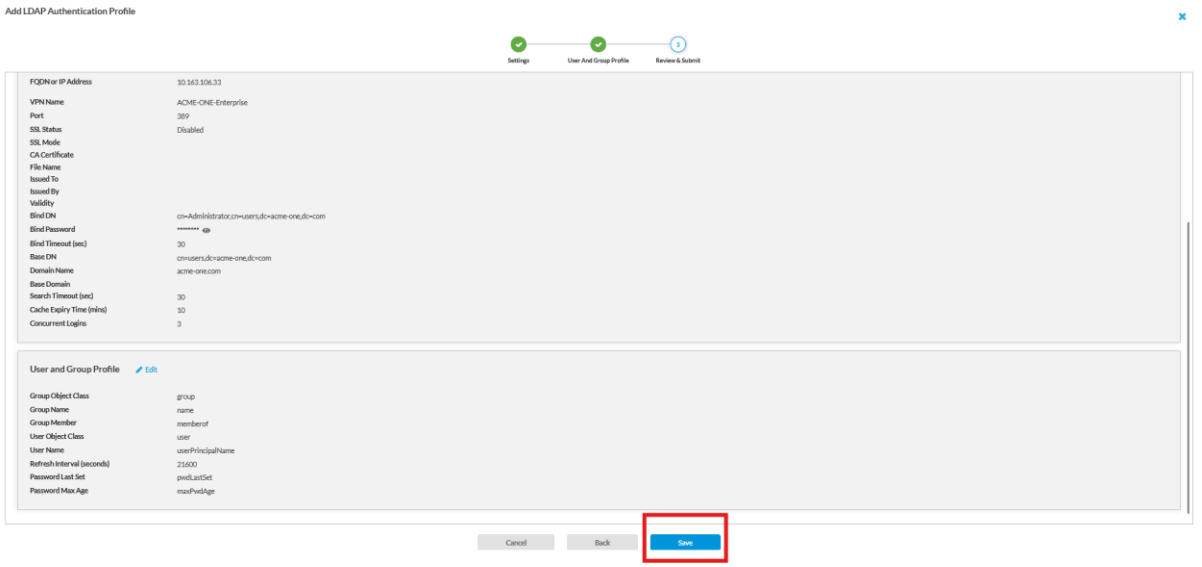
click **Next** to proceed.



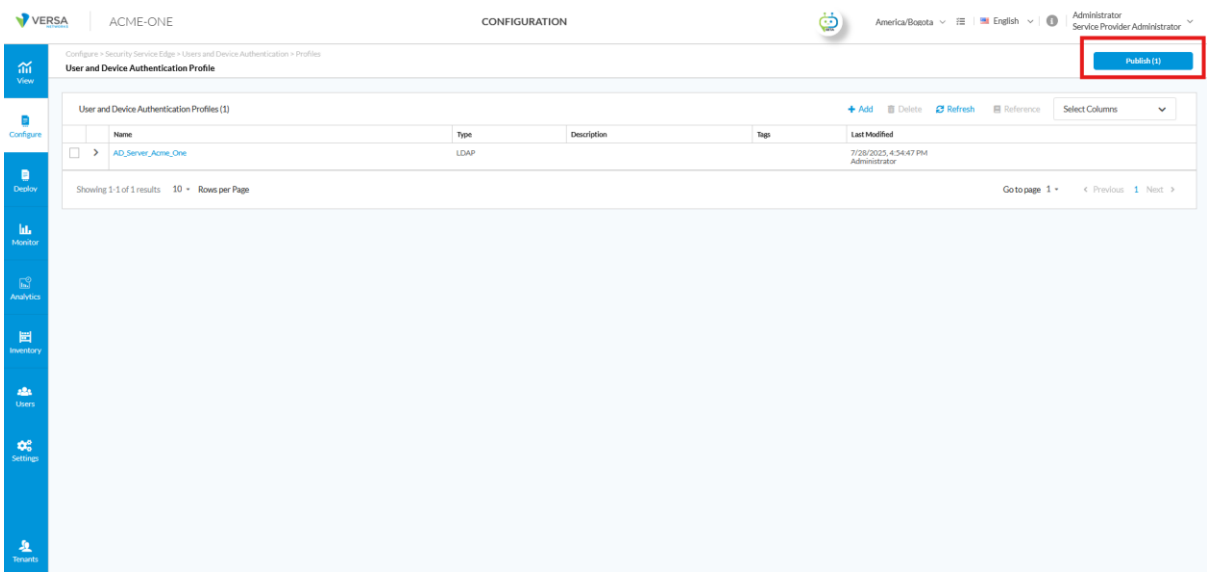
Next, fill in the **Name** field with a descriptive reference, such as *AD_Server_ACME-ONE*, and review all parameters to ensure they are correctly configured.



Then Save.



Go to Publish



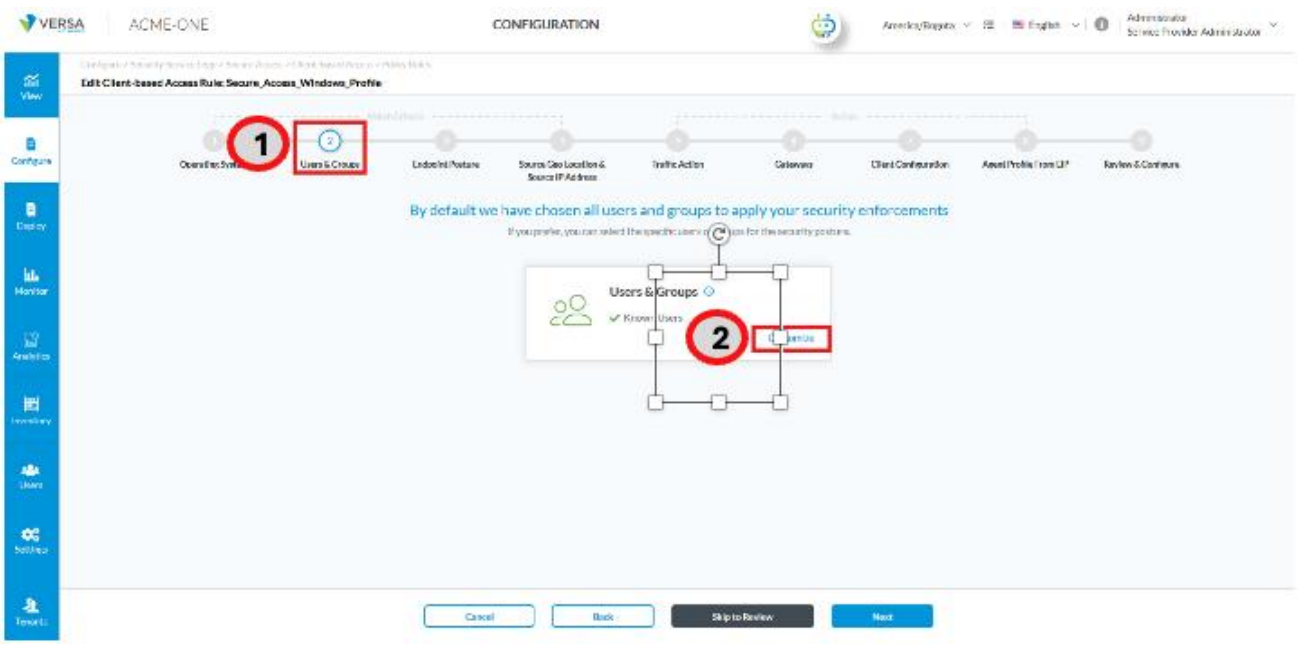
After creating and Publishing the Authentication Profile, you must apply them to the Secure Access Client policy to enforce authentication and apply the corresponding security policies.

Navigate to:

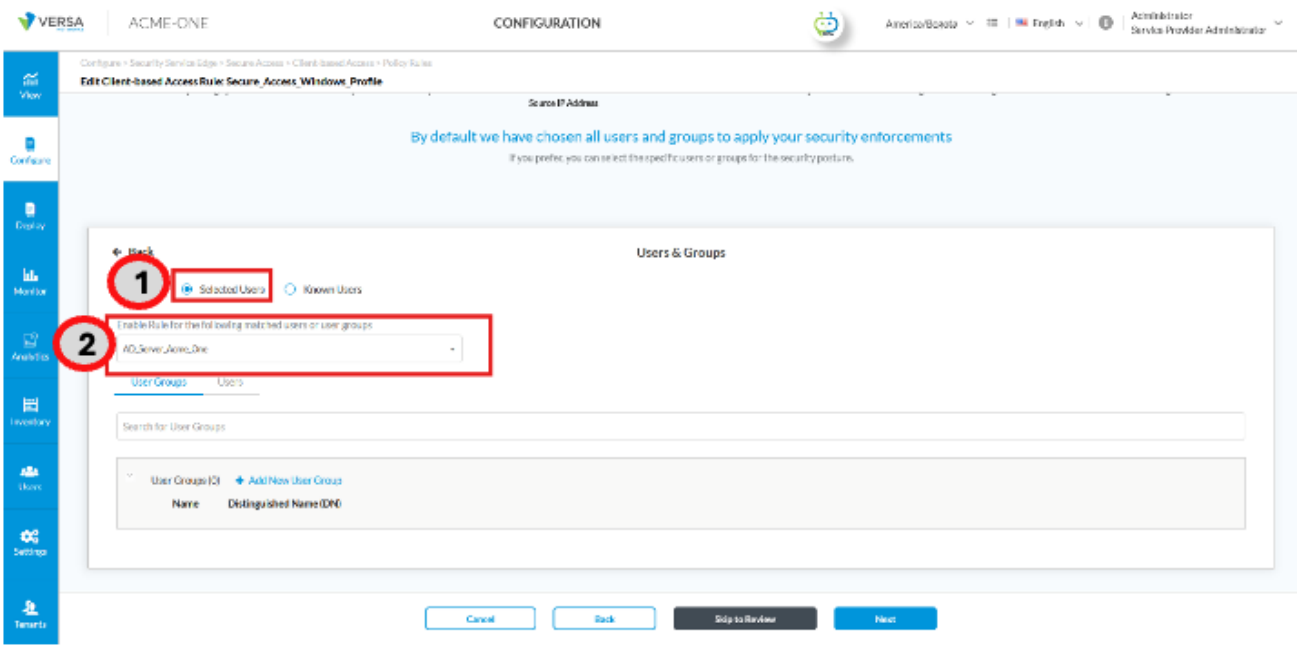
Configure > Security Service Edge > Secure Access > Client-based Access > Rules.

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.

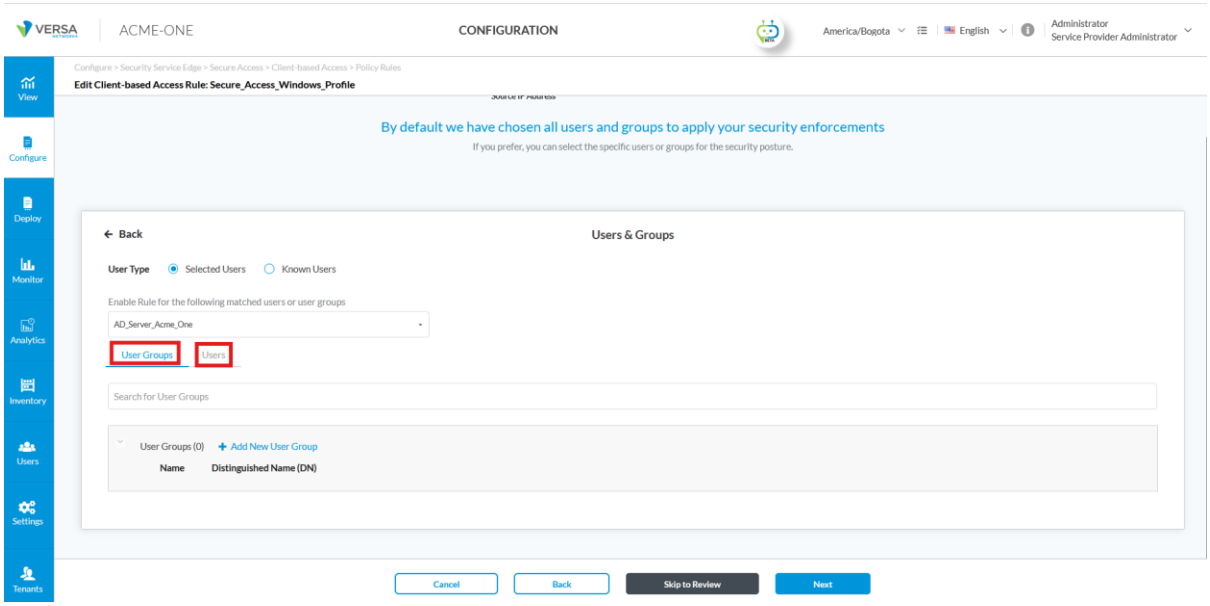


In the **Users & Groups** customization panel, select **Selected Users** as the user type. Then, under **Enable Rule for the following matched users or user groups**, choose the appropriate authentication profile (Example., AD_Server_Acme_One). This allows the policy to enforce access control based on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



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

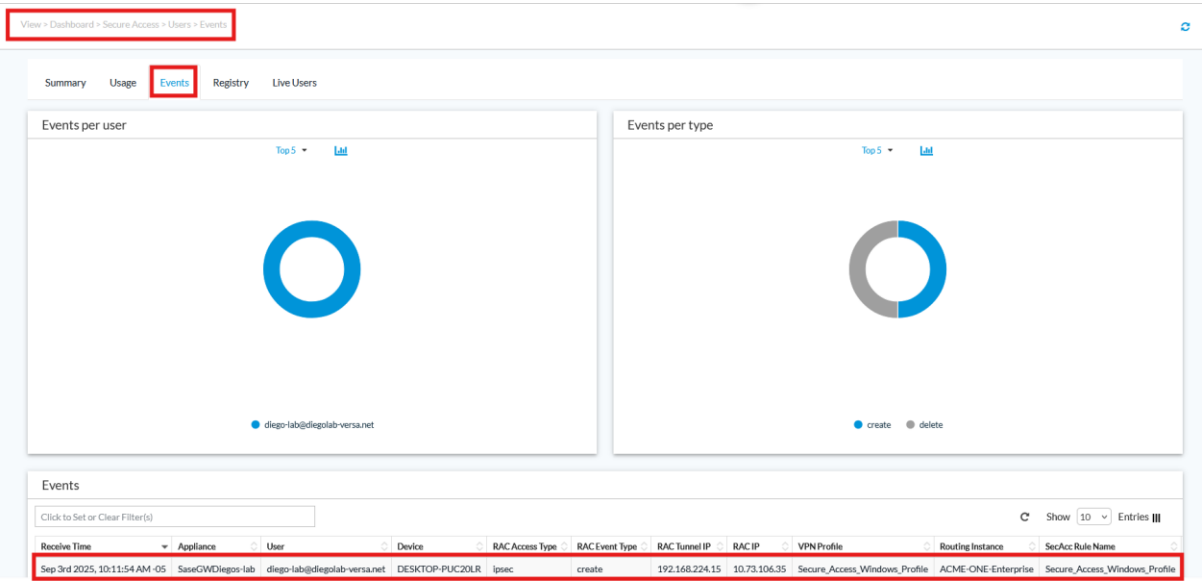
Use the **User Groups** or **Users** tabs to select the desired entries.



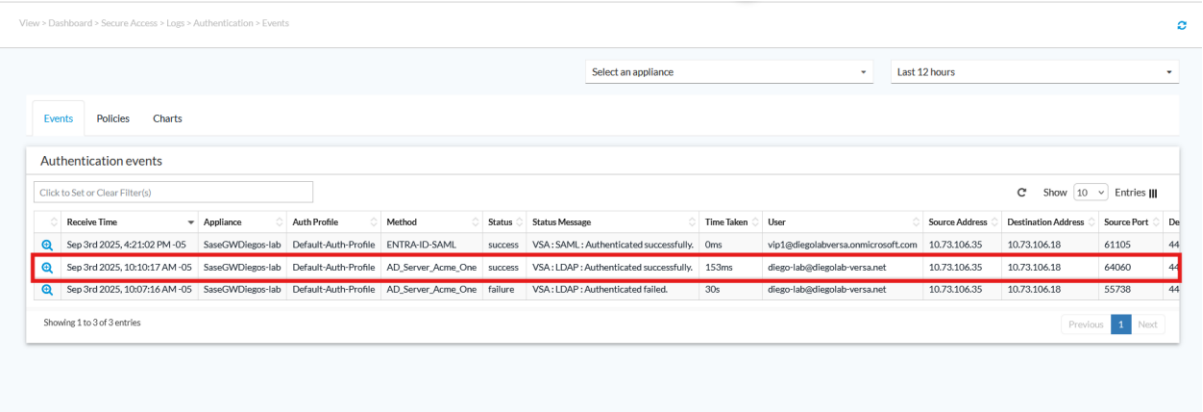
After reviewing all configuration sections, click **Save** to apply the settings to the current Secure Access Profile. Then go to the **Publish** section at the top-right corner of the screen and click **Publish**.

VERIFICATION

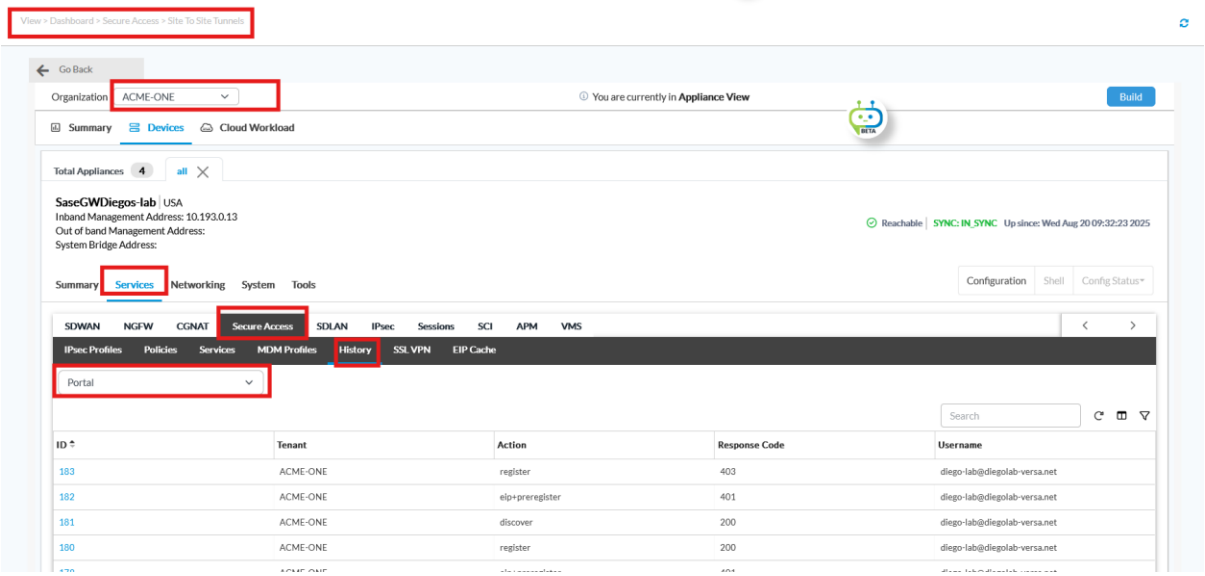
When a user connects to the Gateway and LDAP/AD authentication is enabled, the Secure Access Gateway forwards the authentication request to the configured LDAP server profile. The user credentials are validated against Active Directory, and upon success, group or role attributes are retrieved to enforce access policies. 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.

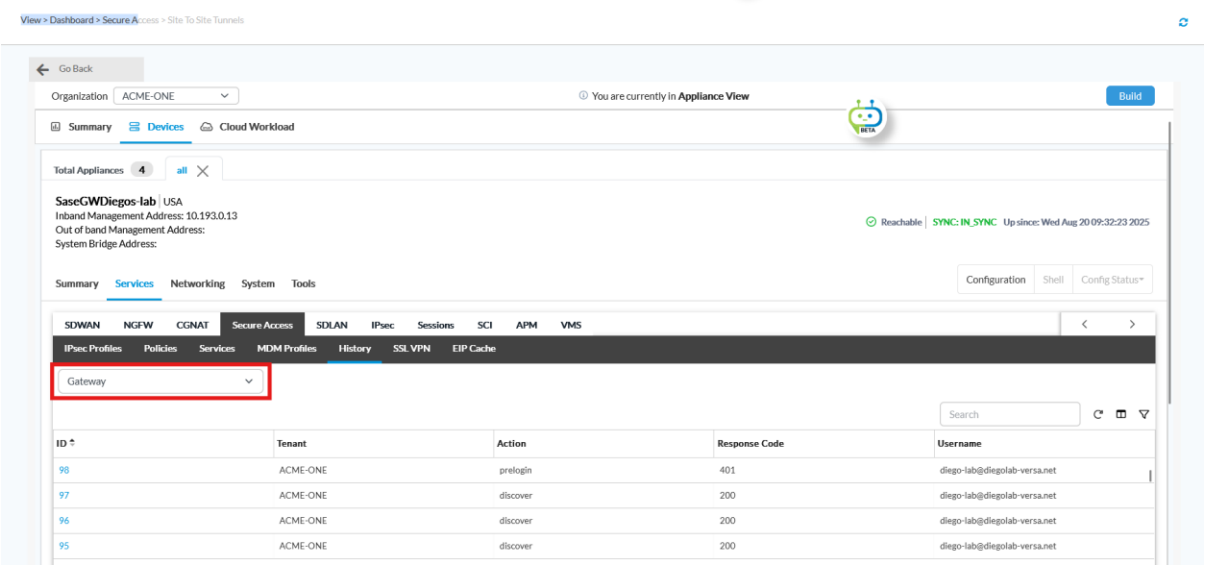


You would see the method used and the authenticated user in the Authentication Logs under **View > Dashboard > Secure Access > Logs > Authentication > Events**.



Under View > Dashboard > Secure Access > Site To Site Tunnels Click on View Advance Monitor in the Gateway, Choose the **Organization** then **Services > Secure Access > History** drop down **Portal or Gateway** tab shows the authentication flow with response codes (e.g., *200* for success, *401* for failure).





Additionally, administrators can confirm active sessions and mapped LDAP 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 brief
                                                    TIME
                                            SESSION TO      EXPIRATION
IP ADDRESS      NAME                        STATUS  HITS    EXPIRY  MODE
-------------------------------------------------------------------------------
192.168.224.15  diego-lab@diegolab-versa.net  Live    262     60      inactivity

[ok][2025-09-03 09:35:21]
admin@SaseGWDiegos-lab-cli>
```

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.

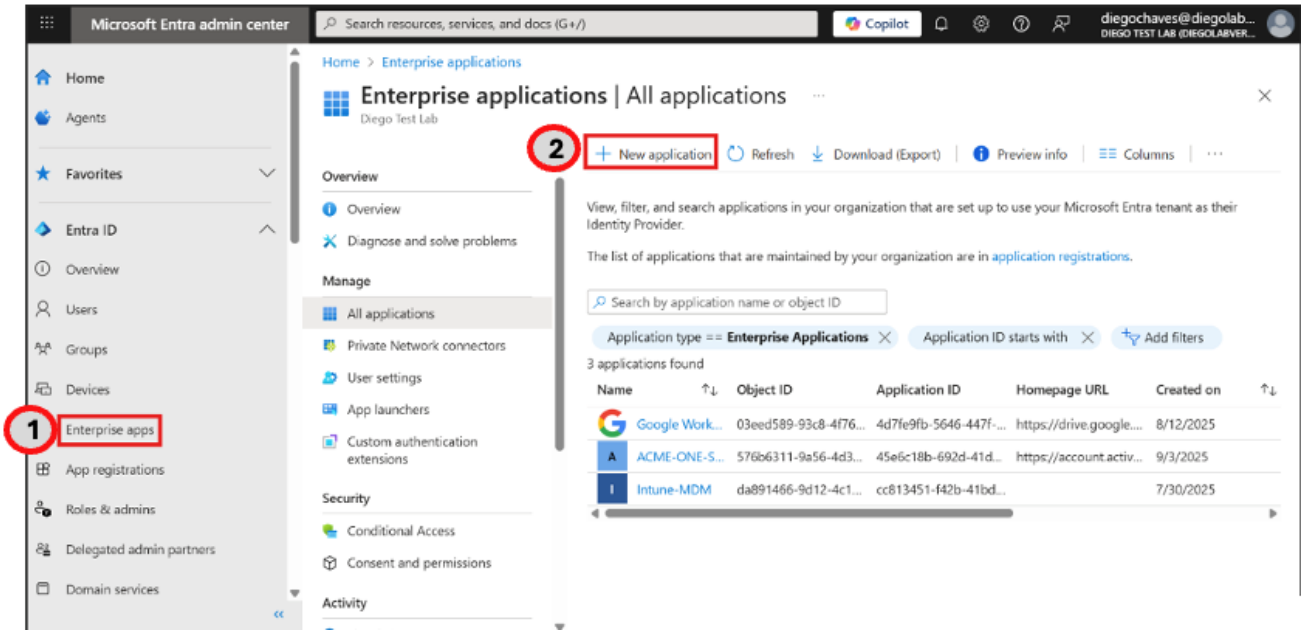
Entra ID Configuration

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**.



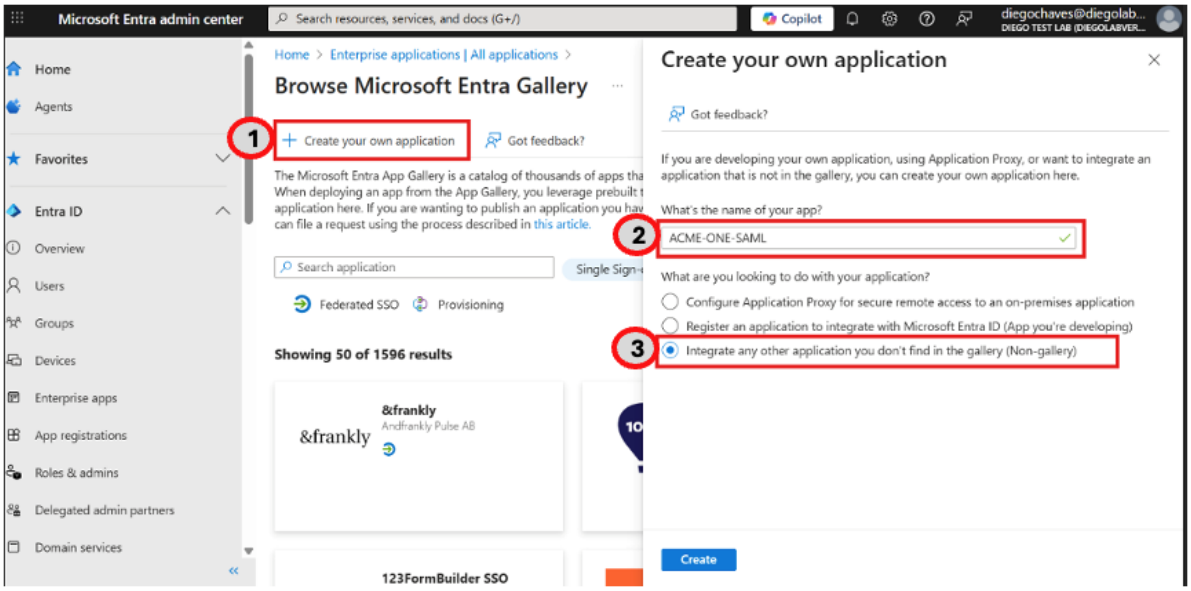
2. Select **Create a new application**

Click **+ Create your own application**.

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

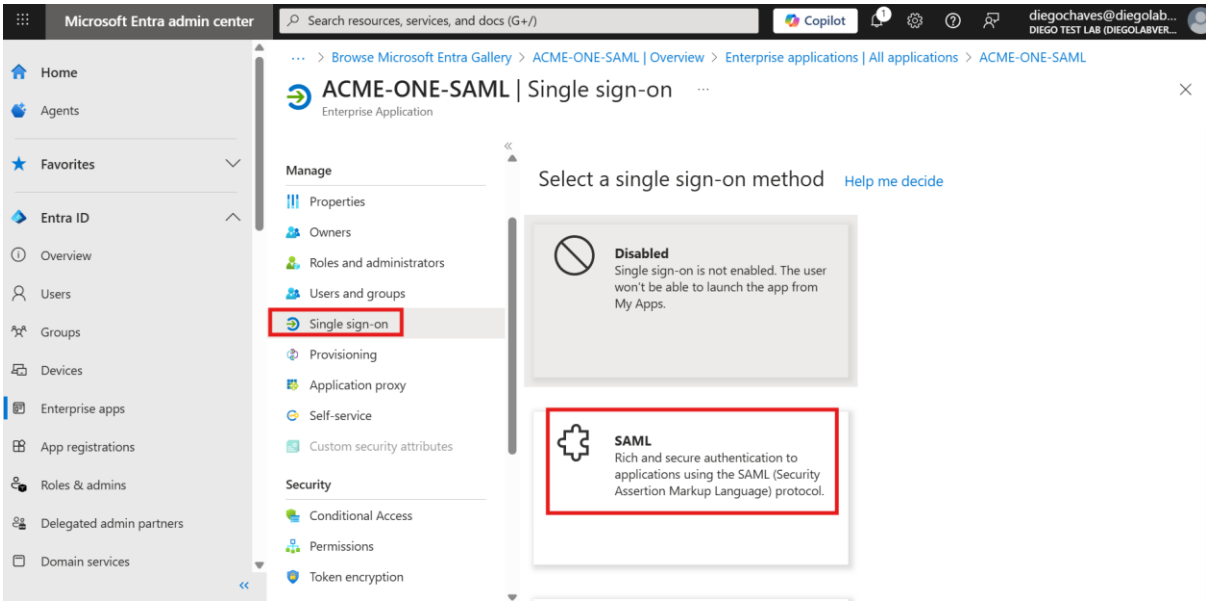
Select **Integrate any other application you don't find in the gallery (Non-gallery)**.

Click **Create**.



3. Set up SAML-based SSO

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



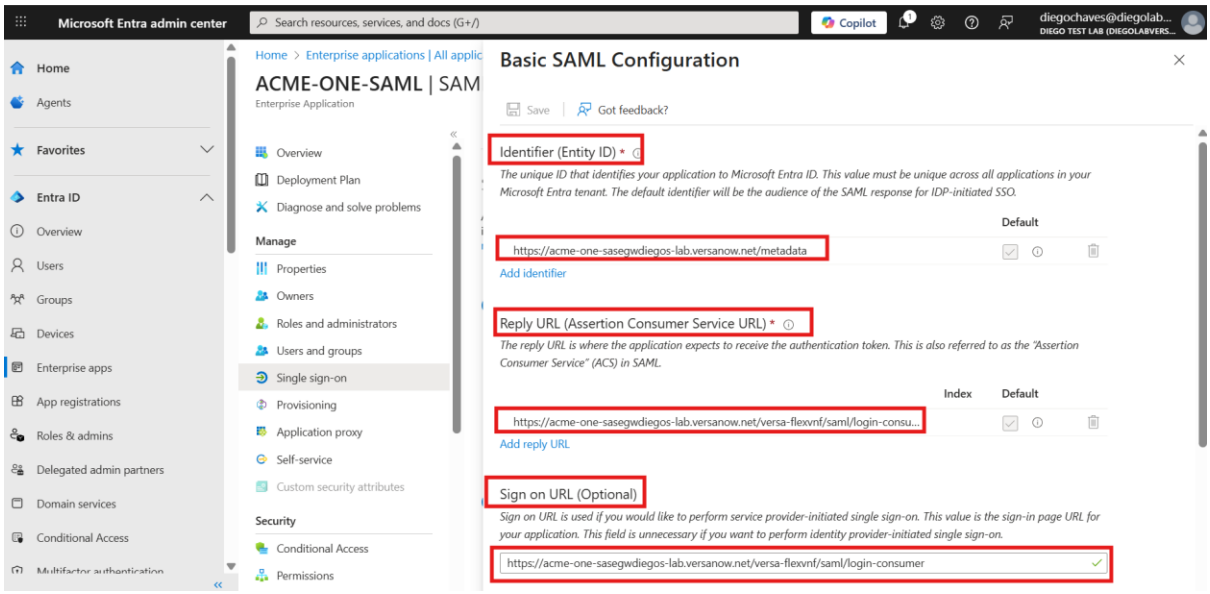
4. In the SAML settings, enter information for the indicates fields.

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-577374553241106028824600 9139" 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>
```

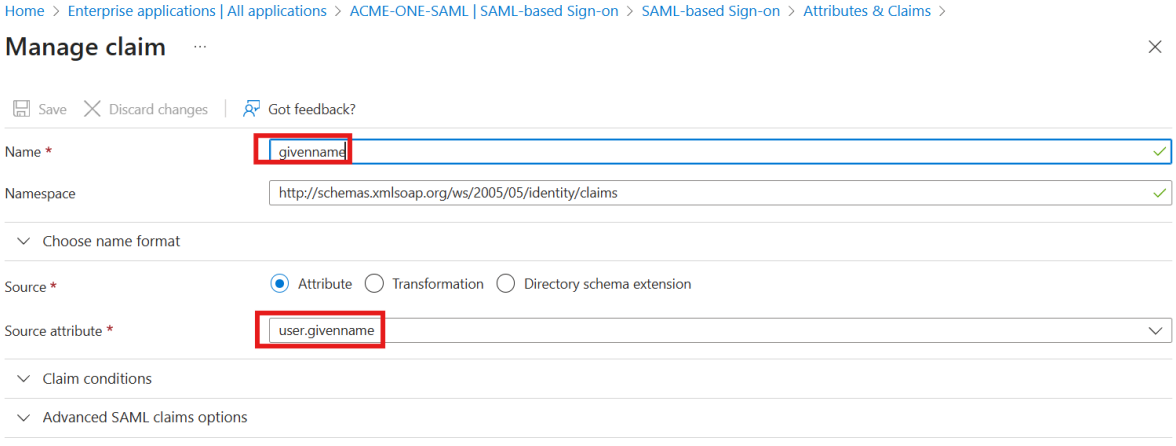
5. Configure the parameters as shown in the previous table, in Basic SAML Configuration and then click **Save**.

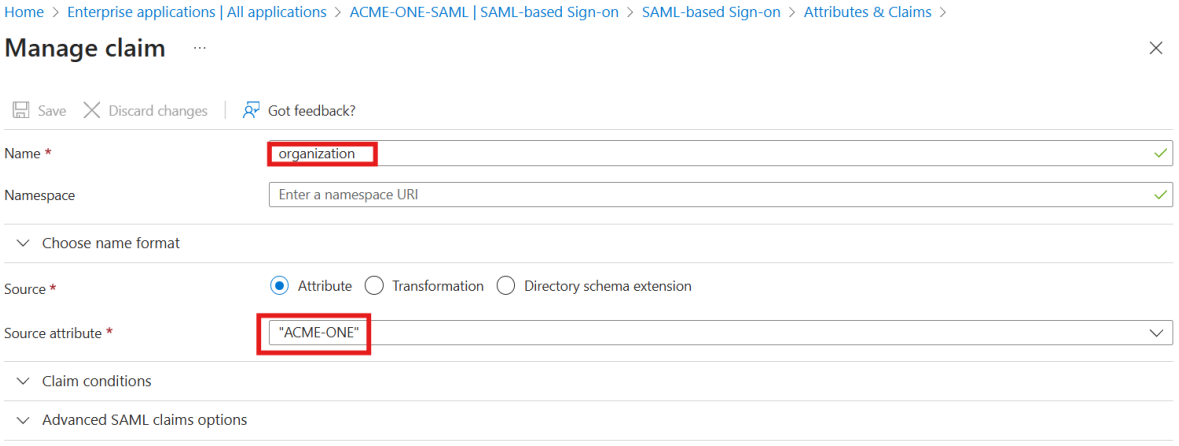


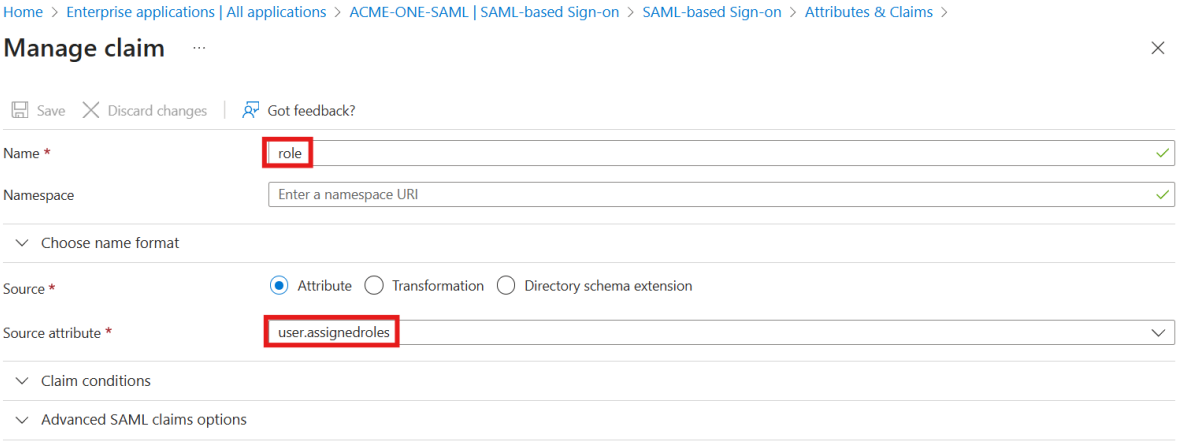
6. Define **Attributes & Claims**.

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

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

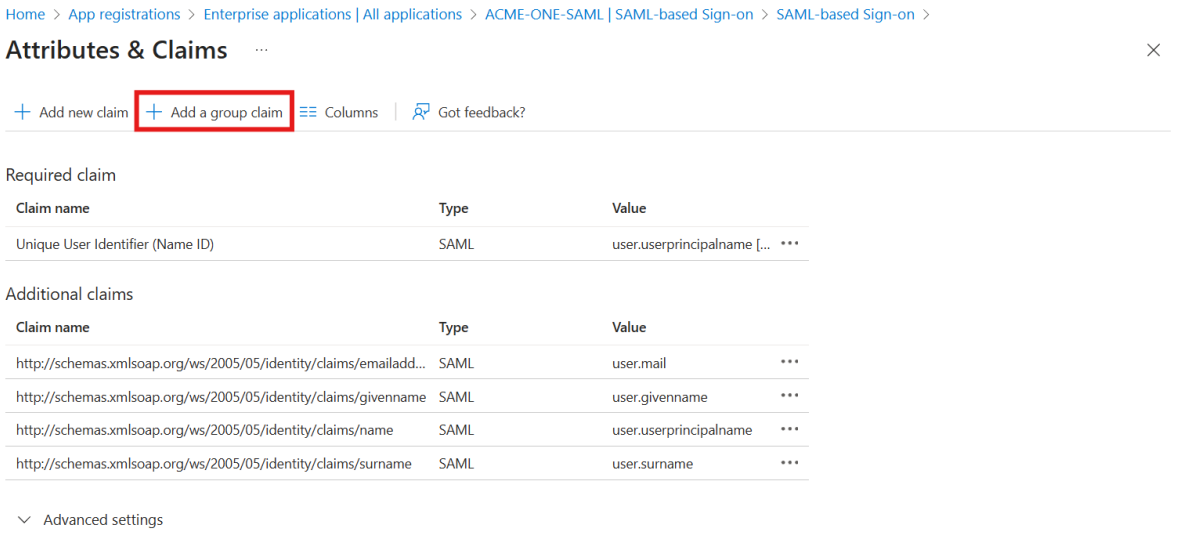




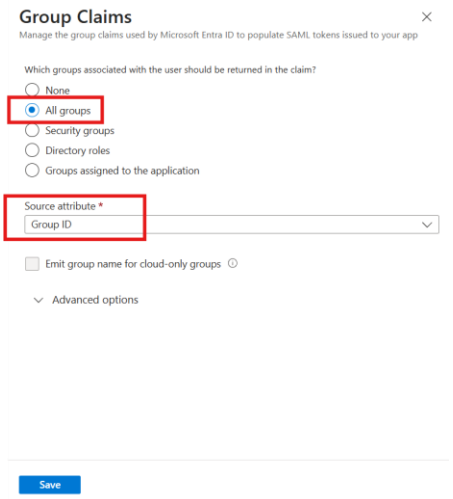


7. Configure **Group Claims referring** to previous table **Group Attribute Statements**.

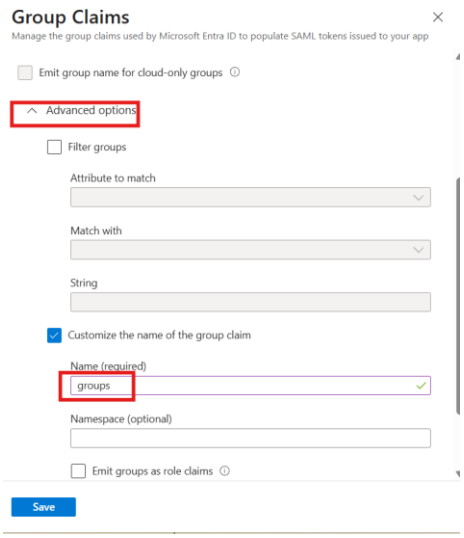
- Click + Add a group Claim



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



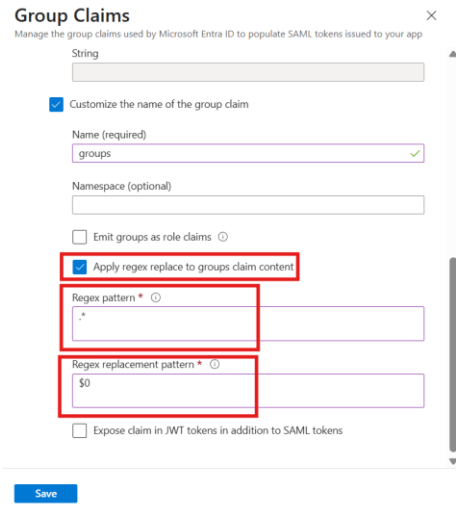
- Click **Advance options** then Enable **Customize the name of the group claim** > set name as groups.



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

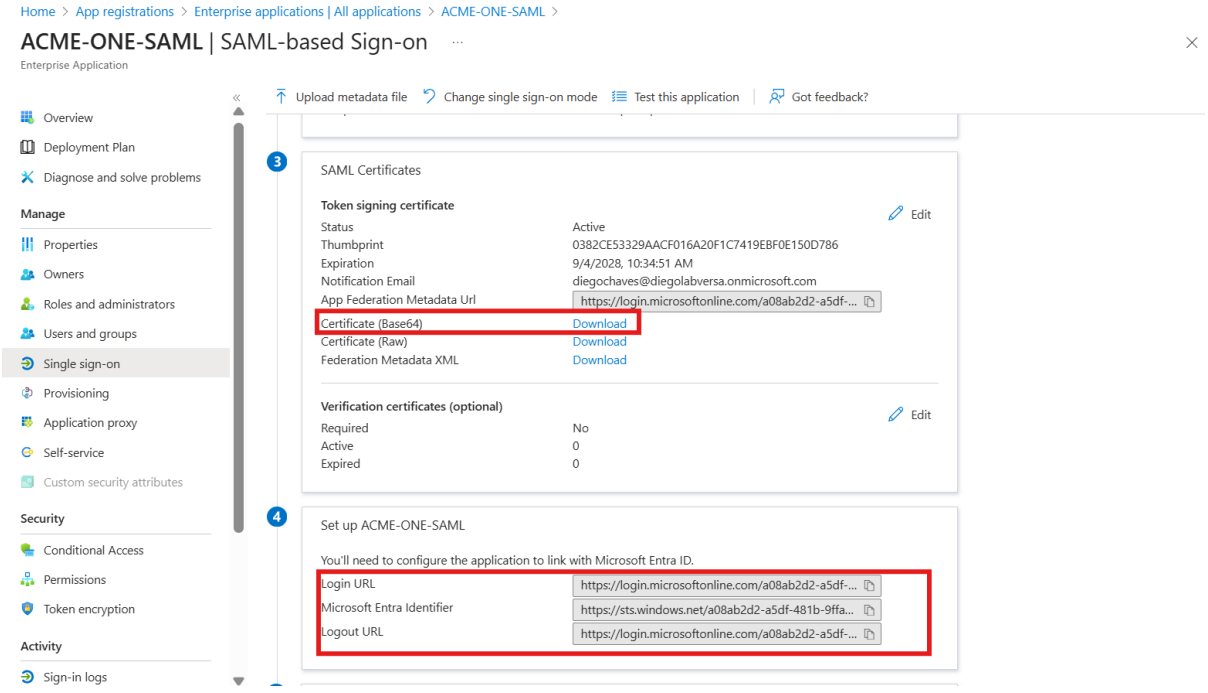
I. Pattern: .*

II. Replacement: $0



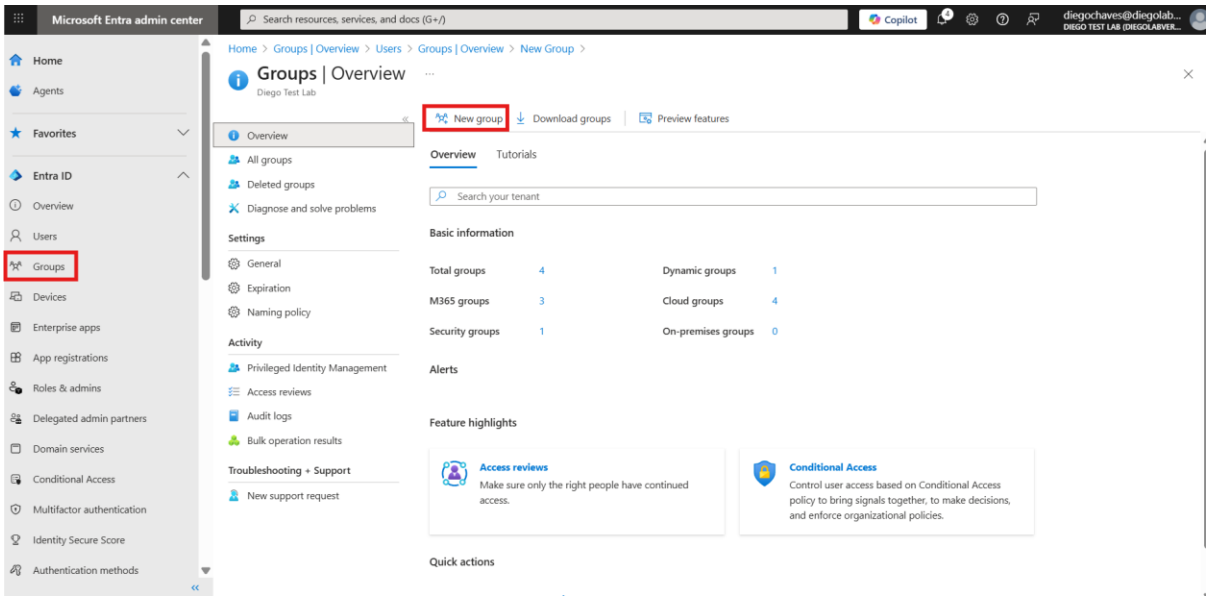
8. Retrieve SAML Integration Details

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.

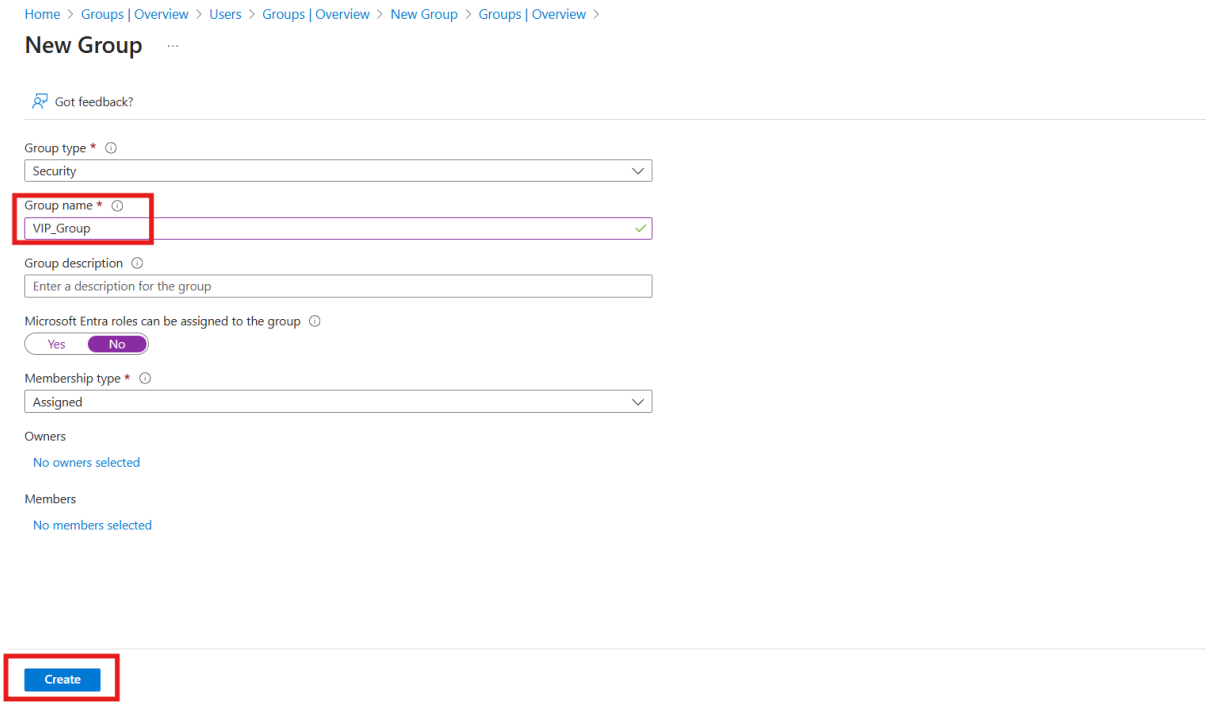


9. Create the Groups and Users.

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



In the name field, enter a group name

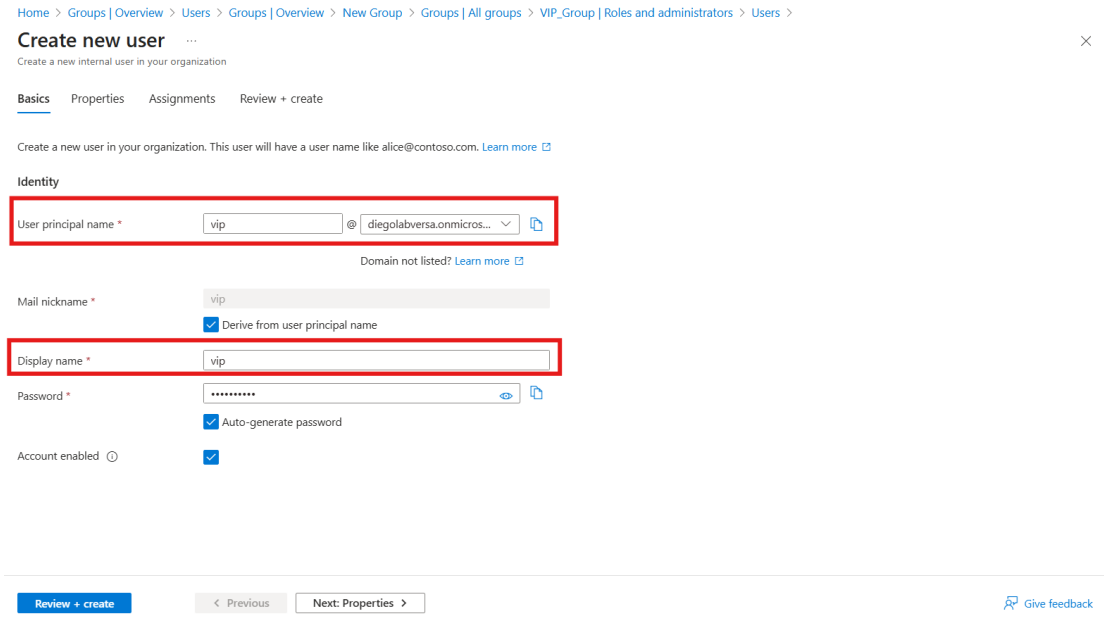


Refresh the page and click to the newly created group "**VIP_Group".** To create users Navigate to Navigate to Microsoft Entra admin Center > user, click New User. In the Basics tab, define the User Principal Name (UPN) and Display Name.

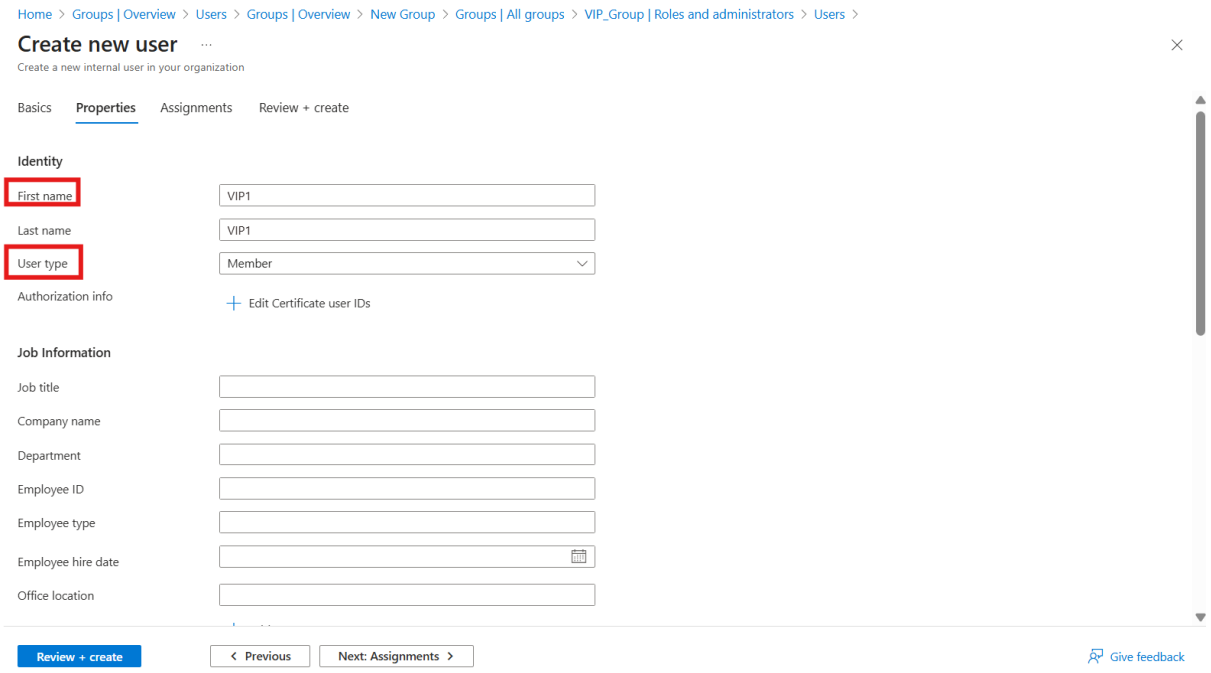
Example:

UPN → vip@acme-one.onmicrosoft.com

Display Name → vip



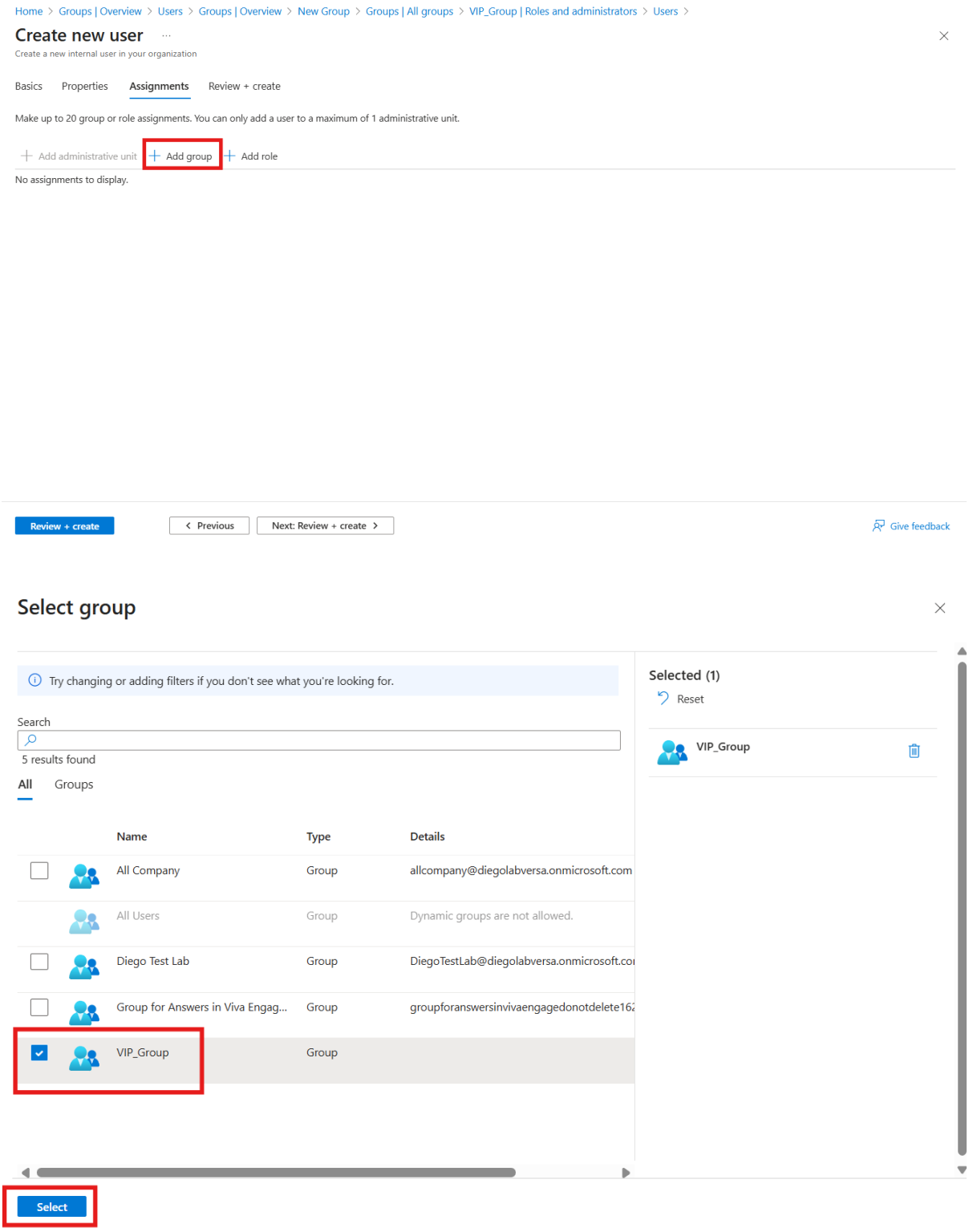
In the **Properties** tab, add first name, last name, and user type (Example, **Member**). Other fields such as job title or department are optional but can be filled for organizational use.



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

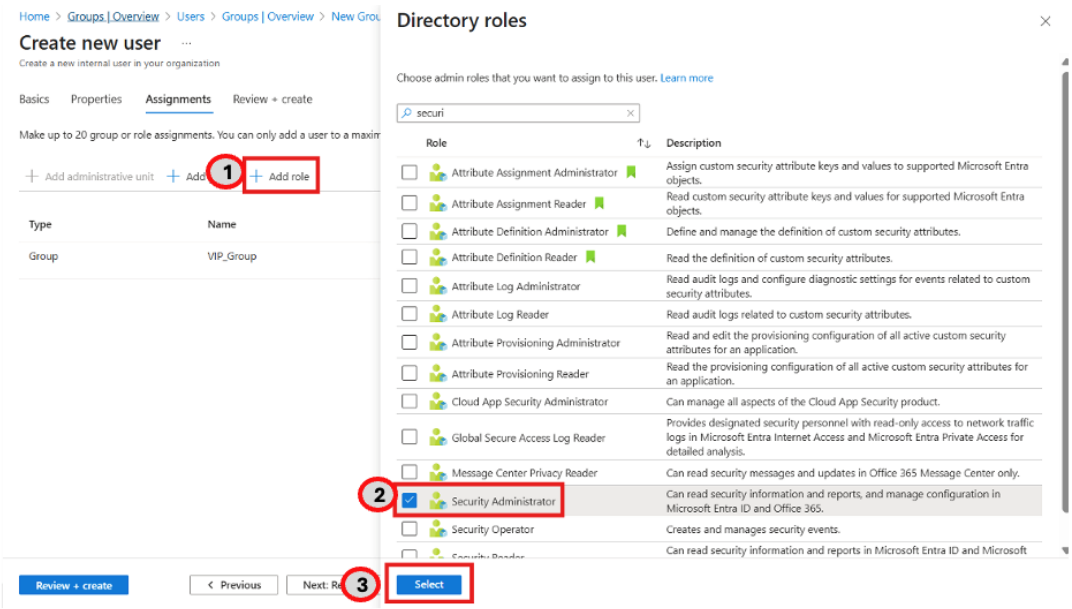
Select the previously created **VIP_Group** (or any other relevant group).

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.

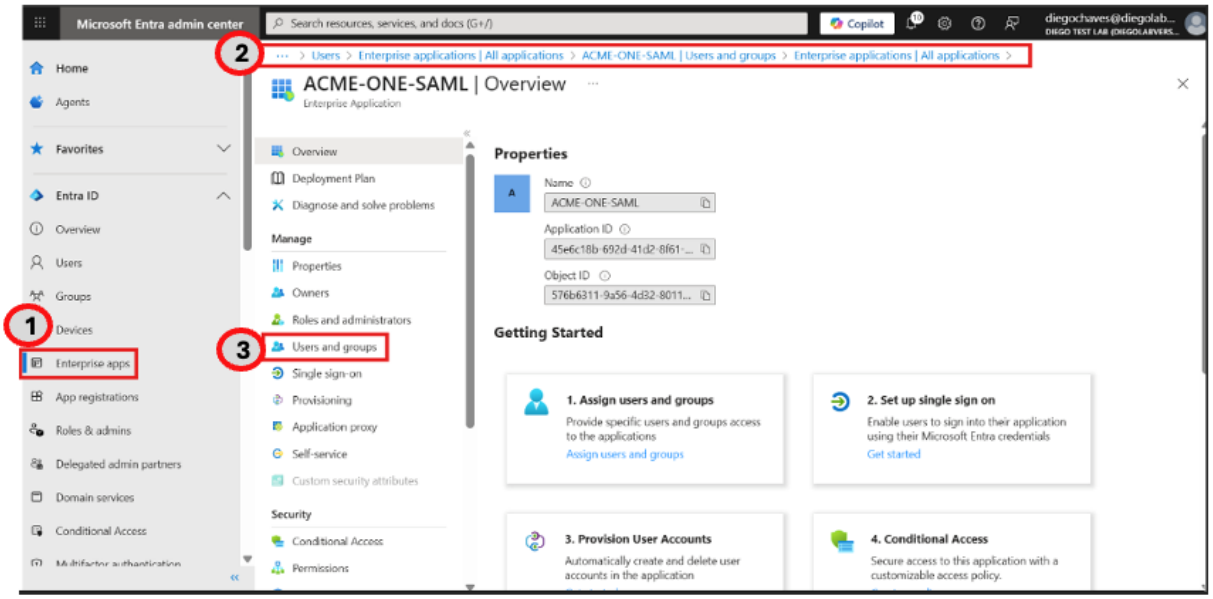
Roles are optional for SAML authentication itself but useful if role claims are mapped into SAML tokens for authorization in downstream apps.



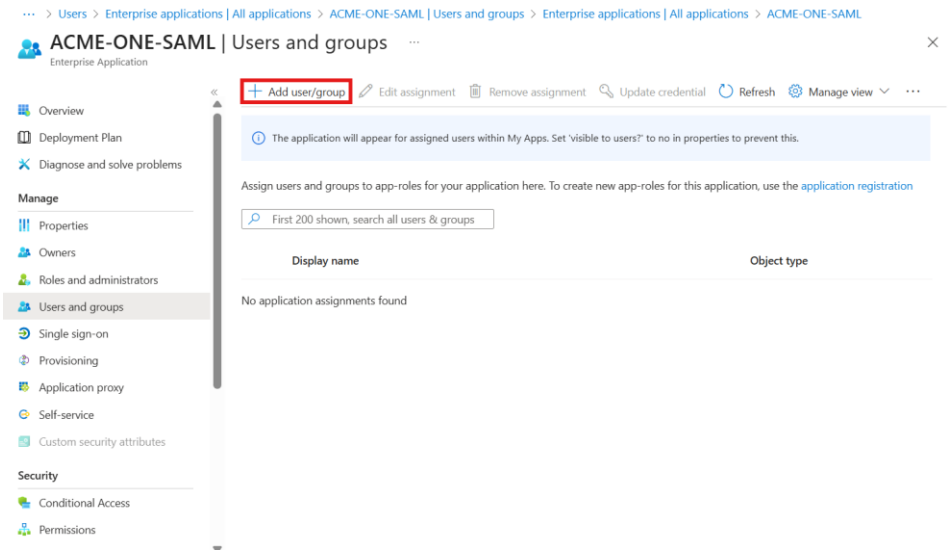
Review & Create

- 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.

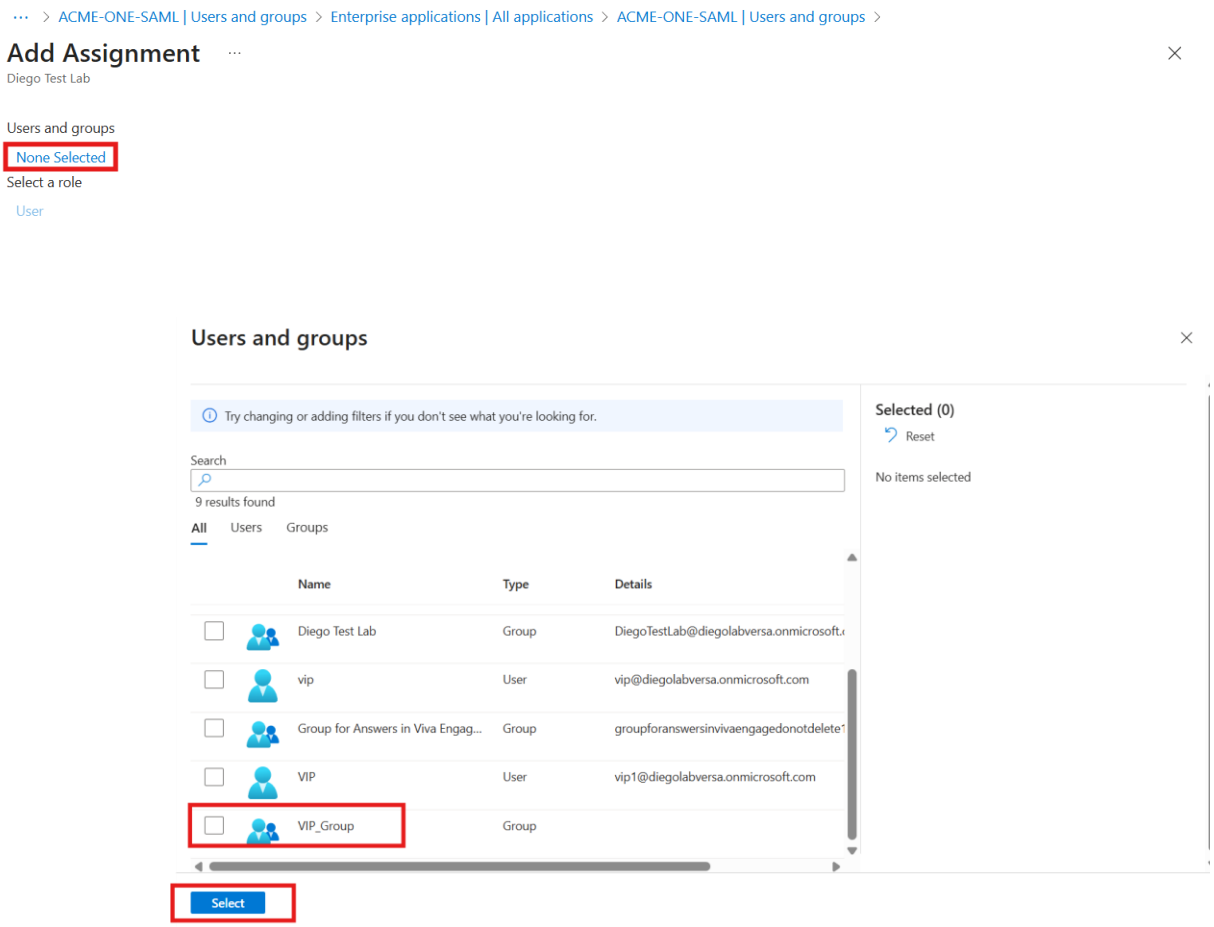
10. Navigate to the **Enterprise Apps** (Example., ACME-ONE-SAML) > **Users and groups**.



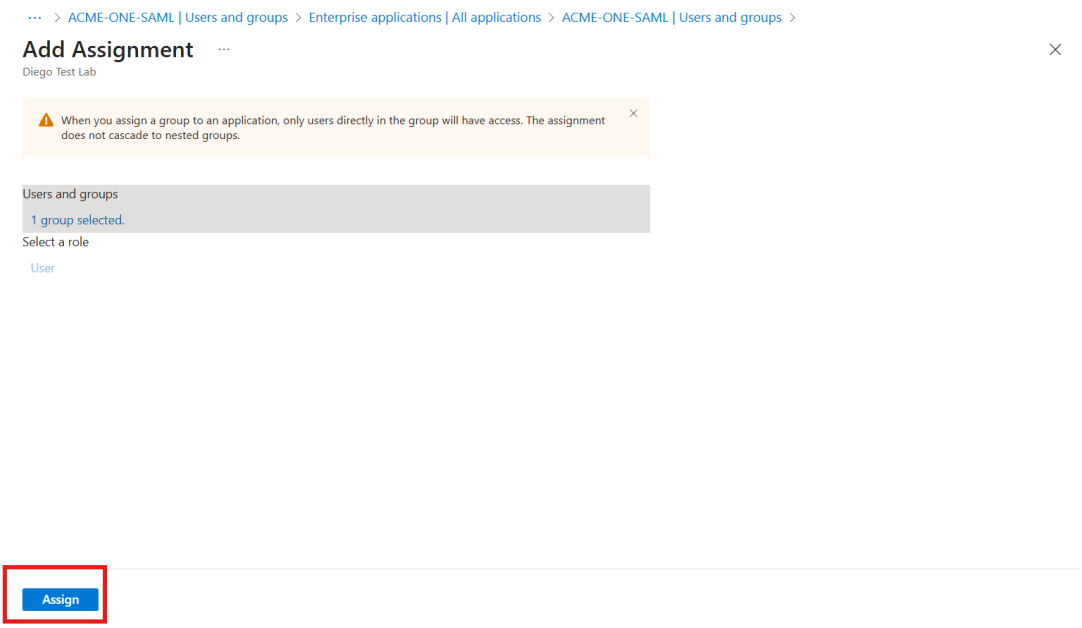
11. Click **Add user/group**, search for the group (Example, VIP_Group), select it, and assign it to the application.



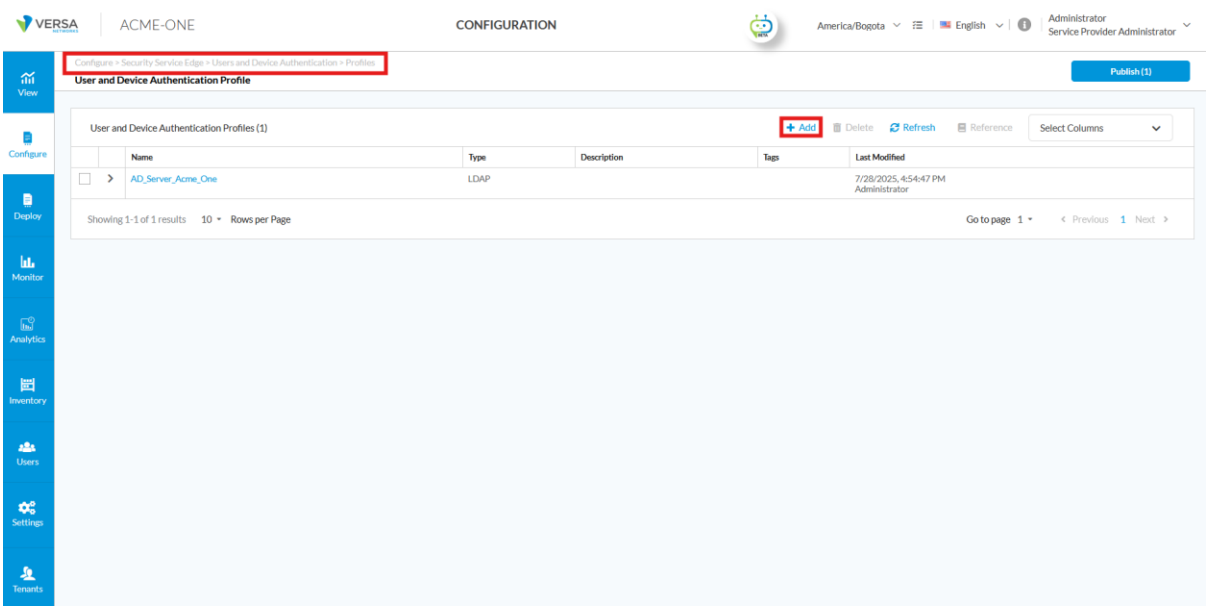
- Confirm the assignment, and the group will appear under the application's **Users and groups** tab.



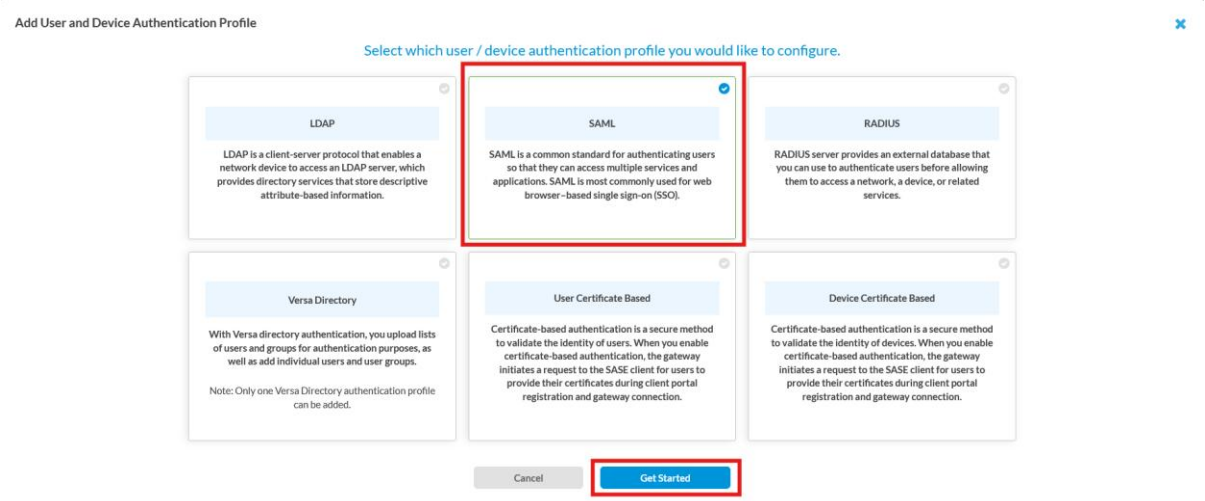
Then click Assign, This ensures all members of the assigned group inherit SAML access to the application without needing individual assignments.



Concerto configuration for ENTRA-ID SAML Authentication Profiles **Navigate to** User and Device Authentication Profiles, then Go to: Configure > Security Service Edge > Users and Device Authentication > Profiles then "+ Add"



Select **SAML,** Click Get Started

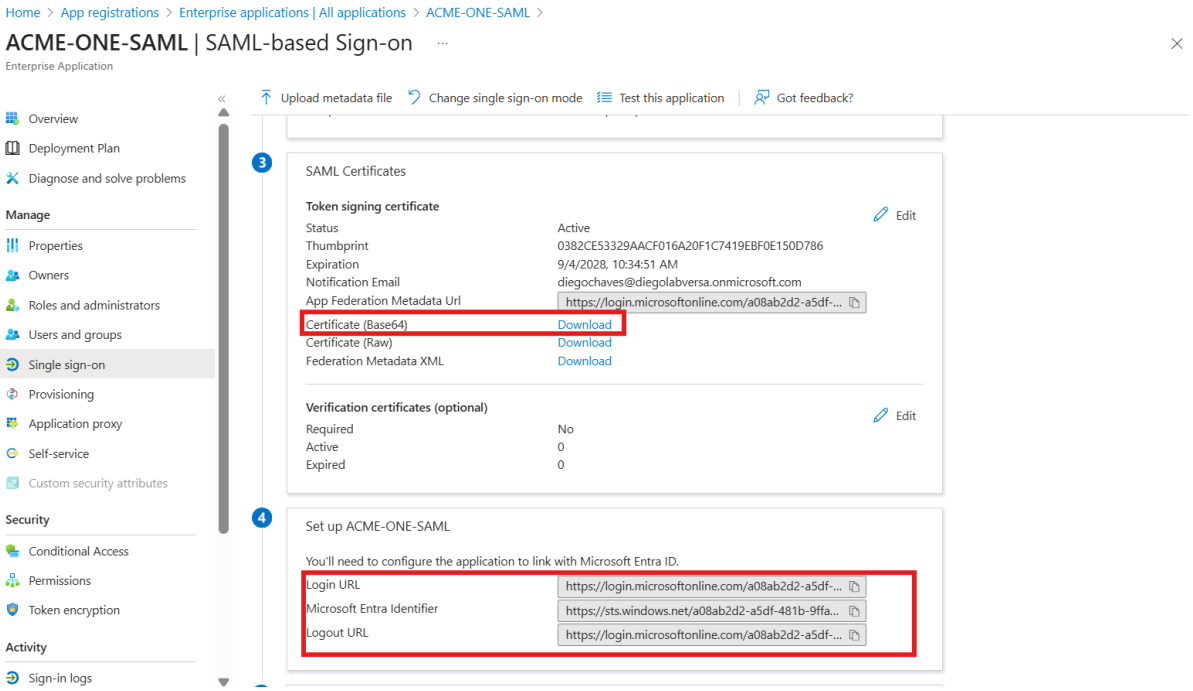


Select **ENTRA-ID**

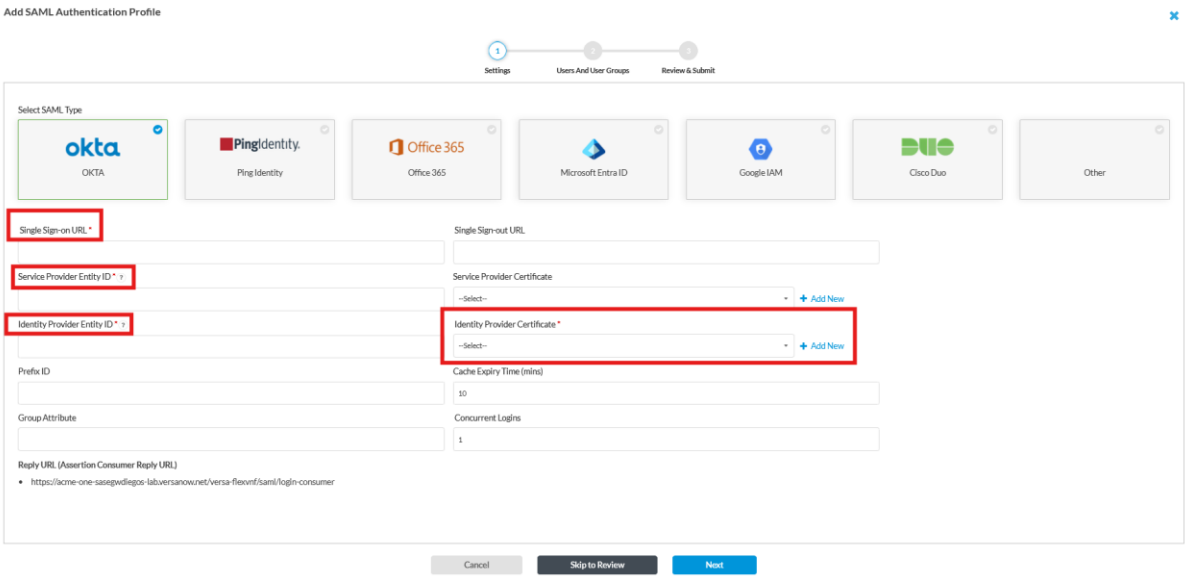
To configure the settings, use the information collected in **Step 8** from the Microsoft ENTRA ID. Go to Entra ID > Enterprise apps > All applications > *ACME-ONE-SAML* > Single sign-on (SAML).

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.



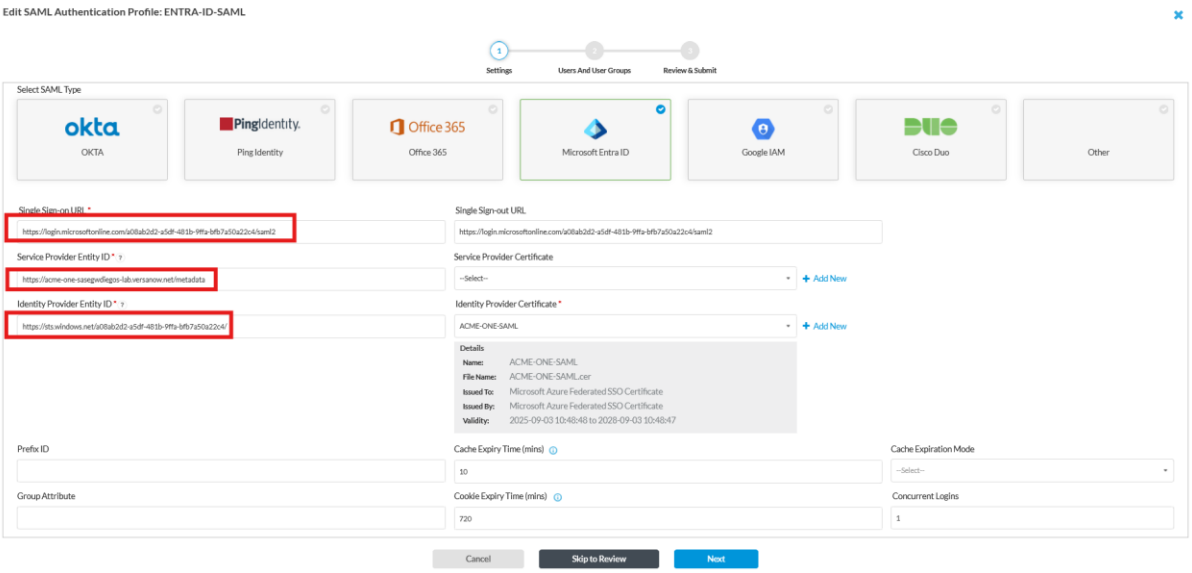
Complete the parameters using the values from the Microsoft Entra id

Example:

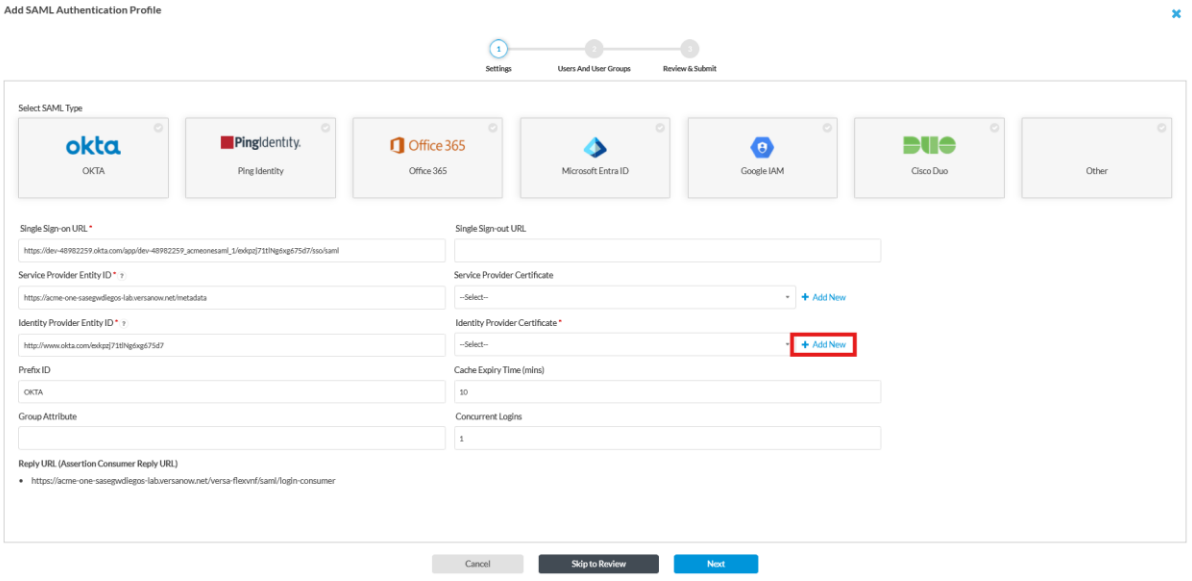
Single Sign-on an out URL: https://login.microsoftonline.com/a08ab2d2-a5df-481b-9ffa-bfb7a50a22c4/saml2

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

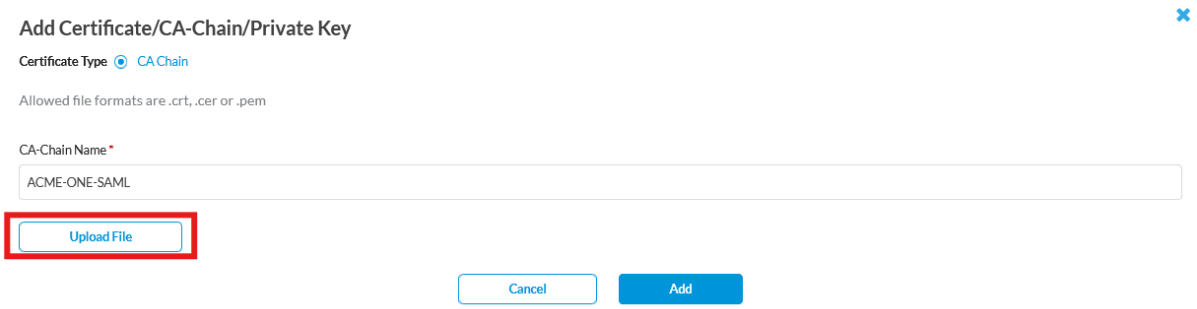
Identity Provider Issuer: https://sts.windows.net/a08ab2d2-a5df-481b-9ffa-bfb7a50a22c4/



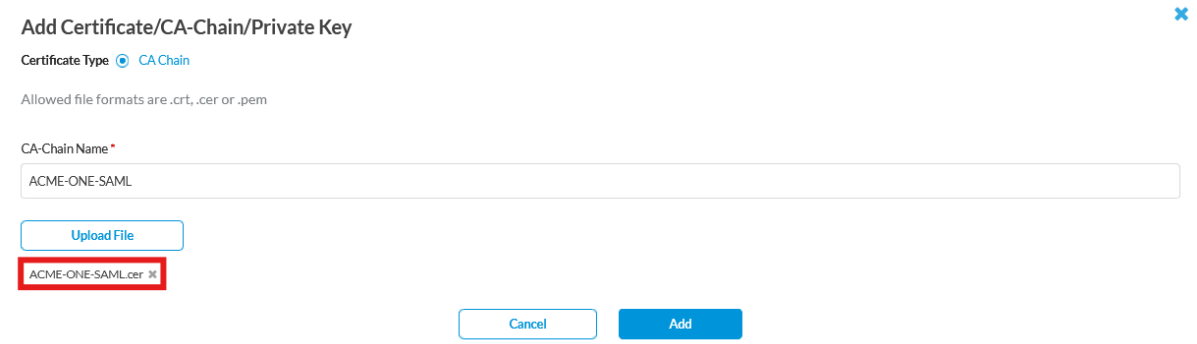
Then Upload the **Identity Provider Certificate** by clicking on the Add New button.



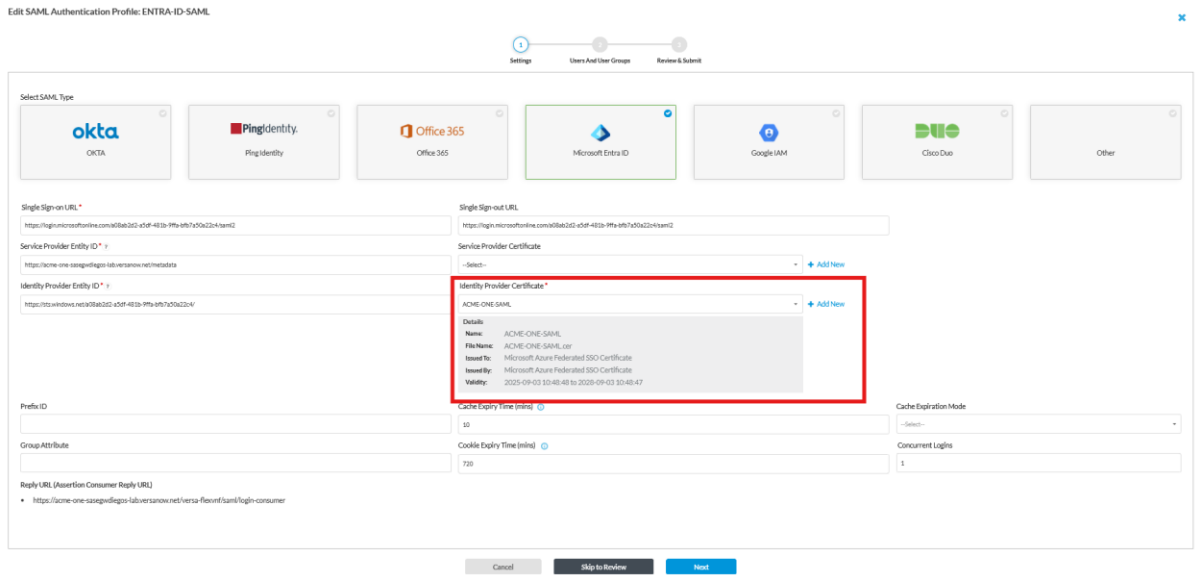
Name to CA-Chain Name upload certificate issue by clicking on the Upload File.



Then Add

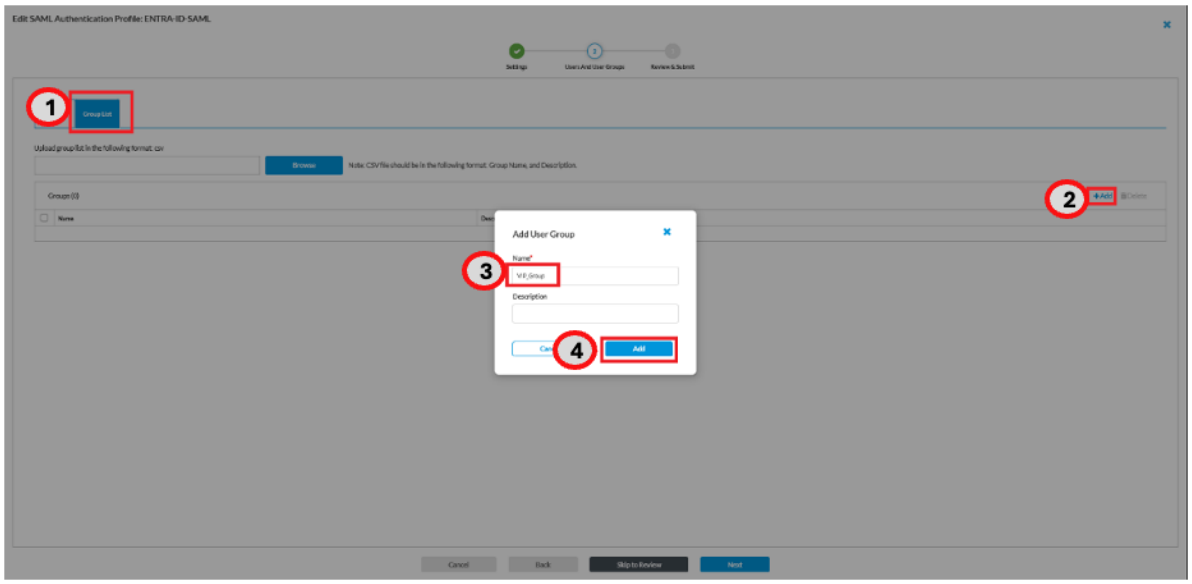


If certificate was uploaded successful, the certificate details will be displayed

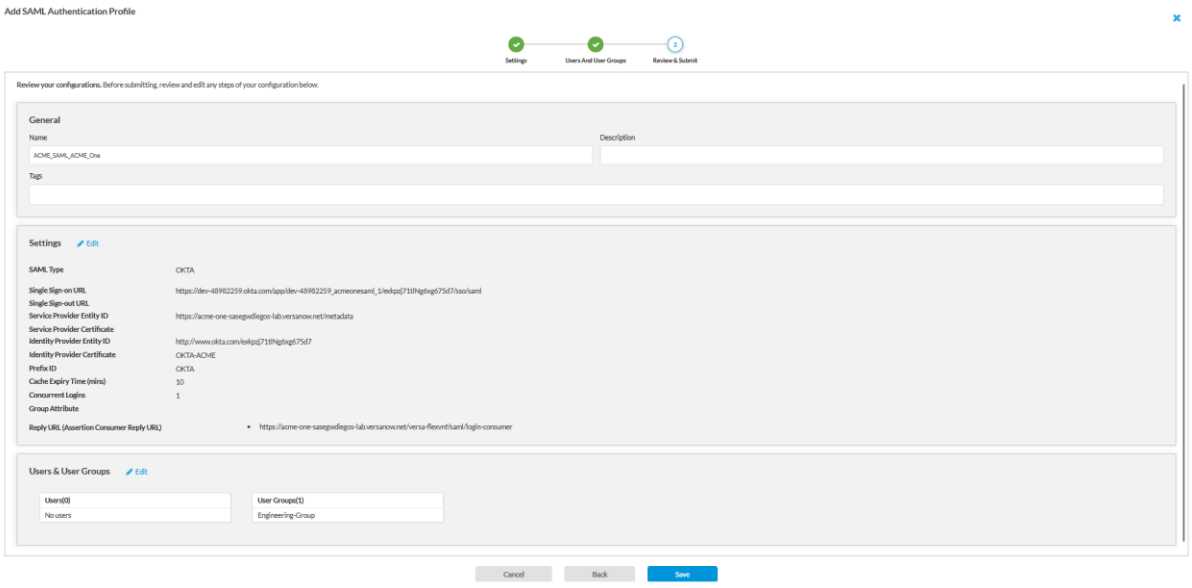


Then **Next**

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.



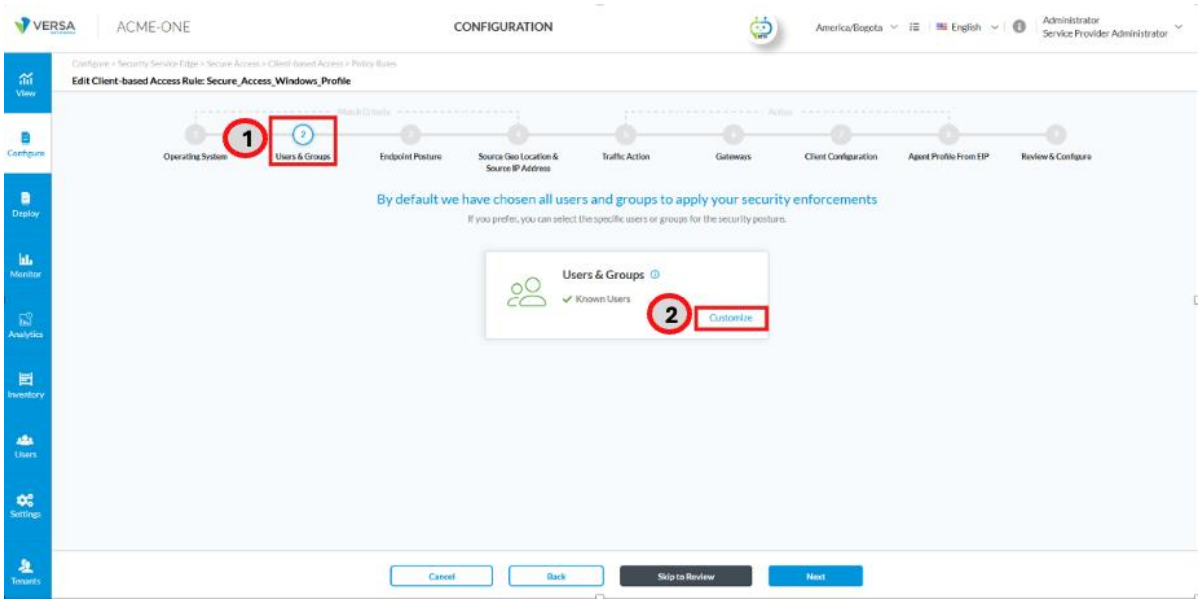
On the **Review & Submit** page, enter a **Name** and **Description** for the profile, then review all configuration details including general information, SAML settings, and assigned users or groups. Once confirmed, click **Save** to complete the profile creation.



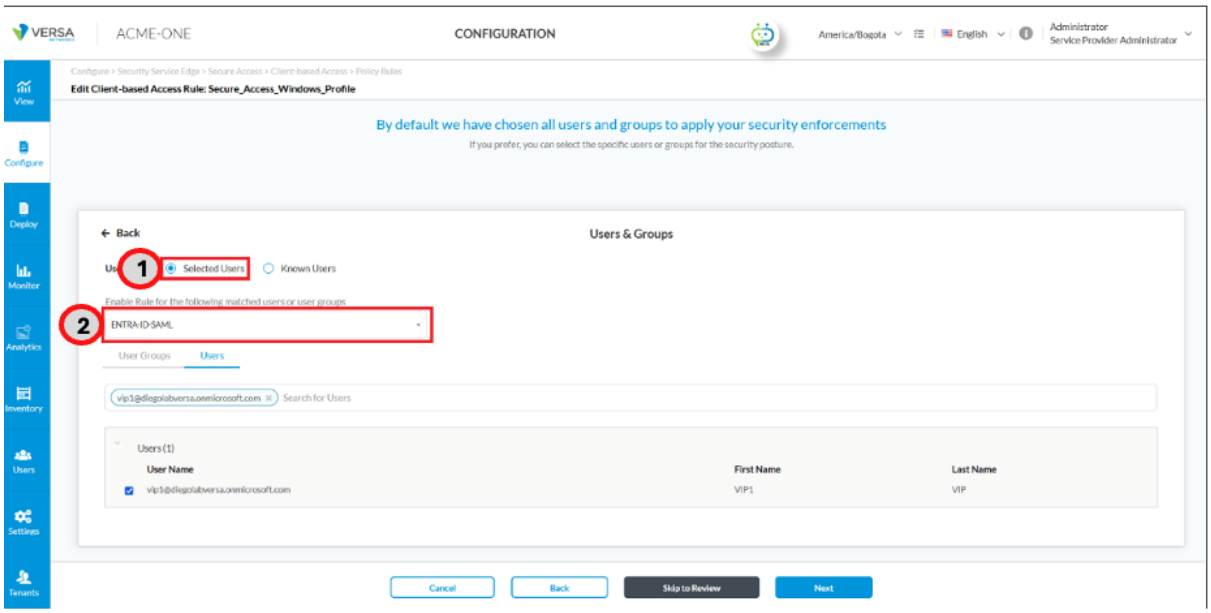
After creating and Publishing the Authentication Profile, you must apply them to the Secure Access Client policy to enforce authentication and apply the corresponding security policies. Navigate to: **Configure > Security Service Edge > Secure Access > Client-based Access > Rules**.

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

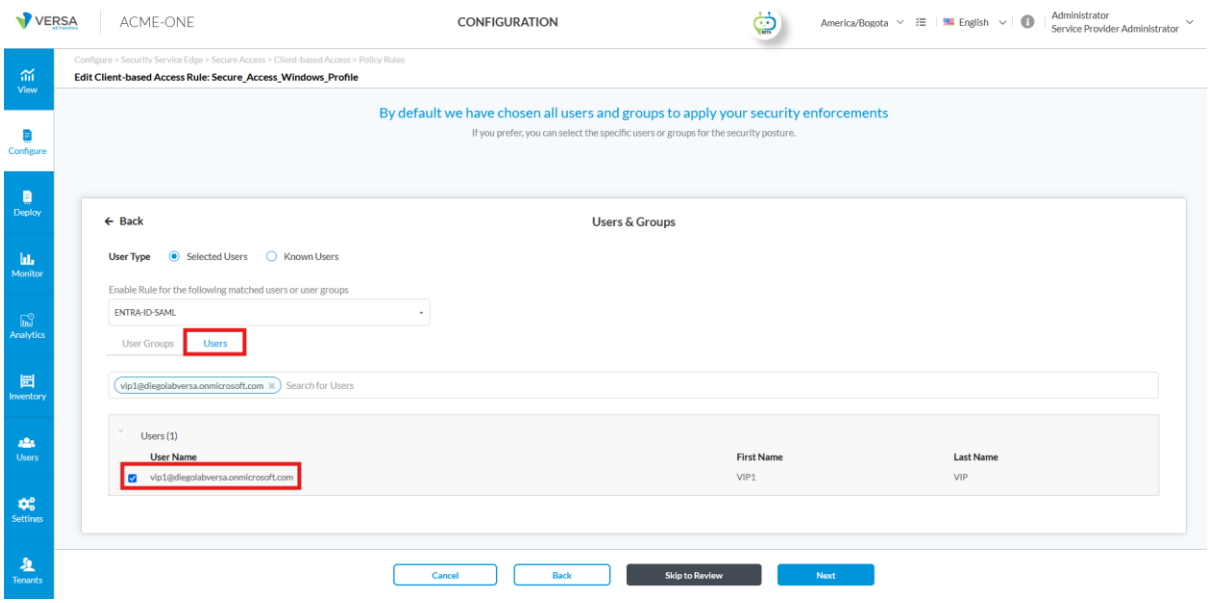
In the **Match Criteria** configuration, navigate to the **Users & Groups** section. Under the **Users & Groups** panel, click on **Customize** to begin specifying user-based access rules using the authentication profile you previously created.



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.



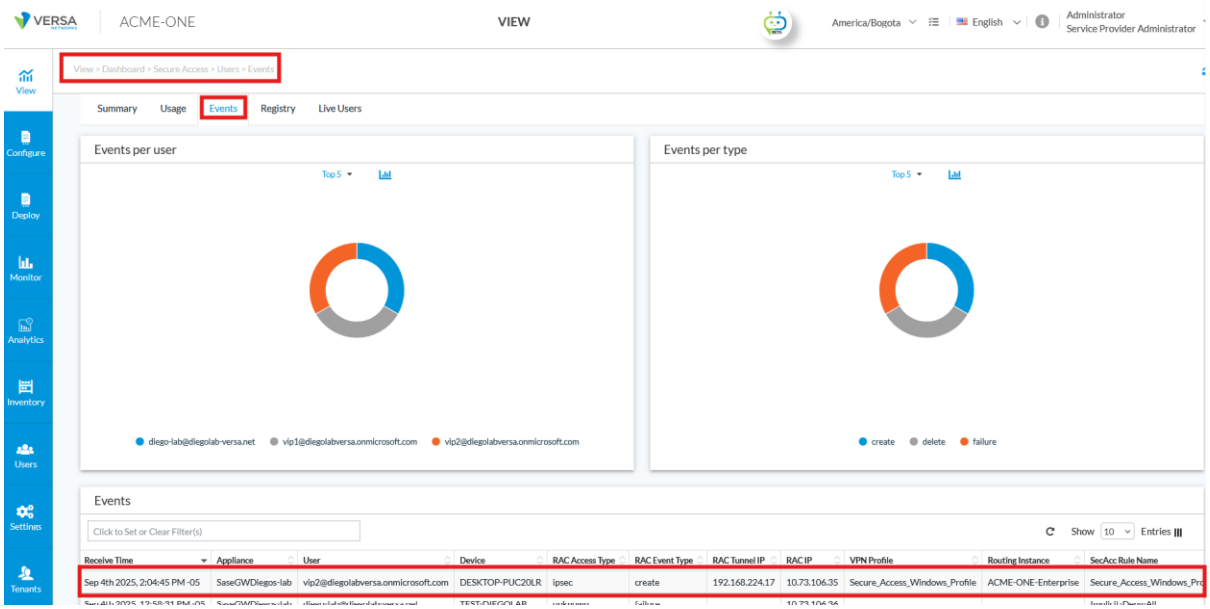
In this step, you can choose to add specific **users** or **groups** to enforce security policies. Use the **User Groups** or **Users** tabs to select the desired entries.



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**.

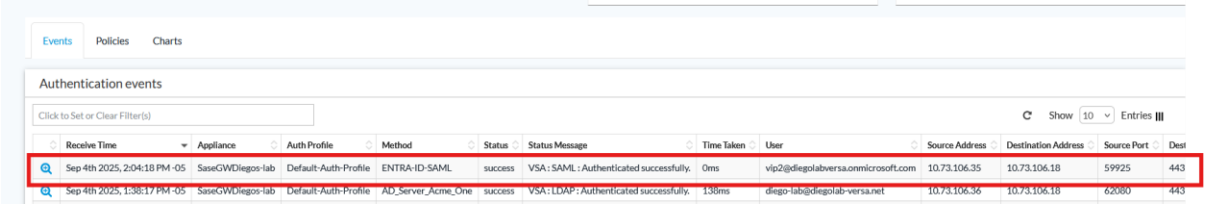
VERIFICATION

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 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 you tenant is that 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

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

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.