

# 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

<b>Title</b>	Step-By-Step Configuration Guide for Versa Secure Internet Access (VSIA)
<b>Author</b>	Versa Professional Services
<b>Version</b>	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 .....	4
Topology.....	6
Configuration steps.....	7
Step 1. Configure Authentication method - SAML (Okta).....	8
Overview.....	8
Okta SAML Configuration.....	8
Step 2: Configure Secure Client Access Profile .....	23
Step 3: Configure Secure Client Access Policy Rules .....	29
Step 4: Configure DNS Filtering to Block AAAA Queries.....	47
Step 5: Configure SaaS Tenant Control.....	52
Step 6: Configure TLS Decryption .....	57
Create a TLS Decryption Profile .....	58
Create TLS Decryption Policy Rules.....	61
Step 7: Configure The File Filtering Profile .....	67
Step 8: Configure URL filtering Profile.....	72
Step 9: Configure Internet Protection Policy Rules.....	76
Internet Protection Policy Rule for Contractor Users .....	76
Internet Protection Policy Rule for IT Users .....	81
Appendix A – Authentication Methods Configuration .....	88
LDAP Active-Directory .....	88
Microsoft Entra ID .....	97
Versa Directory.....	118
About Versa.....	119

## 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

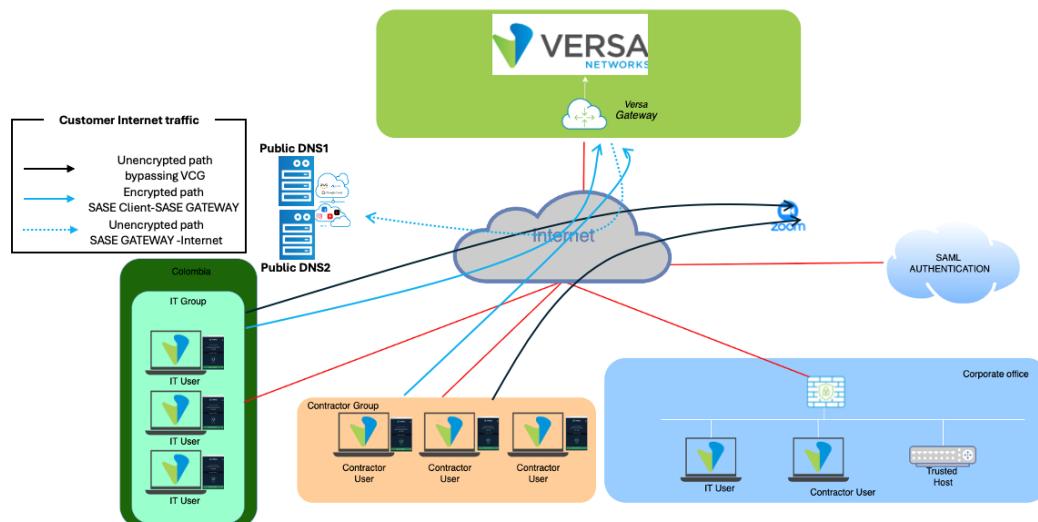
- SSE Gateway: Deploy with VSIA enabled.
- DNS & Monitoring: Configure two public DNS servers and enable Digital Experience Monitoring (DEM) for Office 365.
- SASE Client:
  - Enable Always-On with Trusted Network Detection.
  - Block all traffic if the gateway connection fails.
  - In corporate offices, 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

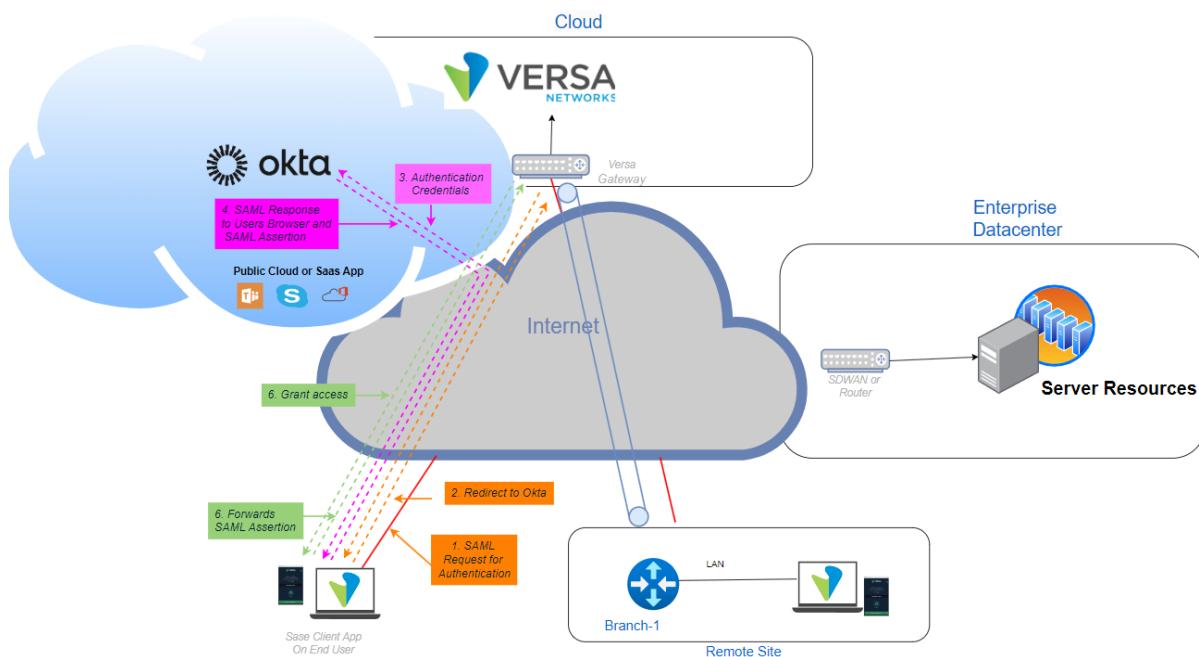
The VSIA configuration consists of the following steps:

- 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**.

**Create a new app integration**

**Sign-in method**

[Learn More](#)

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

**Cancel** **Next**

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

The screenshot shows the Okta Admin Console with the 'Create SAML Integration' wizard. The 'General Settings' tab is active. The 'App name' field is highlighted with a red box and contains 'ACME-ONE-SAML'. The 'Next' button is visible at the bottom right.

#### 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: <code>https://&lt;SASE-GW-FQDN&gt;/versa-flexvnf/saml/login-consumer</code> . Example: <code>https://acme-one-sasegwdiegos-lab.versanow.net/versa-flexvnf/saml/login-consumer</code>
Audience URI (SP Entity ID)	Service Provider (SP) entity ID: Format: <code>https://&lt;SASE-GW-FQDN&gt;/metadata</code> . Example: <code>https://acme-one-sasegwdiegos-lab.versanow.net/metadata</code>
Attribute Statements	Define attributes such as role, organisation, and idle timeout. <i>(Case-sensitive)</i>
Group Attribute Statements (optional)	Enables Versa to import user-to-group mappings from Okta Configuration: - Name: <code>https://schemas.microsoft.com/ws/2008/06/identity/claims/groups</code> Name format: Unspecified Filter: Regex <code>(*)</code> 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-5773745532411060288246009139" IssueInstant="2025-08-08T17:10:21.828Z" Version="2.0"
  xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
    <saml2:Subject>
      <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">userName</saml2:NameID>
      <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <saml2:SubjectConfirmationData NotOnOrAfter="2025-08-08T17:15:22.008Z" Recipient="https://acme-one-sasegwdiegos-lab.versanow.net/versa-flexvnf/saml/login-consumer"/>
      </saml2:SubjectConfirmation>
    </saml2:Subject>
    <saml2:Condition 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:Condition>
    <saml2: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:AuthnInstant>
    <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:AuthnStatement>
  </saml2:Subject>
</saml2:Assertion>

```

- Click Next
- 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.

3 Help Okta Support understand how you configured this application

 The optional questions below assist Okta Support in understanding your app integration.

App type   This is an internal app that we have created

Contact app vendor  It's required to contact the vendor to enable SAML

---

Which app pages did you consult to configure SAML?

Enter links, describe where the pages are, or anything else you think is helpful

Did you find SAML docs for this app?

Enter any links here

Any tips or additional comments?

Placeholder text

[Previous](#) [Finish](#)

## 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.

SAML 2.0

Default Relay State

**Metadata details**

Metadata URL <https://dev-48982259.okta.com/app/exkpzj71tINg6xg675d7/sso/saml/metadata> [Copy](#)

Hide details

**Sign on URL** [https://dev-48982259.okta.com/app/dev-48982259\\_acmeonesaml\\_1/exkpzj71tINg6xg675d7/sso/saml](https://dev-48982259.okta.com/app/dev-48982259_acmeonesaml_1/exkpzj71tINg6xg675d7/sso/saml) [Copy](#)

Sign out URL <https://dev-48982259.okta.com> [Copy](#)

**Issuer** <http://www.okta.com/exkpzj71tINg6xg675d7> [Copy](#)

Signing Certificate [Download](#) [Copy](#)

Certificate fingerprint

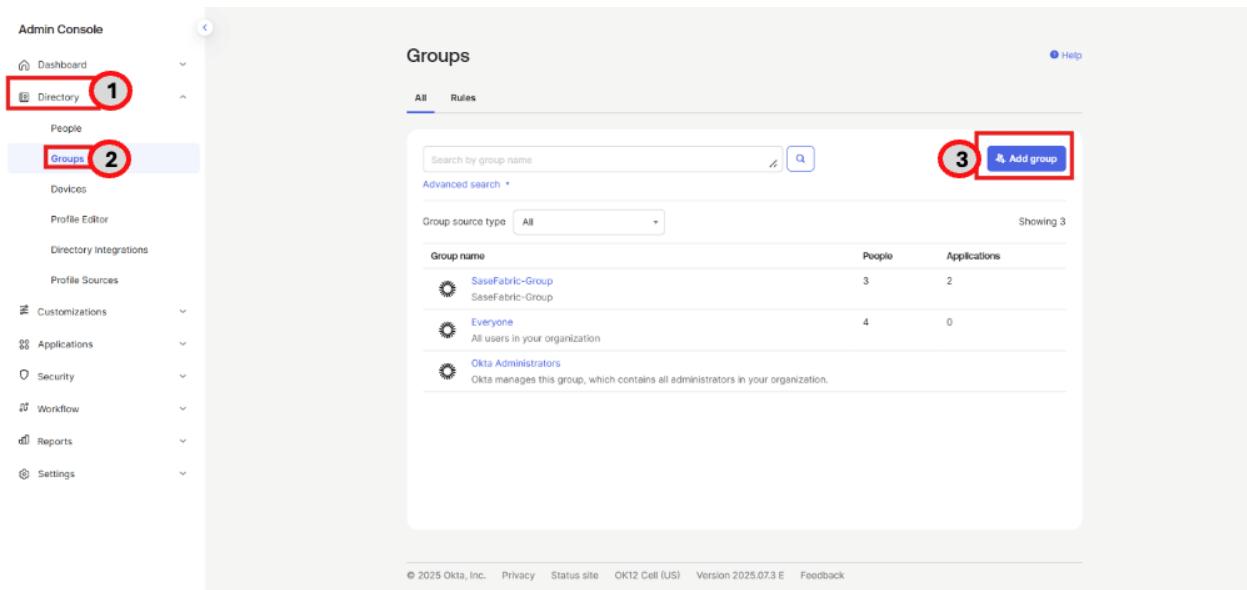
**Note:** Rename the file extension of the downloaded certificate file from. cert to .crt before use.

#### 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
<a href="mailto:ituser1@acme-one.com">ituser1@acme-one.com</a>	IT
<a href="mailto:contractor1@acme-one.com">contractor1@acme-one.com</a>	CONTRACTOR

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



Admin Console

Dashboard

Directory **1**

Groups **2**

People

Devices

Profile Editor

Directory Integrations

Profile Sources

Customizations

Applications

Security

Workflow

Reports

Settings

Groups

Search by group name

Advanced search

Group source type: All

Showing 3

Group name	People	Applications
SaseFabric-Group	3	2
Everyone	4	0
Okta Administrators	0	0

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

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

### Add group

Name

Description (optional)

**Save** **Cancel**

### Add group

Name

Description (optional)

**Save** **Cancel**

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.

The screenshot shows the 'Contractors' group page. At the top, the group name 'Contractors' is highlighted with a red box and circled with a red number '1'. Below it, the creation date 'Created: 12/4/2025' and last modified date 'Last modified: 12/4/2025' are shown, with a 'View logs' link. On the right, an 'Actions' dropdown is visible. The navigation bar below the group name has tabs: 'People' (highlighted with a red box and circled with a red number '2'), 'Applications' (highlighted with a red box and circled with a red number '3'), 'Profile', 'Directories', and 'Admin roles'. The 'Applications' tab is active. The main content area is titled 'Applications' and shows a list of application names starting with '01101110' and ending with '01100111'. A magnifying glass icon is positioned over the list. Below the list, a message says 'No applications assigned to this group' and 'Use Assign applications to assign apps to this group'. To the right, a 'Group Members' section is shown with a list of member names. Below this, a 'How do I edit the group name and description?' link and a 'Hover your mouse over the group name or description to edit them inline.' note are present.

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

## Assign Applications to Contractors

Search...

	Okta Admin Console	<b>Assign</b>
	Okta Workflows	<b>Assign</b>
	Okta Workflows OAuth	<b>Assign</b>
	Versa	<b>Assign</b>
	ACME-ONE-SAML	<b>Assign</b>

**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](mailto:ituser1@acme-one.com) and [contractor1@acme-one.com](mailto:contractor1@acme-one.com)

okta

Admin Console

- Dashboard
- Directory** 1
- People** 2
- Groups
- Devices
- Profile Editor
- Directory Integrations
- Profile Sources
- Customizations
- Applications
- Security
- Workflow
- Reports
- Settings

People

**3** **Add person** **Reset passwords** **More actions**

Showing 4 of 4		
Person & username	Primary email	Status
Test2 Test2 test2@versalab.com	test2@versalab.com	Active
Test test test@versalab.com	test1@versalab.com	Password expired
Diego Chaves diego_hard10@hotmail.com	diego_hard10@hotmail.com	Active
Diego Chaves diego.g@versa-networks.com	diego.g@versa-networks.com	Active

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

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

### Add Person

User type  User

First name

Last name

Username

Primary email

Secondary email (optional)

Groups (optional)

Activation

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

Last name

Username

Primary email

Secondary email (optional)

Groups (optional)

Activation

I will set password

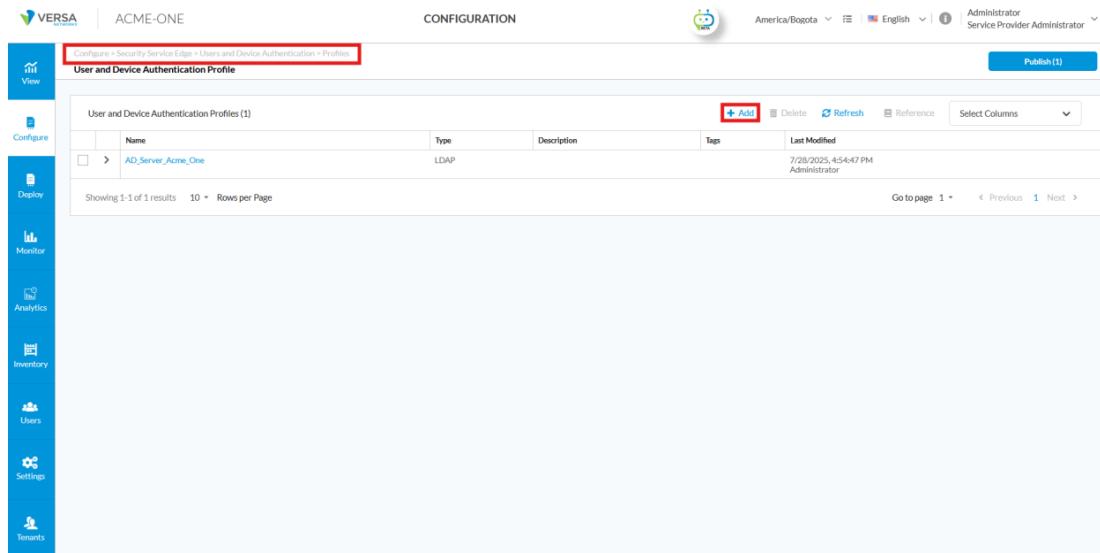
User must change password on first login

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

**Save** **Save and Add Another** **Cancel**

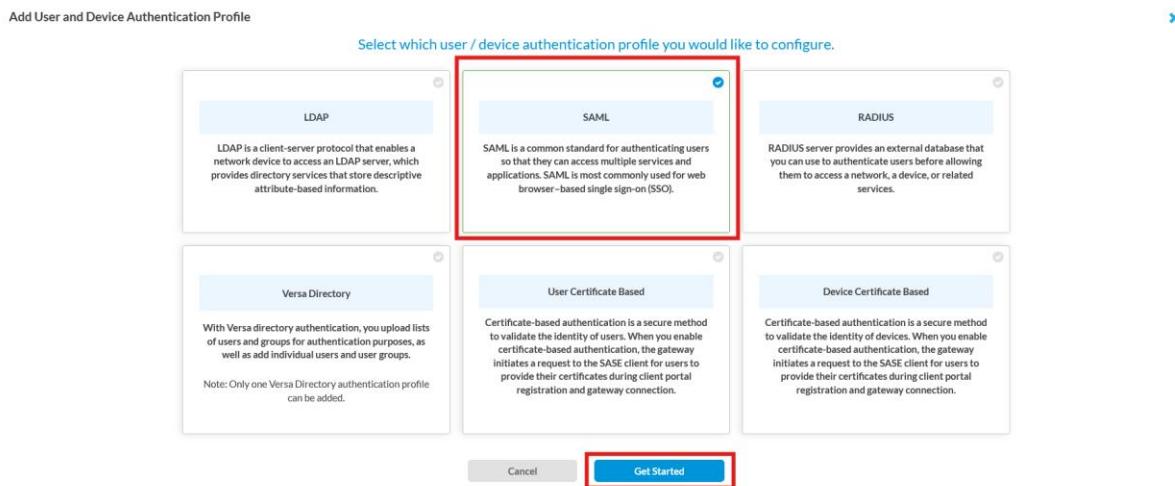
Configure Concerto User Authentication with Okta Navigate to User and Device Authentication Profiles

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



The screenshot shows the VERSA Configuration interface for the 'ACME-ONE' tenant. The left sidebar has icons for View, Configure (highlighted in blue), Deploy, Monitor, Analytics, Inventory, Users, Settings, and Tenants. The main area is titled 'User and Device Authentication Profile' and shows a table with one row: 'AD\_Server\_Acme\_One' (Type: LDAP, Last Modified: 7/28/2025, 4:54:47 PM, Adminstrator). The '+ Add' button in the top right of the table is highlighted with a red box.

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



The screenshot shows the 'Add User and Device Authentication Profile' dialog. It lists several authentication methods: LDAP, SAML, RADIUS, Versa Directory, User Certificate Based, and Device Certificate Based. The 'SAML' option is highlighted with a red box. At the bottom, there are 'Cancel' and 'Get Started' buttons, with the 'Get Started' button highlighted with a red box.

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

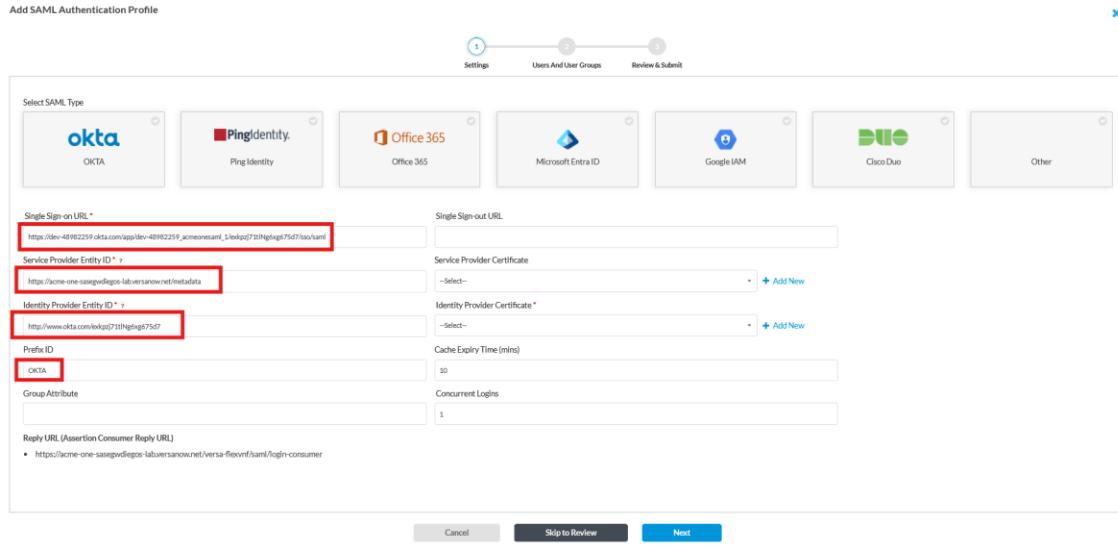
**Single Sign-on URL**, **Service Provider Entity ID** and **Identity Provider Entity ID** are mandatory fields to be configured, and you must upload the signing certificate file issued by Okta.

Complete the parameters using the values from the Okta app:

Example:

- **Single Sign-on URL:** [https://dev-48982259.okta.com/app/dev-48982259\\_acmeonesaml\\_1/exkpzj71tlNg6xg675d7/sso/saml](https://dev-48982259.okta.com/app/dev-48982259_acmeonesaml_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



Add SAML Authentication Profile

1 Settings    2 Users And User Groups    3 Review & Submit

Select SAML Type

Single Sign-on URL \*

Service Provider Entity ID \*

Identity Provider Entity ID \*

Prefix ID

Group Attribute

Single Sign-out URL

Service Provider Certificate

Identity Provider Certificate

Cache Expiry Time (mins)

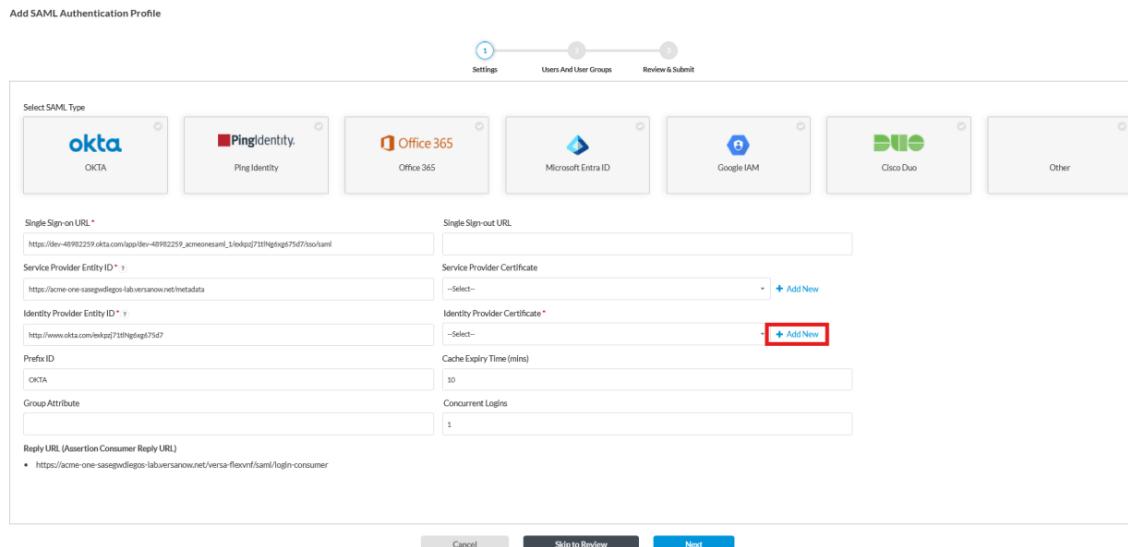
Concurrent Logins

Reply URL (Assertion Consumer Reply URL)

Cancel    Skip to Review    Next

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.



Add SAML Authentication Profile

1 Settings    2 Users And User Groups    3 Review & Submit

Select SAML Type

Single Sign-on URL \*

Service Provider Entity ID \*

Identity Provider Entity ID \*

Prefix ID

Group Attribute

Single Sign-out URL

Service Provider Certificate

Identity Provider Certificate \*

Cache Expiry Time (mins)

Concurrent Logins

Reply URL (Assertion Consumer Reply URL)

Cancel    Skip to Review    Next

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

### Add Certificate/CA-Chain/Private Key

Certificate Type  CA Chain

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

CA-Chain Name \*

OKTA\_ACME

**Upload File**

Cancel

Add

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

### Add Certificate/CA-Chain/Private Key

Certificate Type  CA Chain

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

CA-Chain Name \*

OKTA-ACME

**Upload File**

OKTA-ACME.crt 

Cancel

Add

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

Add SAML Authentication Profile

1 Settings    2 Users And User Groups    3 Review & Submit

Select SAML Type

okta    Pingidentity    Office 365    Microsoft Entra ID    Google IAM    DUO    Cisco Duo    Other

Single Sign-on URL \*

[https://dev-4090229.okta.com/app/dev-4090229\\_acmeacme\\_1/websso/20Nhg0g75d7/test/saml](https://dev-4090229.okta.com/app/dev-4090229_acmeacme_1/websso/20Nhg0g75d7/test/saml)

Service Provider Entity ID \*

<https://acme-one.xangleidapis.versanow.net/metadata>

Identity Provider Entity ID \*

<http://www.okta.com/websso/20Nhg0g75d7>

Identity Provider Certificate \*

OKTA-ACME 

Details

Name	OKTA-ACME
File Name	OKTA-ACME.crt
Issue To	dev-4090229
Issue By	dev-4090229
Validity	2025-08-08 12:23:19 to 2005-08-08 12:24:18

Cache Expiry Time (mins)

10

Concurrent Logins

1

Reply URL (Assertion-Consumer Reply URL)

- <https://acme-one.xangleidapis.versanow.net/versa-fxclient/saml/login-consumer>

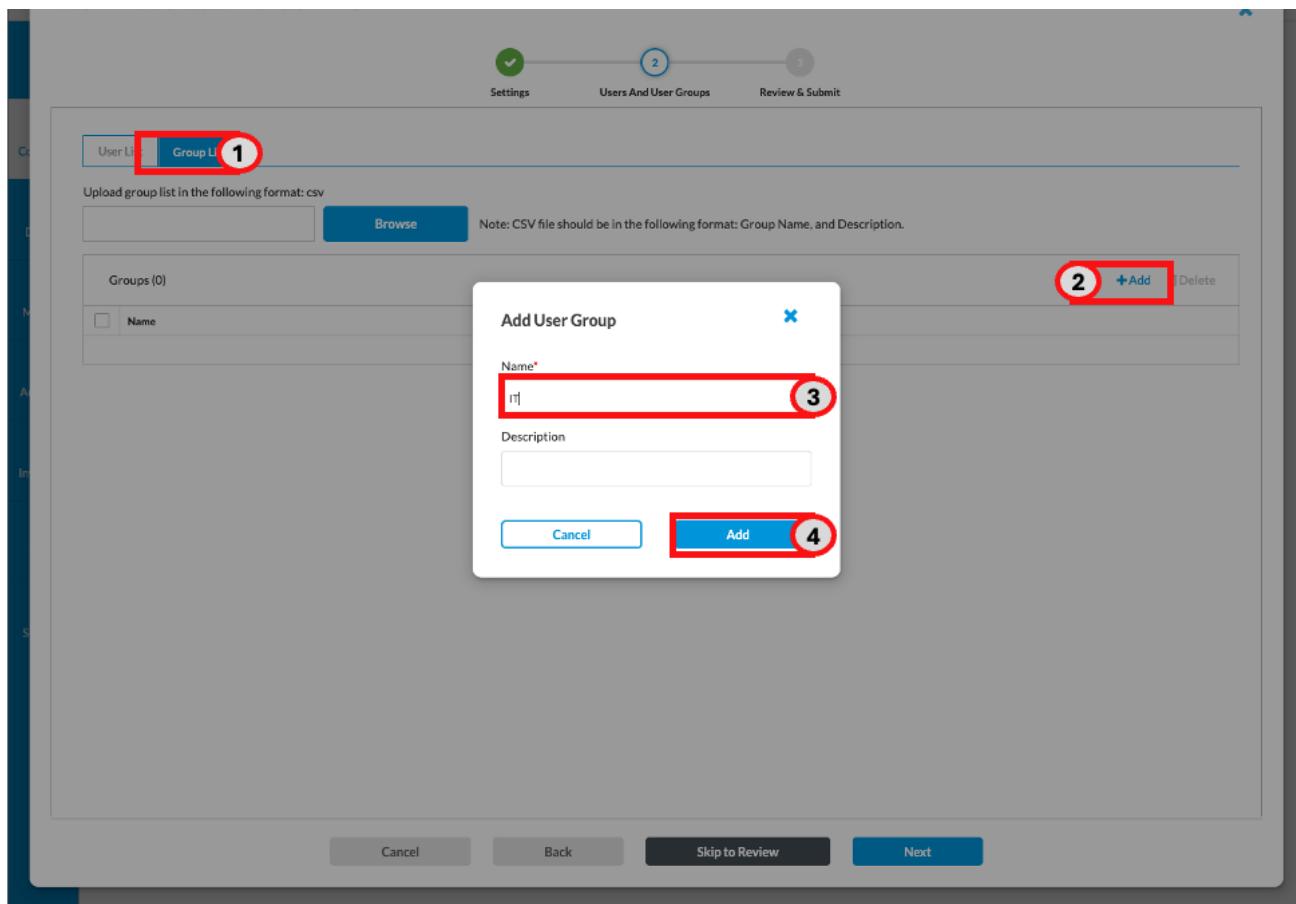
Cancel    Skip to Review    **Next**

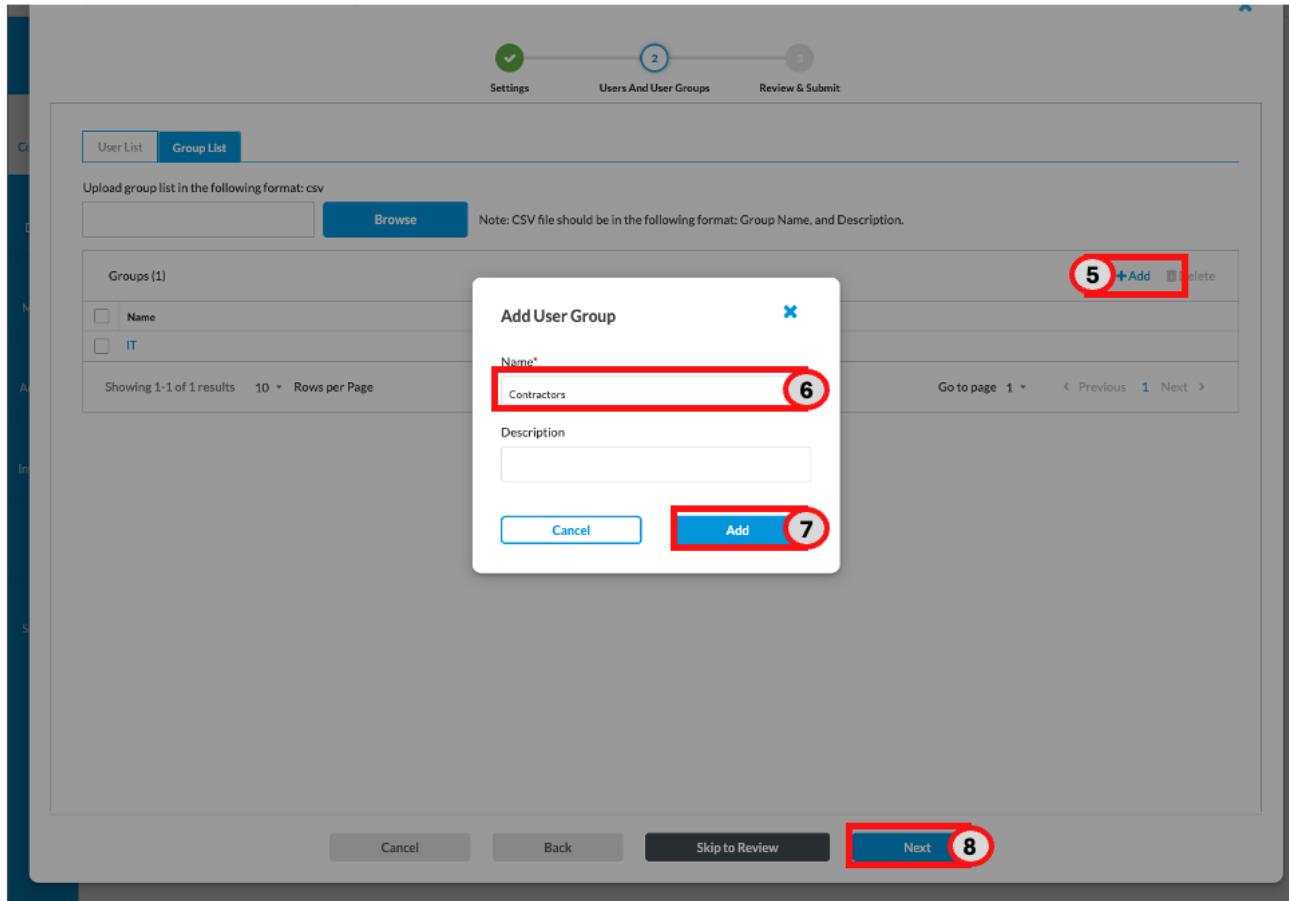
On the **Users and User Groups** page, you can add either individual users or entire groups. Unlike LDAP, SAML-based users and groups do not auto-populate; they must be created manually. These groups can then be referenced when configuring Secure Access Rules and Real-Time Protection Rules.

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.

Add SAML Authentication Profile

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

**General**

Name	ACME_SAML_ACME_One	Description
Tags		

**Settings**

SAML Type	OKTA
Single Sign-on URL	https://dev-40982259.okta.com/app/dev-40982259_acmeonesaml_1/sso/saml
Single Sign-out URL	https://acme-one-saas-sdiegos-lab.versanow.net/metadata
Service Provider Entity ID	https://acme-one-saas-sdiegos-lab.versanow.net/metadata
Service Provider Certificate	http://www.okta.com/certs/2711hg0g75d7
Identity Provider Entity ID	http://www.okta.com/certs/2711hg0g75d7
Identity Provider Certificate	OKTA-ACME
Prefix ID	OKTA
Cache Expiry Time (mins)	30
Concurrent Logins	1
Group Attribute	
Reply URL (Assertion Consumer Reply URL)	https://acme-one-saas-sdiegos-lab.versanow.net/versa/event/saml/login-consumer

**Users & User Groups**

Users(0)	No users	User Group(0)	Engineering-Group
----------	----------	---------------	-------------------

Cancel Back Save

## 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.

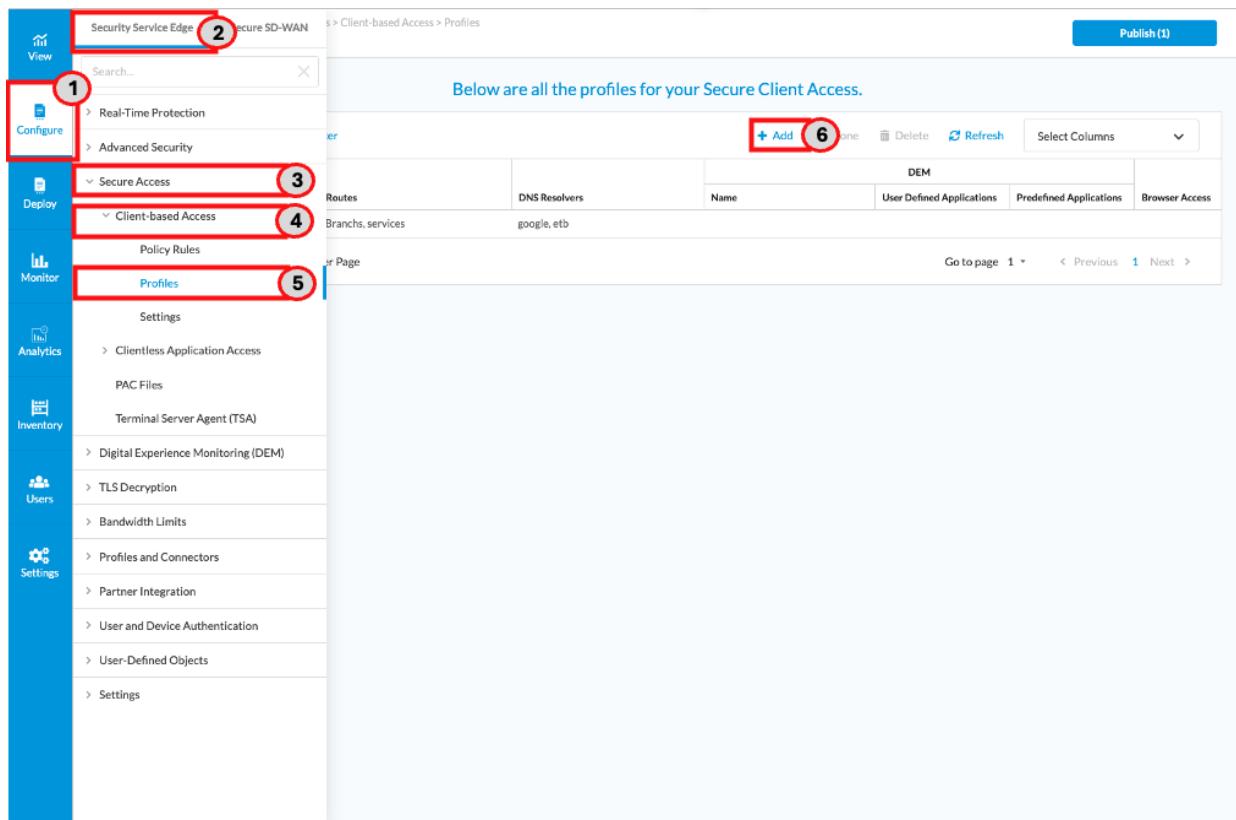
In this Use case:

- 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

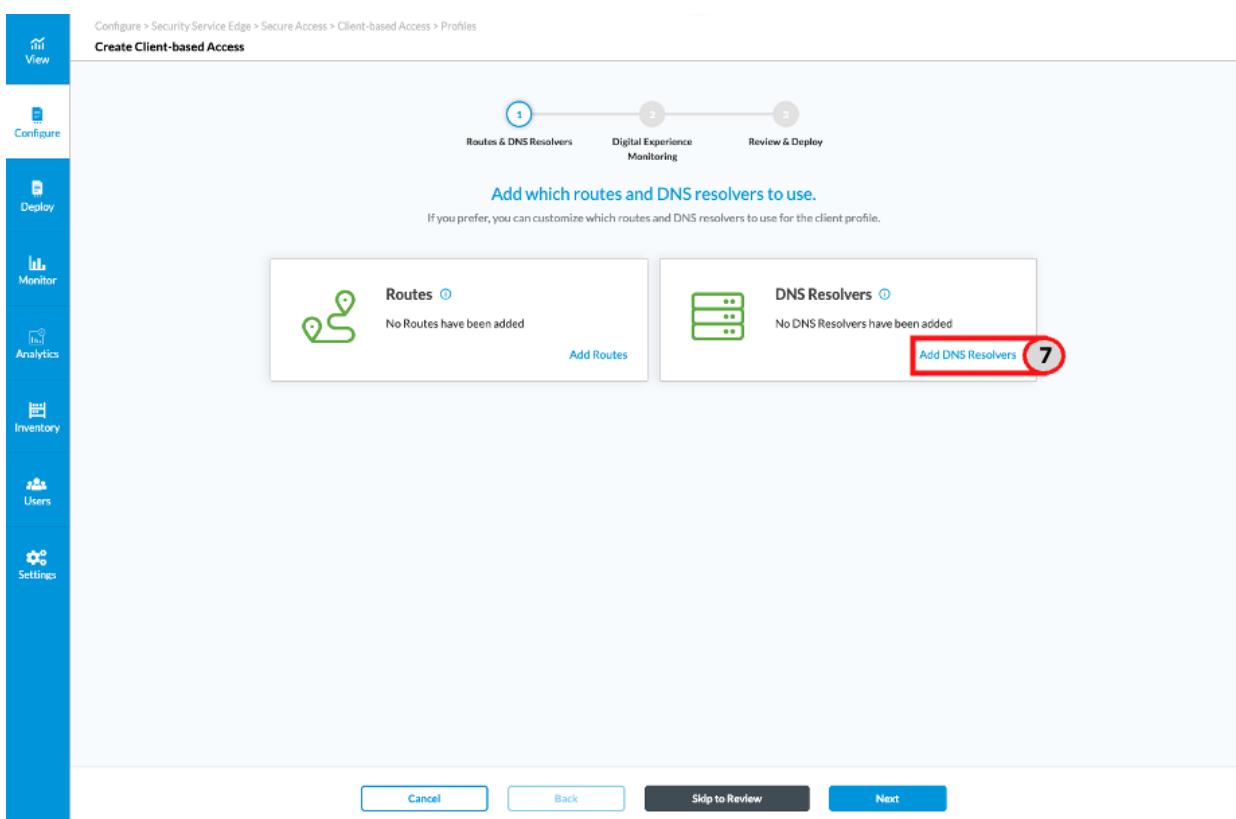
Navigate to [Configure > Security Service Edge > Secure Access > Client-based Access > Profiles](#) and click on [+Add](#) as shown in the figure below.



Below are all the profiles for your Secure Client Access.

DEM	User Defined Applications	Predefined Applications	Browser Access
	google, etb		

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



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

Create Client-based Access

1 Routes & DNS Resolvers 2 Digital Experience Monitoring 3 Review & Deploy

Add which routes and DNS resolvers to use.

If you prefer, you can customize which routes and DNS resolvers to use for the client profile.

**Routes** ⓘ

No Routes have been added

[Add Routes](#)

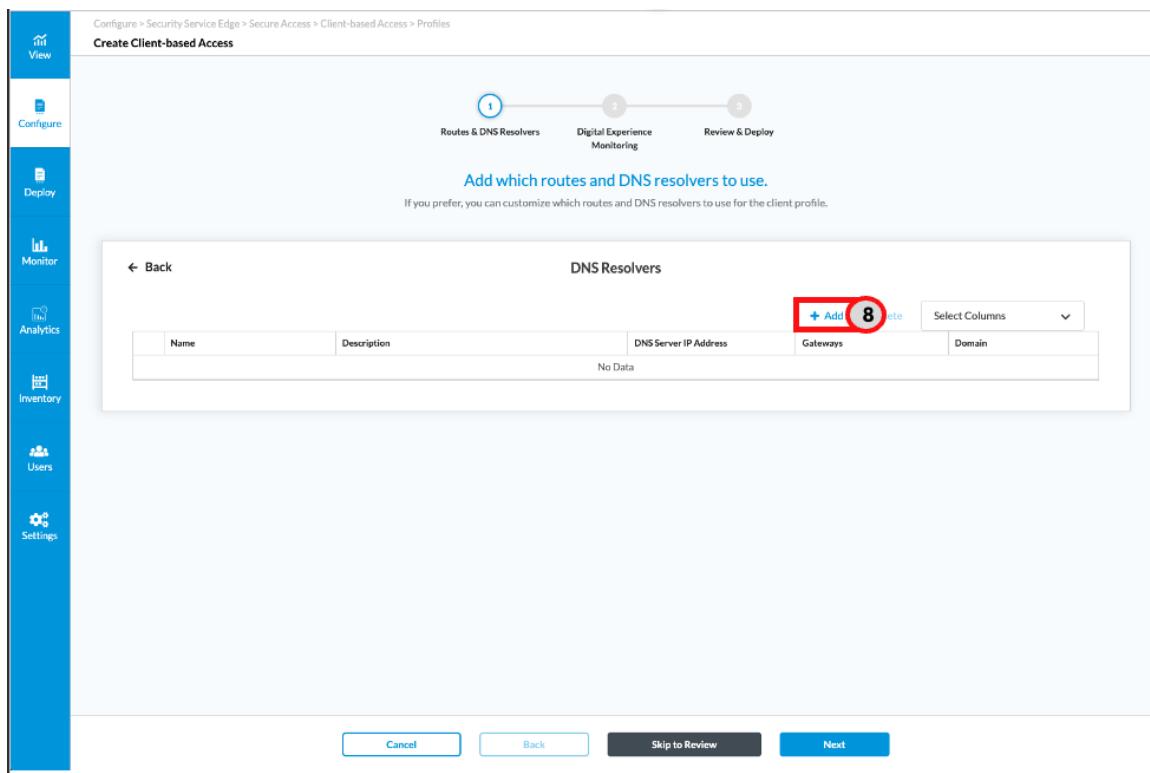
**DNS Resolvers** ⓘ

No DNS Resolvers have been added

[Add DNS Resolvers](#) 7

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

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



Configure > Security Service Edge > Secure Access > Client-based Access > Profiles  
Create Client-based Access

1 Routes & DNS Resolvers 2 Digital Experience Monitoring 3 Review & Deploy

Add which routes and DNS resolvers to use.  
If you prefer, you can customize which routes and DNS resolvers to use for the client profile.

**DNS Resolvers**

**Back**

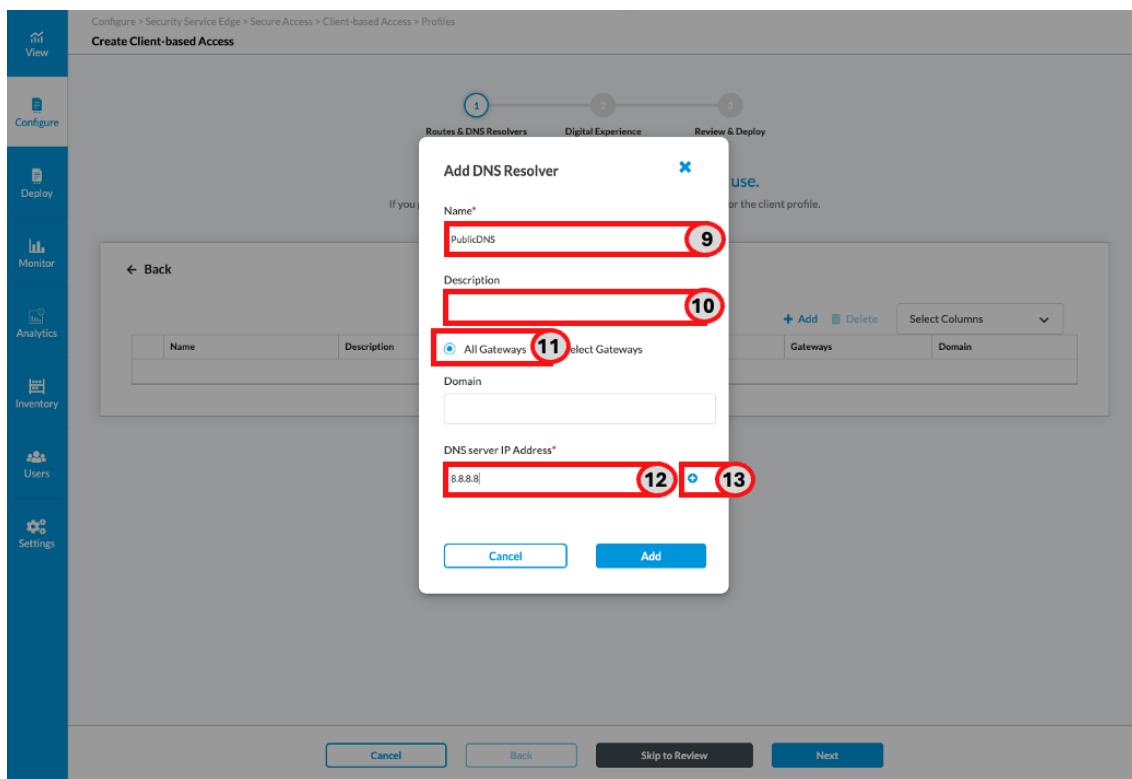
**Name** **Description** **DNS Server IP Address** **Gateways** **Domain**

No Data

**+ Add** (8) **8** **Gateways** **Select Columns**

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

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 > Security Service Edge > Secure Access > Client-based Access > Profiles  
Create Client-based Access

1 Routes & DNS Resolvers 2 Digital Experience Monitoring 3 Review & Deploy

If you prefer, you can customize which routes and DNS resolvers to use for the client profile.

**Add DNS Resolver**

**Name\*** **PublicDNS** (9)

**Description** (10)

**All Gateways** (11) **Select Gateways**

**Domain**

**DNS server IP Address\*** **8.8.8.8** (12) (13)

**Cancel** **Add**

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

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

Edgenet-BR      CONFIGURATION      America/Bogota      English      Dario-Edgenet Enterprise Administrator

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

Create Client-based Access

Add DNS Resolver

Name\*: DNS1

Description:

All Gateways    Select Gateways

Domain:

DNS server IP Address\*: 8.8.8.8  

8.8.4.4   **14**  

**15**   **16**

Cancel   Add   Next

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

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

Create Client-based Access

1   2   3

Routes & DNS Resolvers   Digital Experience Monitoring   Review & Deploy

Click customize to choose your client-based monitoring profile for monitoring the selected network segments.

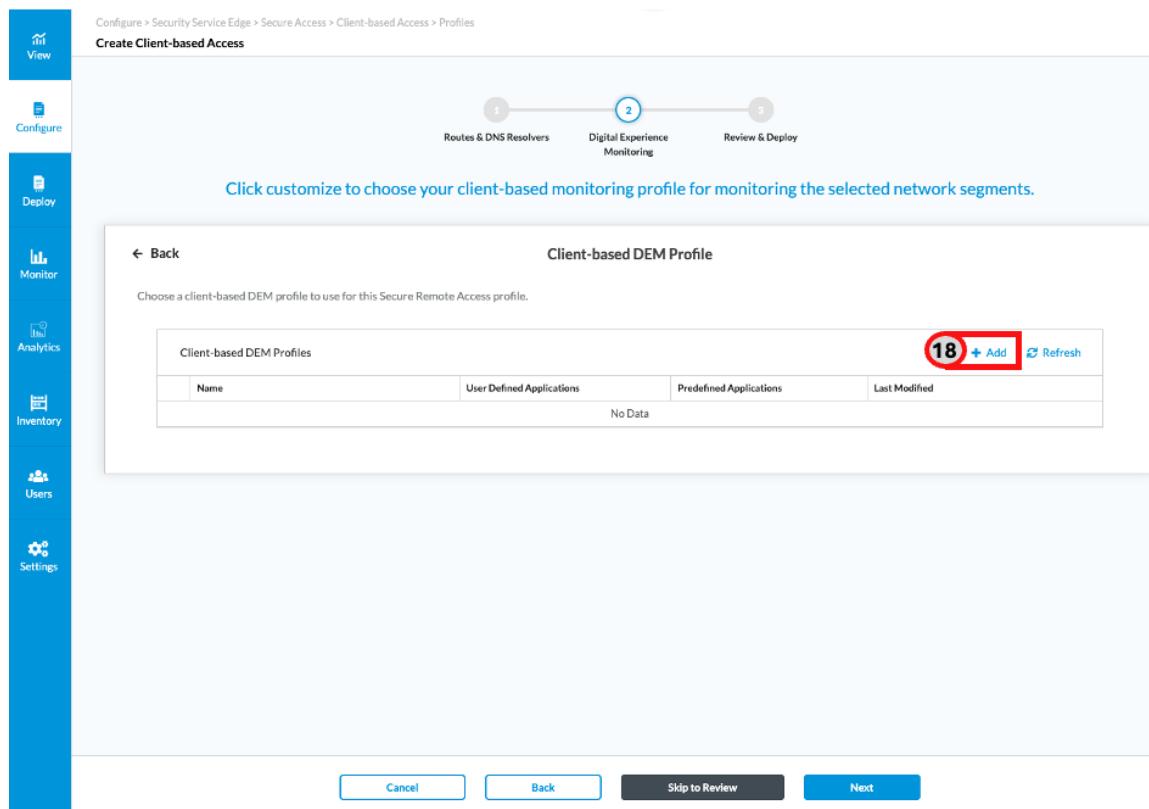
Digital Experience Monitoring

No client-based monitoring profile selected

**17**   **16**

Cancel   Back   Skip to Review   Next

Click **+ Add**.



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

Create Client-based Access

1 2 3

Routes & DNS Resolvers Digital Experience Monitoring Review & Deploy

Click customize to choose your client-based monitoring profile for monitoring the selected network segments.

← Back Client-based DEM Profile

Choose a client-based DEM profile to use for this Secure Remote Access profile.

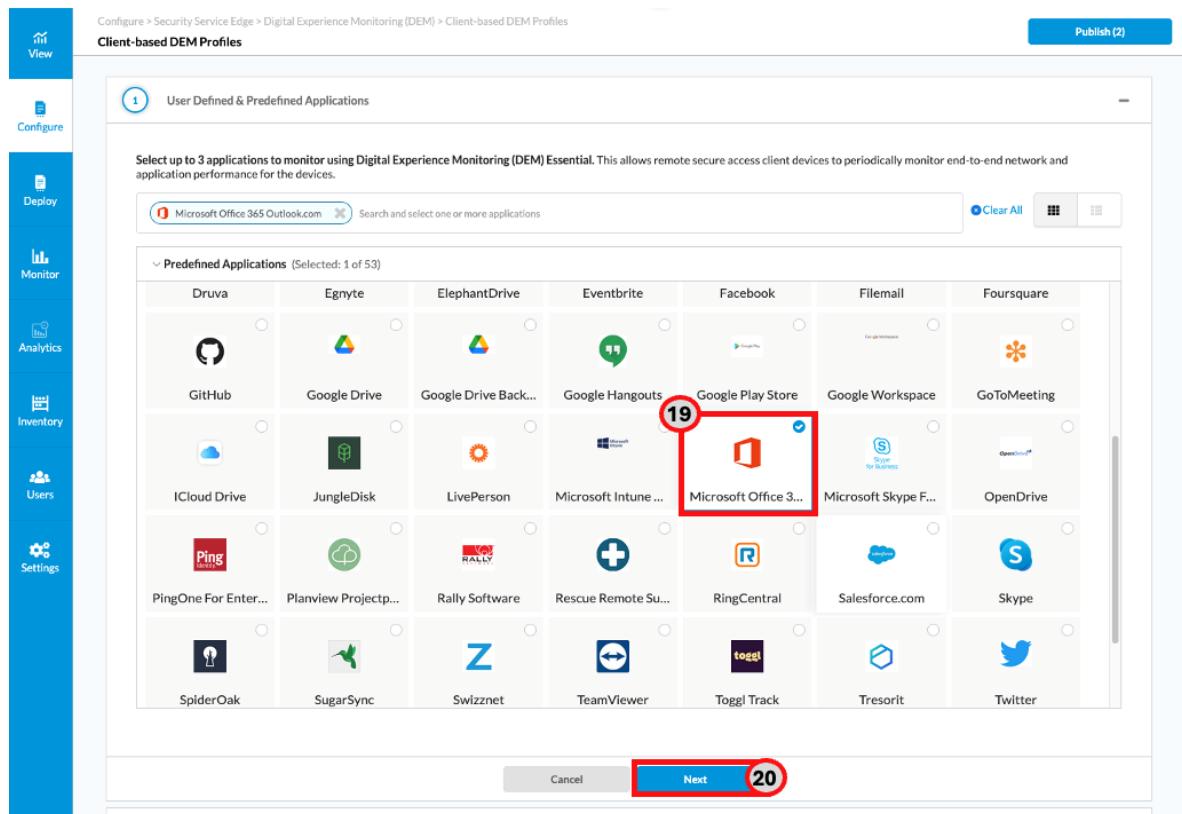
Client-based DEM Profiles

Name	User Defined Applications	Predefined Applications	Last Modified
No Data			

18 + Add Refresh

Cancel Back Skip to Review Next

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



Configure > Security Service Edge > Digital Experience Monitoring (DEM) > Client-based DEM Profiles

Client-based DEM Profiles

1 User Defined & Predefined Applications

Select up to 3 applications to monitor using Digital Experience Monitoring (DEM) Essential. This allows remote secure access client devices to periodically monitor end-to-end network and application performance for the devices.

Search and select one or more applications

Clear All

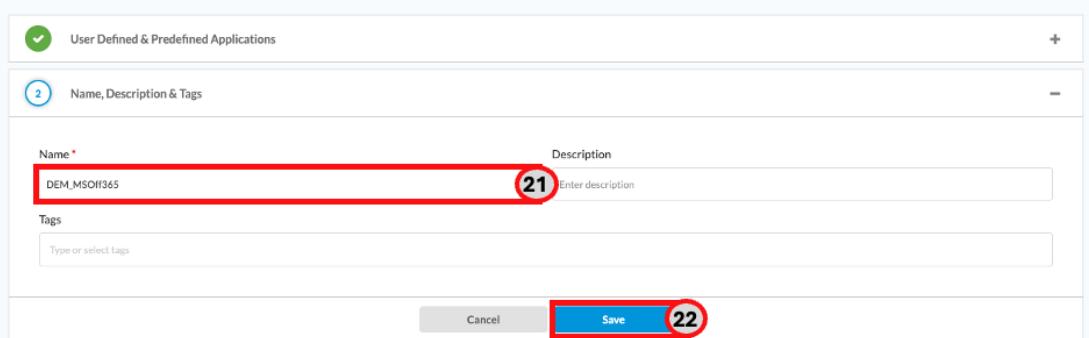
Predefined Applications (Selected: 1 of 53)

Dropbox	Egnyte	ElephantDrive	Eventbrite	Facebook	Filemail	Foursquare
GitHub	Google Drive	Google Drive Back...	Google Hangouts	Google Play Store	Google Workspace	GoToMeeting
ICloud Drive	JungleDisk	LivePerson	Microsoft Intune ...	Microsoft Office 3...	Microsoft Skype F...	OpenDrive
PingOne For Enter...	Planview Projectp...	Rally Software	Rescue Remote Su...	RingCentral	Salesforce.com	Skype
SpiderOak	SugarSync	Swizznet	TeamViewer	Toggl Track	Tresorit	Twitter

19 Microsoft Office 3...

Cancel Next 20

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



Configure > Security Service Edge > Digital Experience Monitoring (DEM) > Client-based DEM Profiles

**Client-based DEM Profiles**

User Defined & Predefined Applications

**2** Name, Description & Tags

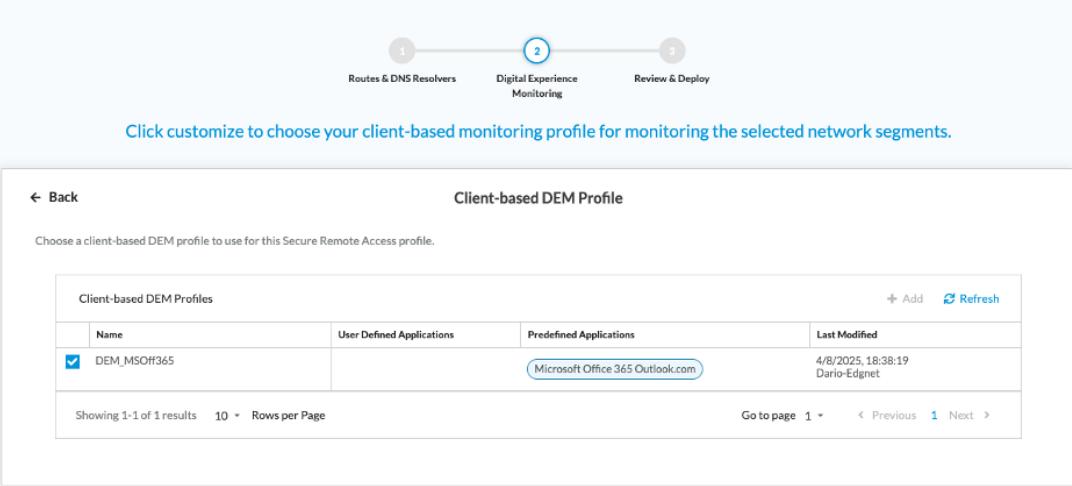
Name\* **DEM\_MSOff365** **21** Description Enter description

Tags Type or select Tags

Cancel **Save** **22**

View, Configure, Deploy, Monitor, Analytics, Inventory, Users, Settings buttons on the left.

Click **Next**.



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

**Create Client-based Access**

1 Routes & DNS Resolvers 2 Digital Experience Monitoring 3 Review & Deploy

Click customize to choose your client-based monitoring profile for monitoring the selected network segments.

**Client-based DEM Profile**

← Back

Choose a client-based DEM profile to use for this Secure Remote Access profile.

Client-based DEM Profiles			
	Name	User Defined Applications	Predefined Applications
<input checked="" type="checkbox"/>	DEM_MSOff365		Microsoft Office 365 Outlook.com <b>21</b>

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

Cancel, Back, Skip to Review, **Next** **23**

View, Configure, Deploy, Monitor, Analytics, Inventory, Users, Settings buttons on the left.

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

Configure > Security Service Edge > Secure Access > Client-based Access > Profiles  
Create Client-based Access

Routes & DNS Resolvers      Digital Experience Monitoring      Review & Deploy

**Review and Configure**  
Below are the configurations of your profile. Review and edit any step of your configuration before validating.

**General**

Name \* **AcmeOne\_SecAccPrfl** 24 Description  
Tags  
Press Enter to add

**Routes & DNS Resolvers** Edit

Routes 0 Added  
DNS Resolvers 2 Added

Name	DNS Server IP Address	Gateways	Domain
PublicDNS	8.8.8.8	All Gateways	
AcmeOneDNS	10.32.0.111	All Gateways	acme-one.com

**Digital Experience Monitoring (DEM)** Edit

Cancel      Back      **Save** 25

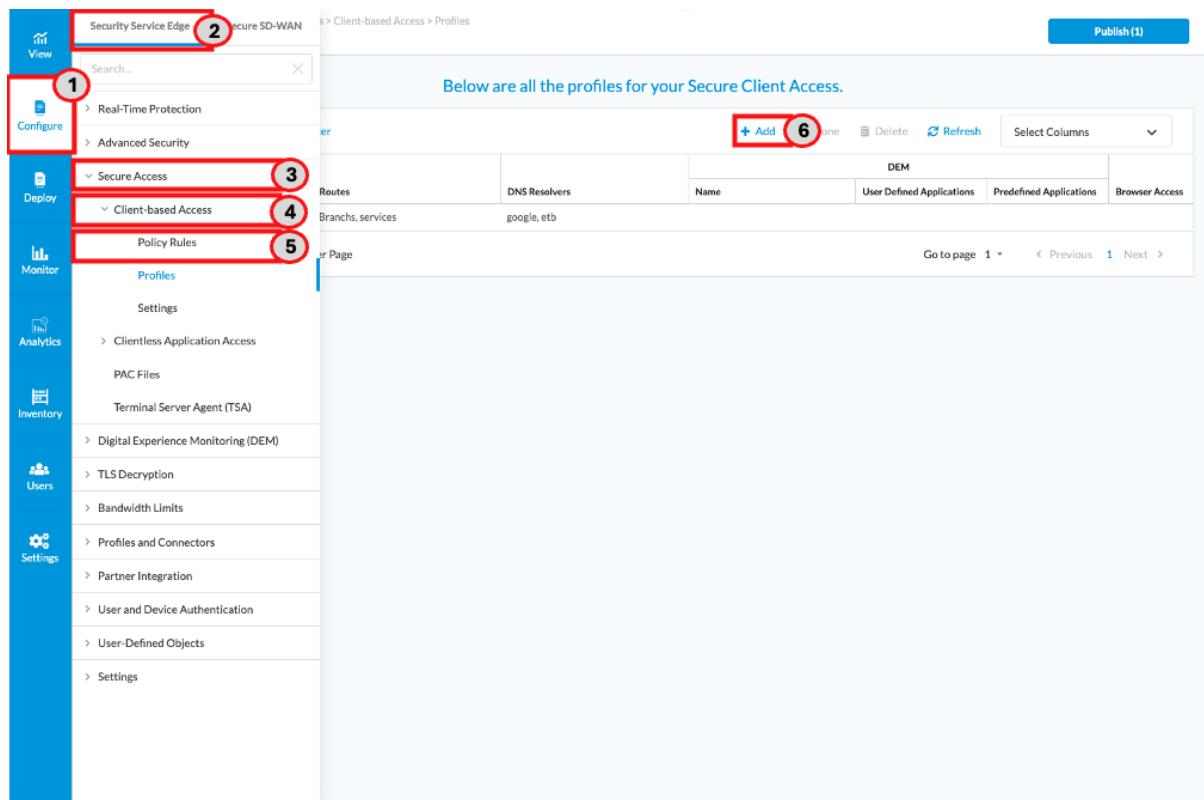
### Step 3: Configure Secure Client Access Policy Rules

Secure Access Policy Rules 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.

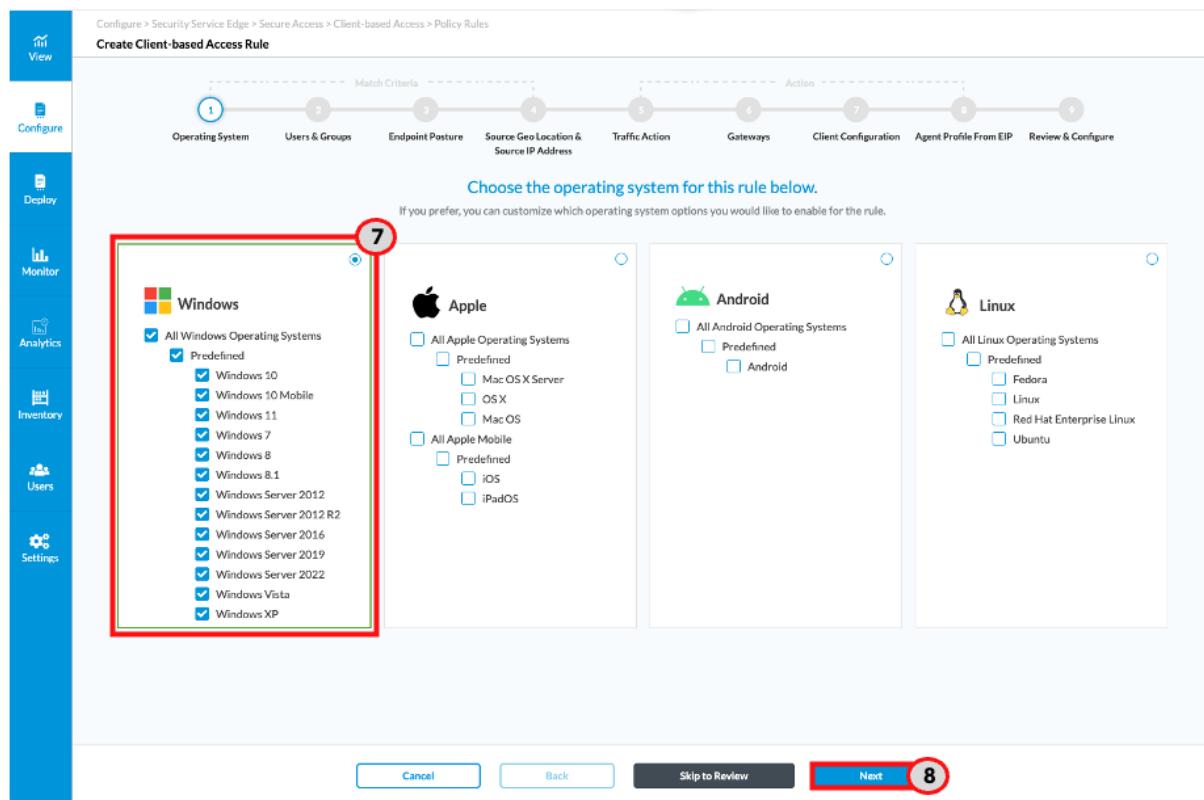
The parameters listed in next table are required to complete the configuration.

Parameter	Description
GeoLocation constraint	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**.



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

**Create Client-based Access Rule**

Match Criteria

Operating System      Users & Groups      Endpoint Posture      Source Geo Location & Source IP Address      Traffic Action      Gateways      Client Configuration      Agent Profile From EIP      Review & Configure

Choose the operating system for this rule below.

If you prefer, you can customize which operating system options you would like to enable for the rule.

**Windows** (7)

- All Windows Operating Systems
  - Predefined
    - Windows 10
    - Windows 10 Mobile
    - Windows 11
    - Windows 7
    - Windows 8
    - Windows 8.1
    - Windows Server 2012
    - Windows Server 2012 R2
    - Windows Server 2016
    - Windows Server 2019
    - Windows Server 2022
    - Windows Vista
    - Windows XP

**Apple**

- All Apple Operating Systems
  - Predefined
    - Mac OS X Server
    - OS X
    - Mac OS
- All Apple Mobile
  - Predefined
    - iOS
    - iPadOS

**Android**

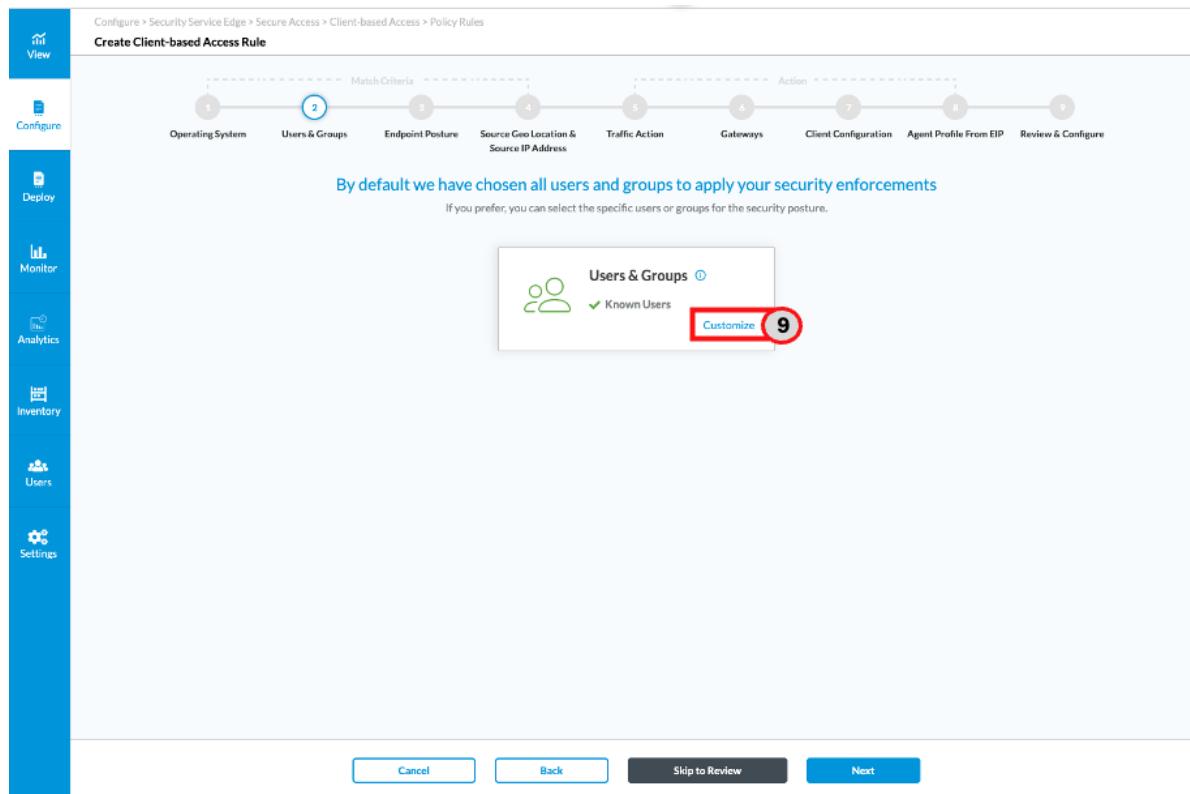
- All Android Operating Systems
  - Predefined
    - Android

**Linux**

- All Linux Operating Systems
  - Predefined
    - Fedora
    - Linux
    - Red Hat Enterprise Linux
    - Ubuntu

**Cancel** **Back** **Skip to Review** **Next** (8)

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



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

Match Criteria

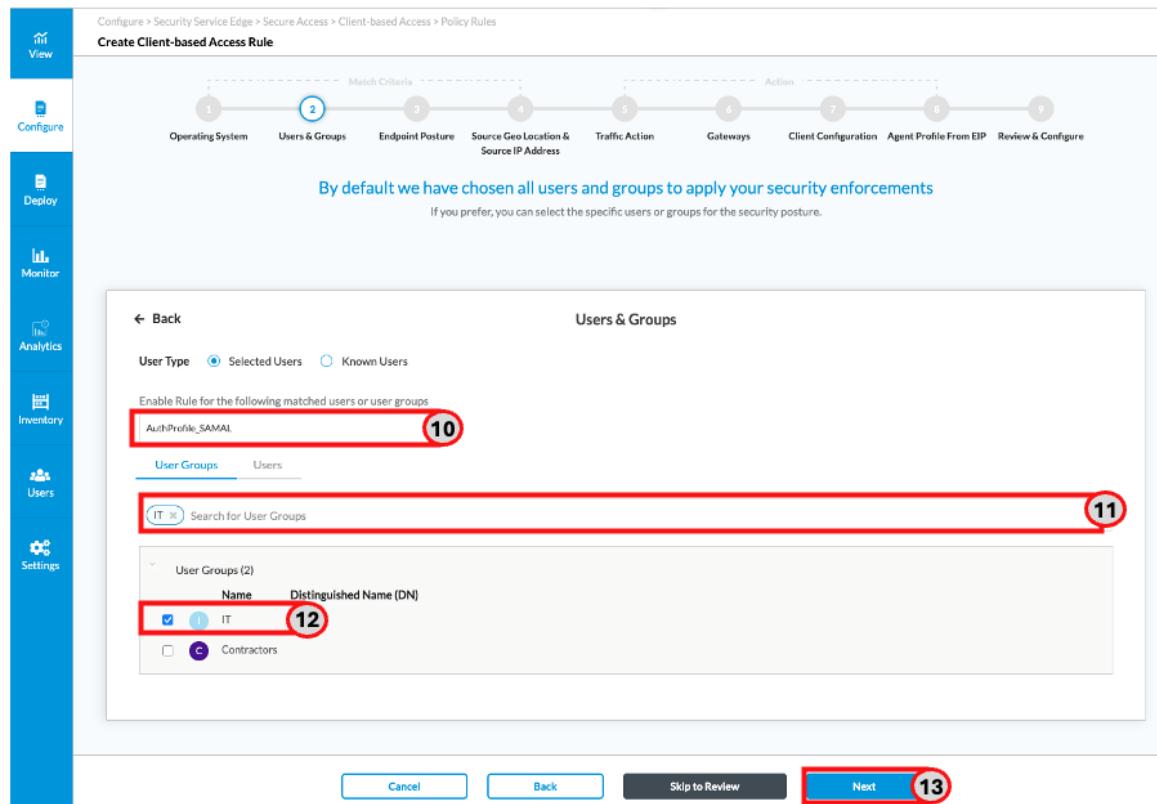
Operating System **2** Users & Groups **3** Endpoint Posture **4** Source Geo Location & Source IP Address **5** Traffic Action **6** Gateways **7** Client Configuration **8** Agent Profile From EIP **9** Review & Configure

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

**Users & Groups**  
 ✓ Known Users **9**  
 Customize

Cancel Back Skip to Review Next

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**.



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

Match Criteria

Operating System **2** Users & Groups **3** Endpoint Posture **4** Source Geo Location & Source IP Address **5** Traffic Action **6** Gateways **7** Client Configuration **8** Agent Profile From EIP **9** Review & Configure

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

**Users & Groups**

User Type  Selected Users  Known Users

Enable Rule for the following matched users or user groups:  
**AuthProfile\_SAML** **10**

User Groups **11** Users

IT  Search for User Groups

User Groups (2)

Name	Distinguished Name (DN)
<input checked="" type="checkbox"/> IT	12
<input type="checkbox"/> Contractors	

Cancel Back Skip to Review **Next** **13**

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

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

Create Client-based Access Rule

Match Criteria

Action

Operating System      Users & Groups      Endpoint Posture      Source Geo Location & Source IP Address      Traffic Action      Gateways      Client Configuration      Agent Profile From EIP      Review & Configure

By default, we have chosen all endpoint devices under endpoint information profile and entity risk bands to apply to your security enforcements.

If you'd like, you can customize your options by choosing what to include or exclude below.

Endpoint Information Profile (EIP)      Device Compliance Status      Entity Risk Bands

Customize      14      Customize      Customize

Customize      14      All Devices      Customize

Customize      All risk bands      Customize

Cancel      Back      Skip to Review      Next

Click **+ Create New EIP Profile**.

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

Create Client-based Access Rule

Match Criteria

Action

Operating System      Users & Groups      Endpoint Posture      Source Geo Location & Source IP Address      Traffic Action      Gateways      Client Configuration      Agent Profile From EIP      Review & Configure

By default, we have chosen all endpoint devices under endpoint information profile and entity risk bands to apply to your security enforcements.

If you'd like, you can customize your options by choosing what to include or exclude below.

← Back      Endpoint Information Profile (EIP)

Select an existing profile or create a new profile with the values for the different EIP attributes collected by the Versa Client. This can be used by the Versa Cloud Gateways for granular policy enforcement based on the end user's entity risk.

User Defined      Predefined

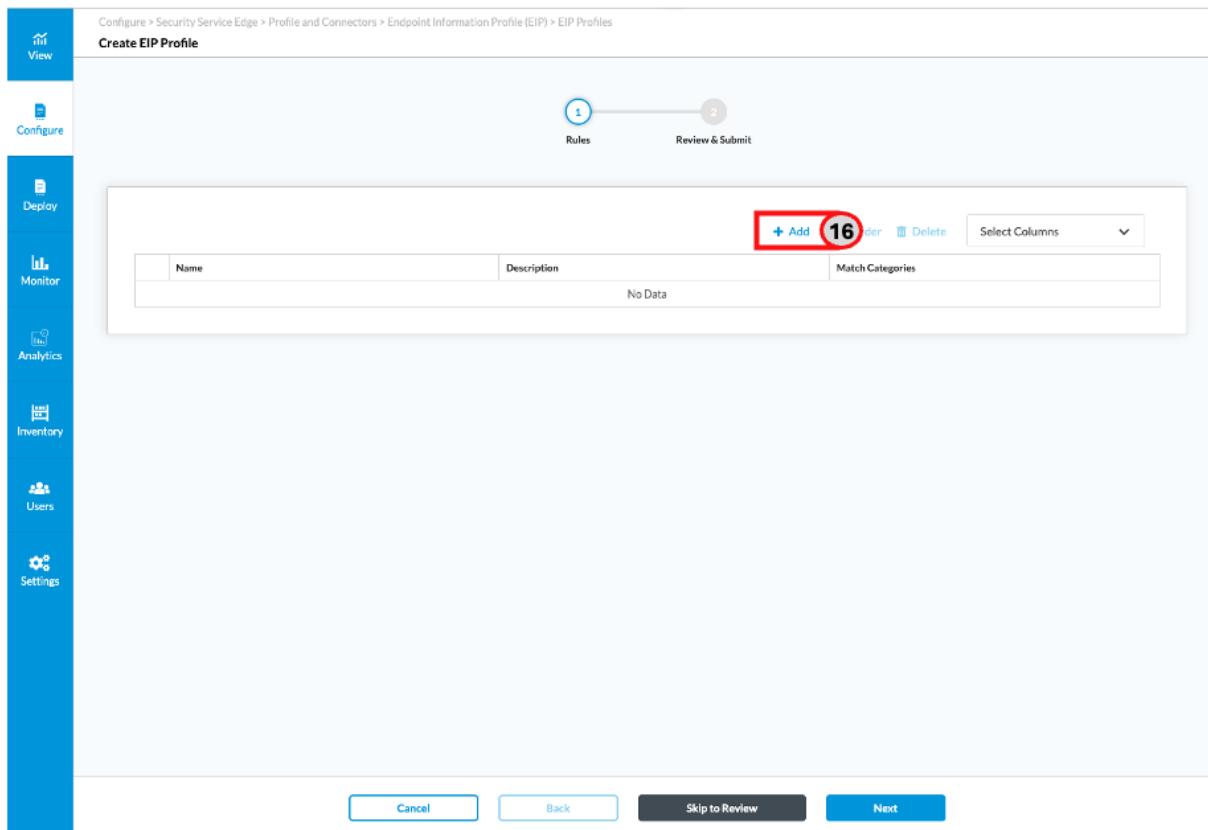
+ Create New EIP Profile      15

+ Add Existing EIP Profile      Delete      Select Columns

	Name	Description	Rules
No User Defined EIP Profiles Added			

Cancel      Back      Skip to Review      Next

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



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles  
**Create EIP Profile**

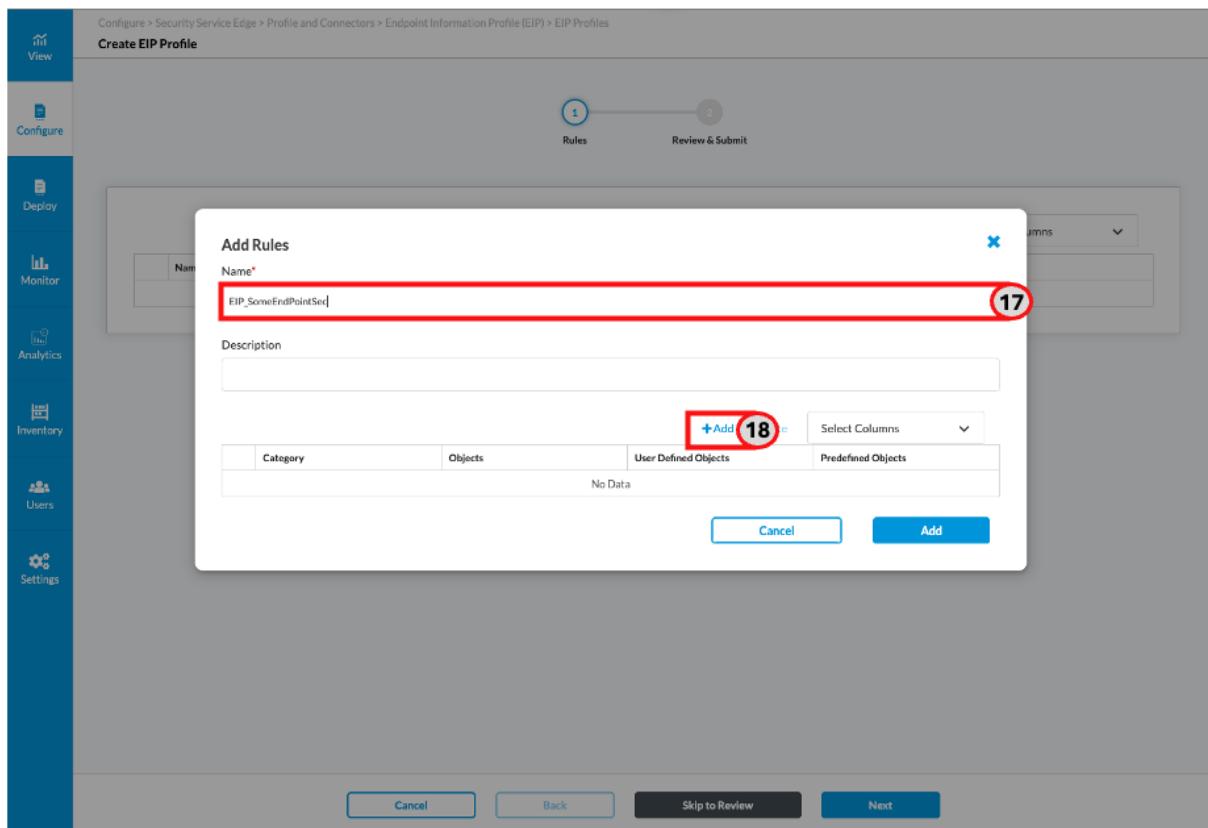
1 Rules 2 Review & Submit

+ Add 16 |  | Select Columns

Name	Description	Match Categories
No Data		

Cancel Back Skip to Review Next

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



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles  
**Create EIP Profile**

1 Rules 2 Review & Submit

Add Rules

Name\* **EIP\_SomeEndPointSel** (labeled 17)

Description

Category	Objects	User Defined Objects	Predefined Objects
No Data			

+ Add 18 |  | Select Columns

Cancel Add

Cancel Back Skip to Review Next

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

Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

Create EIP Profile

1 Rules      2 Review & Submit

Add EIP Object

Category

- eip-object-endpoint\_security-any-installed
- eip-object-endpoint\_security-any-running** (highlighted with a red box and circled with a red number 19)
- eip-object-endpoint\_security-crowdstrike
- eip-object-endpoint\_security-sentinelone
- eip-object-endpoint\_security-software-crowdstrike
- eip-object-endpoint\_security-software-sentinelone
- eip-object-endpoint\_security-any-installed (highlighted with a red box and circled with a red number 20)

Cancel      Add

Click **Add** again.

Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

Create EIP Profile

1 Rules      2 Review & Submit

Add Rules

Name\*  
EIP\_SomeEndPointSec

Description

+Add    Select Columns

Category	Objects	User Defined Objects	Predefined Objects
Endpoint Security	1		> eip-object-endpoint_security-any-installed

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

Cancel      Add (highlighted with a red box and circled with a red number 21)

Click Next.

Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

**Create EIP Profile**

1 Rules 2 Review & Submit

**Rules**

**Add** **Reorder** **Delete** **Select Columns**

Name	Description	Match Categories
EIP_SomeEndPointSec		Endpoint Security

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

**Cancel** **Back** **Skip to Review** **Next 22**

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

Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

**Create EIP Profile**

1 Rules 2 Review & Submit

**Review your EIP Profiles configuration below**

**General**

Name **EIP\_EndPtSecRunning** **23** Description

Tags

Press Enter to add

**Rules** **Edit**

Name	Category	Objects	User Defined Objects	Predefined Objects
EIP_SomeEndPointSec	Endpoint Security	1		> eip-object-endpoint_security-any-installed

**Cancel** **Back** **Save 24**

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

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

Create Client-based Access Rule

Match Criteria

Action

Operating System

Users & Groups

Endpoint Posture

Source Geo Location & Source IP Address

Traffic Action

Gateways

Client Configuration

Agent Profile From EIP

Review & Configure

By default, we have chosen all endpoint devices under endpoint information profile and entity risk bands to apply to your security enforcements.

If you'd like, you can customize your options by choosing what to include or exclude below.

← Back

Endpoint Information Profile (EIP)

Select an existing profile or create a new profile with the values for the different EIP attributes collected by the Versa Client. This can be used by the Versa Cloud Gateways for granular policy enforcement based on the end user's entity risk.

User Defined (1) Predefined

+ Create New EIP Profile

+ Add Existing EIP Profile Delete Select Columns

	Name	Description	Rules
<input type="checkbox"/>	EIP_EndPtSecRunning		1

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

Cancel Back Skip to Review Next 25

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

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

Create Client-based Access Rule

Match Criteria

Action

Operating System

Users & Groups

Endpoint Posture

Source Geo Location & Source IP Address

Traffic Action

Gateways

Client Configuration

Agent Profile From EIP

Review & Configure

By default we've chosen all source geo locations and source IP addresses.

These are location selections for allowing or denying access to the Versa Client. If you prefer, you can select specific geo locations.

Source Geo Location ⓘ

- All Geo locations are selected

Customize 26

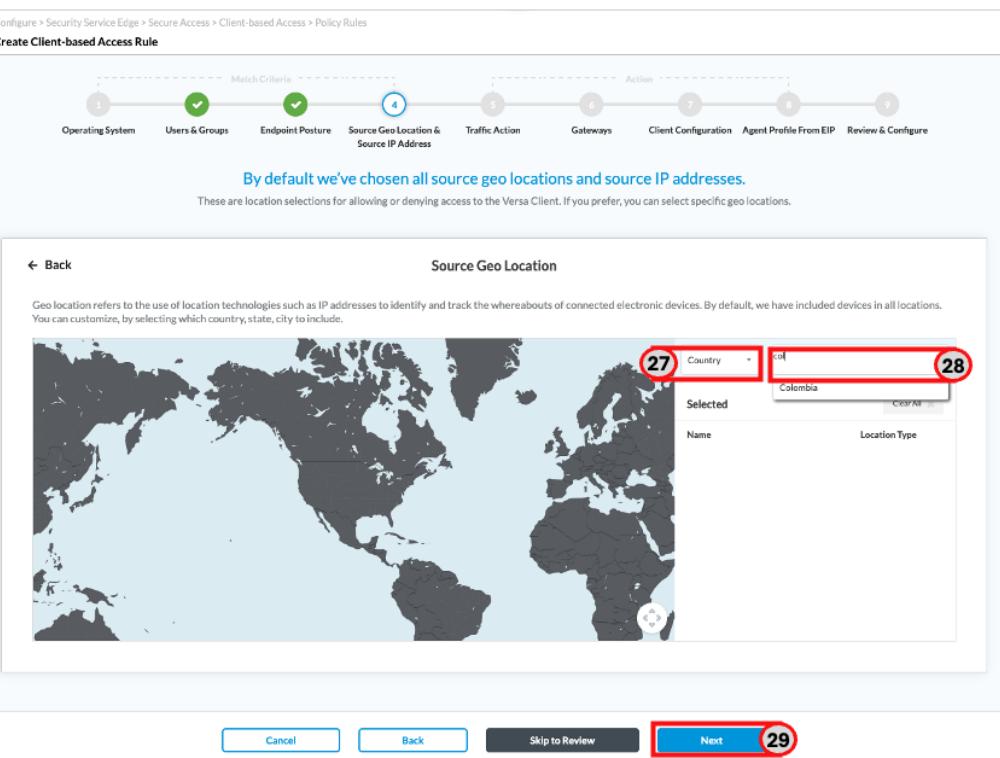
Source IP Address ⓘ

- No source IP addresses have been added

Customize

Cancel Back Skip to Review Next

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



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

Create Client-based Access Rule

Match Criteria

Action

Operating System

Users & Groups

Endpoint Posture

Source Geo Location & Source IP Address

Traffic Action

Gateways

Client Configuration

Agent Profile From EIP

Review & Configure

By default we've chosen all source geo locations and source IP addresses.

These are location selections for allowing or denying access to the Versa Client. If you prefer, you can select specific geo locations.

← Back

Source Geo Location

Geo location refers to the use of location technologies such as IP addresses to identify and track the whereabouts of connected electronic devices. By default, we have included devices in all locations. You can customize, by selecting which country, state, city to include.

27 Country  28

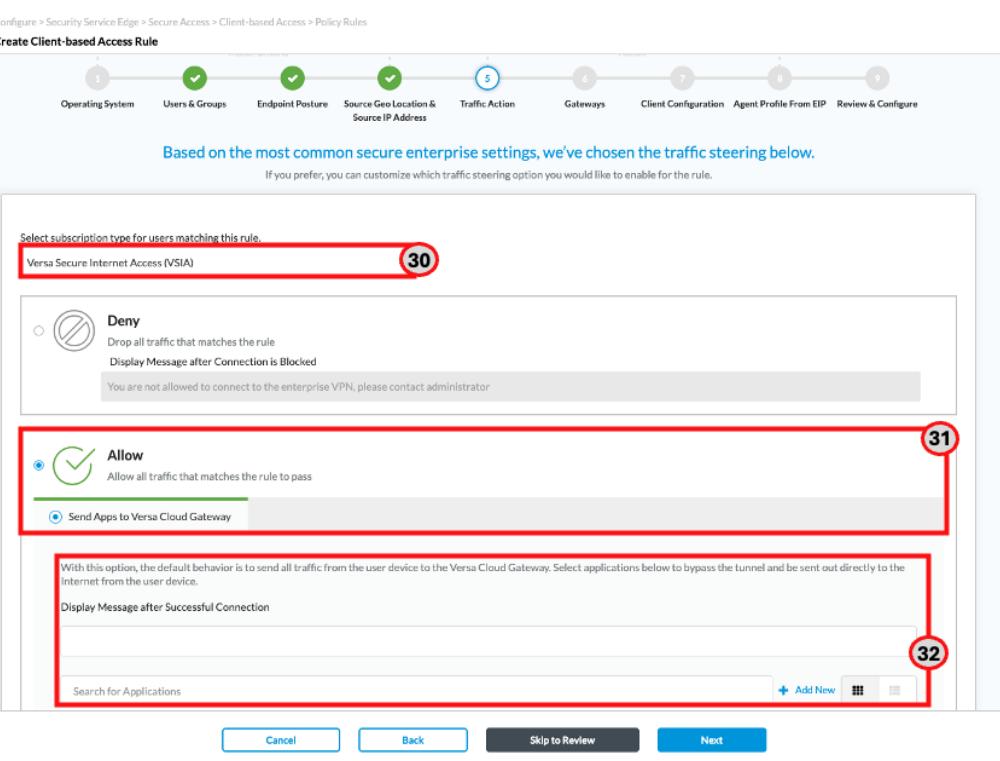
Selected

Name: Colombia

Location Type: City/State

Cancel Back Skip to Review Next 29

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 below.



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

Create Client-based Access Rule

Match Criteria

Action

Operating System

Users & Groups

Endpoint Posture

Source Geo Location & Source IP Address

Traffic Action

Gateways

Client Configuration

Agent Profile From EIP

Review & Configure

Based on the most common secure enterprise settings, we've chosen the traffic steering below.

If you prefer, you can customize which traffic steering option you would like to enable for the rule.

Select subscription type for users matching this rule.

30 Versa Secure Internet Access (VSIA)

Deny

Drop all traffic that matches the rule

Display Message after Connection is Blocked

You are not allowed to connect to the enterprise VPN, please contact administrator

Allow

31 Allow all traffic that matches the rule to pass

Send Apps to Versa Cloud Gateway

With this option, the default behavior is to send all traffic from the user device to the Versa Cloud Gateway. Select applications below to bypass the tunnel and be sent out directly to the Internet from the user device.

Display Message after Successful Connection

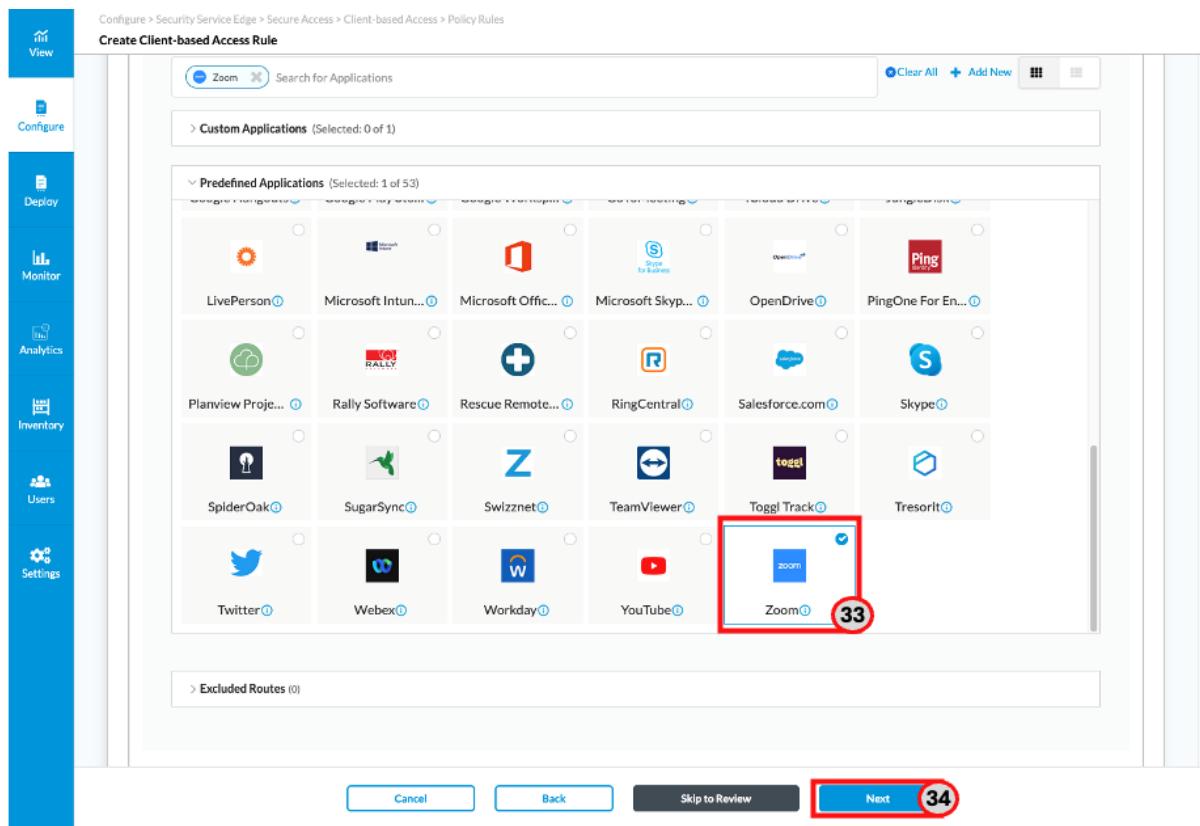
32 Search for Applications

Add New

Cancel Back Skip to Review Next 31 32

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

Applications list, then click **Next**.



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

Create Client-based Access Rule

Search for Applications

Custom Applications (Selected: 0 of 1)

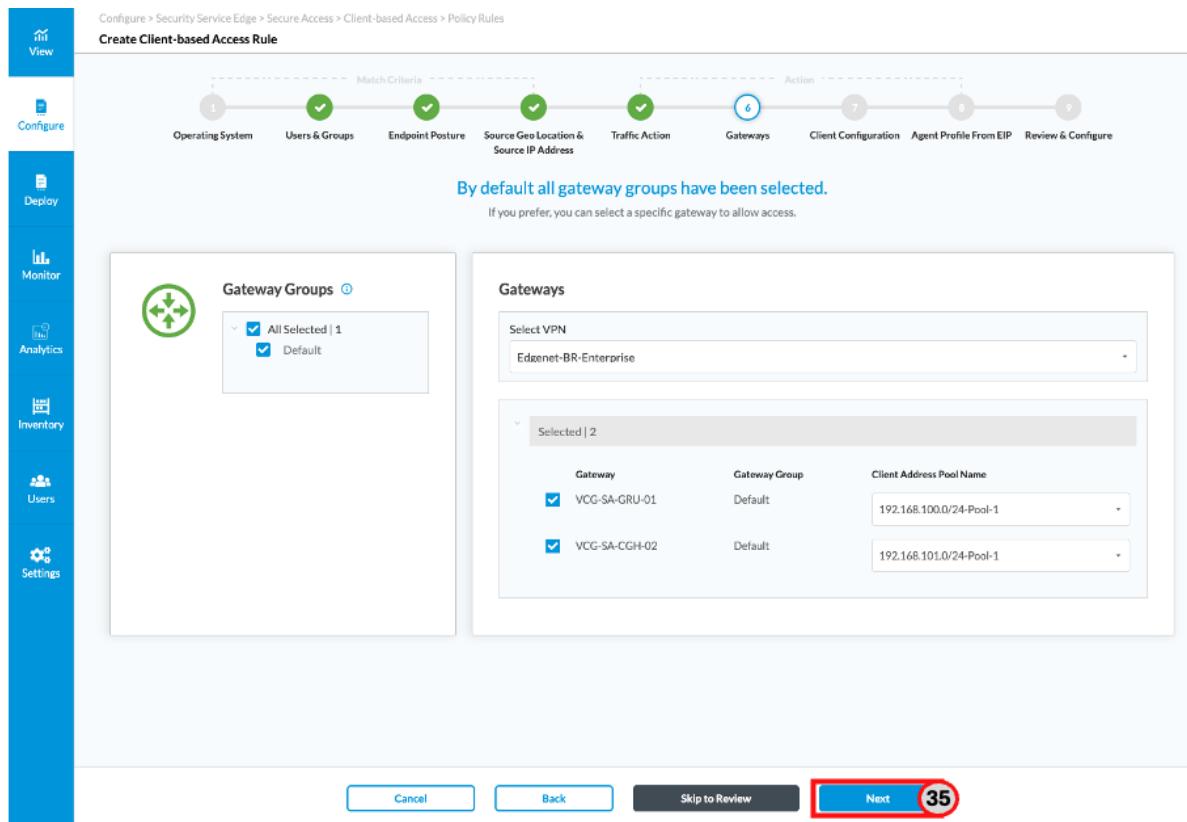
Predefined Applications (Selected: 1 of 53)

LivePerson, Microsoft Intun..., Microsoft Offic..., Microsoft Skyp..., OpenDrive, PingOne For En...  
 Planview Proj..., Rally Software, Rescue Remote..., RingCentral, Salesforce.com, Skype  
 SpiderOak, SugarSync, Swizznet, TeamViewer, Toggl Track, Tresorit  
 Twitter, Webex, Workday, YouTube, Zoom

Excluded Routes (0)

Cancel, Back, Skip to Review, **Next** (34)

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



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

Create Client-based Access Rule

Match Criteria

Operating System, Users & Groups, Endpoint Posture, Source Geo Location & Source IP Address, Traffic Action, Gateways, Client Configuration, Agent Profile From EIP, Review & Configure

By default all gateway groups have been selected.  
 If you prefer, you can select a specific gateway to allow access.

Gateway Groups (1)  
 All Selected | 1  
 Default

Gateways

Select VPN  
 Edenet-BR-Enterprise

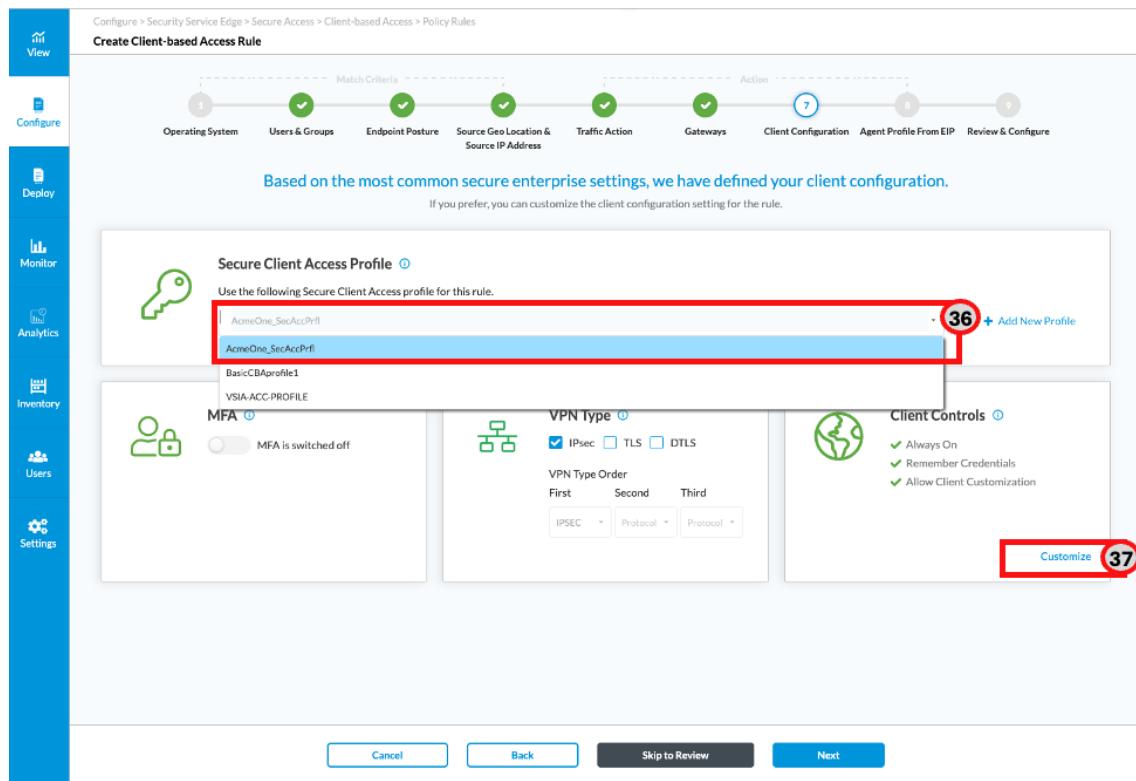
Selected | 2

Gateway	Gateway Group	Client Address Pool Name
VCG-SA-GRU-01	Default	192.168.100.0/24-Pool-1
VCG-SA-CGH-02	Default	192.168.101.0/24-Pool-1

Cancel, Back, Skip to Review, **Next** (35)

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

## Client Controls box.



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

Create Client-based Access Rule

Match Criteria: Operating System, Users & Groups, Endpoint Posture, Source Geo Location & Source IP Address, Traffic Action, Gateways, Client Configuration, Agent Profile From EIP, Review & Configure

**Based on the most common secure enterprise settings, we have defined your client configuration.**  
If you prefer, you can customize the client configuration setting for the rule.

**Secure Client Access Profile** (36)  
Use the following Secure Client Access profile for this rule.  
AcmeOne\_SecAccPrfl  
AcmeOne\_SecAccPrfl  
BasicCBAprofile1  
VSIA-ACC-PROFILE

**MFA** (38)  
MFA is switched off

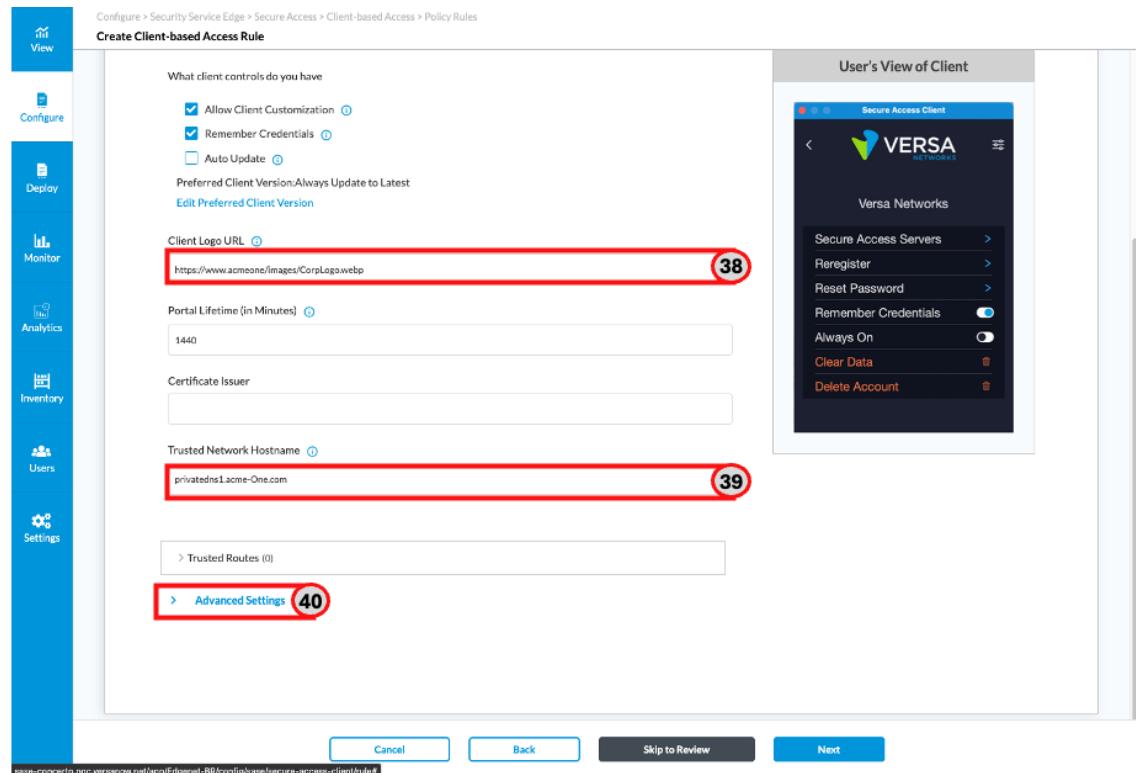
**VPN Type** (38)  
IPsec (checked), TLS, DTLS  
VPN Type Order: First, Second, Third  
IPSEC, Protocol, Protocol

**Client Controls** (37)  
Always On, Remember Credentials, Allow Client Customization

Customize (37)

Cancel, Back, Skip to Review, Next

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 .



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

Create Client-based Access Rule

What client controls do you have  
 Allow Client Customization  
 Remember Credentials  
 Auto Update

Preferred Client Version: Always Update to Latest  
Edit Preferred Client Version

**Client Logo URL** (38)  
https://www.acmeone/images/CorpLogo.webp

Portal Lifetime (in Minutes) (38)  
1440

Certificate Issuer

**Trusted Network Hostname** (39)  
privatedns1acme-one.com

Trusted Routes (0)

> Advanced Settings (40)

Cancel, Back, Skip to Review, Next

User's View of Client (Preview):  
 Secure Access Client  
 VERSA NETWORKS  
 Versa Networks  
 Secure Access Servers >  
 Reregister >  
 Reset Password >  
 Remember Credentials (checked)  
 Always On (checked)  
 Clear Data  
 Delete Account

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 > Security Service Edge > Secure Access > Client-based Access > Policy Rules  
Create Client-based Access Rule

Match Criteria: Operating System, Users & Groups, Endpoint Posture, Source Geo Location & Source IP Address, Traffic Action, Gateways, Client Configuration, Agent Profile From EIP, Review & Configure

Review your Client-based Access Rule Configurations below

General

Name \*  48

Description

Tags

Rule is Enabled

Operating Systems

Operating System Versions

Windows | 13  
Windows 10  
Windows 10 Mobile  
Windows 11  
Windows 7  
Windows 8  
Windows 8.1  
Windows Server 2012  
Windows Server 2012 R2  
Windows Server 2016

Cancel Back Save 49

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

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

Match Criteria: Operating System, Users & Groups, Endpoint Posture, Source Geo Location & Source IP Address, Traffic Action, Gateways, Client Configuration, Agent Profile From EIP, Review & Configure

Review your Client-based Access Rule Configurations below

General

Name \*

Tags

Rule is Enabled

Operating Systems

Operating System Versions

Windows | 13  
Windows 10  
Windows 10 Mobile  
Windows 11  
Windows 7  
Windows 8  
Windows 8.1  
Windows Server 2012  
Windows Server 2012 R2  
Windows Server 2016

Configure Rule Order

How would you like to process rule "AcmeOneSecAccRule1T"?

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) 50

Process the rule in specific placement (select where to place in rule list)

Cancel Save 51

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.

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

**Client-based Access Rules**

Below are all the rules for your Secure Client-based Access.

Rule Name	Operating System Versions	Users & Groups	EIP & Entity Risk Bands	Endpoint Posture	Device Compliance Status	Traffic Action	VPN & Gateway Groups	Status
<input checked="" type="checkbox"/> AcmeOneSecAccRule1 52	✓ Windows Windows 10 Windows 10 Mobile Windows 11 <a href="#">More Details</a>	✓ AuthProfile_SAMA User Groups IT	Endpoint Information Profile (EIP) ✓ User Defined EIP_EndPtSecRunning Entity Risk Bands All risk bands	✓ Managed Status of Devices All Devices	Action Send Apps to Versa Cloud No Client Applications selected ✓ Exclude PreDefined Applications Zoom	VPN Name Edgenet-BR-Enterprise ✓ Gateway Groups Default ✓ Gateways VCG-SA-GRU-01 VCG-SA-CGH-02	Enabled	
<input type="checkbox"/> Acc_Prf_Usuarios	✓ Windows Windows 10 Windows 10 Mobile Windows 11 <a href="#">More Details</a>	✓ SAMALGW1 User Groups Usuarios	Endpoint Information Profile (EIP) ✓ User Defined TestIP Entity Risk Bands All risk bands	✓ Managed Status of Devices All Devices	Action Send Apps to Versa Cloud No Client Applications selected ✓ Exclude PreDefined Applications Zoom Microsoft Office 365 Outlook.com	VPN Name Edgenet-BR-Enterprise ✓ Gateway Groups Default ✓ Gateways VCG-SA-GRU-01 VCG-SA-CGH-02	Enabled	
<input type="checkbox"/> Acc_Prf_Ingenieros	✓ Windows Windows 10 Windows 10 Mobile Windows 11 <a href="#">More Details</a>	✓ SAMALGW1 User Groups Usuarios	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	✓ Managed Status of Devices All Devices	Action Send Apps to Versa Cloud No Client Applications selected ✓ Exclude PreDefined Applications Zoom Microsoft Office 365 Outlook.com	VPN Name Edgenet-BR-Enterprise ✓ Gateway Groups Default ✓ Gateways VCG-SA-GRU-01 VCG-SA-CGH-02	Enabled	
<input type="checkbox"/> TestSAML	✓ Windows Windows 10 Windows 10 Mobile Windows 11 <a href="#">More Details</a>	✓ SAMALGW1 User Groups Ingenieros Usuarios	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	✓ Managed Status of Devices All Devices	Action Breakout to the Internet No Client Applications selected No Predefined Applications selected	VPN Name Edgenet-BR-Enterprise ✓ Gateway Groups Default ✓ Gateways	Enabled	

Showing 1-7 of 7 results 10 + Rows per Page Go to page 1 + < Previous 1 Next >

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

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

**Edit Client-based Access Rule: AcmeOneSecAccRuleContractors**

**Name** 54

**Description** Enter description name

**Tags** Press Enter to add

**Rule is Enabled**

**Operating Systems** [Edit](#)

Operating System Versions Custom Selection

- Windows 10
- Windows 10 Mobile
- Windows 11
- Windows 7
- Windows 8
- Windows 8.1
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

**Users & Groups** [Edit](#) 55

Users & Groups AuthProfile\_SAMA

User Group | 1  
IT

**Buttons** Cancel Back Save

Click **Customize** for Users & Groups.

Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules  
Edit Client-based Access Rule: AcmeOneSecAccRuleContractors

Match Criteria: 1. Operating System, 2. Users & Groups, 3. Endpoint Posture, 4. Source Geo Location & Source IP Address, 5. Traffic Action, 6. Gateways, 7. Client Configuration, 8. Agent Profile From EIP, 9. Review & Configure

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

**Users & Groups**  
User Groups: IT  
Customize 56

Cancel Back Skip to Review Next

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

Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules  
Edit Client-based Access Rule: AcmeOneSecAccRuleContractors

Match Criteria: 1. Operating System, 2. Users & Groups, 3. Endpoint Posture, 4. Source Geo Location & Source IP Address, 5. Traffic Action, 6. Gateways, 7. Client Configuration, 8. Agent Profile From EIP, 9. Review & Configure

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

**Users & Groups**  
User Type: Selected Users  
Enable Rule for the following matched users or user groups: AuthProfile\_SAML  
User Groups: Contractors  
Search for User Groups: Contractors  
User Groups (2):  
1. IT (57) (unchecked)  
2. Contractors (58) (checked)

Cancel Back Skip to Review Next 59

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

Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules  
Edit Client-based Access Rule: AcmeOneSecAccRuleContractors

Match Criteria: 1. Operating System, 2. Users & Groups, 3. Endpoint Posture, 4. Source Geo Location & Source IP Address, 5. Traffic Action, 6. Gateways, 7. Client Configuration, 8. Agent Profile From EIP, 9. Review & Configure

By default, we have chosen all endpoint devices under endpoint information profile and entity risk bands to apply to your security enforcements.

If you'd like, you can customize your options by choosing what to include or exclude below.

**Endpoint Information Profile (EIP)**  
✓ User Defined  
EIP\_EndPtSecRunning  
Customize

**Device Compliance Status**  
✓ Managed Status of Devices  
All Devices  
Customize

**Entity Risk Bands**  
✓ All risk bands  
Customize

**Next 60**

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

Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules  
Edit Client-based Access Rule: AcmeOneSecAccRuleContractors

Match Criteria: 1. Operating System, 2. Users & Groups, 3. Endpoint Posture, 4. Source Geo Location & Source IP Address, 5. Traffic Action, 6. Gateways, 7. Client Configuration, 8. Agent Profile From EIP, 9. Review & Configure

By default we've chosen all source geo locations and source IP addresses.

These are location selections for allowing or denying access to the Versa Client. If you prefer, you can select specific geo locations.

**Source Geo Location**  
✓ Countries  
Colombia  
Customize 61

**Source IP Address**  
No source IP addresses have been added  
Customize

**Next**

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

Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules  
Edit Client-based Access Rule: AcmeOneSecAccRuleContractors

Match Criteria

Operating System    Users & Groups    Endpoint Posture    **Source Geo Location & Source IP Address**    Traffic Action    Gateways    Client Configuration    Agent Profile From EIP    Review & Configure

By default we've chosen all source geo locations and source IP addresses.  
These are location selections for allowing or denying access to the Versa Client. If you prefer, you can select specific geo locations.

Source Geo Location

Geo location refers to the use of location technologies such as IP addresses to identify and track the whereabouts of connected electronic devices. By default, we have included devices in all locations. You can customize, by selecting which country, state, city to include.

Selected (62)

Next (63)

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

Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules  
Edit Client-based Access Rule: AcmeOneSecAccRuleContractors

Internet from the user device.  
Display Message after Successful Connection

Search for Applications (64)

Custom Applications (Selected: 0 of 1)

Predefined Applications (Selected: 1 of 53)

Zoom

Next (65)

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 2<sup>nd</sup>, then click **Save**.

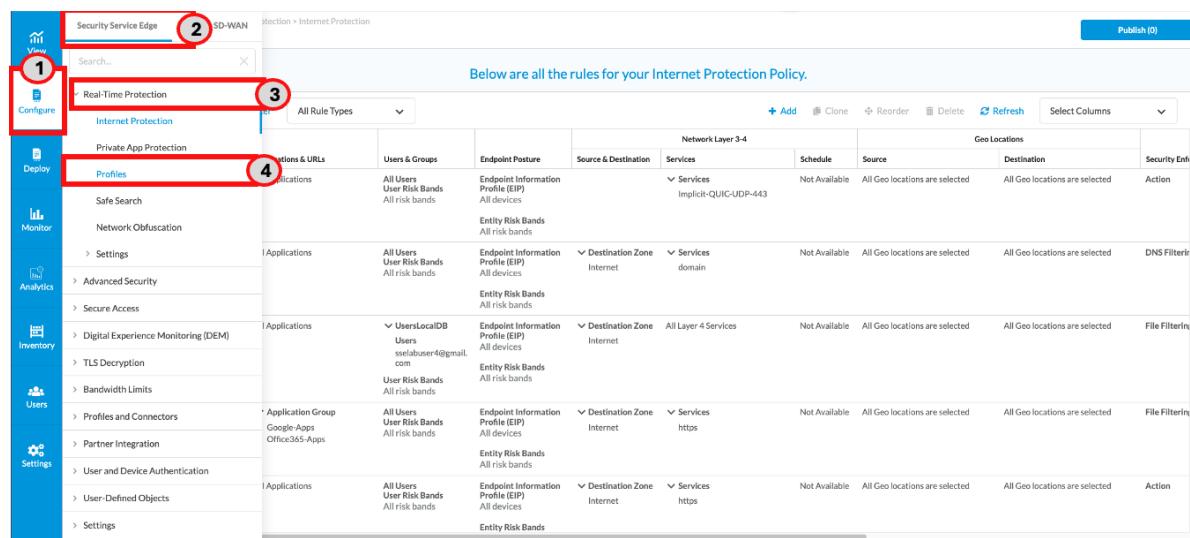
## Step 4: Configure DNS Filtering to Block AAAA Queries

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.

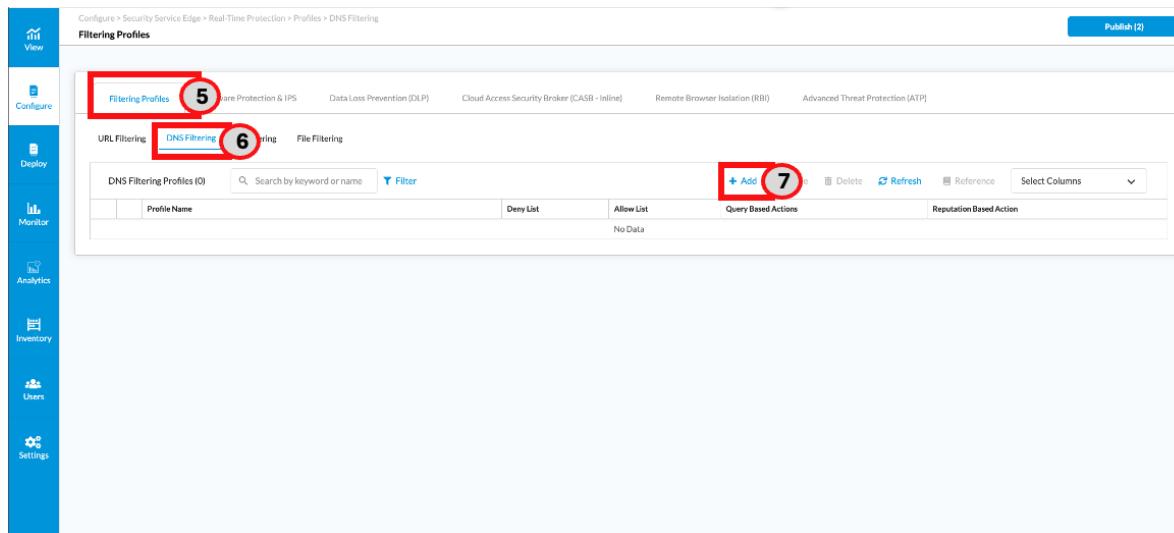
Parameter	Description
Profile Name	Descriptive name for the DNS Filtering Profile
Query Base Action Rule Name	Descriptive name for the Query Base Action Rule
Request Type	Define Query as Request Type
Query Type	Define AAAA as Query Type
Domain Name	Use .* to block all AAAA queries

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



The screenshot shows the VERSA UI interface. The left sidebar has sections for View, Configure, Deploy, Monitor, Analytics, Inventory, Users, and Settings. The main area is titled 'Real-Time Protection' under 'Internet Protection'. It shows a table of rules with columns for Applications & URLs, Users & Groups, Endpoint Posture, Source & Destination, Services, Schedule, Source, Destination, and Security Enf. A red box labeled '1' highlights the 'Configure' icon in the sidebar. A red box labeled '2' highlights the 'Security Service Edge' tab in the top navigation. A red box labeled '3' highlights the 'Real-Time Protection' section. A red box labeled '4' highlights the 'Profiles' link in the 'Real-Time Protection' section.

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



Configure > Security Service Edge > Real-Time Protection > Profiles > DNS Filtering

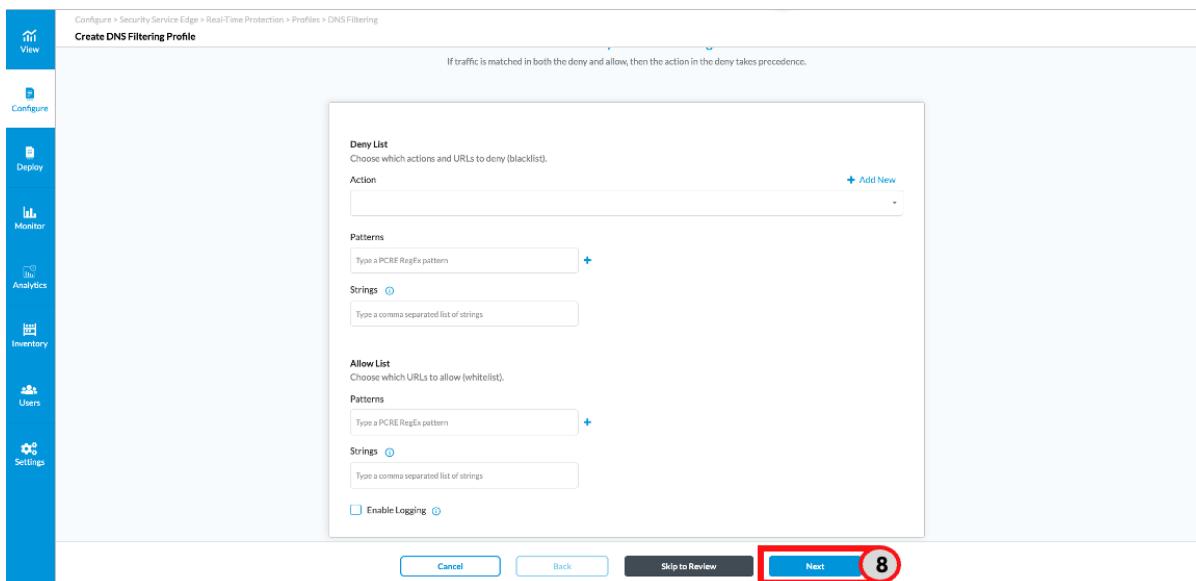
**Filtering Profiles**

5 **Filtering Profiles**

6 **DNS Filtering**

7 **+ Add**

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



Configure > Security Service Edge > Real-Time Protection > Profiles > DNS Filtering

**Create DNS Filtering Profile**

If traffic is matched in both the deny and allow, then the action in the deny takes precedence.

**Deny List**  
Choose which actions and URLs to deny (blacklist).

**Action** **+ Add New**

**Patterns**  
Type a PCRE RegEx pattern **+**

**Strings** **0**  
Type a comma separated list of strings

**Allow List**  
Choose which URLs to allow (whitelist).

**Patterns**  
Type a PCRE RegEx pattern **+**

**Strings** **0**  
Type a comma separated list of strings

**Enable Logging** **0**

**Cancel** **Back** **Skip to Review** **Next** 8

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

Configure > Security Service Edge > Real-Time Protection > Profiles > DNS Filtering  
Create DNS Filtering Profile

Deny & Allow List    2. Query Based Actions    Reputation Based Action    Review & Submit

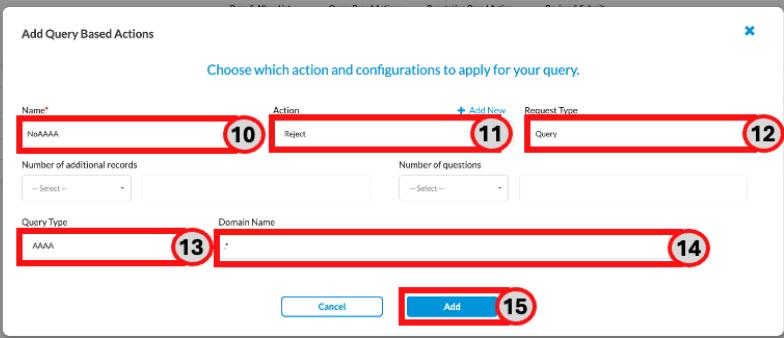
By default, all fields have been configured. Otherwise, you can choose which queries to enforce for your DNS filtering.

Name	Action	Request Type	Details
			No Data

+ Add 9    Select Columns

Cancel    Back    Skip to Review    Next

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**.



Configure > Security Service Edge > Real-Time Protection > Profiles > DNS Filtering

Create DNS Filtering Profile

Add Query Based Actions

Choose which action and configurations to apply for your query.

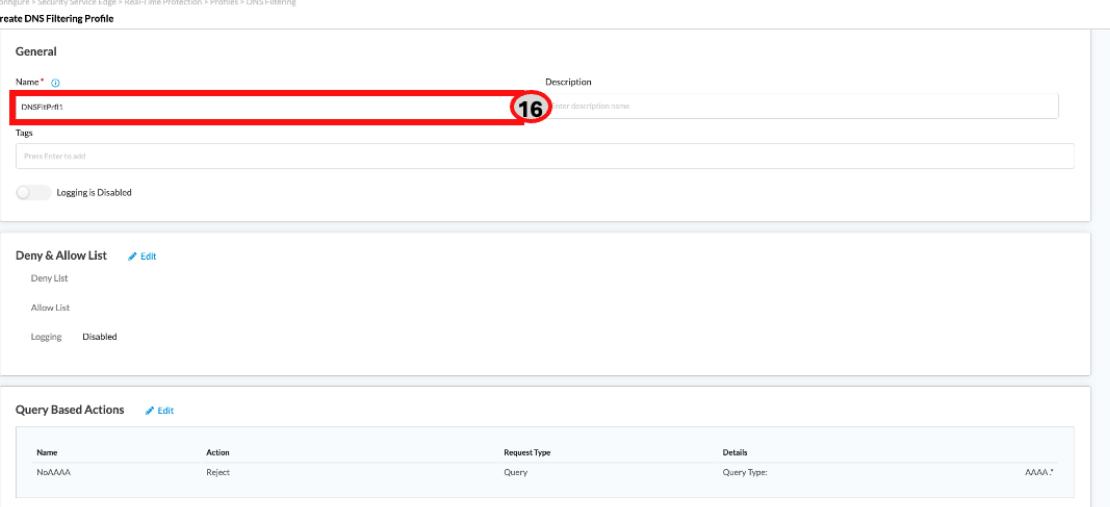
Name\* **10** Action **11** Request Type **12**

Number of additional records **13** Number of questions **14**

Query Type **15** Domain Name

Cancel Next **16**

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



Configure > Security Service Edge > Real-Time Protection > Profiles > DNS Filtering

Create DNS Filtering Profile

General

Name\* **16** Description

Tags

Logging is Disabled

Deny & Allow List

Deny List	Allow List
Logging: Disabled	

Query Based Actions

Name	Action	Request Type	Details
NoAAAA	Reject	Query	Query Type: AAAA.*

Cancel Back Save **17**

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.

Configure > Security Service Edge > Real-Time Protection > Internet Protection

Internet Protection Rules List

Below are all the rules for your Internet Protection Policy.

Rule Name	Applications & URLs	Users & Groups	Endpoint Posture	Source & Destination	Schedule	Source	Geo Locations	Destination	Security Enforcement
Implicit_Drop_Quic	All Applications	All Users User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices  Entity Risk Bands All risk bands	Services Implicit-QUIC-UDP-443	Not Available	All Geo locations are selected	All Geo locations are selected	Action	
Implicit-Allow-DNS	All Applications	All Users User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices  Entity Risk Bands All risk bands	Services domain	Not Available	All Geo locations are selected	All Geo locations are selected	Action	
Implicit-Deny-All	All Applications	All Users User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices  Entity Risk Bands All risk bands	Layer 4 Services are not Enabled	Not Available	All Geo locations are selected	All Geo locations are selected	Action	

Showing 1-3 of 3 results 10 Rows per Page Go to page 1 < Previous 1 Next >

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

Configure > Security Service Edge > Real-Time Protection > Internet Protection

Edit Internet Protection Rule: Implicit-Allow-DNS

User Risk Bands All Risk Bands

Endpoint Posture [Edit](#)

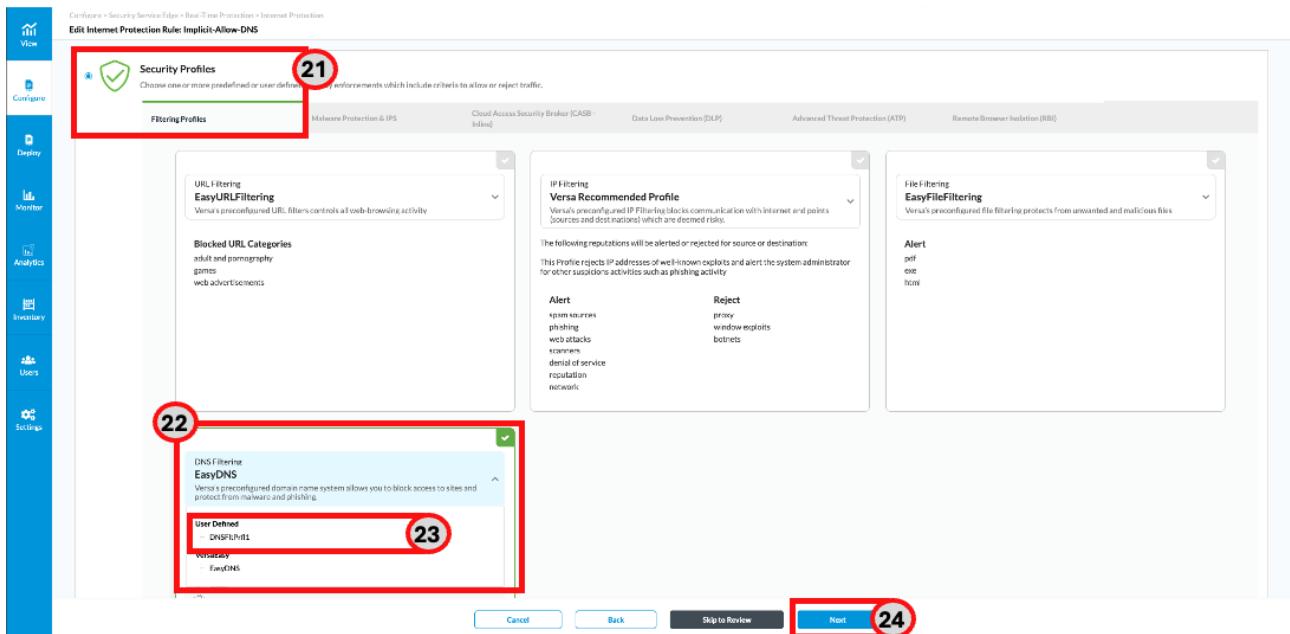
GEO Locations [Edit](#)  
Source  All source Geo locations are selected  
Destination  All destination Geo locations are selected

Network Layer 3-4 [Edit](#)  
Services  
 domain

Security Enforcement [Edit](#) **20**  
Enforcements EasyDNS  
Versa's preconfigured domain name system allows you to block access to sites and protect from malware and phishing.

Cancel Back Save

Change the enforcement action from Allow to **Security Profiles**. Select the **Filtering Profiles** tab, and in the **DNS filtering** section 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.

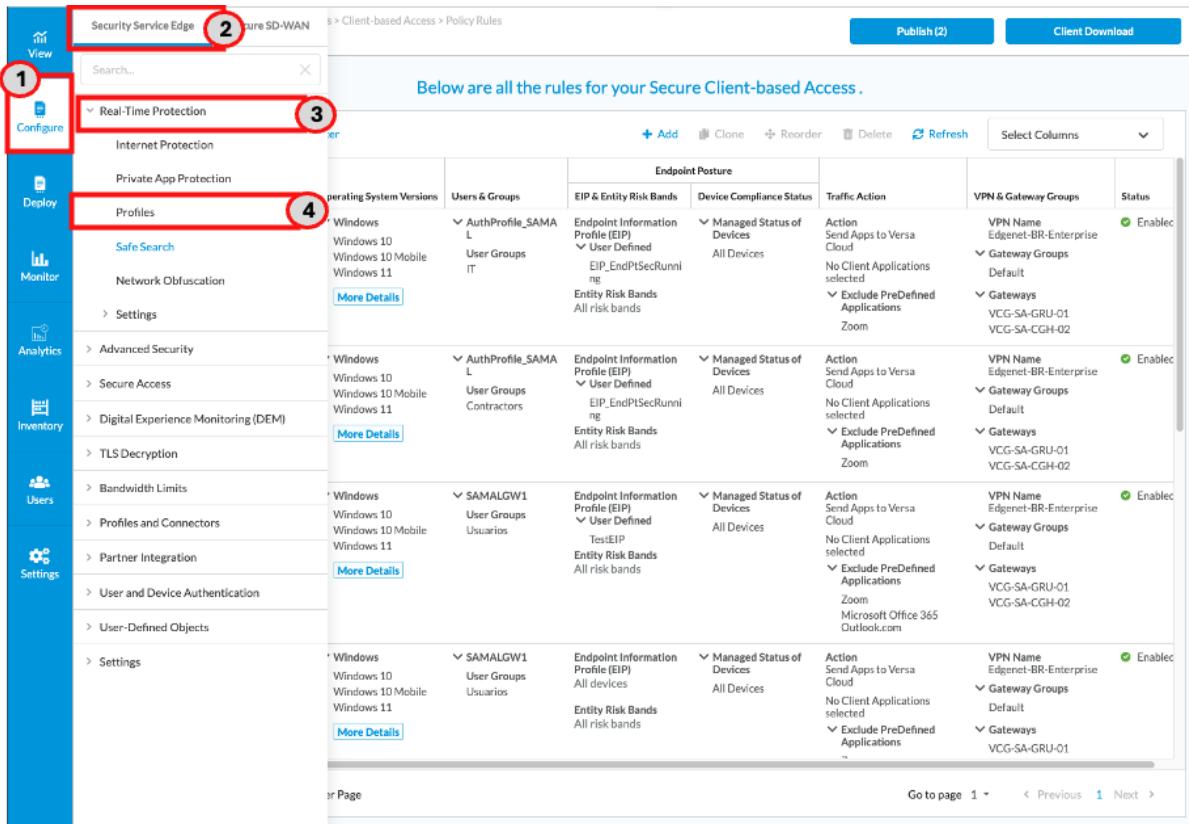
### Why Two Controls Are Required

- 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**.



The screenshot shows the VERSA Security Service Edge interface. The left sidebar has a 'Configure' tab highlighted with a red circle labeled '1'. The main menu bar has a 'Security Service Edge' tab highlighted with a red circle labeled '2'. The 'Real-Time Protection' section is expanded, with a red circle labeled '3' highlighting the 'Profiles' item. A red circle labeled '4' highlights the 'Profiles' section in the main content area. The content area displays a table of policy rules for 'Secure Client-based Access'.

Operating System Versions	Users & Groups	Endpoint Posture		Traffic Action	VPN & Gateway Groups	Status
		EIP & Entity Risk Bands	Device Compliance Status			
Windows	AuthProfile_SAMA L User Groups IT	Endpoint Information Profile (EIP) User Defined EIP_EndPtSecRunni ng Entity Risk Bands All risk bands	Managed Status of Devices All Devices	Action Send Apps to Versa Cloud No Client Applications selected Exclude PreDefined Applications Zoom	VPN Name Edgenet-BR-Enterprise Gateway Groups Default Gateways VCG-SA-GRU-01 VCG-SA-CGH-02	Enabled
Windows	AuthProfile_SAMA L User Groups Contractors	Endpoint Information Profile (EIP) User Defined EIP_EndPtSecRunni ng Entity Risk Bands All risk bands	Managed Status of Devices All Devices	Action Send Apps to Versa Cloud No Client Applications selected Exclude PreDefined Applications Zoom	VPN Name Edgenet-BR-Enterprise Gateway Groups Default Gateways VCG-SA-GRU-01 VCG-SA-CGH-02	Enabled
Windows	SAMALGW1 User Groups Usuarios	Endpoint Information Profile (EIP) User Defined TestEIP Entity Risk Bands All risk bands	Managed Status of Devices All Devices	Action Send Apps to Versa Cloud No Client Applications selected Exclude PreDefined Applications Zoom Microsoft Office 365 Outlook.com	VPN Name Edgenet-BR-Enterprise Gateway Groups Default Gateways VCG-SA-GRU-01 VCG-SA-CGH-02	Enabled
Windows	SAMALGW1 User Groups Usuarios	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Managed Status of Devices All Devices	Action Send Apps to Versa Cloud No Client Applications selected Exclude PreDefined Applications	VPN Name Edgenet-BR-Enterprise Gateway Groups Default Gateways VCG-SA-GRU-01	Enabled

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**

**Cloud Access Security Broker (CASB - Inline)** **5** (highlighted with a red box)

**SaaS Tenant Control** **6** (highlighted with a red box)

**+ Add** **7** (highlighted with a red box)

**Published (2)**

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** Refresh Select Columns

Profile Name	Rules	Application	Action Request
No Data			

View Configure Deploy Monitor Analytics Inventory Users Settings

Click **+ Add**.

Configure > Security Service Edge > Real-Time Protection > Profiles > SaaS Tenant Control

**Create SaaS Tenant Control Profile**

Application Rules **1** → Review & Submit **2**

**Add Application Rules**

**+ Add** **8** (highlighted with a red box)

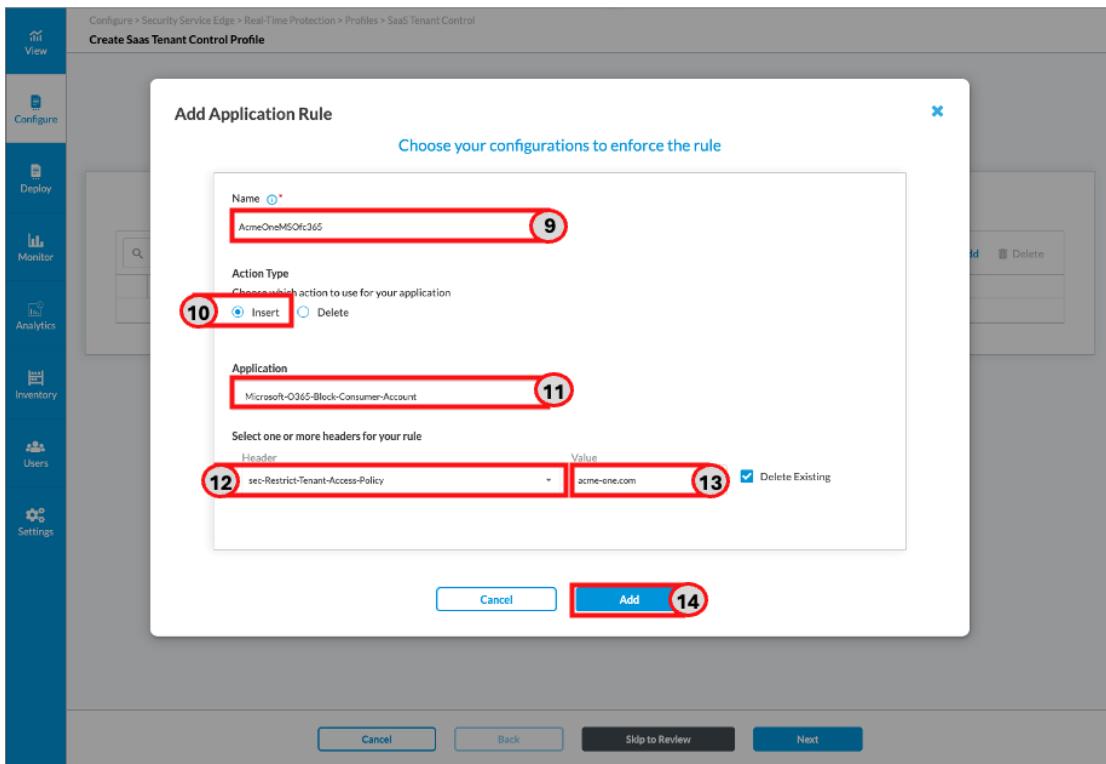
Search

Name	Application	Type	Action Request	Values
No Data				

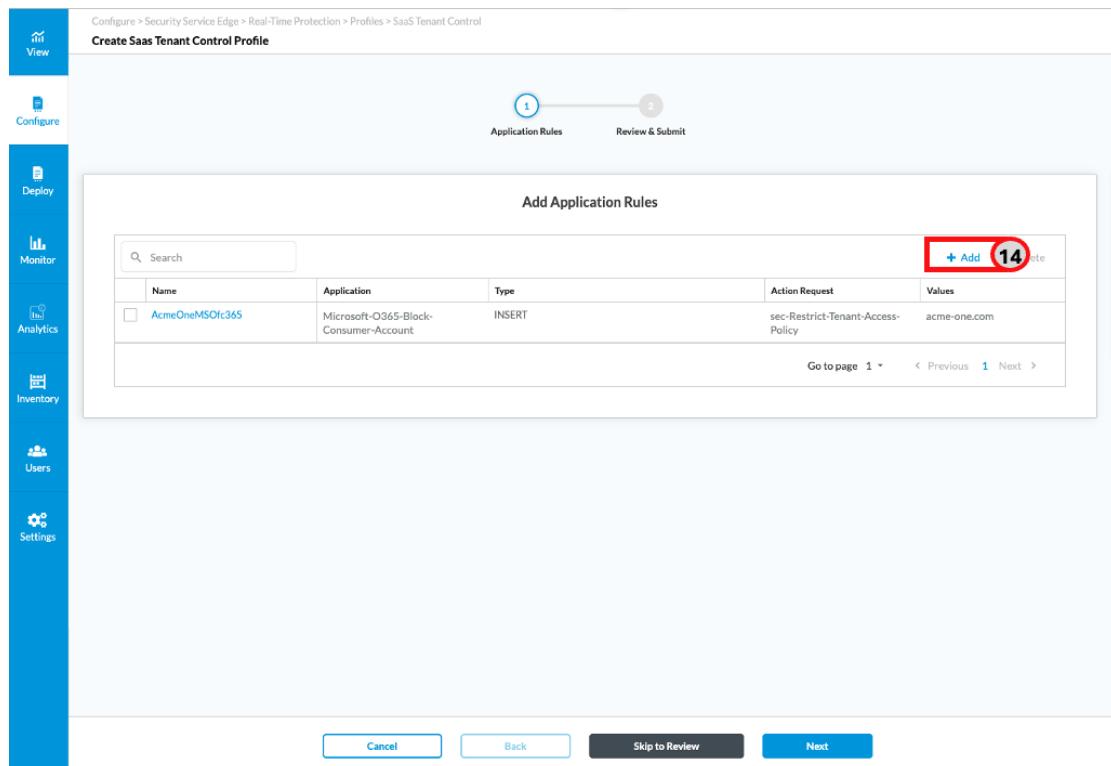
Cancel Back Skip to Review Next

View Configure Deploy Monitor Analytics Inventory Users Settings

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**.

Configure > Security Service Edge > Real-Time Protection > Profiles > SaaS Tenant Control

Create SaaS Tenant Control Profile

Add Application Rule

Choose your configurations to enforce the rule

Name **AcmeOneOf365onlyTnt** **15**

Action Type  
Choose which action to use for your application  
 Insert **16**  Delete

Application  
Microsoft-Office365-Tenant-Restrictions **17**

Select one or more headers for your rule

Header  
 Restrict-Access-To-Tenants **18** Value **acmeone.com** **19**  Delete Existing

Cancel **Add** **20**

Cancel Back Skip to Review **Next** **21**

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

Configure > Security Service Edge > Real-Time Protection > Profiles > SaaS Tenant Control

Create SaaS Tenant Control Profile

Application Rules **1** Review & Submit **2**

Add Application Rules

Search **AcmeOneOf365**

Name	Application	Action Request	Values
AcmeOneOf365	Microsoft-Office365-Tenant-Restrictions	sec-Restrict-Tenant-Access-Policy	acme-one.com

Go to page 1 < Previous 1 Next >

Ok **22**

Cancel Back Skip to Review **Next** **23**

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 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**.

Configure > Security Service Edge > TLS Decryption > Profiles  
Create TLS Decryption Profile

Profile Type      Certificate Setup      Inspection Options      Decryption Options      Review & Validate

**Create a TLS Decryption Profile**

Decryption enforces security policies on encrypted traffic to help prevent malicious content from entering the network and to protect sensitive data disguised as encrypted traffic from leaving the network. You can configure a decryption profile with SSL inspection and policy enforcement information. This section will guide you through the process of configuring the decryption profiles.

**Decryption Profile**

This profile applies both decryption and inspection protocols that you can associate with your decryption rules.

**Inspection Profile**

This profile applies only inspection protocols that you can associate with your decryption rules.

Cancel      Back      Skip to Review      **Next** 7

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

Configure > Security Service Edge > TLS Decryption > Profiles  
Create TLS Decryption Profile

Profile Type      **Certificate Setup**      Inspection Options      Decryption Options      Review & Validate

**We've selected a certificate authority for you by default.**

A certificate authority (CA) is an entity that issues digital certificates to verify the ownership of a public key. Only one certificate can be selected. If you prefer, you can choose another CA to use.

Previously Uploaded Certificates

Acme-one 8 + Add New

**Details**

Name: Acme-one  
File Name: Acme-one.zip  
key: Acme-one.key  
Certificate: Acme-one.crl  
Issued To: VOS Certificate  
Issued By: Versa Concerto Certificate Authority  
Validity: 2024-11-12 23:52:14 to 2029-11-11 23:52:14

Download Certificate

Cancel      Back      Skip to Review      **Next** 9

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

Configure > Security Service Edge > TLS Decryption > Profiles  
Create TLS Decryption Profile

Profile Type      Certificate Setup      **Inspection Options**      Decryption Options      Review & Validate

Based on the most common secure enterprise settings, we've chosen the inspection options, below.  
If you prefer, you can customize which inspection options you'd like to enable for your decryption.

TLS inspection is the process of intercepting and reviewing SSL/TLS encrypted Internet communication between the client and the server. The inspection of SSL/TLS encrypted traffic has become critically important because the vast majority of internet traffic is SSL/TLS encrypted, including malicious traffic.

[More Information](#)

**Certificate Validation**

This is the Internet protocol used by web browsers to determine the revocation status of SSL/TLS certificates supplied by HTTPS websites.

**10** **Verify with OCSP** Enable server certificate verification using the Online Certificate Status Protocol (OCSP). **11** **Block Unknown Certificates** Block SSL sessions whose certificate status is unknown.

Response timeout(seconds) for an OCSP request:  Verify:

**Server Certificate Actions**

Choose what actions should occur for the following server certificate checks.

When the certificate expires, do the following: **12**

When the certificate is received from an untrusted issuer, do the following: **13**

Choose whether to restrict the certificate key usage extensions to either digital signature or key encipherment.

Restrict Certificate Extension

**SSL/TLS Protocol Checks**

Choose what actions should occur for the following SSL/TLS protocol checks.

When the negotiated SSL/TLS protocol between the Client and Server uses an unsupported key length, do the following: **14**

Minimum Supported RSA Key Length:  bits  
Enter a value of 512 bits or higher

When the negotiated SSL/TLS protocol between the Client and Server uses an unsupported cipher, do the following: **15**

When the negotiated SSL/TLS protocol between the Client and Server uses an unsupported protocol version, do the following: **16**

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

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**.

Configure > Security Service Edge > TLS Decryption > Profiles  
Create TLS Decryption Profile

Choose what actions should occur for the following server certificate checks.

When the certificate expires, do the following: **12**

When the certificate is received from an untrusted issuer, do the following: **13**

Choose whether to restrict the certificate key usage extensions to either digital signature or key encipherment.

Restrict Certificate Extension

**SSL/TLS Protocol Checks**

Choose what actions should occur for the following SSL/TLS protocol checks.

When the negotiated SSL/TLS protocol between the Client and Server uses an unsupported key length, do the following: **14**

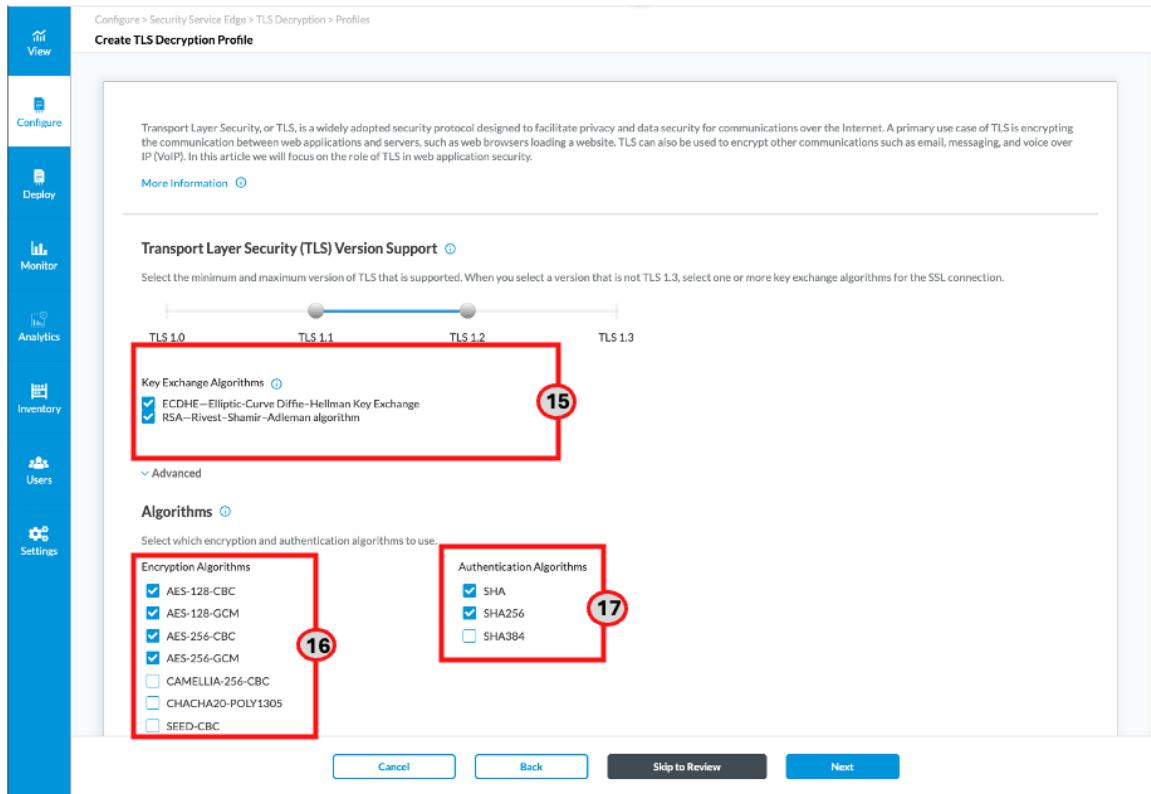
Minimum Supported RSA Key Length:  bits  
Enter a value of 512 bits or higher

When the negotiated SSL/TLS protocol between the Client and Server uses an unsupported cipher, do the following: **15**

When the negotiated SSL/TLS protocol between the Client and Server uses an unsupported protocol version, do the following: **16**

[Cancel](#) [Back](#) [Skip to Review](#) [Next](#) **14**

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



Configure > Security Service Edge > TLS Decryption > Profiles  
Create TLS Decryption Profile

Transport Layer Security (TLS) Version Support

Select the minimum and maximum version of TLS that is supported. When you select a version that is not TLS 1.3, select one or more key exchange algorithms for the SSL connection.

Key Exchange Algorithms

- ECDHE—Elliptic-Curve Diffie-Hellman Key Exchange
- RSA—Rivest-Shamir-Adleman algorithm

15

Advanced

Algorithms

Encryption Algorithms

- AES-128-CBC
- AES-128-GCM
- AES-256-CBC
- AES-256-GCM
- CAMELLIA-256-CBC
- CHACHA20-POLY1305
- SEED-CBC

16

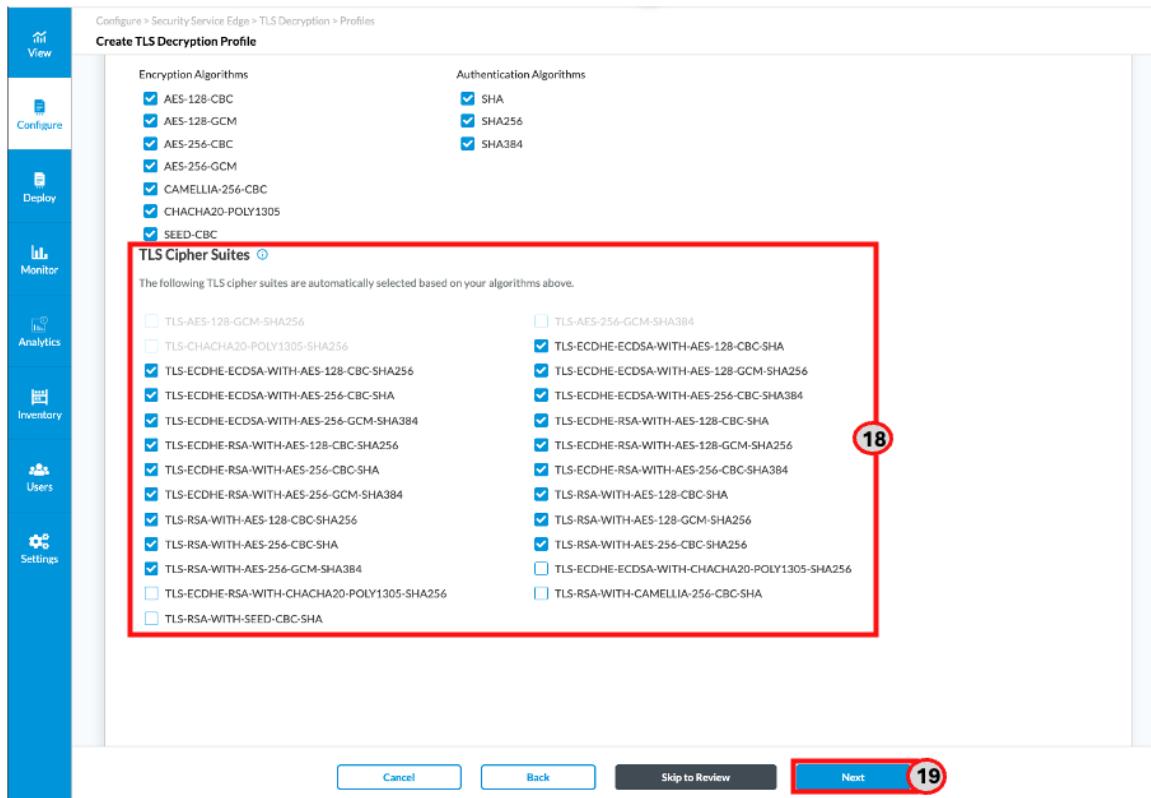
Authentication Algorithms

- SHA
- SHA256
- SHA384

17

Cancel Back Skip to Review Next

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



Configure > Security Service Edge > TLS Decryption > Profiles  
Create TLS Decryption Profile

Encryption Algorithms

- AES-128-CBC
- AES-128-GCM
- AES-256-CBC
- AES-256-GCM
- CAMELLIA-256-CBC
- CHACHA20-POLY1305
- SEED-CBC

Authentication Algorithms

- SHA
- SHA256
- SHA384

TLS Cipher Suites

The following TLS cipher suites are automatically selected based on your algorithms above.

<input type="checkbox"/> TLS-AES-128-GCM-SHA256	<input checked="" type="checkbox"/> TLS-AES-256-GCM-SHA384
<input type="checkbox"/> TLS-CHACHA20-POLY1305-SHA256	<input checked="" type="checkbox"/> TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA
<input checked="" type="checkbox"/> TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256	<input checked="" type="checkbox"/> TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256
<input checked="" type="checkbox"/> TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA	<input checked="" type="checkbox"/> TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384
<input checked="" type="checkbox"/> TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384	<input checked="" type="checkbox"/> TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA
<input checked="" type="checkbox"/> TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256	<input checked="" type="checkbox"/> TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256
<input checked="" type="checkbox"/> TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA	<input checked="" type="checkbox"/> TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384
<input checked="" type="checkbox"/> TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384	<input checked="" type="checkbox"/> TLS-RSA-WITH-AES-128-CBC-SHA
<input checked="" type="checkbox"/> TLS-RSA-WITH-AES-128-CBC-SHA256	<input checked="" type="checkbox"/> TLS-RSA-WITH-AES-128-GCM-SHA256
<input checked="" type="checkbox"/> TLS-RSA-WITH-AES-256-CBC-SHA	<input checked="" type="checkbox"/> TLS-RSA-WITH-AES-256-CBC-SHA256
<input checked="" type="checkbox"/> TLS-RSA-WITH-AES-256-GCM-SHA384	<input type="checkbox"/> TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256
<input type="checkbox"/> TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256	<input type="checkbox"/> TLS-RSA-WITH-CAMELLIA-256-CBC-SHA
<input type="checkbox"/> TLS-RSA-WITH-SEED-CBC-SHA	

18

Cancel Back Skip to Review Next 19

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

Configure > Security Service Edge > TLS Decryption > Profiles

Create TLS Decryption Profile

Review and name your profile

Below are the configurations of your profile. Review and edit any step of your configuration before validating.

**General**

Name \* **20** Acme-one

Description Enter description name

Tags Press Enter to add

**Certificate Setup** **Edit**

Certificate Authority	Acme-one
Issued For	VOS Certificate
Issued By	Versa Concerto Certificate Authority

**Inspection Options** **Edit**

Online Certificate Status Protocol (OCSP)

Verify with OCSP	Disabled
Block Unknown Certificates	Disabled

Server Certificate Actions

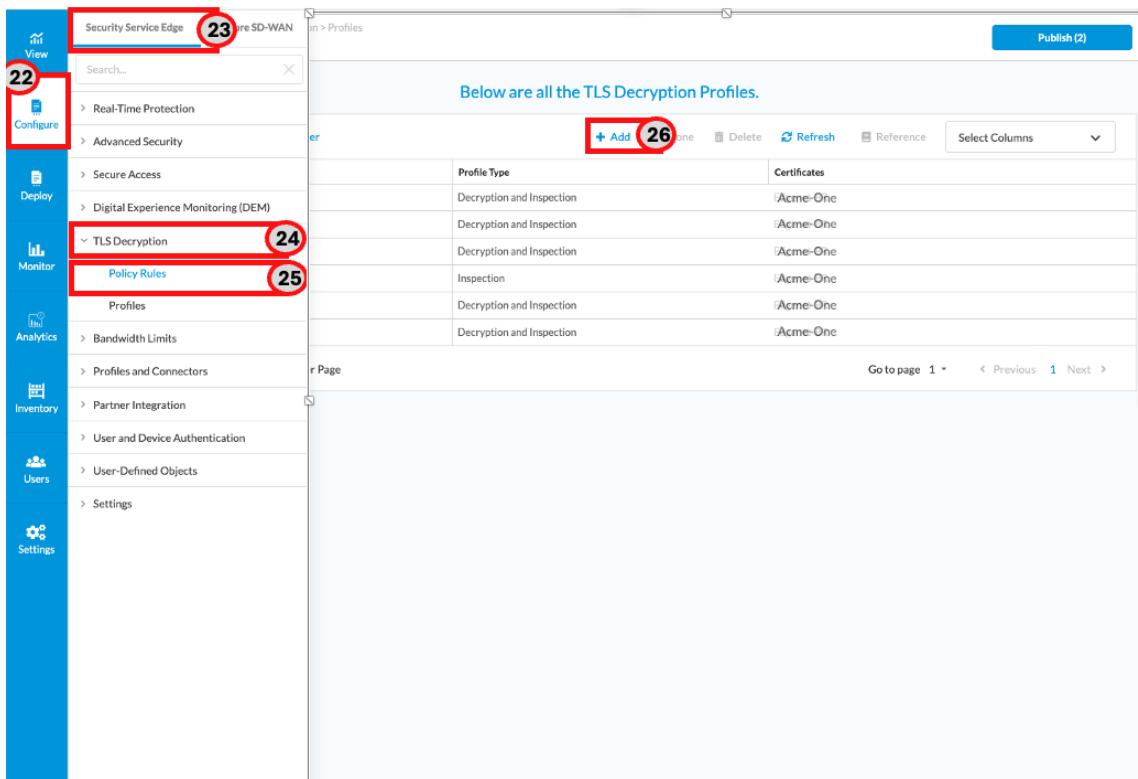
Cancel Back **Save** **21**

## Create TLS Decryption Policy Rules

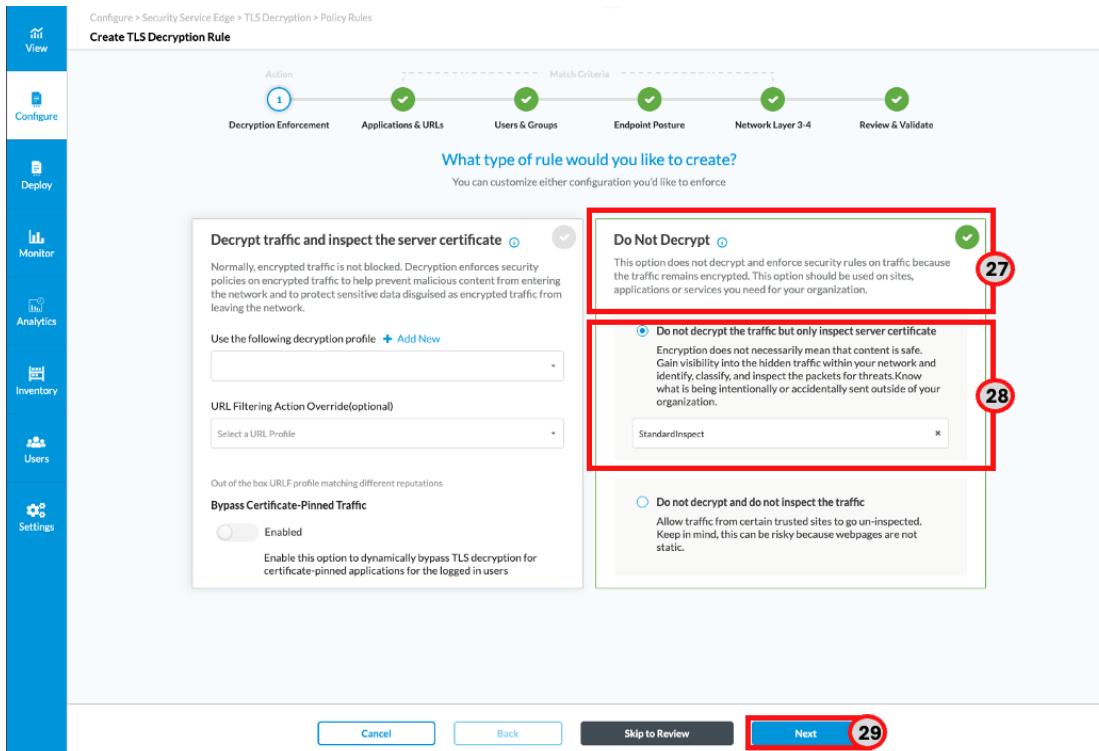
As specified in the use case, two decryption policy rules are needed. The first rule maintains privacy for certain types of regulated traffic, while the second decrypts all remaining traffic.

### 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**.

Configure > Security Service Edge > TLS Decryption > Policy Rules

Create TLS Decryption Rule

Action 1 Match Criteria 2

Decryption Enforcement Applications & URLs Users & Groups Endpoint Posture Network Layer 3-4 Review & Validate

By default, we've included all applications to match.

Applications URL Categories & Reputations **30**

URL Categories [+ Add New](#)

Select one or more URL categories to apply the Rule to.

(financial\_services ) (health\_and\_medicine ) Search or select from list **31**

Reputations

Select one or more reputations to apply the Rule to.

Add Reputation

**Cancel** **Back** **Skip to Review** **Next 32**

Click **Next** in Applications & URLs configuration.

Configure > Security Service Edge > TLS Decryption > Policy Rules

Create TLS Decryption Rule

Action 1 Match Criteria 2 3

Decryption Enforcement Applications & URLs Users & Groups Endpoint Posture Network Layer 3-4 Review & Validate

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

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

Users & Groups

All Users  Customize

**Cancel** **Back** **Skip to Review** **Next 33**

Click **Next** in Endpoint Posture configuration.

Configure > Security Service Edge > TLS Decryption > Policy Rules

Create TLS Decryption Rule

Action: 1. Decryption Enforcement (checked), 2. Applications & URLs (checked), 3. Users & Groups (checked), 4. Endpoint Posture (unchecked), 5. Network Layer 3-4 (unchecked), 6. Review & Validate (unchecked).

Match Criteria: By default, we have chosen all endpoint devices under endpoint information profile and entity risk bands to apply to your security enforcements.

If you'd like, you can customize your options by choosing what to include or exclude below.

**Endpoint Information Profile (EIP)**: All devices (checked). [Customize](#)

**Entity Risk Bands**: All risk bands (checked). [Customize](#)

[Cancel](#) [Back](#) [Skip to Review](#) [Next 34](#)

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

Configure > Security Service Edge > TLS Decryption > Policy Rules

Create TLS Decryption Rule

Action: 1. Decryption Enforcement (checked), 2. Applications & URLs (checked), 3. Users & Groups (checked), 4. Endpoint Posture (checked), 5. Network Layer 3-4 (checked), 6. Review & Validate (unchecked).

All traffic is selected, and it will receive the previously selected security enforcements

If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

**Services**: All layer 4 services (checked). [Customize](#)

**Source & Destination (Layer 3)**: Destination Zone Internet (checked). [Customize](#)

**Schedule**: None Selected. [Customize](#)

[Cancel](#) [Back](#) [Skip to Review](#) [Next 35](#)

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

Configure > Security Service Edge > TLS Decryption > Policy Rules

Create TLS Decryption Rule

Action Match Criteria

Decryption Enforcement Applications & URLs Users & Groups Endpoint Posture Network Layer 3-4 Review & Validate

Review your TLS Decryption Rule configurations below

Below are the configurations of your rule. Review and edit any step of your configuration before deploying.

**General**

Name: AcmeOneNoDecFnINHit

Tags: Press Enter to add

Rule Is Enabled:

**Configure Rule Order**

How would you like to process rule "AcmeOneNoDecFnINHit"?

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) **37**

Process the rule in specific placement (select where to place in rule list)

**Applications & URLs**

URL Categories: financial\_services, health\_and\_medicine

**Decryption Enforcement**

Rule Type: Do Not Decrypt

**Save** **36**

**Save** **38**

## TLS Decryption Policy Rule 2

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

Configure > Security Service Edge > TLS Decryption > Policy Rules

TLS Decryption Rules List

**Below are all the TLS Decryption Rules**

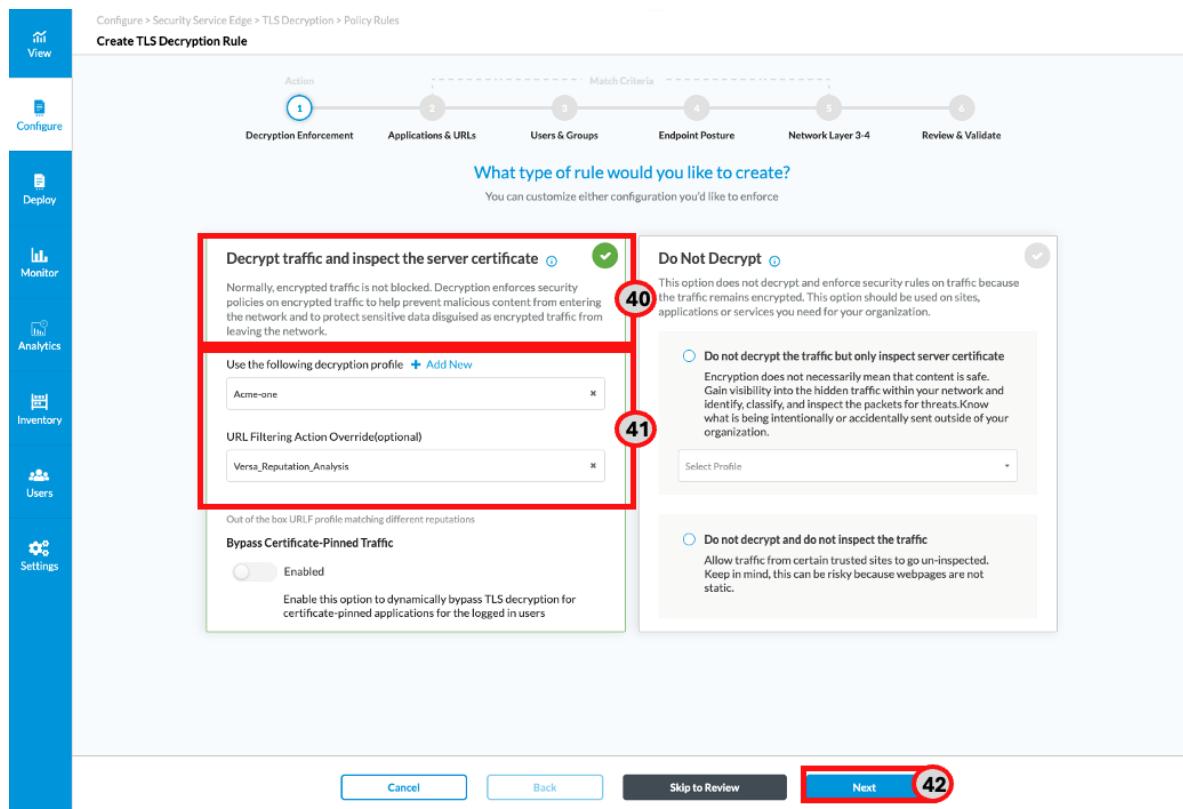
**+ Add** **39**

Rule Name	Decryption Profile	Bypass URL Filtering Profile	Applications & URLs	Users & Groups	Endpoint Posture	Source & Destination	Services
AcmeOneNoDecFnINHit	StandardInspect	None Selected	✓ URL Categories financial_services health_and_medicine	All Users	Endpoint Information Profile (EIP) All devices	✓ Destination Zone Internet	All Layer 4 Services
Decryptptest	Standard	None Selected	All Applications	All Users	Endpoint Information Profile (EIP) All devices	✓ Destination Zone Internet	All Layer 4 Services
Inspecttest	Standard	GenAI_Firewall	All Applications	All Users	Endpoint Information Profile (EIP) All devices	✓ Destination Zone Internet	All Layer 4 Services
M365_Recommended_Policy_Optimize	Do not decrypt and do not inspect the traffic	None Selected	✓ Application O365_WW_OP	All Users	Endpoint Information Profile (EIP) All devices	✓ Destination Zone Internet	Layer 4 Services are not Enabled
M365_Recommended_Policy_Allow	StandardInspect	None Selected	✓ Application O365_WW_AL	All Users	Endpoint Information Profile (EIP) All devices	✓ Destination Zone Internet	Layer 4 Services are not Enabled
M365_Recommended_Policy_Common_and_Default	Standard	None Selected	✓ Application O365_WW_COMM O365_WW_DE	All Users	Endpoint Information Profile (EIP) All devices	✓ Destination Zone Internet	Layer 4 Services are not Enabled

Showing 1-8 of 8 results 10 Rows per Page Go to page 1 < Previous 1 Next >

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

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



Configure > Security Service Edge > TLS Decryption > Policy Rules

Create TLS Decryption Rule

Action

Decryption Enforcement

Applications & URLs

Users & Groups

Endpoint Posture

Network Layer 3-4

Match Criteria

Review & Validate

What type of rule would you like to create?

You can customize either configuration you'd like to enforce

**Decrypt traffic and inspect the server certificate**  ✓

Normally, encrypted traffic is not blocked. Decryption enforces security policies on encrypted traffic to help prevent malicious content from entering the network and to protect sensitive data disguised as encrypted traffic from leaving the network.

Use the following decryption profile  Acme-one

URL Filtering Action Override(optional) Versa\_Reputation\_Analysis

Do Not Decrypt

This option does not decrypt and enforce security rules on traffic because the traffic remains encrypted. This option should be used on sites, applications or services you need for your organization.

Do not decrypt the traffic but only inspect server certificate

Encryption does not necessarily mean that content is safe. Gain visibility into the hidden traffic within your network and identify, classify, and inspect the packets for threats. Know what is being intentionally or accidentally sent outside of your organization.

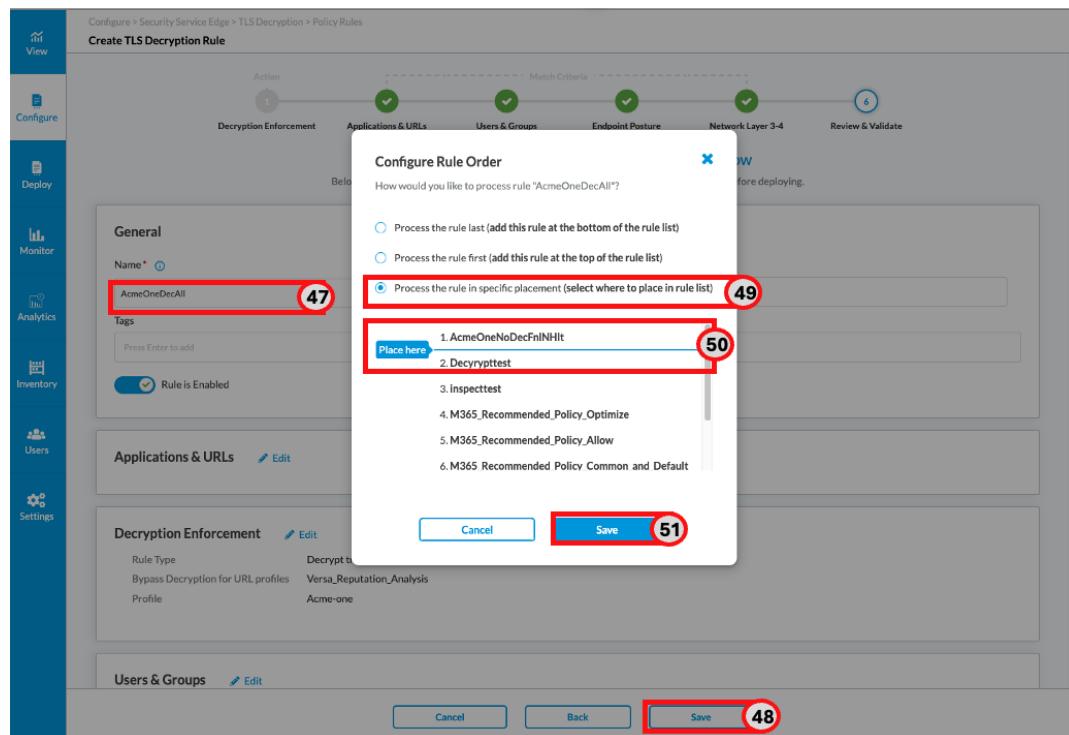
Select Profile

Do not decrypt and do not inspect the traffic

Allow traffic from certain trusted sites to go un-inspected. Keep in mind, this can be risky because webpages are not static.

Cancel Back Skip to Review **Next** 42

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**.



Configure > Security Service Edge > TLS Decryption > Policy Rules

Create TLS Decryption Rule

Action

Decryption Enforcement

Applications & URLs

Users & Groups

Endpoint Posture

Network Layer 3-4

Match Criteria

Review & Validate

Configure Rule Order

How would you like to process rule "AcmeOneDecAll"?

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 list) 49

Place here 1. AcmeOneNoDecFnINHit 2. Decrypttest 3. inspecttest 4. M365\_Recommended\_Policy\_Optimize 5. M365\_Recommended\_Policy\_Allow 6. M365 Recommended Policy Common and Default

General

Name\* AcmeOneDecAll 47

Tags

Press Enter to add

Rule is Enabled

Applications & URLs

Decryption Enforcement

Rule Type Decrypt traffic

Bypass Decryption for URL profiles Versa\_Reputation\_Analysis

Profile Acme-one

Users & Groups

Cancel Save 51

Cancel Back Save 48

## 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.

The screenshot shows the Versa Security Service Edge configuration interface. The left sidebar has tabs for View, Configure, Deploy, Monitor, Analytics, Inventory, Users, and Settings. The 'Configure' tab is selected and highlighted with a red box. Within 'Configure', the 'Real-Time Protection' section is selected, indicated by a red box and a red circle with the number 2. Under 'Real-Time Protection', the 'Profiles' tab is selected and highlighted with a red box and a red circle with the number 4. The main content area shows a table of TLS Decryption Rules. The table has columns for Name, Bypass URL Filtering Profile, Applications & URLs, Users & Groups, Endpoint Posture, Source & Destination, and Services. There are four rows of data in the table. At the bottom of the table, there are buttons for 'Go to page 1' and 'Previous 1 Next'.

Go to the [Filtering Profiles](#) tab, then the [File Filtering](#) tab, then click [+ Add](#).

Configure > Security Service Edge > Real-Time Protection > Profiles > File Filtering

**Filtering Profiles**

5 Filtering Profiles 6 File Filtering 7

URL Filtering DNS Filtering IP Filtering File Filtering

Search by keyword or name Filter Add

Profile Name	Deny List	Allow List	Reputation Based Action	Number Of File Based A...	Protocols	Action
blockfiles	Action: Reject Logging: Disabled	Logging: Enabled	Action: Allow Cloud Lookup: Disabled Logging: Disabled	1	HTTP, SMTP, IMAP, FTP, POP3, MAPI, SMB	Alert

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

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**.

Configure > Security Service Edge > Real-Time Protection > Profiles > File Filtering

Edit File Filtering Profile: blockfiles

1 Deny & Allow List 2 File Based Action 3 Reputation Based Action 4 Files & Protocols 5 Action 6 Review & Submit

By default, all fields have been configured. Otherwise, you can choose which deny and allow actions to enforce for your File filtering.

If traffic is matched in both the deny and allow, then the action in the deny takes precedence.

**Deny List**

Choose which hash values and actions to deny (blacklist).

Action: Reject

SHA256: Specify A SHA-256 hash value +  
SHA384: Specify A SHA-384 hash value +

Enable Logging

**Allow List**

Choose which hash values to allow (whitelist).

SHA256: Specify A SHA-256 hash value +  
SHA384: Specify A SHA-384 hash value +

Enable Logging

Cancel Back Skip to Review Next 8

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

Configure > Security Service Edge > Real-Time Protection > Profiles > File Filtering

Edit File Filtering Profile: blockfiles

1 Deny & Allow List    2 File Based Action    3 Reputation Based Action    4 Files & Protocols    5 Action    6 Review & Submit

By default, all fields have been configured. Otherwise, you can choose which file based actions to enforce for your file filtering.

Name	Action	Protocol	File Type	File Size	Direction
DenyZip	Reject	HTTP, FTP, SMTP, IMAP, POP3, MAPI, SMB	doc, docx, gzip, iso, pdf, ppt, pptx, zip, xlsx	None	Both

+ Add (9)  Show 1-1 of 1 results 10 Rows per Page Go to page 1 < Previous 1 Next >

Cancel Back Skip to Review Next

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.

Add File Based Action

Choose which action and configurations to apply for your file based action.

File Based Action Name: AcmeOneFileBlocking (10)

Action: Reject (11)

File Size: (Empty)

Select the type of protocols to filter.

HTTP (12) is selected

File Types: exe, gzip, zip, 7zip, bzip2, rar, gz (13)

Cancel Add

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

Select the type of protocols to filter.

HTTP	FTP	SMTP	IMAP	POP3	MAPI
SMB					
EXE	PHP	mach_o	WAV	JAR	targa
14	15				

Select the direction of the traffic to filter:

Both	Download	Upload
------	----------	--------

**Save** 15

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

Configure > Security Service Edge > Real-Time Protection > Profiles > File Filtering

**Create File Filtering Profile**

1 Deny & Allow List 2 File Based Action 3 Reputation Based Action 4 Files & Protocols 5 Action 6 Review & Submit

By default, all fields have been configured. Otherwise, you can choose which reputation based actions to enforce for your file filtering.

**Reputation Based Action**  
Specify the reputation base action to enforce on a file.

**Reputation Based Action**

Alert 16

Enable Logging

**Cloud Lookup**  
If enabling cloud lookup of a file for its reputation, specify the cloud profile to use for cloud lookup.

Cloud Lookup State

**Next** 17

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

Configure > Security Service Edge > Real-Time Protection > Profiles > File Filtering

### Create File Filtering Profile

**File Decompression**  
If file decompression is enabled, file filtering can only decompress gzip files.

File Decompression

**File Decompression Limit**  
Specify the action to take when the maximum number of decompression subdirectories is reached.

Alert  Allow  Block  Reject

**Protocol**  
Select one or more protocols to filter the files.

 <b>HTTP</b>	 <b>FTP</b>	 <b>SMTP</b>	 <b>IMAP</b>
 <b>POP3</b>	 <b>MAPI</b>	 <b>SMB</b>	

**Next** 18

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**.

The screenshot shows the Versa Network Platform interface. The left sidebar has icons for View, Configure, Deploy, Monitor, Analytics, Inventory, Users, and Settings. The main navigation bar at the top has 'Security Service Edge' (circled in red, step 2) and 'Real-Time Protection' (circled in red, step 3). The 'Configure' icon in the sidebar is also circled in red (step 1). The 'Profiles' link in the Real-Time Protection sub-menu is circled in red (step 4). The right panel displays a table of URL filtering rules with columns for Deny List, Allow List, URL Categories, Reputations, and Action. The table shows two entries: one for GenAI and one for Versa, both with 'Allow' actions.

Deny List	Allow List	URL Categories	Reputations	Action
Logging: Enabled			GenAI_sanctioned: trustworthy	Allow
			GenAI_tolerated: low_risk, moderate_risk	
			GenAI_unsanctioned: suspicious, high_risk	
Logging: Enabled			Versa_Sanctioned: trustworthy	Allow
			Versa_Moderate: low_risk, moderate_risk	
			Versa_Unsanctioned: suspicious, high_risk	

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

Configure > Security Service Edge > Real-Time Protection > Profiles > URL Filtering

**Filtering Profiles**

**Filtering Profiles** 5 Malware Protection & IPS Data Loss Prevention (DLP) Cloud Access Security Broker (CASB - Inline) Remote Browser Isolation (RBI) Advanced Threat Protection (ATP)

**URL Filtering** 6 Filtering IP Filtering File Filtering

Search by keyword or name Filter All Rule Types

Profile Name Deny List Allow List URL Categories Reputations Action

<input type="checkbox"/> GenAI_Firewall		Logging: Enabled	GenAI_sanctioned: trustworthy GenAI tolerated: low_risk, moderate_risk GenAI_unsanctioned: suspicious, high_risk	Allow
<input type="checkbox"/> Versa_Reputation_Analysis		Logging: Enabled	Versa_Sanctioned: trustworthy Versa_Moderate: low_risk, moderate_risk Versa_Unsanctioned: suspicious, high_risk	Allow

Showing 1-2 of 2 results 10 Rows per Page Go to page 1 < Previous 1 Next >

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

Configure > Security Service Edge > Real-Time Protection > Profiles > URL Filtering

**Create URL Filtering Profile**

for your deny and allow list.

**Deny List**  
Choose which actions and URLs to deny (blacklist).

Action

**Allow List**  
Choose which URLs to allow (whitelist).

Patterns

Strings

**Next** 8

Cancel Back Skip to Review

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.

Configure > Security Service Edge > Real-Time Protection > Profiles > URL Filtering  
Create URL Filtering Profile

Deny & Allow List      Category & Reputations List      Action      Review & Submit

All fields have been configured, by default. Otherwise, you can choose which actions and URLs to enforce for your deny and allow list.

Select Category List  
Specify what action to enforce to the following URL categories.

Action	URL Category	+ Add New
Reject	adult_and_pornography sports gambling weapons violence	+ (10)
	Search or select from list	

Select Reputation List  
Specify what action to enforce to the following reputations.

Action	Reputation	+

Cancel      Back      Skip to Review      Next (11)

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.

Configure > Security Service Edge > Real-Time Protection > Profiles > URL Filtering  
Create URL Filtering Profile

Deny & Allow List      Category & Reputations List      Action (3)      Review & Submit

By default, we will allow all URLs that do not match any criteria specified. Otherwise, you can choose which default action to enforce if there are no criteria matched.

Specify the default action to enforce if no criteria are matched.

Action	+ Add New
Allow	(12)

Decrypt Bypass (14)  
 Cloud Lookup State (13)

Cancel      Back      Skip to Review      Next (14)

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

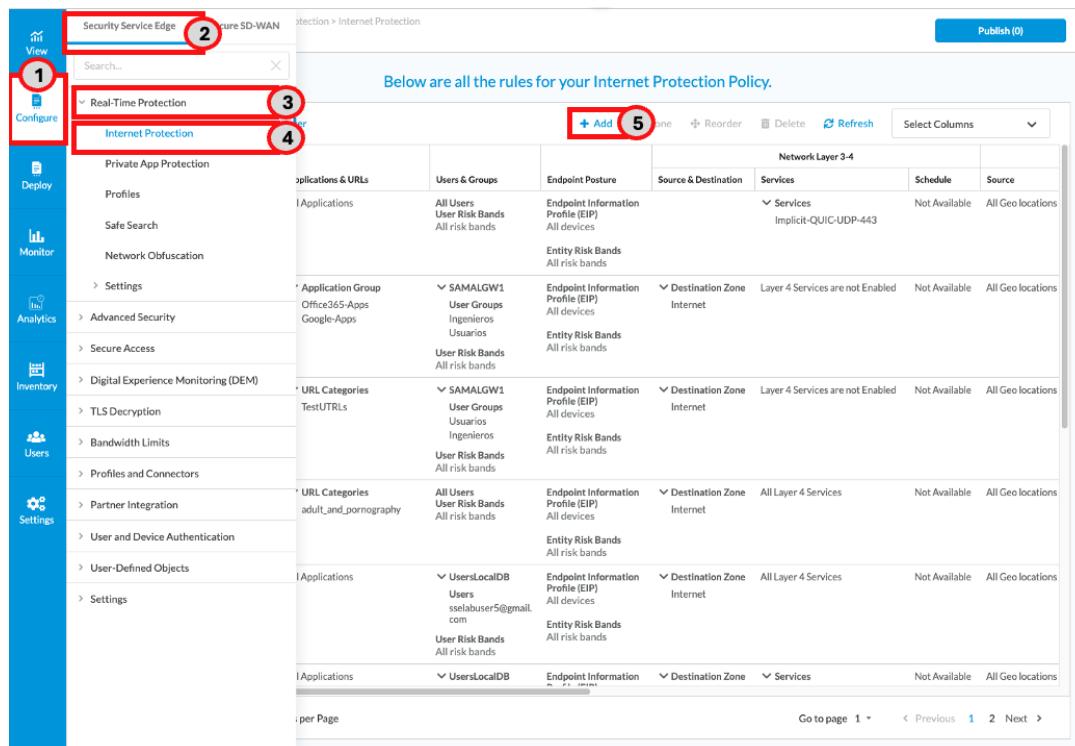
For the first rule, the required information to configure the Internet Protection Rules for Contractor Users is listed below.

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 (block-files 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

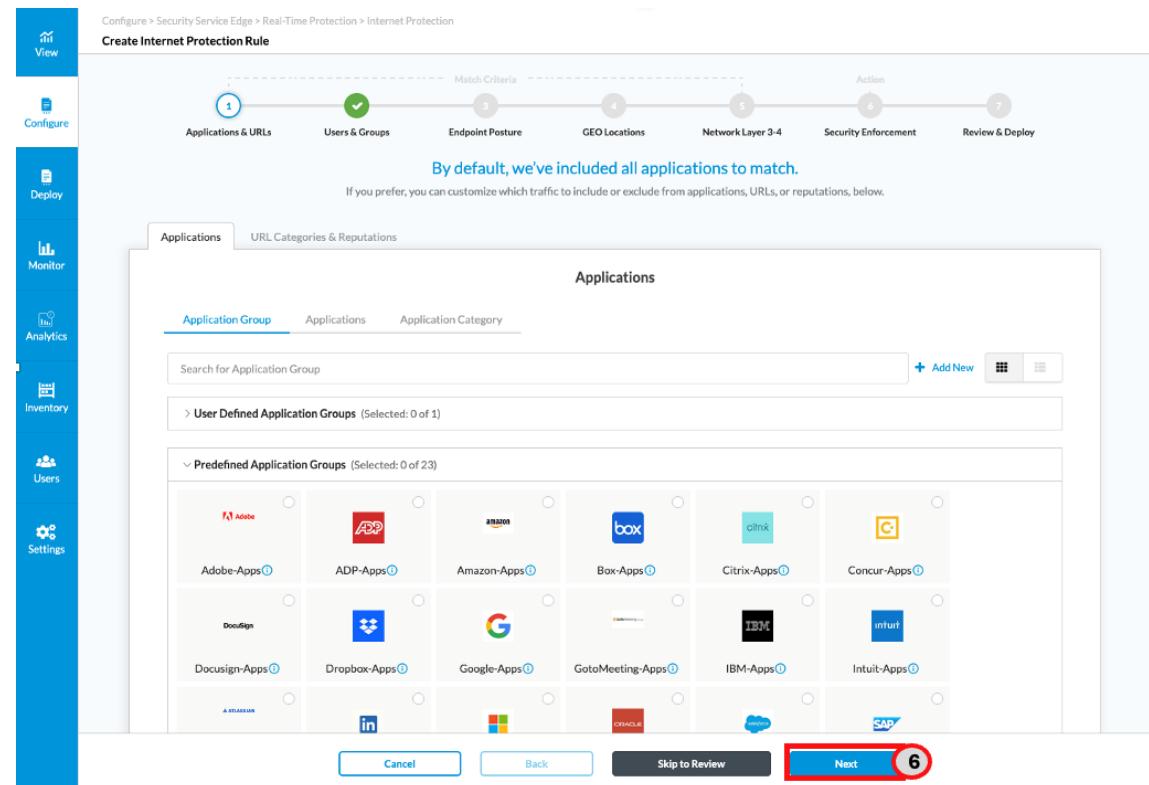


Below are all the rules for your Internet Protection Policy.

Network Layer 3-4	Source & Destination	Services	Schedule	Source
Endpoint Information Profile (EIP) All devices	Services	Implicit-QUIC-UDP-443	Not Available	All Geo locations
Entity Risk Bands All risk bands				
Endpoint Information Profile (EIP) All devices	Destination Zone	Layer 4 Services are not Enabled	Not Available	All Geo locations
Entity Risk Bands All risk bands				
Endpoint Information Profile (EIP) All devices	Destination Zone	Layer 4 Services are not Enabled	Not Available	All Geo locations
Entity Risk Bands All risk bands				
Endpoint Information Profile (EIP) All devices	Destination Zone	All Layer 4 Services	Not Available	All Geo locations
Entity Risk Bands All risk bands				
Endpoint Information Profile (EIP) All devices	Destination Zone	All Layer 4 Services	Not Available	All Geo locations
Entity Risk Bands All risk bands				
Endpoint Information	Services		Not Available	All Geo locations

per Page Go to page 1 < Previous 1 2 Next >

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.



Configure > Security Service Edge > Real-Time Protection > Internet Protection

Create Internet Protection Rule

Match Criteria

Action

By default, we've included all applications to match.

If you prefer, you can customize which traffic to include or exclude from applications, URLs, or reputations, below.

Applications

Applications

Application Group Applications Application Category

Search for Application Group + Add New

User Defined Application Groups (Selected: 0 of 1)

Predefined Application Groups (Selected: 0 of 23)

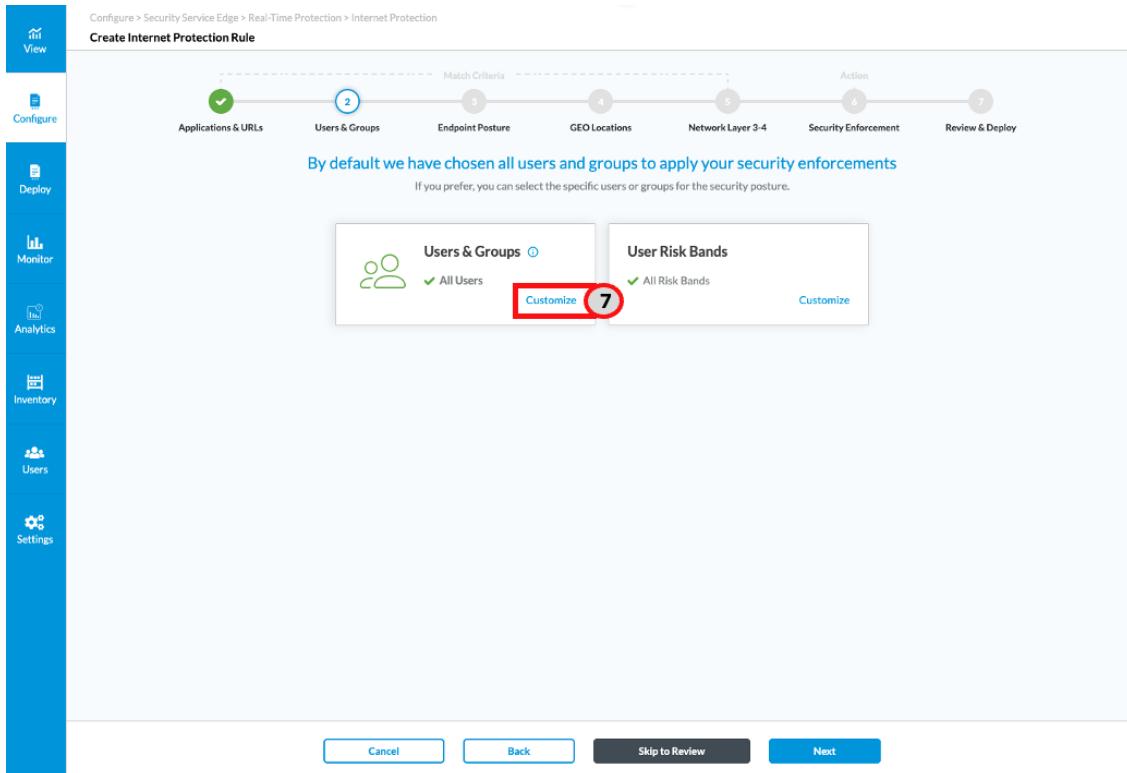
Adobe-Apps ADP Amazon-Apps box citrix Concur-Apps

Dropbox-Apps Google-Apps GotoMeeting-Apps IBM-Apps Intuit-Apps

SAP

Cancel Back Skip to Review Next 6

Click **Customize** under Users & Groups.



Configure > Security Service Edge > Real-Time Protection > Internet Protection

**Create Internet Protection Rule**

Match Criteria

Action

Applications & URLs (1) **2** Users & Groups (2) Endpoint Posture (3) GEO Locations (4) Network Layer 3-4 (5) Security Enforcement (6) Review & Deploy (7)

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

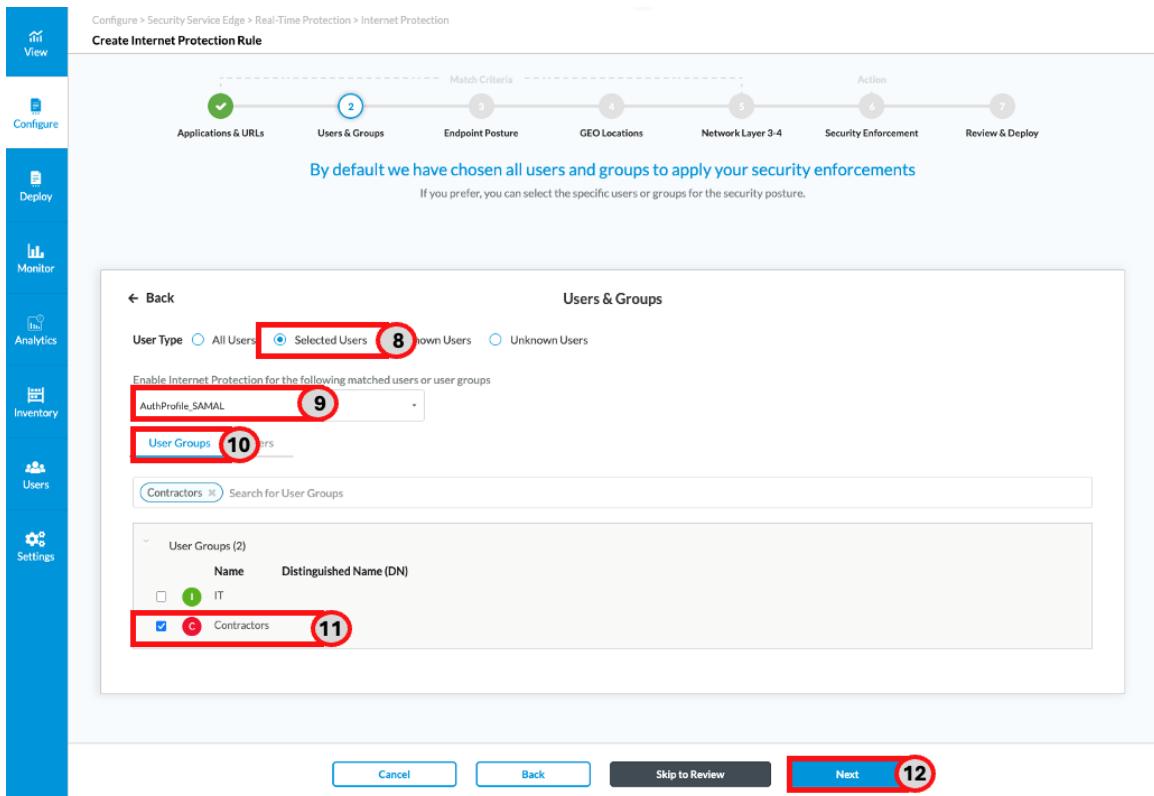
If you prefer, you can select the specific users or groups for the security posture.

**Users & Groups** **7** **Customize**

**User Risk Bands** **Customize**

Cancel Back Skip to Review Next

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**.



Configure > Security Service Edge > Real-Time Protection > Internet Protection

**Create Internet Protection Rule**

Match Criteria

Action

Applications & URLs (1) **2** Users & Groups (2) Endpoint Posture (3) GEO Locations (4) Network Layer 3-4 (5) Security Enforcement (6) Review & Deploy (7)

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

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

**Users & Groups**

User Type  All Users  Selected Users **8**  Unknown Users

Enable Internet Protection for the following matched users or user groups **9**

AuthProfile\_SAML

User Groups **10** Contractors

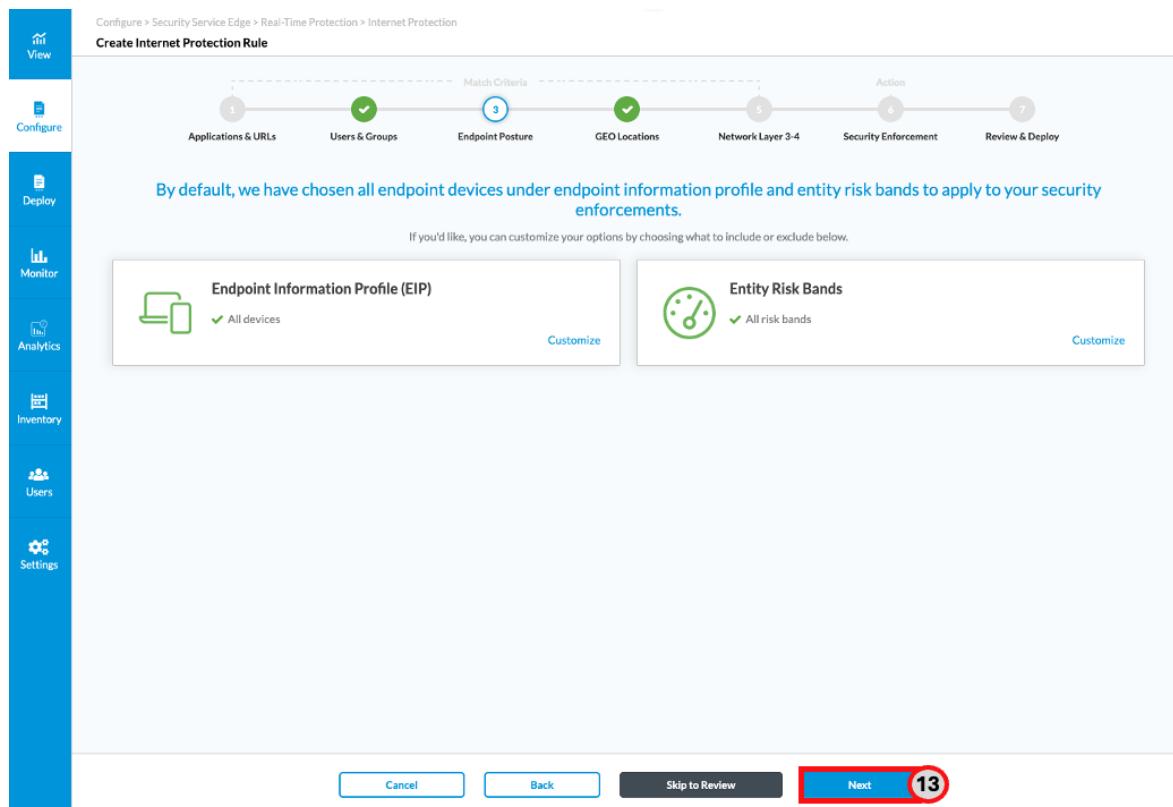
Contractors  Search for User Groups

User Groups (2)

Name	Distinguished Name (DN)
<input type="checkbox"/> IT	
<input checked="" type="checkbox"/> Contractors <b>11</b>	

Cancel Back Skip to Review **12** Next

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



Configure > Security Service Edge > Real-Time Protection > Internet Protection

Create Internet Protection Rule

Match Criteria

1 Applications & URLs 2 Users & Groups 3 Endpoint Posture 4 GEO Locations 5 Network Layer 3-4 6 Security Enforcement 7 Review & Deploy

By default, we have chosen all endpoint devices under endpoint information profile and entity risk bands to apply to your security enforcements.

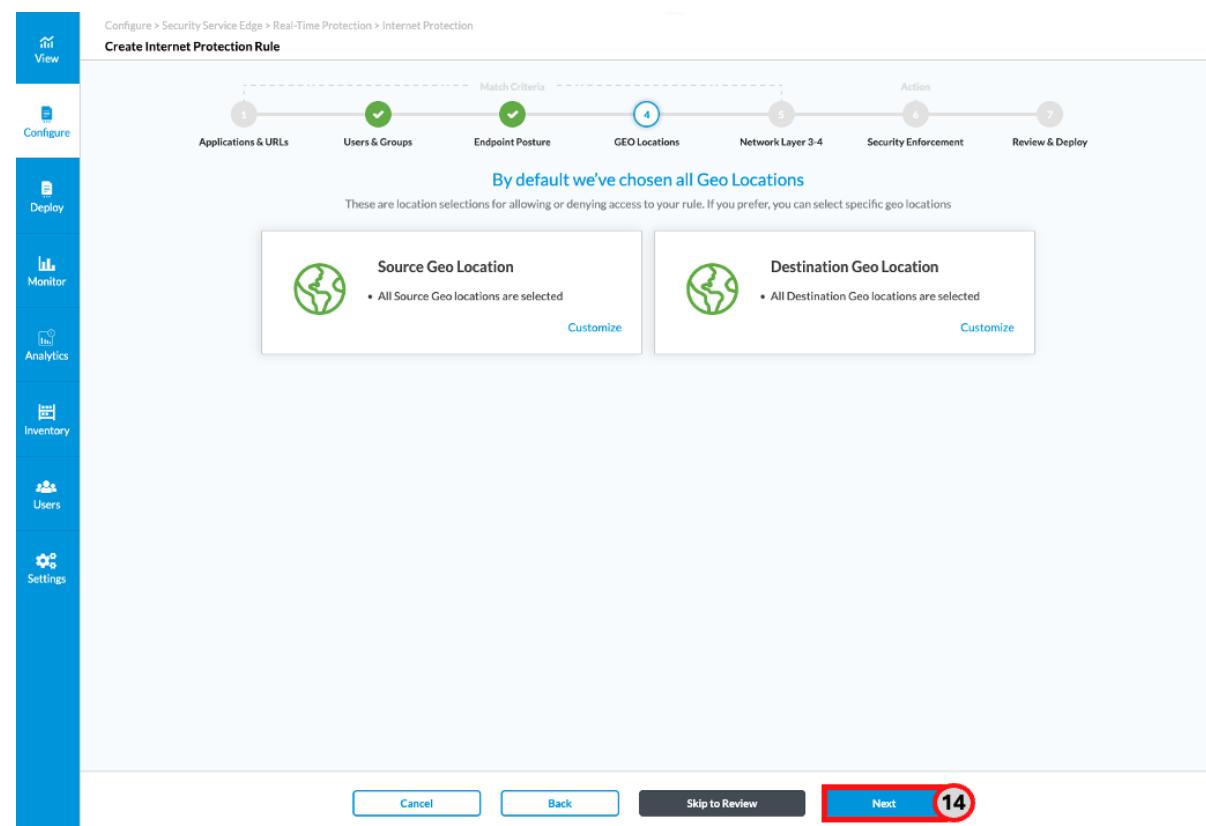
If you'd like, you can customize your options by choosing what to include or exclude below.

Endpoint Information Profile (EIP)  All devices [Customize](#)

Entity Risk Bands  All risk bands [Customize](#)

[Cancel](#) [Back](#) [Skip to Review](#) **Next 13**

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



Configure > Security Service Edge > Real-Time Protection > Internet Protection

Create Internet Protection Rule

Match Criteria

1 Applications & URLs 2 Users & Groups 3 Endpoint Posture 4 GEO Locations 5 Network Layer 3-4 6 Security Enforcement 7 Review & Deploy

By default we've chosen all Geo Locations

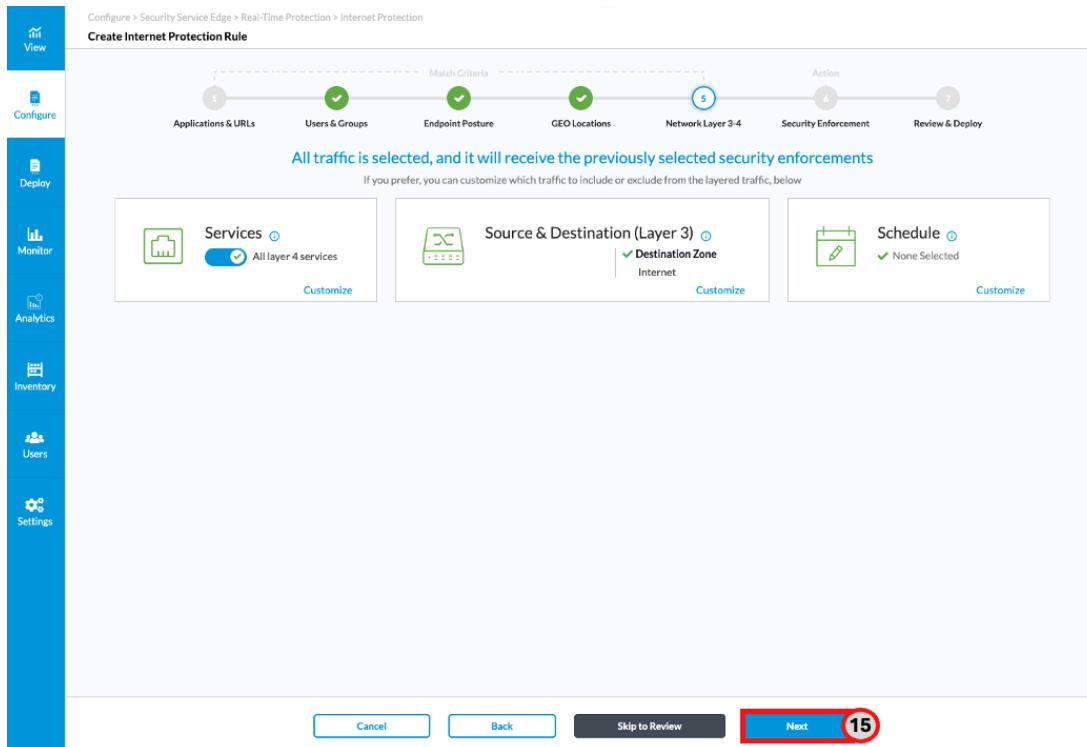
These are location selections for allowing or denying access to your rule. If you prefer, you can select specific geo locations

Source Geo Location  All Source Geo locations are selected [Customize](#)

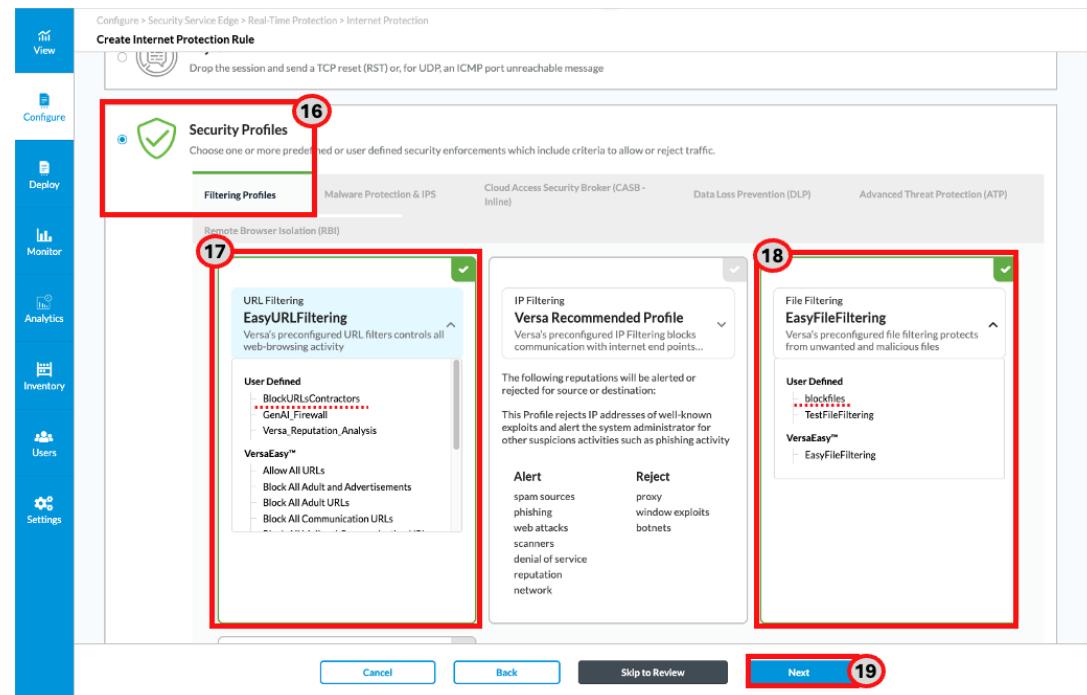
Destination Geo Location  All Destination Geo locations are selected [Customize](#)

[Cancel](#) [Back](#) [Skip to Review](#) **Next 14**

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.

Configure > Security Service Edge > Real-Time Protection > Internet Protection

**Create Internet Protection Rule**

Review your Internet Protection Policy configurations below.

Below are the configurations of your rule. Review and edit any step of your configuration before deploying.

**General**

Name \* **20** AcmeOneCttrsDenyUrls

Description

Tags

Rule is Enabled

**Applications & URLs**

**Users & Groups** **21**

Users & Groups AuthProfile\_SAMAL

User Risk Bands All Risk Bands

User Group | 1

Name Description

Cancel Back Save

## 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**.

Configure > Security Service Edge > Real-Time Protection > Internet Protection

Internet Protection Rules List

Below are all the rules for your Internet Protection Policy.

Rule Name	Applications & URLs	Users & Groups	Endpoint Posture	Network Layer 3-4			
				Source & Destination	Services	Schedule	Source
Implicit_Drop_Quic	All Applications	All Users User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices	Services	Not Available	All Geo locations	
			Entity Risk Bands All risk bands				
AcmeOneClttrsDenyUrls	URL Categories adult_and_pornography sports gambling <a href="#">More Details</a>	AuthProfile_SAMA User Groups Contractors User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices	Destination Zone Internet	All Layer 4 Services	Not Available	All Geo locations
			Entity Risk Bands All risk bands				
AcmeOneITVersaURLcmd	All Applications	AuthProfile_SAMA User Groups IT User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices	Destination Zone Internet	All Layer 4 Services	Not Available	All Geo locations
			Entity Risk Bands All risk bands				
AcmeOneAllowAllEncored	All Applications	AuthProfile_SAMA User Groups IT Contractors User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices	Destination Zone Internet	All Layer 4 Services	Not Available	All Geo locations
			Entity Risk Bands All risk bands				
AllowAll_URLFilter	Application Group Office365-Apps Google-Apps	SAMALGW1 User Groups Ingenieros Usuarios User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices	Destination Zone Internet	Layer 4 Services are not Enabled	Not Available	All Geo locations
			Entity Risk Bands All risk bands				

Showing 1-10 of 17 results 10 ▾ Rows per Page Go to page 1 ▾ < Previous 1 2 Next >

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.

Configure > Security Service Edge > Real-Time Protection > Internet Protection

Create Internet Protection Rule

By default, we've included all applications to match.

If you prefer, you can customize which traffic to include or exclude from applications, URLs, or reputations, below.

Applications URL Categories & Reputations

Applications

Application Group Applications Application Category

Search for Application Group + Add New

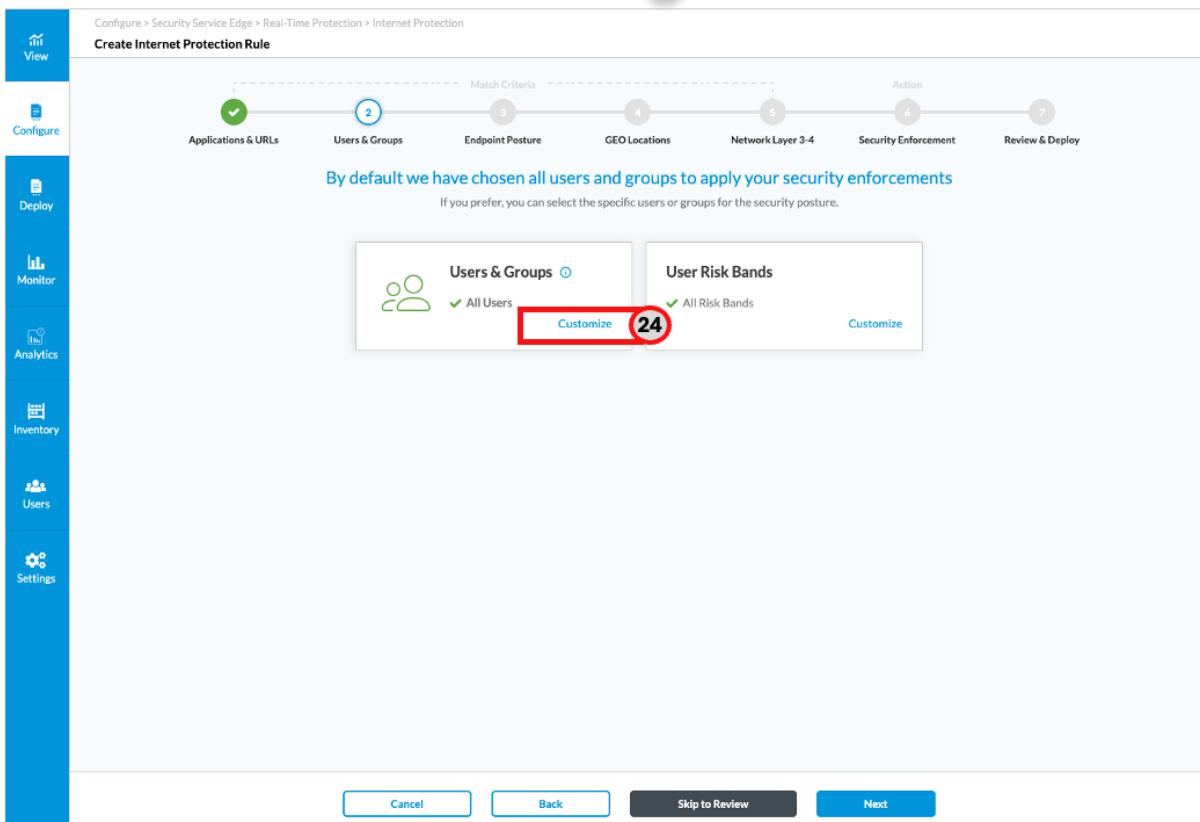
> User Defined Application Groups (Selected: 0 of 1)

Predefined Application Groups (Selected: 0 of 23)

Adobe-Apps	ADP-Apps	Amazon-Apps	Box-Apps	Citrix-Apps	Concur-Apps
Docusign-Apps	Dropbox-Apps	Google-Apps	GotoMeeting-Apps	IBM-Apps	Intuit-Apps
ATLASSIAN	in	Microsoft-365	VMware	SAP	

Cancel Back Skip to Review Next 23

Click **Customize** under Users & Groups.



Configure > Security Service Edge > Real-Time Protection > Internet Protection  
**Create Internet Protection Rule**

Applications & URLs 2 Match Criteria 3 Endpoint Posture 4 GEO Locations 5 Network Layer 3-4 6 Security Enforcement 7 Review & Deploy

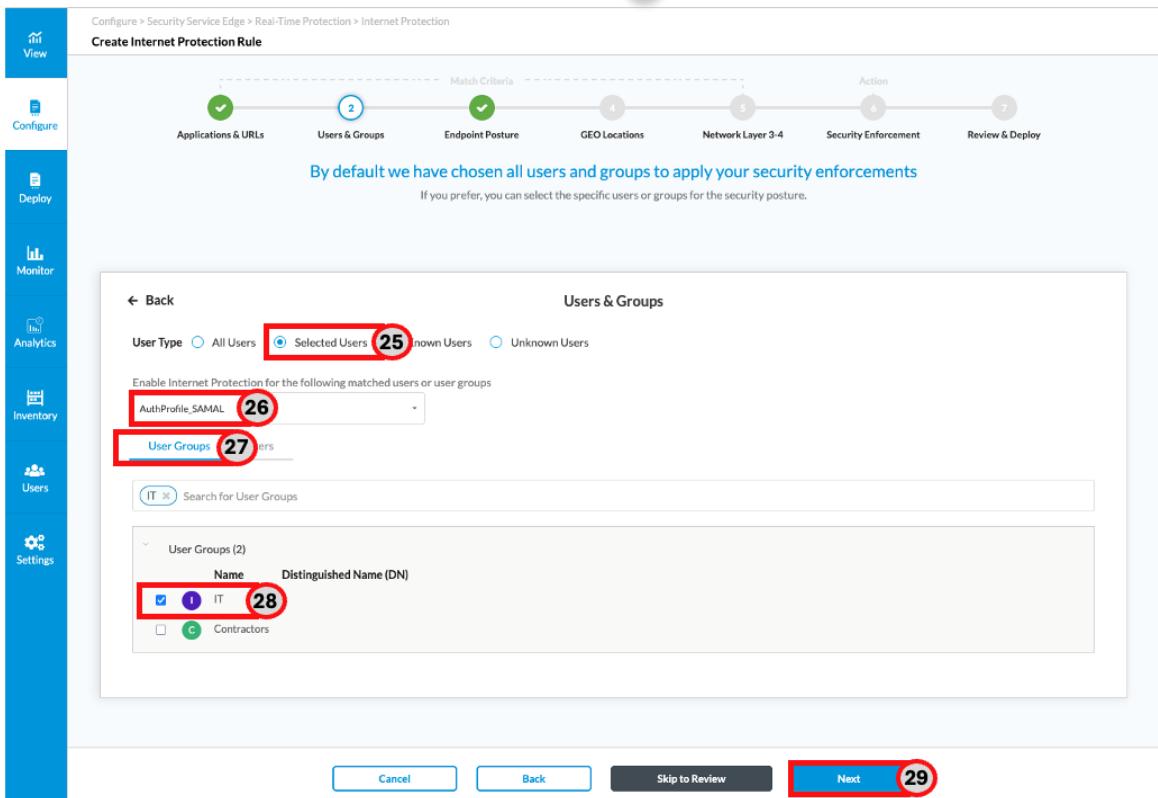
By default we have chosen all users and groups to apply your security enforcements  
 If you prefer, you can select the specific users or groups for the security posture.

**Users & Groups** ①  
 All Users **Customize** ②4

**User Risk Bands**  
 All Risk Bands **Customize**

Cancel Back Skip to Review Next

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**.



Configure > Security Service Edge > Real-Time Protection > Internet Protection  
**Create Internet Protection Rule**

Applications & URLs 2 Match Criteria 3 Endpoint Posture 4 GEO Locations 5 Network Layer 3-4 6 Security Enforcement 7 Review & Deploy

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

**Users & Groups**

User Type  All Users  Selected Users ②5  Known Users  Unknown Users

Enable Internet Protection for the following matched users or user groups  
**AuthProfile\_SAML** ②6

**User Groups** ②7

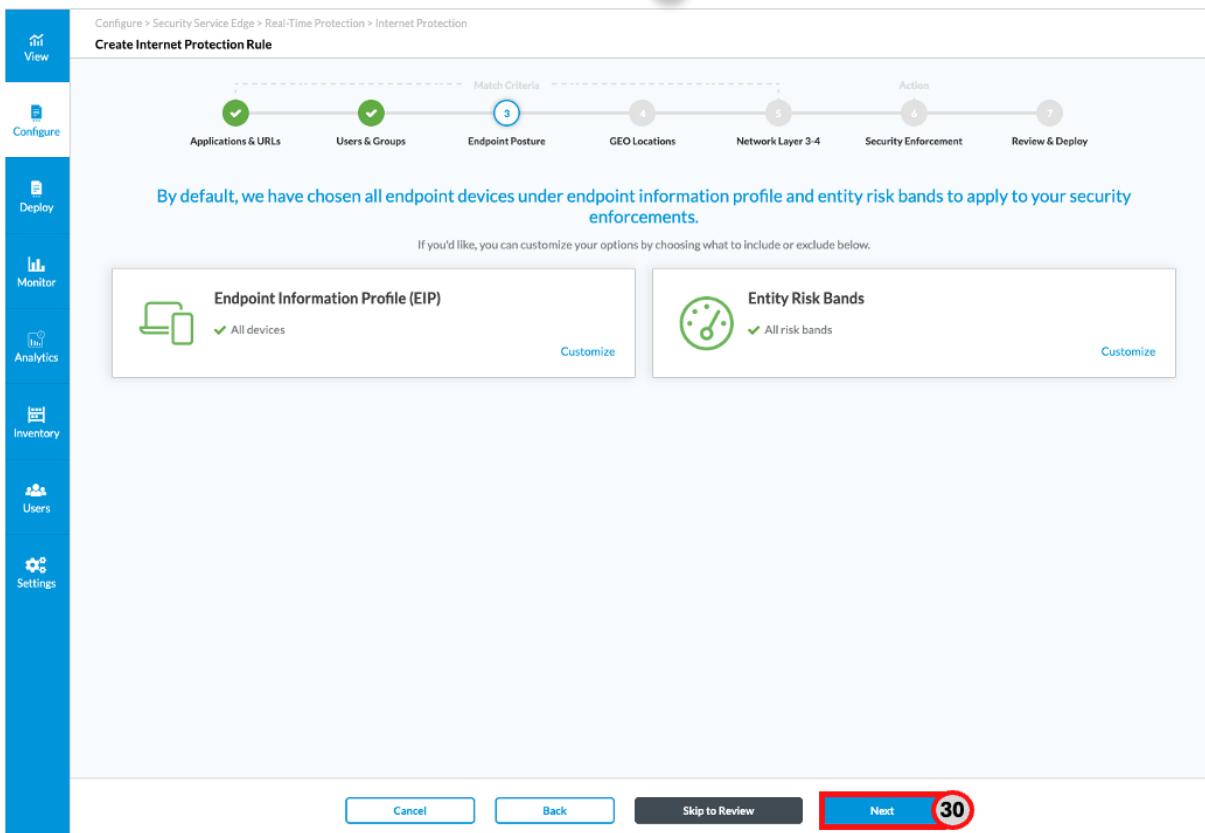
IT  Search for User Groups

User Groups (2)

Name	Distinguished Name (DN)
<input checked="" type="checkbox"/> ②8 IT	
<input type="checkbox"/> ② Contractors	

Cancel Back Skip to Review **Next** ②9

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



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

3

4

5

6

7

By default, we have chosen all endpoint devices under endpoint information profile and entity risk bands to apply to your security enforcements.

If you'd like, you can customize your options by choosing what to include or exclude below.

Endpoint Information Profile (EIP)

Entity Risk Bands

All devices

All risk bands

Customize

Customize

Cancel

Back

Skip to Review

Next 30

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.

Configure > Security Service Edge > Real-Time Protection > Internet Protection

Create Internet Protection Rule

Match Criteria

Applications & URLs    Users & Groups    Endpoint Posture    GEO Locations    Network Layer 3-4    Security Enforcement    Review & Deploy

By default we've chosen all Geo Locations

These are location selections for allowing or denying access to your rule. If you prefer, you can select specific geo locations

Source Geo Location: All Source Geo locations are selected    Destination Geo Location: All Destination Geo locations are selected

Cancel    Back    Skip to Review    **Next 31**

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

Configure > Security Service Edge > Real-Time Protection > Internet Protection

Create Internet Protection Rule

Match Criteria

Applications & URLs    Users & Groups    Endpoint Posture    GEO Locations    Network Layer 3-4    Security Enforcement    Review & Deploy

All traffic is selected, and it will receive the previously selected security enforcements

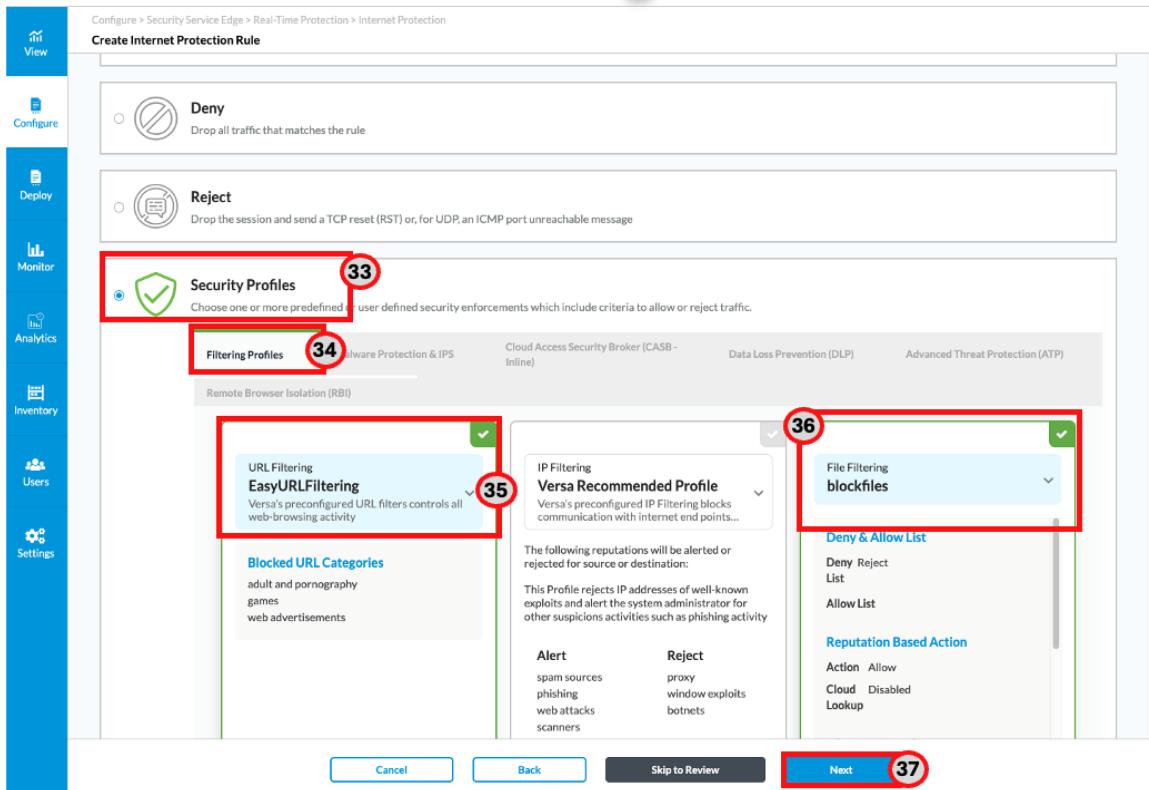
If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

Services: All layer 4 services    Source & Destination (Layer 3): Destination Zone Internet    Schedule: None Selected

Cancel    Back    Skip to Review    **Next 32**

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**.



Configure > Security Service Edge > Real-Time Protection > Internet Protection  
**Create Internet Protection Rule**

Deny  
 Reject  
 Security Profiles **33**  
 Choose one or more predefined or user defined security enforcements which include criteria to allow or reject traffic.

**34** Filtering Profiles **34** Malware Protection & IPS Cloud Access Security Broker (CASB - Inline) Data Loss Prevention (DLP) Advanced Threat Protection (ATP)

Remote Browser Isolation (RBI)

**35** URLFiltering **EasyURLfiltering**  
 Versa's preconfigured URL filters controls all web-browsing activity

Blocked URL Categories  
 adult and pornography  
 games  
 web advertisements

**36** IP Filtering **Versa Recommended Profile**  
 Versa's preconfigured IP Filtering blocks communication with internet end points...

The following reputations will be alerted or rejected for source or destination:  
 This Profile rejects IP addresses of well-known exploits and alert the system administrator for other suspicious activities such as phishing activity

**37** Alert Reject  
 spam sources proxy  
 phishing window exploits  
 web attacks botnets  
 scanners

**Reputation Based Action**  
 Action Allow  
 Cloud Disabled  
 Allow List  
 Lookup

Cancel Back Skip to Review **Next** **37**

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

Review & Deploy

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. Implicit-Allow-DNS

3. AcmeOneITVersaURLRcmnd **41**

4. Implicit\_Deny\_All

Place here

Cancel **42**

Move **42**

Save **39**

Cancel Back

General

Name \* **38**  
AcmeOneITVersaURLRcmnd

Tags

Rule is Enabled

Applications & URLs

All Applications

Users & Groups

User Group | 1

Name Description

IT

Users Device Groups All Device Groups

## Appendix A – Authentication Methods Configuration

### LDAP Active-Directory

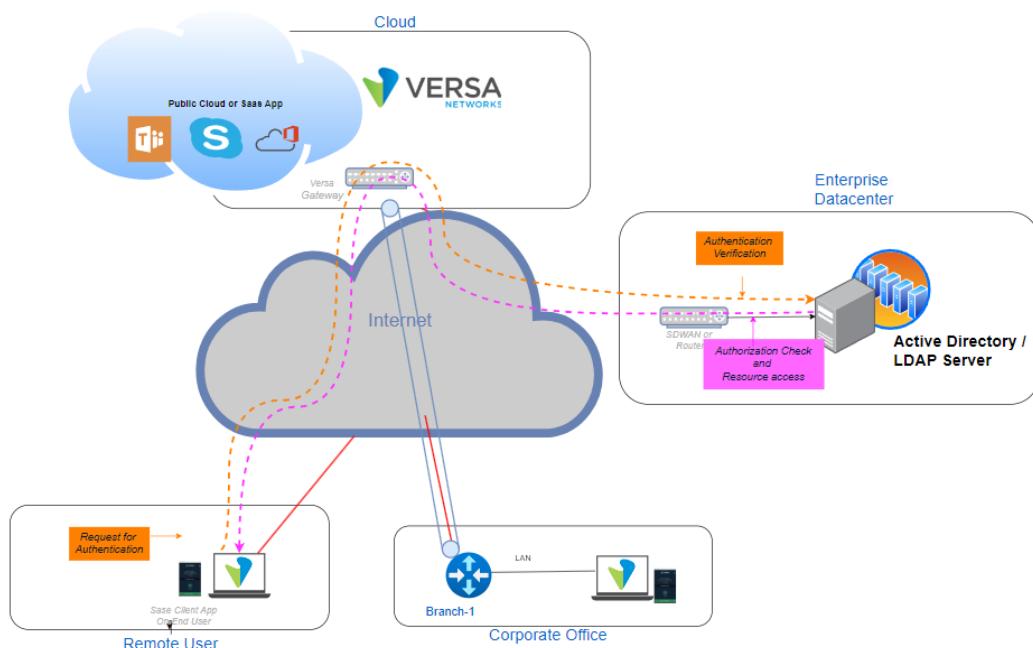
LDAP is a client-server protocol that enables network devices to access directory services storing attribute-based information, allowing for user authentication through querying a directory server. The SSE gateway queries the LDAP server to validate the user, granting or denying access based on the authentication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

#### Scenario

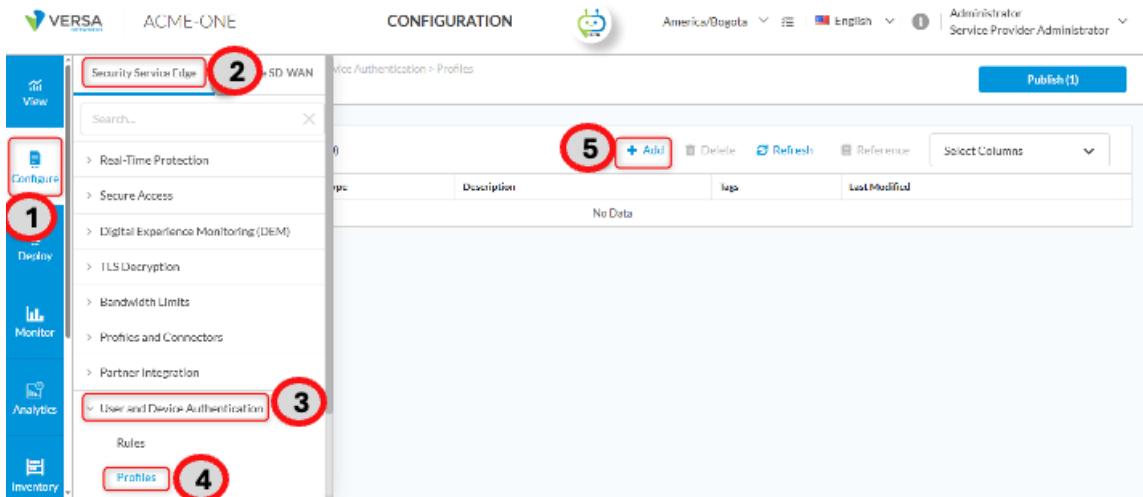
In most enterprise environments, user authentication is centralized through AD/LDAP servers in the data centre. In cases of VSPA or VISA, users securely connect to the SSE gateways using the Versa SASE Client from remote locations, branches, or corporate offices. Authentication requests from the SASE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



ACME-ONE

CONFIGURATION

America/Bogota | English | Administrator | Service Provider Administrator

1

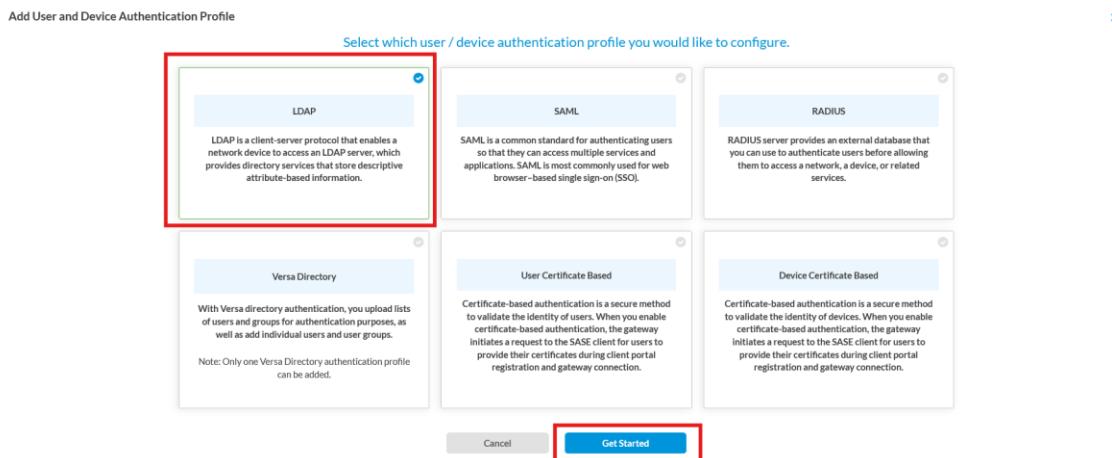
2

3

4

5

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



Add User and Device Authentication Profile

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

LDAP

LDAP is a client-server protocol that enables a network device to access an LDAP server, which provides directory services that store descriptive attribute-based information.

SAML

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

RADIUS

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

Versa Directory

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

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

User Certificate Based

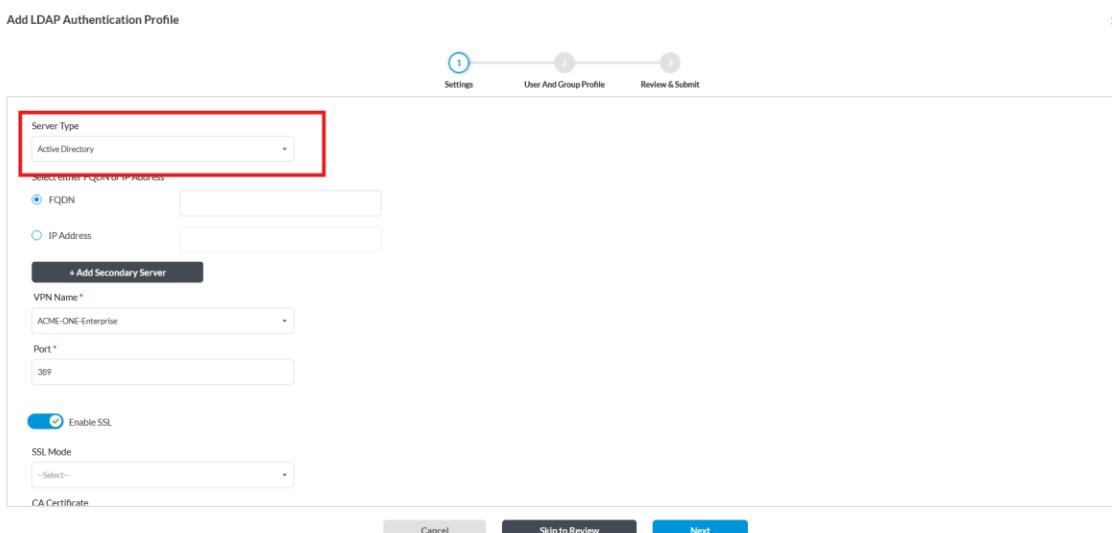
Certificate-based authentication is a secure method to validate the identity of users. When you enable certificate-based authentication, the gateway initiates a request to the SASE client for users to provide their certificates during client portal registration and gateway connection.

Device Certificate Based

Certificate-based authentication is a secure method to validate the identity of devices. When you enable certificate-based authentication, the gateway initiates a request to the SASE client for users to provide their certificates during client portal registration and gateway connection.

Get Started

From the Server Type dropdown, select Active Directory



Add LDAP Authentication Profile

1 Settings 2 User And Group Profile 3 Review & Submit

Server Type

Active Directory

Select Server FQDN or IP Address

FQDN

IP Address

+ Add Secondary Server

VPN Name \*

ACME-ONE-Enterprise

Port \*

389

Enable SSL

SSL Mode

CA Certificate

Cancel Skip to Review Next

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

LDAP Authentication Profile – Parameters		
Parameter	Description	Current Use Case
<b>Server Type</b>	It indicates that the authentication source is Microsoft Active Directory or Open-LDAP.	active directory
<b>FQDN or IP Address</b>	The Fully Qualified Domain Name (FQDN) or IP address of the AD/LDAP server.	10.163.106.33 or ad-server.company.local
<b>VPN Name</b>	Defines which VPN instance or network segment this authentication profile applies to.	ACME-ONE-Enterprise
<b>Port</b>	Port used for LDAP/AD communication. Possible options: 389: Default LDAP port & 636: Default LDAPS (LDAP over SSL)	389 TCP
<b>SSL Status</b>	Enabled/Disabled: Determines if the connection between Versa and the AD server uses SSL/TLS for security. <b>If enabled</b> , you must also specify the CA certificate details (trusted CA/chain) that will be used for TLS communication verification.	Disabled
<b>Bind DN</b>	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
<b>Bind Password</b>	The password for the Bind DN account.	Service account password
<b>Base DN</b>	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
<b>Domain Name</b>	The name of the AD domain.	versa.com
<b>Search Timeout (sec)</b>	Maximum time (in seconds) Versa will wait for a response from the LDAP server during a query.	30
<b>Cache Expiry Time (mins)</b>	How long (in minutes) user/group information retrieved from LDAP will be cached before refreshing.	10
<b>Concurrent Logins</b>	The maximum number of concurrent sessions allowed for the same user.	3

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

Add LDAP Authentication Profile

1. Settings    2. User And Group Profile    3. Review & Submit

Server Type: Active Directory (1)

Selected either FQDN or IP Address\* (2)

FQDN (radio button) IP Address (radio button) 10.183.106.33 (2)

+ Add Secondary Server

Virtual Name\* (3)

ACME-ONE-Enterprise

Port\* (4)

389

Enable SSL (4)

SSL Mode: Select

1. Settings    2. User And Group Profile    3. Review & Submit

Cancel    Skip to Review    Next

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

Add LDAP Authentication Profile

1. Settings    2. User And Group Profile    3. Review & Submit

Virtual Name\* (1)

ACME-ONE-Enterprise

Port\* (2)

389

Enable SSL (4)

Bind DN\* (3)

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

Bind Password\* (4)

\*\*\*\*\*

Bind Timeout (sec) (5)

30

Base DN\* (6)

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

Domain Name\* (7)

acme-one.com

Search Timeout (sec) (8)

30

Cache Expiry Time (mins) (9)

10

Concurrent Logins (10)

3

Cancel    Skip to Review    Next

Next, complete the required fields:

#### LDAP Object and User Attributes

Parameter	Value / Default	Description
Group Object Class	group	Standard AD object class for security and distribution groups. Required to identify groups in the directory.
Group Name	name	Attribute that defines the display name of a group. Used by Versa to match groups during policy evaluation.
Group Member	memberOf	Attribute that lists group memberships for a user object. Ensures Versa can apply policies based on AD group membership.
User Object Class	user	Standard AD object class for user accounts. Required for identifying users in the directory.

User Name	userPrincipalName (recommended) or sAMAccountName	Attribute used for login. userPrincipalName (e.g., user@versanetworks.com) is modern and preferred. sAMAccountName is legacy but still supported.
Password Last Set	pwdLastSet	Attribute showing when a user's password was last changed. Useful for enforcing password expiration policies.
Password Max Age	maxPwdAge	Attribute defining the maximum password lifetime. Derived from the AD domain password policy.
Refresh Interval (sec)	21600 (default = 6 hours)	Determines how often Versa refreshes user and group information from LDAP. Can be tuned based on the frequency of directory changes.

click **Next** to proceed.

Add LDAP Authentication Profile

Group Object Class \*: group

Group Name \*: name

Group Member \*: memberof

User Object Class \*: user

User Name \*: userPrincipalName

Refresh Interval (seconds): 21600

Password Last Set: pwdLastSet

Password Max Age: maxPwdAge

Buttons: Cancel, Back, Skip to Review, **Next**

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

Add LDAP Authentication Profile

General

AD Server Acme One

Settings

Server Type: active-directory  
FQDN or IP Address: 10.163.106.33  
VPN Name: ACME-ONE-Enterprise  
Port: 389  
SSL Status: Disabled  
SSL Mode: CA Certificate  
File Name: acme-one.cer  
Issued To: acme-one.com  
Issued By: acme-one.com  
Validity: 30 days  
Bind DN: cn=Administrator,cn=users,dc=acme-one,dc=com  
Bind Password:  30  
Bind Timeout (sec): 30  
Base DN: cn=users,dc=acme-one,dc=com  
Domain Name: acme-one.com  
Base Domain: acme-one.com  
Search Timeout (sec): 30  
Cache Expiry Time (min): 10  
Concurrent Logins: 3

Description:

Cancel Back Save Review & Submit

Then Save.

Add LDAP Authentication Profile

General

FQDN or IP Address: 10.163.106.33  
VPN Name: ACME-ONE-Enterprise  
Port: 389  
SSL Status: Disabled  
SSL Mode: CA Certificate  
File Name: acme-one.cer  
Issued To: acme-one.com  
Issued By: acme-one.com  
Validity: 30 days  
Bind DN: cn=Administrator,cn=users,dc=acme-one,dc=com  
Bind Password:  30  
Bind Timeout (sec): 30  
Base DN: cn=users,dc=acme-one,dc=com  
Domain Name: acme-one.com  
Base Domain: acme-one.com  
Search Timeout (sec): 30  
Cache Expiry Time (min): 10  
Concurrent Logins: 3

User and Group Profile

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

Cancel Back Save

Go to Publish

ACME-ONE

CONFIGURATION

User and Device Authentication Profiles (1)

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

Showing 1 of 1 results 10 • Rows per Page

Administrator Service Provider Administrator

Publish (1)

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.

ACME-ONE

CONFIGURATION

Edit Client-based Access Rule: Secure\_Access\_Windows\_Profile

Operate System **1** **2** Users & Groups

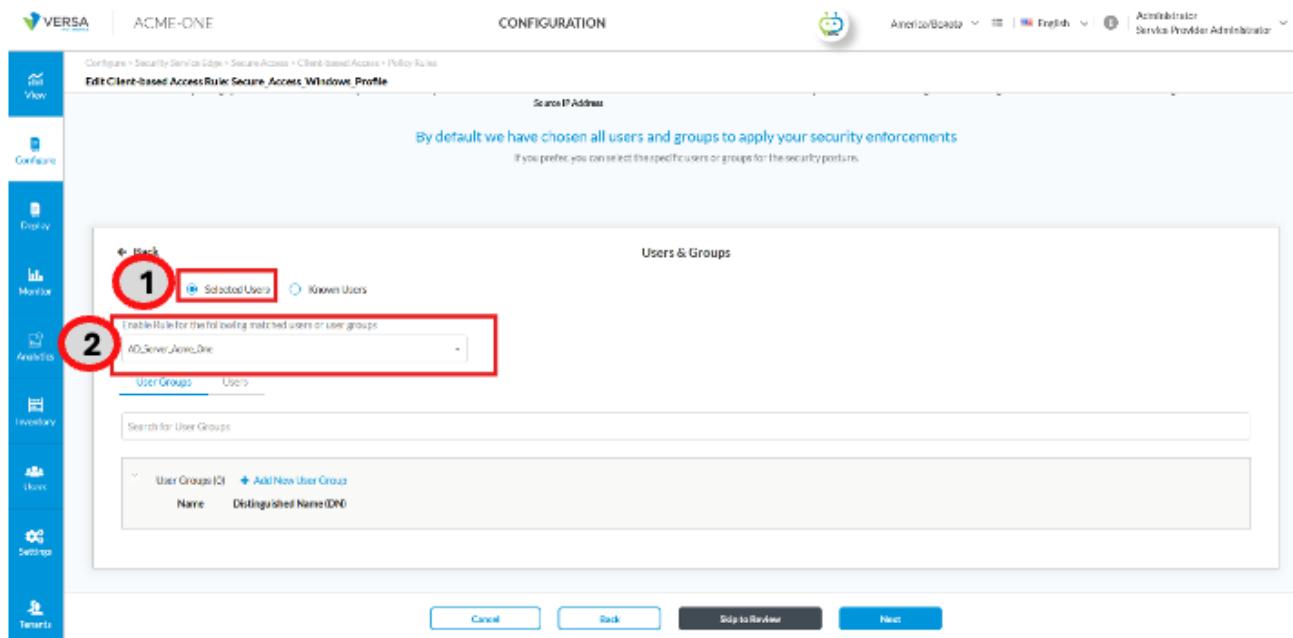
Underline Posture      Source Geo Location & Source IP Address      Traffic Action      Categories      Client Configuration      Asset Profile from UI?      Review & Continue

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

Users & Groups  Known Users **2**  Groups

Cancel Back Skip to Review Next

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



ACME-ONE CONFIGURATION

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

Edit Client-based Access Rule: Secure\_Access\_Windows\_Profile

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

Enable Rule for the following matched users or user groups

AD\_Server\_Acme\_One

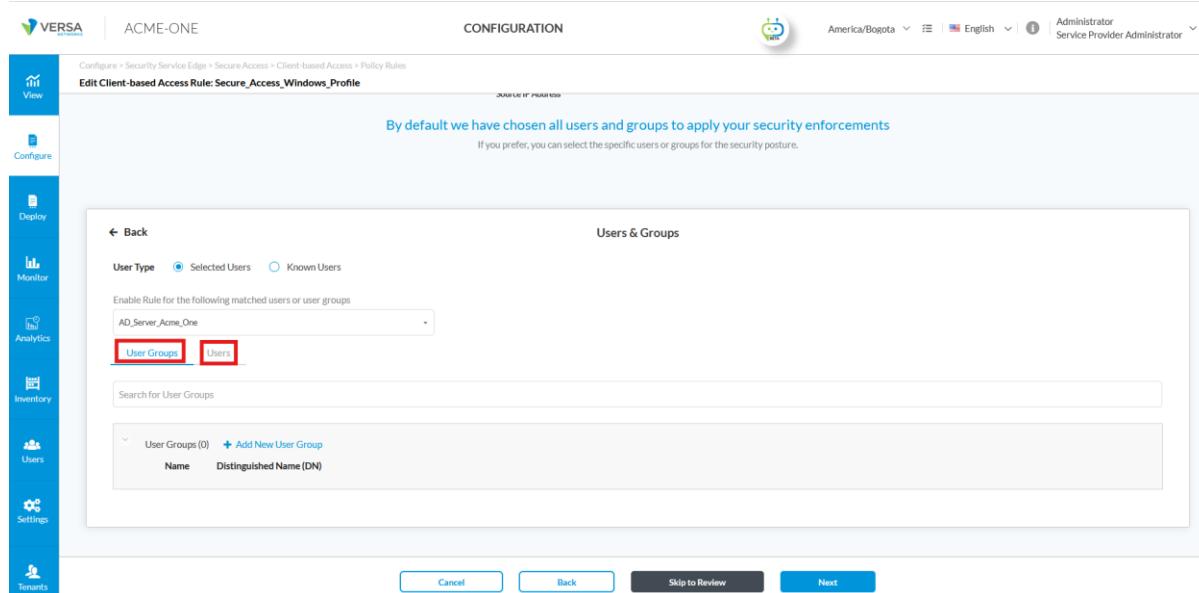
User Groups    Users

Users & Groups

Cancel    Back    Skip to Review    Next

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

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



ACME-ONE CONFIGURATION

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

Edit Client-based Access Rule: Secure\_Access\_Windows\_Profile

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

Enable Rule for the following matched users or user groups

AD\_Server\_Acme\_One

User Groups    Users

Users & Groups

Cancel    Back    Skip to Review    Next

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

## VERIFICATION

When a user connects to the Gateway and 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.

The screenshot shows the 'Events' tab selected in the top navigation bar. It displays two charts: 'Events per user' and 'Events per type', both showing placeholder data with a large blue circle. Below the charts is a table of authentication events:

Receive Time	Appliance	User	Device	RAC Access Type	RAC Event Type	RAC Tunnel IP	RAC IP	VPN Profile	Routing Instance	SecAcc Rule Name
Sep 3rd 2025, 10:11:54 AM -05	SaseGWDiegos-lab	diego-lab@diegolab-versa.net	DESKTOP-PUC20LR	ipsec	create	192.168.224.15	10.73.106.35	Secure_Access_Windows_Profile	ACME-ONE-Enterprise	Secure_Access_Windows_Profile

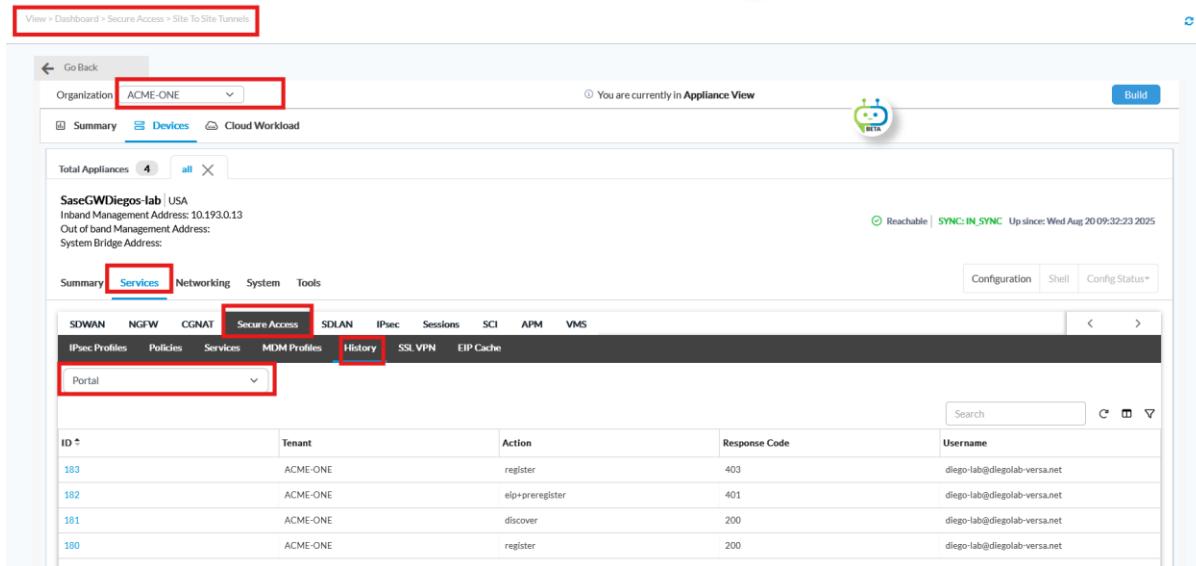
You would see the method used and the authenticated user in the Authentication Logs under **View > Dashboard > Secure Access > Logs > Authentication > Events**.

The screenshot shows the 'Events' tab selected in the top navigation bar. It displays a table of authentication events:

Receive Time	Appliance	Auth Profile	Method	Status	Status Message	Time Taken	User	Source Address	Destination Address	Source Port	De
Sep 3rd 2025, 4:21:02 PM -05	SaseGWDiegos-lab	Default-Auth-Profile	ENTRA-ID-SAML	success	VSA : SAML : Authenticated successfully.	0ms	vip1@diegolabversa.onmicrosoft.com	10.73.106.35	10.73.106.18	61105	44
Sep 3rd 2025, 10:10:17 AM -05	SaseGWDiegos-lab	Default-Auth-Profile	AD_Server_Acme_One	success	VSA : LDAP : Authenticated successfully.	153ms	diego-lab@diegolab-versa.net	10.73.106.35	10.73.106.18	64060	44
Sep 3rd 2025, 10:07:16 AM -05	SaseGWDiegos-lab	Default-Auth-Profile	AD_Server_Acme_One	failure	VSA : LDAP : Authenticated failed.	30s	diego-lab@diegolab-versa.net	10.73.106.35	10.73.106.18	55738	44

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).

View > Dashboard > Secure Access > Site To Site Tunnels



Organization: ACME-ONE

You are currently in Appliance View

Total Appliances: 4

SaseGWDiegos.lab | USA  
Inband Management Address: 10.193.0.13  
Out of band Management Address:  
System Bridge Address:

reachable | SYNC: IN\_SYNC Up since: Wed Aug 20 09:32:23 2025

Summary Services Networking System Tools

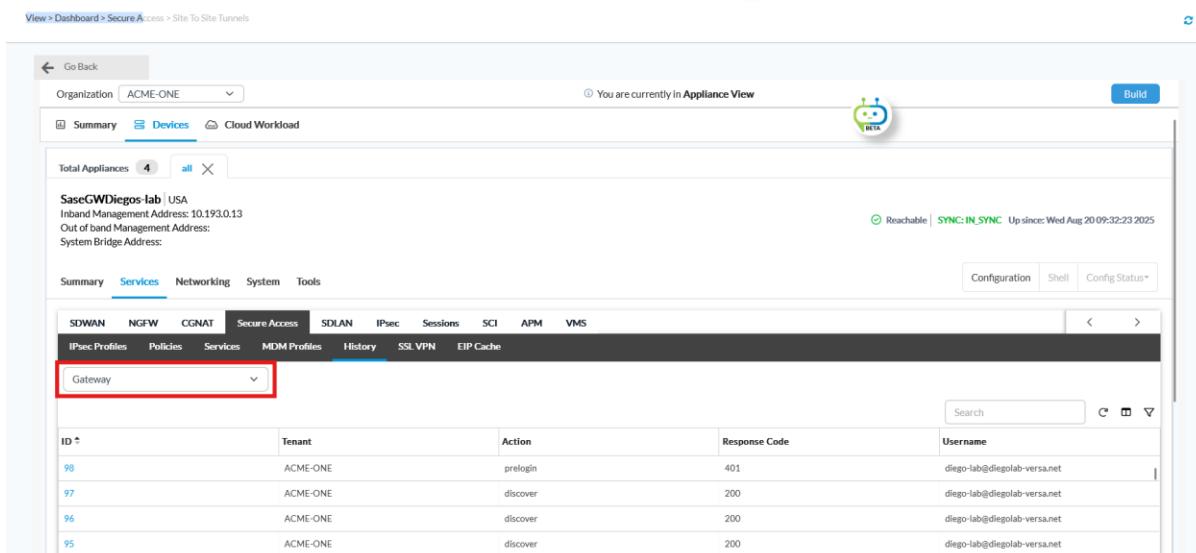
SDWAN NGFW CGNAT Secure Access SDLAN IPsec Sessions SCI APM VMS

IPSec Profiles Policies Services MDM Profiles History SSL VPN EIP Cache

Portal

ID	Tenant	Action	Response Code	Username
183	ACME-ONE	register	403	diego-lab@diegolab-versa.net
182	ACME-ONE	eip+preregister	401	diego-lab@diegolab-versa.net
181	ACME-ONE	discover	200	diego-lab@diegolab-versa.net
180	ACME-ONE	register	200	diego-lab@diegolab-versa.net

View > Dashboard > Secure Access > Site To Site Tunnels



Organization: ACME-ONE

You are currently in Appliance View

Total Appliances: 4

SaseGWDiegos.lab | USA  
Inband Management Address: 10.193.0.13  
Out of band Management Address:  
System Bridge Address:

reachable | SYNC: IN\_SYNC Up since: Wed Aug 20 09:32:23 2025

Summary Services Networking System Tools

SDWAN NGFW CGNAT Secure Access SDLAN IPsec Sessions SCI APM VMS

IPSec Profiles Policies Services MDM Profiles History SSL VPN EIP Cache

Gateway

ID	Tenant	Action	Response Code	Username
98	ACME-ONE	prelogin	401	diego-lab@diegolab-versa.net
97	ACME-ONE	discover	200	diego-lab@diegolab-versa.net
96	ACME-ONE	discover	200	diego-lab@diegolab-versa.net
95	ACME-ONE	discover	200	diego-lab@diegolab-versa.net

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
          STATUS SESSION TO EXPIRATION
IP ADDRESS      NAME      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.

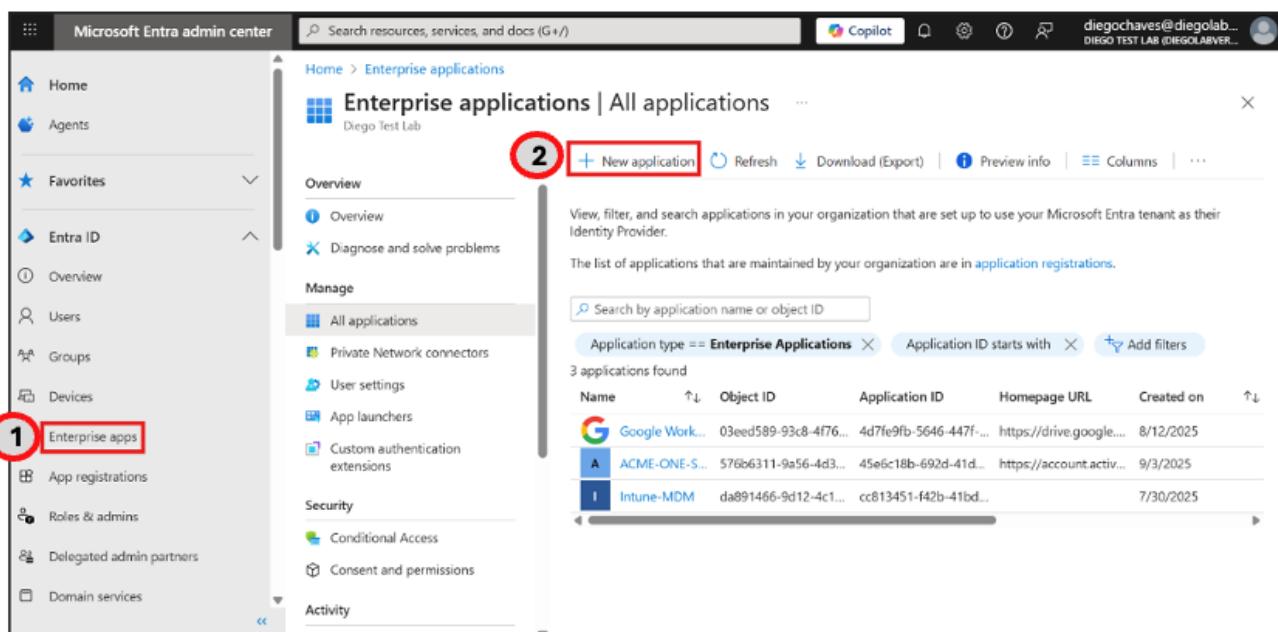
## Entra ID Configuration

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**.



The screenshot shows the Microsoft Entra admin center interface. The left sidebar is titled 'Microsoft Entra admin center' and includes links for Home, Agents, Favorites, Entra ID (Overview, Users, Groups, Devices), Enterprise apps (highlighted with a red circle labeled '1'), App registrations, Roles & admins, Delegated admin partners, and Domain services. The main content area is titled 'Enterprise applications | All applications' and shows a list of registered applications. The top navigation bar includes a search bar, Copilot, and user information (diegochaves@diegolab...). The '+ New application' button in the top right is highlighted with a red circle labeled '2'.

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

2. Select **Create a new application**

Click **+ Create your own application**.

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

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

Click **Create**.

1 + Create your own application

2 ACME-ONE-SAML

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

### 3. Set up SAML-based SSO

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

1 Single sign-on

2 SAML

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

Field	Description
<b>Reply URL (Assertion Consumer Service URL) and Sign on URL (Optional)</b>	Enter the URL to which Okta sends OAuth responses. The responses are sent in the format <b>. https://saseGw-FQDN/versa-flexvnf/saml/login-consumer</b> . (Here the Gateway's FQDN is used as the main URL +/versa-flexvnf/saml/login-consumer ). In the example <b>https://acme-one-sasegwdiegos-lab.versanow.net/versa-flexvnf/saml/login-consumer</b>
<b>Identifier (Entity ID)</b>	Enter the service provider entity ID, which is <b>https://saseGw-FQDNt/metadata</b> . In the example <b>https://acme-one-sasegwdiegos-lab.versanow.net/metadata</b>

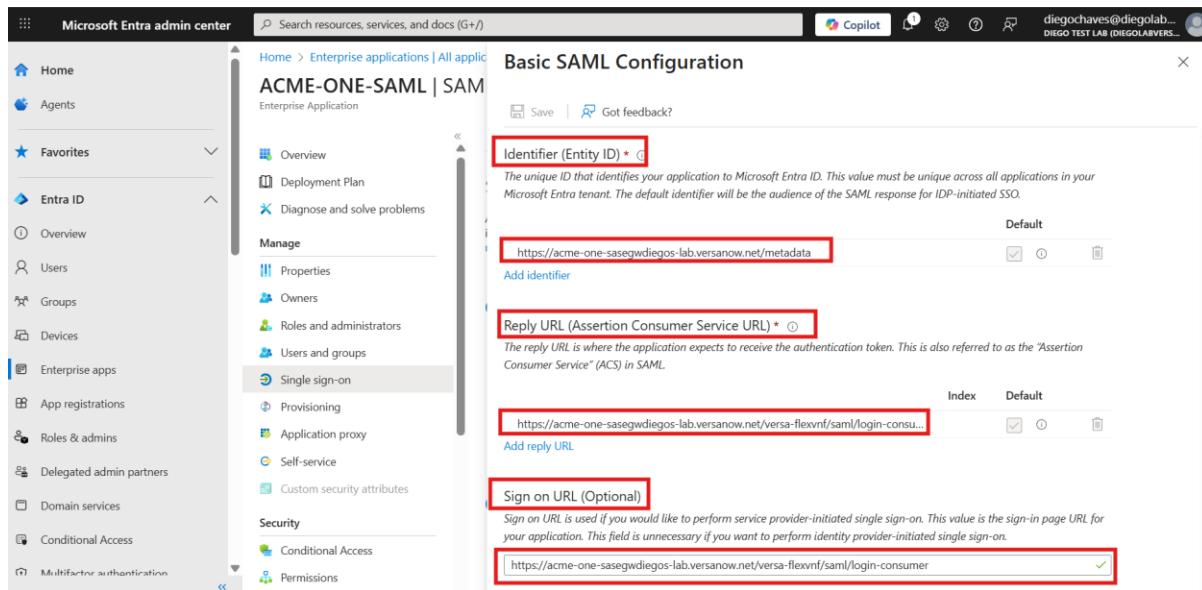
<b>Attribute Statements</b>	Enter the role, organization, and idle timeout attributes. The attribute strings are case sensitive.
<b>Group Attribute Statements (optional)</b>	<p>To allow Versa to receive all user-to-group mappings from Okta, configure a group attribute statement as follows:</p> <p><b>Name:</b> <a href="https://schemas.microsoft.com/ws/2008/06/identity/claims/groups">https://schemas.microsoft.com/ws/2008/06/identity/claims/groups</a></p> <p><b>Name format:</b> Unspecified</p> <p><b>Filter:</b> Select <b>Regex</b> (or equivalent option) and enter <code>*</code></p> <p>This configuration ensures that all groups a user belongs to are included in the SAML assertion. Versa uses this information to apply group-based mappings for Internet Protection rules, Private App Protection, and other user-based policies.</p>
<b>Preview the SAML Assertion</b>	Click to <b>preview the SAML assertion</b> . Copy the metadata and save it as an XML file.

```

<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion ID="id-5773745532411860288246009139" IssueInstant="2025-08-08T17:10:21.828Z" Version="2.0"
  xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
  <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"/>
  <saml2:Subject>
    <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">userN@ame</saml2:NameID>
    <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:c:cm:bearer">
      <saml2:SubjectConfirmationData NotOnOrAfter="2025-08-08T17:15:22.008Z" Recipient="https://acme-one-saseg@diegos-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-saseg@diegos-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:xsi="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">GroupName Match Starts with ".*" (ignores case)
      </saml2:AttributeValue>
    </saml2:Attribute>
  </saml2:AttributeStatement>
</saml2:Assertion>

```

- Configure the parameters as shown in the previous table, in [Basic SAML Configuration](#) and then click **Save**.

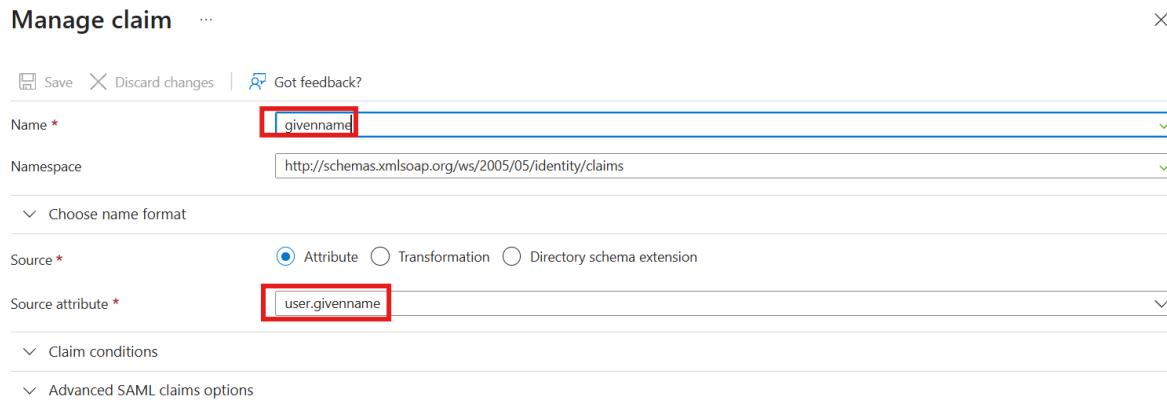


## 6. Define Attributes & Claims.

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

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

Home > Enterprise applications | All applications > ACME-ONE-SAML | SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims >



## Manage claim ...

X

Save Discard changes Got feedback?

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

## Manage claim ...

X

Save Discard changes Got feedback?

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

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

- Click + Add a group Claim

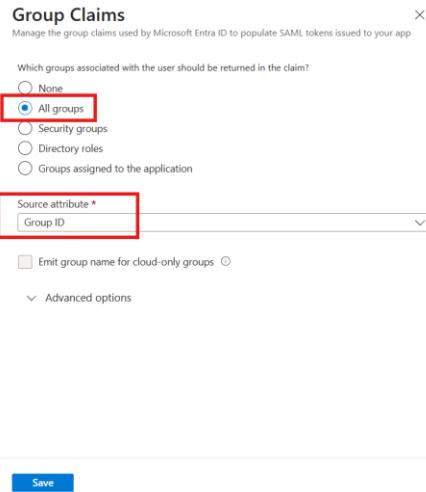
## Attributes &amp; Claims ...

X

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

Required claim		
Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...]
Additional claims		
Claim name	Type	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname
Advanced settings		

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



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

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

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

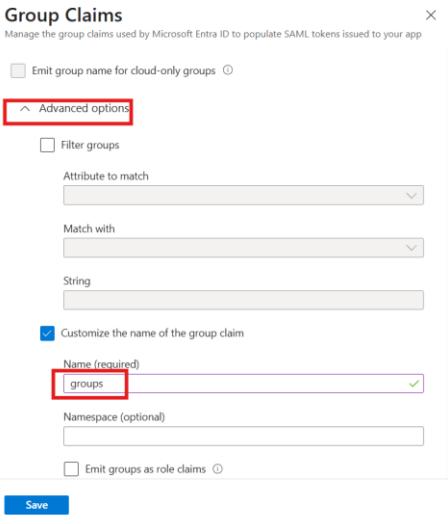
Source attribute \*

Emit group name for cloud-only groups

Advanced options

**Save**

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



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

Emit group name for cloud-only groups

Advanced options

Filter groups

Attribute to match

Match with

String

Customize the name of the group claim

Name (required)

Namespace (optional)

Emit groups as role claims

**Save**

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

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

String

Customize the name of the group claim

Name (required)  ✓

Namespace (optional)

Emit groups as role claims  ⓘ

Apply regex replace to groups claim content

Regex pattern \*

Regex replacement pattern \*

Expose claim in JWT tokens in addition to SAML tokens

**Save**

## 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.

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

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

Enterprise Application

Overview Deployment Plan Diagnose and solve problems

**Manage**

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

**Security**

- Conditional Access
- Permissions
- Token encryption

Activity

Sign-in logs

Upload metadata file Change single sign-on mode Test this application Got feedback?

**3** SAML Certificates

Token signing certificate

Status	Active
Thumbprint	0382CE53329AACF016A20F1C7419EBF0E150D786
Expiration	9/4/2028, 10:34:51 AM
Notification Email	diegochaves@diegolabversa.onmicrosoft.com
App Federation Metadata Url	<a href="https://login.microsoftonline.com/a08ab2d2-a5df-481b-9ffa-13a2a2a2a2a2">https://login.microsoftonline.com/a08ab2d2-a5df-481b-9ffa-13a2a2a2a2a2</a>
Certificate (Base64)	<b>Download</b>
Certificate (Raw)	<a href="#">Download</a>
Federation Metadata XML	<a href="#">Download</a>

Verification certificates (optional)

Required	No
Active	0
Expired	0

**4** Set up ACME-ONE-SAML

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

Login URL	<a href="https://login.microsoftonline.com/a08ab2d2-a5df-481b-9ffa-13a2a2a2a2a2">https://login.microsoftonline.com/a08ab2d2-a5df-481b-9ffa-13a2a2a2a2a2</a>
Microsoft Entra Identifier	<a href="https://sts.windows.net/a08ab2d2-a5df-481b-9ffa-13a2a2a2a2a2">https://sts.windows.net/a08ab2d2-a5df-481b-9ffa-13a2a2a2a2a2</a>
Logout URL	<a href="https://login.microsoftonline.com/a08ab2d2-a5df-481b-9ffa-13a2a2a2a2a2">https://login.microsoftonline.com/a08ab2d2-a5df-481b-9ffa-13a2a2a2a2a2</a>

## 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

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

### New Group

Got feedback?

Group type \*

Group name \*

Group description

Microsoft Entra roles can be assigned to the group

Membership type \*

Owners  
No owners selected

Members  
No members selected

**Create**

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

Example:

UPN → [vip@acme-one.onmicrosoft.com](mailto:vip@acme-one.onmicrosoft.com)

Display Name → vip

Home > Groups | Overview > Users > Groups | Overview > New Group > Groups | All groups > VIP\_Group | Roles and administrators > Users >

### Create new user ...

Create a new internal user in your organization

X

Basics Properties Assignments Review + create

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

#### Identity

User principal name \*

@  

Domain not listed? [Learn more](#)

Mail nickname \*



Derive from user principal name

Display name \*



Password \*



Auto-generate password

Account enabled 

[Review + create](#)

[Previous](#)

[Next: Properties >](#)

 [Give feedback](#)

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

Home > Groups | Overview > Users > Groups | Overview > New Group > Groups | All groups > VIP\_Group | Roles and administrators > Users >

### Create new user ...

Create a new internal user in your organization

X

Basics **Properties** Assignments Review + create

#### Identity

First name 

Last name 

User type 



#### Authorization info

 [Edit Certificate user IDs](#)

#### Job Information

Job title 

Company name 

Department 

Employee ID 

Employee type 

Employee hire date 

Office location 

[Review + create](#)

[Previous](#)

[Next: Assignments >](#)

 [Give feedback](#)

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

Select the previously created **VIP\_Group** (or any other relevant group).

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

## Create new user

X

Create a new internal user in your organization

Basics Properties **Assignments** Review + create

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

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

No assignments to display.

Review + create

&lt; Previous

Next: Review + create &gt;

Give feedback

## Select group

X

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

Search

5 results found

All Groups

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

**Select**

Selected (1)

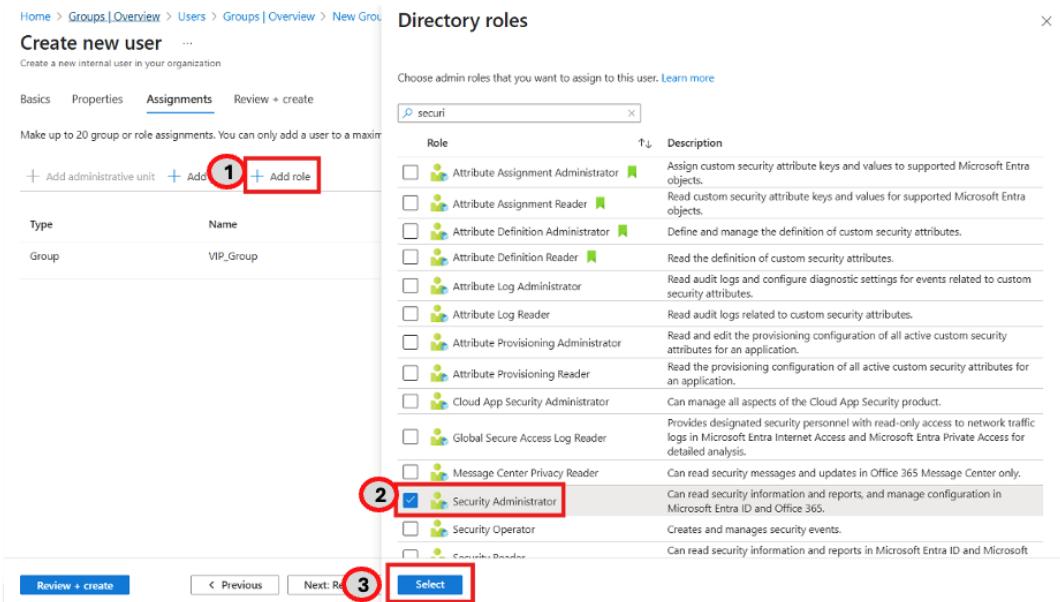
Reset

 VIP\_Group

Unselect

- 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.



**Create new user** ...

Create a new internal user in your organization

Basics Properties **Assignments** Review + create

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

**1** **Add role**

Type Name

Group VIP\_Group

**2** **Security Administrator**

**3** **Select**

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

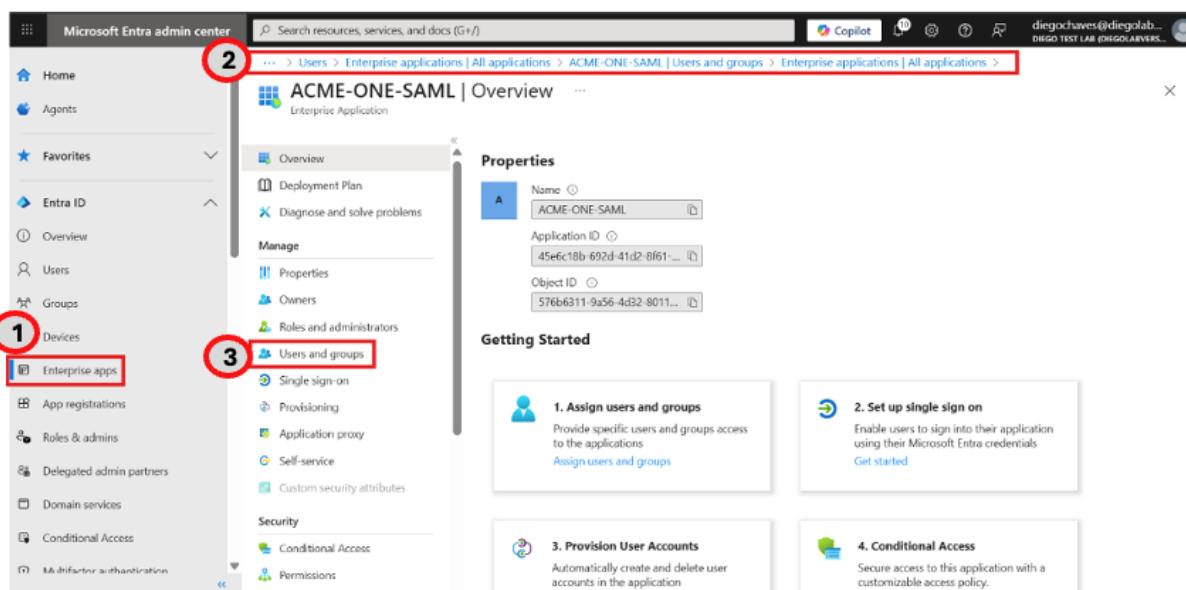
Role	Description
Attribute Assignment Administrator	Assign custom security attribute keys and values to supported Microsoft Entra objects.
Attribute Assignment Reader	Read custom security attribute keys and values for supported Microsoft Entra objects.
Attribute Definition Administrator	Define and manage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

**Review + create** < Previous Next: **3** Select

## Review & Create

- Confirm the user configuration in the **Review + create** tab.
- Assigning Groups to the SAML Application in Entra ID
- Once the group and users are created, the final step is to assign them to the SAML application so they can authenticate.

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



**Microsoft Entra admin center**

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

1 **Enterprise apps**

2 **ACME-ONE-SAML** | Overview

3 **Users and groups**

**Properties**

- Name: ACME-ONE-SAML
- Application ID: 45e6c18b-692d-41d2-6f61...
- Object ID: 576b6311-9a56-4d32-8011...

**Getting Started**

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

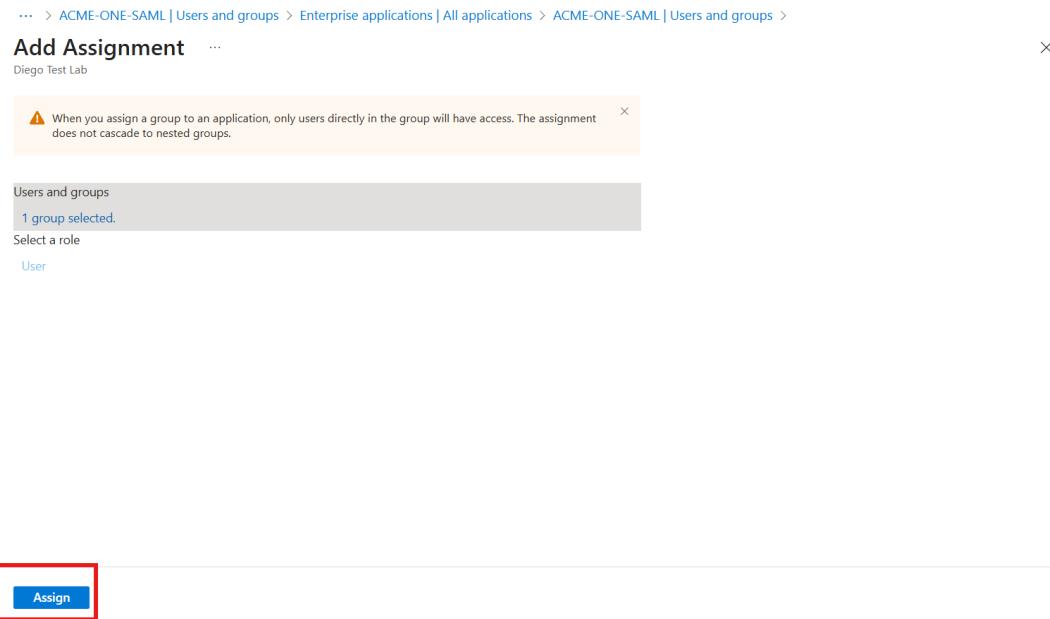
11. Click **Add user/group**, search for the group (Example, VIP\_Group), select it, and assign it to the application.

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

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

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

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



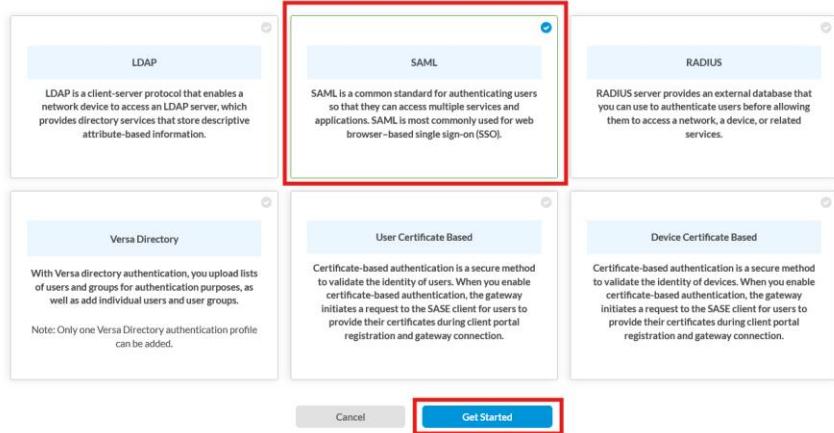
Concerto configuration for ENTRA-ID SAML Authentication Profiles **Navigate to** User and Device Authentication Profiles, then Go to: Configure > Security Service Edge > Users and Device Authentication > Profiles then "+ Add"

	Name	Type	Description	Tags	Last Modified
<input type="checkbox"/>	AD_Server_Acme_One	LDAP			7/28/2025, 4:54:47 PM Administrator

Select **SAML**, Click Get Started

## Add User and Device Authentication Profile

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

Select **ENTRA-ID**

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

From this page, copy/download the values required :

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

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

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

Enterprise Application

Overview Deployment Plan Diagnose and solve problems

**Manage**

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

Conditional Access Permissions Token encryption

**Activity**

Sign-in logs

**3 SAML Certificates**

**Token signing certificate**

- Status: Active
- Thumbprint: 0382CE53329AACF016A20F1C7419EBF0E150D786
- Expiration: 9/4/2028, 10:34:51 AM
- Notification Email: diegochaves@diegolabversa.onmicrosoft.com
- App Federation Metadata Url: <https://login.microsoftonline.com/a08ab2d2-a5df-481b-9ffa-bfb7a50a22c4/saml2>
- Certificate (Base64)** Download
- Certificate (Raw)** Download
- Federation Metadata XML** Download

**Verification certificates (optional)**

- Required: No
- Active: 0
- Expired: 0

**4 Set up ACME-ONE-SAML**

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

- Login URL**: <https://login.microsoftonline.com/a08ab2d2-a5df-481b-9ffa-bfb7a50a22c4/saml2>
- Microsoft Entra Identifier**: <https://sts.windows.net/a08ab2d2-a5df-481b-9ffa-bfb7a50a22c4/>
- Logout URL**: <https://login.microsoftonline.com/a08ab2d2-a5df-481b-9ffa-bfb7a50a22c4/saml2>

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

Add SAML Authentication Profile

1 Settings 2 Users And User Groups 3 Review & Submit

Select SAML Type

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

**Single Sign-on URL \***

**Service Provider Entity ID \***

**Identity Provider Entity ID \***

**Identity Provider Certificate \***

Cache Expiry Time (mins): 10

Concurrent Logins: 1

Reply URL (Assertion Consumer Reply URL)

- <https://acme-one-sasegwdiegos-lab.versanow.net/versaflex/saml/login-consumer>

Cancel Skip to Review Next

Complete the parameters using the values from the Microsoft Entra id

Example:

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

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

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

Edit SAML Authentication Profile: ENTRA-ID-SAML

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

Service Provider Entity ID \*: <https://acme-one-sasegwlegos-labversanow.net/metadata>

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

Prefix ID: OKTA

Group Attribute: OKTA

Cache Expiry Time (mins): 10

Cache Expiry Mode: Select

Cookie Expiry Time (mins): 720

Concurrent Logins: 1

Buttons: Cancel, Skip to Review, Next

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

Add SAML Authentication Profile

Single Sign-on URL: [https://dev-49982259.okta.com/app/dev-49982259\\_acmeoneesaml\\_1/exp/71thqsg75d7/so/saml](https://dev-49982259.okta.com/app/dev-49982259_acmeoneesaml_1/exp/71thqsg75d7/so/saml)

Service Provider Entity ID \*: <https://acme-one-sasegwlegos-labversanow.net/metadata>

Identity Provider Entity ID \*: <https://www.okta.com/exp/71thqsg75d7>

Prefix ID: OKTA

Group Attribute: OKTA

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

Buttons: Cancel, Skip to Review, Next

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

## Add Certificate/CA-Chain/Private Key

Certificate Type  CA Chain

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

CA-Chain Name \*

ACME-ONE-SAML

**Upload File**

**Cancel**

**Add**

Then **Add**

## Add Certificate/CA-Chain/Private Key

Certificate Type  CA Chain

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

CA-Chain Name \*

ACME-ONE-SAML

**Upload File**

**ACME-ONE-SAML.cer**

**Cancel**

**Add**

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

Edit SAML Authentication Profile: ENTRA-ID-SAML

1 Settings    2 Users And User Groups    3 Review & Submit

Select SAML Type



Single Sign-on URL \*

<https://login.microsoftonline.com/008ab2c5-5d8-401b-9f9-0b7a50a224f4/saml2>

Service Provider Entity ID \*

<https://acme-one-saml.sso.versacloud.net/metadata>

Identity Provider Entity ID \*

<https://windows.net/008ab2c5-5d8-401b-9f9-0b7a50a224f4>

Prefix ID

Cache Expiry Time (min)

10

Cache Expiry Mode

—Select—

Group Attribute

Cookie Expiry Time (min)

720

Concurrent Logins

1

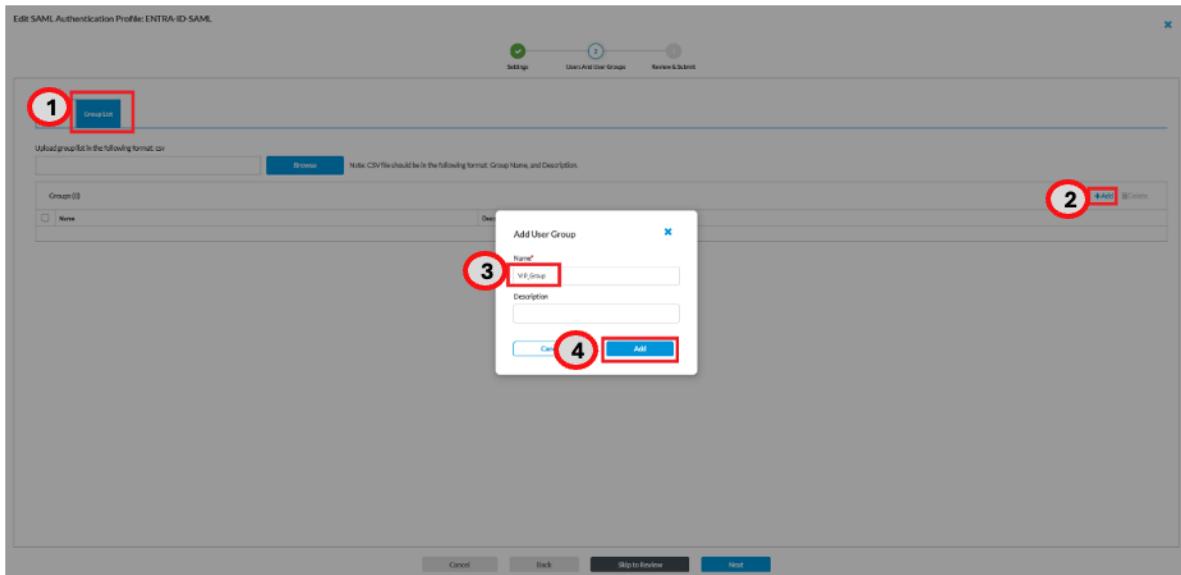
Reply URL (Assertion Consumer Reply URL)

<https://acme-one-saml.sso.versacloud.net/versa-floent/saml/login-consumer>

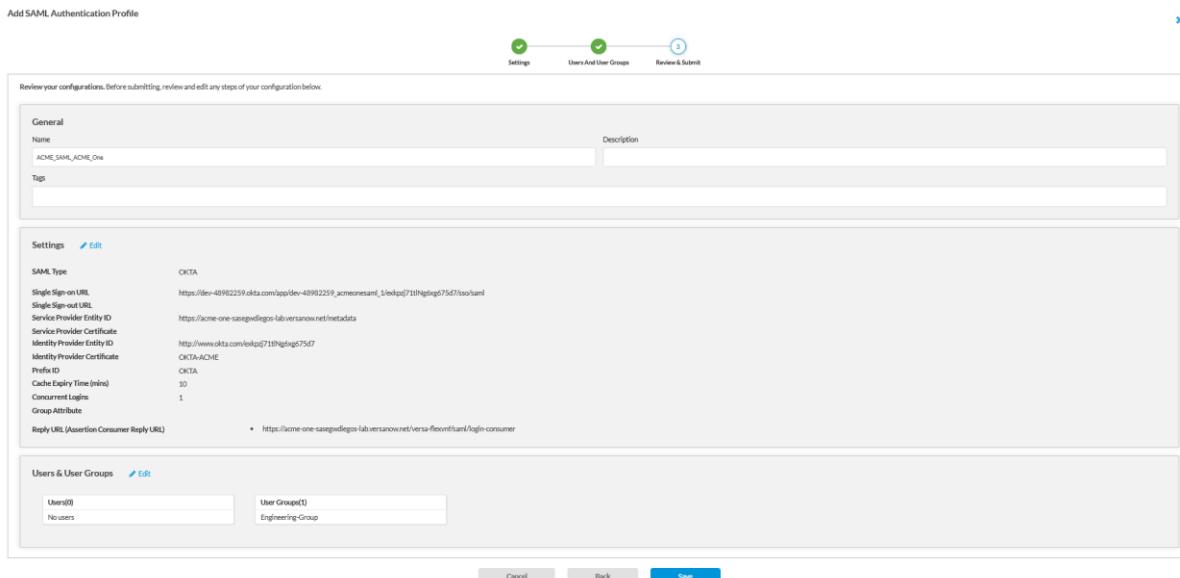
**Cancel**    **Skip to Review**    **Next**

Then **Next**

On the **Users and User Groups** page, you can add individual users or entire groups. Click **User Groups** and add the **VIP1\_Group** created in the Okta app. Click **Add**, then click **Next** to continue.



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



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

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

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

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.

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

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

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

## Versa Directory

Versa Directory is a Versa-hosted IDP service based on LDAP, available for Versa-hosted SSE Services. The prerequisite to use this service for your tenant is that it is enabled on Headend at infrastructure level by Versa or MSP (if using third-party hosted headend): [https://docs.versa-networks.com/Security\\_Service\\_Edge\\_\(SSE\)/Configuration\\_from\\_Concerto/Configure\\_User\\_and\\_Device\\_Authentication#Configure\\_Versa\\_Directory\\_Authentication\\_Using\\_an\\_IAM\\_Server](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_User_and_Device_Authentication#Configure_Versa_Directory_Authentication_Using_an_IAM_Server)

Now to use Versa Directory and create users refer the following document: [https://docs.versa-networks.com/Security\\_Service\\_Edge\\_\(SSE\)/Configuration\\_from\\_Concerto/002\\_Versa\\_SSE\\_Quick\\_Start\\_Guide#Step\\_3:\\_Configure\\_User\\_Authentication](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/002_Versa_SSE_Quick_Start_Guide#Step_3:_Configure_User_Authentication)

## 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](#).