

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

About This Document

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

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

Document Information

Title	Step-By-Step Configuration Guide for Versa Secure Internet Access (VSIA)
Author	Versa Professional Services
Version	V 1.0

Disclaimer

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

Before you begin

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

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

Scenario	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

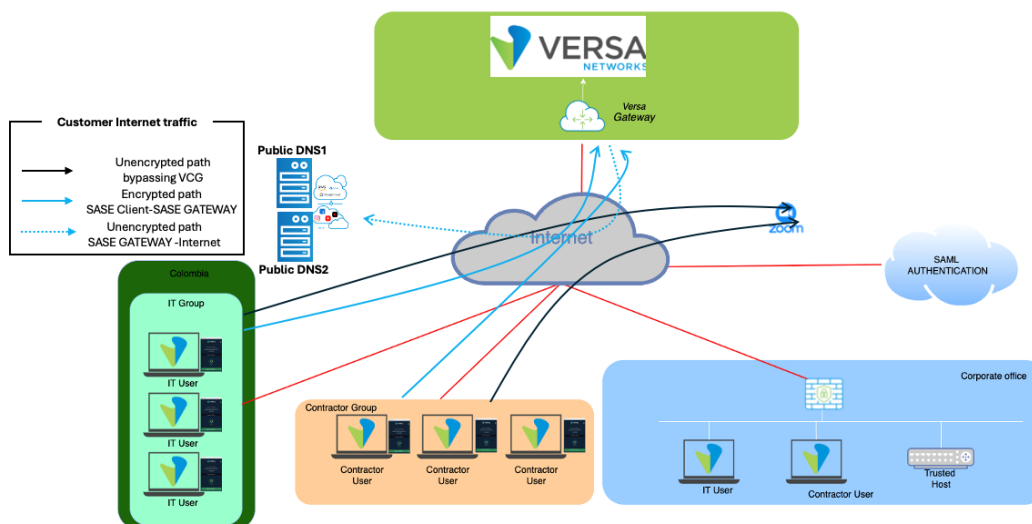
- SSE Gateway: Deploy with VSIA enabled.
- DNS & Monitoring: Configure two public DNS servers and enable Digital Experience Monitoring (DEM) for Office 365.
- SASE Client:
 - Enable Always-On with Trusted Network Detection.
 - Block all traffic if the gateway connection fails.
 - In corporate offices,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

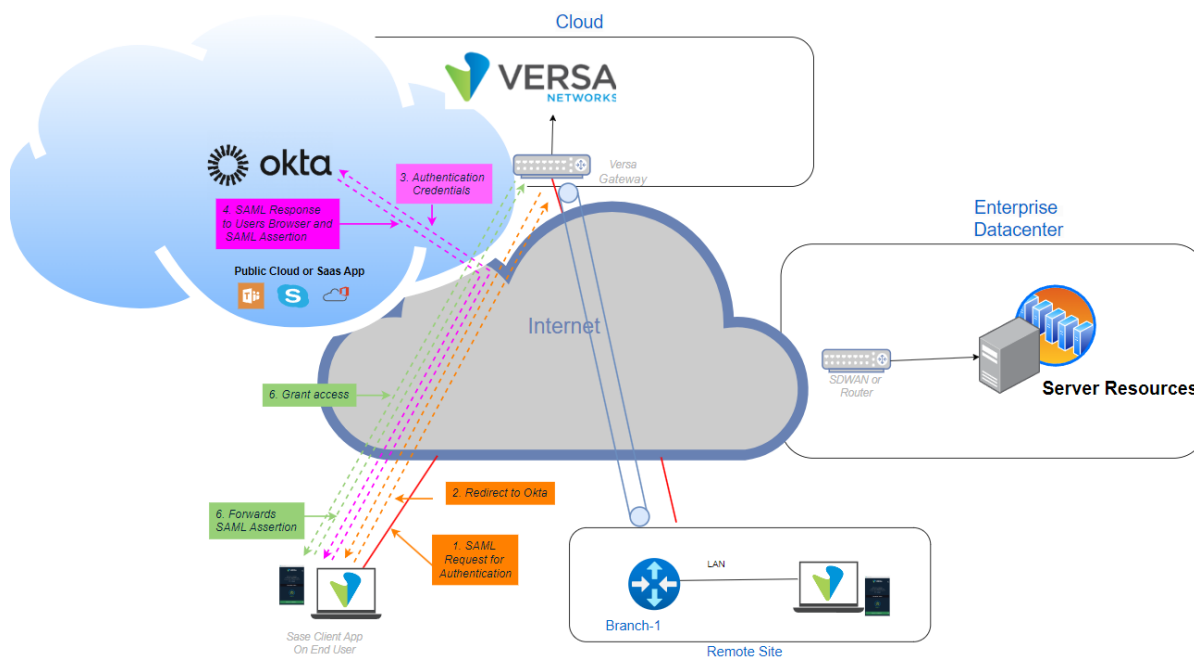
The VSIA configuration consists of the following steps:

- 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.



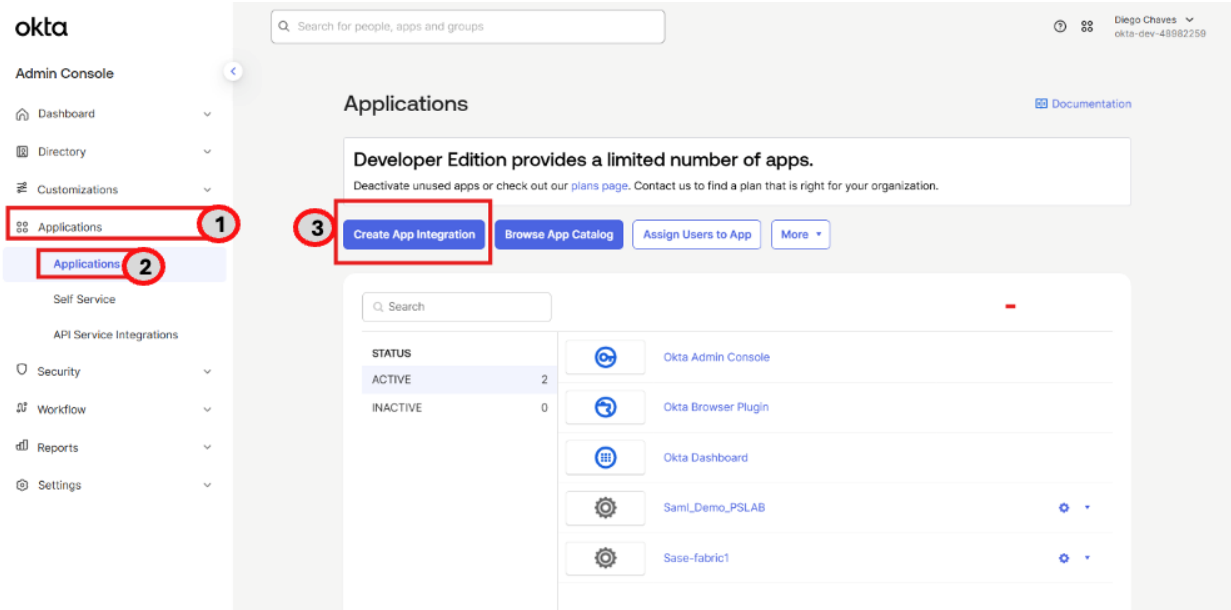
Okta SAML Configuration

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

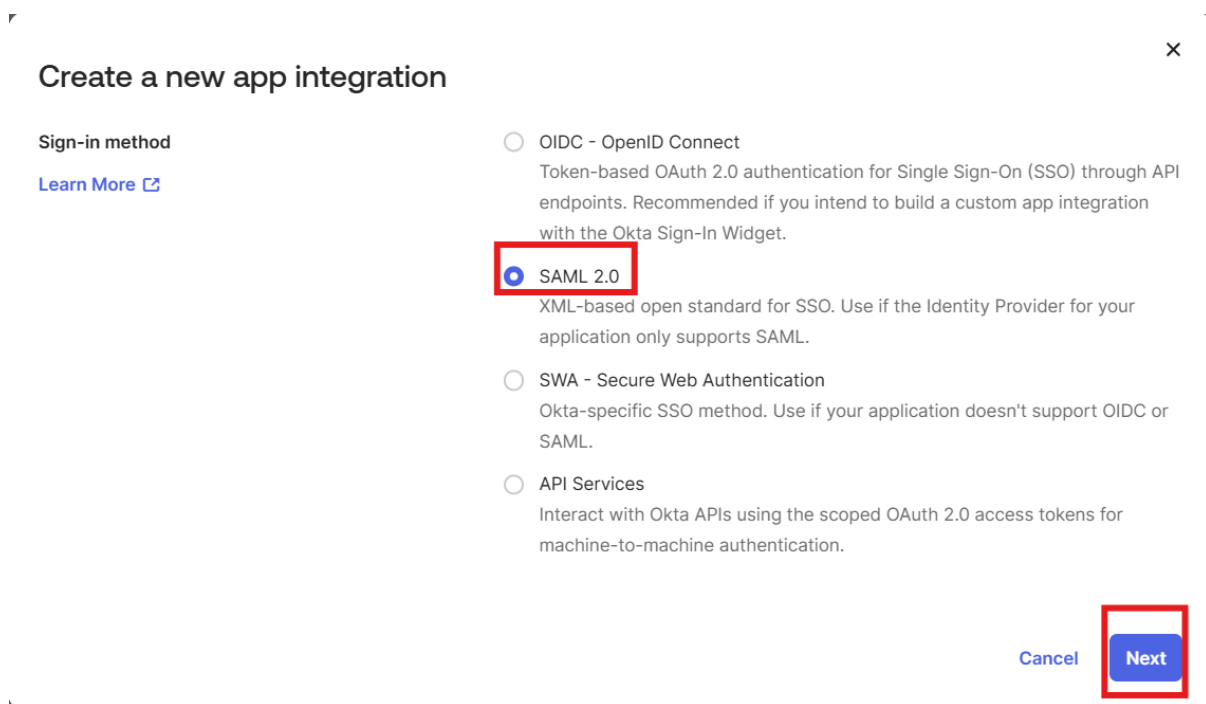
[Create an application on Okta](#)

1. Log in to your Okta admin console.

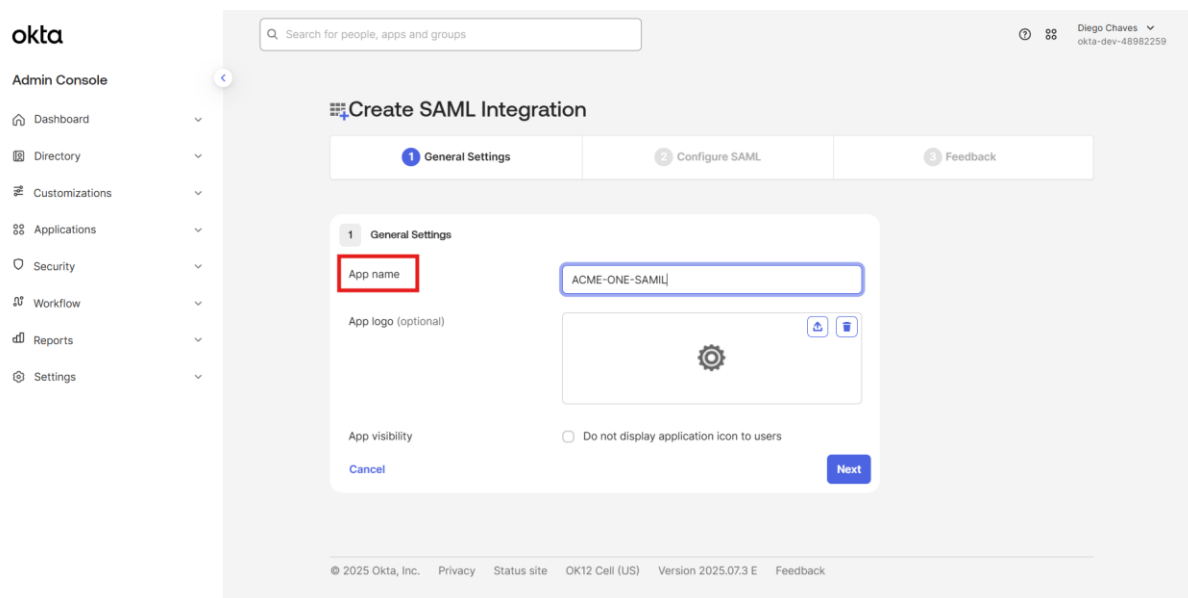
Navigate to: Application (1), then click on Applications (2) >> Create App Integration (3).



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



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



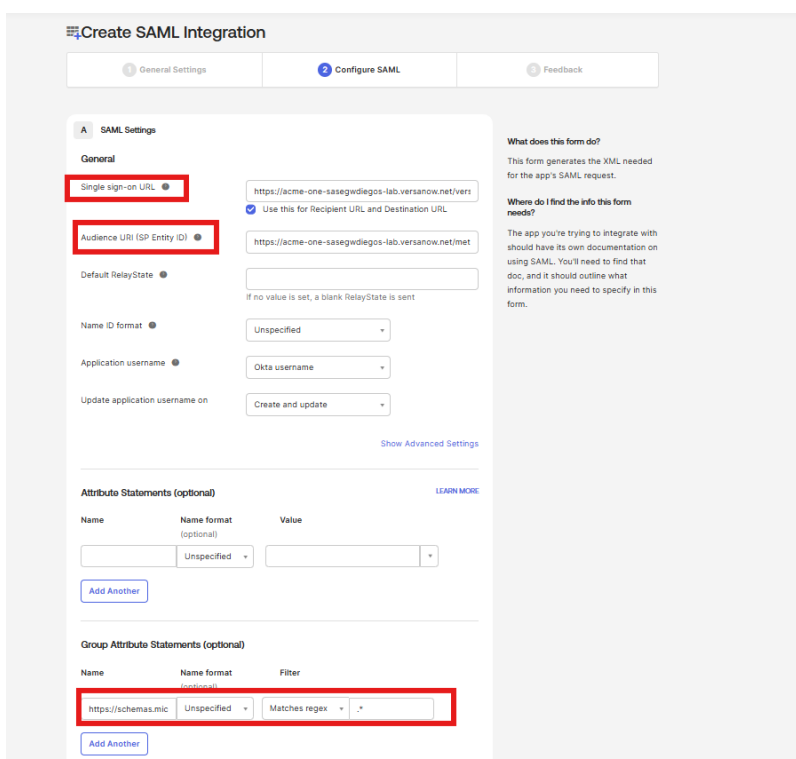
4. Define custom attributes.

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

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

XML output from the SAML Assertion preview:

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion ID="Id-5773745524186088346009139" 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.versaow.net/versa-flexvnf/saml/login-consumer"/>
    </saml2:SubjectConfirmation>
  </saml2:Subject>
  <saml2:Conditions NotBefore="2025-08-08T17:05:22.008Z" NotOnOrAfter="2025-08-08T17:15:22.008Z">
    <saml2:AudienceRestriction>
      <saml2:Audience>https://acme-one-sasegwdiegos-lab.versaow.net/metadata/</saml2:Audience>
    </saml2:AudienceRestriction>
  </saml2:Conditions>
  <saml2:AuthnStatement AuthnInstant="2025-08-08T17:10:21.828Z">
    <saml2:AuthnContext>
      <saml2:AuthnContextClassRef urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport/</saml2:AuthnContextClassRef>
    </saml2:AuthnContext>
  </saml2:AuthnStatement>
  <saml2:AttributeStatement>
    <saml2:Attribute Name="https://schemas.microsoft.com/ws/2008/06/identity/claims/groups" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml2:AttributeValue>
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">GroupName Match Starts with ".*" (ignores case)
      </saml2:AttributeValue>
    </saml2:Attribute>
  </saml2:AttributeStatement>
</saml2:Assertion>
```



Create SAML Integration

General Settings | **Configure SAML** | Feedback

SAML Settings

General

Single sign-on URL

☒ Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID)

Default Relay State

If no value is set, a blank RelayState is sent

Name ID format

Application username

Update application username on

[Show Advanced Settings](#)

Attribute Statements (optional) [LEARN MORE](#)

Name	Name format (optional)	Value
<input type="text" value="https://schemas.mic"/>	<input type="text" value="Unspecified"/>	<input type="text" value="Matches regex .*"/>

[Add Another](#)

Group Attribute Statements (optional)

Name	Name format (optional)	Filter
<input type="text" value="https://schemas.mic"/>	<input type="text" value="Unspecified"/>	<input type="text" value="Matches regex .*"/>

[Add Another](#)

What does this form do?
This form generates the XML needed for the app's SAML request.

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

- 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

1
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_acmeonesaml1/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

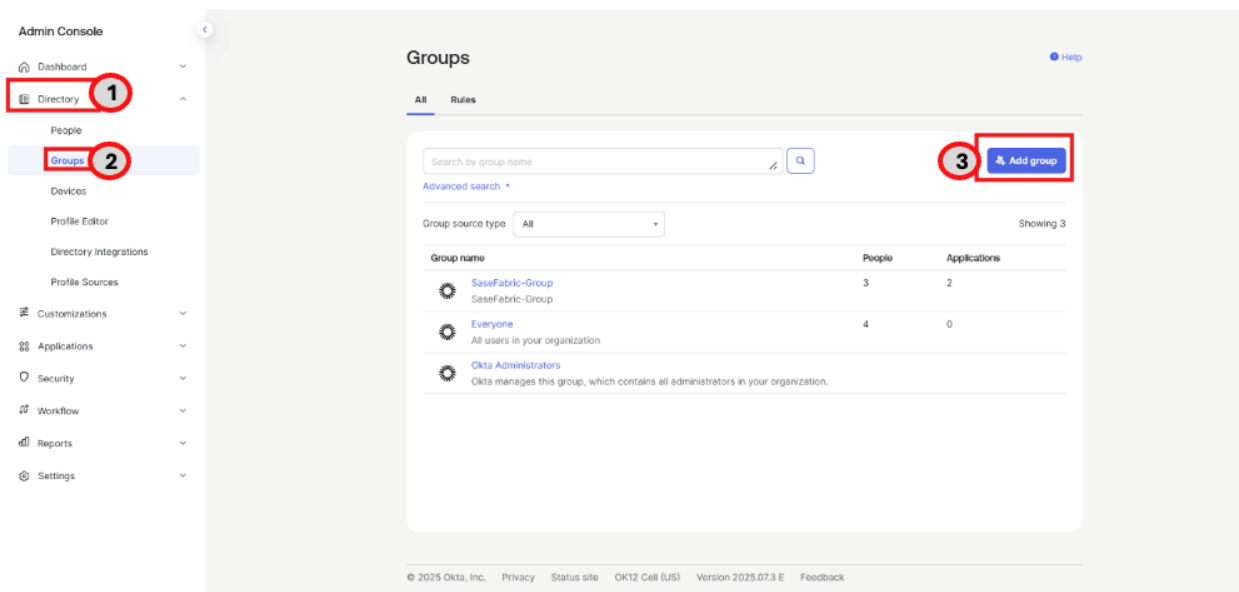
Note: Rename the file extension of the downloaded certificate file from .cert to .crt before use.

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

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



In the name field, enter a group name and click [Save](#).

Add group

Name

Description (optional)

[Save](#)
[Cancel](#)

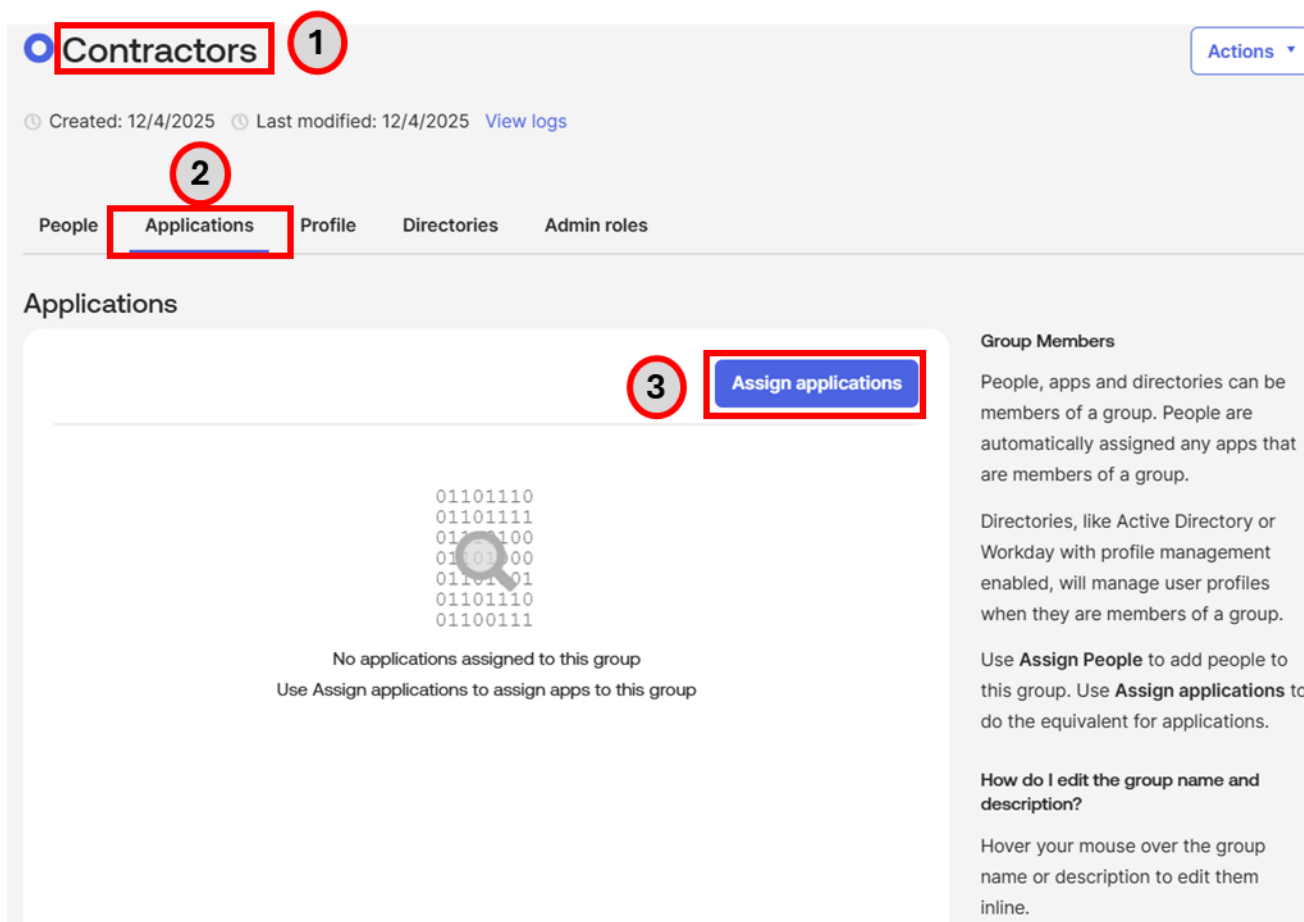
Add group

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.



Contractors 1

Created: 12/4/2025 Last modified: 12/4/2025 [View logs](#)

2

People **Applications** Profile Directories Admin roles

3 **Assign applications**

Applications

01101110
01101111
01101100
01101000
01101001
01101110
01100111

No applications assigned to this group
Use Assign applications to assign apps to this group

Group Members

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

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

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

How do I edit the group name and description?

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

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

Assign Applications to Contractors

X

	Okta Admin Console	Assign
	Okta Workflows	Assign
	Okta Workflows OAuth	Assign
	Versa	Assign
	ACME-ONE-SAML	Assign

[Done](#)

Repeat the same steps for the IT group.


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

The screenshot shows the Okta Admin Console interface. On the left, the 'Admin Console' sidebar is visible with 'Directory' and 'People' highlighted. The main area shows the 'People' page with a search bar and a table of users. The 'Add person' button is highlighted with a red box and labeled '3'.

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

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 Contractor

Last name One

Username contractor1@acme-one.com

Primary email contractor1@acme-one.com

Secondary email (optional)

Groups (optional)

Activation Activate now

☒ I will set password


.....

☒ User must change password on first login

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

Save Save and Add Another Cancel

Add Person

User type  User

First name IT

Last name One

Username ituser1@acme-one.com

Primary email ituser1@acme-one.com

Secondary email (optional)

Groups (optional)

Activation Activate now

☒ I will set password

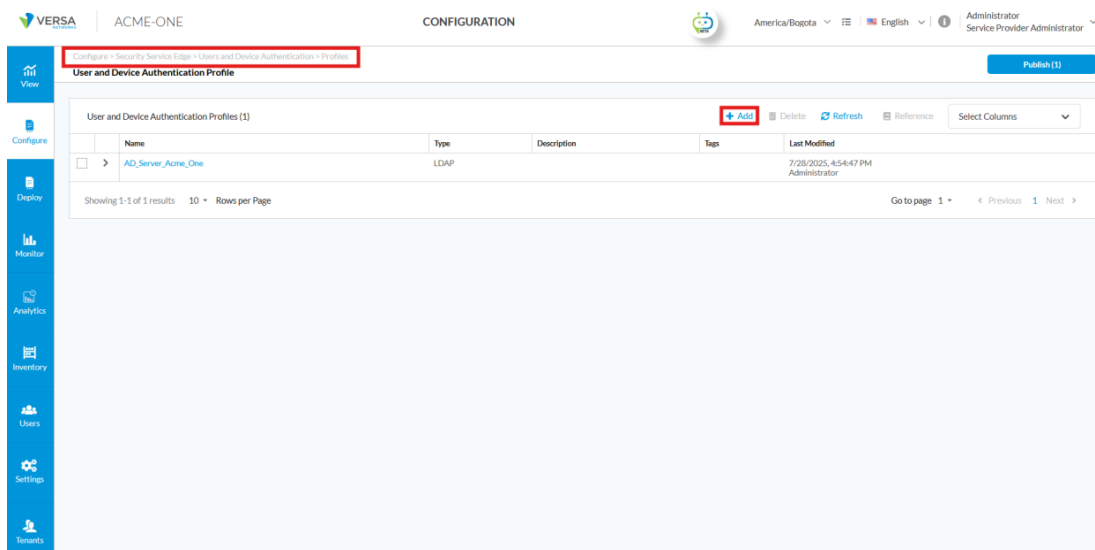
.....

☒ User must change password on first login

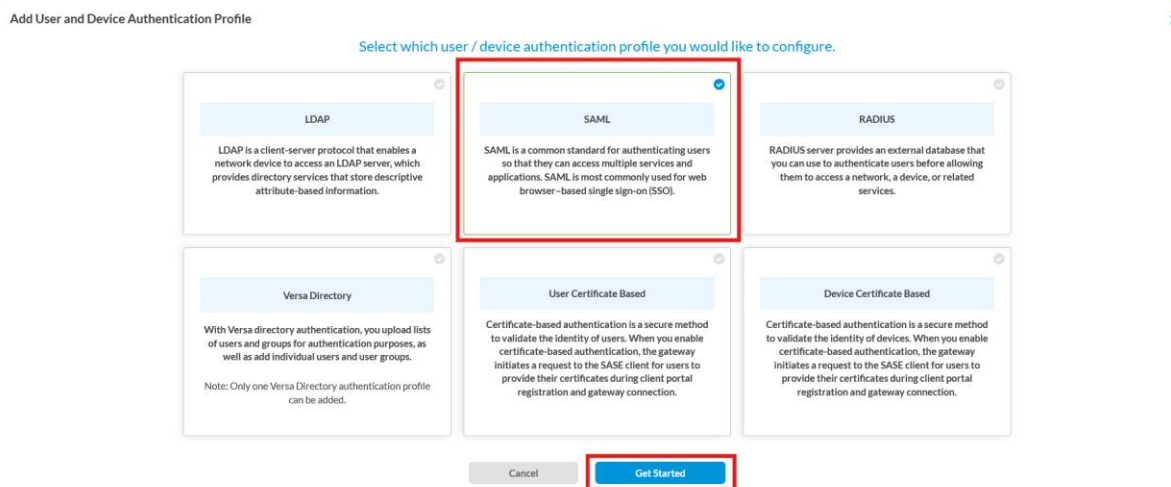
Do not send unsolicited or unauthorized activation emails. [Read more](#)

Save Save and Add Another Cancel

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



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



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

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

Complete the parameters using the values from the Okta app:

Example:

- **Single Sign-on URL:** https://dev-48982259.okta.com/app/dev-48982259_ac-meonesaml_1/exkpzj71tIng6xg675d7/sso/saml
- **Service Provider Entity ID:** <https://acme-one-sasegwdiegos-lab.versanow.net/metadata>
- **Identity Provider Issuer:** <http://www.okta.com/exkpzj71tIng6xg675d7>

Prefix ID: Okta

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

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

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

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



Okta

Okta

Ping Identity

Ping Identity

Office 365

Office 365

Microsoft Entra ID

Microsoft Entra ID

Google IAM

Google IAM

Class Duo

Class Duo

Other

Other

Single Sign-on URL *

https://dev-40982239.okta.com/app/dev-40982239_consumerent_login/7219g1ng7567/authorize

Service Provider Entity ID *

https://acme-one-saasgw4diags-lab.veranov.net/metadata

Identity Provider Entity ID *

https://www.okta.com/help/7219g1ng7567

Prefix ID

OKTA

Group Attribute

Reply URL (Assertion Consumer Reply URL)

https://acme-one-saasgw4diags-lab.veranov.net/versa-flexoft-haml/login-consumer

Single Sign-out URL

Service Provider Certificate

--Select--

+ Add New

Identity Provider Certificate *

OKTA-ACME

+ Add New

Details

Name

OKTA-ACME

File Name

OKTA-ACME.crt

Issued To

dev-40982239

Issued By

dev-40982239

Validty

2025-08-08 12:23:19 to 2035-08-08 12:24:18

Cache Expiry Time (mins)

10

Concurrent Logins

1

Cancel

Skip to Review

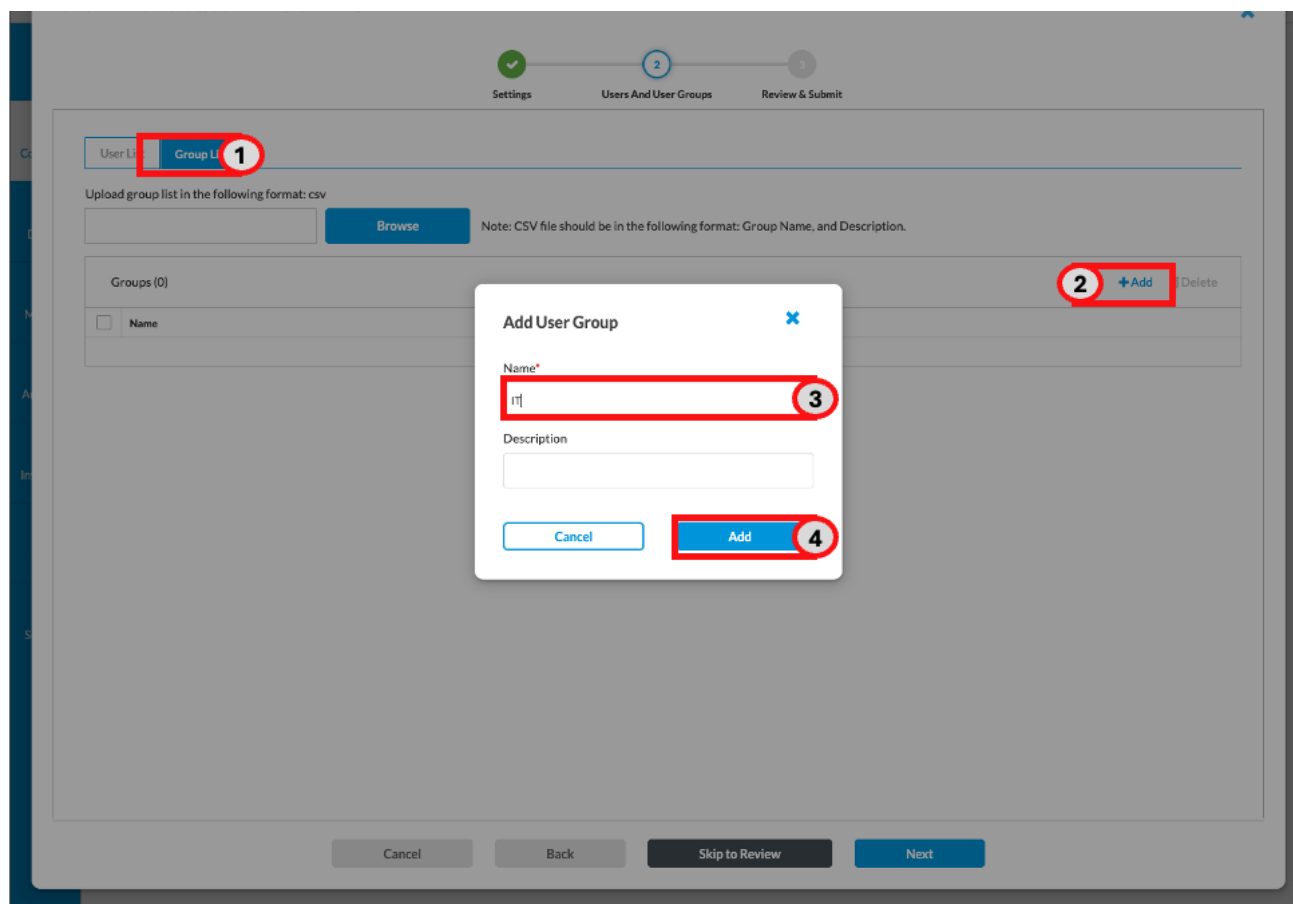
Next

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.

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

General

Name: ACME_SAML_ACHES_One

Description:

Tags:

Settings [Edit](#)

SAML Type	OKTA
Single Sign-on URL	https://dev-48962239.okta.com/app/dev-48962239_acmeonesaml_5/okta/718hgng075d7/sso/saml
Single Sign-out URL	
Service Provider Entity ID	https://acme-one-saasgwellego-lab-versanox.net/metadata
Service Provider Certificate	
Identity Provider Entity ID	https://www.okta.com/okta/718hgng075d7
Identity Provider Certificate	OKTAACHES
Profile ID	OKTA
Cache Expiry Time (min)	30
Concurrent Logins	1
Group Attribute	
Reply URL (Assertion Consumer Reply URL)	https://acme-one-saasgwellego-lab-versanox.net/versa-flexvnt/iam/login/consumer

Users & User Groups [Edit](#)

Users(0): No users

User Groups(1): Engineering Group

Buttons: 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.

The screenshot shows the Versa configuration interface. On the left is a vertical navigation menu with icons for View, Configure, Deploy, Monitor, Analytics, Inventory, Users, and Settings. The main content area is titled "Security Service Edge" and "Secure SD-WAN". Below this, there's a search bar and a list of configuration options. The "Profiles" option is highlighted with a red circle and the number 5. In the main content area, there's a table of profiles. The "Add" button in the table header is highlighted with a red circle and the number 6. Other red circles and numbers 1 through 4 highlight various menu items and table headers.

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

The screenshot shows the "Create Client-based Access" wizard. At the top, there's a progress bar with three steps: 1. Routes & DNS Resolvers, 2. Digital Experience Monitoring, and 3. Review & Deploy. The first step is active. Below the progress bar, there's a section titled "Add which routes and DNS resolvers to use." with a subtext: "If you prefer, you can customize which routes and DNS resolvers to use for the client profile." There are two main sections: "Routes" and "DNS Resolvers". Each section has a list of items and an "Add" button. The "Add DNS Resolvers" button is highlighted with a red circle and the number 7. Other red circles and numbers 1 through 6 highlight various UI elements, including the progress bar, the "Add" buttons, and the "Routes" and "DNS Resolvers" sections.

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.

← Back DNS Resolvers

+ Add (8) Delete (9) Select Columns

Name	Description	DNS Server IP Address	Gateways	Domain
No Data				

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

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.

← Back

Add DNS Resolver

Name* (9) PublicDNS

Description (10)

☒ All Gateways (11) ☐ Select Gateways

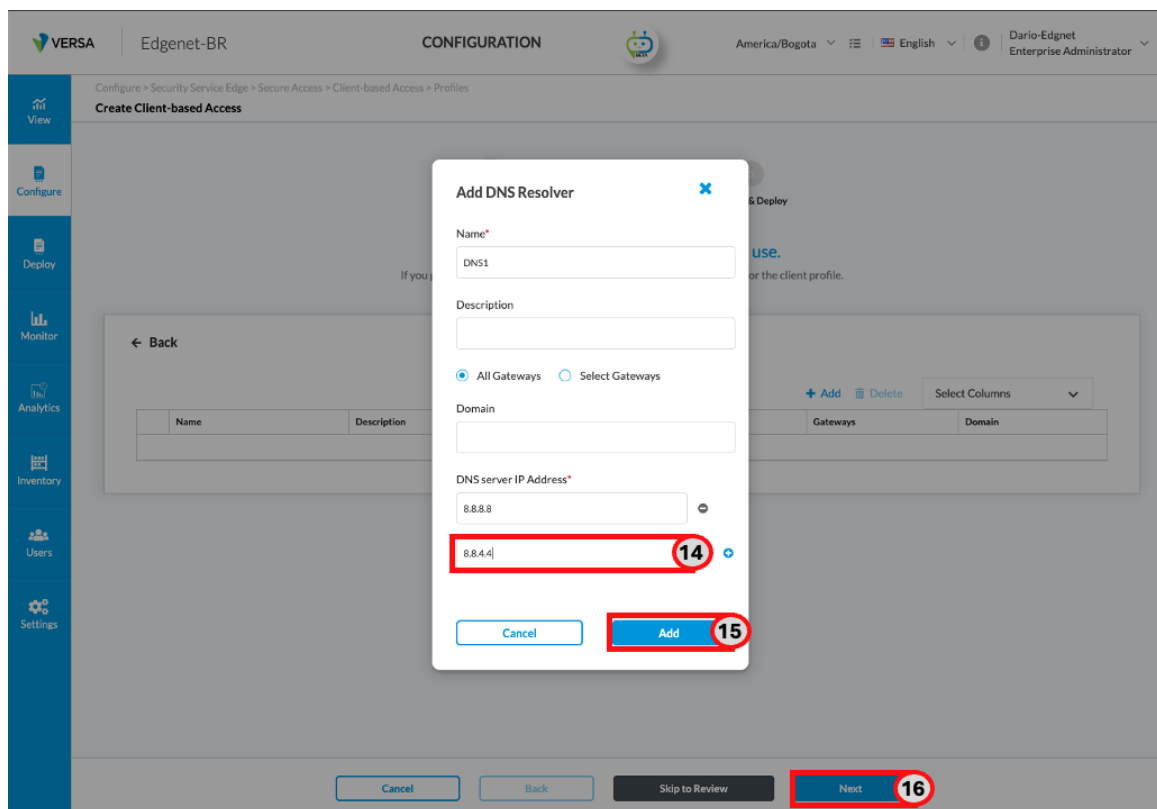
Domain

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

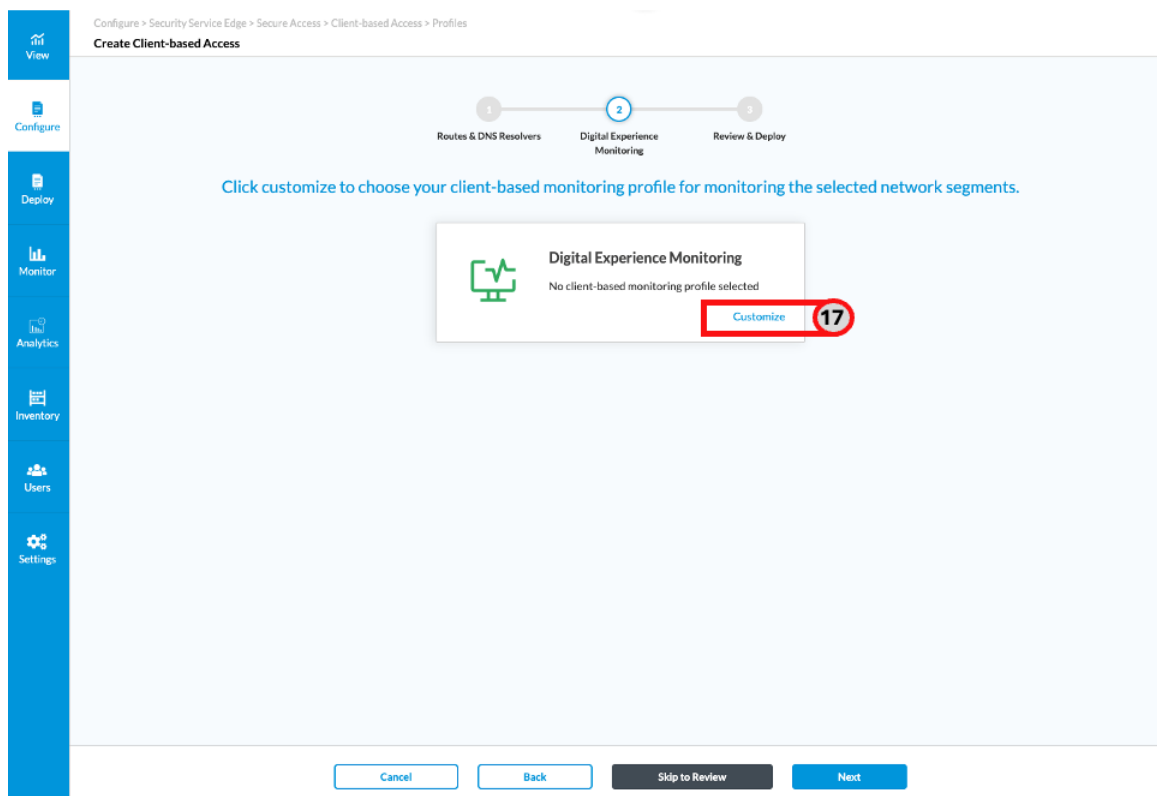
Cancel Add

Cancel Back Skip to Review Next

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



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



Click **+ Add**.

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.

← Back Client-based DEM Profile

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

Client-based DEM Profiles **18** + Add Refresh

Name	User Defined Applications	Predefined Applications	Last Modified
No Data			

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 Publish (2)

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.

Microsoft Office 365 Outlook.com Search and select one or more applications Clear All

Predefined Applications (Selected: 1 of 53)

Druva	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 ...	19 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

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 Publish (2)

✓ User Defined & Predefined Applications +

2 Name, Description & Tags -

Name * 21 DEM_MSOF365 Description 21 Enter description

Tags 21 Type or select tags

Cancel 22 Save

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.

← Back **Client-based DEM Profile**

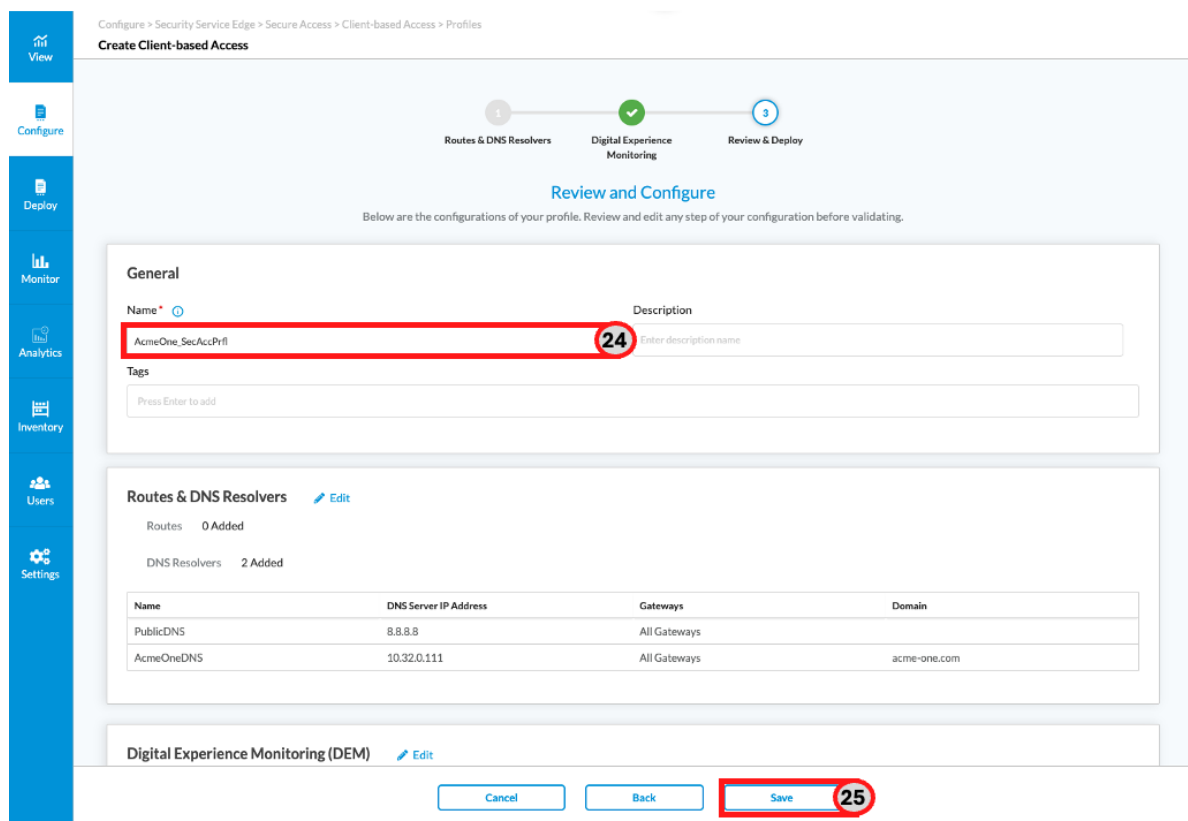
Choose a client-based DEM profile to use for this Secure Remote Access profile.

Client-based DEM Profiles			
Name	User Defined Applications	Predefined Applications	Last Modified
<input checked="" type="checkbox"/> DEM_MSOF365		Microsoft Office 365 Outlook.com	4/8/2025, 18:38:19 Dario-Edgnet

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

Cancel Back Skip to Review 23 Next

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

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

Review and Configure

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

General

Name * 24 Description

Tags

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](#)

25

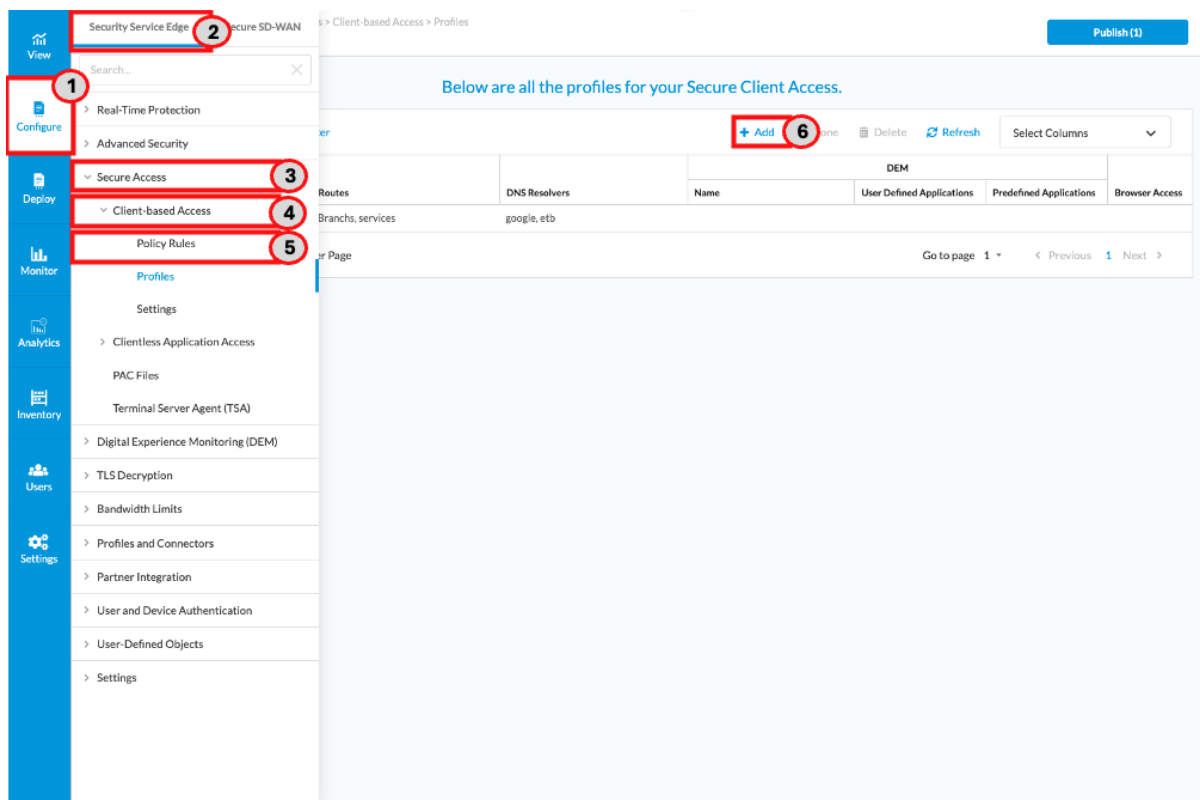
Step 3: Configure Secure Client Access Policy Rules

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

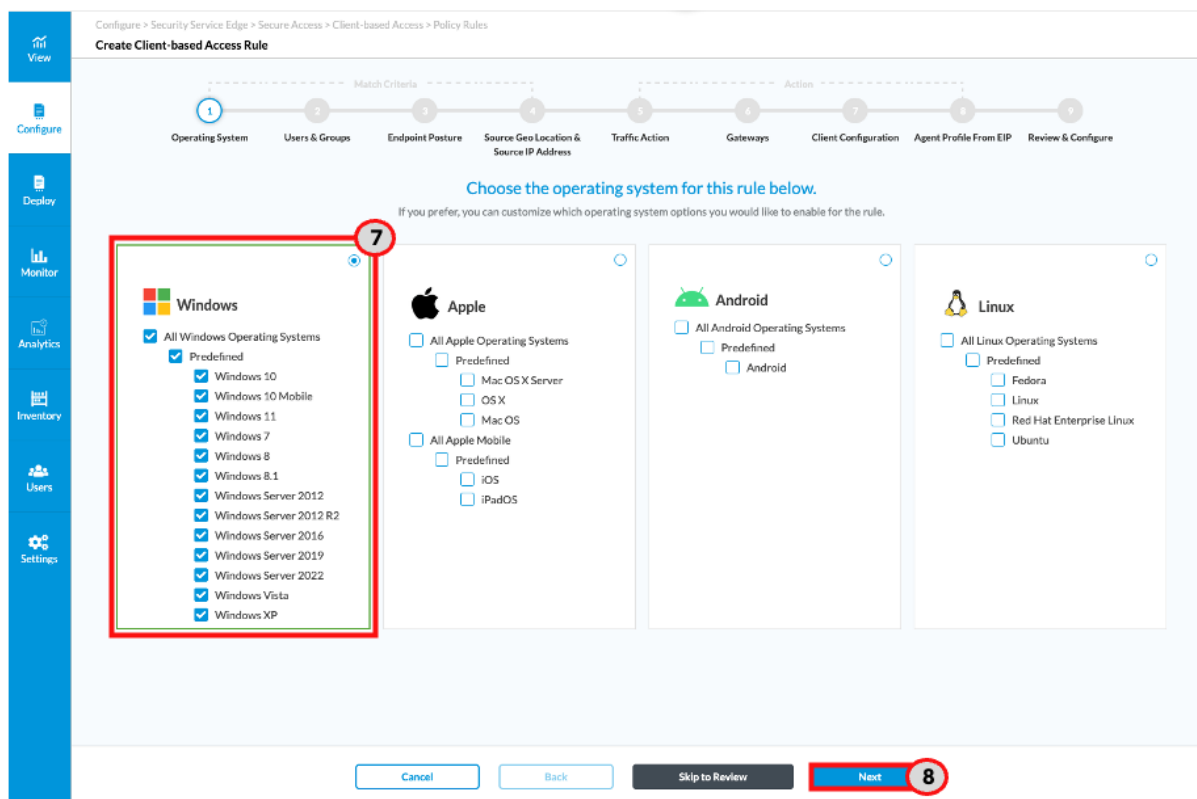
The parameters listed in next table are required to complete the configuration.

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

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



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



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

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

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

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

Create Client-based Access Rule

1 2 3 4 5 6 7 8 9

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)

✓ All devices

[Customize](#) **14**

Device Compliance Status

✓ Managed Status of Devices

All Devices [Customize](#)

Entity Risk Bands

✓ 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

1 2 3 4 5 6 7 8 9

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.

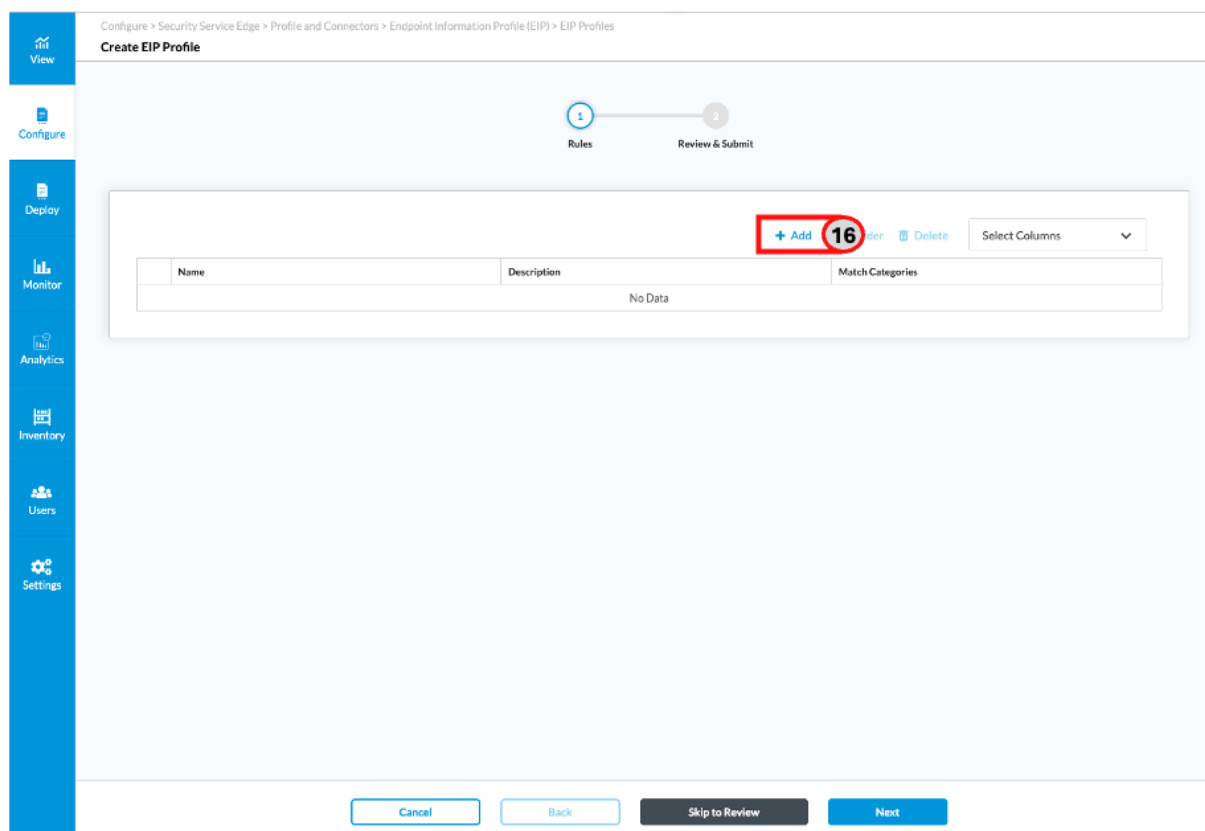
[User Defined](#) [Predefined](#)

[+ Add Existing EIP Profile](#) [Delete](#) [+ Create New EIP Profile](#) **15** [Select Columns](#)

<input type="checkbox"/>	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

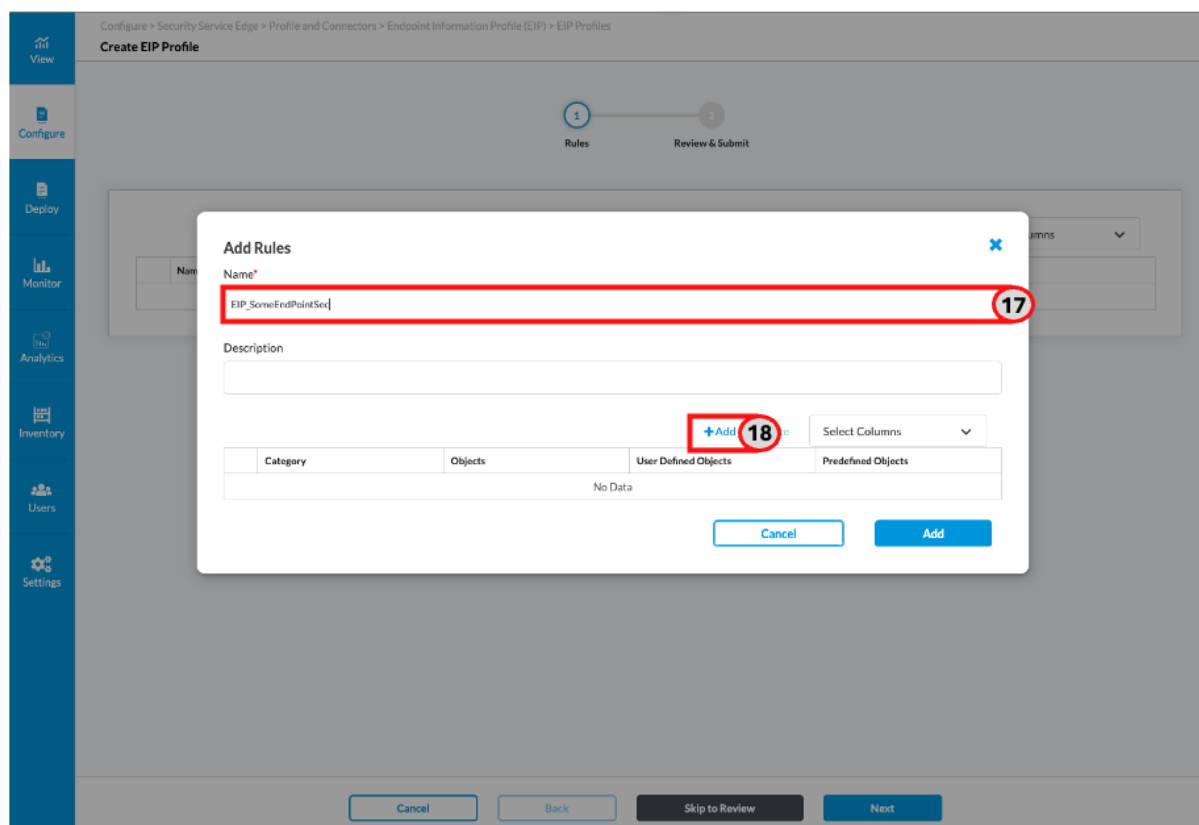
1 Rules 2 Review & Submit

Name	Description	Match Categories
No Data		

+ Add 16 [View](#) [Delete](#) Select Columns

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_SomeEndPointSec 17

Description

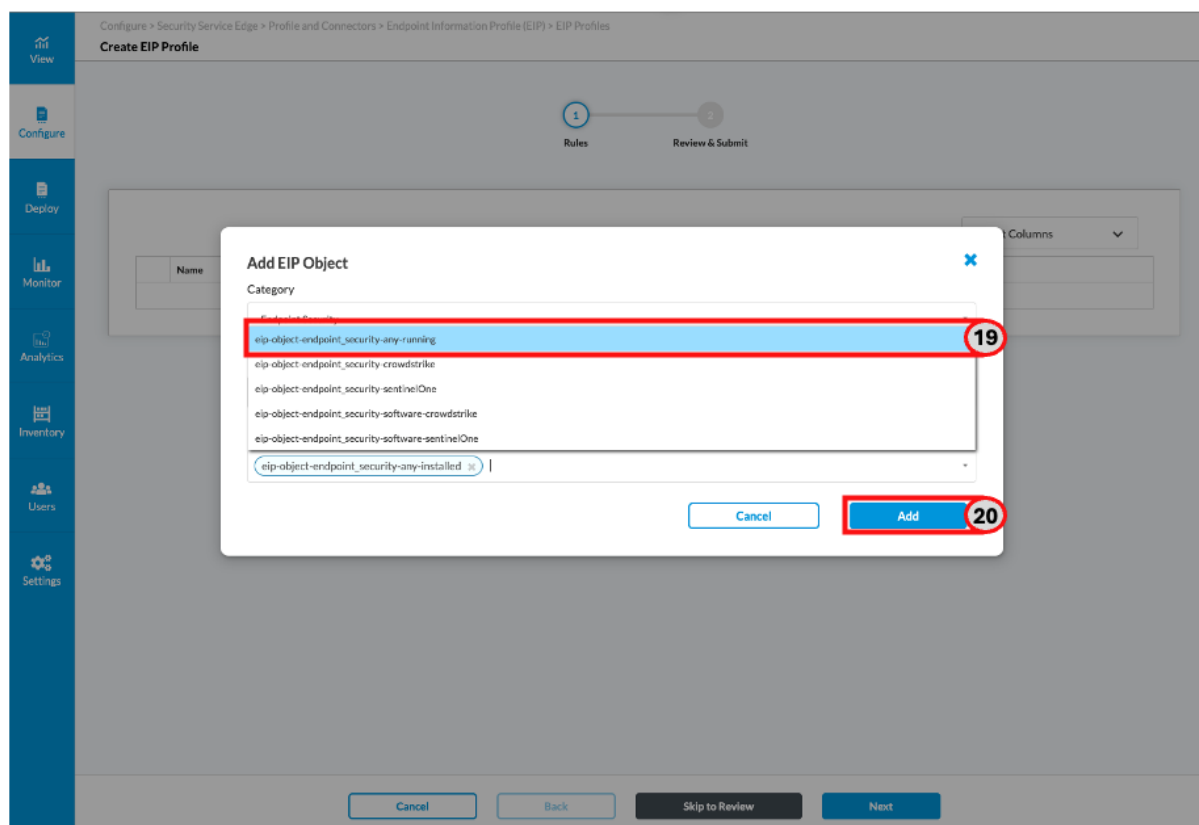
+ Add 18 [View](#) [Delete](#) Select Columns

Category	Objects	User Defined Objects	Predefined Objects
No Data			

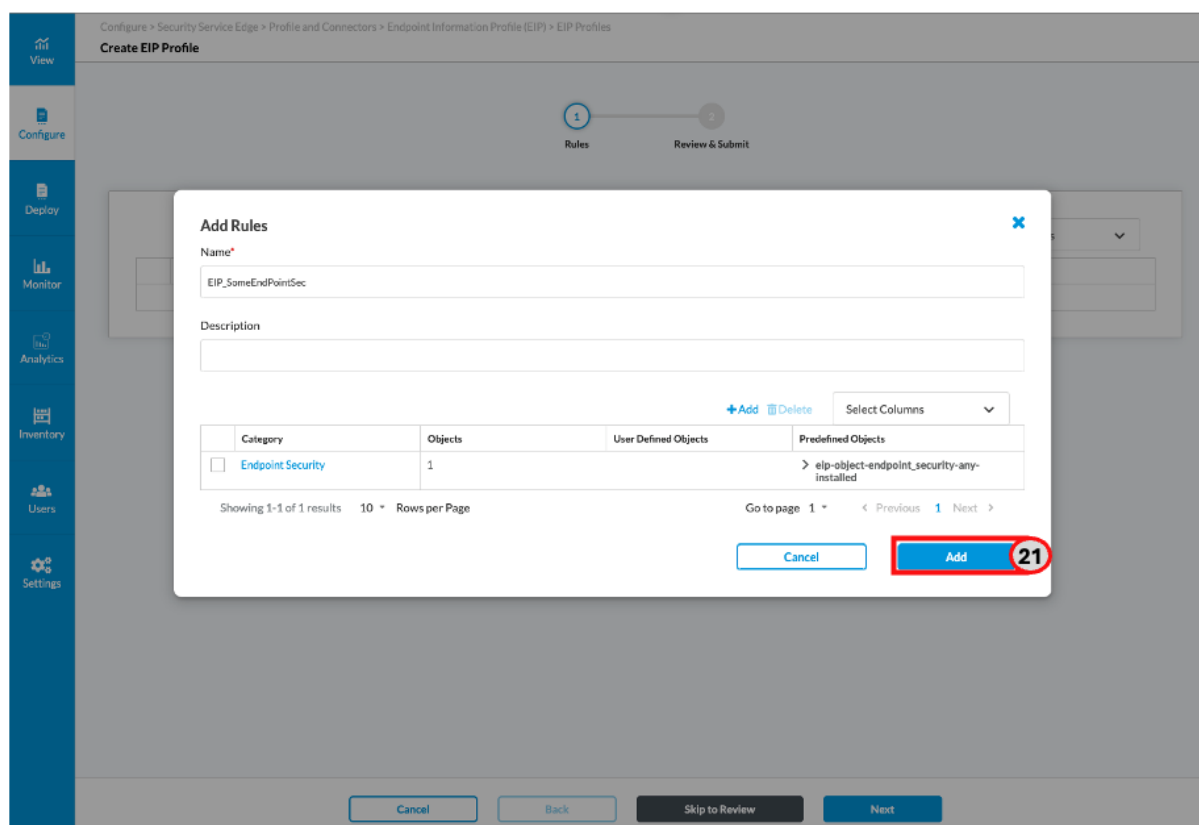
Cancel Add

Cancel Back Skip to Review Next

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



Click **Add** again.



Click Next.

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

Create EIP Profile

1 Rules
2 Review & Submit

Name	Description	Match Categories
<input type="checkbox"/> 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 [?] **23** (see description name)

Description

Tags

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

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.

← 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

+ 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

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

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**.

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.

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

Zoom Search for Applications Clear All Add New

> Custom Applications (Selected: 0 of 1)

> Predefined Applications (Selected: 1 of 53)

LivePerson Microsoft Intun... Microsoft Offi... Microsoft Skyp... OpenDrive PingOne For En...
Planview Proje... 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

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

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

Create Client-based Access Rule

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

All Selected | 1
Default

Gateways

Select VPN
Edzenet-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

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

Client Controls box.

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

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

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

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

Create Client-based Access Rule

Advanced Settings

- ☒ Tamper Protection(Supported only on Windows client from version 7.8) **41**
 - Tamper Protection Override Key **42**
 - ☐ Strict Tunnel Mode
 - ☐ Auto Disconnect Interval
 - ☐ Auto Disconnect Time
 - ☒ Always On **43**
 - Disconnect ☐ Never ☒ Interval (Seconds) 300
 - Override Interval (Seconds) 120
 - Fail ☒ Close **44** ☐ Open
- ☒ Display Gateway (Enable/disable displaying of gateways in Versa Client application)
- ☒ Tunnel Monitoring (Supported from Windows client version 7.6 and Mac client version 7.5) **45**
 - Hosts **45**
 - Interval (Seconds)
 - Interval Retry

Buttons: Cancel, Back, Skip to Review, **Next 46**

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

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

Create Client-based Access Rule

Progress: 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

EIP Agent Profile

Type:

EIP Agent Profiles:

Buttons: Cancel, Back, Skip to Review, **Next 47**

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

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

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

General

Name * 48

Description

Tags

☒ Rule is Enabled

Operating Systems [Edit](#)

Operating System Versions Custom Selection

- 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
 - Windows Server 2019

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

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

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

General

Name *

Tags

☒ Rule is Enabled

Operating Systems [Edit](#)

Operating System Versions Custom Selection

- 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
 - Windows Server 2019

Configure Rule Order

How would you like to process rule "AcmeOneSecAccRuleIT"?

☐ 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

Cancel Back Save

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

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.

Search by keyword or name Filter 53 Clone Reorder Delete Refresh Select Columns

Rule Name	Operating System Versions	Users & Groups	Endpoint Posture	Traffic Action	VPN & Gateway Groups	Status
<input checked="" type="checkbox"/> AcmeOneSecAccRuleIT 52	Windows Windows 10 Windows 10 Mobile Windows 11 More Details	AuthProfile_SAMAL User Groups IT	Endpoint Information Profile (EIP) User Defined EIP_EndPtSecRunni 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-CGH-01 VCG-SA-CGH-02	Enabled
<input type="checkbox"/> Acc_Prfl_Usuarios	Windows Windows 10 Windows 10 Mobile Windows 11 More Details	SAMALGW1 User Groups Uuarios	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
<input type="checkbox"/> Acc_Prfl_Ingenieros	Windows Windows 10 Windows 10 Mobile Windows 11 More Details	SAMALGW1 User Groups Uuarios	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 More Details	SAMALGW1 User Groups Ingenieros Uuarios	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 selec **Edit** in the **Users & Groups** section.

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

Edit Client-based Access Rule: AcmeOneSecAccRuleContractors

Name: AcmeOneSecAccRuleContractors 54 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_SAMAL

- User Group | 1
IT

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

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

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.

← Back **Users & Groups**

User Type ☒ Selected Users ☐ Known Users

Enable Rule for the following matched users or user groups
AuthProfile_SAMAL

[User Groups](#) [Users](#)

[Contractors](#) ⓘ Search for User Groups

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

[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

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](#)

Cancel Back Skip to Review **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

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](#)

Cancel Back Skip to Review 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

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.

← 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.

Country Select Country

Selected Clear All

Name	Location Type

Cancel Back Skip to Review **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

Zoom Search for Applications Clear All Add New

> Custom Applications (Selected: 0 of 1)

▼ Predefined Applications (Selected: 1 of 53)

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

Cancel Back Skip to Review **Next 65**

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

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

Edit Client-based Access Rule: AcmeOneSecAccRuleContractors

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

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

General

Name*

Description

Tags

☒ Rule is Enabled

Operating Systems [Edit](#)

Operating System Versions Custom Selection

- 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
 - Windows Server 2019

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

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

Edit Client-based Access Rule: AcmeOneSecAccRuleContractors

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

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

General

Name*

Tags

☒ Rule is Enabled

Operating Systems [Edit](#)

Operating System Versions Custom Selection

- 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
 - Windows Server 2019

Configure Rule Order

How would you like to process rule "AcmeOneSecAccRuleContractors"?

☐ 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)

Place here

1. AcmeOneSecAccRuleContractors
2. Acc_Profile_Monitors
3. Acc_Profile_Ingenieros
4. TestSAML
5. UC1_windows
6. UC1_MAC

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 Security Service Edge configuration interface. The left sidebar contains a navigation menu with the following items: Configure, Deploy, Monitor, Analytics, Inventory, Users, and Settings. The 'Configure' item is selected. The main area displays the 'Real Time Protection' section, which includes a search bar and a table of rules. The table has columns for Applications, Users & Groups, Endpoint Posture, Source & Destination, Services, Schedule, Source, Geo Locations, and Security End. The table lists several rules, including 'All Users User Risk Bands All risk bands', 'All Users User Risk Bands All risk bands', 'All Users User Risk Bands All risk bands', 'All Users User Risk Bands All risk bands', and 'All Users User Risk Bands All risk bands'. The 'Profiles' link in the left sidebar is highlighted with a red circle and the number 4.

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

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

Filtering Profiles Publish (2)

Filtering Profiles **5** | URL Filtering | DNS Filtering **6** | File Filtering

URL Filtering: **DNS Filtering** **6**

DNS Filtering Profiles (3) Search by keyword or name **Filter** **+ Add** **7**

Profile Name	Deny List	Allow List	Query Based Actions	Reputation Based Action
			No Data	

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 **+**
Type a comma separated list of strings

Allow List
Choose which URLs to allow (whitelist).

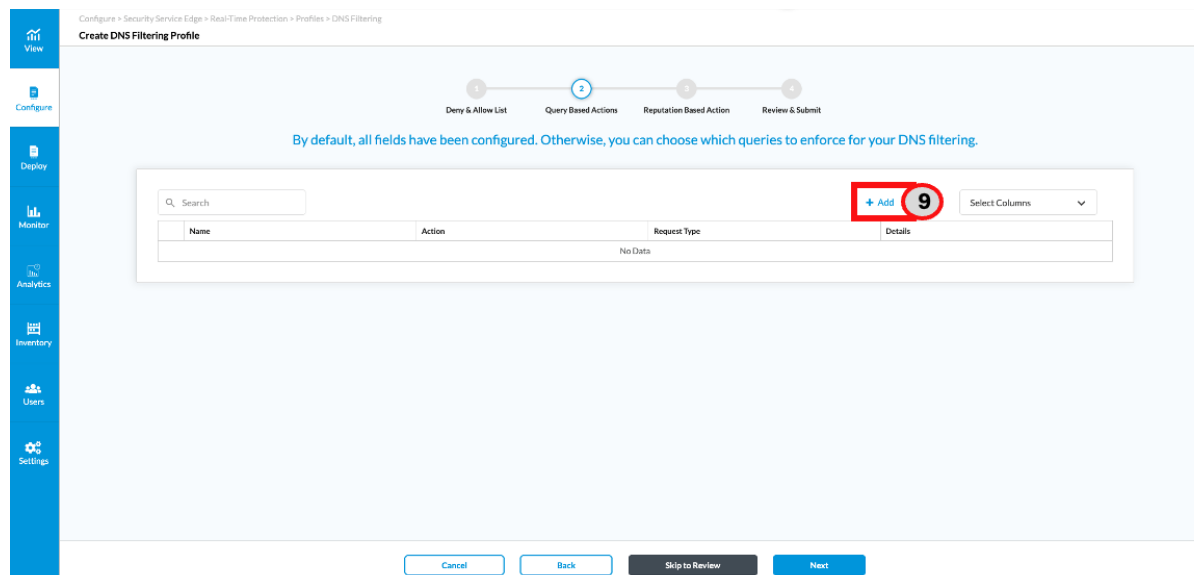
Patterns
Type a PCRE RegEx pattern **+**

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

☐ Enable Logging **+**

Next **8**

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



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

Create DNS Filtering Profile

1 Deny & Allow List 2 Query Based Actions 3 Reputation Based Action 4 Review & Submit

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

Search

+ Add 9 Select Columns

Name	Action	Request Type	Details
No Data			

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

View

Configure

Deploy

Monitor

Analytics

Inventory

Users

Settings

Q Search

Name

Number of additional records

-- Select --

Number of questions

-- Select --

Query Type

AAAA

Domain Name

*

Add Query Based Actions

Choose which action and configurations to apply for your query.

Name*

NoAAAA

Action

Reject

Request Type

Query

Cancel

Add

Cancel

Back

Skip to Review

Next

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

View

Configure

Deploy

Monitor

Analytics

Inventory

Users

Settings

General

Name *

DNSFiltering

Description

For description name

Tags

Press Enter to add

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

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 Publish (2)

Below are all the rules for your Internet Protection Policy.

Search: Implicit **18** Filter All Rule Types + Add Clone Reorder Delete Refresh Select Columns

Rule Name	Applications & URLs	Users & Groups	Endpoint Posture	Source & Destination	Services	Schedule	Source	Destination	Security Enforcement
<input type="checkbox"/> Implicit-Drop-Quic 18	All Applications	All Users User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Source & Destination	Services Implicit-QUIC-UDP-443	Not Available	All Geo locations are selected	All Geo locations are selected	Action
<input type="checkbox"/> Implicit-Allow-DNS 19	All Applications	All Users User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Source & Destination	Services domain	Not Available	All Geo locations are selected	All Geo locations are selected	Action
<input type="checkbox"/> 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	Source & Destination	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

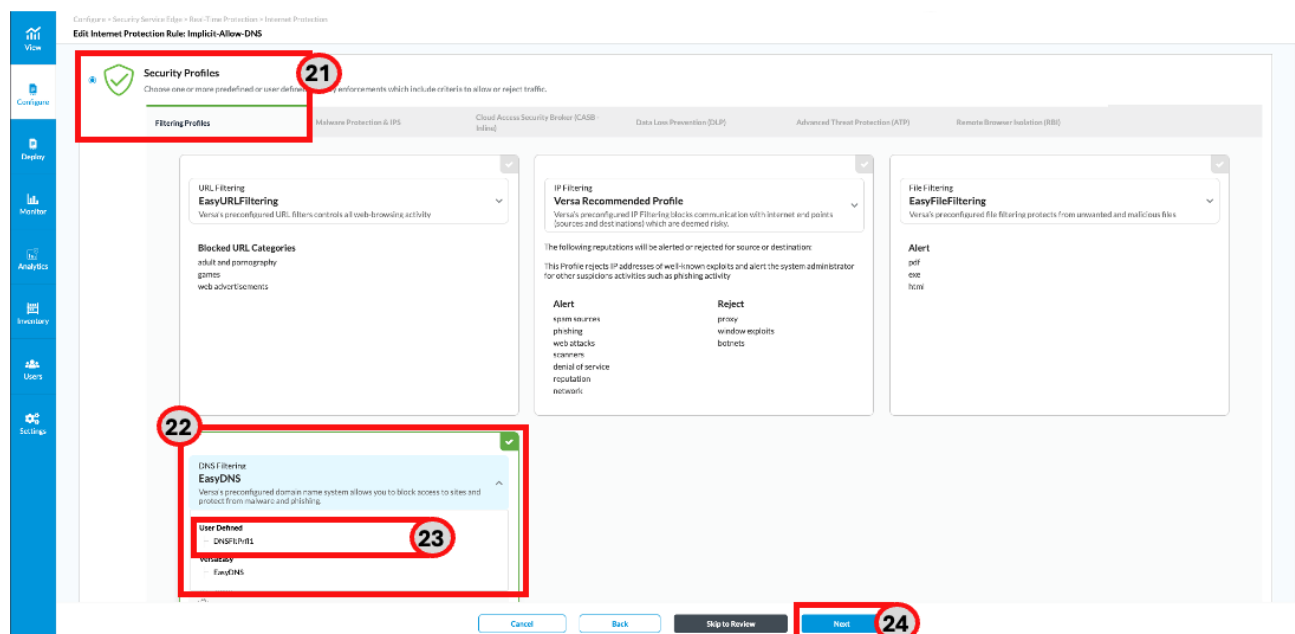
Security Enforcement [Edit](#) **20**

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 configuration interface. The left sidebar contains a navigation menu with icons for View, Configure, Deploy, Monitor, Analytics, Inventory, Users, and Settings. The 'Configure' icon is highlighted with a red circle and the number 1. The 'Security Service Edge' menu item is highlighted with a red circle and the number 2. The 'Real-Time Protection' sub-menu item is highlighted with a red circle and the number 3. The 'Profiles' sub-menu item is highlighted with a red circle and the number 4. The main content area displays a table of rules for Secure Client-based Access. The table has columns for Operating System Versions, Users & Groups, Endpoint Posture (EIP & Entity Risk Bands, Device Compliance Status), Traffic Action, VPN & Gateway Groups, and Status. The table lists several rules for Windows 10, Windows 10 Mobile, and Windows 11, all with a status of 'Enabled'.

Operating System Versions	Users & Groups	Endpoint Posture	Traffic Action	VPN & Gateway Groups	Status	
Windows 10 Windows 10 Mobile Windows 11	AuthProfile_SAMAL 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 Edgernet-BR-Enterprise Gateway Groups Default Gateways VCG-SA-GRU-01 VCG-SA-CGH-02	Enabled
Windows 10 Windows 10 Mobile Windows 11	AuthProfile_SAMAL 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 Edgernet-BR-Enterprise Gateway Groups Default Gateways VCG-SA-GRU-01 VCG-SA-CGH-02	Enabled
Windows 10 Windows 10 Mobile Windows 11	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 Edgernet-BR-Enterprise Gateway Groups Default Gateways VCG-SA-GRU-01 VCG-SA-CGH-02	Enabled
Windows 10 Windows 10 Mobile Windows 11	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 Edgernet-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 Publish (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** **Delete** **Refresh** **Select Columns** **▼**

Profile Name	Rules	Application	Action Request
No Data			

Click **+ Add**.

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

Create SaaS Tenant Control Profile

1 Application Rules 2 Review & Submit

Add Application Rules

Search **+ Add** **8** **Delete**

Name	Application	Type	Action Request	Values
No Data				

Cancel Back Skip to Review Next

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

Add Application Rule

Choose your configurations to enforce the rule

Name

Action Type
Choose which action to use for your application
☒ Insert ☐ Delete

Application

Select one or more headers for your rule

Header	Value
<input type="text" value="sec-Restrict-Tenant-Access-Policy"/>	<input type="text" value="acme-one.com"/>

☒ Delete Existing

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

Add Application Rules

1 Application Rules 2 Review & Submit

Search

Name	Application	Type	Action Request	Values
<input type="checkbox"/> AcmeOneMSOfc365	Microsoft-Office-365-Block-Consumer-Account	INSERT	sec-Restrict-Tenant-Access-Policy	acme-one.com

Go to page 1 * < Previous 1 Next >

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

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

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

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

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

Create SaaS Tenant Control Profile

1

2

Application Rules Review & Submit

Review your SaaS Tenant Control profile Configurations below

General

Name *

SaaSTrnCtrl_AcmeOne_MSOI

24

Description

Tags

Press Enter to add

Application Rules

Edit

Name	Application	Type	Action Request	Values
AcmeOneMSOfc365	Microsoft-O365-Block-Consumer-Account	INSERT	sec-Restrict-Tenant-Access-Policy	acme-one.com

Cancel

Back

Save

25

Step 6: Configure TLS Decryption

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

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

To maintain user privacy and comply with regulations:

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

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

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

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

Create a TLS Decryption Profile

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

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

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

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

Configure > Security Service Edge > TLS Decryption > Profiles

Create TLS Decryption Profile

1 Profile Type 2 Certificate Setup 3 Inspection Options 4 Decryption Options 5 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 OSCP
 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: 5

Verify: Server and Client

Server Certificate Actions

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

When the certificate expires, do the following:

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:
Block

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

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:
Alert
Minimum Supported RSA Key Length: 1024 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:
Alert

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

Cancel Back Skip to Review Next

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, or TLS, is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet. A primary use case of TLS is encrypting the communication between web applications and servers, such as web browsers loading a website. TLS can also be used to encrypt other communications such as email, messaging, and voice over IP (VoIP). In this article we will focus on the role of TLS in web application security.

[More Information](#)

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.

TLS 1.0 TLS 1.1 TLS 1.2 TLS 1.3

Key Exchange Algorithms

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

Advanced

Algorithms

Select which encryption and authentication algorithms to use.

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

[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.

- ☐ TLS-AES-128-GCM-SHA256
- ☐ TLS-CHACHA20-POLY1305-SHA256
- ☒ TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256
- ☒ TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA
- ☒ TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384
- ☒ TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256
- ☒ TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA
- ☒ TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384
- ☒ TLS-RSA-WITH-AES-128-CBC-SHA256
- ☒ TLS-RSA-WITH-AES-256-CBC-SHA
- ☒ TLS-RSA-WITH-AES-256-GCM-SHA384
- ☐ TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256
- ☐ TLS-RSA-WITH-SEED-CBC-SHA
- ☐ TLS-AES-256-GCM-SHA384
- ☒ TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA
- ☒ TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256
- ☒ TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384
- ☒ TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA
- ☒ TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256
- ☒ TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384
- ☒ TLS-RSA-WITH-AES-128-CBC-SHA
- ☒ TLS-RSA-WITH-AES-128-GCM-SHA256
- ☒ TLS-RSA-WITH-AES-256-CBC-SHA256
- ☐ TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256
- ☐ TLS-RSA-WITH-CAMELLIA-256-CBC-SHA

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

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

Configure > Security Service Edge > TLS Decryption > Profiles

Create TLS Decryption Profile

1 Certificate Setup 2 Inspection Options 3 Decryption Options 4 Review & Validate

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
Description

Tags

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

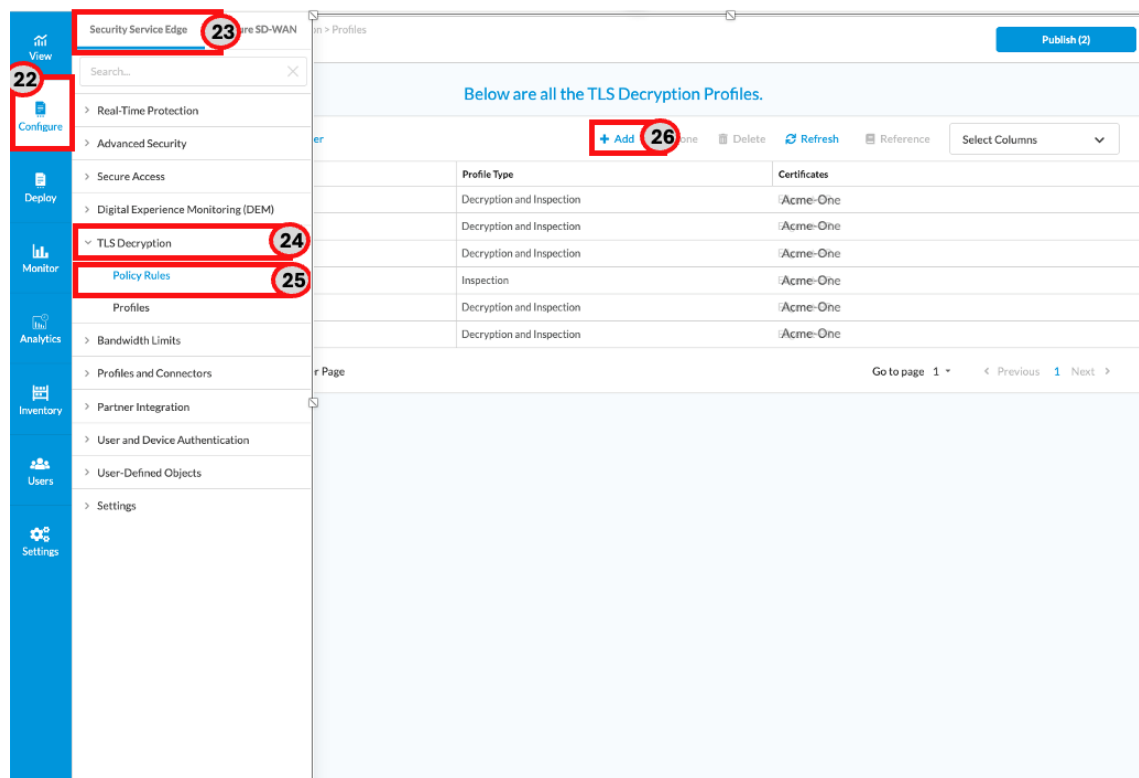
 21

Create TLS Decryption Policy Rules

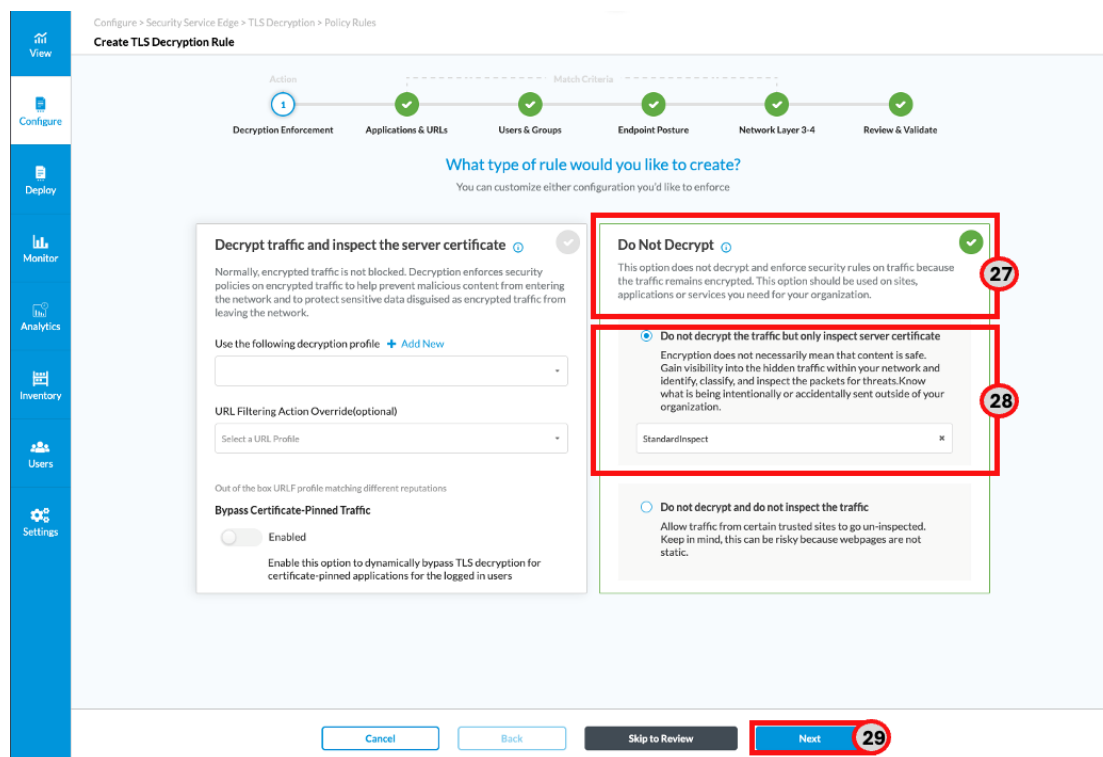
As specified in the use case, two decryption policy rules are needed. The first rule maintains privacy for certain types of regulated traffic, while the second decrypts all remaining traffic.

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 Decryption Enforcement 2 Applications & URLs 3 Users & Groups 4 Endpoint Posture 5 Network Layer 3-4 6 Review & Validate

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

Applications **URL Categories & Reputations** 30

URL Categories & Reputations

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 Users & Groups configuration.

Configure > Security Service Edge > TLS Decryption > Policy Rules

Create TLS Decryption Rule

Action

1 Decryption Enforcement 2 Applications & URLs 3 Users & Groups 4 Endpoint Posture 5 Network Layer 3-4 6 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 2 Applications & URLs 3 Users & Groups 4 **Endpoint Posture** 5 Network Layer 3-4 6 Review & Validate

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

[Customize](#)

Entity Risk Bands

✓ All risk bands

[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 2 Applications & URLs 3 Users & Groups 4 Endpoint Posture 5 **Network Layer 3-4** 6 Review & Validate

Match Criteria

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

[Customize](#)

Source & Destination (Layer 3)

✓ Destination Zone

Internet

[Customize](#)

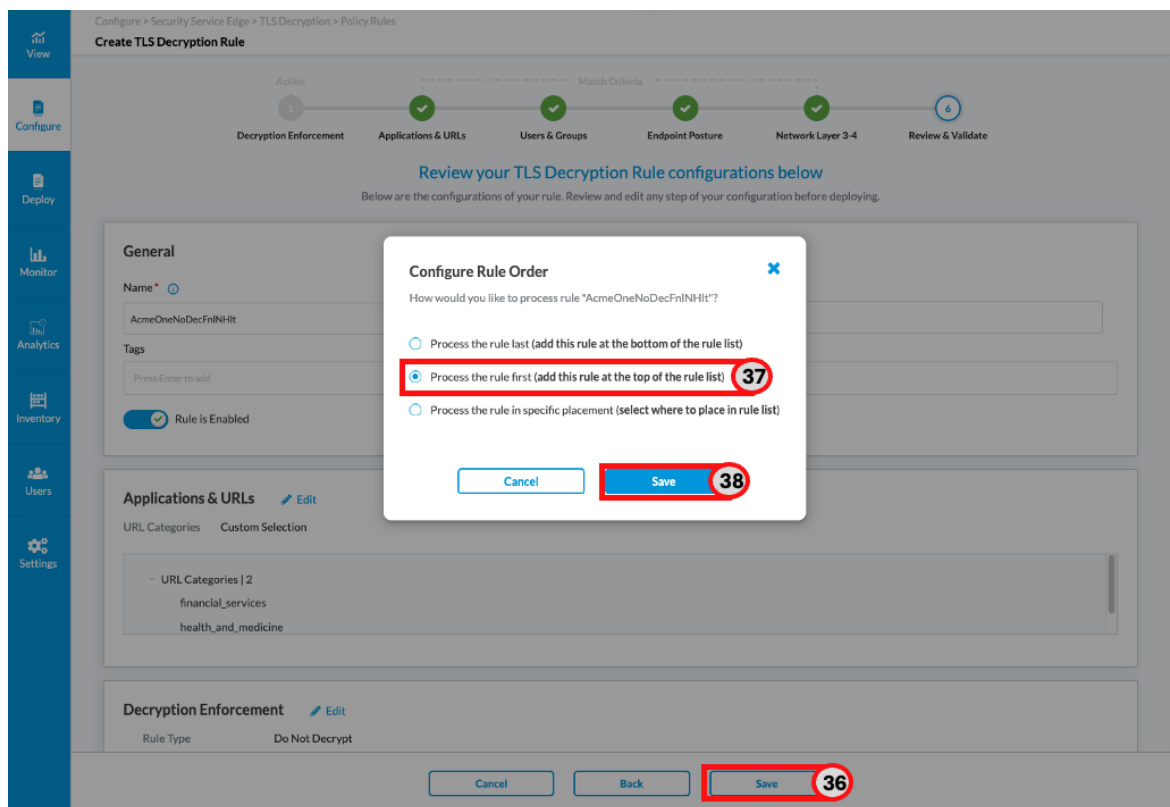
Schedule

✓ None Selected

[Customize](#)

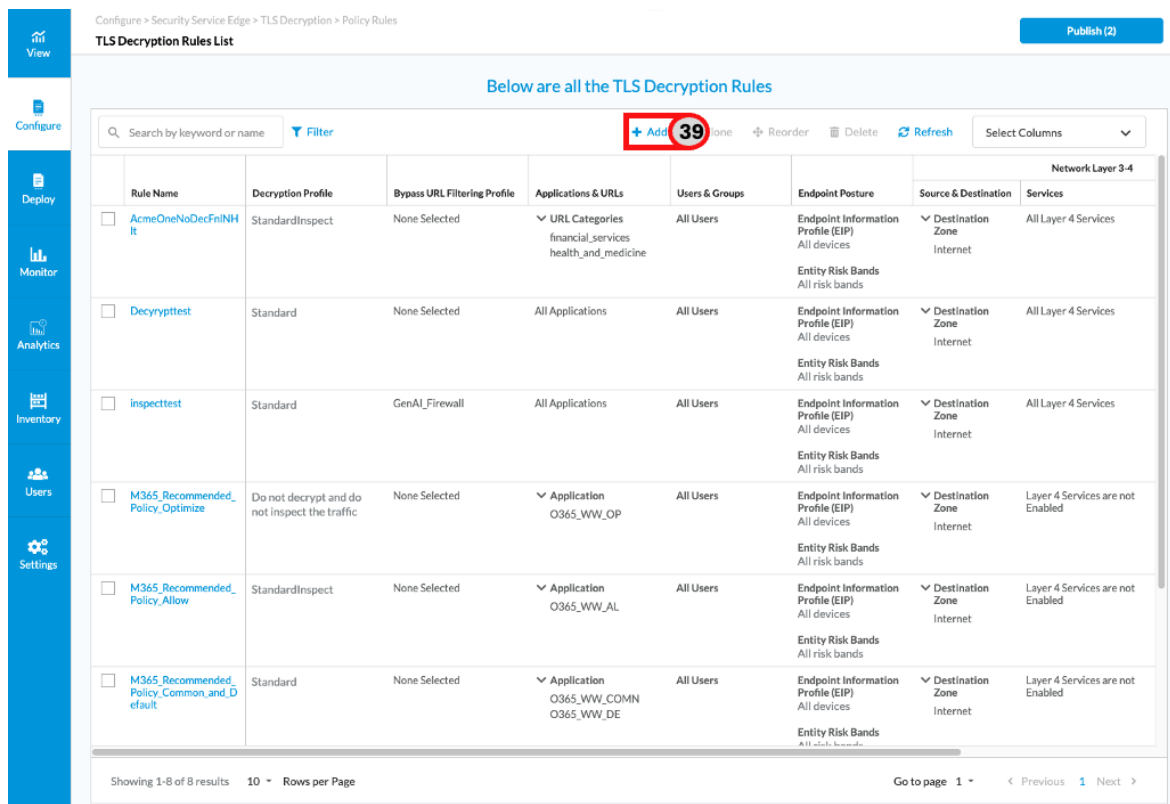
[Cancel](#) [Back](#) [Skip to Review](#) [Next](#) **35**

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



TLS Decryption Policy Rule 2

To create the second rule allowing decryption of all other traffic, click [Add](#).



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

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

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

Step 7: Configure The File Filtering Profile

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

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

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

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

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

The screenshot shows the Versa Security Service Edge configuration interface. The left sidebar contains a navigation menu with the following items: **Configure** (highlighted with a red box and number 1), **Deploy**, **Monitor**, **Analytics**, **Inventory**, **Users**, and **Settings**. Under the **Configure** menu, the following sub-items are listed: **Security Service Edge** (highlighted with a red box and number 2), **Secure SD-WAN**, **Policy Rules**, **Real-Time Protection** (highlighted with a red box and number 3), **Internet Protection**, **Private App Protection**, **Profiles** (highlighted with a red box and number 4), **Safe Search**, **Network Obfuscation**, **Settings**, **Advanced Security**, **Secure Access**, **Digital Experience Monitoring (DEM)**, **TLS Decryption**, **Policy Rules**, **Profiles**, **Bandwidth Limits**, **Profiles and Connectors**, **Partner Integration**, **User and Device Authentication**, **User-Defined Objects**, and **Settings**. The main content area displays a table titled "Below are all the TLS Decryption Rules" with columns: **Bypass URL Filtering Profile**, **Applications & URLs**, **Users & Groups**, **Endpoint Posture**, **Source & Destination**, and **Services**. The table contains several rows of data, including rules for applications like O365_WWW_OP, O365_WWW_AL, O365_WWW_COMN, O365_WWW_DE, and URL Categories like financial_services and health_and_medicine. The bottom of the interface shows a pagination bar with "Go to page 1" and navigation arrows.

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 Publish (2)

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

Search by keyword or name Filter + Add Delete Refresh Reference Select Columns

Profile Name	Deny List	Allow List	Reputation Based Action	Number Of File Based A...	Protocols	Action
<input type="checkbox"/> 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).

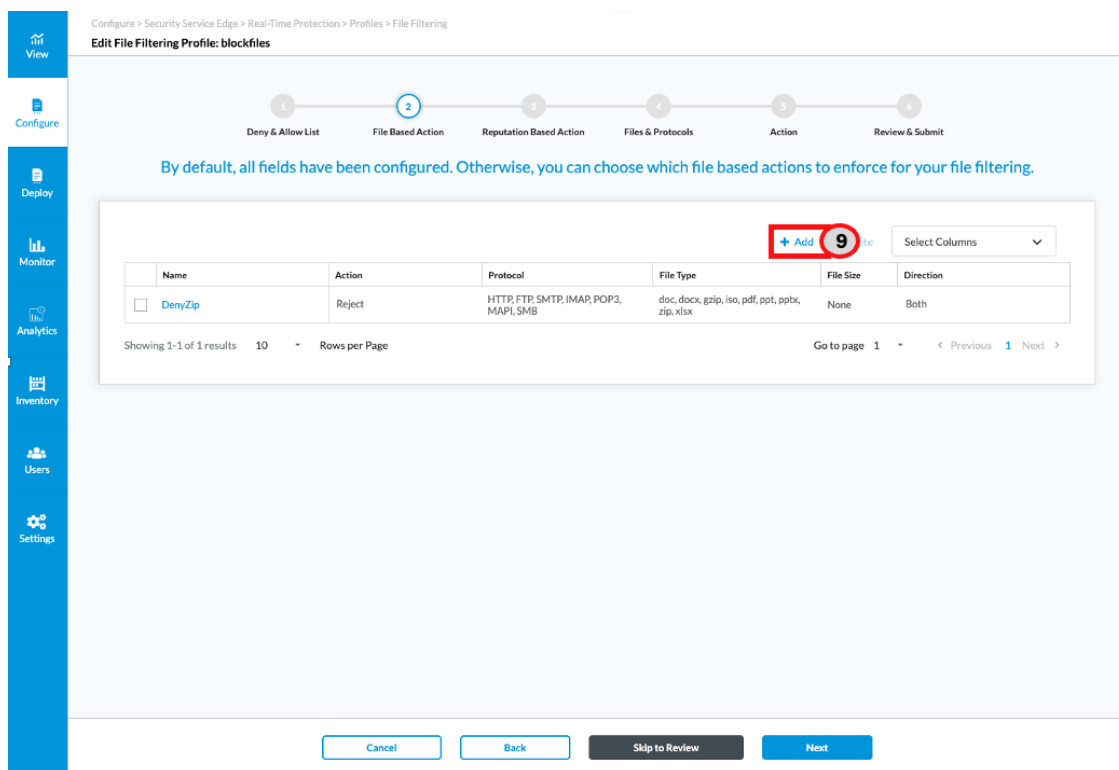
SHA256
Specify A SHA-256 hash value +

SHA384
Specify A SHA-384 hash value +

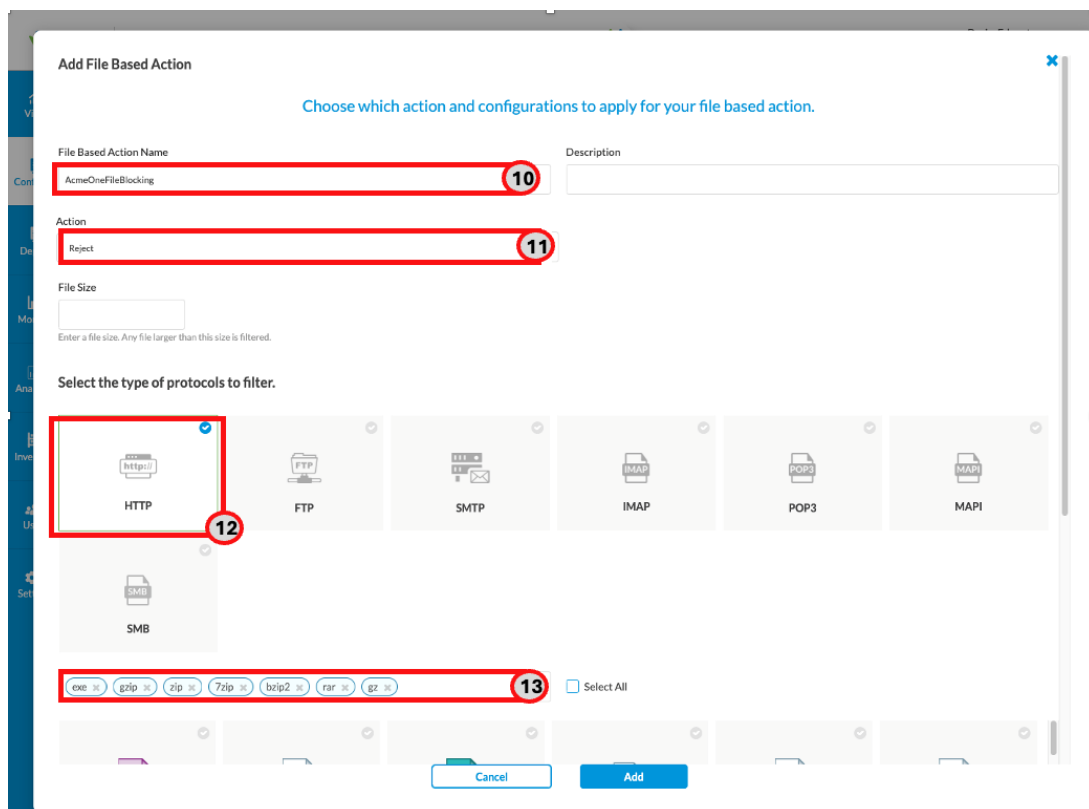
☒ Enable Logging

Cancel Back Skip to Review **Next** 8

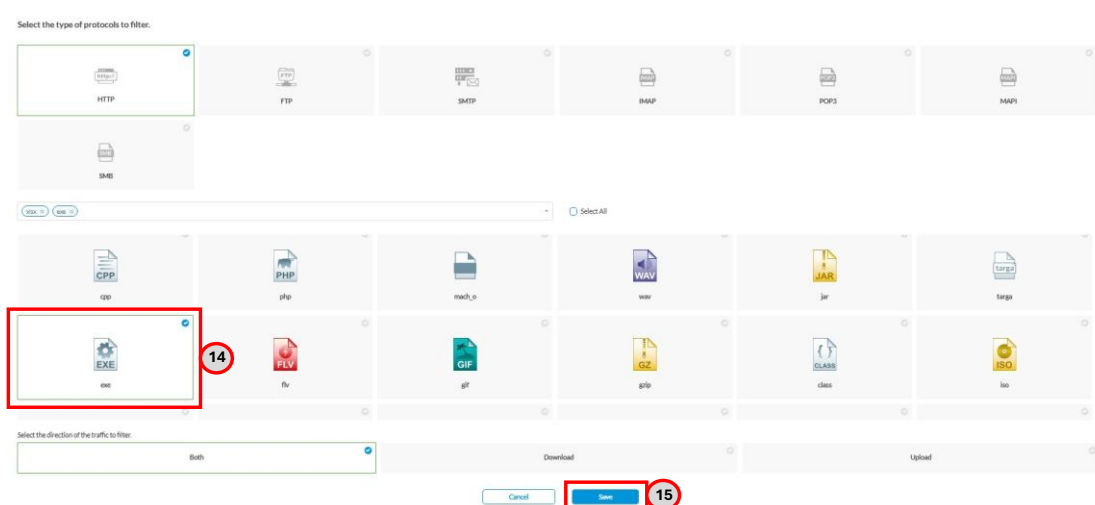
Click **Add** to create a File-based Action based on the file types you want to prevent users from downloading.



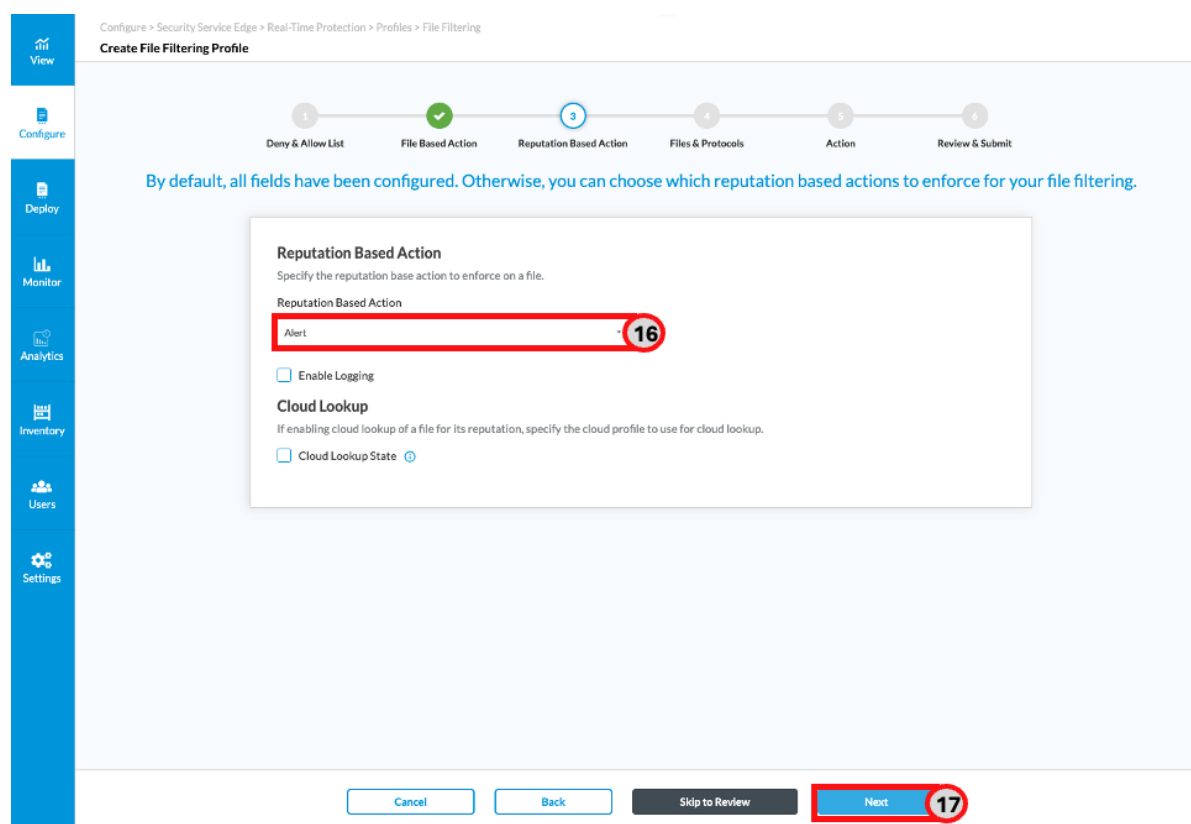
Assign a descriptive **Name**, choose the **Reject** action for the match criteria, select **HTTP** as the protocol to monitor and add the exe, zip, gzip, 7zip, bzip2, rar and exe file types to match.



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



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



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

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

Create File Filtering Profile

View
Configure
Deploy
Monitor
Analytics
Inventory
Users
Settings

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.

HTTP

FTP

SMTP

IMAP

POP3

MAPI

SMB

Cancel
Back
Skip to Review
Next 18

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

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

Review your File Filtering configuration below

General

Name* 19 AcmeOneFiltrngPrft Description or description name

Tags Press Enter to add

☐ Logging is Disabled

Deny & Allow List Edit

Deny List	Reject
Logging	Disabled
Allow List	-
Logging	Disabled

File Based Action Edit

Cancel Back **Save** 20

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:

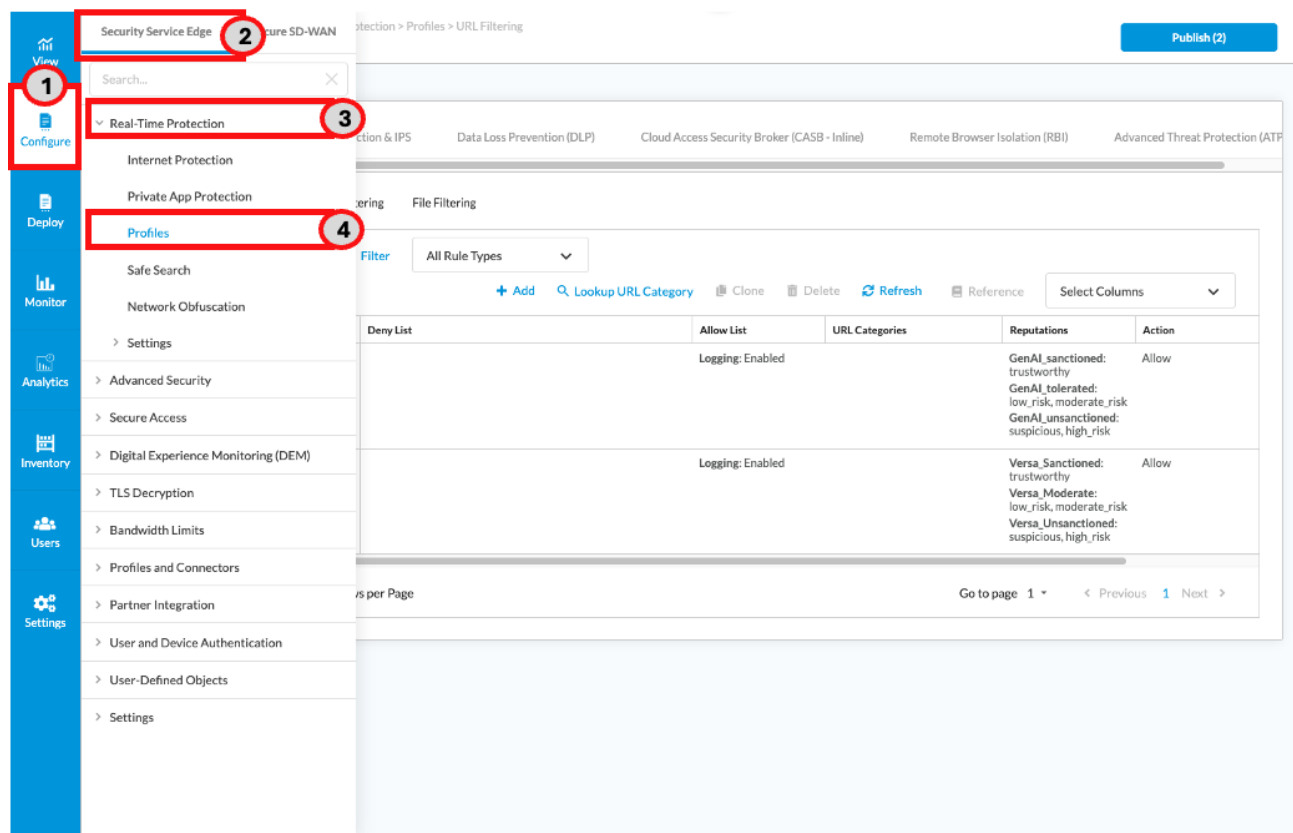
- IT Users: Apply the Versa Recommended URL Filtering Profile.
 - This profile is preconfigured by Versa with a balanced set of controls designed to protect against common threats and enforce corporate-appropriate browsing.
 - It covers high-risk categories such as malware, phishing, botnets, and anonymizers, 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 configuration interface. The left sidebar has a 'Configure' button highlighted with a red circle and the number 1. The 'Security Service Edge' menu item is highlighted with a red circle and the number 2. The 'Real-Time Protection' menu item is highlighted with a red circle and the number 3. The 'Profiles' menu item is highlighted with a red circle and the number 4. The main panel shows the 'URL Filtering' configuration page. It has a search bar, a 'Filter' dropdown, and a table of rules. The table has columns: Deny List, Allow List, URL Categories, Reputations, and Action. The first rule has 'Logging: Enabled' in the Deny List, 'GenAI sanctioned: trustworthy' in the Allow List, 'GenAI tolerated: low_risk, moderate_risk' in the URL Categories, 'GenAI_unsanctioned: suspicious, high_risk' in the Reputations, and 'Allow' in the Action. The second rule has 'Logging: Enabled' in the Deny List, 'Versa_Sanctioned: trustworthy' in the Allow List, 'Versa_Moderate: low_risk, moderate_risk' in the URL Categories, 'Versa_Unsanctioned: suspicious, high_risk' in the Reputations, and 'Allow' in the Action.

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

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

Filtering Profiles Publish (2)

Filtering Profiles 5

URL Filtering 6 Filtering IP Filtering File Filtering

Search by keyword or name Filter All Rule Types

7 + Add Lookup URL Category Clone Delete Refresh Reference Select Columns

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 + Add New

Patterns +
Type a PCRE RegEx pattern

Strings +
Type a comma separated list of strings

Allow List
Choose which URLs to allow (whitelist).

Patterns +
Type a PCRE RegEx pattern

Strings +
Type a comma separated list of strings

☐ Enable Logging +

Cancel Back Skip to Review **Next 8**

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

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

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

Step 9: Configure Internet Protection Policy Rules

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

Internet Protection Policy Rule for Contractor Users

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

Parameter	Description
Rule Name	Name to identify the Internet Protection Rule
Profile Type	Type of profile to enforce a specific rule (File Filtering and URL Filtering Profile)
Profile Name	Name of the profile to enforce a specific rule (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

Security Service Edge > Internet Protection

Below are all the rules for your Internet Protection Policy.

Applications & URLs	Users & Groups	Endpoint Posture	Source & Destination	Services	Schedule	Source
Applications	All Users User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Destination Zone Internet	Layer 4 Services are not Enabled Implicit-QUIC-UDP-443	Not Available	All Geo locations
Application Group Office365-Apps Google-Apps	SAMALGW1 User Groups Ingenieros Usuarios User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Destination Zone Internet	Layer 4 Services are not Enabled	Not Available	All Geo locations
URL Categories TestURLs	SAMALGW1 User Groups Usuarios Ingenieros User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Destination Zone Internet	Layer 4 Services are not Enabled	Not Available	All Geo locations
URL Categories adult_and_pornography	All Users User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Destination Zone Internet	All Layer 4 Services	Not Available	All Geo locations
Applications	UsersLocalDB Users sselauser5@gmail.com User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Destination Zone Internet	All Layer 4 Services	Not Available	All Geo locations
Applications	UsersLocalDB	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Destination Zone Internet	Services	Not Available	All Geo locations

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

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

Cancel Back Skip to Review **Next**

Click **Customize** under Users & Groups.

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

Create Internet Protection Rule

Applications & URLs **Users & Groups** Match Criteria GEO Locations Network Layer 3-4 Action 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

- ☒ All Users
- Customize** **7**

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 **Contractors**. Click **Next**.

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

Create Internet Protection Rule

Applications & URLs **Users & Groups** Match Criteria GEO Locations Network Layer 3-4 Action 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** **8** ☐ Known Users ☐ Unknown Users

Enable Internet Protection for the following matched users or user groups

AuthProfile: SAMAL **9**

User Groups **10**

[Contractors](#) Search for User Groups

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

[Cancel](#) [Back](#) [Skip to Review](#) [Next](#) **12**

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

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

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

View

Configure

Deploy

Monitor

Analytics

Inventory

Users

Settings

1

Applications & URLs

2

Users & Groups

3

Endpoint Posture

4

GEO Locations

5

Network Layer 3-4

6

Security Enforcement

7

Review & Deploy

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*

AcmeOneCttrsDenyUrls

Description

for description name

Tags

Press Enter to add

Rule is Enabled

Applications & URLs

Edit

Users & Groups

Edit

Users & Groups

AuthProfile_SAMAL

Users Device Groups

All Device Groups

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.

Search by keyword or name Filter 22 + Add Clone Reorder Delete Refresh Select Columns

Rule Name	Applications & URLs	Users & Groups	Endpoint Posture	Source & Destination	Services	Schedule	Source
<input type="checkbox"/> 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
<input type="checkbox"/> AcmeOneCttrsDenyUrls	URL Categories adult_and_pornography sports gambling More Details	AuthProfile_SAMAL User Groups Contractors User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Destination Zone Internet	All Layer 4 Services	Not Available	All Geo locations
<input type="checkbox"/> AcmeOneITVersaURLRcmd	All Applications	AuthProfile_SAMAL User Groups IT User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Destination Zone Internet	All Layer 4 Services	Not Available	All Geo locations
<input type="checkbox"/> AcmeOneAllowAllEnforced	All Applications	AuthProfile_SAMAL User Groups IT Contractors User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Destination Zone Internet	All Layer 4 Services	Not Available	All Geo locations
<input type="checkbox"/> 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 Entity Risk Bands All risk bands	Destination Zone Internet	Layer 4 Services are not Enabled	Not Available	All Geo locations

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

1 Applications & URLs 2 Users & Groups 3 Match Criteria 4 GEO Locations 5 Network Layer 3-4 6 Action 7 Security Enforcement 8 Review & Deploy

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

Application Group Applications Application Category

Search for Application Group + Add New Grid List

> 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
LinkedIn-Apps	Microsoft-Apps	Oracle-Apps	Salesforce-Apps	SAP-Apps	

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 | **Users & Groups** | Endpoint Posture | GEO Locations | Network Layer 3-4 | Security Enforcement | 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

✓ 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 | **Users & Groups** | Endpoint Posture | GEO Locations | Network Layer 3-4 | Security Enforcement | 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.

← Back

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"/>	IT 28	
<input type="checkbox"/>	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

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

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

[Customize](#)

Destination Geo Location

- All Destination Geo locations are selected

[Customize](#)

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

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

[Customize](#)

Source & Destination (Layer 3)

☒ Destination Zone

Internet

[Customize](#)

Schedule

☒ None Selected

[Customize](#)

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
Drop all traffic that matches the rule

Reject
Drop the session and send a TCP reset (RST) or, for UDP, an ICMP port unreachable message

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

Filtering Profiles 34

- URL Filtering** 35
Versa's preconfigured URL filters controls all web-browsing activity.
Blocked URL Categories
adult and pornography
games
web advertisements
- IP Filtering** 36
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.
Alert
spam sources
phishing
web attacks
scanners
Reject
proxy
window exploits
botnets
- File Filtering** 37
blockfiles
Deny & Allow List
Deny Reject List
Allow List
Reputation Based Action
Action Allow
Cloud Disabled
Lookup

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

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

Below.

for deploying.

General

Name* 38

AcmeOneITVersaURLRcmd

Tags

Press Enter to add

☒ Rule is Enabled

Applications & URLs Edit

✓ All Applications

Users & Groups Edit

Users & Groups AuthProfile_SAMAL

User Risk Bands All Risk Bands

Users Device Groups All Device Groups

User Group | 1

Name	Description
IT	-

Configure Rule Order

How would you like to process rule "AcmeOneITVersaURLRcmd"?

☐ 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) 40

1. Implicit_Drop_Quic
2. Implicit-Allow-DNS
3. AcmeOneITVersaURLRcmd 41
4. Implicit_Deny_All

Place here

Cancel Move 42

Cancel Back Save 39

Appendix A – Authentication Methods Configuration

LDAP Active-Directory

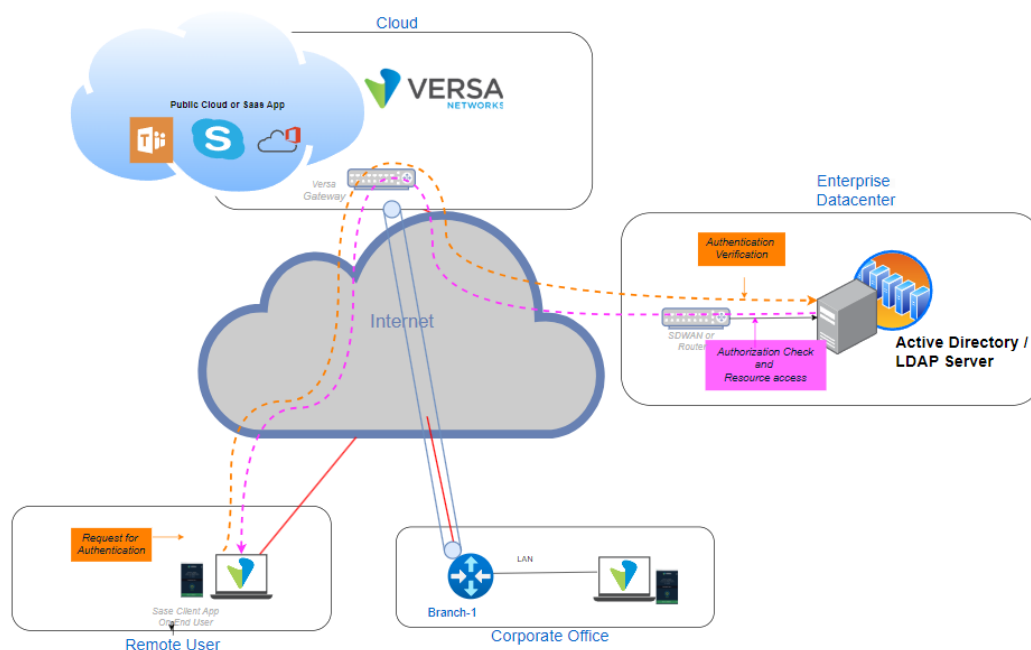
LDAP is a client-server protocol that enables network devices to access directory services storing attribute-based information, allowing for user authentication through querying a directory server. The SSE gateway queries the LDAP server to validate the user, granting or denying access based on the authentication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

Scenario

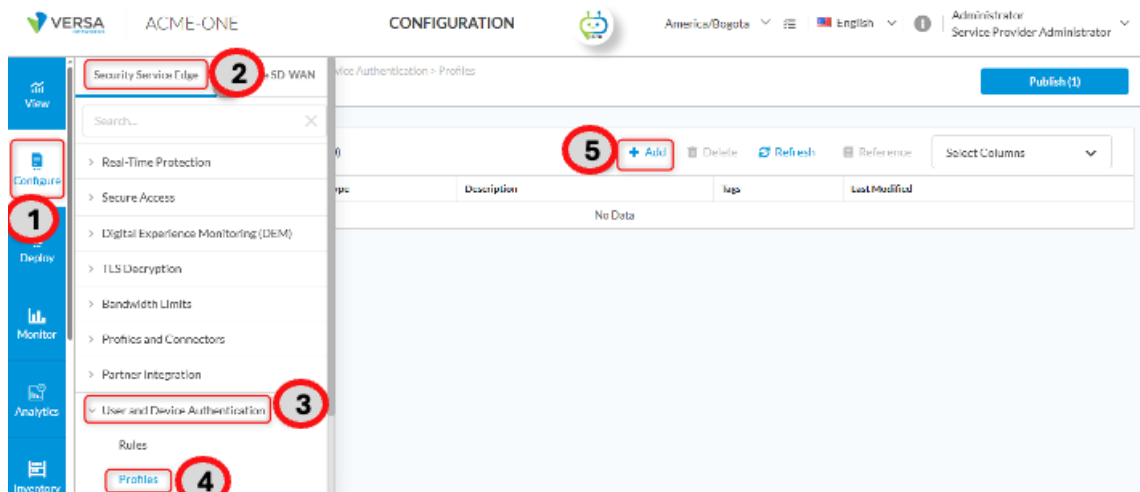
In most enterprise environments, user authentication is centralized through AD/LDAP servers in the data centre. In cases of VSPA or VISA, users securely connect to the SSE gateways using the Versa SASE Client from remote locations, branches, or corporate offices. Authentication requests from the SASE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

Upon successful authentication, users are granted secure access to resources hosted within data centres and to SaaS/cloud applications such as Microsoft Teams, Skype, and Office 365.

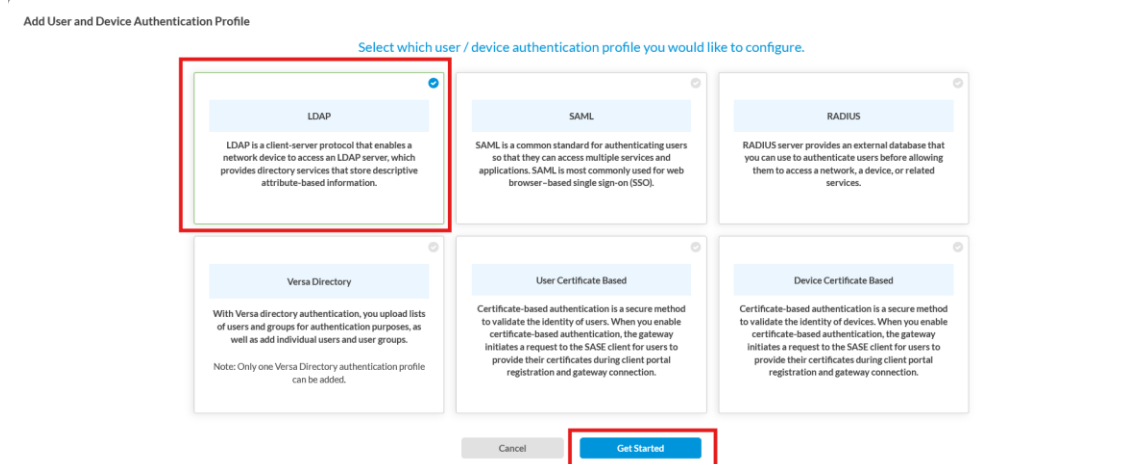
This configuration ensures consistent, identity-based access for both remote and on-premises users, thereby facilitating streamlined policy enforcement based on identity enforcement.



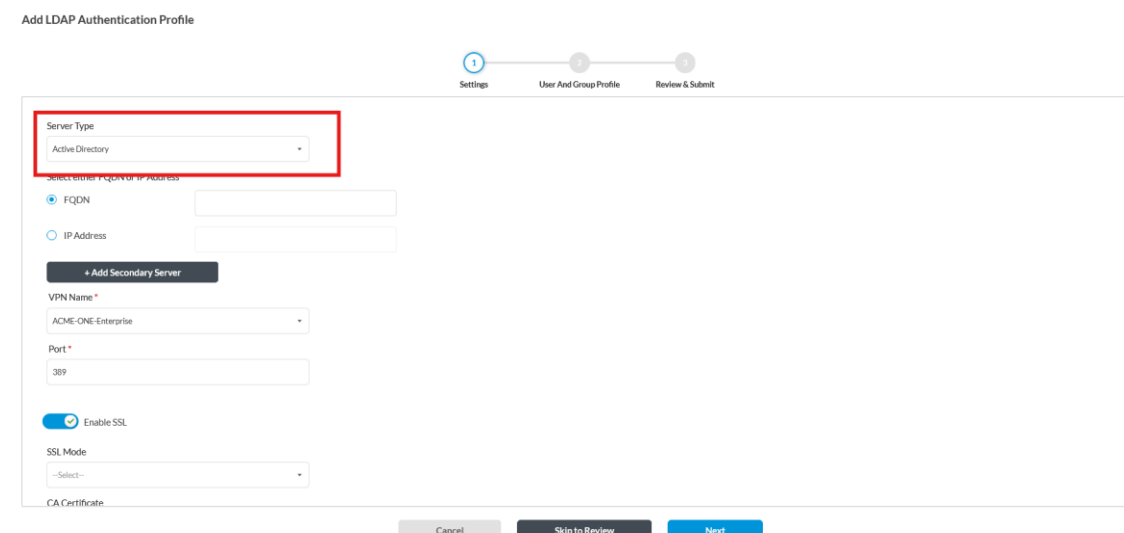
Navigate to User and Device Authentication Configuration Go to: Configure (1) > Security Service Edge (2) > User and Device Authentication (3) > Profiles (4) then "+ Add" (5)



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



From the Server Type dropdown, select Active Directory



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

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

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

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

Next, complete the required fields:

LDAP Object and User Attributes

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

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

click **Next** to proceed.

Add LDAP Authentication Profile



Group Object Class *

Group Name *

Group Member *

User Object Class *

User Name *

Refresh Interval (seconds)

Password Last Set

Password Max Age

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

Settings

User And Group Profile

Review & Submit

General

AD_Server_Acme_One

Description

Tags

Settings

Server Type

active-directory

FQDN or IP Address

10.163.306.33

VPN Name

ACME-ONE-Enterprise

Port

389

SSL Status

Disabled

SSL Mode

CA Certificate

File Name

Issued To

Issued By

Validity

Bind DN

Bind Password

Bind Timeout (sec)

30

Base DN

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

Domain Name

acme-one.com

Base Domain

Search Timeout (sec)

30

Cache Expiry Time (mins)

10

Concurrent Logins

3

Cancel

Back

Save

Then Save.

Add LDAP Authentication Profile

Settings

User And Group Profile

Review & Submit

FQDN or IP Address

10.163.306.33

VPN Name

ACME-ONE-Enterprise

Port

389

SSL Status

Disabled

SSL Mode

CA Certificate

File Name

Issued To

Issued By

Validity

Bind DN

Bind Password

Bind Timeout (sec)

30

Base DN

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

Domain Name

acme-one.com

Base Domain

Search Timeout (sec)

30

Cache Expiry Time (mins)

10

Concurrent Logins

3

User and Group Profile

Group Object Class

group

Group Name

name

Group Member

membersOf

User Object Class

user

User Name

userPrincipalName

Refresh Interval (seconds)

21600

Password Last Set

pwdLastSet

Password Max Age

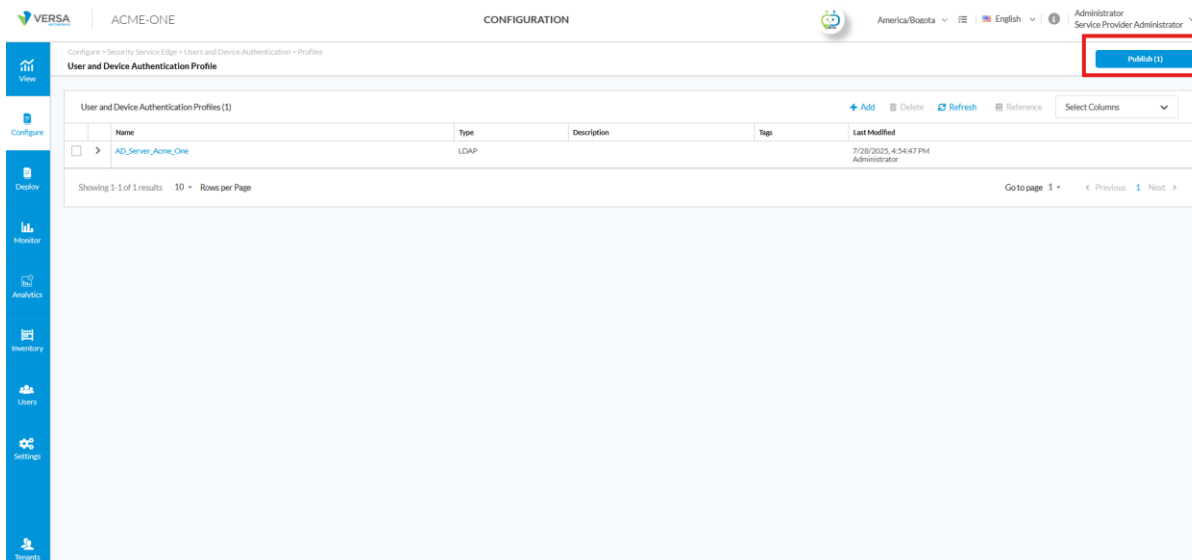
maxPwdAge

Cancel

Back

Save

Go to Publish



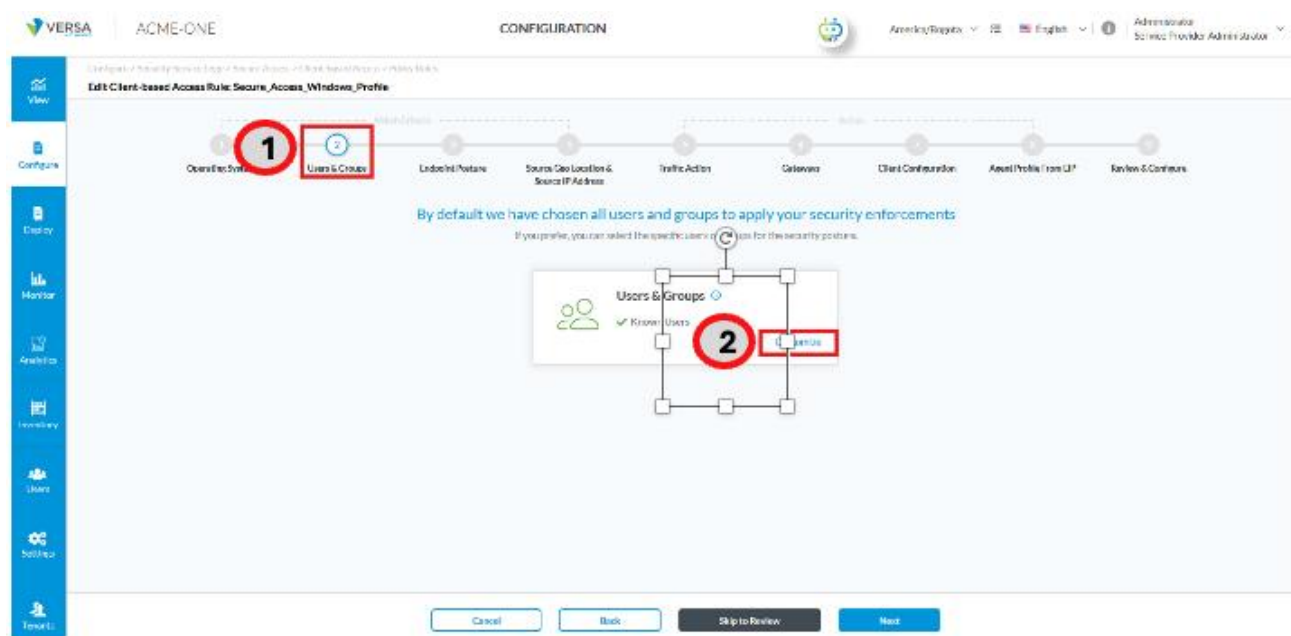
After creating and Publishing the Authentication Profile, you must apply them to the Secure Access Client policy to enforce authentication and apply the corresponding security policies.

Navigate to:

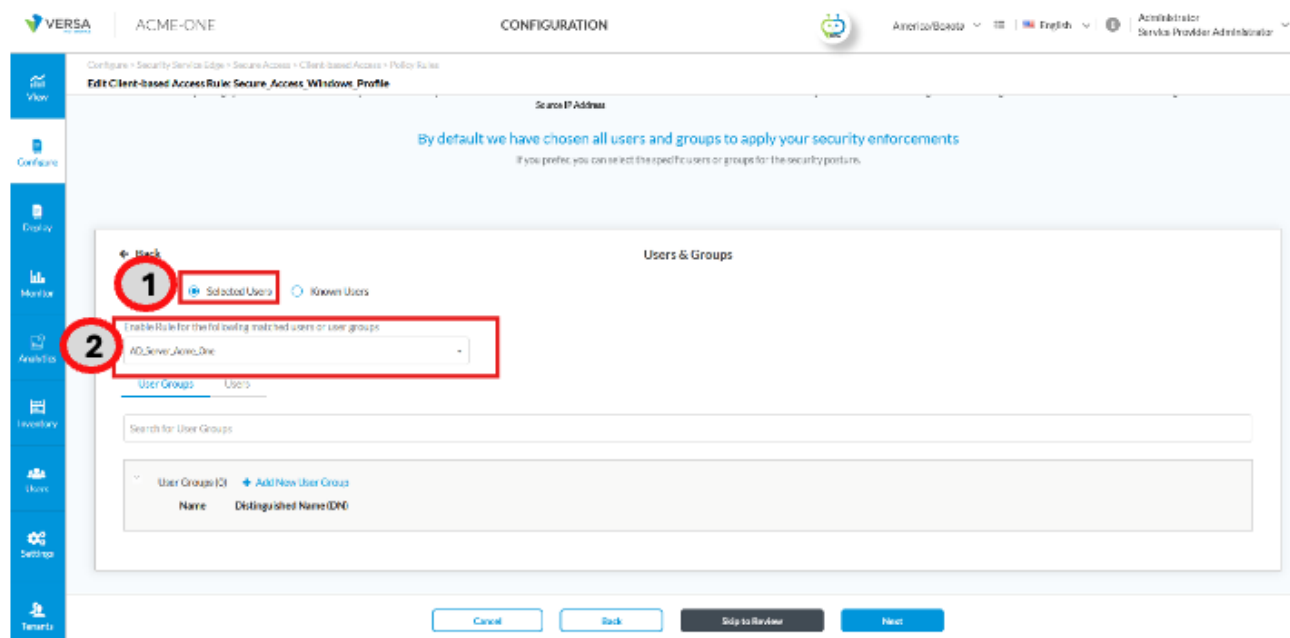
Configure > Security Service Edge > Secure Access > Client-based Access > Rules.

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

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

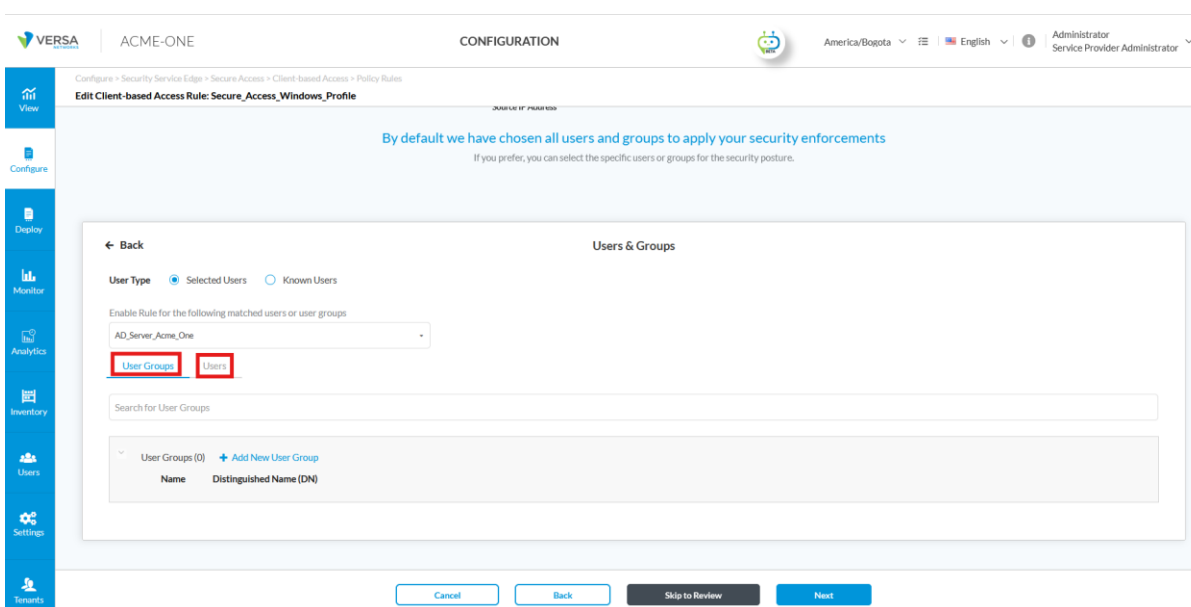


In the **Users & Groups** customization panel, select **Selected Users** as the user type. Then, under **Enable Rule for the following matched users or user groups**, choose the appropriate authentication profile (Example., AD_Server_Acme_One). This allows the policy to enforce access control based on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



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

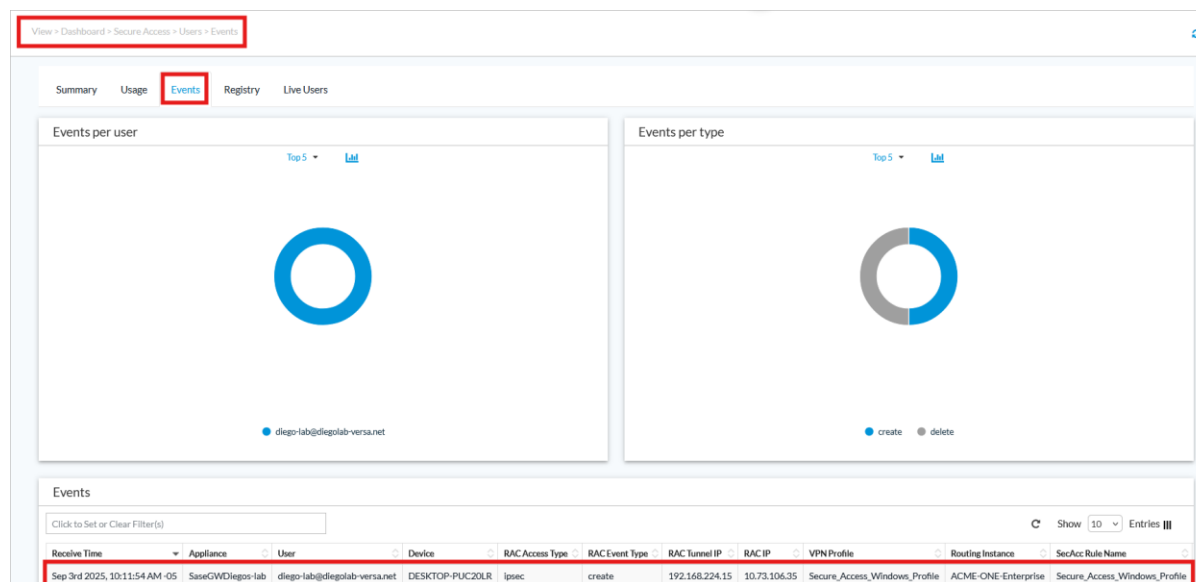
Use the **User Groups** or **Users** tabs to select the desired entries.



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

VERIFICATION

When a user connects to the Gateway and LDAP/AD authentication is enabled, the Secure Access Gateway forwards the authentication request to the configured LDAP server profile. The user credentials are validated against Active Directory, and upon success, group or role attributes are retrieved to enforce access policies. Authentication events can be verified in Concerto under **View > Dashboard > Secure Access > Users > Event**, where successful and failed attempts are logged with details such as username, tunnel IP, and applied profile.



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

Receive Time	Appliance	Auth Profile	Method	Status	Status Message	Time Taken	User	Source Address	Destination Address	Source Port	Destination Port
Sep 3rd 2025, 10:10:17 AM -05	SaseGWDiegios-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	SaseGWDiegios-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

Summary Services Networking System Tools

Secure Access

Portal

ID	Tenant	Action	Response Code	Username
183	ACME-ONE	register	403	diego-lab@diegolab-versa.net
182	ACME-ONE	elip+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

Summary Services Networking System Tools

Secure Access

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
IP ADDRESS  NAME                               STATUS  SESSION  TO    EXPIRATION
-----
192.168.224.15 diego-lab@diegolab-versa.net Live    262     60    inactivity

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

Microsoft Entra ID

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

Scenario

The same scenario described above also applies when using Entra ID as the Identity Provider. Because it is a cloud-

based IdP, Entra ID can seamlessly integrate with Versa SASE via SAML, validating user identities and issuing assertions that grant access to both cloud services and enterprise applications under consistent policy enforcement.

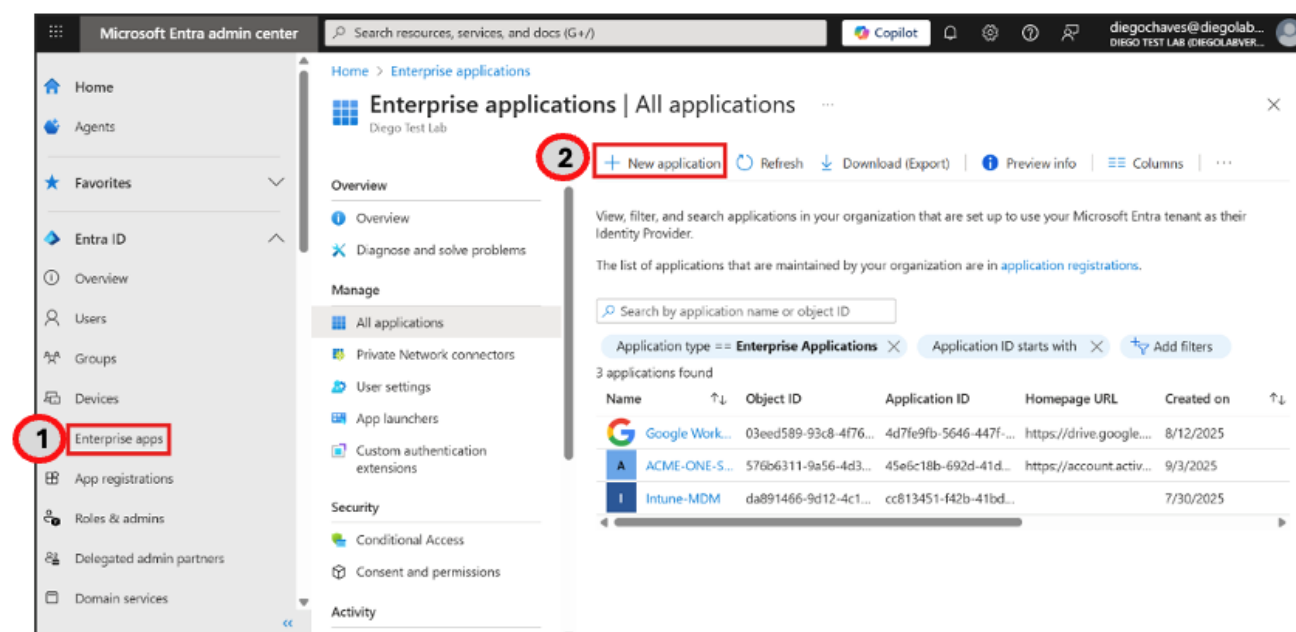
Entra ID Configuration

Create an Enterprise Application in the Entra ID portal.

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

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

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



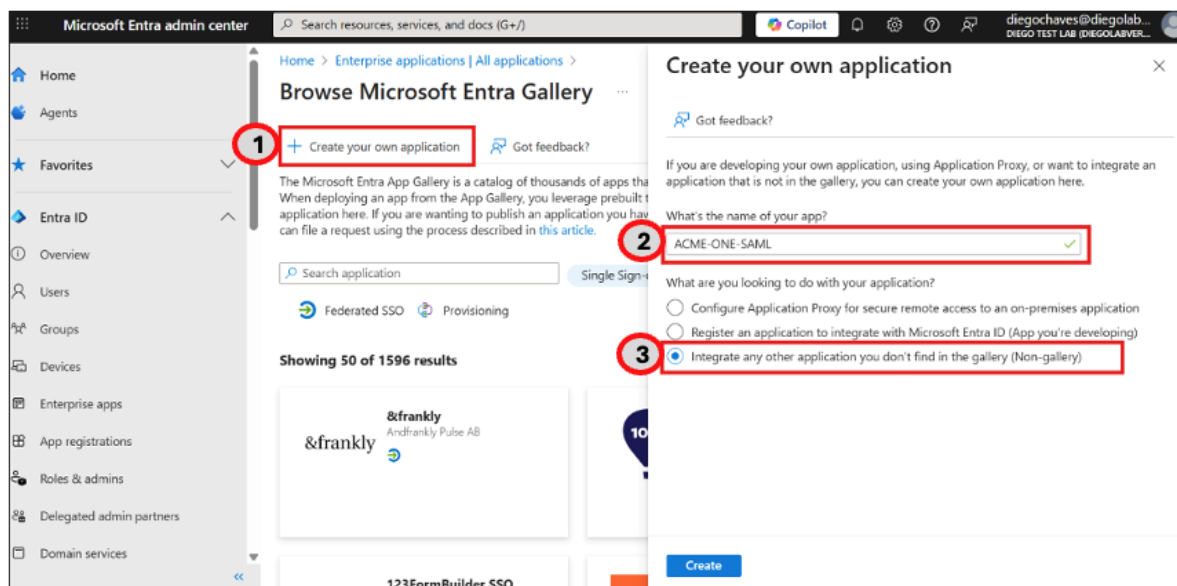
2. Select **Create a new application**

Click + **Create your own application**.

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

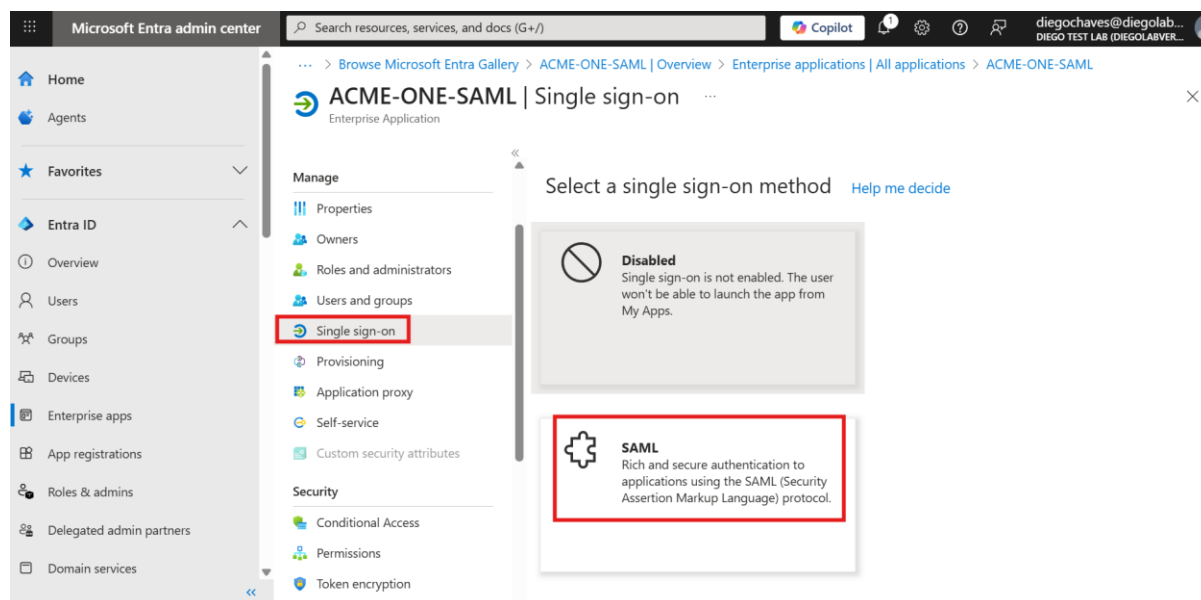
Select **Integrate any other application you don't find in the gallery (Non-gallery)**.

Click **Create**.



3. Set up SAML-based SSO

- Open the newly created application.
- Go to [Single sign-on](#) and [select SAML](#) as the method.



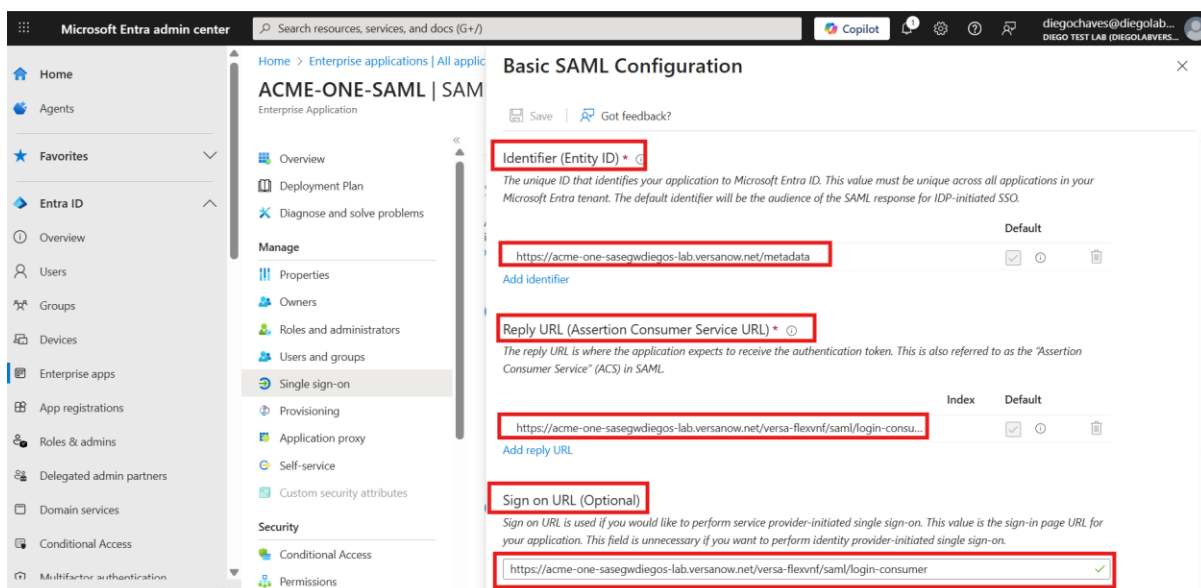
4. In the SAML settings, enter information for the indicates fields.

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

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

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion ID="id-5773745532411060288246009139" IssueInstant="2025-08-08T17:10:21.828Z" Version="2.0"
  xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"/>
  <saml2:Subject>
    <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified" userName/>
    <saml2: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.versaflow.net/versa-flexvnf/saml/login-consumer"/>
    </saml2:SubjectConfirmation>
  </saml2:Subject>
  <saml2:Conditions NotBefore="2025-08-08T17:05:22.008Z" NotOnOrAfter="2025-08-08T17:15:22.008Z">
    <saml2:AudienceRestriction>
      <saml2:Audience>https://acme-one-sasegwdiegos-lab.versaflow.net/metadata/saml2:Audience</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: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>
        <xs:string xmlns:xs="http://www.w3.org/2001/XMLSchema" type="xs:string">GroupName Match Starts with ".*" (ignores case)</xs:string>
      </saml2:AttributeValue>
    </saml2:Attribute>
  </saml2:AttributeStatement>
</saml2:Assertion>
```

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



Microsoft Entra admin center | Search resources, services, and docs (G+)

Basic SAML Configuration

Identifier (Entity ID) *

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

https://acme-one-sasegwdiegolab-versanow.net/metadata

Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

https://acme-one-sasegwdiegolab-versanow.net/versa-flexvnt/saml/login-consu...

Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

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

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

Save | Discard changes | Got feedback?

Name * givenname

Namespace http://schemas.xmlsoap.org/ws/2005/05/identity/claims

Choose name format

Source * ☒ Attribute ☐ Transformation ☐ Directory schema extension

Source attribute * user.givenname


Claim conditions

Advanced SAML claims options

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

Manage claim ...



 Save
  Discard changes
  Got feedback?

Name * ✓

Namespace ✓

Choose name format

Source * ☒ Attribute ☐ Transformation ☐ Directory schema extension

Source attribute * ✓

Claim conditions

Advanced SAML claims options

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

Manage claim ...



 Save
  Discard changes
  Got feedback?

Name * ✓

Namespace ✓

Choose name format

Source * ☒ Attribute ☐ Transformation ☐ Directory schema extension

Source attribute * ✓

Claim conditions

Advanced SAML claims options





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

- Click **+ Add a group Claim**

[Home](#) > [App registrations](#) > [Enterprise applications | All applications](#) > [ACME-ONE-SAML | SAML-based Sign-on](#) > [SAML-based Sign-on](#) >

Attributes & Claims ...



 Add new claim
  Add a group claim
  Columns
  Got feedback?

Required claim

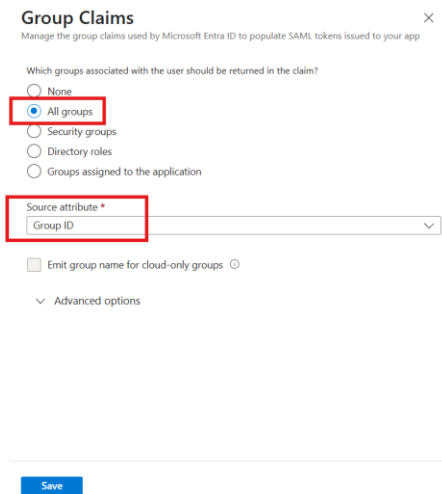
Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...]

Additional claims

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

Advanced settings

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



Group Claims ×

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

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

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

Source attribute *

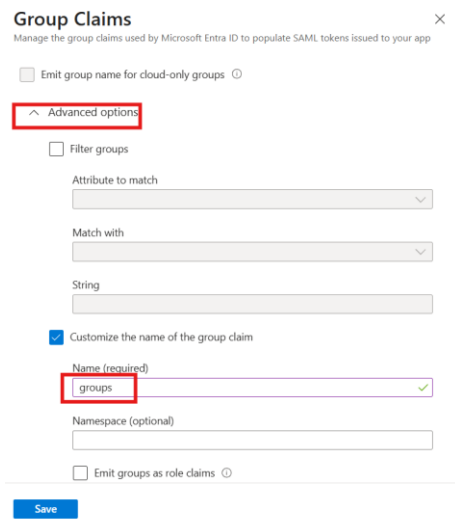
Group ID

☐ Emit group name for cloud-only groups ⓘ

Advanced options

Save

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



Group Claims ×

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

☐ Emit group name for cloud-only groups ⓘ

Advanced options

☐ Filter groups

Attribute to match

Match with

String

☒ Customize the name of the group claim

Name (required)

groups

Namespace (optional)

☐ Emit groups as role claims ⓘ

Save

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

Group Claims

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

String

☒ Customize the name of the group claim

Name (required)
groups ✓

Namespace (optional)

☐ Emit groups as role claims

☒ Apply regex replace to groups claim content

Regex pattern *
.*

Regex replacement pattern *
\$0

☐ Expose claim in JWT tokens in addition to SAML tokens

Save

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 [Edit](#)

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-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional) [Edit](#)

Required	No
Active	0
Expired	0

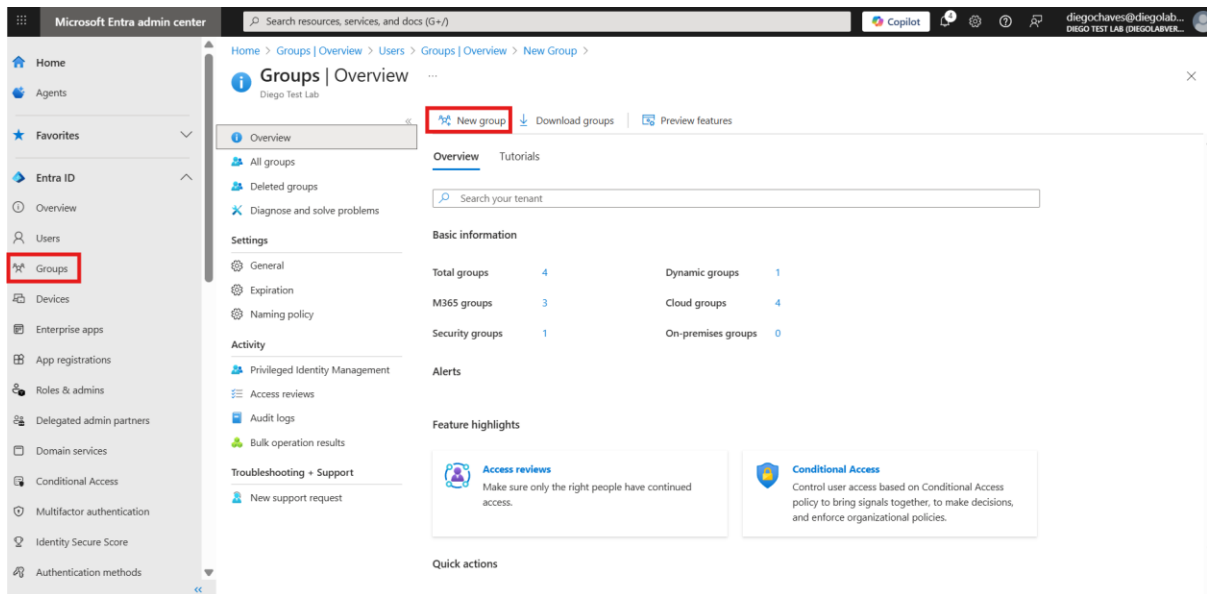
4 Set up ACME-ONE-SAML

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

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

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 * ⓘ
Security

Group name * ⓘ
VIP_Group

Group description ⓘ
Enter a description for the group

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

Membership type * ⓘ
Assigned

Owners
No owners selected

Members
No members selected

Create

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

Example:

UPN → vip@acme-one.onmicrosoft.com

Display Name → vip

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

Create new user

Create a new internal user in your organization

Basics Properties Assignments Review + create

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

Identity

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

Mail nickname * vip ☒ Derive from user principal name

Display name * vip

Password * ☒ Auto-generate password

Account enabled ☒

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

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

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

Create new user

Create a new internal user in your organization

Basics **Properties** Assignments Review + create

Identity

First name VIP1

Last name VIP1

User type Member

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

Job Information

Job title

Company name

Department

Employee ID

Employee type

Employee hire date

Office location

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

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

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

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

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

Create new user

Create a new internal user in your organization

Basics Properties **Assignments** Review + create

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

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

No assignments to display.


Review + create

< Previous

Next: Review + create >

 Give feedback






Select group

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

Search

5 results found

All Groups

	Name	Type	Details
<input type="checkbox"/>	 All Company	Group	allcompany@diegolabversa.onmicrosoft.com
	 All Users	Group	Dynamic groups are not allowed.
<input type="checkbox"/>	 Diego Test Lab	Group	DiegoTestLab@diegolabversa.onmicrosoft.com
<input type="checkbox"/>	 Group for Answers in Viva Engag...	Group	groupforanswersinvivaengagedonotdelete16%
<input checked="" type="checkbox"/>	 VIP_Group	Group	

Selected (1)

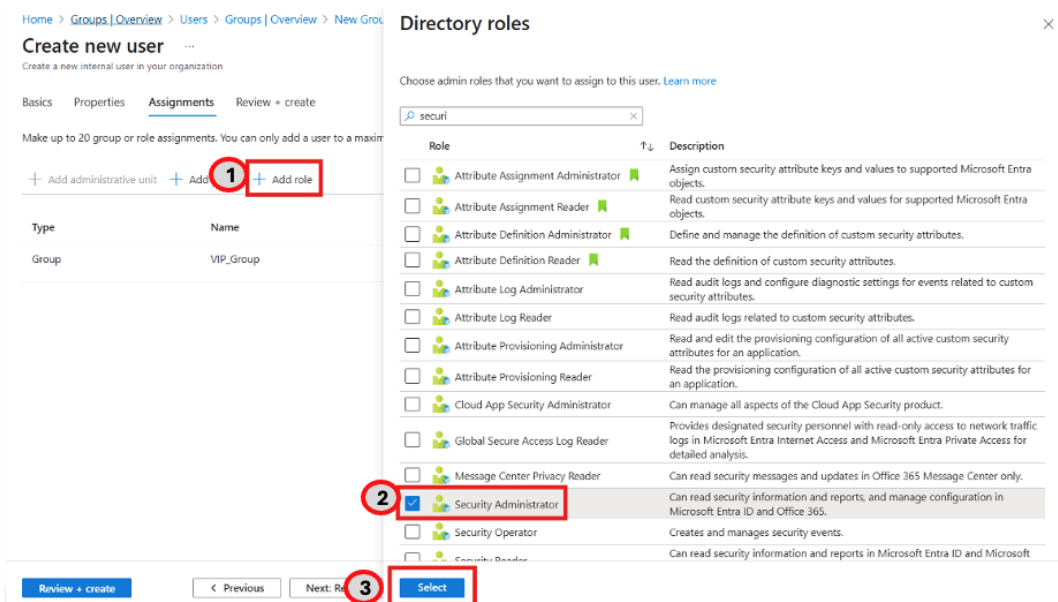
 Reset

 VIP_Group 

Select

- Still under **Assignments**, click **Add Role**.
 - From the directory roles list, assign security-related roles as required. For example:
 - **Security Reader** – allows read access to security reports.
 - **Security Administrator** – manages security configuration.

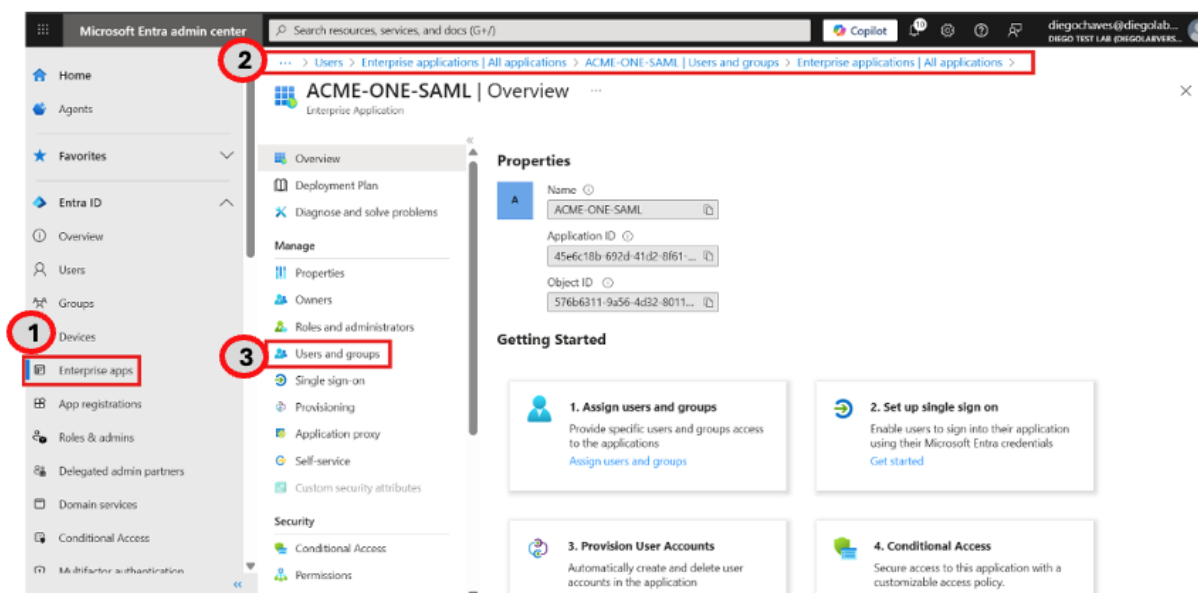
Roles are optional for SAML authentication itself but useful if role claims are mapped into SAML tokens for authorization in downstream apps.



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**.



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

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

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

Enterprise Application

Overview
Deployment Plan
Diagnose and solve problems

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

Security
Conditional Access
Permissions

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

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

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

First 200 shown, search all users & groups

Display name	Object type
No application assignments found	

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

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

Add Assignment

Diego Test Lab

Users and groups

None Selected

Select a role

User

Users and groups ...

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

Search

9 results found

All Users Groups

	Name	Type	Details
<input type="checkbox"/>	Diego Test Lab	Group	DiegoTestLab@diegolabversa.onmicrosoft.com
<input type="checkbox"/>	vip	User	vip@diegolabversa.onmicrosoft.com
<input type="checkbox"/>	Group for Answers in Viva Engag...	Group	groupforanswersin vivaengagedonotdelete1
<input type="checkbox"/>	VIP	User	vip1@diegolabversa.onmicrosoft.com
<input type="checkbox"/>	VIP_Group	Group	

Selected (0)
Reset
No items selected

Select

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

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

Add Assignment

Diego Test Lab

×

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

Users and groups

1 group selected.

Select a role

User

Assign

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

VERSA ACME-ONE CONFIGURATION

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

User and Device Authentication Profile

Publish (1)

Use and Device Authentication Profiles (1)

+ Add Delete Refresh Reference Select Columns

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

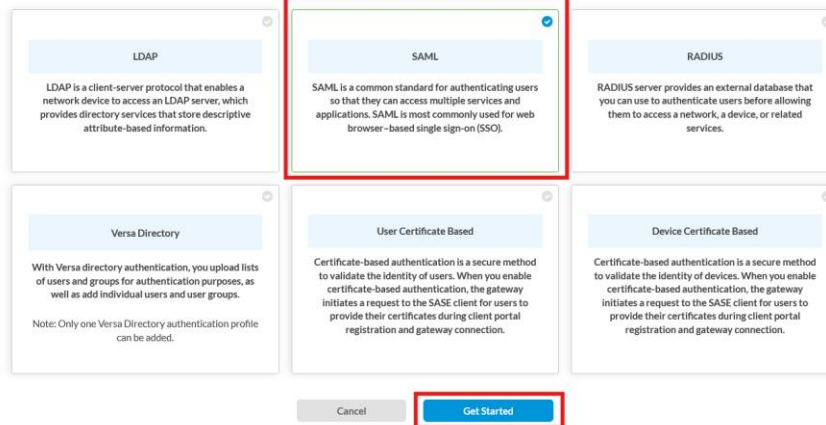
Showing 1-1 of 1 results 10 Rows per Page

Go to page 1 < Previous 1 Next >

Select **SAML**, Click Get Started

Add User and Device Authentication Profile

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



The dialog shows six authentication profile options:

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

Buttons: Cancel, **Get Started**

Select **ENTRA-ID**

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

From this page, copy/download the values required :

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

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

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

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Custom security attributes

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-in logs

Upload metadata file

Change single sign-on mode

Test this application

Got feedback?

SAML Certificates

Token signing certificate

Status

Active

Edit

Thumbprint

0382CE5329AACF016A20F1C7419EBF0E150D786

Expiration

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

Notification Email

diegochaves@diegolabversa.onmicrosoft.com

App Federation Metadata Url

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

Certificate (Base64)

Download

Certificate (Raw)

Download

Federation Metadata XML

Download

Verification certificates (optional)

Required

No

Edit

Active

0

Expired

0

Set up ACME-ONE-SAML

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

Login URL

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

Microsoft Entra Identifier

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

Logout URL

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

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

Add SAML Authentication Profile

Settings

Users And User Groups

Review & Submit

Select SAML Type

Okta

Ping Identity

Office 365

Microsoft Entra ID

Google IAM

Cisco Duo

Other

Single Sign-on URL *

Service Provider Entity ID *

Identity Provider Entity ID *

Single Sign-out URL

Service Provider Certificate

Identity Provider Certificate *

Prefix ID

Cache Expiry Time (mins)

Group Attribute

Concurrent Logins

Reply URL (Assertion Consumer Reply URL)

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

Cancel

Skip to Review

Next

Complete the parameters using the values from the 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

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

Add SAML Authentication Profile

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

Settings Users And User Groups Review & Submit

OKTA

OKTA

Pingidentity

Ping Identity

Office 365

Office 365

Microsoft Entra ID

Microsoft Entra ID

Google IAM

Google IAM

Cisco Duo

Cisco Duo

Other

Other

Single Sign-on URL *

https://login.microsoftonline.com/8b4b2c1-4d5f-482b-9f9e-8b7d0a22c41e2

Service Provider Entity ID *

https://acme-one-sasagidgms-fab-versaflow.net/metadata

Identity Provider Entity ID *

https://sts.windows.net/8b4b2c1-4d5f-482b-9f9e-8b7d0a22c41e2/

Identity Provider Certificate *

ACME-ONE-SAML

Details

Name

ACME-ONE-SAML

File Name

ACME-ONE-SAML.cer

Issued To

Microsoft Azure Federated SSO Certificate

Issued By

Microsoft Azure Federated SSO Certificate

Validity

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

Cache Expiry Time (min)

10

Cache Expiration Mode

...

Group Attribute

Cookie Expiry Time (min)

720

Concurrent Logins

1

Reply URL (Assertion Consumer Reply URL)

https://acme-one-sasagidgms-fab-versaflow.net/versa-flow/uaa/login-consumer

Cancel

Skip to Review

Next

Then **Next**

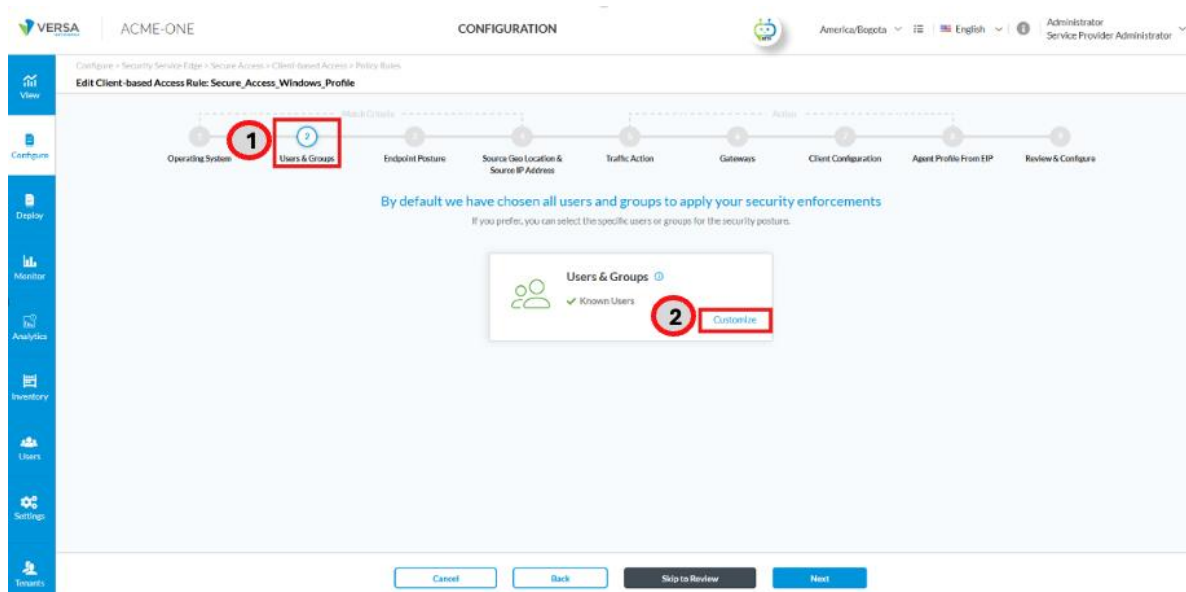
On the **Users and User Groups** page, you can add individual users or entire groups. Click **User Groups** and add the **VIP1_Group** created in the Okta app. Click **Add**, then click **Next** to continue.

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.

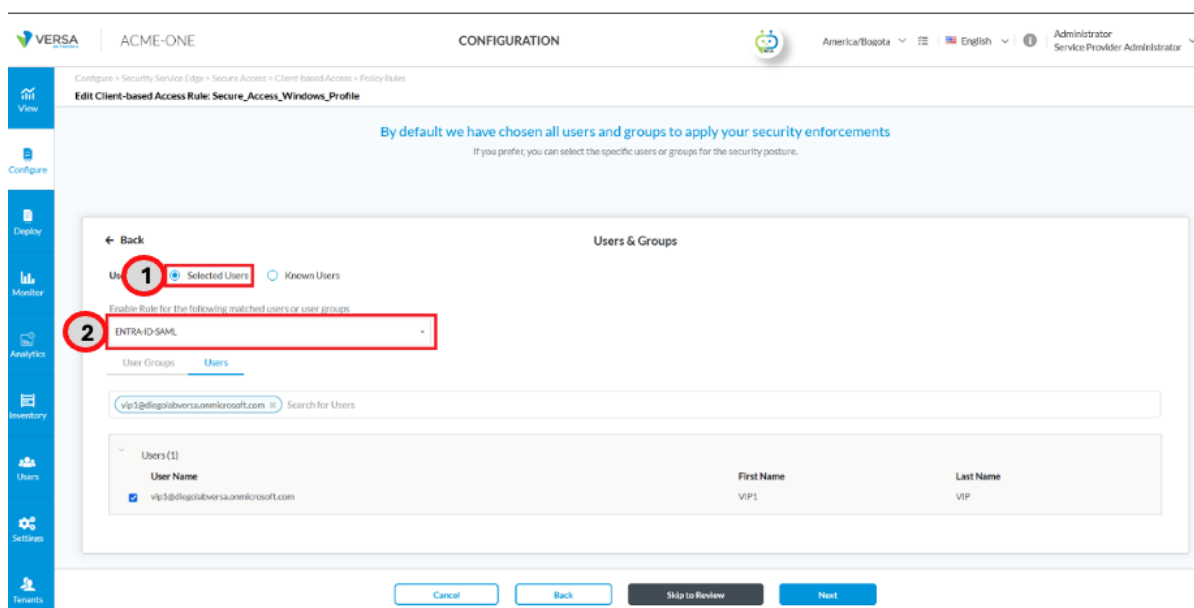
After creating and Publishing the Authentication Profile, you must apply them to the Secure Access Client policy to enforce authentication and apply the corresponding security policies. Navigate to: **Configure > Security Service Edge > Secure Access > Client-based Access > Rules**.

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.

VERSA | ACME-ONE | CONFIGURATION

America/Bogota | English | Administrator Service Provider Administrator

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

Edit Client-based Access Rule: Secure_Access_Windows_Profile

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

← Back

Users & Groups

User Type: ☒ Selected Users ☐ Known Users

Enable Rule for the following matched users or user groups
ENTRA-ID-SAML

User Groups: **Users**

Search for Users: vip1@diegolabversa.onmicrosoft.com

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

Cancel Back Skip to Review Next

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

VERIFICATION

When a user connects to the Gateway and SAML is enabled, the Gateway redirects the login to the configured IdP (Example, Okta or Entra ID). After the user completes credentials/MFA, the IdP returns a **signed SAML assertion** to the Gateway. The Gateway validates the signature and audience, extracts the **NameID** and any mapped attributes (email, groups/roles), and—if successful—establishes the session and applies the matching Secure Access policy. Authentication events can be verified in Concerto under **View > Dashboard > Secure Access > Users > Event**, where successful and failed attempts are logged with details such as username, tunnel IP, and applied profile.

VERSA | ACME-ONE | VIEW

America/Bogota | English | Administrator Service Provider Administrator

View > Dashboard > Secure Access > Users > Events

Summary Usage **Events** Registry Live Users

Events per user

Events per type

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 4th 2025, 2:04:45 PM -05	SaseGWDiegolab-versa-net	vip2@diegolabversa.onmicrosoft.com	DESKTOP-PUC20LR	ipsec	create	192.168.224.17	10.73.106.35	Secure_Access_Windows_Profile	ACME-ONE-Enterprise	Secure_Access_Windows_Profile

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

Secure Access > Logs > Authentication > Events.

Authentication events											
Click to Set or Clear Filter(s)											
Receive Time	Appliance	Auth Profile	Method	Status	Status Message	Time Taken	User	Source Address	Destination Address	Source Port	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	138ms	diego-lab@diegolab-versa.net	10.73.106.36	10.73.106.18	62080	443

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

```
admin@SaseGWDiegos-lab-cli> show orgs org-services ACME-ONE user-identification live-users list
-----^
syntax error: incomplete path
[error][2025-09-04 12:11:46]
admin@SaseGWDiegos-lab-cli> show orgs org-services ACME-ONE user-identification live-users list brief

```

IP ADDRESS	NAME	STATUS	SESSION HITS	TIME TO EXPIRY	EXPIRATION MODE
192.168.224.17	vip2@diegolabversa.onmicrosoft.com	Live	17	60	inactivity

```
[ok][2025-09-04 12:11:50]
admin@SaseGWDiegos-lab-cli>
```

Versa Directory

Versa Directory is a Versa-hosted IDP service based on LDAP, available for Versa-hosted SSE Services. The prerequisite to use this service for you tenant is that enabled on Headend at infrastructure level by Versa or MSP(if using third-party hosted headend): [https://docs.versa-networks.com/Security Service Edge \(SSE\)/Configuration from Concerto/Configure User and Device Authentication#Configure Versa Directory Authentication Using an IAM Server](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](#).