

# Step-By-Step Configuration Guide for Versa Secure Private Access (VSPA) & 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 Private Access (VSPA) and Versa Secure Internet Access (VSIA).

Versa Secure Access Solutions deliver comprehensive, software-defined connectivity and security for today's hybrid workforce. Built on Versa's industry-leading Secure Access Service Edge (SASE) framework, these solutions ensure secure, reliable access to both enterprise and internet resources – anywhere, anytime.

Versa Secure Private Access (VSPA) enables employees to securely connect to enterprise applications hosted in on-premises data centers, private clouds, or public clouds. Leveraging the Zero Trust Network Access (ZTNA) framework, VSPA safeguards users and applications through identity-driven, policy-based access control, seamlessly integrating networking, security, and cloud-delivered services.

Versa Secure Internet Access (VSIA) provides secure and optimized internet connectivity from any location. It protects users, devices, and data through advanced security capabilities – including Secure Web Gateway (SWG), Next-Generation Firewall-as-a-Service (NGFWaaS), Cloud Access Security Broker (CASB), and Data Loss Prevention (DLP). VSIA extends protection to headquarters, branches, home offices, remote workers, travelers.

Together, Versa Secure Private Access and Versa Secure Internet Access offer a unified approach to Zero Trust and SASE – empowering enterprises with secure, seamless access to both private and public resources.

## Document Information

Title	Config Guide for Versa Secure Private Access (VSPA) & Versa Secure Internet Access
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.

## Contents

Scenario .....	4
Topology.....	5
Topology Overview.....	5
Configuration Steps .....	8
Step 1: Set Up Site-to-Site Tunnel .....	8
Step 2: Configure Authentication Method .....	13
Provision SCIM Service .....	19
Step 3: Configure User-Defined Object.....	21
Step 4: Secure Access Profile: Configure DNS Server .....	23
Step 5: Define Secure Access rules .....	26
Step 6: Trusted Network Detection: When the user is in the office.....	32
Step 7: DNS Proxy for Private Domain Resolution.....	35
Step 8: Enforce TLS Policies: Do-Not-Decrypt for Health/Finance   Decrypt the rest.....	41
Step 9: Configure Real-Time Protection Profiles and Rules .....	53
Custom URL Filtering Profile.....	53
Malware Protection & IPS Profile (Predefined) .....	56
Internet Protection Rules .....	56
Private Protection Rules .....	61
SaaS Tenant Control.....	69
Appendix A - Authentication Method - Microsoft Entra ID .....	72
About Versa.....	73

## Scenario

ACME-ONE, a global enterprise, needs two things at the same time:

- **Secure remote access** for users working outside the office who need to reach private applications in their datacenters.
- **Secure internet access** for users inside branches and campuses—without wrecking performance or user experience.

To deliver this, ACME-ONE uses **Versa Secure Private Access (VSPA)** and **Versa Secure Internet Access (VSIA)** together as a unified Zero Trust framework.

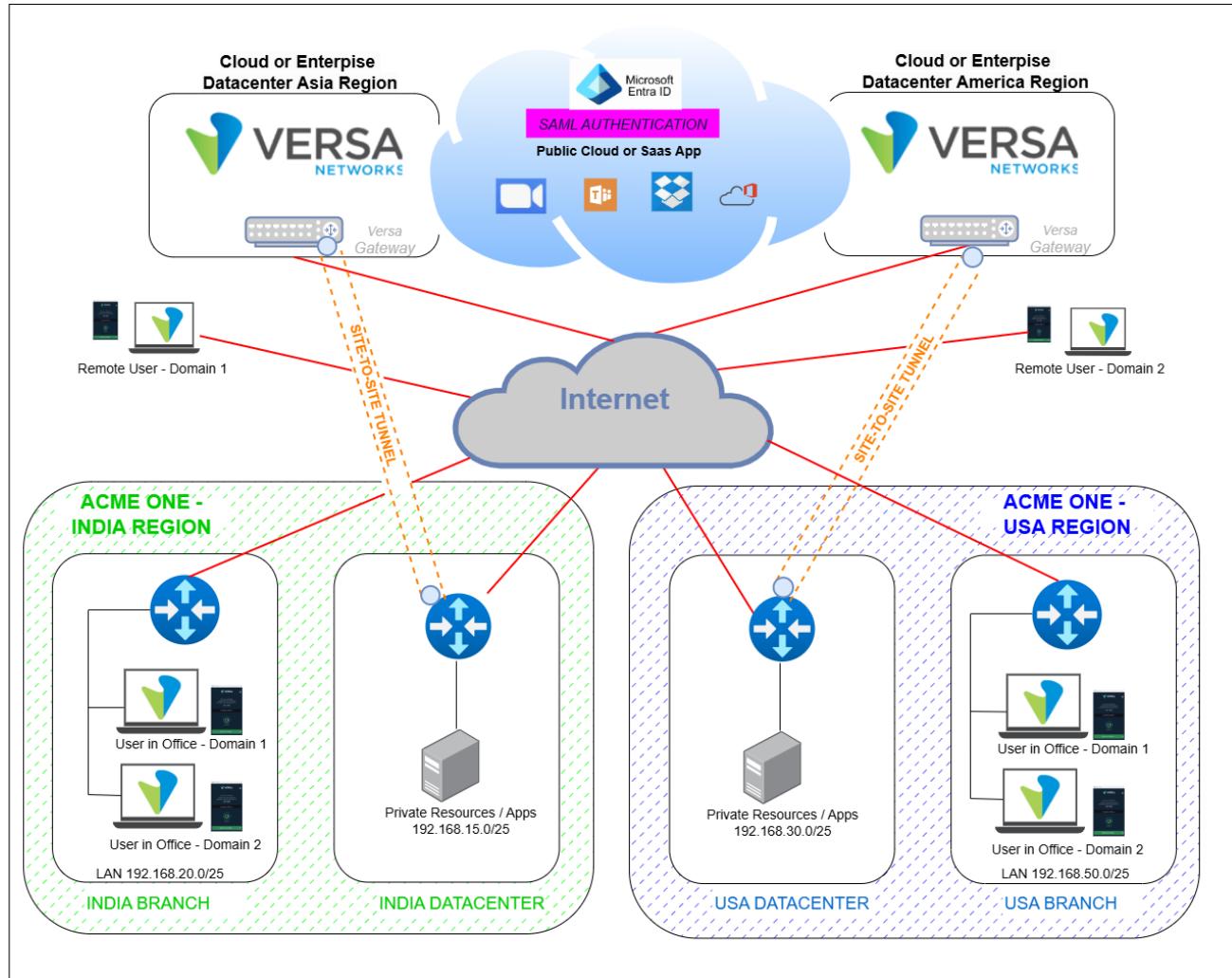
- **VSPA** brokers least-privilege access from remote endpoints to private applications through the SSE gateway.
- **VSIA** secures web traffic for branch/campus users, optimizes SaaS performance, and applies policy enforcement for all outbound internet use.

Identity services come from **Microsoft Entra ID**, which also handles user and group lifecycle automation using **SCIM**.

### Customer Requirements

- Strong authentication (Microsoft Entra ID).
- Policy enforcement is based on users or groups.
- Local Breakout of approved application's traffic (conferencing apps).
- Security enforcement via SSE Gateway: TLS encryption/decryption, Antivirus (AV), Intrusion Prevention System (IPS), URL Filtering.
- Exclude approved URL categories from TLS inspection and enforcement.
- Avoid access to personal and/or external SaaS Tenant.

# Topology



## Topology Overview

This topology represents ACME-ONE solution with 2 regions (India and USA) datacenters and branches. The datacenters of each region connect to the nearest cloud-hosted Versa SASE gateways through encrypted tunnels. The organization also has remote users connecting directly to the internet from outside the branches.

### 1. Remote Users (Work from Home)

- Endpoints run the Versa SASE Client
- Authentication via Entra ID (SAML/OIDC, MFA enforced)
- Remote access to private apps is routed through datacenter IPsec tunnels and into the SSE gateways

- SSE gateways provide a DNS proxy with Split-DNS for internal zone resolution
- Local breakout is allowed for trusted Conferencing Apps (Zoom)
- Remaining internet traffic goes through the SSE Gateway
- TLS decryption is applied to all internet traffic except regulated financial/medical categories
- High/medium risk + unknown/undefined traffic is fully inspected (AV + IPS)
- URL filtering blocks high-risk and reputation-based threats; uncategorized/undefined URLs should be blocked.

## 2. Branch & Campus Topology

- Branch users run the Versa SASE Client for user identification, but with the Trusted Network Detection (TND) Gateway Assisted feature, it creates only a control channel to the Gateways without any tunneling. This will bypass all traffic, including local private traffic. Internet traffic should be routed to the SSE gateway using the site-to-site tunnels, except for the conference application (Zoom).
- Authentication is performed via Entra ID (SAML/OIDC + MFA).
- Internet traffic is decrypted, inspected, and enforced with AV/IPS, except for regulated categories (finance and health)/sites (Do-Not-Decrypt policies).

### Key Steps

- **Establish SASE–Datacenter Site-to-Site Tunnels**
  - Build IPsec tunnels from global SASE gateways to each datacenter region.
- **Integrate Microsoft Entra ID (SAML)**
  - Configure identity provider settings on the Versa gateways
  - Enable MFA and SCIM-based user/group sync
- **Secure Access Profiles**
  - Define DNS servers (no domains)
- **Secure Access Rules (VSIA + VSPA)**
  - Create SA rules for VSIA+VSPA

- Add exceptions for trusted applications (Zoom)
- Enforce identity-based policies
- **TLS Decryption Policies**
  - Add URL category-based bypass rules first
  - Then Apply decryptions for all traffic.
- **Trusted Network Detection**
  - Detect when users are on campus and auto-switch private app flows to LAN
- **SaaS Tenant Control**
  - Enforce corporate-only access to O365 and sanctioned SaaS tenants
- **Apply SSE Security Controls**
  - AV, IPS, DLP as required
  - Web filtering based on group, app, and security posture
- **Real-Time Protection**
  - Block high-risk URL categories and reputation-based threats
  - Enforce controls for uncategorized traffic

# Configuration Steps

## Step 1: Set Up Site-to-Site Tunnel

The site-to-site tunnel is essential for allowing remote users connected to the gateway to access enterprise-hosted private applications. The Versa gateway and the customer data center (DC) firewall (or any other device behind which enterprise applications are hosted) establish a tunnel the gateway uses to route remote user traffic to the enterprise's private applications.

Log in to the Concerto UI using your enterprise administrator credentials (Tenant Admin) to configure a site-to-site tunnel.

Navigate to **Configure > Security Service Edge > Settings > Site-to-Site Tunnels and click + Add.**

This will take you to the new tunnel configuration page.

Gateway	Type	Duration	Tags	Last Modified By & Date	Status	Actions
demo1	IPsec			7/9/2025, 4:06:43 PM admin@192.168.1.100	Enabled	<a href="#">View Settings</a> <a href="#">Download.txt</a>

The tunnel configuration is completed through four wizard screens, as illustrated below. The first section (Enter TYPE) is displayed by default for configuration. Clicking Next at each section moves on to the next section of the tunnel configuration.



The default tunnel selection is IPsec. The remaining details, including tunnel type, remote address, and other parameters, should be configured as outlined below.

1. Selecting "Enter TYPE"
  - A. Keep the default selection on **Type** as IPsec, and Tunnel status is default enabled.
  - B. Choose the correct **Tunnel Type**. If necessary, use the drop-down menu to change it from the default Route-Based tunnel to the **Policy-Based** tunnel. This document shows details related to the Route-Based tunnel.
  - C. The third step shown in the screenshot is **Tunnel Initiate**, which can be triggered by modes like "Responder Only", "Traffic", or "Automatic". When EBGP is used, "Responder Only" works fine. However, when using a static route, it should be set to "Automatic" or "Traffic". In our use case, we can choose Automatic.

Note that Versa Gateway is set as 'responder only' for the IPsec tunnel. So, the peer must initiate the request for the tunnel for the negotiation to start.

- D. Choose the correct originating Versa SASE gateway from the **Versa Gateway** drop-down menu. Typically, each tenant would be provisioned into multiple gateways for redundancy; this option allows you to choose the appropriate gateway from which you need to build a secure tunnel to your enterprise destination.
- E. Use the **Remote Public IP Address or FQDN** field to enter your enterprise firewall details as the tunnel endpoint.

Note: When configuring Local Identity > Type > FQDN, you must enter the specific FQDN of the SASE Gateway that you want to establish the site-to-site tunnel with from the remote site. This **FQDN** appears below the text "**Local Public Gateway FQDN**" in the image below. In our case, it would be acme-one-demo1.versanow.net.

F. Click **Next** to proceed to the next section to provide IPSec Parameters.

2. Selecting "Enter IPSEC INFORMATION"; Clicking Next in the above section will bring you to this part of the screen, where IPsec-related details are to be provided. Refer to the image below.

A. Provide IKE and IPsec parameters according to your configuration requirements. The image below shows the default selection; use the drop-down menus to modify as needed. The following table summarizes the recommended settings for both IKE (Phase

1) and IPsec (Phase 2). Note that while some vendors use a shorter lifetime (3600 seconds), we recommend 28800 seconds for consistency and reduced rekeying overhead.

Phase	Parameter	Value
IKE (Phase 1)	Encryption	AES-256
	Authentication	SHA-256
	DH Group	14
	Lifetime (seconds)	28800
IPsec (Phase 2)	Encryption	AES-256
	Authentication	SHA-256
	PFS (DH Group)	14
	Lifetime (seconds)	28800

- B. Choose the desired Authentication mode. The default selection is a pre-shared key (PSK). If "Certificate" is to be chosen, then Local and remote certificate names and CA chains are to be added.
- C. For pre-shared-key based authentication, add Local and Remote identities (Identity Type such as Email, IP, FQDN) and their corresponding Value and Share Key.
- D. Click **Next.**

### 3. Selecting "Enter ADDRESS & ROUTING / POLICY CONFIGURATIONS"

In this section, configure the tunnel interface IP, usually a /30 from your enterprise segment. Select the VPN name assigned to your tenant at the Gateway, the MTU value, and either Static or EBGP as your preferred routing protocol. Refer to the image below.

- A. Under "Setup the Versa SASE Gateway routing towards the enterprise VPN" configure the following

Add a Tunnel Virtual Interface address that is routable within your enterprise network. This typically involves using one IP from a /30 IPv4 address, with the other usable IP from the same /30 to be configured at your enterprise IPsec endpoint.

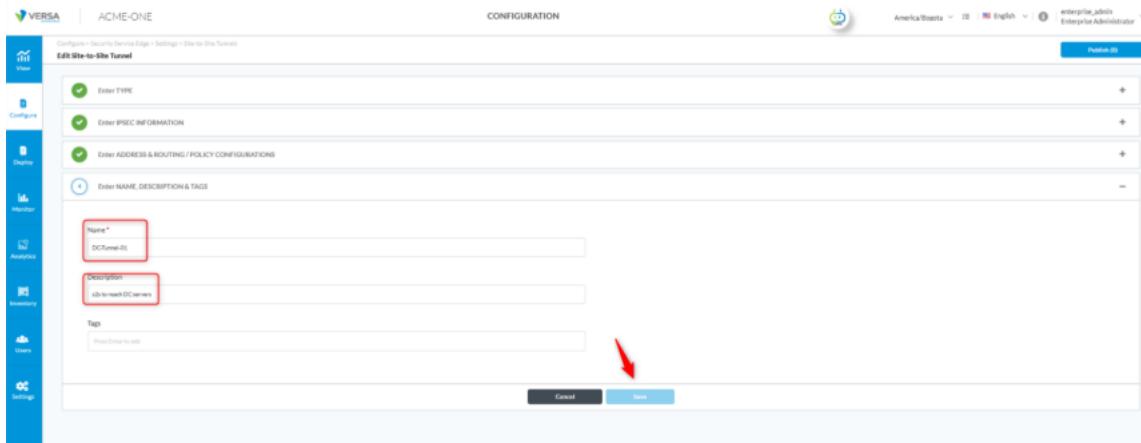
**VPN Name** to be selected from drop-down, usually the VPN name assigned to your tenant by the service provider, named as <TenantName-Enterprise>

Set **MTU**: Versa recommends that the maximum transmission unit be set to 1300 for IPsec-based tunnels

Under Static Routes and Routing Protocols, configure the following

- Click **+ Add** to create a new route.
- Set Routing Protocol to None.
- Enter the destination subnet. (In our case, we need to enter the server subnets one by one: 192.168.15.0/25, 192.168.20.0/25, 192.168.30.0/25, 192.168.50.0/25).
- Assign a preference value between 1–255 (lower = higher priority).
- Routing Protocol select None.
- Click **Save**.

#### 4. Completing section Enter NAME, DESCRIPTION & TAGS



Notes: Ensure that the IPSec tunnel on the peer firewall is configured using the same parameters described in this guide.

NOTE: For high availability and dynamic routing across multiple tunnels, EBGP is recommended.

## Step 2: Configure Authentication Method

Versa SASE supports various authentication methods, including LDAP and SAML. This example utilizes Microsoft Entra ID with SCIM for users' authentication when connecting via the SASE client.

See **Appendix A** for other authentication methods, configurations and options available on the Microsoft Entra ID portal.

For the configurations needed on the Concerto, navigate to:

**Configure > Security Service Edge > User and Device Authentication > Profiles and click + Add** and follow these steps. Refer to the image below.

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

Now, we need to complete the 3 steps as follows: (**Settings, User and Group Profile, Review & Submit**)

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

## Add SAML Authentication Profile

1

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 \*

Prefix ID

Group Attribute

Cache Expiry Time (mins) 10

Cookie Expiry Time (mins) 720

Concurrent Logins 1

Reply URL (Assertion Consumer Reply URL)

- https://acme-one-sasegw2.versanow.net/versa-flexvnf/saml/login-consumer
- https://acme-one-sasegw1.versanow.net/versa-flexvnf/saml/login-consumer

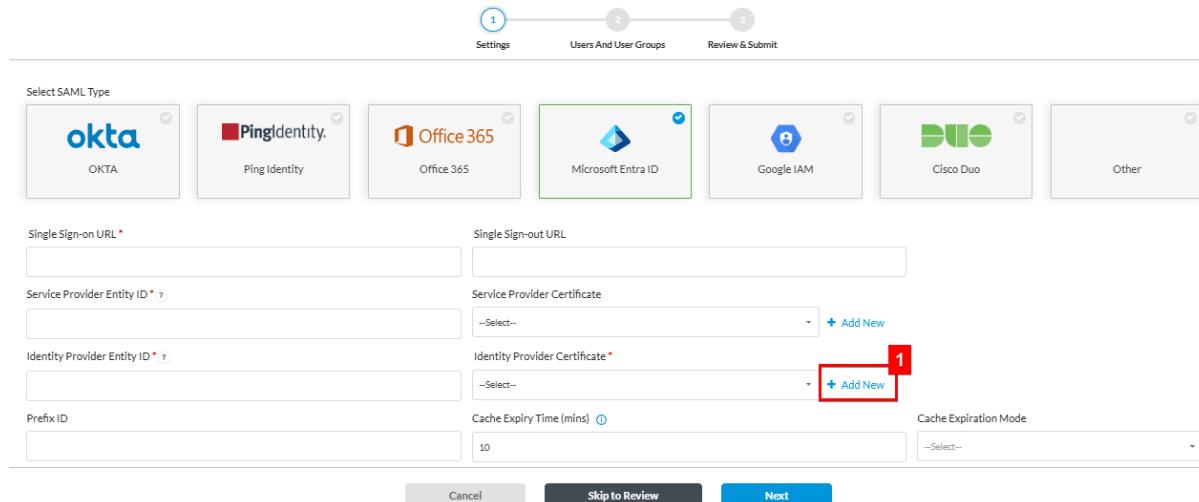
Cancel Skip to Review Next

Example:

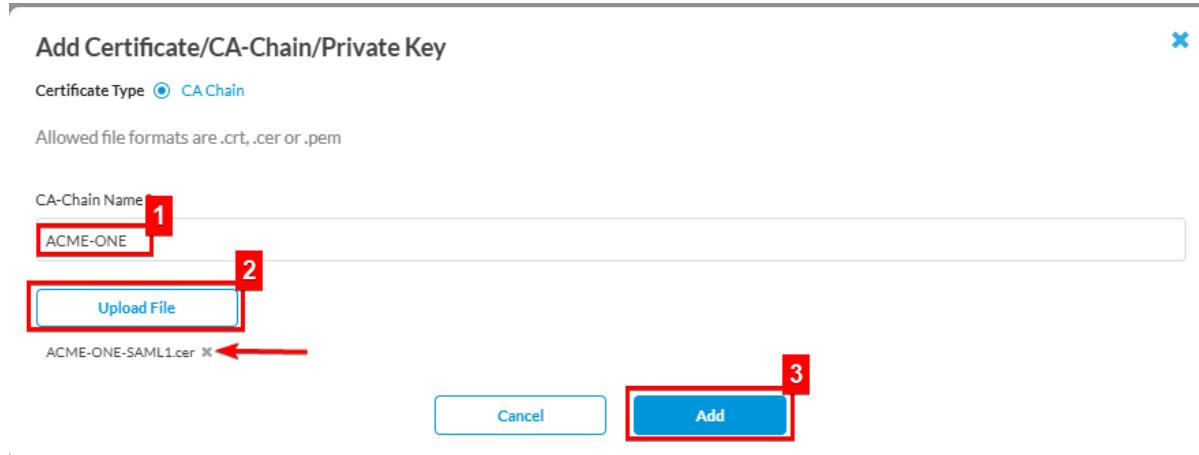
- Single Sign-on URL:** <https://login.microsoftonline.com/900afbfd-92ce-441a-abc6-ad81e25b7711/saml2>
- Single Sign-out URL:** <https://login.microsoftonline.com/900afbfd-92ce-441a-abc6-ad81e25b7711/saml2>
- Service Provider Entity ID:** <https://acme-one-sasegw1.versanow.net/metadata>
- Identity Provider Issuer:** <https://sts.windows.net/900afbfd-92ce-441a-abc6-ad81e25b7711/>

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

## Add SAML Authentication Profile

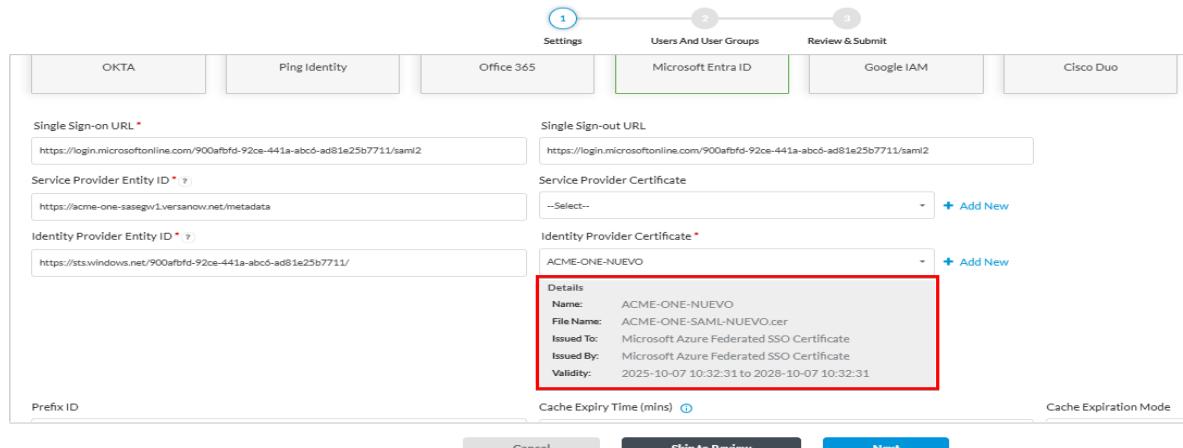


Assign a descriptive name for **CA-Chain Name**, then upload certificate by clicking on the **Upload File**. Locate the certificate and click **Add**



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

## Edit SAML Authentication Profile: MSEntraID-OscarNuevo



Then **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 users or groups can then be referenced when configuring Secure Access Rules and Real-Time Protection Rules.

In this case we will add manually 2 users ([vip@oscarlabsase.onmicrosoft.com](mailto:vip@oscarlabsase.onmicrosoft.com) and [remotevip@oscarlabsase.onmicrosoft.com](mailto:remotevip@oscarlabsase.onmicrosoft.com)) for testing purposes. Click **+Add**.

Edit SAML Authentication Profile: MSEntraID-OscarNuevo

Settings (1) Users And User Groups (2) Review & Submit (3)

User List Group List

Upload user list in the following format: csv  Browse Note: CSV file should be in the following format: UserName\*,First Name, and Last Name.

Users (0)

<input type="checkbox"/> User Name	First Name	Last Name
No Data		

**1**

Cancel Back Skip to Review Next

Add the **Username, First Name** and click **Save** for both users.

**Edit User**

User Name\*

First Name

Last Name

**Edit User**

User Name\*

First Name

Last Name

Click **Next** to proceed.

Edit SAML Authentication Profile: MSEntraID-OscarNuevo

1

2

3

Settings    Users And User Groups    Review & Submit

User List    Group List

Upload user list in the following format: csv

Browse    Note: CSV file should be in the following format: UserName\*,First Name, and Last Name.

Users (2)

+ Add    Delete

User Name	First Name	Last Name
<a href="#">vip@oscarlabsbase.onmicrosoft.com</a>	vip	
<a href="#">remotevip@oscarlabsbase.onmicrosoft.com</a>	remotevip	

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

Cancel    Back    Skip to Review    **Next** 1

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.

Edit SAML Authentication Profile: MSEntraID-OscarNuevo

1

2

3

Settings    Users And User Groups    Review & Submit

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

**General**

Name **1** MSEntraID-ACME

Description

Tags

Press Enter to add

**Settings** **2**

SAML Type EntralID

Single Sign-on URL <https://login.microsoftonline.com/900afbfd-92ce-441a-abc6-ad81e25b7711/saml2>

Single Sign-out URL <https://login.microsoftonline.com/900afbfd-92ce-441a-abc6-ad81e25b7711/saml2>

Service Provider Entity ID <https://acme-one-sasegw1.versanow.net/metadata>

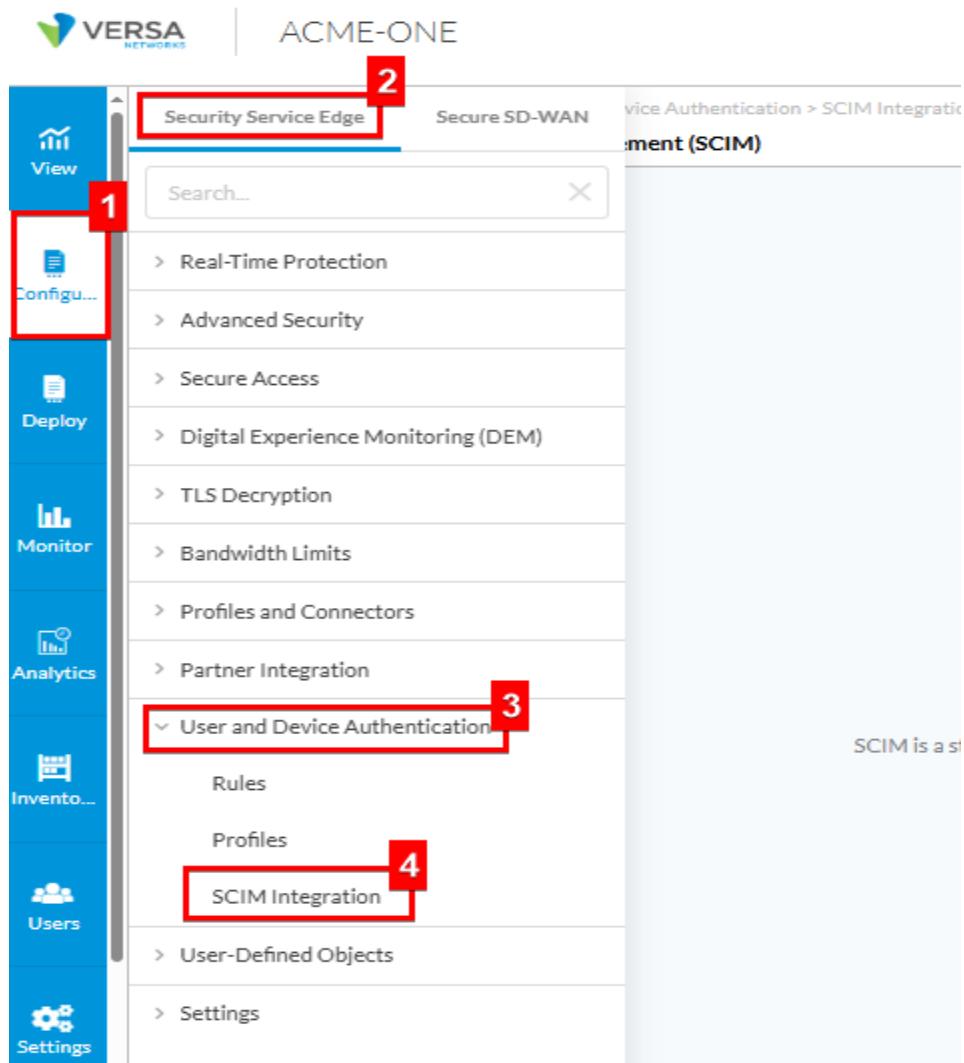
Service Provider Certificate

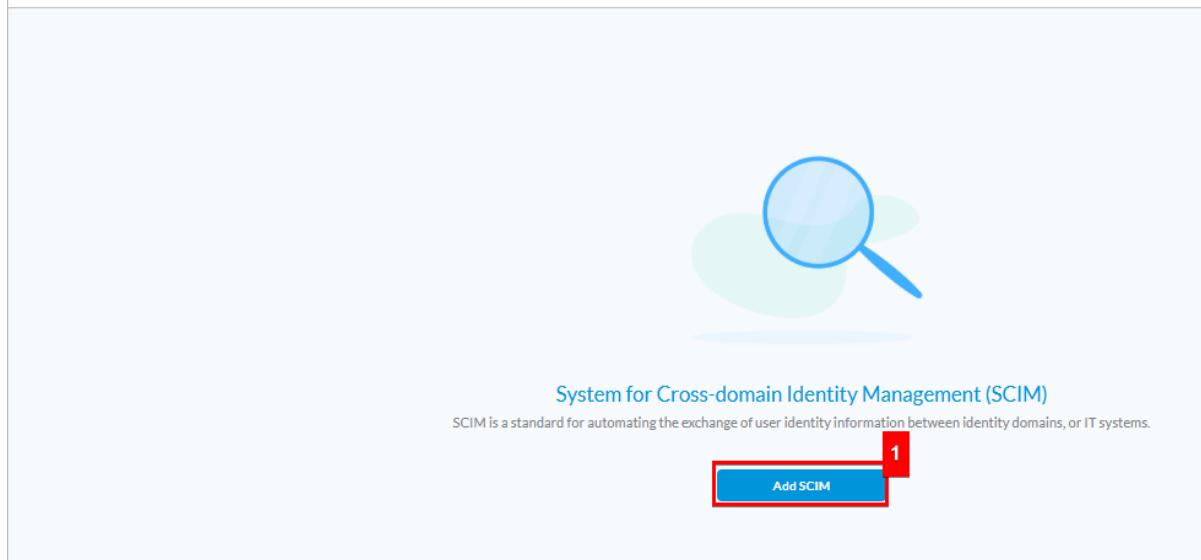
Cancel    Back    **Save** 2

NOTE: As an alternative; to avoid adding the users manually, there is the option to enable **SCIM** integration to automate user and group provisioning. SCIM service can be leveraged as another method for managing users and groups. Unlike LDAP-based authentication profiles, SCIM operates as part of a separate identity provisioning setup outside of the profile configuration workflow. The SCIM provisioning steps are mentioned below.

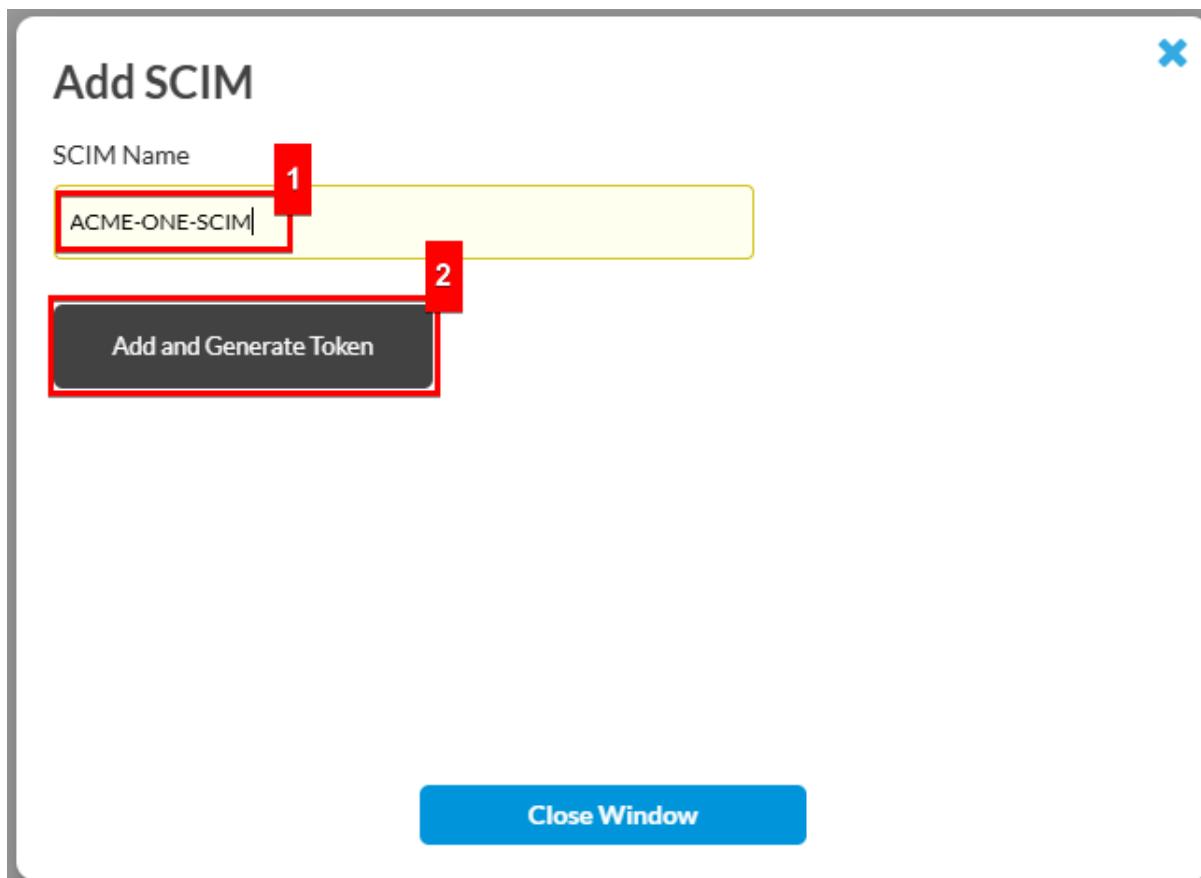
## Provision SCIM Service

Navigate to **Configure > Security Service Edge > User and Device Authentication > SCIM Integration + Add SCIM** and follow these steps. Refer to the image below.



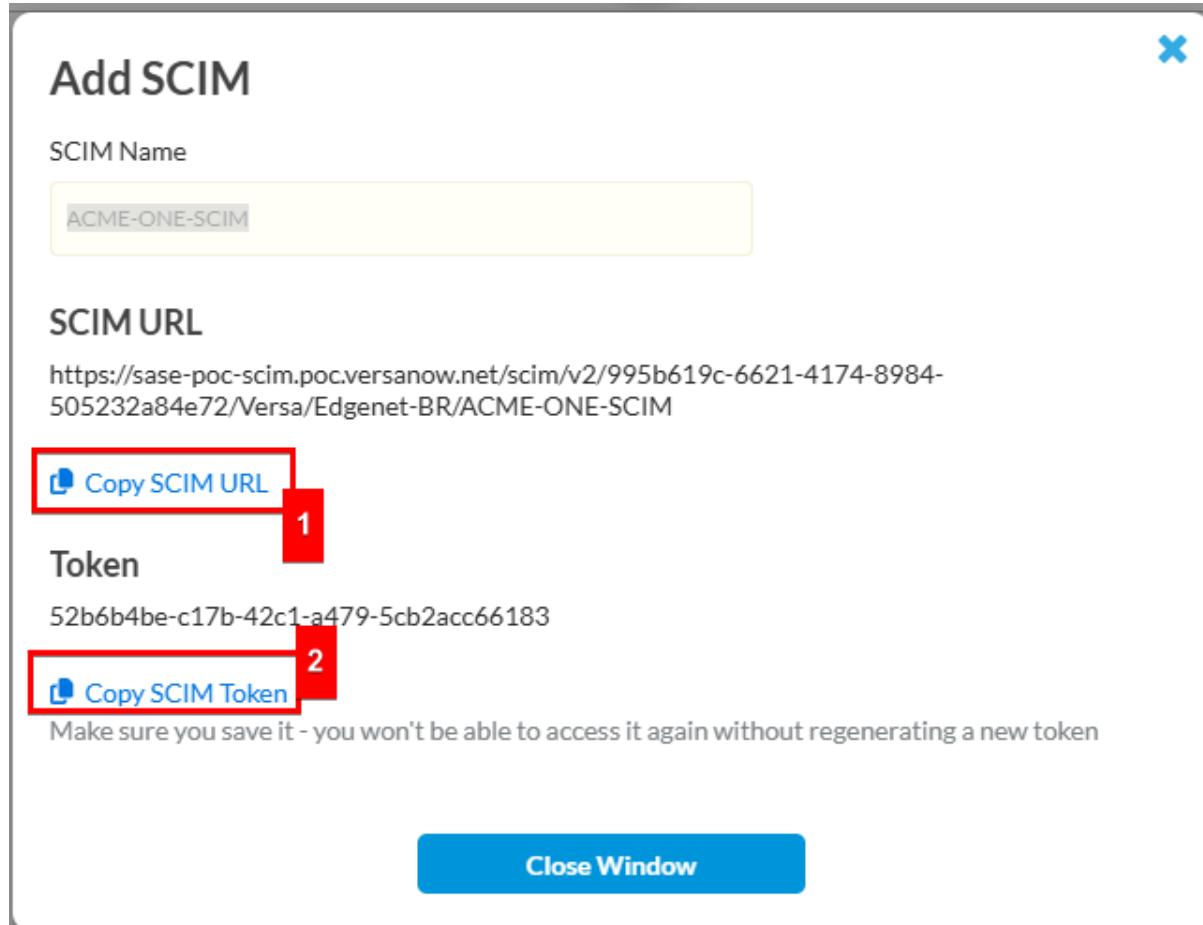


When the Add SCIM popup window displays. enter a **name** in the SCIM Name field. Ensure that you use a unique name to identify the IdP from which users or user groups are provisioned and click on **Add and Generate Token**



The following window displays. Copy the SCIM URL and token and save them.

The URL includes the tenant's name, VMS ID, SCIM cloud server FQDN, and the SCIM name that you provide in the Add SCIM screen. You use this URL and token when you provision SCIM using Microsoft Entra ID. Entering these details in Entra creates a channel between the IdP and SCIM cloud server.



### Step 3: Configure User-Defined Object

Versa supports a variety of user-defined objects (Example, Applications, services). When a particular object is not listed under pre-defined objects, we can define the object using the User-defined (Custom) Object.

Custom applications can be classified as:

- Any application that needs to interact with the **client** or be referenced in a **Secure Access Rule** must be defined as a **Client Native Application**. For split tunnelling or DEM use case.
- Applications that interact with the **gateway** or are referenced in **Real-Time Protection Rules** must be defined as **Private Applications**. To allow or block a private application.

In our case, we will create a couple of **Private Applications** to be used in our **Private Protection Policies**. The following section outlines the steps to create a Private Application.

To create a **Private Application**, navigate to

**Configure > Security Service Edge > User-Defined Objects > Applications > Private Application**

Then, create the test apps **india-portal.acme-one.com** and **usa-apps.acme-one.com** as follows:

**india-portal.acme-one.com:**

Match Criteria

Configure > Security Service Edge > User-Defined Objects > Applications

**Add Private Application**

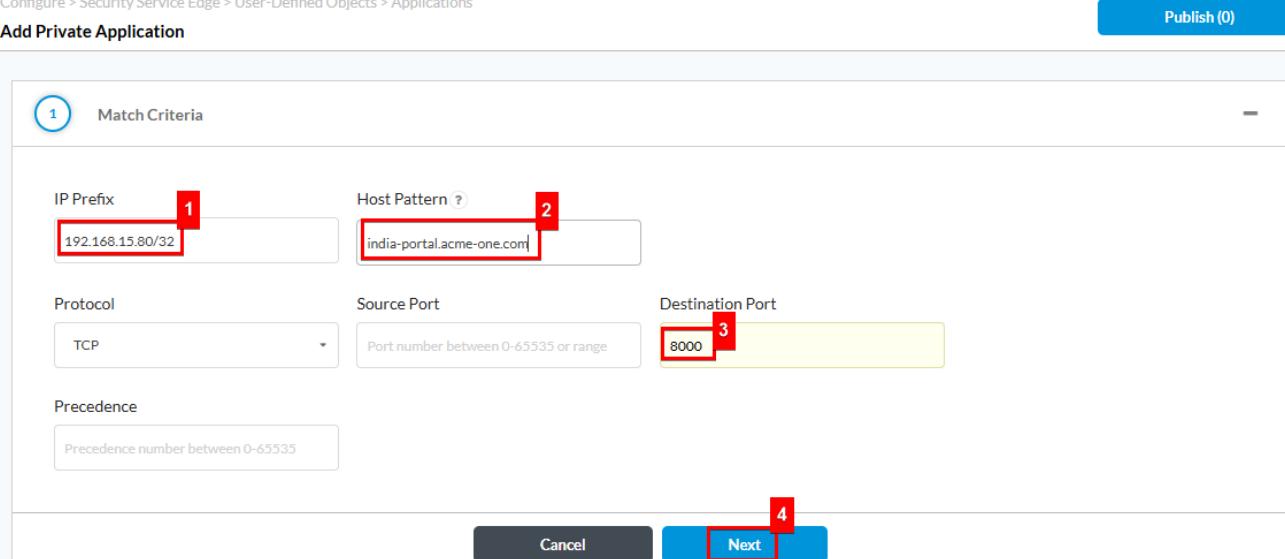
**Match Criteria**

1 IP Prefix **192.168.15.80/32** 2 Host Pattern **india-portal.acme-one.com**

Protocol **TCP** Source Port **Port number between 0-65535 or range** Destination Port **8000** 3

Precedence **Precedence number between 0-65535**

**Next** 4



Application Attributes

Configure > Security Service Edge > User-Defined Objects > Applications

**Edit Private Application**

**Application Attributes**

**Risk**  
Each application has been assessed and assigned a risk level (1 – lowest to 5 – highest) by the Versa Networks security research team. The number in each card indicates applications with the same risk.

**Productivity**  
Each application has been assessed and assigned a productivity level (1 – lowest to 5 – highest) by the Versa Networks security research team. The number in each card indicates applications with the same productivity.

**Family**

- Business-system
- Collaboration
- General-internet
- Antivirus
- Application-service
- Audio-video
- Authentication
- Behavioral
- Compression
- Database
- Encrypted
- Encrypted-tunnel
- Erp
- File-server
- File-transfer
- Forum
- Game
- Instant-messaging
- Internet-utility
- Mail
- Microsoft-office
- Middleware
- Network-management
- Peer-to-peer
- Printer
- Routing
- Security-service
- Standard
- Telephone
- Terminal
- Thin-client
- Tunneling
- Unknown
- Wap
- Web
- Webmail

**Application Tags - Security**

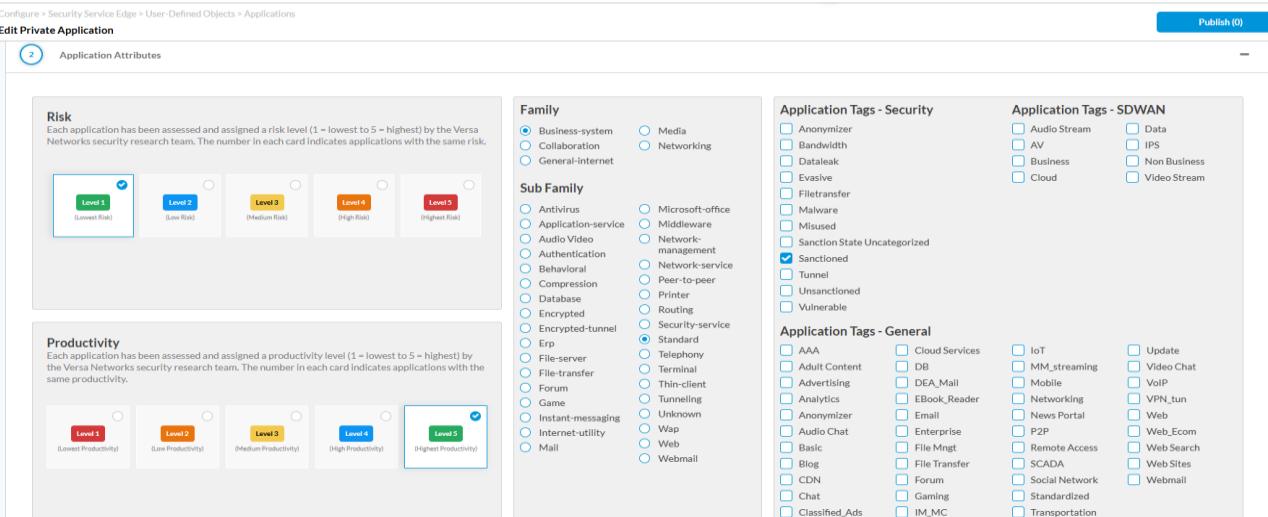
- Anonymizer
- Bandwidth
- Dataleak
- Evasive
- Filetransfer
- Malware
- Misused
- Sanction State Uncategorized
- Sanctioned
- Tunnel
- Unsanctioned
- Vulnerable

**Application Tags - SDWAN**

- Audio Stream
- Data
- IPS
- Business
- Non Business
- Cloud
- Video Stream

**Application Tags - General**

- AAA
- Adult Content
- Advertising
- Analytics
- Anonymizer
- Basic
- Blog
- CDN
- Chat
- Classified\_Ads
- Cloud Services
- DB
- DEA\_Mail
- EBook\_Reader
- Email
- Enterprise
- File\_Mgmt
- File\_Transfer
- Forum
- Gaming
- IM\_MC
- IoT
- MM\_streaming
- Mobile
- Networking
- News Portal
- P2P
- Remote Access
- SCADA
- Social Network
- Standardized
- Web
- Web, Ecom
- Web Search
- Web Sites
- Webmail
- Update
- Video Chat
- VoIP
- VPN\_tun
- Transportation



Name, Description, Tags & Application Image.

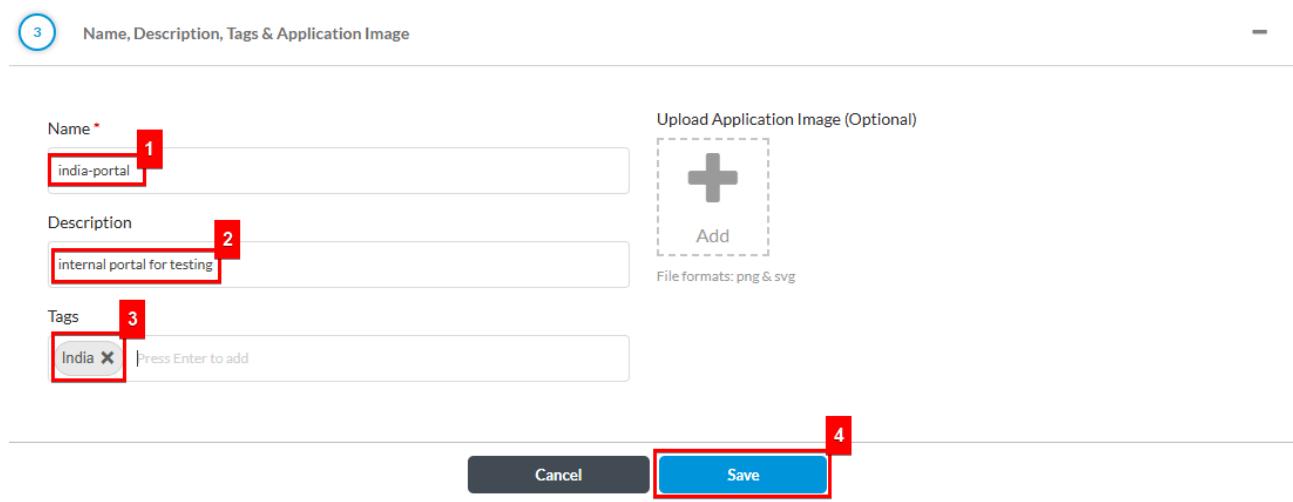
3 Name, Description, Tags & Application Image

1 Name: india-portal

2 Description: internal portal for testing

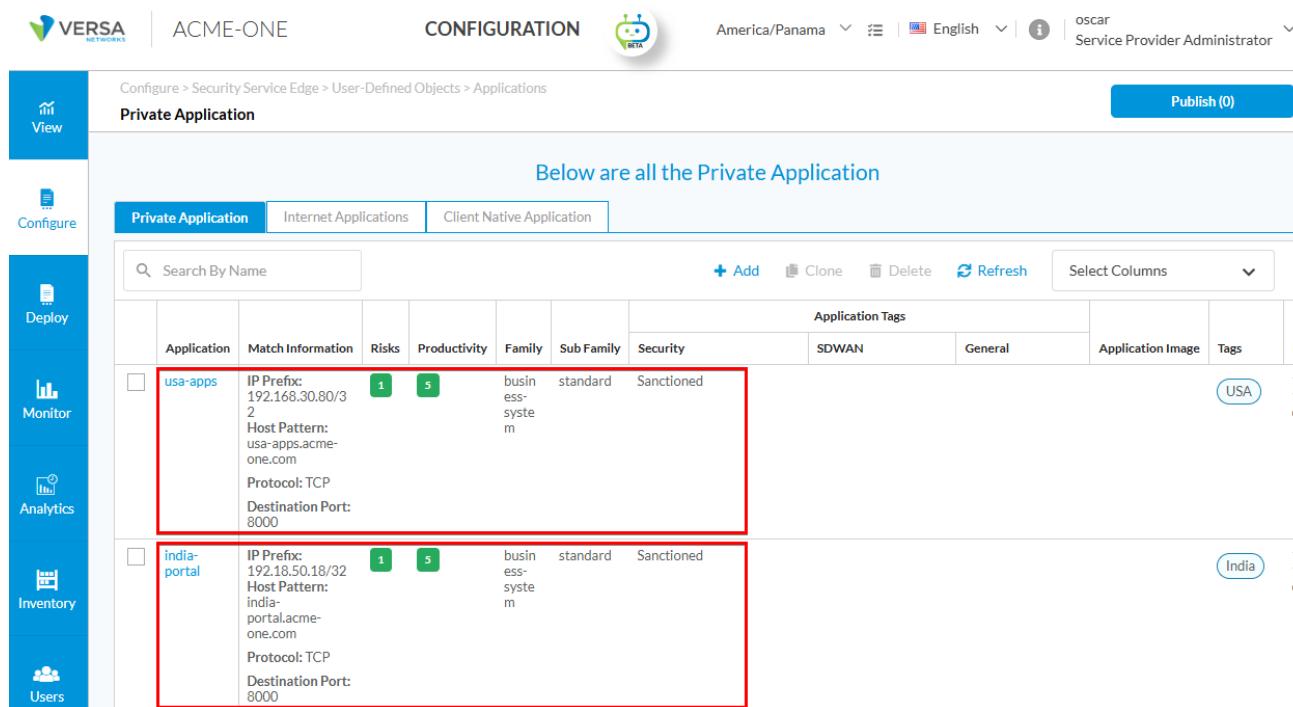
3 Tags: India

4 Save



Do the same for the other application ([usa-apps.acme-one.com](http://usa-apps.acme-one.com)) or any other one you want to test.

The private app definitions should resemble the image below.



ACME-ONE CONFIGURATION

Configure > Security Service Edge > User-Defined Objects > Applications

**Private Application**

Below are all the Private Application

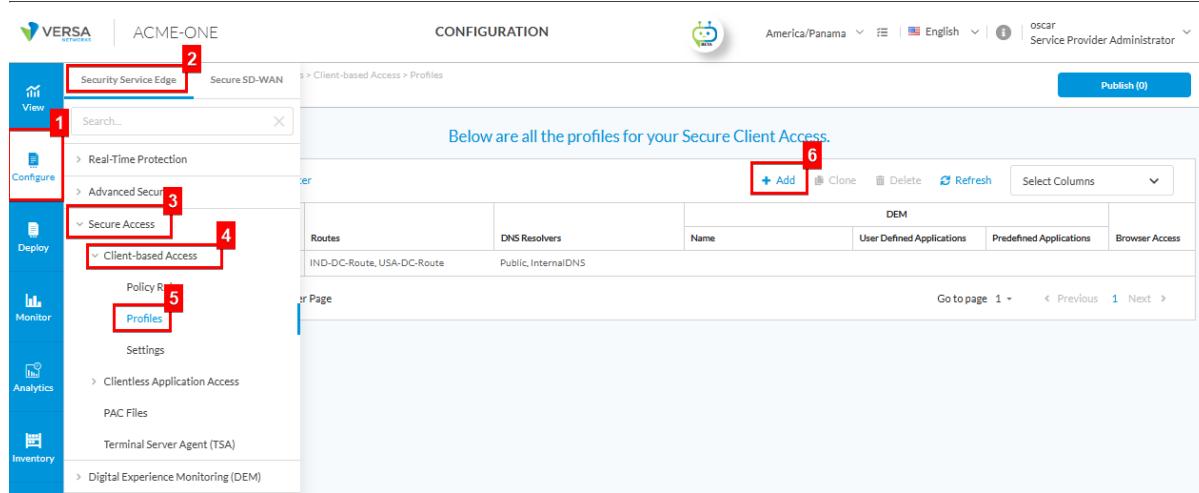
Application	Match Information	Risks	Productivity	Family	Sub Family	Security	SDWAN	General	Application Image	Tags
usa-apps	IP Prefix: 192.168.30.80/32 Host Pattern: usa-apps.acme-one.com Protocol: TCP Destination Port: 8000	1	5	business-system	standard	Sanctioned				USA
india-portal	IP Prefix: 192.18.50.18/32 Host Pattern: india-portal.acme-one.com Protocol: TCP Destination Port: 8000	1	5	business-system	standard	Sanctioned				India

#### Step 4: Secure Access Profile: Configure DNS Server

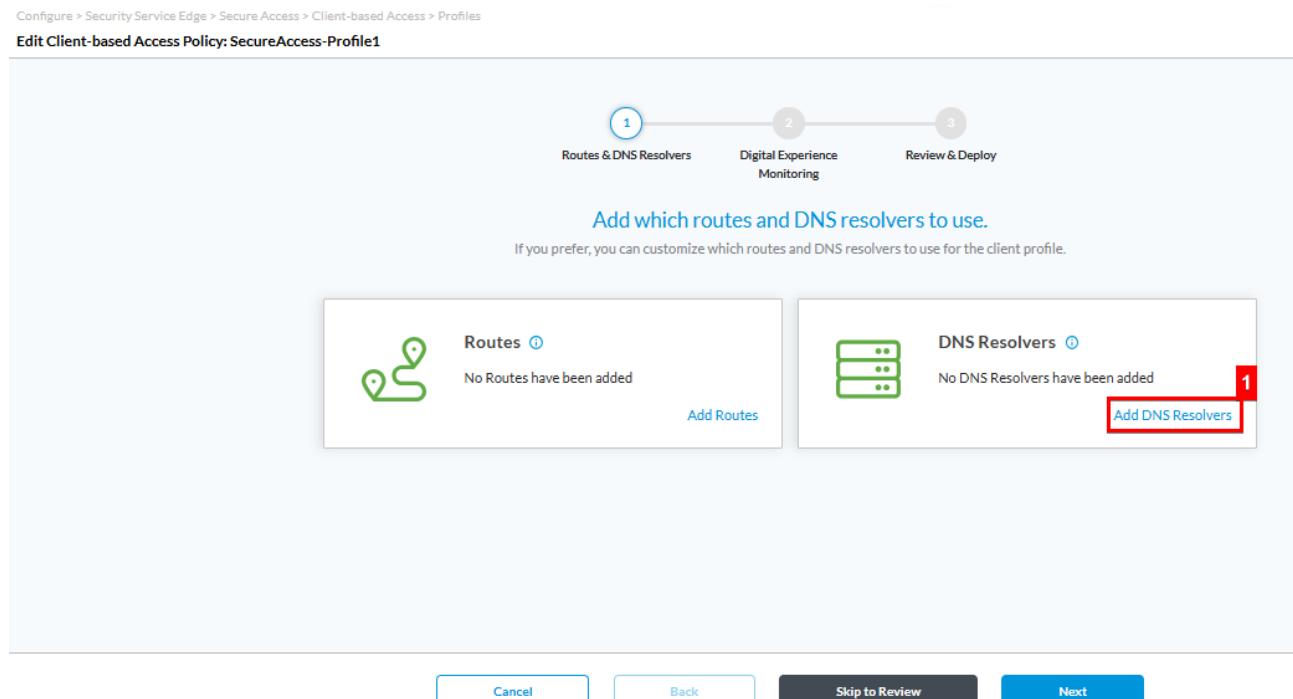
For the VSIA & VSPA setup, we need to configure the DNS server IP address without Domains. In this case, ACME-ONE uses public DNS server 8.8.8.8.

Note: **Secondary DNS Server** – It is recommended to configure one or more redundant DNS servers to ensure name resolution continuity in the event of a primary DNS server failure. In this configuration, a secondary DNS server is not defined because it is optional for this deployment scenario.

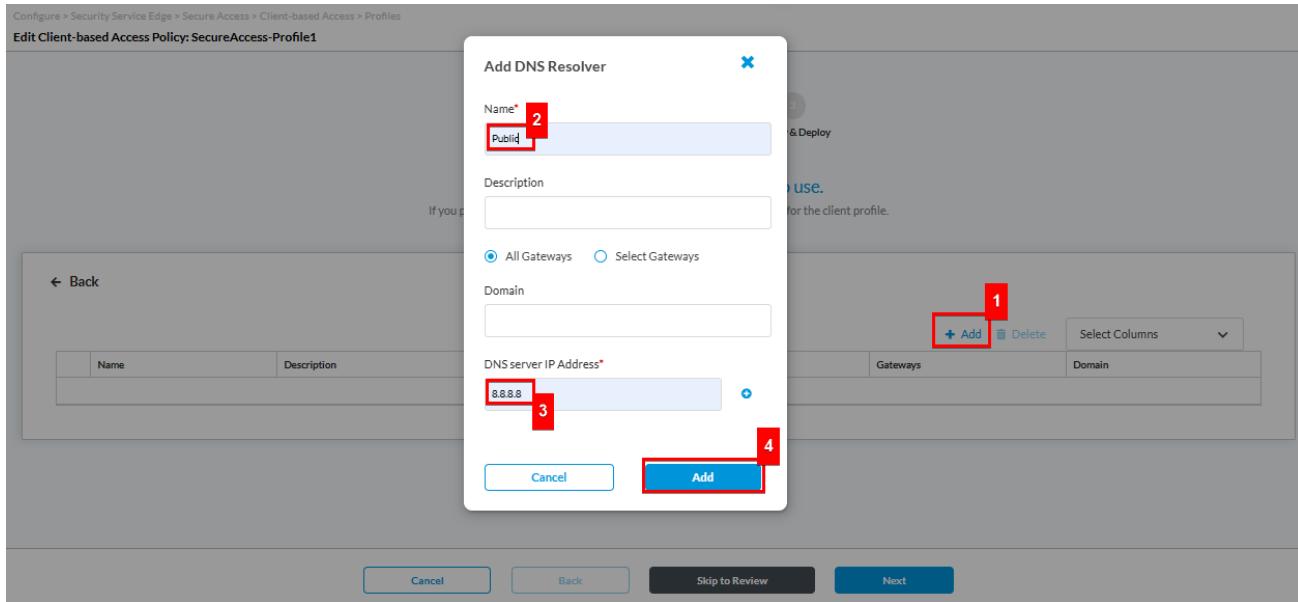
To create a Secure Access profile, navigate to **Configure > Security Service Edge > Secure Access > Client-based Access > Profiles** and click on **+Add** as shown in the figure below.



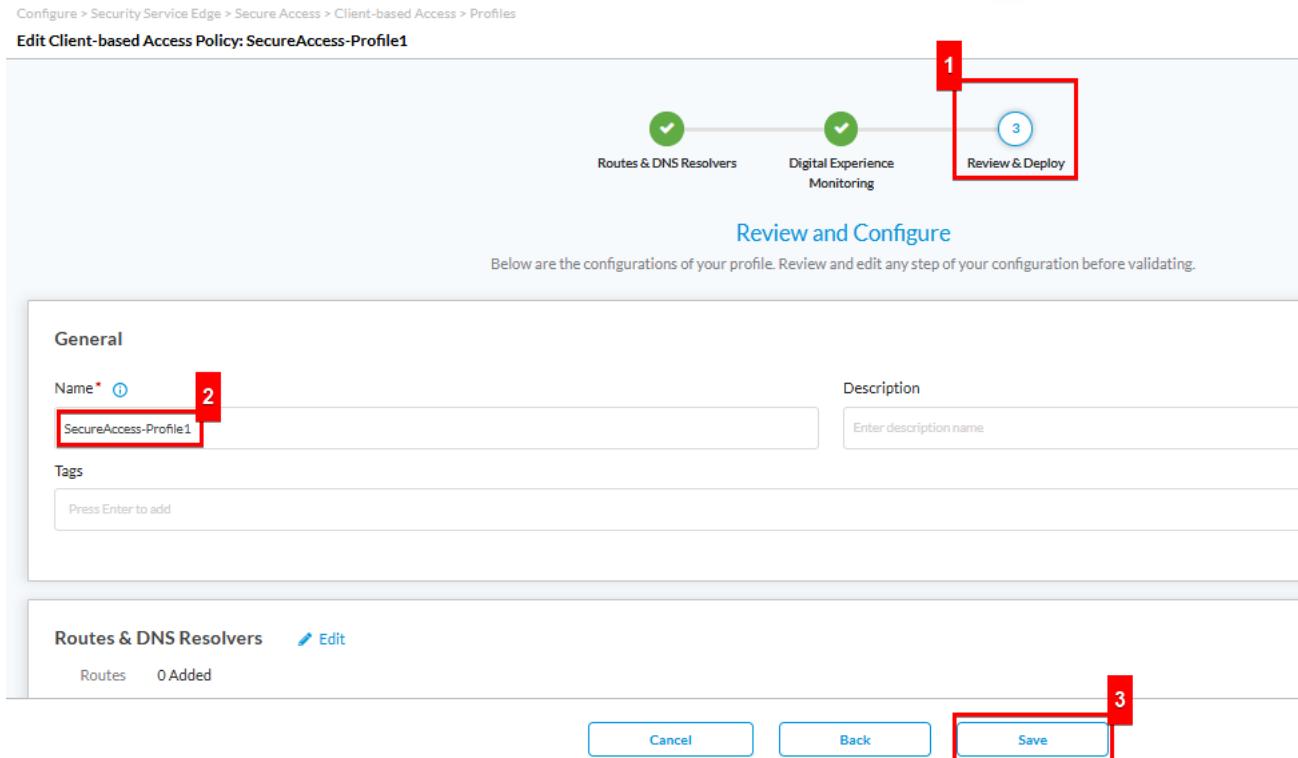
Click on **Add DNS Resolvers**



Insert the DNS information and click **Add**. Then click **Next** until Review & Deploy section.



Then click **Next** until **Review & Deploy** section. Add a descriptive **Name** and click **Save**.



## Step 5: Define Secure Access rules

In VSPA + VSIA setup, the SSE Gateway is the default gateway for private and public traffic.

When the users are working from home, all traffic is routed through the SSE Gateway but to meet the requirements of this case, the only exception will be conferencing applications traffic, which will be configured to break out locally.

When users are in the office, the Trusted Network Detection (TND) Gateway Assisted feature will be used to bypass private traffic locally and the remaining internet traffic will continue to be routed via the SSE gateway, including the same exception of conferencing application (Zoom).

The TND feature will be configured in the next step of this document.

To meet the requirements of this case; since only one level of users is being used for testing purposes, only one secure client access rule is needed to enable local breakout for conferencing application (Zoom), so that these applications are sent directly to the Internet without passing through the SASE gateways.

To configure navigate to **Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules** and click on **+Add**.

Operating System Versions	Users & Groups	Endpoint Posture	Traffic Action	VPN & Gateway Groups	Status	Last Modified By & Date
Windows Windows 10 Windows 10 Mobile Windows 11	MSentralID-OscarNuevo Users vip@oscarlabsbase.onmicrosoft.com remotevip@oscarlabsbase.onmicrosoft.com	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Managed Status of Devices All Devices No Client Applications selected Exclude PreDefined Applications Microsoft Office 365 Outlook.com Zoom	Send Apps to Versa Cloud VPN Name ACME-ONE-Enterprise Gateway Groups Default Global SageGWgroupACMEone Gateways SageGW2 SageGW1	Enabled	10/10/2025, 12:28:4 oscar

For this example, we are setting up the secure access rule according to these requirements:

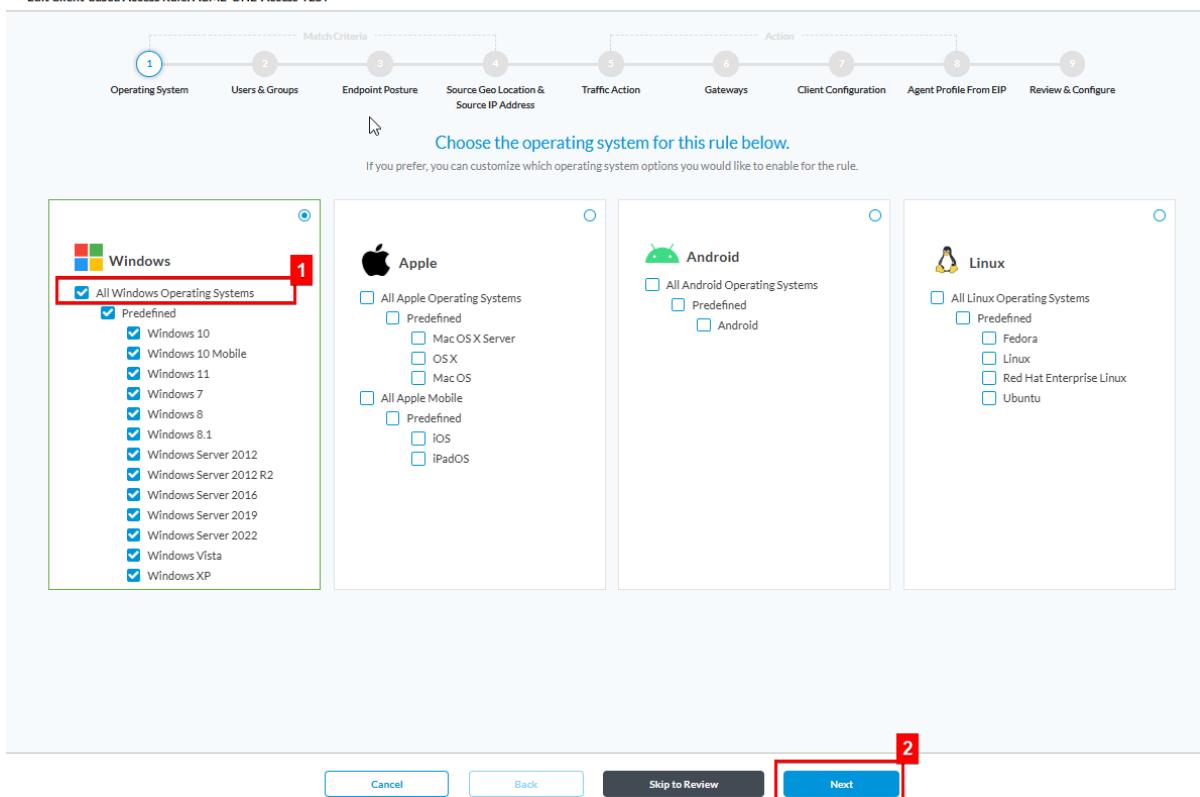
Knob	Current Use Case	Reason	Best Practice (Production)
<b>Operating Systems</b>	All Windows versions	Ensures compatibility with all Windows OS versions in the enterprise.	Limit to <i>supported/managed OS versions only</i> (e.g., Win11). Block EOL OS (Win7) to reduce risk.
<b>Users &amp; Groups</b>	All required user or groups (vip and remotevip)	Broad inclusion for testing.	Apply <b>least-privilege access</b> : segment users by role and sensitivity (e.g., Finance vs. Contractors). Specific

			rules for each user can also be considered if each user group has different access requirements, location etc.
<b>Endpoint Posture</b>	Management Status: All devices EIP Profile: no eip profile	No Enforcement required from the users devices.	Require managed devices and endpoint compliance where possible. Strengthens endpoint hygiene
<b>Source Geo Location</b>	All	No geo-restriction defined.	Restrict access to <b>approved geographies</b> where the company operates. Deny or challenge high-risk regions.
<b>Source IP Address</b>	None	As all users need this breakout	We can define an IP address to enforce the user connection from a specific location and a WAN circuit.
<b>Traffic Action</b>	Subscription: VSPA (Versa Secure Private Access) & VSIA (Versa Secure Internet Access)	Secure access to internal applications and secure internet traffic	Same as lab.
<b>Traffic Action</b>	Allow – Send Apps to Versa Cloud Gateway. Add Zoom to the applications	All traffic will go the gateways, but the applications added will bypass the tunnels.	Select approved applications that are trusted and need no enforcement to optimize their performance sending the traffic directly to the internet
<b>Gateways</b>	Select the gateways available for this tenant	Select the gateway that we want the user to connect to	Select gateways according to the type of user and the regional gateways that will serve them, ensuring that a redundant gateway is always included in the rule to guarantee high availability and low latency.
<b>Client Configuration</b>	Select the Secure Client Access Profile: SecureAccess-Profile1	Select the profile created in step 3	Same as lab
<b>MFA</b>	Disabled	Not required in the lab.	<b>Enable MFA</b> (Email or TOTP as per the requirement). Critical for Zero Trust.
<b>VPN Type</b>	IPsec	Flexibility during lab testing.	Define the order of preference (Recommended: DTLS > IPsec > TLS).
<b>Client Controls</b>	Default values	Defaults are sufficient for the lab use case.	Harden controls (Tamper Protection, Tunnel Monitoring, Always-On with Trusted Network Detection).
<b>EIP Agent Profile</b>	Blank	Optional in the lab.	To enforce real-time posture evaluation with EIP. Continuous evaluation is key for Zero Trust.

For this use case, select **All Windows** versions and then click **Next**.

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

Edit Client-based Access Rule: ACME-ONE-Access-TEST



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

**Windows**

All Windows Operating Systems

Predefined

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

**Apple**

All Apple Operating Systems

Predefined

- Mac OS X Server
- OSX
- Mac OS

All Apple Mobile

Predefined

- iOS
- iPadOS

**Android**

All Android Operating Systems

Predefined

**Linux**

All Linux Operating Systems

Predefined

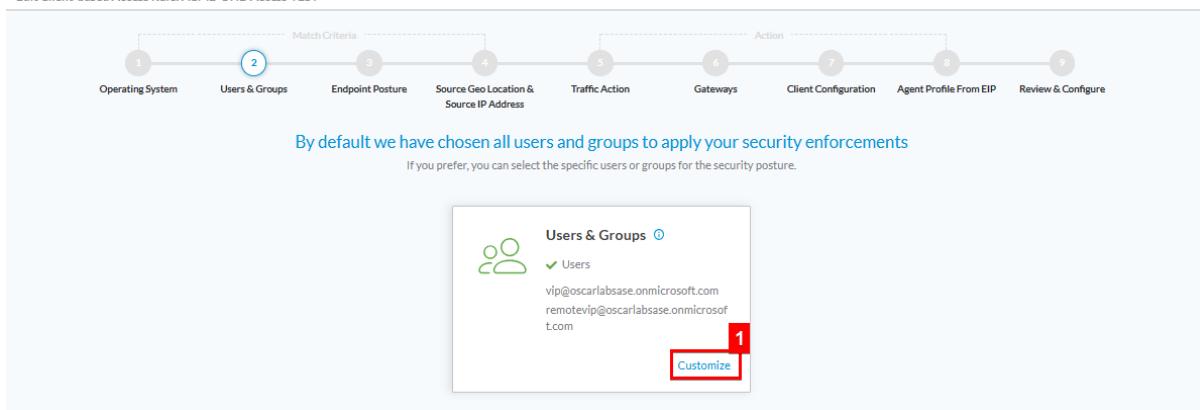
- Fedora
- Linux
- Red Hat Enterprise Linux
- Ubuntu

**Cancel** **Back** **Skip to Review** **Next** **2**

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

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

Edit Client-based Access Rule: ACME-ONE-Access-TEST



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**

Users

vip@oscarlabsase.onmicrosoft.com  
remotevip@oscarlabsase.onmicrosoft.com

**Customize** **1**

**Cancel** **Back** **Skip to Review** **Next** **2**

In the users and groups configuration, select the SAML authentication profile created before in step 2, Fill the name of users that need to use these specific applications, and then click Next. In this case, as an example we only used 2 users.

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

**Users & Groups**

User Type:  Selected Users  Known Users

Enable Rule for the following matched users or user groups:  
MSEntralID-OscarNuevo

User Groups:  Users (highlighted)

Search for Users:  (vip@oscarlabsbase.onmicrosoft.com) (remotevip@oscarlabsbase.onmicrosoft.com)  Search for Users

Users (2):

User Name	First Name	Last Name
<input checked="" type="checkbox"/> vip@oscarlabsbase.onmicrosoft.com	vip	-
<input checked="" type="checkbox"/> remotevip@oscarlabsbase.onmicrosoft.com	remotevip	-

Cancel Back Skip to Review Next (highlighted)

Then click Next until the **Traffic Action** section

For the traffic action configuration first select the Subscription type corresponding to your License, in this case **VSPA & VSIA**. Select **allow**, this action will send the matching traffic to the gateway, but the applications selected in the list bellow will be sent out directly to the internet. In this case **Zoom**. Then click **next**.

Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules  
Edit Client-based Access Rule: ACME-ONE-Access-TEST

Based on the most common secure enterprise settings, we've chosen the traffic steering below.  
If you prefer, you can customize which traffic steering option you would like to enable for the rule.

Select subscription type for users matching this rule.

Versa Secure Private Access (VSPA) & Versa Secure Internet Access (VSIA)

Deny  
Drop all traffic that matches the rule  
Display Message after Connection is Blocked  
You are not allowed to connect to the enterprise VPN, please contact administrator

Allow  
Allow all traffic that matches the rule to pass

Send Apps to Versa Cloud Gateway    Breakout To Internet

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

Display Message after Successful Connection

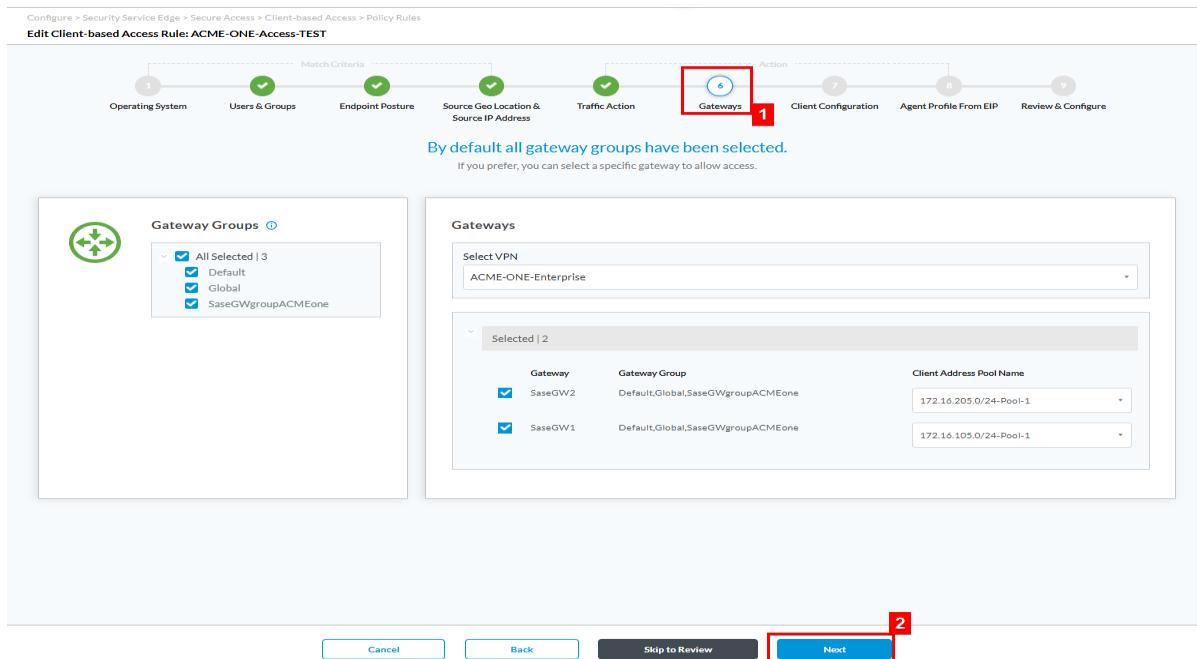
WELCOME ACME ONE

Search for Applications

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  
Edit Client-based Access Rule: ACME-ONE-Access-TEST



Match Criteria

Action

Gateways 1

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.

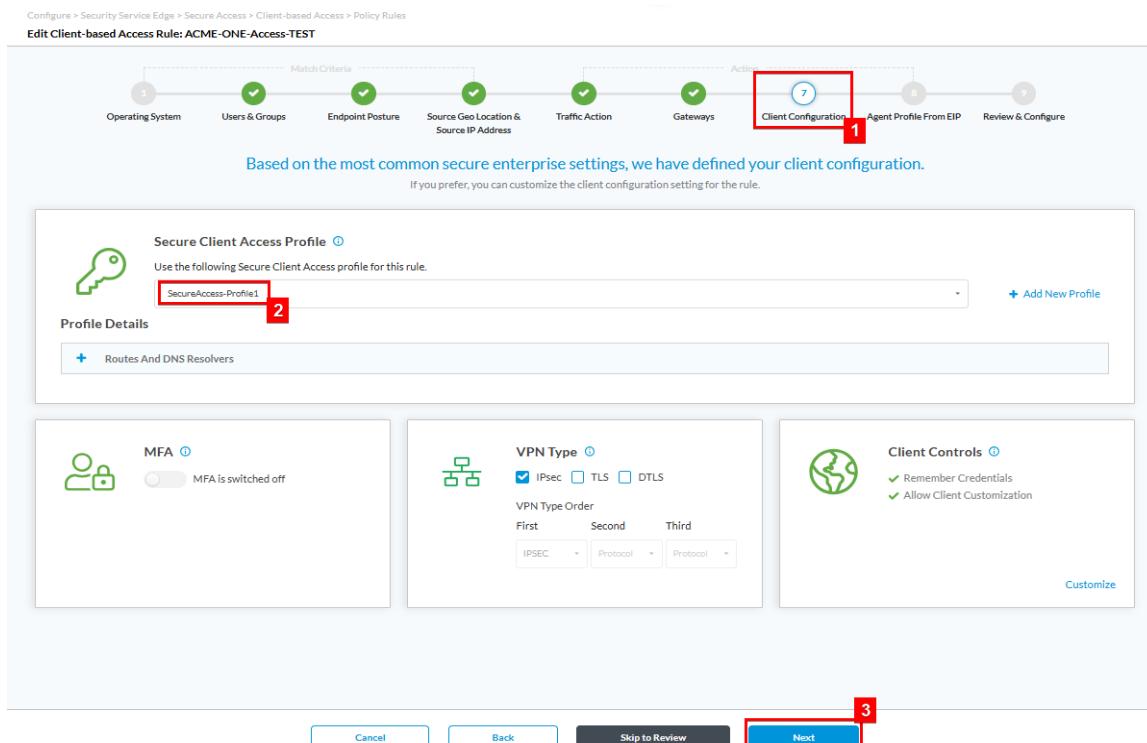
Gateway Groups 2

Gateways 3

Cancel Back Skip to Review Next

Select the **Secure Client Access Profile** to be used with this rule the click **Next**.

Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules  
Edit Client-based Access Rule: ACME-ONE-Access-TEST



Match Criteria

Action

Client Configuration 1

Agent Profile From EIP

Review & Configure

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

Secure Client Access Profile 2

SecureAccess-Profile1

+ Add New Profile

Profile Details

+ Routes And DNS Resolvers

MFA 3

MFA is switched off

VPN Type 4

VPN Type Order

First Second Third

IPSEC Protocol Protocol

Client Controls 5

Remember Credentials

Allow Client Customization

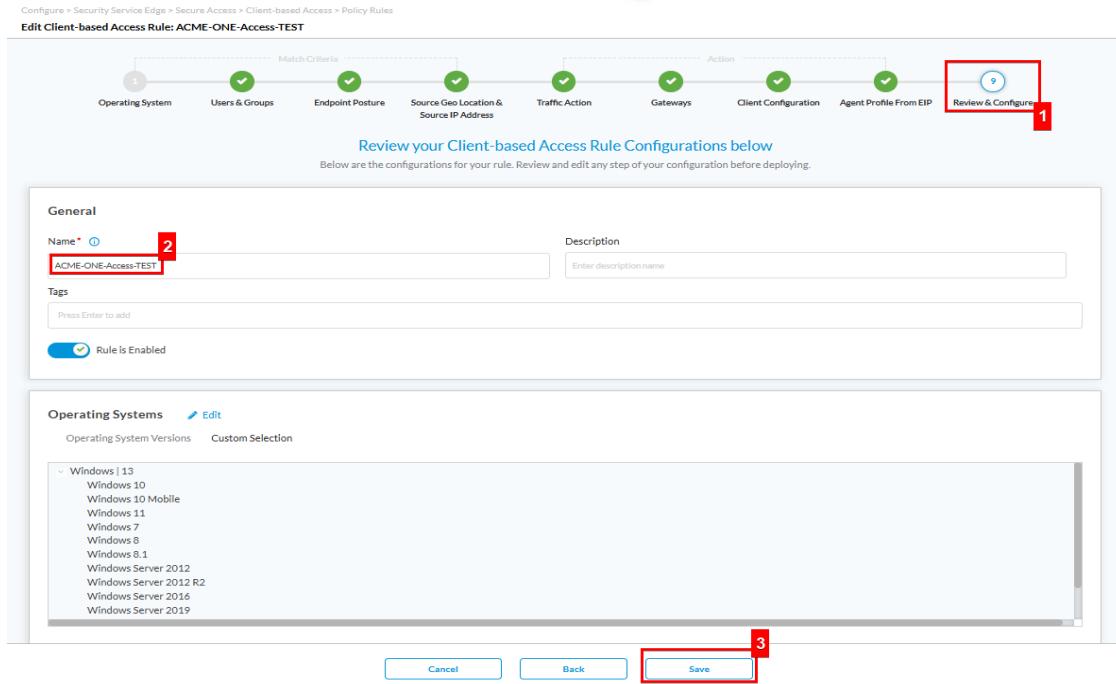
Customize

Cancel Back Skip to Review Next

Then click **Next** until **Review & Configuration** section and assign a descriptive **Name** for the Access Rule, if you need to verify you can scroll down and check the configuration. If it's required, you can edit the configuration again. Now click **Save**.

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

Edit Client-based Access Rule: ACME-ONE-Access-TEST



Match Criteria

Action

Review & Configure 1

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  2

Description

Tags

Rule Is Enabled

Operating Systems 3

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

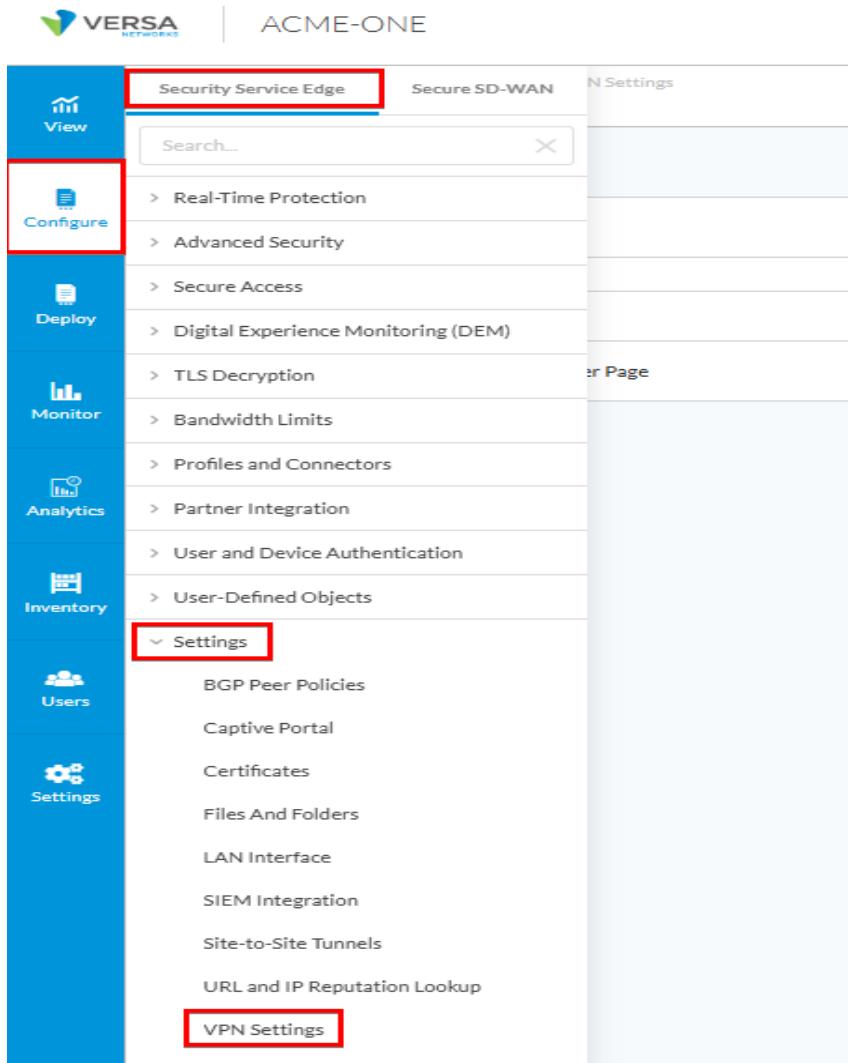
Define the rule to be evaluated first and click Save.

## Step 6: Trusted Network Detection: When the user is in the office

ACME-ONE can use this feature to bypass the SASE gateway when the SASE client is located behind their trusted network/corporate office. In this mode, the secure tunnel to the SASE gateway will not be formed when the SASE client is already behind a trusted network and instead uses the site-to-site connection to the Versa SASE gateways.

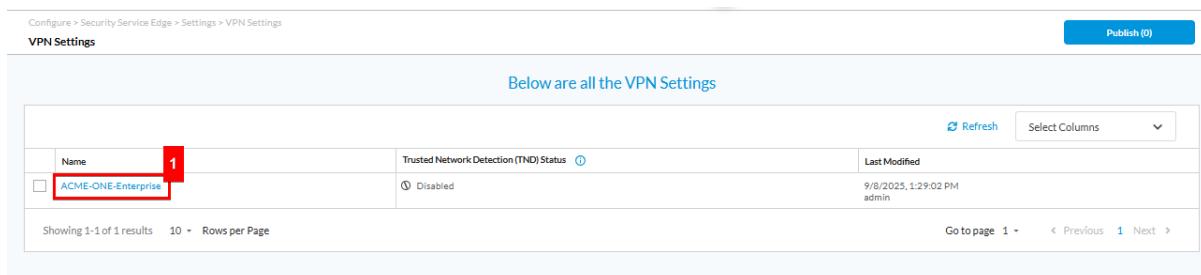
When the Versa SASE client initiates registration with the SASE Gateway, the gateway determines whether the client is in a trusted or untrusted network based on the IP address used to connect (private vs. public) and responds accordingly.

To Configure Trusted Network Detection – Gateway-Assisted, edit the already created VPN in **Configure > Security Service Edge > VPN Settings**.



The screenshot shows the VERSA Network Management Platform interface. The left sidebar has tabs: View, Configure (highlighted with a red box), Deploy, Monitor, Analytics, Inventory, Users, and Settings. The main content area shows the 'ACME-ONE' device. Under 'Security Service Edge', the 'VPN Settings' section is highlighted with a red box. The 'VPN Settings' section contains the following items: BGP Peer Policies, Captive Portal, Certificates, Files And Folders, LAN Interface, SIEM Integration, Site-to-Site Tunnels, URL and IP Reputation Lookup, and VPN Settings (highlighted with a red box).

Click on the VPN name to open and edit the settings



The screenshot shows the 'VPN Settings' page. The URL is 'Configure > Security Service Edge > Settings > VPN Settings'. The page title is 'VPN Settings'. The content area shows a table with the following data:

Name	Trusted Network Detection (TND) Status	Last Modified
ACME-ONE-Enterprise	Disabled	9/8/2025, 1:29:02 PM admin

Below the table, it says 'Showing 1-1 of 1 results' and 'Rows per Page'. At the bottom right, it says 'Go to page 1 < Previous 1 Next >'. There are 'Refresh' and 'Select Columns' buttons at the top right of the table.

Enable the Trusted mode with DNS Configuration. There is no need to add Domain Name Servers as these fields are used to add a DNS server to the SASE Gateways. Then click **Save**.

## Edit Settings for ACME-ONE-Enterprise



### Change TND Status

Enabling Gateway Assisted Trusted Network Detection (TND) requires creating Real-Time Protection Internet Protection rules when using external LDAP, SAML, or Radius User Authentication Profiles.

For example, when leveraging Azure Active Directory for SAML authentication, the relevant Microsoft applications (Microsoft and Windows Marketplace) and application groups (Office365-Apps) should be allowed for all users from the TND source zone(s) (i.e., site-to-site on premises to SASE Gateway tunnels) to the Internet destination zone.

Enabled

1

Domain Name Server

Configure name servers to resolve domain names by VOS in this VPN.

Primary IP Address	Secondary IP Address
Cancel	Save

2

Once the above configuration is saved, we need to Publish the configurations so that concerto derives the configuration to the SASE Gateways. The concerto portal **will not** request to publish.

Configure > Security Service Edge > Settings > VPN Settings								
VPN Settings								
Below are all the VPN Settings								
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 33%;">Name</th><th style="width: 33%;">Trusted Network Detection (TND) Status</th><th style="width: 33%;">Last Modified</th></tr> </thead> <tbody> <tr> <td>ACME-ONE-Enterprise</td><td>Enabled</td><td>10/20/2025, 9:15:12 AM oscar</td></tr> </tbody> </table>			Name	Trusted Network Detection (TND) Status	Last Modified	ACME-ONE-Enterprise	Enabled	10/20/2025, 9:15:12 AM oscar
Name	Trusted Network Detection (TND) Status	Last Modified						
ACME-ONE-Enterprise	Enabled	10/20/2025, 9:15:12 AM oscar						
Showing 1-1 of 1 results	10	Rows per Page						
<span style="border: 1px solid #0072bc; padding: 2px 5px; border-radius: 5px; color: #0072bc;">Publish (0)</span>	<span style="color: red; font-size: 2em;">1</span>	<span style="font-size: small;">Go to page 1 &lt; Previous 1 Next &gt;</span>						

Captive portal VR and Interface IP addresses are automatically populated with pre-defined configuration.

admin@SaseGW1:~> show interfaces brief   tab							admin@SaseGW1:~> show interfaces brief   tab						
NAME	MAC	OPER	ADMIN	TENANT	VRF	IP	NAME	MAC	OPER	ADMIN	TENANT	VRF	IP
eth-0/0	52:0:49:0b:07:01	up	up	0	global	10.73.107.7/16	eth-0/0	52:0:49:0b:07:01	up	up	0	global	10.73.107.7/16
eth-0/1	n/a	down	up	0	global	fe80::500a:49ff:fe0b:701/64	eth-0/1	n/a	up	up	0	global	fe80::500a:49ff:fe0b:701/64
lt-1/2.0	n/a	up	up	2	INET-Transport-VR	169.254.128.2/31	lt-1/2.0	n/a	up	up	2	INET-Transport-VR	169.254.128.2/31
lt-1/2.1	n/a	up	up	4	SASEDEM02-Enterprise	169.254.128.3/31	lt-1/2.1	n/a	up	up	4	SASEDEM02-Enterprise	169.254.128.3/31
lt-1/4.0	n/a	up	up	5	INET-Transport-VR	169.254.128.4/31	lt-1/4.0	n/a	up	up	5	INET-Transport-VR	169.254.128.4/31
lt-1/4.1	n/a	up	up	5	ACME-ONE-Enterprise	169.254.128.5/31	lt-1/4.1	n/a	up	up	5	ACME-ONE-Enterprise	169.254.128.5/31
lt-1/5.0	n/a	up	up	2	OscarLAB-Control-VR	10.30.0.4/32	lt-1/5.0	n/a	up	up	5	ACME-ONE-Enterprise-TNDNOB	169.254.64.0/31
ptv1025	n/a	up	up	2	SASEDEM02-Control-VR	10.30.0.2/32	ptv1025	n/a	up	up	5	ACME-ONE-Enterprise-TNDNOB	172.16.105.1/31
ptv1035	n/a	up	up	5	ACME-ONE-Control-VR	10.30.0.3/32	ptv1035	n/a	up	up	5	OscarLAB-Control-VR	10.30.0.3/32
ptv1036	n/a	up	up	5	ACME-ONE-Control-VR	10.30.0.4/32	ptv1036	n/a	up	up	5	ACME-ONE-Control-VR	10.30.0.4/32
tv1-0/2	n/a	up	up	2	OscarLAB-Control-VR	10.30.0.4/32	tv1-0/2	n/a	up	up	5	ACME-ONE-Enterprise	169.254.64.7/31
tv1-0/2.0	n/a	up	up	4	SASEDEM02-Control-VR	10.30.0.4/32	tv1-0/2.0	n/a	up	up	2	OscarLAB-Control-VR	10.30.0.4/32
tv1-0/22.0	n/a	up	up	4	SASEDEM02-Control-VR	10.30.0.4/32	tv1-0/22.0	n/a	up	up	4	SASEDEM02-Control-VR	10.30.0.4/32
tv1-0/23.0	n/a	up	up	4	SASEDEM02-Control-VR	10.30.0.5/32	tv1-0/23.0	n/a	up	up	5	OscarLAB-Control-VR	10.30.0.2/32
tv1-0/24	n/a	up	up	5	ACME-ONE-Control-VR	10.30.0.4/32	tv1-0/24	n/a	up	up	5	OscarLAB-Control-VR	10.30.0.4/32
tv1-0/24.0	n/a	up	up	5	ACME-ONE-Control-VR	10.30.0.4/32	tv1-0/24.0	n/a	up	up	4	SASEDEM02-Control-VR	10.30.0.4/32
tv1-0/25	n/a	up	up	5	ACME-ONE-Control-VR	10.30.0.5/32	tv1-0/25	n/a	up	up	5	SASEDEM02-Control-VR	10.30.0.4/32
tv1-0/25.0	n/a	up	up	5	ACME-ONE-Control-VR	10.30.0.5/32	tv1-0/25.0	n/a	up	up	5	ACME-ONE-Control-VR	10.30.0.5/32
tv1-0/3.0	n/a	up	up	2	OscarLAB-Control-VR	10.30.0.5/32	tv1-0/24	n/a	up	up	5	ACME-ONE-Control-VR	10.30.0.4/32
tv1-0/6002	n/a	up	up	2	INET-Transport-VR	169.254.0.2/31	tv1-0/25	n/a	up	up	5	ACME-ONE-Control-VR	10.30.0.5/32
tv1-0/603	n/a	up	up	5	INET-Transport-VR	169.254.0.2/31	tv1-0/25.0	n/a	up	up	5	ACME-ONE-Control-VR	10.30.0.5/32
tv1-1/103.0	n/a	up	up	2	OscarLAB-LAN-VR	169.254.0.3/31	tv1-0/26	n/a	up	up	2	OscarLAB-Control-VR	10.30.0.5/32
tv1-1/104	n/a	up	up	4	SASEDEM02-Enterprise	172.16.100.0/32	tv1-0/26.0	n/a	up	up	5	INET-Transport-VR	169.254.0.2/31
tv1-1/104.0	n/a	up	up	5	ACME-ONE-Enterprise	172.16.105.0/32	tv1-0/602	n/a	up	up	5	INET-Transport-VR	169.254.0.2/31
							tv1-0/603	n/a	up	up	2	OscarLAB-LAN-VR	169.254.0.3/31
							tv1-0/603.0	n/a	up	up	2	OscarLAB-LAN-VR	169.254.0.3/31

Now a DNS entry should be created for the FQDN portal domain to resolve the TNDNOB private ip.

In this case,

1

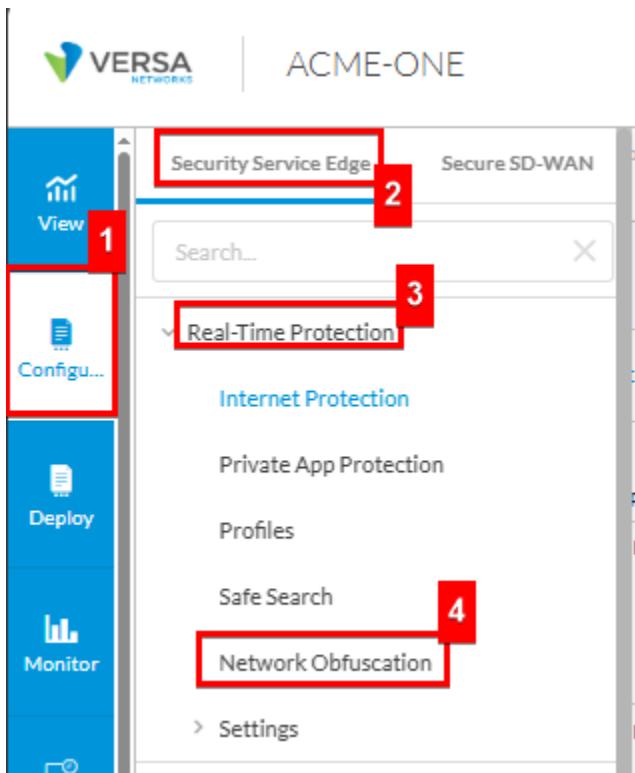
Domain Name	FQDN	IP Address
Portal	acme-one.versanow.net	172.16.105.1
Group	acme-one-sasegwgroupacmeone.versanow.net	172.16.105.1
Gateway	acme-one-sasegw1.versanow.net	172.16.105.1

## Step 7: DNS Proxy for Private Domain Resolution

When users are working from home with VSIA+VSPA, client DNS routes point to the SASE Gateways. This organization has internal applications and services that require customized DNS handling. To meet the requirements of this scenario, we need to configure selective DNS requests to be forwarded through a DNS proxy to the corporate DNS. All other external DNS queries, such as those for websites or cloud services, can be sent to the global DNS server for standard resolution.

This example explains how to configure a DNS proxy with network obfuscation for Versa SASE client.

Go to **Configure > Security Service Edge > Real-Time Protection > Network Obfuscation**.



Go to **Application Obfuscation** tab and then slide the toggle to Enabled. Then click **+ Obfuscate Applications**.

Configure > Security Service Edge > Real-Time Protection > Network Obfuscation

Network Obfuscation

Application Obfuscation

Enable Network Obfuscation

+ Obfuscate Applications

In the Obfuscate Applications screen, make sure the tenant is selected and enter a regex pattern for customer private domains/app in **+Add New Application**.

## Obfuscate Applications



Add applications you want to obfuscate.

Traffic Source 1

Private Applications with Host Pattern 2 + Add New Application

Search or select one or more private applications with Host Pattern

Resolvers

Enter one or more resolver IP address

Do not Obfuscate these applications

+ Add another application group

Cancel
Add

We will add the pattern of the private domain **.\*acme-one.com** and then click **Next**.

1 Match Criteria

IP Prefix

Host Pattern 1

Protocol  Source Port  Destination Port

Precedence

Cancel
Next 2

In **Application Attributes** a tag is necessary, we used Business and click **Next**.

## Create Application

Match Criteria

Application Attributes 1

**Risk**  
Each application has been assessed and assigned a risk level (1 = lowest to 5 = highest) by the Versa Networks security research team. The number in each card indicates applications with the same risk.

Level 1 (Lowest Risk) 2

Level 2 (Low Risk)

Level 3 (Medium Risk)

Level 4 (High Risk)

Level 5 (Highest Risk)

**Family**

- Business-system
- Media
- Collaboration
- Networking
- General-Internet

**Sub Family**

- Antivirus
- Application-service
- Audio-Video
- Authentication
- Behavioral
- Compression
- Database
- Encrypted
- Encrypted-tunnel
- Microsoft-office
- Middleware
- Network-management
- Network-service
- Peer-to-peer
- Printer
- Routing
- Security-service
- Standard
- Telephony

**Application Tags - Security**

- Anonymizer
- Bandwidth
- Dataleak
- Evasive
- Filetransfer
- Malware
- Misused
- Sanction State Uncategorized
- Sanctioned
- Tunnel
- Unsanctioned
- Vulnerable

**Application Tags - SDWAN**

- Audio Stream
- Data
- AV 2
- IPS
- Non Business
- Cloud
- Video Stream

**Application Tags - General**

- AAA
- Cloud Services
- IoT
- Update

Define the **Name** for the added application domains/URL.

## Create Application

Match Criteria

Application Attributes

Name, Description, Tags & Application Image 3

Name\* 1

PRIVATE-APP-URL

Description

Tags

Press Enter to add

Upload Application Image (Optional)

Add

File formats: png & svg

Cancel 2 Save

Select the created Application. The resolver would be the internal DNS server that can resolve private domains. Set "Do not obfuscate" and "add another application group"

## Obfuscate Applications



Add applications you want to obfuscate.

Traffic Source

Private Applications with Host Pattern

[+ Add New Application](#)

1  X

2  X

3  Do not Obfuscate these applications

4 [+ Add another application group](#)

[Cancel](#) [Add](#)

Do not define any application, so the rest of the domains are matched, and DNS resolver is defined as the public DNS. Then click **Add**.

## Obfuscate Applications



ACME-ONE-Enterprise

Private Applications with Host Pattern + Add New Application

Resolvers + Add New Application

Enter one or more resolver IP address

Do not Obfuscate these applications

Private Applications with Host Pattern + Add New Application

Search or select one or more private applications with Host Pattern

Resolvers + Add New Application  1

Enter one or more resolver IP address + Add New Application  2

Do not Obfuscate these applications + Add New Application  3

Cancel Add

Now set Enable Network Obfuscation and click Save

Configure > Security Service Edge > Real-Time Protection > Network Obfuscation Publish (0)

Network Obfuscation

Application Obfuscation + Obfuscate Applications

Obfuscate the IP addresses of private applications. When a user tries to resolve the FQDN of a private application, the SSE GW will respond with a resolved IP address randomly allocated from a private pool. When the user's traffic to the application reaches the SSE GW, the destination address is replaced with the real IP address of the private application.

Enable Network Obfuscation 1

Obfuscated Applications (1)

Traffic Source	Private Applications	Resolvers	Obfuscated
<input type="checkbox"/> ACME-ONE-Enterprise	<input type="text" value="PRIVATE-APP-URL"/>	<input type="text" value="192.168.15.53"/> <input type="text" value="8.8.8.8"/>	No

Showing 1-1 of 1 results 10 Rows per Page Go to page 1

Cancel Save 2

## Step 8: Enforce TLS Policies: Do-Not-Decrypt for Health/Finance | Decrypt the rest.

In this scenario to maintain user privacy and comply with regulations:

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

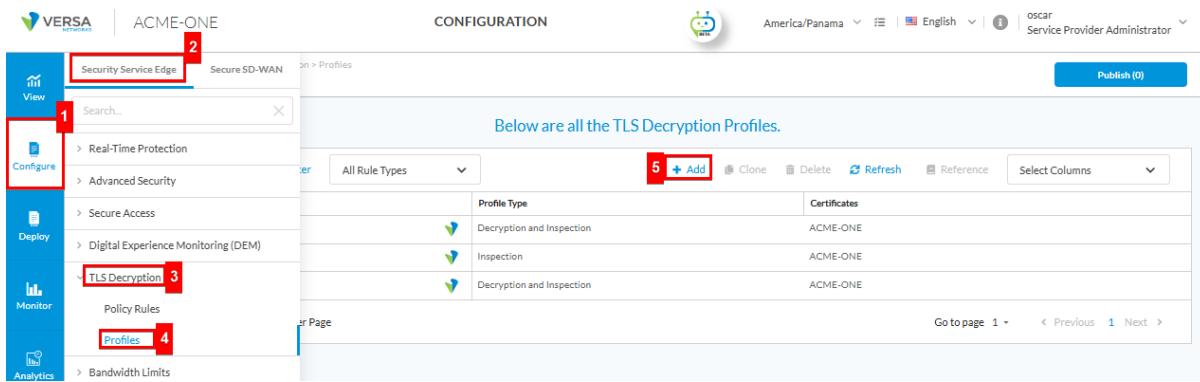
The required information to complete the configuration is in the next list.

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

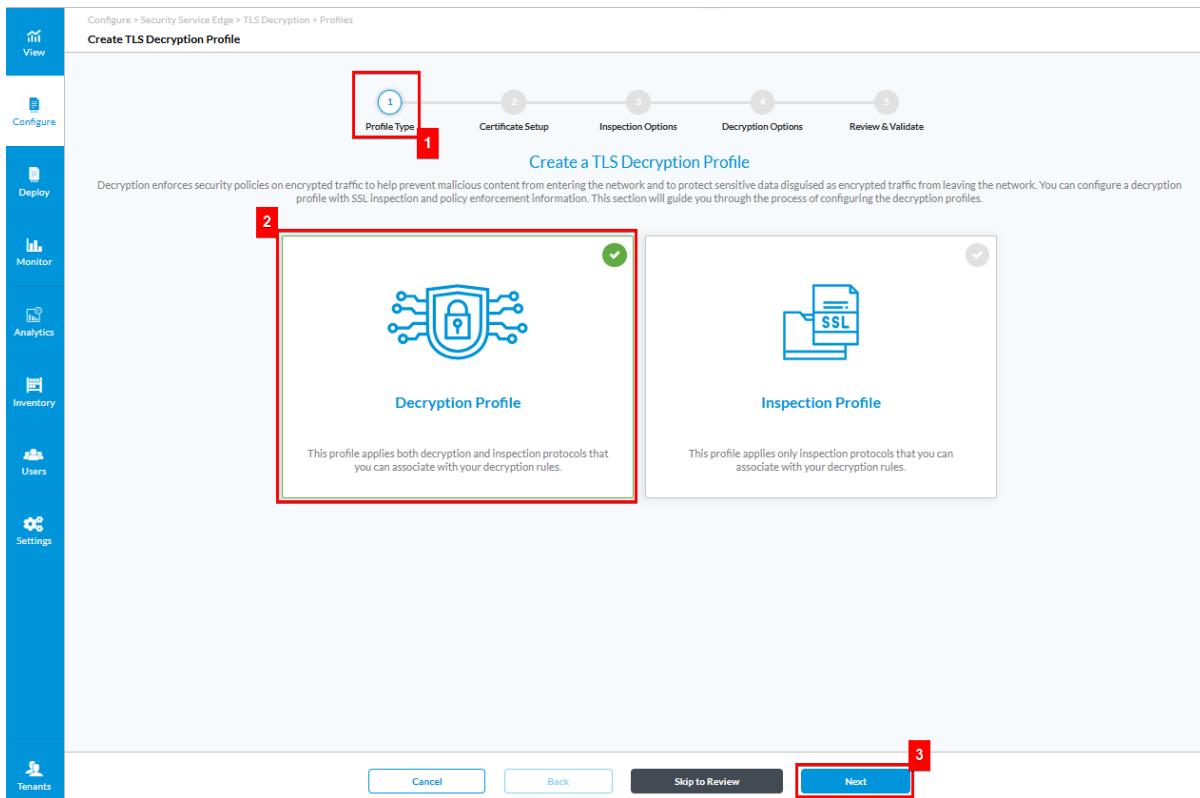
Versa includes some predefined profiles you can use, but if some specific/custom profile is required, please follow the steps listed below to create a new one.

To meet the requirements on this scenario we will need to configure

Configure TLS decryption, first create a decryption profile in **Configure > Security Service Edge > TLS Decryption > Profiles > +Add**.



For this case choose **Decryption Profile**



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

Configure &gt; Security Service Edge &gt; TLS Decryption &gt; Profiles

## Create TLS Decryption Profile

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

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

Previously Uploaded Certificates

ACME-ONE 2

+ Add New

**Details**

Name: ACME-ONE  
File Name: ACME-ONE.zip  
key: ACME-ONE.key  
Certificate: ACME-ONE.crt  
Issued To: VOS Certificate  
Issued By: Versa Concerto Certificate Authority  
Validity: 2025-09-08 11:26:15 to 2030-09-07 11:26:15

Download Certificate

Cancel Back Skip to Review Next 3

Enable OSCP Verification and blocking Unknown Certificates, now scroll down.

Configure &gt; Security Service Edge &gt; TLS Decryption &gt; Profiles

## Create TLS Decryption Profile

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.

1 **Verify with OCSP** 2 **Block Unknown Certificates**

Block SSL sessions whose certificate status is unknown.

Response timeout(seconds) for an OCSP request Verify 5 Server and Client

**Server Certificate Actions**

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

When the certificate expires, do the following:

Alert

Cancel Back Skip to Review Next

Block Expired and Unknown Certificates and Alert Unsupported Key Lengths, Unsupported Cipher and Unsupported Protocol Version. Then click Next.

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

**Server Certificate Actions** ①

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** ②

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

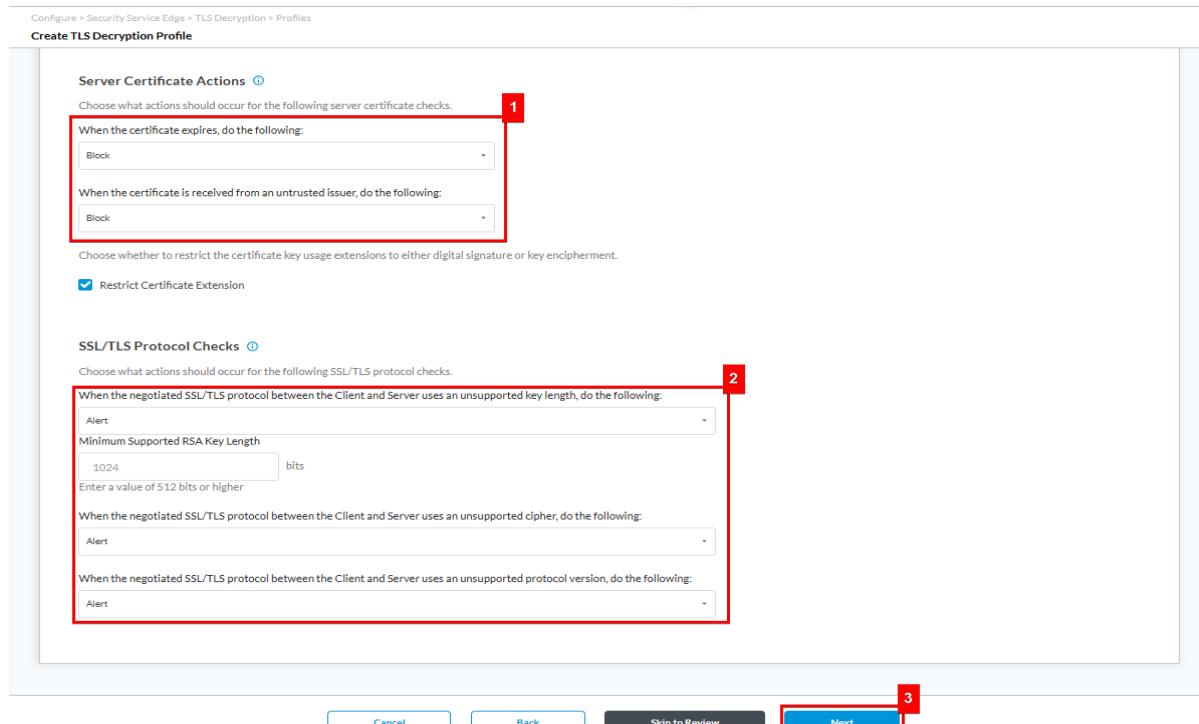
When the negotiated SSL/TLS protocol between the Client and Server uses an unsupported cipher, do the following:

Alert

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

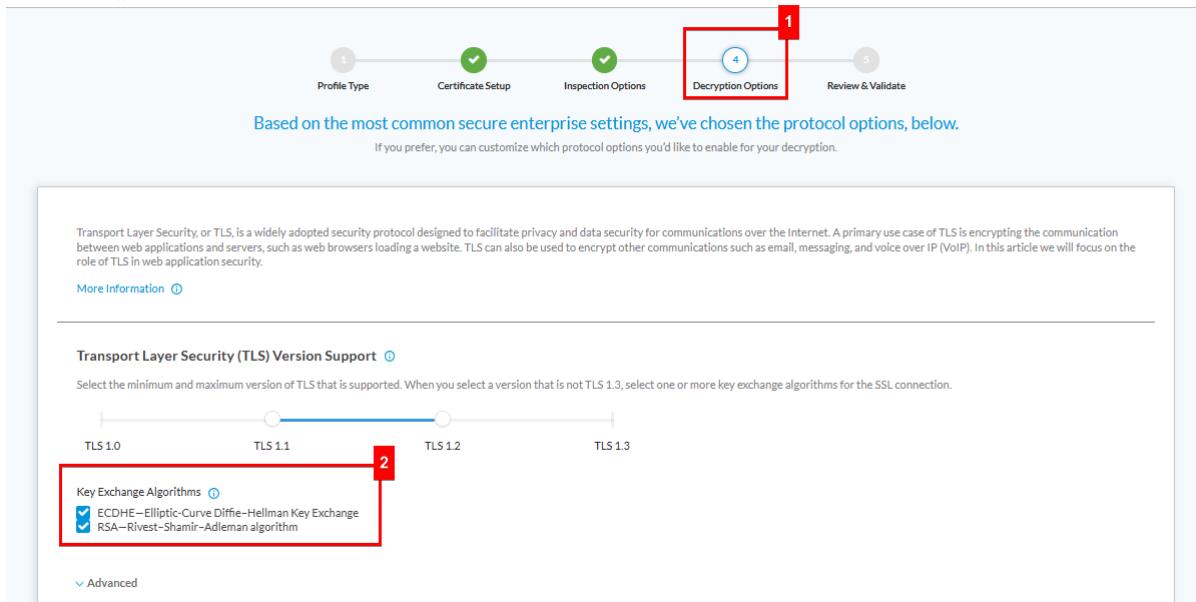
Alert

Cancel Back Skip to Review **Next** ③



Select Key Exchange Algorithms, choose Encryption and Authentication Algorithms, now scroll down.

## Create TLS Decryption Profile



Based on the most common secure enterprise settings, we've chosen the protocol options, below.

If you prefer, you can customize which protocol options you'd like to enable for your decryption.

Transport Layer Security (TLS) Version Support

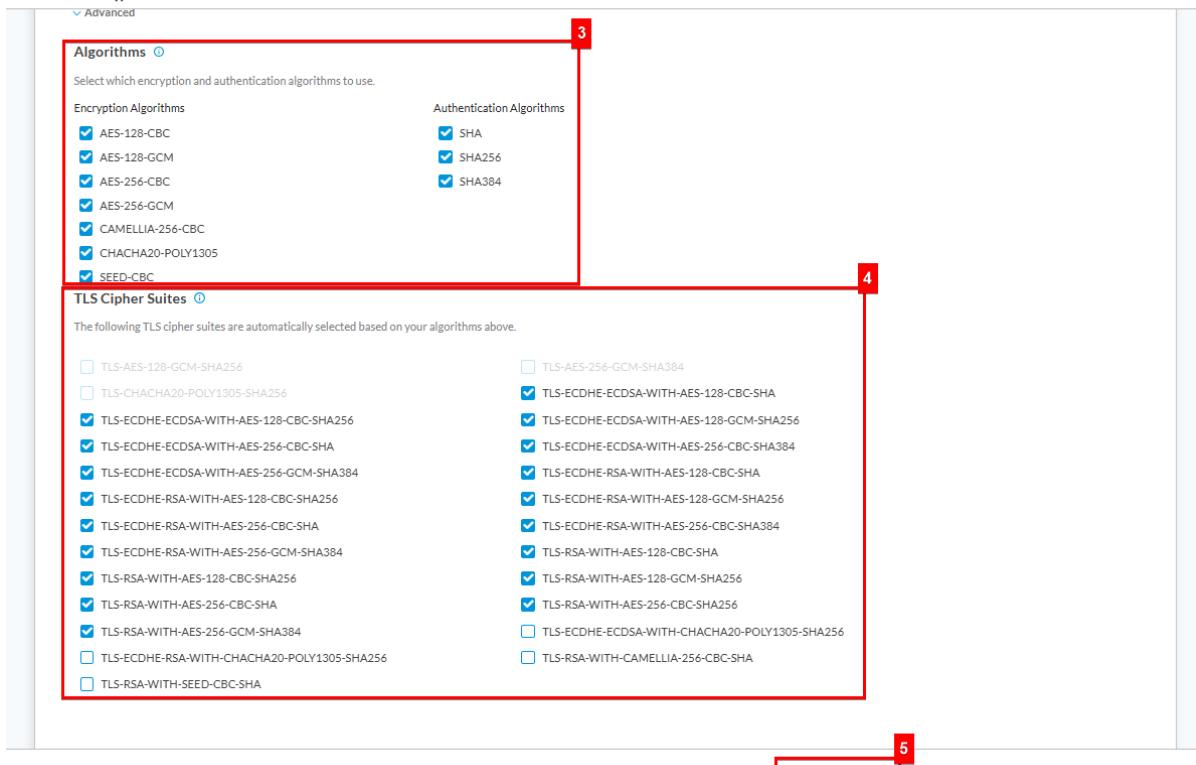
Select the minimum and maximum version of TLS that is supported. When you select a version that is not TLS 1.3, select one or more key exchange algorithms for the SSL connection.

Key Exchange Algorithms

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

Advanced

## Create TLS Decryption Profile



Algorithms

Select which encryption and authentication algorithms to use.

Encryption Algorithms	Authentication Algorithms
<input checked="" type="checkbox"/> AES-128-CBC	<input checked="" type="checkbox"/> SHA
<input checked="" type="checkbox"/> AES-128-GCM	<input checked="" type="checkbox"/> SHA256
<input checked="" type="checkbox"/> AES-256-CBC	<input checked="" type="checkbox"/> SHA384
<input checked="" type="checkbox"/> AES-256-GCM	
<input checked="" type="checkbox"/> CAMELLIA-256-CBC	
<input checked="" type="checkbox"/> CHACHA20-POLY1305	
<input checked="" type="checkbox"/> SEED-CBC	

TLS Cipher Suites

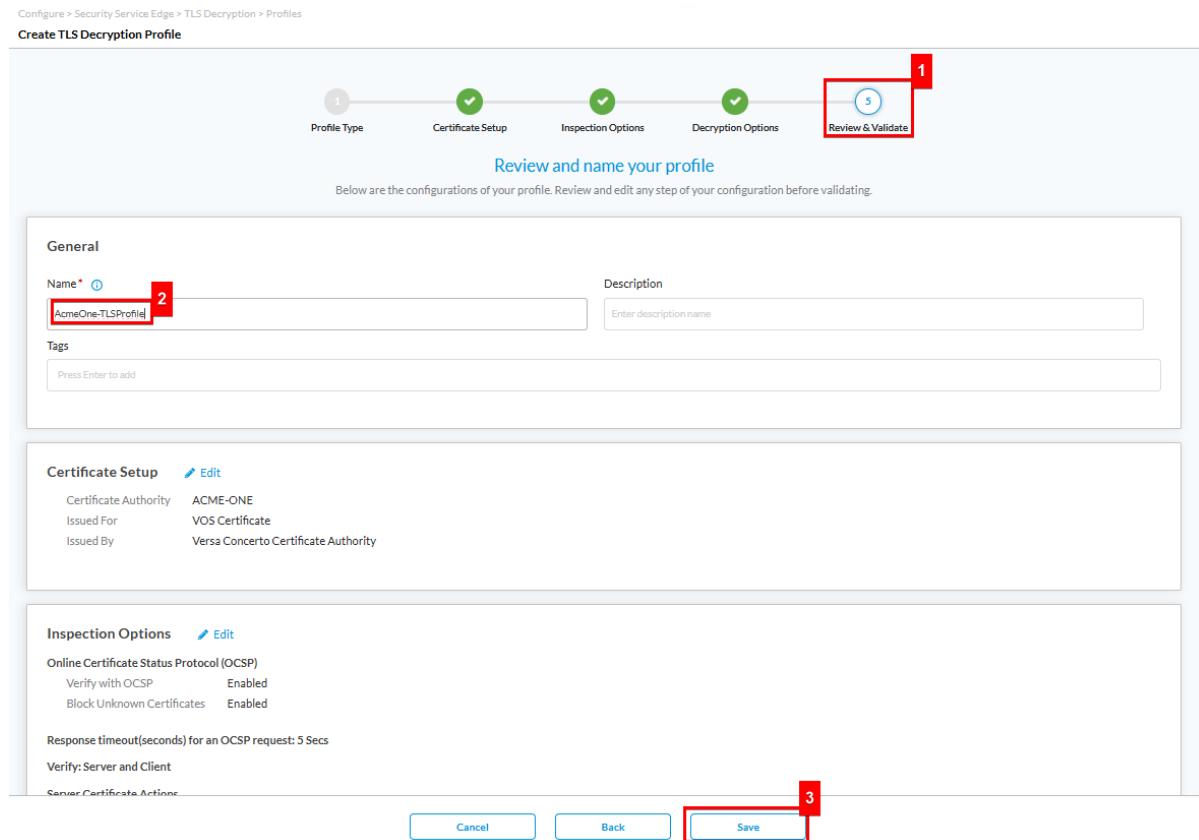
The following TLS cipher suites are automatically selected based on your algorithms above.

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

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

Configure > Security Service Edge > TLS Decryption > Profiles

Create TLS Decryption Profile



Review and name your profile

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

**General**

Name\*  2

Description

Tags

**Certificate Setup**

Certificate Authority: ACME-ONE  
Issued For: VOS Certificate  
Issued By: Versa Concerto Certificate Authority

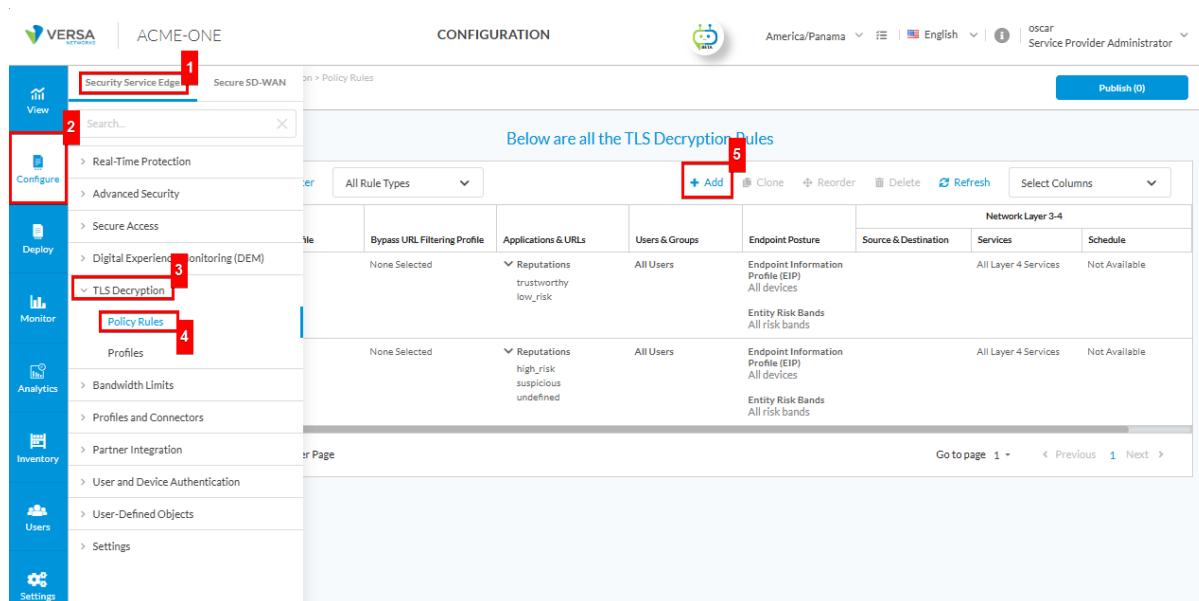
**Inspection Options**

Online Certificate Status Protocol (OCSP)  
Verify with OCSP: Enabled  
Block Unknown Certificates: Enabled

Response timeout(seconds) for an OCSP request: 5 Secs  
Verify: Server and Client  
Server Certificate Actions

3

Now, to create the 2<sup>nd</sup> rule to avoid Health and Financial URLs to be decrypted, go to **Configure > Security Service Edge > TLS Decryption > Policy Rules**, Then Click **Add** to create a new TLS Decryption Policy Rule.



ACME-ONE

CONFIGURATION

Secure SD-WAN

Below are all the TLS Decryption Rules

Profile	Bypass URL Filtering Profile	Applications & URLs	Users & Groups	Endpoint Posture	Network Layer 3-4
None Selected	▼ Reputations trustworthy low_risk	All Users	Endpoint Information Profile (EIP) All devices	All Layer 4 Services	Not Available
None Selected	▼ Reputations high_risk suspicious undefined	All Users	Endpoint Information Profile (EIP) All devices	All Layer 4 Services	Not Available

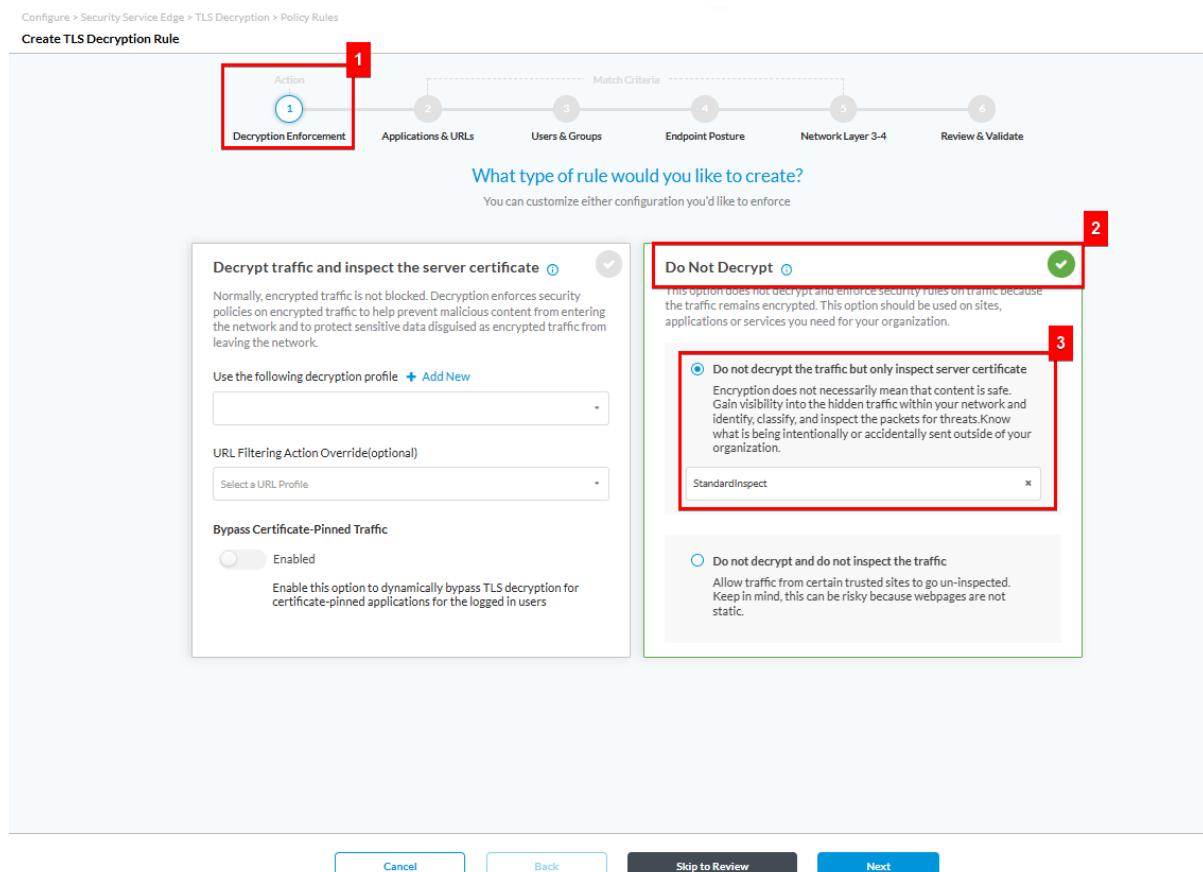
Page: 1 of 1

Go to page: 1 | < Previous | Next >

Select **Do Not Decrypt** Option and the option to Inspect Certificates with the **Standard Inspect** Profile, Then Click **Next**.

Configure > Security Service Edge > TLS Decryption > Policy Rules

Create TLS Decryption Rule



What type of rule would you like to create?

You can customize either configuration you'd like to enforce

**Decrypt traffic and inspect the server certificate**

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

Use the following decryption profile [+ Add New](#)

URL Filtering Action Override(optional)

Bypass Certificate-Pinned Traffic

Enabled

Enable this option to dynamically bypass TLS decryption for certificate-pinned applications for the logged in users

**Do Not Decrypt**

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

Do not decrypt the traffic but only inspect server certificate

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

Do not decrypt and do not inspect the traffic

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

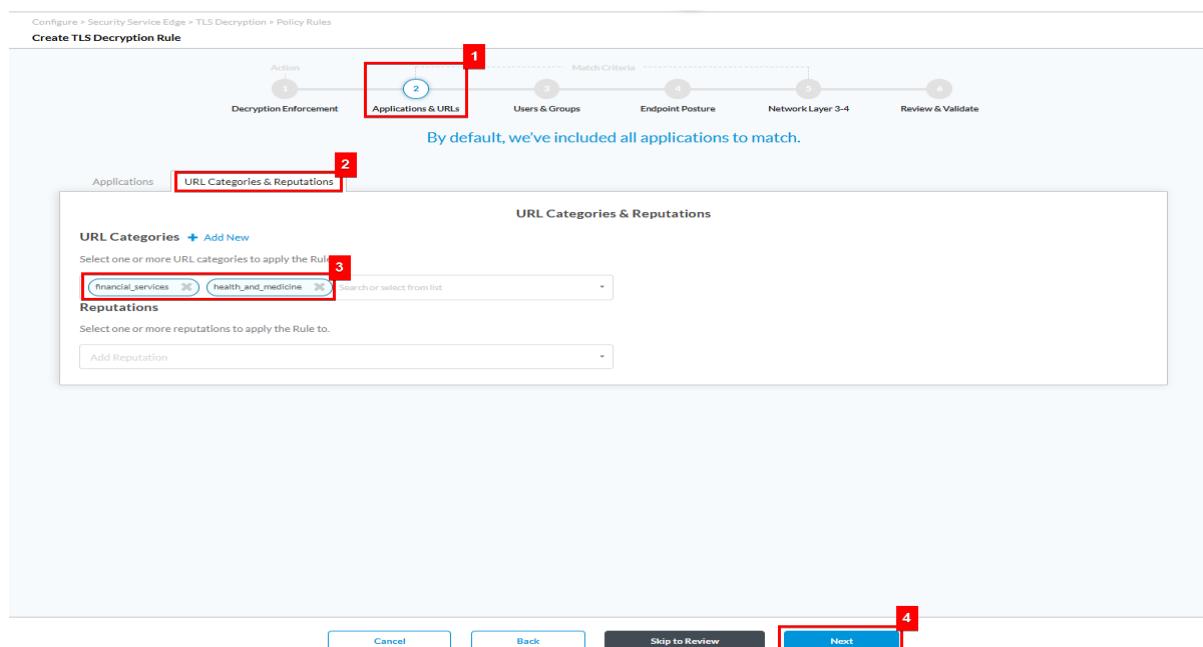
StandardInspect

Cancel Back Skip to Review Next

From **URLs Categories and Reputations**, search for **financial\_services** and **health\_and\_medicine** categories, then Click **Next**.

Configure > Security Service Edge > TLS Decryption > Policy Rules

Create TLS Decryption Rule



Action

Decryption Enforcement

Applications & URLs

Users & Groups

Endpoint Posture

Network Layer 3-4

Match Criteria

Review & Validate

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

**URL Categories & Reputations**

**URL Categories** [+ Add New](#)

Select one or more URL Categories to apply the Rule.

financial\_services  health\_and\_medicine [Search or select from list](#)

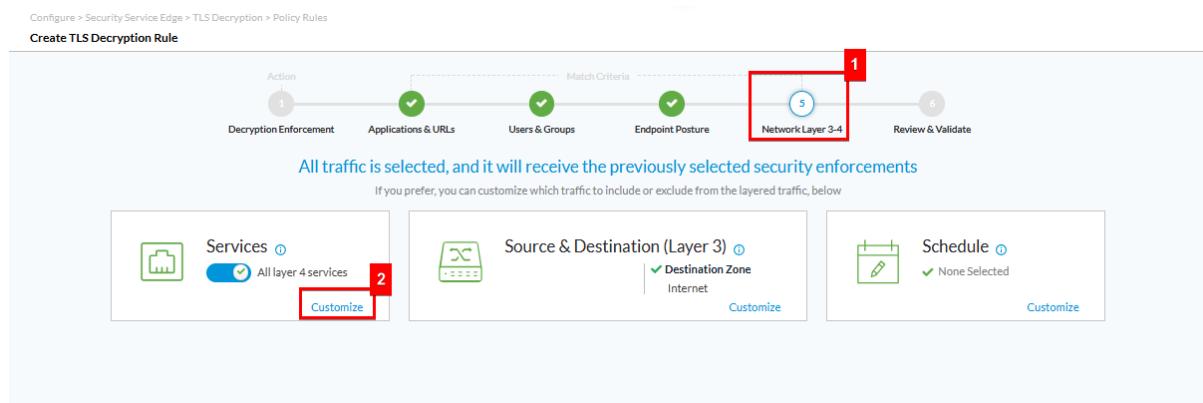
**Reputations**

Select one or more reputations to apply the Rule to.

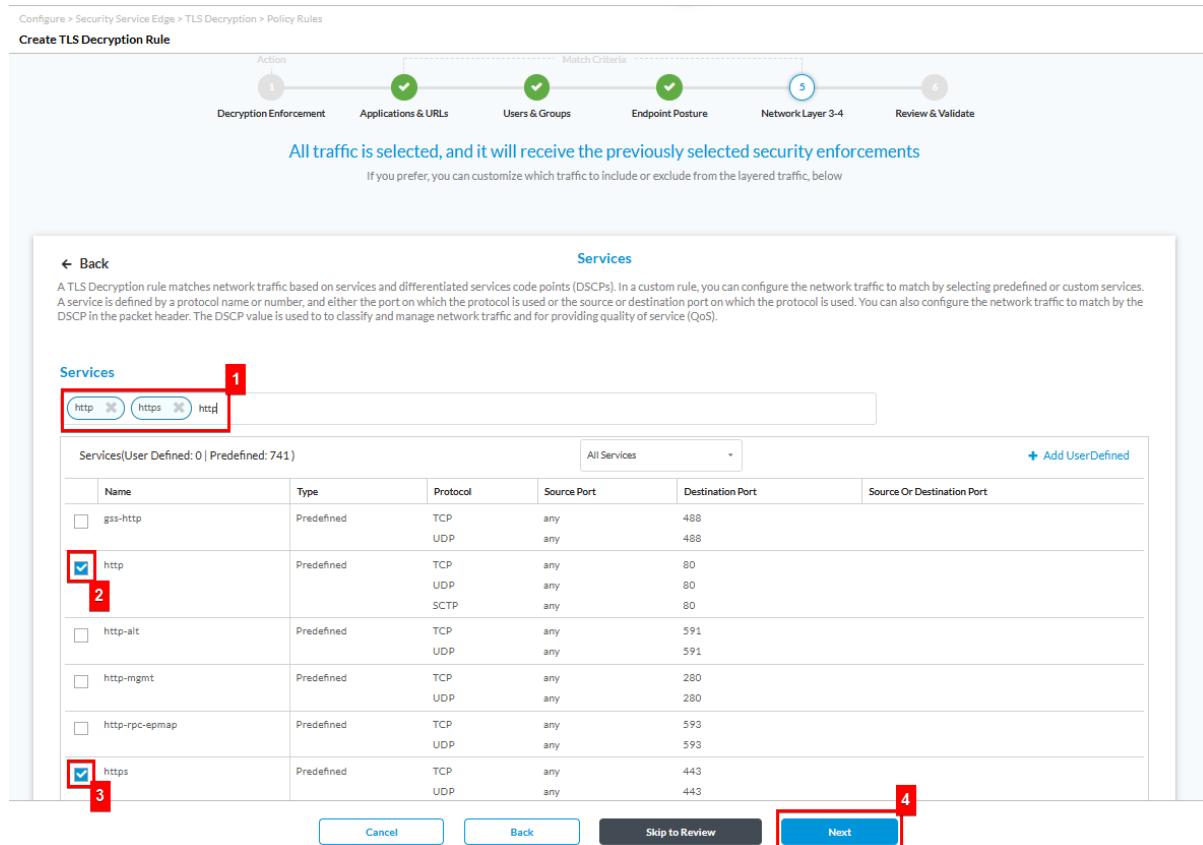
[Add Reputation](#)

Cancel Back Skip to Review Next

Click **Next** in **Users & Groups** and in **Endpoint Posture**, until you reach **Network Layer 3-4**. Click on **Customize** in section **Services**.



Look for http and add services **http** and **https** to avoid resources consumption looking for other services. Then Click **Next**.



Add descriptive **Name**, click **Save** to finish, Configure Rule order window will be deployed. Select Process Rule First option and then click Save again.

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

**Review your TLS Decryption Rule configurations below**

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

**General**

Name\* ① **AcmeOne-DoNotDecrypt** ②

Description: Enter description name

Tags: Press Enter to add

Rule is Enabled:

**Applications & URLs** ④ Edit

URL Categories: financial\_services, health and medicine

**Decryption Enforcement** ⑤ Edit

Rule Type: Do Not Decrypt

Inspect Traffic Enabled: Inspect the server certificate

Profile: StandardInspect

**Review & Validate** ⑥

**Configure Rule Order**

How would you like to process rule "AcmeOne-DoNotDecrypt"?

①  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)

**Save** ②

To create the rule allowing to decrypt all traffic, click **Add**.

Configure > Security Service Edge > TLS Decryption > Policy Rules

**TLS Decryption Rules List**

Below are all the TLS Decryption Rules

Rule Name	Decryption Profile	Bypass URL Filtering Profile	Applications & URLs	Users & Groups	Endpoint Posture	Source & Destination	Services	Schedule
Standardinspect	Standard	None Selected	Reputations trustworthy low_risk	All Users	Endpoint Information Profile (EIP) All devices		All Layer 4 Services	Not Available
RiskyWebsites	Strict	None Selected	Reputations high_risk suspicious undefined	All Users	Endpoint Information Profile (EIP) All devices		All Layer 4 Services	Not Available
AcmeOne-DoNotDecrypt	StandardInspect	None Selected	URL Categories financial_services health_and_medicine	All Users	Endpoint Information Profile (EIP) All devices	Destination Zone Internet	Services http https	Not Available

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

Select **Decrypt Traffic and Inspect server Certificate**, Select the **Decryption Profile** and **URL Filtering Action Override**, then click Next.

Configure > Security Service Edge > TLS Decryption > Policy Rules

**Edit TLS Decryption Rule: AcmeOneDecryptAll**

What type of rule would you like to create?  
You can customize either configuration you'd like to enforce

Action: 1. Decryption Enforcement

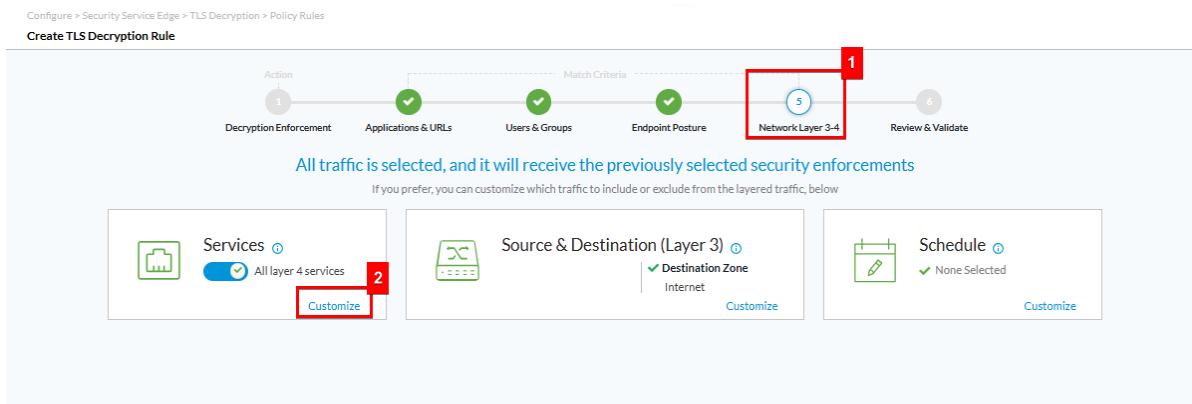
Match Criteria: 2. Applications & URLs, 3. Users & Groups, 4. Endpoint Posture, 5. Network Layer 3-4, 6. Review & Validate

Decryption Enforcement: 2. Decrypt traffic and inspect the server certificate (selected), 3. AcmeOne-TLSProfile

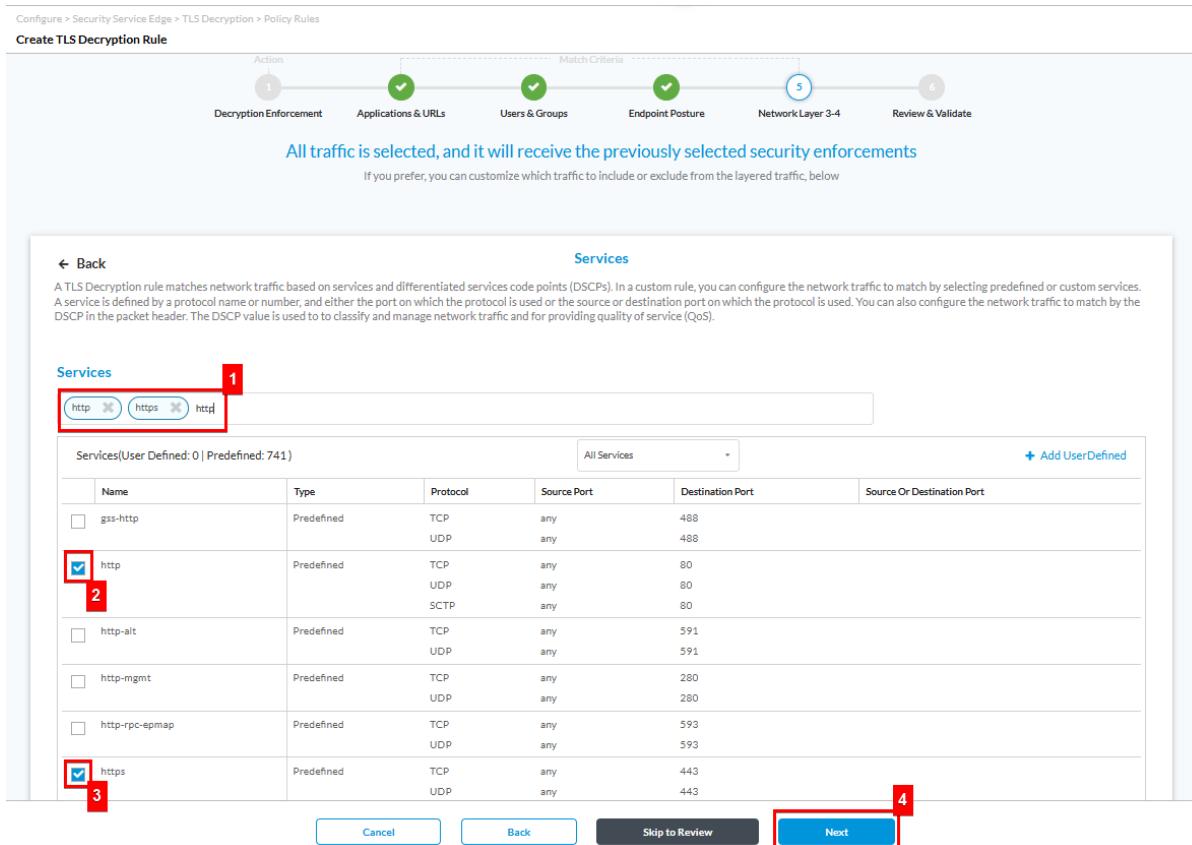
Do Not Decrypt: 4. Do not decrypt the traffic but only inspect server certificate (selected), 5. Do not decrypt and do not inspect the traffic

Buttons: Cancel, Back, Skip to Review, Next

Click **Next** in **Applications and URLs**, **Users & Groups** and in **Endpoint Posture**, until you reach **Network Layer 3-4**. Click on **Customize** in section **Services**.



Look for **http** and add services **http** and **https** to avoid resources consumption looking for other services. Then Click **Next**.



Add descriptive **Name**, click **Save** to finish, Configure Rule order window will be deployed. Select Process the Rule in specific placement, place it in the second position and then click Save again.

## Create TLS Decryption Rule

## Configure Rule Order



How would you like to process rule "AcmeOneDecryptAll"?

- 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)

1

2

Place here →

- 1. AcmeOne-DoNotDecrypt
- 2. StandardInspect
- 3. RiskyWebsites

3

Cancel

Move

Place the rule in the second position, after the **DoNotDecrypt** rule.

## Step 9: Configure Real-Time Protection Profiles and Rules

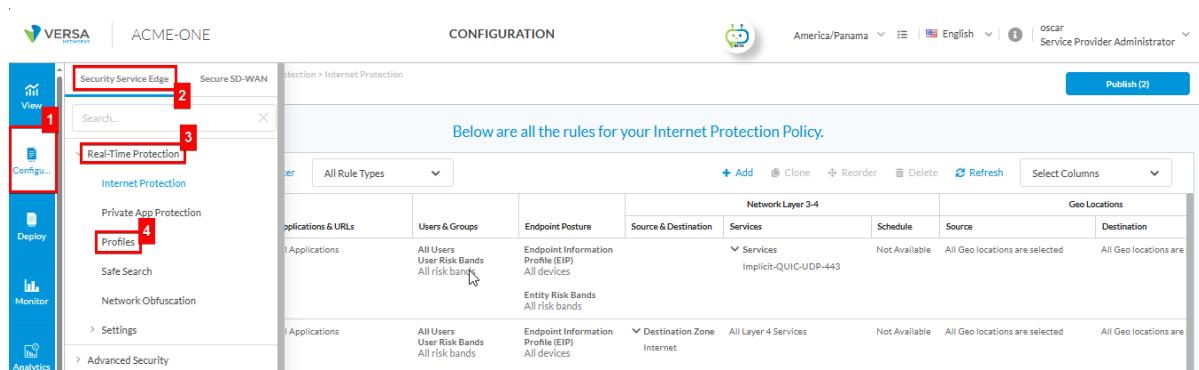
- First, create different profiles to ensure secure access in accordance with the organization's requirements. For this case, two profiles will be used: a custom profile for URL Filtering and a predefined profile for Malware protection.
- Once all profiles are created or selected from predefined options, proceed to configure the protection policies.
- Next, configure SaaS Tenant Control to ensure users access O365 only with corporate domain accounts. This prevents logins with personal or third-party accounts, reducing the risk of data leakage or use of unmanaged, non-compliant environments.

### Custom URL Filtering Profile

In this use case, all the users will be enforced by one URL filtering profile that blocks the following categories of sites: malware, phishing, botnet, adult, and illegal. Also, URL filtering blocks high-risk and uncategorized/undefined URLs reputation-based threats. The others reputations will be allowed.

To meet these requirements, we will need to create a custom URL Filtering Profile as follows:

Go to **Configure > Security Service Edge > Real Time Protection > Profiles**.



Network Layer 3-4		Geo Locations					
Applications	Users & Groups	Endpoint Posture	Source & Destination	Services	Schedule	Source	Destination
All Applications	All Users User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices	▼ Services	Not Available Implicit-QUIC-UDP-443	All Geo locations are selected	All Geo locations are selected	All Geo locations are selected
All Applications	All Users User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices	▼ Destination Zone	All Layer 4 Services Internet	Not Available	All Geo locations are selected	All Geo locations are selected

Go to **Filtering Profiles**, select **URL Filtering**, then click **+Add** to create the profile.

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

**Filtering Profiles**

**1** **Filtering Profiles** (highlighted in red)

**2** **URL Filtering** (highlighted in red)

**3** **+ Add** (highlighted in red)

Table:

Profile Name	Deny List	Allow List	URI Categories	Reputations	Action
Versa\_Reputation\_Analysis		Logging: Enabled		Versa\_Sanctioned: trustworthy Versa\_Moderate: low\_risk, moderate\_risk Versa\_Unsanctioned: suspicious, high\_risk	Allow

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

There is no specific URLs to allow or deny, so click Next in Deny/Allow List Action without making any changes.

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

**Create URL Filtering Profile**

1 Deny & Allow List (highlighted in blue)

2 Category & Reputations List

3 Action

4 Review & Submit

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

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

Action  **+ Add New**

Patterns  **+**

Strings  **+**

**1** **Next** (highlighted in red)

Cancel Back Skip to Review

Select Block in the **Action** field for Category List section, search and select the **URL Categories** malware, phishing, botnet, adult, illegal.

Then select Block in the first **Action** field for Reputation List section, search and select **Reputation** high\_risk and undefined. Click on the **+** to add a second **Action** field, select Allow then search and select **Reputation** trustworthy, low\_risk and moderate\_risk. Then click **Next** to continue.

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

### Edit URL Filtering Profile: AcmeOne-High-Risk-Categories

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

Action 1 Block URL Category

Action 2 Add New

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

Action 3 Block Reputation

Action 4 Add New

Action 5 Allow Reputation

Action 6 Add New

Select Allow as default **Action** if the URL does not match any URL category nor reputation. Enabled **Cloud lookup State**. This helps provide visibility into millions of URLs and categories beyond what can be stored locally. Click **Next** to continue.

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

### Create URL Filtering Profile

Deny & Allow List	Category & Reputations List	Action	Review & Submit
By default, we will allow all URLs that do not match any criteria specified. Otherwise, you can choose which default action to enforce if there are no criteria matched.			

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

Action 1 Allow

2 Decrypt Bypass

3 Cloud Lookup State

Cancel Back Skip to Review Next

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

## Malware Protection & IPS Profile (Predefined)

ACME-ONE requires the enablement of Antivirus and Intrusion Prevention System (IPS) for safeguarding internet traffic to detect, block, and neutralize malicious threats before they can compromise your devices or data.

By default, Versa SASE provides predefined security profiles to protect against malware and IPS. In this scenario, we will use those predefined profiles available because they both meet the requirements for these threats. Therefore, there is no need to create customs profiles in this section.

### Internet Protection Rules

Now that all the profiles required to enforce the security of the use case are ready to be used, we will proceed with the internet protection rules configuration. For this case, all users; with no exception, need to be secured with these profiles therefore we will create one Real-time Protection rule for all users accessing the Internet, as follows:

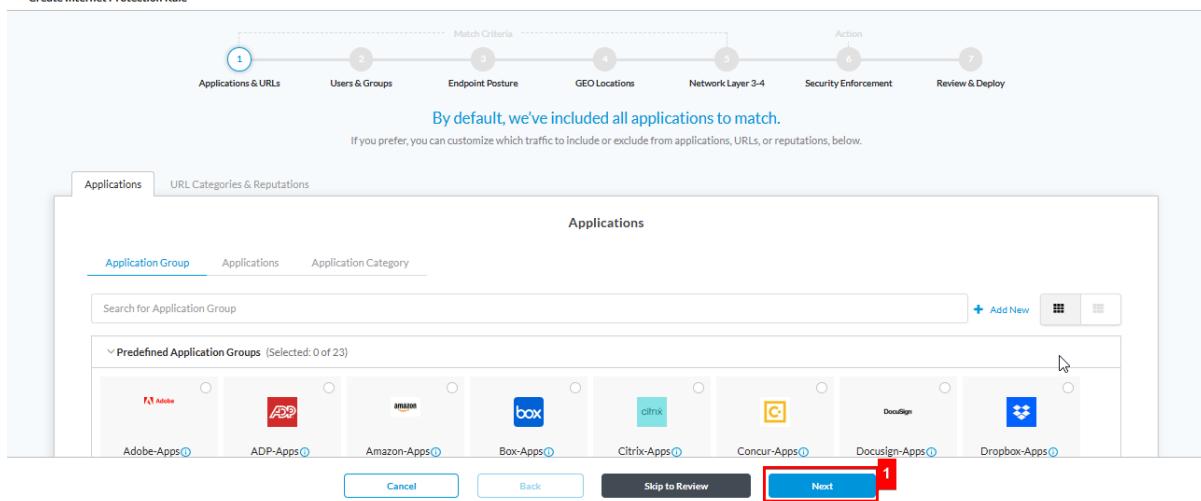
Navigate to

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

Click on **+Add**. Each Internet Protection rule consists of a set of match criteria and the corresponding enforcement action. Note that the match criteria on the same tab are 'OR' ed and on different tabs is 'AND'.

URL Filtering, Antivirus, and IPS will be performed using a profile, so no matching applications or URL is required, just click **Next** without making any changes.

## Create Internet Protection Rule



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

Create Internet Protection Rule

1 Applications & URLs 2 Users & Groups 3 Match Criteria 4 Endpoint Posture 5 GEO Locations 6 Network Layer 3-4 7 Action 7 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 URL Categories & Reputations

Applications

Application Group Applications Application Category

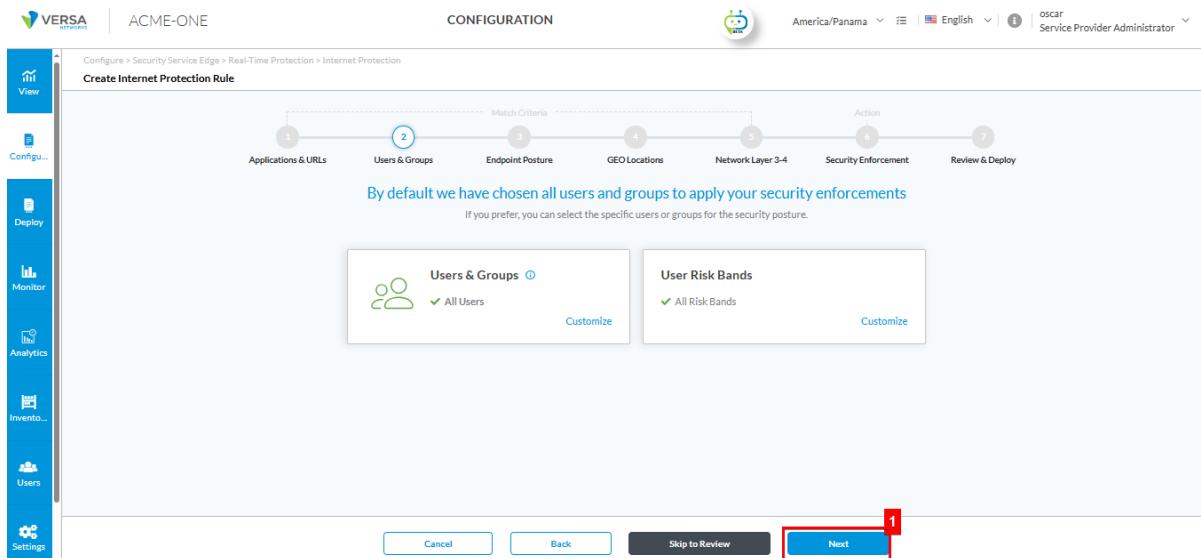
Search for Application Group + Add New

Predefined Application Groups (Selected: 0 of 23)

Adobe Apps ADP-Apps Amazon-Apps Box-Apps Citrix-Apps Concur-Apps DocuSign-Apps Dropbox-Apps

Cancel Back Skip to Review **Next**

In the Users & Groups section you can customize and select the users or groups to match this protection. In this case the protection will be enabled for all users so there is no need to apply any change and just click **Next**.



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

Create Internet Protection Rule

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

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

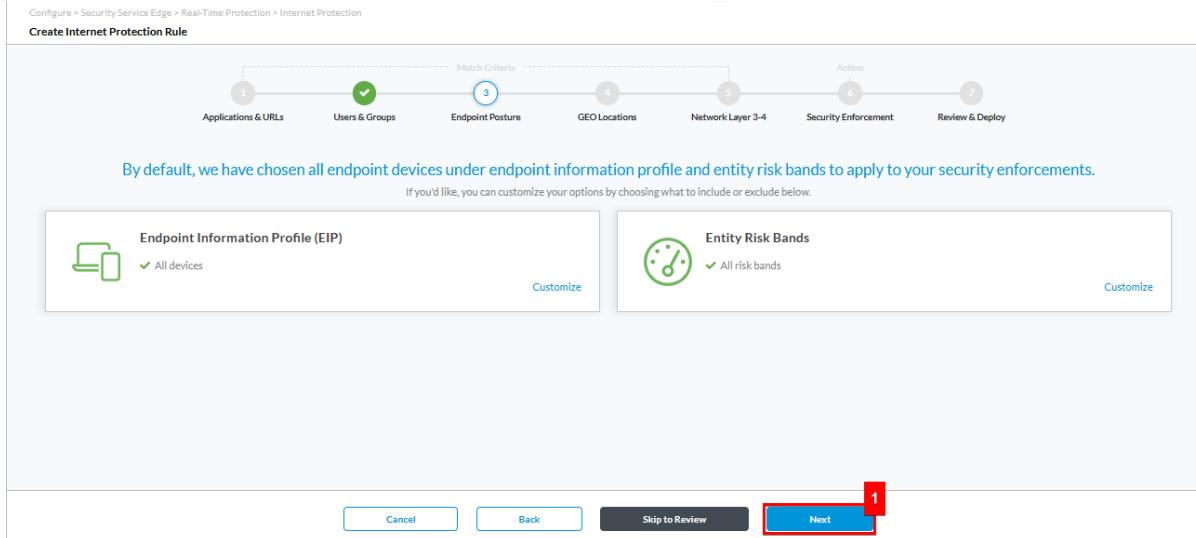
Users & Groups All Users Customize

User Risk Bands All Risk Bands Customize

Cancel Back Skip to Review **Next**

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

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



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.

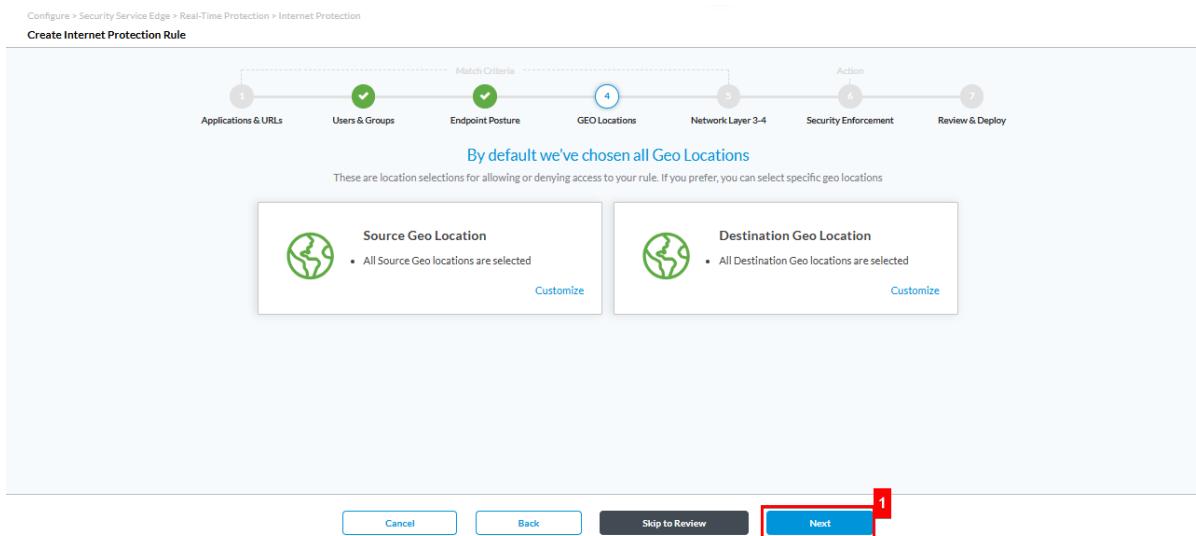
Endpoint Information Profile (EIP)  
✓ All devices  
Customize

Entity Risk Bands  
✓ All risk bands  
Customize

Cancel Back Skip to Review **Next** 1

Click **Next** in Geo Posture section, no match criteria for geo location for traffic.

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



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** 1

In the Network Layer section, keep the Internet as the Destination Zone for this rule and click **Next**.

## Create Internet Protection Rule

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) [Customize](#)

Schedule  None Selected [Customize](#)

**Next** 1

In the **Security Enforcement** section scroll down and Select **Security Profiles**

## Create Internet Protection Rule

Choose the type of enforcement action for your Internet Protection Rule.

Enable TCP Keepalive  
Sends keepalive probes to maintain idle TCP connections for long-running applications like VNC or RDP

Allow  
Allow all traffic that matches the rule to pass

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

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

**URL Filtering** **EasyURLFiltering**  
Versa's preconfigured URL filters controls all web-browsing activity

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

**File Filtering** **EasyFileFiltering**  
Versa's preconfigured file filtering protects from unwanted and malicious files

In section **Filtering Profiles** enable **URL Filtering** and select the User Defined **AcmeOne-High Risk-Categories** profile that was created before.

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

Edit Internet Protection Rule: InternetAccessRule

Reject

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

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

**2**  **Filtering Profiles**

**3**  **Malware Protection & IPS**

**4**  **Cloud Access Security Broker (CASB - Inline)**

**5**  **URL Filtering**  
**EasyURLFiltering**  
Versa's preconfigured URL filters controls all web-browsing activity

**6**  **IP Filtering**  
**Versa Recommended Profile**  
Versa's preconfigured IP Filtering blocks communication with internet end points (sources and destinations) which...

**7**  **File Filtering**  
**EasyFileFiltering**  
Versa's preconfigured file filtering protects from unwanted and malicious files

**8**  **Advanced Threat Protection (ATP)**

**9**  **Data Loss Prevention (DLP)**

**10**  **Remote Browser Isolation (RBI)**

Cancel Back Skip to Review **Next**

Then click on the section **Malware Protection & IPS** and enable the Malware protection check mark, select the Versa's preconfigured **EasyMalware Protection** and the Intrusion Protection System (IPS) check mark with the Versa's preconfigured **EasyIPS** protection and click **Next**.

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

Create Internet Protection Rule

Reject

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

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

**2**  **Malware Protection & IPS**

**3**  **Cloud Access Security Broker (CASB - Inline)**

**4**  **Advanced Threat Protection (ATP)**

**5**  **Data Loss Prevention (DLP)**

**6**  **Remote Browser Isolation (RBI)**

**7**  **URL Filtering**  
**EasyURLFiltering**  
Versa's preconfigured URL filters controls all web-browsing activity

**8**  **IP Filtering**  
**Versa Recommended Profile**  
Versa's preconfigured IP Filtering blocks communication with internet end points (sources and destinations) which...

**9**  **File Filtering**  
**EasyFileFiltering**  
Versa's preconfigured file filtering protects from unwanted and malicious files

**10**  **Malware Protection**  
**EasyMalware Protection**  
Versa's preconfigured malware protection scans web and email traffic

**11**  **Intrusion Protection System (IPS)**  
**EasyIPS**  
Versa's preconfigured IPS identifies and protects your network against security vulnerabilities

**12**  **Cloud Access Security Broker (CASB - Inline)**

**13**  **Advanced Threat Protection (ATP)**

**14**  **Data Loss Prevention (DLP)**

**15**  **Remote Browser Isolation (RBI)**

**16**  **URL Filtering**  
**EasyURLFiltering**  
Versa's preconfigured URL filters controls all web-browsing activity

**17**  **IP Filtering**  
**Versa Recommended Profile**  
Versa's preconfigured IP Filtering blocks communication with internet end points (sources and destinations) which...

**18**  **File Filtering**  
**EasyFileFiltering**  
Versa's preconfigured file filtering protects from unwanted and malicious files

**19**  **Advanced Threat Protection (ATP)**

**20**  **Data Loss Prevention (DLP)**

**21**  **Remote Browser Isolation (RBI)**

Cancel Back Skip to Review **Next**

Use a descriptive **Name** and Click **Save** to create this rule. Save the rule after implicit **Implicit\_Drop\_Quic** rule

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

**General**

Name\*  1

Description

Tags

Rule is Enabled

**Applications & URLs**  2

All Applications

### Configure Rule Order

How would you like to process rule "InternetAccessRule"?

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) 1

Process the rule in specific placement (select where to place in rule list) 2

Place here 3

1. Implicit\_Drop\_Quic  
2. Test-AllowAll  
3. GenAI\_Firewall  
4. Implicit-Allow-DNS  
5. Implicit-Deny-All

## Private Protection Rules

Next, we create a Real-Time Private App Protection policy to secure traffic from remote users accessing internal applications hosted in the datacenters. To begin, make sure that the Private Applications from Step 3 have been configured.

For this case, we need to create Real-time Private Protection policies for our test users accessing the previously defined private apps, as follows:.

Navigate to

**Configure > Security Service Edge > Real-Time Protection > Private App Protection,**

Click on **+Add** (Click on Let's Go, if this is your first Private App Rule). Each private protection rule consists of a set of match criteria and the corresponding enforcement action. Note that the match criteria on the same tab are 'OR' ed and on different tabs is 'AND'.

The screenshot shows the Versa Network Management Platform interface. The left sidebar has the following tabs: View (highlighted with a red box and number 1), Configure, Deploy, Monitor, Analytics, Inventory, Users, Settings, and Tenants. The main configuration pane shows the 'Real-Time Protection' section with 'Private App Protection' selected (highlighted with a red box and number 4). A list of pre-selected criteria is shown in a table with the following rows:

<input checked="" type="checkbox"/> Applications	All Private applications, URLs and reputations will be allowed and protected.
<input checked="" type="checkbox"/> Users and User Groups	All users and user groups will be included in the security enforcement.
<input checked="" type="checkbox"/> Source Geo Location & Source IP Address	All source geo locations have been selected.
<input checked="" type="checkbox"/> Network Layer 3-4	All traffic is selected and will receive the previously selected enforcements.
<input checked="" type="checkbox"/> Security Enforcement	Settings for Malware Protection and IPS have been pre-configured.

A large blue 'Setup Site-to-Site Tunnel' button is visible. At the bottom right of the configuration pane, a red box and number 5 highlight the 'Lets Go' button.

Select the previously created applications (**India-portal** and **Usa-apps**) and click **Next**.

Configure > Security Service Edge > Real-Time Protection > Private App Protection

### Edit Private App Protection Rule: PrivateAppsAccessRule

By default, we've included all applications to match.  
If you prefer, you can customize which traffic to include or exclude from applications below.

Applications

Application Group **Applications**

India-portal **usa-apps** Search for Applications **Clear All** **Add New**

User Defined Applications (Selected: 2 of 3)

india-portal PRIVATE-APP-URL usa-apps

Predefined Applications (Selected: 0 of 12)

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

In the Users & Groups section you can customize and select the users or groups to match this protection. In this case the protection will be enabled for **remotevip** test users and click **Next**.

← Back

User Type  All Users  Selected Users  Known Users  Unknown Users

Enable Private App Protection for the following matched users or user groups

MSEntralD-OscarNuevo

User Groups **Users**

remotevip@oscarlabsase.onmicrosoft.com Search for Users

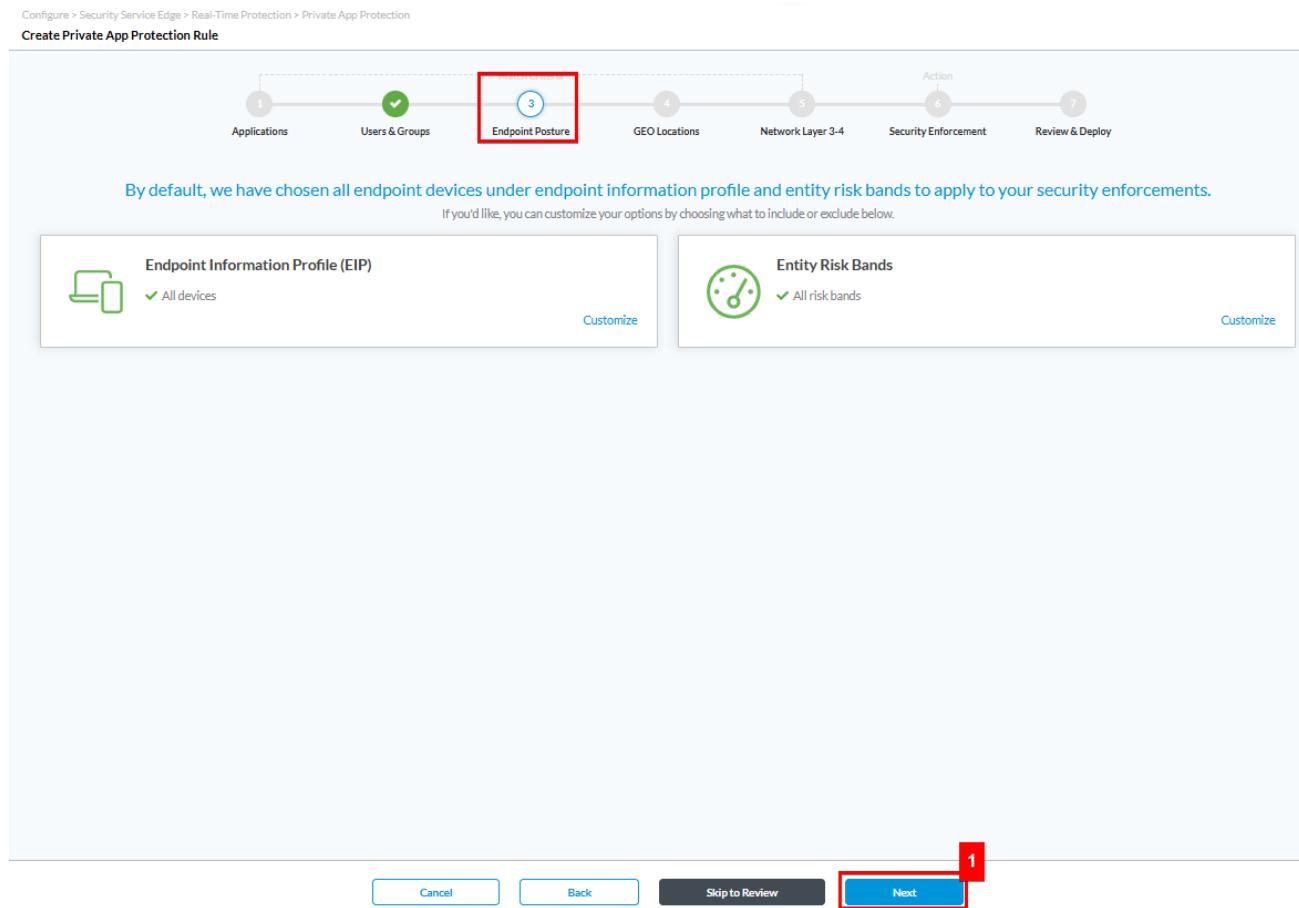
Users (2)

User Name	First Name	Last Name
<input type="checkbox"/> vip@oscarlabsase.onmicrosoft.com	vip	-
<input checked="" type="checkbox"/> remotevip@oscarlabsase.onmicrosoft.com	remotevip	-

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

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

Configure > Security Service Edge > Real-Time Protection > Private App Protection  
Create Private App Protection Rule



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 1 Next

Click **Next** in Geo Posture section, no match criteria for geo location for traffic.

Configure &gt; Security Service Edge &gt; Real-Time Protection &gt; Private App Protection

## Create Private App Protection Rule

By default we've chosen all Geo Locations

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

Source Geo Location

- All Source Geo locations are selected

Destination Geo Location

- All Destination Geo locations are selected

Cancel Back Skip to Review **Next** 1

In **Network Layer 3-4** section, keep the default values to match all traffic from remote users to internal applications. Click **Next**.

Configure > Security Service Edge > Real-Time Protection > Private App Protection

Create Private App Protection Rule

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

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

Services  All layer 4 services

Source & Destination (Layer 3)   
Source Zone: SD-WAN Zone  
Destination Zone: SD-WAN Zone

Schedule  None Selected

Cancel Back Skip to Review **Next** 1

In the **Security Enforcement** section scroll down and Select **Security Profiles**

## Create Private App Protection Rule

Please select one of the below security filters to move forward.

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

Choose the type of enforcement action for your Private Application Protection Rule.

Enable TCP Keepalive  
Sends keepalive probes to maintain idle TCP connections for long-running applications like VNC or RDP

Allow  
Allow all traffic that matches the rule to pass

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

Filtering Profiles Malware Protection & IPS Data Loss Prevention (DLP) Remote Browser Isolation (RBI)

Malware Protection  
**EasyMalware Protection**  
Versa's preconfigured malware protection scans web and email traffic

Blocked Malware  
viruses  
ransomware

Intrusion Protection System (IPS)  
**EasyIPS**  
Versa's preconfigured IPS identifies and protects your network against security vulnerabilities

Predefined IPS Profile Override  
-- Select --

Then click on the section **Malware Protection & IPS** and enable the Malware protection check mark, select the Versa's preconfigured **EasyMalware Protection** and the Intrusion Protection System (IPS) check mark with the Versa's preconfigured **EasyIPS** protection and click **Next**.

Configure > Security Service Edge > Real-Time Protection > Private App Protection

#### Create Private App 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**  
Choose one or more predefined or user defined security enforcements which include criteria to allow or reject traffic.

**Filtering Profiles** 1

**Malware Protection & IPS** 2 3

**Data Loss Prevention (DLP)**

**Remote Browser Isolation (RBI)**

**Malware Protection**  
**EasyMalware Protection**  
Versa's preconfigured malware protection scans web and email traffic

**Blocked Malware**

- viruses
- ransomware
- spyware
- worms
- trojans
- adware
- unwanted applications

**Intrusion Protection System (IPS)**  
**EasyIPS**  
Versa's preconfigured IPS identifies and protects your network against security vulnerabilities

**Predefined IPS Profile Override**

**Blocked Vulnerabilities**  
high severity & medium+ confidence attacks  
medium+ cvss & medium+ confidence attacks

4 5 6 7

Cancel Back Skip to Review Next

Use a descriptive **Name** and Click **Save** to create this rule.

Configure > Security Service Edge > Real-Time Protection > Private App Protection

#### Create Private App Protection Rule

1
2
3
4
5
6
7

Match Criteria

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

**Review your Private App Protection Policy configurations below.**

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

**General**

Name\* 1

Description

Tags

Rule is Enabled

**Applications** Edit

All Applications

**Users & Groups** Edit

Cancel Back Save

## SaaS Tenant Control

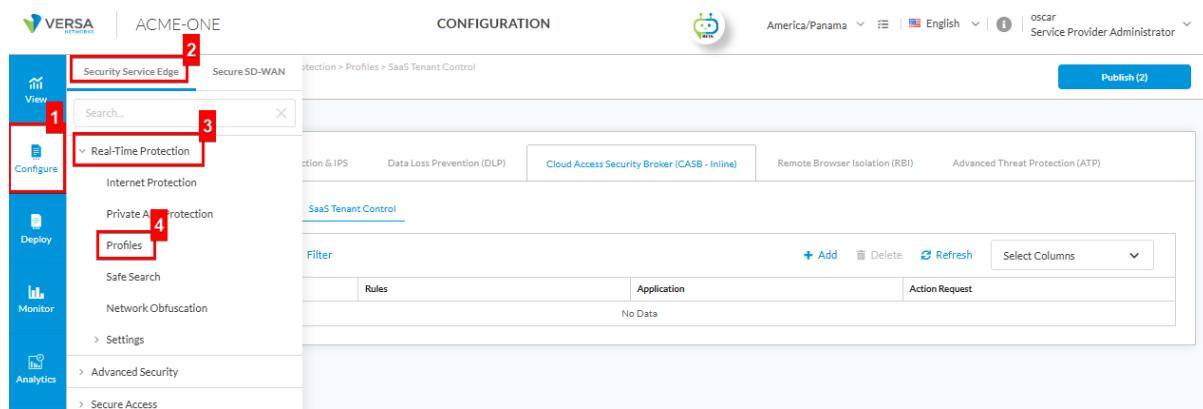
In this scenario, users cannot use personal accounts for Office 365, users cannot use other organizations' tenants and only the corporate Office 365 tenant is accessible. To ensure these restrictions, two controls are required.

### Why Are Two Controls Required?

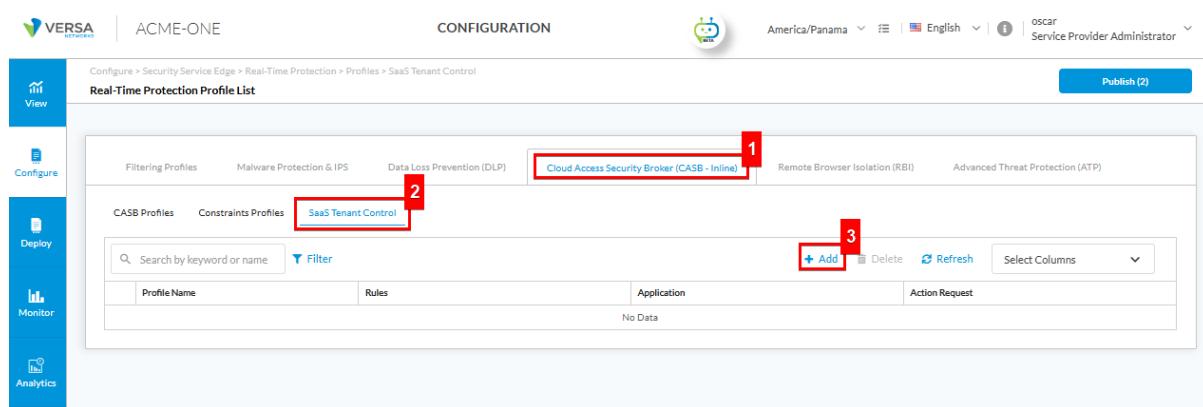
**Office 365 Block Consumer Account:** This control prevents users from signing in with personal Microsoft accounts (e.g., @outlook.com, @hotmail.com, @live.com). Without this restriction, users could bypass corporate monitoring and store or share sensitive data in unmanaged personal accounts.

**Microsoft-Office365-Tenant-Restrictions:** This control enforces access to a specific corporate tenant (e.g., oscarlabsase.onmicrosoft.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.

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



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



Click on **Add** to create a Rule.

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

Create SaaS Tenant Control Profile

Application Rules      Review & Submit

Add Application Rules

Search

Name      Application      Type      Action Request      Values

No Data

+ Add      Delete

Assign a Descriptive **Name**, select the **Insert** Option, In the **Application** Menu look for Microsoft-O365-Block-Consumer-Account to filter consumer/public domains, for **Header** option use Sec-Restrict-Tenant-Access-policy with the **Value** oscarlabsase.onmicrosoft.com. Then Click **Add**.

Add Application Rule

Choose your configurations to enforce the rule

Name \* **1**  
AcmeOneMSOfic365

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

Application **3**  
Microsoft-O365-Block-Consumer-Account

Select one or more headers for your rule

Header **4**  
sec-Restrict-Tenant-Access-Policy

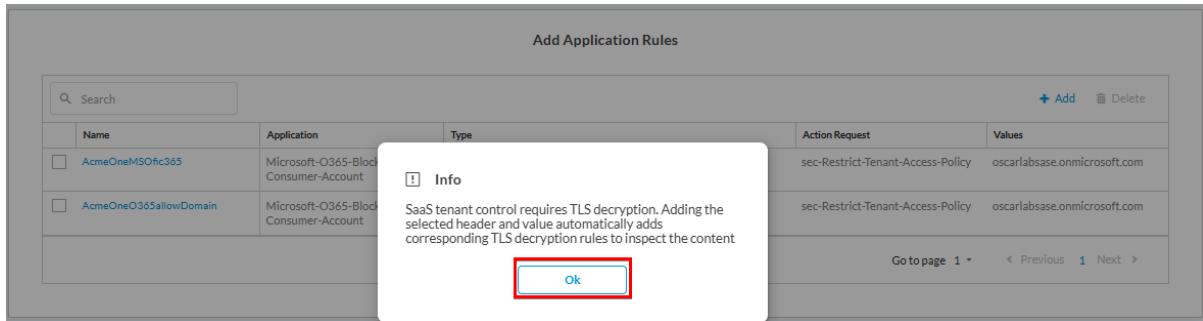
Value **5**  
oscarlabsase.onmicrosoft.com    Delete Existing

**6** Add

Select **Add** again to create a restriction for corporate domains different to acme-one.com

Assign a Descriptive **Name**, select the **Insert** Option, In the **Application** Menu look for Microsoft-Office365-Tenant-Restrictions to filter corporate domains, for **Header** option use Restrict-Access-To-Tenants with the **Value** oscarlabsase.onmicrosoft.com. Then Click **Add** and then **Next**.

Click **Ok** in the information window reporting the TLS decryption rule creation, 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

Application Rules      Review & Submit

Review your SaaS Tenant Control profile Configurations below

**General**

Name \* SaaSTenantCtrl\_O365 1      Description

Tags

**Application Rules** Edit

Name	Application	Type	Action Request	Values
AcmeOneMSOfc365	Microsoft-O365-Block-Consumer-Account	INSERT	sec-Restrict-Tenant-Access-Policy	oscarlabsbase.onmicrosoft.com
AcmeOneO365allowDomain	Microsoft-Office365-Tenant-Restrictions	INSERT	Restrict-Access-To-Tenants	oscarlabsbase.onmicrosoft.com

Cancel      Back      Save 2

## Appendix A - Authentication Method - 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. For this and other authentication methods configuration please refer to document [Step-By-Step-Authentication-Methods-Configuration.docx](#)

## 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](#).