Versa SSE Quick Start Guide

This guide describes the minimum configuration requirements to set up an SSE Client through Concerto. You can find more advanced SSE configurations on the Versa Documentation Portal.

The following links provide more basic Concerto information:

- Quick video on Concerto configuration
- Concerto Home Screen Overview

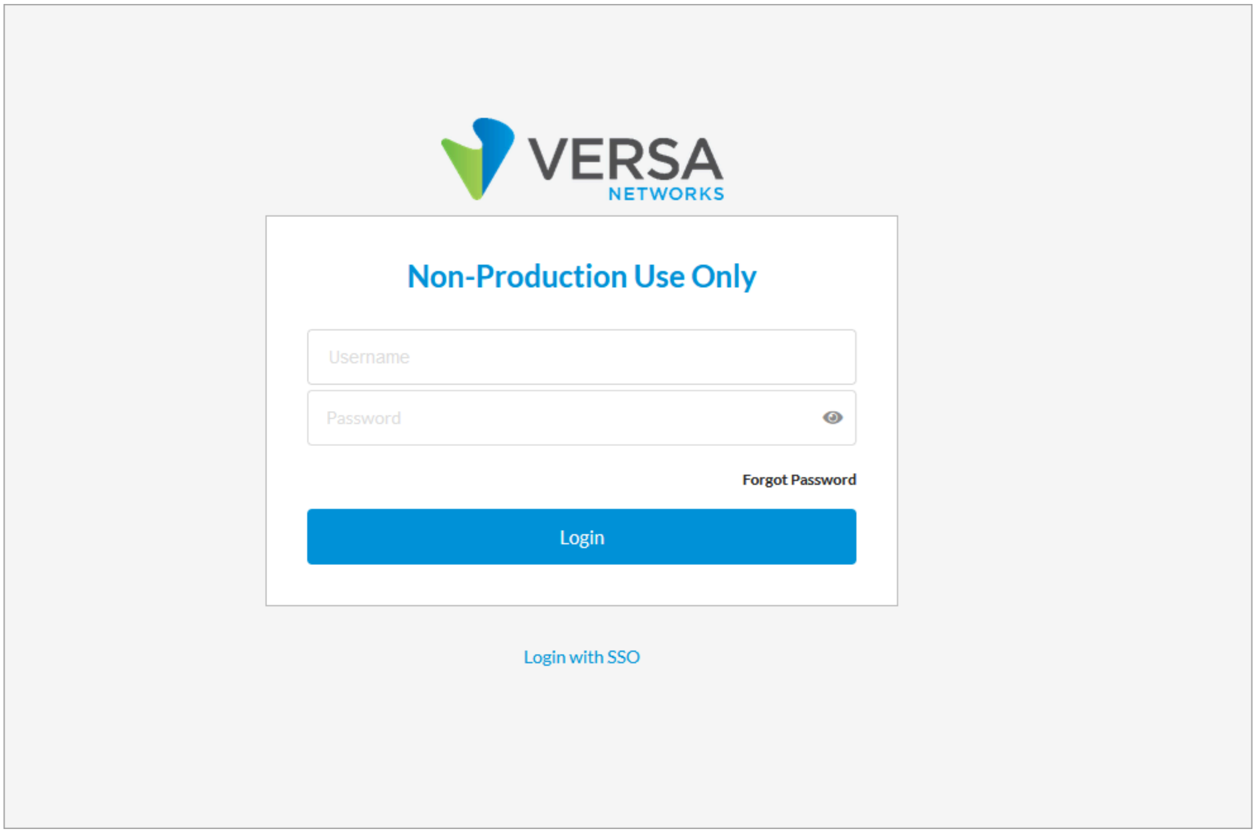
For more information on the required configuration steps outlined in this guide, see the following articles on the Versa Documentation Portal:

- Configure Site-to-Site Tunnels
- User and Device Authentication
- Versa SASE Client Install
- Configure TLS Decryption
- Configure SASE Secure Client Access Profiles
- Configure SASE Secure Client Access Rules
- Configure SASE Internet Protection Rules
- Configure SASE Private Application Protection Rules
- Publish SASE Gateways

This Quick Start Guide covers the following steps to set up an SSE Client through Concerto:

Step 1: Log in to Concerto

Log in to Concerto Orchestrator using the credentials and URL provided to you. You may be asked to change your password if you are logging into the portal for the first time.



Non-Production Use Only

Username

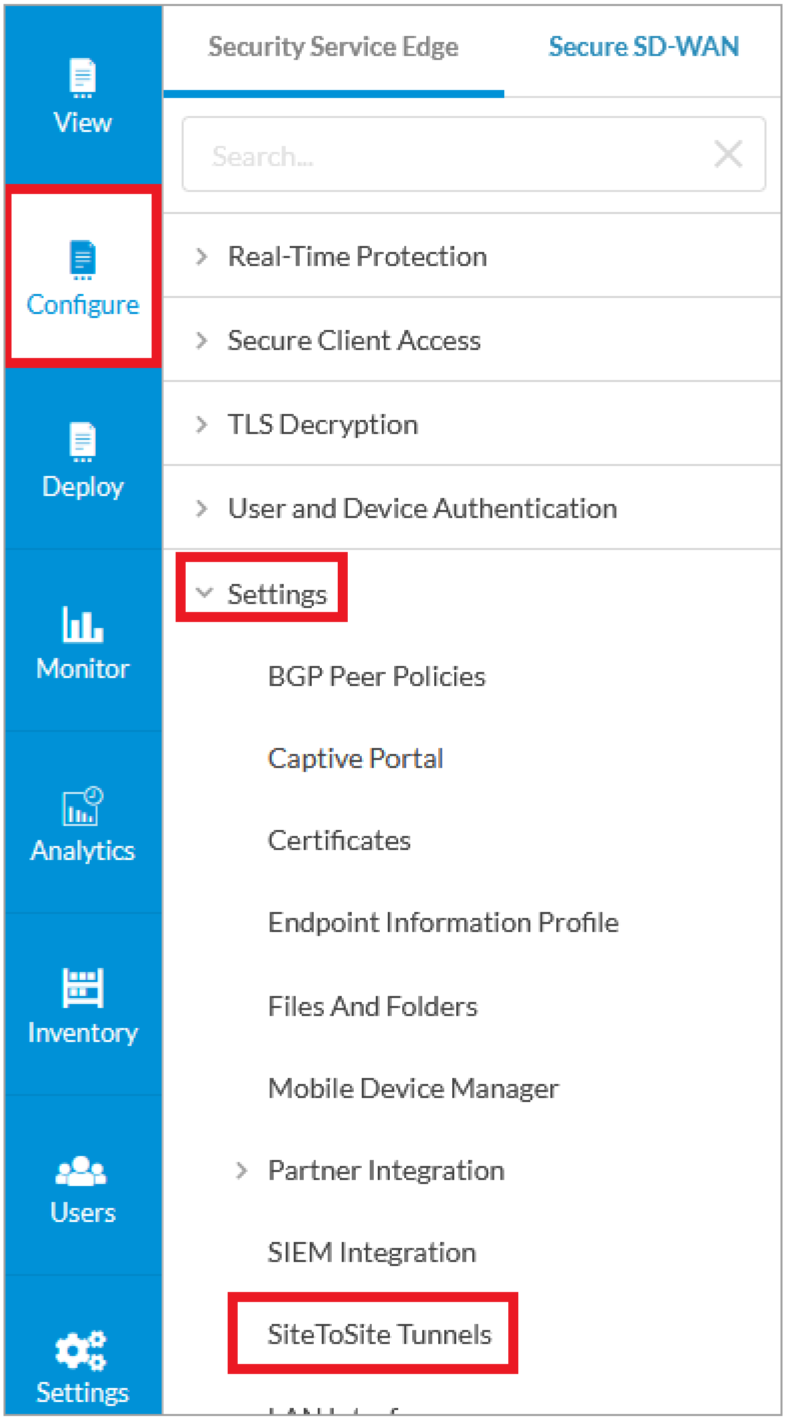
Password

Step 2: Configure Site-to-Site Tunnel or SD-WAN

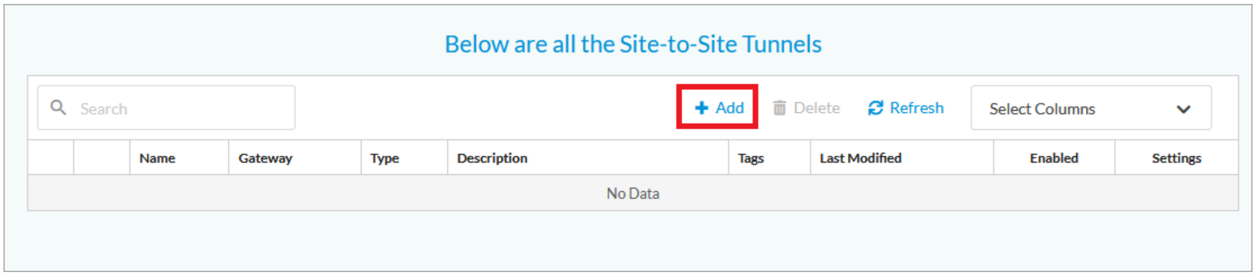
For more information, see Configure Site-to-Site Tunnels.

Select Configure > Settings > Site-To-Site Tunnels. (If you do not have an IPsec tunnel endpoint to use [existing branch router or datacenter edge router], you can skip Step 2).

Note that this step is needed if you are interconnecting your private enterprise network into the Versa SSE infrastructure – whether for connectivity to your IDP or your internal private networks. If you have purchased Versa SD-WAN, you can use SD-WAN instead of IPsec/GRE for connectivity into the gateways from your enterprise network. (You must confirm your purchase with Versa account team).


View
Configure
Deploy
Monitor
Analytics
Inventory
Users
Settings
Security Service Edge
Secure SD-WAN
Search...
Real-Time Protection
Secure Client Access
TLS Decryption
User and Device Authentication
Settings
BGP Peer Policies
Captive Portal
Certificates
Endpoint Information Profile
Files And Folders
Mobile Device Manager
Partner Integration
SIEM Integration
SiteToSite Tunnels

Click + Add.



Below are all the Site-to-Site Tunnels

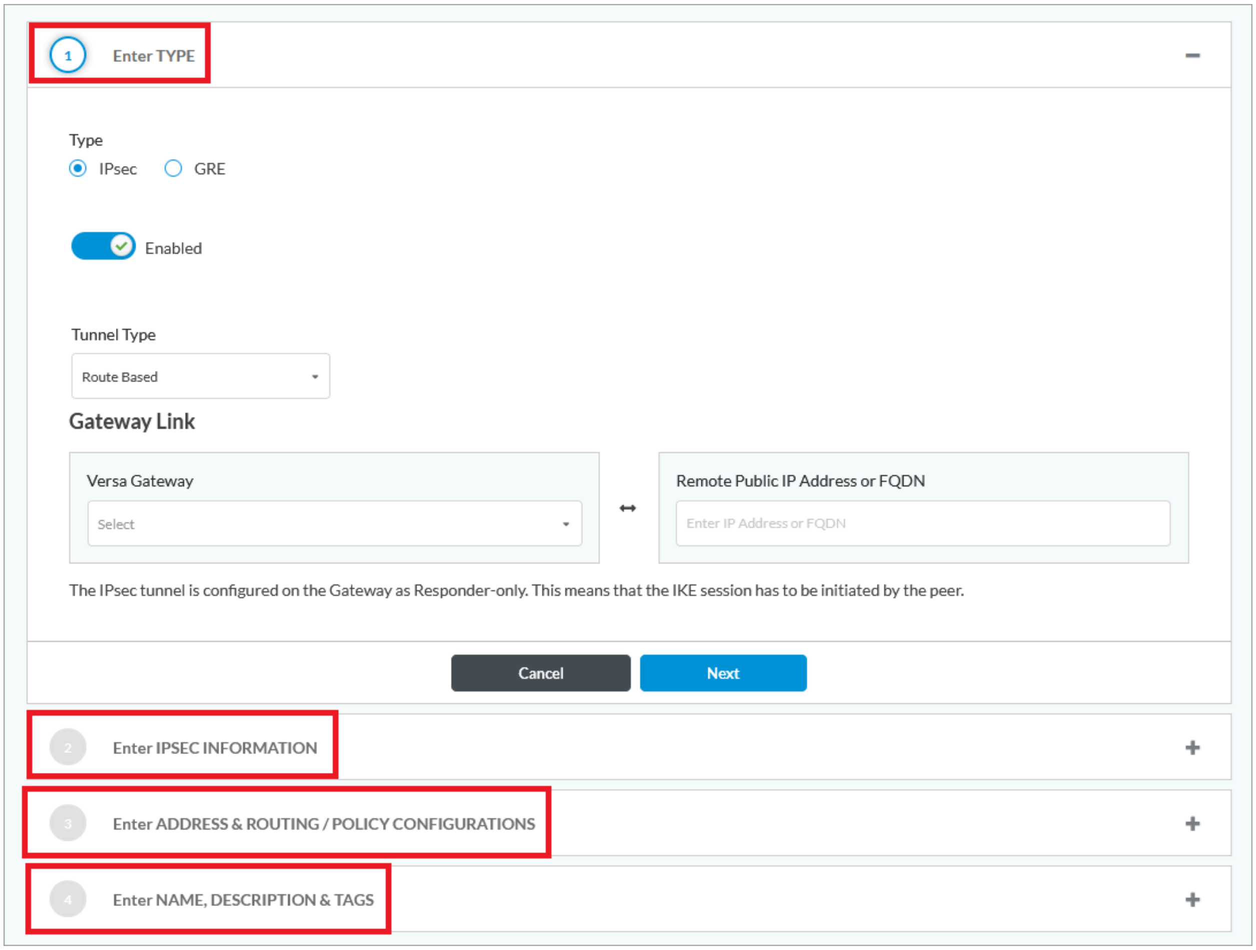
Search

+ Add · Delete · Refresh · Select Columns

		Name	Gateway	Type	Description	Tags	Last Modified	Enabled	Settings
No Data									

You need to configure the following parameters according to your tunnel requirements:

- Type
- IPsec Information
- Address and Routing/Policy Configurations
- Name, Description, and Tags.



1 Enter TYPE

Type

● IPsec ○ GRE

Enabled

Tunnel Type

Route Based

Gateway Link

Versa Gateway: Select

Remote Public IP Address or FQDN: Enter IP Address or FQDN

The IPsec tunnel is configured on the Gateway as Responder-only. This means that the IKE session has to be initiated by the peer.

Cancel · Next

2 Enter IPSEC INFORMATION

3 Enter ADDRESS & ROUTING / POLICY CONFIGURATIONS

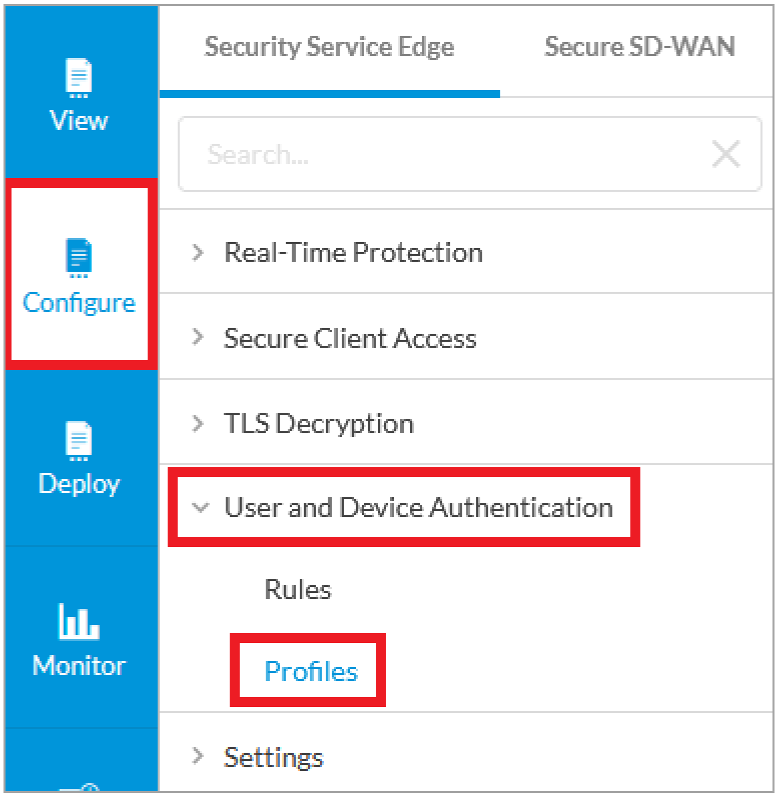
4 Enter NAME, DESCRIPTION & TAGS

Step 3: Configure User Authentication

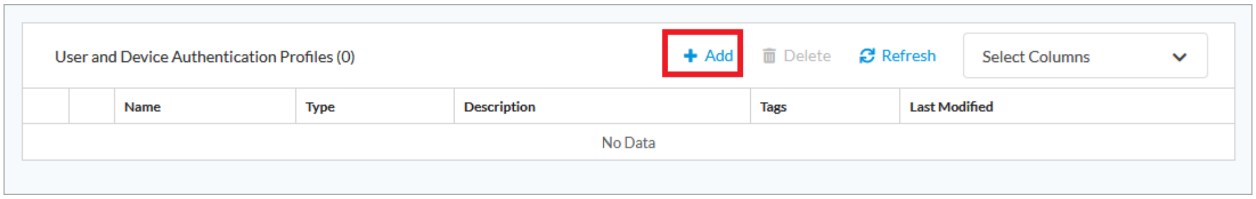
For more information, see User and Device Authentication.

For authorized access, you must be authenticated by Versa Secure Client.

Select Configure > User and Device Authentication > Profiles.



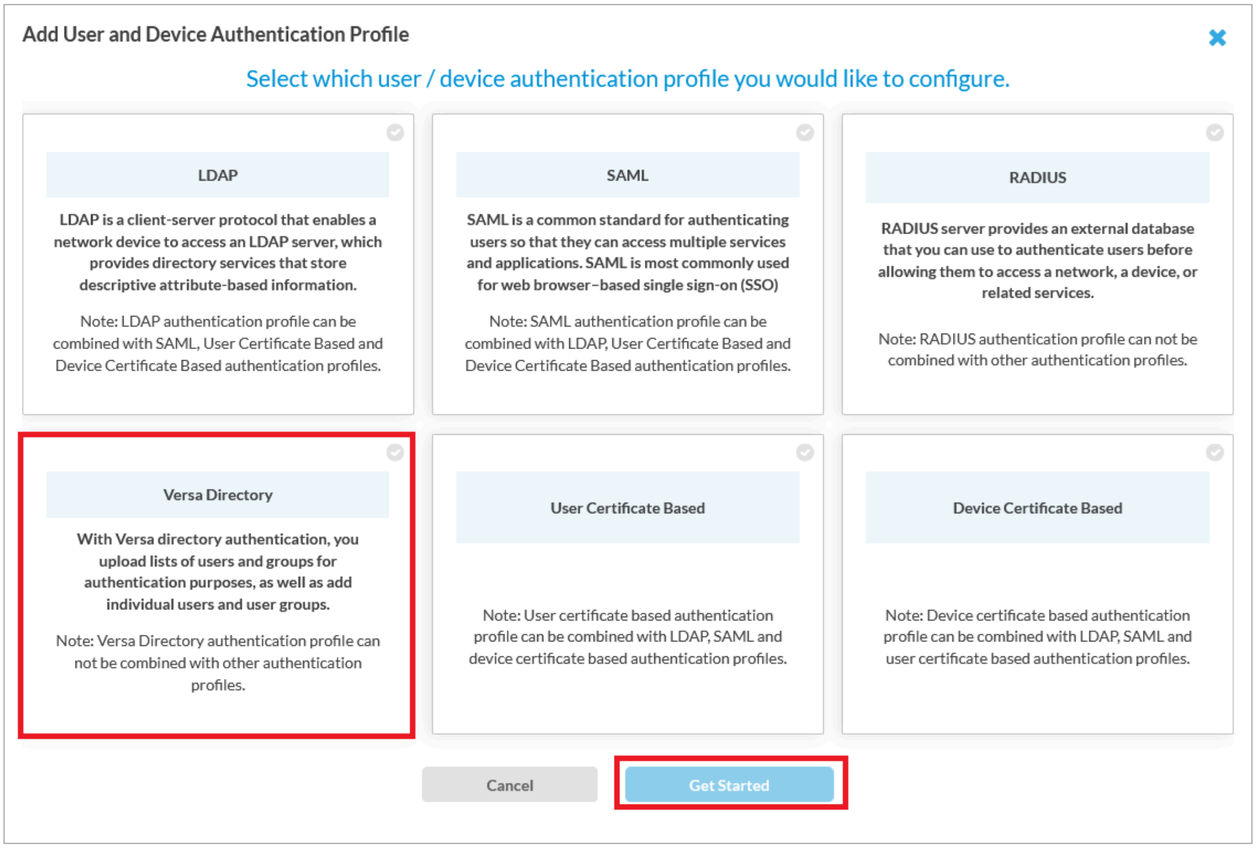
In the User and Device Authentication Profile page, click + Add.



User and Device Authentication Profiles (0)

	Name	Type	Description	Tags	Last Modified
	No Data				

There are many ways you can integrate an IDP to utilize authentication methods such as SAML, RADIUS, or LDAP. The simplest way is to use a Versa Directory, which is an IDP hosted by Versa Networks for customers who do not have an IDP. The following output focuses on using Versa Directory. Refer to the documentation if selecting SAML, LDAP, or RADIUS for descriptions of the fields required for input and relevant instructions.



Add User and Device Authentication Profile

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

LDAP

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

Note: LDAP authentication profile can be combined with SAML, User Certificate Based and Device Certificate Based authentication profiles.

SAML

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

Note: SAML authentication profile can be combined with LDAP, User Certificate Based and Device Certificate Based authentication profiles.

RADIUS

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

Note: RADIUS authentication profile can not be combined with other authentication profiles.

Versa Directory

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

Note: Versa Directory authentication profile can not be combined with other authentication profiles.

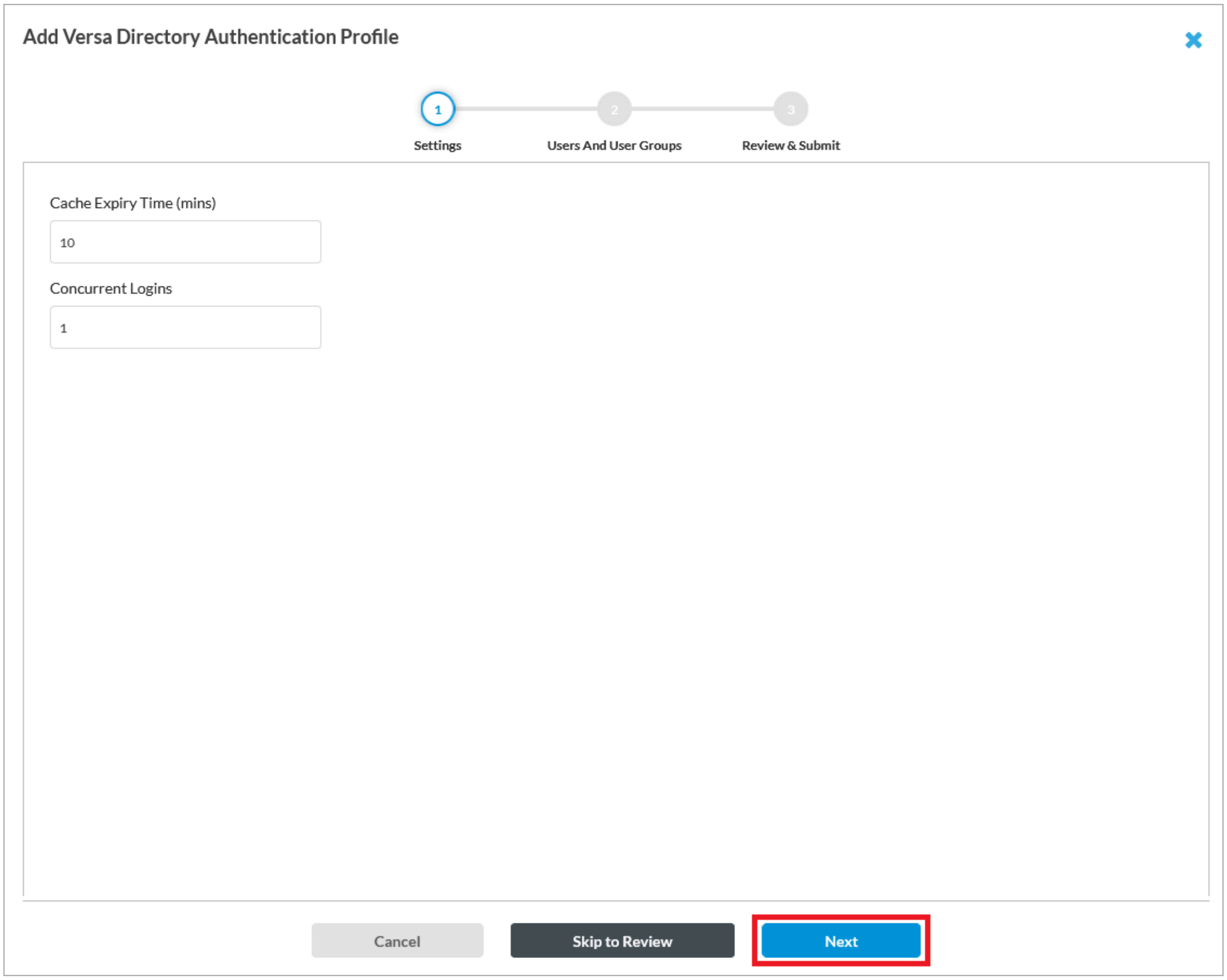
User Certificate Based

Note: User certificate based authentication profile can be combined with LDAP, SAML and device certificate based authentication profiles.

Device Certificate Based

Note: Device certificate based authentication profile can be combined with LDAP, SAML and user certificate based authentication profiles.

You can use the default settings or add more concurrent logins for testing.



Add Versa Directory Authentication Profile

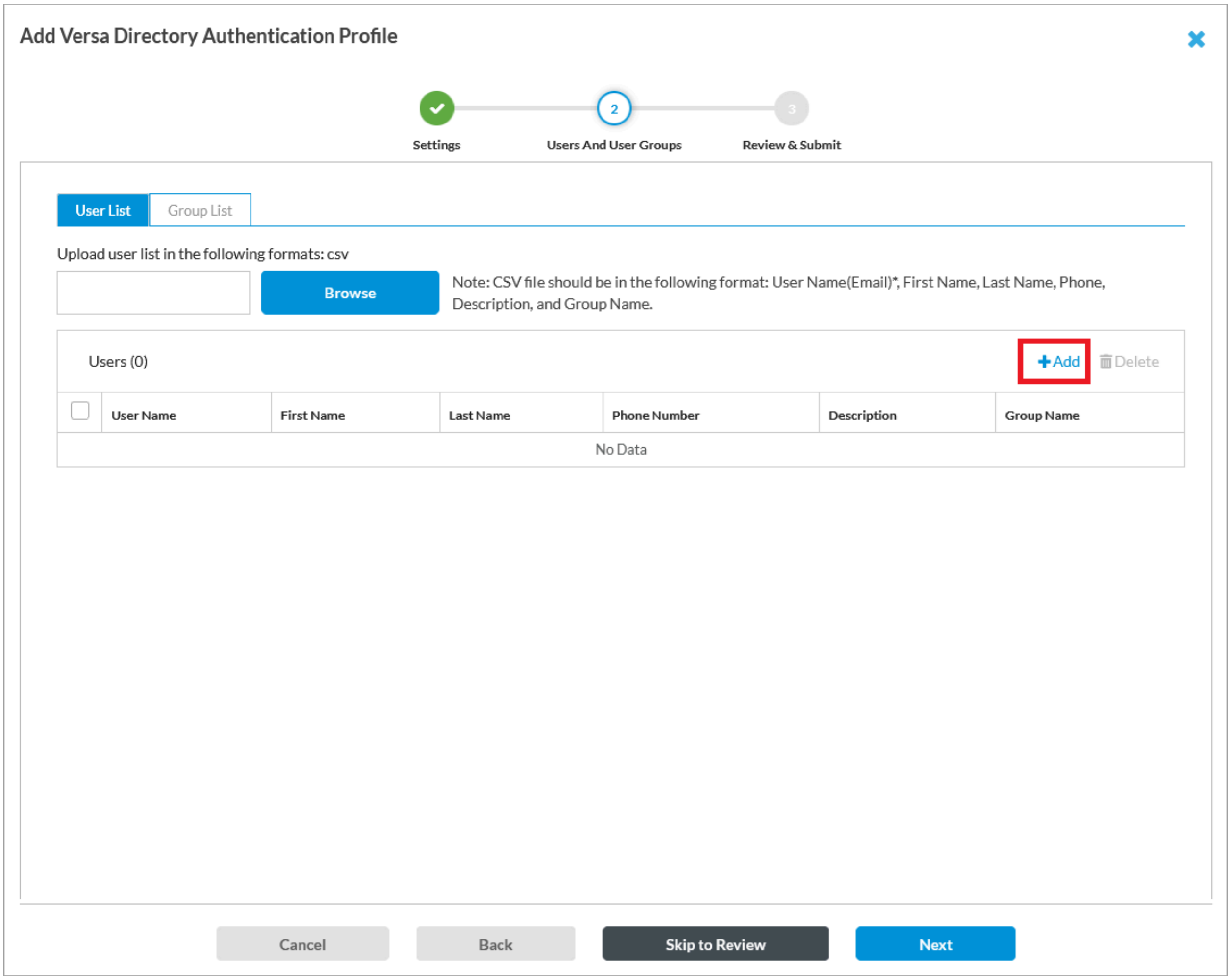
Cache Expiry Time (mins)

10

Concurrent Logins

1

Click + Add to create users.



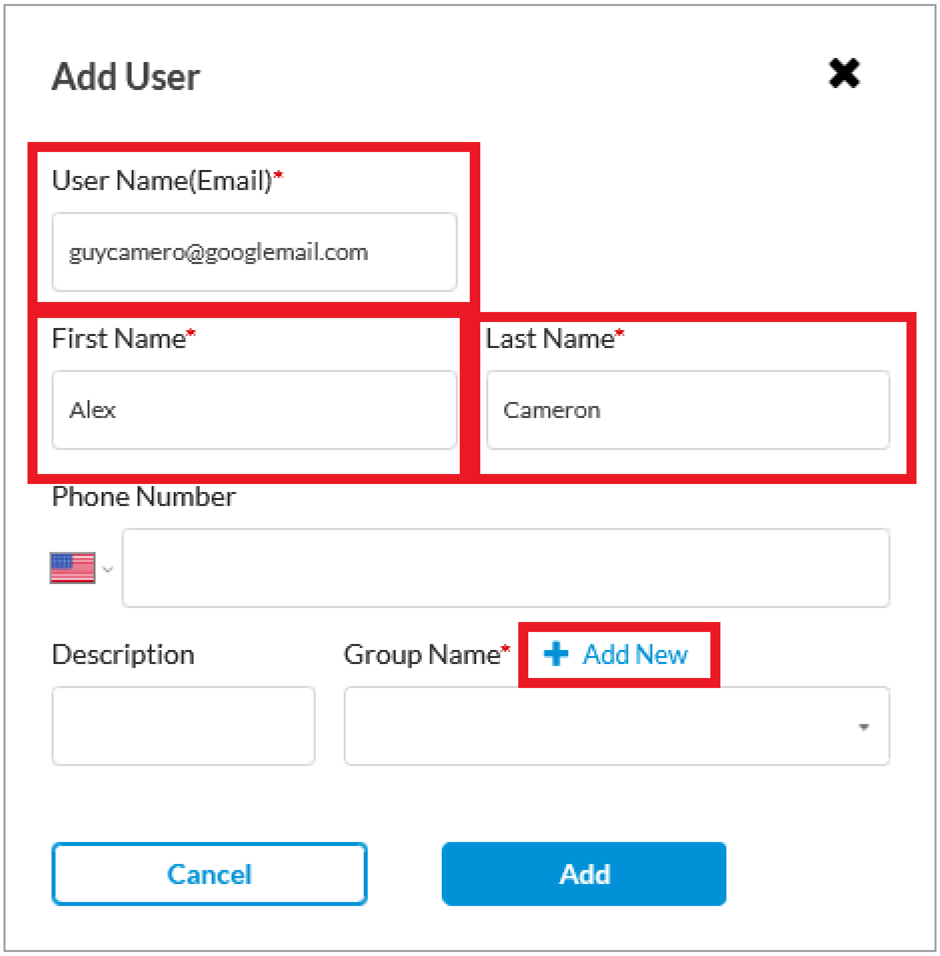
Upload user list in the following formats: csv

Note: CSV file should be in the following format: User Name(Email)*, First Name, Last Name, Phone, Description, and Group Name.

□	User Name	First Name	Last Name	Phone Number	Description	Group Name
No Data						

Add the user email which will be the user's login name, First Name, and Last Name, and then click + Add New to create a group for the user.

Note: A valid email address capable of receiving messages is required.

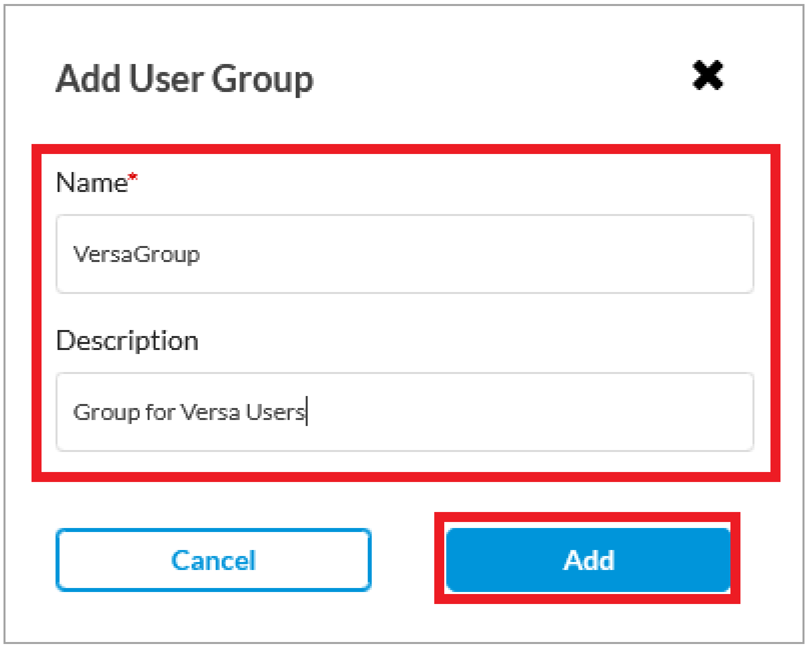


User Name(Email)*: guycamero@googlemail.com

First Name*: Alex

Last Name*: Cameron

Enter the name for the user group.


Add User Group

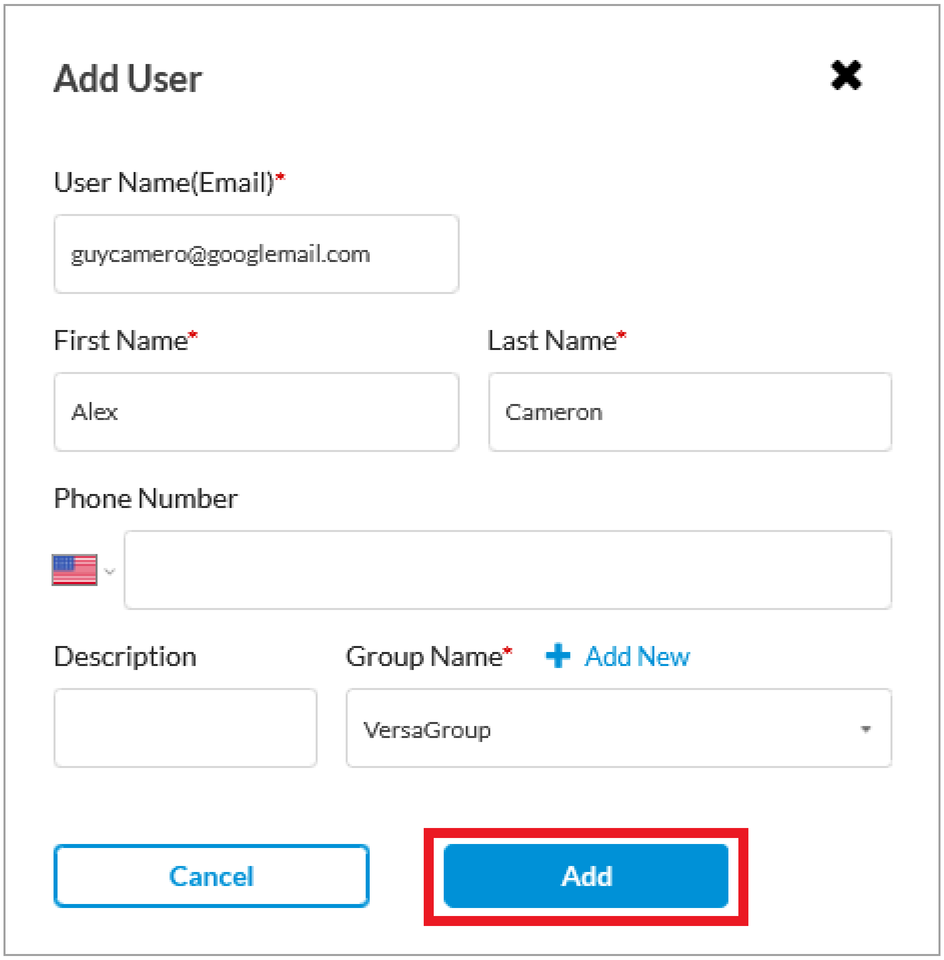
Name*

VersaGroup

Description

Group for Versa Users

Click Add.



Add User

User Name(Email)*: guycamero@googlemail.com

First Name*: Alex

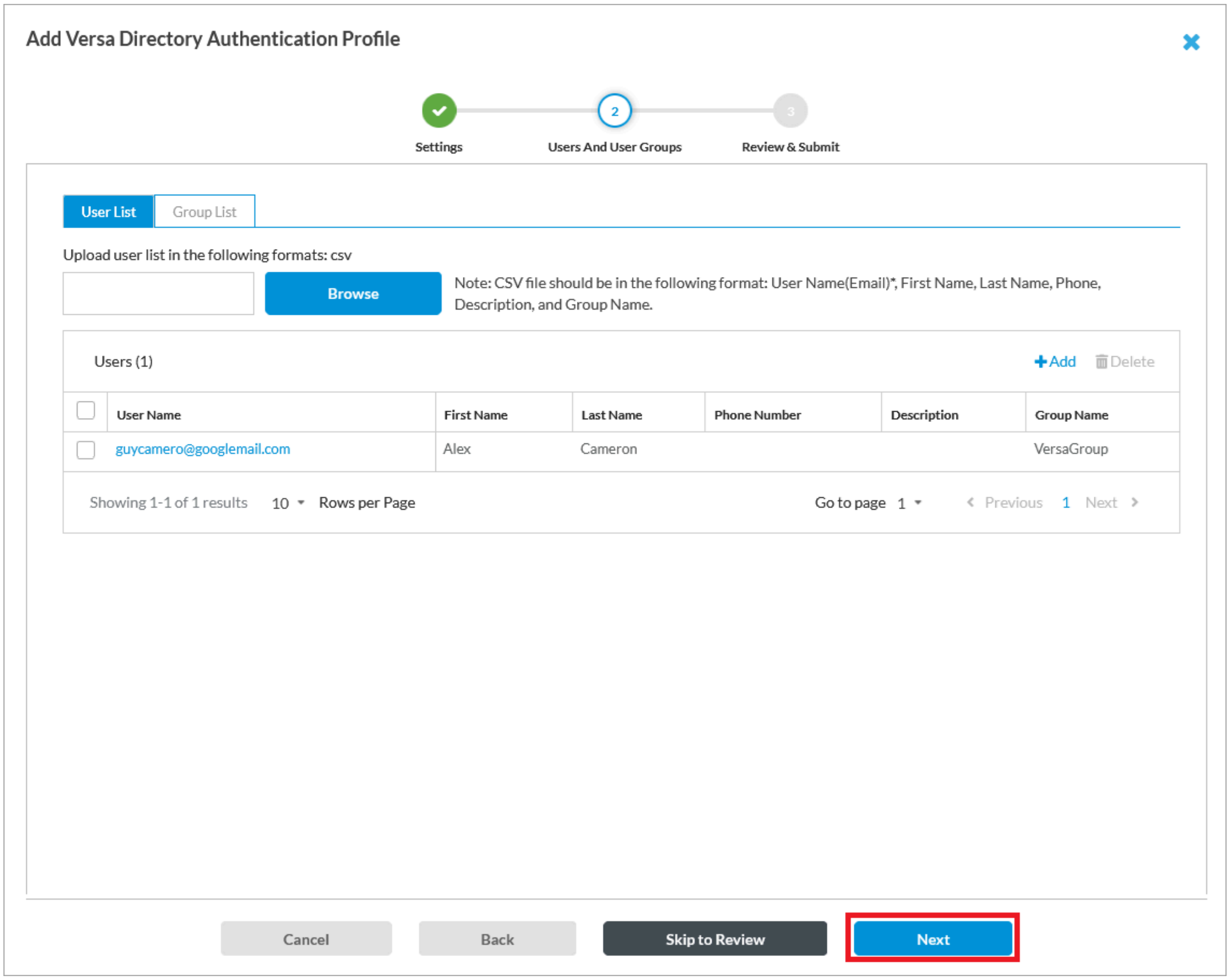
Last Name*: Cameron

Phone Number:

Description:

Group Name*: VersaGroup

Click Next to continue.



Add Versa Directory Authentication Profile

Upload user list in the following formats: csv

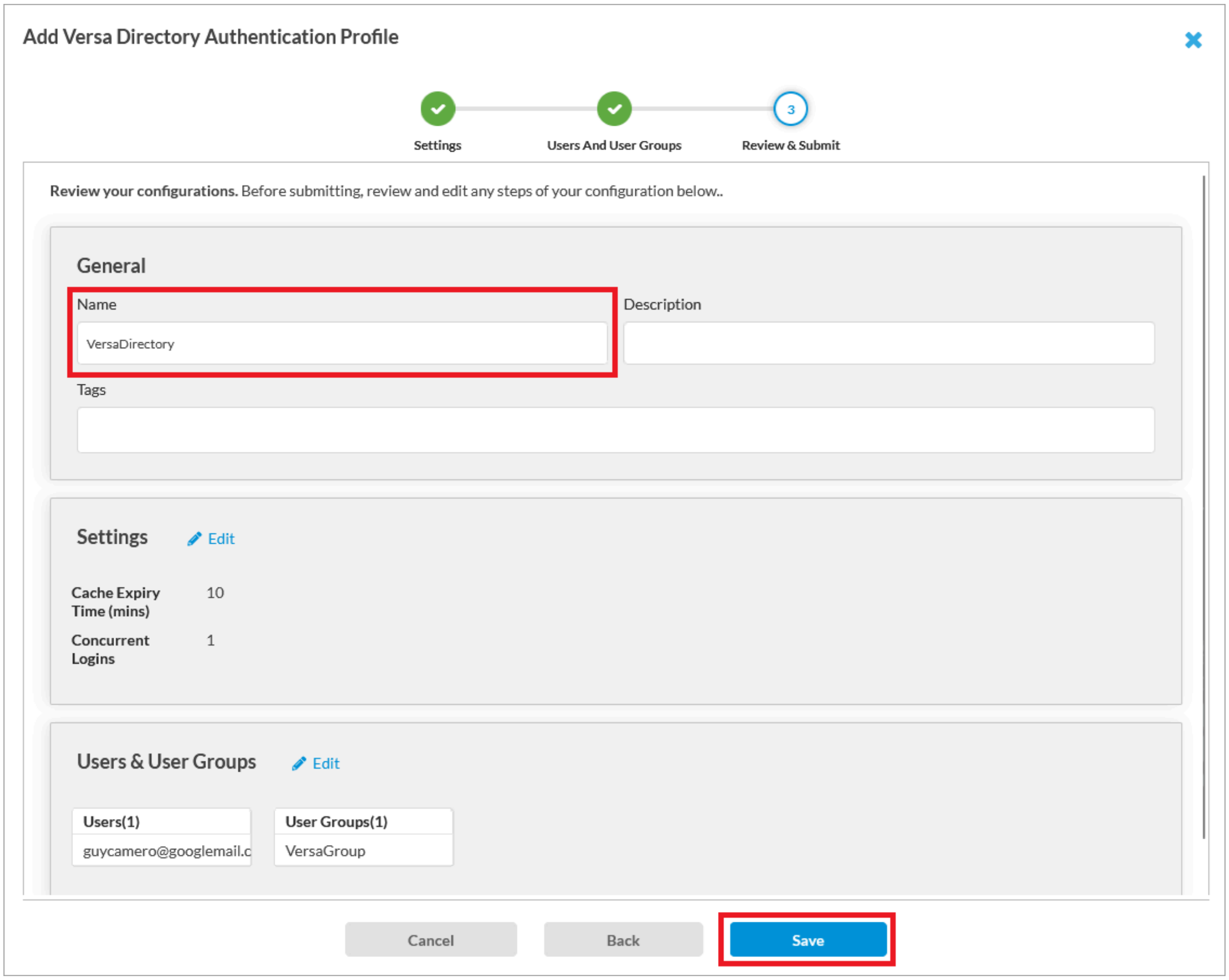
Note: CSV file should be in the following format: User Name(Email)*, First Name, Last Name, Phone, Description, and Group Name.

Users (1)

□	User Name	First Name	Last Name	Phone Number	Description	Group Name
□	guycamero@googlemail.com	Alex	Cameron			VersaGroup

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

Enter a name for the new directory authentication profile and select Save.



Add Versa Directory Authentication Profile

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

General

Name: VersaDirectory

Description:

Tags:

Settings

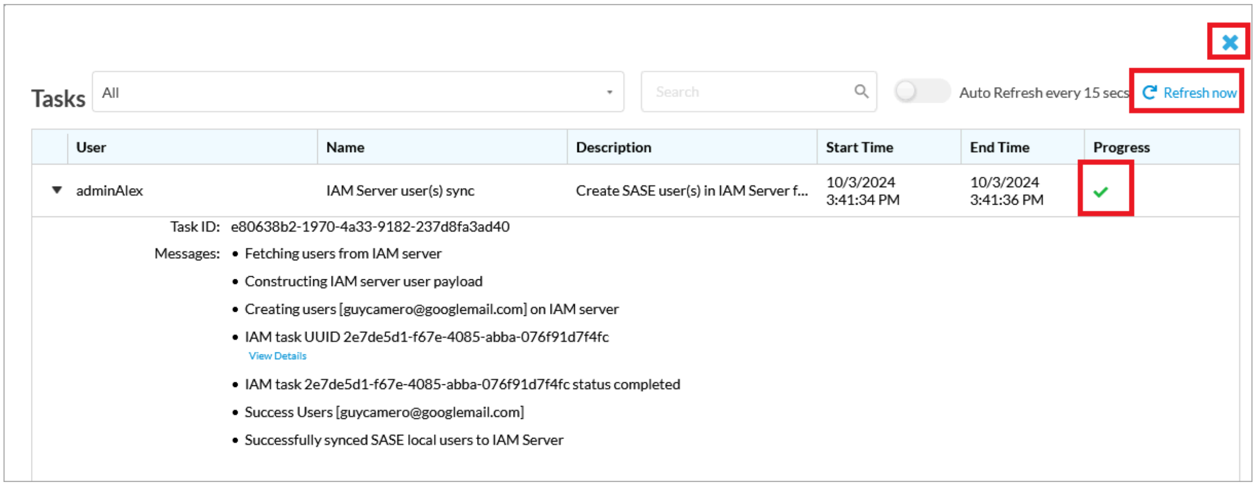
Cache Expiry Time (mins): 10

Concurrent Logins: 1

Users & User Groups

Users(1)	User Groups(1)
guycamero@googlemail.c	VersaGroup

The new profile is saved to Concerto. You can click Refresh Now to check that the status is successful. Close the window when it is finished.



Tasks

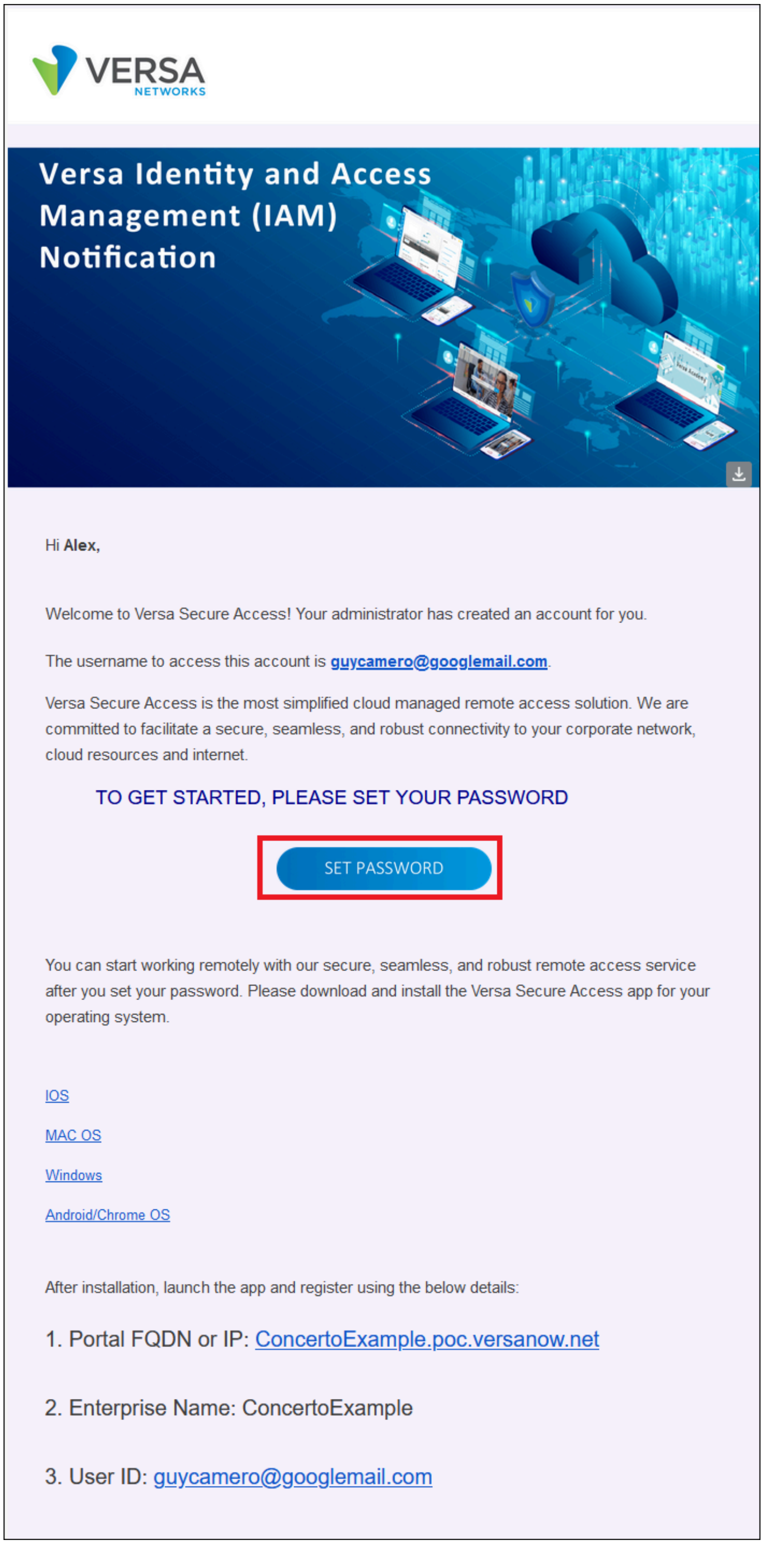
User	Name	Description	Start Time	End Time	Progress
adminAlex	IAM Server user(s) sync	Create SASE user(s) in IAM Server f...	10/3/2024 3:41:34 PM	10/3/2024 3:41:36 PM	✓

Task ID: e80638b2-1970-4a33-9182-237d8fa3ad40

Messages:
- Fetching users from IAM server
- Constructing IAM server user payload
- Creating users [guycamero@googlemail.com] on IAM server
- IAM task UUID 2e7de5d1-f67e-4085-abba-076f91d7f4fc
  View Details
- IAM task 2e7de5d1-f67e-4085-abba-076f91d7f4fc status completed
- Success Users [guycamero@googlemail.com]
- Successfully synced SASE local users to IAM Server

Step 4: Set the Versa Directory User Password and Install SASE Client

Log in to the email account that was referenced in the Versa Directory. Your email should have a message from Versa Networks letting you know a new account was created. Click SET PASSWORD to create a new password.



Hi **Alex,**

Welcome to Versa Secure Access! Your administrator has created an account for you.

The username to access this account is **guycamero@googlemail.com**.

Versa Secure Access is the most simplified cloud managed remote access solution. We are committed to facilitate a secure, seamless, and robust connectivity to your corporate network, cloud resources and internet.

TO GET STARTED, PLEASE SET YOUR PASSWORD

You can start working remotely with our secure, seamless, and robust remote access service after you set your password. Please download and install the Versa Secure Access app for your operating system.

IOS

MAC OS

Windows

Android/Chrome OS

After installation, launch the app and register using the below details:

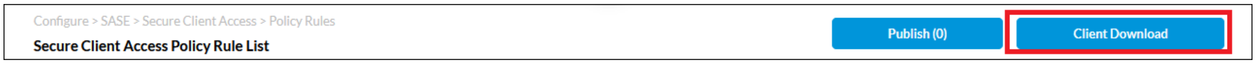
1. Portal FQDN or IP: ConcertoExample.poc.versanow.net

2. Enterprise Name: ConcertoExample

3. User ID: guycamero@googlemail.com

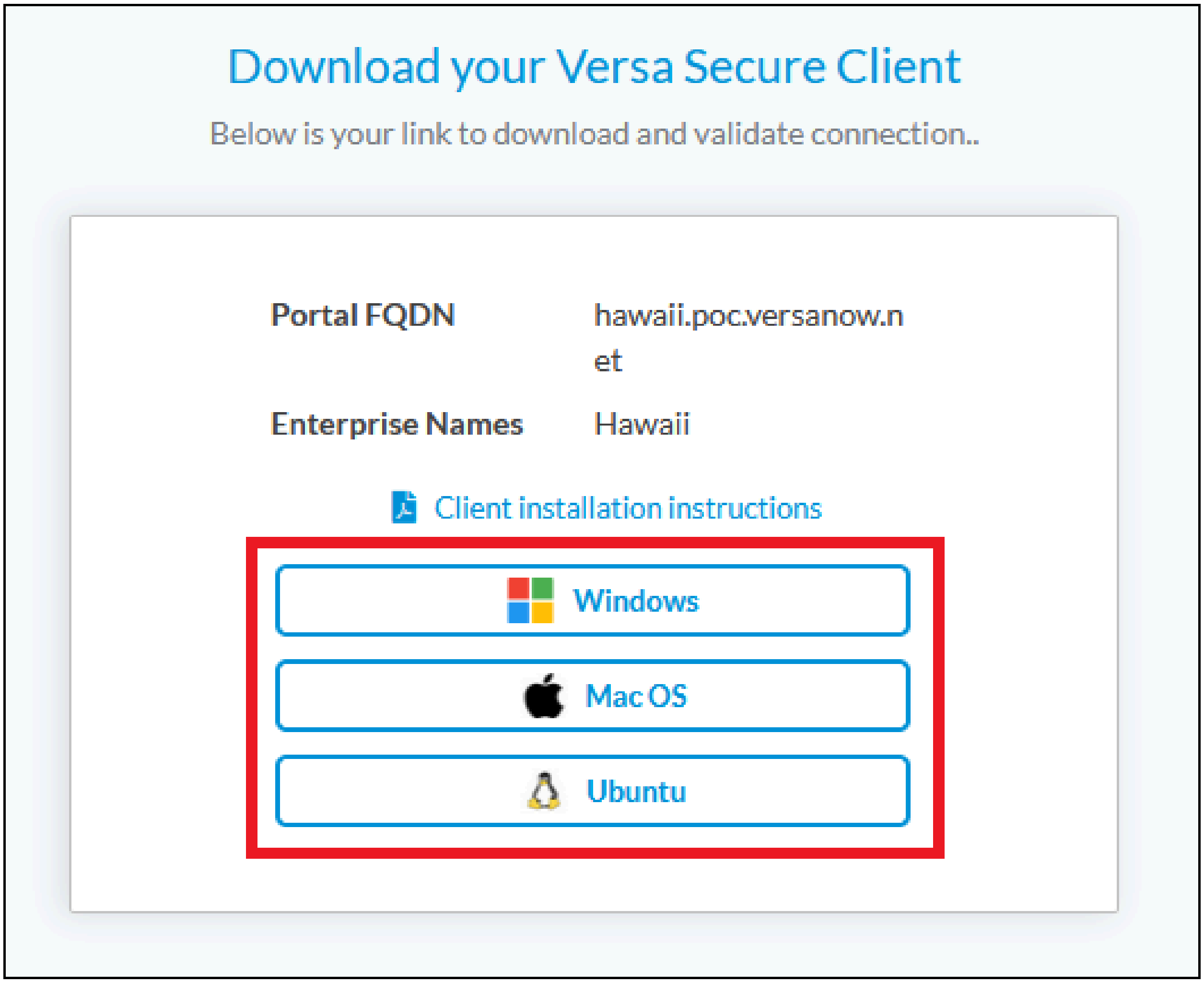
Note that if you are an enterprise user that will be leveraging Versa Directory, all users (email addresses) will receive the welcome message to set their password. If you are an administrator and your enterprise is using a different IDP, such as Okta, Azure AD, or Entrata, you will have to generate an email to your organization with the download link and instructions (or automate this process using your IT automation tools).

To access this information, navigate to Configure > Secure Client Access > Policy Rules. In the upper right corner, next to Publish, click the Client Download link.



Configure > SASE > Secure Client Access > Policy Rules

Secure Client Access Policy Rule List



Download your Versa Secure Client

Below is your link to download and validate connection..

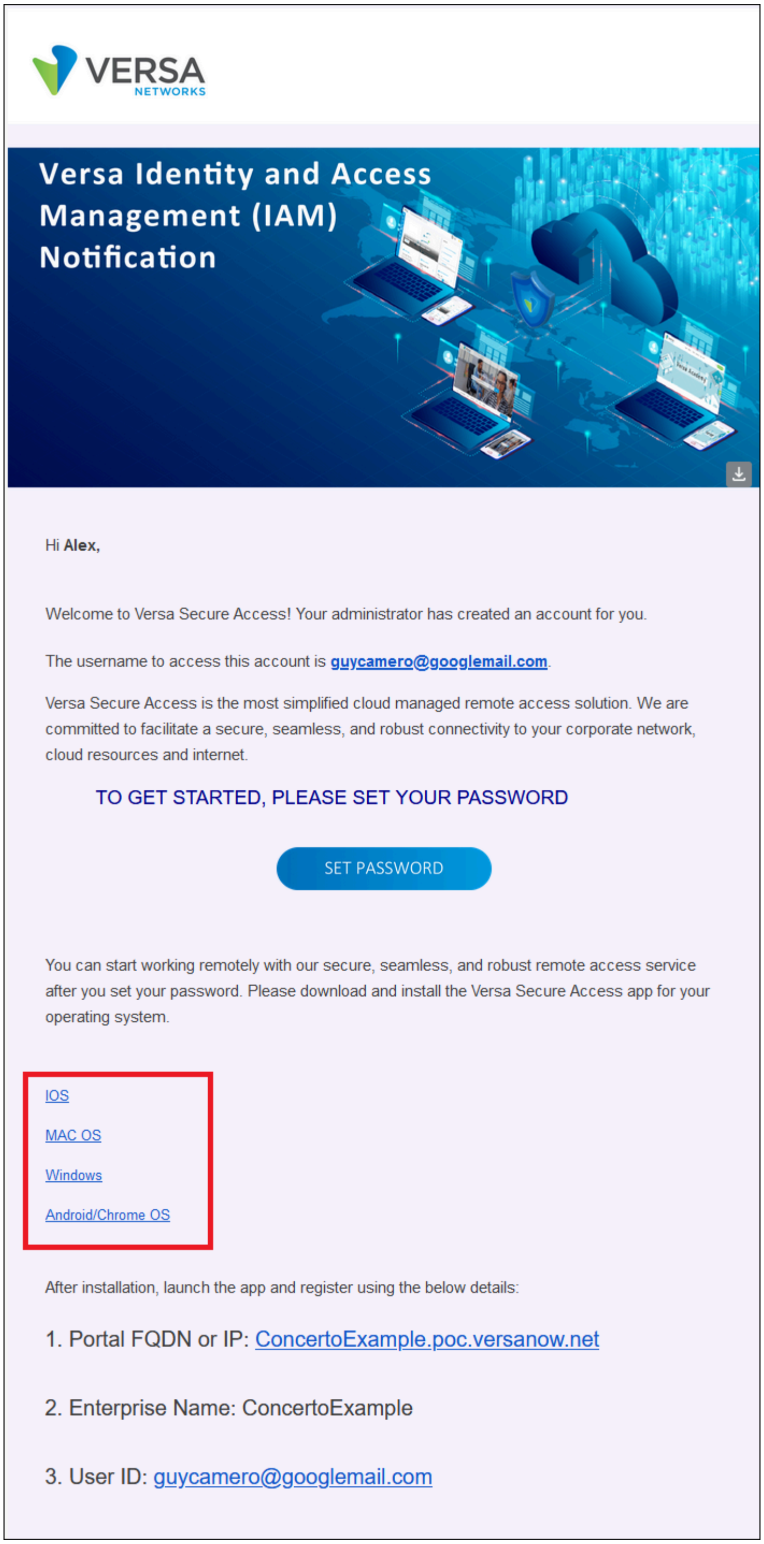
Portal FQDN hawaii.poc.versanow.net

Enterprise Names Hawaii

Client installation instructions

From the device on which you want to install the Versa Client, open the email from Versa, and then select to install the correct software for your device.

Windows is used as an example in this guide.



Versa Identity and Access Management (IAM) Notification

Hi **Alex,**

Welcome to Versa Secure Access! Your administrator has created an account for you.

The username to access this account is **guycamero@googlemail.com**.

Versa Secure Access is the most simplified cloud managed remote access solution. We are committed to facilitate a secure, seamless, and robust connectivity to your corporate network, cloud resources and internet.

TO GET STARTED, PLEASE SET YOUR PASSWORD

You can start working remotely with our secure, seamless, and robust remote access service after you set your password. Please download and install the Versa Secure Access app for your operating system.

IOS

MAC OS

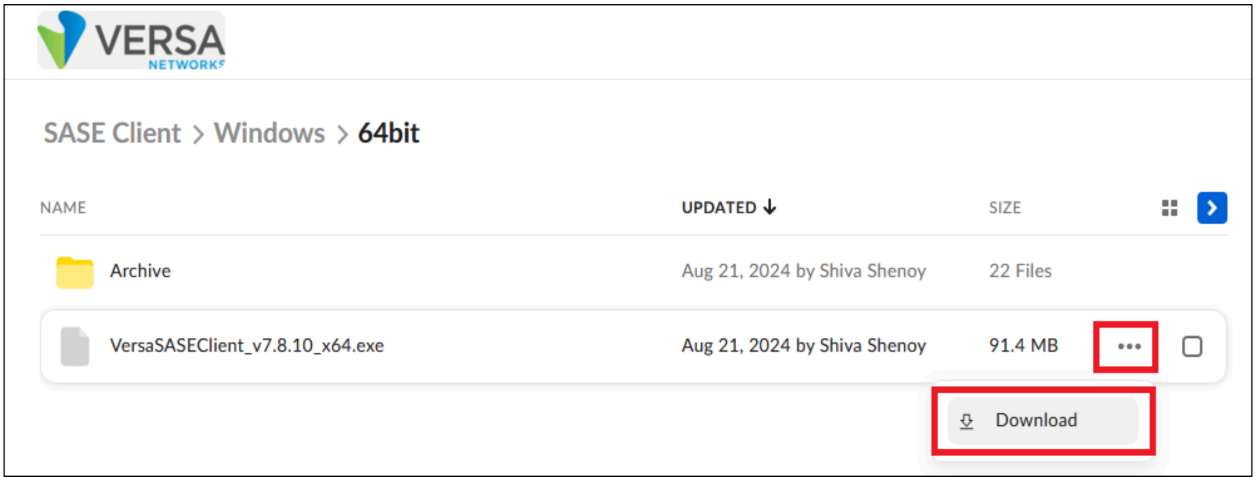
Windows

Android/Chrome OS

After installation, launch the app and register using the below details:

1. Portal FQDN or IP: ConcertoExample.poc.versanow.net
2. Enterprise Name: ConcertoExample
3. User ID: guycamero@googlemail.com

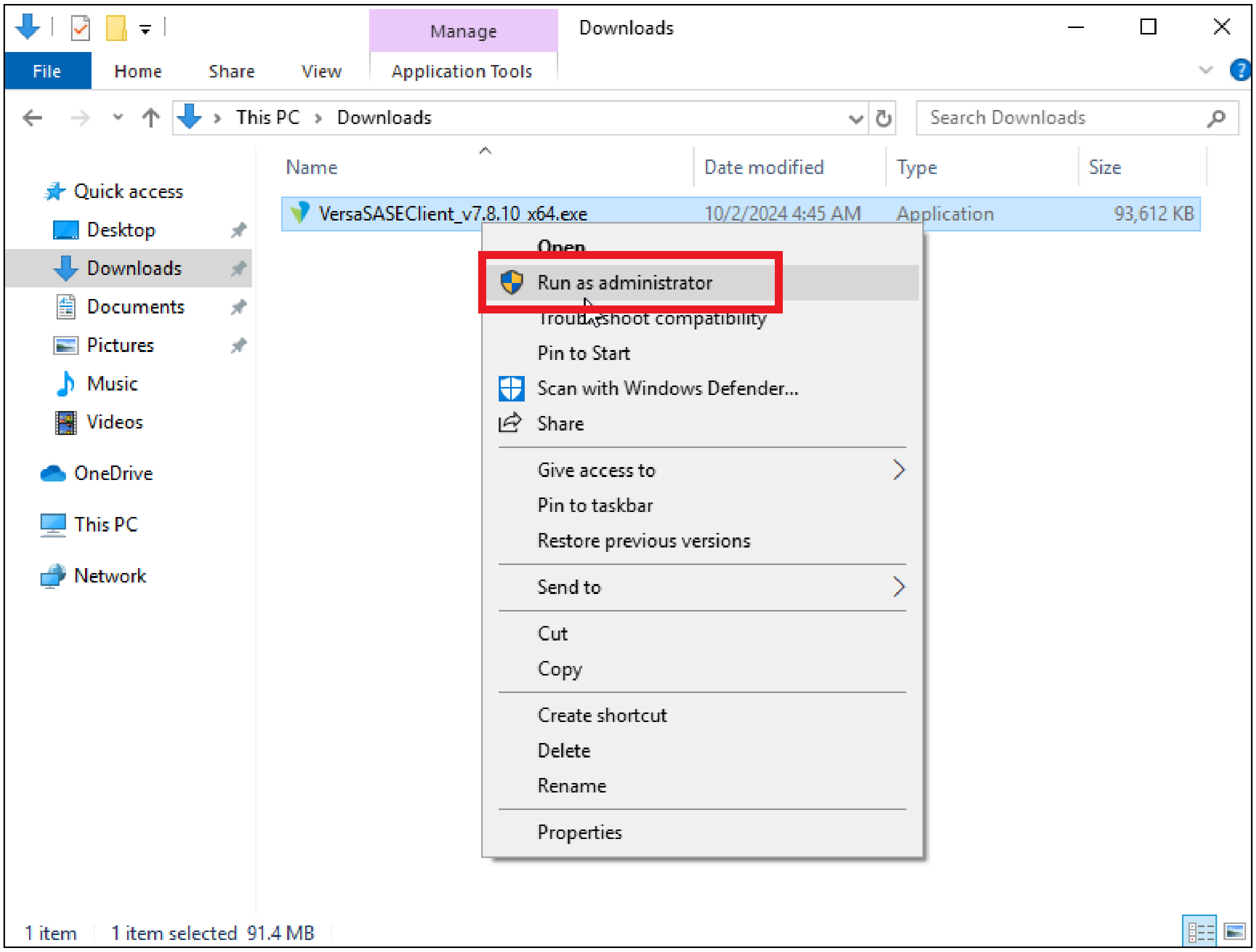
Follow the steps to download the Versa SASE Client.



SASE Client > Windows > 64bit

NAME	UPDATED ↓	SIZE
Archive	Aug 21, 2024 by Shiva Shenoy	22 Files
VersaSASEClient_v7.8.10_x64.exe	Aug 21, 2024 by Shiva Shenoy	91.4 MB

Install the Versa SASE Client executable.



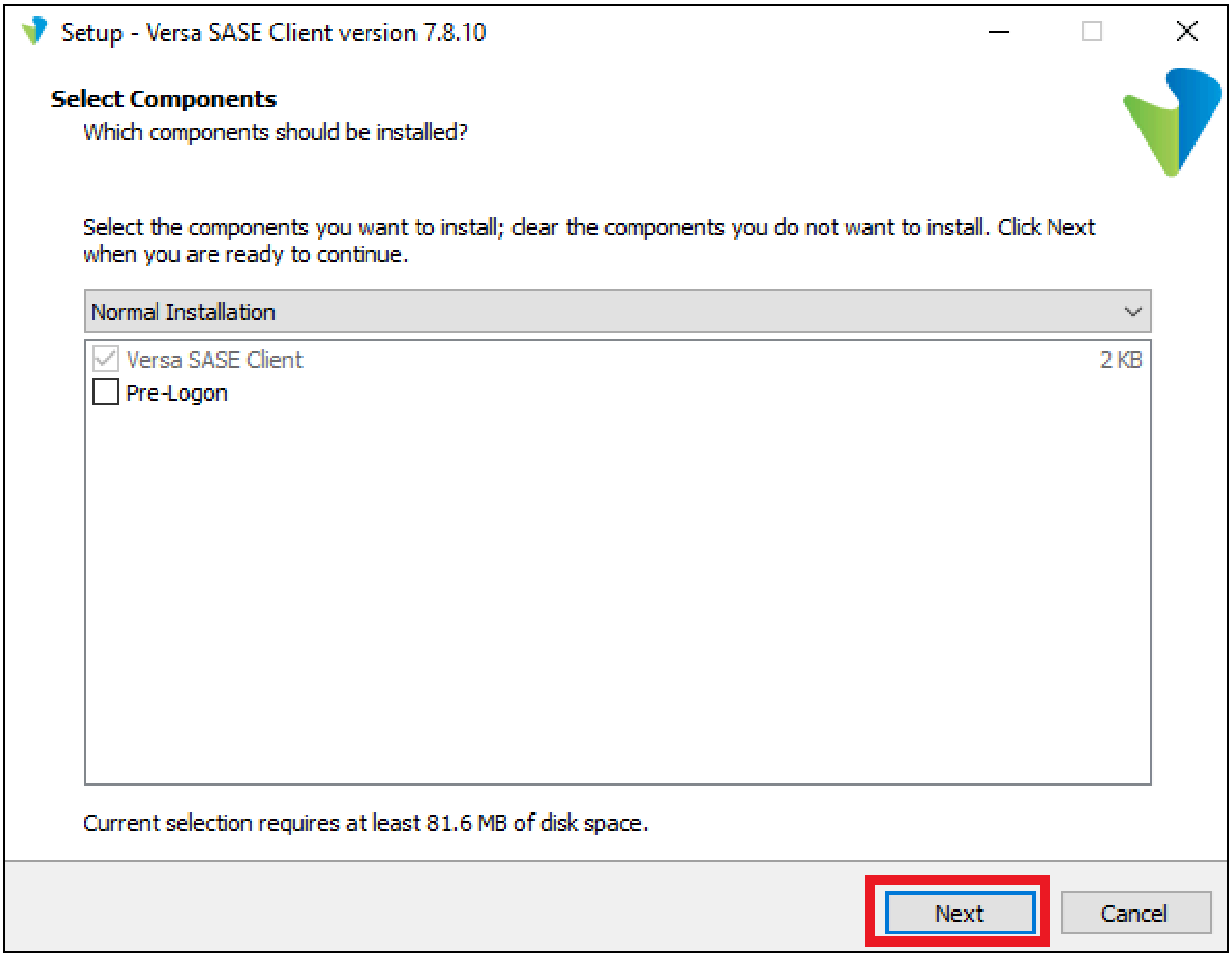
Downloads

This PC > Downloads

Name	Date modified	Type	Size
VersaSASEClient_v7.8.10_x64.exe	10/2/2024 4:45 AM	Application	93,612 KB

1 item 1 item selected 91.4 MB

Click Next to continue.



Select Components

Which components should be installed?

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

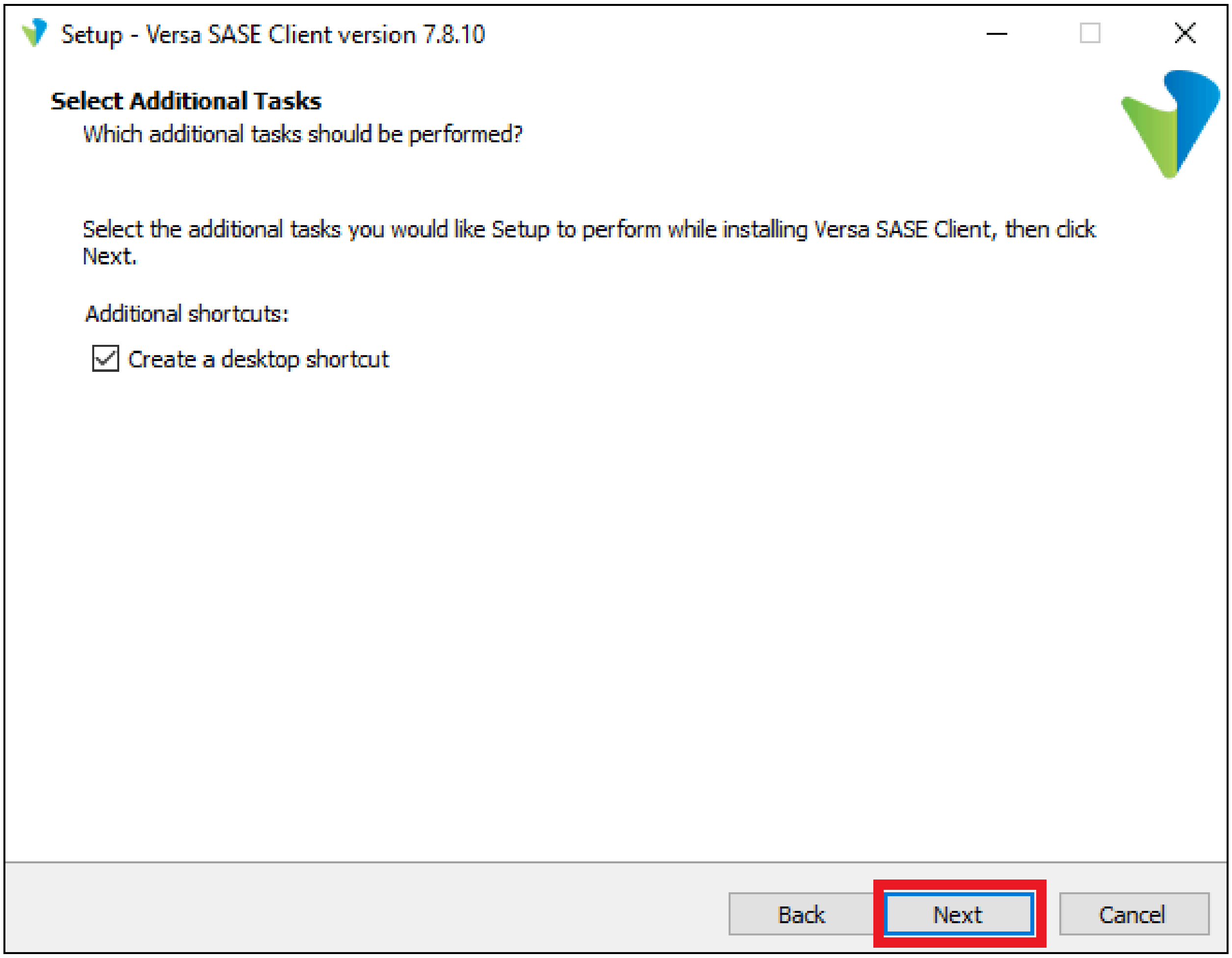
Normal Installation

☑ Versa SASE Client 2 KB

□ Pre-Logon

Current selection requires at least 81.6 MB of disk space.

Create a desktop shortcut, if you prefer, and then click Next.



Setup - Versa SASE Client version 7.8.10

Select Additional Tasks

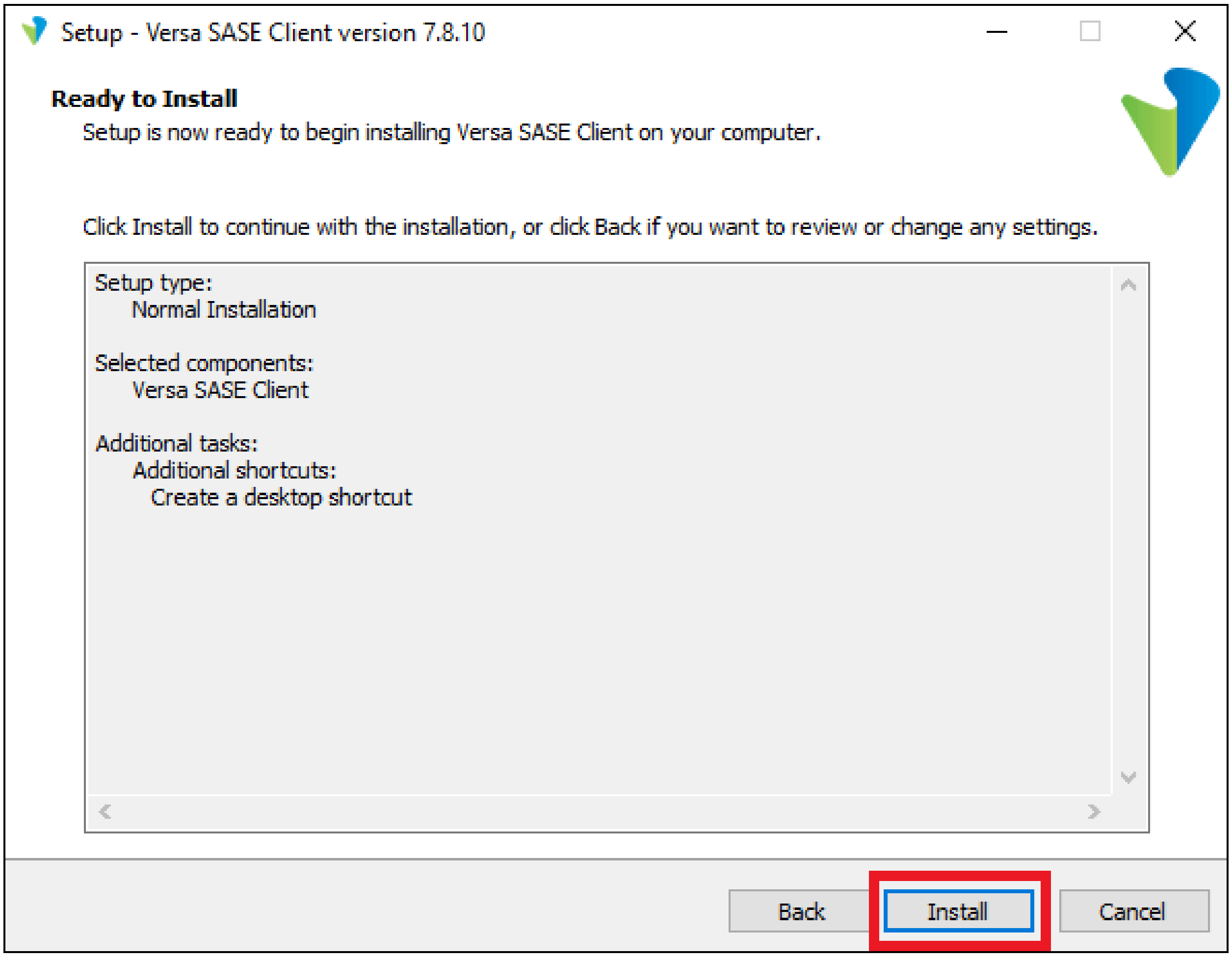
Which additional tasks should be performed?

Select the additional tasks you would like Setup to perform while installing Versa SASE Client, then click Next.

Additional shortcuts:

☑ Create a desktop shortcut

Select Install to install Versa SASE Client with the set configuration.



Ready to Install

Setup is now ready to begin installing Versa SASE Client on your computer.

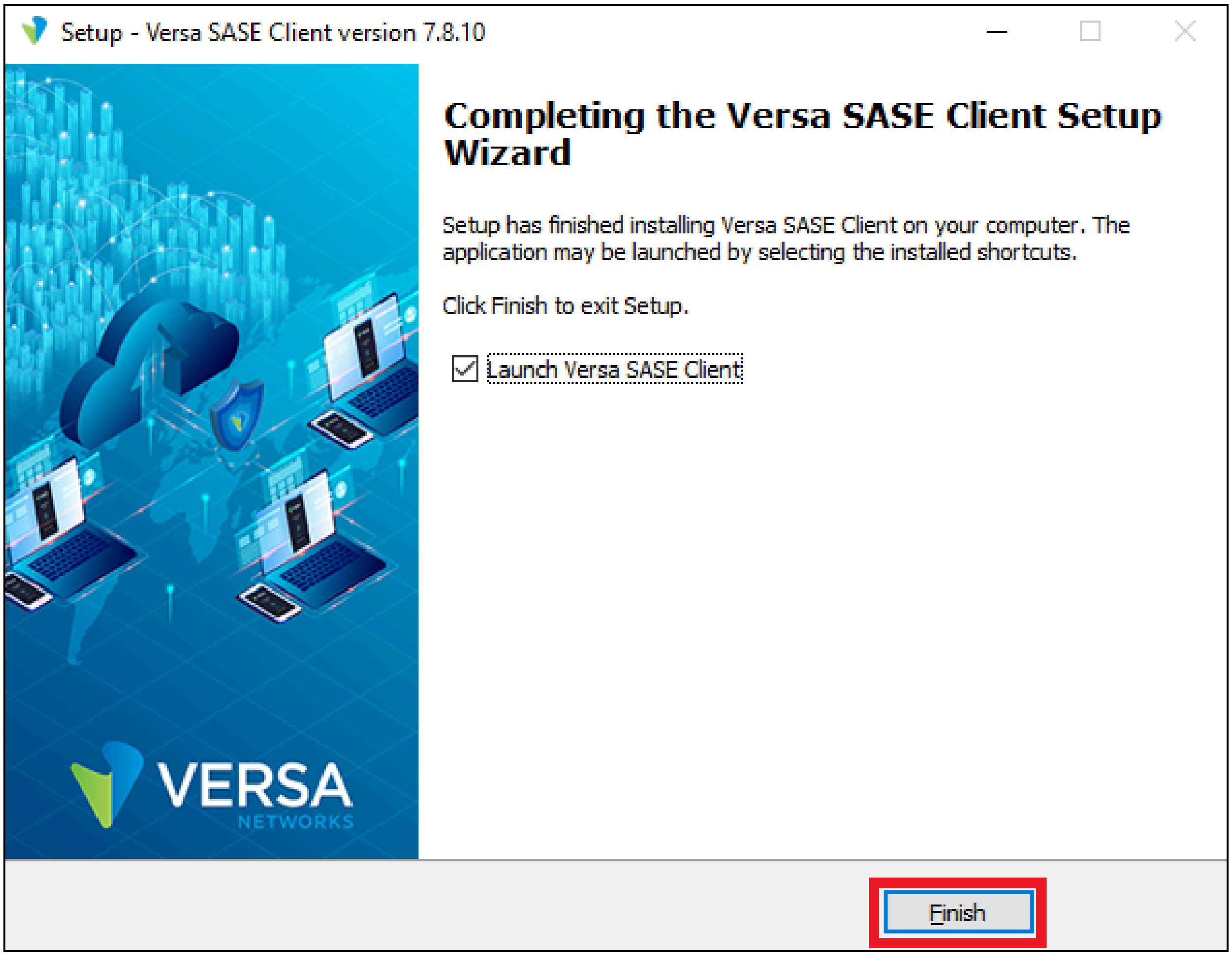
Click Install to continue with the installation, or click Back if you want to review or change any settings.

```
Setup type:
    Normal Installation

Selected components:
    Versa SASE Client

Additional tasks:
    Additional shortcuts:
      Create a desktop shortcut
```

Select Finish when completed. The Versa SASE Client screen displays after finalizing configurations in Concerto.



Setup - Versa SASE Client version 7.8.10

Completing the Versa SASE Client Setup Wizard

Setup has finished installing Versa SASE Client on your computer. The application may be launched by selecting the installed shortcuts.

Click Finish to exit Setup.

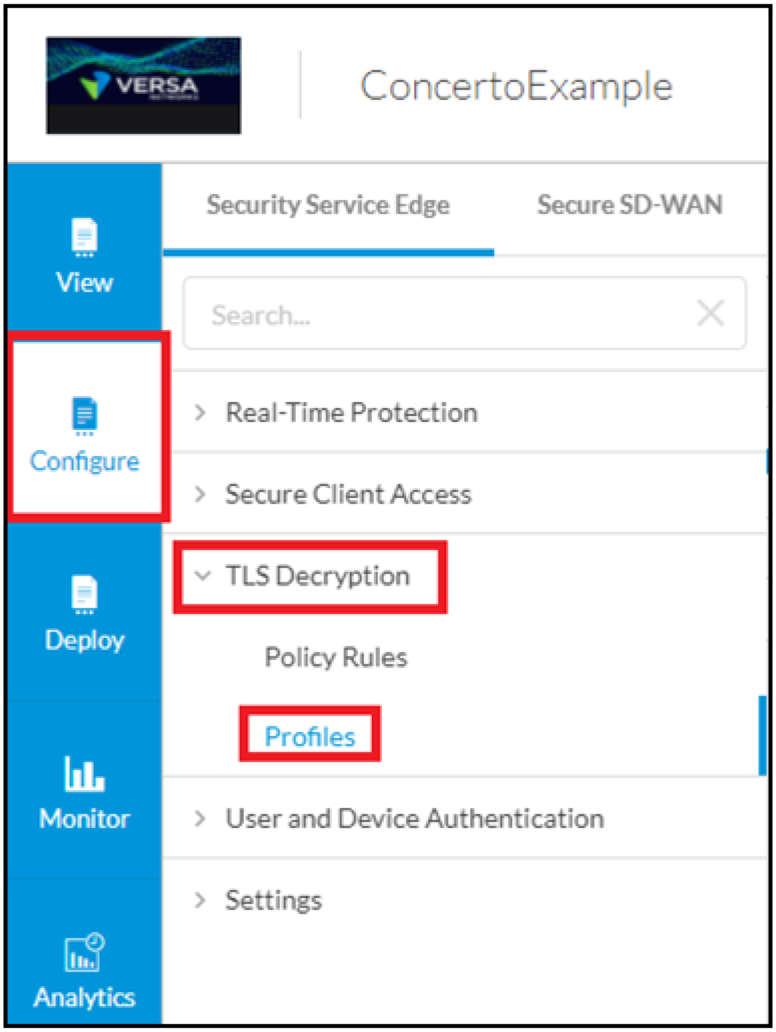
☑ Launch Versa SASE Client

Step 5: Configure Decryption Profiles

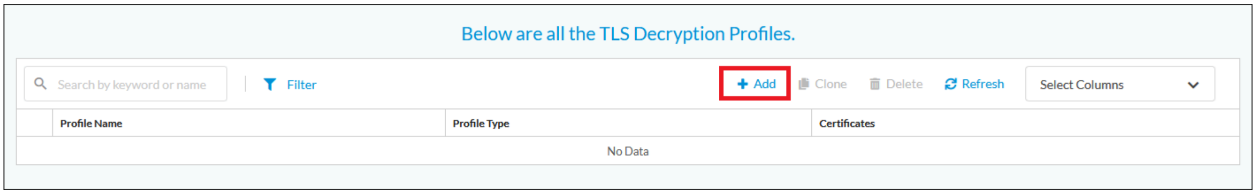
For more information, see Configure TLS Decryption.

The TLS decryption configuration is optional, however it provides additional capabilities and is required when using advanced security protection functions such as CASB and DLP. You can upload your own certificate chain or leverage the auto-generated certificate provided and signed by Versa Networks, and is installed on your client machines when the Versa SASE client application is installed.

In the Concerto Orchestrator, click Configure > TLS Decryption > Profiles.

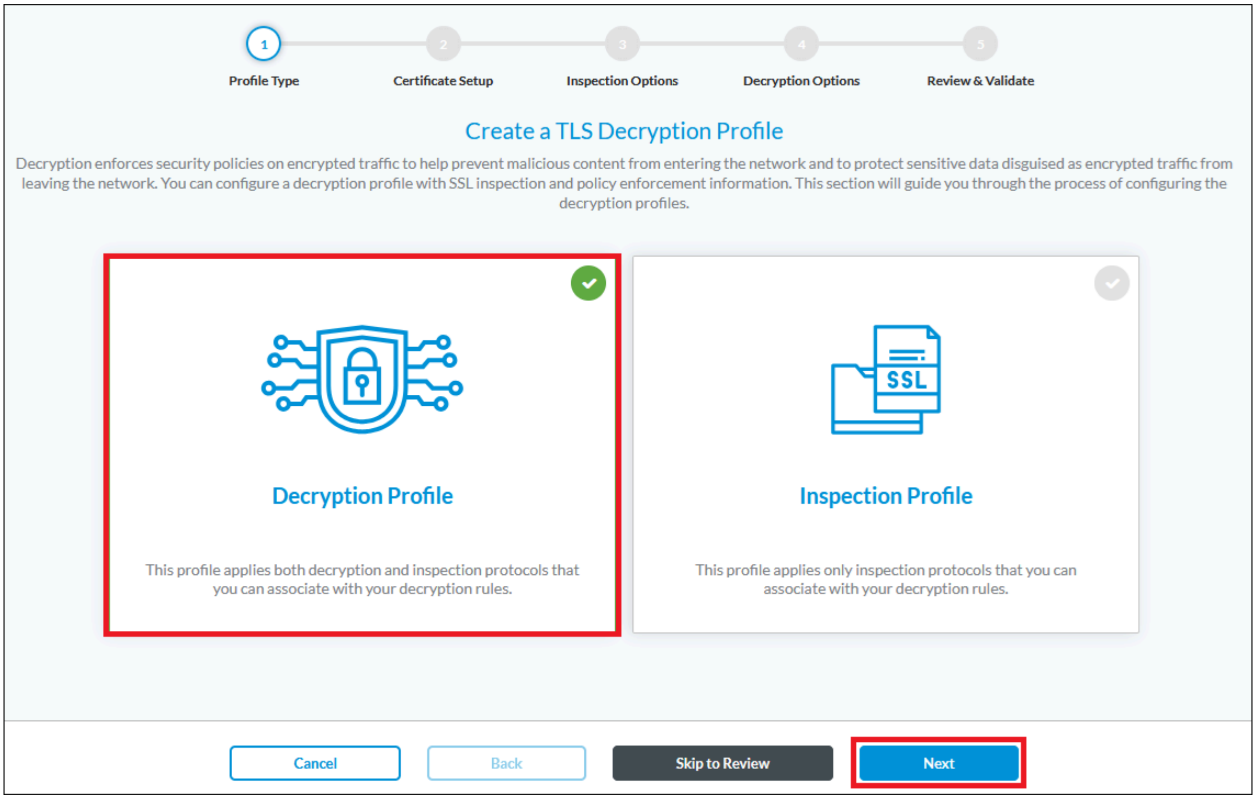


Click +Add to create a TLS decryption profile.


Below are all the TLS Decryption Profiles.
Search by keyword or name
Filter
+ Add
Clone
Delete
Refresh
Select Columns

Profile Name	Profile Type	Certificates
	No Data	

Depending on your requirements, you can decrypt traffic or inspect traffic. Select Decryption Profile, and then click Next.



Create a TLS Decryption Profile

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

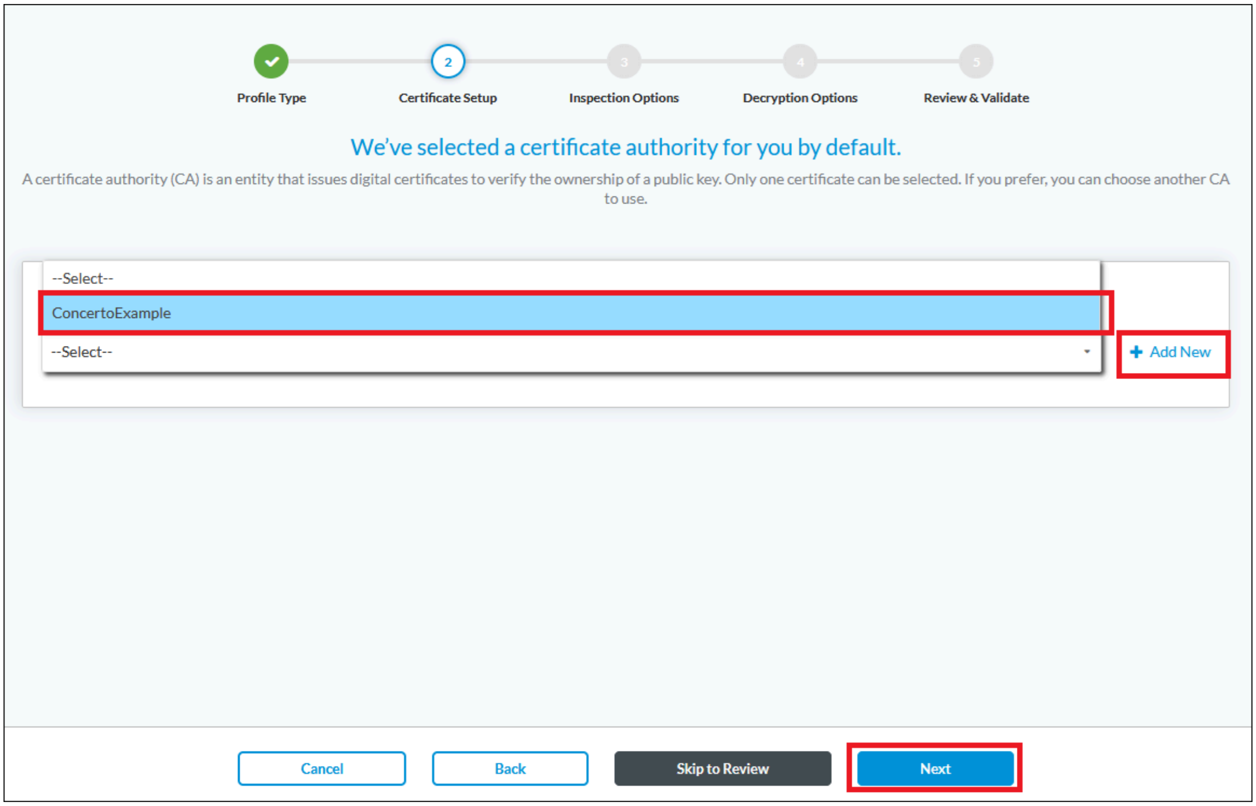
Decryption Profile

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

Inspection Profile

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

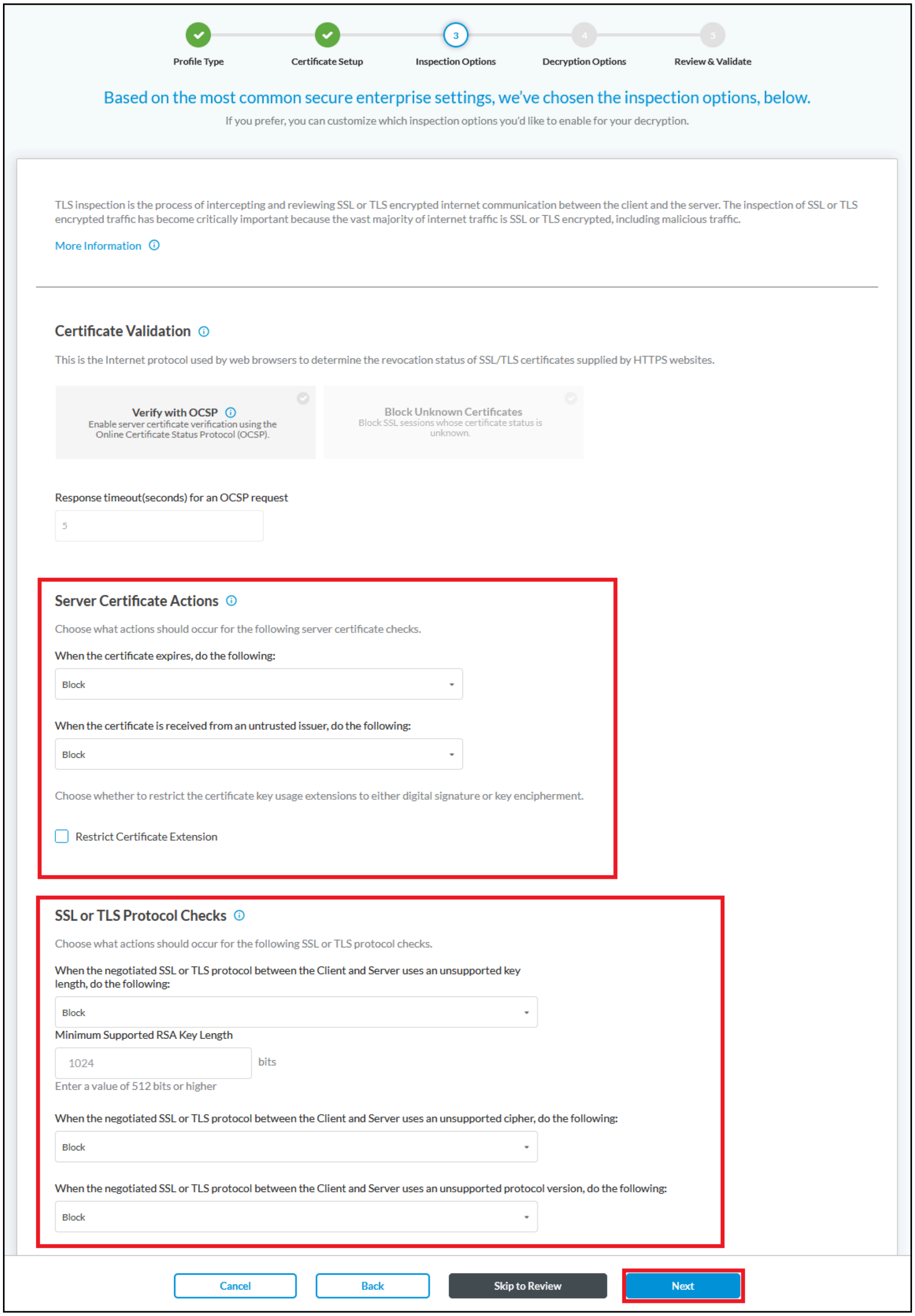
Versa Networks automatically creates a CA Certificate for you. You can upload your own certificate, but for this example, the Versa-generated certificate is used.



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.

Under Inspection Options, configure how to handle unsupported or expired certificates.



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 or TLS encrypted internet communication between the client and the server. The inspection of SSL or TLS encrypted traffic has become critically important because the vast majority of internet traffic is SSL or 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.

Verify with OCSP
Enable server certificate verification using the Online Certificate Status Protocol (OCSP).

Block Unknown Certificates
Block SSL sessions whose certificate status is unknown.

Response timeout(seconds) for an OCSP request: 5

Server Certificate Actions

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 or TLS Protocol Checks

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

When the negotiated SSL or TLS protocol between the Client and Server uses an unsupported key length, do the following: Block

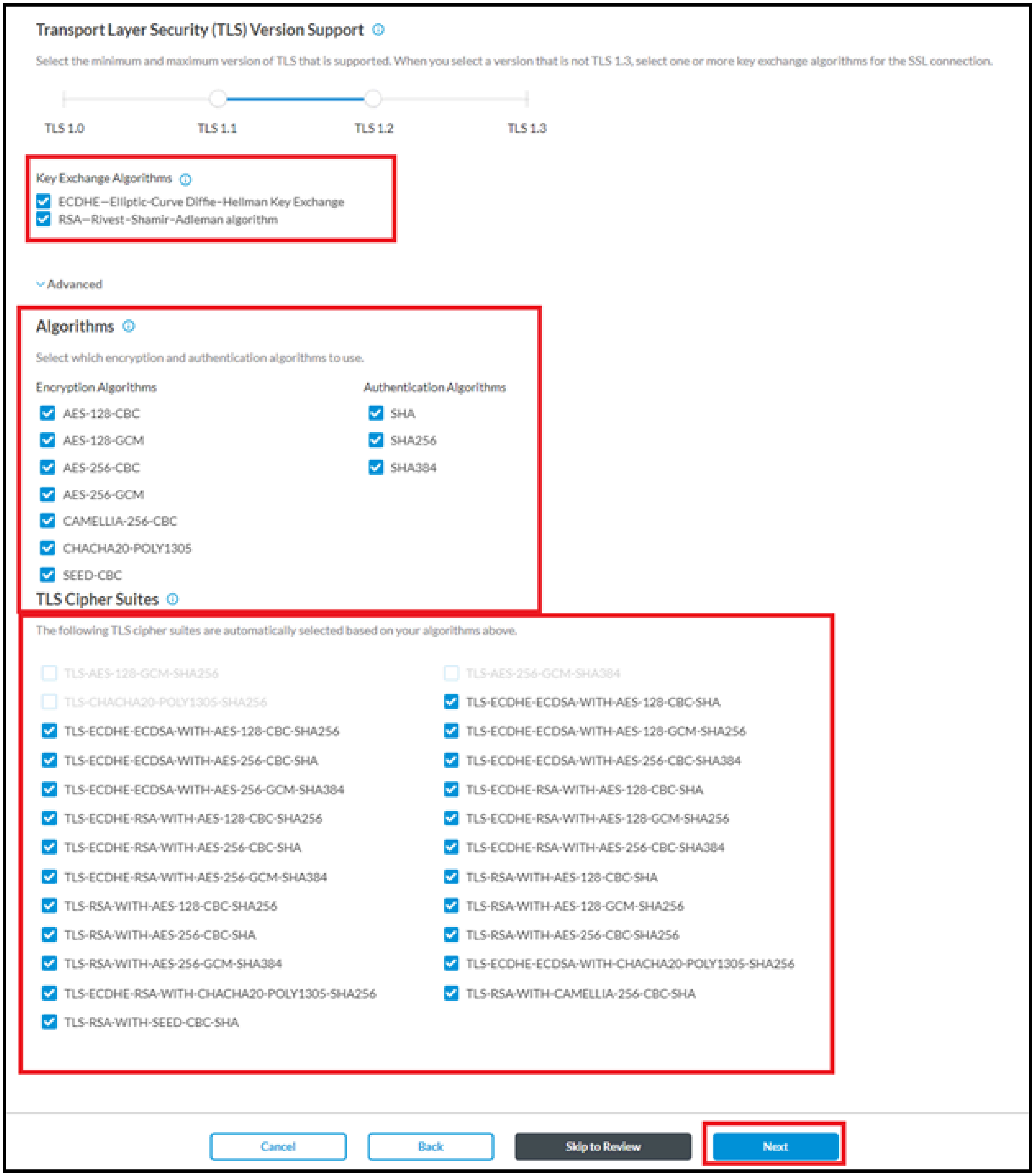
Minimum Supported RSA Key Length: 1024 bits

Enter a value of 512 bits or higher

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

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

Select the decryption options you would like to support. This example uses the following settings.



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

Algorithms

Select which encryption and authentication algorithms to use.

Encryption Algorithms

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

Authentication Algorithms

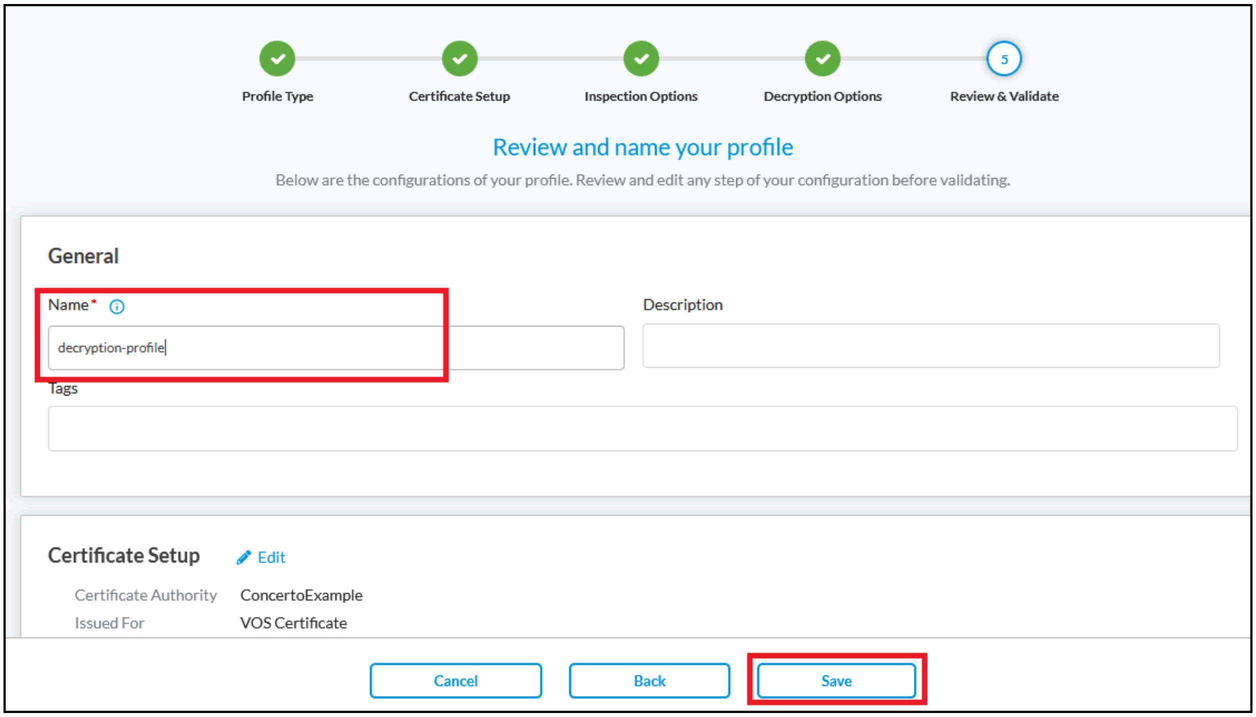
- ☑ SHA
- ☑ SHA256
- ☑ SHA384

TLS Cipher Suites

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

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

Enter the decryption profile name and select Save.



Review and name your profile

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

General

Name* : decryption-profile

Description

Tags

Certificate Setup

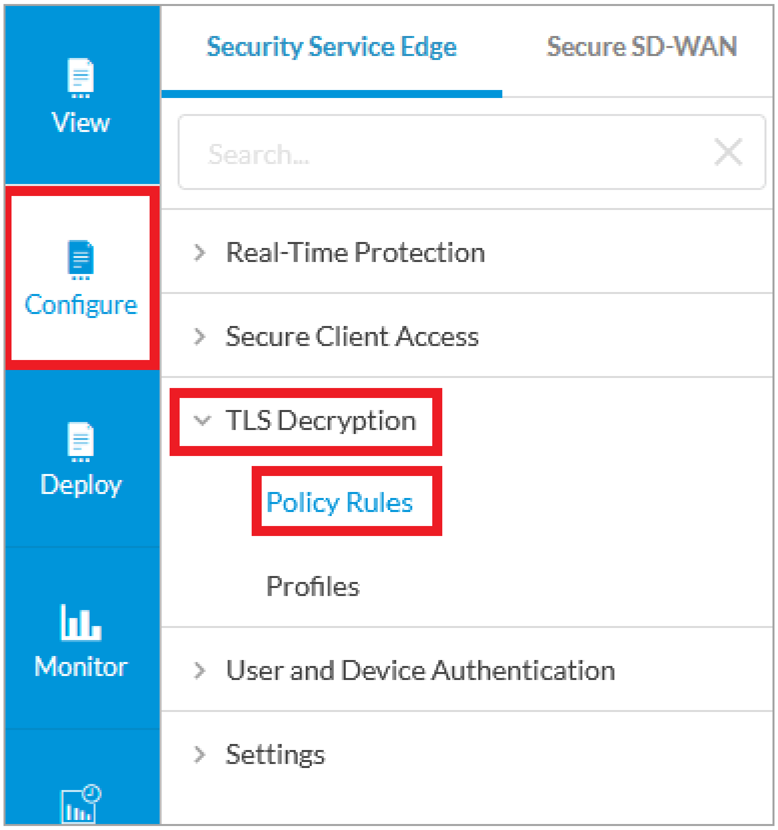
Certificate Authority: ConcertoExample

Issued For: VOS Certificate

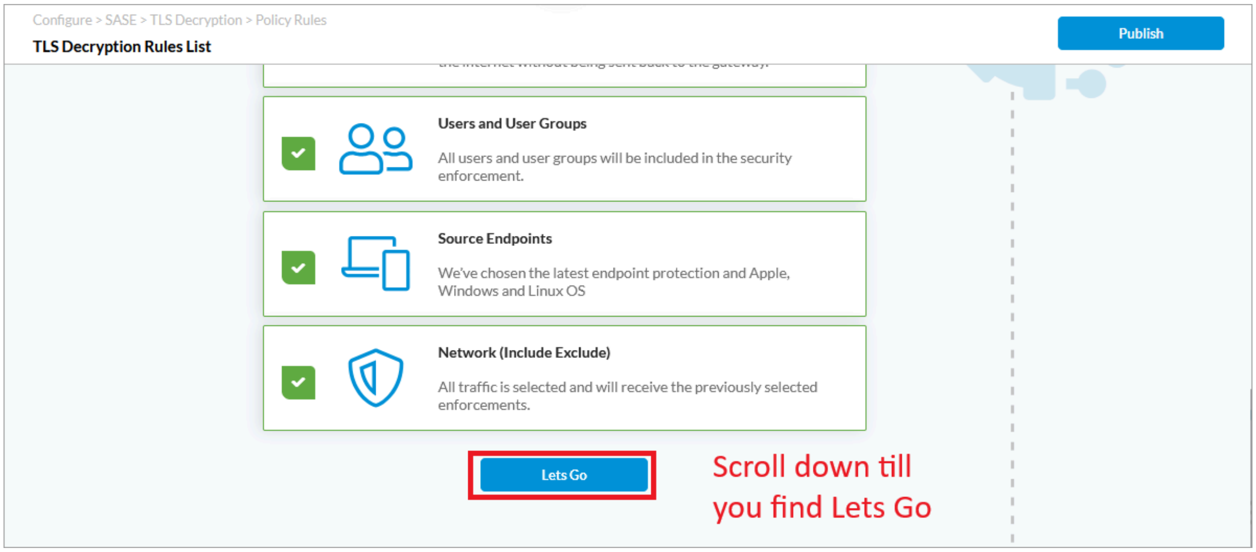
Step 6: Configure a TLS Decryption Policy Rule

For more information, see Configure TLS Decryption.

Select Configure > TLS Decryption > Policy Rules.



In the TLS Decryption Rules List window, scroll down and click Let's Go.


Configure > SASE > TLS Decryption > Policy Rules
TLS Decryption Rules List
Publish
Lets Go
Scroll down till
you find Lets Go

☑ **Users and User Groups**

All users and user groups will be included in the security enforcement.

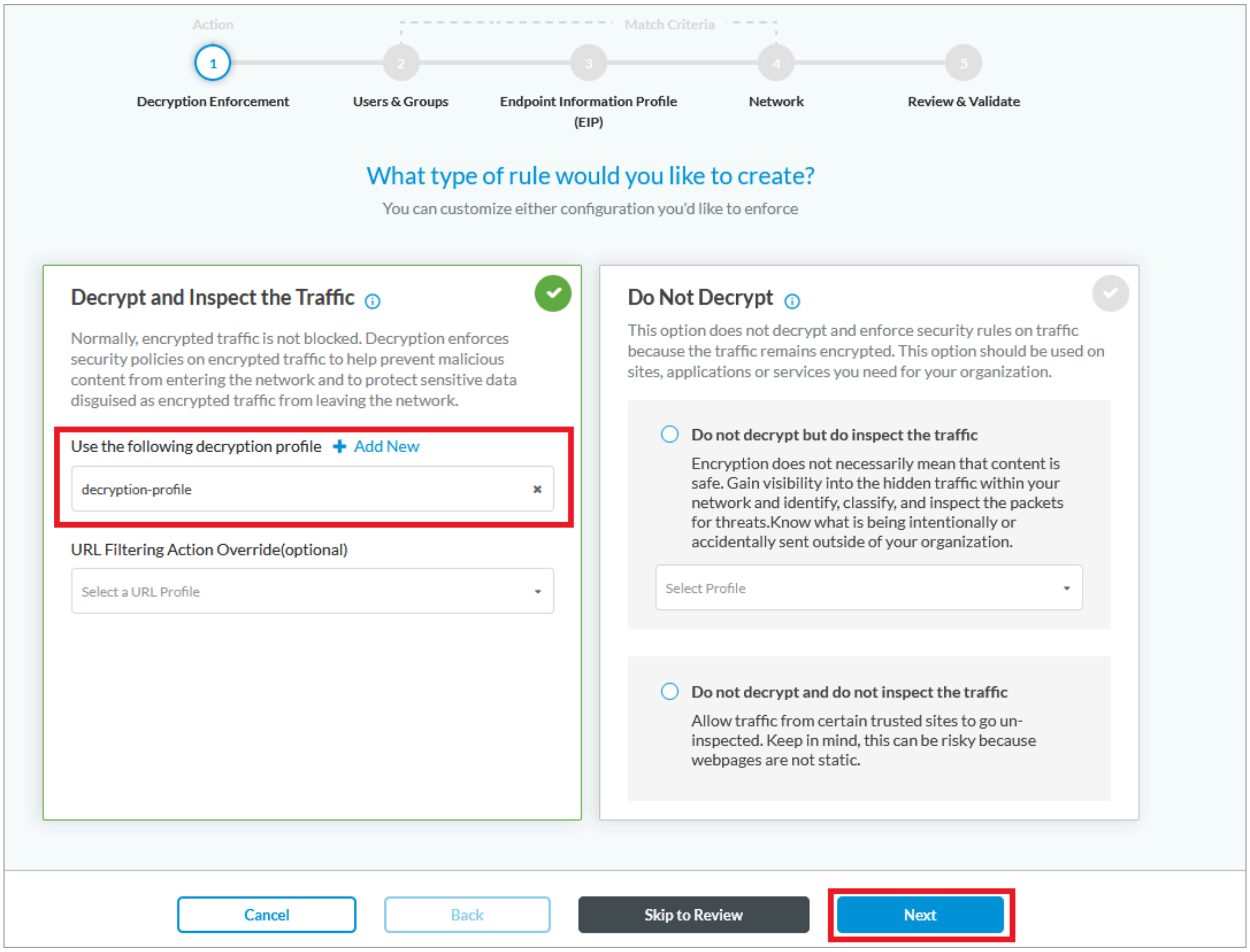
☑ **Source Endpoints**

We've chosen the latest endpoint protection and Apple, Windows and Linux OS

☑ **Network (Include Exclude)**

All traffic is selected and will receive the previously selected enforcements.

Select a decrypt and inspect profile to use in the Decrypt and Inspect the Traffic pane. Note that you can also create Do Not Decrypt rules for traffic that you do not want to decrypt. For example, you can choose not to decrypt personal user information such as financial information.



What type of rule would you like to create?

You can customize either configuration you'd like to enforce

Decrypt and Inspect the Traffic ✓

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

decryption-profile ×

URL Filtering Action Override(optional)

Select a URL Profile

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 but do inspect the traffic**

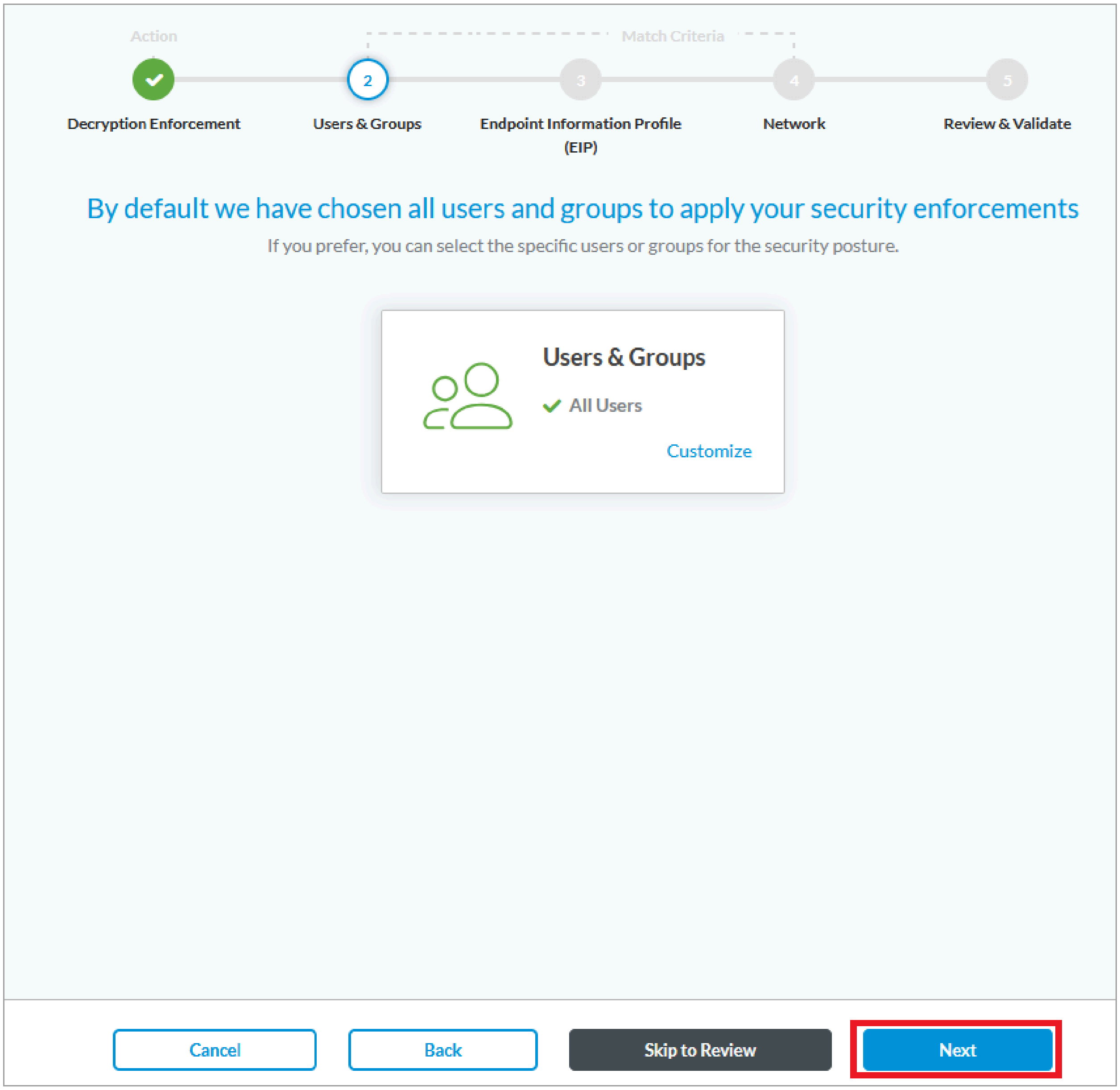
Encryption does not necessarily mean that content is safe. Gain visibility into the hidden traffic within your network and identify, classify, and inspect the packets for threats.Know what is being intentionally or accidentally sent outside of your organization.

Select Profile

○ **Do not decrypt and do not inspect the traffic**

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

For Users & Groups, you can retain the default option All Users, or you can select specific users or groups.



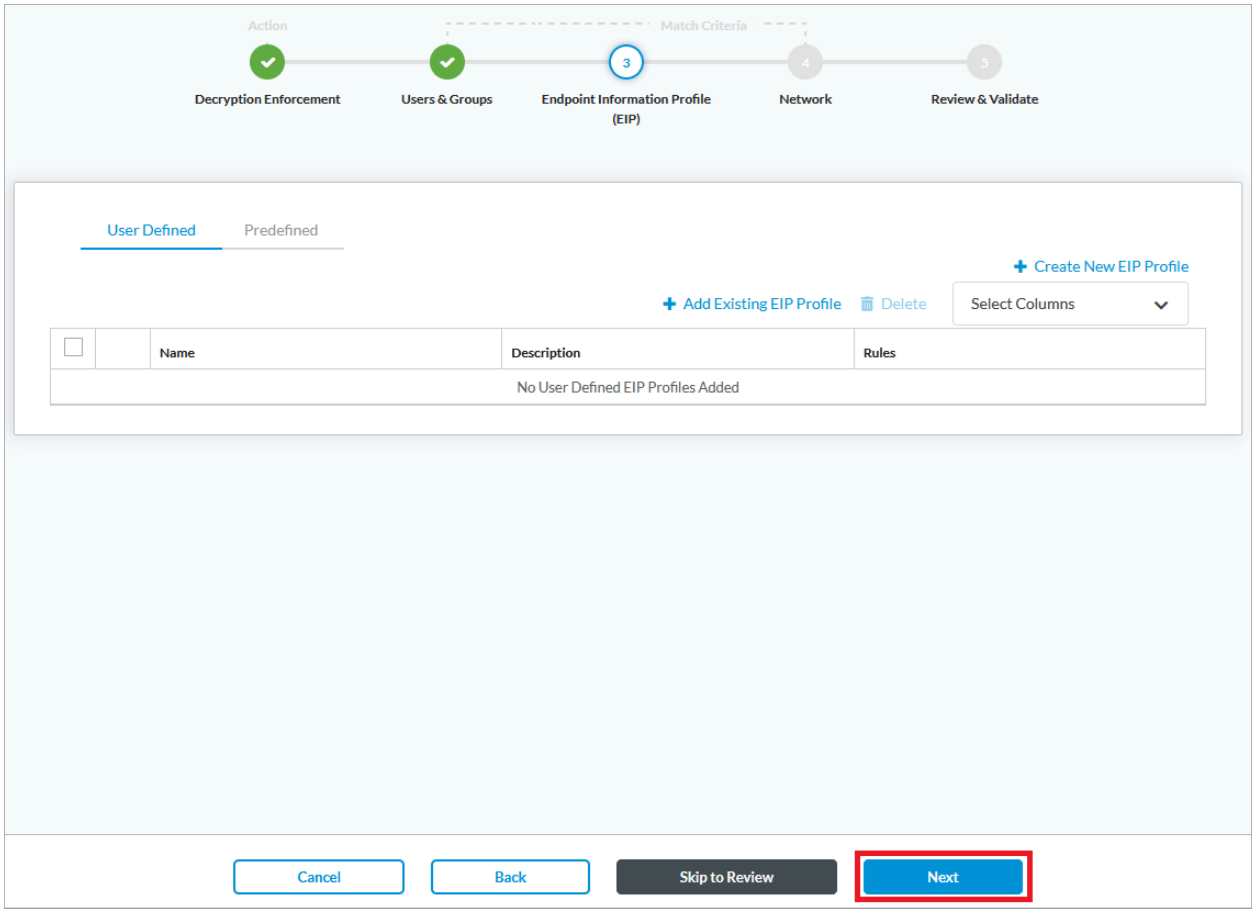
By default we have chosen all users and groups to apply your security enforcements

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

Users & Groups

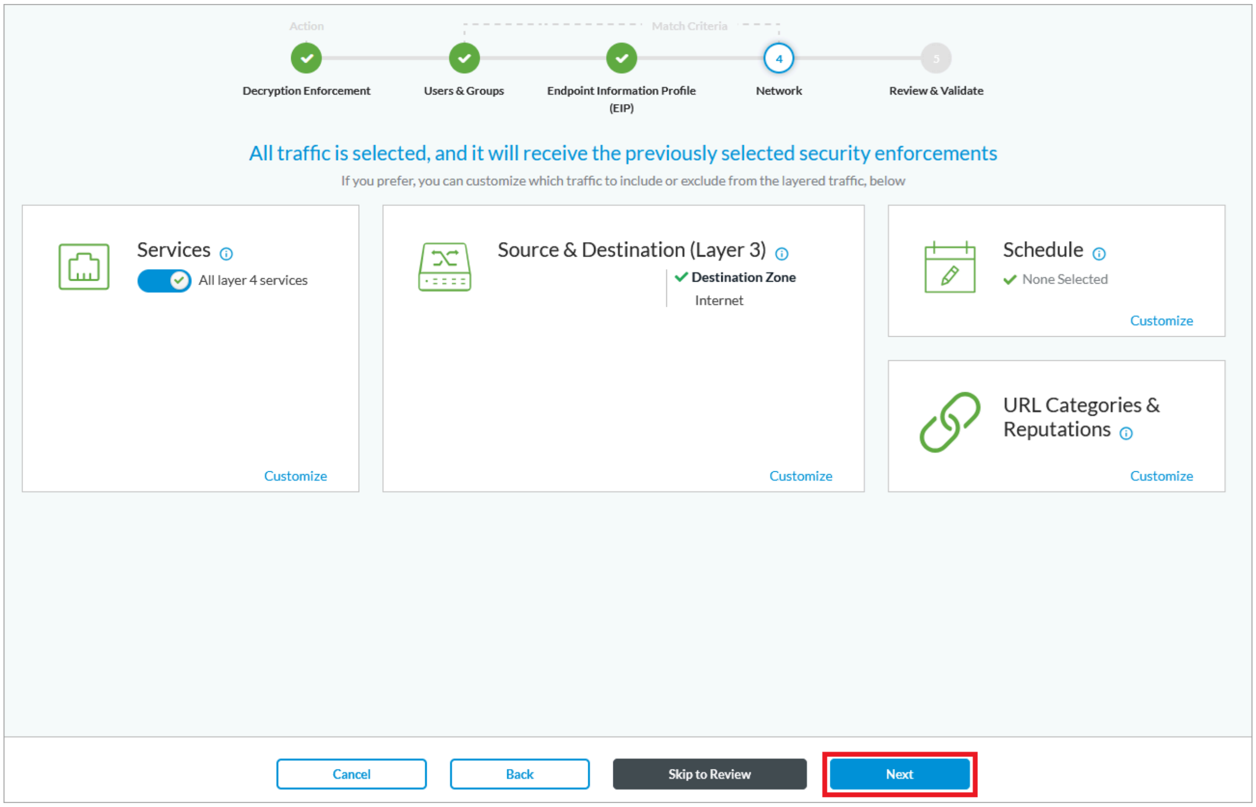
✓ All Users

Endpoint Information Profiles (EIP) allow you to validate additional details about the posture of a user's device before taking actions. We do not use EIP profiles in this example. For more information about about EIP, see Configure Endpoint Information Profiles.



□		Name	Description	Rules
No User Defined EIP Profiles Added				

The Network step provides additional ways to identify and control policies. In this example, we use the default settings. Click Next.



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

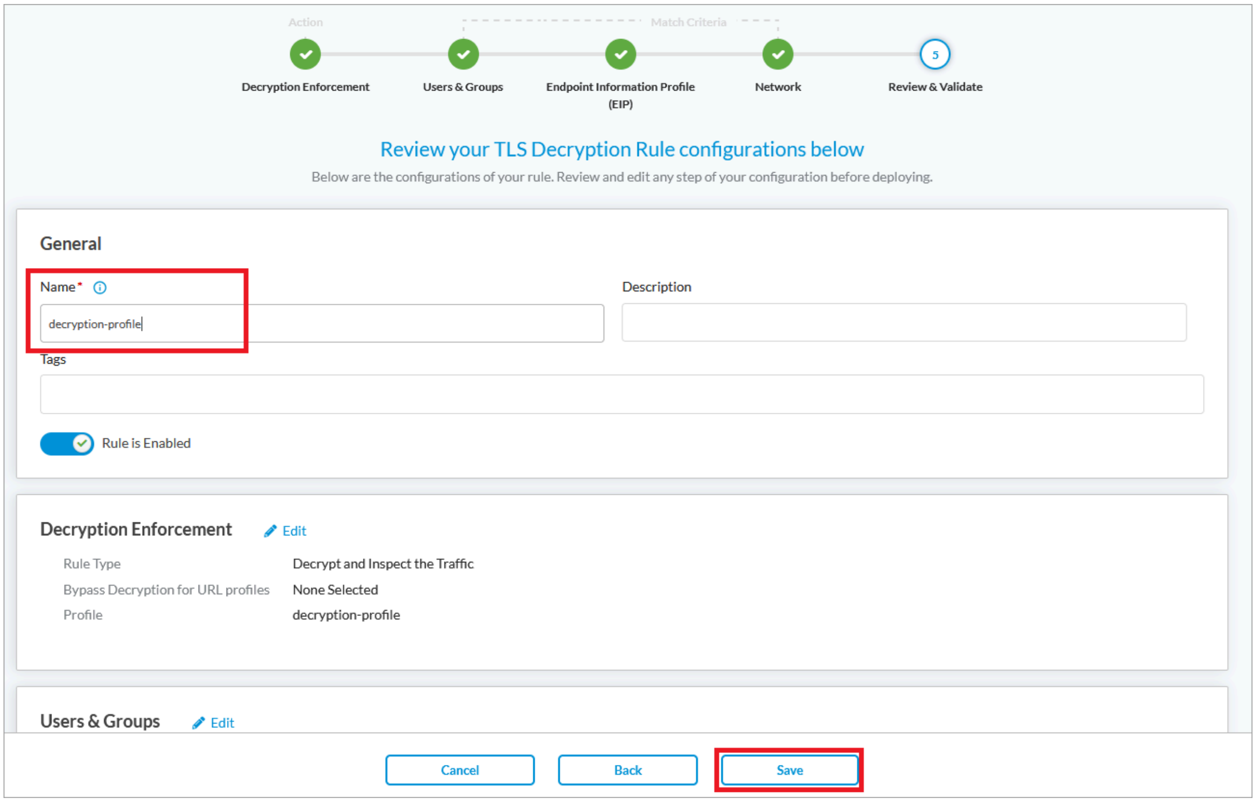
If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

Services: All layer 4 services

Source & Destination (Layer 3): ✓ Destination Zone: Internet

Schedule: ✓ None Selected

Enter a Name, and then click Save to finalize and save the decryption rule.



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*: decryption-profile

Description:

Tags:

Rule is Enabled

Decryption Enforcement ✎ Edit

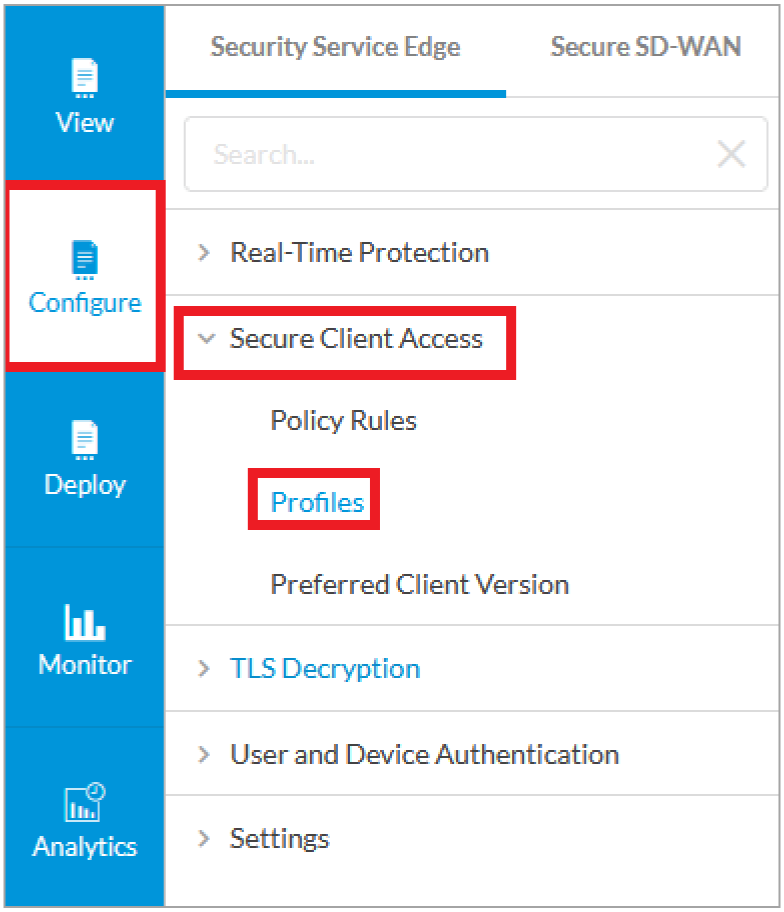
Rule Type	Decrypt and Inspect the Traffic
Bypass Decryption for URL profiles	None Selected
Profile	decryption-profile

Users & Groups ✎ Edit

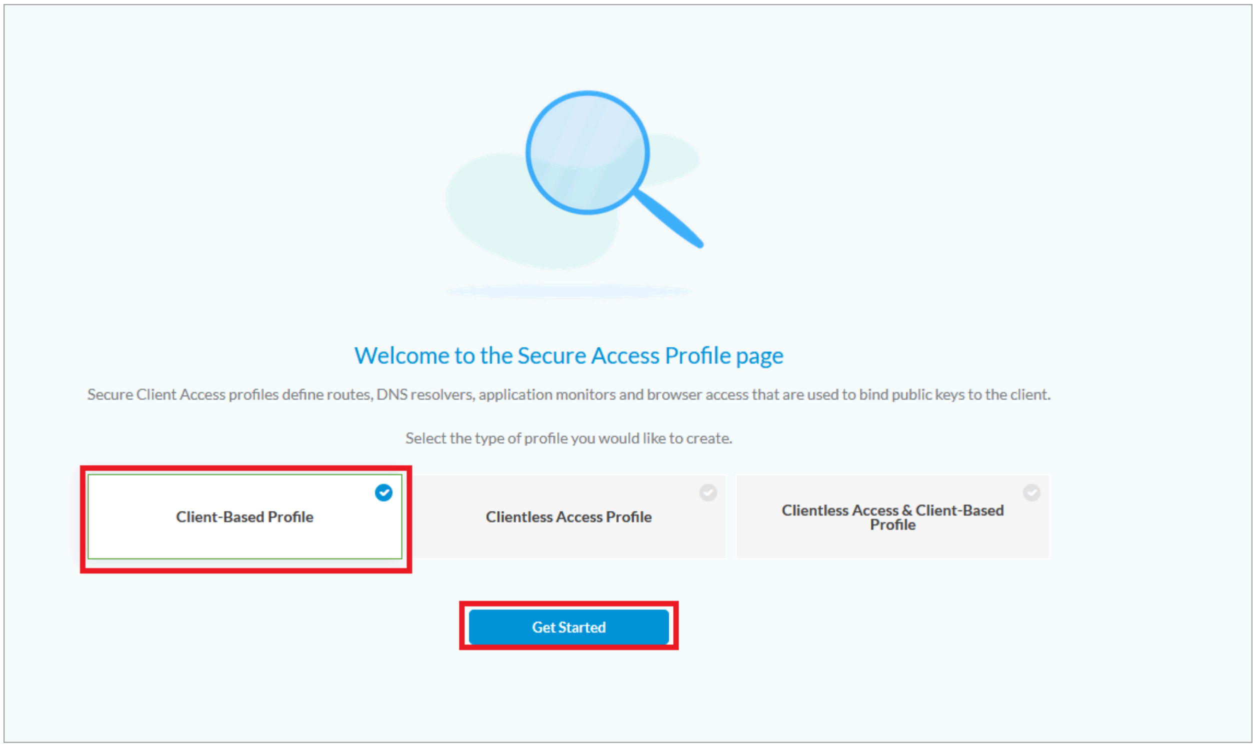
Step 7: Configure a Secure Client Access Profile

For more information, see Configure SASE Secure Client Access Profiles.

Select Configure > Secure Client Access > Profiles.



Select Client-Based Profile and click Get Started.



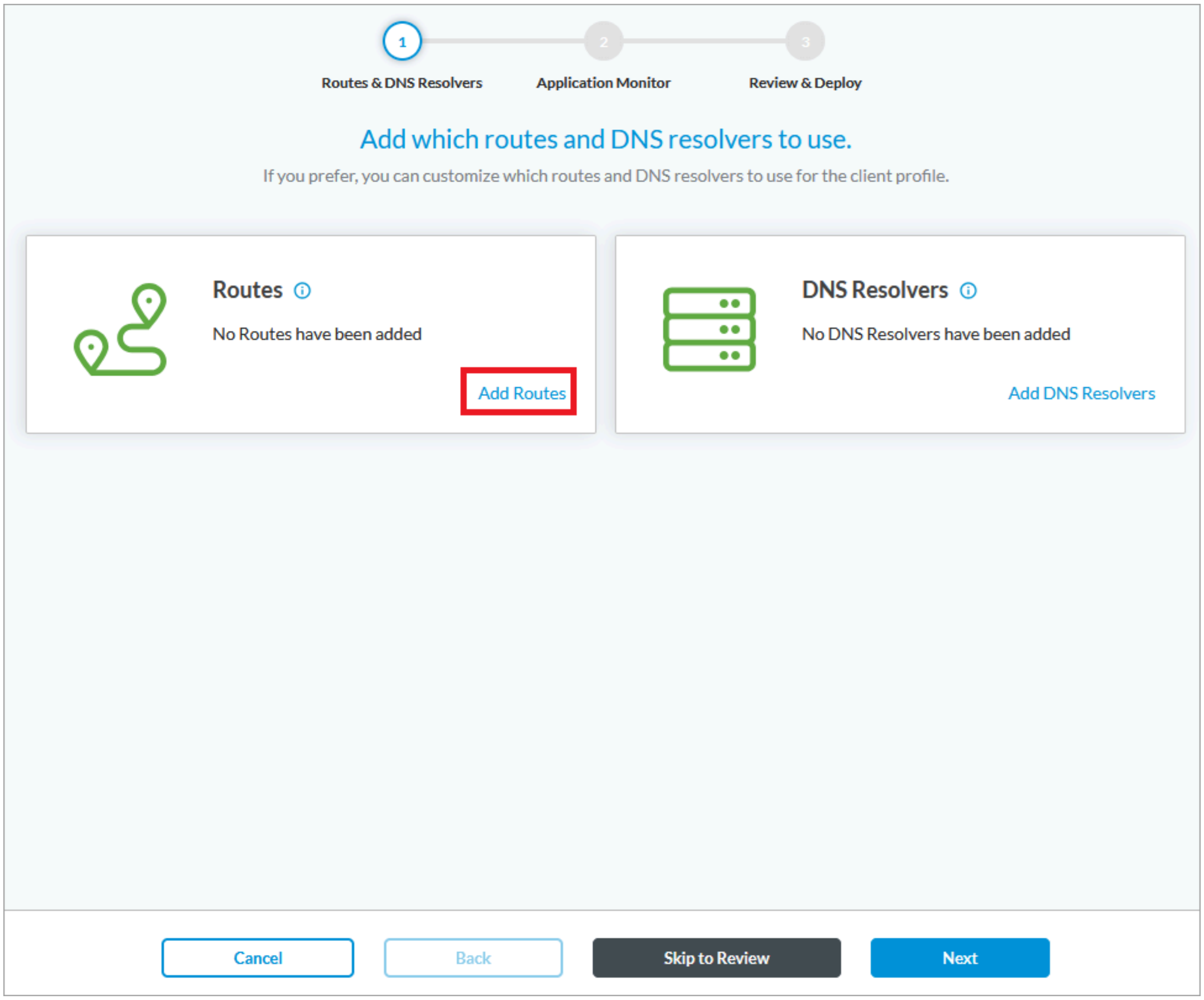
Welcome to the Secure Access Profile page

Secure Client Access profiles define routes, DNS resolvers, application monitors and browser access that are used to bind public keys to the client.

Select the type of profile you would like to create.

Client-Based Profile ✓
Clientless Access Profile
Clientless Access & Client-Based Profile
Get Started

Add some routes to reach your site-to-site tunnel or your private network with SD-WAN through Versa Gateways. Note that if you did not configure a site-to-site tunnel in Step 2, and you are using only the Versa Secure Internet Access (VSIA) solution, you can skip adding the routes, but you must configure a DNS resolver.



Add which routes and DNS resolvers to use.

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

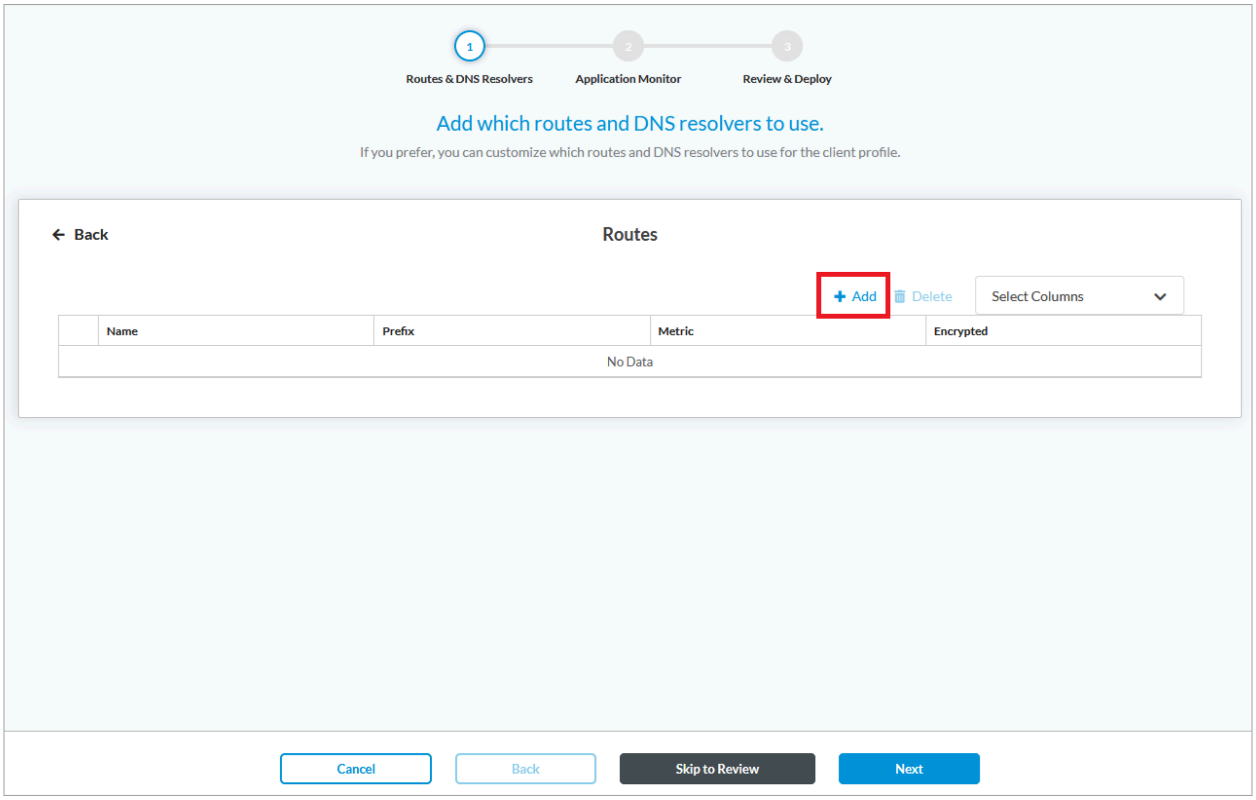
Routes

No Routes have been added

DNS Resolvers

No DNS Resolvers have been added

Click +Add to add routes.



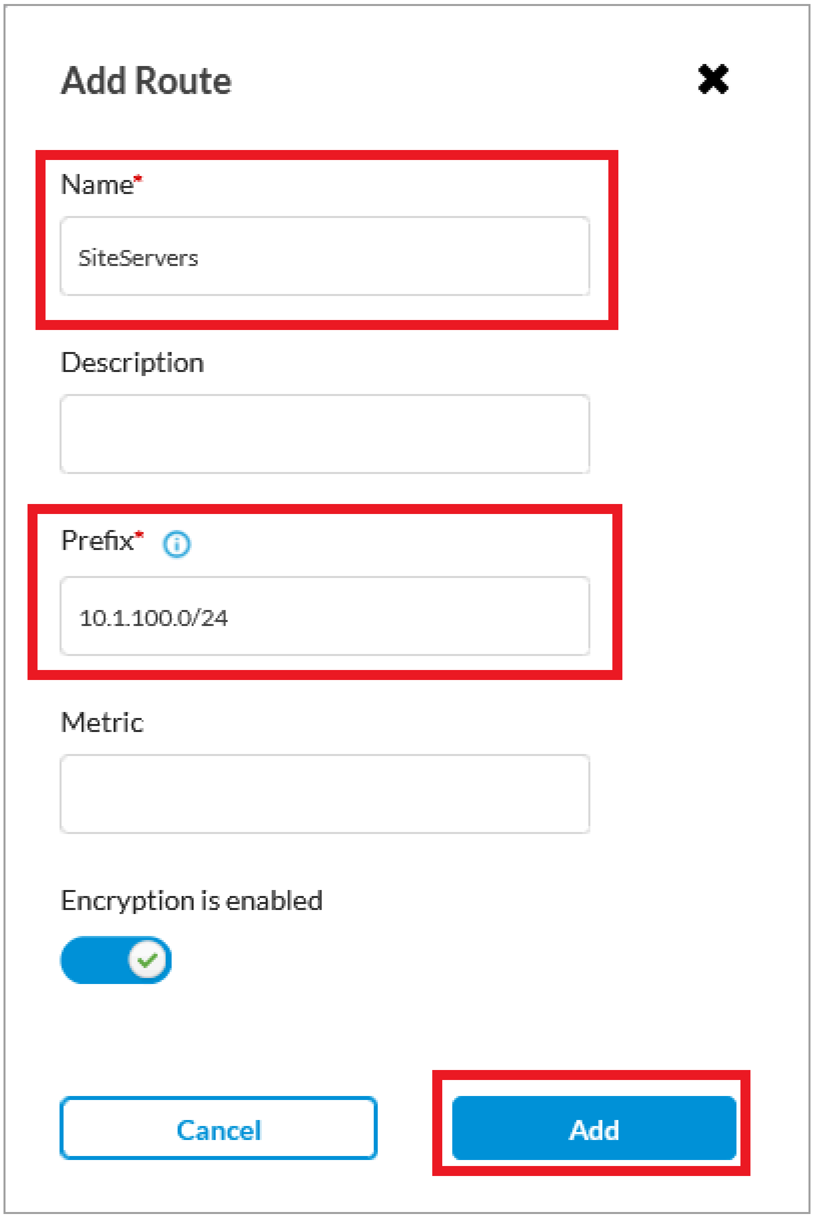
Add which routes and DNS resolvers to use.

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

Routes

	Name	Prefix	Metric	Encrypted
		No Data		

In the Add Route window, enter a name and prefix, and then click Add.



Add Route

Name*

SiteServers

Description

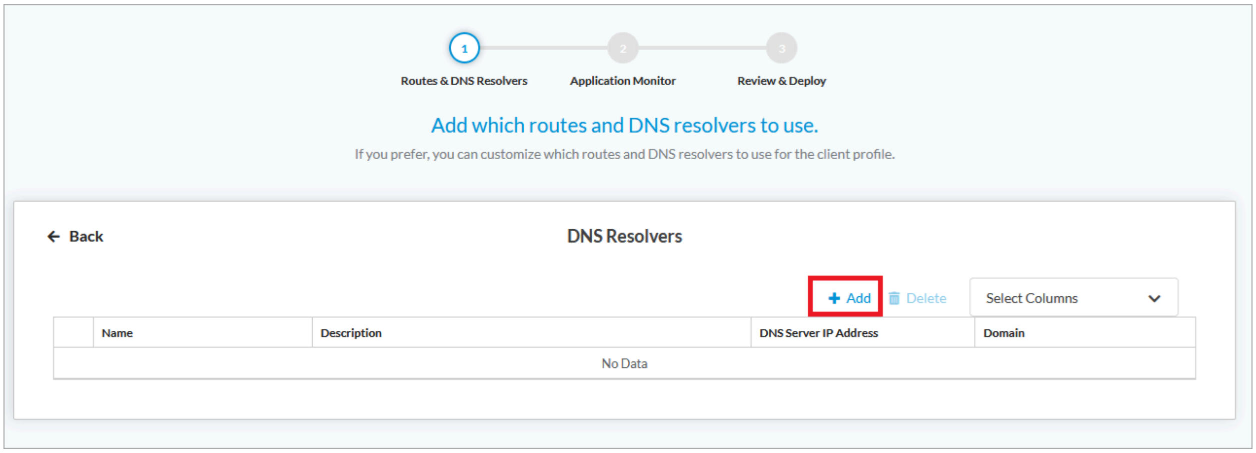
Prefix*

10.1.100.0/24

Metric

Encryption is enabled

To configure a DNS Resolver, click Back after adding routes, and click + Add in the DNS Resolvers pane.



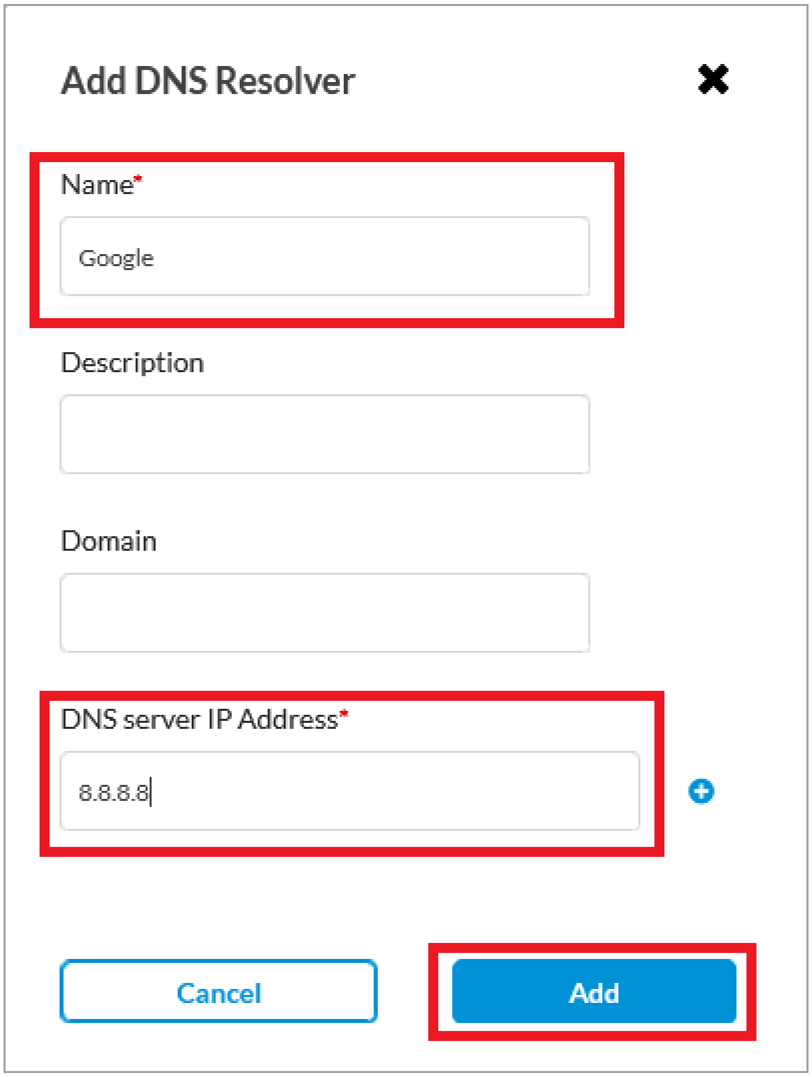
Add which routes and DNS resolvers to use.

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

DNS Resolvers

	Name	Description	DNS Server IP Address	Domain
No Data				

In the Add DNS Resolver window, enter Name and DNS Server IP Address, and then click Add.



Add DNS Resolver

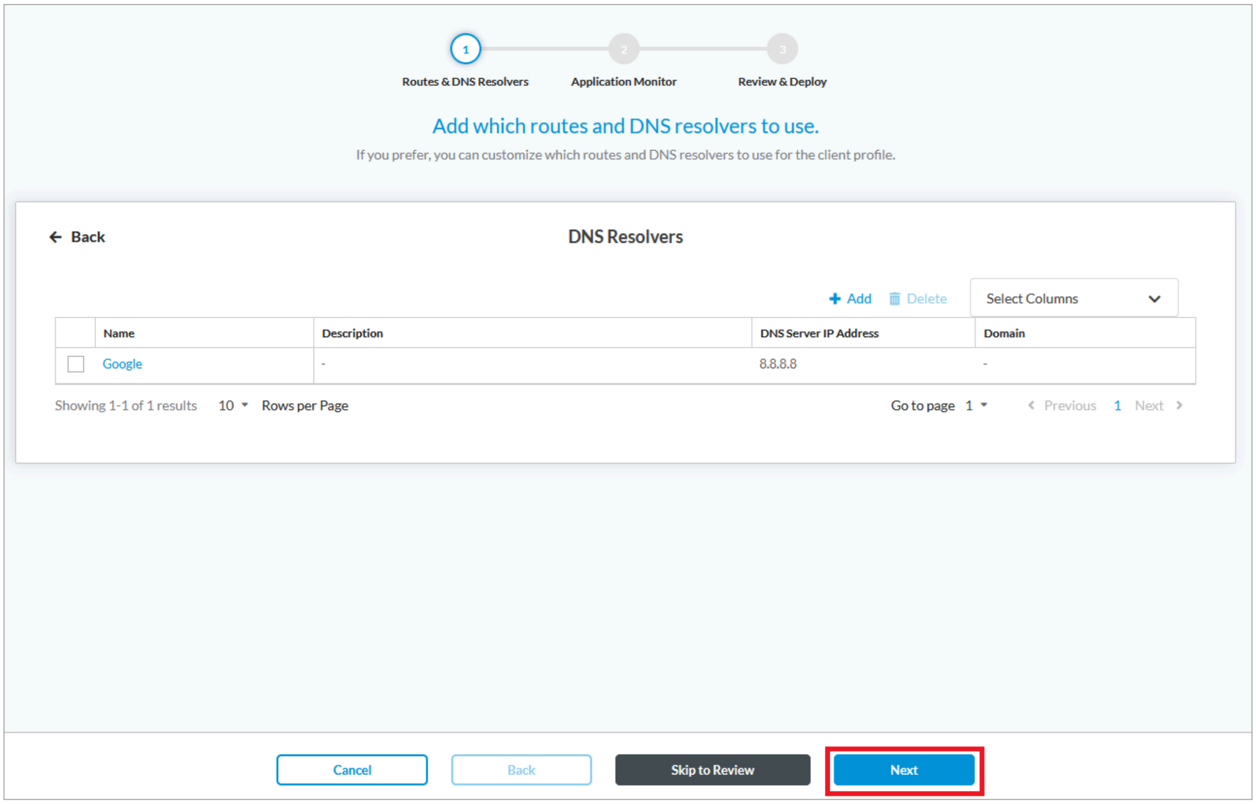
Name*: Google

Description:

Domain:

DNS server IP Address*: 8.8.8.8

After configuring a DNS Resolver, click Next.



Add which routes and DNS resolvers to use.

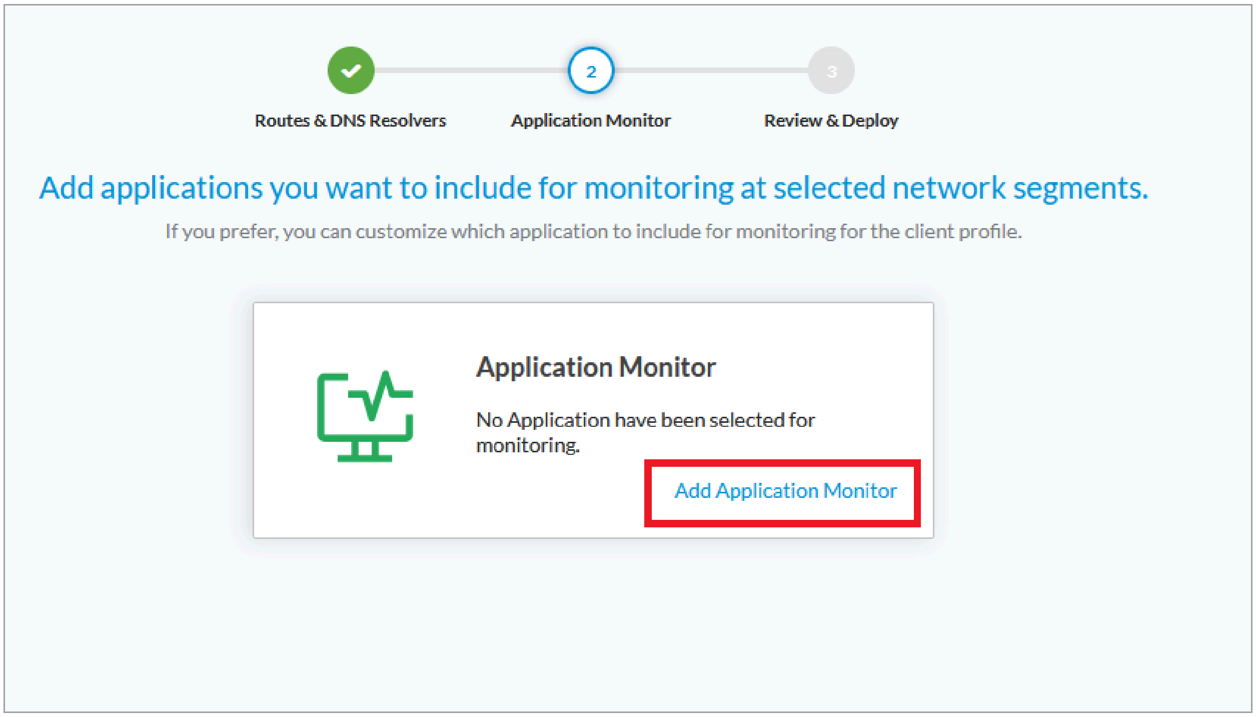
If you prefer, you can customize which routes and DNS resolvers to use for the client profile.

DNS Resolvers

	Name	Description	DNS Server IP Address	Domain
□	Google	-	8.8.8.8	-

Showing 1-1 of 1 results 10 Rows per Page Go to page 1 ‹ Previous 1 Next ›

During this step, click Add Application Monitor to enable DEM application monitoring.



Add applications you want to include for monitoring at selected network segments.

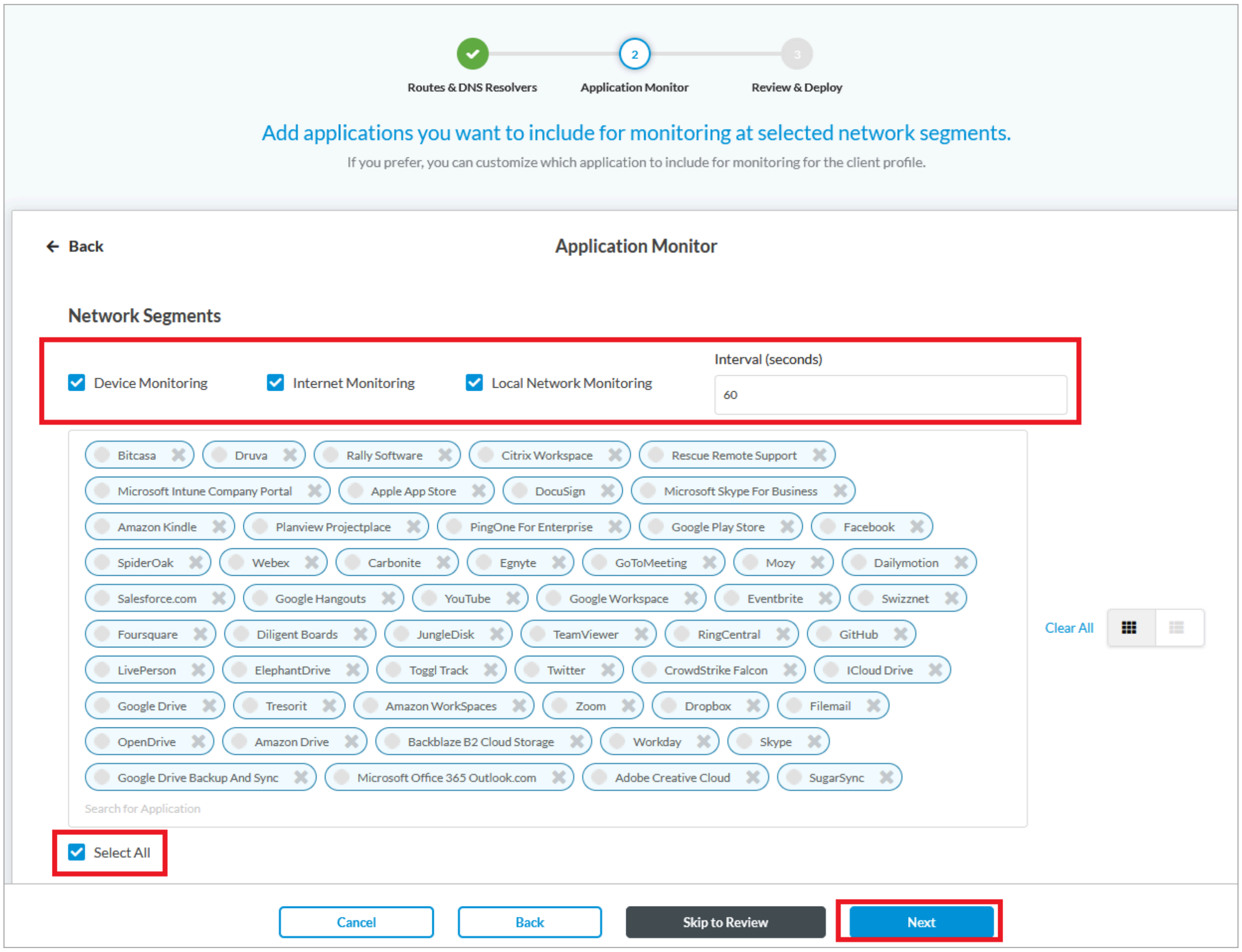
If you prefer, you can customize which application to include for monitoring for the client profile.

Application Monitor

No Application have been selected for monitoring.

In the Application Monitor Configuration screen, select Device Monitoring, Internet Monitoring, and Local Network Monitoring.

Set the Interval as 60 seconds, check Select All applications, and then click Next.



Add applications you want to include for monitoring at selected network segments.

If you prefer, you can customize which application to include for monitoring for the client profile.

Network Segments

☑ Device Monitoring ☑ Internet Monitoring ☑ Local Network Monitoring

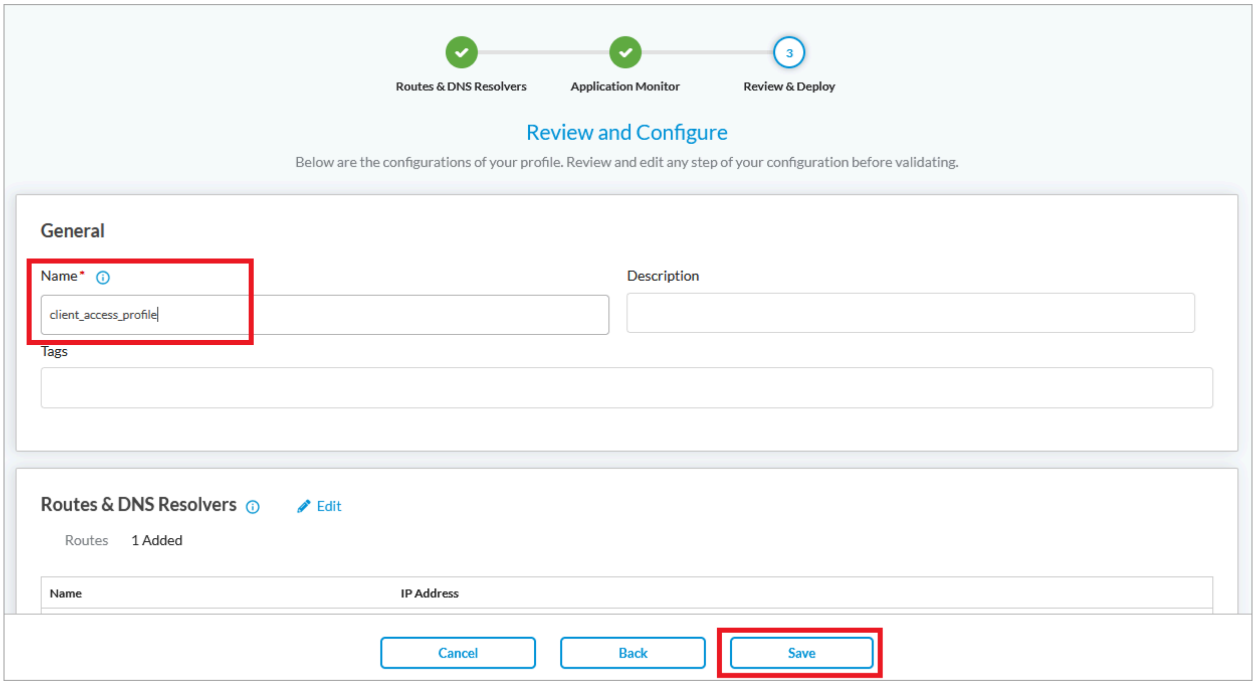
Interval (seconds): 60

Bitcasa, Druva, Rally Software, Citrix Workspace, Rescue Remote Support, Microsoft Intune Company Portal, Apple App Store, DocuSign, Microsoft Skype For Business, Amazon Kindle, Planview Projectplace, PingOne For Enterprise, Google Play Store, Facebook, SpiderOak, Webex, Carbonite, Egnyte, GoToMeeting, Mozy, Dailymotion, Salesforce.com, Google Hangouts, YouTube, Google Workspace, Eventbrite, Swizznet, Foursquare, Diligent Boards, JungleDisk, TeamViewer, RingCentral, GitHub, LivePerson, ElephantDrive, Toggl Track, Twitter, CrowdStrike Falcon, ICloud Drive, Google Drive, Tresorit, Amazon WorkSpaces, Zoom, Dropbox, Filemail, OpenDrive, Amazon Drive, Backblaze B2 Cloud Storage, Workday, Skype, Google Drive Backup And Sync, Microsoft Office 365 Outlook.com, Adobe Creative Cloud, SugarSync

Search for Application

☑ Select All

Enter a policy name in the Name field, and then click Save.



Review and Configure

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

General

Name* client_access_profile

Description

Tags

Routes & DNS Resolvers

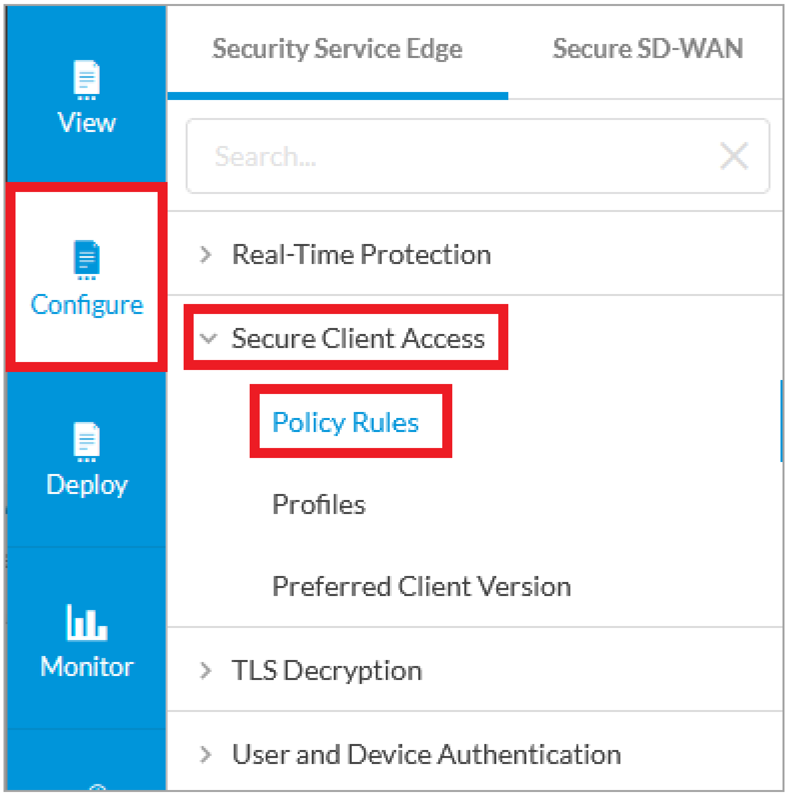
Routes 1 Added

Name	IP Address

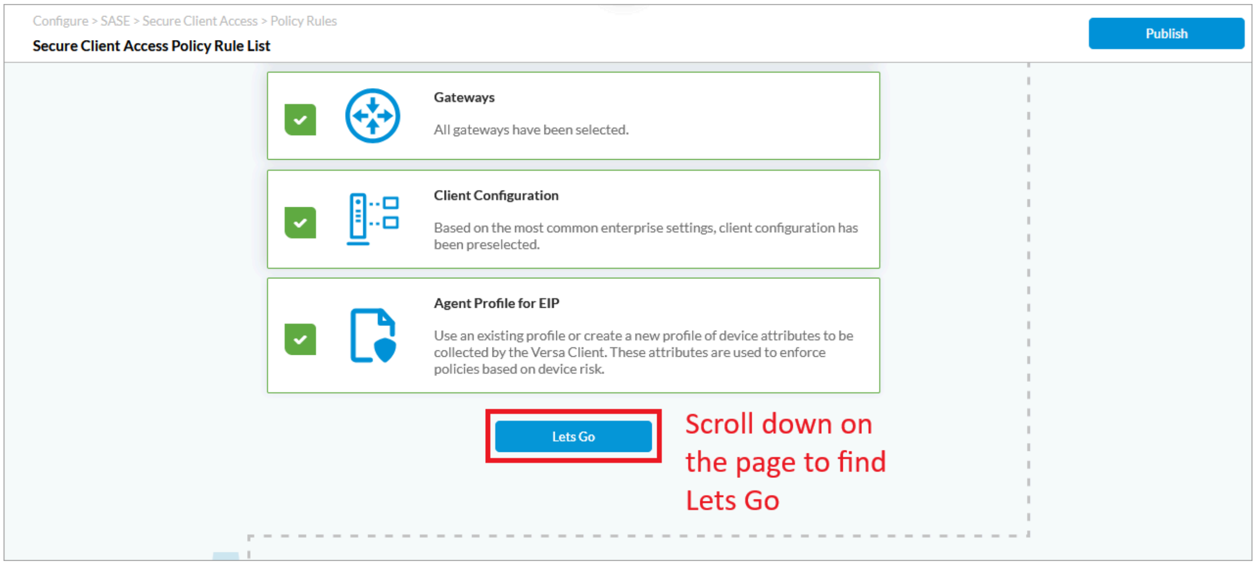
Step 8: Configure a Secure Client Access Policy Rule

For more information, see Configure SASE Secure Client Access Rules.

Select Configure > Secure Client Access > Policy Rules.



In the Secure Client Access Policy Rule List window, scroll down and click Let's Go.


Configure > SASE > Secure Client Access > Policy Rules

Secure Client Access Policy Rule List

Gateways

All gateways have been selected.

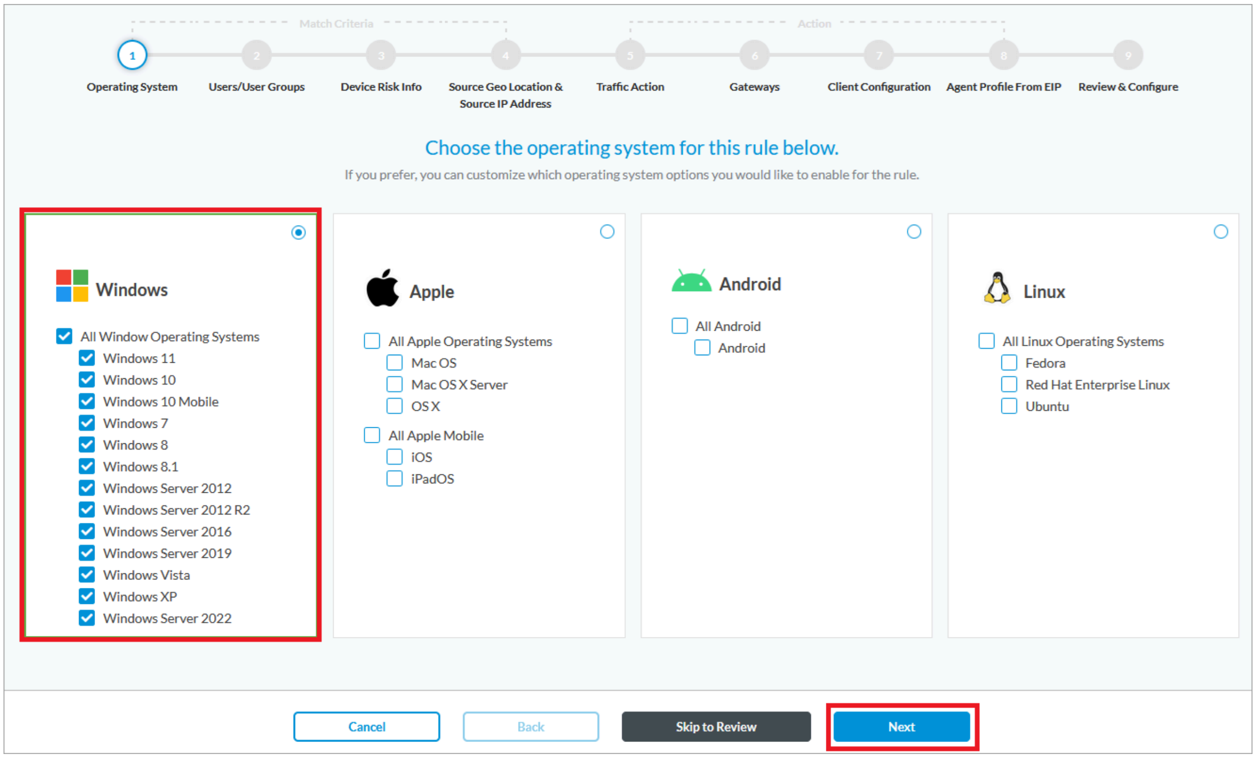
Client Configuration

Based on the most common enterprise settings, client configuration has been preselected.

Agent Profile for EIP

Use an existing profile or create a new profile of device attributes to be collected by the Versa Client. These attributes are used to enforce policies based on device risk.

Select the operating system to use. For this example policy, we use Windows.



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

○ Apple

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

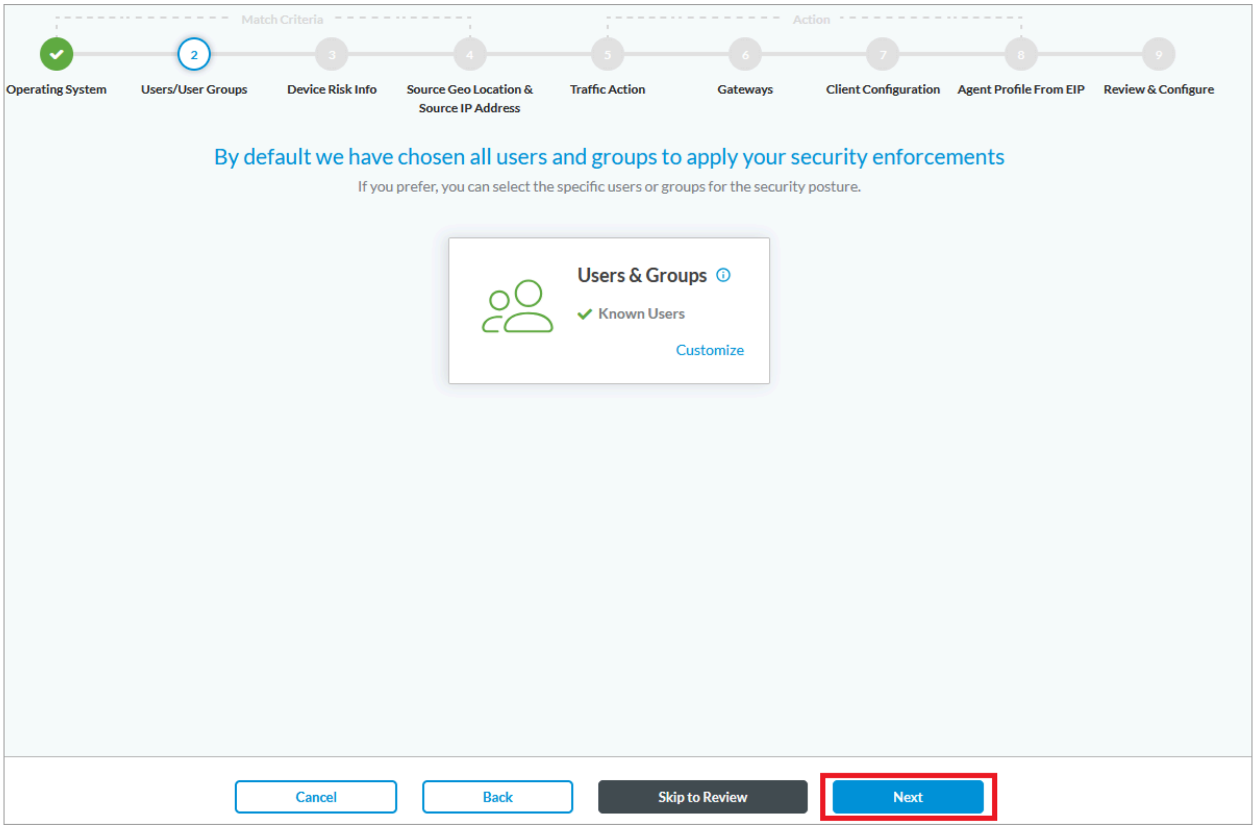
○ Android

- ☐ All Android
  - ☐ Android

○ Linux

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

This policy uses the option for Known Users, but you can select a specific user or group of users that match or utilize this profile rule.



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

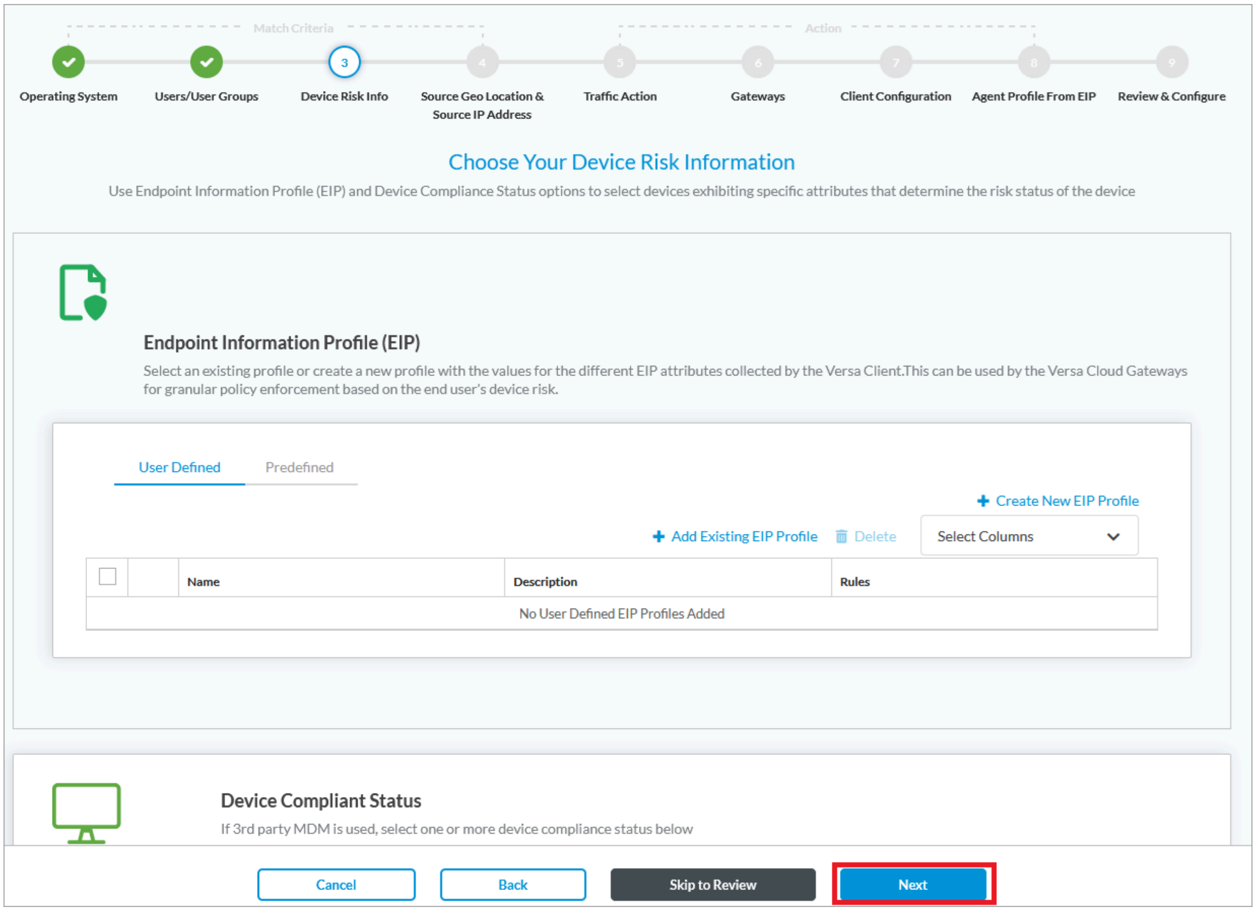
If you prefer, you can select the specific users or groups for the security posture.

Users & Groups

✓ Known Users

Customize

Endpoint Information Profile (EIP) and compliance check with MDM can identify additional potential risks on a device. To keep this policy simple, click Next without configuration changes.



Choose Your Device Risk Information

Use Endpoint Information Profile (EIP) and Device Compliance Status options to select devices exhibiting specific attributes that determine the risk status of the device

Endpoint Information Profile (EIP)

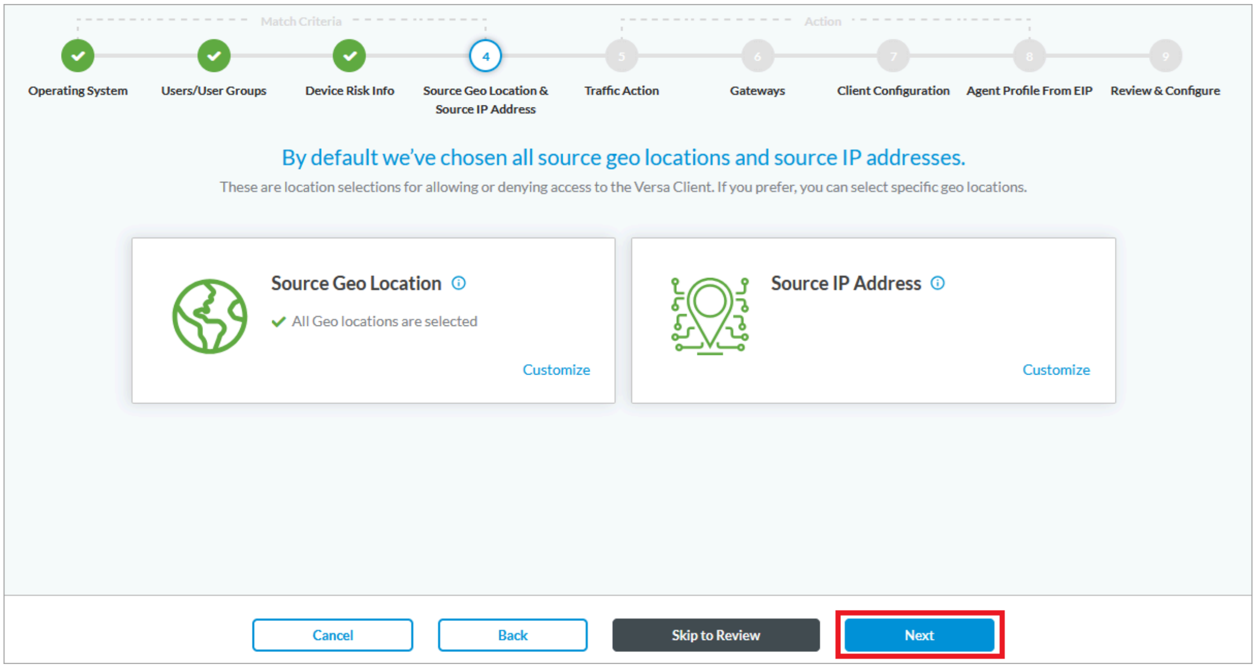
Select an existing profile or create a new profile with the values for the different EIP attributes collected by the Versa Client.This can be used by the Versa Cloud Gateways for granular policy enforcement based on the end user's device risk.

□		Name	Description	Rules
			No User Defined EIP Profiles Added	

Device Compliant Status

If 3rd party MDM is used, select one or more device compliance status below

You can manage user access based on Source geographic location and source IP address. In this simple policy example, we use the default.



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

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

Source Geo Location

✓ All Geo locations are selected

Customize

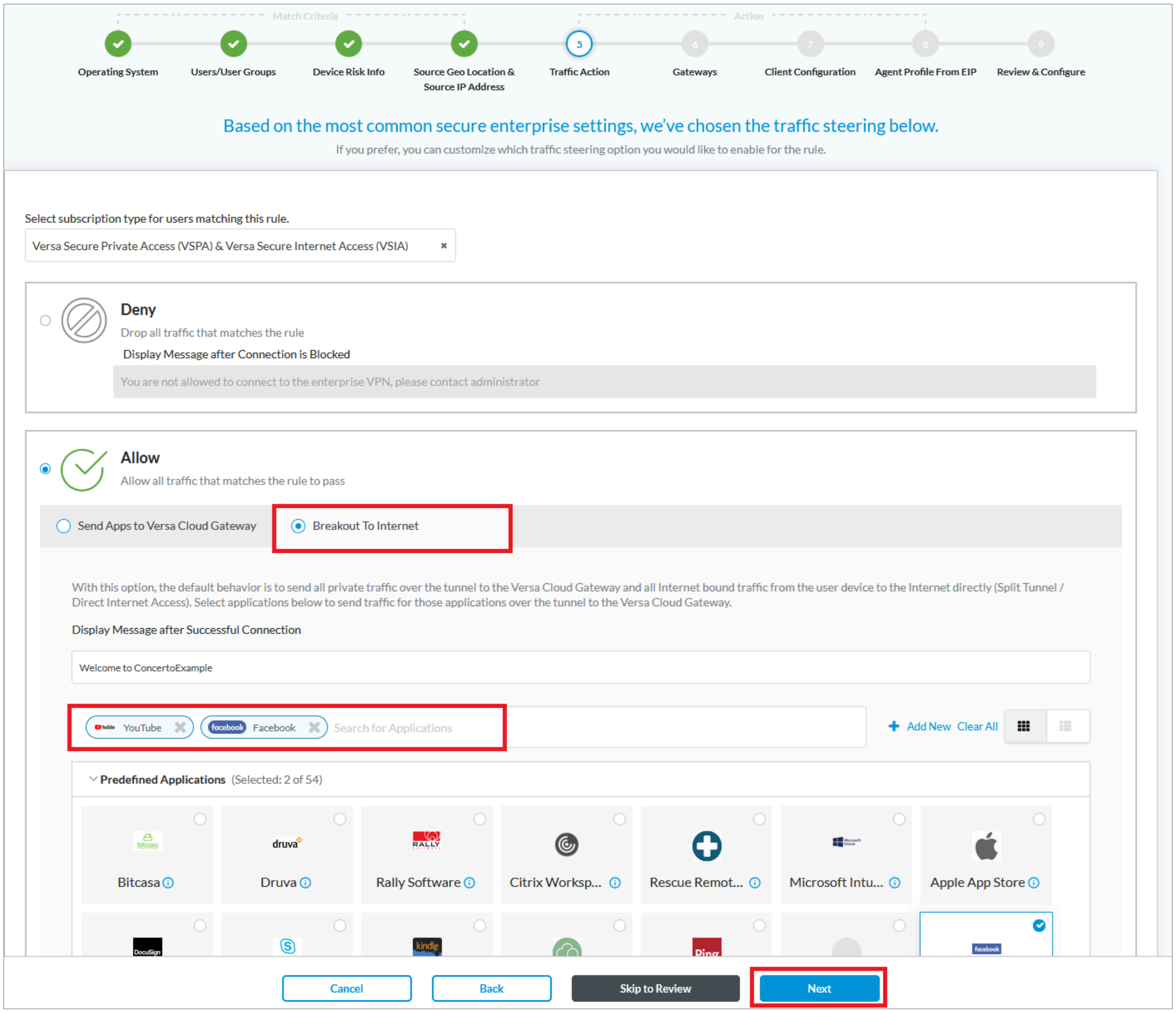
Source IP Address

Customize

Based on previously configured constraints, you can now define how you want to control applications. In this policy, we allow traffic that matches the rule to pass.
We select the option Breakout to Internet to configure all traffic to go directly to the internet rather than through the gateway. You can specify which applications are sent through the gateway. In the following example, we select YouTube and Facebook.

Note that the field "Select Subscription type for users matching this rule" aligns to the license type you purchase. The options are:

- VSPA (Versa Secure Private Access)—focused on ZTNA for private network control and access.
- VSIA (Versa Secure Internet Access)—focused on ZTNA for public application control (Internet).
- VSPA + VSIA—focused on both.



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 private traffic over the tunnel to the Versa Cloud Gateway and all Internet bound traffic from the user device to the Internet directly (Split Tunnel / Direct Internet Access). Select applications below to send traffic for those applications over the tunnel to the Versa Cloud Gateway.

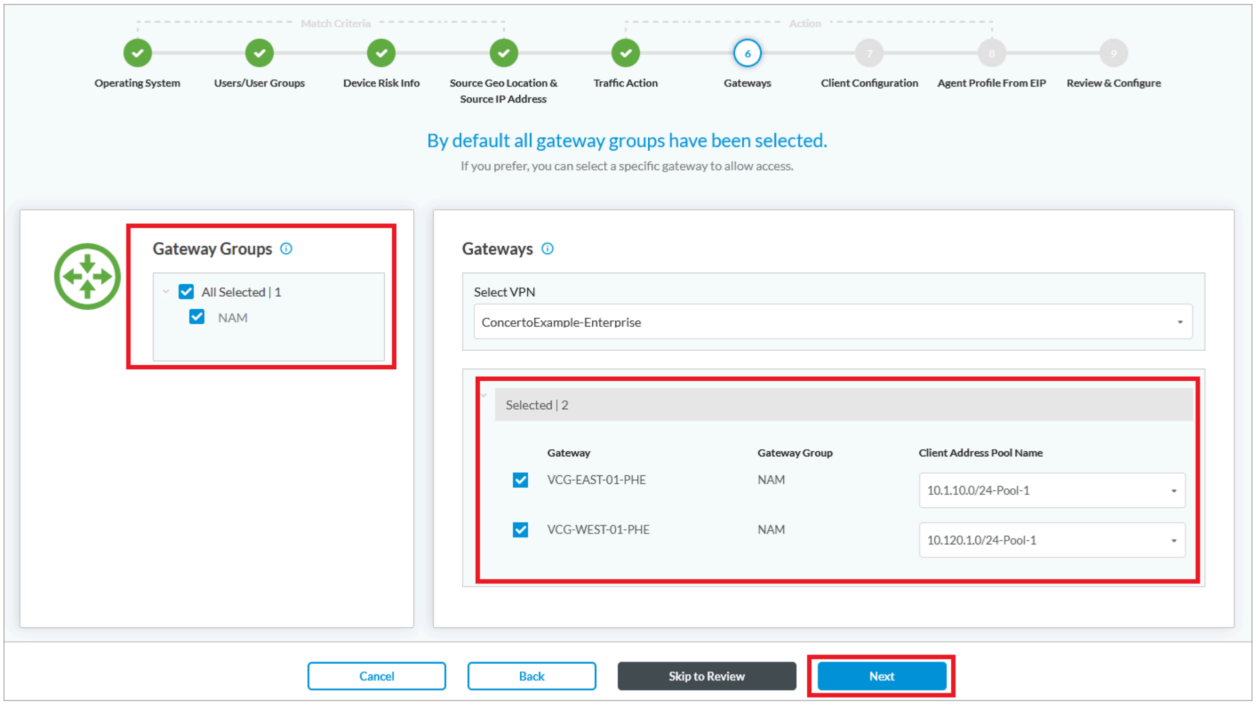
Display Message after Successful Connection

Welcome to ConcertoExample

YouTube ✕ Facebook ✕ Search for Applications

The following screen varies based on the Concerto headend and Versa Cloud Gateways that are provisioned for you. If your deployment does not match, select the gateways in your environment you want to use to quickly validate this policy.

In this example, there is one gateway group for the two Versa Cloud Gateways in this SASE headend. This allows for configurations such as Best Gateway Selection, which is auto-configured and provided based on the group name and grouping of the attached gateways.



By default all gateway groups have been selected.

If you prefer, you can select a specific gateway to allow access.

☑ All Selected | 1

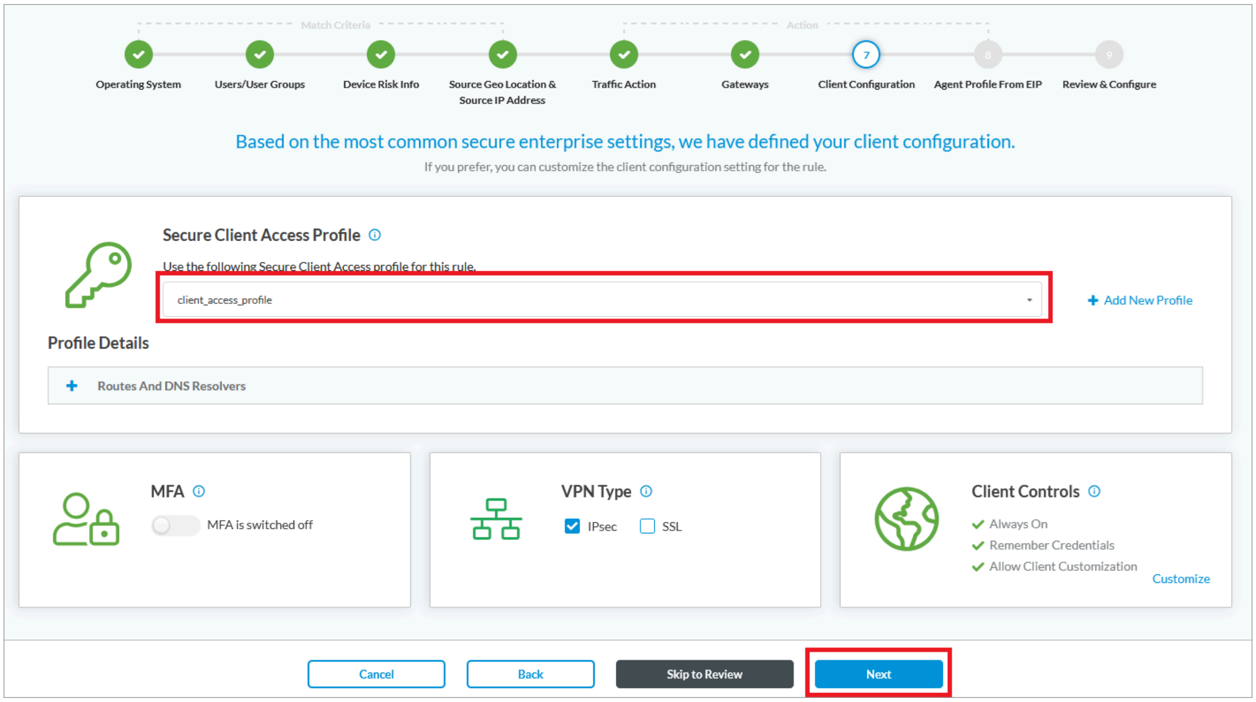
☑ NAM

Select VPN: ConcertoExample-Enterprise

Selected | 2

	Gateway	Gateway Group	Client Address Pool Name
☑	VCG-EAST-01-PHE	NAM	10.1.10.0/24-Pool-1
☑	VCG-WEST-01-PHE	NAM	10.120.1.0/24-Pool-1

In the Client Configuration screen, select the Secure Client Access Profile that you created in Step 7.



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.

Use the following Secure Client Access profile for this rule.

client_access_profile

MFA is switched off

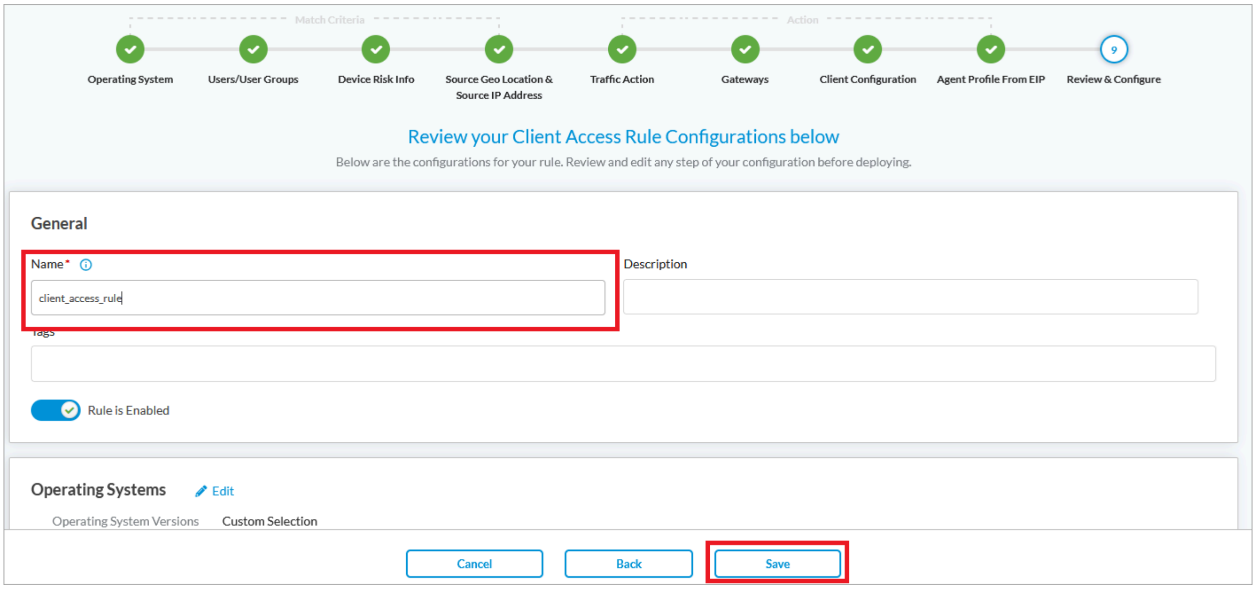
☑ IPsec ☐ SSL

✓ Always On

✓ Remember Credentials

✓ Allow Client Customization

Enter a name for your policy in the Name field, and then click Save.



Review your Client Access Rule Configurations below

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

General

Name* client_access_rule

Description

Tags

Rule is Enabled

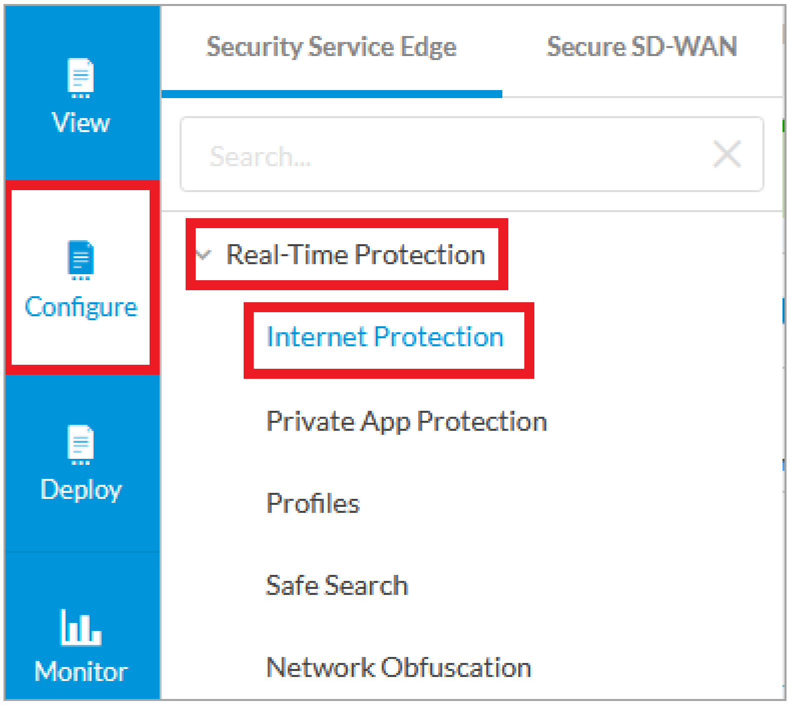
Operating Systems

Operating System Versions Custom Selection

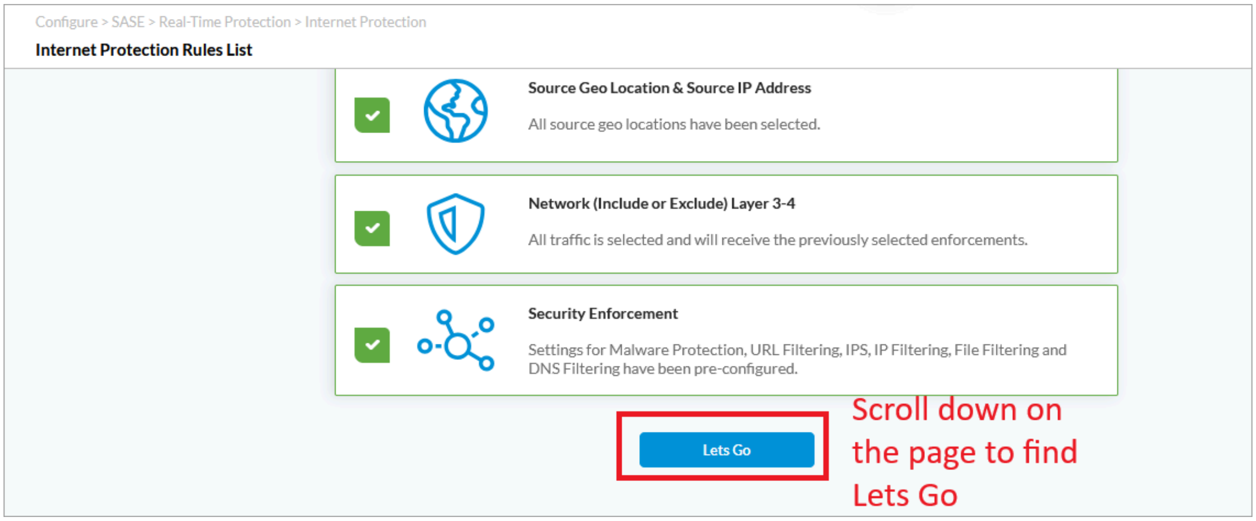
Step 9: Create an Internet Protection Policy

For more information, see Configure SASE Internet Protection Rules.

Select Configure > Real-Time Protection > Internet Protection.



Scroll down and click Let's Go.


Configure > SASE > Real-Time Protection > Internet Protection

Internet Protection Rules List

Source Geo Location & Source IP Address

All source geo locations have been selected.

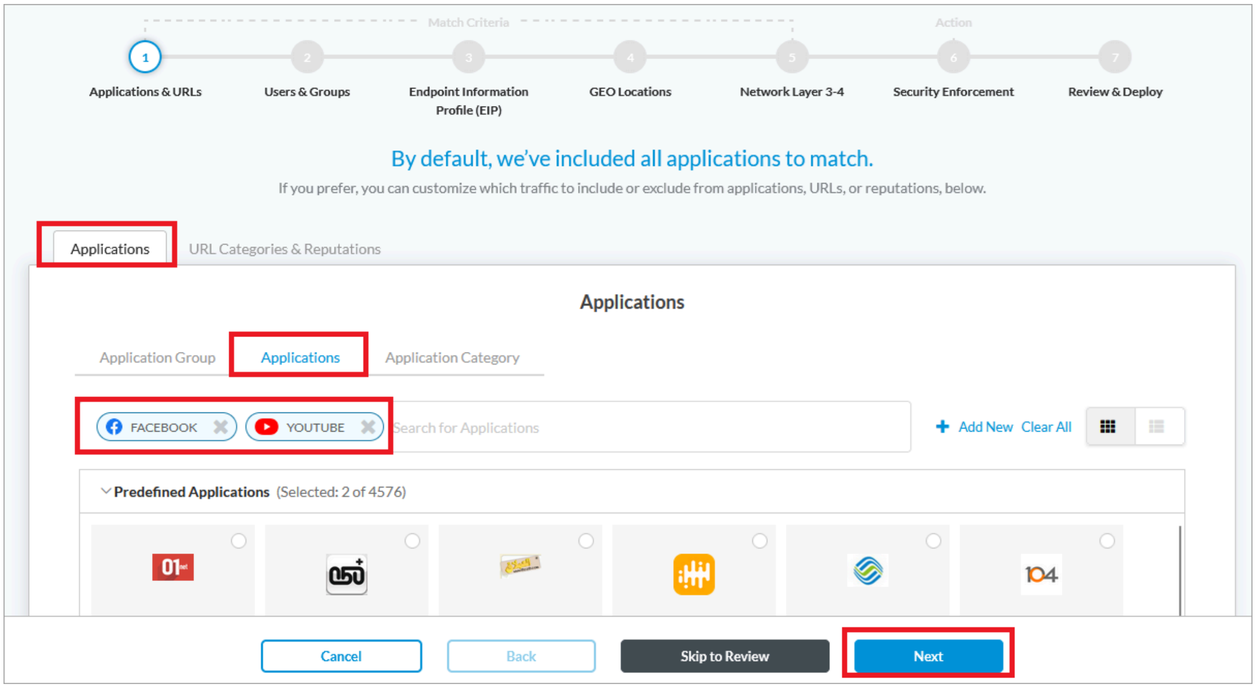
Network (Include or Exclude) Layer 3-4

All traffic is selected and will receive the previously selected enforcements.

Security Enforcement

Settings for Malware Protection, URL Filtering, IPS, IP Filtering, File Filtering and DNS Filtering have been pre-configured.

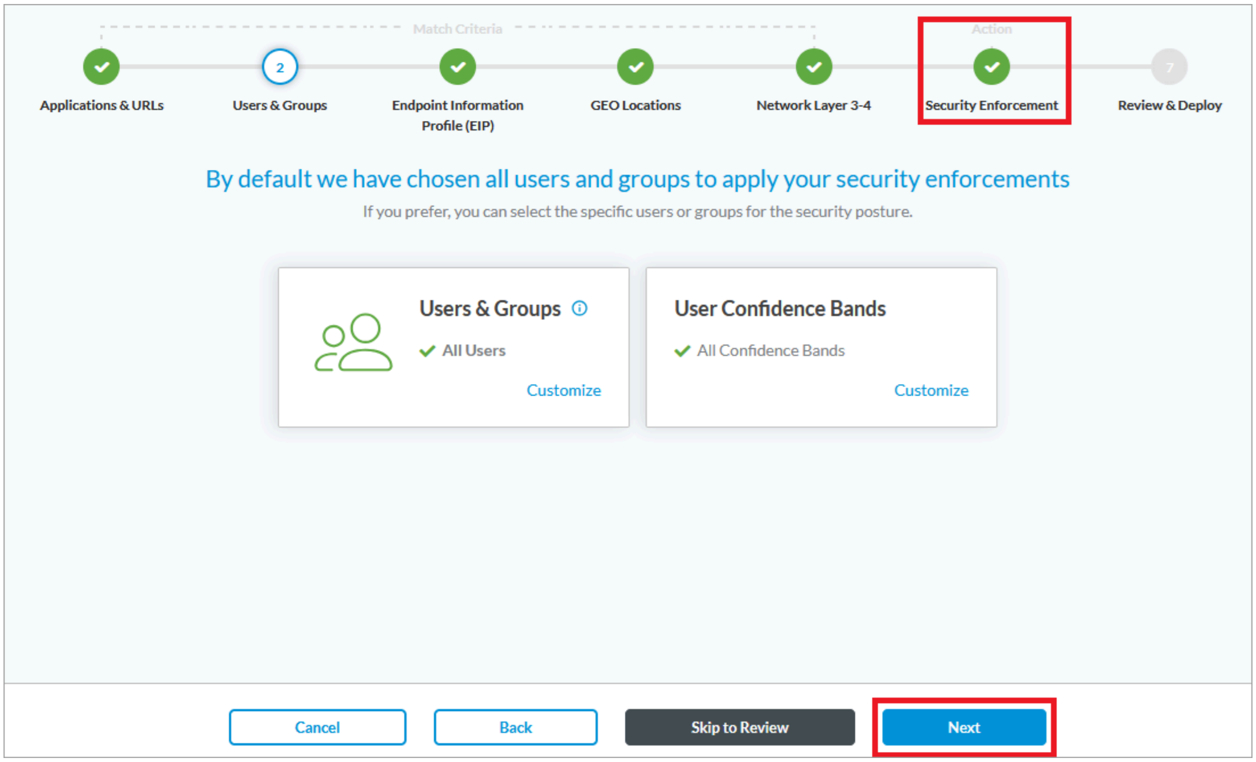
In the Applications and URLs screen, select the Applications tab, then select Facebook and YouTube as the applications for this policy.


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.

Predefined Applications (Selected: 2 of 4576)

Click Next to use the default settings for EIP, GEO Locations, and Network Layer 3-4, until you reach Security Enforcement.



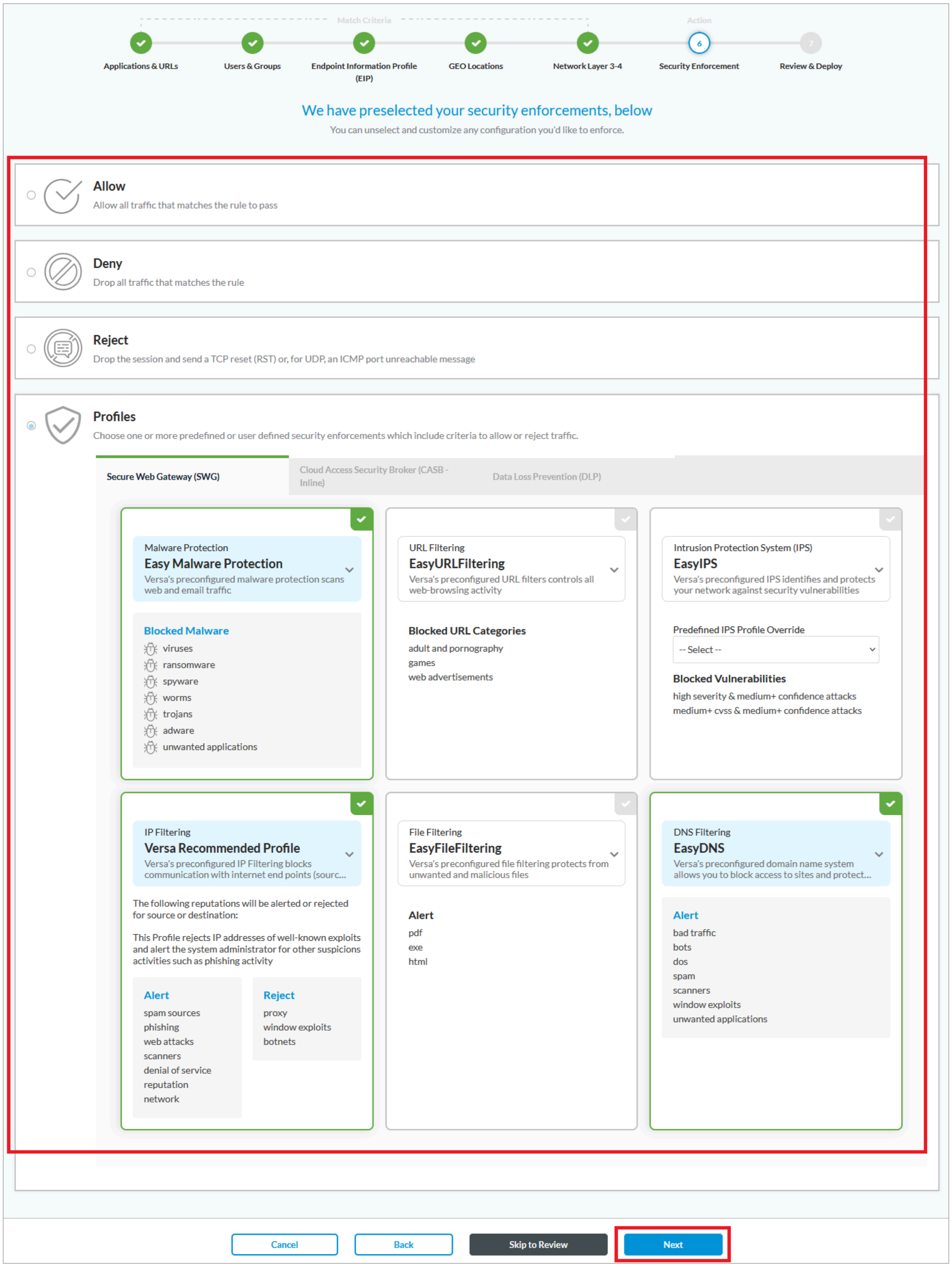
By default we have chosen all users and groups to apply your security enforcements

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

Users & Groups
✓ All Users

User Confidence Bands
✓ All Confidence Bands

The Security Enforcement screen displays options to control the selected applications as you want. You can allow, deny or reject applications, as well as use security profiles to utilize security enforcements for better data security. Note that the enforcement options vary based on your license.



We have preselected your security enforcements, below

You can unselect and customize any configuration you'd like to enforce.

○ **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

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

Secure Web Gateway (SWG) | Cloud Access Security Broker (CASB - Inline) | Data Loss Prevention (DLP)

✓ Malware Protection
Easy Malware Protection
Versa's preconfigured malware protection scans web and email traffic

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

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

Blocked URL Categories
- adult and pornography
- games
- web advertisements

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

Predefined IPS Profile Override
-- Select --

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

✓ IP Filtering
Versa Recommended Profile
Versa's preconfigured IP Filtering blocks communication with internet end points (sourc...

The following reputations will be alerted or rejected for source or destination:

This Profile rejects IP addresses of well-known exploits and alert the system administrator for other suspicions activities such as phishing activity

Alert
- spam sources
- phishing
- web attacks
- scanners
- denial of service
- reputation
- network

Reject
- proxy
- window exploits
- botnets

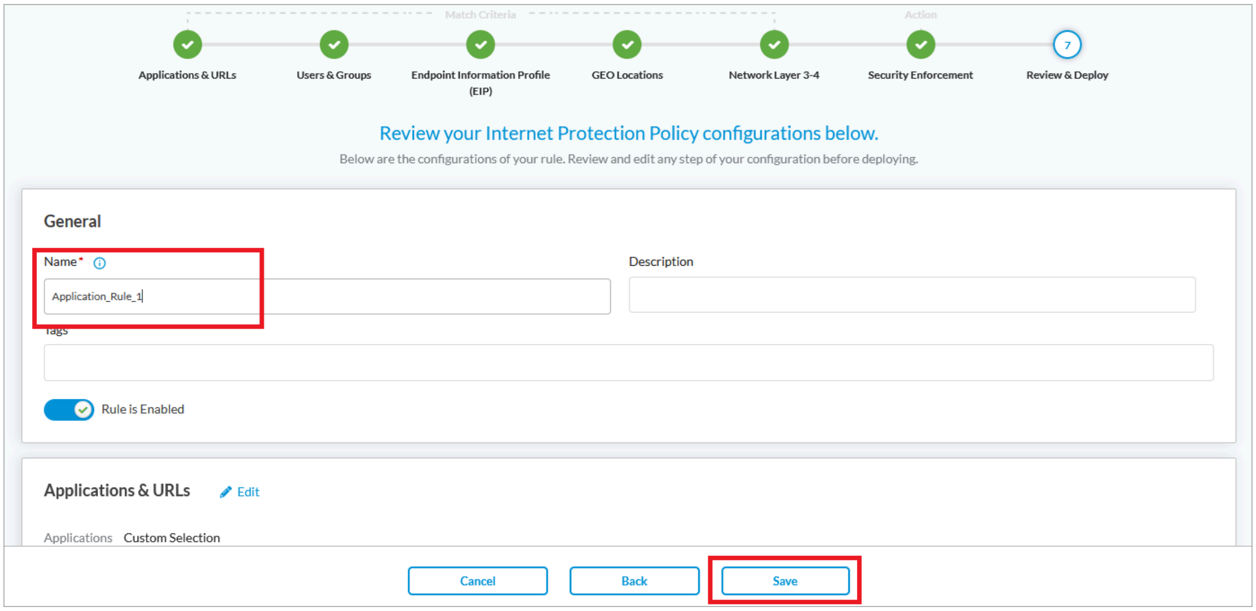
File Filtering
EasyFileFiltering
Versa's preconfigured file filtering protects from unwanted and malicious files

Alert
- pdf
- exe
- html

✓ DNS Filtering
EasyDNS
Versa's preconfigured domain name system allows you to block access to sites and protect...

Alert
- bad traffic
- bots
- dos
- spam
- scanners
- window exploits
- unwanted applications

In the Review & Deploy screen, enter a name for new policy in the Name field and click Save.



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*: Application_Rule_1

Description:

Tags:

Rule is Enabled

Applications & URLs

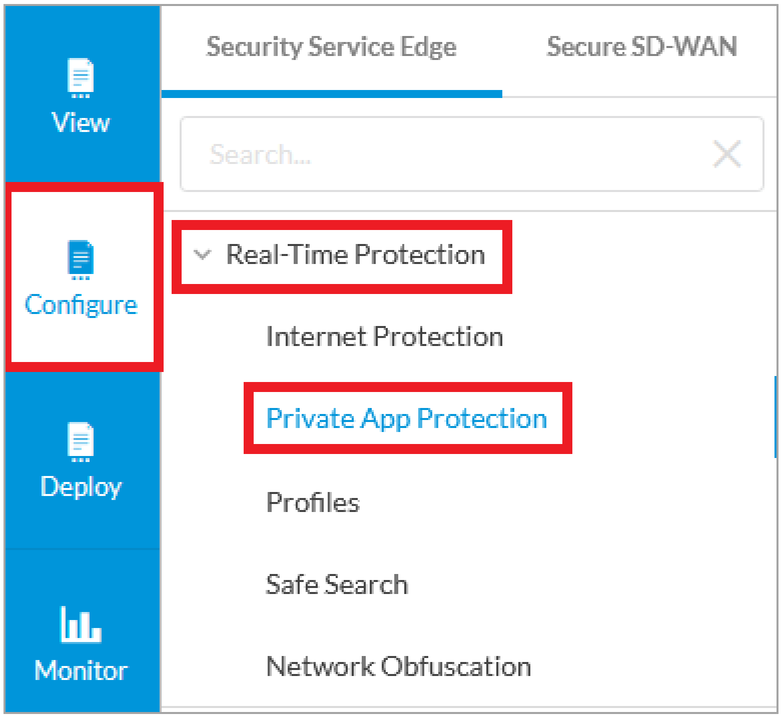
Applications: Custom Selection

Step 10: Create a Private Protection Policy (Optional)

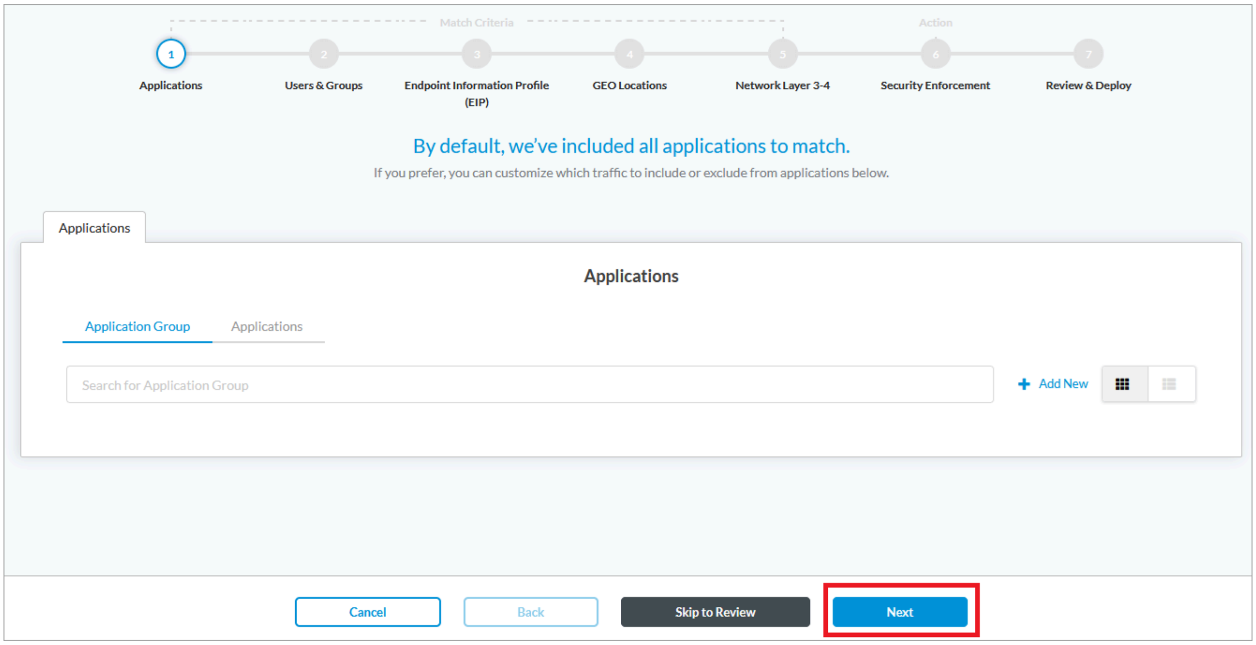
For more information, see Configure SASE Private Application Protection Rules.

In this step, we configure rules to protect private applications. (You can skip Step 10 if you did not create a site-to-site tunnel in Step 2).

Select Configure > Real-Time Protection > Private App Protection.



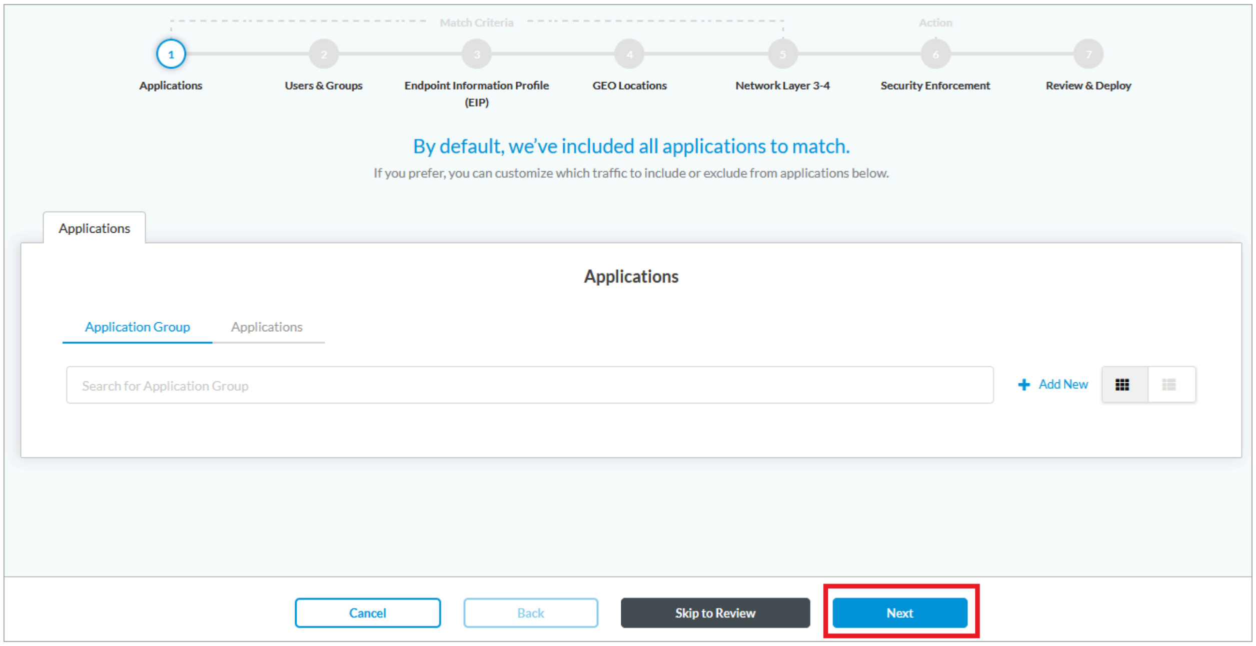
In the Private App Protection Rules List window, scroll down and click Let's Go.



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

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

For this policy, we protect all applications that users are allowed to access. Leaving the list blank uses Any as the selector. Click Next.

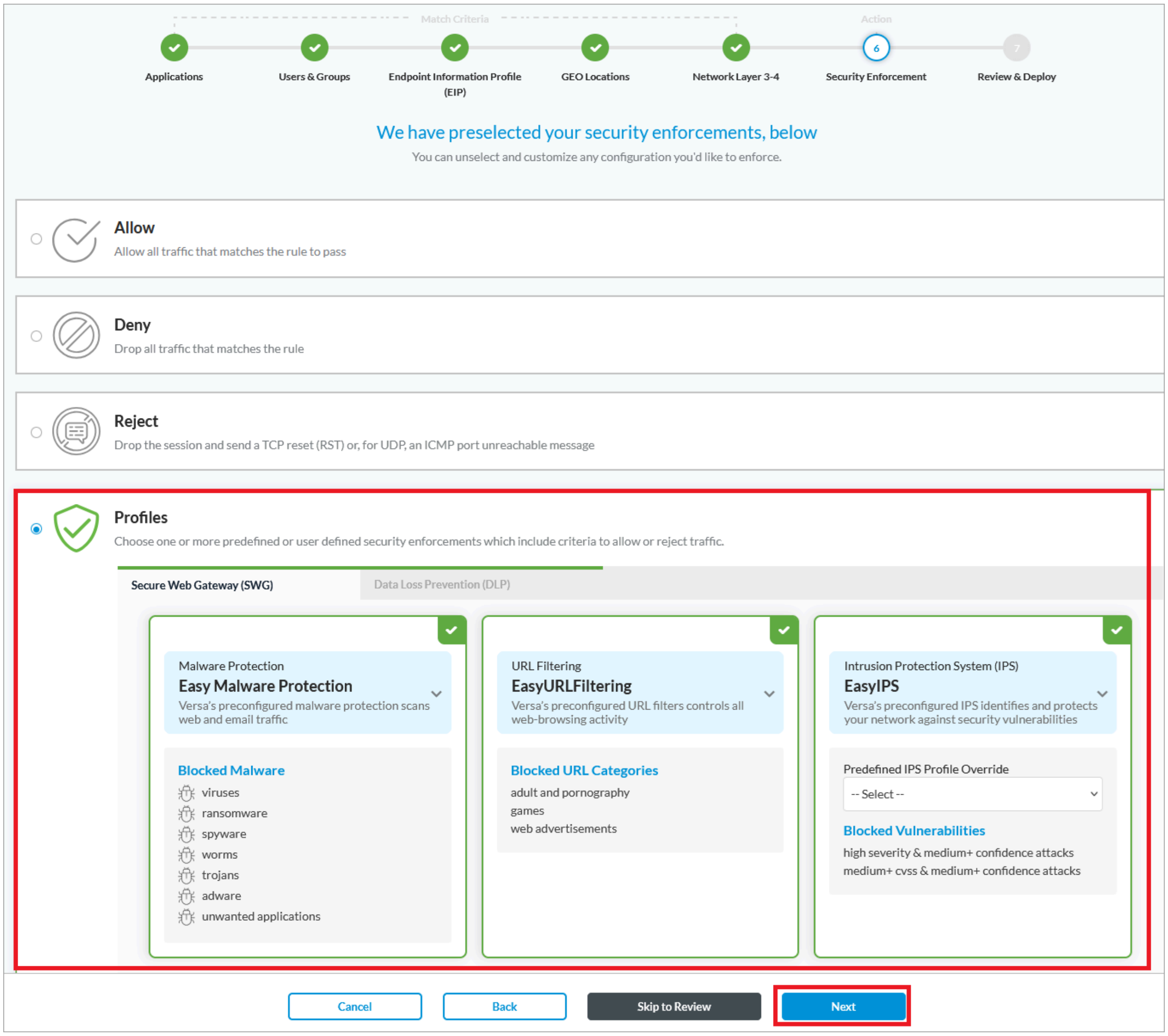


By default, we've included all applications to match.

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

Click Next to progress through the screens for Users & Groups, Endpoint Information Profiles, GEO Locations, and Network Layer 3-4, until you reach the Security Enforcement screen. Note that the enforcement options that are available depend on your license.

In the Security Enforcement screen, under Profiles, select the required protection policies, and then click Next.



We have preselected your security enforcements, below

You can unselect and customize any configuration you'd like to enforce.

○ **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

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

Secure Web Gateway (SWG) | Data Loss Prevention (DLP)

✓ Malware Protection
Easy Malware Protection
Versa's preconfigured malware protection scans web and email traffic

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

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

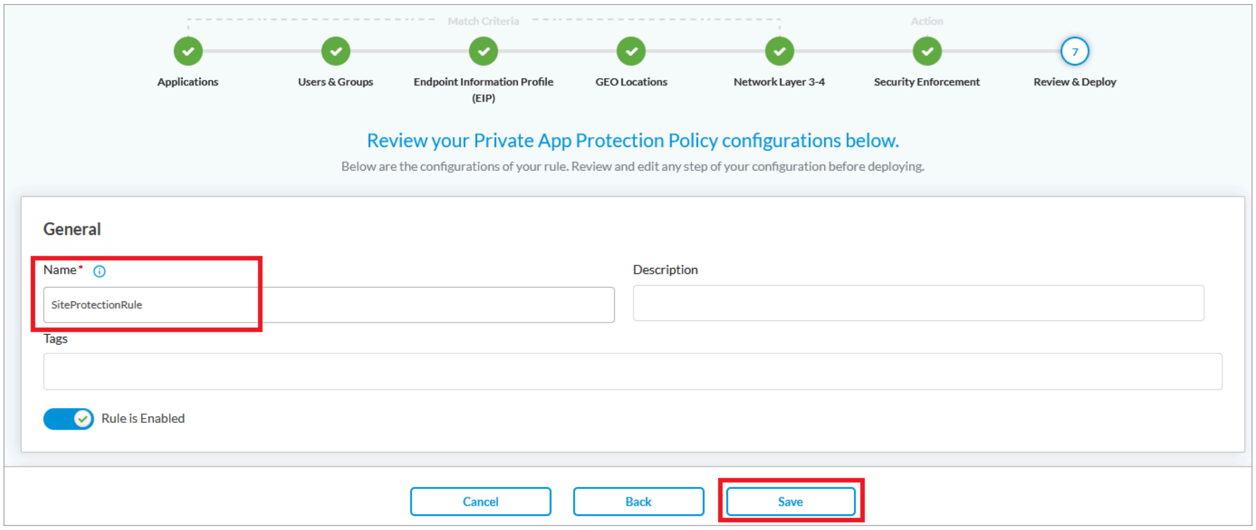
Blocked URL Categories
adult and pornography
games
web advertisements

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

Predefined IPS Profile Override
-- Select --

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

Enter a name for the policy in the Name field, and then click Save.



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* : SiteProtectionRule

Description

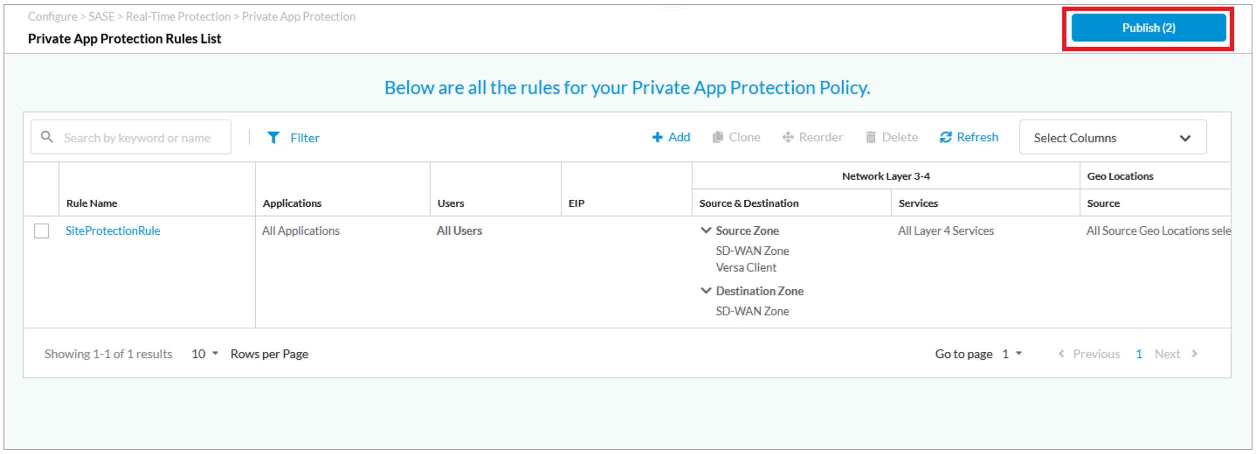
Tags

Rule is Enabled

Step 11: Publish Policies to Gateways

For more information, see Publish SASE Gateways.

After you configure the required policies, you can push them to the Gateways. To do this, click Publish on the top right side of the page.


Configure > SASE > Real-Time Protection > Private App Protection
Publish (2)
Search by keyword or name
Filter
Add
Clone
Reorder
Delete
Refresh
Select Columns
Go to page 1
Previous
1
Next

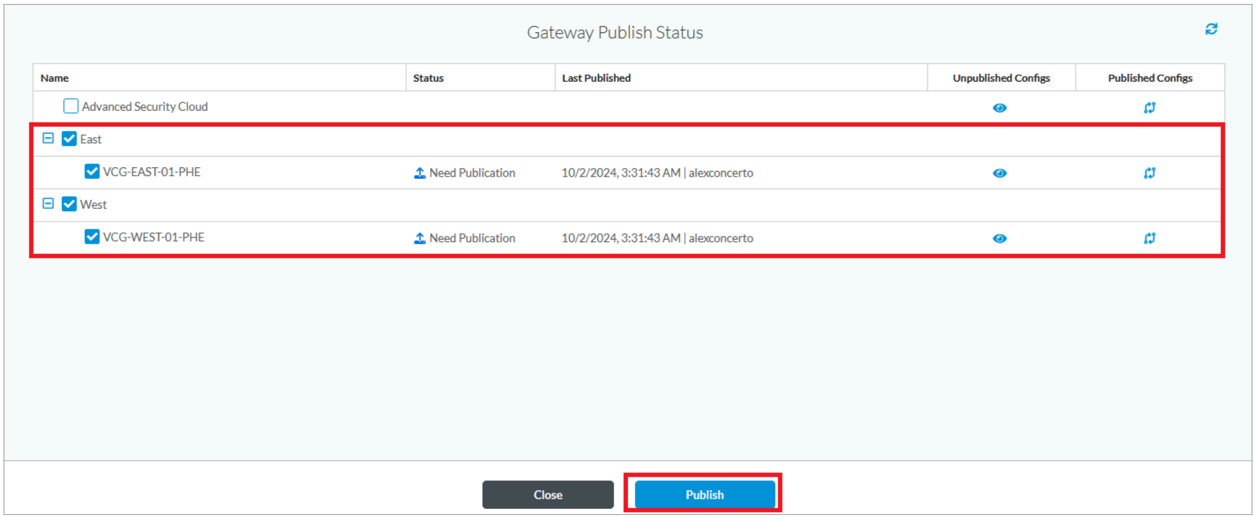
Private App Protection Rules List

Below are all the rules for your Private App Protection Policy.

					Network Layer 3-4		Geo Locations
	Rule Name	Applications	Users	EIP	Source & Destination	Services	Source
□	SiteProtectionRule	All Applications	All Users		Source Zone SD-WAN Zone Versa Client Destination Zone SD-WAN Zone	All Layer 4 Services	All Source Geo Locations sele

Showing 1-1 of 1 results 10 Rows per Page

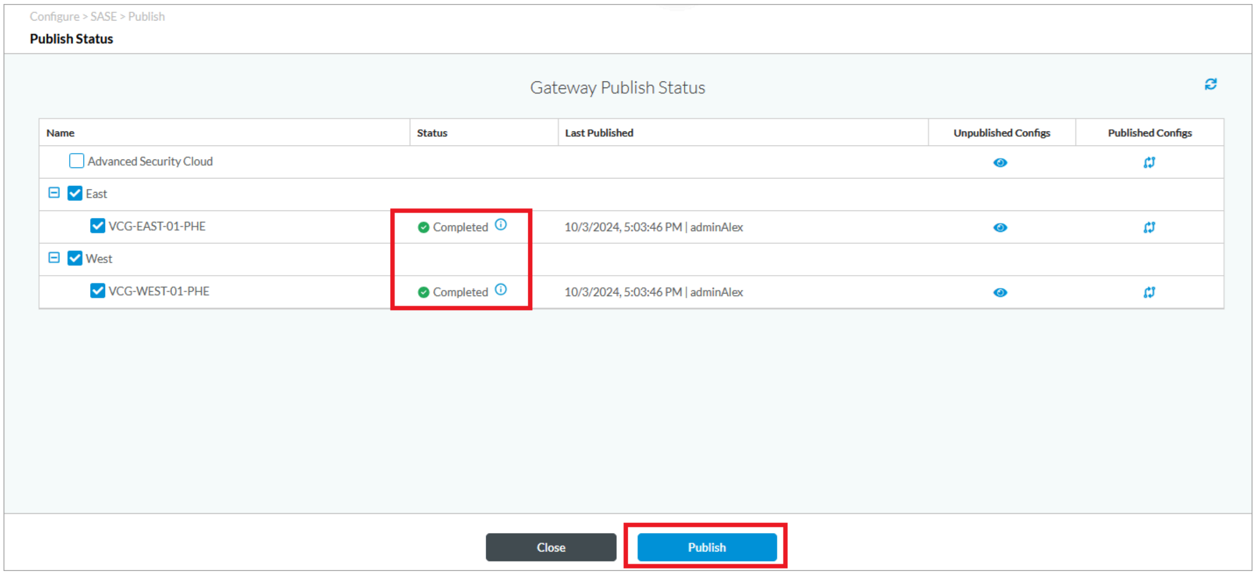
Verify that the required gateways are selected, and then click Publish.



Gateway Publish Status

Name	Status	Last Published	Unpublished Configs	Published Configs
☐ Advanced Security Cloud			👁	🔄
⊟ ☑ East				
☑ VCG-EAST-01-PHE	Need Publication	10/2/2024, 3:31:43 AM | alexconcerto	👁	🔄
⊟ ☑ West				
☑ VCG-WEST-01-PHE	Need Publication	10/2/2024, 3:31:43 AM | alexconcerto	👁	🔄

Wait for the status indicators to change to Completed, and then click Close.



Configure > SASE > Publish

Publish Status

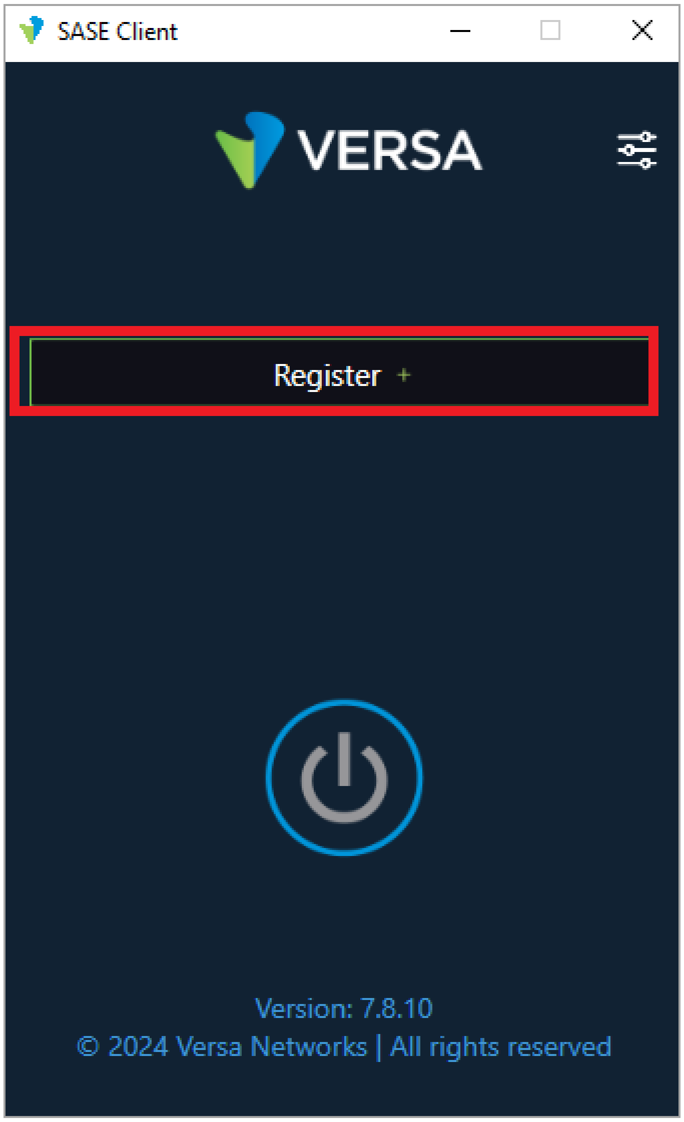
Gateway Publish Status

Name	Status	Last Published	Unpublished Configs	Published Configs
☐ Advanced Security Cloud			👁	🔄
⊟ ☑ East				
☑ VCG-EAST-01-PHE	✓ Completed ⓘ	10/3/2024, 5:03:46 PM | adminAlex	👁	🔄
⊟ ☑ West				
☑ VCG-WEST-01-PHE	✓ Completed ⓘ	10/3/2024, 5:03:46 PM | adminAlex	👁	🔄

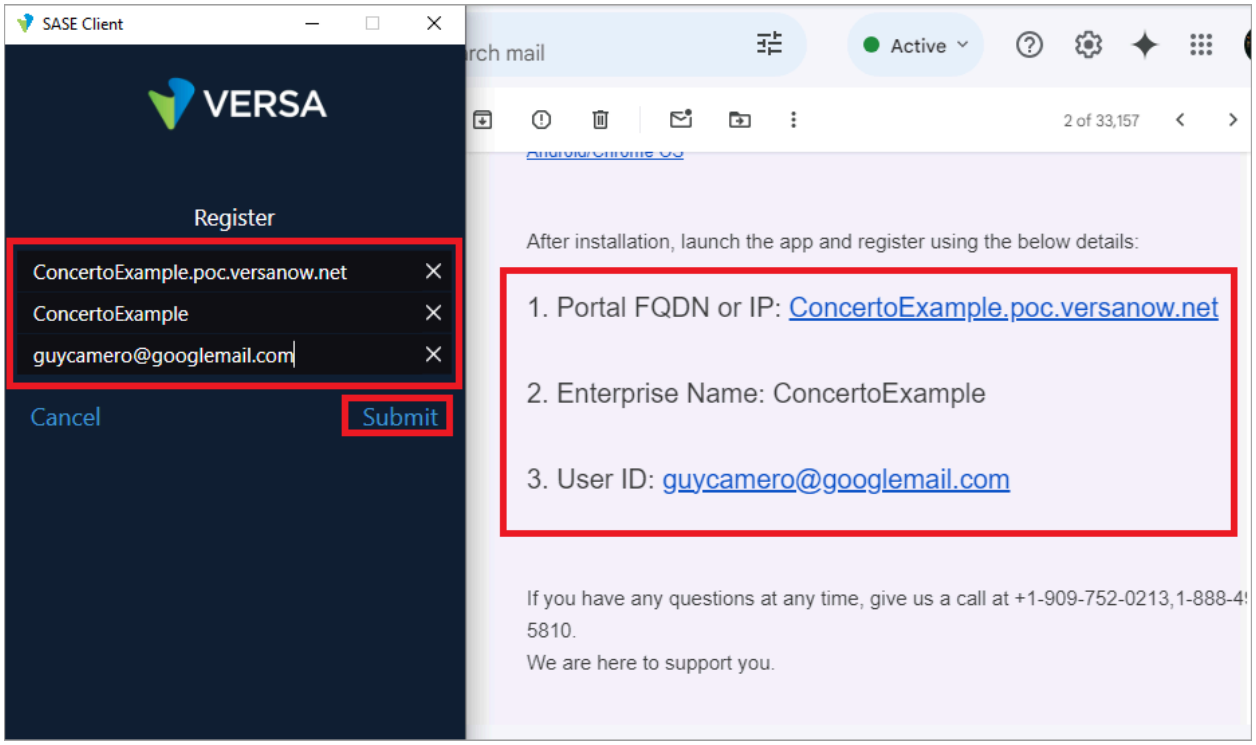
Step 12: Connect to Gateways Using the Configured Client Policy

After you configure the required policies, connect to the gateways from a Windows device using the following procedure.

Open the Versa SASE client, and then click Register.



The email that you receive in the email account configured in Step 3 contains details about how to register the account. Copy the details for Portal FQDN or IP, Enterprise Name, and User ID from the email.



ConcertoExample.poc.versanow.net

ConcertoExample

guycamero@googlemail.com

After installation, launch the app and register using the below details:

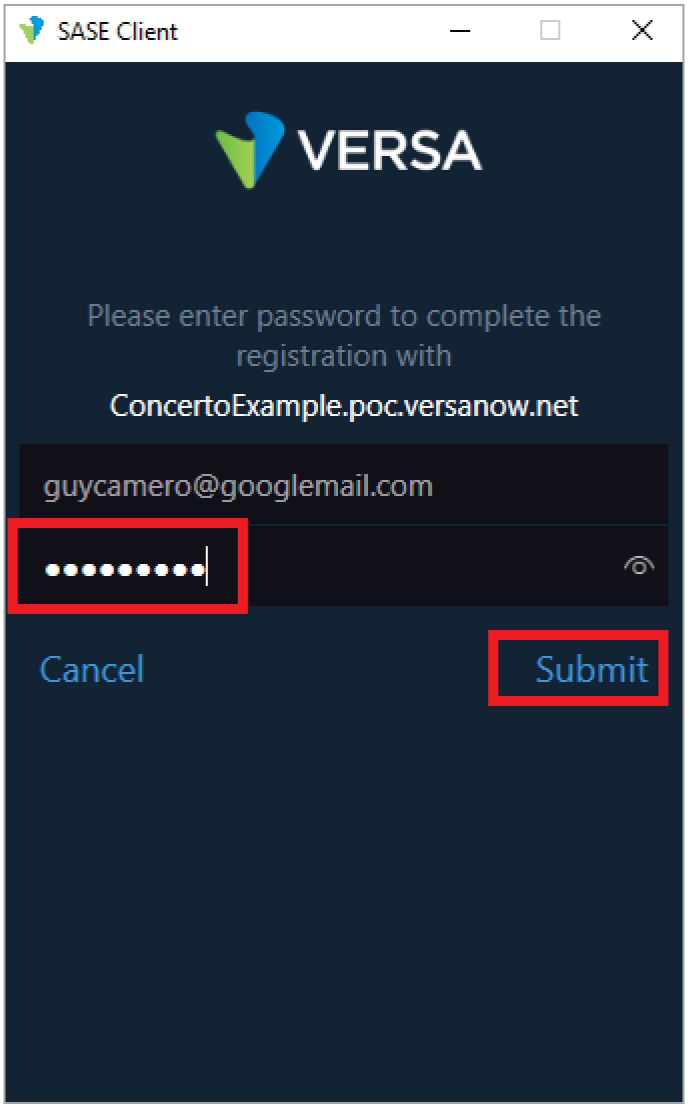
1. Portal FQDN or IP: ConcertoExample.poc.versanow.net

2. Enterprise Name: ConcertoExample

3. User ID: guycamero@googlemail.com

If you have any questions at any time, give us a call at +1-909-752-0213,1-888-4! 5810.
We are here to support you.

When prompted, enter the the configured password, and then click Submit.



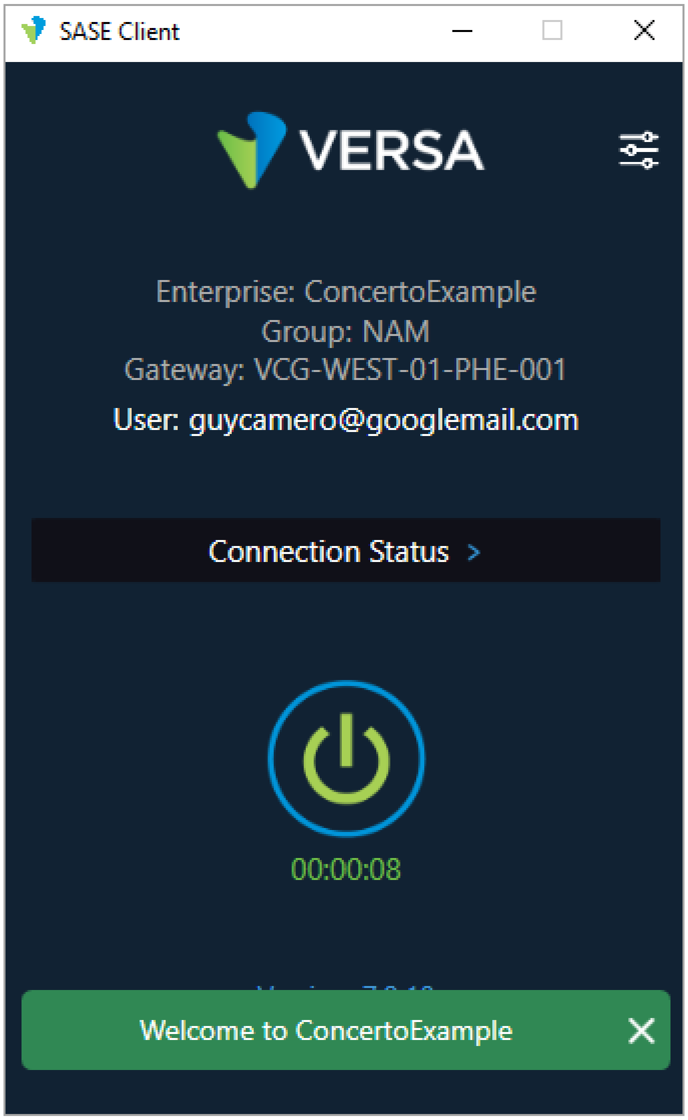
Please enter password to complete the registration with

ConcertoExample.poc.versanow.net

guycamero@googlemail.com

••••••••••

After a few moments the SASE client connects to a gateway.

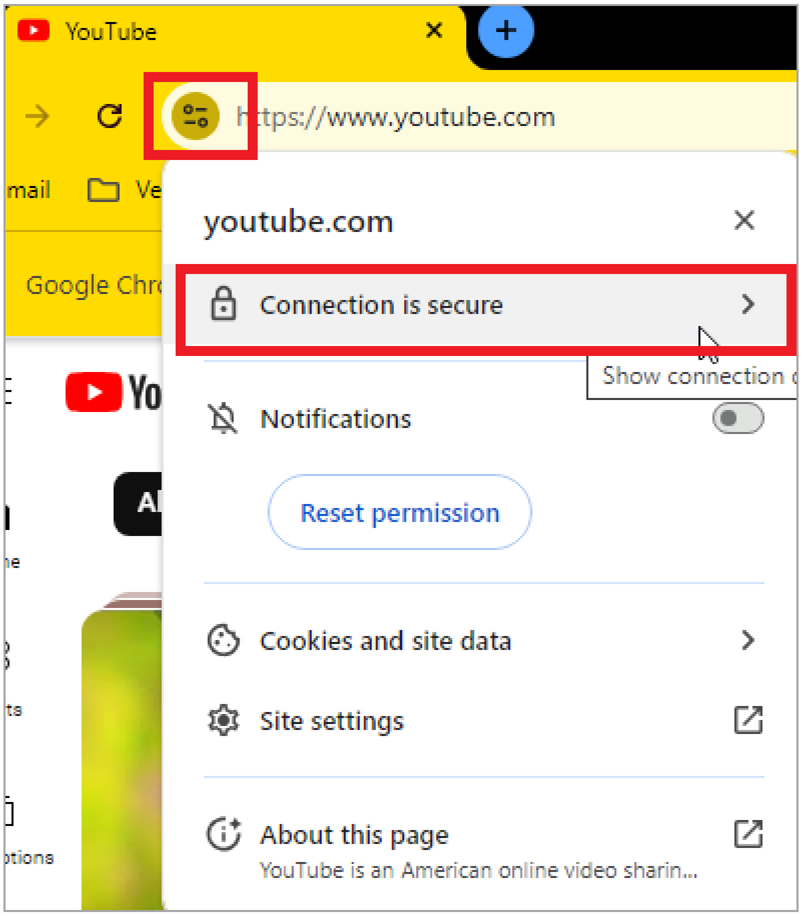


Enterprise: ConcertoExample
Group: NAM
Gateway: VCG-WEST-01-PHE-001
User: guycamero@googlemail.com

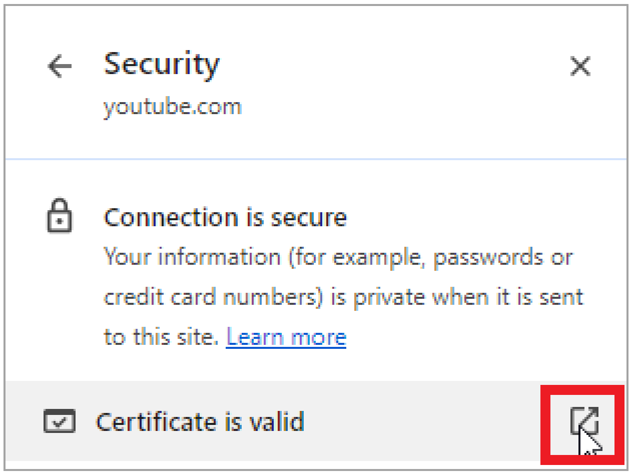
00:00:08

Welcome to ConcertoExample

Next, you can validate the traffic sent through the gateway. For example, open YouTube to verify if the decryption policy is active. To do this, click the Site Information icon next to the YouTube URL, and then click Connection is secure.

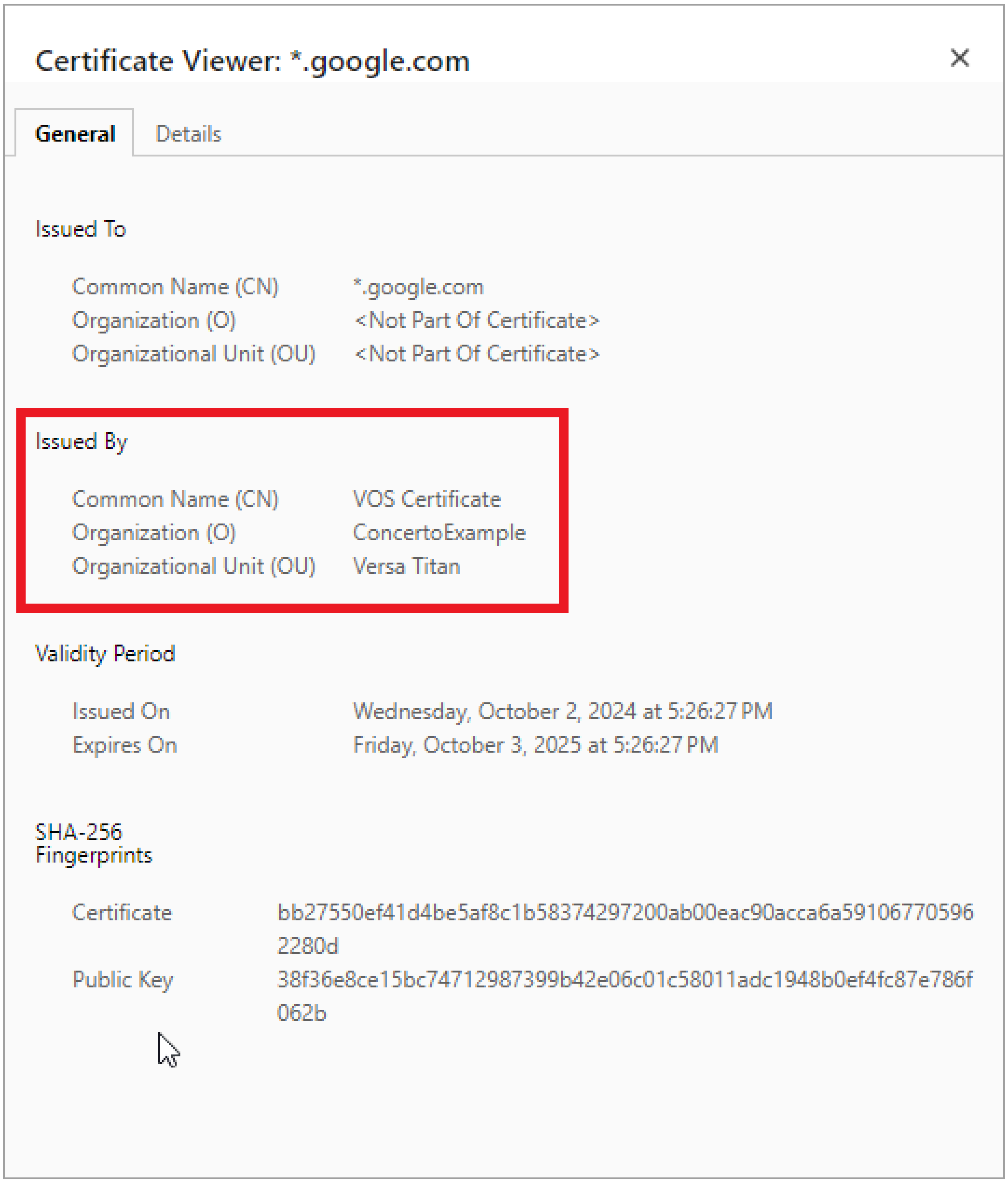


Click the ↗ icon next to Certificate is valid.



Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

You can view the VOS certificate in use.



Certificate Viewer: *.google.com

Issued To

Common Name (CN)	*.google.com
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	VOS Certificate
Organization (O)	ConcertoExample
Organizational Unit (OU)	Versa Titan

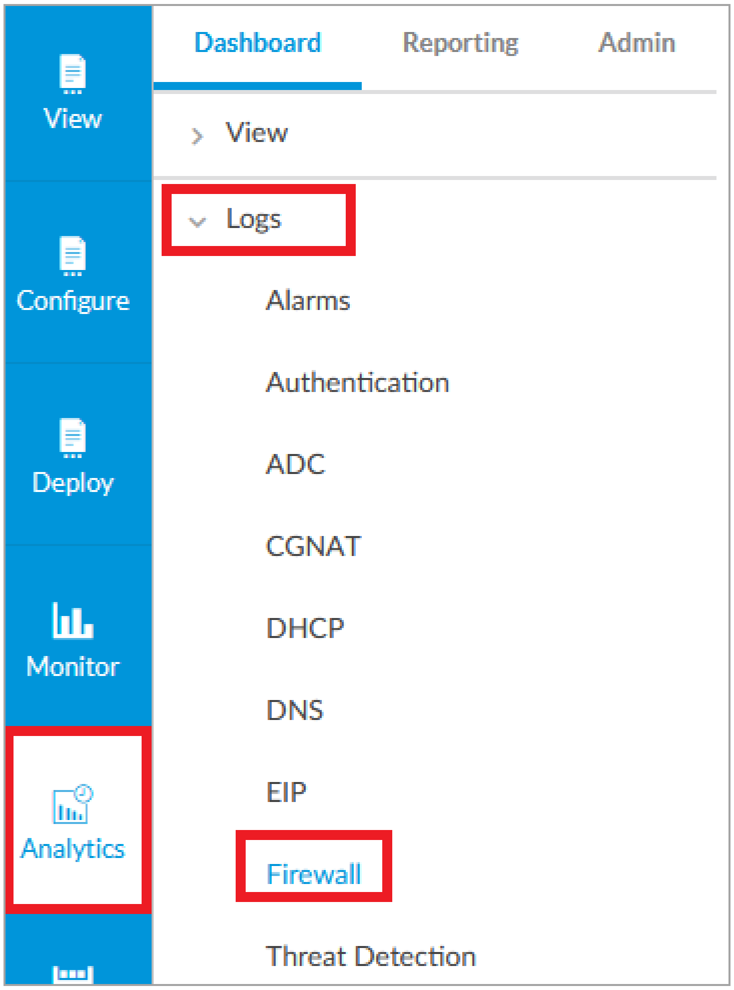
Validity Period

Issued On	Wednesday, October 2, 2024 at 5:26:27 PM
Expires On	Friday, October 3, 2025 at 5:26:27 PM

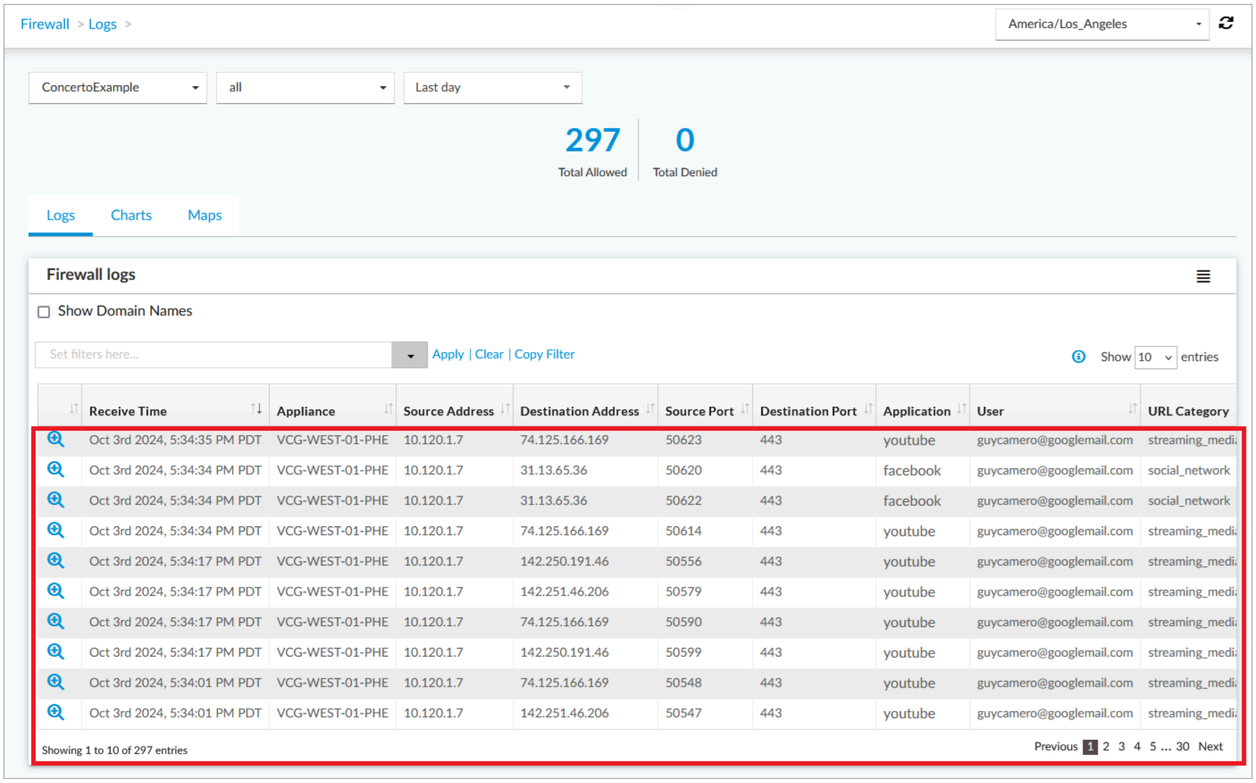
SHA-256 Fingerprints

Certificate	bb27550ef41d4be5af8c1b58374297200ab00eac90acca6a591067705962280d
Public Key	38f36e8ce15bc74712987399b42e06c01c58011adc1948b0ef4fc87e786f062b

Next, go to Analytics > Logs > Firewall.



After a few minutes, you can view logs for the applications that are sent through the gateways.



Firewall > Logs >

America/Los_Angeles

ConcertoExample | all | Last day

297 Total Allowed | 0 Total Denied

Logs | Charts | Maps

Firewall logs

□ Show Domain Names

Set filters here... Apply | Clear | Copy Filter

Show 10 entries

	Receive Time	Appliance	Source Address	Destination Address	Source Port	Destination Port	Application	User	URL Category
🔍	Oct 3rd 2024, 5:34:35 PM PDT	VCG-WEST-01-PHE	10.120.1.7	74.125.166.169	50623	443	youtube	guycamero@googlemail.com	streaming_medi
🔍	Oct 3rd 2024, 5:34:34 PM PDT	VCG-WEST-01-PHE	10.120.1.7	31.13.65.36	50620	443	facebook	guycamero@googlemail.com	social_network
🔍	Oct 3rd 2024, 5:34:34 PM PDT	VCG-WEST-01-PHE	10.120.1.7	31.13.65.36	50622	443	facebook	guycamero@googlemail.com	social_network
🔍	Oct 3rd 2024, 5:34:34 PM PDT	VCG-WEST-01-PHE	10.120.1.7	74.125.166.169	50614	443	youtube	guycamero@googlemail.com	streaming_medi
🔍	Oct 3rd 2024, 5:34:17 PM PDT	VCG-WEST-01-PHE	10.120.1.7	142.250.191.46	50556	443	youtube	guycamero@googlemail.com	streaming_medi
🔍	Oct 3rd 2024, 5:34:17 PM PDT	VCG-WEST-01-PHE	10.120.1.7	142.251.46.206	50579	443	youtube	guycamero@googlemail.com	streaming_medi
🔍	Oct 3rd 2024, 5:34:17 PM PDT	VCG-WEST-01-PHE	10.120.1.7	74.125.166.169	50590	443	youtube	guycamero@googlemail.com	streaming_medi
🔍	Oct 3rd 2024, 5:34:17 PM PDT	VCG-WEST-01-PHE	10.120.1.7	142.250.191.46	50599	443	youtube	guycamero@googlemail.com	streaming_medi
🔍	Oct 3rd 2024, 5:34:01 PM PDT	VCG-WEST-01-PHE	10.120.1.7	74.125.166.169	50548	443	youtube	guycamero@googlemail.com	streaming_medi
🔍	Oct 3rd 2024, 5:34:01 PM PDT	VCG-WEST-01-PHE	10.120.1.7	142.251.46.206	50547	443	youtube	guycamero@googlemail.com	streaming_medi

Showing 1 to 10 of 297 entries

Previous 1 2 3 4 5 ... 30 Next

You can also test connectivity through your site-to-site tunnel using Ping.