
Configure SASE for SIM



For supported software information, click [here](#).

When using traditional solutions for IoT and mobility projects, service providers face many challenges to provide enterprises with private mobility that offers both an optimal user experience and data privacy to enterprises. Some of these challenges include:

- Dependency on software clients to access internal applications from outside the enterprise premises. This dependency causes security issues, inconsistent application experience, and operational complexity for the IT team, which has to manage the various software clients.
- Most IoT devices are black-box systems, so they do not allow the installation of software clients and agents, which leads to security gaps.
- Legacy VPN concentrator technologies cannot provide effective segmentation and instead provide access to the entire network, thus increasing overall risk to the organization.
- Many enterprise IT teams cannot monitor network activity when devices are outside the enterprise network and are not connected to the VPN.

The Versa Operating System™ (VOS™) SASE for SIM allows organizations to deploy SASE in a flexible manner. SASE for SIM requires minimal infrastructure change and seamlessly fits into the existing networks of mobile network operators (MNOs) by adding a SASE domain. SASE for SIM allows seamless remote access to corporate data and applications while protecting against cyber attacks and threats.

SASE for SIM is a clientless solution that helps secure SIM-enabled IoT and user devices connected over 2G, 3G, 4G, and 5G networks. To provide network security, SASE for SIM authenticates and authorizes devices using the unique international mobile subscriber identity (IMSI). It provides zero-trust connectivity for SIM-enabled devices connecting to internet or SaaS applications, and to applications hosted by an enterprise in data center, private cloud, or virtual private cloud instances of public cloud providers. SASE for SIM offers password-less authentication to identify users and to enforce zero-trust policies. SASE for SIM provides a full security suite that includes antivirus, intrusion detection system (IDS), intrusion prevention system (IPS), antivirus, SSL decryption, and URL filtering.

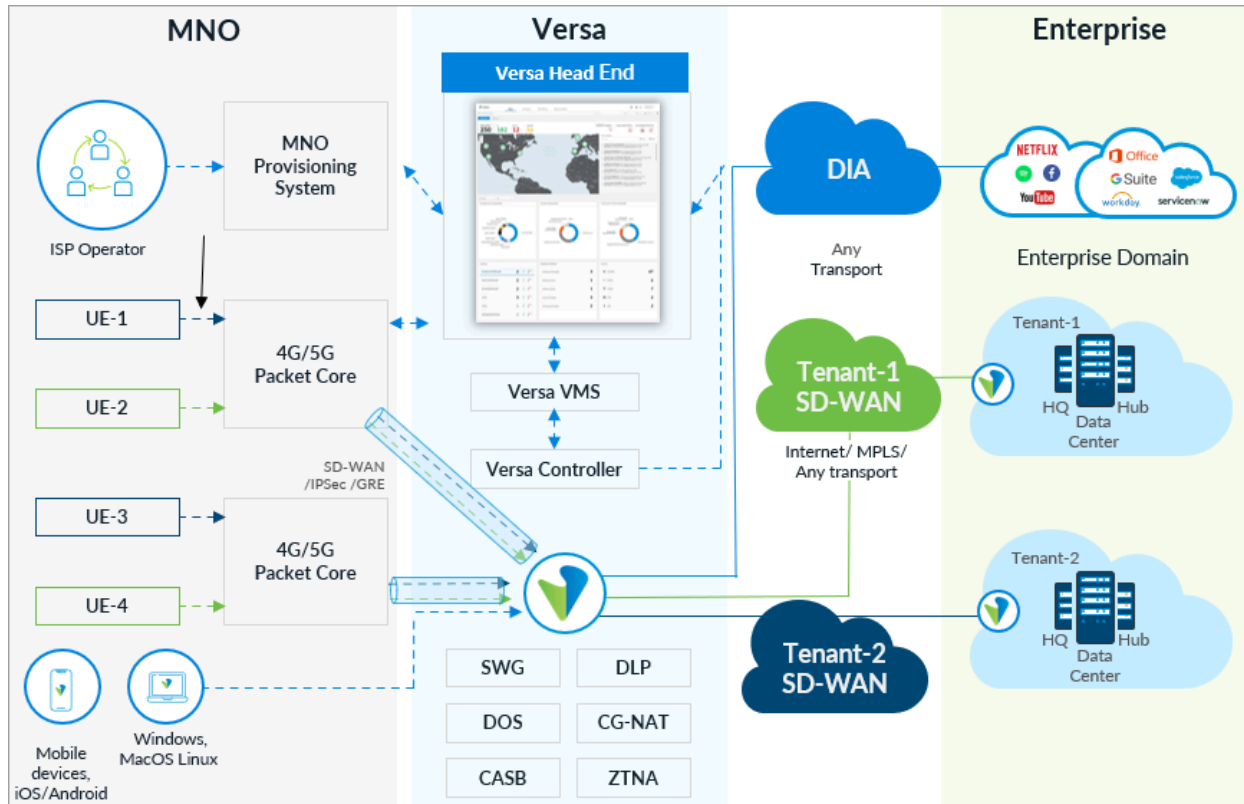
This article provides an overview of SASE for SIM, and it describes how to enable SASE for SIM on Concerto, how to configure device user groups, and users, and how to associate device groups with real-time protection and advanced security rules.

SASE for SIM Architecture

VOS SASE for SIM provides traffic segregation by using Versa Messaging Service (VMS) to identify tenants. VMS integrates with the Versa Concerto and Director orchestration provisioning systems and with Versa Analytics to provide private mobility services.

The following figure illustrates how SASE for SIM operates:

- Identify the tenant data that is received by gateways, which are configured by the mobile network operator or mobile virtual network operator (MVNO) provisioning systems.
- Versa SASE gateways map user traffic to an SD-WAN overlay or break it out locally after applying security policies.
- Obfuscate device information before sending it to the cloud.
- Use multitenancy to serve multiple customers over a single VOS instance.
- No requirement for a VPN client on the device.
- Support 4G, 5G, and WiFi mobility.



For mobile device users, SASE for SIM allows service providers to use the mobile SIM (IMSI) to authorize devices on a network, thus allowing clientless access to a company's services and applications.

SASE for SIM Components

SASE for SIM uses the following Versa headend components :

- Versa Director
- Versa Concerto
- Versa Controller
- Versa Analytics
- VMS

You can integrate a service provider's orchestration platform with Versa Director or Concerto. You perform the following on Concerto and Director to integrate with VMS:

- Configure a VMS connector from a Director node and enable SASE for SIM service for the connector. For more information, see [Configure Versa Messaging Service](#).
- Perform VMS-related tenant onboarding from Concerto.
- Configure users and user groups for tenants on Concerto or Director nodes, which then share the group, tenant, IMSI (user ID), and solution tier information with VMS.

Versa Analytics analyzes logs and events and provides reports and analytics for SASE for SIM events shared by VMS. The following are the types of VMS events:

- Activities—Start-stop events for each IMSI-to-IP address combination
- Exceptions—Errors that occur while processing data for orchestration, accounting, and Kafka

VMS integrates with Versa Controller to connect to a VOS device over an IPsec tunnel and for configuration of an Analytics application delivery controller (ADC).

VMS integrates with other Versa components for SASE for SIM as follows:

- Concerto or Director nodes—For user, tenant, or group orchestration
- VOS devices—VMS shares the following information with VOS devices:
 - IMSI-to-IP address mapping information that it receives from RADIUS server or Kafka connector
 - Tenant and group information from Concerto or Director nodes
- Controller—To connect to VOS over IPsec tunnel and for the Analytics ADC configuration
- Analytics nodes—For logging

Director and Concerto nodes share the IMSI details of a tenant with VMS. VMS shares the IP address allocated by the private gateway with a mobile device along with the IMSI information to the service provider's AAA proxy server. It then receives the IMSI-to-IP address information from the AAA proxy server through AAA accounting-start and accounting-stop messages, which it distributes to all subscribed SASE gateways and VOS devices. VOS devices use this information, along with the policy configuration for each group and tenant, to apply traffic-steering policies for SD-WAN, security, SSE, and SASE services.

SASE for SIM Flow

This section describe the SASE for SIM flow in a service provider environment.

SASE for SIM integrates with RADIUS accounting messages and Kafka interface.

Orchestration is provided by Versa Concerto or Versa Director:

- Service provider on-boards tenant.
- Service provider or tenant orchestrates the IMSI (userID), IMEI, group, and solution-tier information using Concerto.

Information flows between the AAA proxy and the VMS node:

- End user device attaches to a packet gateway via a mobile attach, which is an identity service to share information.
- Packet gateway assigns an IP address to the device.
- Packet gateway sends RADIUS accounting start messages, containing the current IP address and IMSI, to the AAA proxy, which shares it to VMS.
- VMS maps the IMSI or IP address to tenants.
- VMS send the information from Concerto/Director and AAA (Radius or Kafka) to VOS.

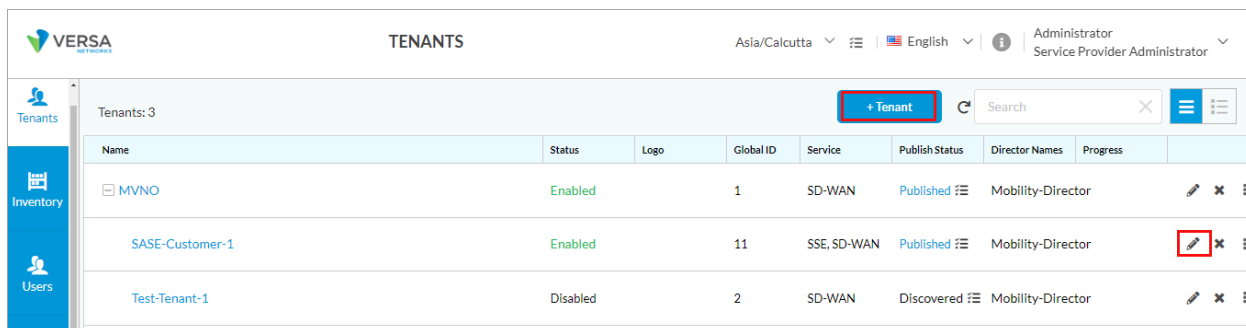
Traffic travels from the end user device to a Versa SASE gateway:

- End user traffic goes through the service provider's infrastructure and reaches the Versa SASE gateway, which maps traffic to the tenant based on the information provided by VMS.
- Traffic traverses the tunnel virtual interface (TVI) interface and reaches the virtual router (VR).
- Traffic reaches the service provider network, and is then directed to the internet or direct internet access (DIA) depending on the traffic policy.

Enable SASE for SIM

To enable SASE for SIM for a tenant:

1. Go to the Tenants dashboard screen.



Name	Status	Logo	Global ID	Service	Publish Status	Director Names	Progress
MVNO	Enabled		1	SD-WAN	Published	Mobility-Director	
SASE-Customer-1	Enabled		11	SSE, SD-WAN	Published	Mobility-Director	
Test-Tenant-1	Disabled		2	SD-WAN	Discovered	Mobility-Director	

2. Click + Tenant to add a tenant or click the Edit icon to update an existing tenant. The Create/Edit Tenant window

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_SASE_for_SIM](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_SASE_for_SIM)

Updated: Wed, 23 Oct 2024 08:38:36 GMT

Copyright © 2024, Versa Networks, Inc.

displays, and Step 1, General, is selected.

Configure > Tenant

Create Tenant

1
General

2
Security Service Edge

3
Roles
(Tenant Active Roles)

4
Review & Submit

Tenant Name

Enabled

Description

Global Tenant ID

12

Parent Tenant

Select

Managed Service Provider (MSP)

Disabled

Select Services

☐ Secure SD-WAN

☒ Security Service Edge (SSE)

☒ SASE for SIM

Directors

Host

Mobility-Director

Is Default

Controllers

Controller-2

Controller-4

Controller-3

Controller-1

ZTP Type

☒ Serial Number

☐ URL

SDWAN Solution Tiers

Work-From-Home

Premier-Secure-SDWAN

Prime-Secure-SDWAN

Prime-SDWAN

Premier-Elite-SDWAN

Non-SDWAN Solution Tiers

Search for Solution Tiers

Appliance Preferred Version

Cancel

Back

Skip to Review

Next

3. In Select Services, click Security Service Edge (SSE) and SASE-for-SIM. Note that you must select Security Service Edge (SSE) to enable SASE for SIM.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_SASE_for_SIM](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_SASE_for_SIM)

Updated: Wed, 23 Oct 2024 08:38:36 GMT

Copyright © 2024, Versa Networks, Inc.

4. For information about configuring other parameters, see [Configure SASE Tenants](#).
5. Save the changes.

Add SASE for SIM Device Groups and Devices

You can create and manage groups of mobile devices in a private mobile network. You then add devices and associate devices with groups. The devices and device groups that you create are automatically published to Versa Director, which publishes the information to VMS.

Add a SASE for SIM Device Group

You add a device group for SASE for SIM.

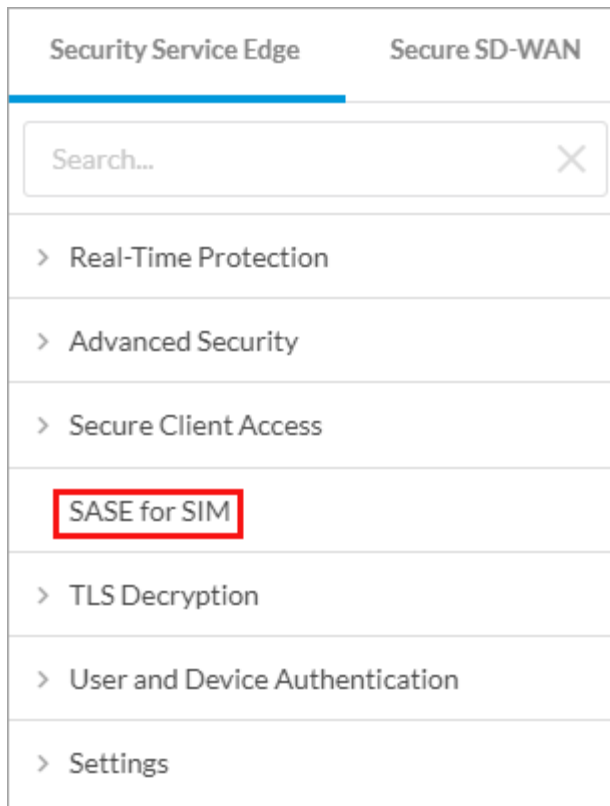
Note that the following groups are configured and displayed by default, and you cannot modify or delete them:

- VSPA-Default—Versa Secure Private Access (VSPA) service provides access to the internet and public clouds for employees working in branch offices, home offices, and remotely. It also provides secure access to the internet for service provider users.
- VSIA-Default—Versa Secure Internet Access (VSIA) service allows a distributed workforce to securely access private data centers and private clouds from branch offices, home offices, and anywhere else. It also provides secure access to private enterprise resources for service provider users.
- VSIA-VSPA-Default—Combination of VSIA and VSPA. It provides secure access to the internet and private enterprise resources for service provider users.

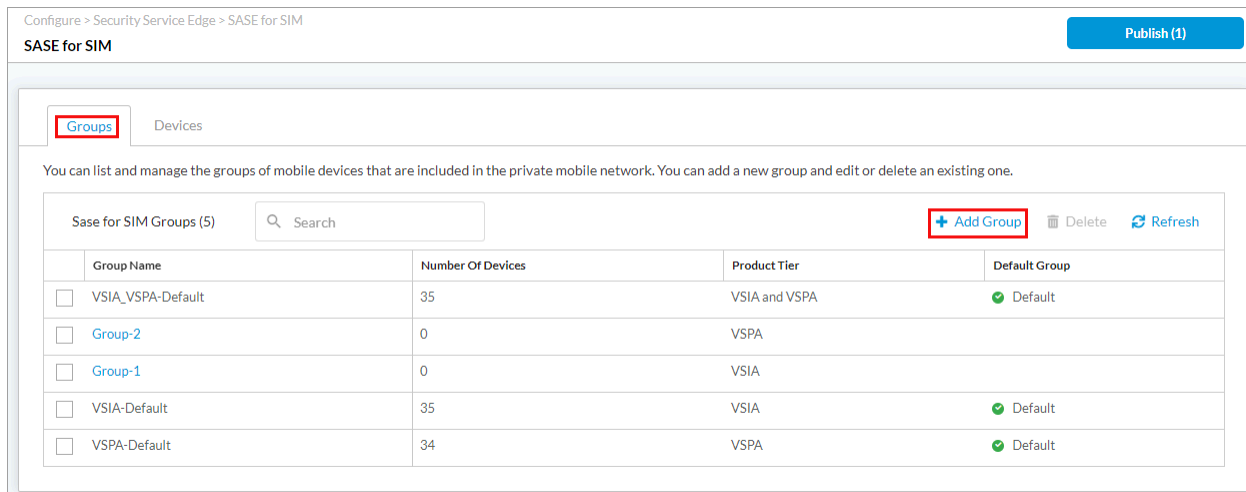
If you provision a device user without associating the user with a group, the user is provisioned to the default group associated with your license tier. You can also add custom device groups.

To add SASE for SIM device groups:

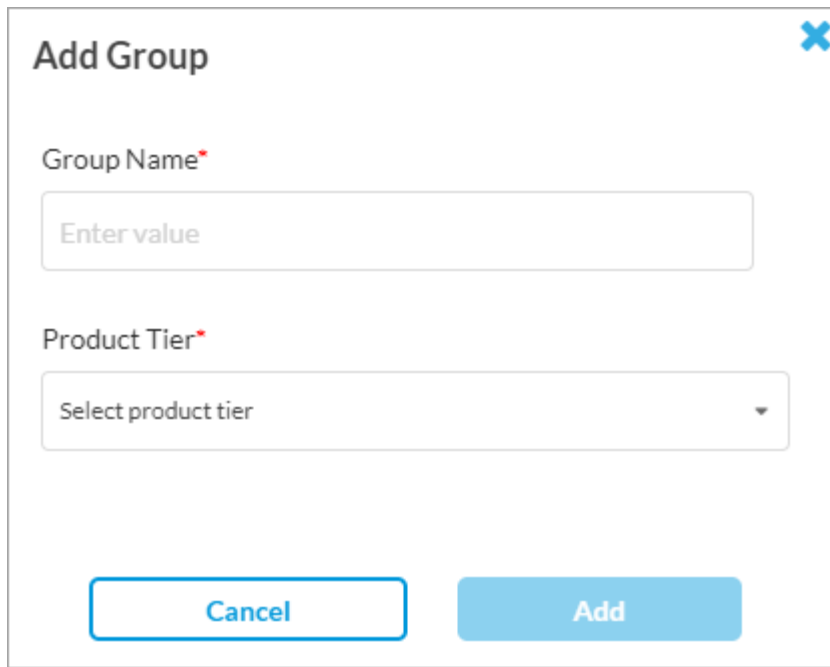
1. Go to Configure > Secure Services Edge > SASE for SIM.



The SASE for SIM screen displays.



2. Select the Groups tab.
3. Click + Add Group, and then enter information for the following fields in the Add Group screen.

A dialog box titled "Add Group" with a blue close button (X) in the top right corner. It contains two required fields: "Group Name" with a text input box containing the placeholder "Enter value", and "Product Tier" with a dropdown menu containing the placeholder "Select product tier". At the bottom, there are two buttons: "Cancel" and "Add".

Add Group

Group Name*

Enter value

Product Tier*

Select product tier

Cancel Add

4. Enter a name for the group in the Group Name field.
5. In the Product Tier field, select a tier:
 - VSIA
 - VSPA
 - VSIA and VSPAFor more information, see [View Subscription Information](#).
6. Click Add.

Add a SASE for SIM Device

1. In the SASE for SIM window, select the Devices tab.

Configure > Security Service Edge > SASE for SIM

SASE for SIM Publish (1)

Groups **Devices**


You can list and manage the mobile devices that are included in the private mobile network. You can add a new mobile device, and edit or delete an existing one.

Show Filter Bar Applied Filters (0) Reset to Default Filter

Devices (10) Delete Refresh **Add Device** Download CSV File Select Columns

<input type="checkbox"/>	IMSI	IMEI	MSISDN	USER GROUPS	PRODUCT TIER	LOCATION	Tags	Status	DATE ADDED	LAST MODIFIED
<input type="checkbox"/>	12345456667			VSIA-Default	VSIA			ACTIVATED	Fri, Mar 29, 2024 23:03 PM UTC	Fri, Mar 29, 2024 23:03 PM UTC
<input type="checkbox"/>	2345678904	2345678904	2345678904	VSIA_VSPA-Default	VSIA and VSPA			ACTIVATED	Tue, Apr 02, 2024 04:14 AM UTC	Tue, Apr 02, 2024 04:14 AM UTC
<input type="checkbox"/>	2345678908	2345678908	2345678908	VSIA-Default	VSIA			ACTIVATED	Tue, Apr 02, 2024 04:14 AM UTC	Tue, Apr 02, 2024 04:14 AM UTC
<input type="checkbox"/>	2345678909	2345678909	2345678909	VSIA_VSPA-Default	VSIA and VSPA			ACTIVATED	Tue, Apr 02, 2024 04:14 AM UTC	Tue, Apr 02, 2024 04:14 AM UTC

2. Click Add Device. The following options display.

Add Device 

Add Single Device

Bulk upload via file

3. To add a single device, click Add Single Device. The Add Single Device screen displays. Enter information for the following fields.

Add Single Device



IMSI*

Enter value

Product Tier*

Select product tier

Group Name

Select product tier first

IMEI

Enter value

☐ Strict IMEI Check

MSISDN

Enter value

SOC Code

Enter value

Status

ACTIVATED

LOCATION

Enter value

Tags

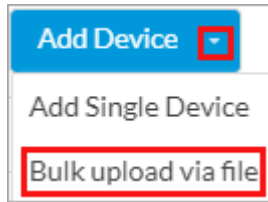
Press Enter to add

Cancel

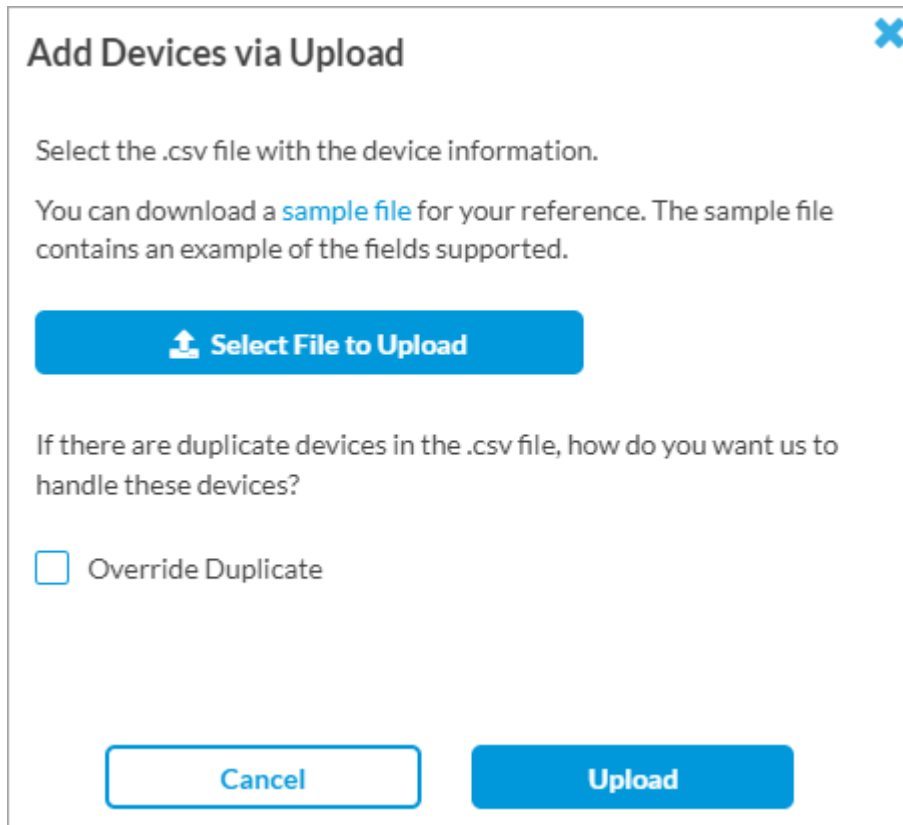
Add

Field	Description
IMSI	Enter the IMSI of the device that SASE for SIM uses to authorize devices in a network.
Product Tier	<p>Select a product option:</p> <ul style="list-style-type: none"> ◦ VSIA—Provide secure access to the internet for service provider users. ◦ VSPA—Provide secure access to private enterprise resources for service provider users. ◦ VSIA and VSPA—Provides both VSIA and VSPA access.
Group Name	Select a device group for the device. You can add a device or user to multiple groups for a tenant or license tier. For more information, see Add a SASE for SIM Device Group , above.
IMEI	Enter the 15-digit International Mobile Equipment Identity (IMEI) number of the device.
Strict IMEI Check	Select to enable strict IMEI checking. For device lock-in or device verification, the VOS device validates the first 14 digits of the IMEI number for each request that it receives from the service provider interface (either RADIUS or Kafka). If the IMEI does not match, the user is not provisioned. This check prevents SIM activation from an unidentified device.
MSISDN	Enter the Mobile Station International Subscriber Directory Number (MSISDN), which is the phone number associated with a single SIM card and is the number to which you call or send an SMS message.
SOC Code	Enter the 12-bit System Operator Code (SOC) that identifies a service provider. A mobile station uses SOC along with System Identity (SID) to acquire or reject services offered by specific service providers.
Status	<p>Select the status:</p> <ul style="list-style-type: none"> ◦ Activated ◦ Suspended
Location	Enter the location of the device.
Tags	Enter a tag and press enter to add the tag.

4. Click Add.
5. To upload many devices, in the Device tab, click Add Device and select Bulk Upload via File.



The Add Devices via Upload window displays.



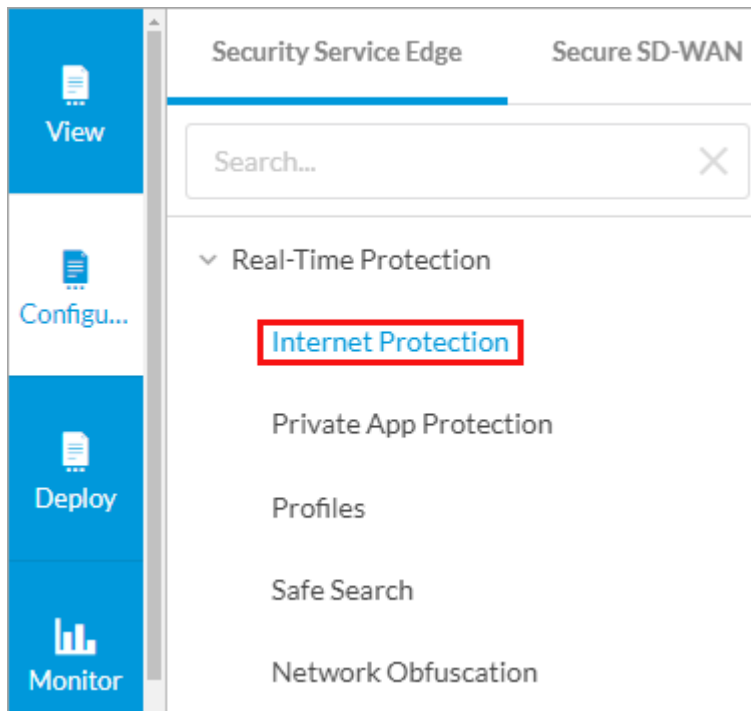
6. Click Select File to Upload to upload a .csv file that includes information of devices. You can download a sample file from this window for reference.
7. Click Override Duplicate to avoid uploading devices that are already added.
8. Click Upload.

Associate Device Groups with Rules

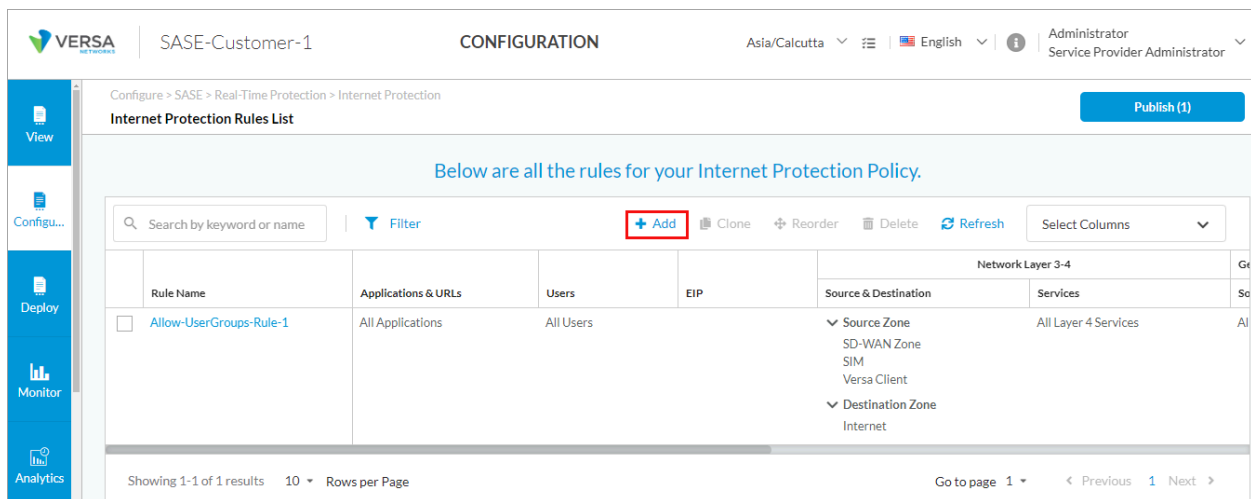
You can associate SASE for SIM device groups with Internet Protection and Private App Protection rules. The section describes how to associate private mobility device groups with an internet protection rule.

To add SASE for SIM device groups to an internet protection rule match criteria:

1. Go to Configure > Real-Time Protection > Internet Protection.



The Internet Protection Rules List screen displays all configured internet protection rules.



2. Click + Add to create a rule. The Create Internet Protection Rule screen displays.
3. Select Step 2, User Groups.

7. Click Submit in the Review and Deploy screen.

For information about associating device groups with a private application protection rule, see [Configure SASE Private Application Protection Rules](#).

Supported Software Information

Releases 12.1.1 and later support all content described in this article.

Additional Information

[Configure SASE Internet Protection Rules](#)

[Configure SASE Private Application Protection Rules](#)

[Configure SASE Tenants](#)

[Configure Versa Messaging Service](#)

[View Subscription Information](#)