

---

## Configure SASE Tenants

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

You can configure a tenant to be a managed service provider (MSP) tenant. When you enable MSP on a tenant, the SASE service is automatically assigned to the tenant. You can configure multiple VPNs per SASE tenant, and you can configure logging services for SASE tenants that subscribe to the Versa SASE fabric service

This article describes how to add a new SASE tenant to a parent organization.

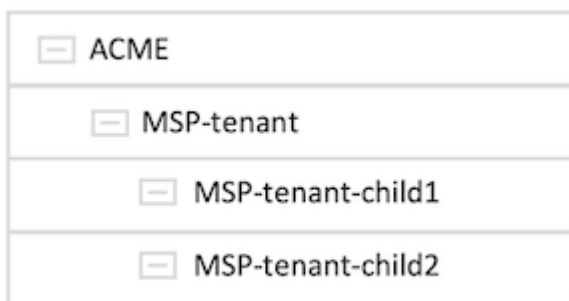
For information about configuring an SD-WAN tenant, see [Configure a Secure SD-WAN Tenant](#).

---

## MSP Tenant Overview

You can configure a tenant to be a managed service provider (MSP) tenant. When you enable MSP on a tenant, the SASE service is automatically assigned to the tenant. An MSP tenant does not own any SASE gateways itself, but it can have subtenants that have access to the gateways that are owned by the MSP tenant's parent tenant.

The following figure illustrates the hierarchy of an MSP tenant. Here, the tenant named MSP-tenant is an MSP tenant that does not own any gateways, but its parent, ACME, does own gateways. The subtenants of MSP-tenant are MSP-tenant-child1 and MSP-tenant-child2, and they have access to the gateways owned by ACME.



When you create an MSP tenant, you configure it to have one of the following gateway types:

- **Shared**—The MSP tenant does not own any of the gateways. This tenant is onboarded onto Director and Controller nodes, but it is not provisioned on the gateways. Any non-MSP subtenant inherits gateways from the parent tenant of an MSP tenant, that is, from the ancestor tenant that has gateways. For example, if an MSP tenant called MSP-tenant is the child of the tenant called ACME, any subtenant of MSP-tenant can access all gateways available on

the ACME tenant. MSP-tenant provides its subtenants with access to ACME's gateways, even though MSP-tenant does not own any gateways itself.

- **Dedicated**—The MSP tenant owns the gateways. After the tenant is created from Concerto or directly from the Director organization workflow, SSE gateways are created directly on Versa Director with the MSP tenant as the provider organization. Concerto then does the following to discover the dedicated gateways from the Director nodes:
  - **Discover the Director nodes**—Discover the MSP tenants that were onboarded directly to Versa Director. If an MSP tenant was created in Concerto, this operation does not apply.
  - **Use the appliance discovery process** to discover the gateways owned by the MSP tenant on the Director nodes.

For MSP tenants using the dedicated gateway type, its subtenants have access only to the MSP-owned gateways retrieved from the Director node. For information about discovering appliances, see [Discover VOS Devices for a Published Tenant](#).

You can configure an MSP tenant only for SASE tenants, not for SD-WAN tenants. However, for tenants that use both SASE and SD-WAN services, you can configure an MSP tenant as part of the SASE service configuration. For information about configuring the SD-WAN service on a tenant, see [Configure a Secure SD-WAN Tenant](#).

You can configure multiple VPNs per SASE tenant. Also, within each VPN on a given SASE gateway, you can now configure more than one IP address pool. The multiple VPNs are isolated from other available VPNs on the tenant (unless you explicitly configure them to connect to the other VPNs). As a result, you can configure overlapping IP addresses in the VPNs.

**Note:** Only enterprise users who have the permission to onboard tenants can create or manage their subtenants.

You can configure logging services for SASE tenants that subscribe to the Versa SASE fabric service. You can configure the following types of logs:

- CGNAT logs
- DNS logs
- Web logs (HTTP/HTTPS)

---

## Create a SASE Tenant

1. Go to the Tenants dashboard screen.

VERSA

TENANTS



















































EnglishadminService Provider Administrator

Tenants

Tenants 2

+ Tenant

Search...

NAME	STATUS	LOGO	GLOBAL ID	SERVICE	PUBLISH STATUS	PROGRESS	
VERSA	Enabled		1	SD-WAN	Published		  
ACME	Enabled		16	SASE	Published		  
							  
							  
							  
							  
							  
							  
							  
							  
							  
							  
							  
							  
							  
							  

2. Click +Tenant. In the Create screen, in Step 1, General, enter information for the following fields.

## Create Tenant



## Tenant Name

☒ Enabled

## Description

## Global Tenant ID

## Parent Tenant

Managed Service Provider (MSP) ☒ Enabled

## Gateway Type

## Select Services

☐ Secure SD-WAN ☒ Security Service Edge (SSE) ☐ SASE for SIM

## Directors

## Host

☒ Is Default

## Controllers

## ZTP Type

☒ Serial Number ☐ URL

## SDWAN Solution Tiers

## Non-SDWAN Solution Tiers



## Appliance Preferred Version


Cancel

Back

Skip to Review

Next

Field	Description
Tenant Name	Enter a name for the tenant.
Enabled	<p>Click the slider to enable the new tenant after you create it.</p> 
Global Tenant ID	The tenant is assigned a global ID automatically. However, you can enter a different global tenant ID.
Parent Tenant	Select a parent tenant.
Managed Service Provider (MSP) (Group of Fields)	<p>Click the slider to enable MSP mode for the tenant. In this mode, the SSE service is selected automatically, and you cannot deselect it. Note that if a tenant has already been deployed as a non-MSP tenant, you cannot change the tenant to an MSP tenant and then redeploy it. Also note that you can also select the Secure SD-WAN service for the MSP tenant. For more information , see Configure a Secure SD-WAN Tenant.</p> 
<ul style="list-style-type: none"> <li>Gateway Type</li> </ul>	<p>If you enable MSP mode, select the gateway type:</p> <ul style="list-style-type: none"> <li>Dedicated—Create an MSP tenant that owns its gateways.</li> <li>Shared—Create an MSP tenant that does not own any of the gateways. Note that you can change the gateway type to Dedicated later. This is the default.</li> </ul>

Field	Description
<ul style="list-style-type: none"> <li>Select Services</li> </ul>	<ul style="list-style-type: none"> <li>Select SASE as a Service (Security Service Edge). If you enabled MSP mode, SSE is automatically selected, and you cannot deselect it.</li> <li>(For Releases 12.1.1 and later) SASE for SIM—Click to enable SASE for SIM for the client. This option is enabled only if you select Security Service Edge (SSE). For more information, see <a href="#">Configure SASE for SIM</a>.</li> </ul>
Directors	<p>Select one or more Director nodes to associate with tenant. Then click the slider to designate a Director as the default Director. The default Director node authenticates all Administrator users, whether the users are local or internal to the Director node.</p> 
Controllers	Select one or more Controller nodes to associate with the tenant.
ZTP Type	<p>Select the type of ZTP to use:</p> <ul style="list-style-type: none"> <li>Serial Number</li> <li>URL—For on-premises SD-WAN devices</li> </ul>
Solution Tiers	Select one or more licensing solution tiers.
Appliance Preferred Version	Select the VOS software version for the tenant to use.

3. Click Next. In Step 2, Security Service Edge, configure the usage type. Enter information for the following fields.

Configure > Tenant

Create Tenant

General

2 Security Service Edge

3 Roles  
(Tenant Active Roles)

4 Review & Submit

Define usage, tenant product and region configuration.

1 Select Usage Type

Enterprise Names

Tenant16

Press Enter to add

Pre-logout Enabled

Select Usage Type

Based on the Number of Users

Based on Bandwidth

Total Bandwidth

1 Gbps

Maximum Site to Site Tunnels

VSA Client Encryption Algorithms

IPsec Transform

Select

IPsec Group

Select

Next

2 Select Tenant Product

3 Select Region

Cancel

Back

Skip to Review

Next

Field	Description
Select Usage Type (Group of Fields)	
<ul style="list-style-type: none"> <li>Pre-logout Enabled</li> </ul>	Click the slider to enable pre-logout for a Versa SASE client. The pre-logout connection method allows a client device to establish a VPN connection to an organization's network. Pre-logout authenticates a user on the client device and then establishes a secure connection to the organization's network.
<ul style="list-style-type: none"> <li>VSA Client Encryption Algorithms (Group of Fields)</li> </ul>	
<ul style="list-style-type: none"> <li>IPsec Transform</li> </ul>	Select an IPsec transform encryption algorithm from the list. The options are: <ul style="list-style-type: none"> <li>esp-aes128-md5</li> <li>esp-aes256-md5</li> <li>esp-nnull-md5</li> </ul>

Field	Description
<ul style="list-style-type: none"> <li>◦ IPsec Group</li> </ul>	<p>Select an IPsec group encryption algorithm from the list. The options are:</p> <ul style="list-style-type: none"> <li>◦ Diffie-Hellman Group 14—2048-bit modulus</li> <li>◦ Diffie-Hellman Group 15—3072-bit modulus</li> <li>◦ Diffie-Hellman Group 16—4096-bit modulus</li> <li>◦ Diffie-Hellman Group 21—521-bit elliptic curve</li> <li>◦ Diffie-Hellman Group 25—192-bit elliptic curve</li> </ul>
<ul style="list-style-type: none"> <li>◦ Based on Bandwidth</li> </ul>	Click to configure the subscription usage type based on the amount of bandwidth used. This is the default.
<ul style="list-style-type: none"> <li>◦ Based on the Number of Users</li> </ul>	Click to configure the subscription usage type based on the number of users.
Total Bandwidth	<p>If you select the usage type based on bandwidth, select the total amount of subscribed bandwidth to allocate to the tenant.</p> <p><i>Range:</i> 250 Mbps through 10 Gbps</p> <p><i>Default:</i> None</p>
Maximum Site-to-Site Tunnels	<p>Enter the maximum number of site-to-site tunnels allowed across all gateways.</p> <p><i>Range:</i> 0 through 5000</p> <p><i>Default:</i> None</p>

- Click Next. In the Select Tenant Product group of fields, select the Versa Secure Access Fabric product bundles for the tenant. The Versa Secure Access Fabric product bundles combine the Versa Networks SSE and network-as-a-service solution to provide a secure network-as-a-solution service. Note that the available bundles are different depending on whether you configure the tenant based on the number of users or based on the allocated bandwidth.
- If, in Step 3, you configure the tenant based on the number of users, the following screen displays. Select one or both bundles. If you configured the tenant based on bandwidth, continue with Step 6.



✓ GENERAL
2 SECURITY SERVICE EDGE
✓ ROLES  
(TENANT ACTIVE ROLES)
1 REVIEW & SUBMIT

Define usage, tenant product and region configuration.

✓ SELECT USAGE TYPE
+

2 SELECT TENANT PRODUCT
-

**Select product for this tenant**

☐ **Versa Secure Internet Access (VSIA)**  
VSIA is a cloud-managed, cloud-delivered solution which helps secure Enterprise sites, home offices, and traveling users accessing distributed applications without compromising both security and user experience.

Essential ▾

Internet Protection Rules Maximum

☒ Direct Internet Access from Gateways

☐ **Versa Secure Private Access (VSPA)**  
VSPA is a cloud managed, cloud-delivered solution which helps secure Enterprise sites, home offices, and traveling users accessing distributed applications without compromising security using the latest Zero Trust Network Access framework.

Essential ▾

Private App Protection Rules Maximum

**Select logging for this tenant**

Web Logs

Select type ▾

Domain Name System (DNS) Logs

Select type ▾

Carrier-grade NAT (CGNAT) Logs

Select type ▾

Back
Next

a. For the Versa Secure Internet Access (VSIA) bundle, enter information for the following fields.

☒ **Versa Secure Internet Access (VSIA)**  
VSIA is a cloud-managed, cloud-delivered solution which helps secure Enterprise sites, home offices, and traveling users accessing distributed applications without compromising both security and user experience.



Essential ▾

Internet Protection Rules Maximum

☒ Direct Internet Access from Gateways

**VSIA Subscription Information**

<p>Number of VSIA Users</p> <input style="width: 100%;" type="text"/>	<p>License Start Date</p> <div style="display: flex; align-items: center;"> <input style="width: 100%;" type="text" value="mm / dd / yyyy"/> <div style="border: 2px solid red; width: 15px; height: 15px; margin-left: 5px;"></div> </div>	<p>License End Date</p> <div style="display: flex; align-items: center;"> <input style="width: 100%;" type="text" value="mm / dd / yyyy"/> <div style="border: 2px solid red; width: 15px; height: 15px; margin-left: 5px;"></div> </div>
---	---	---

Field	Description
Versa Secure Internet Access (VSIA)	Click to select the VSIA bundle, and then select a specific VSIA product bundle: <ul style="list-style-type: none"> <li>▪ Elite</li> <li>▪ Essential</li> <li>▪ Professional</li> </ul>
Optional Add-ons for VSIA Professional bundle	If you choose the VSIA Professional bundle, you can select one or more of the following: <ul style="list-style-type: none"> <li>▪ API-Based Data Protection</li> <li>▪ Data Loss Prevention</li> <li>▪ Advanced Threat Protection</li> </ul>
Internet Protection Rules Maximum	Enter the maximum number of internet protection rules that can be configured on the tenant.
Direct Internet Access from Gateways	Click the slider to enable direct internet access (DIA) from the tenant gateways.
VSIA Subscription Information (Group of Fields)	
▪ Number of VSIA Users	Enter the total number of VSIA users for the tenant.
▪ License Start Date	Enter the start date of the VSIA license. To choose the date from the calendar, click the  Calendar icon.
▪ License End Date	Enter the end date of the VSIA license. To choose the date from the calendar, click the  Calendar icon.

- b. For the Versa Secure Private Access (VSPA) bundle, enter information for the following fields.

☒ **Versa Secure Private Access (VSPA)** Essential

VSPA is a cloud managed, cloud delivered, private access service connecting distributed users with distributed applications without compromising security using the latest Zero Trust Network Access framework.

Private App Protection Rules Maximum

VSPA Subscription Information



Number of VSPA Users <input type="text"/>	License Start Date <input type="text" value="mm / dd / yyyy"/>	License End Date <input type="text" value="mm / dd / yyyy"/>
--	---	---

Field	Description
Versa Secure Private Access (VSPA)	Click to choose the VSPA bundle, and then select a specific VSPA product bundle: <ul style="list-style-type: none"> <li>▪ Essential</li> <li>▪ Professional</li> </ul>
Private Application Protection Rules Maximum	Enter the maximum number of private application protection rules that can be configured for the tenant.
VSPA Subscription Information (Group of Fields)	
▪ Number of VSPA Users	Enter the total number of VSPA users for the tenant.
▪ License Start Date	Enter the start date of the VSPA license. To choose the date from the calendar, click the  Calendar icon.
▪ License End Date	Enter the end date of the VSPA license. To choose the date from the calendar, click the  Calendar icon.

- c. If you select both the VSIA and VSPA product bundles, enter information for the following additional information.

VSIA & VSPA Bundle Subscription Information

Number of VSIA and VSPA Users <input type="text"/>	License Start Date <input type="text" value="mm / dd / yyyy"/>	License End Date <input type="text" value="mm / dd / yyyy"/>
---	---	---

Field	Description
Number of VSIA and VSPA Users	Enter the total number of the tenant's VSIA and VSPA users.
License Start Date	Enter the start date of the VLIA and VSPA licenses. To choose the date from the calendar, click the  Calendar icon.
License End Date	Enter the end date of the VSIA and VSPA licenses. To choose the date from the calendar, click the  Calendar icon.

6. If, in Step 3, you configure the tenant based on bandwidth, the following screen displays. Enter information for the following fields.

Configure > Tenant  
Create

GENERAL SECURITY SERVICE EDGE ROLES (TENANT ACTIVE ROLES) REVIEW & SUBMIT

Define usage, tenant product and region configuration.

SELECT USAGE TYPE +

2 SELECT TENANT PRODUCT -

Select product for this tenant

☒ **Versa Secure Access Fabric - Essential Bundle**  
Versa Secure Access Fabric combines Versa's SSE offerings with Network as a Service solution to offer a Secure Network as a Service solution. Bundle options:  
✓ Versa Secure Internet Access (VSIA) Essential ✓ Versa Secure Private Access (VSPA) Essential ✓ Premier Secure SD-WAN

☐ **Versa Secure Access Fabric - Essential Plus Bundle**  
Versa Secure Access Fabric combines Versa's SSE offerings with Network as a Service solution to offer a Secure Network as a Service solution. Bundle options:  
✓ Versa Secure Internet Access (VSIA) Essential ✓ Versa Secure Private Access (VSPA) Professional ✓ Premier Secure SD-WAN

☐ **Versa Secure Access Fabric - Professional Bundle**  
Versa Secure Access Fabric combines Versa's SSE offerings with Network as a Service solution to offer a Secure Network as a Service solution. Bundle options:  
✓ Versa Secure Internet Access (VSIA) Professional ✓ Versa Secure Private Access (VSPA) Professional ✓ Premier Secure SD-WAN

☐ **Versa Secure Access Fabric - Elite Bundle**  
Versa Secure Access Fabric combines Versa's SSE offerings with Network as a Service solution to offer a Secure Network as a Service solution. Bundle options:  
✓ Versa Secure Internet Access (VSIA) Elite ✓ Versa Secure Private Access (VSPA) Professional ✓ Premier Secure SD-WAN

Internet Protection Rules Maximum: 500 Private App Protection Rules Maximum: 50

☒ Direct Internet Access from Gateways

Select logging for this tenant

Web Logs

Select type

Domain Name System (DNS) Logs

Select type

Carrier-grade NAT (CGNAT) Logs

Select type

Next

1

SELECT REGION

+

Cancel

Back

Skip to Review

Next

Field	Description
Select Product for This Tenant (Group of Fields)	Select the product bundle for the tenant.
<ul style="list-style-type: none"> <li>Versa Secure Access Fabric—Essential Bundle</li> </ul>	<p>This bundle includes:</p> <ul style="list-style-type: none"> <li>Versa Secure Internet Access (VSIA) Essential</li> <li>Versa Secure Private Access (VSPA) Essential</li> <li>Premier Secure SD-WAN</li> </ul>
<ul style="list-style-type: none"> <li>Versa Secure Access Fabric—Essential Plus Bundle</li> </ul>	<p>This bundle includes:</p> <ul style="list-style-type: none"> <li>Versa Secure Internet Access (VSIA) Essential</li> <li>Versa Secure Private Access (VSPA) Professional</li> <li>Premier Secure SD-WAN</li> </ul>
<ul style="list-style-type: none"> <li>Versa Secure Access Fabric—Professional Bundle</li> </ul>	<p>This bundle includes:</p> <ul style="list-style-type: none"> <li>Versa Secure Internet Access (VSIA) Professional</li> <li>Versa Secure Private Access (VSPA) Professional</li> <li>Premier Secure SD-WAN</li> </ul> <p>You can also choose one or more of the following options:</p> <ul style="list-style-type: none"> <li>Advanced Threat Protection (Cloud Malware Sandbox with Antivirus and Artificial Intelligence/ Machine Learning (AI/ML). (For Releases 12.1.1 and later) If you select this option, Advance Security Cloud displays as Step 3.</li> <li>API-Based Data Protection</li> <li>Data Loss Prevention</li> </ul> <div> <p><input checked="" type="radio"/> Versa Secure Access Fabric - Professional Bundle</p> <p><small>Versa Secure Access Fabric combines Versa's SSE offerings with Network as a Service solution to offer a Secure Network as a Service solution. Bundle options:</small></p> <p> <input checked="" type="checkbox"/> Versa Secure Internet Access (VSIA) Professional         <input checked="" type="checkbox"/> Versa Secure Private Access (VSPA) Professional         <input checked="" type="checkbox"/> Premier Secure SD-WAN       </p> <p>Optional add-ons for professional bundle only: <input type="checkbox"/> API Based Data Protection <input type="checkbox"/> Data Loss Prevention <input type="checkbox"/> Advanced Threat Protection (Cloud Malware Sandbox with A/V</p> </div>
<ul style="list-style-type: none"> <li>Versa Secure Access Fabric—Elite Bundle</li> </ul>	<p>This bundle includes:</p> <ul style="list-style-type: none"> <li>Versa Secure Internet Access (VSIA) Elite</li> </ul>

	<ul style="list-style-type: none"> <li>◦ Versa Secure Private Access (VSPA) Professional</li> <li>◦ Premier Secure SD-WAN</li> </ul> <p>(For Releases 12.1.1 and later) If you select this option, Advance Security Cloud displays as Step 3.</p>
Internet Protection Rules Maximum	<p>Enter the maximum number of internet protection rules allowed.</p> <p><i>Default:</i> 500</p> <p><i>Range:</i> 1 through 999999</p>
Private Application Protection Rules Maximum	<p>Enter the maximum number of private application protection rules allowed.</p> <p><i>Default:</i> 50</p> <p><i>Range:</i> 1 through 999999</p>
Direct Internet Access from Gateways	<p>Click to disable direct internet access (DIA) from gateways. When this option is enabled, the SASE gateway sends all internet-bound traffic using the default route configured on it. In typical deployments, the default route sends traffic towards the enterprise data center over a site-to-site IPsec tunnel. By default, the Versa Secure Internal Access (VSIA) feature, which is included in both bundles, enables DIA for all internet-bound traffic coming from a tenant.</p>
Select Logging for this tenant.	<p>Configure the logging to use for the tenant.</p>
<ul style="list-style-type: none"> <li>◦ Web Logs</li> </ul>	<p>Click to select web logs.</p> <p>Click the down-arrow and then select the type of logging service to enable:</p> <ul style="list-style-type: none"> <li>◦ Advanced Logging Service—ALS is a cloud-based service that processes and stores log files. To use ALS, the provider organization configures a LEF profile on the SASE gateway.</li> <li>◦ Analytics—Send logs to the Versa Analytics cluster for processing.</li> <li>◦ Archive—Send logs to the ALS service for archiving only; the logs are not processed.</li> </ul>

	<p>However, you can process the logs offline. To use the archive option, the provider organization configures a LEF profile on the SASE profile. This profile must be different from the LEF profile used for the ALS option.</p>
<ul style="list-style-type: none"> <li>Domain Name System (DNS) Logs</li> </ul>	<p>Click to select DNS logs.</p> <p>Click the down-arrow and then select the type of logging service to enable:</p> <ul style="list-style-type: none"> <li>Advanced Logging Service—ALS is a cloud-based service that processes and stores log files. To use ALS, the provider organization configures a LEF profile on the SASE gateway.</li> <li>Analytics—Send logs to the Versa Analytics cluster for processing.</li> <li>Archive—Send logs to the ALS service for archiving only; the logs are not processed. However, you can process the logs offline. To use the archive option, the provider organization configures a LEF profile on the SASE profile. This profile must be different from the LEF profile used for the ALS option.</li> </ul>
<ul style="list-style-type: none"> <li>Carrier-Grade NAT (CGNAT) Logs</li> </ul>	<p>Click to select CGNAT logs.</p> <p>Click the down-arrow and then select the type of logging service to enable:</p> <ul style="list-style-type: none"> <li>Advanced Logging Service—ALS is a cloud-based service that processes and stores log files. To use ALS, the provider organization configures a LEF profile on the SASE gateway.</li> <li>Analytics—Send logs to the Versa Analytics cluster for processing.</li> <li>Archive—Send logs to the ALS service for archiving only; the logs are not processed. However, you can process the logs offline. To use the archive option, the provider organization configures a LEF profile on the SASE profile. This profile must be different from the LEF profile used for the ALS option.</li> </ul>

7. (For Releases 12.1.1 and later.) If, in Step 6, you select Versa Secure Access Fabric—Elite Bundle or Versa Secure Access Fabric—Professional Bundle as the tenant product and then select Advanced Threat Protection, the Step 3 Advance Security Cloud screen displays. In this screen, you enter the RBI and ATP/DLP cloud instance



information for the regions of the tenant that you select in Step 2, Security Service Edge. ATP and RBI cloud instance information is shared with the Versa Cloud Gateway (VCG) so that the VCG can connect to the cloud service to initiate sandboxing or RBI. Enter information for the following fields.

1

General

2

Security Service Edge

3

Advance Security Cloud

4

Roles  
(Tenant Active Roles)

5

Review & Submit

Configure each of the regions Remote Browser Isolation (RBI) & Advanced Threat Protection (ATP) / Data Loss Prevention (DLP)

Below are the regions you have selected in the previous step. Enter the information for Remote Browser Isolation (RBI) and Advanced Threat Protection (ATP) / Data Loss Prevention (DLP) below.

Regions	Gateways	ATP/DLP Instance	ATP/DLP Authentication Token	ATP/DLP Token Expiry Time [secs]	RBI Instance	RBI Authentication Token
USA-East	1					
USA-West	1					

Cancel

Back

Skip to Review

Next

Field	Description
Regions	Displays the name of the region you selected in the Security Service Edge screen.
Gateways	Displays the number of gateways associates with a region.
ATP/DLP Instance	Select the ATP or DLP cloud instance for the tenant to connect to VCG. For more information, see <a href="#">Configure Advanced Threat Protection</a> and <a href="#">Configure Data Loss Prevention in Concerto</a> .
ATP/DLP Authentication Token	Enter the authentication token for the tenant to use to refresh the access tokens when making API requests to the cloud or private sandbox service.
ATP/DLP Token Expiry Time	Enter how often to refresh access tokens when making API requests to the cloud or private sandbox service, in seconds
RBI Instance	Select the RBI cloud instance for the tenant to connect to VCG.
RBI Authentication Token	Enter the authentication token for the tenant to use to refresh the access tokens when making API requests to the cloud for RBI service.

- Click Next to go to Step 3, Select Region. This screen displays the available regions and how many gateways are currently being used in each region.

**3 SELECT REGION**

**Available Regions**  
Select the regions to assign to this tenant. Once selected, click region's View Details to assign gateways.

Search...

**USA-East**  
Gateways Used  
**0**  
[View Details](#)

**USA-West**  
Gateways Used  
**0**  
[View Details](#)

Select a region to view it's details and settings.

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

- To display information about the gateways in the region and to assign new gateways to the region, click View Details.

**Region Details: USA-East**

Search to select Gateways

Select the gateways

[+ Create Gateway Group](#) [Delete Gateway](#)

- Click in the search box to view the gateways in the region, click the checkbox next to a gateway name, and then click the Add button to add it to the region.

**Region Details: USA-East**

Search to select Gateways

Select the gateways

[+ Create Gateway Group](#) [Delete Gateway](#)

☒ USA-East-GW-1

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

The gateway is added to the region. For example:

Region Details: **USA-East**

+ Create Gateway Group 🗑️ Delete Gateway

☐ Gateway USA-East-GW-1

Allocated Bandwidth (Mbps)

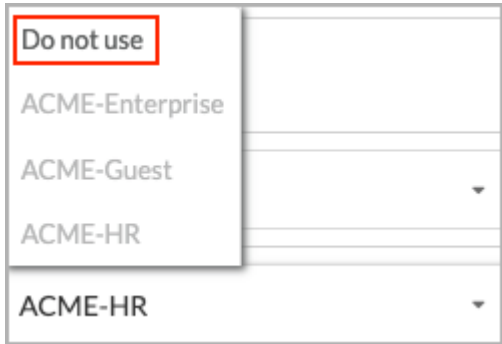
PORTAL	GATEWAY GROUP	VPN	CLIENT ADDRESS POOL NAME	CLIENT ADDRESS POOL
<input checked="" type="checkbox"/>	USA-East	tenant1111-Enterprise	<input type="text"/>	<input type="text"/> +

11. To display information about the gateway, including the gateway group, VPN, and client address pool name and IP address, click the down arrow next to the gateway name. For each VPN, you can configure one or more client address pool. For a gateway, you can add multiple client address pools for each VPN. To define which users are assigned to the pools, you use a secure access policy, and you can then apply access restrictions to a pool of users using the same VPN.
12. To configure gateway information, enter information for the following fields. Note that in a single VPN on a gateway, the client pool address name and client pool addresses must be unique. However, if a gateway has multiple VPNs, you can use the same address pool name and address pool range for more than one VPN, because the VPNs do not share information. The IP addresses for each pool in a VPN must not overlap both for the selected gateway and across all gateways.


☐ Gateway USA-East-GW-1

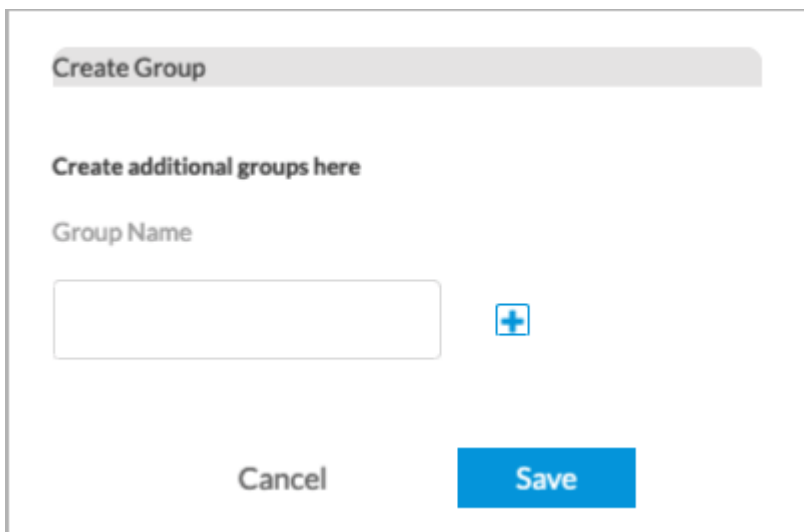
Allocated Bandwidth (Mbps)

PORTAL	GATEWAY GROUP	VPN	CLIENT ADDRESS POOL NAME	CLIENT ADDRESS POOL
<input checked="" type="checkbox"/>	USA-East	tenant1111-Enterprise	Pool1	10.1.3.0/24
			Pool2	10.1.4.0/24

Field	Description
Allocated Bandwidth	<p>Enter the maximum amount of bandwidth that a tenant can use on the gateway.</p> <p><i>Range:</i> 0 through 999999 Mbps</p> <p><i>Default:</i> None</p>
Portal	Click the slider to enable the secure access portal service on the gateway.
Gateway Group	Select a gateway group to which to assign the gateway.
VPN	<p>Select one or more VPNs to assign them to the gateway. The VPN select column shows all VPNs that are available for the tenant. Note that if you configure no VPNs on a tenant, the SASE service uses a default VPN with the name <i>tenant-name</i>-Enterprise. Also note that because guest VPNs should not be extended to SASE gateways, they are not displayed in the VPN selection column.</p> <p>If multiple tenants are available on a tenant and you do not want to provision one of them on a gateway, select Do Not Use.</p>  <p>To assign an unused VPN to a gateway later, select it to assign to the gateway.</p>

Client Address Pool Name	Enter a name for the client address pool. If you configure more than one address pool for the same VPN, the pools must have unique names. However, if multiple VPNs are available for the same gateway, you can use the same client address pool name in each VPN.
Client Address Pool	Enter a valid IP address range to use for the client address pool. The minimum address pool size is a /24 subnet. If you configure more than one address pool for the same VPN, the pools must have unique IP address ranges. However, if multiple VPNs are available for the same gateway, you can use the same client IP address range in each VPN.

13. To create a group of gateways that you can then assign to a region, click **Create Gateway Group** . You can then assign one or more VPNs to the gateway group, as described above. To create a gateway group:
  - a. Enter a name for the group.
  - b. Click the  Add icon to add gateway groups.
  - c. Click **Save** to create the gateway groups.



14. Click **Next** to display the Step 3, Roles screen.

GENERAL SECURITY SERVICE EDGE **ROLES (TENANT ACTIVE ROLES)** REVIEW & SUBMIT

Select user roles applicable to the tenant. By default, all predefined roles have been selected.

<input type="checkbox"/>	ROLES
<input checked="" type="checkbox"/>	Enterprise Operator
<input checked="" type="checkbox"/>	Service Provider Operator
<input type="checkbox"/>	spo
<input type="checkbox"/>	Test
<input type="checkbox"/>	TestSPO
<input type="checkbox"/>	external SPO
<input type="checkbox"/>	Sadmin1
<input checked="" type="checkbox"/>	Enterprise Administrator
<input checked="" type="checkbox"/>	Service Provider Administrator

Cancel Back Skip to Review **Next**

15. Click the checkbox next to Roles to assign all roles to the tenant, or select individual roles to assign to the tenant.
16. Click Next. In Step 4, Review & Submit, review the information you configured.

GENERAL SECURITY SERVICE EDGE ROLES (TENANT ACTIVE ROLES) **REVIEW & SUBMIT**

Review and submit your tenant

Below are the configurations of your tenant. Review and edit any step of your configuration before submitting.

**General** [Edit](#)

Tenant Name: newTenant  
Global Tenant ID: 78  
Enabled: Yes  
Parent Tenant: VERSA  
Services: SSE  
ZTP Type: Serial Number  
Appliance Preferred Version

**Directors**

Host: Director-102  
Is Default: Yes  
Controllers: 1

**CONTROLLERS | 1**

- SASE-Controller-1


**SOLUTION TIERS | 5**

- Work-From-Home
- Premier-Secure-SDWAN
- Prime-Secure-SDWAN
- Prime-SDWAN

**Security Service Edge** [Edit](#)

Disable Direct Internet Access from Gateways: No

Cancel Back Save Publish

17. To change any of the information, click the  Edit icon in the section, and then make the changes.
18. Click Publish to create the tenant on the selected gateways. Click Save to save the configuration so that you can publish it later.

---

## Supported Software Information

Releases 11.1.1 and later support all content described in this article, except:

- Release 11.4.1 adds support for the Versa Secure Access Fabric Elite product bundle.
- Release 12.1.1 adds support to enable pre-login for Versa SASE clients and to add RBI and ATP/DLP cloud instance details for tenant regions.

---

## Additional Information

[Configure a Secure SD-WAN Tenant](#)

[Configure Advanced Threat Protection](#)

[Configure Data Loss Prevention in Concerto](#)

[Configure SASE Certificates](#)

[Configure SASE for SIM](#)

[Configure SASE Site-to-Site Tunnels](#)

[Configure SASE TLS Decryption](#)

[Configure SASE User-Defined Objects](#)