Configure a Secure SD-WAN Tenant

For supported software information, click here.

The Tenants screen displays all configured tenants for a service provider. This screen displays when you first log in to the Concerto orchestrator as a Service Provider Administrator.

For Releases 11.1.1 and later, you can create a tenant that runs one or both of the following service types:

- Secure SD-WAN
- Security Service Edge (SASE)

For Releases 12.1.1 and later, can assign a non-SD-WAN solution tier to a tenant. The non-SD-WAN solution tier consists of the following:

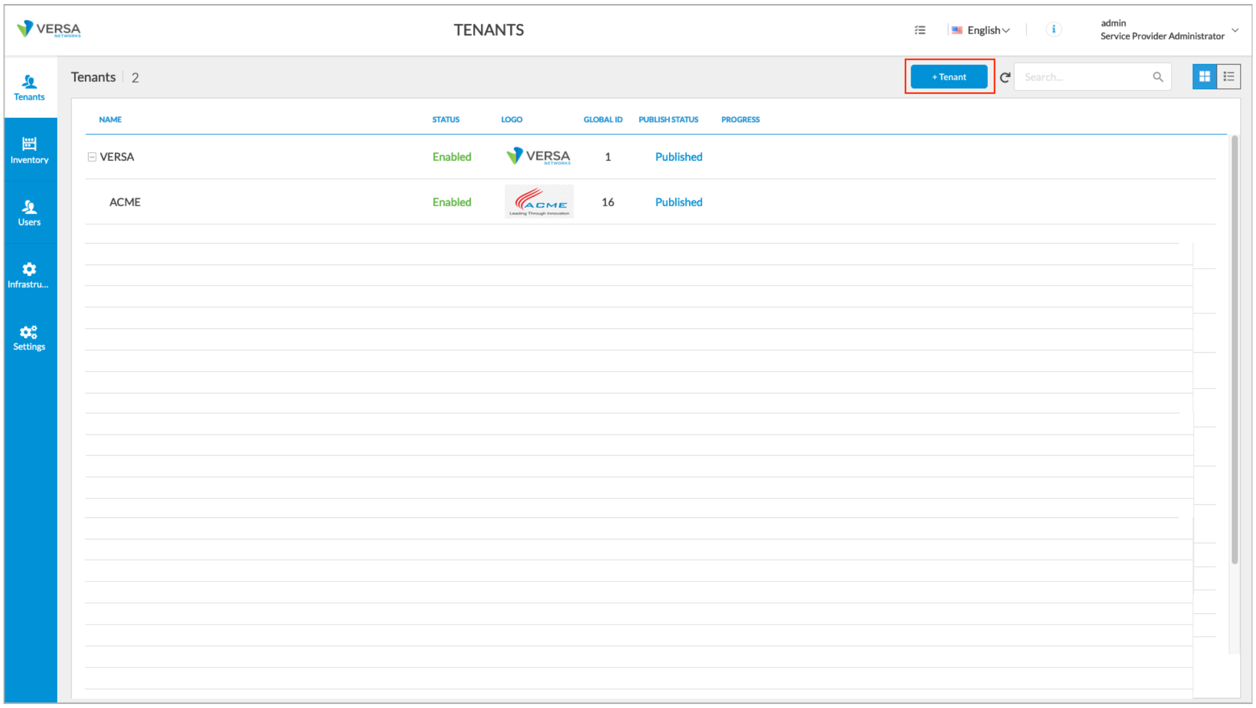
- Next-generation firewall (NGFW)
- ProNet
- Unified threat management (UTM)

You can choose options from the SD-WAN or the non-SD-WAN solution tier, but you cannot choose options from both tiers.

This article describes how to create a secure SD-WAN tenant. For information about creating a SASE tenant, see Create SASE Tenants.

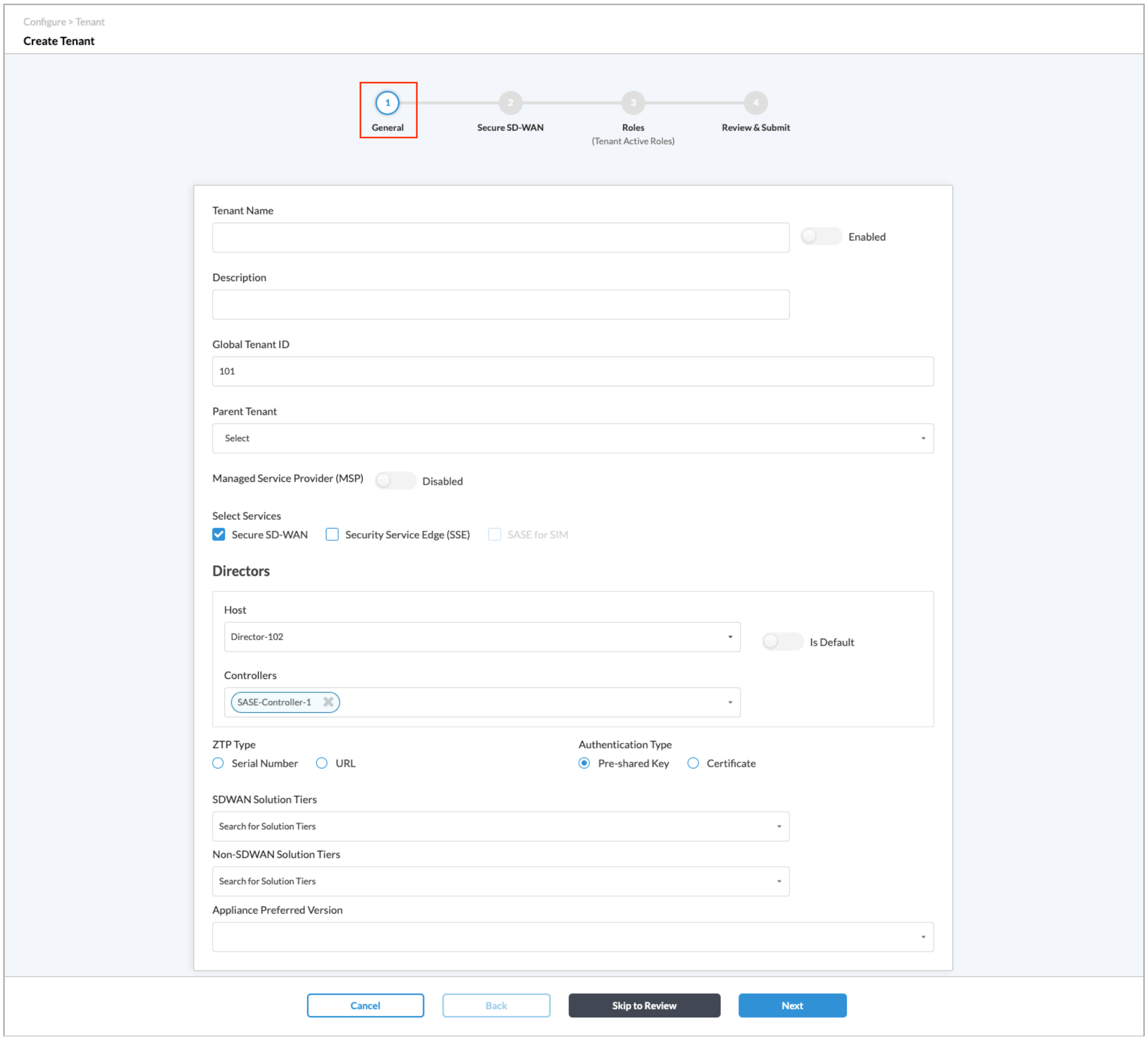
Create a Secure SD-WAN Tenant

1. Go to the Tenants home screen.



NAME	STATUS	LOGO	GLOBAL ID	PUBLISH STATUS	PROGRESS
VERSA	Enabled	VERSA	1	Published	
ACME	Enabled	ACME	16	Published	

2. On the Tenants screen, click + Tenant. The Create screen displays, and Step 1, General, is selected. Enter information for the following fields.



Configure > Tenant

Create Tenant

Tenant Name

Enabled

Description

Global Tenant ID: 101

Parent Tenant: Select

Managed Service Provider (MSP) Disabled

Select Services

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

Directors

Host: Director-102 Is Default

Controllers: SASE-Controller-1

ZTP Type: ○ Serial Number ○ URL

Authentication Type: ● Pre-shared Key ○ Certificate

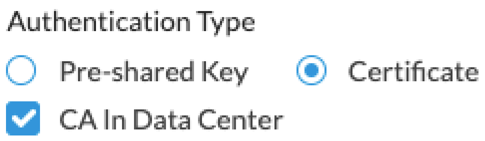
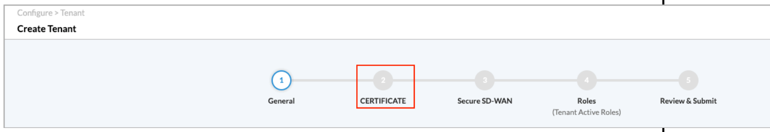
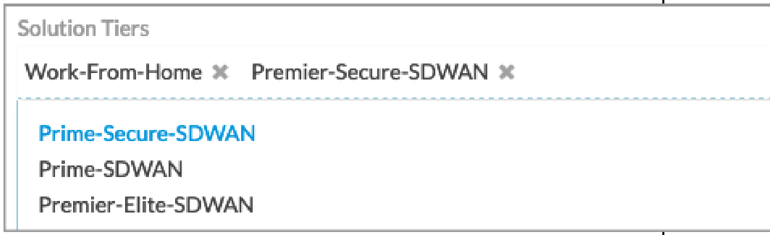
SDWAN Solution Tiers: Search for Solution Tiers

Non-SDWAN Solution Tiers: Search for Solution Tiers

Appliance Preferred Version

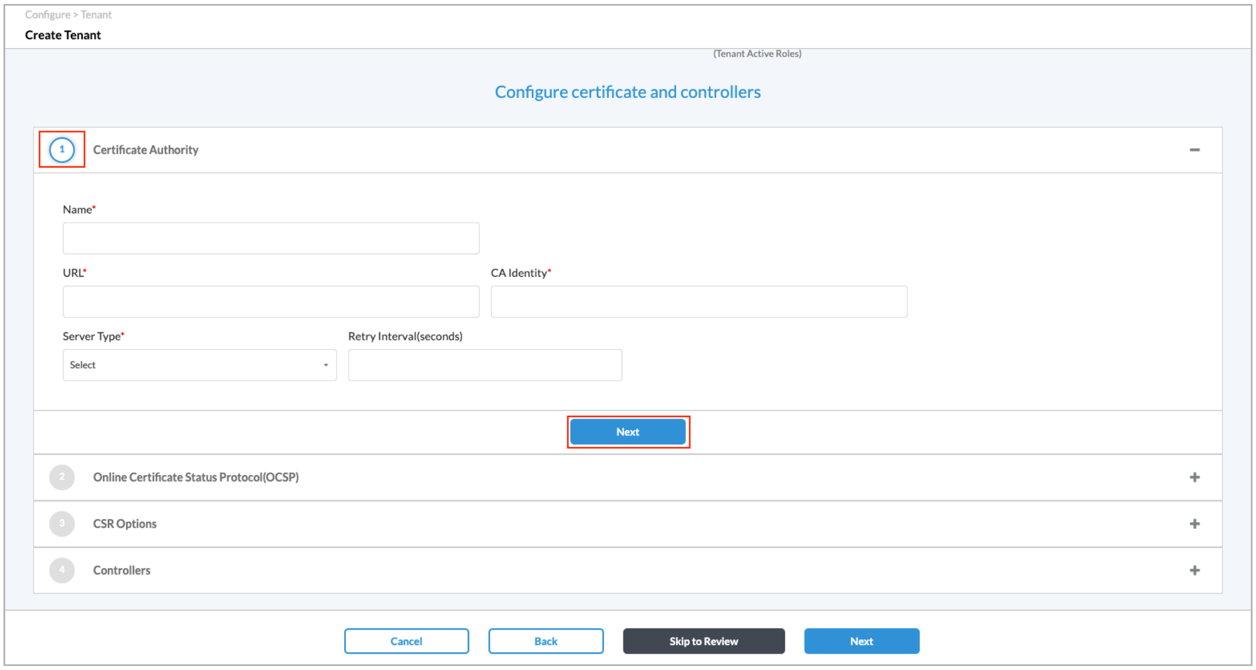
Field	Description
Tenant Name	Enter a name for the tenant.
Enabled	Click the slider bar to enable the tenant. Enabled Click the slider bar a second time to disable the

Field	Description
	tenant.
Global Tenant ID	The global tenant ID is assigned automatically.
Parent Tenant	Select the parent tenant.
Select Services	Select Secure-SD-WAN.
Directors (Group of Fields)	
◦ Host	Select a host Director node. For information about configuring Director nodes, see Create a Director Cluster.
◦ Is Default	Click to designate the host as the default Director node for the tenant. If you configure only one Director node, that node is the default. If you configure two or more Director nodes, click the Is Default slide bar to select the default Director node.
Controllers	Select one or more Controller nodes.
ZTP Type	Choose the type of ZTP to use to initialize the tenant: ◦ Serial Number ◦ URL

Field	Description
Authentication Type (for Releases 12.1.1 and later)	 Authentication Type ○ Pre-shared Key ● Certificate ☑ CA In Data Center
◦ Preshared Key	Use a preshared key for authentication. This is the default.
◦ Certificate	Use a public key infrastructure (PKI) certificate for authentication. If you select the PKI certificate authentication type, the Certificate step is added to the tenant configuration workflow.  Configure > Tenant Create Tenant 1 General — 2 CERTIFICATE — 3 Secure SD-WAN — 4 Roles (Tenant Active Roles) — 5 Review & Submit
◦ CA in Data Center	Select if the certificate authority (CA) is located behind a Controller node. Otherwise, the workflow assumes that the CA is accessible over the WAN interfaces.
SD-WAN Solution Tiers	Select an SD-WAN solution tier. Click the down arrow to display the available solution tiers, which are inherited from the parent tenant. Then, click the name of the tier to select it.  Solution Tiers Work-From-Home ✖ Premier-Secure-SDWAN ✖ Prime-Secure-SDWAN Prime-SDWAN Premier-Elite-SDWAN
Non-SD-WAN Solution Tiers	(For Releases 12.1.1 and later.) Select a non-SD-WAN solution tier. Click the down arrow to display the available solution tiers, which are inherited from the

Field	Description
	parent tenant. Then, click the name of the tier to select it. ◦ NGFW ◦ ProNet ◦ UTM
Appliance Preferred Version	Select the preferred Versa Operating System™ (VOS™) software version for the device.

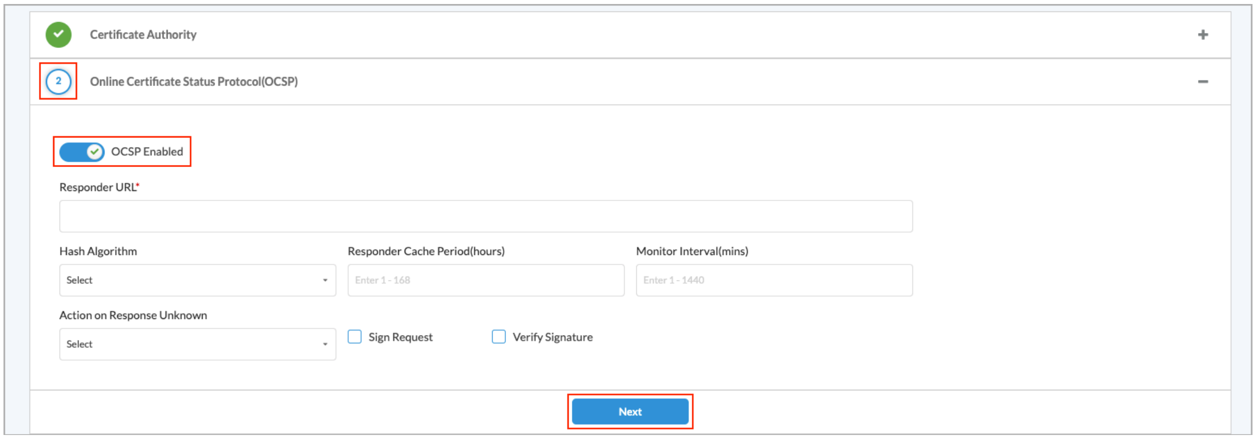
3. Click Next. For Releases 12.1.1 and later:
   - If you select the PKI Certificate authentication type for the tenant, the Step 2, Certificate screen displays. Enter information for the following fields.
   - If you select the Preshared Key authentication type for the tenant, the Certificate step does not display. Continue with Step 4.



Field	Description
Name (Required)	Enter a name for the CA.
URL (Required)	Enter the URL of the CA server enrollment service. This is the URL to which CA certificate and enrollment requests are sent.

Field	Description
CA Identity (Required)	Enter the name of the CA server: ◦ For the CMP server type, enter CN=*CA-name*. ◦ For the GCP server type, enter GCP-CA. ◦ For the SCEP server type, enter *CA-name*.
Server Type (Required)	Select a server type: ◦ ACME—Automatic Certificate Management Environment. ◦ CMP—Select if the CA server is using the Certificate Management Protocol for enrollment. ◦ SCEP—Select if the CA server is using the Simple Certificate Enrollment Protocol.
Retry Interval	Enter the time interval, in seconds, at which to attempt o retrieve the certificate.

a. Click Next to go to the Online Certificate Status Protocol (OCSP) section, and then enter information for the following fields.

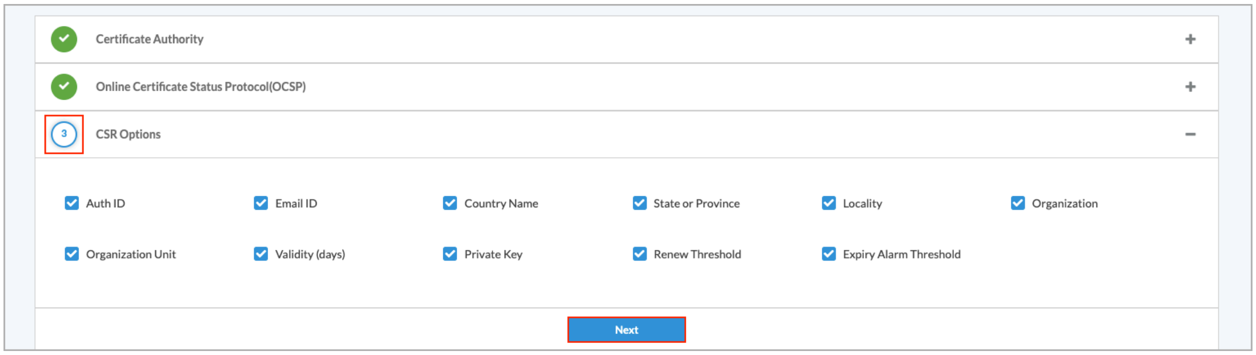


Field	Description
OCSP Enabled	Click the slider bar to enable OCSP.
Responder URL (Required)	Enter the URL of the OCSP responder that reports the status of a certificate.

Field	Description
Hash Algorithm	Select the hash algorithm to use when preparing the OCSP request.
Responder Cached Period	Enter how long, in hours, to cache OCSP responses. *Range*: 1 through 168 hours *Default*: None (no cache is created)
Monitor Interval	Enter the time interval at which to verify the validity of the certificate status. *Range*: 1 through 1440 minutes *Default*: None (monitoring is disabled)
Action on Response Unknown	Select the action to take on the IPsec tunnel when an unknown response is received from the OCSP responder: ▪ Tunnel Down—Bring down the IPsec tunnel. ▪ Tunnel Up—Bring up the IPsec tunnel.
Sign Request	Click to have the OCSP responder verify the signature before responding to certificate requests.
Verify Signature	Click to have the VOS device verify the signature of OCSP responder.

b. Click Next to go to the CSR Options section, and then select the certificate signing request (CSR) options to include in the certificate. These options define the attributes that the CA uses to authenticate the VOS device and configure the appropriate attributes in the certificate that is then sent back to the device. The CSR Options workflow configures these attributes on the device when it sends the CSR. Note that you configure he CSR options for each device; they are not associated with a master profile.

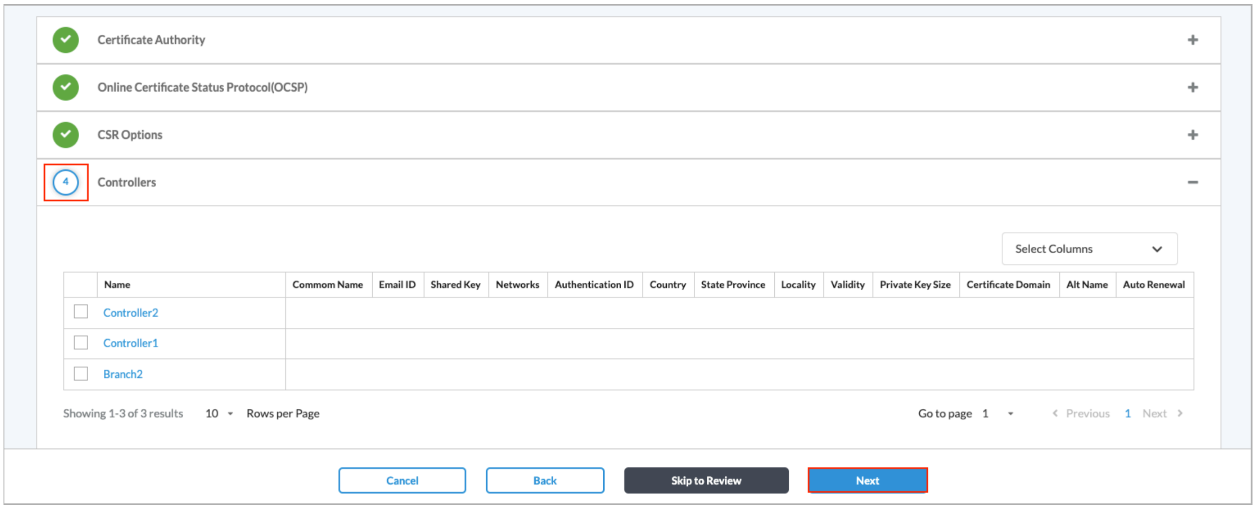
   After you select the CSR options, go to the Controllers section, and the enter information for each attribute.



☑ Auth ID ☑ Email ID ☑ Country Name ☑ State or Province ☑ Locality ☑ Organization

☑ Organization Unit ☑ Validity (days) ☑ Private Key ☑ Renew Threshold ☑ Expiry Alarm Threshold

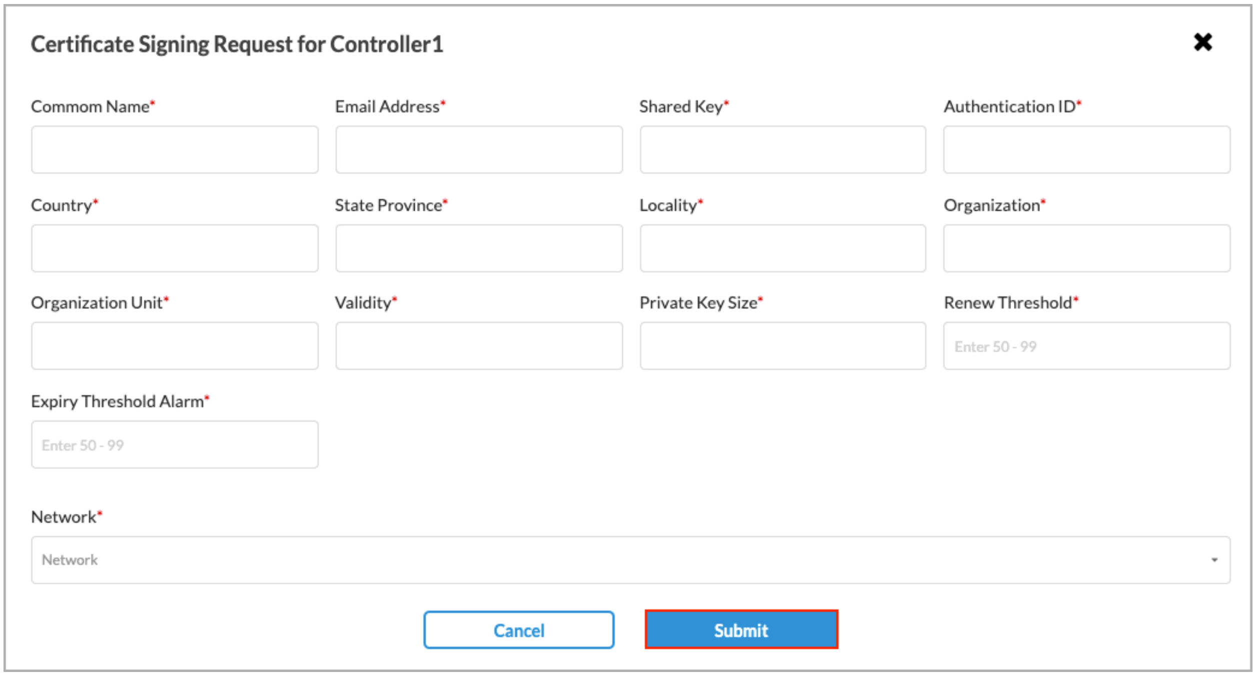
c. Click Next to go to the Controllers section.



	Name	Commom Name	Email ID	Shared Key	Networks	Authentication ID	Country	State Province	Locality	Validity	Private Key Size	Certificate Domain	Alt Name	Auto Renewal
□	Controller2													
□	Controller1													
□	Branch2													

Showing 1-3 of 3 results 10 Rows per Page

d. Click the name of a controller node. In the Certificate Signing Request for Controller screen, enter information for the following fields. Note that only the CSR options that you previously selected display in the Certificate Signing Request screen, and you must provide information for each field.



Certificate Signing Request for Controller1

Commom Name*

Email Address*

Shared Key*

Authentication ID*

Country*

State Province*

Locality*

Organization*

Organization Unit*

Validity*

Private Key Size*

Renew Threshold*

Enter 50 - 99

Expiry Threshold Alarm*

Enter 50 - 99

Network*

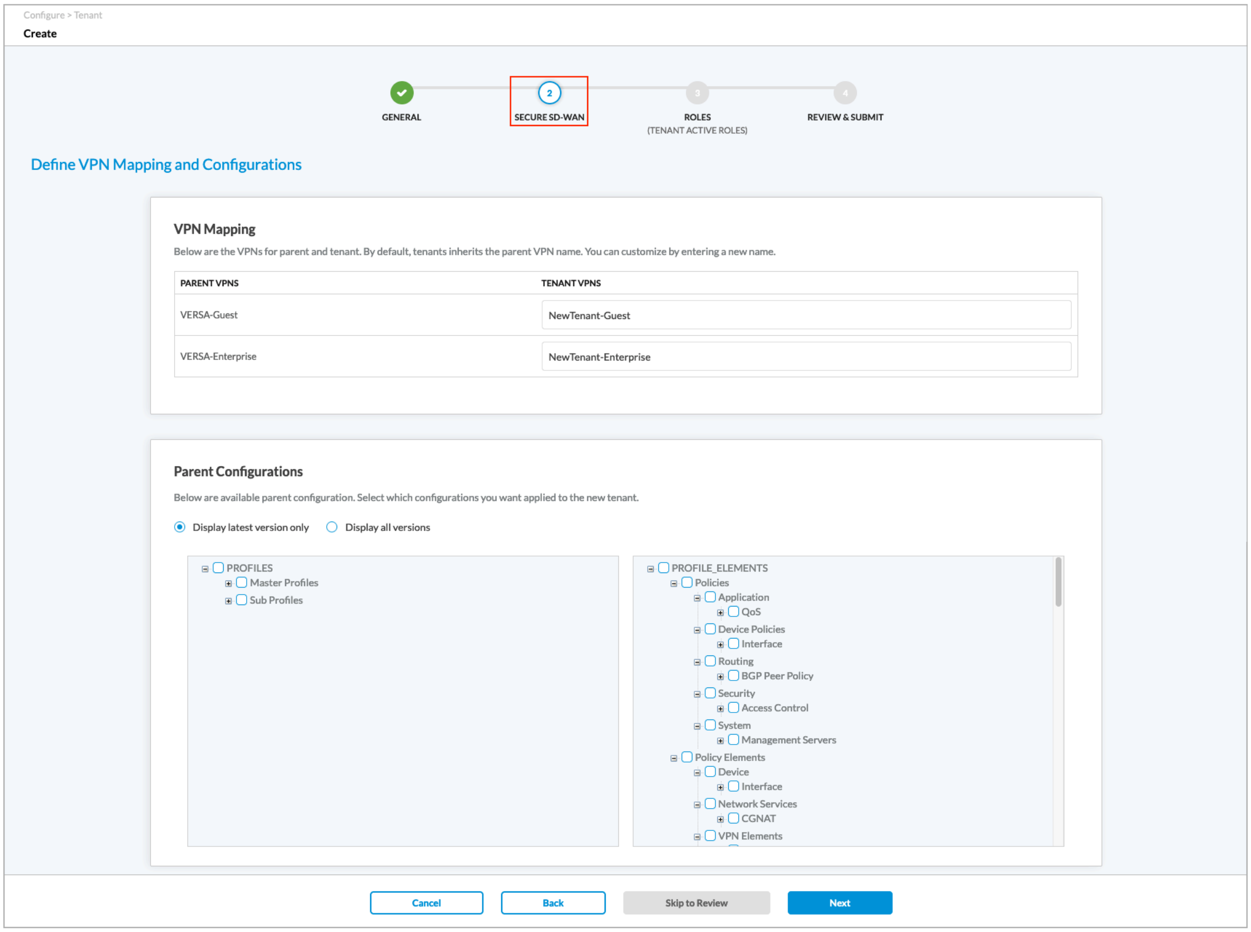
Network

Field	Description
Common Name (Required)	Enter the name of the certificate. The name is an identity that you also must configure on the CA server. Both names must match so that the CA server can issue the certificate. Because this attribute is mandatory, it does not appear in the CSR options section.
Email Address	Enter the email address for the device requesting the certificate.
Shared Key (Required)	Enter the shared key to authenticate the certificate request. The shared key is a password and must match the shared key on the server. Because this attribute is mandatory, it does not appear in the CSR options section.
Authentication ID	Enter the authentication identifier for the device requesting the certificate.
Country	Enter the country of the device requesting the certificate.
State Province	Enter the state or province of the device requesting the certificate.
Locality	Enter the locality, or city, of the device requesting the certificate.

Field	Description
Organization	Enter the organization of the device requesting the certificate.
Organization Unit	Enter the organizational unit of the device requesting the certificate, such as Sales or IT.
Validity	Enter the number of days that the certificate will be valid.
Private Key Size	Enter the size of the private key.
Renew Threshold	Enter a percentage value to modify when the certificate renews. For example, if the certificate renewal duration is configured to be 365 days in the Validity attribute, and you modify it to 50 percent, the certificate is renewed in 182.5 days. *Range*: 50 through 99 percent
Expiry Threshold Alarm	Enter a percentage value to modify when a device sends an alarm that the certificate is about to expire. For example, if the expiration threshold alarm for the certificate is configured to be 365 days in the Validity attribute, and you modify it to 75 percent, an alarm is sent in 273.75 days. *Range*: 50 through 99 percent
Network (Required)	Select the network to use to obtain the certificate. This attribute is mandatory, so it does not dieplay in the CSR options section.

e. Click Submit.
When you finish configuring a new device and publish it, the data that you entered above is converted into bind data. To view the bind data, go to the Deploy lifecycle. See Update CSR Bind Data for an Appliance before Publishing.

4. Click Next, or select Step 2, Secure SD-WAN. The default VPN mapping for the new tenant displays. By default, the VPNs for parent tenants and tenants are inherited. To change the name of the tenant VPN, enter a new name in the field.



Configure > Tenant

Create

Define VPN Mapping and Configurations

VPN Mapping

Below are the VPNs for parent and tenant. By default, tenants inherits the parent VPN name. You can customize by entering a new name.

PARENT VPNS	TENANT VPNS
VERSA-Guest	NewTenant-Guest
VERSA-Enterprise	NewTenant-Enterprise

Parent Configurations

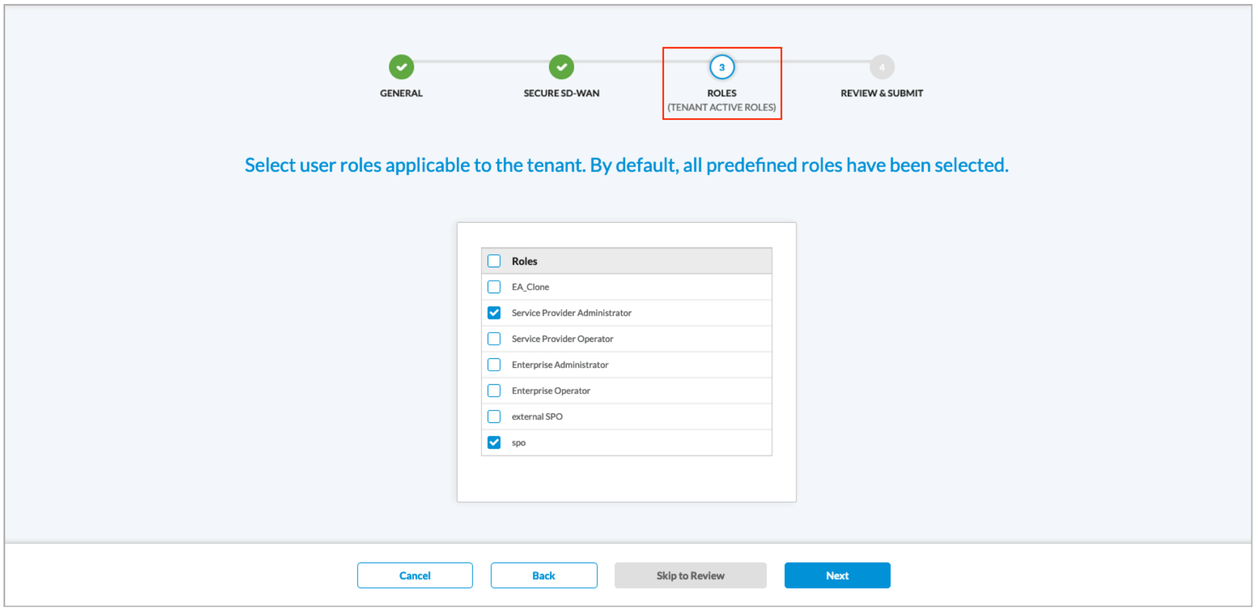
Below are available parent configuration. Select which configurations you want applied to the new tenant.

● Display latest version only ○ Display all versions

```
⊟ □ PROFILES
    ⊞ □ Master Profiles
    ⊞ □ Sub Profiles
```

```
⊟ □ PROFILE_ELEMENTS
    ⊟ □ Policies
        ⊟ □ Application
            ⊞ □ QoS
        ⊟ □ Device Policies
            ⊞ □ Interface
        ⊟ □ Routing
            ⊞ □ BGP Peer Policy
        ⊟ □ Security
            ⊞ □ Access Control
        ⊟ □ System
            ⊞ □ Management Servers
    ⊟ □ Policy Elements
        ⊟ □ Device
            ⊞ □ Interface
        ⊟ □ Network Services
            ⊞ □ CGNAT
        ⊟ □ VPN Elements
```

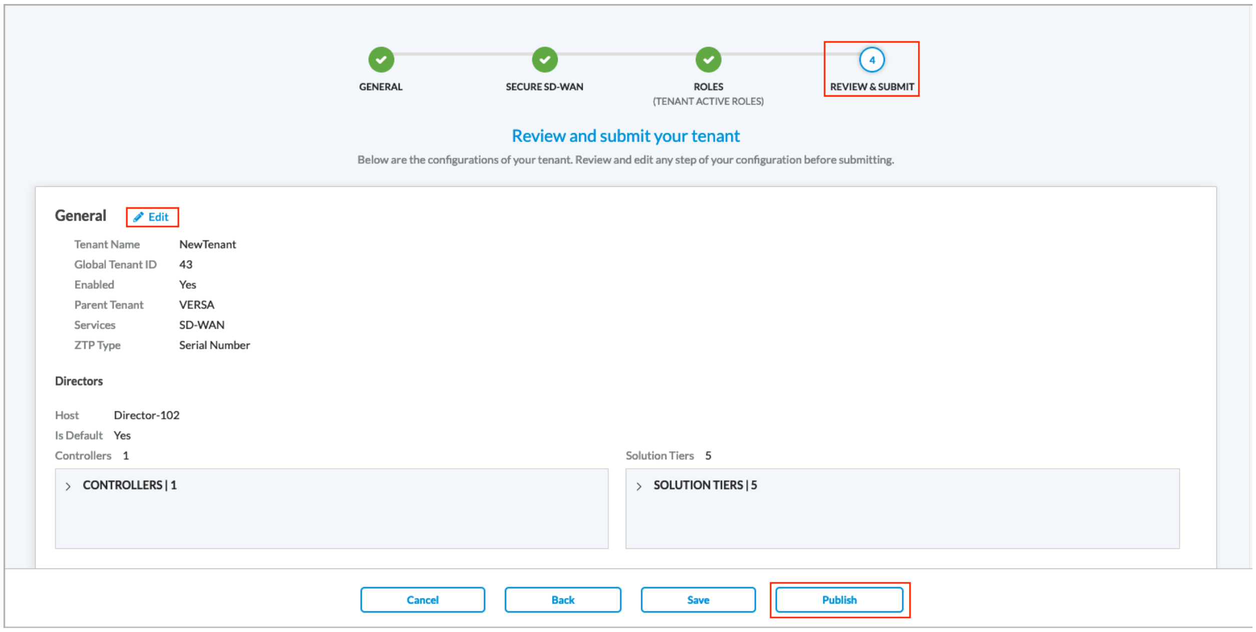
5. The Parent Configurations section displays all the parent's reusable profiles and profile elements.
    a. Select either Display Latest Version Only or Display All Versions.
    b. Select a profile to assign to the tenant from the Profiles list and the profile elements to assign to the tenant from the Profile Elements.
    c. To display the available resources in each category, click the ⊞ Plus icon.
    d. For more information about profiles and profile elements, see Configure Profiles.
6. Click Next, or select Step 3, Roles, to assign one or more roles to the tenant.



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

☐	Roles
☐	EA_Clone
☑	Service Provider Administrator
☐	Service Provider Operator
☐	Enterprise Administrator
☐	Enterprise Operator
☐	external SPO
☑	spo

7. Check the user roles for the new tenant. By default, all predefined roles are selected.
8. Click Next, or select Step 4, 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

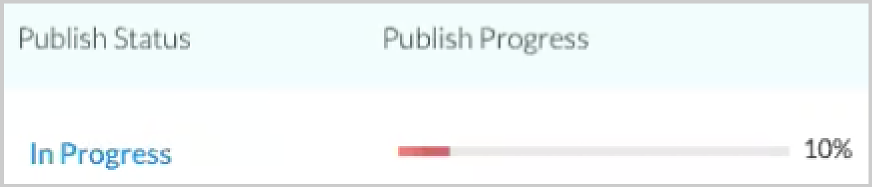
Tenant Name	NewTenant
Global Tenant ID	43
Enabled	Yes
Parent Tenant	VERSA
Services	SD-WAN
ZTP Type	Serial Number

Directors

Host	Director-102
Is Default	Yes
Controllers	1

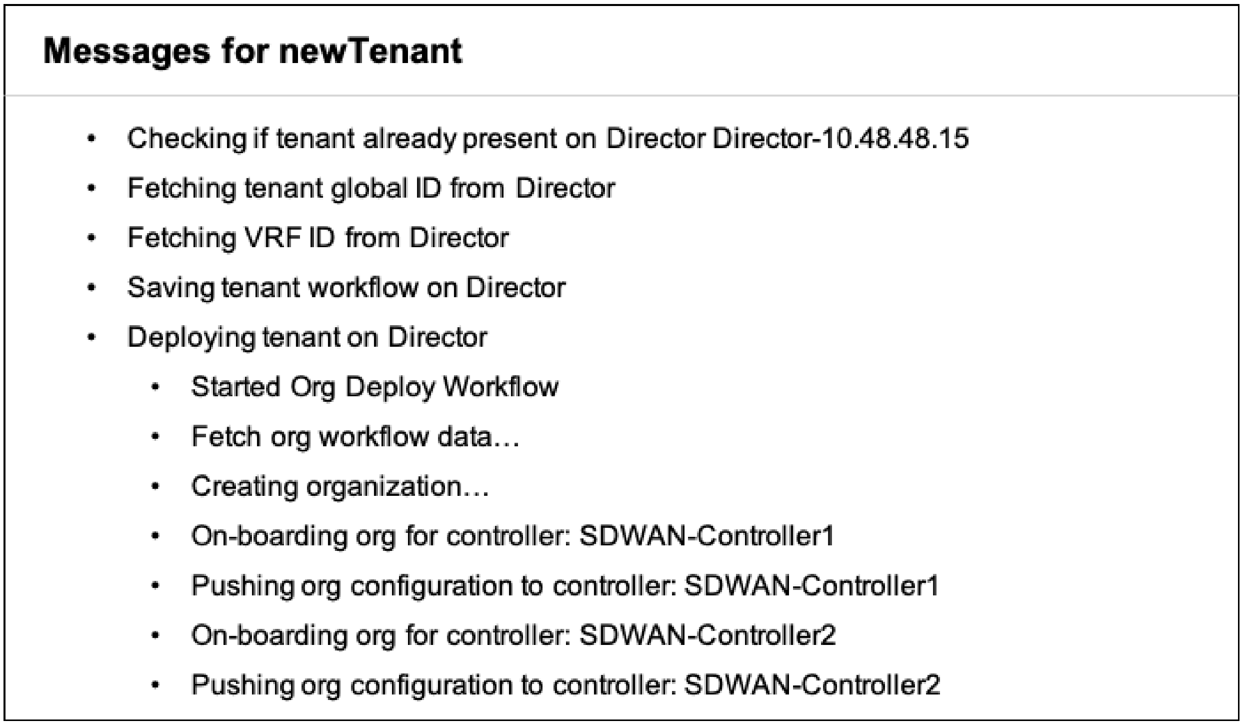
Solution Tiers 5

9. Review the configuration. Click the ✎ Edit icon to make changes.
10. Click Publish to publish the tenant to both the Director and Controller nodes. A progress bar shows displays during the publishing process.



Publish Status	Publish Progress
In Progress	10%

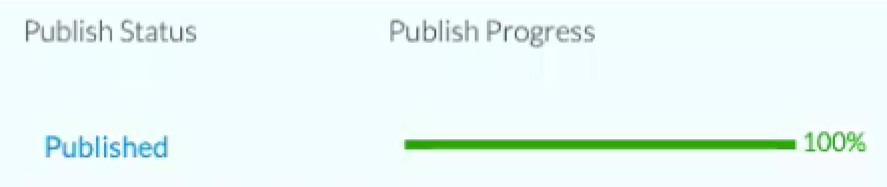
11. Click In Progress to view publish status messages.



Messages for newTenant

- Checking if tenant already present on Director Director-10.48.48.15
- Fetching tenant global ID from Director
- Fetching VRF ID from Director
- Saving tenant workflow on Director
- Deploying tenant on Director
    - Started Org Deploy Workflow
    - Fetch org workflow data…
    - Creating organization…
    - On-boarding org for controller: SDWAN-Controller1
    - Pushing org configuration to controller: SDWAN-Controller1
    - On-boarding org for controller: SDWAN-Controller2
    - Pushing org configuration to controller: SDWAN-Controller2

When the publishing process completes, the Publish Status column displays Published for the new tenant.



Publish Status	Publish Progress
Published	100%

12. To verify that the tenant has been published successfully, do one of the following:

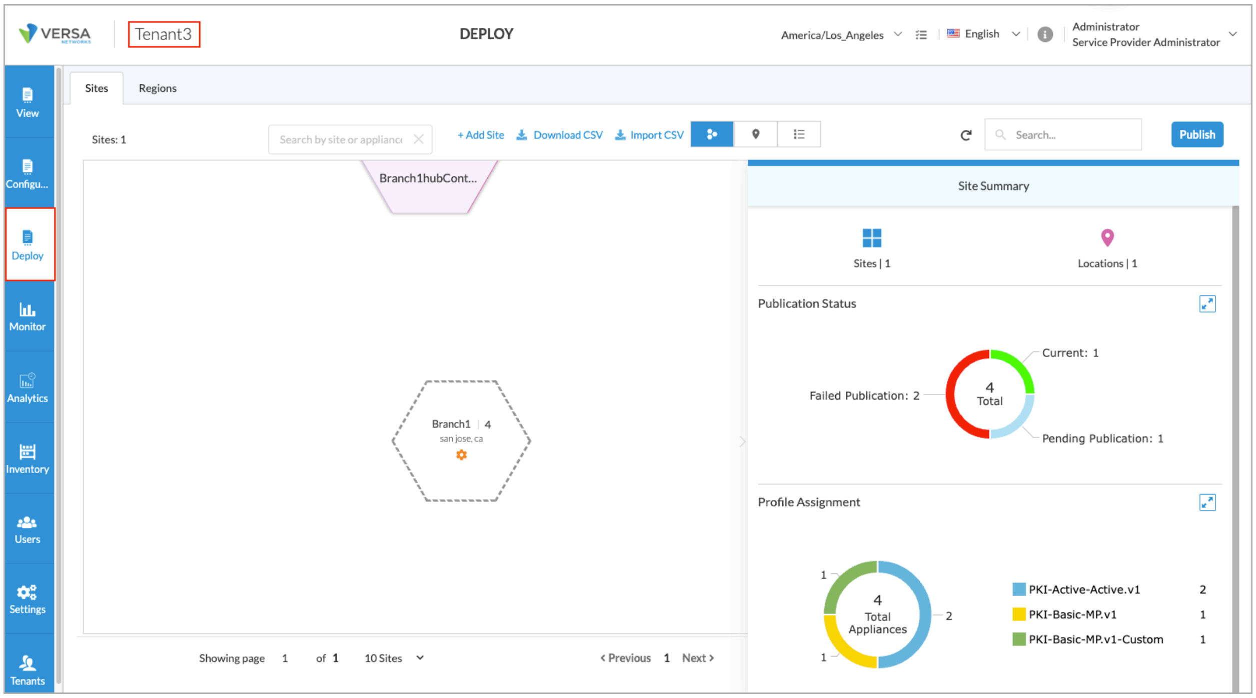
- On the Concerto orchestrator home page, check the entries in the Tasks menu.
- On the Director node, check the entries in the Director Task menu.
- On the Director node, select the Workflows tab in the top menu bar and then select Infrastructure >

Organizations in the left menu bar. The new tenant displays in the list of organizations.

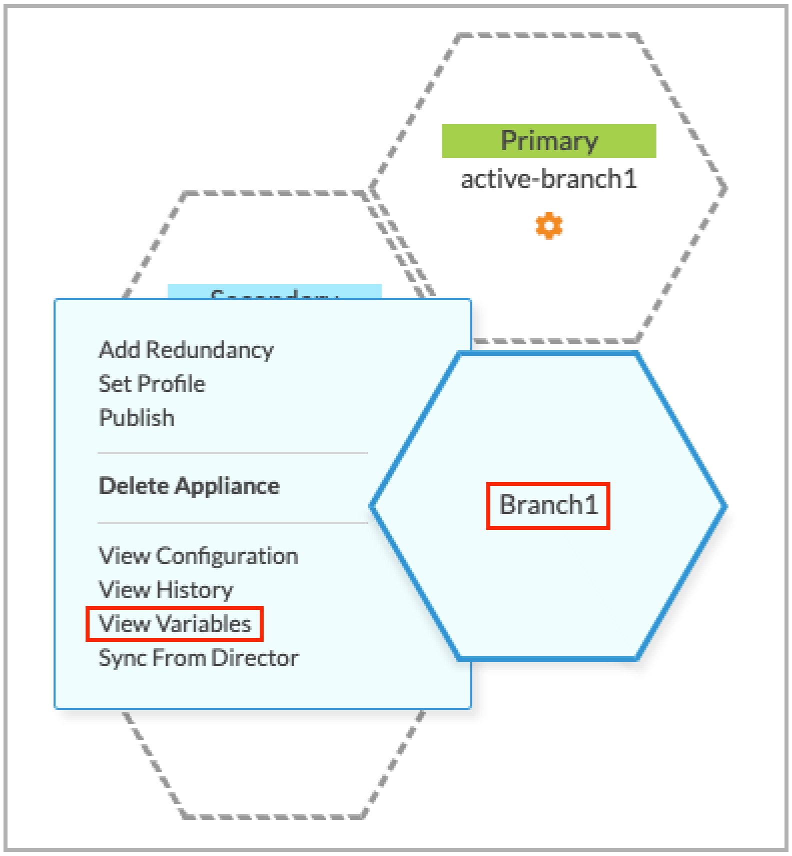
Update CSR Bind Data for an Appliance before Publishing

After you configure the CSR options for a tenant appliance, you can view and revise the options:

1. Select the Tenant on which the appliance is configured, and then double-click the branch that contains the device (Branch1 in the example below).

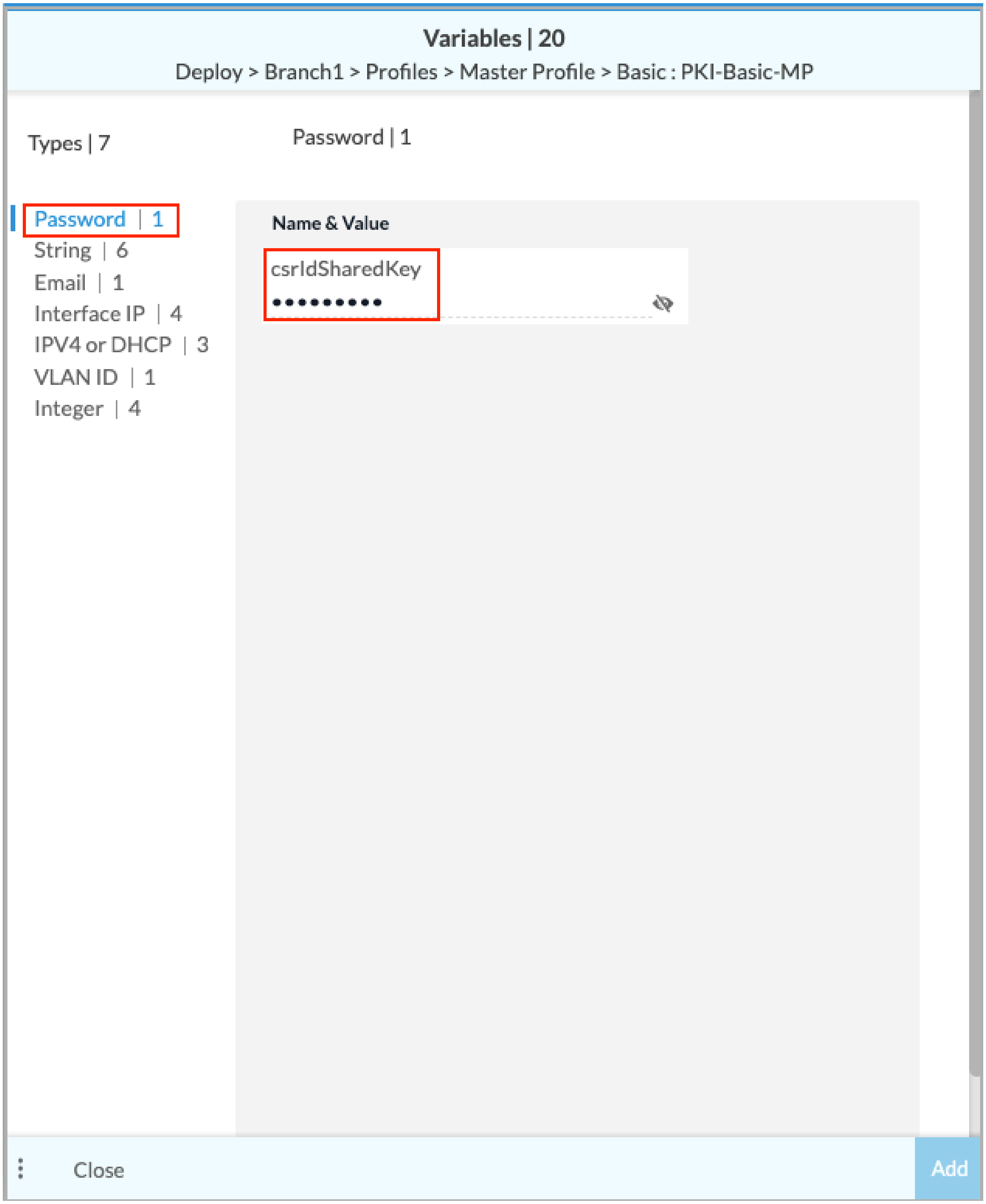


2. Select View Variables in the popup menu.



The Variables panel displays in the right portion of the screen, with the Password variable highlighted. The Name & Value field displays the Shared Key CSR bind variable. Note that the Shared Key bind variable is mandatory, so it is not listed in the configurable CSR Options screen.

The String, Email, and Integer variables also contain CSR bind data. You can change the bind data as needed before you publish the appliance.


Variables | 20

Deploy > Branch1 > Profiles > Master Profile > Basic : PKI-Basic-MP

Types | 7

Password | 1

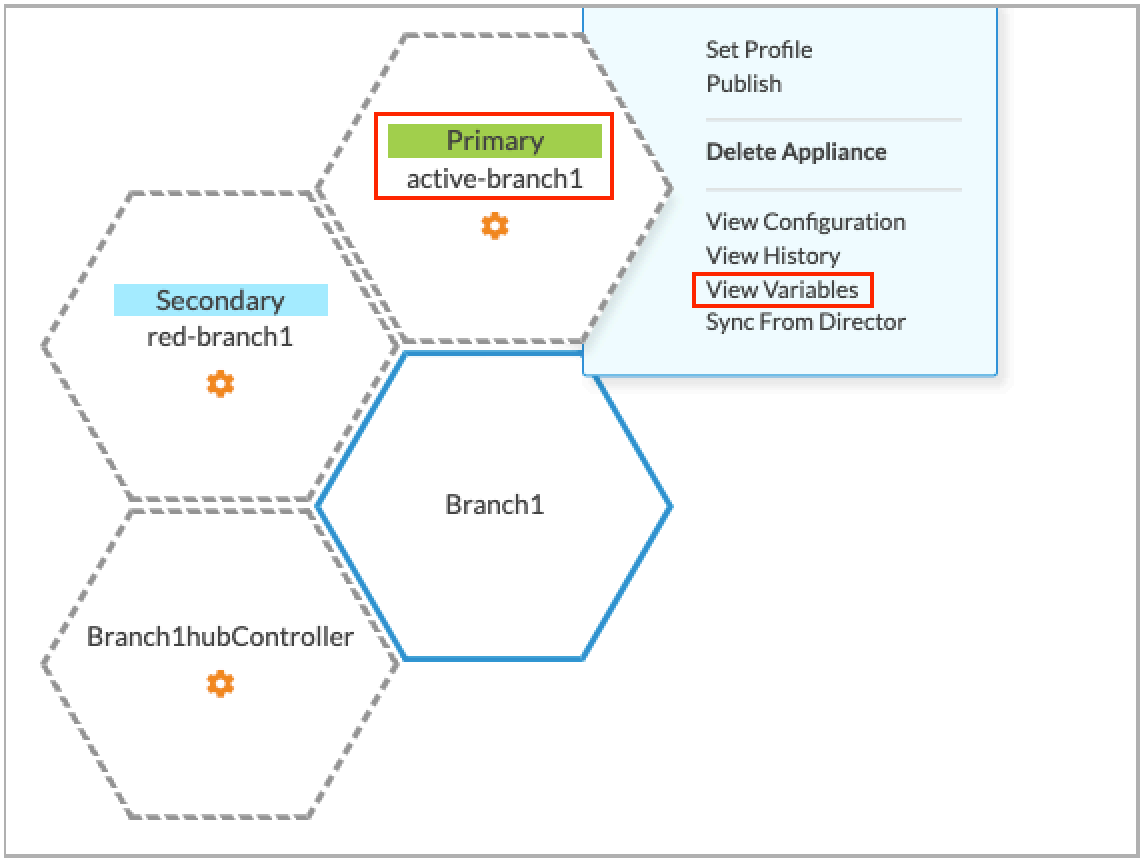
- Password | 1
- String | 6
- Email | 1
- Interface IP | 4
- IPV4 or DHCP | 3
- VLAN ID | 1
- Integer | 4

Name & Value

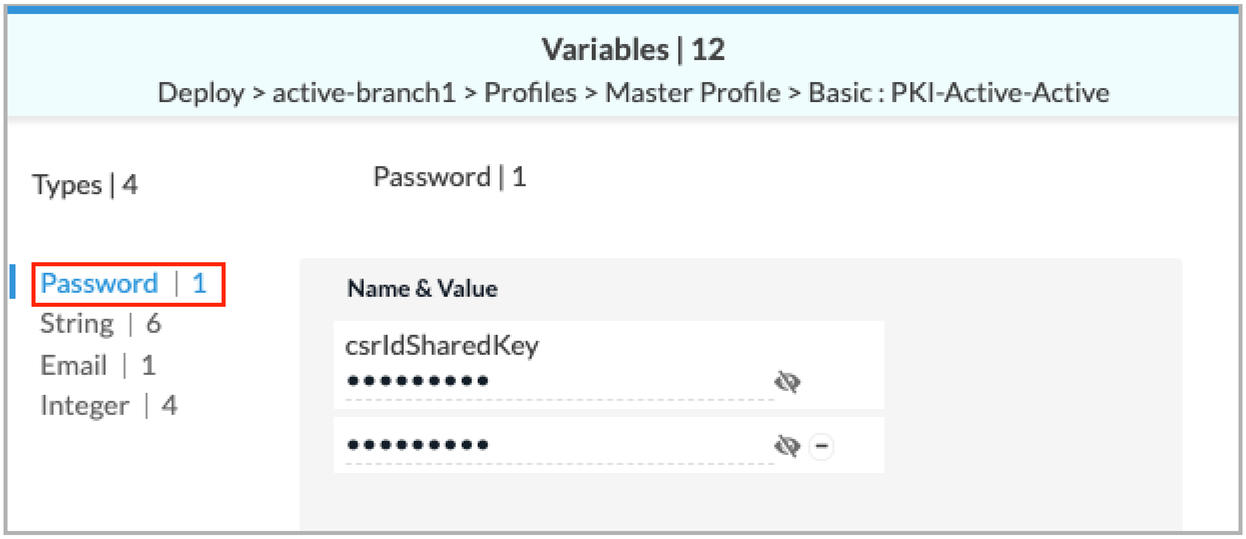
csrIdSharedKey

••••••••••

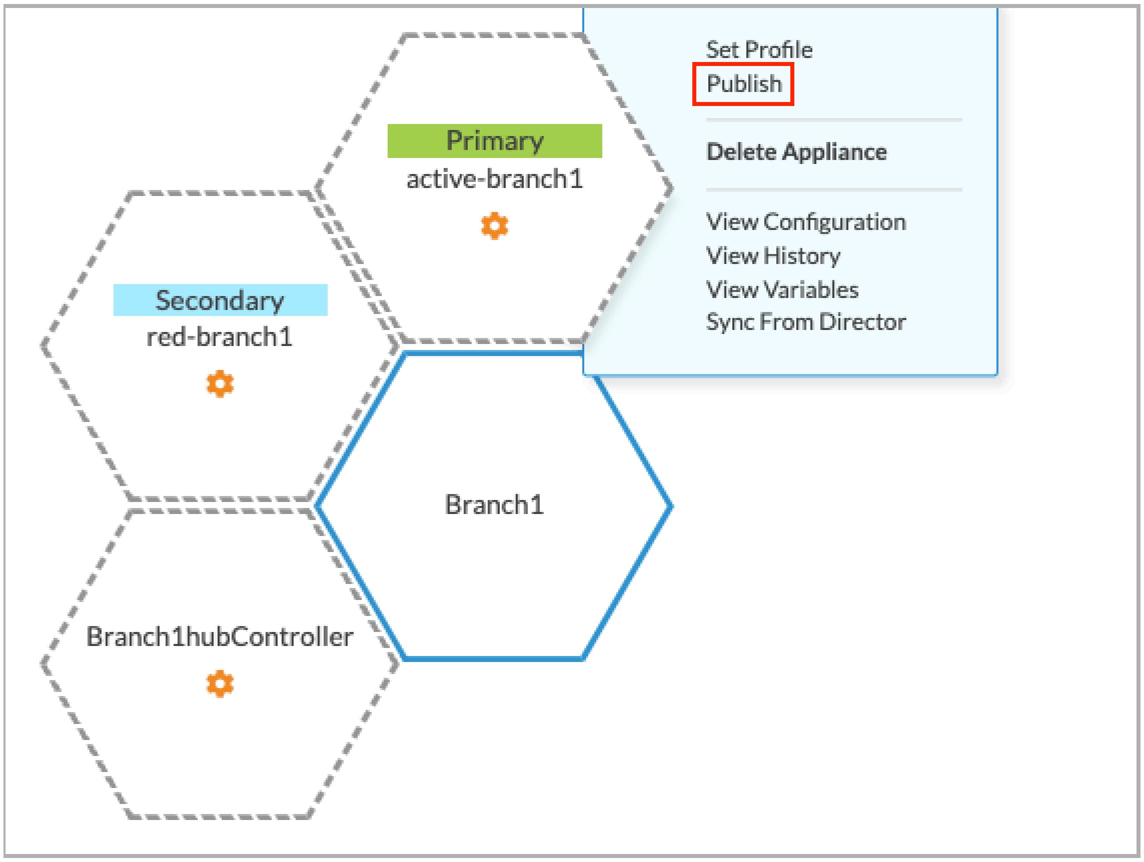
3. If the appliance is in an active–active configuration, click View Variables for the primary appliance. Note that for active–active configurations, you must define the bind variables for both the primary and secondary appliances in the Variables screen for the primary device.



The Variables screen displays. The example screen below shows two entries for the Shared Key variable, one for the primary device and one for the secondary device. You must specify two variables for all the CSR bind variables, except the Email variable.



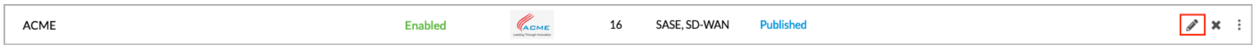
4. Before publishing the appliance, click each variable to review the entries. You can revise the entries as needed.



5. Click Publish to publish the appliance.

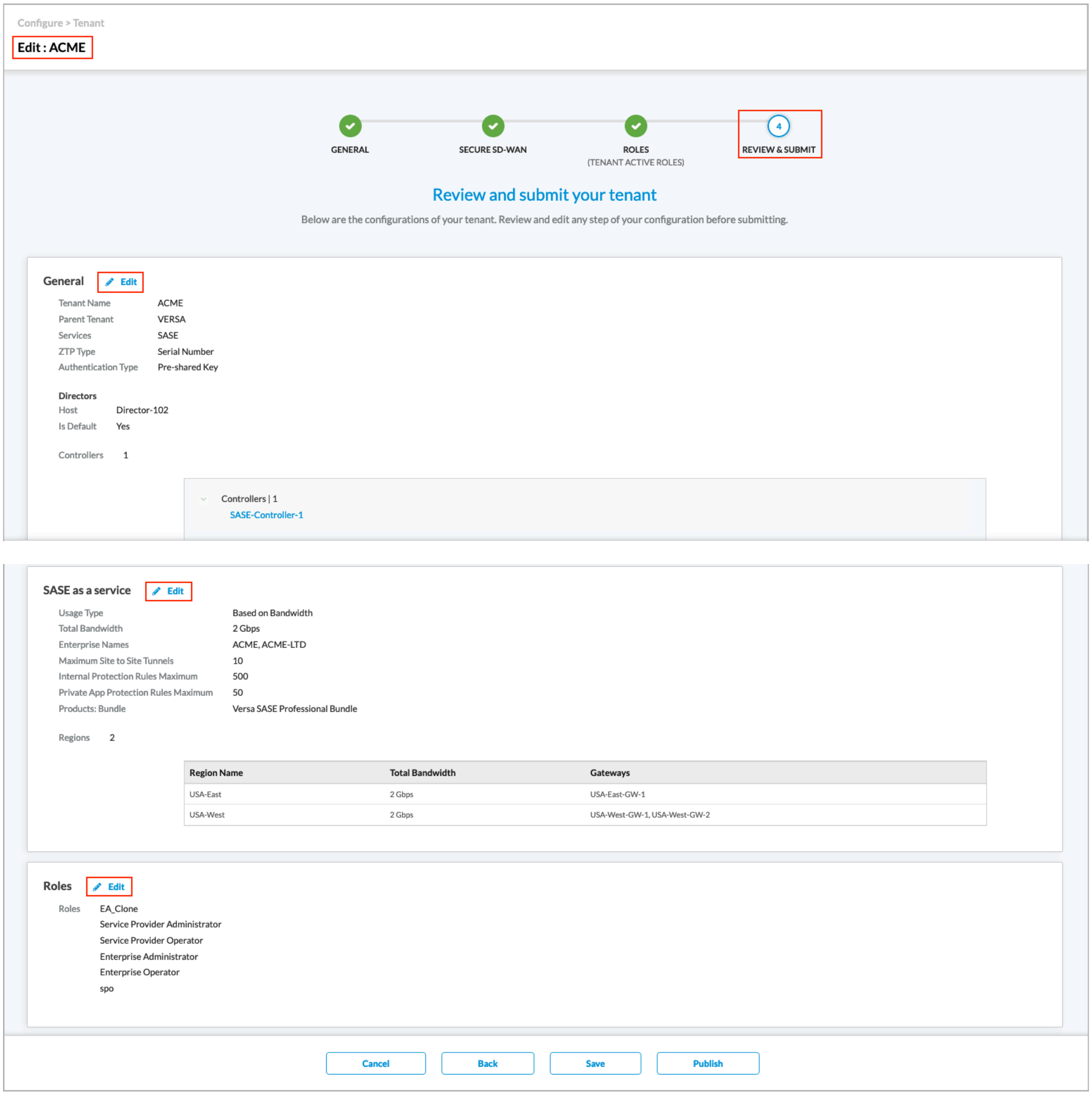
Update Information about an Existing SD-WAN Tenant

1. In the row for the tenant, click the ✏ Edit icon.



ACME	Enabled		16	SASE, SD-WAN	Published

The Edit *Tenant* screen displays.



Configure > Tenant

Edit : ACME

Review and submit your tenant

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

General

Tenant Name	ACME
Parent Tenant	VERSA
Services	SASE
ZTP Type	Serial Number
Authentication Type	Pre-shared Key

Directors

Host	Director-102
Is Default	Yes

Controllers 1

Controllers | 1
SASE-Controller-1

SASE as a service

Usage Type	Based on Bandwidth
Total Bandwidth	2 Gbps
Enterprise Names	ACME, ACME-LTD
Maximum Site to Site Tunnels	10
Internal Protection Rules Maximum	500
Private App Protection Rules Maximum	50
Products: Bundle	Versa SASE Professional Bundle

Regions 2

Region Name	Total Bandwidth	Gateways
USA-East	2 Gbps	USA-East-GW-1
USA-West	2 Gbps	USA-West-GW-1, USA-West-GW-2

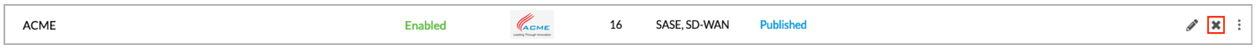
Roles

Roles EA_Clone
Service Provider Administrator
Service Provider Operator
Enterprise Administrator
Enterprise Operator
spo

2. Click the ✎ Edit icon in any of the sections to edit that section.
3. Click Save to publish the tenant information later, or click Publish to publish the tenant information immediately.

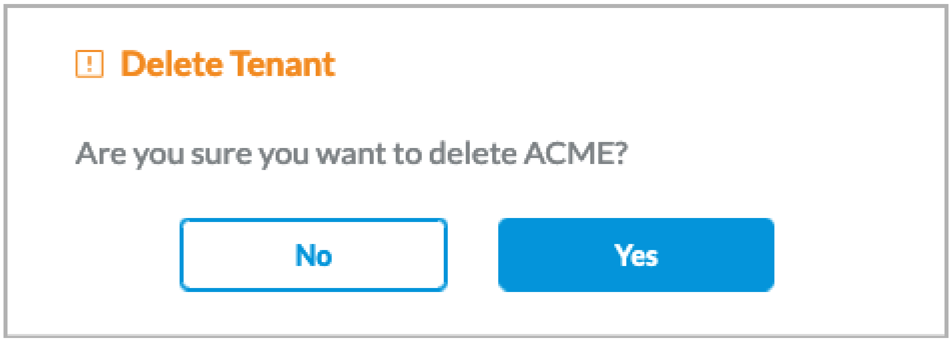
Delete a Tenant

1. In the row for the tenant, click the ✖ Delete icon.



ACME	Enabled		16	SASE, SD-WAN	Published

2. Click Yes in the Delete Tenant popup window.

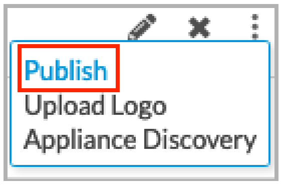


Are you sure you want to delete ACME?

Publish a Tenant Configuration to Versa Director

To immediately publish the tenant's configuration to the Director node and its connected devices:

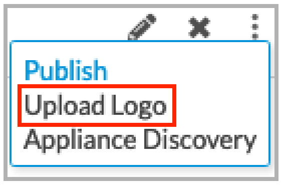
1. In the row for the tenant, click the ⋮ More icon.



2. Select Publish to publish the tenant configuration.

Upload a Tenant Logo

1. In the row for the tenant, click the ⋮ More icon.



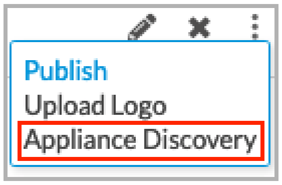
2. Select Upload Logo. For more information see Upload a Tenant Logo.

Discover VOS Devices for a Published Tenant

For Releases 10.2.1 and later.

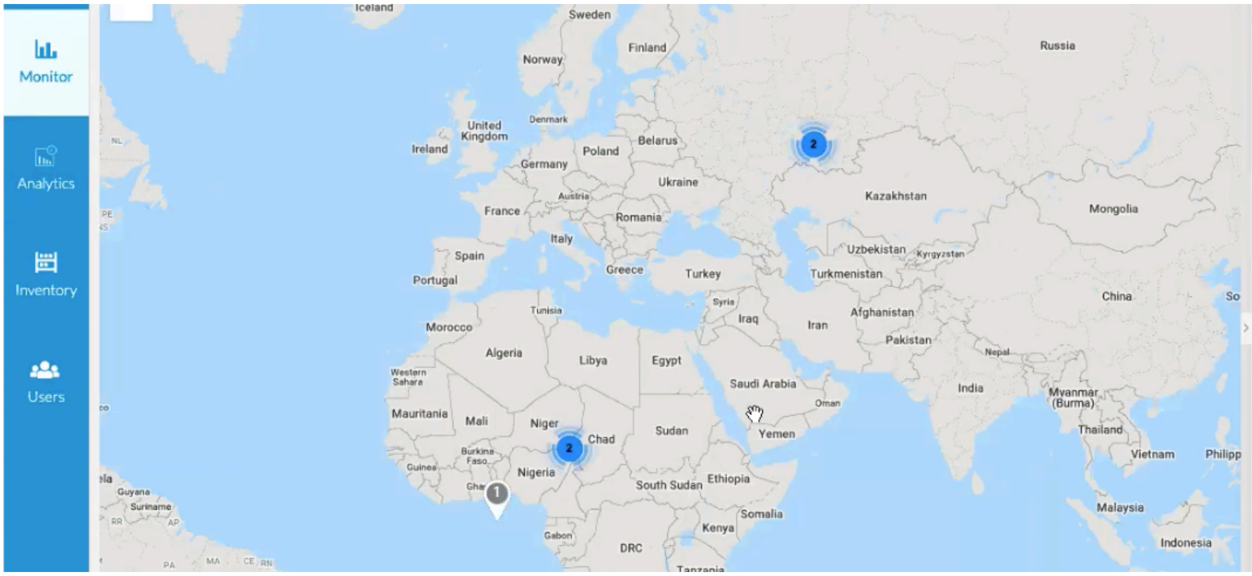
To discover VOS devices for a published tenant on a Director node:

1. In the row for the tenant, click the ⋮ More icon.

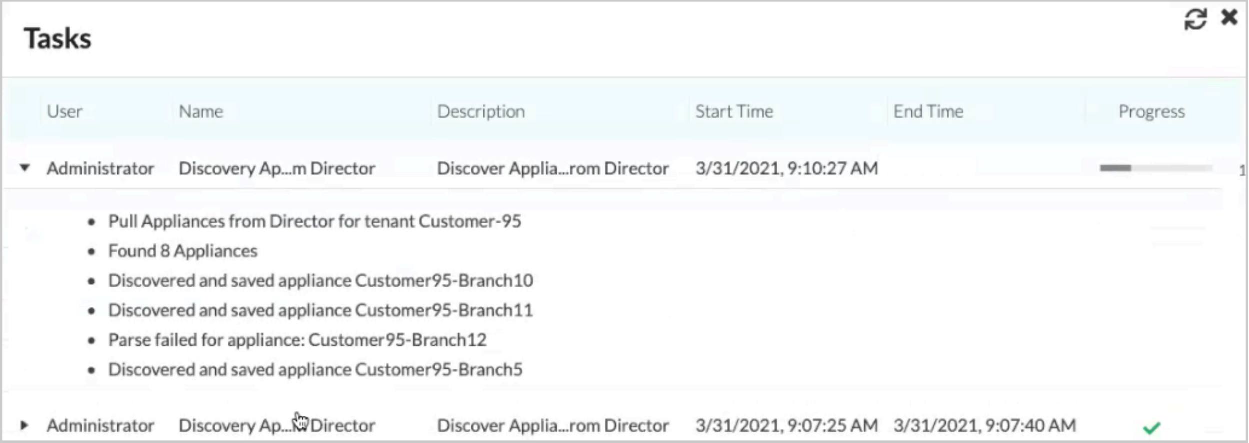


Publish
Upload Logo
Appliance Discovery

2. Select Appliance Discovery.
3. Wait while Concerto performs the discovery operation. Note that Concerto does not discover Controller nodes.
4. During discovery, click the tenant name in the main screen to display the Map or Honeycomb view for the tenant. Site icons in Map view change to blue and hexagons are added in Honeycomb view as appliances are discovered.



During discovery, click the ☰ Tasks icon to display discovery operation messages.



Tasks

User	Name	Description	Start Time	End Time	Progress
Administrator	Discovery Ap...m Director	Discover Applia...rom Director	3/31/2021, 9:10:27 AM		
	• Pull Appliances from Director for tenant Customer-95 • Found 8 Appliances • Discovered and saved appliance Customer95-Branch10 • Discovered and saved appliance Customer95-Branch11 • Parse failed for appliance: Customer95-Branch12 • Discovered and saved appliance Customer95-Branch5				
Administrator	Discovery Ap...Director	Discover Applia...rom Director	3/31/2021, 9:07:25 AM	3/31/2021, 9:07:40 AM	✓

When discovery completes, you can view the discovered VOS devices in the Monitor lifecycle, and the Concerto orchestrator begins populating the summary window with information from the discovered appliances. Updating the summary window may take a few minutes to complete. The Concerto orchestrator automatically maps discovered VOS devices to a site matching the location of the VOS device. If the Concerto orchestrator does not find a site matching the VOS device location, it creates a site for the location and maps the VOS device to the site.

Supported Software Information

Releases 10.1.1 and later support all content described in this article, except:

- Release 11.1.1 allows you to configure a Security Service Edge (SASE) tenant.
- Release 12.1.1 allows you to create a tenant with a non-SD-WAN solution tier and to use a PKI certificate for authentication.

Additional Information

Concerto Home Screen Overview
Create a Director Cluster
Create SASE Tenants