Configure Basic Features

For supported software information, click here.

As part of the initial software configuration of a Versa Operating System™ (VOS™) devices, you configure the following basic features:

- Provider organizations
- Tenant organizations, if needed
- Controller nodes
- Device templates
- Service templates
- Devices
- Device groups

Before You Begin

Before you begin the initial software configuration of VOS devices, do the following:

- Create an Analytics cluster to capture the log information from the VOS devices. See Set Up Analytics in Perform Initial Software Configuration.

Also, you can optionally do the following:

- Change the default private IP address space
- Change the AS number of the MP-BGP overlay network

By default, the Director node uses the IP prefix 10.0.0.0/8 when generating overlay IP addresses for each branch. To change to a different private address space, issue the following command on the primary (active) Director node in configuration mode. In this command, *ip-prefix* can be 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16, and *number* can be 64, 128, 256, 512, 1024, or 2048. If the number of organizations is greater than 128, the IP prefix must be 10.0.0.0/8.

> Administrator@Director1% **set nms sdwan overlay-address-scheme ipv4-prefix** *ip-prefix* **maximum-organizations** *number*

For example:

> Administrator@Director1% **set nms sdwan overlay-address-scheme ipv4-prefix 192.168.0.0/16 maximum-organizations 128**

By default, the SD-WAN overlay network uses AS number 64512 when establishing MP-IBGP adjacencies between Controllers and VOS branch devices. To change to a different 4-byte AS number, issue the following command on the primary (active) Director node in configuration mode. In this command, *number* can be a value from 1 through 4294967295.

> Administrator@Director1% **set nms sdwan global-config overlay-mpbgp-as** *number*

For example:

> Administrator@Director1% **set nms sdwan global-config overlay-mpbgp-as 755128**

Create Provider Organizations

An organization is a group of devices covered by a single software license. An organization includes VOS, Versa Analytics, Versa Director, and Versa Controller devices.

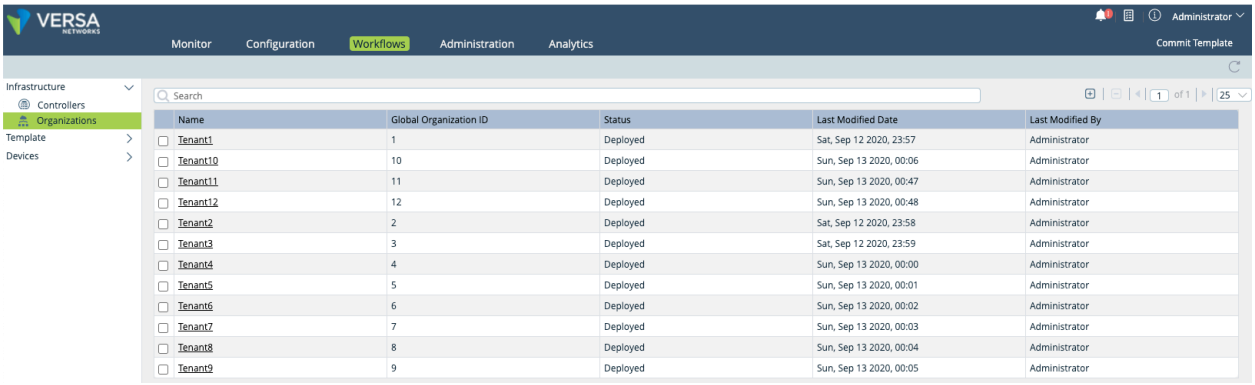
For provider organizations, the VOS device can support either single tenants or multiple tenants. Single tenancy is a single organization that has no child, or subordinate, organizations. Multitenancy comprises a parent-child organization hierarchy that shares hardware resources, resulting in savings in setup time and operational costs. The software license plan associated with the parent organization is automatically inherited by the child organizations.

You create provider organizations using Versa Director Workflows. This is the recommended method. However, you can also create them manually.

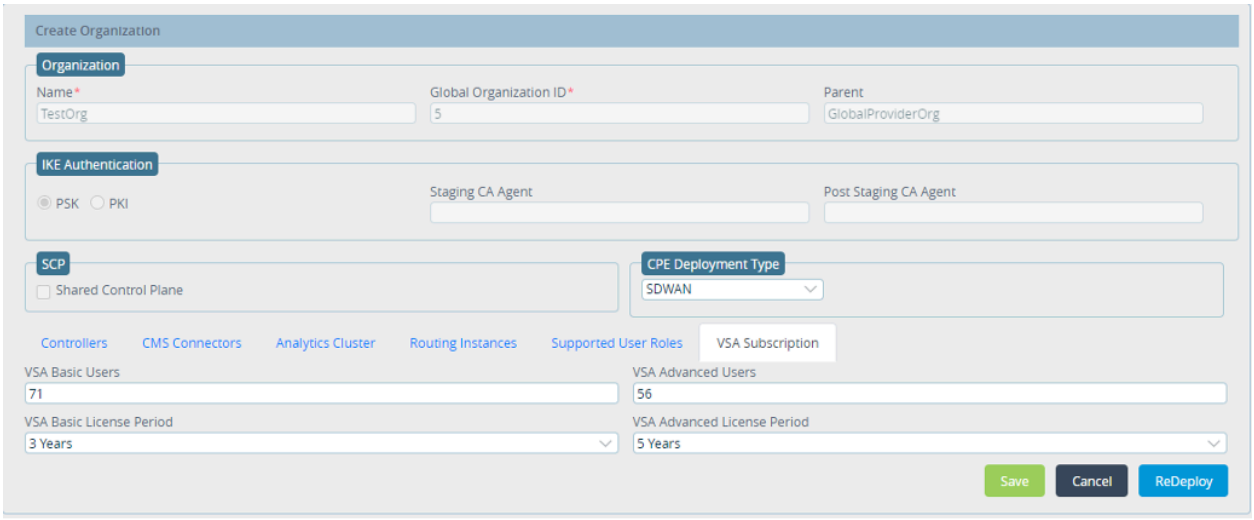
After you create an organization, you need to create at least one "admin" user, and it is recommended that you create at least one other, non-admin user.

Add a Provider Organization

1. In Director view, select the Workflows tab in the top menu bar.
2. Select Infrastructure > Organizations in the left menu bar.



3. Click the Add icon to add an organization. Enter information for the following fields.



Field	Description
Name (Required)	Enter a name for the organization.
Global Organization ID	The value for this field is automatically populated with the next available organization identifier. You can change the value. The organization ID must be unique across the network. *Range:* 1 through 31
Parent	For multitenancy, select the name of the parent organization.
IKE Authentication	Mode of IKE authentication.
◦ PSK	Click to enable preshared key IKE authentication.

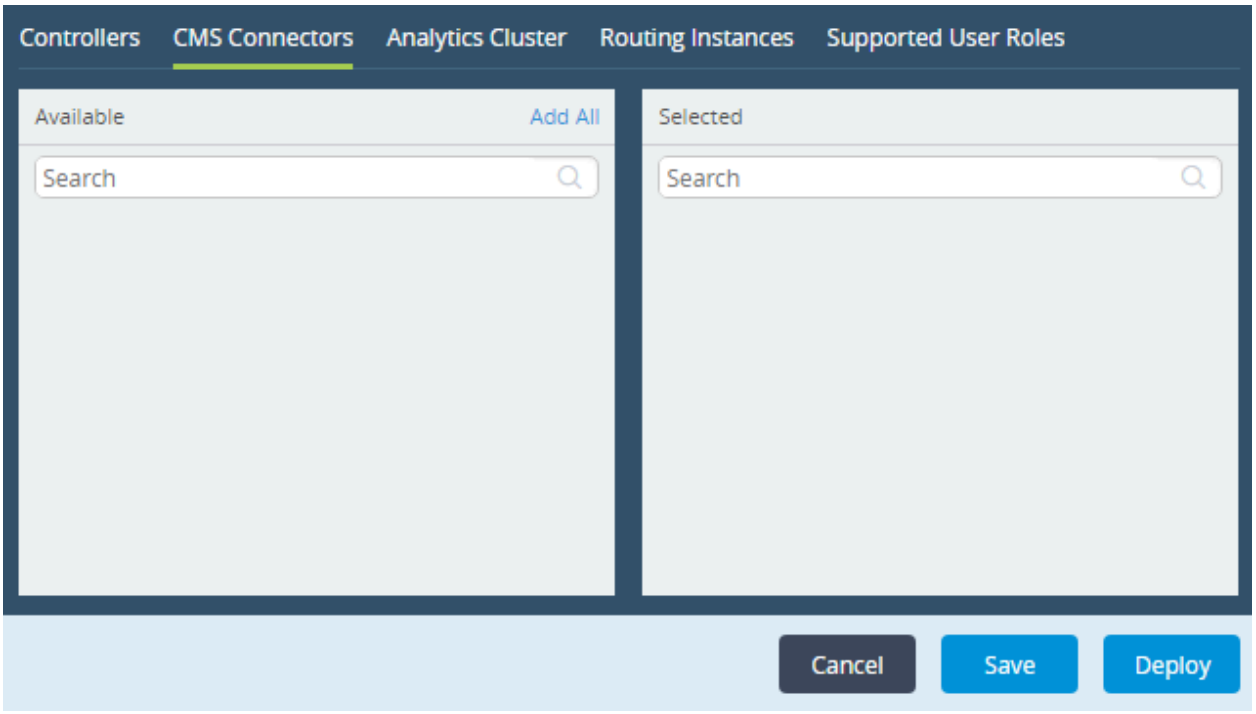
Field	Description
◦ PKI	(For Releases 22.1.1 and later.) Click to select a staging or port staging CA profile. For more information, see Configure a Common Certificate Authority. (For Releases 21.2 and earlier.) Click to enable public key infrastructure authentication.
◦ Staging CA Agent	(For Release 22.1.1 and later.) Select the CA profile to associate with staging. The CA profiles listed are those that you created as described in Configure a Common Certificate Authority. (For Releases 21.2 and earlier.) Enter the IP address of the certificate agent (CA) for staging templates.
◦ Post Staging CA Agent	(For Release 22.1.1 and later.) Select the CA profile to associate with post staging. The CA profiles listed are those that you created as described in Configure a Common Certificate Authority. (For Releases 21.2 and earlier.) Enter the IP address of the certificate agent (CA) for post-staging templates.
SCP	Shared control plane.
◦ Shared Control Plane	For multitenancy, click to have the organization share the control (management) plane with its parent organization or organizations. When you enable a shared control plane, the organization shares the control VR routing instance and the IPsec tunnels to the Controller nodes with its parent organization. The organization does not have either its own control VR routing instance or its own IPsec tunnels to the Controller nodes.
CPE Deployment Type	Select a CPE deployment type.

4. Select the Controllers tab, and enter information for the following fields.

Field	Description
Available	Search for the Controller node or Controller nodes to associate with the organization, and click Add All to

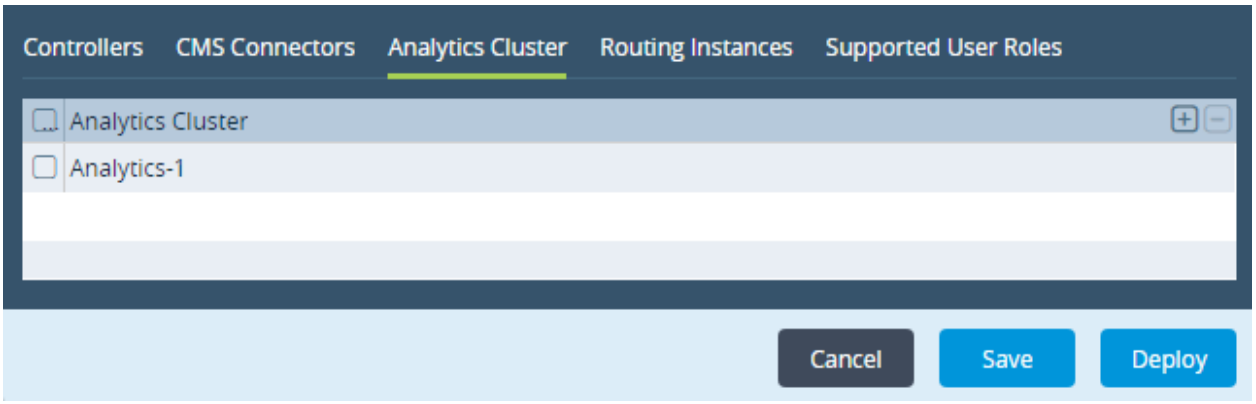
Field	Description
	select them.
Selected	Lists the Controller nodes associated with the organization.

5. Select the CMS Connectors tab, and enter information for the following fields.

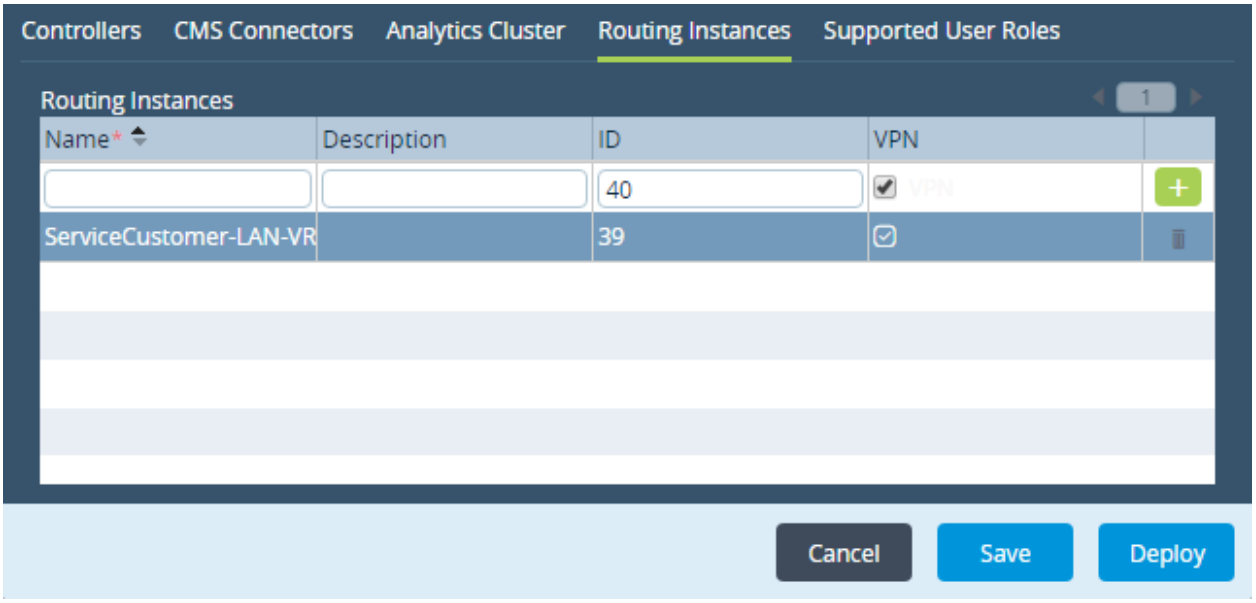


Field	Description
Available	Search for the CMS connector or connectors to associate with the organization, and click Add All to select them.
Selected	Lists the connectors associated with the organization.

6. Select the Analytics Cluster tab. Select the Analytics cluster or clusters to associate with the organization. Click the Add icon to add an Analytics cluster to the list.

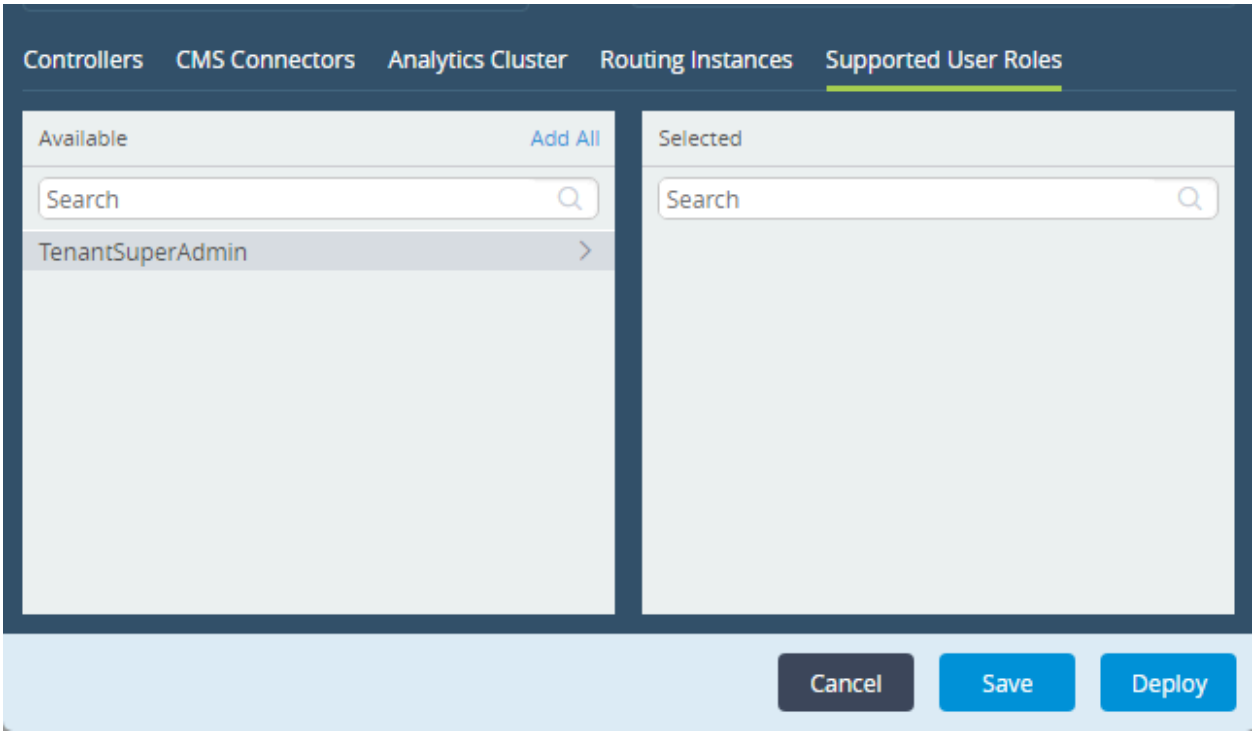


7. Select the Routing Instances tab to define virtual routing instances for the organization. Enter information for the following fields.



Field	Description
Name (Required)	Enter a name for the routing instance.
Description	Enter a text description for the routing instance.
ID	Enter a numeric identifier for the routing instance.
VPN	Click to enable a VPN on the routing instance.
Add icon	Click to add the routing instance to the organization.

8. Select the Supported User Roles tab, and enter information for the following fields.



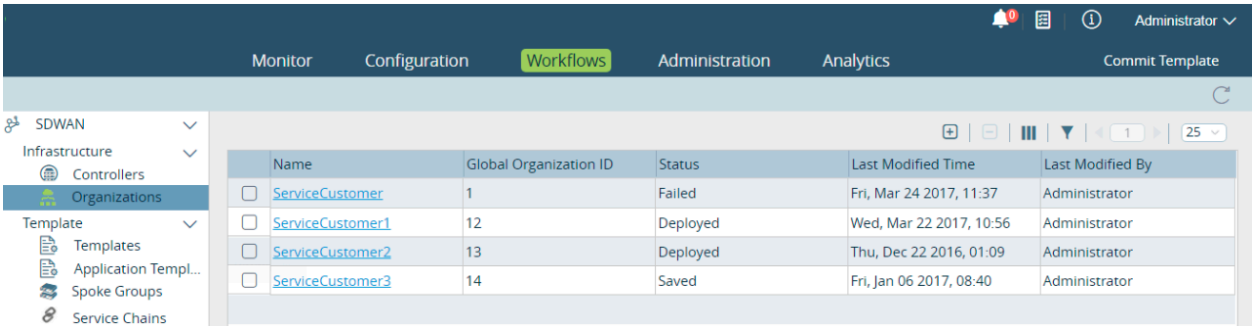
Field	Description
Available	Search for the user role or roles to associate with the organization, and click Add All to select them.
Selected	Lists the roles associated with the organization.

9. Select the VSA Subscription tab to configure the number of Versa Secure Access (VSA) licenses for both basic and advanced users per organization using Versa Director.

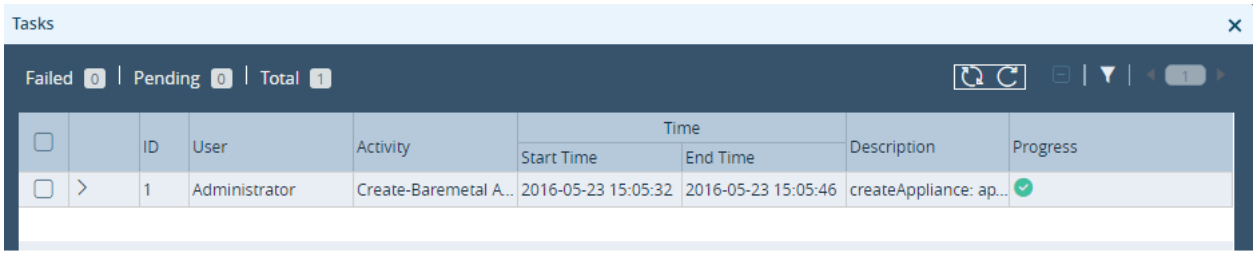
Field	Description
VSA Basic Users	Enter the number of VSA basic users for the organization. The minimum number of basic users is 50.
VSA Advanced Users	Enter the number of VSA advanced users for the organization. The minimum number of advanced

Field	Description
	users is 50.
VSA Basic License Period	Enter the license period for VSA basic users. The license period is 1, 3, or 5 years.
VSA Advanced License Period	Enter the license period for VSA advanced users. The license period is 1, 3, or 5 years.

10. Click Save to add the organization.
11. Click Deploy to onboard the organization. The main pane displays the new organization as well as other organizations.



You can monitor the progress and status of the organization creation process in the Tasks dashboard. In case the organization creation is unsuccessful, view the error messages for possible debug information. To view the Tasks dashboard, click the Tasks icon in the top menu bar.



The icon in the Progress column indicates the status of the task. A red exclamation point icon indicates a problem or error condition. Click the arrow (>) in the second column to display more information about the task, including any error messages.

Modify an Organization's Configuration

To modify an organization's configuration, follow one of the procedures for adding an organization. After you are finished making the changes, click Save and then click Redeploy for the changes to take affect.

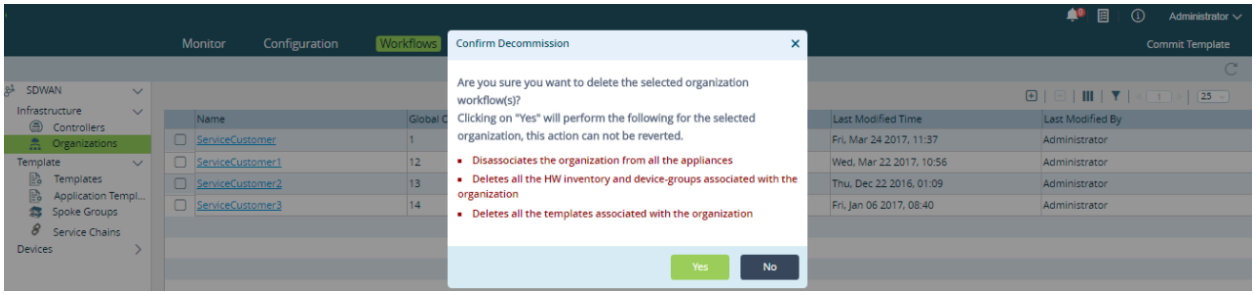
Remove an Organization

When you remove an organization, the organization is deleted and decommissioned. The decommissioning process does the following:

- Disassociates the organization from all VOS devices.
- Deletes the hardware inventory and device groups associated with the organization.
- Deletes all templates associated with the organization.
- Moves the VSA user licenses to the terminated state

To remove an organization:

1. Display the organization list:
   a. Select the Workflows tab from the top menu bar, and select Organizations from the left menu bar.
   b. Or, Select the Administration tab from the top menu bar, and select Organizations from the left menu bar.
2. Click the checkbox next to the organization name.
3. Click the Delete icon:



4. Click Yes.

Create Versa Operating System Users

Versa Operating System (VOS) supports the following users:

- System users
- Organization users
- Default users

System User Attributes

A system user has the following attributes:

- Can log in to the Versa VOS host OS and CLI.
- Is created in Linux when the user is configured.

- Can assume the role of an administrator or operator. As an administrator, a system user can modify any part of configuration, while as an operator, the system user can only view the configuration.
- The allowed login is shell or CLI. If shell is selected, the system user lands on Bash mode. When CLI is selected, the user lands on the CLI prompt.
- Can SSH to port 22 and port 2024. When port 2024 is passed to SSH, the user always lands on CLI, irrespective of the login configured. System users can launch a shell from CLI.
- VOS supports password-less authentication for system users using the SSH public key. This enhances security, protecting the system against the brute force password attacks of SSH.
- Can configure multiple SSH keys.

```
root@gothamcli(config)% set system users john password john123 login shell role admin
root@gothamcli(config)% show | compare
 system {
    users john {
        password $1$GYdCkdSz$yiukA.B95.M8vbF3jl1pp0;
        sshpublickey laptop {
            "sshrsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCyhCqGWaZmpji
xaKVqjK2Ij4QUaJuiA1T+pSTveaJxrNSiCWzfKibY+
y/QV0a3+0Y4SQ5W9gkyMbL6Mrk1afqnznp5y20gMIbt
ul58aJ/Q09Ygu2qg4ULb7iUgHBzwunk2hViKez06yMD
jbsE3JGvk5chffSbWXWrkObgwcHkn6KPLiYSW0cEbVS
Qa1bbF7GSJhIX6QWR17IWjp7MiD569aYxf6rI/WdjSI
StO1p7mm01Y93sXnYn7hLs+8mmgV7aF18ZLtMy6x6of
b7yoyov/UQZA9L7+Wy0YtHJ+BF5oM1reG7FwxBHdwbq
p/ZqKF3R9kisxDAEWbsQBcVTSYI mmehra@quake";
        }
        login shell;
        role admin;
    }
}
```

Organization User Attributes

A organization user has the following attributes:

- Can log into only CLI.
- Can SSH to only port 2024. Port 22 is disallowed.
- Cannot launch “shell” from the CLI.
- Password-less authentication is currently not supported.
- While creating an organization user, @Org is appended to the user name, to create unique user names. For instance, in the following example, the username is john@kayak. Here, the user can SSH as:

```
ssh 'john@kayak'@77.1.1.1 p 2024    (or)
ssh 77.1.1.1 l john@kayak p 2024
root@gothamcli(config)% set orgs org Customer1 users john role tenantadmin
root@gothamcli(config)% show | compare
 orgs {
    org Kayak {
```

```
        users john {
            password $1$atCDHNyk$aaHOaHcP76UXyCKV7ymoz/;
            role tenantadmin;
        }
    }
}
```

VOS provides the following predefined RBAC roles that can be assigned to an organization user:

Role	Description
adcadmin	Can view and modify the ADC configuration.
cgnatadmin	Can view and modify the CGNAT configuration.
sdwanadmin	Can view and modify the SD-WAN configuration.
securityadmin	Can view and modify the security configuration.
tenantadmin	Can view and modify the tenant configuration.
oper	Can only view the tenant configuration.

Default User Attributes

A default user has the following attributes:

- By default, VOS has two system users—admin and versa. You cannot delete these users.
- The default password for these users is versa123.
- Admin is a super user with sudo privileges. Admin can SSH to the box on port 22 and port 2024.
- Versa is a console user. Versa can only login via the physical or virtual console.
- The password for admin and versa can be modified or deleted via CLI. Password-less authentication can be set for admin via SSH public keys. For example:

```
root@cli(config)% show system users
users admin {
    login shell;
    role  admin;
}
users versa {
    login shell;
    role  admin;
}
```

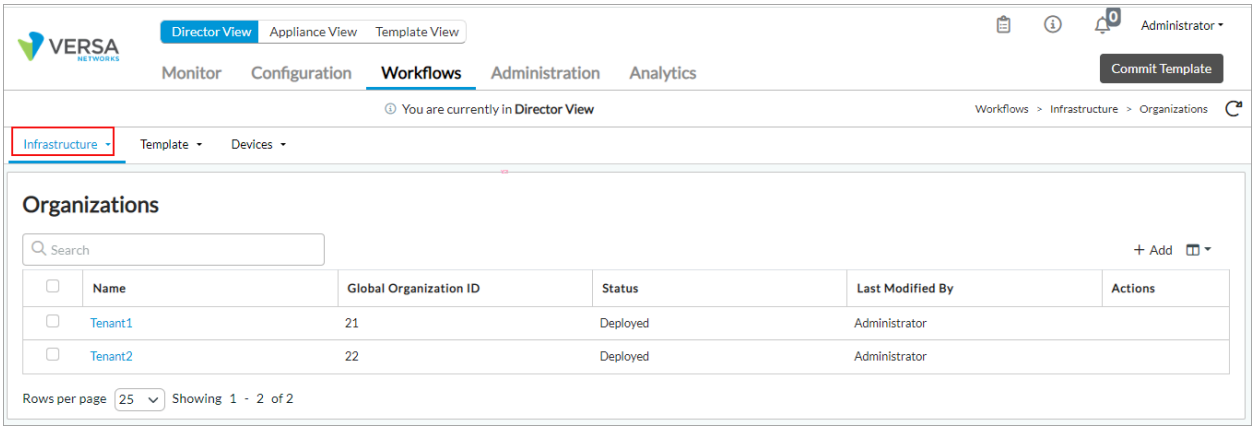
Create Customer Organizations

If your organization has customers (also called tenants), you configure organizations for them.

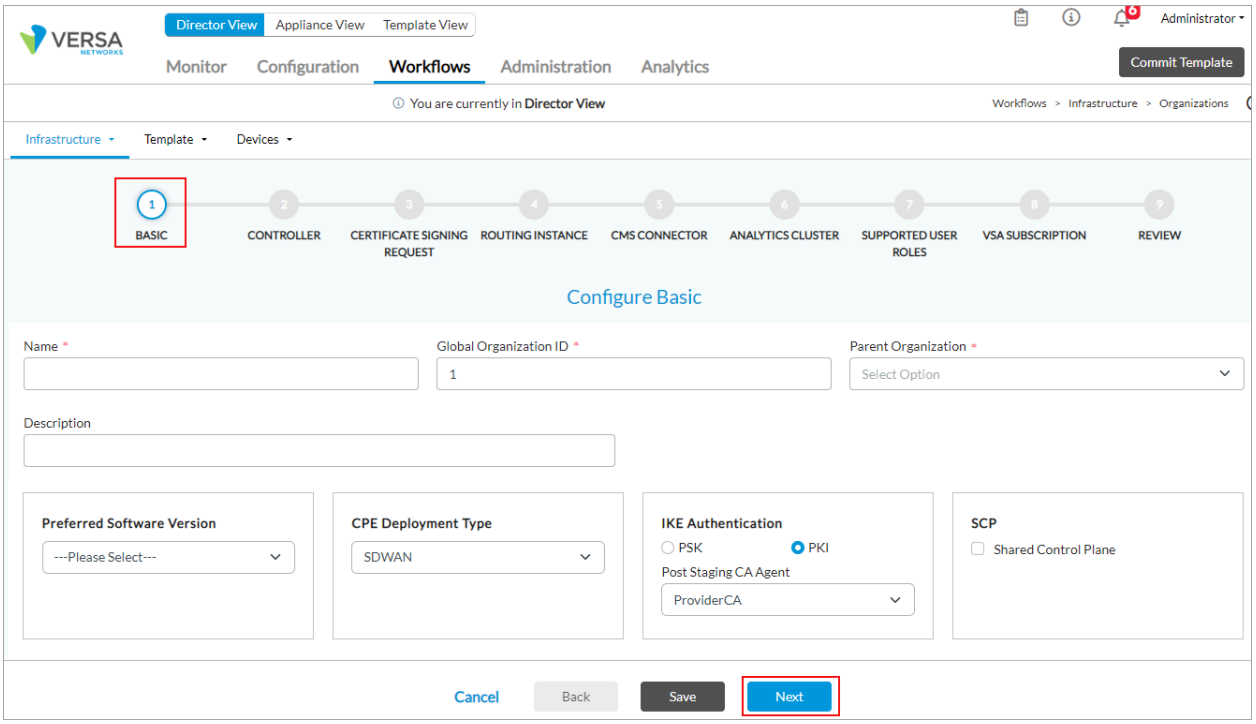
In Releases 22.1.1 and later, you use a workflow wizard to create a customer organization.

To add a customer organization:

1. In Director view, select the Workflows tab in the top menu bar.
2. Select Infrastructure > Organizations in the horizontal menu bar.

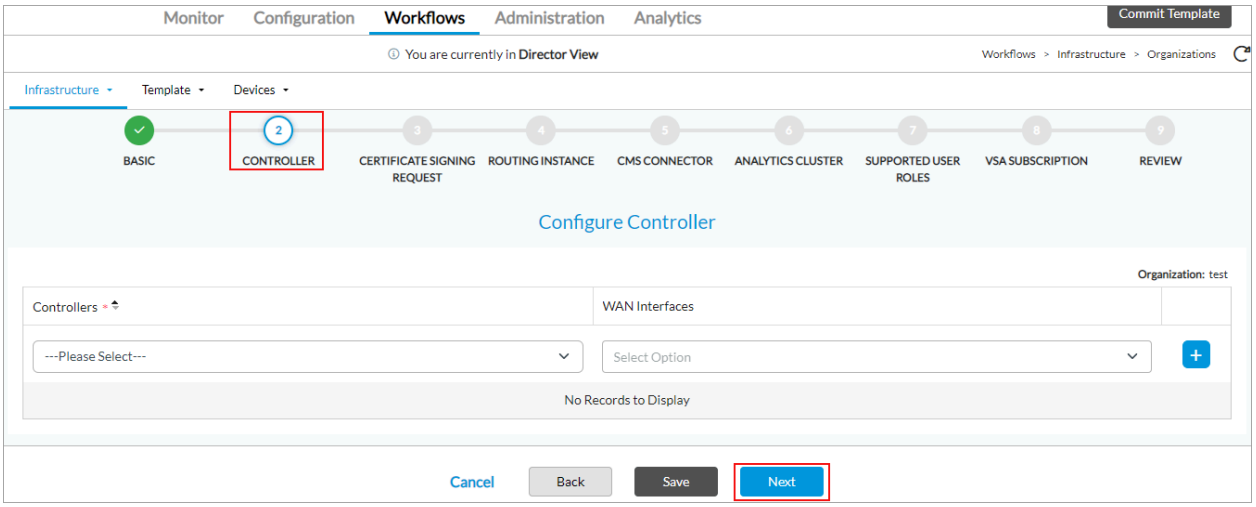


3. Click the Add icon.
4. Click Step 1, Basic. The Configure Basic screen displays. Enter information for the following fields.



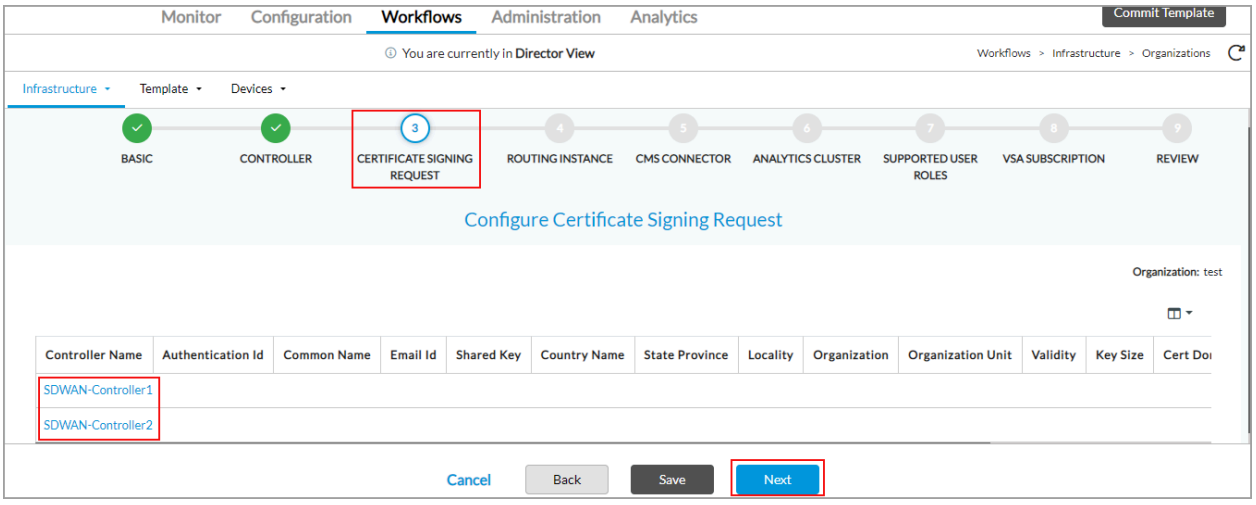
Field	Description
Name (Required)	Enter a name for the organization.
Global Organization ID	The value for this field is automatically populated with the next available organization identifier. You can change the value. The organization ID must be unique across the network. *Range:* 1 through 31
Parent	For multitenancy, select the name of the parent organization.
IKE Authentication	Select the IKE authentication mode, PSK or PKI. If you select PKI, you can select a CA profile. When you select PKI, The Certificate Signing Request screen displays as Step 3.
◦ PSK	Click to enable preshared key IKE authentication.
◦ PKI	Click to enable public key infrastructure authentication and select the staging and post stating CA agent.
◦ Staging CA Agent	Select the CA agent for certificate agent (CA) for staging templates. The profiles displayed are those that you created, as described in Configure a Common Certificate Authority.
◦ Post Staging CA Agent	Select the CA agent for certificate agent (CA) for post staging templates. The profiles displayed are those that you created, as described in Configure a Common Certificate Authority.
SCP	Shared control plane.
◦ Shared Control Plane	For multitenancy, click to have the organization share the control (management) plane with its parent organization or organizations. When you enable a shared control plane, the organization shares the control VR routing instance and the IPsec tunnels to the Controller nodes with its parent organization. The organization does not have either its own control VR routing instance or its own IPsec tunnels to the Controller nodes.
CPE Deployment Type	Select a CPE deployment type.

5. Click Save to save the configuration, or click Next to continue. The Step 2, Configure Controller screen displays. Enter information for the following fields.



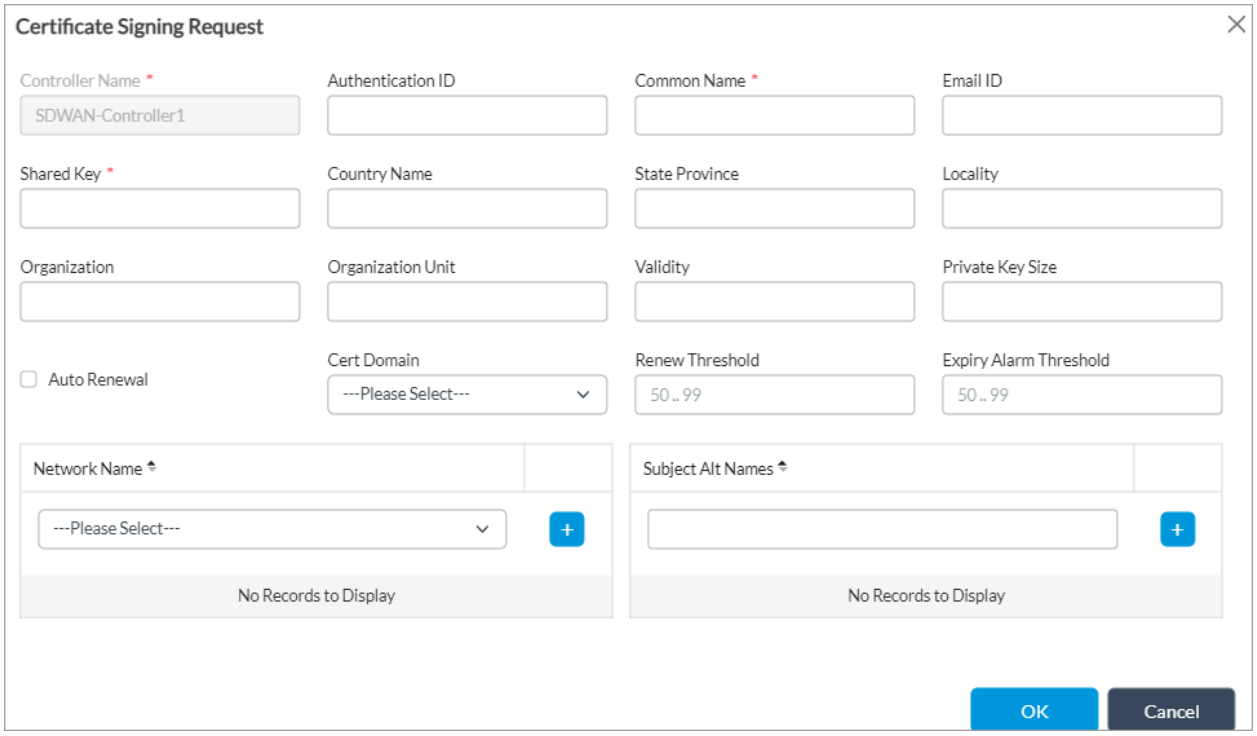
Field	Description
Controllers	Search for the Controller node or Controller nodes to associate with the organization, and click the + Add icon to add them.
WAN Interfaces	Select the WAN interface to associate with the organization or or click Select All and + Add icon to add the interface or interfaces.

6. Click Save to save the configuration, or click Next to continue. The Step 3, Configure Certificate Signing Request screen displays. Note that this screen displays only if you select PKI as the IKE authentication option in the Basic screen. This screen displays the Controller nodes associated with a common CA profile.



7. To update the certificate signing request (CSR), click the controller. The Certificate Signing Request popup screen displays. The parameters depend on the values for which the CA authenticates the CSR. Enter information for the

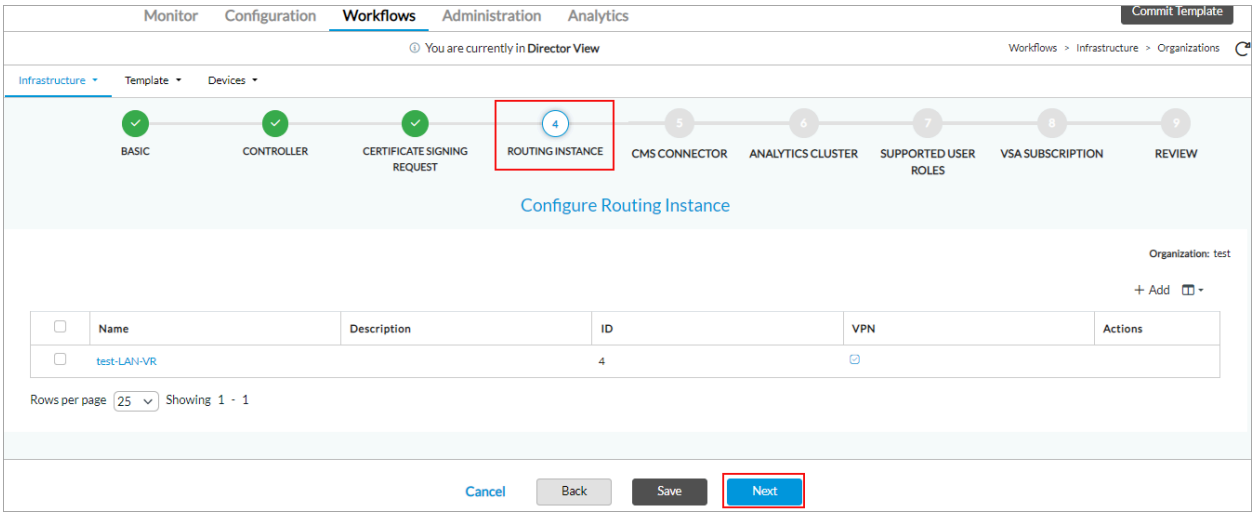
following fields.



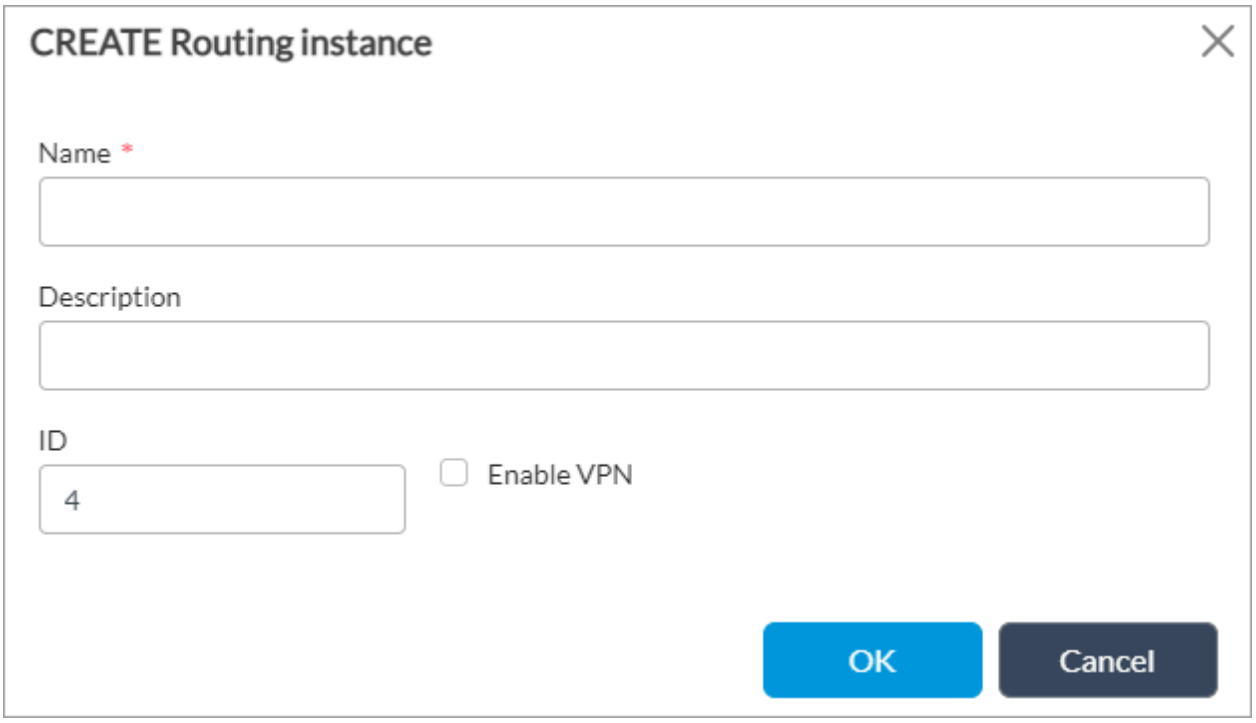
Field	Description
Controller Name	Displays the name of the Controller node
Authentication ID	Enter the authentication identifier for the CSR.
Common Name (Required)	Enter the name of the certificate. The name is an identity that you also must configure on the certificate authority server. Both names must match so that the CA server cam issue the certificate.
Email ID	Enter the email address of the user who downloads the certificate. This email address must be registered on the CA server.
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.
Country	Enter the two-letter ISO abbreviation for the country. For example, US.
State Province	Enter th state or province where the organization is legally located, for example, California. It is recommended that you avoid abbreviations.
Locality	Enter the city or locality where the organization is legally located. For example, Santa Clara or SC.
Organization	Enter the exact legal name of your organization. Do not abbreviate the organization name. For example, versa-networks.com.
Organization Unit	Enter the section of the organization. For example, IT.
Validity	Enter the validity length of the certificate, in days. For example, 365.
Private Key Size	Enter the size for generating a key pair.
Auto Renewal	Click to enable automatic renewal of the generated certificate.
Cert Domain	Select the domain to which the certificate applies. The certificate domain is either systemwide or per tenant.
Renew Threshold	Enter the certificate renewal threshold value, which is a percentage of the certificate validity time. *Range:* 50 through 99 percent

	Default: 75 percent
Expiry Alarm Threshold	Enter the certificate expiration alarm threshold value, which is a percentage of the certificate validity time. *Range:* 50 through 99 percent *Default:* 80 percent
Network Name	Select the type of network to use.
Subject Alternate Name	Enter the DNS hostname, and then click the + Add icon to add it. It can be the domain name, a wildcard, or an IP address.

8. Click Save to save the configuration, or click Next to continue. The Step 4, Configure Routing Instance screen displays where you can define virtual routing instances for the organization.

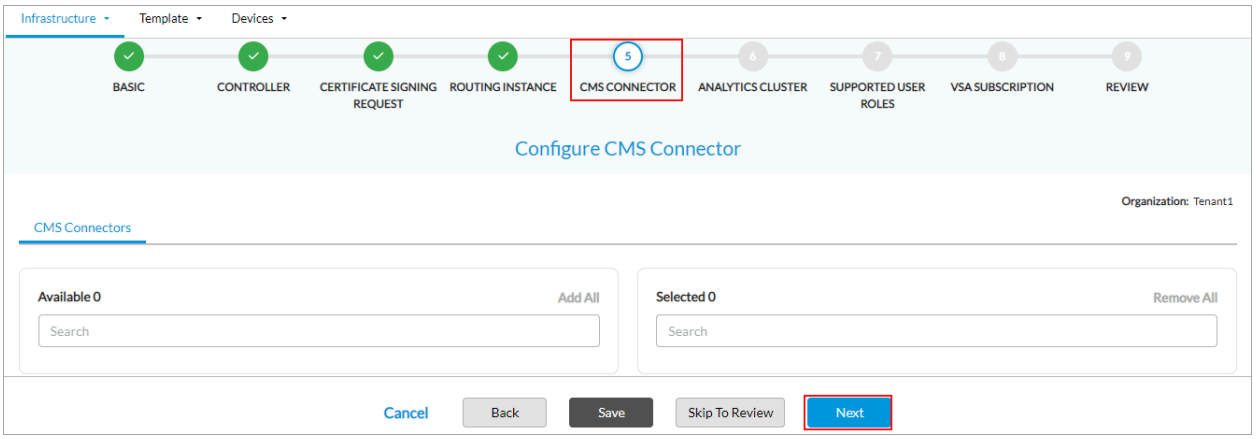


9. Click the + Add icon to add routing instances. The Configure Create Routing Instance popup screen displays. Enter information for the following fields.



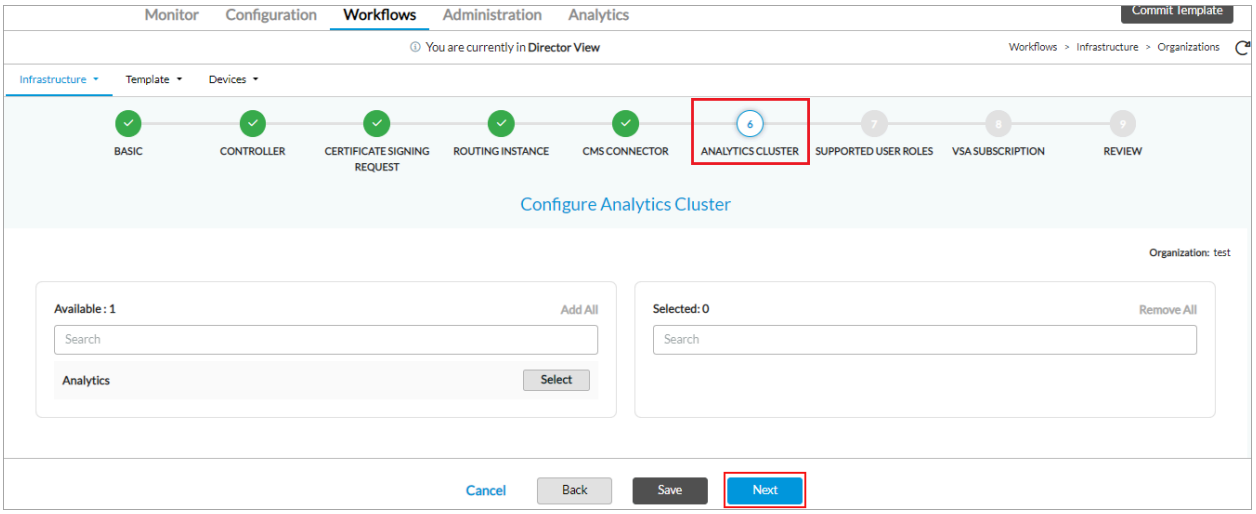
Field	Description
Name (Required)	Enter a name for the routing instance.
Description	Enter a text description for the routing instance.
ID	Enter a numeric identifier for the routing instance.
VPN	Click to enable a VPN on the routing instance.

10. Click Save to save the configuration, or click Next to continue. The Step 5, Configure CMS Connector screen displays. Enter information for the following fields.

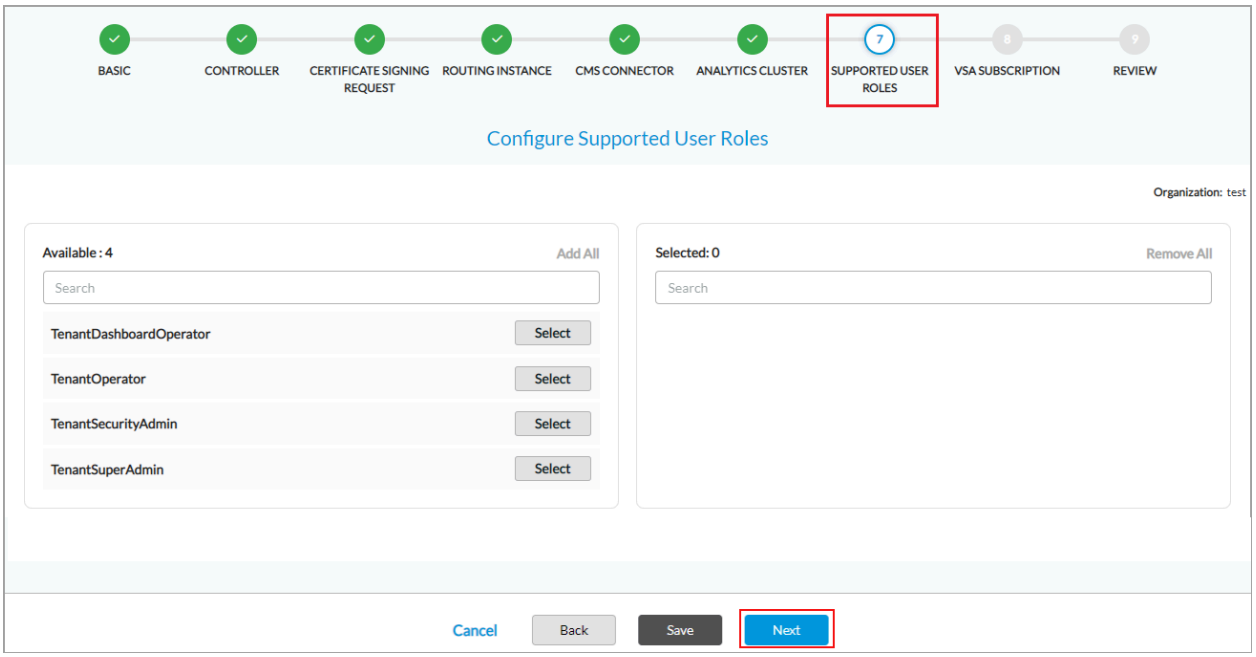


Field	Description
Available	Search for the CMS connector or connectors to associate with the organization, and then click Add All to select them.
Selected	Lists the connectors associated with the organization.

11. Click Save to save the configuration, or click Next to continue. The Step 6, Configure Analytics Cluster screen displays. Select the Analytics cluster or clusters to associate with the organization.

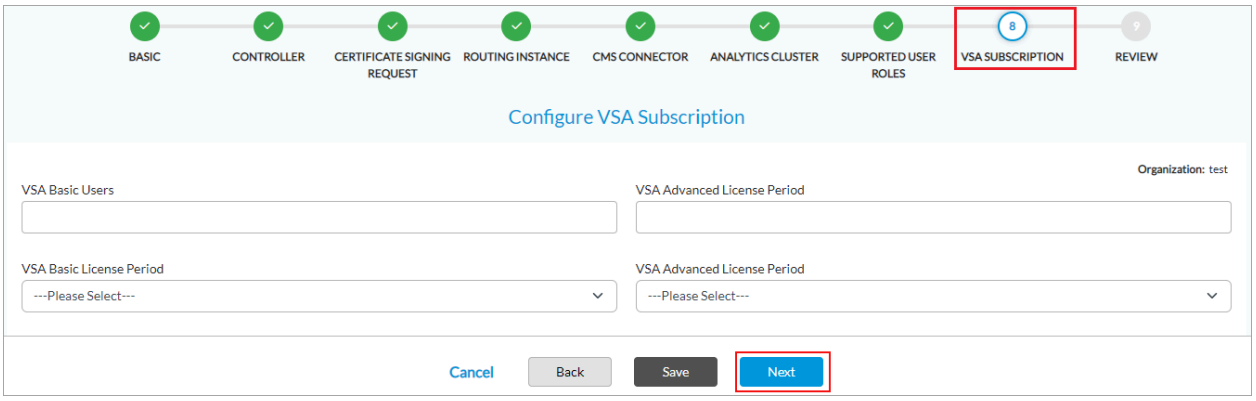


12. Click Save to save the configuration, or click Next to continue. The Step 7, Configure Supported User Roles screen displays. Enter information for the following fields.



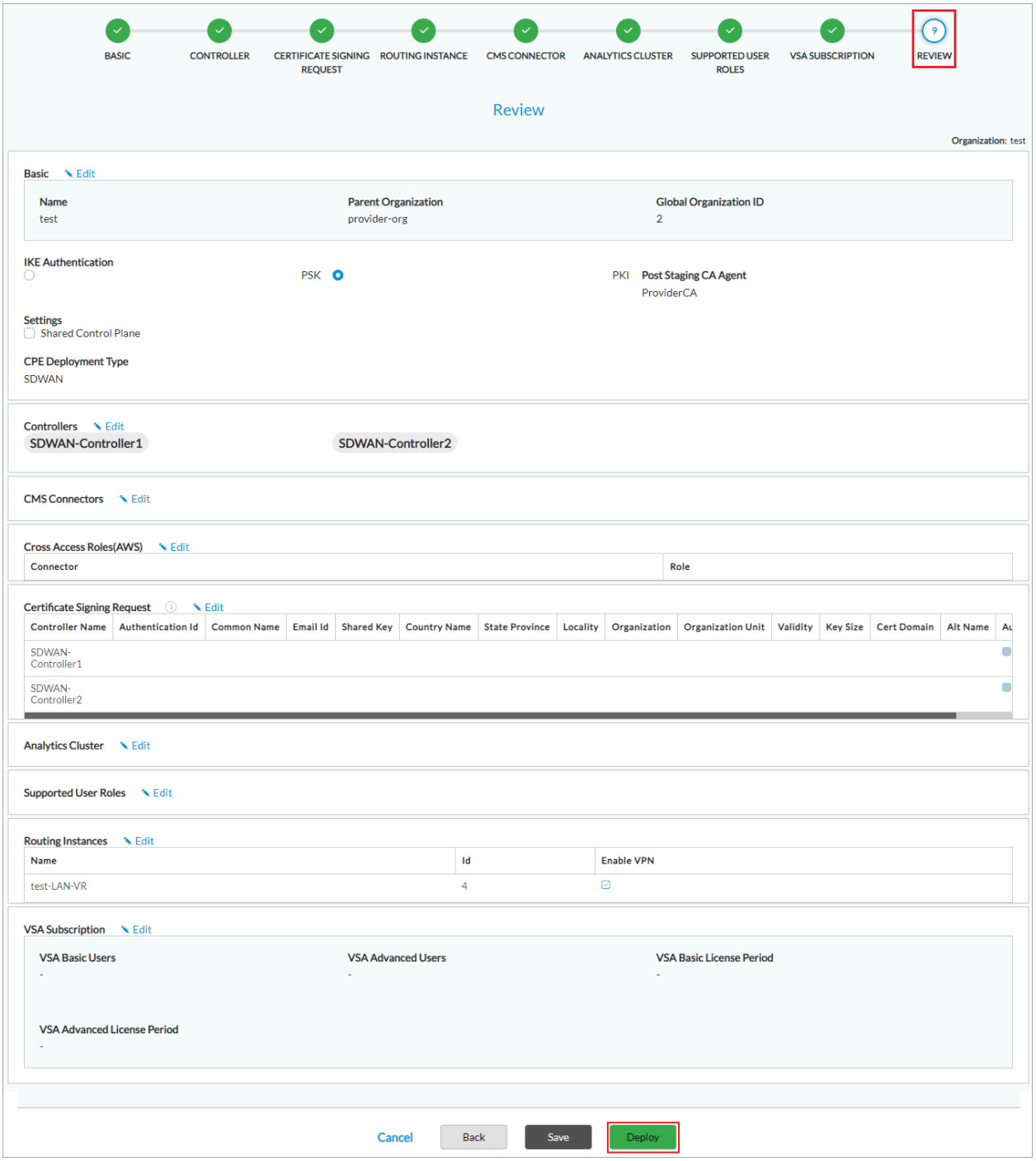
Field	Description
Available	Search for the user role or roles to associate with the organization, and then click Add All to select them.
Selected	Lists the roles associated with the organization.

13. Click Save to save the configuration, or click Next to continue. The Step 8, Configure VSA Subscription screen displays. You can configure the number of Versa Secure Access (VSA) licenses for both basic and advanced users per organization using Versa Director. Enter information for the following fields.



Field	Description
VSA Basic Users	Enter the number of VSA basic users for the organization. The minimum number of basic users is 50.
VSA Advanced Users	Enter the number of VSA advanced users for the organization. The minimum number of advanced users is 50.
VSA Basic License Period	Enter the license period for VSA basic users. The license period can be 1, 3, or 5 years.
VSA Advanced License Period	Enter the license period for VSA basic users. The license period can be 1, 3, or 5 years.

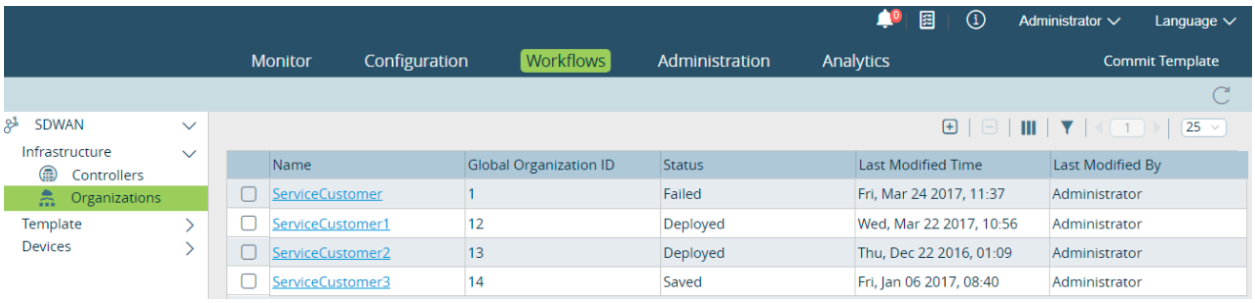
14. Click Save to save the configuration, or click Next to continue. The Step 8, Review screen displays.



15. Click Save to add the organization.
16. Click Deploy to onboard the organization. The main pane displays the new organization as well as other organizations.

Create Customer Organizations For Releases 21.2 and Earlier

The procedure for creating customer organizations is the same as for creating provider organizations, as described in Create Provider Organizations above. The only difference is that in the Create Organization popup window, in the Parent field, you select the name of the provider organization. When you click Deploy to create the customer organization, the main pane shows the customer organizations.



When a provider organization has two or more tenants, you configure multitenancy by associating the tenant organizations with a Controller node. For more information, see Configure Multitenancy.

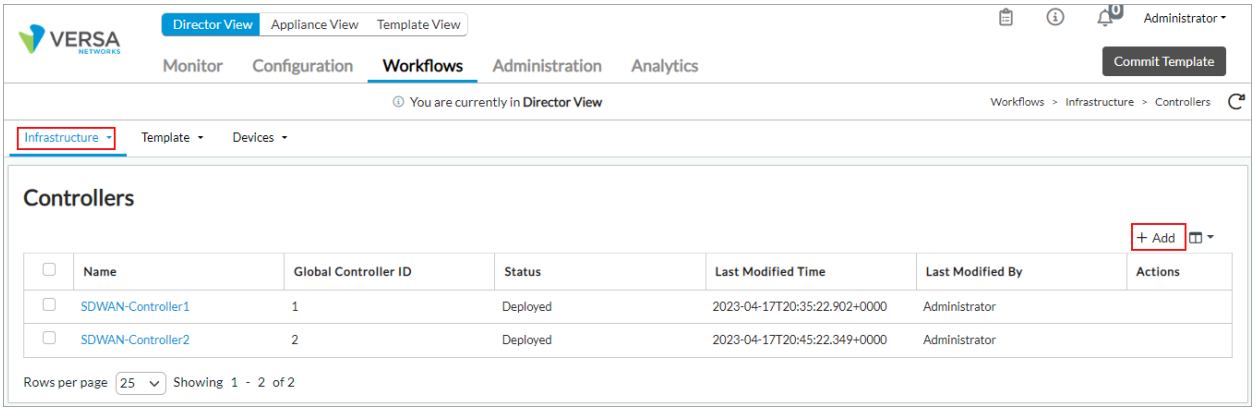
Add a Controller Node

You can deploy a Controller node on a bare-metal server or on a virtual machine (VM). For redundancy, configure two Controller nodes that operate in active-active mode.

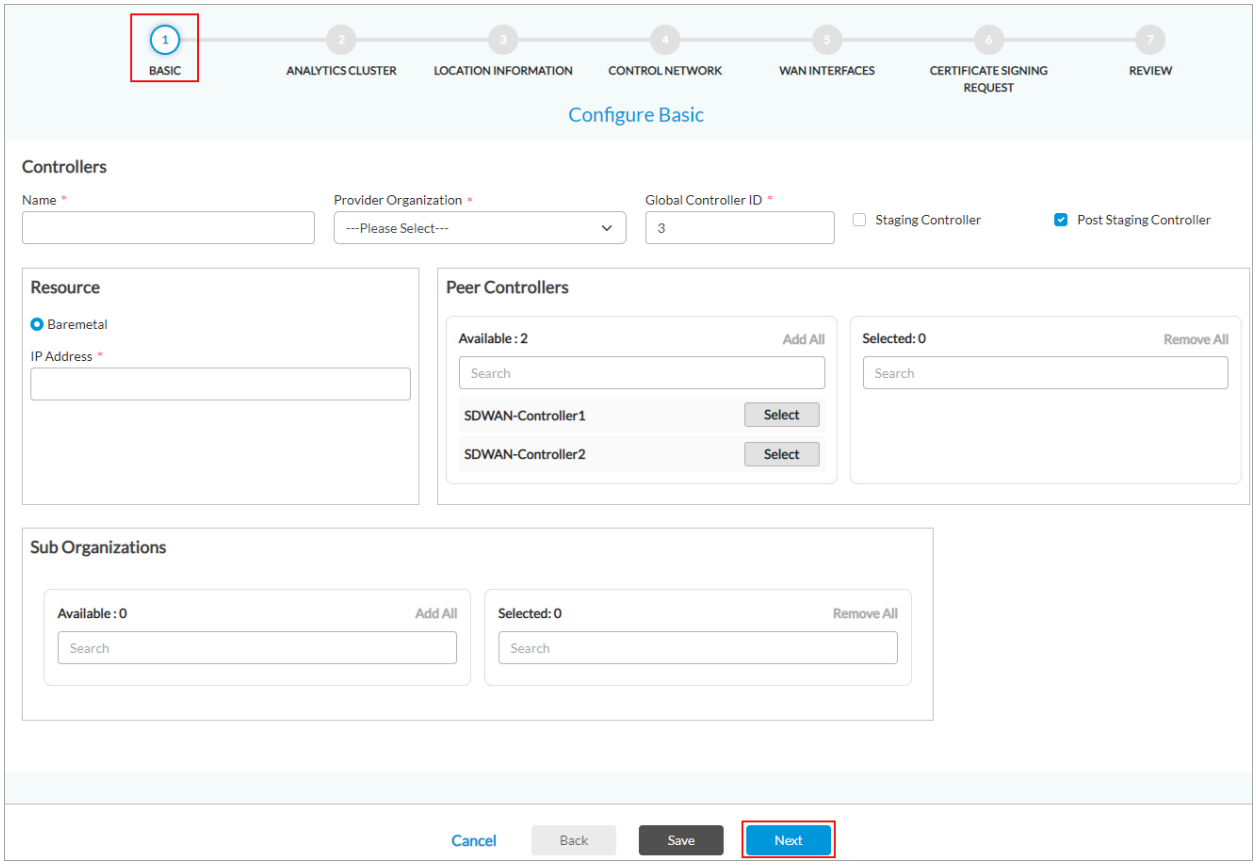
In Releases 22.1.1 and later, you use a workflow wizard to create a Controller node.

To add a Controller node:

1. In Director view, select the Workflows tab in the top menu bar.
2. Select Infrastructure > Controllers in the horizontal menu bar.

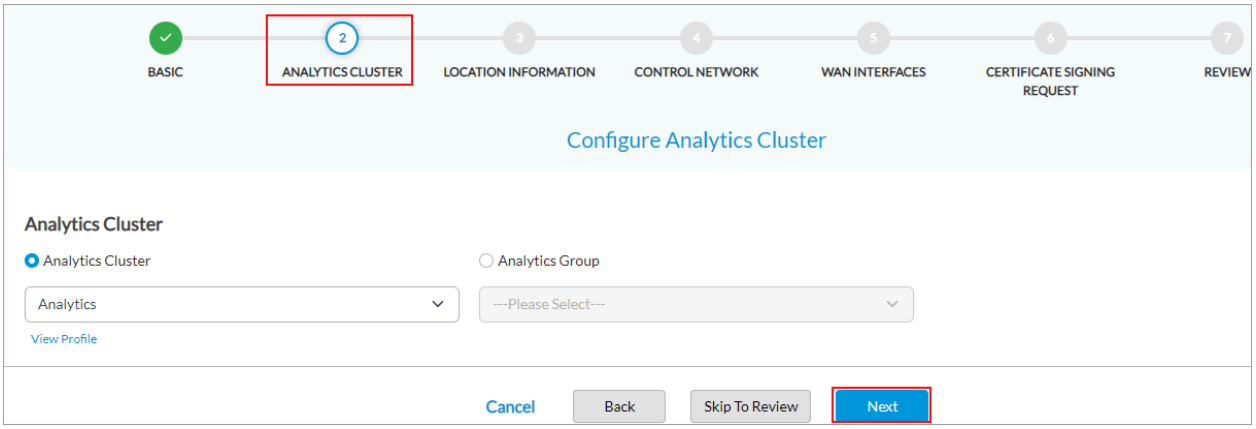


3. Click the Add icon.
4. Click Step 1, Basic. The Configure Basic screen displays. Enter information for the following fields.



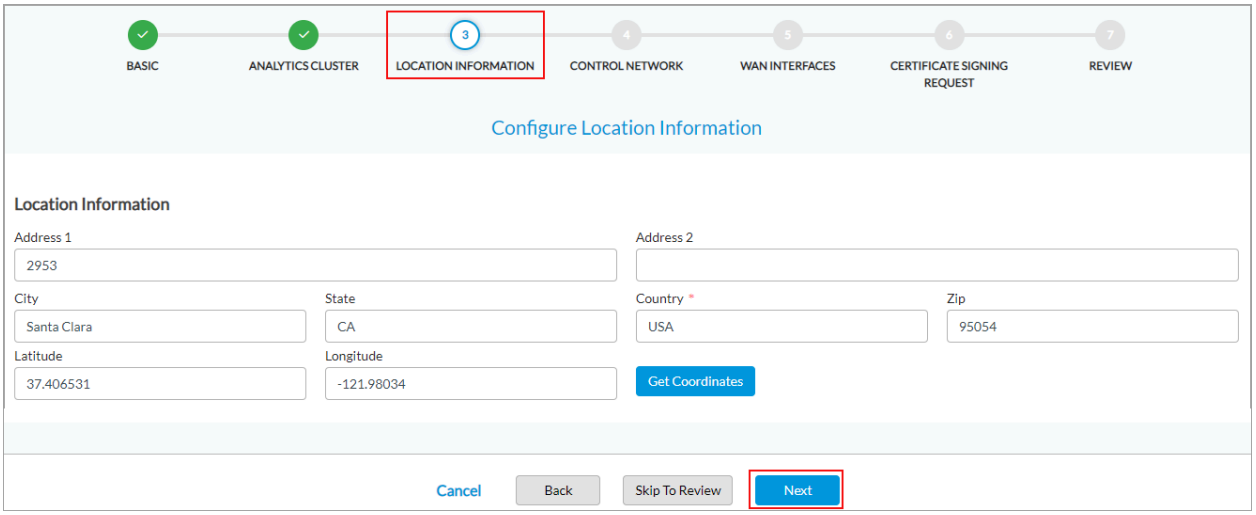
Field	Description
Name	Enter a name for the Controller node.
Provider Organization	Select the name of the provider organization. When you select a provider organization that uses PKI-based IKE authentication, the Certificate Signing Request screen displays as Step 6. For more information, see Configure a Common Certificate Authority.
Global Controller ID	ID assigned to the controller. The system populates the value automatically with the next available ID. You can change it to a different available value. *Range:* 1 through 511
Staging Controller	Click to enable the Controller node to be a staging Controller node.
Post-Staging Controller	Click to enable the Controller node to be a post-staging Controller node
Resource (Group of Fields)	
◦ Bare Metal	Click to deploy the Controller node on a bare-metal platform.
◦ IP Address	Enter the IP address of the interface address to the bare-metal server or VM.
Peer Controllers	When you are configuring two Controller nodes for active-active mode (for redundancy), select the Controller node that is the peer of this new Controller node. When you deploy the new Controller node, the configuration is pushed to both the new Controller node and the peer Controller node. The new Controller node then establishes an IPsec tunnel and an MP-BGP session with the peer Controller node that the two Controller nodes use for communication between each other, and they form a mesh of route reflectors.
Suborganizations	Select the suborganization to autoprovision on the Controller node.

5. Click Save to save the configuration, or click Next to continue. The Step 2, Configure Analytics Cluster screen displays. Enter information for the following fields.



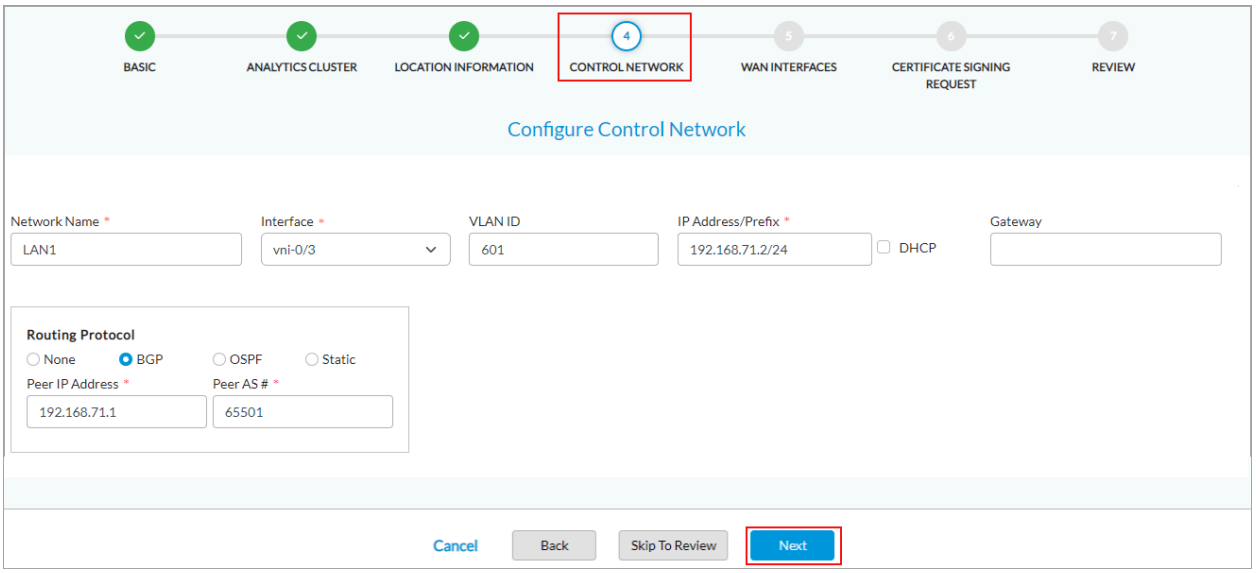
Field	Description
Analytics Cluster	Click to select a configured analytics cluster. The Controller node sends the analytics logs to the selected cluster. If you select this, Analytics Group is disabled and vice versa. Click + Add New to create an analytics cluster.
Analytics Group	Click to select a configured analytics group. The Controller node sends the analytics logs to the selected group. Click + Add New to create an analytics group.

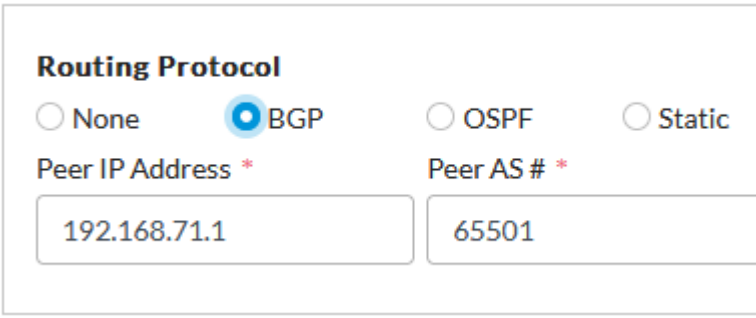
6. Click Save to save the configuration, or click Next to continue. The Step 3, Configure Local Information screen displays. Enter the Controller's location information, and then click Get Coordinates to automatically populate the latitude and longitude from the controller address.

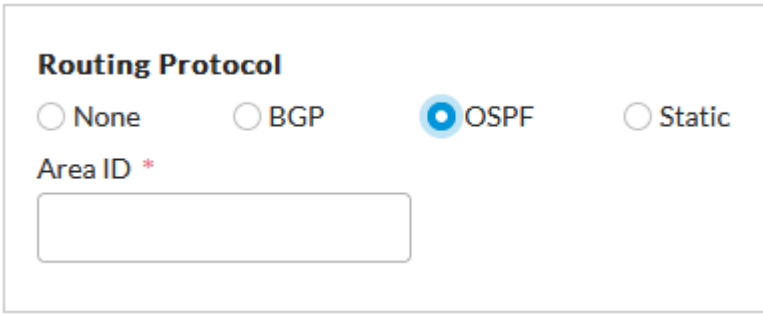
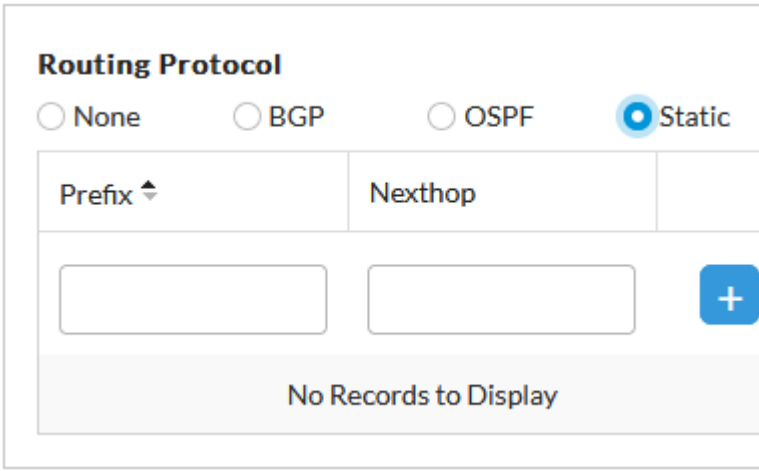


7. Click Save to save the configuration, or click Next to continue. The Step 4, Configure Control Network screen displays. You can configure the Controller node's control network interface, which is the interface that connects the Controller node to the Director node and that facilitates communication from the Director node, through the

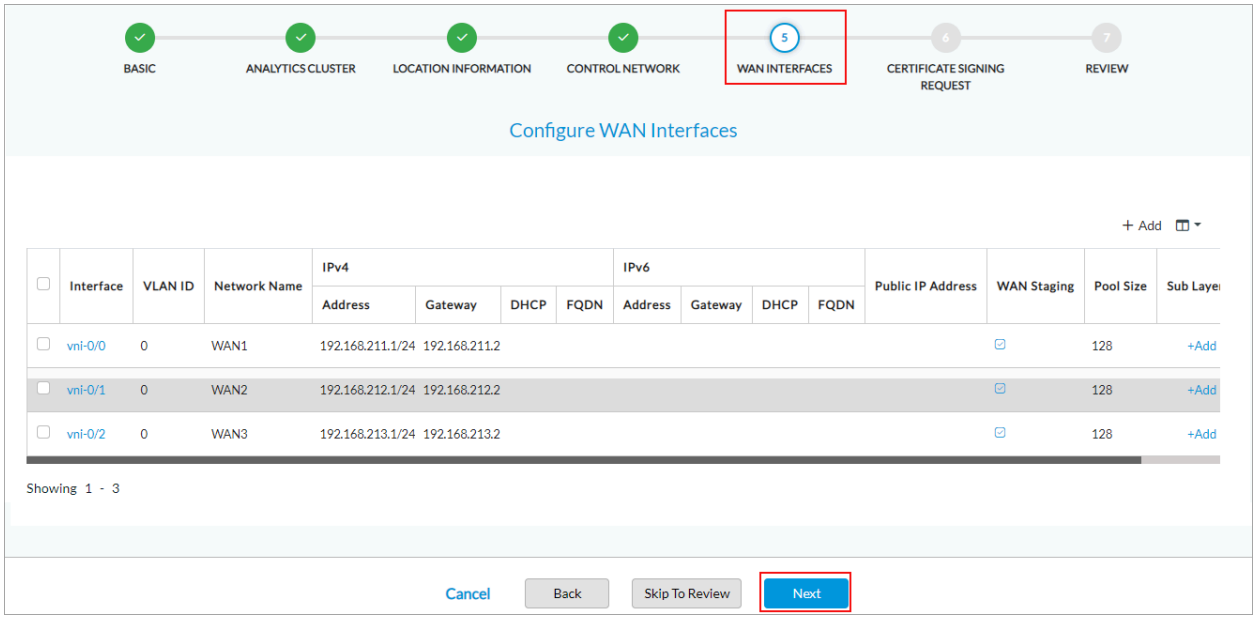
Controller node, to the branch VOS devices. Enter information for the following fields.



Field	Description
Network Name	Enter a name for the network.
Interface	Select the interface to use for the network.
VLAN ID	Enter the VLAN ID of the network.
IP Address/Prefix	Enter the IP prefix and prefix length of the network.
DHCP	Click to enable DHCP, to automatically allocate the network IP address.
Gateway	Enter the IP address of the gateway device.
Routing Protocol (Group of Fields)	Select the routing protocol to use.
◦ None	Click to not use a routing protocol.
◦ BGP	Click to use BGP. Enter information for the following fields.  ◦ Peer IP Address—Enter the IP address of the BGP routing peer. ◦ Peer AS Number—Enter the peer's AS number.
◦ OSPF	Click to use OSPF. Enter information for the following fields.

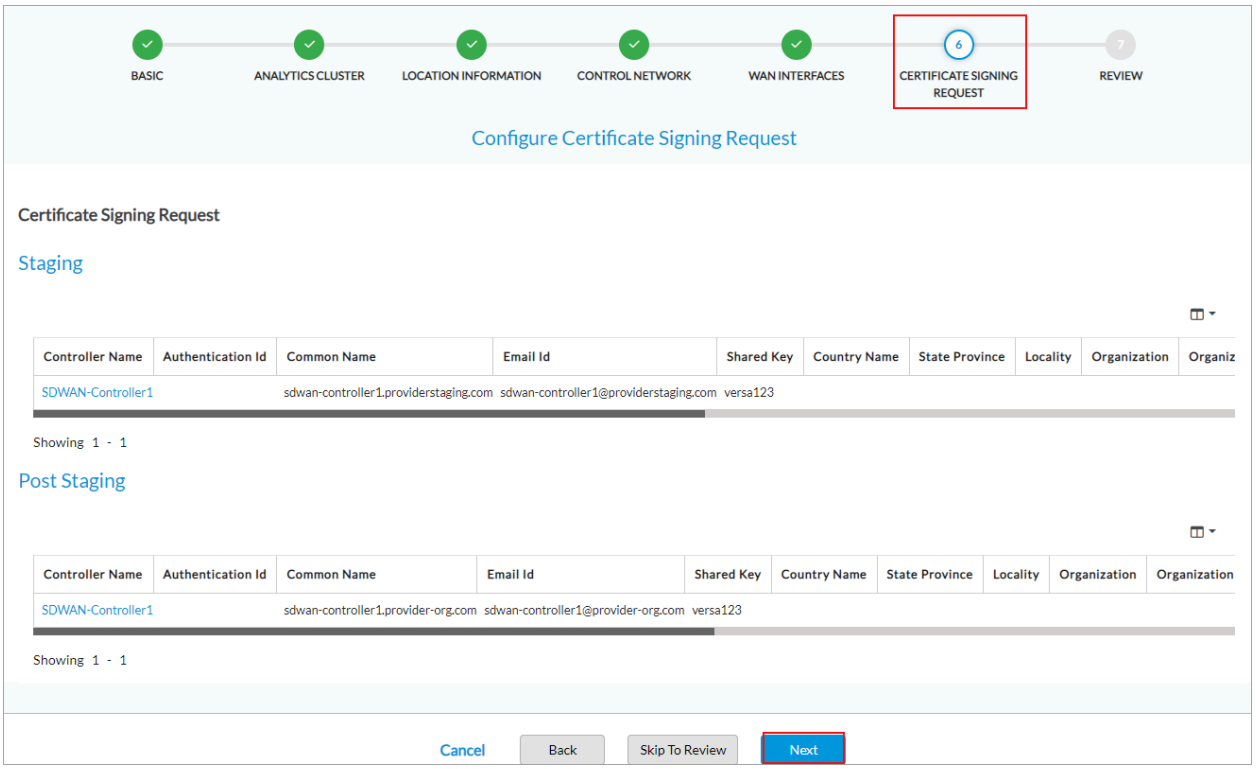
	 ◦ Area ID—Enter the Controller's area ID.
◦ Static	Click to use static routes. Enter information for the following fields.  ◦ Prefix—Enter the prefix for the static route. ◦ Next Hop—Enter the next hop for the static route. Then, click the Add icon.

8. Click Save to save the configuration, or click Next to continue. The Step 5, Configure Control Network screen displays. You enter information about the interfaces that the Controller uses to communicate with remote branches. Enter information for the following fields.

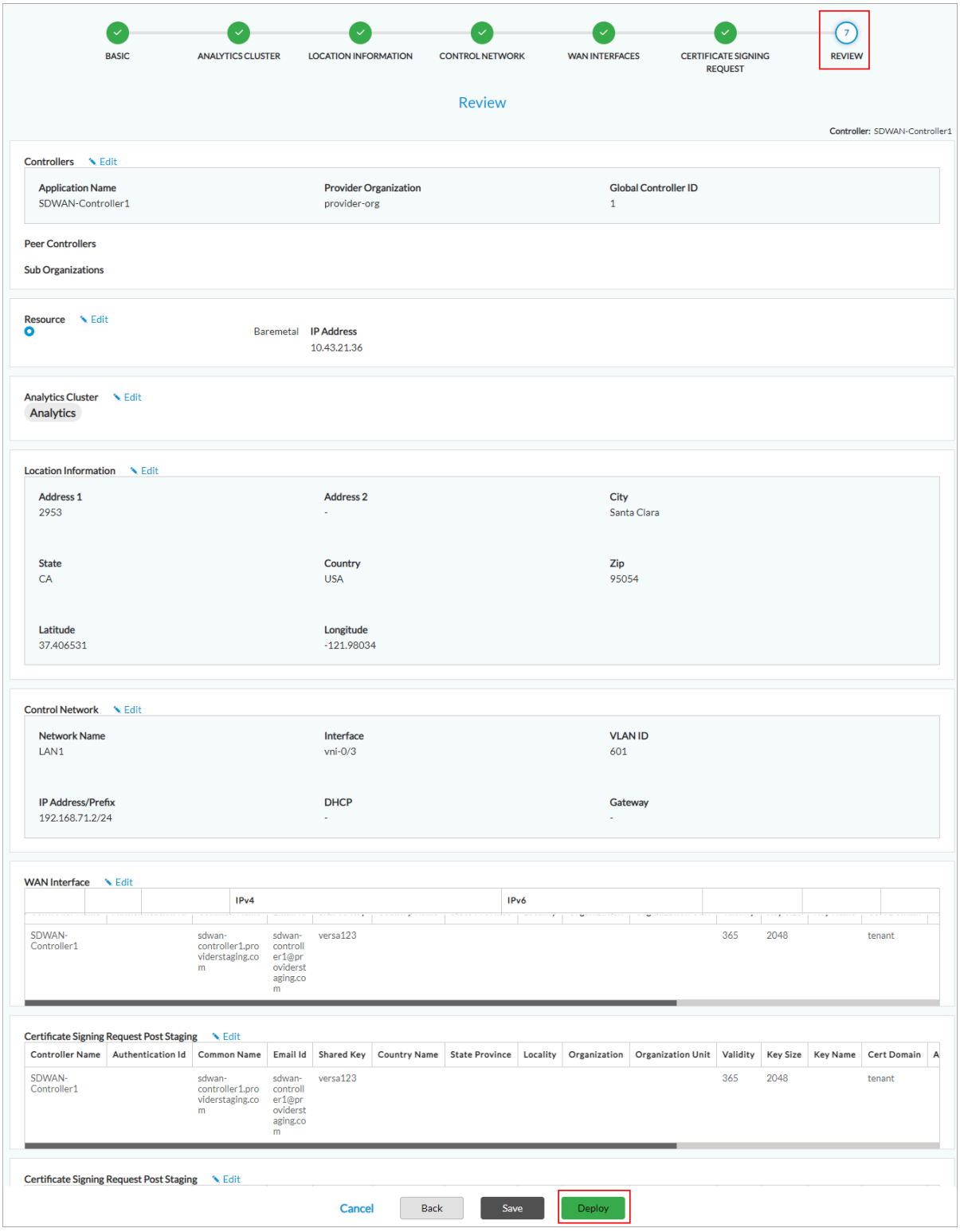


Field	Description
Interface	Displays the Controller interfaces. Only vni interfaces are displayed.
VLAN ID	For VLAN interfaces, select the VLAN ID of the interface.
Network Name	Select the name of the network.
IPv4 (Group of Fields)	
◦ Address	Enter the IPv4 IP address of the interface.
◦ Gateway	Enter the IPv4 address of the gateway.
◦ DHCP	Click to enable DHCP, to automatically allocate addresses.
◦ FQDN	Enter the fully qualified domain name for the Controller.
IPv6 (Group of Fields)	
◦ Address	Enter the IPv6 IP address of the interface.
◦ Gateway	Enter the IPv6 address of the gateway.
◦ DHCP	Click to enable DHCP, to automatically allocate addresses.
◦ FQDN	Enter the fully qualified domain name for the Controller.
Public IP Address	Enter the public IP address of the interface.

9. Click Save to save the configuration, or click Next to continue. The Step 6, Configure Certificate Signing Request screen displays. Note that this screen displays if you select a provider organization that uses PKI-based IKE authentication on Step 1, Configure Basic screen. Staging and/or post staging Controllers display based on your selection in Step 1, Configure Basic screen. Click on the Controller to view the CSR details.



10. Click Save to save the configuration, or click Next to continue. The Step 8, Review screen displays.



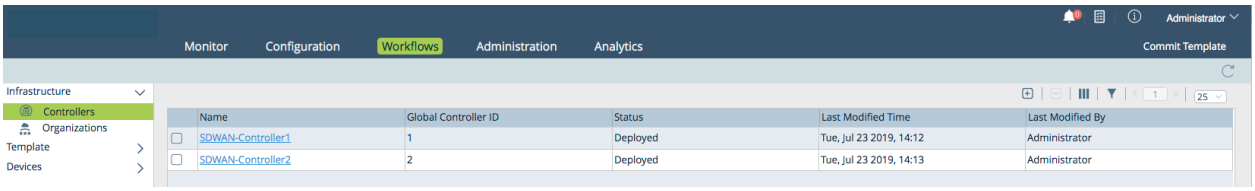
a. Click Save to add the Controller.

b. Click Deploy to activate the Controller node.

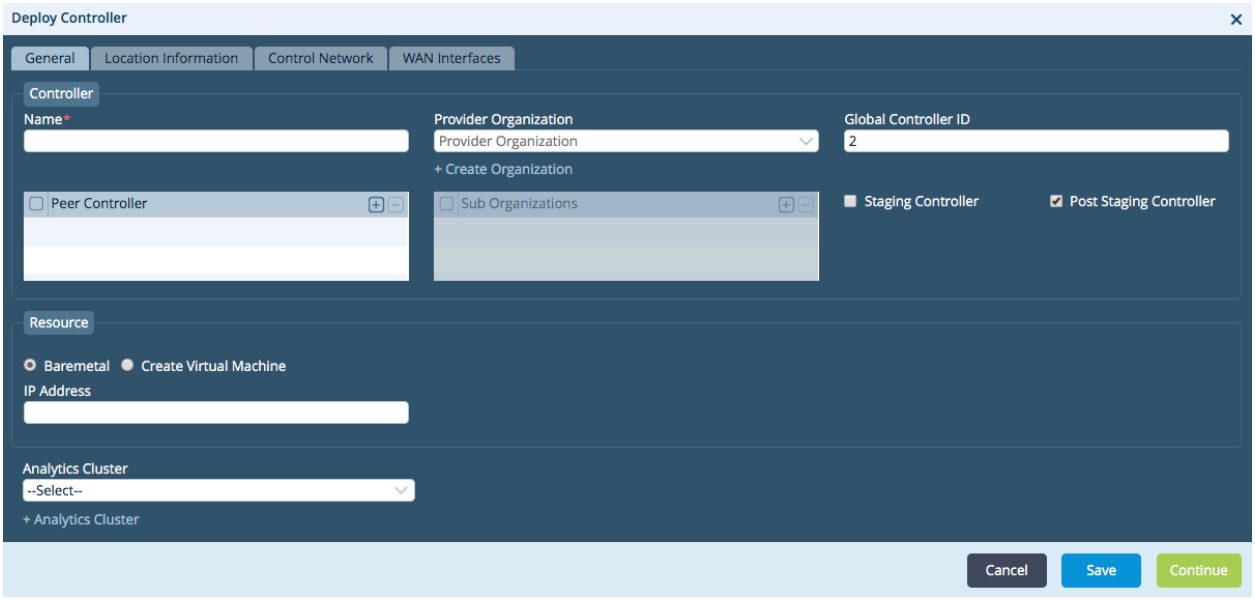
Add a Controller Node for Releases 21.2 and Earlier

To add a Controller node:

1. In Director view, select the Workflows tab in the top menu bar.
2. Select Infrastructure > Controllers in the left menu bar.
3. Click the Add icon. The Deploy Controller popup window displays.



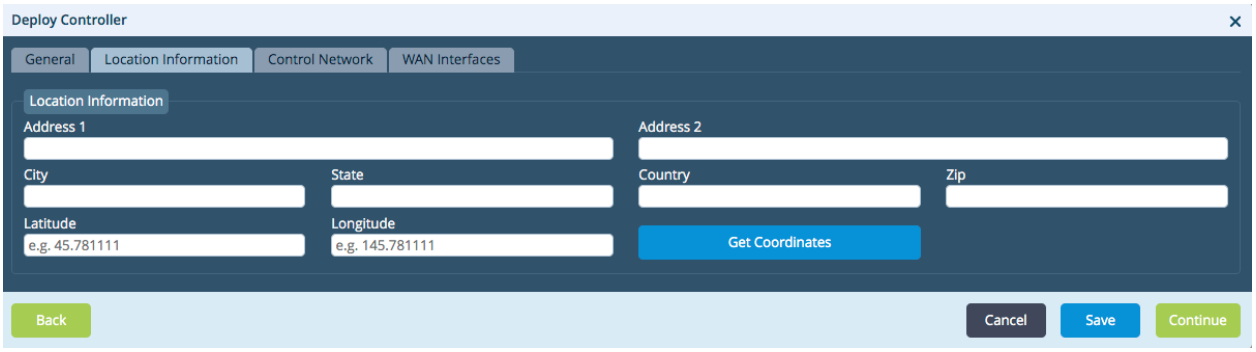
4. Select the General tab, and enter information for the following fields.



Field	Description
Name	Enter a name for the Controller node.
Provider Organization	Select the name of the provider organization.
Global Controller ID	ID assigned to the controller. The system populates the value automatically with the next available ID. You can change it to a different available value. *Range:* 1 through 511
Peer Controller	When you are configuring two Controller nodes for active-active mode (for redundancy), select the Controller node that is the peer of this new Controller node. When you deploy the new Controller node, the configuration is pushed to both the new Controller node and the peer Controller node. The new Controller node then establishes an IPsec tunnel and an MP-BGP session with the peer Controller node that the two Controller nodes use for communication between each other, and they form a mesh of route reflectors.
Suborganizations	Select the suborganization to autoprovision on the Controller node.
Staging Controller	Click to enable the Controller node to be a staging Controller node.
Post-Staging Controller	Click to enable the Controller node to be a post-staging Controller node
Bare Metal	Click to deploy the Controller node on a bare-metal platform.
Create Virtual Machine	Click to deploy the Controller node on a VM.
IP Address	Enter the IP address of the interface address to the bare-metal server or VM.
Analytics Cluster	Select the name of a configured analytics cluster. The Controller node sends the analytics logs to the selected cluster.

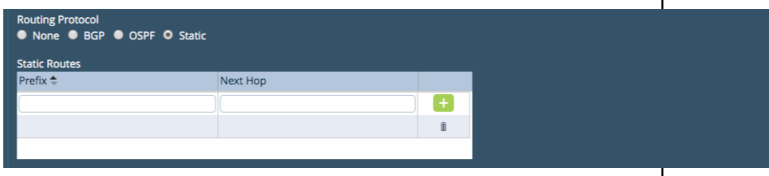
5. Click Continue.
6. Select the Location Information tab. Enter the Controller's location information, and then click Get Coordinates to

automatically populate the latitude and longitude from the controller address.

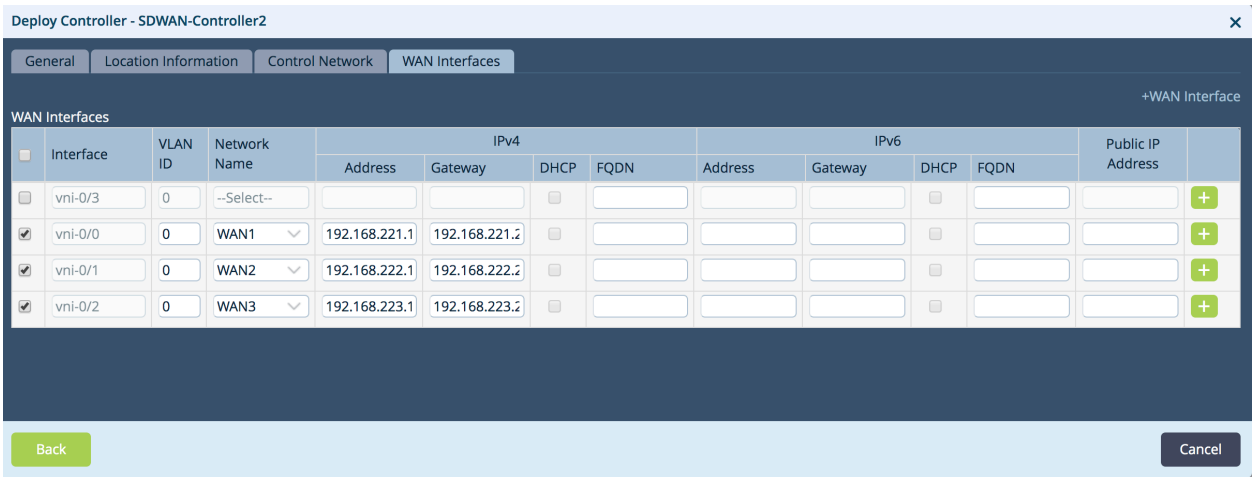


7. Click Continue.
8. Select the Control Network tab to configure the Controller node's control network interface, which is the interface that connects the Controller node to the Director node and that facilitates communication from the Director node, through the Controller node, to the branch VOS devices. Enter information for the following fields.

Field	Description
Network Name	Enter a name for the network.
Interface	Select the interface to use for the network.
VLAN ID	Enter the VLAN ID of the network.
IP Address/Mask	Enter the IP prefix and prefix length of the network.
DHCP	Click to enable DHCP, to automatically allocate the network IP address.
Gateway	Enter the IP address of the gateway device.
Routing Protocol (Group of Fields)	Select the routing protocol to use.
◦ None	Click to not use a routing protocol.
◦ BGP	Click to use BGP. Enter information for the following fields.  ◦ Peer IP Address—Enter the IP address of the BGP routing peer. ◦ Peer AS Number—Enter the peer's AS number.
◦ OSPF	Click to use OSPF. Enter information for the following fields.  ◦ Area ID—Enter the Controller's area ID.
◦ Static	Click to use static routers. Enter information for the following fields.

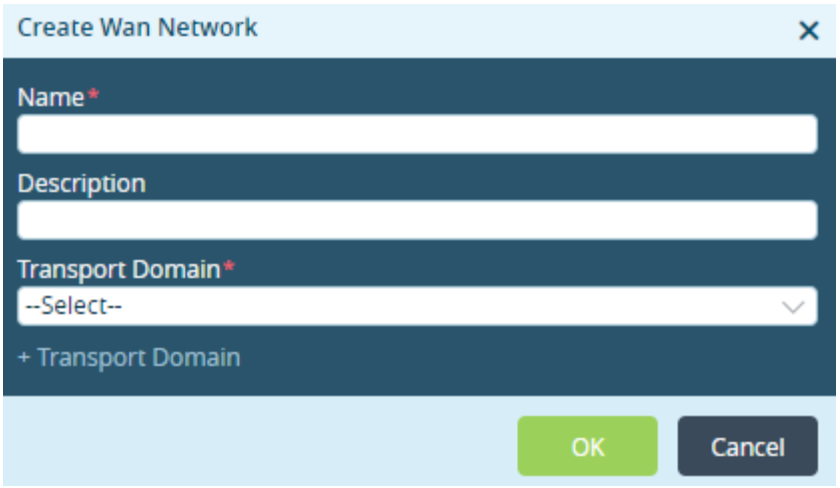
	 ◦ Prefix—Enter the prefix for the static route. ◦ Next Hop—Enter the next hop for the static route. Then, click the Add icon.

9. Click Continue.
10. Select the WAN Interfaces tab to enter information about the interfaces that the Controller uses to communicate with remote branches. Enter information for the following fields.



Field	Description
Interface	Displays the Controller interfaces. Only vni interfaces are displayed.
VLAN ID	For VLAN interfaces, select the VLAN ID of the interface.
Network Name	Select the name of the network.
IPv4 (Group of Fields)	
◦ Address	Enter the IPv4 IP address of the interface.
◦ Gateway	Enter the IPv4 address of the gateway.
◦ DHCP	Click to enable DHCP, to automatically allocate addresses.
◦ FQDN	Enter the fully qualified domain name for the Controller.
IPv6 (Group of Fields)	
◦ Address	Enter the IPv6 IP address of the interface.
◦ Gateway	Enter the IPv6 address of the gateway.
◦ DHCP	Click to enable DHCP, to automatically allocate addresses.
◦ FQDN	Enter the fully qualified domain name for the Controller.
Public IP Address	Enter the public IP address of the interface.

11. Click + WAN Interface to create an interface. Enter information for the following fields.



Field	Description
Name	Enter a name for the WAN interface.
Description	Enter a text description for the interface.
Transport Domain	Select the transport domain to which the WAN interface belongs.

12. Click +Transport Domain to create a transport domain. Enter information for the following fields.

Field	Description
Name	Enter a name for the transport domain.
Description	Enter a text description for the transport domain.
Transport Domain ID	Enter the ID of the transport domain.

13. Click OK.
14. Click Deploy to activate the Controller node

To view the status of the Controller creation and activation, click the Tasks icon.

Create Device Templates

Device templates are a baseline configuration that can be deployed across branches, saving time and effort when you are configuring and deploying similar services across a branch network. There are two types of device templates:

- Staging templates—You typically create staging templates to use when testing VOS devices in a preproduction network or proof-of-concept (POC) situation to ensure that the devices and the basic configuration work properly.

Because staging templates are for testing, you can configure only a limited set of features with them. You can create staging templates for WAN interfaces only, not for LAN interfaces.

- Post-staging templates—These are production templates that contain the complete configuration required to deploy network services on VOS branch devices. Post-staging templates can include configurations for both WAN and LAN interfaces.

You can associate a group of devices with one staging template and one post-staging template.

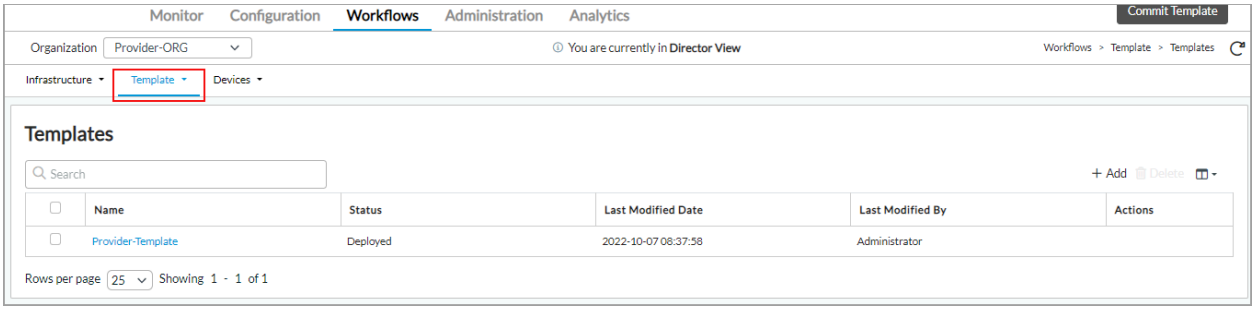
This section describes how to create post-staging (production) device templates. For information about configuring staging (testing) device templates, see Create Staging Templates in Create and Manage Staging and Post-Staging Templates.

A post-staging template contains the complete configuration for deploying network services at the branch level. You can configure post-staging templates for both LAN and WAN interfaces.

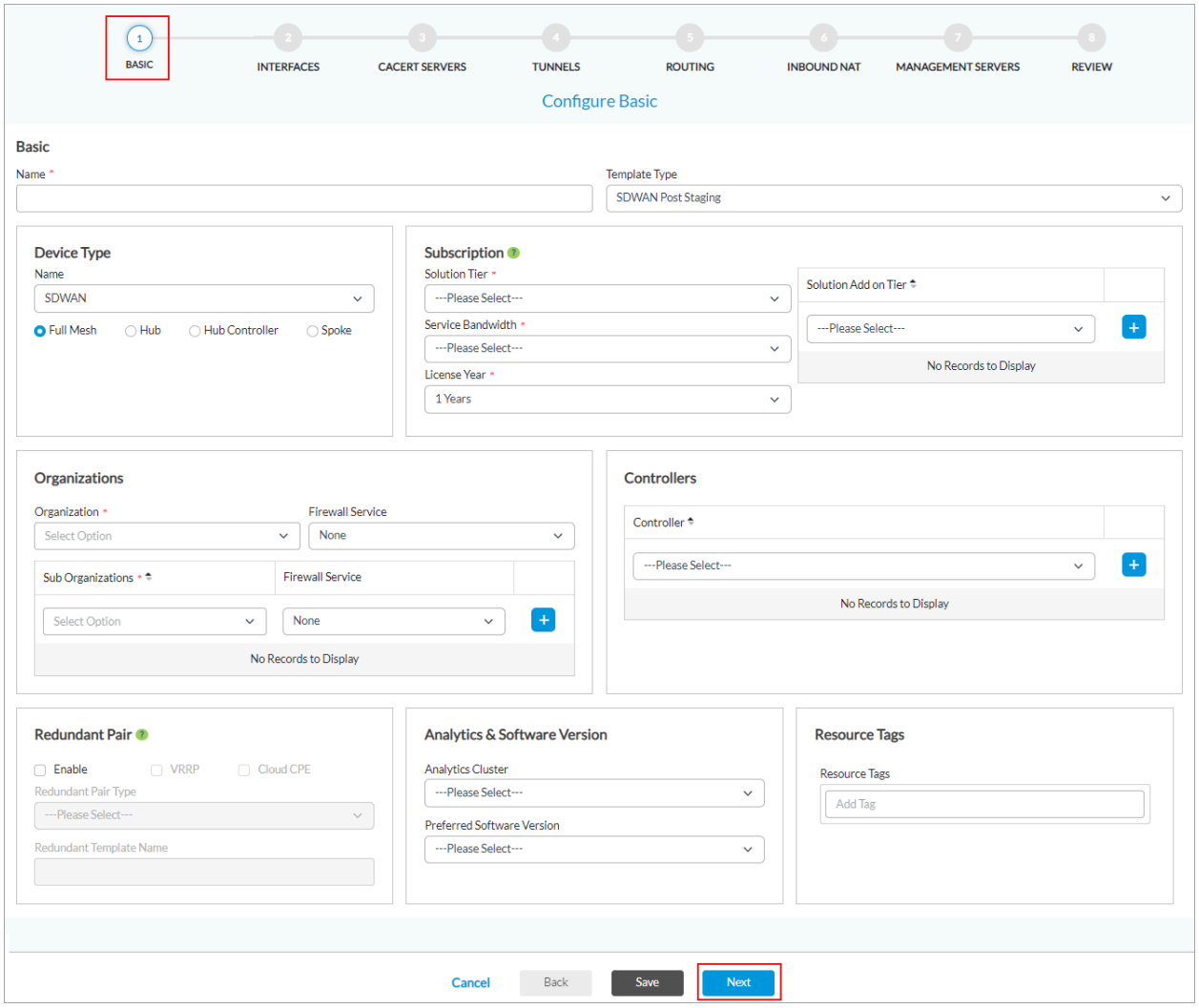
In Releases 22.1.1 and later, you use a workflow wizard to create a device template.

To add a post-staging template:

1. In Director view, select the Workflows tab in the top menu bar.
2. Select Template > Templates in the horizontal menu bar.



3. Click the Add icon.
4. Click Step 1, Basic. The Configure Basic screen displays. Enter information for the following fields.

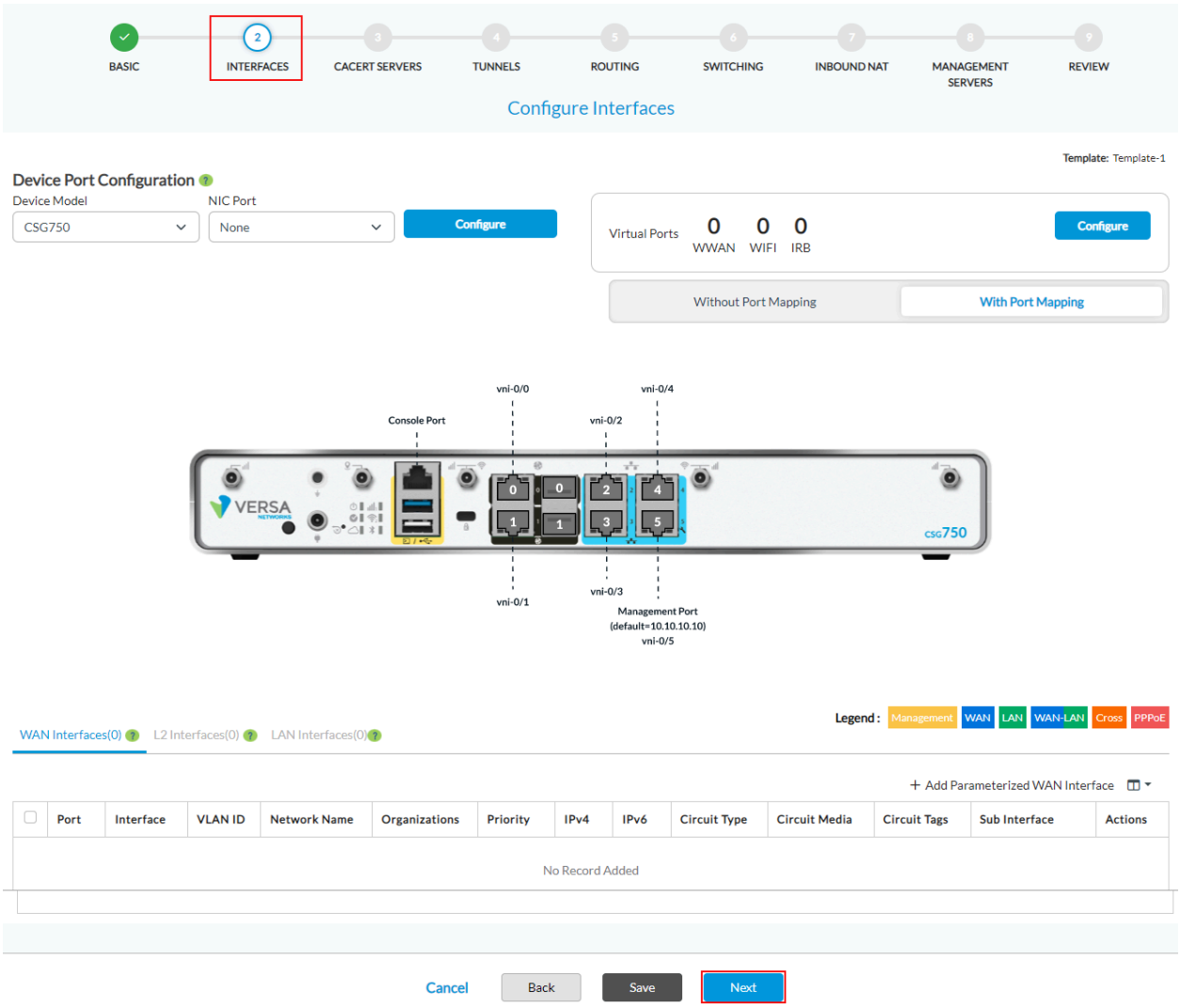


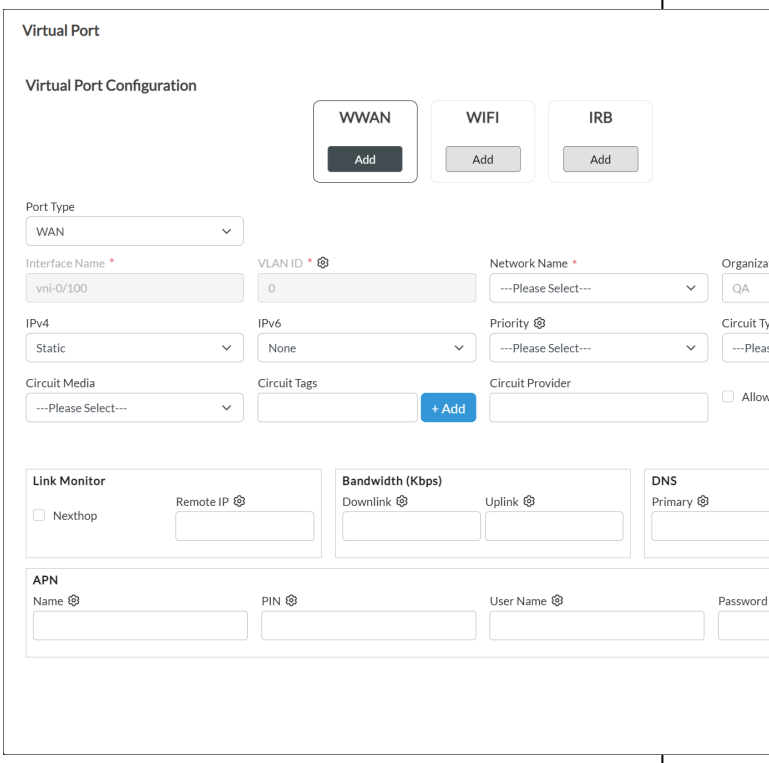
Field	Description
Name (Required)	Enter a name for the template. *Value:* Text string from 1 through 255 characters *Default:* None
Type (Required)	Select the template type: ◦ SD-WAN Post-Staging—Create a template for an operational network. ◦ SD-WAN Staging—Create a template for proof-of-concept (POC) or other test network.
Device Type	Select the device type based on the solution tier: ◦ vCPE—For routing tiers (ProNet, Net Pro, Advanced Routing) or security tiers (NGFW, UTM). ◦ SD-WAN—For Prime SD-WAN, Prime Secure, Premier Secure, and Premier Elite SD-WAN. If you select SD-WAN, select the topological role of the VOS device: ◦ Full Mesh—VOS device is in a full-mesh topology. This is the default. ◦ Hub—VOS device is a hub in a hub-and-spoke topology. ◦ Hub Controller—VOS device is a hub-controller node (HCN) in a hub-and-spoke topology. ◦ Spoke—VOS device is a spoke in a hub-and-spoke topology. If you select this option, enter the name of the spoke group in the Spoke Group field. For more information, see Create SD-WAN Spoke Groups. *Default:* Full Mesh
Subscription (Group of Fields)	
◦ Solution Tier	Select the licensing tier: ◦ Premier Elite SD-WAN ◦ Premier Secure SD-WAN

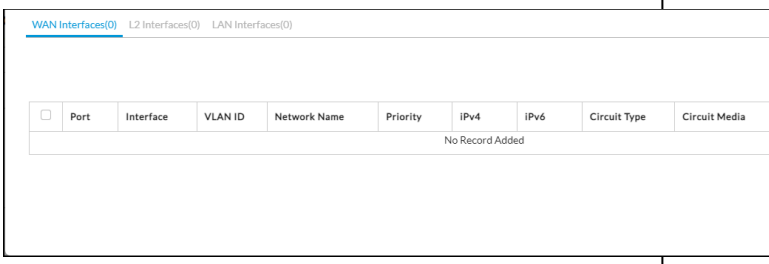
	◦ Prime SD-WAN ◦ Prime Secure SD-WAN For more information, see Licensing Overview.
◦ Service Bandwidth	Select the bandwidth, in Mbps or Gbps, to use for solution tier that corresponds to the license that the device is using.
◦ Solution Add-On Tier	(For Releases 21.1.1 and later.) Select the add-on licensing tier. You can use an add-on tier to add additional services to a licensing tier. For example, you can add NGFW or UTM to a standard SD-WAN by using an add-on.
◦ License Period	(For Releases 21.1.1 and later.) Select the period, in years, for which the license is valid. The options are 1 year, 3 years, and 5 years.
Organizations (Group of Fields)	
◦ Organization (Required)	Select the organization to which the template applies. When you select a provider organization that uses PKI-based IKE authentication, the CA Certificate Servers screen displays as Step 3. For more information, see Configure a Common Certificate Authority.
◦ Firewall Service	Select the Firewall type for the organization, NextGen Firewall or Stateful Firewall.
◦ Suborganizations	For full-mesh and hub device types, click the + Add icon to associate one or more suborganizations with the template. Select the suborganization from the drop-down list. To remove a suborganization from the list, select the suborganization and click the Delete icon.
◦ Firewall Service	Select the Firewall type for the suborganization, NextGen Firewall or Stateful Firewall.
Controllers (Required)	For full-mesh and hub device types, click the + Add icon to associate one or more Controllers with the template. Select the controller from the drop-down list. To remove a Controller from the list, select the Controller and click the Delete icon.
Redundant Pair (Group of Fields)	Redundant pair option generates additional configuration template for redundant/standby CPE

	deployed at the same site in HA pair.
◦ Enable	Click to create a redundant template, which is required when you are using active-active redundancy.
◦ VRRP	Click to enable VRRP for the redundant pair. Enabling VRRP mode automatically creates VRRP configuration on LAN interfaces in both active and standby templates.
◦ Cloud CPE	Click to enable a cloud-based CPE solution for redundancy.
◦ Redundant Template Name	Enter the name of the template to use for redundancy
Analytics and Software Version (Group of Fields)	
◦ Analytics Cluster	Select the Analytics cluster to use.
◦ Preferred Software Version	Select the preferred version of the software to deploy on the VOS device. Note that during the zero-touch provisioning (ZTP) process, the Director node upgrades a branch device to the minimum software version, which is a version that is backwards compatible with up to the two previous software versions.
Resource Tags	(For Releases 22.1.1 and later.) Enter a tag name, and then click Add icon to add the resource tag.

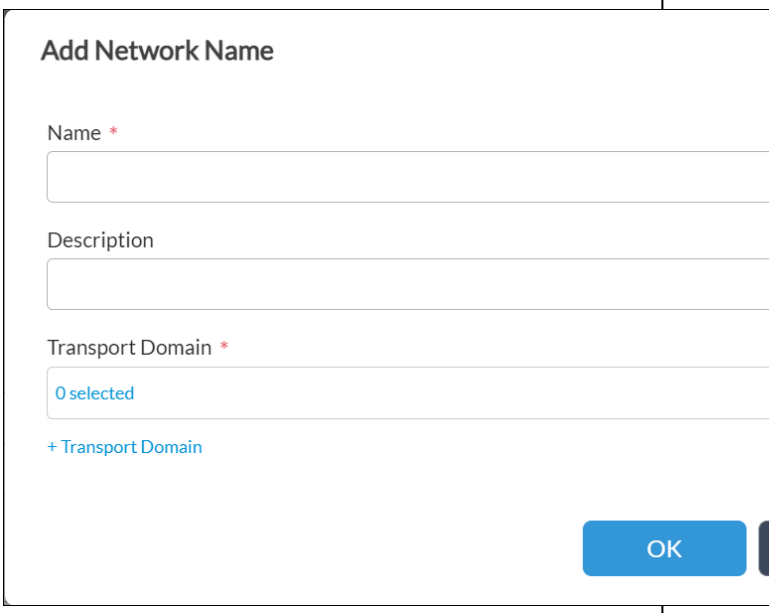
5. Click Save to save the configuration, or click Next to continue. The Step 2, Configure Interfaces screen displays to configure the device's port and interfaces on the ports. Enter information for the following fields.



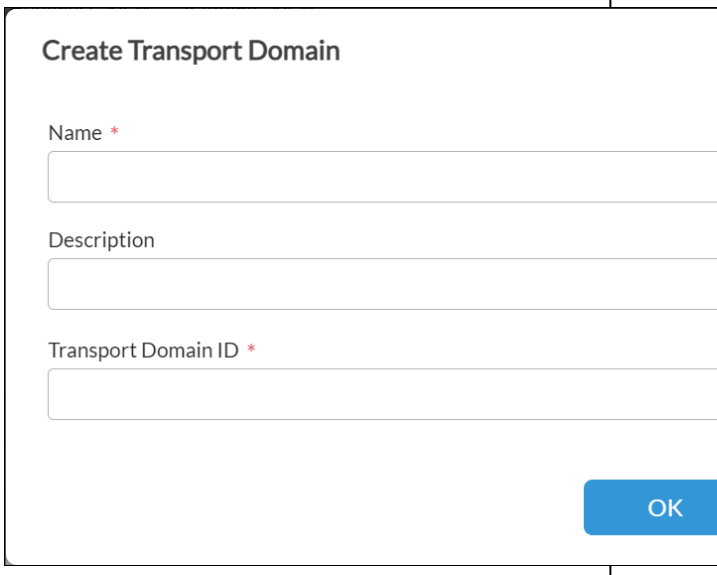
Field	Description
Device Port Configuration (Group of Fields)	Configure the WAN, LAN, and cross-connect ports on the VOS device.
◦ Device Model	Select a device model.
◦ Number of Ports	Select the number of ports on the device.
◦ Virtual Ports	To configure virtual ports, click Configure in the Virtual Ports box. 
◦ WWAN (LTE in earlier releases)	(For Releases 22.1.1 and later, LTE interfaces are called WWAN interfaces.) Click Configure in the Virtual Ports box and then click Add in the WWAN box to configure WWAN on a WAN interface. You can create up to four WWAN instances per WAN interface. The VOS device automatically assigns a port number from 100 through 103 to the WWAN interface.

	The term *WWAN interfaces* is used to represent LTE, 4G, and 5G interfaces. Click Save to commit the WWAN configuration and create the WWAN interface.
◦ WiFi	Click Configure in the Virtual Ports box and then click Add in the WiFi box to configure WiFi for the LAN or Layer 2 interface. (Layer 2 interfaces are supported for Releases 21.1.1 and later.) You can create up to eight WiFi interfaces on a LAN or Layer 2 interface. The VOS device automatically assigns a port number from 200 through 207 for each WiFi interface. Note that these interfaces support only DHCPv4.
◦ IRB	(For Releases 21.1.1 and later.) Click Configure in the Virtual Ports box and then click Add in the IRB box to configure Integrated routing and bridging (IRB) on a WAN or LAN interface. IRB associates a Layer 3 interface with a Layer 2 bridge domain so that packets can be routed to and from the bridge domain. On IRB interfaces, you can configure all standard Layer 3 interface settings, such as DHCP and VRRP.
◦ T1/E1	(For Releases 21.2.1 and later.) Click Configure in the Virtual Ports box and then click Add in the T1/E1 box to configure T1/E1 on a WAN or LAN interface. For a T1/E1 workflow, VLAN ID is applicable to Frame Relay encapsulation and it represents the DLCI number.
◦ DSL	(For Releases 21.2.1 and later.) Click Configure in the Virtual Ports box and then click Add in the DSL box to configure DSL on a WAN or LAN interface.
WAN Interfaces (Group of Fields)	This section populates when you add a WAN, a LAN and WAN, or a PPPoE interface for a port, with one row for each port: 

◦ Port Number	Prepopulated with the number of the WAN port you select in the Device Port Configuration box, including PPPoE and WWAN interfaces. If you select Redundancy in the General tab, this field shows port mapping of the redundant CPE. When you select a LAN interface on the Primary device, LAN interfaces are automatically selected on the redundant device. If the active, redundant CPEs are not connected to the exact same WAN networks, select a cross-connect port on the Primary device.
◦ Interface	Prepopulated with the vni interface and subinterface numbers based on the port you select in the Device Port Configuration box.
◦ VLAN ID	Enter the VLAN identifier for the subinterfaces. To parameterize the VLAN ID, click the Parameterize icon.
◦ Network Name	Select the network to which the WAN interface connects. To create a new network name, click + Add New in the network name drop-down list. In the Add Network Name popup window, enter the following information and then click OK.

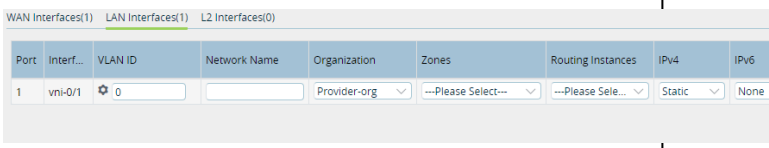


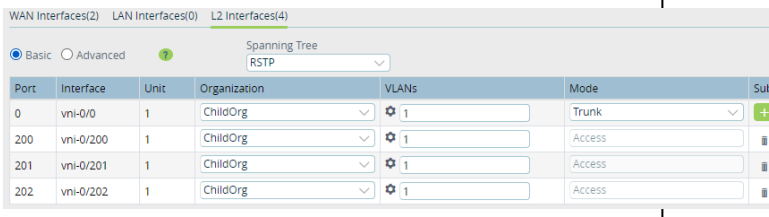
- Name (Required)—Enter a name for the WAN interface.
- Description—Enter an interface description
- Transport Domain (Required)—Click to select the transport domain:
  - Internet
  - MPLS
- To create a transport domain, click + Transport Domain and enter the following information:



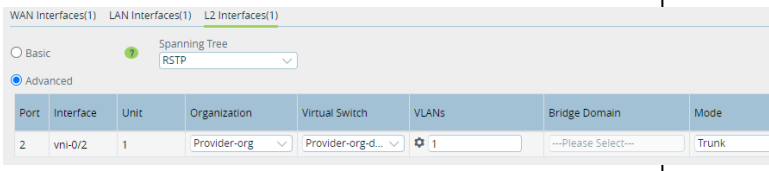
	▪ Name— (Required) Enter a transport domain name. ▪ Description—Enter a transport domain description. ▪ Transport Domain ID —(Required) Enter a transport domain ID.
◦ Priority	Enter a number for the link priority for WAN traffic. To parameterize the priority, click the Parameterize icon. If you do not assign a priority to a WAN circuit, the SD-WAN traffic steering engine adds the WAN interface to the default forwarding profile and assigns the default priority (which is the lowest priority) to the interface. (The traffic steering engine creates a default forwarding profile that is based on the configured priorities of the WAN circuits and uses this forwarding profile to steer all traffic originating from the site.) For example, if the traffic steering engine assigns the MPLS circuit priority 1 and the broadband circuit priority 2, the traffic uses MPLS as the primary circuit, because this circuit has a higher priority, and traffic fails over to the broadband circuit. If you do not assign a priority to the broadband circuit, the same behavior occurs because the broadband circuit has been assigned the default priority, which is the lowest priority. If you do not assign a priority to either the MPLS or broadband circuit, they both have the default priority, and traffic is load-balanced between them. It is recommended that you use the default forwarding profile for simple uses cases. To create more advanced traffic steering policies that involve SLA-based link and path prioritization, see Configure SD-WAN Traffic Steering. *Default*: None *Range*: 1 through 15 (1 is the highest priority and 15 is the lowest priority) (for Releases 22.1.1 and later); 1 through 8 (for Releases 21.2 and earlier)

◦ IPv4	Use IPv4 addressing on the WAN interface. ◦ Static—Use static IP addresses. When you select Static, a bind-data variable for the interface's static address is automatically generated in the template. ◦ DHCP—Use DHCP to obtain an IP address.
◦ IPv6	Use IPv6 addressing on the WAN interface. ◦ Static—Use static IP addresses. When you select Static, a bind-data variable for the interface's static address is automatically generated in the template. ◦ DHCP—Use DHCP to obtain an IP address.
◦ Circuit Type	Select access circuit type such as broadband, IP, or MPLS.
◦ Circuit Media	Select physical medium used by the access circuit: ◦ DSL ◦ LTE ◦ T1 ◦ T3 ◦ Cable ◦ Ethernet
◦ Circuit Tags	Enter a text list of circuit tags and, then click the Add icon.
◦ Subinterface	Click the  Add icon to add a subinterface on the WAN port. Another row is added to the WAN Interfaces table. For the subinterface, configure all the fields described above.
◦ Link Monitor	Select to monitor the reachability of the next hop or remote IP address on the WAN interface. If the monitored address becomes unreachable, DIA traffic is directed to another WAN interface if possible.
◦ Allow SSH to CPE	Click to allow SSH sessions to the CPE device on the underlay IP address of WAN interface.

◦ Circuit Provider	Enter the access circuit service provider's name.
◦ Bandwidth (Kbps) (Group of Fields)	
◦ Downlink	Enter the bandwidth available on the link for downloading data, in kilobytes per second (Kbps). *Range*: 1 through 10000000 Kbps *Default*: None
◦ Uplink	Enter the bandwidth available on the link for uploading data, in kilobytes per second (Kbps). *Range*: 1 through 10000000 Kbps *Default*: None
LAN Interfaces (Group of Fields)	This section populates when you add LAN interfaces or WiFi ports, with one row for each port. 
◦ Port Number	Prepopulated with the number of the port you select in the Device Port Configuration box.
◦ Interface	Prepopulated with the vni interface and subinterface numbers based on the port you select in the Device Port Configuration box.
◦ VLAN ID	Enter the VLAN ID for the subinterfaces. To parameterize the VLAN ID, click the ⚙ Parameterize icon.
◦ Network Name	Select the network to which the interface connects.
◦ Organization	Select the organization to which the interface belongs.
◦ Zones	Select the zone to which the interface belongs. If you do not select a zone, the interface is automatically

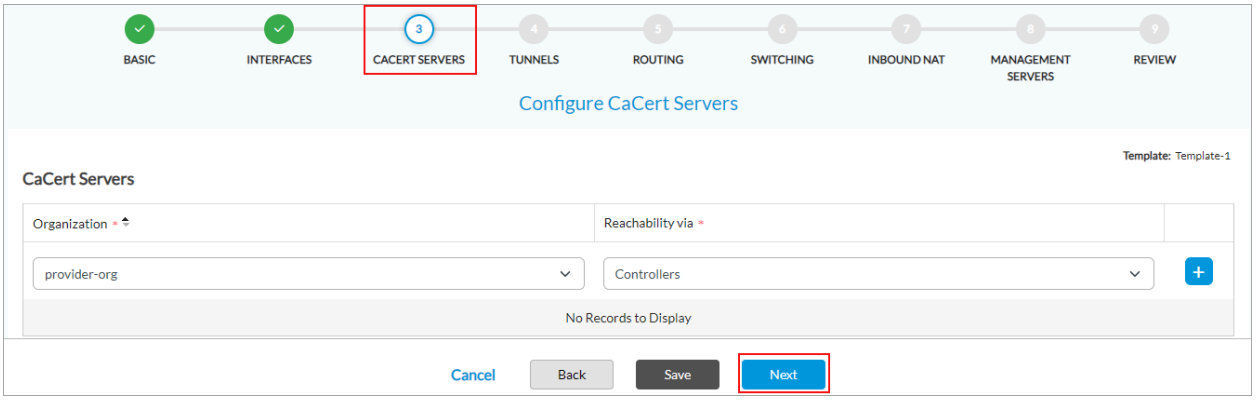
	associated with a zone based on the LAN network name.
◦ Routing Instance	Select the organization's routing instance with which the LAN interface is associated.
◦ IPv4	Use IPv4 addressing on the LAN interface. ◦ Static—Use static IP address.es When you select Static, a bind-data variable for the interface's static address is automatically generated in the template. ◦ DHCP—Use DHCP to obtain an IP address.
◦ IPv6	Use IPv6 addressing on the LAN interface. ◦ Static—Use static IP addresses. When you select Static, a bind-data variable for the interface's static address is automatically generated in the template. ◦ DHCP—Use DHCP to obtain an IP address.
◦ Sub Interface	Click the Add icon to add a subinterface on the LAN port. Another row is added to the WAN Interfaces table. For the subinterface, configure all the fields described above.
Layer 2 Interfaces (Group of Fields)	(For Releases 21.1.1 and later.) This section populates when you add Layer 2 interfaces for a port, with one row for each port.
◦ Basic	Click to create a simple Layer 2 configuration. Enter information for the following fields. 
◦ Advanced	Click to create an advanced configuration, such as a service provider configuration. Enter information for the following fields.

Updated: Wed, 23 Oct 2024 07:23:08 GMT

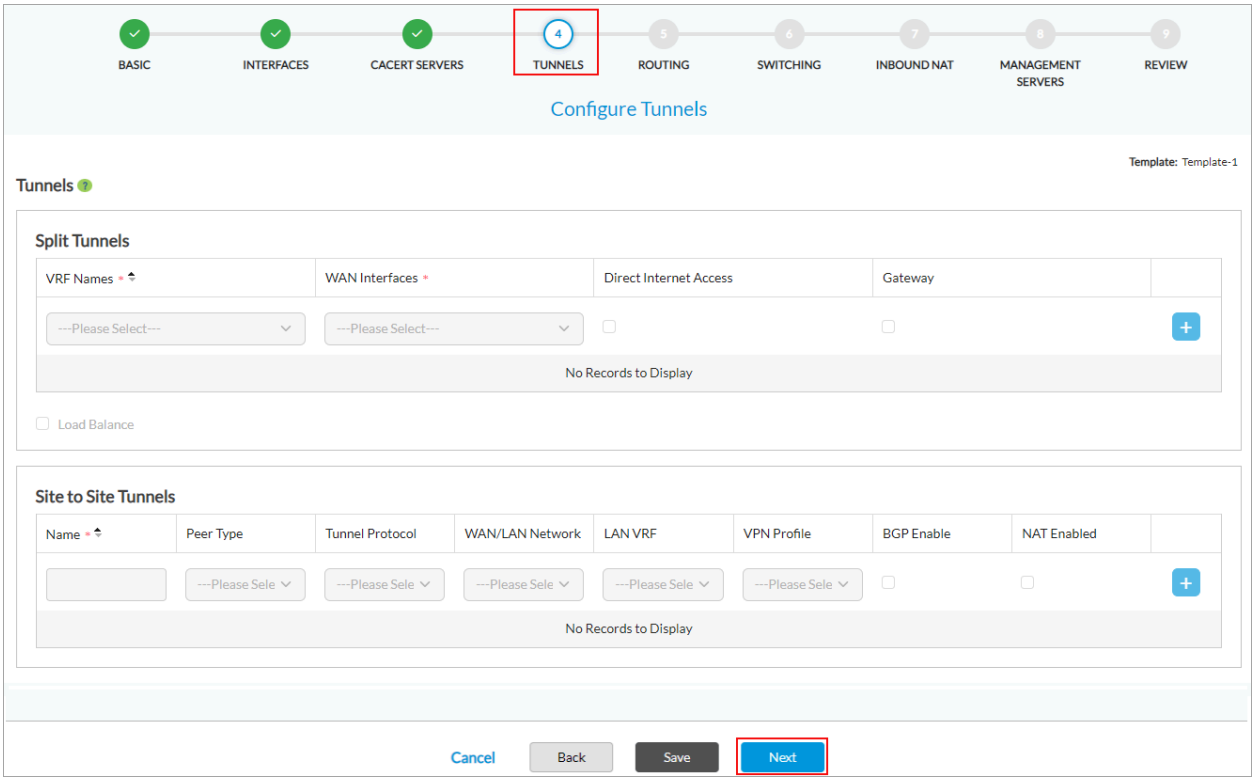
	
◦ Spanning Tree	Select the spanning tree protocol: ◦ None ◦ MSTP ◦ RSTP ◦ STP
◦ Port Number	Prepopulated with the number of the Layer 2 port (wired or WiFi) that you selected in the Device Port Configuration box.
◦ Interface	Prepopulated with the VIN interface and subinterface numbers of the port you selected in the Device Port Configuration box.
◦ Unit	Autogenerated unit or subinterface number of the Layer 2 interface. The first interface has unit ID 1, and subsequent interface unit IDs are generated in sequential order. Note that a WiFi port can have only one unit.
◦ Organization	Select the organization to which the Layer 2 interface belongs.
◦ VLANs	Select a VLAN to associate with the Layer 2 interface. To parameterize the VLAN ID, click the Parameterize icon. Note that when you parameterize the VLAN ID in the device workflow, you can enter only one value. If you need IRB-LAN support for the parameterized VLAN, copy and paste the same variable name from the Layer 2 tab to the IRB LAN row in the LAN tab.
◦ Virtual Switch	For the Advanced option, select a virtual switch to associate with the Layer 2 interface. The drop-down list displays the virtual switches associated with the organization.

◦ Bridge Domain	For the Advanced option, select the bridge domain for the Layer 2 interface. Selecting a bridge domain enables VLAN translation on the subinterface.
◦ Mode	Select the subinterface traffic mode for the VLAN: ◦ Access ◦ Trunk For WiFi ports, the mode is always Access. If the VLANs or bridge domains have more than one VLAN ID, the mode must be trunk. If there are multiple subunits, only one subunit can be in Access mode.
◦ Subinterface	Click the  Add icon to add a subinterface on the Layer 2 port. Another row is added to the Layer 2 Interfaces table. For the subinterface, configure all the fields described above.
◦ More	Click More to configure additional attributes for the interfaces. The Native VLAN ID popup window displays. Note that these attributes are configured at port level, not for subinterfaces. Native VLAN ID: enter the Native VLAN ID of the port. Native VLAN ID is required only if the mode of sub-units is Trunk. *Range*: 1 to 4094
◦ Native VLAN ID	When the subunit mode is Trunk, center the native VLAN ID of the port. *Range:* 1 through 4094

6. Click Save to save the configuration, or click Next to continue. The Step 3, Configure CA Certificate Servers screen displays. This screen displays if you select an organization that uses PKI-based IKE authentication in Step 1, Configure Basic screen. Enter information for the following fields.



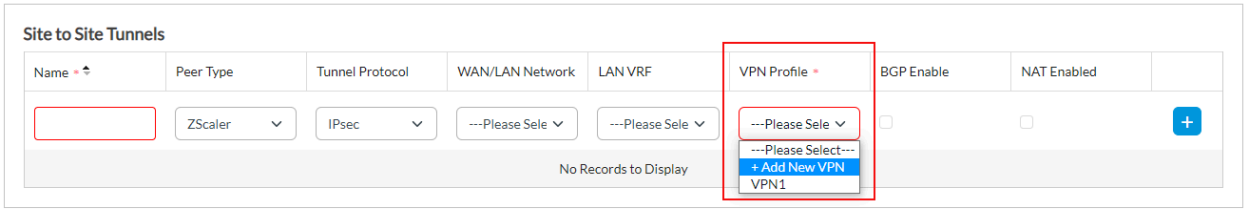
7. Select the interface to fetch CA certificate for the organizations you select from Configure Basic screen. Select the interface and click + Add to add the interface for each organization.
8. Click Save to save the configuration, or click Next to continue. The Step 4, Configure Tunnels screen displays. (You can configure site-to-site tunnels for Releases 20.2 and later.) Split tunnels allow traffic to flow from a common source to different destinations over different interfaces. For example, you can configure a split tunnel to allow traffic to flow from a common source to an SD-WAN site and a non–SD-WAN site. Enter information for the following fields.



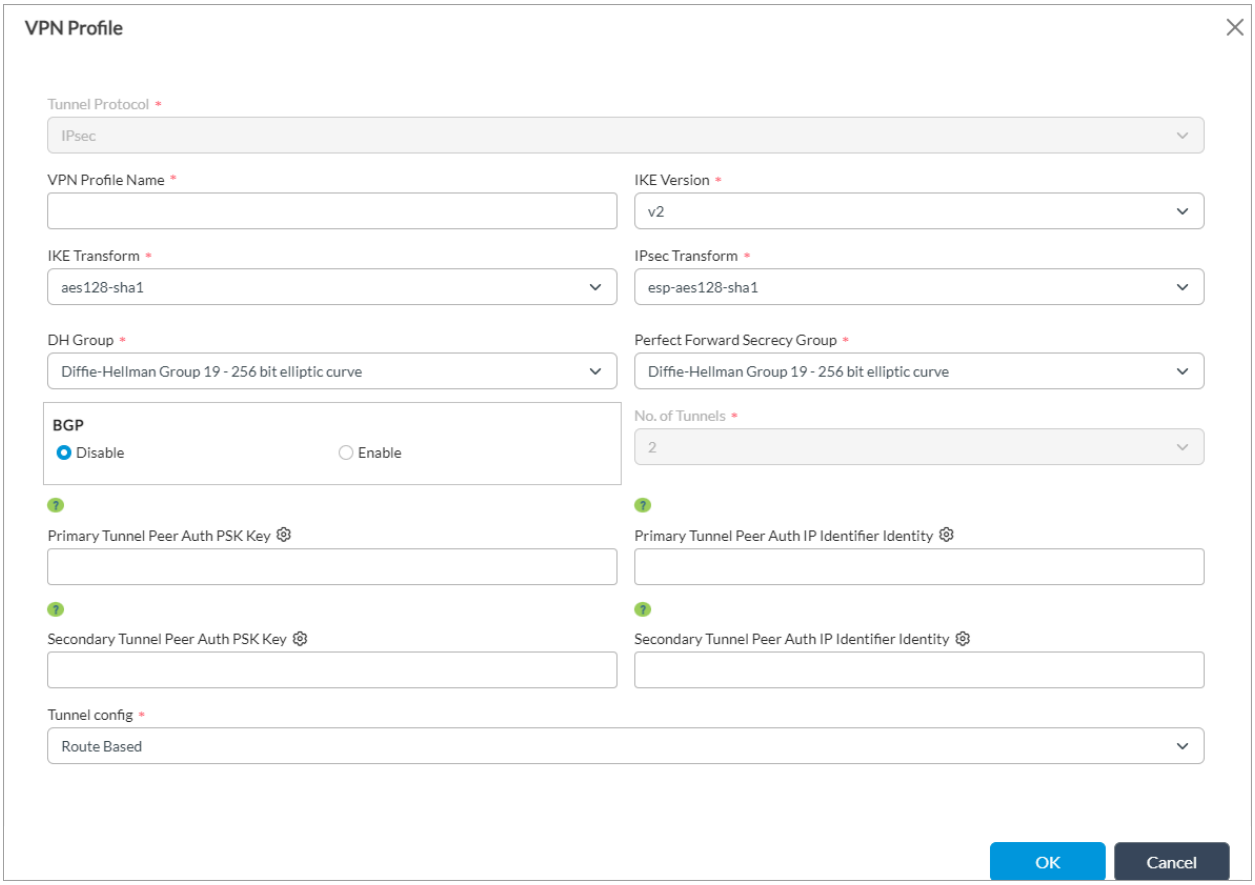
Field	Description
Split Tunnels (Group of Fields)	
◦ VRF Names	Select the name of the VRF.
◦ WAN Interfaces	Select the name of the WAN interface. If you select more than two WAN interfaces from the same LAN VR to configure direct internet access (DIA), the interface that is first on the list has the highest priority unless you enable load balancing by clicking Load Balance.
◦ DIA	Click to enable DIA. Source NATing is performed before packets are sent out to the WAN interface.
◦ Gateway	Click to allow the local router to act as a gateway between other SD-WAN sites and non–SD-WAN sites. The traffic between SD-WAN and non–SD-WAN sites flows through the gateway SD-WAN device. In gateway mode, routes that the router learns from an SD-WAN overlay are advertised to MPLS PE routers, and routes that the router learns from MPLS PE routers are advertised to SD-WAN overlay. Note that you do not need to configure split tunnels on SD-WAN sites.
◦ + Add icon	Click the + Add icon to add the split tunnel to the template.
◦ Load Balance	Click to enable balancing of the traffic load among the split tunnels if you have more than one split tunnel.
Site-to-Site Tunnels (Group of Fields)	
◦ Name	Enter a name for the site-to-site tunnel.
◦ Peer Type	Select the hosted-cloud or peer type, depending on the device at the other end of the tunnel: ◦ Azure Virtual WAN—Deploy a tunnel on Azure Virtual WAN. ◦ AWSTransitGW—Deploy a tunnel on AWS transit endpoint. ◦ Others—Deploy a tunnel on a third-party device that supports IPsec tunnels, such as Cisco, Juniper, and Palo Alto. ◦ Zscaler—Deploy a tunnel on a Zscaler endpoint.

Tunnel Protocol	Select the tunnel protocol to use to reach the peer: ◦ IPsec—Default tunnel protocol for the peer types AWS Transit Gateway, Azure Virtual WAN, Others, and Zscaler. ◦ GRE—Select GRE for the peer type Zscaler.
◦ WAN/LAN Network	Select the network to use. For the peer types AWS Transit Gateway and Azure Virtual WAN, you can select only WAN networks. For the peer types Zscaler and Others, you can select any network.
◦ LAN VRF	Select the virtual routing instance to use to reach the LAN, to allow users in the routing instance to access the tunnel to communicate with the gateway. The virtual routing instance is the tunnel termination endpoint.
◦ VPN Profile	When you select the peer type Zscaler or Others and a virtual routing instance, select a VPN profile to associate with the tunnel and with the LAN VRF organization. If a VPN profile is not available, create one, as described in Step 11. When the peer type is Zscaler, you must create VPN profile with two tunnels, and this field lists only VPN profiles with two tunnels. When you select the peer type Others or Zscaler, and if a VPN profile is not available, click the + Add New VPN option in the VPN Profile field. See Steps 9 and 10, below.
◦ BGP Enabled	For the peer type Azure Virtual WAN, click to enable BGP. For the peer type AWS Transit Gateway, this field is checked automatically. For the peer types Zscaler and Others, this field is checked automatically if BGP is enabled in the VPN profile, and it is not checked if BGP is not enabled in the VPN profile.
◦ Add icon	Click the Add icon to add the site-to-site tunnel to the template.

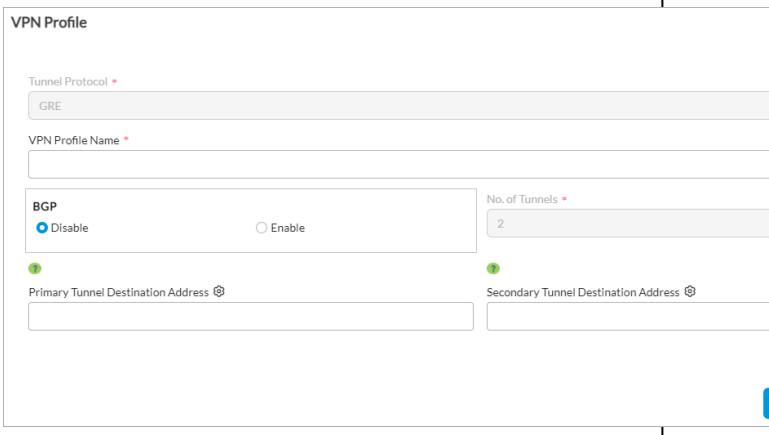
9. If you select the peer type Others or Zscaler, and if a VPN profile is not available, click the + Add New VPN option in the VPN Profile field.

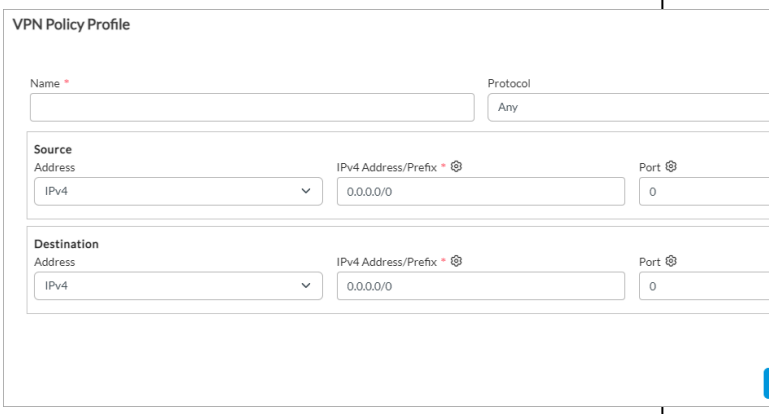


10. In the Create VPN Profile popup window, enter information for the following fields.



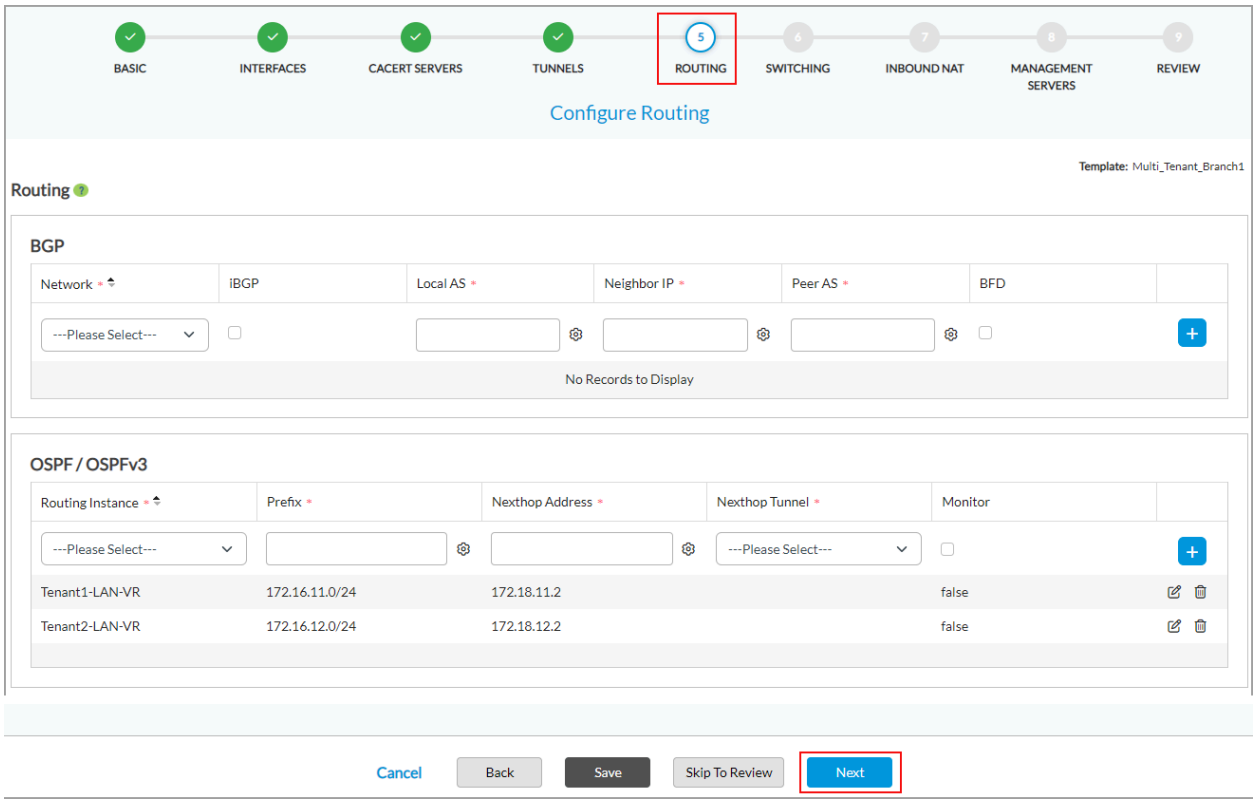
Field	Description
Tunnel Protocol (Required)	IPsec or GRE tunnel protocol for the peer type that you selected when you configured the site-to-site tunnel is selected automatically.
VPN Profile Name (Required)	Enter a name for the VPN profile.
IKE Version (Required	Select the IKE version: ◦ v1 ◦ v2 ◦ v2-or-v1
IKE Transform (Required)	Select the IKE transform algorithm to use for data encryption.
IPsec Transform (Required)	Select the IPsec transform algorithm to use for data encryption.
BGP	Select the BGP state: ◦ Disable ◦ Enable
No. of Tunnels (Required)	Enter how many tunnels to create between the VOS device and the Zscaler unmanaged device or between the VOS device and the third-party managed device. For Zscaler tunnels, you must create two tunnels.
For the IPsec tunnel protocol	Enter information for the following fields.
◦ Primary Tunnel Peer Authenticaiton PSK Key	Enter the primary tunnel preshared key (PSK) to use with the peer. If you leave this field empty, you are prompted to enter the peer authentication key in the device bind data when you deploy the workflow.
◦ Primary Tunnel Peer Authentication IP Identifier Identity	Enter the primary tunnel IP address of the peer authentication device. If you leave this field empty, you are prompted to enter the peer authentication IP identifier identity under device bind data when you deploy the workflow.
◦ Secondary Tunnel Peer Authentication PSK Key	Enter the secondary tunnel PSK to use with the peer. If you leave this field empty, you are prompted to enter the peer authentication key in the device bind

	data when you deploy the workflow.
◦ Secondary Tunnel Peer Authentication IP Identifier Identity	Enter the secondary tunnel IP address of the peer authentication device. If you leave this field empty, you are prompted to enter the peer authentication IP identifier identity under device bind data when you deploy the workflow.
For the GRE tunnel protocol	Enter information for the following fields: 
◦ Primary Tunnel Destination Address	Enter the primary tunnel destination IP address of the authentication device.
◦ Secondary Tunnel Destination Address	Enter the secondary tunnel destination IP address of the authentication device.
Tunnel Configuration (Required)	Select the tunnel configuration.
◦ Route Based	Use a route-based configuration.
◦ Policy Based	Use a policy-based configuration. If you select this option, click + Add icon to add a policy. In the VPN Policy Profile popup window, enter information for the following fields.



- Name—Enter a name for the policy.
- Protocol—Select a protocol:
  - ICMP
  - TCP
  - UDP
- Source (Group of Fields)—Enter information about the traffic source:
  - Address—Select the IPv4 address type.
  - IPv4 Address/Prefix—Enter the IPv4 source prefix or address.
  - Port—Enter the source port number.
- Destination (Group of Fields)—Enter information about the traffic destination:
  - Address—Select the IPv4 address type.
  - IPv4 Address/Prefix—Enter the IPv4 destination prefix or address.
  - Port—Enter the source port number.
- Click OK.

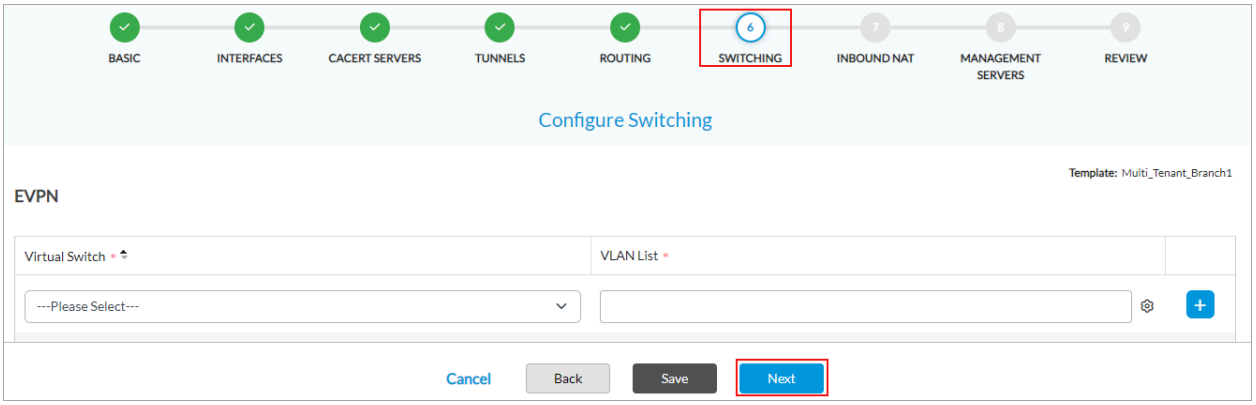
11. Click Save to save the configuration, or click Next to continue. The Step 5, Configure Routing screen displays. You can configure BGP, OSPF, and static routing. For each routing protocol, click the Parameterize icon to generate the routing information dynamically, or enter information for the following fields and then click the Add icon.



Field	Description
BGP (Group of Fields)	Configure BGP.
◦ Network	Select the name of the network on which to configure BGP.
◦ Local AS	Enter the local autonomous system (AS) number. To parameterize the local AS number. click the Parameterize icon.
◦ Neighbor IP	Enter the IP address of the BGP neighbor (peer). To parameterize the IP address, click the Parameterize icon.
◦ Peer AS	Enter the AS number of the peer. To parameterize the peer AS number, click the Parameterize icon.
◦ Add icon	Click the Add icon to add the BGP configuration to the template.
OSPF/OSPFv3 (Group of Fields)	Configure OSPF.
◦ Network Name	Select the name of the network on which to configure OSPF
◦ Area	Enter the OSPF area number.
◦ BFD	Click to enable BFD.
Add icon	Click the Add icon to add the OSPF configuration to the template.
Static Routes (Group of Fields)	Configure static routing.
◦ Routing Instance	Select the name of the routing instance in which to configure the static route.
◦ Prefix	Enter the prefix and prefix length of the static route. To parameterize the IP prefix, click the Parameterize icon.
◦ Next Hop	Enter the IP address of the next hop. To parameterize

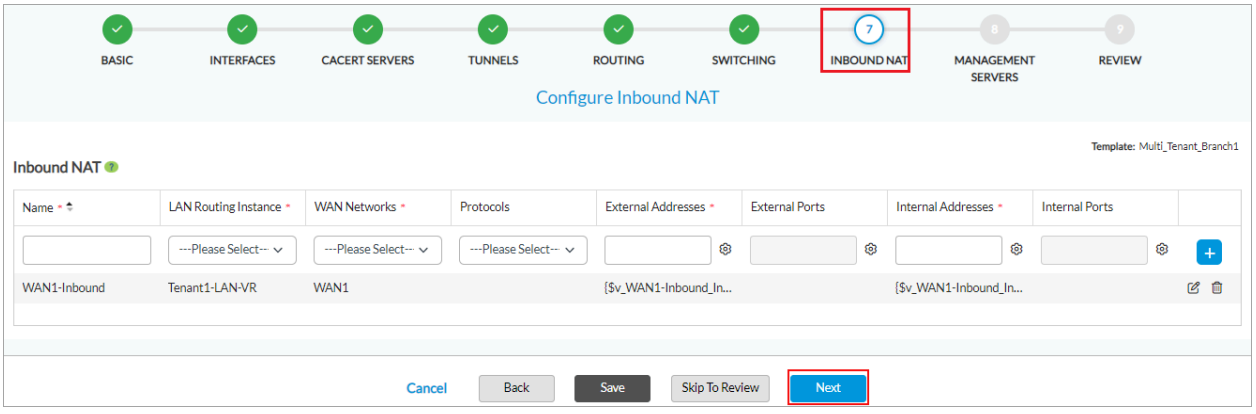
	the next hop IP address, click the Parameterize icon.
Add icon	Click the Add icon to add the static route to the template.

12. Click Save to save the configuration, or click Next to continue. The Step 6, Configure Switching screen displays. Note that this tab is displayed only when you select Layer 2 as the type of interface in the Step 2, Interfaces screen in Step 5, above. Enter information for the following fields.



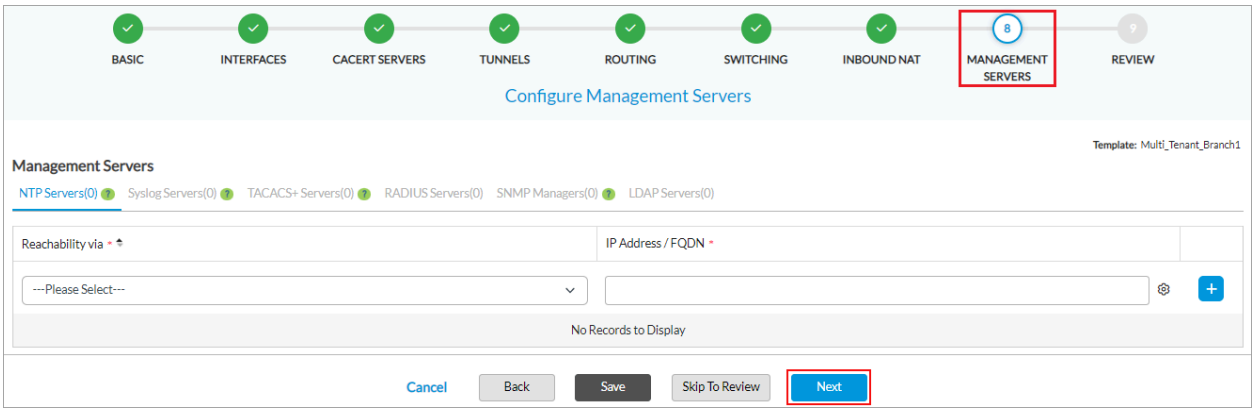
Field	Description
Virtual Switch	Select the VLAN switch to associate with EVPN. For each virtual switch, the workflow configures the following: ◦ Unique route distinguisher (RD) and route target (RT) values ◦ VLANs for all the VLAN fields in the Interfaces tab for which EVPN is enabled ◦ Family Layer 2 VPN-EVPN in the control virtual router (VR) of the associated organization
VLAN List	Enter the VLANs. You can specify individual VLANs or VLAN ranges, separated by commas. If you add more than one row, with different VLANs or VLAN ranges, for each virtual switch, ensure that you avoid duplicate and overlapping values. Click the Parameterize icon to specify the default parameterized variable. If you edit the parameterized value, you must retain the {$v*__*} format.

13. Click Save to save the configuration, or click Next to continue. The Step 7, Configure Inbound NAT screen displays. You configure NAT rules so that traffic inbound from an external network can reach internal LAN servers. Enter information for the following fields.



Field	Description
Name	Enter a name for the NAT rule.
WAN Network	Select the WAN network on which to enable inbound NAT port forwarding.
LAN Routing Instance	Select the routing instance that connects the internal LAN server to the CPE.
Protocol	Select the protocol of the application that runs on the internal LAN server: ◦ ICMP ◦ TCP ◦ UDP
External Addresses	Enter the IP prefix or a range of IP addresses for the WAN interface to use for NAT. To enter a range, separate the IP addresses with a hyphen; for example, 1.1.1.1-1.1.1.2.
External Ports	Enter the external ICMP, TCP, or UDP port or port range for the WAN interface to use for NAT.
Internal Addresses	Enter the IP prefix or a range of IP addresses of the LAN servers to which to send NATed traffic. To specify a range, separate the IP addresses with a hyphen; for example, 1.1.1.1-1.1.1.2.
Internal Ports	Enter the external ICMP, TCP, or UDP port or port range to which to send NATed traffic.
+ Add icon	Click the + Add icon to add the inbound NAT instance.

14. Click Save to save the configuration, or click Next to continue. The Step 8, Configure Management Servers screen displays.

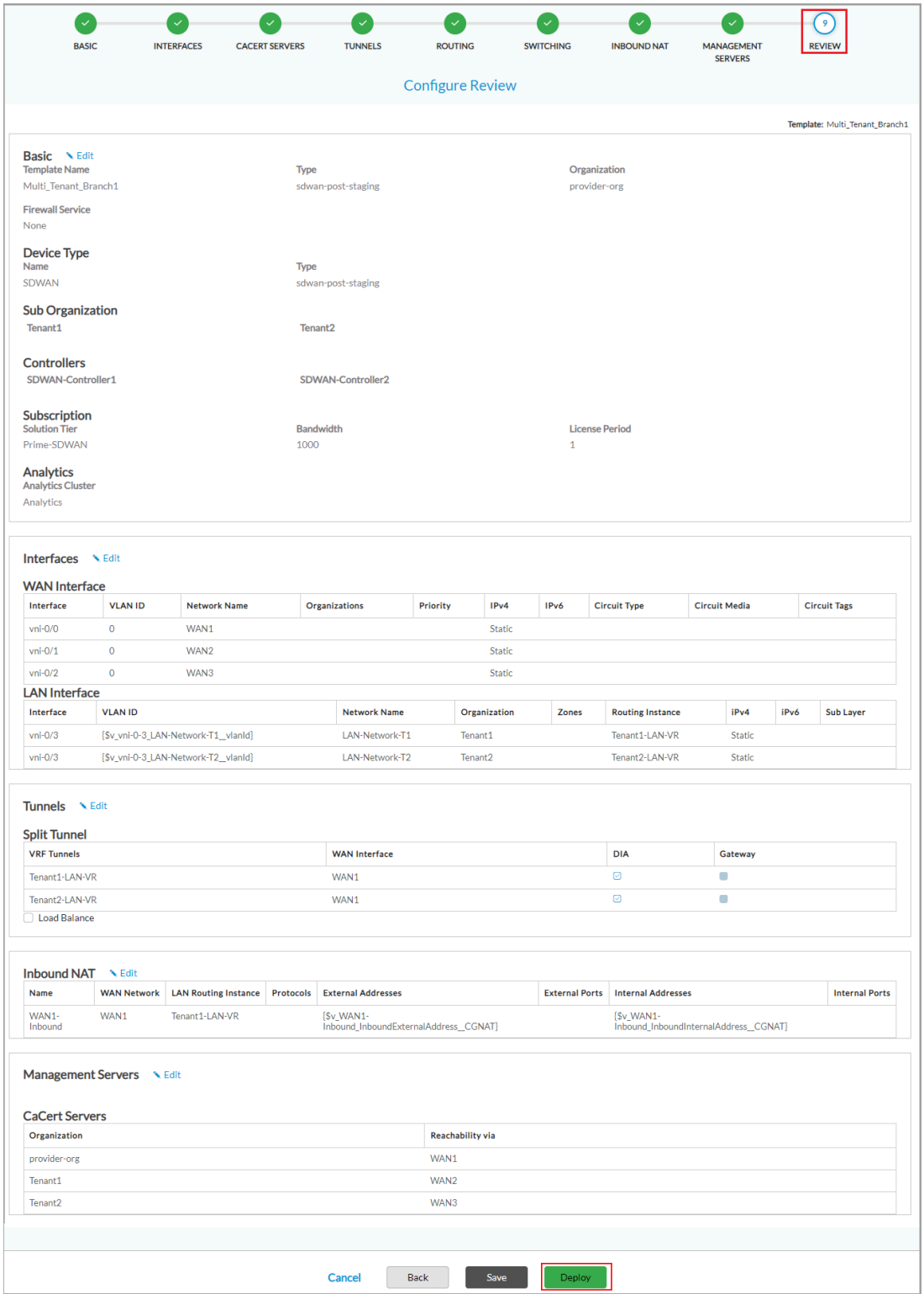


Field	Description
NTP Servers (Group of Fields)	Configure NTP servers.
◦ Reachability via	Select the network to use to reach the NTP server.
◦ IP Address	Enter the IP address of the NTP server. To parameterize the IP address, click the Parameterize icon.
◦ Add icon	Click the Add icon to add the NTP server to the template
Syslog Servers (Group of Fields)	Configure syslog servers.
◦ Reachability via	Select the network to use to reach the syslog server.
◦ IP Address	Enter the IP address of the syslog server. To parameterize the IP address, click the Parameterize icon.
◦ Add icon	Click the Add icon to add the syslog server to the template
TACACS+ Servers (Group of Fields)	Configure TACACS+ servers.
◦ Reachability via	Select the network to use to reach the TACACS+ server.
◦ IP Address/FQDN	Enter the IP address or fully qualified domain name of the TACACS+ server. To parameterize the IP address or domain name, click the Parameterize icon
◦ Authentication Key	Enter the authentication key, or password, of the TACACS+ server. To parameterize the key, click the Parameterize icon.
◦ Actions	Select one or both TACACS+ server actions: ◦ Accounting—Log all TACACS+ activity. ◦ Authentication—Use TACACS+ authentication to determine whether a user can access a system.

◦ Add icon	Click the Add icon to add the TACACS+ server to the template
RADIUS Servers (Group of Fields)	Configure RADIUS servers.
◦ Reachability via	Select the network to use to reach the RADIUS server.
◦ IP Address/FQDN	Enter the authentication key, or password, of the TACACS+ server. To parameterize the key, click the Parameterize icon.
Authentication Key	Enter the authentication key, or password, of the RADIUS server. To parameterize the key, click the Parameterize icon.
◦ Actions	Select one or more RADIUS server actions: ◦ Accounting—Log all RADIUS activity. ◦ Authentication—Use RADIUS authentication to determine whether a user can access a system. ◦ WiFi Authentication—Use RADIUS authentication to allow a device to access a WiFi network.
◦ Add icon	Click the Add icon to add the RADIUS server to the template
SNMP Managers (Group of Fields)	Configure SNMP servers.
◦ Versions	Select the version or versions of version to use: ◦ v1 ◦ v2c ◦ v3
◦ Community	Enter the SNMP community string to use to access the SNMP server.
◦ Username	For SNMPv3, enter the username to access the SNMP server. To parameterize the username, click the Parameterize icon.
◦ Password	For SNMPv3, enter the password to access the

	SNMP server. To parameterize the password, click the Parameterize icon.
◦ Reachability via	Select the network to use to reach the SNMP server.
◦ IP Address	Enter the IP address of the SNMP server. To parameterize the IP address, click the Parameterize icon.
◦ Add icon	Click the Add icon to add the SNMP server to the template
LDAP Servers (Group of Fields)	Configure LDAP servers.
◦ Reachability via	Select the network to use to reach the LDAP server.
◦ IP Address/FQDN	Enter the IP address or fully qualified domain name of the LDAP server. To parameterize the IP address or domain name, click the Parameterize icon.
◦ Domain Name	Enter the domain name in which the LDAP server resides. To parameterize the domain name, click the Parameterize icon.
◦ Base DN	Enter the point from which the LDAP server searches for users. For example, DC=example-domain,DC=com
◦ Bind DN	Enter the user and user's location in the LDAP directory tree. For example, CN=username,CN=Users,DC=example-domain,DC=com
◦ Bind Password	Enter the password to use to authenticate the user.
◦ Add icon	Click the Add icon to add the LDAP server to the template.

15. Click Save to save the configuration, or click Next to continue. The Step 9, Review screen displays.

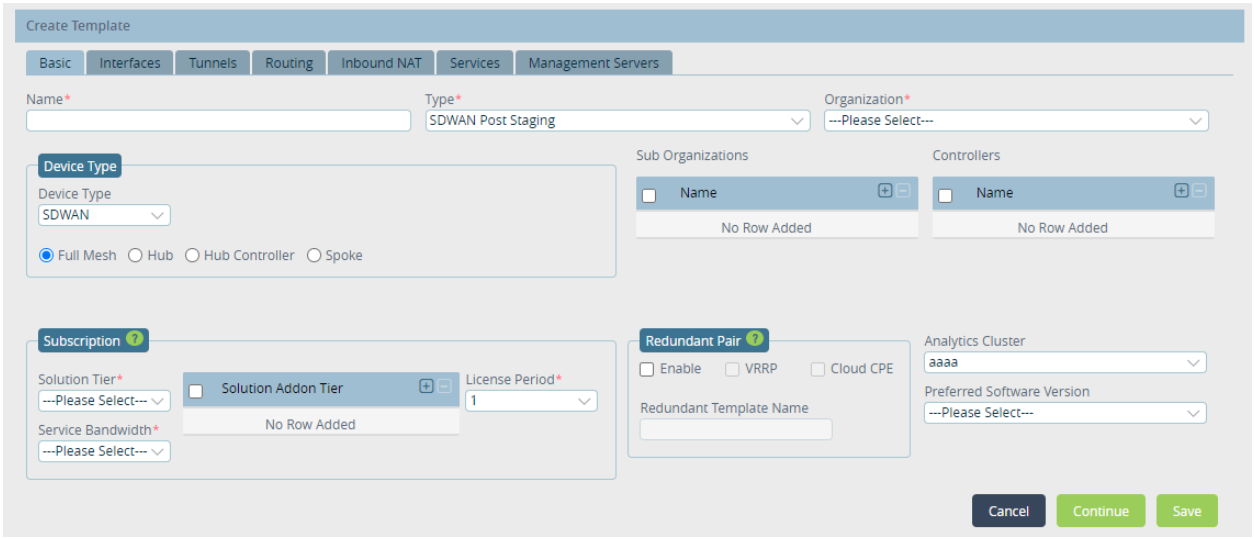


16. Click Save to add the template.
17. Click Deploy to associate a post-staging template with the Controller nodes, organizations, and other selected entities.

Create Device Templates for Releases 21.2 and Earlier

To create a post-staging device template:

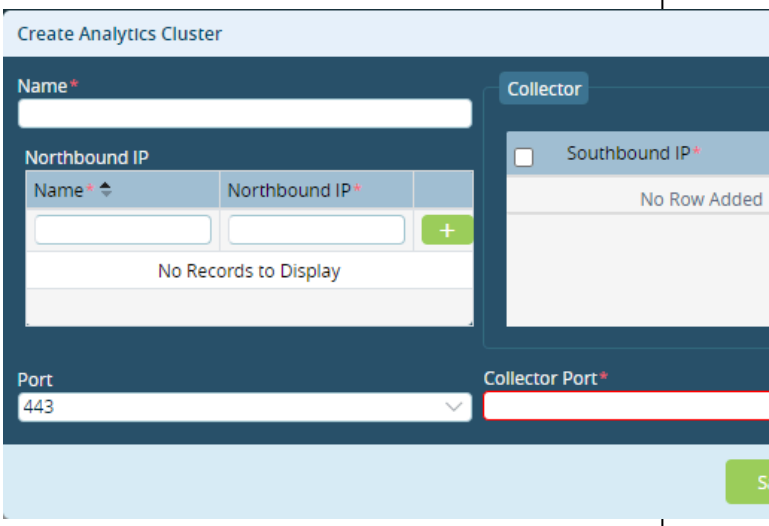
1. In Director view, select the Workflows tab in the top menu bar.
2. Select Template > Templates in the left menu bar.
3. Click the Add icon to create a new template. The Create Template window displays. For the eight tabs (for Releases 21.1.1 and later, the Switching tab is included) on this window, provide configuration information, as described in the following steps. Required information is indicated with a red asterisk. Click Continue to move to the next tab in sequence and Back to move to the previous tab, or select a tab to move directly to its window. For Releases 21.1.0 and earlier, the Create Template window is displayed as a popup window.



4. Select the Basic tab to configure basic interface properties. Enter information for the following fields.

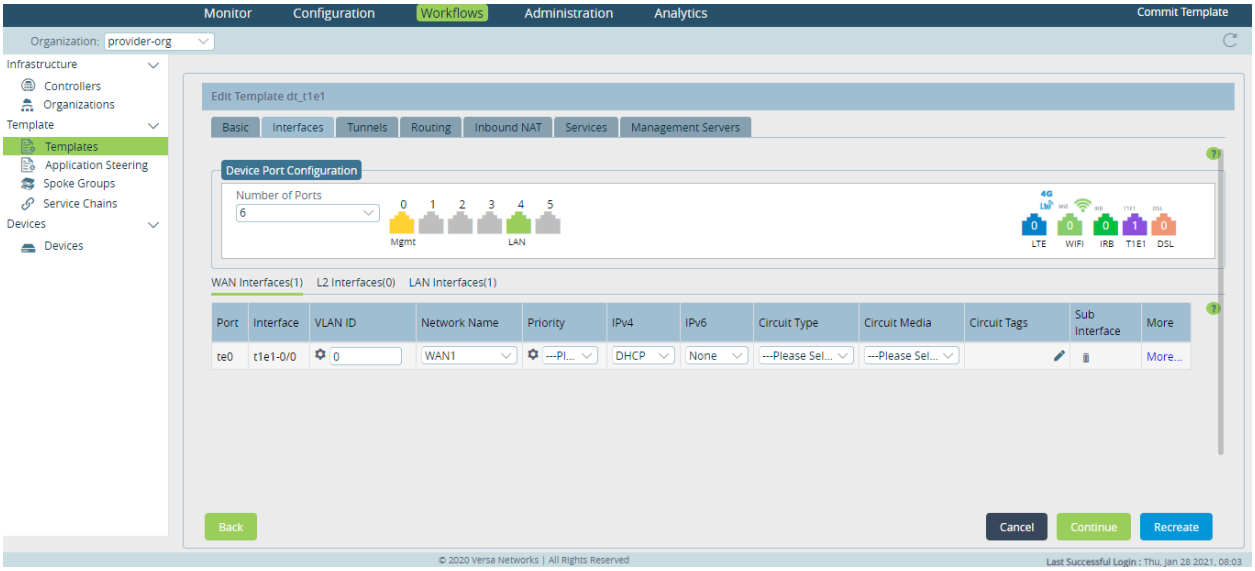
Field	Description
Name (Required)	Enter a name for the template. *Value:* Text string from 1 through 255 characters *Default:* None
Type (Required)	Select the template type: ◦ SD-WAN Post-Staging—Create a template for an operational network. ◦ SD-WAN Staging—Create a template for proof-of-concept (POC) or other test network.
Organization (Required)	Select the organization to which the template applies.
Device Type	Select the device type based on the solution tier: ◦ vCPE—For routing tiers (ProNet, Net Pro, Advanced Routing) or security tiers (NGFW, UTM). ◦ SD-WAN—For Prime SD-WAN, Prime Secure, Premier Secure, and Premier Elite SD-WAN. If you select SD-WAN, select the topological role of the VOS device: ◦ Full Mesh—VOS device is in a full-mesh topology. This is the default. ◦ Hub—VOS device is a hub in a hub-and-spoke topology. ◦ Hub Controller—VOS device is a hub-controller node (HCN) in a hub-and-spoke topology. ◦ Spoke—VOS device is a spoke in a hub-and-spoke topology. If you select this option, enter the name of the spoke group in the Spoke Group field. For more information, see Create SD-WAN Spoke Groups. *Default:* Full Mesh
Suborganizations	For full-mesh and hub device types, click the Add icon to associate one or more suborganizations with the template. Select the suborganization from the drop-down list. To remove a suborganization from the list, select the suborganization and click the Delete icon.

Controllers (Required)	For full-mesh and hub device types, click the Add icon to associate one or more Controllers with the template. Select the controller from the drop-down list. To remove a Controller from the list, select the Controller and click the Delete icon.
Subscription (Group of Fields)	
◦ Solution Tier	Select the licensing tier: ◦ Premier Elite SD-WAN ◦ Premier Secure SD-WAN ◦ Prime SD-WAN ◦ Prime Secure SD-WAN For more information, see Licensing Overview.
◦ Service Bandwidth	Select the bandwidth, in Mbps or Gbps, to use for solution tier that corresponds to the license that the device is using.
◦ Solution Add-On Tier	(For Releases 21.1.1 and later.) Select the add-on licensing tier. You can use an add-on tier to add additional services to a licensing tier. For example, you can add NGFW or UTM to a standard SD-WAN by using an add-on.
◦ License Period	(For Releases 21.1.1 and later.) Select the period, in years, for which the license is valid. The options are 1 year, 3 years, and 5 years.
Redundant Pair (Group of Fields)	Redundant pair option generates additional configuration template for redundant/standby CPE deployed at the same site in HA pair.
◦ Enable	Click to create a redundant template, which is required when you are using active-active redundancy.
◦ VRRP	Click to enable VRRP for the redundant pair. Enabling VRRP mode automatically creates VRRP configuration on LAN interfaces in both active and standby templates.
◦ Cloud CPE	Click to enable a cloud-based CPE solution for redundancy.
◦ Redundant Template Name	Enter the name of the template to use for redundancy

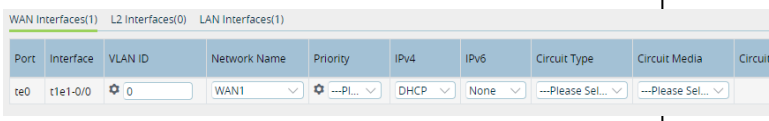
Analytics Cluster	Select the Analytics cluster to use. Select + Add Analytics Cluster to create an Analytics cluster. In the Create Analytics Cluster popup window, enter the following information, and then click Save.  ◦ Name (Required)—Enter a name for the cluster. ◦ Northbound IP—Enter a name to identify the northbound IP address, enter the IP address for the northbound interface, and click the Add icon to add the IP address. ◦ Collector—Enter information about the Analytics cluster collector: ▪ Southbound IP—(Required) Enter the IP address for the southbound interface, and click the Add icon to add the IP address. ◦ Port—Select the port number. ◦ Collector Port (Required)—Enter the port number to use for the northbound connection.
Preferred Software Version	Select the preferred version of the software to deploy on the VOS device. Note that during the zero-touch provisioning (ZTP) process, the Director node upgrades a branch device to the minimum software version, which is a version that is backwards compatible with up to the two previous software versions.

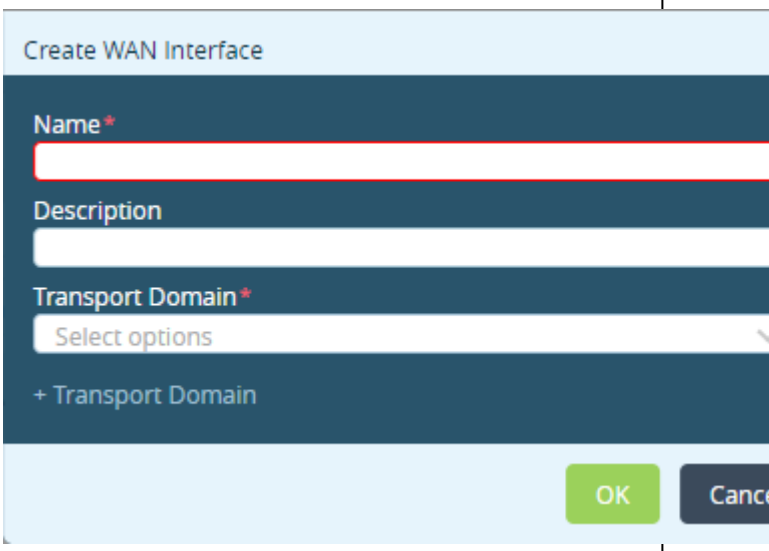
Updated: Wed, 23 Oct 2024 07:23:08 GMT

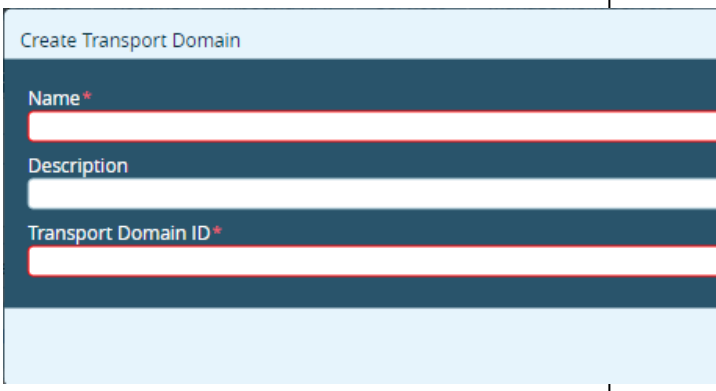
5. Click Continue.
6. Select the Interfaces tab to configure the device's port and interfaces on the ports. Enter information for the following fields.



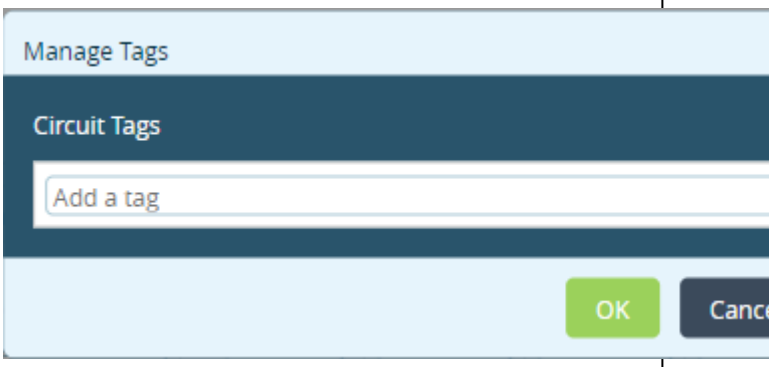
Field	Description
Device Port Configuration (Group of Fields)	Configure the WAN, LAN, and cross-connect ports on the VOS device.
◦ Number of Ports	Select the number of ports on the device.
◦ Port icons	For the port icons immediately to the right of the Number of Ports field, right-click the port icon, and from the popup window select the type of interface to configure on the port: ◦ LAN (green) ◦ Layer 2 (green)—(For Releases 21.1.1 and later). When you select this icon, the Switching tab displays. ◦ Management (yellow)—Port 0 is always the management interface. ◦ PPPoE (light blue) ◦ WAN (dark blue) ◦ LAN (green) ◦ Unassigned (gray)
◦ LTE (blue port icon)	Click the blue LTE port icon on the right side of the Device Port Configuration box to configure LTE on a WAN interface. You can create up to four LTE instances per WAN interface. The VOS device automatically assigns a port number from 100 through 103 to the LTE interface. Click Save to commit the LTE configuration and create the LTE interface.
◦ WiFi	Click the green WiFi port icon on the right side of the Device Port Configuration box to configure WiFi for the LAN or Layer 2 interface. (Layer 2 interfaces are supported for Releases 21.1.1 and later.) You can create up to eight WiFi interfaces on a LAN or Layer 2 interface. The VOS device automatically assigns a

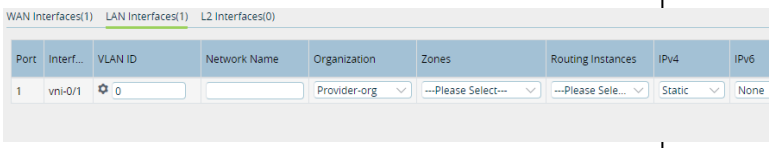
	port number from 200 through 207 for each WiFi interface. Note that these interfaces support only DHCPv4.
◦ IRB	(For Releases 21.1.1 and later.) Click the green IRB port icon on the right side of the Device Port Configuration box to configure Integrated routing and bridging (IRB) on a WAN or LAN interface. IRB associates a Layer 3 interface with a Layer 2 bridge domain so that packets can be routed to and from the bridge domain. On IRB interfaces, you can configure all standard Layer 3 interface settings, such as DHCP and VRRP.
◦ T1/E1	(For Releases 21.2.1 and later.) Click the purple T1/E1 port icon on the right side of the Device Port Configuration box to configure T1/E1 on a WAN or LAN interface. For a T1/E1 workflow, VLAN ID is applicable to Frame Relay encapsulation and it represents the DLCI number.
◦ DSL	(For Releases 21.2.1 and later.) Click the pink DSL port icon on the right side of the Device Port Configuration box to configure DSL on a WAN or LAN interface.
WAN Interfaces (Group of Fields)	This section populates when you add a WAN, a LAN and WAN, or a PPPoE interface for a port, with one row for each port: 
◦ Port Number	Prepopulated with the number of the WAN port you select in the Device Port Configuration box, including PPPoE and LTE interfaces. If you select Redundancy in the General tab, this field shows port mapping of the redundant CPE. When you select a LAN interface on the Primary device, LAN interfaces are automatically selected on the redundant device.

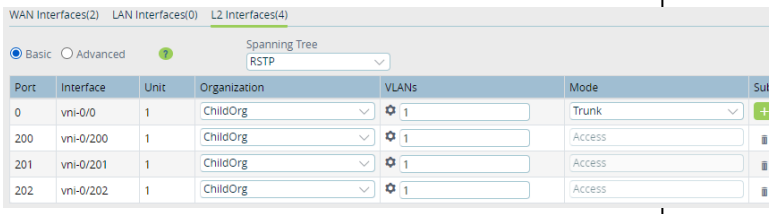
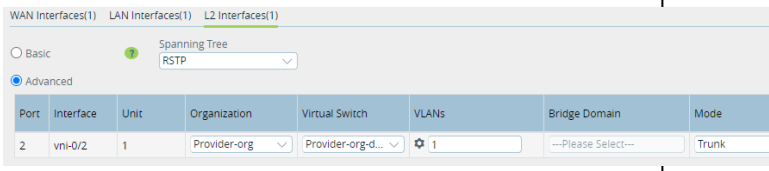
	If the active, redundant CPEs are not connected to the exact same WAN networks, select a cross-connect port on the Primary device.
◦ Interface	Prepopulated with the vni interface and subinterface numbers based on the port you select in the Device Port Configuration box.
◦ VLAN ID	Enter the VLAN identifier for the subinterfaces. To parameterize the VLAN ID, click the ⚙ Parameterize icon.
◦ Network Name	Select the network to which the WAN interface connects. To create a new network name, click + Create WAN Network. In the Create WAN Interface popup window, enter the following information and then click OK.  ◦ Name (Required)—Enter a name for the WAN interface. ◦ Description—Enter an interface description ◦ Transport Domain (Required)—Click to select the transport domain: ▪ Internet ▪ MPLS

	◦ To create a transport domain, click + Transport Domain and enter the following information:  ▪ Name— (Required) Enter a transport domain name. ▪ Description—Enter a transport domain description. ▪ Transport Domain ID —(Required) Enter a transport domain ID.
◦ Priority	Enter a number for the link priority for WAN traffic. To parameterize the priority, click the Parameterize icon. If you do not assign a priority to a WAN circuit, the SD-WAN traffic steering engine adds the WAN interface to the default forwarding profile and assigns the default priority (which is the lowest priority) to the interface. (The traffic steering engine creates a default forwarding profile that is based on the configured priorities of the WAN circuits and uses this forwarding profile to steer all traffic originating from the site.) For example, if the traffic steering engine assigns the MPLS circuit priority 1 and the broadband circuit priority 2, the traffic uses MPLS as the primary circuit, because this circuit has a higher priority, and traffic fails over to the broadband circuit. If you do not assign a priority to the broadband circuit, the same behavior occurs because the broadband circuit has been assigned the default priority, which is the lowest priority. If you do not assign a priority to either the

	MPLS or broadband circuit, they both have the default priority, and traffic is load-balanced between them. It is recommended that you use the default forwarding profile for simple uses cases. To create more advanced traffic steering policies that involve SLA-based link and path prioritization, see Configure SD-WAN Traffic Steering. *Default*: None *Range*: 1 through 15 (1 is the highest priority and 15 is the lowest priority) (for Releases 22.1.1 and later); 1 through 8 (for Releases 21.2 and earlier)
◦ IPv4	Use IPv4 addressing on the WAN interface. ◦ Static—Use static IP addresses. When you select Static, a bind-data variable for the interface's static address is automatically generated in the template. ◦ DHCP—Use DHCP to obtain an IP address.
◦ IPv6	Use IPv6 addressing on the WAN interface. ◦ Static—Use static IP addresses. When you select Static, a bind-data variable for the interface's static address is automatically generated in the template. ◦ DHCP—Use DHCP to obtain an IP address.
◦ Circuit Type	Select access circuit type such as broadband, IP, or MPLS.
◦ Circuit Media	Select physical medium used by the access circuit Select the access circuit type: ◦ DSL ◦ LTE ◦ T1 ◦ T3 ◦ Cable

	◦ Ethernet
◦ Circuit Tags	Click Add Tag icon. In the Manage Tags popup window, enter the circuit tag name an click OK. 
◦ Subinterface	Click the Add icon to add a subinterface on the WAN port. Another row is added to the WAN Interfaces table. For the subinterface, configure all the fields described above.
◦ Link Monitor	Select to monitor the reachability of the next hop or remote IP address on the WAN interface. If the monitored address becomes unreachable, DIA traffic is directed to another WAN interface if possible.
◦ Allow SSH to CPE	Click to allow SSH sessions to the CPE device on the underlay IP address of WAN interface.
◦ Circuit Provider	Enter the access circuit service provider's name.
◦ Bandwidth (Kbps) (Group of Fields)	
◦ Downlink	Enter the bandwidth available on the link for downloading data, in kilobytes per second (Kbps). *Range*: 1 through 10000000 Kbps *Default*: None

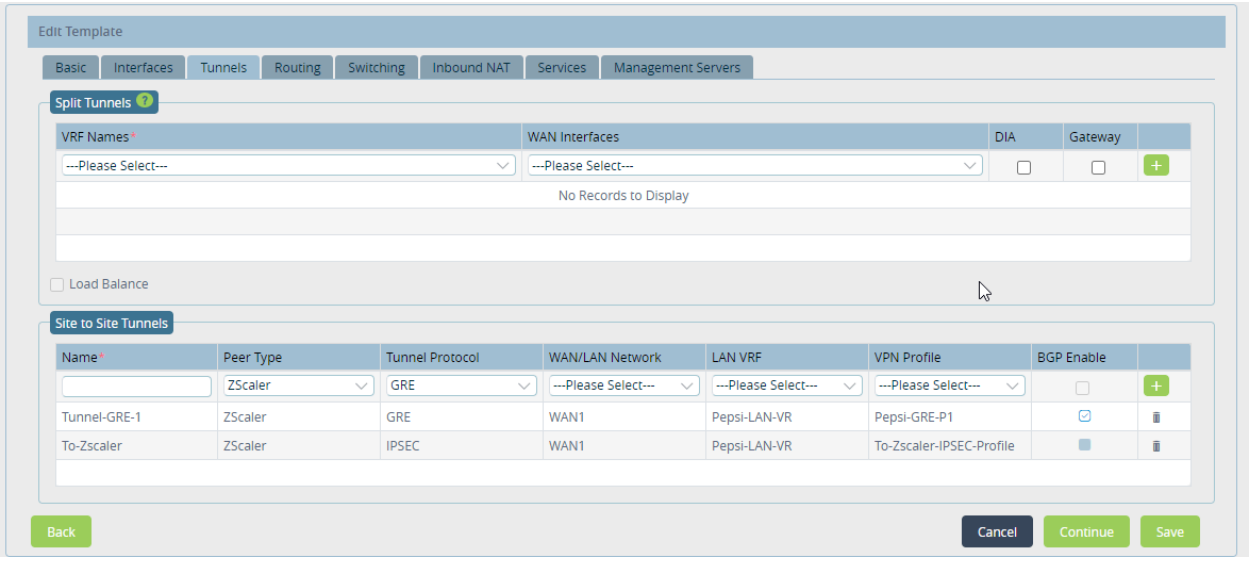
◦ Uplink	Enter the bandwidth available on the link for uploading data, in kilobytes per second (Kbps). *Range*: 1 through 10000000 Kbps *Default*: None
LAN Interfaces (Group of Fields)	This section populates when you add LAN interfaces or WiFi ports, with one row for each port. 
◦ Port Number	Prepopulated with the number of the port you select in the Device Port Configuration box.
◦ Interface	Prepopulated with the vni interface and subinterface numbers based on the port you select in the Device Port Configuration box.
◦ VLAN ID	Enter the VLAN ID for the subinterfaces. To parameterize the VLAN ID, click the Parameterize icon.
◦ Network Name	Select the network to which the interface connects.
◦ Organization	Select the organization to which the interface belongs.
◦ Zones	Select the zone to which the interface belongs. If you do not select a zone, the interface is automatically associated with a zone based on the LAN network name.
◦ Routing Instance	Select the organization's routing instance with which the LAN interface is associated.
◦ IPv4	Use IPv4 addressing on the LAN interface. ◦ Static—Use static IP address.es When you select Static, a bind-data variable for the interface's static address is automatically generated in the template. ◦ DHCP—Use DHCP to obtain an IP address.

◦ IPv6	Use IPv6 addressing on the LAN interface. ◦ Static—Use static IP addresses. When you select Static, a bind-data variable for the interface's static address is automatically generated in the template. ◦ DHCP—Use DHCP to obtain an IP address.
◦ Sub Interface	Click the Add icon to add a subinterface on the LAN port. Another row is added to the WAN Interfaces table. For the subinterface, configure all the fields described above.
Layer 2 Interfaces (Group of Fields)	(For Releases 21.1.1 and later.) This section populates when you add Layer 2 interfaces for a port, with one row for each port.
◦ Basic	Click to create a simple Layer 2 configuration. Enter information for the following fields. 
◦ Advanced	Click to create an advanced configuration, such as a service provider configuration. Enter information for the following fields. 
◦ Spanning Tree	Select the spanning tree protocol: ◦ None ◦ MSTP ◦ RSTP ◦ STP
◦ Port Number	Prepopulated with the number of the Layer 2 port

	(wired or WiFi) that you selected in the Device Port Configuration box.
◦ Interface	Prepopulated with the VIN interface and subinterface numbers of the port you selected in the Device Port Configuration box.
◦ Unit	Autogenerated unit or subinterface number of the Layer 2 interface. The first interface has unit ID 1, and subsequent interface unit IDs are generated in sequential order. Note that a WiFi port can have only one unit.
◦ Organization	Select the organization to which the Layer 2 interface belongs.
◦ VLANs	Select a VLAN to associate with the Layer 2 interface. To parameterize the VLAN ID, click the Parameterize icon. Note that when you parameterize the VLAN ID in the device workflow, you can enter only one value. If you need IRB-LAN support for the parameterized VLAN, copy and paste the same variable name from the Layer 2 tab to the IRB LAN row in the LAN tab.
◦ Virtual Switch	For the Advanced option, select a virtual switch to associate with the Layer 2 interface. The drop-down list displays the virtual switches associated with the organization.
◦ Bridge Domain	For the Advanced option, select the bridge domain for the Layer 2 interface. Selecting a bridge domain enables VLAN translation on the subinterface.
◦ Mode	Select the subinterface traffic mode for the VLAN: ◦ Access ◦ Trunk For WiFi ports, the mode is always Access. If the VLANs or bridge domains have more than one VLAN ID, the mode must be trunk. If there are multiple subunits, only one subunit can be in Access mode.
◦ Subinterface	Click the Add icon to add a subinterface on the

	Layer 2 port. Another row is added to the Layer 2 Interfaces table. For the subinterface, configure all the fields described above.
◦ More	Click More to configure additional attributes for the interfaces. The Native VLAN ID popup window displays. Note that these attributes are configured at port level, not for subinterfaces. Native VLAN ID: enter the Native VLAN ID of the port. Native VLAN ID is required only if the mode of sub-units is Trunk. *Range*: 1 to 4094
◦ Native VLAN ID	When the subunit mode is Trunk, cnter the native VLAN ID of the port. *Range:* 1 through 4094

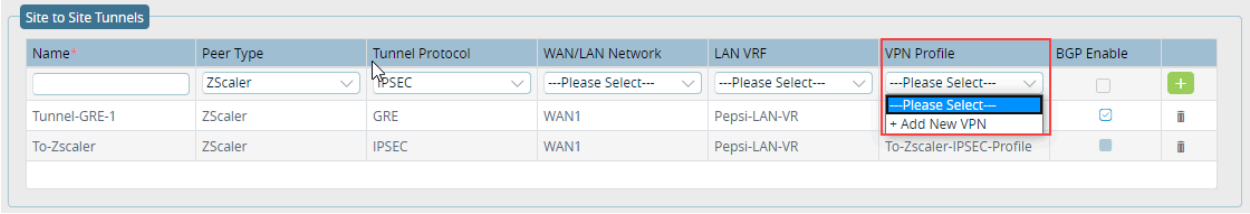
7. Click Continue.
8. Select the Tunnels tab to create split tunnels and site-to-site tunnels. (You can configure site-to-site tunnels for Releases 20.2 and later.) Split tunnels allow traffic to flow from a common source to different destinations over different interfaces. For example, you can configure a split tunnel to allow traffic to flow from a common source to an SD-WAN site and a non–SD-WAN site. Enter information for the following fields.



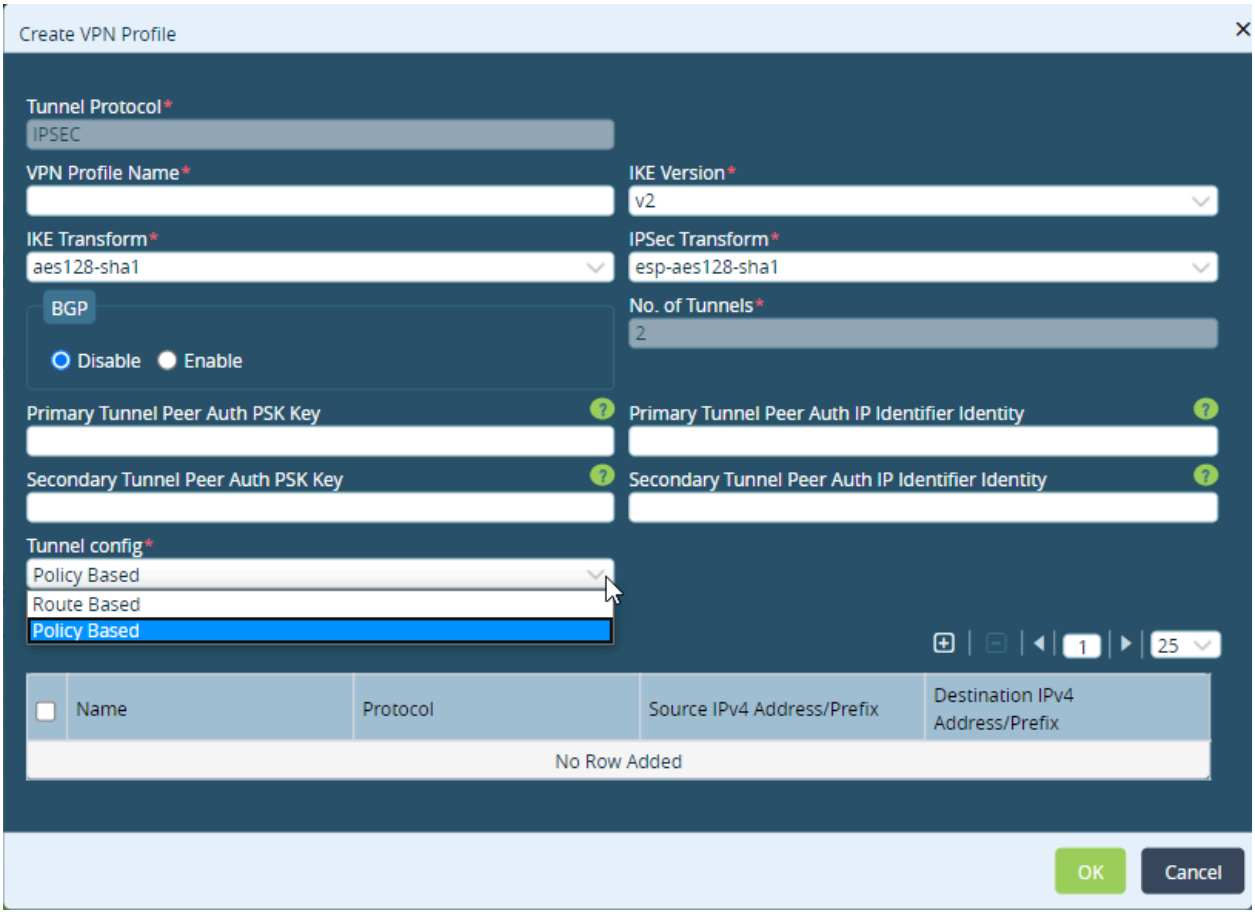
Field	Description
Split Tunnels (Group of Fields)	
◦ VRF Names	Select the name of the VRF.
◦ WAN Interfaces	Select the name of the WAN interface. If you select more than two WAN interfaces from the same LAN VR to configure direct internet access (DIA), the interface that is first on the list has the highest priority unless you enable load balancing by clicking Load Balance.
◦ DIA	Click to enable DIA. Source NATing is performed before packets are sent out to the WAN interface.
◦ Gateway	Click to allow the local router to act as a gateway between other SD-WAN sites and non–SD-WAN sites. The traffic between SD-WAN and non–SD-WAN sites flows through the gateway SD-WAN device. In gateway mode, routes that the router learns from an SD-WAN overlay are advertised to MPLS PE routers, and routes that the router learns from MPLS PE routers are advertised to SD-WAN overlay. Note that you do not need to configure split tunnels on SD-WAN sites.
◦  Add icon	Click the  Add icon to add the split tunnel to the template.
◦ Load Balance	Click to enable balancing of the traffic load among the split tunnels if you have more than one split tunnel.
Site-to-Site Tunnels (Group of Fields)	
◦ Name	Enter a name for the site-to-site tunnel.
◦ Peer Type	Select the hosted-cloud or peer type, depending on the device at the other end of the tunnel: ◦ Azure Virtual WAN—Deploy a tunnel on Azure Virtual WAN. ◦ AWSTransitGW—Deploy a tunnel on AWS transit endpoint. ◦ Others—Deploy a tunnel on a third-party device that supports IPsec tunnels, such as Cisco, Juniper, and Palo Alto. ◦ Zscaler—Deploy a tunnel on a Zscaler endpoint.

Field	Description
Tunnel Protocol	Select the tunnel protocol to use to reach the peer: ◦ IPsec—Default tunnel protocol for the peer types AWS Transit Gateway, Azure Virtual WAN, Others, and Zscaler. ◦ GRE—Select GRE for the peer types AWS Transit Gateway (for Releases 22.1 and later) and Zscaler.
◦ WAN/LAN Network	Select the network to use. For the peer types AWS Transit Gateway and Azure Virtual WAN, you can select only WAN networks. For the peer types Zscaler and Others, you can select any network.
◦ LAN VRF	Select the virtual routing instance to use to reach the LAN, to allow users in the routing instance to access the tunnel to communicate with the gateway. The virtual routing instance is the tunnel termination endpoint.
◦ VPN Profile	When you select the peer type Zscaler or Others and a virtual routing instance, select a VPN profile to associate with the tunnel and with the LAN VRF organization. If a VPN profile is not available, create one, as described in Step 11. When the peer type is Zscaler, you must create VPN profile with two tunnels, and this field lists only VPN profiles with two tunnels. When you select the peer type Others or Zscaler, and if a VPN profile is not available, click the + Add New VPN option in the VPN Profile field. See Steps 9 and 10, below.
◦ BGP Enabled	For the peer type Azure Virtual WAN, click to enable BGP. For the peer type AWS Transit Gateway, this field is checked automatically. For the peer types Zscaler and Others, this field is checked automatically if BGP is enabled in the VPN profile, and it is not checked if BGP is not enabled in the VPN profile.
◦  Add icon	Click the  Add icon to add the site-to-site tunnel to the template.

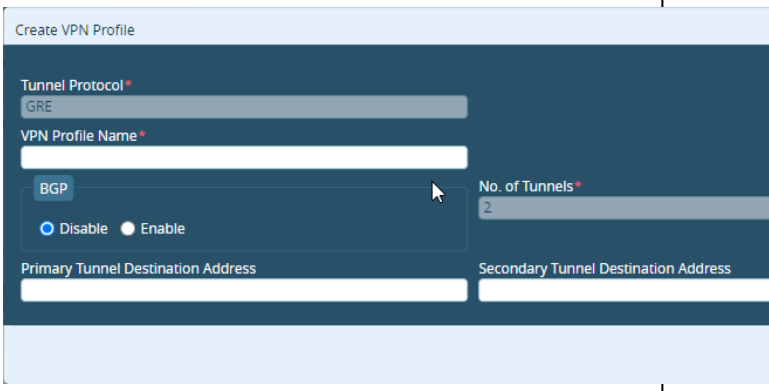
9. If you select the peer type Others or Zscaler, and if a VPN profile is not available, click the + Add New VPN option in the VPN Profile field.

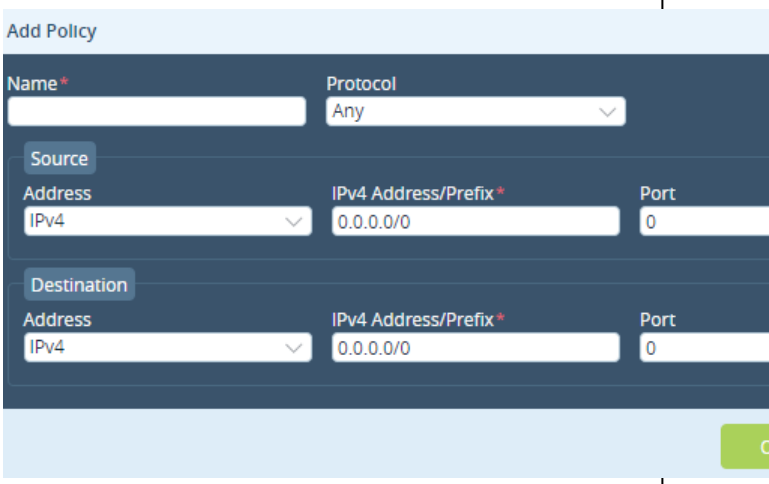


10. In the Create VPN Profile popup window, enter information for the following fields.



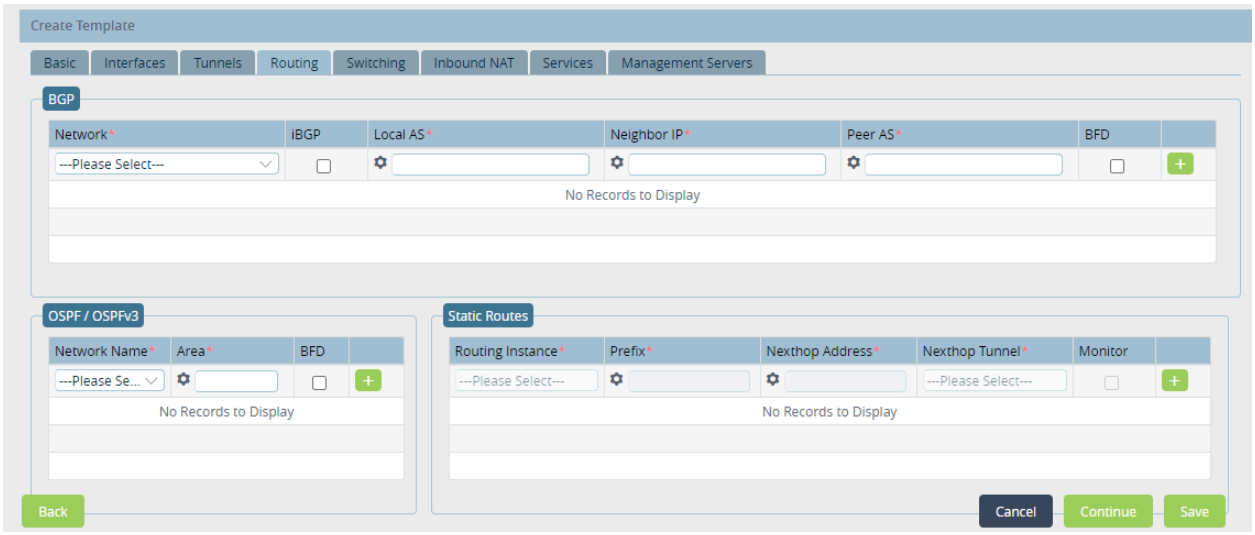
Field	Description
Tunnel Protocol (Required)	IPsec or GRE tunnel protocol for the peer type that you selected when you configured the site-to-site tunnel is selected automatically.
VPN Profile Name (Required)	Enter a name for the VPN profile.
IKE Version (Required	Select the IKE version: ◦ v1 ◦ v2 ◦ v2-or-v1
IKE Transform (Required)	Select the IKE transform algorithm to use for data encryption.
IPsec Transform (Required)	Select the IPsec transform algorithm to use for data encryption.
BGP	Select the BGP state: ◦ Disable ◦ Enable
No. of Tunnels (Required)	Enter how many tunnels to create between the VOS device and the Zscaler unmanaged device or between the VOS device and the third-party managed device. For Zscaler tunnels, you must create two tunnels.
For the IPsec tunnel protocol	Enter information for the following fields.
◦ Primary Tunnel Peer Authenticaiton PSK Key	Enter the primary tunnel preshared key (PSK) to use with the peer. If you leave this field empty, you are prompted to enter the peer authentication key in the device bind data when you deploy the workflow.
◦ Primary Tunnel Peer Authentication IP Identifier Identity	Enter the primary tunnel IP address of the peer authentication device. If you leave this field empty, you are prompted to enter the peer authentication IP identifier identity under device bind data when you deploy the workflow.
◦ Secondary Tunnel Peer Authentication PSK Key	Enter the secondary tunnel PSK to use with the peer. If you leave this field empty, you are prompted to enter the peer authentication key in the device bind

	data when you deploy the workflow.
◦ Secondary Tunnel Peer Authentication IP Identifier Identity	Enter the secondary tunnel IP address of the peer authentication device. If you leave this field empty, you are prompted to enter the peer authentication IP identifier identity under device bind data when you deploy the workflow.
For the GRE tunnel protocol	Enter information for the following fields: 
◦ Primary Tunnel Destination Address	Enter the primary tunnel destination IP address of the authentication device.
◦ Secondary Tunnel Destination Address	Enter the secondary tunnel destination IP address of the authentication device.
Tunnel Configuration (Required)	Select the tunnel configuration.
◦ Route Based	Use a route-based configuration.
◦ Policy Based	Use a policy-based configuration. If you select this option, click the Add icon to add a policy. In the Add Policy popup window, enter information for the following fields.

	 ◦ Name—Enter a name for the policy. ◦ Protocol—Select a protocol: ▪ ICMP ▪ TCP ▪ UDP ◦ Source (Group of Fields)—Enter information about the traffic source: ▪ Address—Select the IPv4 address type. ▪ IPv4 Address/Prefix—Enter the IPv4 source prefix or address. ▪ Port—Enter the source port number. ◦ Destination (Group of Fields)—Enter information about the traffic destination: ▪ Address—Select the IPv4 address type. ▪ IPv4 Address/Prefix—Enter the IPv4 destination prefix or address. ▪ Port—Enter the source port number. ◦ Click OK.

11. Click Continue.

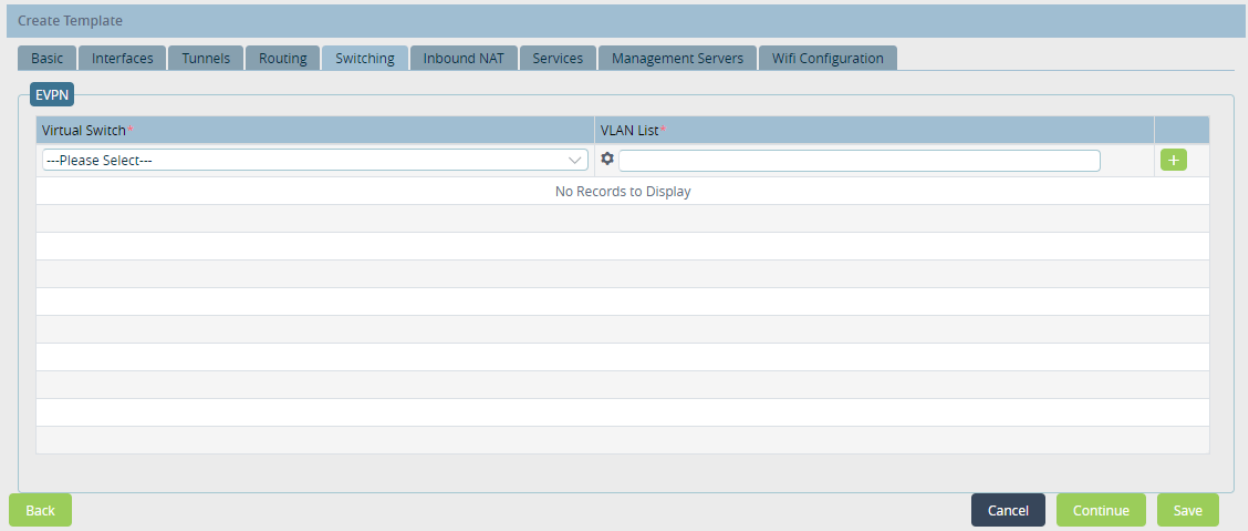
12. Select the Routing tab to configure BGP, OSPF, and static routing. For each routing protocol, click the Parameterize icon to generate the routing information dynamically, or enter information for the following fields and then click the Add icon.



Field	Description
BGP (Group of Fields)	Configure BGP.
◦ Network	Select the name of the network on which to configure BGP.
◦ Local AS	Enter the local autonomous system (AS) number. To parameterize the local AS number. click the Parameterize icon.
◦ Neighbor IP	Enter the IP address of the BGP neighbor (peer). To parameterize the IP address, click the Parameterize icon.
◦ Peer AS	Enter the AS number of the peer. To parameterize the peer AS number, click the Parameterize icon.
◦ Add icon	Click the Add icon to add the BGP configuration to the template.
OSPF/OSPFv3 (Group of Fields)	Configure OSPF.
◦ Network Name	Select the name of the network on which to configure OSPF
◦ Area	Enter the OSPF area number.
◦ BFD	Click to enable BFD.
Add icon	Click the Add icon to add the OSPF configuration to the template.
Static Routes (Group of Fields)	Configure static routing.
◦ Routing Instance	Select the name of the routing instance in which to configure the static route.
◦ Prefix	Enter the prefix and prefix length of the static route. To parameterize the IP prefix, click the Parameterize icon.
◦ Next Hop	Enter the IP address of the next hop. To parameterize the next hop IP address, click the Parameterize

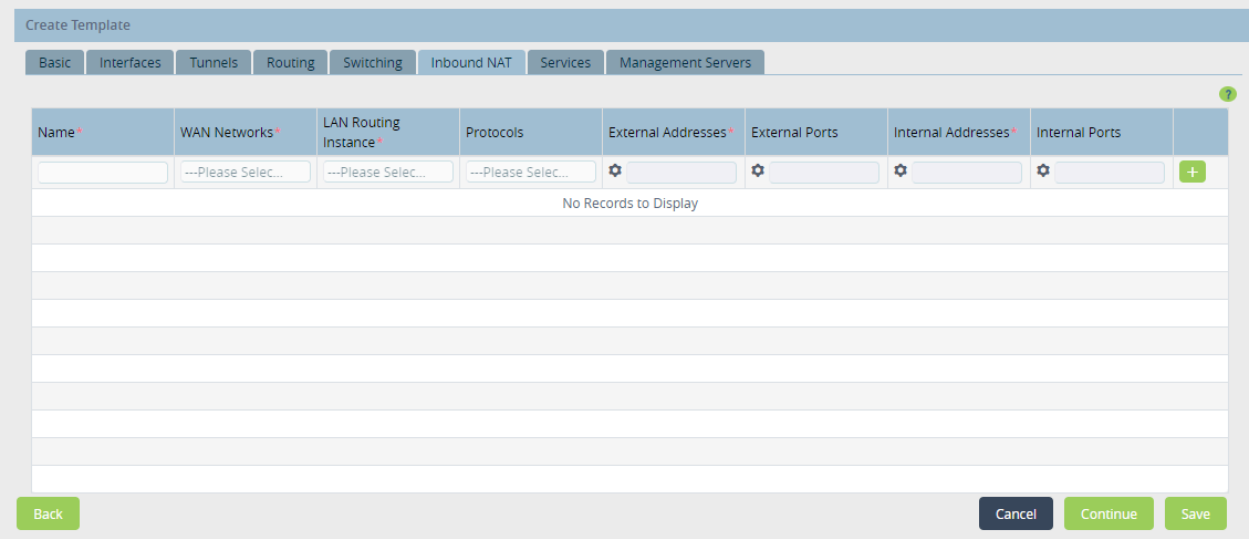
	icon.
Add icon	Click the Add icon to add the static route to the template.

9. Click Continue.
10. (For Releases 21.1.1 and later.) Select the Switching tab to configure Ethernet VPN (EVPN) over SD-WAN. Note that this tab is displayed only when you select Layer 2 as the type of interface in the Interfaces tab, in Step 6, above. Enter information for the following fields.



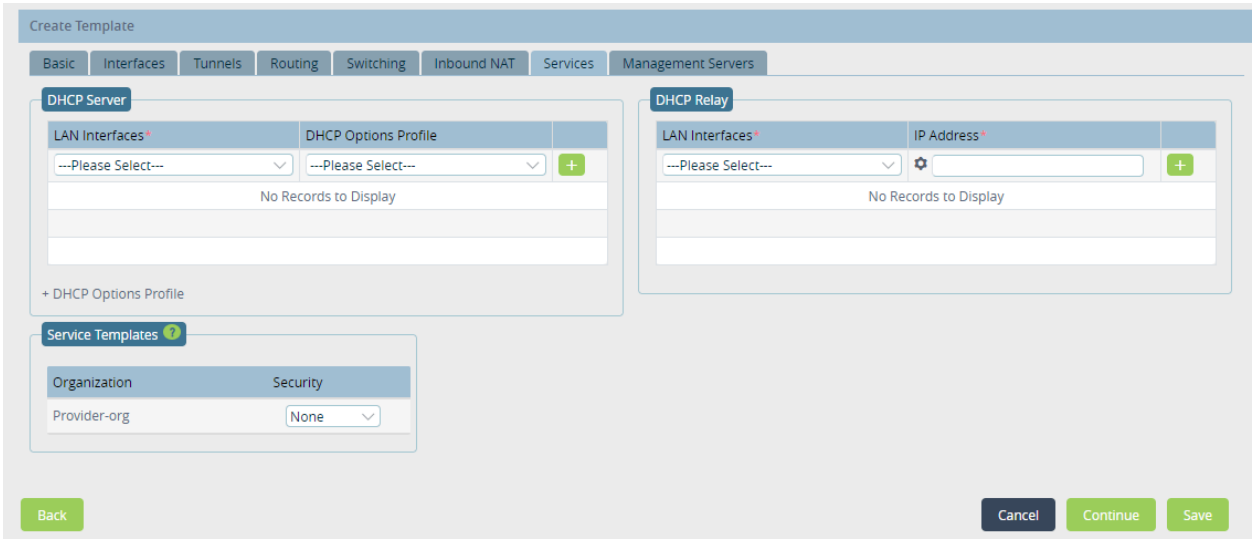
Field	Description
Virtual Switch	Select the VLAN switch to associate with EVPN. For each virtual switch, the workflow configures the following: ◦ Unique route distinguisher (RD) and route target (RT) values ◦ VLANs for all the VLAN fields in the Interfaces tab for which EVPN is enabled ◦ Family Layer 2 VPN-EVPN in the control virtual router (VR) of the associated organization
VLAN List	Enter the VLANs. You can enter individual VLANs or VLAN ranges, separated by commas. If you add more than one row, with different VLANs or VLAN ranges, for each virtual switch, ensure that you avoid duplicate and overlapping values. Click the Parameterize icon to enter the default parameterized variable. If you edit the parameterized value, you must retain the {$v*__*} format.

11. Select the Inbound NAT tab to configure NAT rules so that traffic inbound from an external network can reach internal LAN servers. Enter information for the following fields.



Field	Description
Name	Enter a name for the NAT rule.
WAN Network	Select the WAN network on which to enable inbound NAT port forwarding.
LAN Routing Instance	Select the routing instance that connects the internal LAN server to the CPE.
Protocol	Select the protocol of the application that runs on the internal LAN server: ◦ ICMP ◦ TCP ◦ UDP
External Addresses	Enter the IP prefix or a range of IP addresses for the WAN interface to use for NAT. To enter a range, separate the IP addresses with a hyphen; for example, 1.1.1.1-1.1.1.2.
External Ports	Enter the external ICMP, TCP, or UDP port or port range for the WAN interface to use for NAT.
Internal Addresses	Enter the IP prefix or a range of IP addresses of the LAN servers to which to send NATed traffic. To enter a range, separate the IP addresses with a hyphen; for example, 1.1.1.1-1.1.1.2.
Internal Ports	Enter the external ICMP, TCP, or UDP port or port range to which to send NATed traffic.
Add icon	Click the Add icon to add the inbound NAT instance.

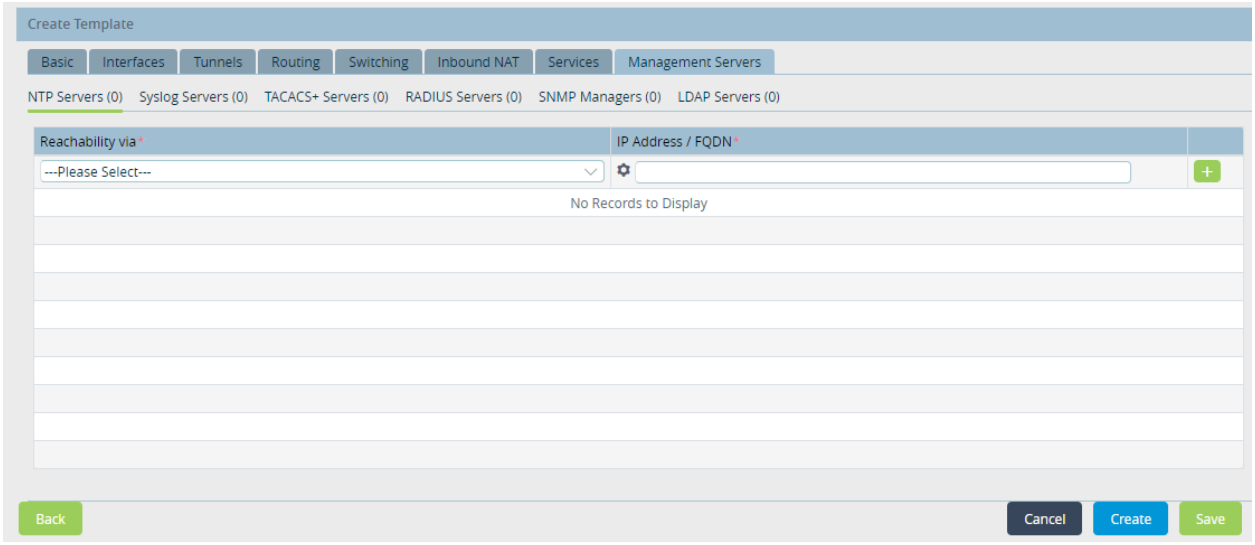
12. Click Continue.
13. Select the Services tab to configure DHCP servers and relays, and service templates. Enter information for the following fields.



Field	Description
DHCP Server (Group of Fields)	Enable DHCP server functionality on a LAN interface
◦ LAN Interfaces	Select the LAN interface to act as a DHCP server.
◦ DHCP Options Profile	Select the DHCP options profile for the DHCP server to use
◦  Add icon	Click the  Add icon to add the DHCP server configuration to the template.
DHCP Relay (Group of Fields)	Configure a DHCP relay server.
◦ LAN Interfaces	Select the LAN interface to act as a DHCP relay server.
◦ IP Address	Enter the IP address for the DHCP relay server
◦  Add icon	Click the  Add icon to add the DHCP server configuration to the template.
Service Templates (Group of Fields)	Configure service templates. Service templates to define common configurations for a specific network function or service. You can associate a service template with one or more device templates.
◦ Organization	Displays the name of the organization.
◦ Security	Select the type of security protocol to implemented in the template: ◦ None—Do not use security. ◦ NGFW—Use the security provided by next-generation firewalls. ◦ SFW—Use the security provided by the selected stateful firewall.
◦ Applications	Select one or more security service templates, which define common security policies, to apply to the configuration.
◦ Advanced CoS	Select one or more advanced CoS service templates, which configure advanced CoS policies.

◦ Service Chains	Select one or more service chain service templates. You use these templates to chain third-party VNFs or PNFs on uCPE.
◦ General	Select one or more general service chains.

14. Click Continue.
15. Select the Management Servers tab, configure information for various network servers. Enter information for the following fields.



Field	Description
NTP Servers (Group of Fields)	Configure NTP servers.
◦ Reachability via	Select the network to use to reach the NTP server.
◦ IP Address	Enter the IP address of the NTP server. To parameterize the IP address, click the Parameterize icon.
◦ Add icon	Click the Add icon to add the NTP server to the template
Syslog Servers (Group of Fields)	Configure syslog servers.
◦ Reachability via	Select the network to use to reach the syslog server.

Field	Description
◦ IP Address	Enter the IP address of the syslog server. To parameterize the IP address, click the Parameterize icon.
◦ Add icon	Click the Add icon to add the syslog server to the template
TACACS+ Servers (Group of Fields)	Configure TACACS+ servers.
◦ Reachability via	Select the network to use to reach the TACACS+ server.
◦ IP Address/FQDN	Enter the IP address or fully qualified domain name of the TACACS+ server. To parameterize the IP address or domain name, click the Parameterize icon
◦ Authentication Key	Enter the authentication key, or password, of the TACACS+ server. To parameterize the key, click the Parameterize icon.
◦ Actions	Select one or both TACACS+ server actions: ◦ Accounting—Log all TACACS+ activity. ◦ Authentication—Use TACACS+ authentication to determine whether a user can access a system.
◦ Add icon	Click the Add icon to add the TACACS+ server to the template
RADIUS Servers (Group of Fields)	Configure RADIUS servers.
◦ Reachability via	Select the network to use to reach the RADIUS server.
◦ IP Address/FQDN	Enter the authentication key, or password, of the TACACS+ server. To parameterize the key, click the Parameterize icon.
Authentication Key	Enter the authentication key, or password, of the RADIUS server. To parameterize the key, click the Parameterize icon.

Field	Description
◦ Actions	Select one or more RADIUS server actions: ◦ Accounting—Log all RADIUS activity. ◦ Authentication—Use RADIUS authentication to determine whether a user can access a system. ◦ WiFi Authentication—Use RADIUS authentication to allow a device to access a WiFi network.
◦ Add icon	Click the Add icon to add the RADIUS server to the template
SNMP Managers (Group of Fields)	Configure SNMP servers.
◦ Versions	Select the version or versions of version to use: ◦ v1 ◦ v2c ◦ v3
◦ Community	Enter the SNMP community string to use to access the SNMP server.
◦ Username	For SNMPv3, enter the username to access the SNMP server. To parameterize the username, click the Parameterize icon.
◦ Password	For SNMPv3, enter the password to access the SNMP server. To parameterize the password, click the Parameterize icon.
◦ Reachability via	Select the network to use to reach the SNMP server.
◦ IP Address	Enter the IP address of the SNMP server. To parameterize the IP address, click the Parameterize icon.
◦ Add icon	Click the Add icon to add the SNMP server to the template
LDAP Servers (Group of Fields)	Configure LDAP servers.

Field	Description
◦ Reachability via	Select the network to use to reach the LDAP server.
◦ IP Address/FQDN	Enter the IP address or fully qualified domain name of the LDAP server. To parameterize the IP address or domain name, click the Parameterize icon.
◦ Domain Name	Enter the domain name in which the LDAP server resides. To parameterize the domain name, click the Parameterize icon.
◦ Base DN	Enter the point from which the LDAP server searches for users. For example, DC=example-domain,DC=com
◦ Bind DN	Enter the user and user's location in the LDAP directory tree. For example, CN=username,CN=Users,DC=example-domain,DC=com
◦ Bind Password	Enter the password to use to authenticate the user.
◦ Add icon	Click the Add icon to add the LDAP server to the template.

18. Click Create. This associates a post-staging template with the controllers, organizations, and other selected entities.

If modify the configuration defined in an existing template, you must redeploy the template for the changes to take effect.

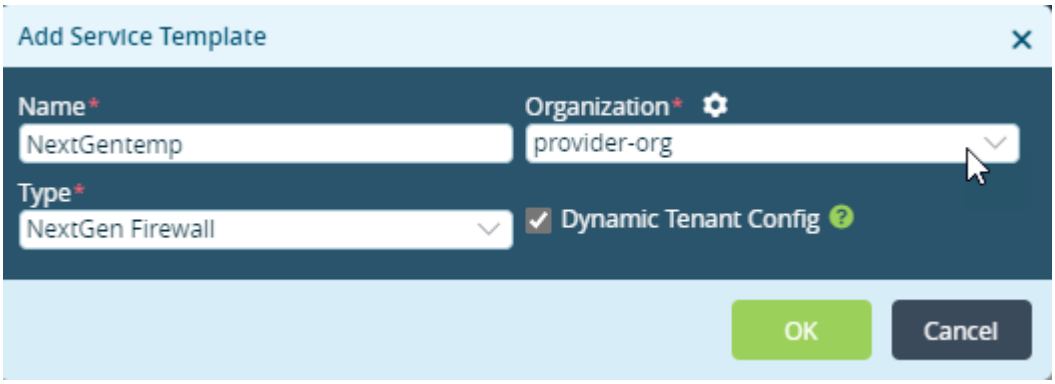
Create Service Templates

You create service templates so that you are able to configure the application-steering, NGFW, QoS, service chain, stateful firewall, and secure access properties for VOS devices. After you create a service template, you associate it with

a device template.

To create a service template:

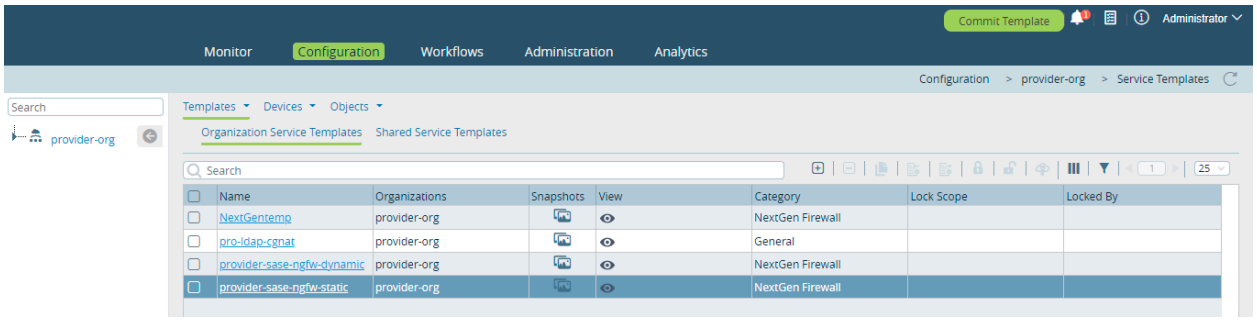
1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Service Templates in the horizontal menu bar.
   c. Select an organization in the main pane.
2. Click the Add icon to add a service template. In the Add Service Template popup window, enter information for the following fields.



Field	Description
Name	Enter a name for the service template.
Organization	Select the organization to associate with the service template.
Type	Select the type of the service template: ◦ Stateful Firewall—Allows you to configure the following services: ▪ DoS protection ▪ Security and security settings ◦ NextGen Firewall—Allows you to configure the following services: ▪ Authentication ▪ Decryption ▪ DoS protection ▪ Security and security settings ▪ Secure web proxy ◦ QoS—Allows you to configure the following services: ▪ AppQoS ▪ Associate interfaces and networks

Field	Description
	▪ Drop profiles ▪ Forwarding class map ▪ QoS profiles ▪ Read-write rules ▪ Schedulers ▪ Scheduler maps ◦ General—Allows you to configure all available services. ◦ Application Steering—Allows you to configure the following services: ▪ Class of service ▪ CoS and SD-WAN policy ▪ Zones ◦ Service Chain—Allows you to configure the following objects: ▪ Address ▪ Address groups ▪ Cloud profiles ▪ Custom objects ▪ Schedules ▪ SNAT pools ◦ Secure Access—Allows you to configure the following objects: ▪ Secure access routes ▪ DNS resolvers ▪ Secure access servers ▪ Secure access profiles ▪ Secure access portal and/or gateway
Dynamic Tenant Configuration	(For Releases 22.1.3 and later.) Click to automatically select the service template an organization is being dynamically instantiated.

3. Click OK. The main pane lists the service template.



To clone, import, or export a template, select the template from the main pane and click the Clone, Import, or Export icon. For more information, see Create and Manage Staging and Post-Staging Templates.

To view the service template configuration in the CLI, click the Eye icon in the View column. For example:

To associate a service template with a device template:

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the horizontal menu bar.
   c. Select an organization in the main pane.
2. Click the Edit icon.
3. Click the Service Templates tab.
4. From the Organization list, select the name of the organization.
5. From the Override list, select an policy override option:
   - No Conflict—Do not override the provider policies defined in the service template
   - Override Referred Template

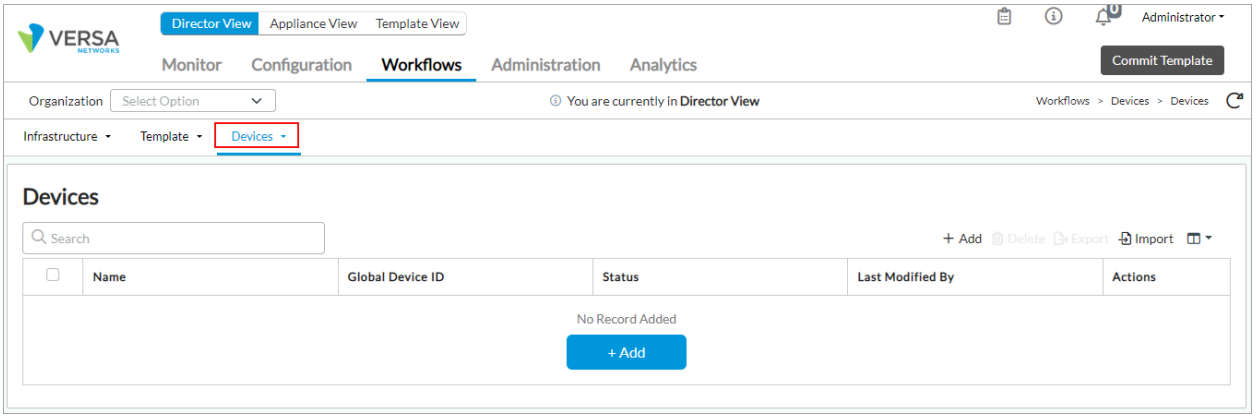
- Override with Referred Template

6. Click the Security button to select the type of security protocol in Service Templates list:
   - Stateful Firewall
   - NextGen Firewall
7. In the Service Class section, select the name of the service template in the Service Templates list.
8. In the General section, select the name of the template from the Service Templates list.
9. Click OK.

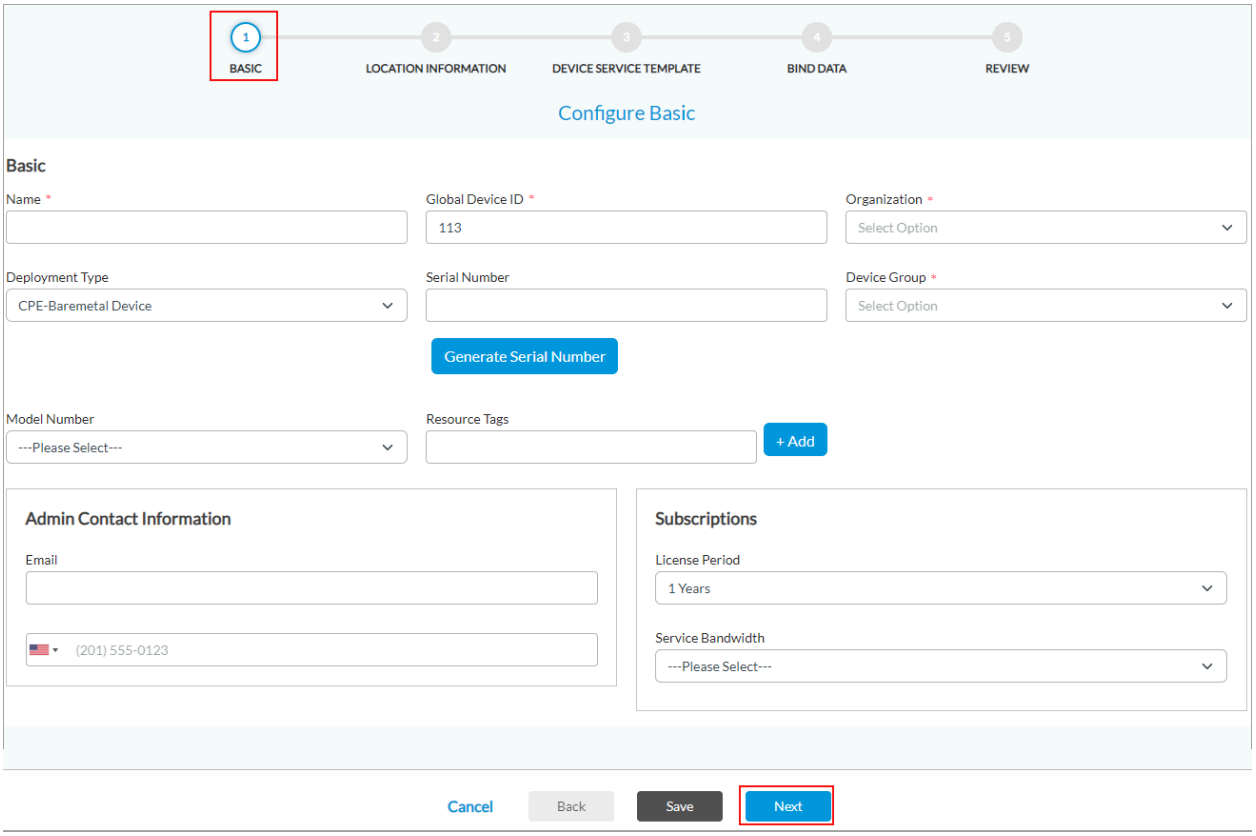
Create Devices and Device Groups

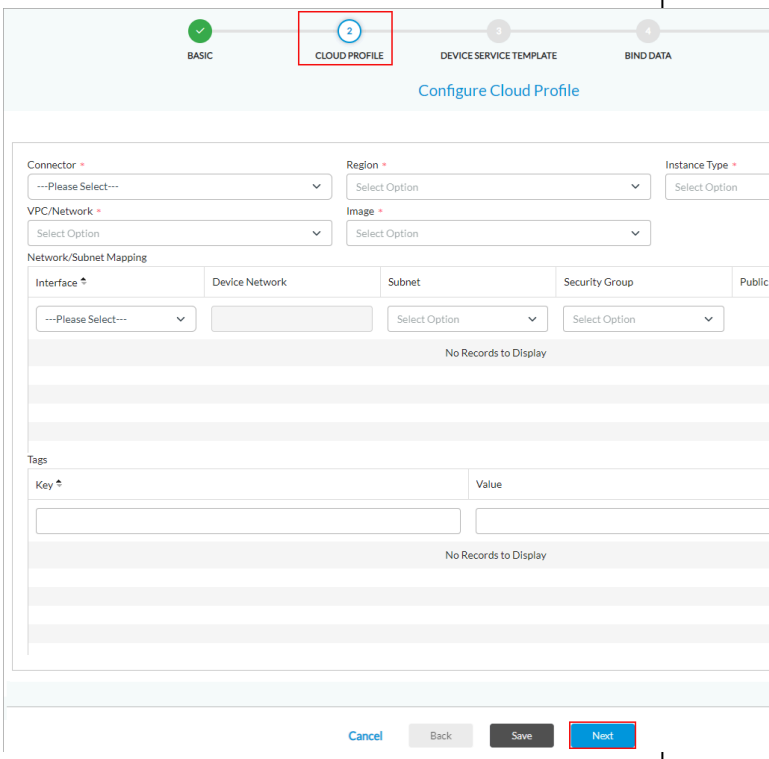
In Releases 22.1.1 and later, you use a workflow wizard to create devices and device groups. Note that the order of the wizard screens depends on what you selected for the Deployment Type and Device Group fields in the Step 1, Basic screen.

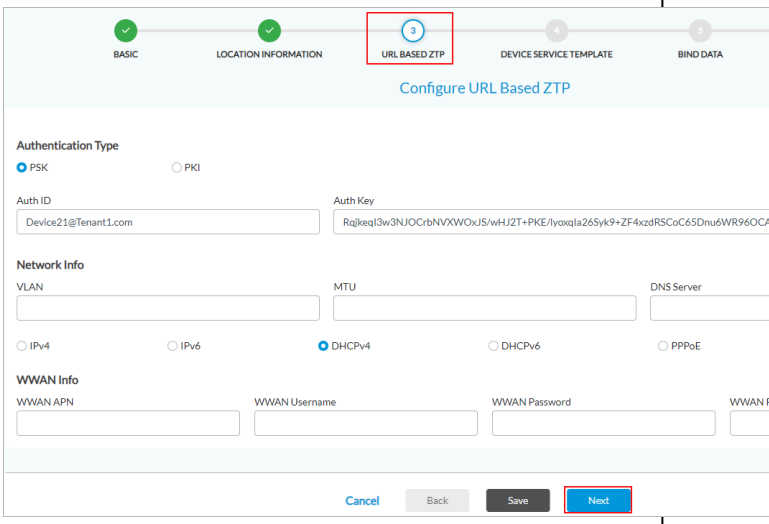
1. In Director view, select the Workflows tab in the top menu bar.
2. Select Devices > Devices in the horizontal menu bar. The following screen displays.

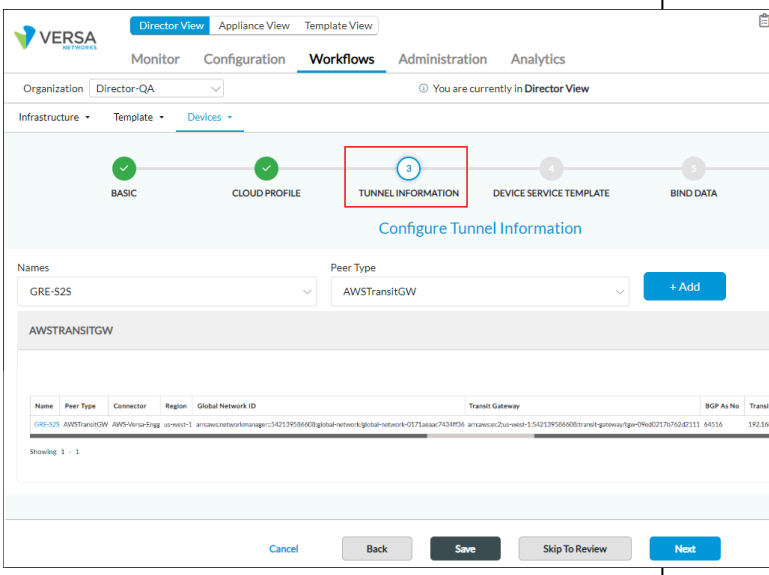


3. Click the + Add to add a device.
4. Click Step 1, Basic. The Configure Basic screen displays. Enter information for the following fields. Note that the URL-Based ZTP tab is displayed only when you select a device group for which URL-based ZTP is enabled. The Tunnel Information tab is displayed when you select a device group that has a template associated with it and the template includes tunnels.

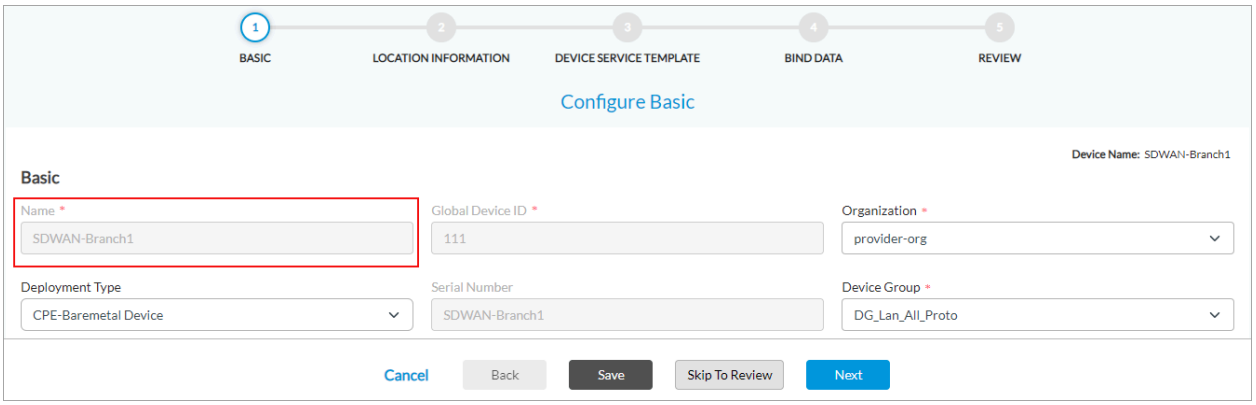


Field	Description
Name	Enter a name for the device.
Global Device ID	Displays ID assigned to the device. The system populates the value automatically with the next available ID. You can change it to a different available value between 1 and 31.
Organization	Select the organization to which the device belongs.
Deployment Type	Select the type of deployment: ◦ CPE Bare-Metal Device ◦ CPE Public Cloud If you select CPE Public Cloud, Step 2 displays the Cloud Profile tab. For more information, see Configure a Public Cloud Device To Be a Virtual CPE Router or an SD-WAN Gateway. 
Serial Number (Required)	Enter the chassis/device ID for the branch device. This must be a unique value per device. Click Generate Serial Number to generate a unique serial

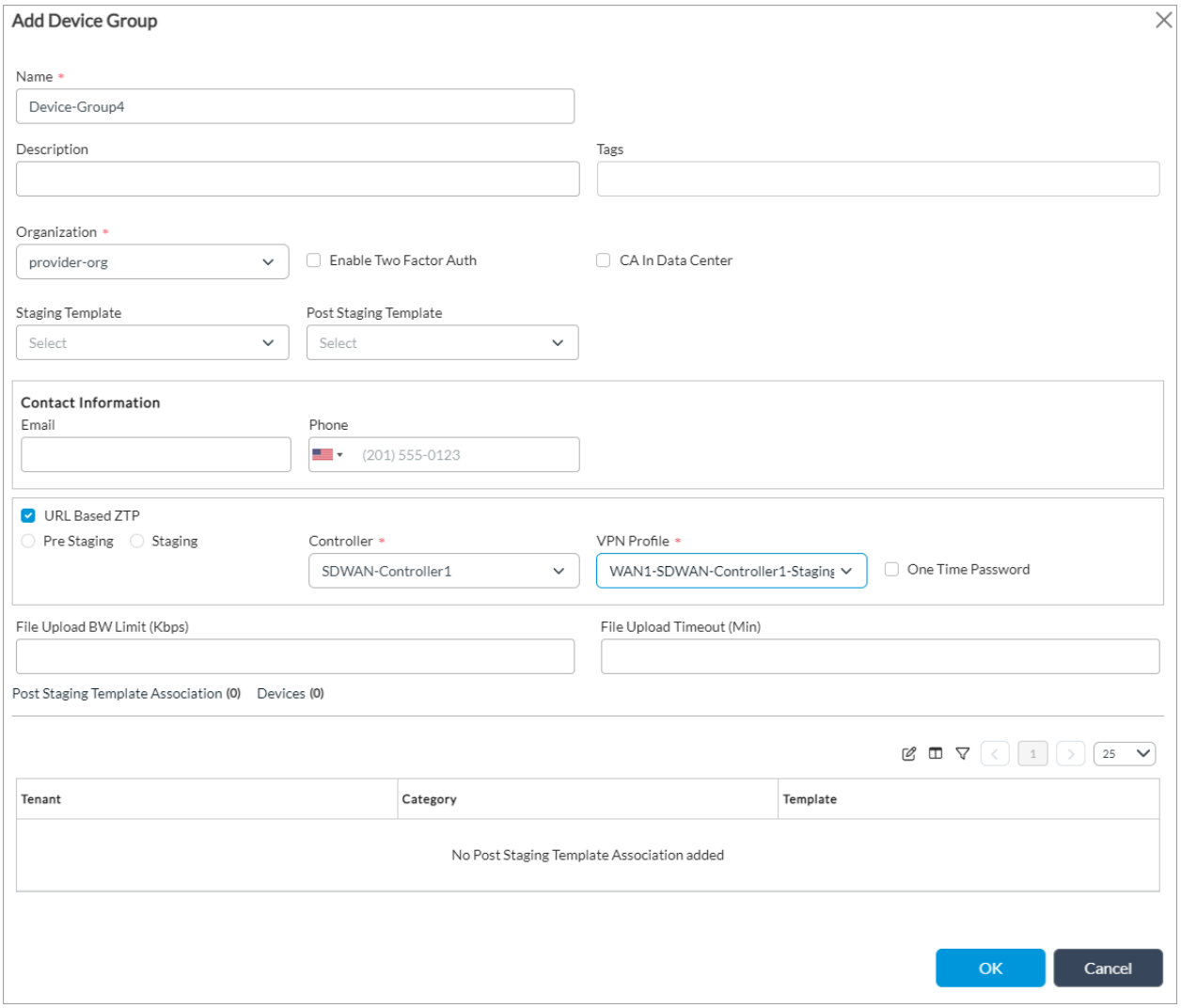
	number.
Device Group	Select the device group to which the device belongs. If you select a device group on which URL-based ZTP is enabled, Step 3 displays the URL-Based ZTP screen. For more information, see Activate VOS Devices.  If you select a device group that has a template associated with it and the template includes tunnels, Step 3 (displayed as Step 4 if URL-Based ZTP is Step 3) displays the Tunnel Information screen. For more information, see Configure Site-to-Site Tunnels.

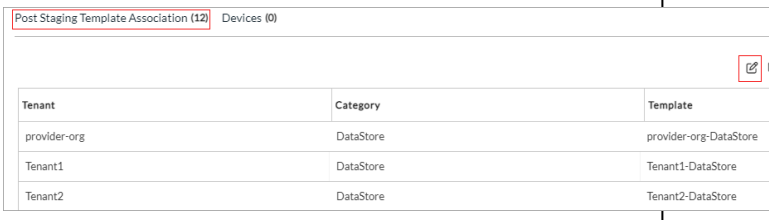
	
Model Number	Select the model of the device.
Resource Tags	(For Releases 22.1.1 and later.) Enter a tag name, and then click Add icon to add the resource tag.
Admin Contact Information	Enter the contact email address and phone number of the administrator.
Subscription (Group of Fields)	For Releases 21.1.1 and later.
◦ Service Bandwidth	Select the bandwidth, in Mbps or Gbps, to use for service that the device offers.
◦ License Period	Select the period, in years, for which the device license is valid. *Values:* 1, 3, 5 years

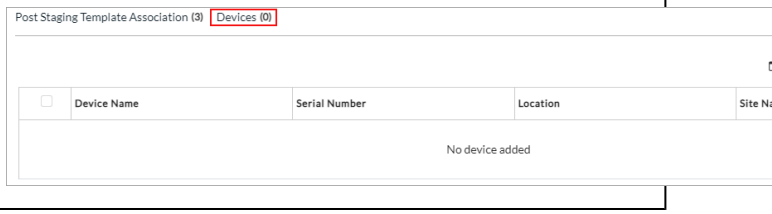
Note that once you deploy a device, you cannot change the name of the device in Versa Director. To change the device name, you must delete the device and add a new device. If you open the Add Device screen after the device has been deployed, the Name field is grayed out (not editable), as shown in the following screenshot.



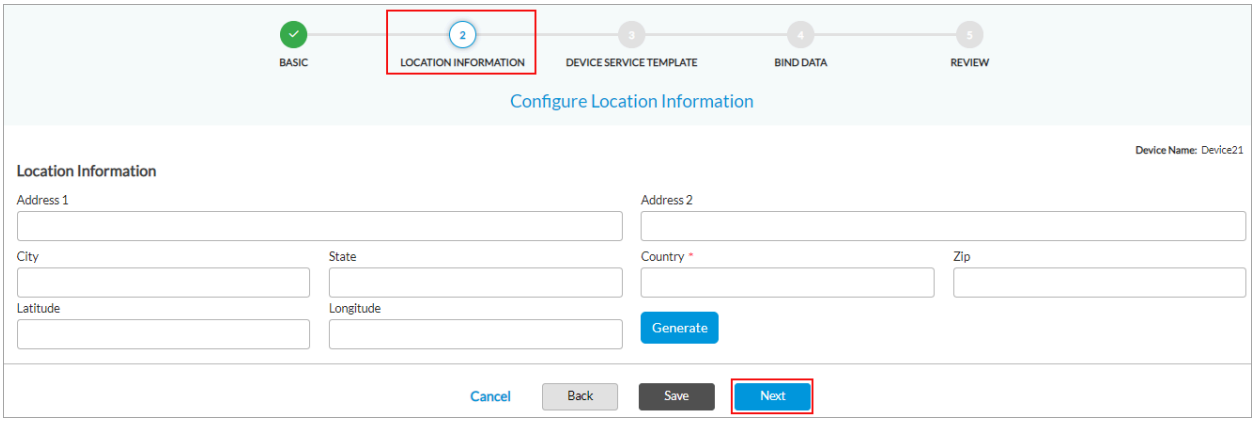
3. To create a device group, click + Device Group. Enter information for the following fields.



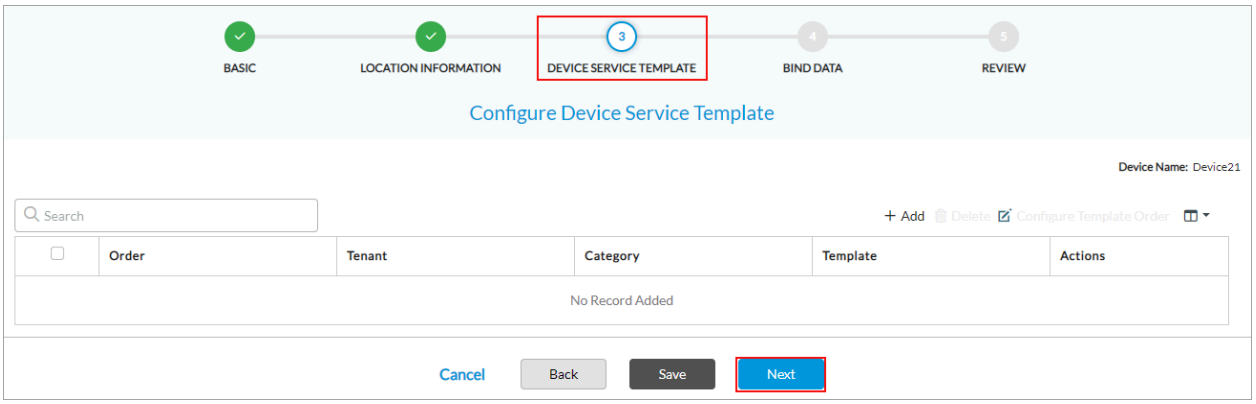
Field	Description
Name	Enter a name for the device group.
Description	Enter a text description for the group.
Tags	Enter a text string or phrase to associate with the rule. Tags allow you to locate a group when you perform a filtered search of all groups. *Value:* Text string from 1 through 255 characters *Default:* None
Organization	Select the organization to which the device group belongs.
Enable Two-Factor Authentication	Click to be notified through email when a branch performs zero-touch provisioning (ZTP).
CA in Data Center	Click to enable certificate authority. If enabled, during global ZTP, the CSR request goes over the IPSec tunnel, and the branch receives a CA-signed certificate. All tunnels that are established use this certificate.
Staging Template	Select the name of a staging template.
Post-Staging Template	Select the name of a post-staging template.
General	Select the name of a general template.
Contact Information (Group of Fields)	
◦ Email	Enter the email ID to use for two-factor authentication.
◦ Phone	Enter the phone number to use for two-factor authentication.
Post-Staging Template Association (Tab)	Click the Edit icon to edit the post-staging template association information. 

◦ Tenant	Enter the name of the tenant.
◦ Category	Select the tenant category.
◦ Template	Select the post-staging template to associate with the template.
Devices Tab	Click the Delete icon to delete device information. 

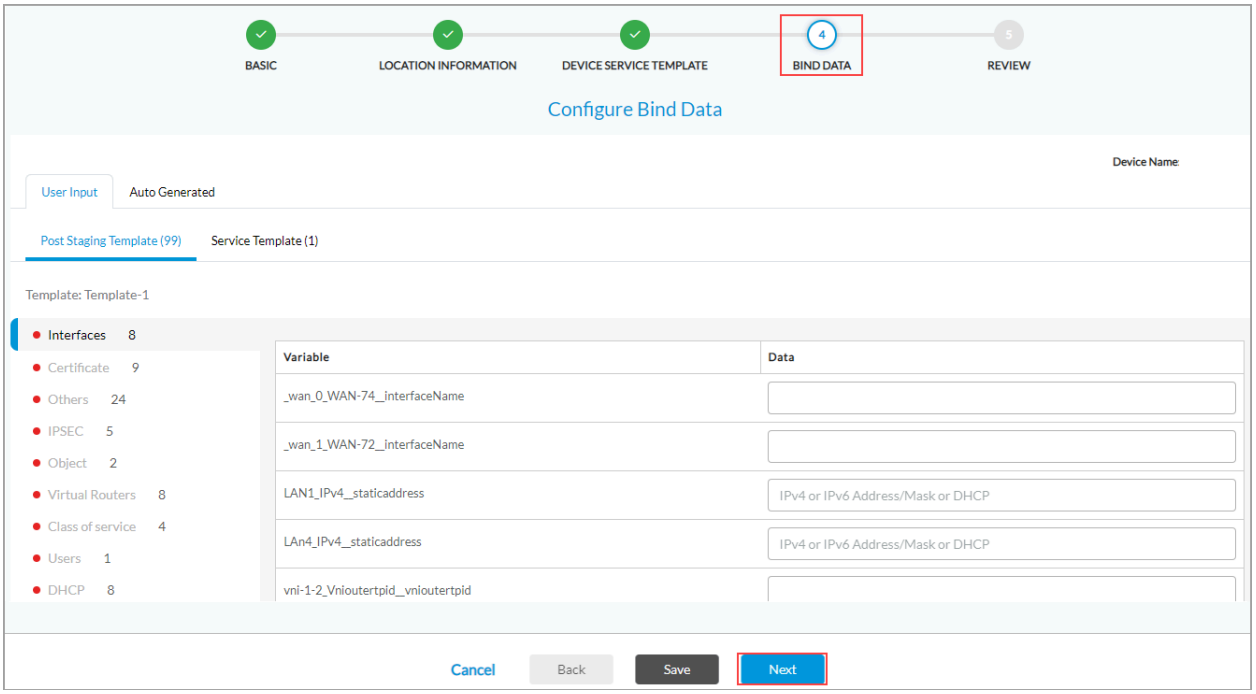
4. Click OK to complete adding a device group.
5. Click Save to save the configuration, or click Next to continue. The Step 2, In the Location Information tab displays. Enter the applicable location information of the Controller node, or click Generate to automatically populate the latitude and longitude from the Controller address.



6. Click Save to save the configuration, or click Next to continue. The Step 3, Device Service Template Screen displays. Add the required values to add a service template associated with the device. For more information, see Associate a Device-Specific Service Template with a Device below.

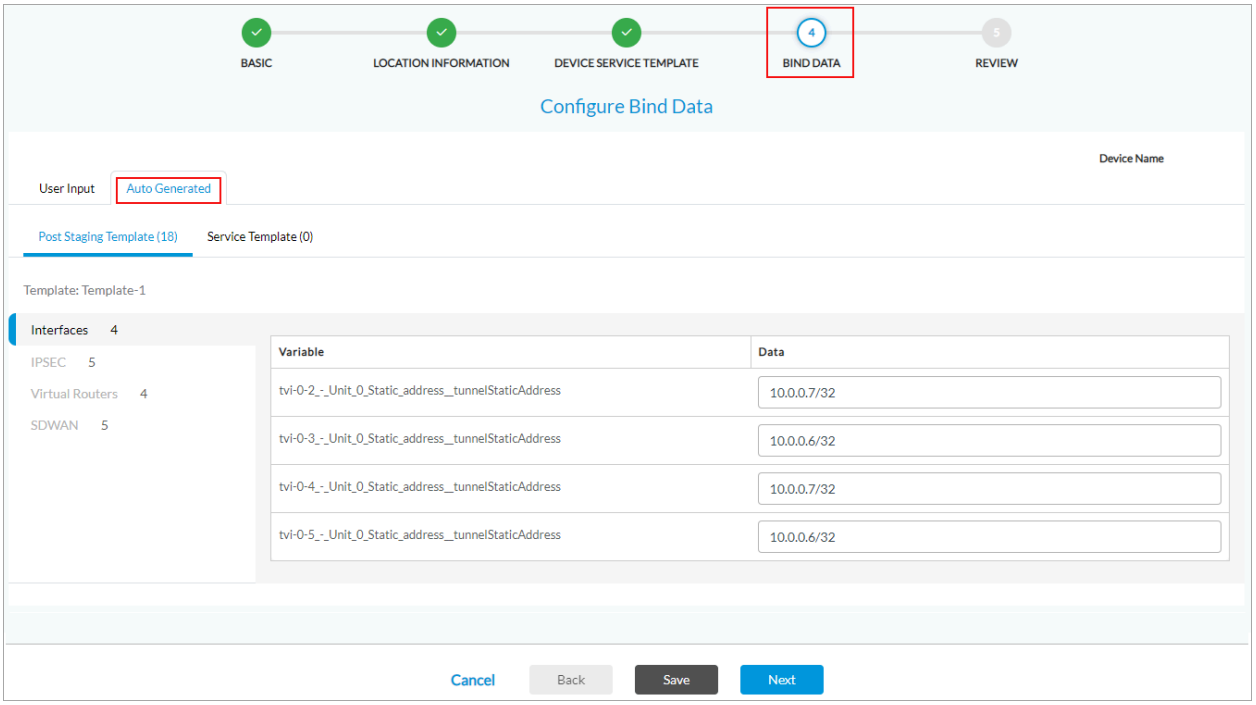


7. Click Save to save the configuration, or click Next to continue. The Step 3, Device Service Template Screen displays. In the Bind Data tab, add the required field values for the templates for which you have not enabled DHCP. If you enable DHCP for a template, the system populates the values dynamically. Note that the system validates the bind data variables per the specified variable type. If they do not match, an error message displays.

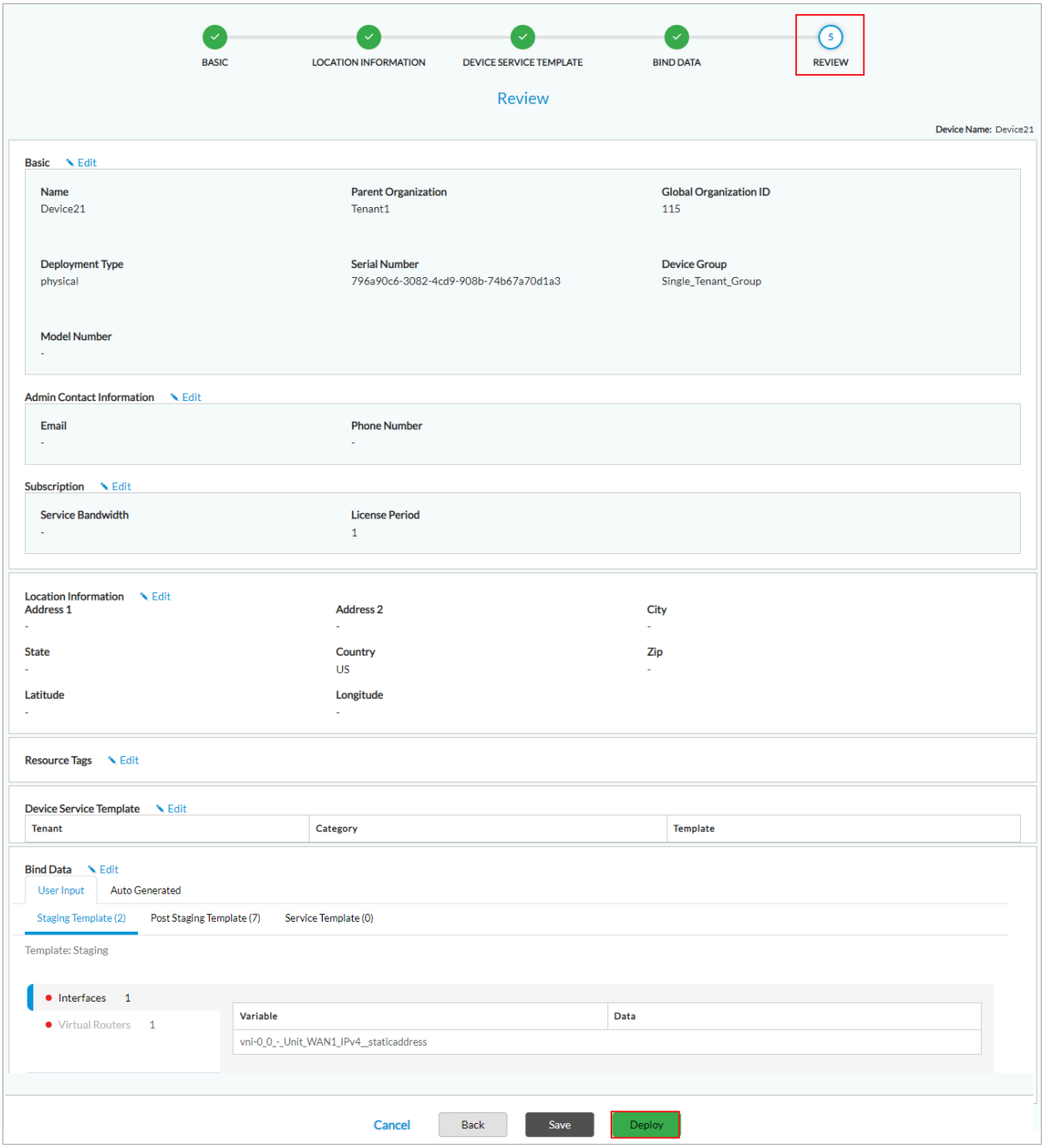


8. Click a variable to edit the values.

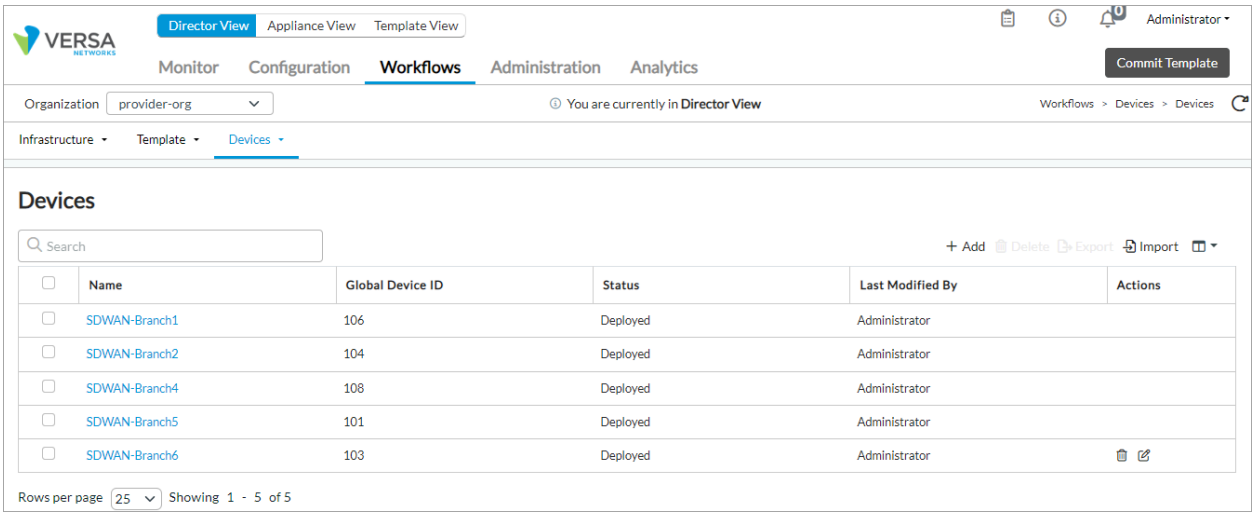
9. Select the Autogenerated tab to view and edit the values.



10. Click a variable to edit the values.
11. Click Save to save the configuration, or click Next to continue. The Step 5, Review screen displays.

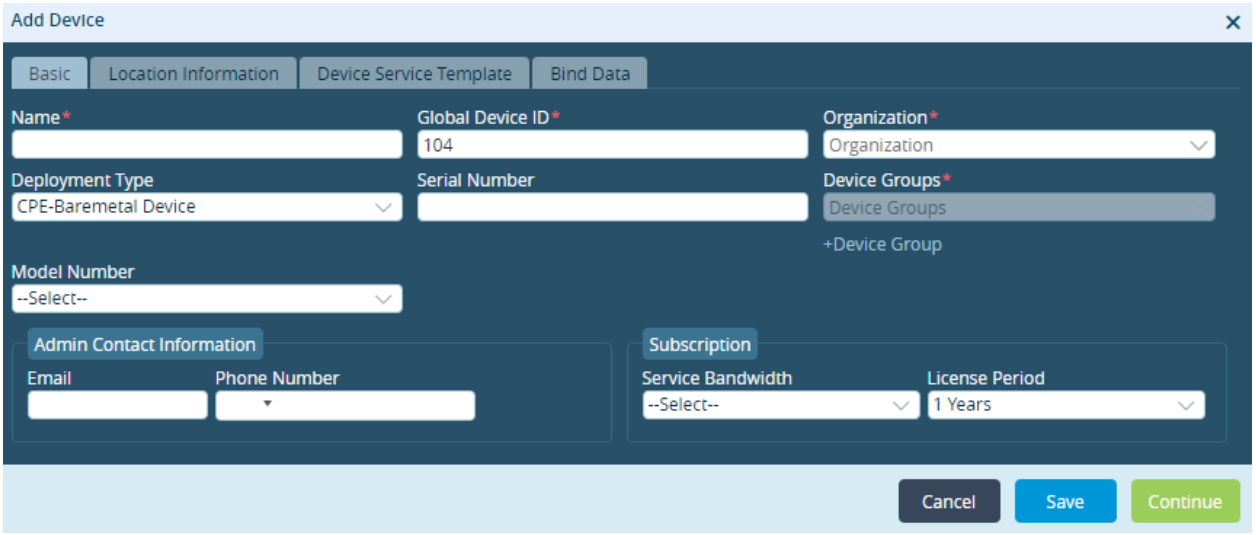


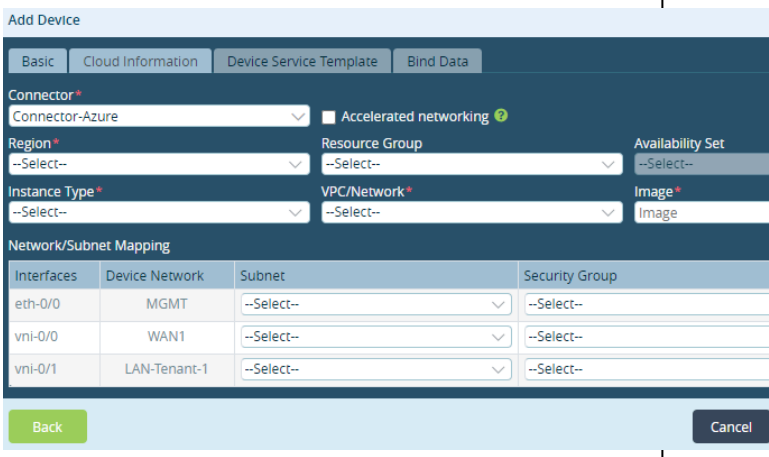
12. Click Deploy to onboard the device.

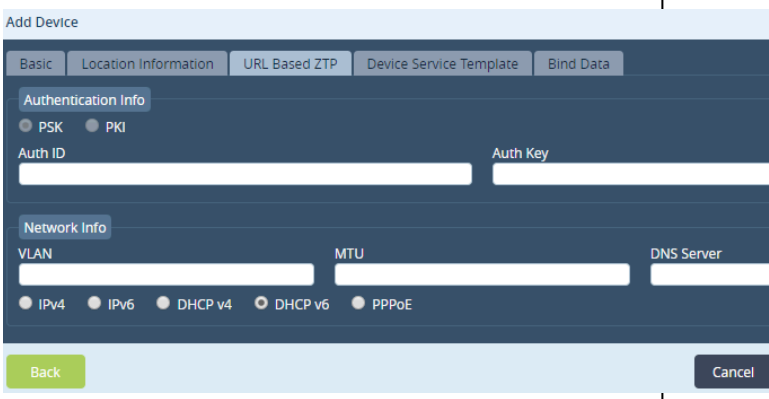
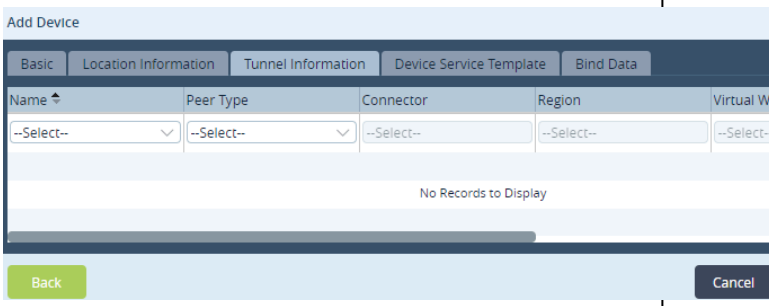


Create Devices and Device Groups in Releases 21.2 and Earlier

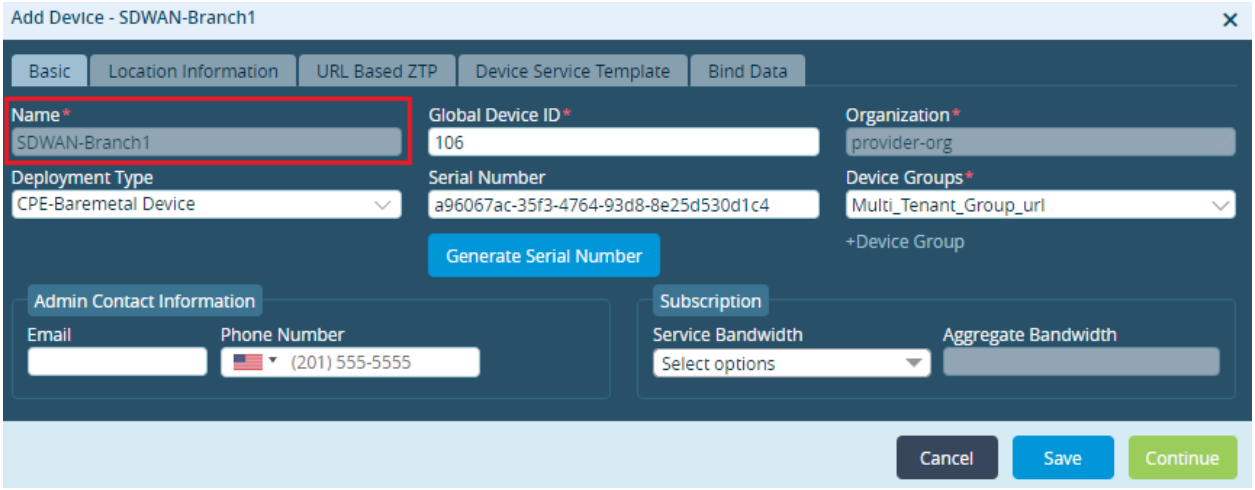
1. In Director view:
   a. Select the Workflows tab in the top menu bar.
   b. Select Devices > Devices in the left menu bar.
   c. Select an organization in the main pane
2. Click the Add icon to add a device. In the Basic tab, configure information about the device. Enter information for the following fields. Note that the URL Based ZTP tab is displayed only when you select a device group for which URL-based ZTP is enabled. The Tunnel Information tab is displayed, when you select a device group that has a template associated with it and the template includes tunnels.



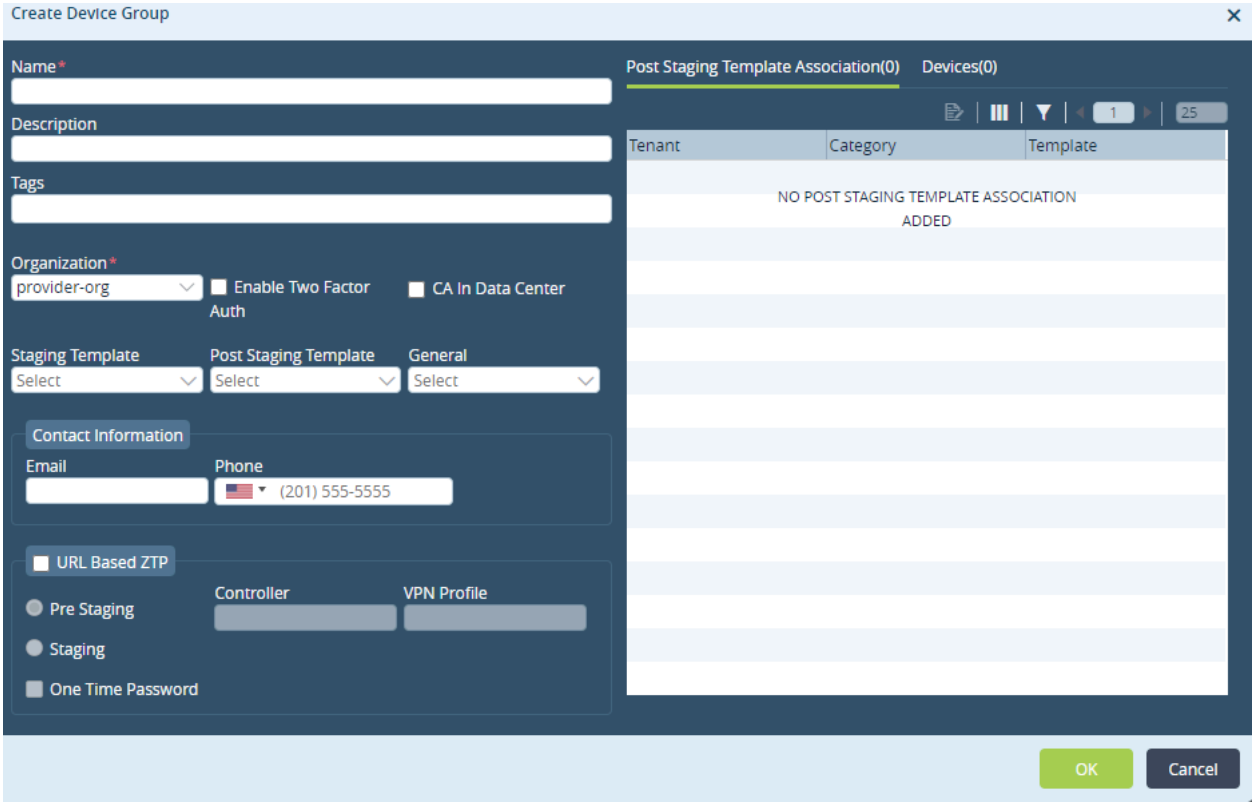
Field	Description
Name	Name of the device.
Global Device ID	ID assigned to the device. The system populates the value automatically with the next available ID. You can change it to a different available value between 1 and 31.
Organization	Organization for the device.
Deployment Type	Select the type of deployment: ◦ CPE Baremetal Device ◦ CPE Public Cloud If you select CPE Public Cloud, the Add Device popup window displays the Cloud Information tab. For more information, see Configure a Public Cloud Device To Be a Virtual CPE Router or an SD-WAN Gateway. 
Serial Number	Chassis/device ID for the branch device. This must be a unique value per device.
Device Groups	Select the device group to which the device belongs. If you select a device group on which URL-based ZTP is enabled, the Add Device popup window displays the URL-Based ZTP tab. For more information, see Activate VOS Devices.

	 If you select a device group that has a template associated with it and the template includes tunnels, the Add Device popup window displays the Tunnel Information tab. For more information, see Configure Site-to-Site Tunnels. 
Model Number	Select the model of the device from the drop-down list.
Admin Contact Information	Provide the contact email address and phone number of the administrator.
Subscription (Group of Fields)	For Releases 21.1.1 and later.
◦ Service Bandwidth	Select the bandwidth, in Mbps or Gbps, to use for service that the device offers.
◦ License Period	Select the period, in years, for which the device license is valid. *Values:* 1, 3, 5 years

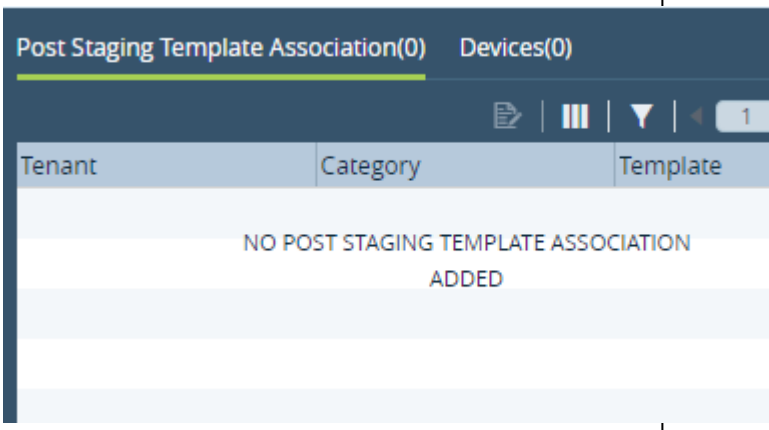
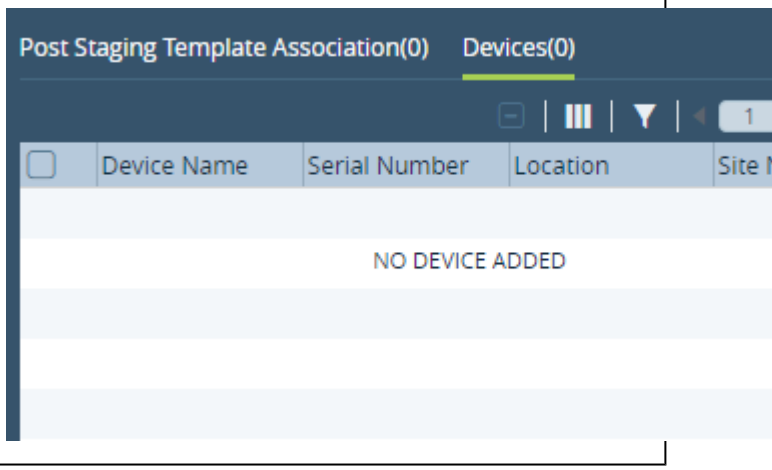
Note that once you deploy a device, you cannot change the name of the device in Versa Director. To change the device name, you must delete the device and add a new device. If you open the Add Device screen after the device has been deployed, the Name field is grayed out (not editable), as shown:



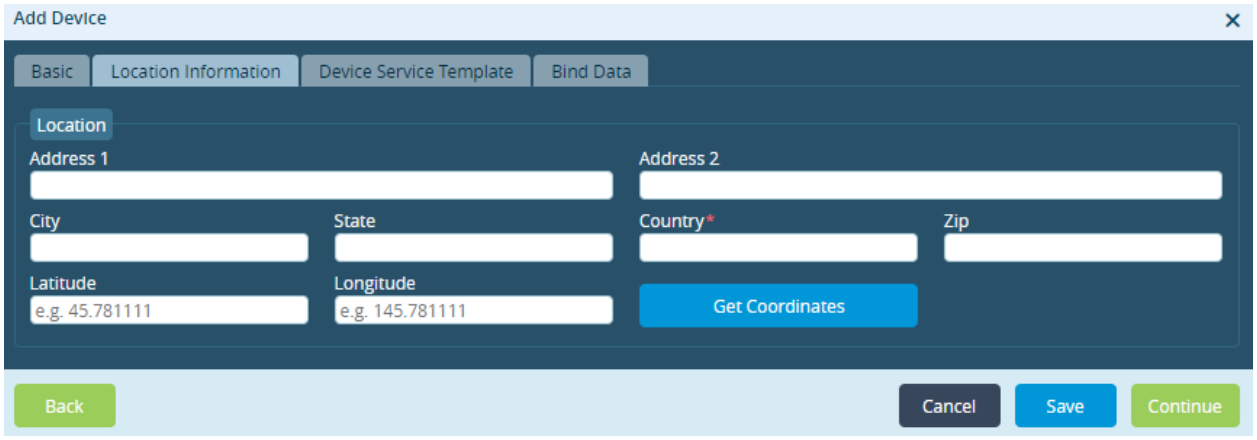
3. To create a device group, click + Device Group. Enter information for the following fields.



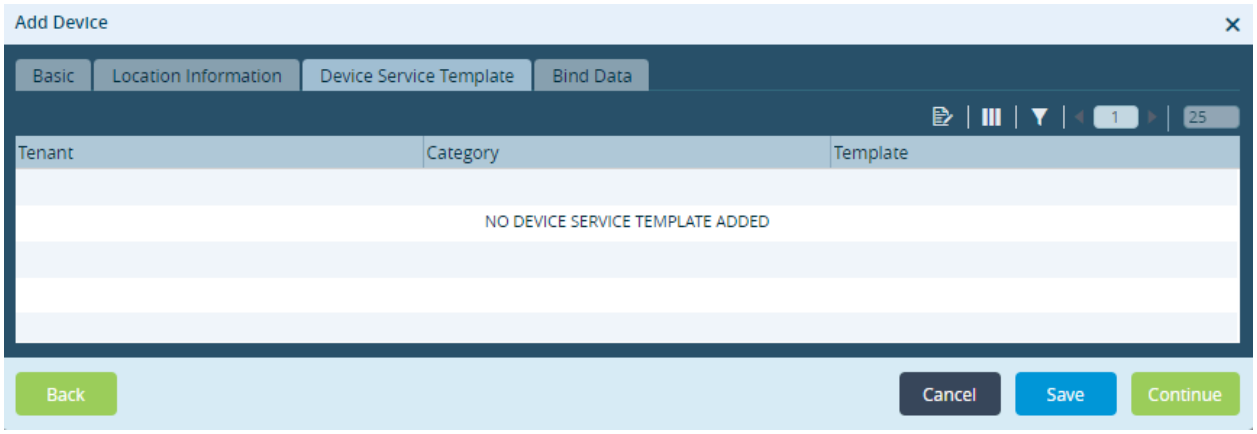
Field	Description
Name	Enter a name for the device group.
Description	Enter a text description for the group.
Tags	Enter a text string or phrase to associate with the rule. Tags allow you to locate a policy when you perform a filtered search of all policies. *Value:* Text string from 1 through 255 characters *Default:* None
Organization	Select the organization to which the device group belongs.
Enable Two-Factor Authentication	Click to be notified via email when a branch performs zero-touch provisioning (ZTP).
CA in Data Center	Click to enable certificate authority. If enabled, during global ZTP, the CSR request goes over the IPSec tunnel, and the branch receives a CA-signed certificate. All tunnels that are established use this certificate.
Staging Template	Select the name of a staging template.
Post-Staging Template	Select the name of a post-staging template.
General	Select the name of a general template.
Contact Information (Group of Fields)	
◦ Email	Enter the email ID to use for two-factor authentication.
◦ Phone	Enter the phone number to use for two-factor authentication.
Post-Staging Template Association (Tab)	Click the  Edit icon to edit the post-staging template association information.

	
◦ Tenant	Enter the name of the tenant.
◦ Category	Select the tenant category.
◦ Template	Select the post-staging template to associate with the template.
Devices Tab	Click the Delete icon to delete device information. 

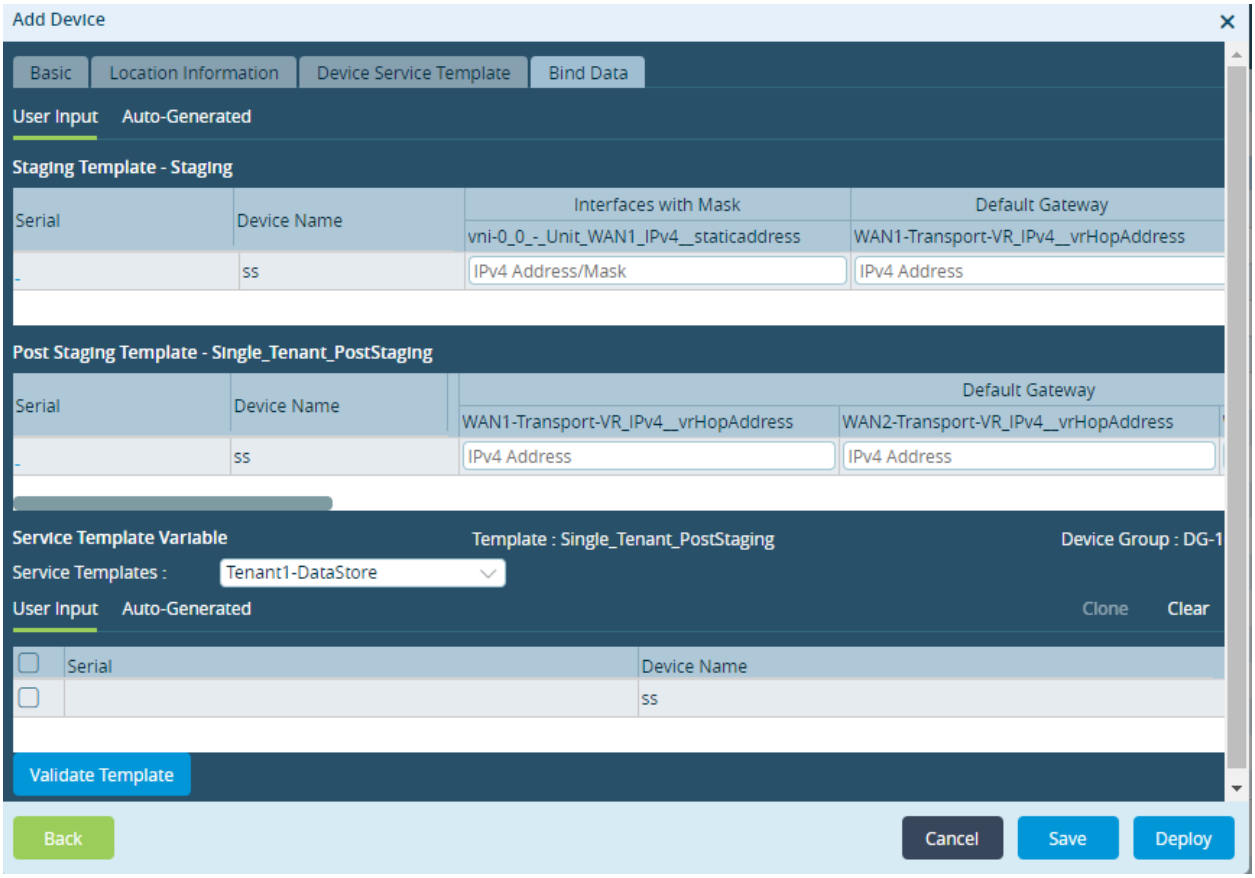
4. Click OK to complete adding a device group.
5. Click Continue on the Add Device screen.
6. In the Location Information tab, enter the applicable location information of the controller, click Get Coordinates to automatically populate the latitude and longitude from the Controller address, and click Continue.



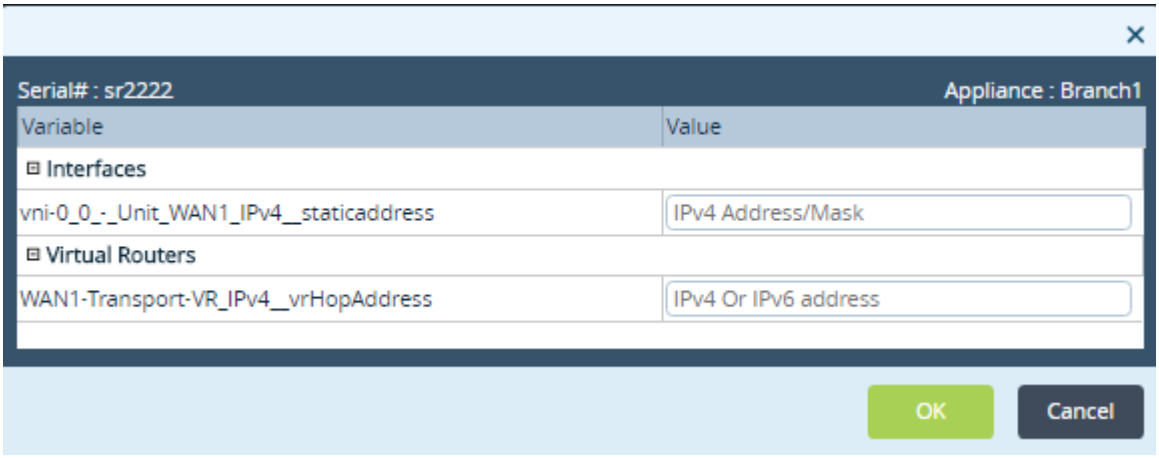
7. In the Device Service Template tab, add the required field values to add a service template associated with the device. For more information, see Associate a Device-Specific Service Template with a Device.



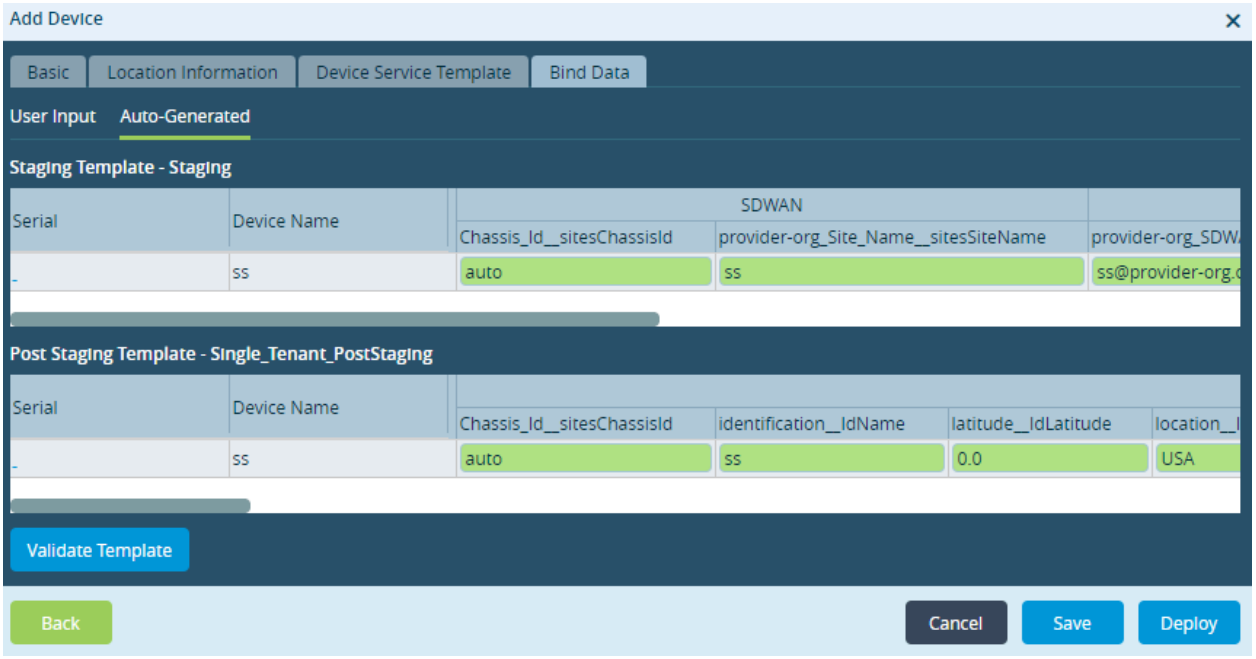
8. In the Bind Data tab, add the required field values for the templates for which you have not enabled DHCP. If you enable DHCP for a template, the system populates the values dynamically. Note that the system validates the bind data variables per the specified variable type. If they do not match, an error message displays.



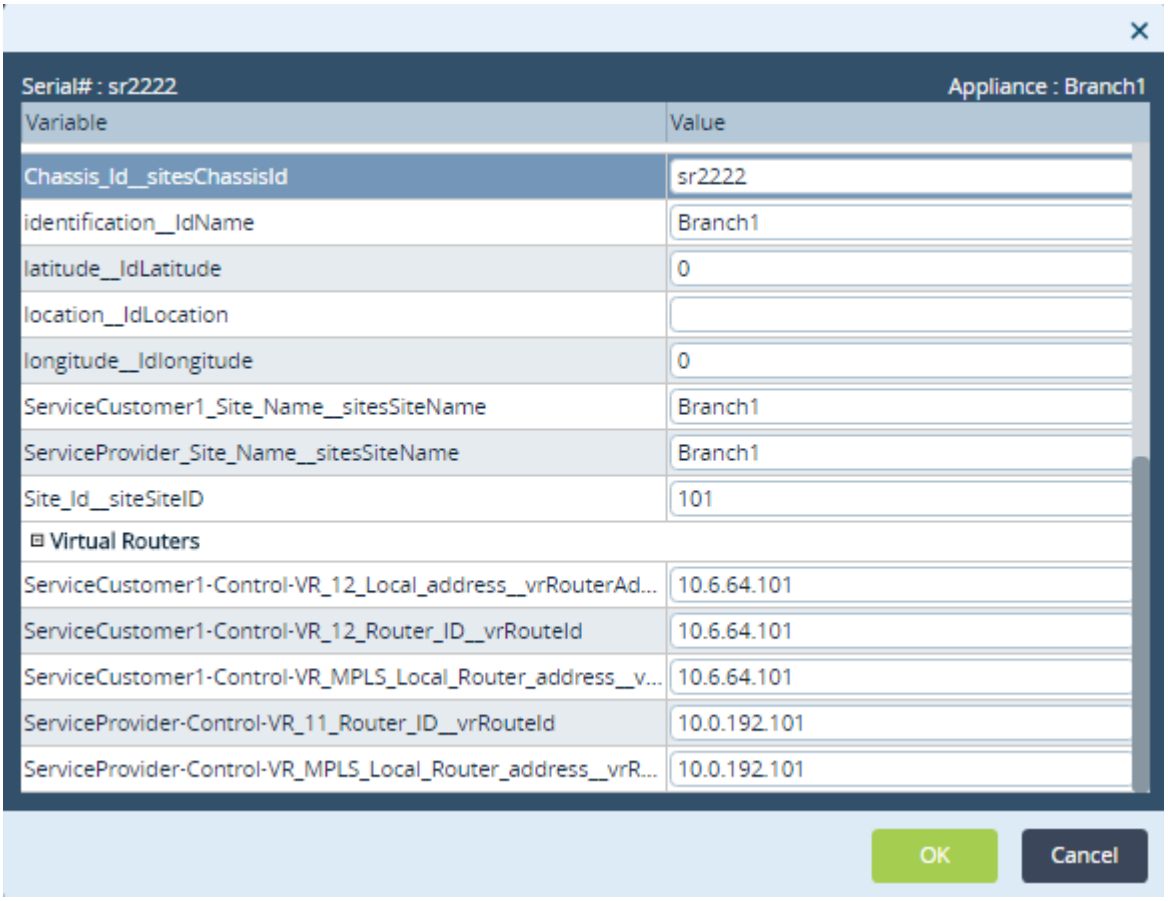
9. Click the serial number to edit the values.



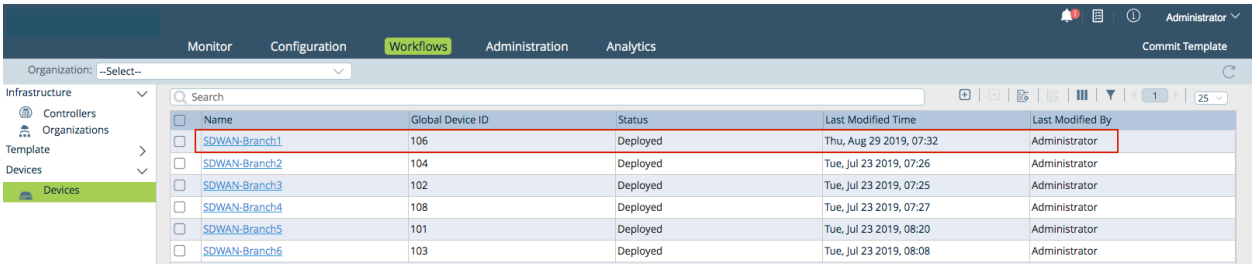
10. Select the Autogenerated tab to view and edit the values.



11. Click the serial number to edit the values.



12. Click Deploy. This onboards the device.



Associate a Device-Specific Service Template with a Device

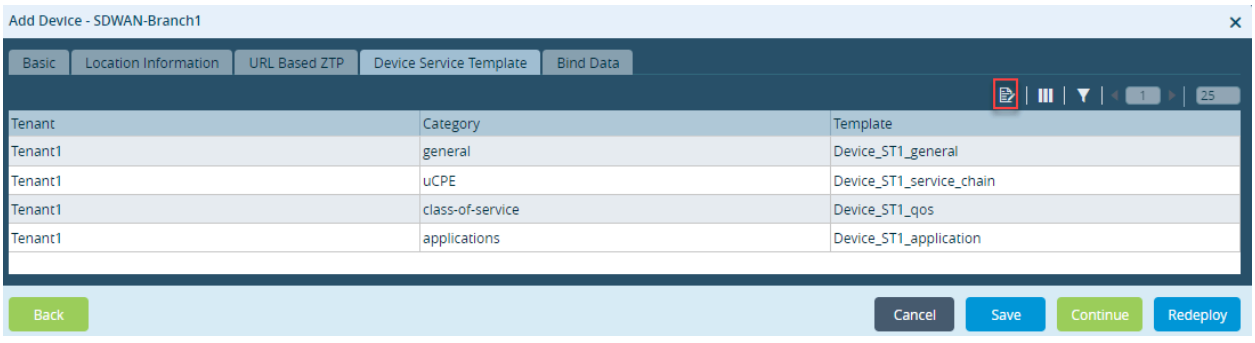
In addition to associating service templates with device groups, you can associate them with devices, either when you add a new device or when you edit existing device. You can associate one or more templates with or without bind data device-specific configuration.

When you associate a device-specific service template with a device, the templates are applied to the device in the following order:

1. Associate the device-specific service template with the device.
2. Associate the device group template with the device. This process applies the group-wide service template parameters with the device, and it overwrites any overlapping configuration parameters in the device-specific service template, replacing them with the parameters in the device group template.
3. Associate the device-specific service template with the device a second time. This process overwrites any overlapping configuration parameters in the device group template, in effect returning the parameter values to those specified in the device-specific service template, and it retains the other group-wide service template parameters.

To associate a device-specific service template with a device:

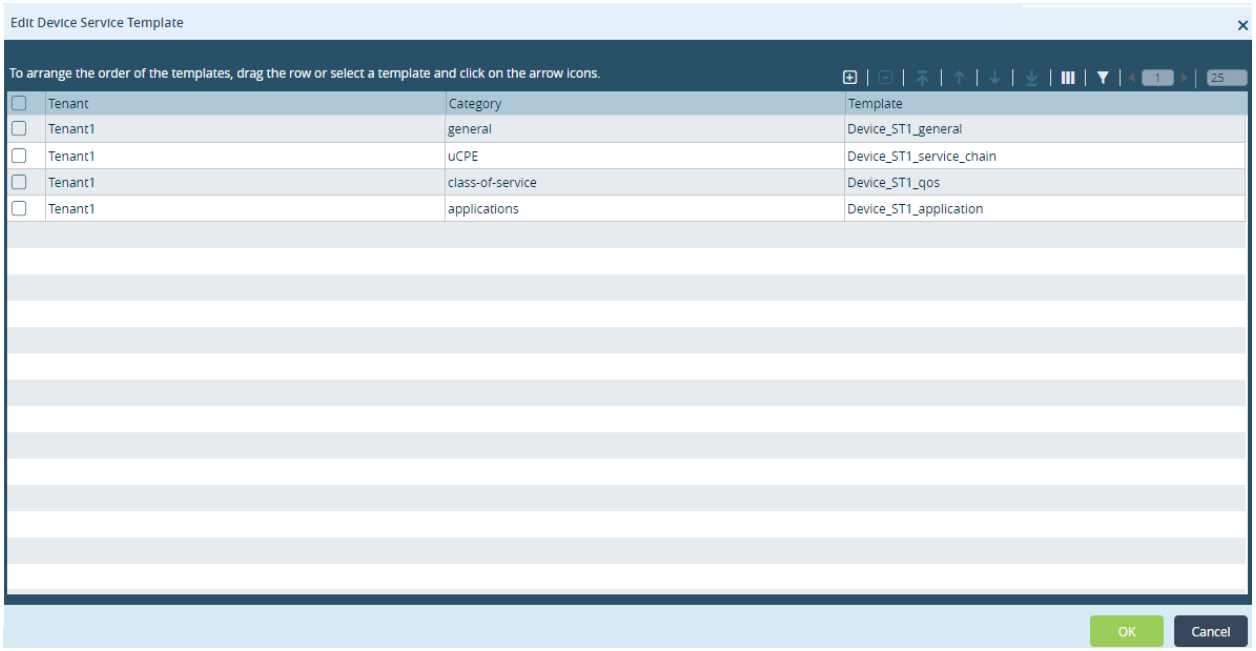
1. Select the Device Service Template tab in the Add or Edit Device window. The window is either blank or it displays a list of the service templates associated with the device.



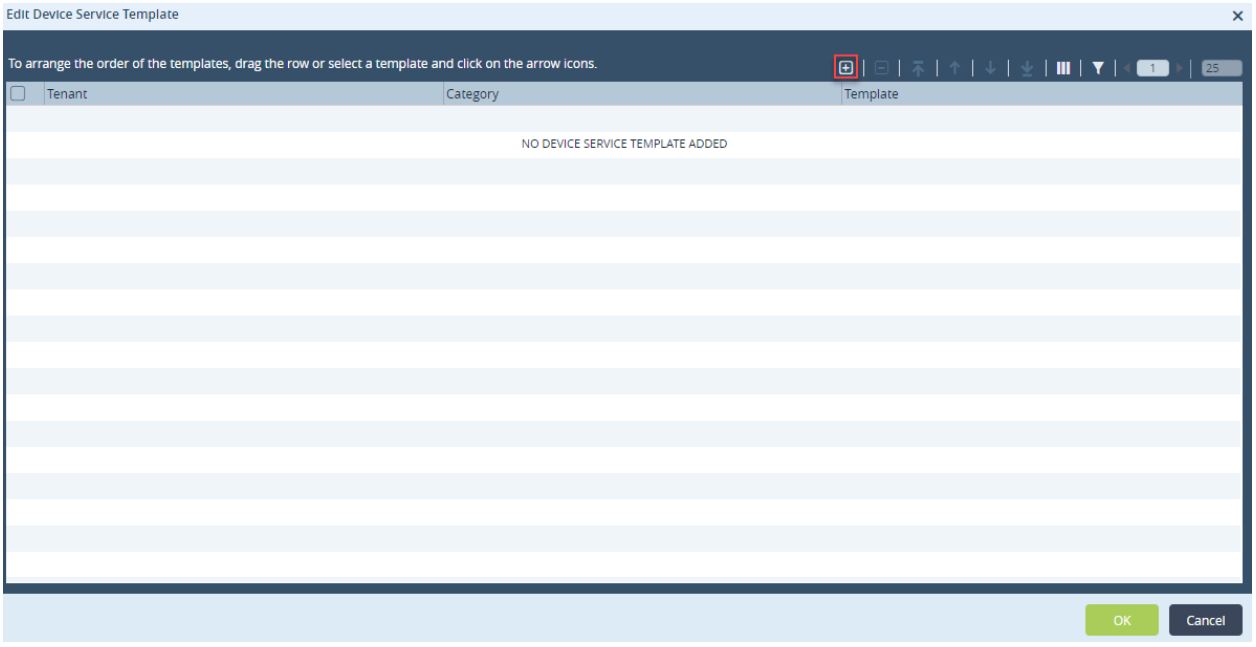
2. Click the Edit icon to edit the device service template. The Edit Device Service Template popup window

displays.

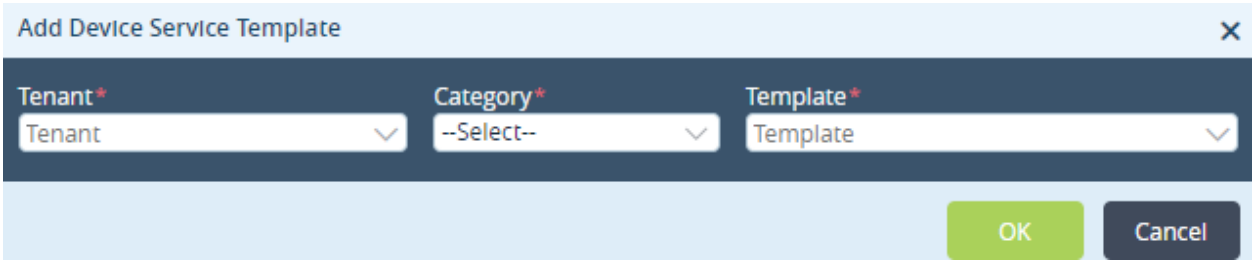
3. If the window lists existing templates, reorder the templates by dragging and dropping them, if desired.



4. If the window lists no templates, click the Add icon to add a new device service template.



5. In the Add Device Service Template popup window, enter information for the following fields.



Field	Description
Tenant	Select the name of the tenant.
Category	Select the category of the service template: ◦ Stateful Firewall—Allows you to configure the following services: ▪ DoS protection ▪ Security and security settings ◦ NextGen Firewall—Allows you to configure the following services: ▪ Authentication ▪ Decryption ▪ DoS protection ▪ Security and security settings ▪ Secure web proxy ◦ QoS—Allows you to configure the following services: ▪ AppQoS ▪ Associate interfaces and networks ▪ Drop profiles ▪ Forwarding class map ▪ QoS profiles ▪ Read-write rules ▪ Schedulers ▪ Scheduler maps ◦ General—Allows you to configure all available services. ◦ Application Steering—Allows you to configure the following services: ▪ Class of service ▪ CoS and SD-WAN policy ▪ Zones ◦ Service Chain—Allows you to configure the following objects: ▪ Address ▪ Address groups ▪ Cloud profiles ▪ Custom objects ▪ Schedules ▪ SNAT pools ◦ Secure Access—Allows you to configure the following objects: ▪ Secure access routes

	▪ DNS resolvers ▪ Secure access servers ▪ Secure access profiles ▪ Secure access portal and/or gateway
Template	Select the template to use. The drop-down lists the templates available based on the opt

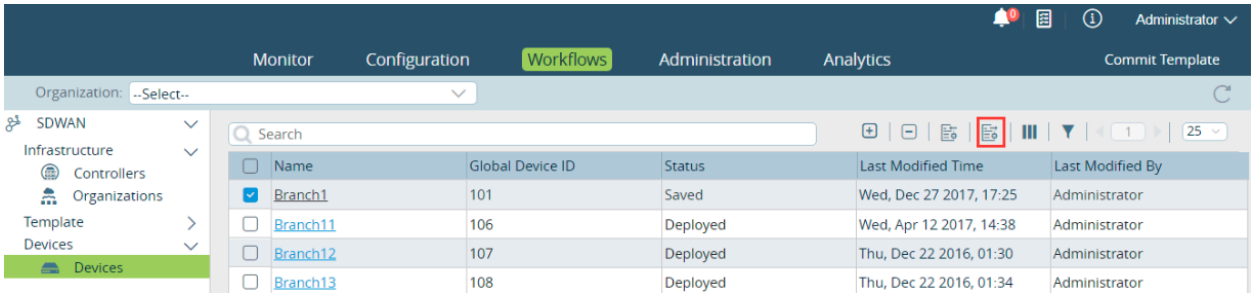
6. Click OK.

Import and Export Devices in Bulk

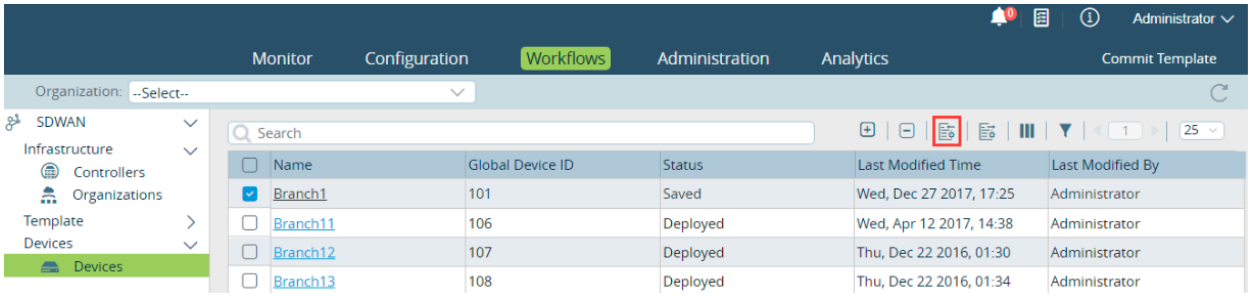
You can add multiple devices in bulk instead of adding a single device at a time, and you can export devices in bulk so that you can import later.

To import or export devices in bulk:

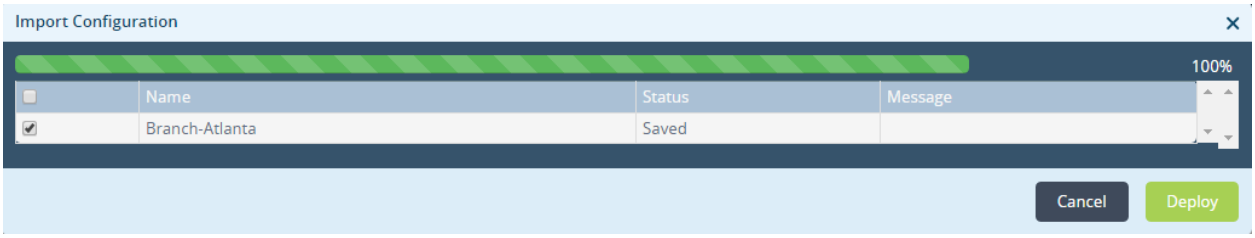
1. Add a device to a device group, as described earlier in this article.
2. Select a device to add multiple devices in its device group.



3. Click the Export icon. This exports the device configuration as an Excel file.
4. Add other devices that belong to the same device group in the file and save it.
5. Select the check box of the device of the device group into which devices are to be imported. Click the Import icon on the top right menu bar.



6. Click Browse to select the Excel file that has the device details and click OK. This imports the devices.
7. Click Deploy.



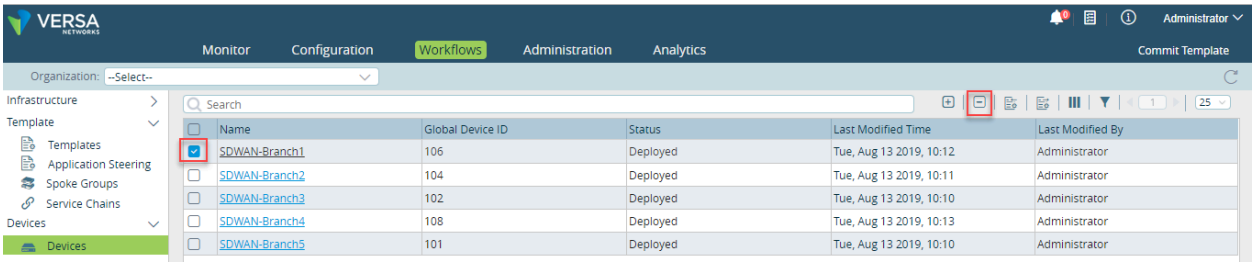
Delete a Device

Deleting a device does the following to decommission the device:

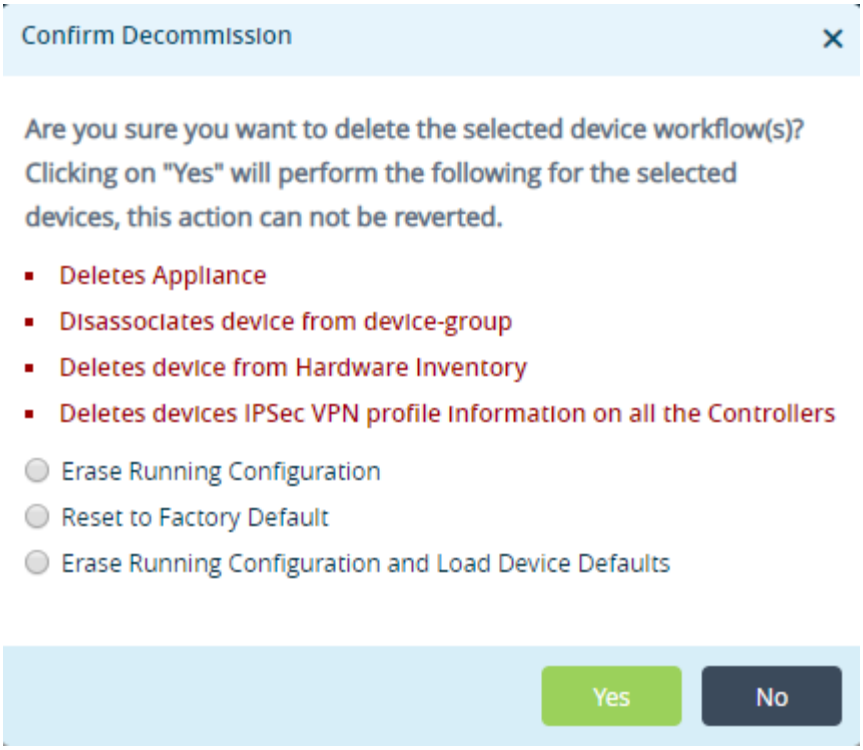
- Deletes the appliance associated with it.
- Disassociates the device from the device group.
- Deletes the device from the hardware inventory.
- Deletes the device's IPsec VPN profile information.

To delete a device:

1. In Director view, select Workflows from the top menu bar.
2. Select Devices > Devices from the left menu bar.
3. Click the checkbox for the device, and click the Delete icon.



4. In the Confirm Decommission popup window, select none, or one or more of the following options. (These options are available for Releases 20.2 and later.)



Field	Description
Erase Running Configuration	Click to erase the running configuration on the device.
Reset to Factory Default	Click to erase the information stored in the device's internal memory and to return the it left the factory.
Erase Running Configuration and Load Device Defaults	Click to erase the running configuration on the device and to load a user-defined defa

5. Click Yes.

Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Release 20.2.1 adds support for device-level service templates.
- Release 21.1.1 adds support for Layer 2 ports and interfaces tab in the Create Template window > Interfaces tab. The Interfaces tab also supports configuration of Integrated routing and bridging (IRB) on a WAN or LAN interface.
- Release 21.1.1 adds support for the Solution Add-On Tier and License Period fields in the Create Template > Basic tab.
- Release 21.1.1 adds support for the Switching tab (for Layer 2 interfaces) in the Create Template window.
- Release 21.1.1 adds support for the Service Bandwidth and License Period fields in the Add Device window > Basic

tab.

- Release 21.2.1 adds support for the T1/E1 and DSL interfaces in the Workflows > Template > Templates > Interfaces tab.
- Releases 22.1.1 adds workflows to create customer organizations, controller nodes, device templates, and devices are via wizards; adds support for PKI-based certificates in workflows; increases the WAN link priority value from 8 to 15; adds support for the GRE tunnel protocol for the peer type AWS Transit Gateway; renames LTE interfaces to WWAN; add support for Resource Tag field in workflows templates.
- Release 22.1.3 add support for the dynamic tenant configuration field in the Add Service Template window.

Additional Information

Configure Interfaces
Configure Multitenancy
Create and Manage Staging and Post-Staging Templates
Director GUI Overview
Licensing Overview
Understand SD-WAN Interface Numbering