Create and Manage Staging and Post-Staging Templates

For supported software information, click here.

You use device configuration templates, simply called device templates, to create baseline configurations that you can distribute automatically across many Versa Operating System^{TM} (VOS^{TM}) devices. Device templates are a baseline configuration that you can deploy across multiple branches, thus saving you time and effort when you are configuring and deploying similar services on many branch devices.

There are two types of device templates:

- Staging templates—You typically create staging templates for 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.
- Post-staging templates—These are production templates that contain the complete configuration required to deploy network services on VOS branch devices.

You use workflows to create templates to configure VOS devices. (You also use workflows to create templates to configure application steering, spoke groups, and services chains.)

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

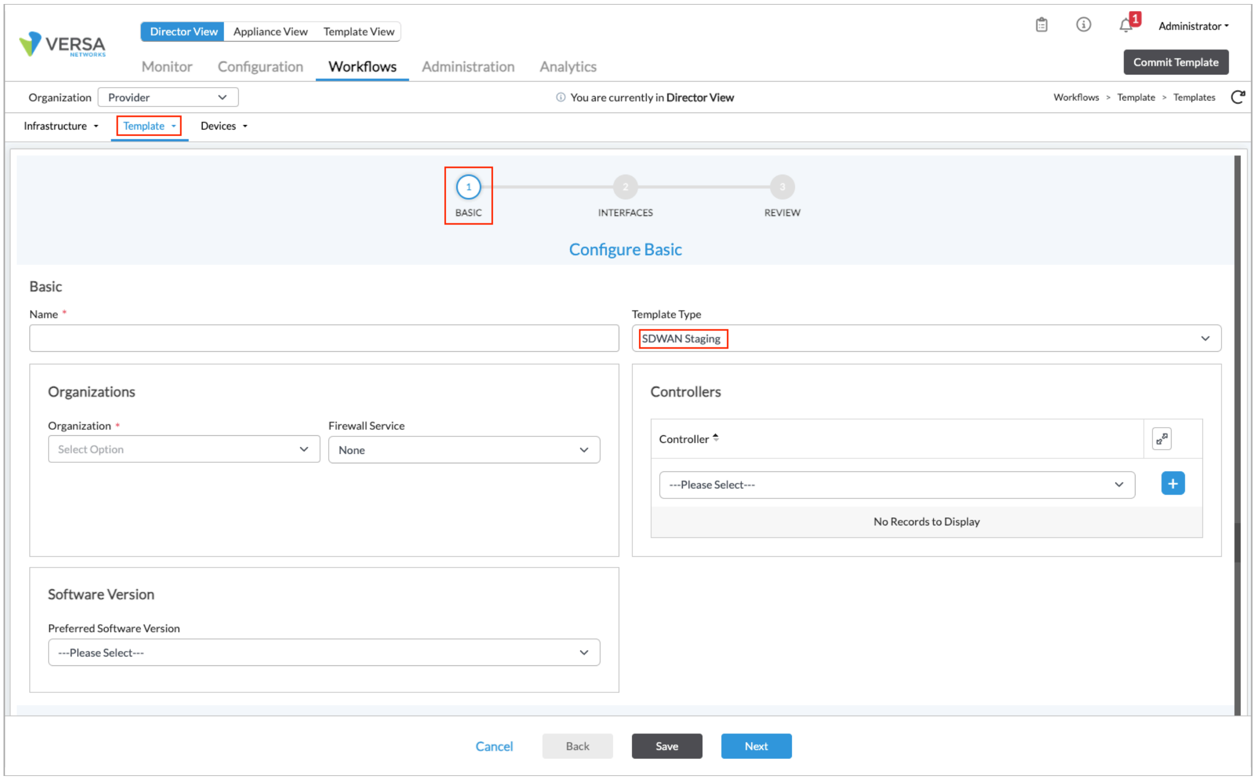
After you have created a staging or a post-staging template, you can modify, clone, import, and export it.

Create Staging Templates

You can create staging templates for WANs only, not for LANs.

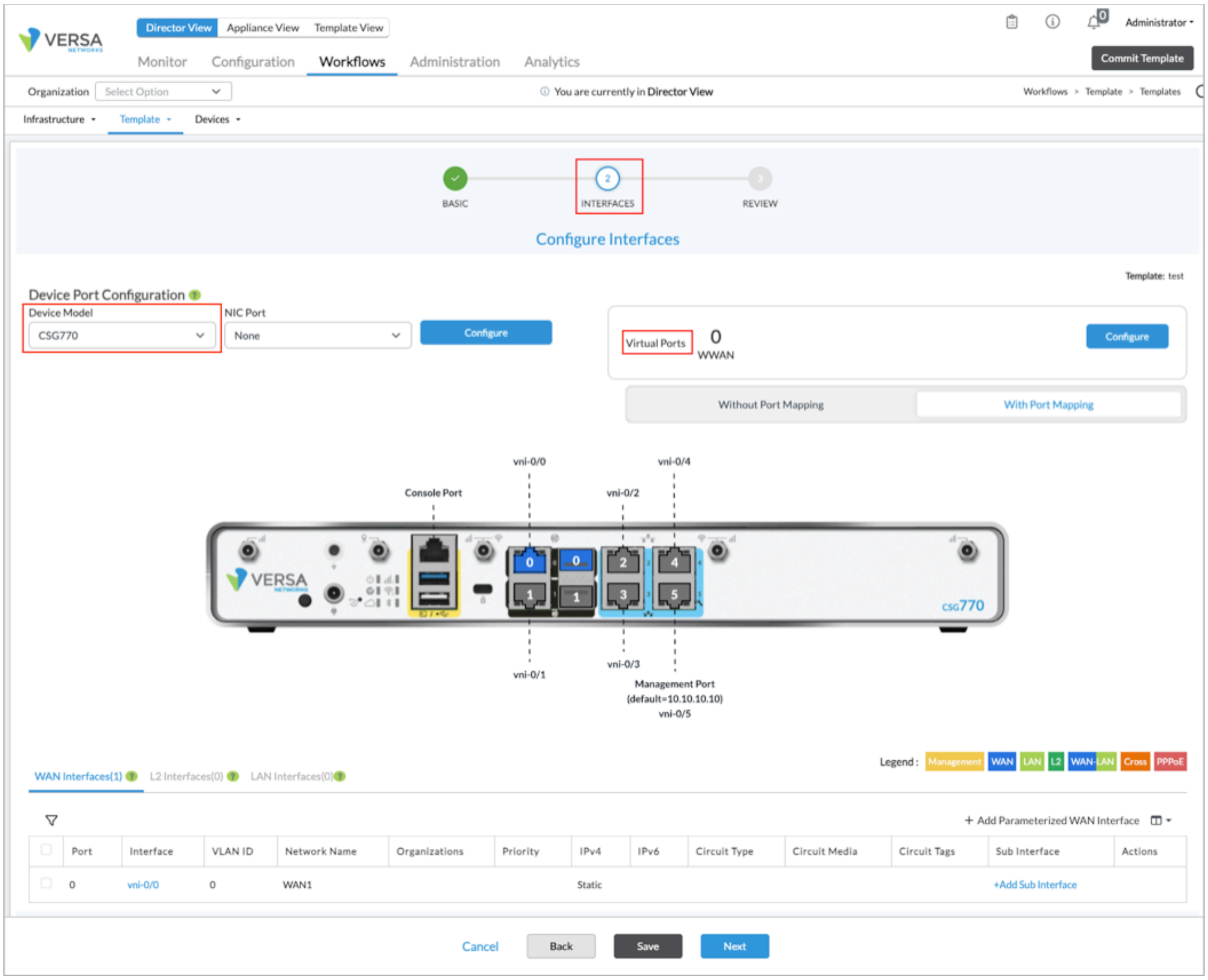
To create a staging template:

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 to create a staging template. The following screen displays. In the Basic tab, enter information for the following fields.



Field	Description
Name (Required)	Enter a name for the staging template.
Type (Required)	Select the template type SD-WAN Staging.
Organization (Required)	Select the provider organization to associate with the template.
Controllers	Select one or more Controller nodes to associate with the template.
Preferred Software Version	Select the preferred version of the software that should be deployed on the Director node.

4. Click Continue, or select the Interfaces tab.
5. Select the Interfaces tab, and associate ports and interfaces with the template. Enter information for the following fields.



Organization: Select Option

Configure Interfaces

Template: test

Device Port Configuration

Device Model: CSG770

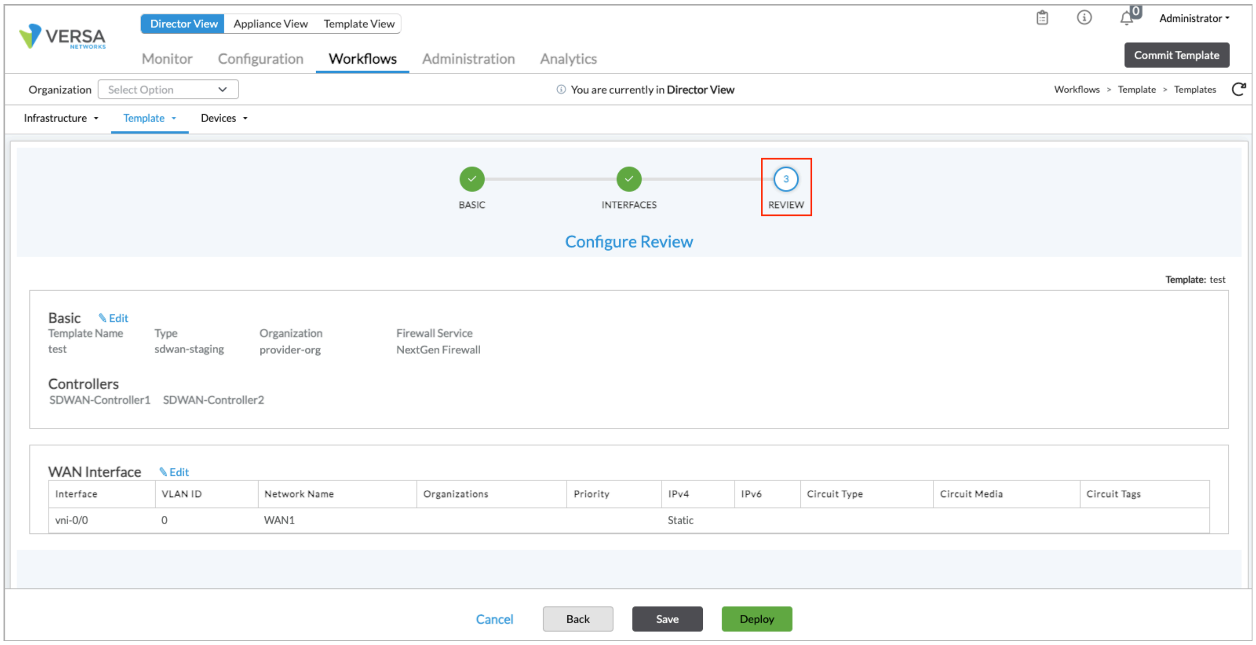
NIC Port: None

Virtual Ports: 0 WWAN

□	Port	Interface	VLAN ID	Network Name	Organizations	Priority	IPv4	IPv6	Circuit Type	Circuit Media	Circuit Tags	Sub Interface	Actions
□	0	vni-0/0	0	WAN1			Static					+Add Sub Interface	

Field	**Description**
Device Port Configuration (Group of Fields)	
◦ Device Model	Select a device model.
◦ NIC Port	Select a NIC port, and the click Configure in the Device Port Configuration section to configure the port.
◦ WWAN (For Releases 22.1.1 and later; called LTE in earlier releases)	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. For more information, see Configure WWAN. The term *WWAN interfaces* is used to represent LTE, 4G, and 5G interfaces.
WAN Interfaces	Enter configuration information for each WWAN interface for LTE, 4G, or 5G service and save the configuration to populate the WAN interfaces configuration. For more information, see Configure a WAN Interface To Use for WWAN.

5. Select the Review tab and then click Deploy to activate the staging template and to associate the staging template with Controllers.



Template: test

Basic

Template Name	Type	Organization	Firewall Service
test	sdwan-staging	provider-org	NextGen Firewall

Controllers

SDWAN-Controller1 SDWAN-Controller2

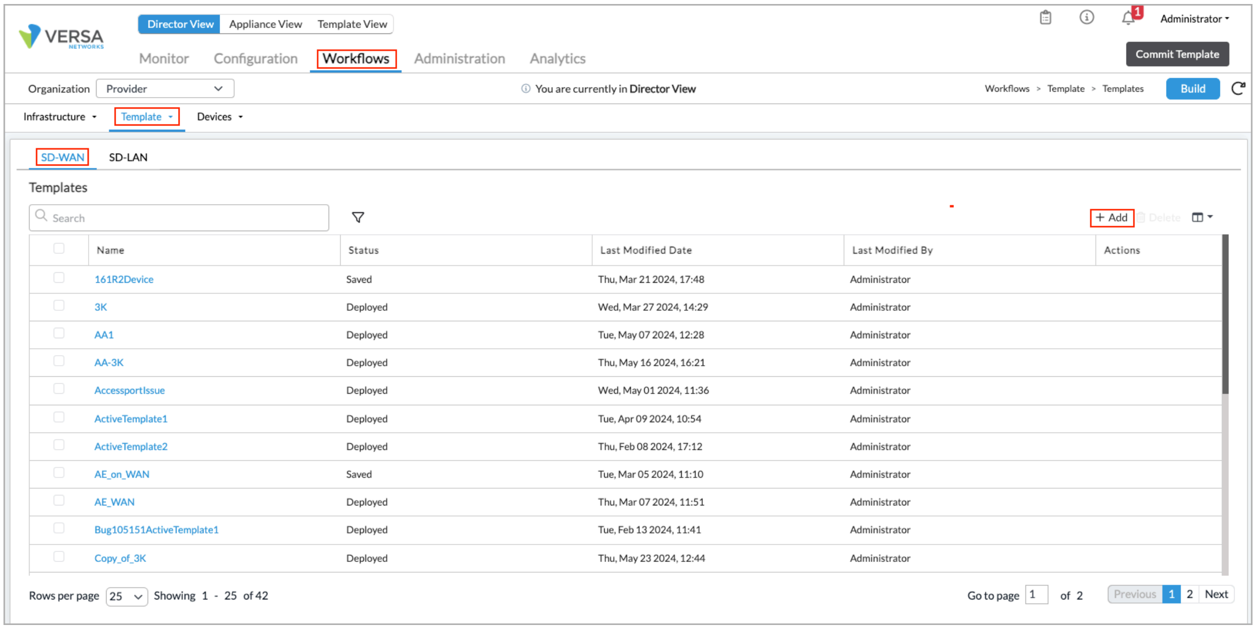
WAN Interface

Interface	VLAN ID	Network Name	Organizations	Priority	IPv4	IPv6	Circuit Type	Circuit Media	Circuit Tags
vni-0/0	0	WAN1			Static				

Create 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.

1. In Director view, select the Workflows tab in the top menu bar.
2. Select an organization.
3. Select Template > Templates in the horizontal menu bar and SD-WAN from the horizontal submenu bar.

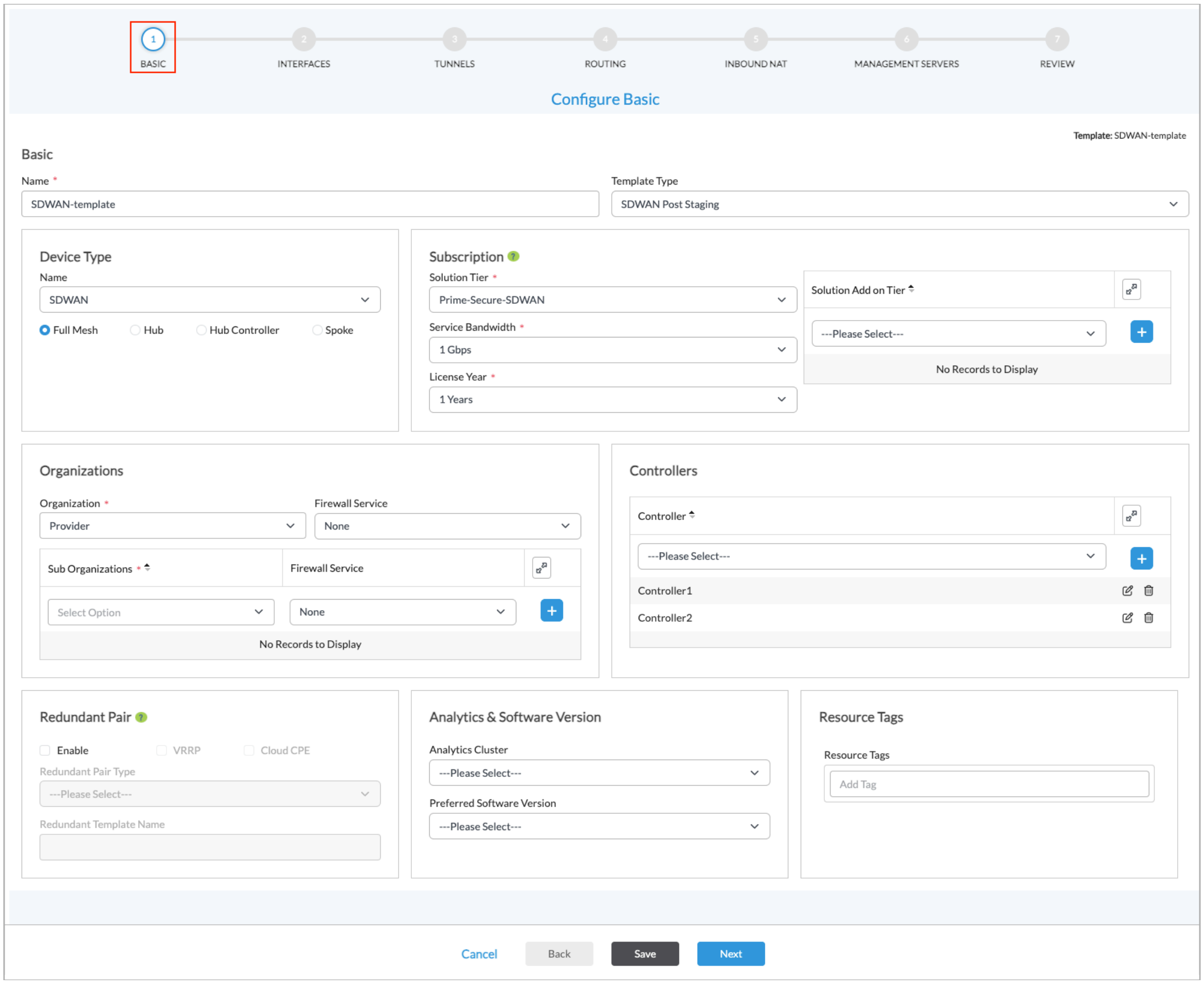


	Name	Status	Last Modified Date	Last Modified By	Actions
□	161R2Device	Saved	Thu, Mar 21 2024, 17:48	Administrator	
□	3K	Deployed	Wed, Mar 27 2024, 14:29	Administrator	
□	AA1	Deployed	Tue, May 07 2024, 12:28	Administrator	
□	AA-3K	Deployed	Thu, May 16 2024, 16:21	Administrator	
□	AccessportIssue	Deployed	Wed, May 01 2024, 11:36	Administrator	
□	ActiveTemplate1	Deployed	Tue, Apr 09 2024, 10:54	Administrator	
□	ActiveTemplate2	Deployed	Thu, Feb 08 2024, 17:12	Administrator	
□	AE_on_WAN	Saved	Tue, Mar 05 2024, 11:10	Administrator	
□	AE_WAN	Deployed	Thu, Mar 07 2024, 11:51	Administrator	
□	Bug105151ActiveTemplate1	Deployed	Tue, Feb 13 2024, 11:41	Administrator	
□	Copy_of_3K	Deployed	Thu, May 23 2024, 12:44	Administrator	

Rows per page 25 Showing 1 - 25 of 42

Go to page 1 of 2 Previous 1 2 Next

4. Click the + Add icon to create a new template. The Create Template popup window displays. For the eight steps (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 Next to move to the next step in sequence and Back to move to the previous step, or select a step to move directly to its window. For Releases 21.1.0 and earlier, the Create Template window is displayed as a popup window.



Configure Basic

Template: SDWAN-template

Basic

Name * SDWAN-template

Template Type: SDWAN Post Staging

Device Type

Name: SDWAN

● Full Mesh ○ Hub ○ Hub Controller ○ Spoke

Subscription

Solution Tier *: Prime-Secure-SDWAN

Service Bandwidth *: 1 Gbps

License Year *: 1 Years

Solution Add on Tier: ---Please Select---

No Records to Display

Organizations

Organization *: Provider

Firewall Service: None

Sub Organizations *	Firewall Service
Select Option	None

No Records to Display

Controllers

Controller
---Please Select---
Controller1
Controller2

Redundant Pair

□ Enable □ VRRP □ Cloud CPE

Redundant Pair Type: ---Please Select---

Redundant Template Name:

Analytics & Software Version

Analytics Cluster: ---Please Select---

Preferred Software Version: ---Please Select---

Resource Tags

Resource Tags: Add Tag

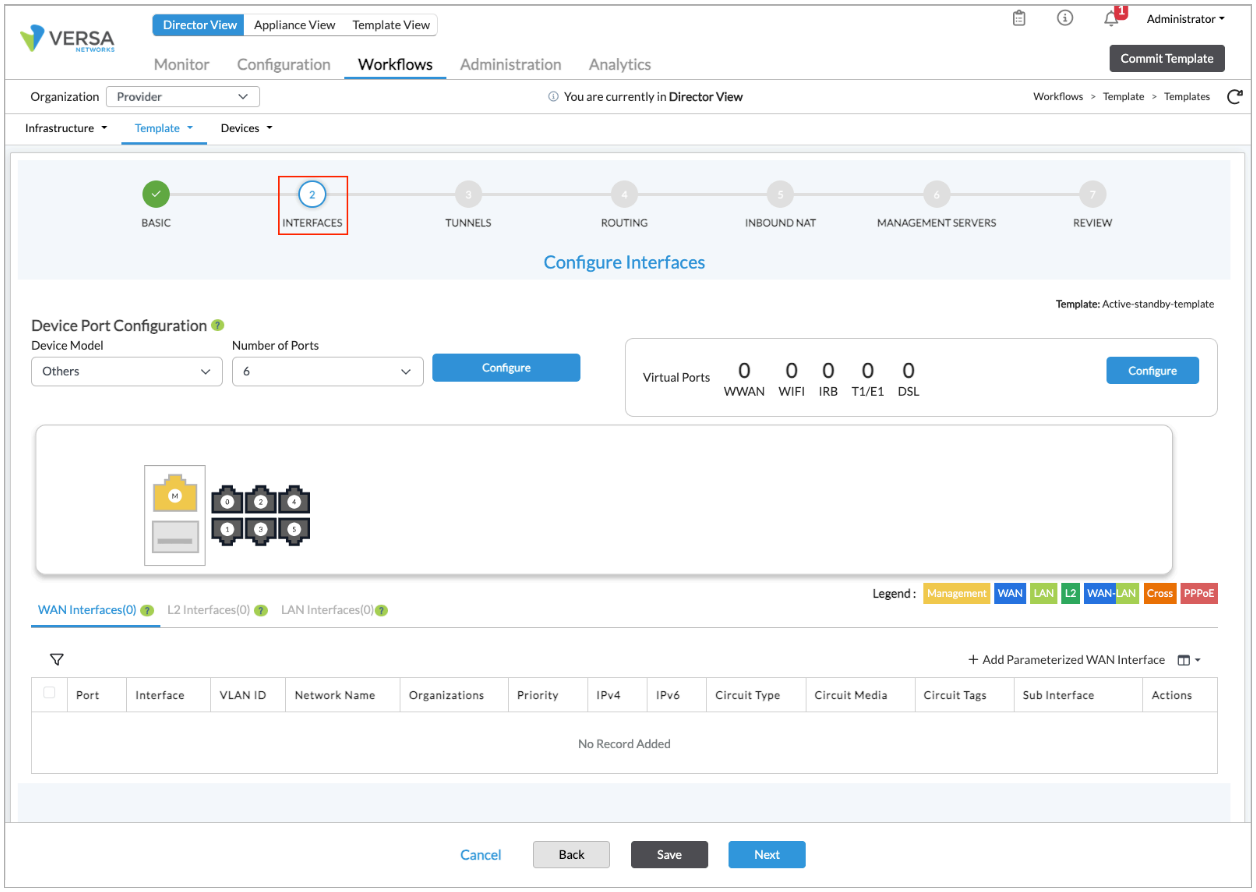
5. Click Step 1, Basic. The Configure Basic screen displays. Enter information for the following fields.

Field	Description
Name (Required)	Enter a name for the template. *Value:* Text string from 1 through 255 characters *Default:* None
Template Type (Required)	Select the template type SD-WAN Post-Staging.
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—Click for a device in a full-mesh topology. This is the default. ◦ Hub—Click to have the device be a hub in a hub-and-spoke topology. If you select this device type, the Region field is enabled. Select the region. ◦ Hub Controller—Click to have the device act as a hub and a Controller for the spokes. Selecting this device type enables the Region and Staging fields. Select the region. ◦ Spoke—Click to have the device be a spoke in a hub-and-spoke topology. Selecting this device type enables the Spoke Group field. Select the name of the spoke group. For more information, see Create an SD-WAN Spoke Group. *Default:* Full Mesh
Subscription (Group of Fields)	
◦ Solution Tier (Required)	Select the solution tier that corresponds to the license that the device is using: ◦ Work-From-Home ◦ Premier Secure SD-WAN ◦ Prime Secure SD-WAN ◦ Prime SD-WAN ◦ Premier Elite SD-WAN

	For more information, see Licensing Overview.
◦ Service Bandwidth (Required)	Select the bandwidth to use for solution tier that corresponds to the license that the device is using.
◦ License Year (Required)	Select the period, in years, for which the license is valid. The options are 1 year, 3 years, and 5 years.
◦ Solution Add-On Tier	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.
Organizations (Group of Fields)	
◦ Organization (Required)	Select the organization to which the template applies.
◦ Firewall Service	Select the Firewall type for the organization: ◦ NGFW (next-generation firewall) ◦ SFW (stateful firewall)
◦ Suborganizations (Required)	For full-mesh and hub device types, select the name of the suborganization associated with the template.
◦ Firewall Service	Select the Firewall type for the suborganization: ◦ NGFW (next-generation firewall) ◦ SFW (stateful firewall)
Controllers	For full-mesh and hub device types, select name of the controller associated with the template and click the + Add icon.
Redundant Pair (Group of Fields)	
◦ Enable	Click to create a redundant template.
◦ VRRP	Click to enable VRRP.
◦ Cloud CPE	Click to enable cloud-based solutions.

◦ Redundant Pair Type	Select redundant pair type. The options are: ◦ Active-Active ◦ (For Release 22.1.1 and later.) Active-Standby
◦ Redundant Template Name	(For Active-Active redundant pairs only.) Enter the name of the redundant template.
Analytics and Software Version (Group of Fields)	
◦ Analytics Cluster	Select an analytics cluster.
◦ Preferred Software Version	Select the preferred version of the software that should be deployed on Versa Director. The preferred software version applies to zero-touch provisioning (ZTP). During ZTP, Versa Director upgrades a branch to the preferred version, if applicable. The preferred version can be backward compatible for up to two previous VOS versions.
Resource Tags	(For Releases 22.1.1 and later.) Enter a tag name, and then click Add icon to add the resource tag.

4. 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.



Organization: Provider

You are currently in Director View

Configure Interfaces

Template: Active-standby-template

Device Port Configuration

Device Model: Others

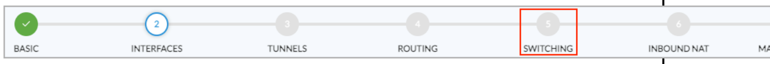
Number of Ports: 6

Virtual Ports	WWAN	WIFI	IRB	T1/E1	DSL
	0	0	0	0	0

□	Port	Interface	VLAN ID	Network Name	Organizations	Priority	IPv4	IPv6	Circuit Type	Circuit Media	Circuit Tags	Sub Interface	Actions

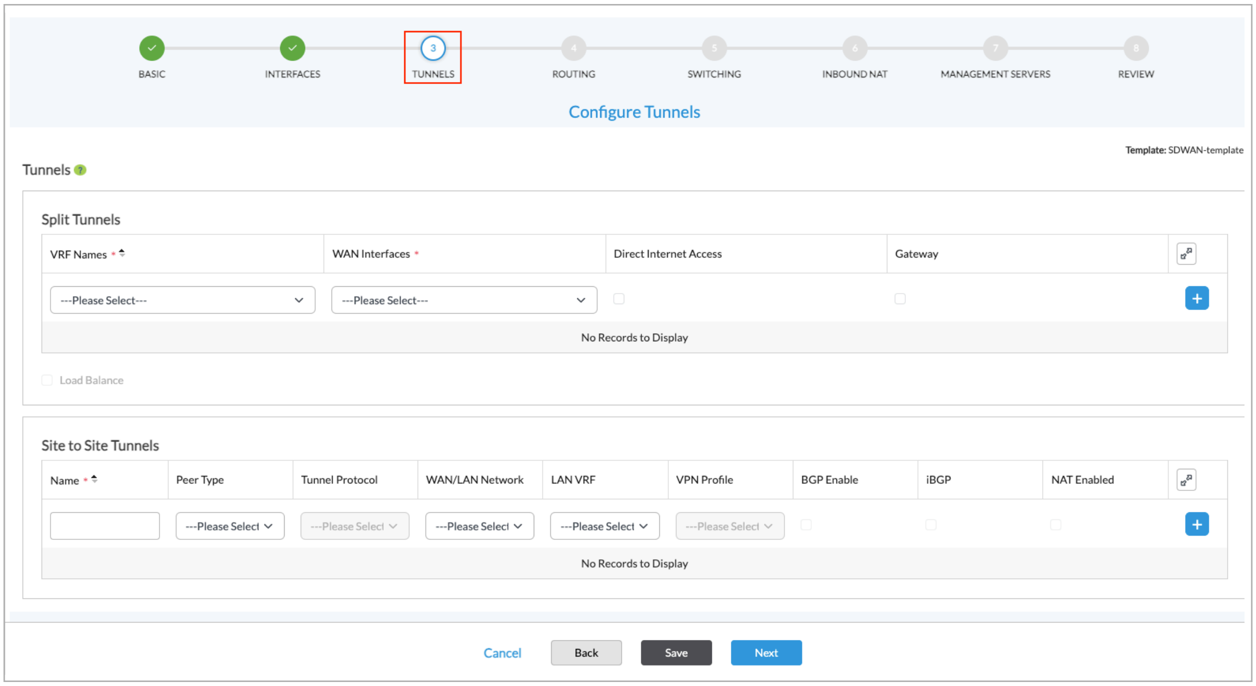
No Record Added

Field	Description
Device Port Configuration (Group of Fields)	
◦ Device Model	Select a device model.
◦ NIC Port	Select a NIC port, and then click Configure in the Device Port Configuration section to configure the port. Note: The NIC port field is not visible for the following device models: ◦ CSG2500 ◦ CSG3300 ◦ CSG3500 ◦ CSG5000
Virtual Ports (Group of Fields)	
◦ WWAN (For Releases 22.1.1 and later; called LTE in earlier releases)	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. For more information, see Configure WWAN. The term *WWAN interfaces* is used to represent LTE, 4G, and 5G interfaces.
◦ WiFi	Click Configure in the Virtual Ports box and then click Add in the WiFi box to configure WiFi as LAN ports. You can create up to eight WiFi interfaces on the LAN interface. The device automatically assigns port numbers to the LAN interfaces that range from 200 to 207. Note that only DHCP v4 is supported. For more information, see Configure Layer 2 Forwarding.
◦ IRB	(For Releases 21.1.1 and later.) Click Configure in the Virtual Ports box, and then click Add in the Integrated

	routing and bridging (IRB) box to configure 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. For more information, see Configure Layer 2 Forwarding.
◦ 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	Enter configuration information for each WWAN interface for LTE, 4G, or 5G service and then save the configuration to populate the WAN interfaces configuration. For more information, see Configure a WAN Interface To Use for WWAN.
L2 Interfaces	Enter configuration information for each L2 interface and then save the configuration to populate the L2 interfaces configuration. Note that once you add an L2 interface, the Switching tab appears as Step 5 in the workflow.  ✓ BASIC 2 INTERFACES 3 TUNNELS 4 ROUTING 5 SWITCHING 6 INBOUND NAT MA
LAN Interfaces	Enter configuration information for each LAN interface and then save the configuration to populate the LAN interfaces configuration. For each physical port, you can add up to 4096 subinterfaces. For each subinterface, you must configure a network name, which is used for traffic identification.

	Note that the interface and subinterface network names in a Workflow template must be unique. To have multiple subinterfaces belong to the same network, modify the configuration later from the Templates > Device Template menu. For information about adding and modifying network interfaces, see Configure Interfaces.

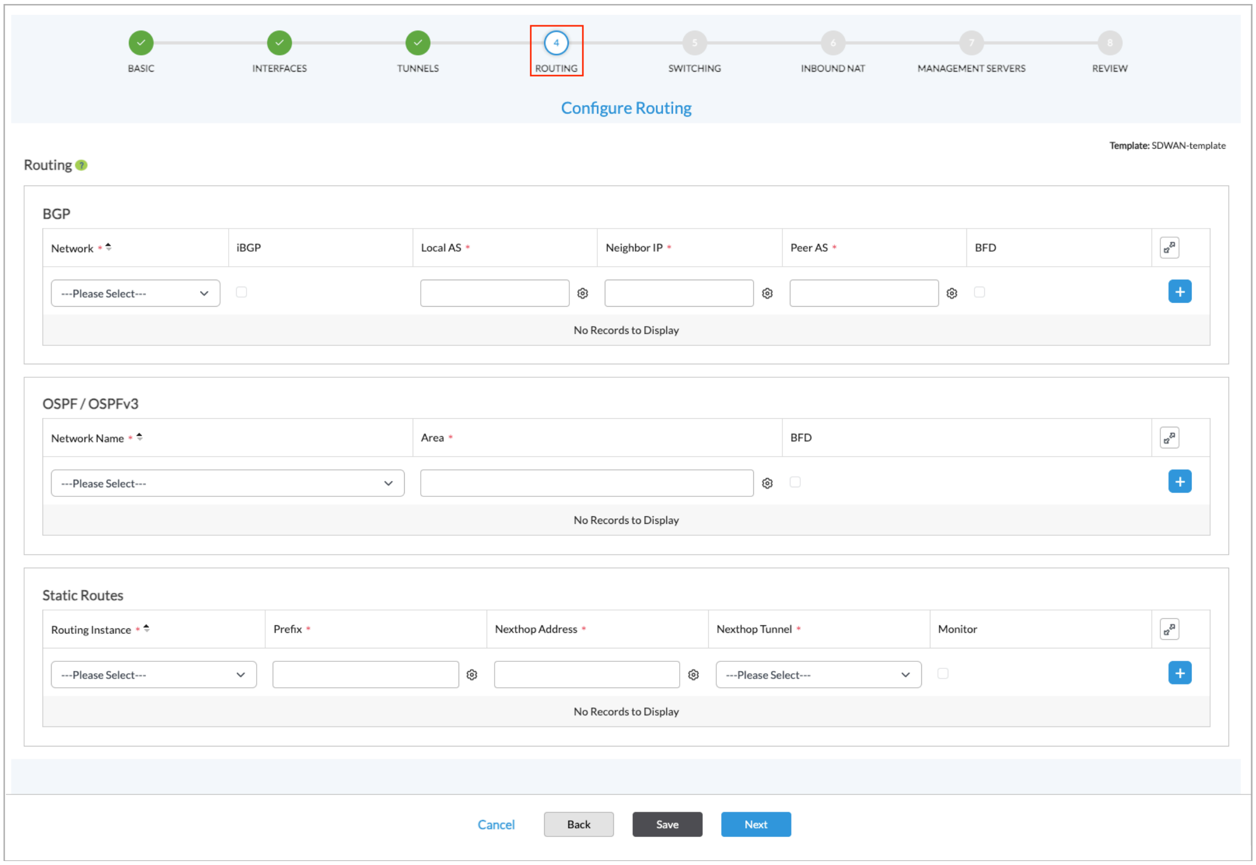
5. Click Save to save the configuration, or click Next to continue.
6. The Step 3, Configure Tunnels screen displays. (You can configure site-to-site tunnels for Releases 20.2 and later.) Split tunnels allow traffic to flow from a common source to different destinations over different interfaces. For 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 a VRF name.
◦ WAN Interfaces	Select a WAN interface.
◦ Direct Internet Access	Click to enable direct internet access (DIA). Source NATing is performed before packets are sent out to the WAN interface.
◦ Gateway	Click to have the local router as a gateway between other SD-WAN sites and non–SD-WAN sites. Split tunnels are not required on SD-WAN sites. Traffic between SD-WAN and non–SD-WAN sites flows through the gateway SD-WAN device. In gateway mode, routes learned from the SD-WAN overlay are advertised to MPLS PE routers, and routes learned from MPLS PE routers are advertised to SD-WAN overlay.
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: ◦ Azure Virtual WAN—Deploy a tunnel on Azure Virtual WAN. ◦ Unmanaged—Deploy a tunnel on any third-party device that supports IPsec tunnels, such as Cisco, Palo Alto, and Juniper. ◦ Zscaler Unmanaged—Deploy a tunnel on a Zscaler endpoint
WAN/LAN Network	Select the network to use. For the peer type Azure Virtual WAN, you can select only WAN networks. For the peer type Unmanaged or Zscaler Unmanaged, 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 Unmanaged or Zscaler Unmanaged 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 Configure a Site-to-Site Tunnel. When the peer type is Zscaler, you must create two tunnels, and this field lists only VPN profiles with two tunnels.
BGP Enabled	For the peer type Azure Virtual WAN, click to enable BGP. For the peer type Unmanaged or Zscaler Unmanaged, 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.

7. Click Save to save the configuration, or click Next to continue. The Step 4, 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.



Configure Routing

Template: SDWAN-template

Routing

BGP

Network *	iBGP	Local AS *	Neighbor IP *	Peer AS *	BFD
---Please Select---	□				□

No Records to Display

OSPF / OSPFv3

Network Name *	Area *	BFD
---Please Select---		□

No Records to Display

Static Routes

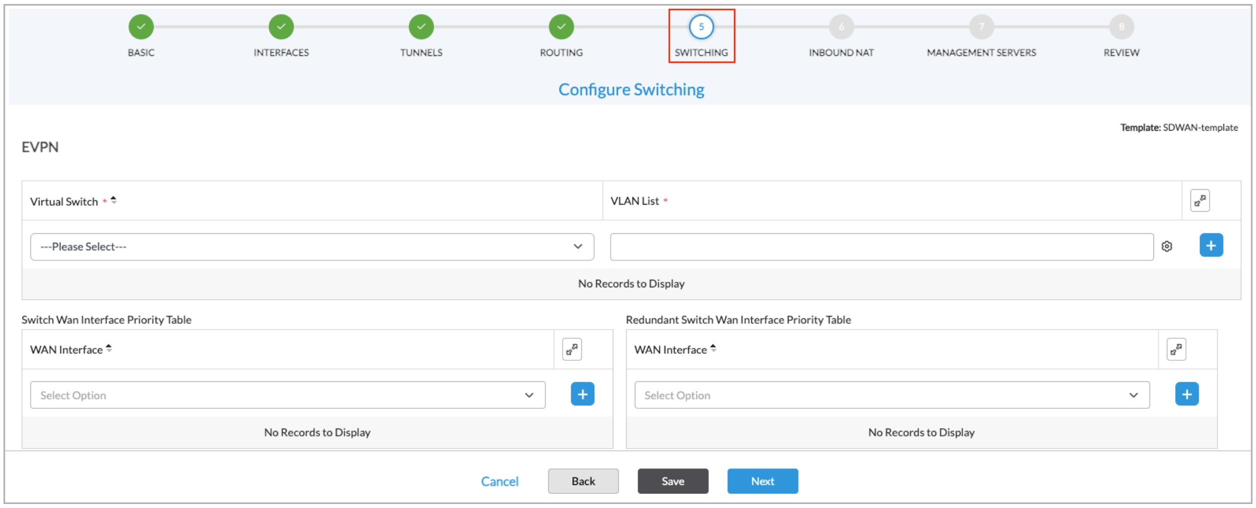
Routing Instance *	Prefix *	Nexthop Address *	Nexthop Tunnel *	Monitor
---Please Select---			---Please Select---	□

No Records to Display

Field	**Description**
BGP (Group of Fields)	Enter the following data or click the ⚙ Parameterize icon to generate data dynamically. Click the + Add icon.
◦ Network	Select the name of the network.
◦ IBGP	Click to run IBGP.
◦ Local AS	Enter the local autonomous system number.
◦ Neighbor IP	Enter the neighbor's IP address.
◦ Peer AS	Enter the neighbor's autonomous system number
◦ BFD	Click to enable bidirectional forwarding.
OSPF/OSPFv3 (Group of Fields)	Enter the following data or click the ⚙ Parameterize icon to generate data dynamically. Click the + Add icon.
◦ Network Name	Select the name of the network.
◦ Area	Enter the OSPF area number.
◦ BFD	Click to enable bidirectional forwarding.
Static Routes (Group of Fields)	Enter the following data or click the ⚙ Parameterize icon to generate data dynamically. Click the + Add icon.
◦ Routing Instance	Select the name of the routing instance.
◦ Prefix	Enter the IP prefix of the static route.

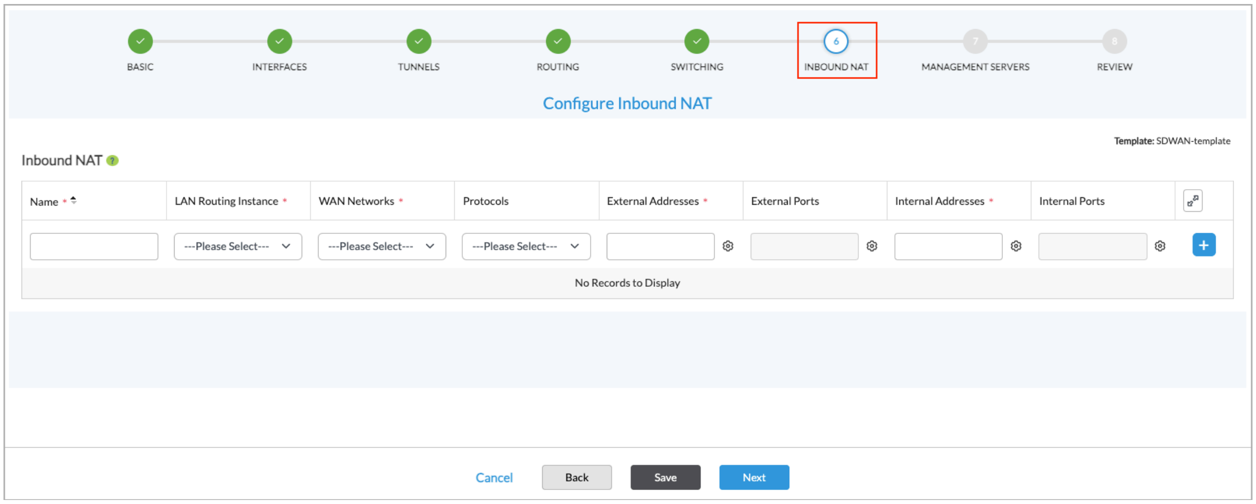
◦ Next Hop	Enter the IP address of the next hop.

8. Click Save to save the configuration, or click Next to continue. For Releases 21.1.1 and later, select the Switching step to configure Ethernet VPN (EVPN) over SD-WAN. Note that this step is displayed only when you select Layer 2 (L2) as the type of interface in the Interfaces tab, in Step 4, 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.
Switch WAN Interface Priority Table—WAN Interface	Select the primary WAN interface to use to manage the switch, then click the + Add icon. Select the secondary WAN interface to use if the primary WAN interface fails and click the + Add icon. The priority is determined by the order in which you select the interfaces.
Redundant Switch WAN Interface Priority Table—WAN Interface	Select the primary WAN interface to use to manage the redundant switch, then click the + Add icon. Select the secondary WAN interface to use if the primary WAN interface fails and click the + Add icon. The priority is determined by the order in which you select the interfaces.

9. Click Save to save the configuration, or click Next to continue. The Step 6, 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.



Configure Inbound NAT

Template: SDWAN-template

Inbound NAT

Name *	LAN Routing Instance *	WAN Networks *	Protocols	External Addresses *	External Ports	Internal Addresses *	Internal Ports
	---Please Select---	---Please Select---	---Please Select---				

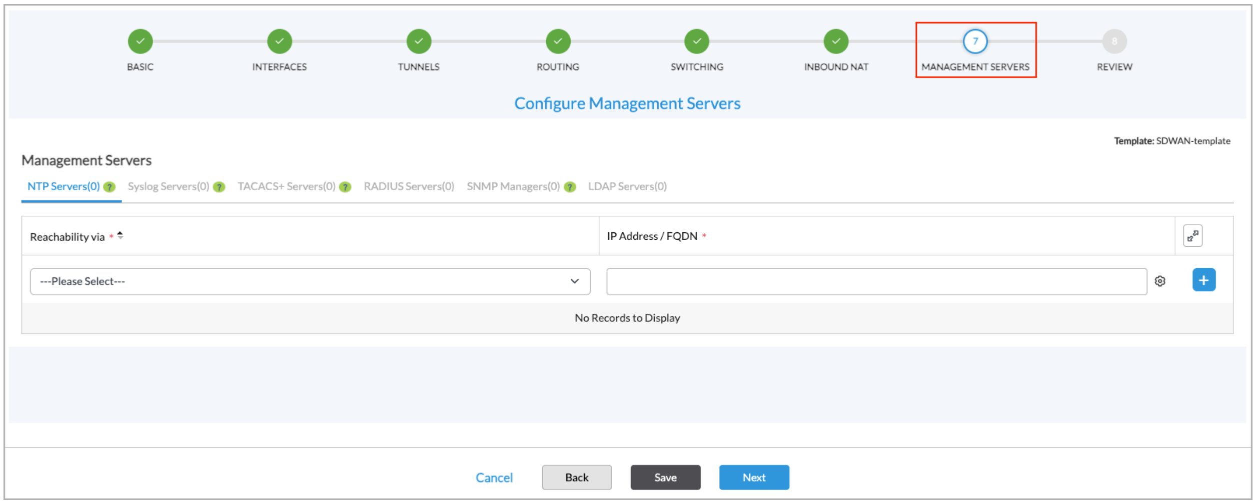
No Records to Display

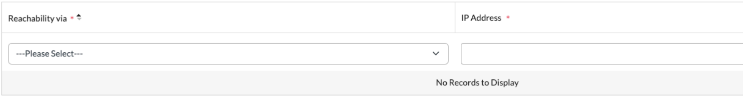
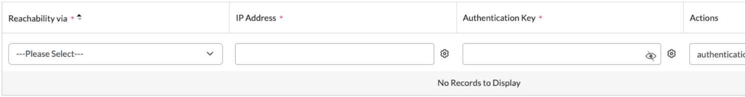
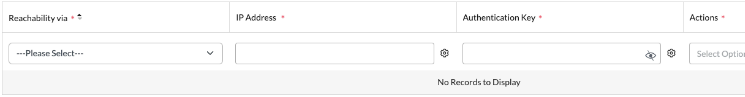
Field	Description
Name	Enter a name for the inbound NAT.
LAN Routing Instance	Select a LAN routing instance.
WAN Network	Select a WAN network.
Protocol	Select a protocol to be used for routing. The options are: ◦ TCP ◦ UDP ◦ ICMP
External Addresses	Enter the source address of the incoming traffic.
External Ports	Enter the source port of the incoming traffic.
Internal Addresses	Enter the address to which traffic is to be sent.
Internal Ports	Enter the port to which traffic is to be sent.

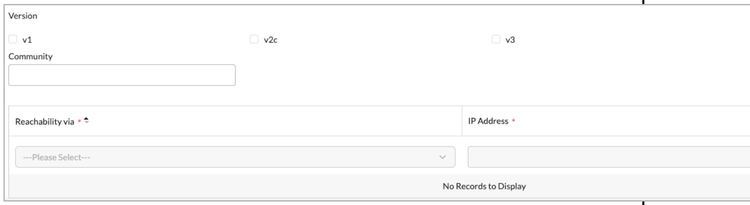
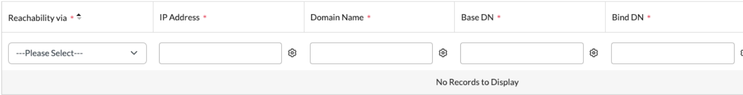
10. Click the + Add icon.

12. Click Next to continue. The Step 7, Configure Management Servers screen displays. Management servers allow to configure the networks and IP addresses of different servers. Enter information for the following fields.

    Click the + Add icon at the end of each line to add the options to the configuration.

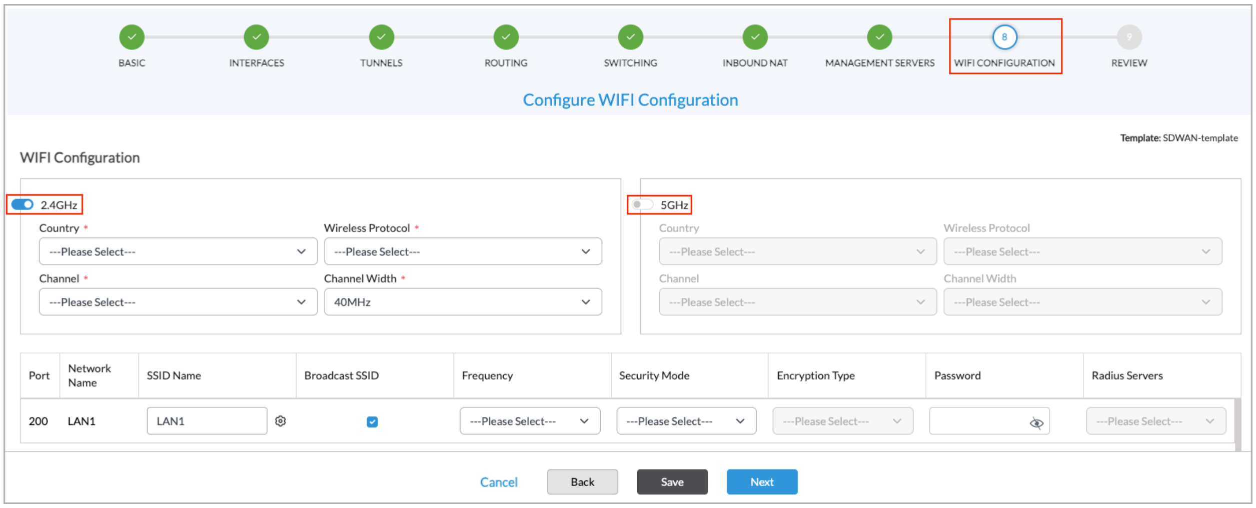

BASIC
INTERFACES
TUNNELS
ROUTING
SWITCHING
INBOUND NAT
7
MANAGEMENT SERVERS
8
REVIEW
Configure Management Servers
Template: SDWAN-template
Management Servers
NTP Servers(0)
Syslog Servers(0)
TACACS+ Servers(0)
RADIUS Servers(0)
SNMP Managers(0)
LDAP Servers(0)
Reachability via *
IP Address / FQDN *
---Please Select---
+
No Records to Display
Cancel
Back
Save
Next

Field	Description
NTP Servers (Tab)	
◦ Reachability via	Select the network to use to access the NTP server.
◦ IP Address/FQDN	Enter the IP address or FQDN of the NTP server.
Syslog Servers (Tab)	 Reachability via * IP Address * ---Please Select--- No Records to Display
◦ Reachability via	Select the network to use to access the syslog server.
◦ IP Address	Enter the IP address of the syslog server.
TACACS+ Servers (Tab)	 Reachability via * IP Address * Authentication Key * Actions ---Please Select--- authenticatio No Records to Display
◦ Reachability via	Select the network to use to access the TACACS+ server.
◦ IP Address	Enter the IP address or FQDN of the TACACS+ server.
◦ Authentication Key	Enter the authentication key to use to access the TACACS+ server.
◦ Actions	Select the actions to take, either Authentication or Accounting.
RADIUS Servers (Tab)	 Reachability via * IP Address * Authentication Key * Actions * ---Please Select--- Select Optio No Records to Display
◦ Reachability via	Select the network to use to access the RADIUS server.
◦ IP Address	Enter the IP address of the RADIUS server.
◦ Authentication Key	Enter the authentication key to use to access the RADIUS server.

◦ Actions	Select actions to be taken, either Authentication, Accounting, or WiFi-authentication.
SNMP Managers (Tab)	 Version v1 v2c v3 Community Reachability via * IP Address * ---Please Select--- No Records to Display
◦ Versions	Select the SNMP version: ◦ v1 ◦ v2c ◦ v3
◦ Community	Enter the SNMP community string to use for access.
◦ Username	(For v3 only.) Enter a user name.
◦ Password	(For v3 only.) Enter a password for the user.
◦ Reachability via	Select the network to use to access the SNMP manager.
◦ IP Address	Enter the IP address of the SNMP manager.
LDAP Servers (Tab)	 Reachability via * IP Address * Domain Name * Base DN * Bind DN * ---Please Select--- No Records to Display
◦ Reachability via	Select the network to use to access the LDAP server.
◦ IP Address	Enter the IP address of the LDAP server.
◦ Domain Name	Enter the domain name to use for LDAP searches, for example, versa-networks.com.
◦ Base DN	Enter the base distinguished name DN to use when an LDAP client initiates a search.
◦ Bind DN	Enter the bind distinguished name (DN) to use when logging in to the LDAP server.

◦ Bind Password	Enter the password that the bind DN uses when logging in to the LDAP server.

13. Click Next to continue. The Step 8, Configure WiFi Configuration screen displays. Note that this step is displayed only when you configure a WiFi virtual interface in Step 4 in the Interfaces tab. For more information, see Configure WiFi. |



Configure WIFI Configuration

Template: SDWAN-template

WIFI Configuration

2.4GHz

Country * ---Please Select---

Wireless Protocol * ---Please Select---

Channel * ---Please Select---

Channel Width * 40MHz

5GHz

Country ---Please Select---

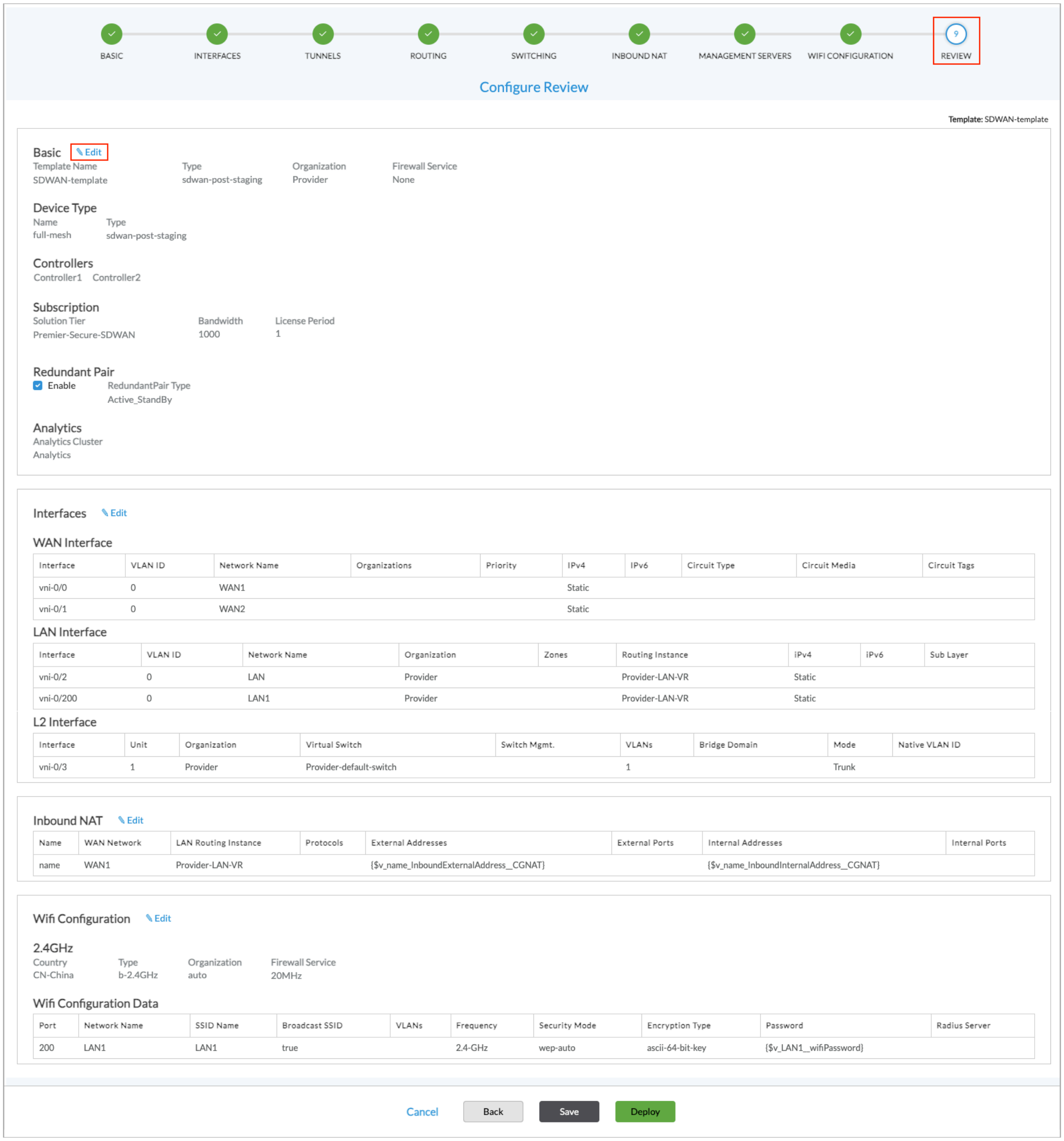
Wireless Protocol ---Please Select---

Channel ---Please Select---

Channel Width ---Please Select---

Port	Network Name	SSID Name	Broadcast SSID	Frequency	Security Mode	Encryption Type	Password	Radius Servers
200	LAN1	LAN1	☑	---Please Select---	---Please Select---	---Please Select---		---Please Select---

14. Click Next to go to Step 9, Review. You can review the configuration and make changes by click the ✏ Edit icon in the main sections.



Configure Review

Template: SDWAN-template

Basic ✎ Edit

Template Name	Type	Organization	Firewall Service
SDWAN-template	sdwan-post-staging	Provider	None

Device Type

Name	Type
full-mesh	sdwan-post-staging

Controllers

Controller1 Controller2

Subscription

Solution Tier	Bandwidth	License Period
Premier-Secure-SDWAN	1000	1

Redundant Pair

☑ Enable	RedundantPair Type
	Active_StandBy

Analytics

Analytics Cluster
Analytics

Interfaces ✎ Edit

WAN Interface

Interface	VLAN ID	Network Name	Organizations	Priority	IPv4	IPv6	Circuit Type	Circuit Media	Circuit Tags
vni-0/0	0	WAN1			Static				
vni-0/1	0	WAN2			Static				

LAN Interface

Interface	VLAN ID	Network Name	Organization	Zones	Routing Instance	iPv4	iPv6	Sub Layer
vni-0/2	0	LAN	Provider		Provider-LAN-VR	Static		
vni-0/200	0	LAN1	Provider		Provider-LAN-VR	Static		

L2 Interface

Interface	Unit	Organization	Virtual Switch	Switch Mgmt.	VLANs	Bridge Domain	Mode	Native VLAN ID
vni-0/3	1	Provider	Provider-default-switch		1		Trunk	

Inbound NAT ✎ Edit

Name	WAN Network	LAN Routing Instance	Protocols	External Addresses	External Ports	Internal Addresses	Internal Ports
name	WAN1	Provider-LAN-VR		{$v_name_InboundExternalAddress__CGNAT}		{$v_name_InboundInternalAddress__CGNAT}	

Wifi Configuration ✎ Edit

2.4GHz

Country	Type	Organization	Firewall Service
CN-China	b-2.4GHz	auto	20MHz

Wifi Configuration Data

Port	Network Name	SSID Name	Broadcast SSID	VLANs	Frequency	Security Mode	Encryption Type	Password	Radius Server
200	LAN1	LAN1	true		2.4-GHz	wep-auto	ascii-64-bit-key	{$v_LAN1__wifiPassword}	

15. Click Save to add the template.
16. Click Deploy to activate the post-staging template. This associates a post-staging template with the Controller nodes, organizations, and other selected entities.

Modify Templates

To modify a staging template:

1. In Director view, select the Workflows tab in the top menu bar.
2. Select Template > Templates from the horizontal menu bar.
3. Select the template from the main pane.
4. Deselect the associated Controllers and organizations, or associate new Controllers and organizations.
5. Change the ports and interfaces.
6. Click Redeploy.

To modify a post-staging template:

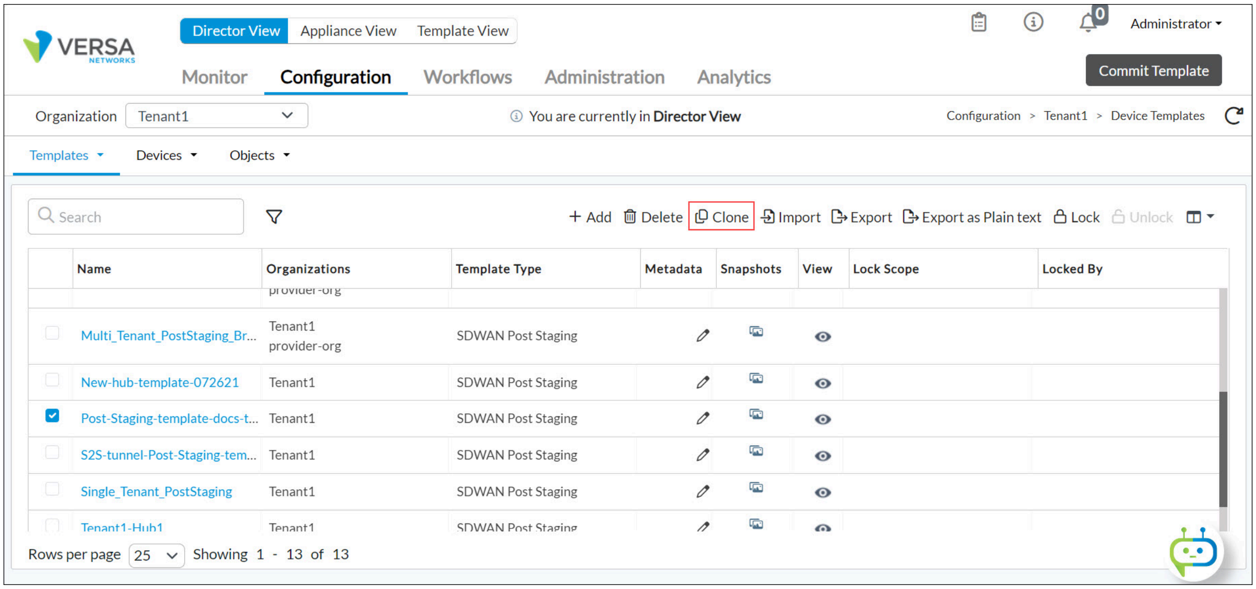
1. In Director view, select the Workflows tab in the top menu bar.
2. Select Template > Templates from the horizontal menu bar.
3. Select the template from the main pane.
4. Deselect the associated Controllers and organizations, or associate new Controllers and organizations.
5. Change the ports and interfaces.
6. Click Redeploy.

Clone Templates

To associate an existing template with another organization, you can clone the template and then modify it. When you clone a template from Configuration > Templates screen, the Templates sections are cloned, and all changes that you have made to the template using workflows and all changes that you have made manually to the template are copied to the clone.

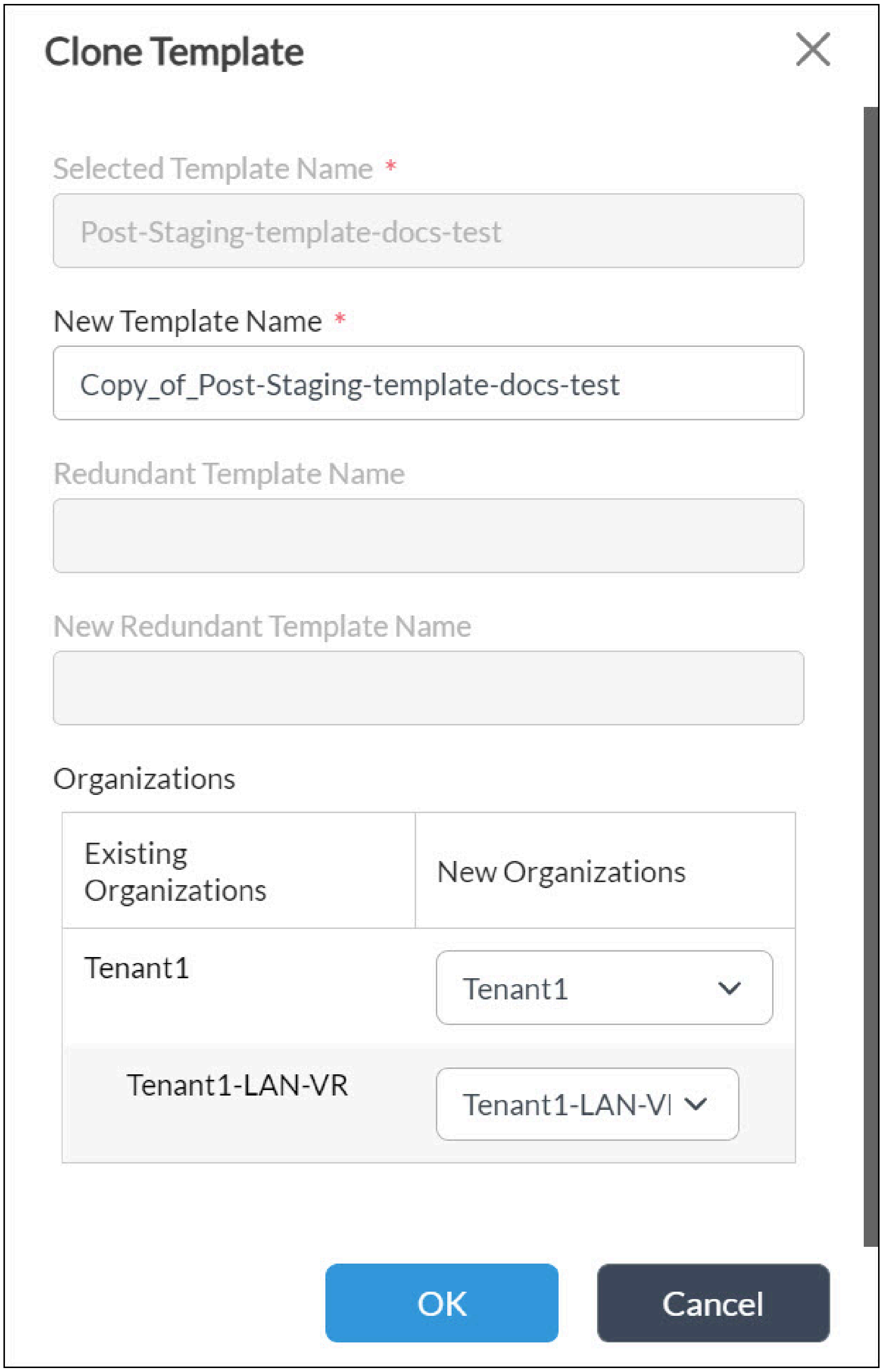
To clone a template:

1. In Director view, select the Configuration tab in the top menu bar.
2. Select Template > Templates in the horizontal menu bar.
3. In the main pane, select the template that you want to clone.
4. Click the ⧉ Clone icon.



	Name	Organizations	Template Type	Metadata	Snapshots	View	Lock Scope	Locked By
		provider-org						
□	Multi_Tenant_PostStaging_Br...	Tenant1 provider-org	SDWAN Post Staging	✎		●		
□	New-hub-template-072621	Tenant1	SDWAN Post Staging	✎		●		
☑	Post-Staging-template-docs-t...	Tenant1	SDWAN Post Staging	✎		●		
□	S2S-tunnel-Post-Staging-tem...	Tenant1	SDWAN Post Staging	✎		●		
□	Single_Tenant_PostStaging	Tenant1	SDWAN Post Staging	✎		●		
□	Tenant1-Hub1	Tenant1	SDWAN Post Staging	✎		●		

5. In the Clone Template popup window, enter information for the following fields.



Clone Template

Selected Template Name *

Post-Staging-template-docs-test

New Template Name *

Copy_of_Post-Staging-template-docs-test

Redundant Template Name

New Redundant Template Name

Organizations

Existing Organizations	New Organizations
Tenant1	Tenant1
Tenant1-LAN-VR	Tenant1-LAN-VI

Field	Description
New Template Name	Enter a name for the cloned template name.
New Organizations	Select the organizations to associate with the template.

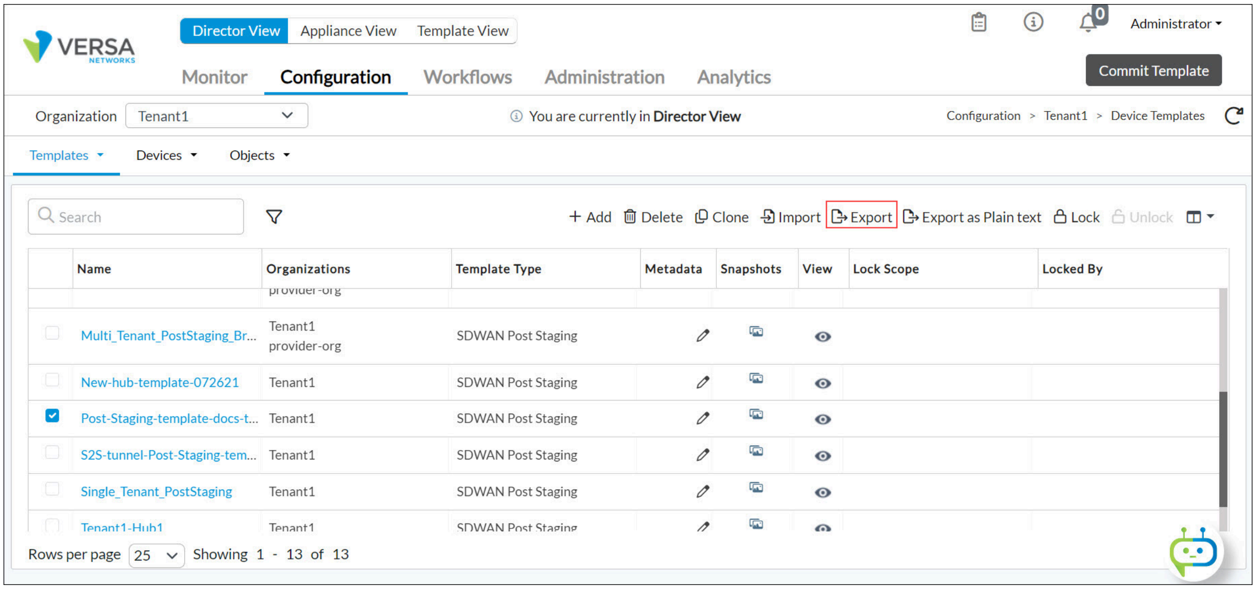
6. Click OK.

Export Templates

To archive or store a device template, you export the template to your local machine. The template is exported as a .cfg file.

To export a template:

1. In Director view, select the Configuration tab in the top menu bar.
2. Select Template > Templates in the horizontal menu bar.
3. In the main pane, select the template that you want to export.
4. Click the Export icon.



	Name	Organizations	Template Type	Metadata	Snapshots	View	Lock Scope	Locked By
		provider-org						
☐	Multi_Tenant_PostStaging_Br...	Tenant1 provider-org	SDWAN Post Staging					
☐	New-hub-template-072621	Tenant1	SDWAN Post Staging					
☑	Post-Staging-template-docs-t...	Tenant1	SDWAN Post Staging					
☐	S2S-tunnel-Post-Staging-tem...	Tenant1	SDWAN Post Staging					
☐	Single_Tenant_PostStaging	Tenant1	SDWAN Post Staging					
☐	Tenant1-Hub1	Tenant1	SDWAN Post Staging					

Rows per page 25 Showing 1 - 13 of 13

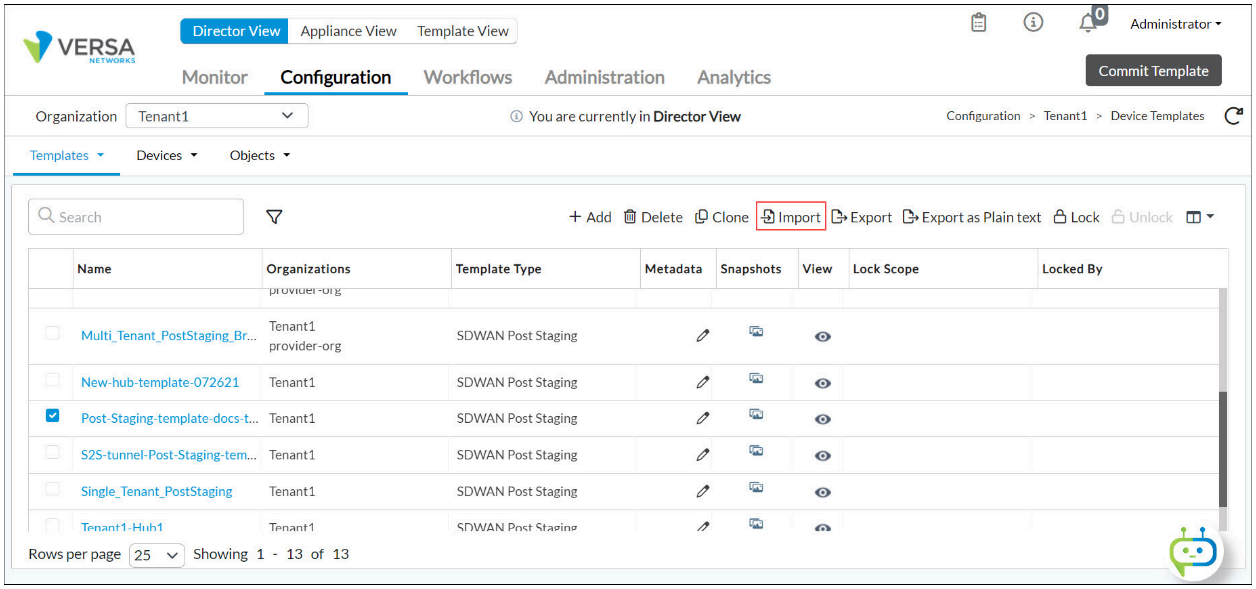
Import Templates

To restore an archived device template or to copy the configuration from one template to another, you import a template. Doing this replaces the existing configuration with the one in the imported template. The imported template must have the same name as the existing template.

To import a template:

1. If the template you are importing does not have the same name as the existing template, rename the template you are importing.
2. In Director view, select the Configuration tab in the top menu bar.

3. Select Template > Templates in the horizontal menu bar.
4. In the main pane, select the template that you want to import.
5. Click the Import icon.



	Name	Organizations	Template Type	Metadata	Snapshots	View	Lock Scope	Locked By
		provider-org						
☐	Multi_Tenant_PostStaging_Br...	Tenant1 provider-org	SDWAN Post Staging	✎	▭	👁		
☐	New-hub-template-072621	Tenant1	SDWAN Post Staging	✎	▭	👁		
☑	Post-Staging-template-docs-t...	Tenant1	SDWAN Post Staging	✎	▭	👁		
☐	S2S-tunnel-Post-Staging-tem...	Tenant1	SDWAN Post Staging	✎	▭	👁		
☐	Single_Tenant_PostStaging	Tenant1	SDWAN Post Staging	✎	▭	👁		
☐	Tenant1-Hub1	Tenant1	SDWAN Post Staging	✎	▭	👁		

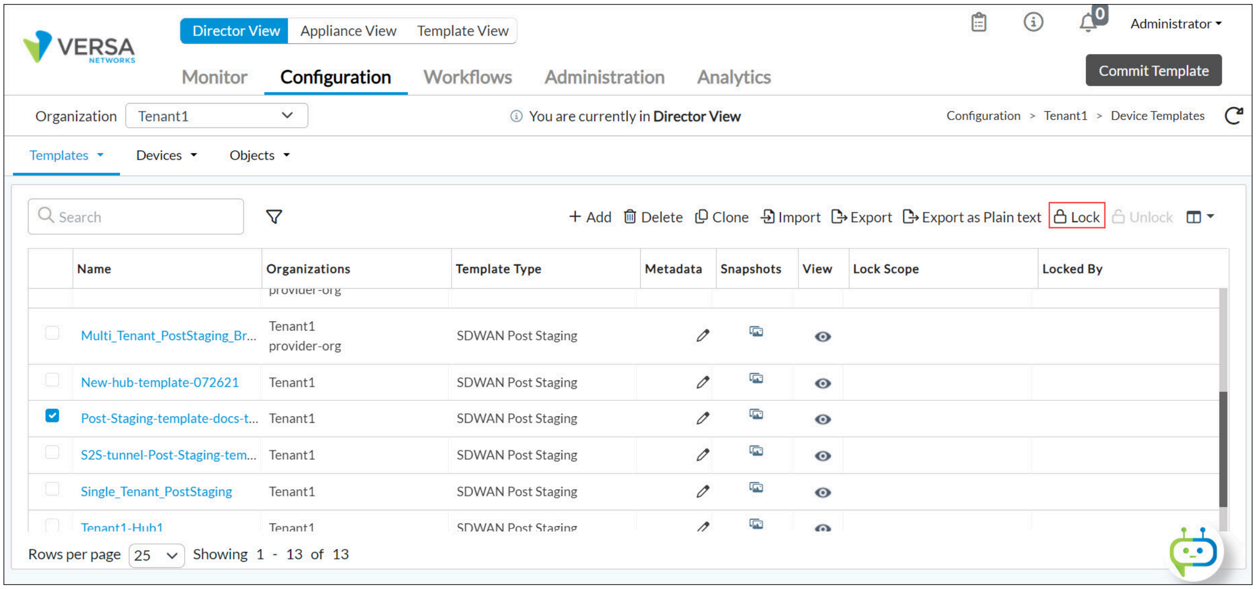
6. Click Browse to select the template file to import.
7. Click Browse to select the template file to be imported. The template must have the same name as the template to which it is imported.
8. Click OK.This copies the configuration of the imported template and associates it with the same organization.

Lock and Unlock Templates

To prevent anyone from making changes to a template, you lock the template.

To lock a template:

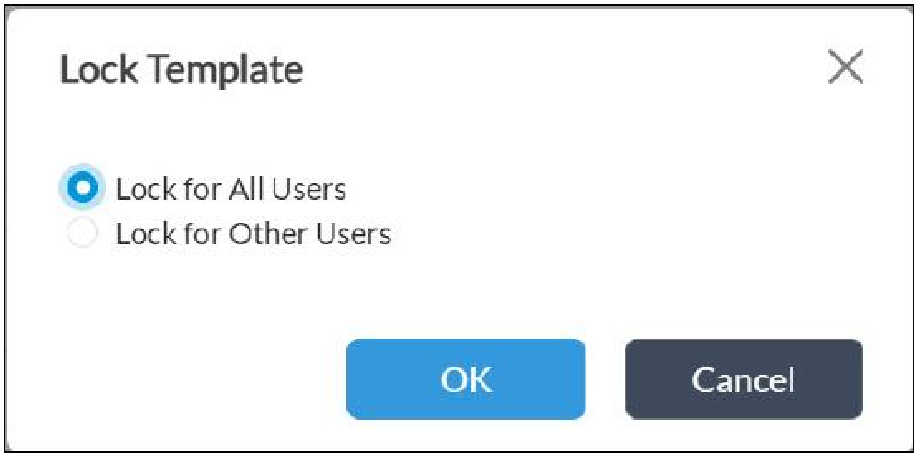
1. In Director view, select the Configuration tab in the top menu bar.
2. Select Template > Templates in the horizontal menu bar.
3. In the main pane, select the template that you want to lock.
4. Click the Lock icon.



	Name	Organizations	Template Type	Metadata	Snapshots	View	Lock Scope	Locked By
		provider-org						
□	Multi_Tenant_PostStaging_Br...	Tenant1 provider-org	SDWAN Post Staging					
□	New-hub-template-072621	Tenant1	SDWAN Post Staging					
☑	Post-Staging-template-docs-t...	Tenant1	SDWAN Post Staging					
□	S2S-tunnel-Post-Staging-tem...	Tenant1	SDWAN Post Staging					
□	Single_Tenant_PostStaging	Tenant1	SDWAN Post Staging					
□	Tenant1-Hub1	Tenant1	SDWAN Post Staging					

Rows per page 25 Showing 1 - 13 of 13

5. Select Lock for all users or Lock for other users. In Lock for other users, the template is locked for all users, except the user who is logged into the system.

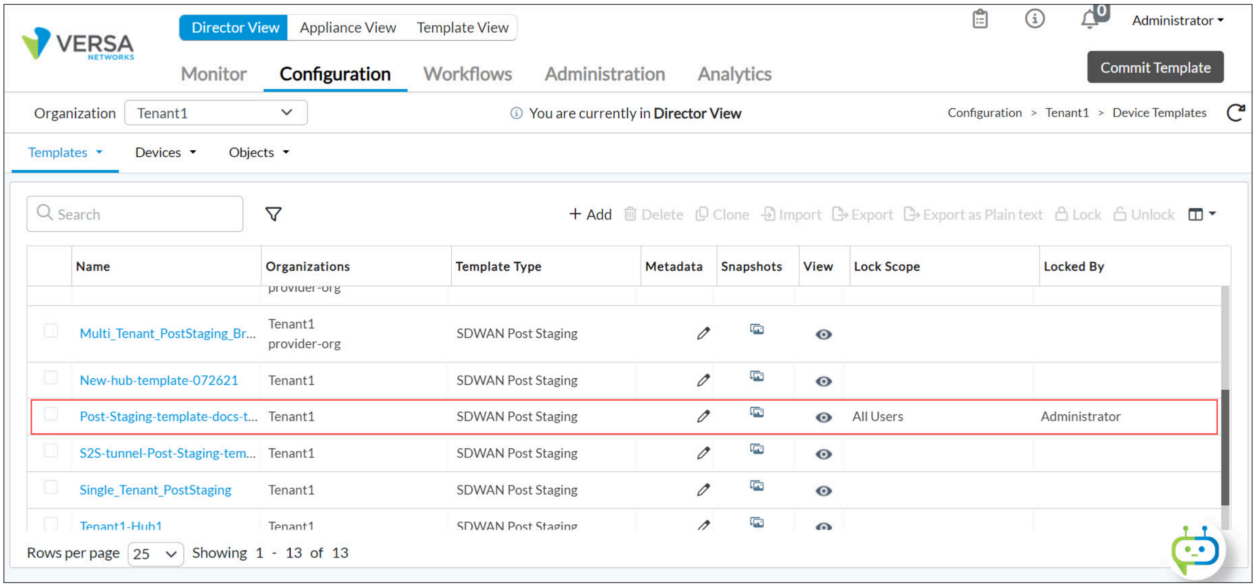


Lock Template

● Lock for All Users

○ Lock for Other Users

6. Click OK. The template is locked.



Name	Organizations	Template Type	Metadata	Snapshots	View	Lock Scope	Locked By
	provider-org						
Multi_Tenant_PostStaging_Br...	Tenant1 provider-org	SDWAN Post Staging	✎	▣	👁		
New-hub-template-072621	Tenant1	SDWAN Post Staging	✎	▣	👁		
Post-Staging-template-docs-t...	Tenant1	SDWAN Post Staging	✎	▣	👁	All Users	Administrator
S2S-tunnel-Post-Staging-tem...	Tenant1	SDWAN Post Staging	✎	▣	👁		
Single_Tenant_PostStaging	Tenant1	SDWAN Post Staging	✎	▣	👁		
Tenant1-Hub1	Tenant1	SDWAN Post Staging	✎	▣	👁		

To unlock a template that is locked:

1. In Director view, select the Configuration tab in the top menu bar.
2. Select Template > Templates in the horizontal menu bar.
3. In the main pane, select the template that you want to lock.
4. Click the 🔓 Unlock icon.

Supported Software Information

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

- Release 21.1.1 add support for configuring switching and IRB, and add the Switching tab on the Create Template screen.
- In Releases 22.1.1, LTE interfaces are renamed to WWAN interfaces; add support for Resource Tag field; add support for active-standby redundant pairs of devices.

Additional Information

Configure Service Chains
Create an SD-WAN Spoke Group
Create Application-Steering Templates
Overview of Configuration Templates