

---

## Configure SD-LAN Using Workflow Templates

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

To configure SD-LAN on a Versa Operating System™ (VOS™) device, you use a configuration wizard on the Director node. The configuration wizard guides you through the creation of a workflows template, which defines the SD-LAN options that you want to use. For some options, the template refers to profiles and policies, which you can also configure using the wizard. After you complete the SD-LAN workflows template, you deploy the configuration to the switch, which activates the switch in the network.

You can use the SD-LAN configuration wizard to do the following:

- Create the SD-LAN template—Configure basic information about the switch.
- Configure switch ports—Set up physical and virtual interfaces.
- Configure global switching profiles—Configure global profiles for VXLAN, routing, management servers, and 802.1X authentication.
- Configure SD-LAN profiles—Create profiles for ports, 802.1X authentication, and multihoming.
- Configure SD-LAN policies—Configure access control list (ACL) policies.

This article describes how to perform the initial configuration of SD-LAN using the configuration wizard on a Director node.

---

## Before You Begin

Before you start the SD-LAN configuration wizard, ensure that you have the following information:

- Your global organization ID
- Versa CSX switch device type and model
- Versa licensing solution tier that has been purchased for your switch hardware
- Versa licensing add-on tier that has been purchased for your switch hardware
- License period that has been purchased for your software

---

## Access the Configuration Wizard

To access the wizard to configure SD-LAN:

---

[https://docs.versa-networks.com/Secure\\_SD-LAN/Configuration\\_from\\_Director/Configure\\_SD-LAN\\_Using\\_Workflow\\_Templates](https://docs.versa-networks.com/Secure_SD-LAN/Configuration_from_Director/Configure_SD-LAN_Using_Workflow_Templates)

Updated: Wed, 23 Oct 2024 08:45:33 GMT

Copyright © 2024, Versa Networks, Inc.

1. Log in to the Director node.
2. Click Director View in the top menu bar.
3. Select the Workflows tab.
4. Select Template > Templates in the horizontal menu bar. The Template screen displays.
5. Select the SD-LAN tab, and then select the Templates tab. The screen displays the templates that are already configured.

Organization: Select Option

You are currently in Director View

Workflows > Template > Templates

SD-WAN SD-LAN

Templates Profiles Policies

Search

+ Add Delete

Name	Status	Organization	Description	Firewall Service	Analytics Enabled	Type	Device Type	Device Model	Subscription Solu...	Sub
4K1	Deployed	Provider				sdwan-post-staging	access-switch	CSX4300	Essential	3
TeeOne	Deployed	Tenant1				sdwan-post-staging	access-switch	CSX4300	Professional	3

Rows per page: 25 Showing 1 - 2 of 1

6. From here, you can do the following:
  - [Create the SD-LAN template](#)—Select the Templates tab in the horizontal menu bar.
  - [Configure SD-LAN profiles](#)—Select the Profiles tab in the horizontal menu bar.
  - [Configure SD-LAN policies](#)—Select the Policies tab in the horizontal menu bar.

## Create SD-LAN Templates

To begin configuring SD-LAN features, you create an SD-LAN template, and then you configure the switch model, licensing information, and other basic information.

To create an SD-LAN template:

1. If you are continuing from the previous section, skip to Step 3.
2. In Director view:
  - a. Select the Workflows tab in the top menu bar.
  - b. Select Template > Templates in the horizontal menu bar. The Template screen displays.
  - c. Select the SD-LAN tab, and then select the Templates tab. The screen displays the templates that are already configured.
3. In the Templates tab, click + Add. The Configure Initial screen displays. For Release 22.1.3, this is called the Configure Basic screen.

VERSA NETWORKS

Director View | Appliance View | Template View

Monitor | Configuration | **Workflows** | Administration | Analytics

Organization: Select Option | You are currently in Director View | Workflows > Template > Templates

Infrastructure > **Template** > Devices >

1 INITIAL CONFIGURATION 2 CONFIGURE INTERFACES 3 SWITCH 4 MANAGEMENT SERVERS 5 REVIEW

**Configure Initial Configuration**

**Basic**

Name \*

Device Type \*

Choose Access Switch Device Model \*

Type

Organization \*

Analytic Cluster

**Subscription**

Solution Tier \*

License Period \*


Solution Add on Tier

**Controllers**

Controller

Cancel Back Save Next

4. Enter information for the following fields.

Field	Description
Name	Enter a name for the template.
Choose Access Switch Device Model	<p>Select the switch model:</p> <ul style="list-style-type: none"> <li>◦ CSX4300</li> <li>◦ CSX4500</li> <li>◦ CSX8300</li> </ul>
Organization	Select the name of the organization to which the template applies.
Analytics Cluster	Select the Analytics cluster to which to send logs to Versa Analytics.
Controllers	Select the name of the Controller node to manage the switch device, and then click the  Add icon. You can add more than one Controller node to the list.
Subscription (Group of Fields)	Configure information about the software license subscription that has been purchased for the switch hardware.
<ul style="list-style-type: none"> <li>◦ Solution Tier</li> </ul>	<p>Select the solution tier that corresponds to the license that the device is using:</p> <ul style="list-style-type: none"> <li>◦ Elite</li> <li>◦ Essential</li> <li>◦ Professional</li> </ul> <p>For more information, see <a href="#">Licensing Overview</a>.</p>
<ul style="list-style-type: none"> <li>◦ License Period</li> </ul>	<p>Select how long the license is valid:</p> <ul style="list-style-type: none"> <li>◦ 1 year</li> <li>◦ 2 years</li> <li>◦ 5 years</li> </ul>
Solution Add-On Tier	Select the add-on licensing tier to add additional

	services to a licensing tier: <ul style="list-style-type: none"> <li>◦ On-prem ZTNA</li> </ul>
--	--

5. Click Save to save the template, or click Next to advance to Step 2, Configure Interfaces.

---

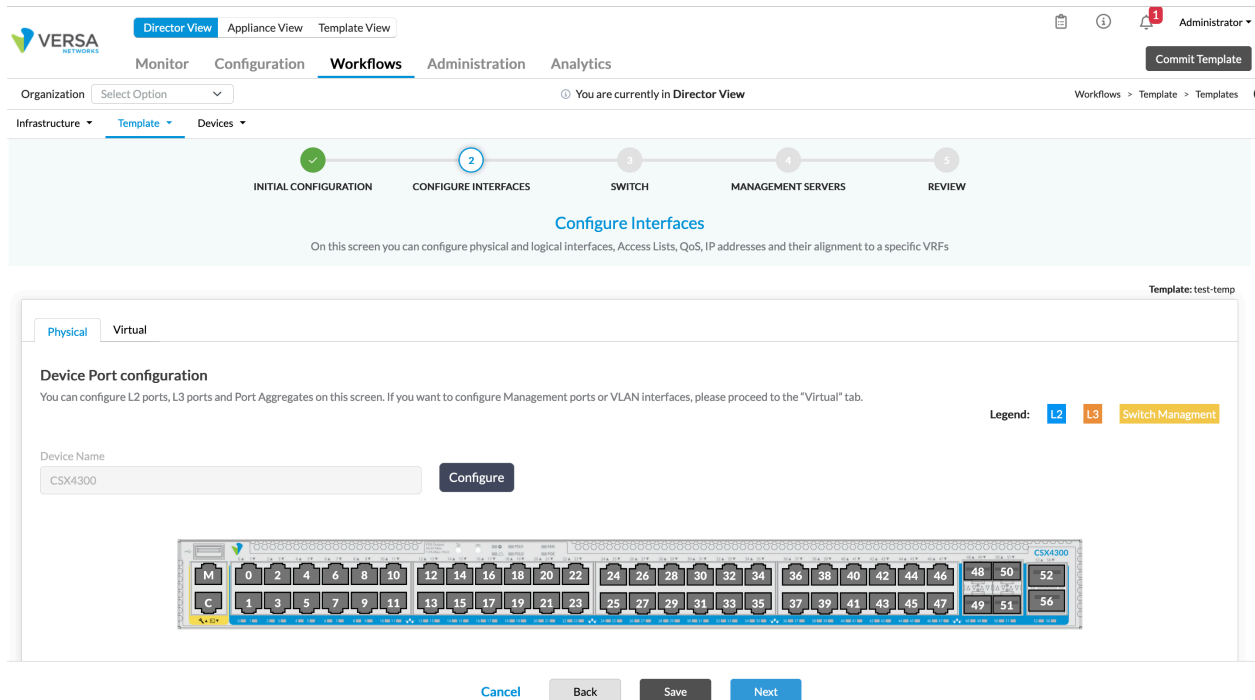
## Configure Physical Switch Ports

Physical switch ports can be categorized into Layer 2 and Layer 3 ports. Layer 2 ports forward Ethernet frames within the same LAN, and Layer 3 ports can communicate across IP networks.

You can set up a Layer 2 or Layer 3 port in the workflow template and configure interface-level options for that port. For some options, you can configure a profile using a separate workflow, and then associate the port with that profile. For information on configuring profiles, see [Create SD-LAN Profiles](#).

To configure physical switch ports:

1. If you are continuing from the previous section, skip to Step 3.
2. In Director view:
  - a. Select the Workflows tab in the top menu bar.
  - b. Select Template > Templates in the horizontal menu bar. The Template screen displays.
  - c. Select the SD-LAN tab, and then select the Templates tab. The screen displays the templates that are already configured.
  - d. Select a template. The Initial Configuration screen displays. For Release 22.1.3, this is called the Configure Basic screen.
3. Click Step 2, Configure Interfaces, or click Next at the bottom of the screen. The Configure Interfaces screen displays.



4. Select the Physical tab in the horizontal menu bar to configure the physical ports on the switch. A graphic displays a representation of the physical ports available in the switch's hardware. Each port icon is labeled with the port number.
  - For Releases 22.1.4 and later:
    - Blue—Layer 2 port
    - Orange—Layer 3 port
    - Yellow—Switch management port (replaces inband management port)
  - For Release 22.1.3:
    - Blue—Access port
    - Orange—Layer 3 port
    - Yellow—Inband management port
5. Click Configure to the right of the Device Name field. The Create Port Configuration popup window displays.

Create Port Configuration

1

2

PORT SELECTION

PROFILES

Legend:

L2

L3

Selected Port Number

None

Cancel

Back

Next

From here, you can configure the following types of ports:

- Layer 2—Configure a port as a switching interface.
- Layer 3—Configure a port as a routing interface.

## Configure a Layer 2 Port

Layer 2 ports include access ports, which connect end users to the switch, and trunk ports, which connect the switch to other switches or routers.

- Access port—Sends and receives Ethernet frames in untagged form. An access port can belong to only one VLAN, known as the access VLAN, and it associates untagged packets with that VLAN. An access port discards tagged frames that do not have a VLAN ID that matches the access VLAN ID.
- Trunk port—Accepts tagged packets. The VLAN ID of the packets must match one of the VLAN IDs that you specify in the VLAN ID List field.

To configure a Layer 2 port on a switch:

1. In the Create Port Configuration popup window, click the numbered port icon on the graphic for the port that you want to configure. The following screenshot shows that Port 12 is selected.

Create Port Configuration

1

2

PORT SELECTION

PROFILES

Legend: L2 L3

Selected Port Number

Port:12 x

Cancel

Back

Next

- In the Selected Port Number field, verify that the selected port number displays.
- Click Next. The Step 2, Profiles popup window displays.

Create Port Configuration

✓

2

PORT SELECTION

PROFILES

Selected Port Number

Port:12 Edit

Port Type

L2

AE

VxLan

Multihomed: (Required VxLAN on)

Port Profile \*

Select Option

Multihomed Profile

---Please Select---

Switching Profile \*

---Please Select---

Cancel

Back

Done

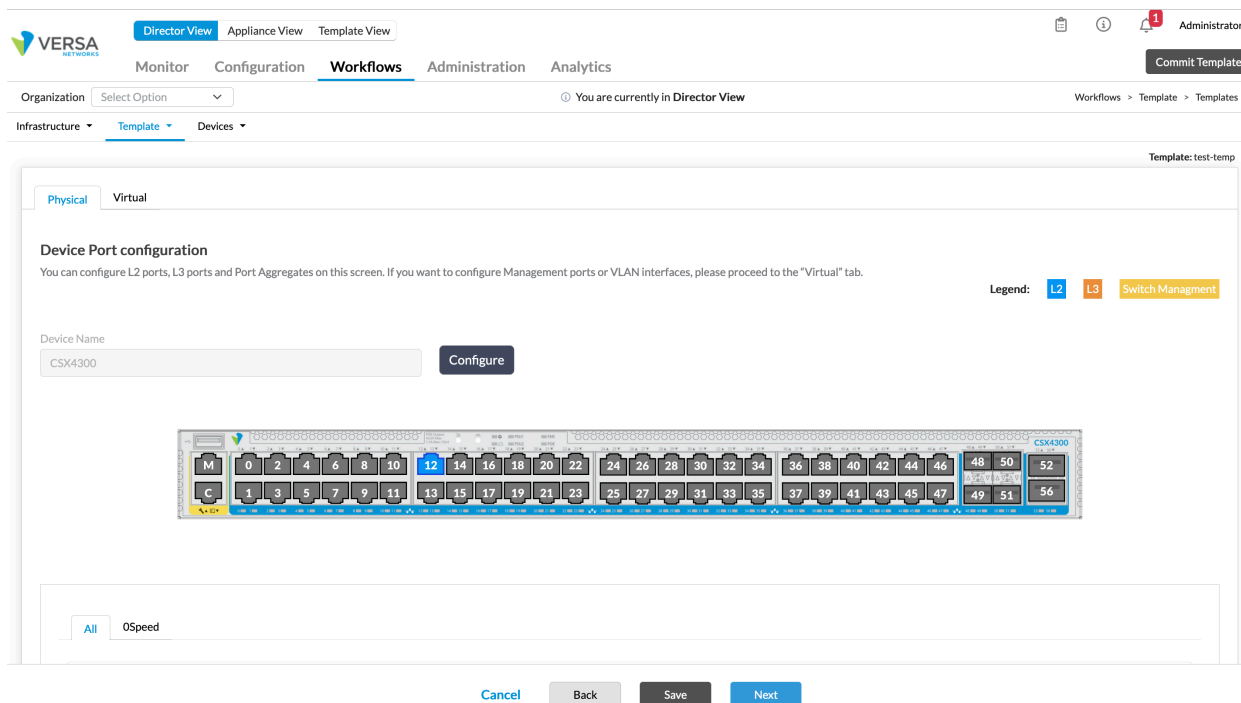
- Enter information for the following fields.



Field	Description
Port Type	For Releases 22.1.4 and later, select Layer 2. This is the default.  For Release 22.1.3, select Access.
AE (Group of Fields)	Click the slider to associate the physical port with a logical aggregated Ethernet interface.
◦ AE Number	Enter the number of the aggregated Ethernet interface.
◦ Chassis ID	Enter the chassis ID number, which is used in calculating the port ID that is associated with the port. <i>Range: 1 through 7</i>
◦ Administrative Key	Enter a numerical administrative key, which is an operational key used in calculating the port ID. <i>Range: 1 through 65535</i>
◦ LACP (Group of Fields)	Click the slider to enable the link aggregation control protocol (LACP).
◦ LACP Mode	Select the LACP mode: <ul style="list-style-type: none"> <li>◦ Active—Enable LACP unconditionally.</li> <li>◦ Passive—Enable LACP only when an LACP device is detected.</li> </ul>
◦ Periodic	Select the periodicity: <ul style="list-style-type: none"> <li>◦ Fast—1 second</li> <li>◦ Slow—30 seconds</li> </ul>
VXLAN	Click the slider to enable or disable virtual extensible LAN (VXLAN) on the port. This enables you to run Layer 2 Ethernet VPN (EVPN) over a Layer 3 IP network using VXLAN.
Multihomed	If you enable VXLAN, click the slider to enable or disable multihoming on the port. This enables you to connect to more than one network, generally to increase reliability or performance.
Port Profile	Select the port profile to associate with the port, or select + Create New to create a new profile. For more information, see <a href="#">Configure Port Profiles</a> .
Multihomed Profile	Select the multihomed profile to associate with the port, or select + Create New to create a new profile.

	multihomed profile see <a href="#">Configure Multihomed Profiles</a> .
Switching Profile	Select the switching profile to associate with the port, or select + Create switching profile, see <a href="#">Configure a Switching Profile</a> .

- Click Done to return to the Configure Interfaces screen. The configured Layer 2 port displays as a blue port icon in the physical port graphic. The following screenshot shows that Port 12 is configured as a Layer 2 port.



- Click Save.

## Configure a Layer 3 Port

A Layer 3 port is a physical port that behaves like a router interface instead of like a switch interface. It has an IP address and supports routing protocols.

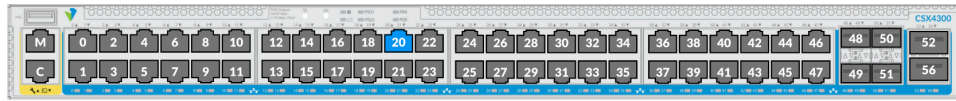
To configure a Layer 3 port on the switch:

- In the Create Port Configuration popup window, click the numbered port icon on the graphic for the port you want to configure. The following screenshot shows that Port 20 is selected.

## Create Port Configuration



Legend: L2 L3



Selected Port Number

Port:20 x

Cancel

Back

Next

2. In the Selected Port Number field, verify that the selected port number appears.
3. Click Next. The Step 2, Profiles popup window displays.

## Create Port Configuration



Selected Port Number

Port:20 Edit

Port Type

L3

Description

Speed

Auto

Duplex

Auto

Network Name

Underlay

Port *	VLAN	IPv4 Address Prefix *
---Please Select---		

Cancel

Back

Done

4. Enter information for the following fields.

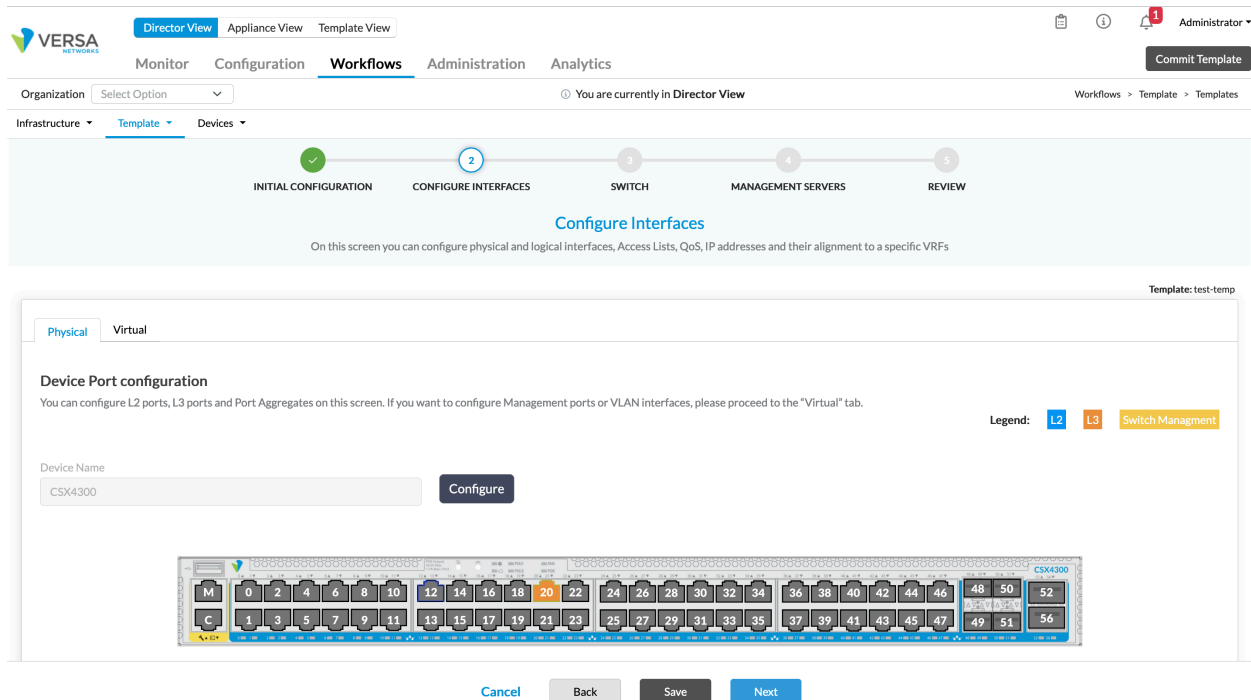
[https://docs.versa-networks.com/Secure\\_SD-LAN/Configuration\\_from\\_Director/Configure\\_SD-LAN\\_Using\\_Workflow\\_Templates](https://docs.versa-networks.com/Secure_SD-LAN/Configuration_from_Director/Configure_SD-LAN_Using_Workflow_Templates)

Updated: Wed, 23 Oct 2024 08:45:33 GMT

Copyright © 2024, Versa Networks, Inc.

Field	Description
Port Type	Select Layer 3.
Description	Enter a text description for the port.
Speed	Select the data transfer speed, in megabits per second (Mbps): <ul style="list-style-type: none"> <li>◦ 10</li> <li>◦ 100</li> <li>◦ 1000</li> <li>◦ 2500</li> <li>◦ 5000</li> <li>◦ 10000</li> </ul>
Duplex	Select how to negotiate between the device interface and switch interface. <ul style="list-style-type: none"> <li>◦ Auto—Have the switch automatically determine the negotiation type.</li> <li>◦ Full—Transmit data in both directions on a signal carrier at the same time.</li> <li>◦ Half—Transmit data in one direction at a time.</li> </ul>
Port	Select the port for VLAN and address configuration.
VLAN ID	Enter the VLAN ID. Click the Tool icon to parameterize the VLAN ID.
IPv4 Address Prefix	Enter the IPv4 address or prefix. Click the Tool icon to parameterize the IPv4 address or prefix.

- Click Done to return to the Configure Interfaces screen. The configured Layer 3 port now displays as an orange port icon in the physical port graphic. The following screenshot shows Port 20 configured as a Layer 3 port.



6. Click Save.

## Configure Virtual Switch Ports

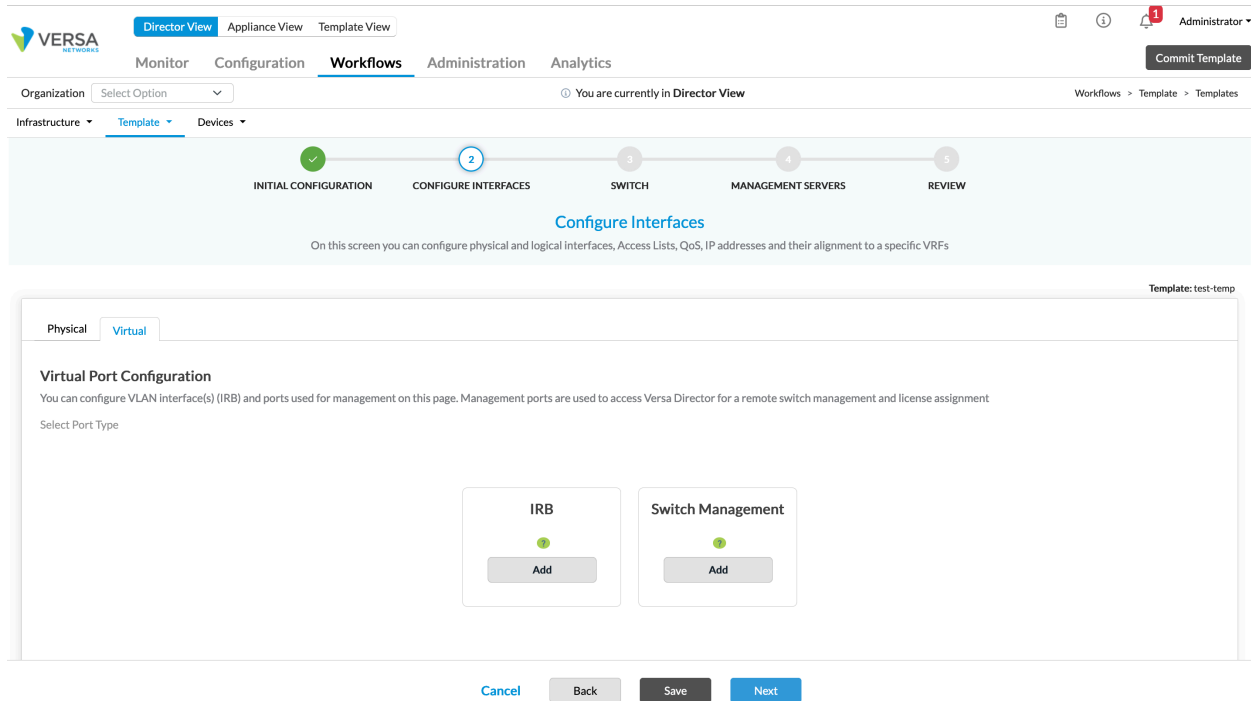
A virtual port on a switch is similar to a physical switch port except that a virtual switch port exists only as a software entity on the switch. Versa SD-LAN supports the following types of virtual ports:

- **Aggregated Ethernet**—Link aggregation combines multiple Ethernet ports on the switch using LACP. Link aggregation increases total throughput beyond what a single port can sustain and provides redundancy for connectivity in case all but one of the physical links fails. You create aggregated Ethernet interfaces when you configure physical ports using the configuration wizard. For more information, see [Configure a Layer 2 Port](#), above.
- **Switch management**—You can configure a management interface to manage the switch remotely using protocols such as Telnet or SSH. You can use a switch management interface for both management and network traffic.
- **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 Dynamic Host Configuration Protocol (DHCP) and Virtual Router Redundancy Protocol (VRRP).

To configure virtual switch ports:

1. If you are continuing from the previous section, skip to Step 3.
2. In Director view:
  - a. Select the Workflows tab in the top menu bar.
  - b. Select Template > Templates in the horizontal menu bar. The Template screen displays.
  - c. Select the SD-LAN tab, and then select the Templates tab. The screen displays the templates that are already configured.

- d. Select a template. The Initial Configuration screen displays. For Release 22.1.3, this is called the Configure Basic screen.
3. Click Step 2, Configure Interfaces, or click Next at the bottom of the screen. The Configure Interfaces screen displays.
4. Select the Virtual tab in the horizontal menu bar. The Virtual Port Configuration screen displays.



5. From here, you can configure the following types of ports:
  - Inband management (for Release 22.1.3)
  - IRB
  - Switch management (for Releases 22.1.4 and later; replaces inband management)

## Configure IRB Ports

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 virtual ports, you can configure some standard Layer 3 interface settings, such as DHCP.

To configure an IRB port on a switch:

1. On the Virtual tab, click Add in the IRB pane. The Virtual Port Configuration—IRB popup window displays.

## Virtual Port Configuration - IRB



Description

IRB Interface Number \*

1..126

Network Name \*

e.g. LAN1

VLAN \*

1..4094

Organization

Provider



IPv4 Address Prefix

IPv6 Address Prefix

Virtual Router \*

---Please Select---



☐ Enable DHCP Server

DHCP Options Profile

---Please Select---



DHCP Relay Forwarding Addresses

[cancel](#)

[Add](#)

2. Enter information for the following fields.

Field	Description
Description	Enter a text description for the IRB virtual port.
IRB Interface Number	Enter the IRB interface number. <i>Range:</i> 1 through 128
Network Name	Enter the logical network name for the interface.
VLAN	Enter the VLAN ID for the IRB virtual port. Click the Tool icon to parame <i>Range:</i> 1 through 4094
Organization	Select the organization with which the IRB virtual port is associated.
IPv4 Address Prefix	Enter the IPv4 address or prefix for the interface. Click the Tool icon to
IPv6 Address Prefix	Enter the IPv6 address or prefix for the interface. Click the Tool icon to
Virtual Router	Select a virtual router to associate with the port.
Enable DHCP Server (Group of Fields)	Click to have the IRB virtual port act as a DHCP server.
<ul style="list-style-type: none"> <li>DHCP Options Profile</li> </ul>	Select the DHCP options profile to associate with the server. To creat Profile popup window, enter information for the following fields, and th <ul style="list-style-type: none"> <li>Organization</li> <li>Name</li> <li>Domain Name</li> </ul>
<ul style="list-style-type: none"> <li>DHCP Relay Forwarding Addresses</li> </ul>	Enter the IP address of the DHCP server to which messages are forw clients to the DHCP server. It is positioned between the DHCP server



3. Click Add.

## Configure a Switch Management Interface

1. In the Virtual Port Configuration screen, click Add in the Switch Management pane. (For Release 22.1.3, this is called the Inband Management pane.) The Virtual Port Configuration—Switch Management popup window displays.




## Management Interface

VLAN *	Port *	IPv4 Address	IPv6 Address	Transport Domain *	
<input type="text"/>	 Select Option ▼	---Please Select--- ▼	---Please Select--- ▼	Select Option ▼	
No Records to Display					

cancel

Add

2. Enter information for the following fields.

Field	Description
VLAN	Enter the VLAN ID for the port. Click the Tool icon to parameterize the VLAN. <i>Range: 1 through 4094</i>
Port	Select the port number.
IPv4 Address	Select an address type: <ul style="list-style-type: none"> <li>DHCP—Use DHCP to dynamically assign an IPv4 address for the interface.</li> <li>Static—Use a static IPv4 address for the interface.</li> </ul>
IPv6 Address	Select an address type: <ul style="list-style-type: none"> <li>DHCP—Use DHCPv6 to dynamically assign an IPv6 address for the interface.</li> <li>Static—Use a static IPv6 address for the interface.</li> </ul>
Transport Domain	Select the transport domain: <ul style="list-style-type: none"> <li>Internet</li> </ul>
	Click to add the interface.

3. Click Add.

# Configure Global Configuration Profiles

You can configure global configuration profiles to define the following switch-level parameters on the VOS device:

- 802.1X authentication
- Routing
- Switching
- Virtual extensible LAN (VXLAN)

To configure global configuration profiles for Releases 22.1.4 and later:

1. If you are continuing from the previous section, skip to Step 3.
2. In Director view:
  - a. Select the Workflows tab in the top menu bar.
  - b. Select Template > Templates in the horizontal menu bar. The Template screen displays.
  - c. Select the SD-LAN tab, and then select the Templates tab. The screen displays the templates that are already configured.
  - d. Select a template.
3. In the Step 1, Initial screen, click Step 3, Switch, or click Next at the bottom of the screen. ;The Configure Switch screen displays.

The screenshot shows the Versa Networks Director web interface. At the top, there's a navigation bar with tabs: Director View (selected), Appliance View, and Template View. Below this is a horizontal menu with: Monitor, Configuration, Workflows (selected), Administration, and Analytics. A 'Commit Template' button is on the right. The main area shows a workflow progress bar with five steps: INITIAL CONFIGURATION, CONFIGURE INTERFACES, SWITCH (current step, circled in blue), MANAGEMENT SERVERS, and REVIEW. Below the progress bar, the 'Switch Configuration' section displays four cards: 'VxLAN Global Configuration' (Configure), 'Routing Global Configuration' (Configure), 'Global Switching Profile' (Edit), and '802.1x Profile selection' (Configure). The 'Global Switching Profile' card is selected, opening a modal window titled 'Global Switching Profile'. This modal has a 'Virtual Switch' dropdown menu with 'Provider-default-switch' selected. At the bottom of the modal are 'Cancel', 'Back', 'Save', and 'Next' buttons.

4. From here, you can configure the following switch-level parameters:
  - 802.1X authentication profile
  - Global switching profile
  - Routing global configuration

[https://docs.versa-networks.com/Secure\\_SD-LAN/Configuration\\_from\\_Director/Configure\\_SD-LAN\\_Using\\_Workflow\\_Templates](https://docs.versa-networks.com/Secure_SD-LAN/Configuration_from_Director/Configure_SD-LAN_Using_Workflow_Templates)

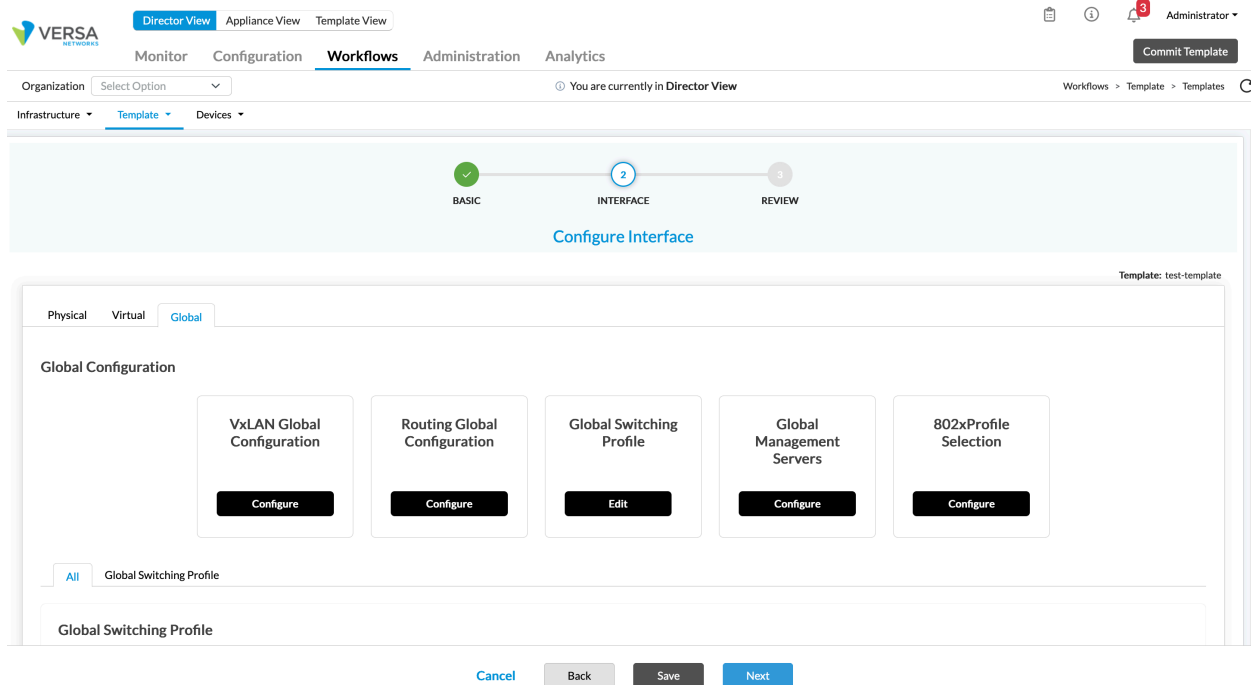
Updated: Wed, 23 Oct 2024 08:45:33 GMT

Copyright © 2024, Versa Networks, Inc.

- VXLAN global configuration

To configure global configuration profiles for Release 22.1.3:

1. If you are continuing from the previous section, skip to Step 3.
2. In Director view:
  - a. Select the Workflows tab in the top menu bar.
  - b. Select Template > Templates in the horizontal menu bar. The Template screen displays.
  - c. Select the SD-LAN tab, and then select the Templates tab. The screen displays the templates that are already configured.
  - d. Select a template.
3. In the Step 1, Basic screen, click Step 2, Interfaces, or click Next at the bottom of the screen. The Step 2, Interface screen displays.
4. Select the Global tab in the horizontal menu bar. The Global Configuration screen displays.



5. From here, you can configure the following global switch parameters:
  - 802.1X profile selection
  - Global management servers
  - Global switching profile
  - Routing profile
  - VXLAN profile

---

## Configure a Global VXLAN Profile

VXLAN is a data plane encapsulation protocol that allows you to run Layer 2 Ethernet VPN (EVPN) over a Layer 3 IP network using standard VXLAN encapsulation over UDP. In multitenant and cloud environments, VXLAN allows a network to handle much larger traffic loads than traditional VLANs while providing the same traffic isolation and segmentation as traditional VLANs.

Before you can configure the global VXLAN profile, you must first configure at least one physical port on the switch as a Layer 3 interface. For more information, see [Configure a Layer 3 Port](#), above.

To configure a global VXLAN profile:

1. In the Global Configuration screen, click Configure in the VXLAN Global Configuration pane. The VXLAN Global Configuration popup window displays.

VxLAN Global Configuration

Description

Local AS 0 to 4294967295

VTEP IP Address \*

VxLAN Bridge Domain List

VNID	Bridge Domain VLAN	
	---Please Select---	+
No Records to Display		

IP Address	iBGP	Peer AS	
	<input type="checkbox"/>		+
No Records to Display			

cancel Add

2. Enter information for the following fields:

Field	Description
Description	Enter a text description for the global VXLAN profile.
Local AS	Enter the local autonomous system (AS) number. <i>Range:</i> 0 through 4294967295
VTEP IP Address	Enter the IP address for the VXLAN tunnel endpoint (VTEP).
VXLAN Bridge Domain List	Enter a list of VLANs to use in the VXLAN Ethernet VPN (EVPN) tunnel.
VNID	Enter the VXLAN network identifier.
Bridge Domain VLAN	Select the bridge domain VLAN to map to the VNID.
IP Address	Enter the IP addresses for the VXLAN EVPN neighbors to which the VTEP connects over the EVPN tunnel.
IBGP	Click to enable IBGP.
Peer AS	If you do not select IBGP, enter the peer AS number.

3. Click Add.

## Configure Global Routing

You create a global routing profile to configure parameters for static routing and the Open Shortest Path First (OSPF) routing protocol.

Before you can configure the global routing profile, you must first configure at least one physical port on the switch as a Layer 3 interface. For more information, see [Configure a Layer 3 Port](#), above.

To configure a global routing profile:

1. In the Global Configuration screen, click Configure in the Routing Global Configuration pane. The Routing Global Configuration popup window displays.

Routing Global Configuration

Static

OSPF

Description

Area Number

0..4294967295

Network Name

Underlay

BFD

cancel

Add

2. Enter information for the following fields:

Field	Description
Static (Group of Fields)	Click Static to configure static IP routes.
◦ Prefix	Enter the IP address prefix for the static route
◦ Next-Hop Address	Enter the next-hop IP address for the static route.
OSPF (Group of Fields)	Click to configure OSPF.
◦ Description	Enter a text description for the OSPF configuration.
◦ Area Number	Enter the OSPF area ID. A backbone area has an area ID of 0.0.0.0. A
◦ BFD	Click to enable BFD for OSPF. When BFD is enabled, if OSPF goes d

3. Click Add.

## Modify the Global Switching Profile

The configuration wizard includes a global switching profile with predefined options for spanning-tree protocols that you can modify. You can also configure a profile for interface-level switching options and associate it with a port when you configure the port as a Layer 2 interface. For more information, see [Configure a Switching Profile](#).

To modify the global switching profile:

1. In the Global Configuration screen, click Edit in the Global Switching Profile pane. The Global Switching Profile

popup window displays.

Global Switching Profile

Virtual Switch

Provider-default-switch

Global Spanning Tree Profile

RSTP

Spanning Tree Bridge Priority

32768

cancel

Add

2. Enter information for the following fields:

Field	Description
Global Spanning-Tree Profile	Select a protocol for the profile: <ul style="list-style-type: none"><li>◦ MSTP—Multiple Spanning-Tree Protocol</li><li>◦ RSTP—Rapid Spanning-Tree Protocol</li></ul>
Spanning-Tree Bridge Priority	Enter the spanning-tree bridge priority value to use to determine wh priority value configures a higher priority.

3. Click Add.

## Select the 802.1X Global Profile

You can associate the template with a profile to use for processing 802.1X authentication requests. If you are using an external RADIUS server for 802.1X authentication, the profile includes the information that the authenticator uses to communicate with the server.

You can pre-configure the 802.1X profile using a separate workflow. For more information, see [Configure 802.1X Authentication Profiles](#).

To select the 802.1X Global Profile:

1. In the Global Configuration screen, click Configure in the 802.1X Profile Selection pane. The 802.1X Profile Selection popup window displays.

802.1x Profile Selection
✕

802.1x Profile

---Please Select---

cancel

Add

2. Enter information for the following fields:

Field	Description
802.1X Profile	Select a profile, or select + Create New to create a new profile. See <a href="#">Co</a>
Source Network	Select the source network: <ul style="list-style-type: none"> <li>Underlay</li> <li>Management Interface</li> </ul>

3. Click Add.

## Configure Global Management Servers

You can configure the following network management servers at the global level:

- Domain Name System (DNS) servers—A DNS server maintains a directory of domain names and translates them to IP addresses.
- Lightweight Directory Access Protocol (LDAP) servers—Performs a variety of operations, including storing and retrieving data such as user names, passwords, and email addresses; searching for data that match a set of criteria; and authenticating clients.
- Network Time Protocol (NTP) servers—NTP synchronizes clock times on the computers in a network.
- RADIUS servers—RADIUS is a distributed client-server system that secures networks against unauthorized access. It is recommended that you configure either a RADIUS server or a TACACS+ server, but not both.
- Simple Network Management Protocol (SNMP) servers—SNMP is an open standard networking protocol that is used for managing, monitoring, and organizing data about networking devices on both LANs and WANs.
- Syslog servers—Syslog servers consolidate logs from multiple sources into a single location.
- TACACS+ servers—TACACS+ provides detailed accounting information and flexible administrative control over authentication and authorization processes. It is recommended that you configure either a RADIUS server or a TACACS+ server, but not both.

To configure global management servers for Releases 22.1.4 and later:

- If you are continuing from the previous section, skip to Step 3.



2. In Director view:
  - a. Select the Workflows tab in the top menu bar.
  - b. Select Template > Templates in the horizontal menu bar. The Template screen displays.
  - c. Select the SD-LAN tab, and then select the Templates tab. The screen displays the templates that are already configured.
  - d. Select a template. The Step 1, Initial Configuration screen displays. In Release 22.1.3, this is the Step 1, Basic screen.
3. Click Step 4, Management Servers. The Configure Management Servers screen displays.

The screenshot shows the Versa Networks Director View interface. At the top, there are tabs for 'Director View', 'Appliance View', and 'Template View'. Below these are navigation tabs: 'Monitor', 'Configuration', 'Workflows' (selected), 'Administration', and 'Analytics'. A 'Commit Template' button is in the top right. The main header shows 'Organization: Select Option' and a status message 'You are currently in Director View'. Below the header, there's a breadcrumb trail: 'Infrastructure > Template > Devices'. The main content area features a workflow progress bar with five steps: 'INITIAL CONFIGURATION', 'CONFIGURE INTERFACES', 'SWITCH', 'MANAGEMENT SERVERS' (highlighted with a blue circle and the number 4), and 'REVIEW'. Below the progress bar, the title 'Configure Management Servers' is displayed. A list of server types is shown: 'NTP Servers(0)', 'Syslog Servers(0)', 'TACACS+ Servers(0)', 'RADIUS Servers', 'SNMP Managers(0)', 'LDAP Servers(0)', and 'DNS Servers(0)'. The 'Template: test-temp' is noted on the right. Below this is a form with two main sections: 'Reachability via' with a dropdown menu (currently showing '---Please Select---') and 'IP Address / FQDN' with a text input field. A 'No Records to Display' message is shown below the form. At the bottom, there are buttons for 'Cancel', 'Back', 'Save', and 'Next'.

4. Enter information for the following fields.

Field	Description
NTP Servers (Tab)	Select to configure one or more NTP servers.
<ul style="list-style-type: none"> <li>◦ Reachability Via</li> </ul>	Select the network to use to reach the NTP server: <ul style="list-style-type: none"> <li>◦ Controllers—Go through the Controller node to reach the NTP server.</li> <li>◦ Management interface—Use the management interface to reach the NTP server.</li> </ul>
<ul style="list-style-type: none"> <li>◦ IP Address/FQDN</li> </ul>	Enter the IP address or fully qualified domain name (FQDN) of the NTP server.
<ul style="list-style-type: none"> <li>◦ Add icon</li> </ul>	Click to add the NTP server.
Syslog Servers (Tab)	Select to configure a syslog server.
<ul style="list-style-type: none"> <li>◦ Reachability Via</li> </ul>	Select the network to use to reach the syslog server: <ul style="list-style-type: none"> <li>◦ Controllers—Go through the Controller node to reach the syslog server.</li> <li>◦ Management interface—Use the management interface to reach the syslog server.</li> </ul>
<ul style="list-style-type: none"> <li>◦ IP Address</li> </ul>	Enter the IP address of the syslog server. Click the Tool icon to parameterize the syslog server.
<ul style="list-style-type: none"> <li>◦ Add icon</li> </ul>	Click to add the syslog server.
TACACS+ Servers (Tab)	Select to configure a TACACS+ server.
<ul style="list-style-type: none"> <li>◦ Reachability Via</li> </ul>	Select the network to use to reach the TACACS+ server: <ul style="list-style-type: none"> <li>◦ Controllers—Go through the Controller node to reach the TACACS+ server.</li> <li>◦ Management interface—Use the management interface to reach the TACACS+ server.</li> </ul>
<ul style="list-style-type: none"> <li>◦ IP Address</li> </ul>	Enter the IP address of the TACACS+ server. Click the Tool icon to parameterize the TACACS+ server.
<ul style="list-style-type: none"> <li>◦ Authentication Key</li> </ul>	Enter the authentication key for the TACACS+ server. Click the Tool icon to parameterize the TACACS+ server.
<ul style="list-style-type: none"> <li>◦ Actions</li> </ul>	Select one or more server actions: <ul style="list-style-type: none"> <li>◦ Accounting</li> <li>◦ Authentication</li> </ul>
<ul style="list-style-type: none"> <li>◦ Add icon</li> </ul>	Click to add the TACACS+ server.

RADIUS Servers (Tab)	Select to configure a RADIUS server.
◦ Reachability Via	Select the network to use to reach the RADIUS server: <ul style="list-style-type: none"> <li>◦ Controllers—Go through the Controller node to reach the RADIUS server.</li> <li>◦ Management interface—Use the management interface to reach the RADIUS server.</li> </ul>
◦ IP Address	Enter the IP address of the RADIUS server. Click the Tool icon to parameterize the IP address.
◦ Authentication Key	Enter the authentication key for the RADIUS server. Click the Tool icon to parameterize the authentication key.
◦ Actions	Select one or more server actions: <ul style="list-style-type: none"> <li>◦ Accounting</li> <li>◦ Authentication</li> <li>◦ WiFi Authentication</li> </ul>
◦ Add icon	Click to add the RADIUS server.
SNMP Servers (Tab)	Select to configure a SNMP server.
◦ Version	Select one or more SNMP versions: <ul style="list-style-type: none"> <li>◦ v1</li> <li>◦ v2c</li> <li>◦ v3</li> </ul>
◦ Community	Community—Enter a community name. A community is a group of devices that share the same configuration.
◦ Username	For SNMPv3 only, enter the username to use to access the SNMP server.
◦ Password	For SNMPv3 only, enter the password to use to access the SNMP server.
◦ Reachability Via	Select the network to use to reach the SNMP server: <ul style="list-style-type: none"> <li>◦ Controllers—Go through the Controller node to reach the SNMP server.</li> <li>◦ Management interface—Use the management interface to reach the SNMP server.</li> </ul>
◦ IP Address	Enter the IP address of the RADIUS server. Click the Tool icon to parameterize the IP address.
◦ Add icon	Click to add the SNMP server.

LDAP Servers (Tab)	Select to configure an LDAP server.
◦ Reachability Via	Select the network to use to reach the LDAP server: <ul style="list-style-type: none"> <li>◦ Controllers—Go through the Controller node to reach the LDAP server.</li> <li>◦ Management interface—Use the management interface to reach the LDAP server.</li> </ul>
◦ IP Address	Enter the IP address of the LDAP server. Click the Tool icon to parameterize the IP address.
◦ Domain Name	Enter the domain name (DN) in which the LDAP server resides. Click the Tool icon to parameterize the domain name.
◦ Base DN	Enter the base DN of the LDAP directory location. Click the Tool icon to parameterize the base DN.
◦ Bind DN	Enter the bind distinguished name (DN) authentication credentials for binding to the LDAP server.
◦ Bind Password	Enter the bind password. Click the Tool icon to parameterize the bind password.
◦ Add icon	Click to add the LDAP server.
DNS Servers (Tab)	Select to configure a DNS server.
◦ Reachability Via	Select the network to use to reach the DNS server: <ul style="list-style-type: none"> <li>◦ Controllers—Go through the Controller node to reach the DNS server.</li> <li>◦ Management interface—Use the management interface to reach the DNS server.</li> </ul>
◦ IP Address/FQDN	Enter the IP address or fully qualified domain name (FQDN) of the DNS server.
◦ Add icon	Click to add the DNS server.

5. Click Save or Next to proceed to the next step in the workflow.

To configure global management servers for Release 22.1.3:

1. If you are continuing from the previous section, skip to Step 4.
2. In Director view:
  - a. Select the Workflows tab in the top menu bar.
  - b. Select Template > Templates in the horizontal menu bar. The Template screen displays.
  - c. Select the SD-LAN tab, and then select the Templates tab. The screen displays the templates that are already configured.

- d. Select a template. The Configure Basic screen displays.
3. Click Step 2, Interfaces, or click Next at the bottom of the screen. The Configure Interface screen displays.
4. Select the Global tab in the horizontal menu bar. The Global Configuration screen displays.
5. Click Configure in the Global Management Servers box. The Global Management Server popup window displays.

6. Enter information for the fields. For field descriptions, see Step 4 of the procedure for Release 22.1.4, above.
7. Click Add to add the global management servers.
8. Click Save or Next to proceed to the next step in the workflow.

## Create SD-LAN Profiles

The SD-LAN profiles workflow allows you to configure some SD-LAN components as a profile that you can reuse for different interfaces or devices. You can associate a pre-configured profile with a specific port, or as part of the global switch configuration.

You can configure profiles for the following SD-LAN components:

- 802.1X authentication
- Multihoming
- Ports
- Switching

## Configure 802.1X Authentication Profiles

When you configure global switch parameters in the workflow template, you can associate the template with an 802.1X authentication profile. For more information, see [Select the 802.1X Global Profile](#).

To configure the 802.1X profile for Releases 22.1.4 and later:

1. In Director view:

[https://docs.versa-networks.com/Secure\\_SD-LAN/Configuration\\_from\\_Director/Configure\\_SD-LAN\\_Using\\_Workflow\\_Templates](https://docs.versa-networks.com/Secure_SD-LAN/Configuration_from_Director/Configure_SD-LAN_Using_Workflow_Templates)

Updated: Wed, 23 Oct 2024 08:45:33 GMT

Copyright © 2024, Versa Networks, Inc.

- a. Select the Workflows tab in the top menu bar.
  - b. Select Template > Templates in the horizontal menu bar. The Template screen displays.
  - c. Select the SD-LAN tab, and then select the Profiles tab. The Profiles screen displays, showing the profile types in the left menu bar.
2. Click 802.1X Profile in the left menu bar. The screen displays the 802.1X profiles that are already configured.
  3. Click the + 802.1X Profile icon. The Configure 802.1X Profile screen displays.
  4. Click the + 802.1X Profile icon. The Configure 802.1X Profile screen displays.

**Configure 802.1x Profile**

802.1x Profile Name \*  Description

Organization \*  Guest VLAN ID \*  Default Auth VLAN ID \*  Mode \*

802.1x Radius Server

Name *	Description	IP Address or Hostname *	Server Port *	Auth Key *
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

No Records to Display

[Cancel](#) [Save](#)

5. Enter information for the following fields:

Field	Description
802.1X Profile Name	Enter a name for the 802.1X profile.
Description	Enter a text description for the 802.1X profile.
Organization	Select the name of the organization to which the profile applies.
Guest VLAN ID	Enter the ID of the guest VLAN.
Default Authentication VLAN ID	Enter the ID of the default VLAN to use for authentication.
Mode	Select the 802.1X supplicant mode used to authenticate end devices. <ul style="list-style-type: none"> <li>Multiple—Allow multiple end devices to connect to the port. If one device authenticates, all other devices can connect.</li> <li>Single—Authenticate only the first end device. All other end devices are denied access until the first device logs out. The subsequent devices effectively bypass authentication. The subsequent devices effectively bypass authentication.</li> <li>Single Secure—Allow only one end device to connect to the port. If one device authenticates, all other devices are denied access until the first device logs out.</li> </ul>
802.1X RADIUS Server (Group of Fields)	
◦ Name	Enter a name for the RADIUS server.
◦ Description	Enter a text description for the RADIUS server.
◦ IP Address of Hostname	Enter the IP address of the RADIUS server.
◦ Server Port	Enter the number of the listening port on the RADIUS server. For example, 1812.
◦ Authentication Key	Enter the authentication key for the RADIUS server.
◦ Add icon	Click to add the RADIUS server.

6. Click Save.

To configure the 802.1X profile for Release 22.1.3:

1. In Director view:
  - a. Select the Workflows tab in the top menu bar.
  - b. Select Template > Templates in the horizontal menu bar. The Template screen displays.
  - c. Select the SD-LAN tab, and then select the Profiles tab. The Profiles screen displays, showing the profile types in the left menu bar.

2. Click 802.1X Profile in the left menu bar. The screen displays the 802.1X profiles that are already configured.
3. Click the + 802.1X Profile icon. The Configure 802.1X Profile screen displays.
4. Select the 802.1X profile type:
  - Local—Perform 802.1X authentication on the local VOS device. VOS devices support certificate authentication based on EAP-TLS.
  - Remote—Perform 802.1X authentication using a RADIUS server.
5. For a local 802.1X profile, enter information for the following fields.

Field	Description
802.1X Profile Name	Enter a name for the 802.1X profile.
Description	Enter a text description for the 802.1X profile.
Organization	Select the name of the organization to which the profile applies.
MAC Address Bypass (Group of Fields)	
◦ MAC Address	Enter the MAC address of the device that is allowed to bypass the 802.1X authentication process.
◦ Description	Enter a text description for the MAC address.
◦ Add icon	Click to add the MAC address.

6. For a remote 802.1X profile, enter information for the following fields.



Field	Description
802.1X Profile Name	Enter a name for the 802.1X profile.
Description	Enter a text description for the 802.1X profile.
Guest VLAN ID	Enter the ID of the guest VLAN.
Default Authentication VLAN ID	Enter the ID of the default VLAN to use for authentication.
Mode	Select the 802.1X supplicant mode used to authenticate end devices. <ul style="list-style-type: none"> <li>Multiple—Allow multiple end devices to connect to the port. If one device authenticates, all other devices can also authenticate.</li> <li>Single—Authenticate only the first end device. All other end devices are denied any further authentication. The subsequent devices effectively remain in the unauthorized state.</li> <li>Single Secure—Allow only one end device to connect to the port. If one device authenticates, all other devices are denied authentication. If the first device logs out, the port returns to the unauthorized state.</li> </ul>
802.1X RADIUS Server (Group of Fields)	
◦ Name	Enter a name for the RADIUS server.
◦ Description	Enter a text description for the RADIUS server.
◦ IP Address of Hostname	Enter the IP address of the RADIUS server.
◦ Server Port	Enter the number of the listening port on the RADIUS server. For example, 1812.
◦ Routing Instance	Select the routing instance to use to communicate with the RADIUS server.
◦ Authentication Key	Enter the authentication key for the RADIUS server.
◦ Add icon	Click to add the RADIUS server.

7. Click Save to add the 802.1X profile.

## Configure Multihomed Profiles

When you configure a physical port as a Layer 2 port, you can associate the port with a multihomed profile. For information on configuring a Layer 2 port, see [Configure a Layer 2 Port](#).

To configure a multihomed profile:

[https://docs.versa-networks.com/Secure\\_SD-LAN/Configuration\\_from\\_Director/Configure\\_SD-LAN\\_Using\\_Workflow\\_Templates](https://docs.versa-networks.com/Secure_SD-LAN/Configuration_from_Director/Configure_SD-LAN_Using_Workflow_Templates)

Updated: Wed, 23 Oct 2024 08:45:33 GMT

Copyright © 2024, Versa Networks, Inc.

1. In Director view:
  - a. Select the Workflows tab in the top menu bar.
  - b. Select Template > Templates in the horizontal menu bar. The Template screen displays.
  - c. Select the SD-LAN tab, and then select the Profiles tab. The Profiles screen displays, showing the profile types in the left menu bar.
2. Click Multihomed Profile in the left menu bar. The screen displays the multihomed profiles that are already configured.
3. Click the + Multihomed Profile icon. The Configure Multihomed Profile screen displays.
4. Enter information for the following fields:

Field	Description
Multihomed Profile Name	Enter a name for the multihomed profile.
Description	Enter a text description for the multihomed profile.
Ethernet Segment ID	Enter the Ethernet segment identifier.
Switch ID/System MAC Address	Enter the switch identifier or system MAC address.
Mode	Select the active mode: <ul style="list-style-type: none"> <li>◦ All-active—Use active-active mode. This is the default mode.</li> <li>◦ Single-active—Use active-standby mode.</li> </ul> <i>Default:</i> All-active
Organization	Select the name of the organization to which the profile applies.

5. Click Save.

---

## Configure Port Profiles

When you configure a physical port as a Layer 2 port, you associate the port with a port profile. For information on configuring a Layer 2 port, see [Configure a Layer 2 Port](#).

To configure the port profile:

1. In Director view:
  - a. Select the Workflows tab in the top menu bar.

- b. Select Template > Templates in the horizontal menu bar. The Template screen displays.
  - c. Select the SD-LAN tab, and then select the Profiles tab. The Profiles screen displays, showing the profile types in the left menu bar.
2. Click Port Profile in the left menu bar. The screen displays the port profiles that are already configured.
3. Click + Port Profile. The Configure Port Profile screen displays.
4. Enter information for the following fields.

Field	Description
Profile Name	Enter a name for the port profile.
Description	Enter a text description for the port profile.
Speed	<p>Select the data transfer speed, in megabits per second (Mbps):</p> <ul style="list-style-type: none"> <li>◦ 10</li> <li>◦ 100</li> <li>◦ 1000</li> <li>◦ 2500</li> <li>◦ 5000</li> <li>◦ 10000</li> <li>◦ Auto—Have the switch automatically determine the data transfer speed.</li> </ul> <p><i>Default: ;Auto</i></p>
Duplex	<p>Select how to negotiate between the device interface and switch interface:</p> <ul style="list-style-type: none"> <li>◦ Auto—Have the switch automatically determine the negotiation type.</li> <li>◦ Full—Transmit data in both directions on a signal carrier at the same time.</li> <li>◦ Half—Transmit data in one direction at a time.</li> </ul> <p><i>Default: Auto</i></p>
Interface Mode	<p>Select the mode for the interface:</p> <ul style="list-style-type: none"> <li>◦ Access—Have the interface accept untagged packets. The packets are assigned to the default VLAN.</li> <li>◦ Trunk—Have the interface accept tagged packets. The VLAN ID of the packets must be in the VLAN ID List field.</li> </ul>
Organization	Select the name of the organization to which the profile applies.

Field	Description
PoE	Select whether to use Power over Ethernet (PoE) on the port to provide power. <ul style="list-style-type: none"> <li>Off—Disable PoE on the port.</li> <li>On—Enable PoE on the port.</li> </ul>
LLDP	Select whether to use Link Layer Discovery Protocol (LLDP) on the port: <ul style="list-style-type: none"> <li>Off—Disable LLDP on the port.</li> <li>On—Enable LLDP on the port.</li> </ul>
802.1X Profile	Click the slider to associate the port with a 802.1X profile.
Virtual Switch	Select a virtual switch to associate with the port.
ACL In	Select an incoming ACL policy to associate with the port. For information on ACLs, see <a href="#">ACLs</a> .
VLAN	For an access mode interface, enter the identifier of the VLAN to which the port belongs.
VLAN ID List	For a trunk mode interface, identify the VLANs for which the interface can forward traffic. For example, 10-20, a list of VLAN IDs separated by spaces (for example, 10 20 30). Click the Tool icon to parameterize the VLAN IDs.
Native VLAN ID	For a trunk mode interface, identify the VLAN to associate with untagged traffic. In conjunction with trunk Layer 2 ports to allow an untagged packet to be treated as a specific VLAN ID.

5. Click Save.

## Configure a Switching Profile

When you configure a physical port as a Layer 2 port, you associate the port with a switching profile. For information on configuring a Layer 2 port, see [Configure a Layer 2 Port](#).

To configure the switching profile:

1. In the Profiles tab, select Port Profile in the left menu bar. The screen displays the port profiles that are already

configured.

2. Click + Port Profile. The Configure Switching Profile screen displays.

Configure Switching Profile

Switching Profile

Switching Profile Name \*

Organization \*

BPDU Guard

Spanning Tree Edge

Cancel Save

3. Enter information for the following fields:

Field	Description
Switching Profile Name	Enter a name for the profile.
Organization	Select the name of the organization to which the template applies.
BPDU Guard	Click to enable BPDU guard. BPDU guard disables an STP port if it receives a BPDU.
Spanning-Tree Edge	Click to configure ports that are connected to end nodes to be edge ports. Ports configured as spanning-tree edge ports directly transition to the forwarding state. Edge ports do not generate topology changes when the link state changes.

4. Click Save.

## Configure SD-LAN ACL Policies

An ACL policy consists of rules which define the conditions for matching packets and the actions to take when a match occurs. An ACL policy can have one or more rules, and the rules are evaluated in the order in which they are listed in the ACL policy until a match occurs. When a rule matches, the action associated with that rule is applied to the traffic, and no further rules in the ACL policy are evaluated.

When you configure a port profile, you can associate the profile with an ACL policy. For more information on configuring a port profile, see [Configure Port Profiles](#).

To configure SD-LAN ACL policies:

1. In Director view, select the Workflows tab in the top menu bar.
2. Select Template > Templates in the horizontal menu bar. The Template screen displays.
3. Select the SD-LAN tab, and then select the Policies tab.
4. On Policies tab, click + Add. The Configure ACL Policy screen displays.

Organization: Select Option

Infrastructure: Template Devices

SD-WAN: SD-LAN

Templates Profiles Policies

**Configure ACL Policy**  
Create an access list policy to control traffic allowed and blocked on a port.

**General**

Policy Name \*  
Policy Name

Description  
Description

Organization \*  
---Please Select---

**ACL Rules**

+ Add Edit Clone Delete Reorder

Layer2

Name	State	Rule Action	Source MAC Address	Destination MAC Address	Ether Type	Ether Type Value	Source IPv4 Address/Prefix	Destination IPv4 Address/Prefix	Source IPv6 Address/Prefix	Destination IPv6 Address/Prefix	Source Port
------	-------	-------------	--------------------	-------------------------	------------	------------------	----------------------------	---------------------------------	----------------------------	---------------------------------	-------------

Cancel Deploy

5. In the General group of fields, enter information for the following fields.

Field	Description
Policy Name	Enter a name for the ACL policy. The name can be up to 127 characters.
Description	Enter a text description for the ACL policy. The description can be up to 127 characters.
Organization	Enter the organization to which the ACL policy belongs.

6. In the ACL Rules menu, click + Add. The ACL Rule popup window displays.

ACL RULE
×

Layer2

Name \*

Input Name

Description

Input Description

Action

Allow

Block

Service

☐ Insert at Top

Source MAC Address ⓘ

Destination MAC Address ⓘ

Ether Type

---Please Select---

Ether Type Value

Source IPv4 Address/Prefix ⓘ

Destination IPv4 Address/Prefix ⓘ

Source IPv6 Address/Prefix ⓘ

Destination IPv6 Address/Prefix ⓘ

Source Port ⓘ

Destination Port ⓘ

IP Version

---Please Select---

DSCP

0..63

Protocol

ICMP

---Please Select---

ICMPv6

---Please Select---

Tunnel Type

---Please Select---

Forwarding Type

---Please Select---

Source SGT ID

---Please Select---

Destination SGT ID

IEEE 802.1p

Counter

☐ Packet
☐ Byte
☐ Policer Dropped Packet
☐ Policer Dropped Byte

cancel
Add

7. Enter information for the following fields.

Field	Description
Name	Enter a name for the ACL policy rule. The name can be up to 63 characters.
Description	Enter a text description for the ACL policy rule. The description can be up to 127 characters.
Action	<p>Click to select the action to take when a packet matches the rule:</p> <ul style="list-style-type: none"> <li>◦ Allow—Allow the packet.</li> <li>◦ Block—Deny the packet.</li> <li>◦ Service—Use a service, such as antivirus filtering, firewalls, or traffic engineering, to process the packet.</li> </ul>
Insert at Top	Click to place the rule at the beginning of all the policy's rules.
Source MAC Address	Enter the source MAC address to match.
Destination MAC Address	Enter the destination MAC address to match.
Ether Type	<p>Click to select the Ether Type to match:</p> <ul style="list-style-type: none"> <li>◦ ARP</li> <li>◦ IPv4</li> <li>◦ IPv6</li> </ul>
Ether Type Value	Enter a numeric value for the Ether Type to match.
Source IPv4 Address/Prefix	Enter the source IPv4 address or prefix to match.
Destination IPv4 Address/Prefix	Enter the destination IPv4 address or prefix to match.
Source IPv6 Address/Prefix	Enter the source IPv6 address or prefix to match.
Destination IPv6 Address/Prefix	Enter the source IPv6 address or prefix to match.
Source Port	Enter the source port number to match.
Destination Port	Enter the destination port number to match.



IP Version	<p>Select the IP version to match:</p> <ul style="list-style-type: none"> <li>◦ IPv4</li> <li>◦ IPv6</li> </ul>
DSCP	Enter the Differentiated Services Code Point value to match.
Protocol	Enter the protocol number to match.
ICMP	<p>Select the type of ICMP message to match:</p> <ul style="list-style-type: none"> <li>◦ Address Mask Reply</li> <li>◦ Address Mask Request</li> <li>◦ Destination Unreachable</li> <li>◦ Echo Reply</li> <li>◦ Echo Request</li> <li>◦ Information Reply</li> <li>◦ Information Request</li> <li>◦ Parameter Problem</li> <li>◦ Redirect</li> <li>◦ Router Advertisement</li> <li>◦ Router Selection</li> <li>◦ Source Quench</li> <li>◦ Time Exceeded</li> <li>◦ Timestamp Reply</li> <li>◦ Timestamp Request</li> <li>◦ Traceroute</li> </ul>
ICMPv6	<p>Select the type of ICMPv6 message to match:</p> <ul style="list-style-type: none"> <li>◦ Destination Unreachable</li> <li>◦ Echo Reply</li> <li>◦ Echo Request</li> <li>◦ Information Reply</li> <li>◦ Information Response</li> <li>◦ Multicast Listener Done</li> <li>◦ Multicast Listener Query</li> <li>◦ Multicast Listener Report</li> </ul>

	<ul style="list-style-type: none"> <li>◦ Neighbor Advertisement</li> <li>◦ Neighbor Solicitation</li> <li>◦ Packet Too Big</li> <li>◦ Parameter Problem</li> <li>◦ Redirect</li> <li>◦ Router Advertisement</li> <li>◦ Router Renumbering</li> <li>◦ Router Solicitation</li> <li>◦ Time Exceeded</li> </ul>
Tunnel Type	Click to select the tunnel type to match: <ul style="list-style-type: none"> <li>◦ None</li> <li>◦ VXLAN</li> </ul>
Forwarding Type	Click to select the forwarding type to match: <ul style="list-style-type: none"> <li>◦ Any</li> <li>◦ Layer 2 Switched</li> <li>◦ Layer 3 Routed</li> </ul>
Source SGT ID	Enter the source scalable group tag (SGT) identifier. You can use the source SGT to match the microsegment for a traffic flow.

8. Click Add to add the rule to the ACL policy.

---

## Software Release Information

Releases 22.1.3 and later support all content described in this article, except:

- In Release 22.1.4, minor changes have been made to the workflow GUI.

---

## Additional Information

[Configure Microsegmentation](#)

[Configure NPU Policy-Based Forwarding](#)

[Licensing Overview](#)