



Activate VOS Devices



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

You can activate Versa Operating System™ (VOS™) devices automatically and remotely using zero-touch provisioning (ZTP), and you can also activate a VOS device from the CLI on the device. For VOS devices in a virtual environment, you can use cloud-init functionality to automatically onboard them.

You can use the following methods to activate new VOS devices:

- Global ZTP—Global ZTP allows you to activate multiple VOS devices remotely. The VOS device activation process begins automatically when it powers on. The device uses the call-home feature to connect to a cloud-based staging server. The staging server validates the VOS device and redirects it to a staging Controller node, which completes the activation process. For global ZTP to work, you must provide Versa Networks with the serial numbers of all your VOS devices and the FQDN or IP address of the staging Controller node.
- URL-based ZTP—URL-based ZTP allows an onsite administrator to activate a VOS device. The administrator connects a laptop to the VOS device, or over a wireless network via a mobile phone for WiFi-enabled VOS devices, and clicks an email link to a staging Controller node, which completes the activation process.
- From the CLI—A site administrator can connect to the CLI on a VOS device and run a staging script that activates the device.

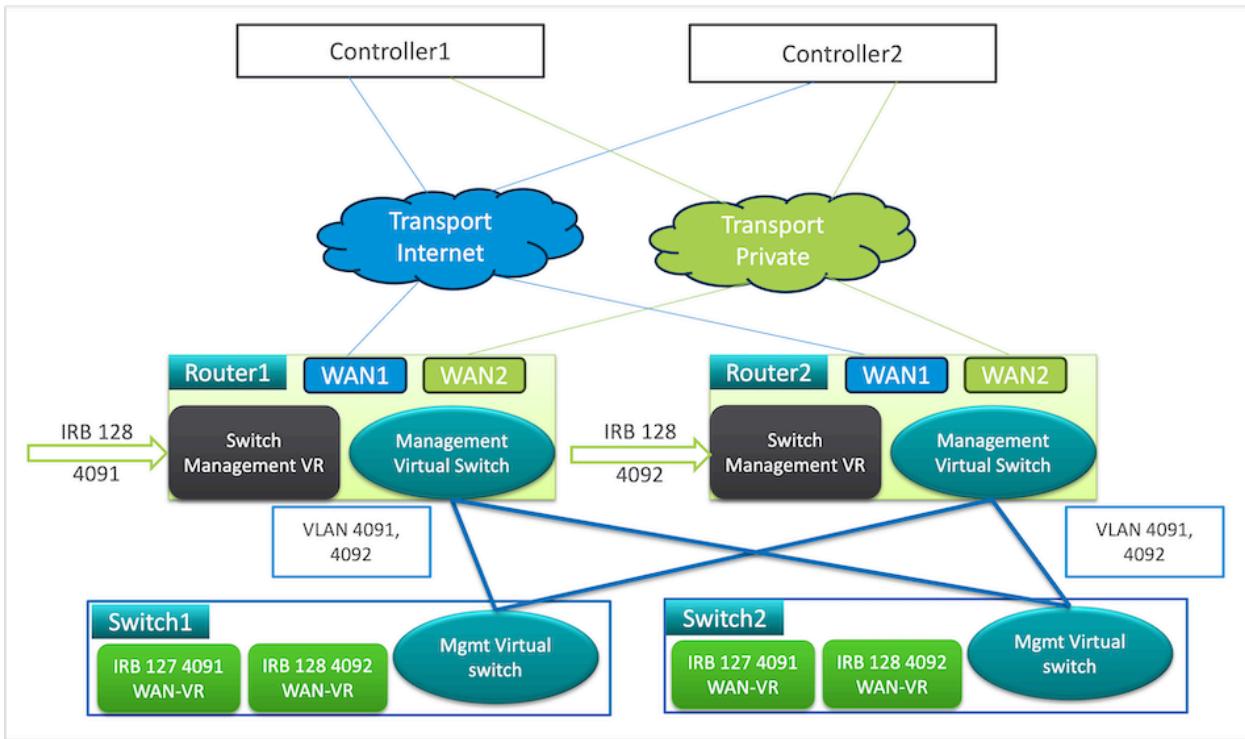
For Releases 22.1.3 and later, you can configure an SD-WAN edge device, such as a Versa Cloud Services Gateway (CSG) 750, to manage Layer 2 access and core switches.

Configure an SD-WAN Branch Edge Device to Manage Access and Core Switches

For Releases 22.1.3 and later.

You can use Workflow templates to configure an SD-WAN branch edge device, such as a Versa Cloud Services Gateway (CSG) 750, to manage access and core switches. You configure Layer 2 interfaces on the WAN edge device to provide the device management connection between the SD-LAN switches connected to it and the management Controller node in the SD-WAN network.

The following figure shows a single SD-WAN branch that has two SD-WAN edge devices (Router 1 and Router 2). The two branch devices are configured as an active-active pair. Together, they manage two SD-LAN (Switch 1 and Switch 2), and they provide connectivity between the switches and two Controller nodes (Controller 1 and Controller 2).



SD-WAN branch edge devices and the SD-LAN access and core switches use VLANs to communicate with each other in the branch. You must assign VLAN IDs to the Layer 2 interfaces on each SD-WAN branch edge device that provides connectivity to the access and core switches, and you must configure the same VLAN IDs to the virtual ports on the switches that connect to the SD-WAN branch edge devices. Note that if there is only one SD-WAN branch edge device in the branch, you need only one VLAN to connect the SD-WAN branch edge device to the switches.

To configure an SD-WAN device to manage switches, you use both the SD-WAN and SD-LAN Workflows. For SD-WAN, you configure Layer 2 interfaces, and you create a monitor on each WAN interface to use to manage the access switches. For the SD-LAN, you configure a device management interface on the switch to connect to the SD-WAN.

Configure Layer 2 Interfaces

To configure the Layer 2 interfaces on the SD-WAN branch edge device:

1. In Director view, select the Workflows tab in the top menu bar.
2. Select Template > Templates in the horizontal menu bar, and then select the SD-WAN tab. The screen displays the SD-WAN templates that are already configured.

The screenshot shows the VERSA Director View interface. The top navigation bar includes Director View, Appliance View, Template View, Monitor, Configuration, Workflows (which is highlighted with a red box), Administration, and Analytics. The top right corner shows the user is 'Administrator' with a notification count of 0. Below the navigation, there are dropdown menus for Organization (Provider), Infrastructure (Template), and Devices. A breadcrumb path at the top right indicates 'Workflows > Template > Templates'. The main content area is titled 'SD-WAN' and shows a table of templates. The table has columns for Name, Status, Last Modified Date, Last Modified By, and Actions. Two entries are listed: 'SDWAN-Branch3' (Deployed, 2023-12-22 01:37:55, Administrator) and 'tmp2' (Deployed, 2023-12-22 01:34:19, Administrator). A search bar and a 'Rows per page' dropdown are also present.

3. Click a template in the main pane, and then select Step 2, Interfaces.
4. Select the Interfaces tab. The following screen displays.

The screenshot shows the 'Configure Interfaces' step of the workflow for the 'SDWAN-Branch3' template. The top navigation and breadcrumb are identical to the previous screenshot. The main content area shows a progress bar with steps: BASIC (green checkmark), INTERFACES (highlighted with a red box), TUNNELS, ROUTING, SWITCHING, INBOUND NAT, MANAGEMENT SERVERS, and REVIEW. Below the progress bar is a title 'Configure Interfaces' and a note 'Template: SDWAN-Branch3'. The central part of the screen is a 'Device Port Configuration' section for a 'CSG750' device. It shows 'NIC Port' set to 'None' and a 'Configure' button. To the right is a summary of 'Virtual Ports': 0 WWAN, 0 WIFI, 0 IRB, with a 'Configure' button. Below this are two tabs: 'Without Port Mapping' and 'With Port Mapping'. A diagram of the CSG750 device shows its physical ports (Console Port, Management Port, LAN ports 0-5) and their corresponding virtual port mappings (vni-0/0 to vni-0/5). At the bottom left, there are tabs for 'WAN Interfaces(2)', 'L2 Interfaces(2)' (highlighted with a red box), and 'LAN Interfaces(1)'. A legend at the bottom right identifies interface types: Management (blue), WAN (orange), LAN (green), L2 (red), WAN/AN (yellow), Cross (purple), and PPPoE (pink). The bottom of the screen shows a table of configured interfaces and buttons for 'Cancel', 'Back', 'Save', 'Skip To Review', and 'Next'.

5. Click the L2 Interfaces subtab, which displays the Layer 2 interfaces that are already configured.
6. Click an interface name. The Edit Layer 2 Interface popup window displays.

https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Initial_Configuration

Updated: Wed, 23 Oct 2024 07:22:59 GMT

Copyright © 2024, Versa Networks, Inc.

Edit L2 Interface Port - 3

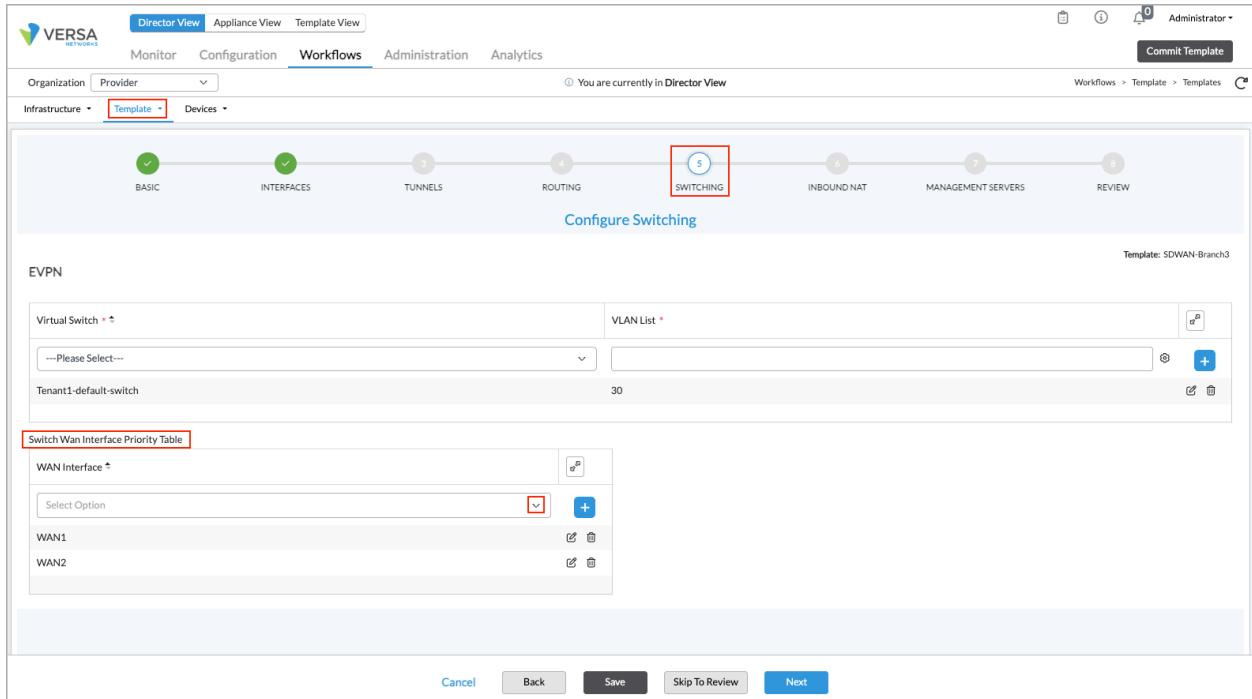
<input checked="" type="radio"/> Basic	<input type="radio"/> Advanced	<input checked="" type="checkbox"/> Switching Interface Management	<input checked="" type="checkbox"/> Advertise Default Route
Spanning Tree	Port *	Interface Name *	Organization *
MSTP	3	vni-0/3	Provider
VLANs:	Mode	Native VLAN ID *	
[VLANs]	Trunk	4091	
<input type="button" value="Done"/> <input type="button" value="Cancel"/>			

7. To create a LAN VR on the SD-WAN branch device, click Switching Interface Management. This LAN VR provides connectivity between the access switches and the Controller nodes.
8. To allow the access switches to be able to connect to other types of servers, such as DNS and DHCP servers, click Advertise Default Route so that the switches advertise a default route to the servers.
9. In the Native VLAN ID field, enter a VLAN ID. It is recommended that you use VLAN ID 4091 or 4092. If you choose a different VLAN ID, ensure that you use the same VLAN ID in the SD-LAN configuration. For more information, see [Configure the SD-LAN Devices Using Workflows](#), below.
10. Click Done.

Select the WAN Interfaces To Manage the Access Switches

To select the WAN interfaces to use to manage the access switches and assign a priority to each interface:

1. In Director view, select the Workflows tab in the top menu bar.
2. Select Template > Templates in the horizontal menu bar.
3. Select Template in the horizontal menu bar, and then select the SD-WAN tab.
4. Select Step 5, Switching.



5. In the Switch WAN Interface Priority Table, select the primary WAN interface to use to manage the switch, and then select the secondary WAN interface to use if the primary WAN interface fails. The priority is determined by the order in which you select the interfaces. In the screenshot above, WAN1 is listed first, so it is the primary WAN interface and WAN 2 is the secondary WAN interface. If WAN1 fails, WAN2 takes over the management of the switch.
6. Click Save.

Create a Monitor on the WAN Interfaces

To determine whether the WAN interfaces are up or down, and to provide the proper SLA connectivity from the access switches towards the Controller nodes, you configure a monitor on each of the WAN interfaces that you are using to manage the access switches.

To create a monitor on an WAN interface to use to manage the access switches:

1. In Director view, select the Workflows tab in the top menu bar.
2. Select Template > Templates in the horizontal menu bar.
3. Select Template in the horizontal menu bar, and then select the SD-WAN tab. The main pane displays the templates that are already configured.

The screenshot shows the VERSA Director View interface. The top navigation bar has tabs for Director View, Appliance View, and Template View, with Director View selected. Below the navigation is a header with Monitor, Configuration, Workflows (highlighted with a red box), Administration, and Analytics. A sub-header shows Organization (Provider selected), Infrastructure (Template selected), and Devices. To the right are buttons for Commit Template and a bell icon. The main content area is titled "Templates" and shows a table with columns: Name, Status, Last Modified Date, Last Modified By, and Actions. Two entries are listed: SDWAN-Branch3 (Deployed, 2023-12-22 01:37:55, Administrator) and tmp2 (Deployed, 2023-12-22 01:34:19, Administrator). Below the table are buttons for Rows per page (25) and Showing 1 - 2 of 2.

- Select the template that includes the WAN interfaces that you are using. The following screen displays.

The screenshot shows the VERSA Director View interface, specifically the "INTERFACES" step of a workflow. The top navigation and header are identical to the previous screenshot. The main content area shows a "Configure Interfaces" section with a "Device Port Configuration" panel for a CSG750 model with no NIC port. It also shows a device diagram with ports labeled vni-0/0 through vni-0/5, and a table of WAN interfaces (vni-0/0, vni-0/1, vni-0/2, vni-0/3, vni-0/4, vni-0/5) with their respective details. At the bottom, there are buttons for Cancel, Back, Save, Skip To Review, and Next.

- Select Step 2, Interfaces, select the WAN Interfaces tab, and then click a WAN (vni) interface. The Edit WAN Interface Port popup window displays.

https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Initial_Configuration

Updated: Wed, 23 Oct 2024 07:22:59 GMT

Copyright © 2024, Versa Networks, Inc.

6. In the Link Monitor field, enter the IP address of a remote device to monitor to ensure that the WAN interface is up and can reach the device in the cloud. If the WAN interface is down and cannot connect to the remote device, the next WAN interface listed in the [Switch WAN Interface Priority Table](#) becomes the primary WAN interface.
7. Click Done.
8. Repeat Steps 5 through 7 on the second WAN interface.
9. Click Done.

Configure the SD-LAN Devices Using Workflows

Access switches must connect to the edge devices in the WAN so that the access switches can reach the Controller node. A branch's WAN edge devices provide WAN connectivity between the access switches and the Controller node. This connectivity is required so that the Director node can provision the access switches using zero-touch provisioning (ZTP).

On the access switch, you configure a device management interface to connect to the WAN edge device. You configure the device management interface for WAN connectivity using the SD-LAN Workflows template.

Before you begin this procedure, you must have a template for the access switch. To create a template using SD-LAN workflow, see [Configure SD-LAN Using Workflow Templates](#).

To configure a device management interface for WAN connectivity:

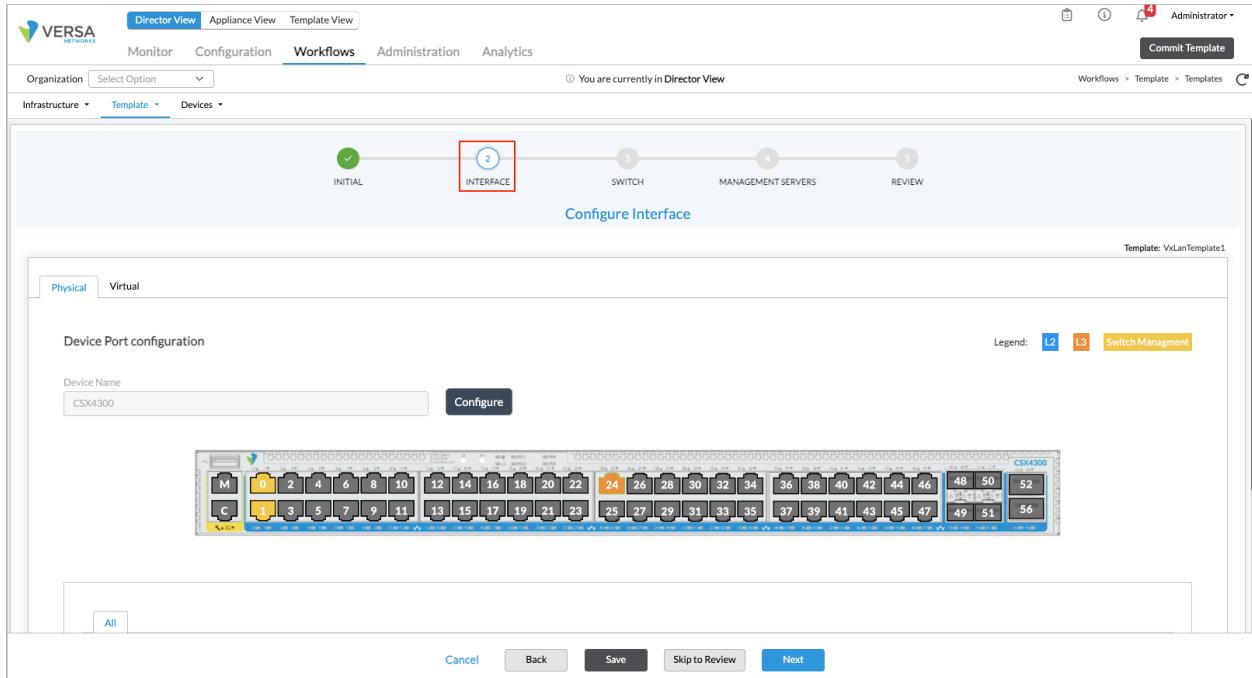
1. In Director view, select the Workflows tab.
2. Select Template > Templates in the horizontal menu bar. The Template screen displays.
3. Select the SD-LAN tab, and then select the Templates subtab. The screen displays the templates that are already configured.

The screenshot shows the Director View Workflows page. The top navigation bar includes Director View, Appliance View, Template View, Monitor, Configuration, Workflows (selected), Administration, and Analytics. The right side shows the user is an Administrator. The main content area is titled "Workflows > Template > Templates". It displays a table of templates under the "SD-LAN" category. The table columns include Name, Status, Organization, Description, Firewall Service, Analytics Enabled, Type, Device Type, Device Model, Subscription Solu..., and Sub. Two entries are listed: "4K1" (Deployed, Provider) and "TeeOne" (Deployed, Tenant). A search bar and pagination controls (Rows per page: 25, Showing 1 - 2 of 1) are also present.

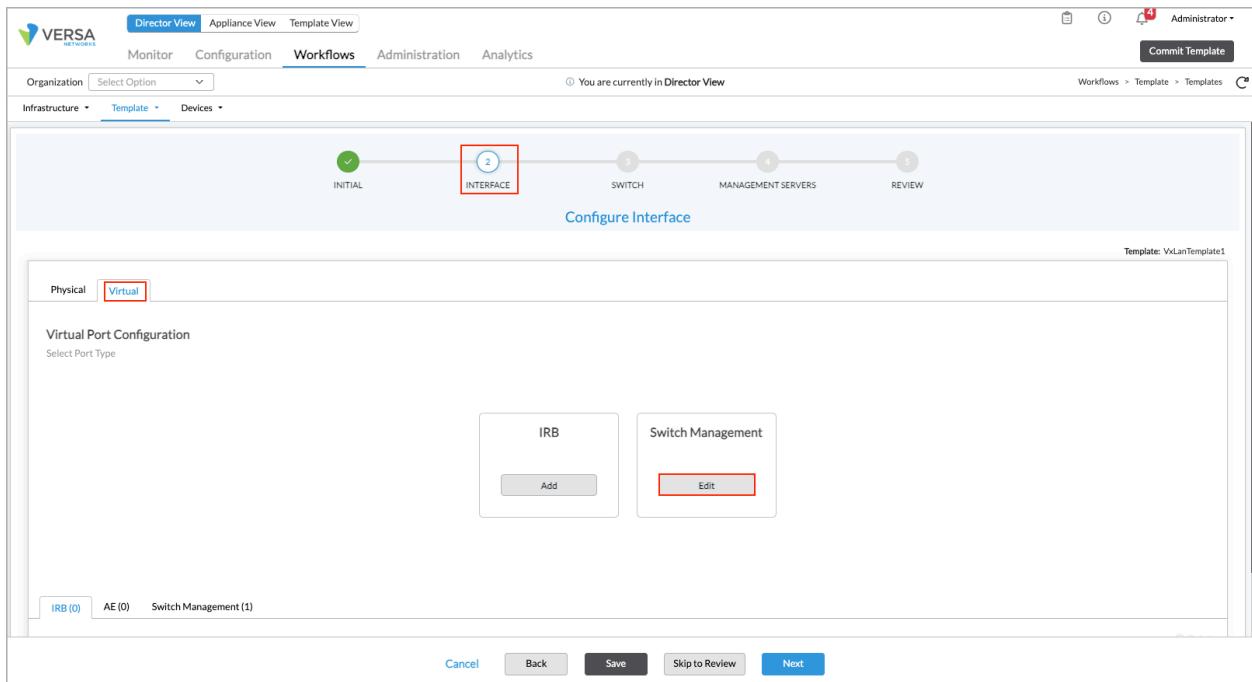
- Select the template for the access switch you want to configure. The Configure Initial screen displays with Step 1, Initial, selected by default.

The screenshot shows the Configure Initial screen. At the top, a progress bar indicates the steps: INITIAL (selected), INTERFACE, SWITCH, MANAGEMENT SERVERS, and REVIEW. The main area is titled "Configure Initial" and shows the "Basic" configuration section. It includes fields for Name (VxLanTemplate1), Type (sdwan-post-staging), Organization (Provider), and Analytics Cluster (Versa-Analytics). To the right, there is a "Subscription" panel with fields for Platform (CSX4300), Solution Tier (Essential), and License Period (1Yr). Below that is a "Solution Addon Tier" panel with the option "On-prem ZTNA". At the bottom, there are buttons for Cancel, Back, Save, Skip to Review, and Next (highlighted with a red box).

- Select Step 2, Interface, or click Next at the bottom of the screen. The Step 2, Interface screen displays with the Physical tab selected by default.



6. Select the Virtual tab in the horizontal menu bar. The Virtual Port Configuration screen displays.



7. If you have already configured a switch management interface on the switch, click Edit in the Switch Management field. Otherwise, click Add. The Virtual Port Configuration—Device Management popup window displays.

https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Initial_Configuration/
 Updated: Wed, 23 Oct 2024 07:22:59 GMT
 Copyright © 2024, Versa Networks, Inc.

Virtual Port Configuration - Switch Management

Management Interface

VLAN *	Port *	IPv4 Address	IPv6 Address	Transport Domain *	
<input type="text"/>	Select Option	---Please Select---	---Please Select---	Select Option	
4091	48	Dhcp		Internet,MPLS	
4092	49	Dhcp		Internet,MPLS	

cancel **Add**

8. Enter information for the following fields.

Field	Description
VLAN	Enter the VLAN ID to use to connect the WAN edge device. This must match the Native VLAN ID on the WAN edge device. It is recommended that you use VLAN ID 4091 or 4092.
Port	Select the port number.
IPv4 Address	Select the IPv4 address: <ul style="list-style-type: none"> ◦ DHCP—Use the Dynamic Host Configuration Protocol to dynamically assign the IP address to a Versa or a non-Versa WAN edge device. ◦ Static—Assign an IPv4 address. You can select this option if the switch is connecting to a non-Versa WAN edge device. Do not select it if the switch is connecting to a Versa WAN edge device.
Transport Domain	Select the transport domains for the switch to reach the Controller node. This field lists the transport domains associated with the same template. If the Controller nodes have two transport domains, select both. <ul style="list-style-type: none"> ◦ Internet ◦ MPLS
Add	Click to add the interface.

9. If the access switch connects to a second WAN edge device in the branch, repeat Step 8 to add a second device management interface. You must use a different VLAN ID for each WAN connection.

https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Initial_Configuration/...

Updated: Wed, 23 Oct 2024 07:22:59 GMT

Copyright © 2024, Versa Networks, Inc.

10. Click Add.

Use Global ZTP To Activate a VOS Device

Global ZTP activates a VOS device automatically when the device powers on. After the device powers on, it connects to the internet and obtains its WAN IP address, gateway, and name-server server information using DHCP. Then it uses the call-home feature to connect to a cloud-based staging server. The staging server validates the VOS device's owner (generally either an enterprise or a service provider) and redirects the device to the enterprise's or service provider's staging Controller node, which completes the activation process. The VOS device communicates with the staging Controller node over an IPsec IKE connection. For this initial connection, authentication is done using public key infrastructure (PKI). Each VOS device has a Versa signed certificate, and the private key is stored in the device's Trusted Platform Module (TPM) chip. After the initial staging process, you can replace this signed certificate with one that is signed by your certificate authority (CA).

For global ZTP to work, you must provide Versa Networks with the serial numbers of all your VOS devices and the FQDN or IP address of the staging Controller node. Versa Networks then creates an inventory entry for the VOS device, which is used by the Versa Networks prestaging server to validate the device when it powers on. If you know the FQDN or IP address of the post-staging Controller node, you can provide this information instead, to skip the provider prestaging step (Step 2 below).

Note that global ZTP is supported only in VOS releases that have not reached end of life (EOL) or end of support (EOS). For more information, see [Versa Networks Software Release Lifecycle and End-of-Life Policy](#).

Using global ZTP to activate a VOS device occurs in three steps, as illustrated in Figure 1:

1. **Versa Networks prestaging**—When the VOS device powers on, it connects to the Versa Networks staging Controller node. Based on the information in the inventory, the Versa Networks staging Controller node validates the VOS device and redirects it to the staging Controller node of the enterprise or service provider. The VOS device then reboots.
2. **Provider prestaging**—The enterprise or service provider claims the device, prompts for authentication using two-factor authentication, and redirects the VOS device to its staging Controller node. The VOS device then reboots.
3. **Provider staging and post-staging**—The enterprise or service provider authenticates the VOS devices using preshared keys (PSK) or public key infrastructure (PKI), and then the VOS device onboards customers (tenants). Then, IKE sessions are established between the provider and tenants. If you skipped the provider prestaging step, you claim the device here: you are prompted for authentication using two-factor authentication before tenants are onboarded. Note that the staging process takes only a few minutes, so rekeying the IKE and IPsec keys during this process is not necessary. However, after staging completes, IKE and IPsec generate new keys to use for the control and data path connections.

Figure 1: Global ZTP

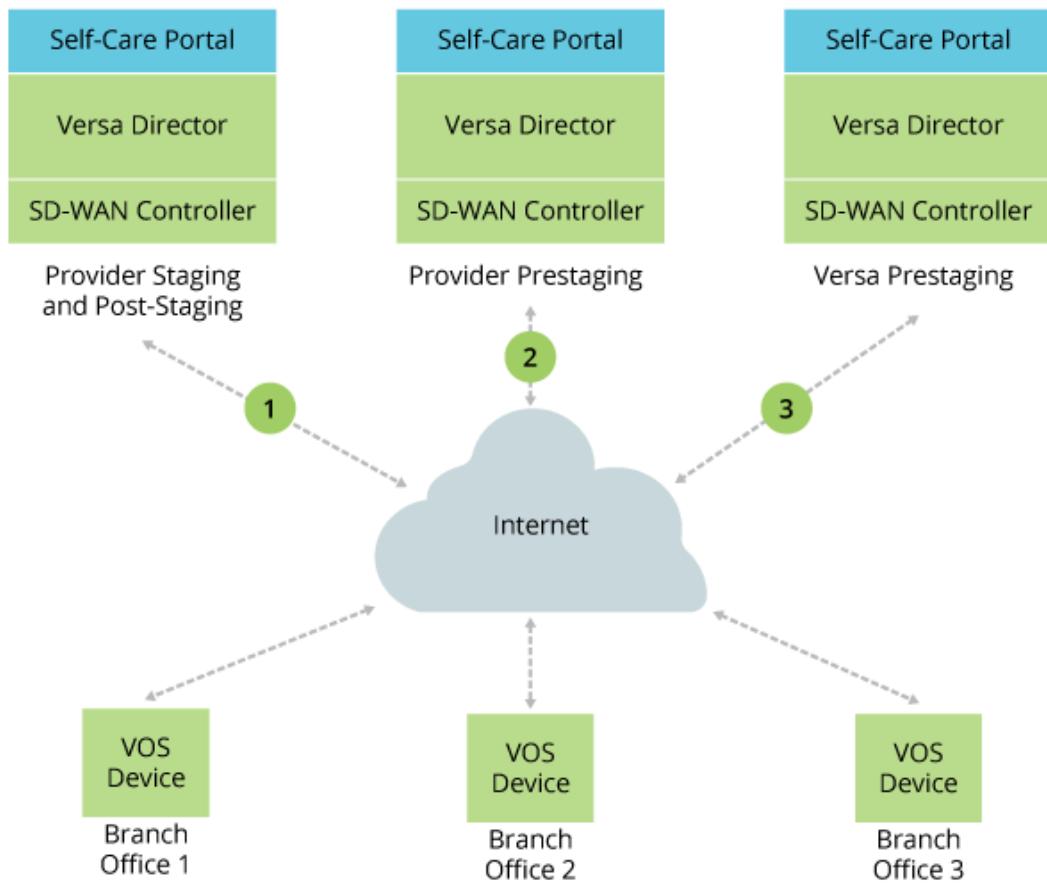
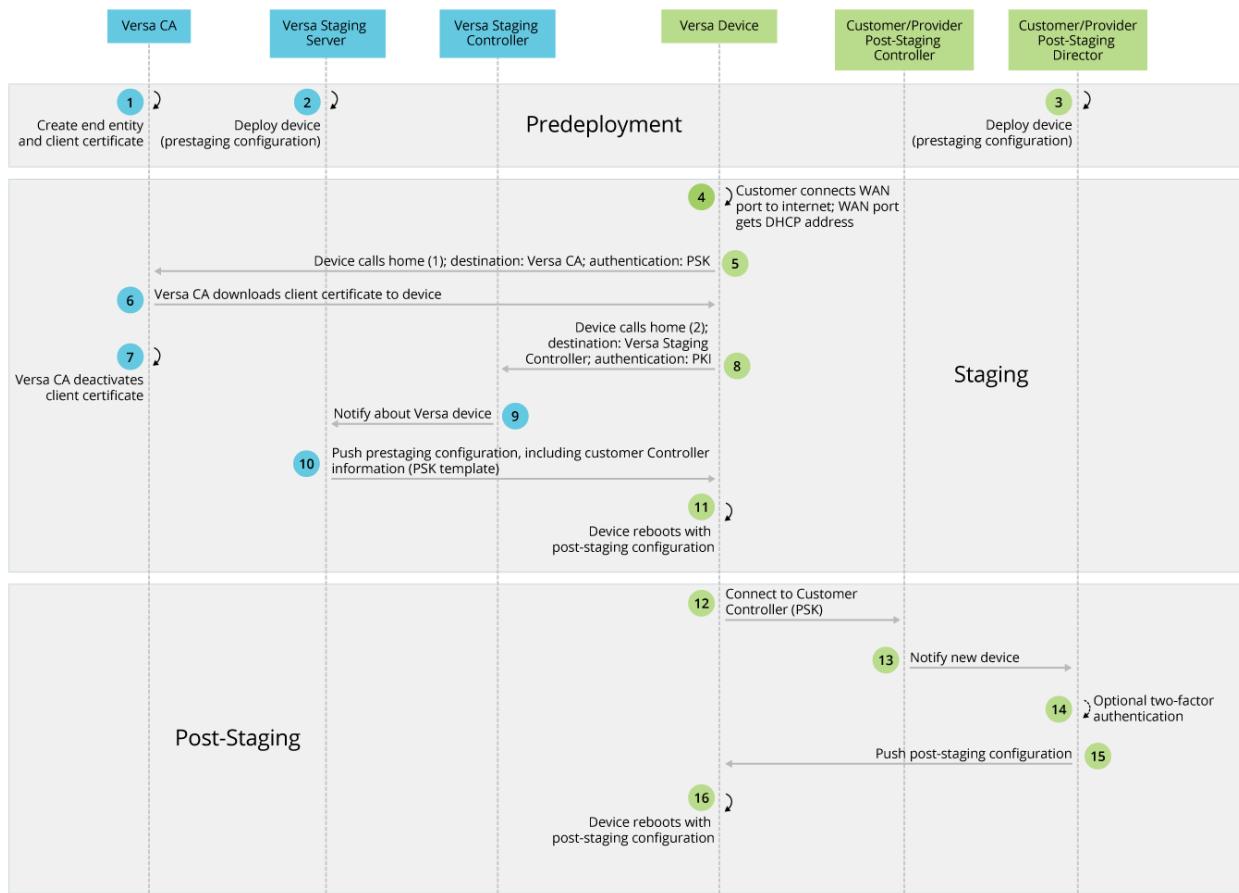


Figure 2 illustrates the device activation flow.

Figure 2: Versa Networks Device Activation Call Flow



To activate VOS devices using global ZTP:

1. Ensure that you have created a public Controller node for the VOS devices to connect to. After the VOS device boots, it connects to the Versa Networks cloud-hosted staging Controller node.
2. Log in to the cloud-hosted Versa Director.
3. Select the Configuration tab in the top menu bar.
4. Select Templates > Device Templates in the horizontal menu bar.
5. Select one of the following standard templates to use to associate bind data with the VOS devices you are activating:
 - Versa Prestaging—Select if the device uses another prestaging Controller node. This template includes bind data for the global tenant ID, preshared key authentication parameters for the prestaging Controller node, and the IP address of the prestaging Controller node.
 - Versa Staging—Select if the device uses a post-staging Controller node whose IP address you know. This template includes bind data for the global tenant ID, preshared key authentication parameters for the staging Controller node, and the IP address of the staging Controller node.
 - Versa Staging FQDN—Select if the device uses a post-staging Controller node whose FQDN you know. This template includes bind data for the global tenant ID, preshared key authentication parameters for the staging Controller node, and the FQDN of the staging Controller node.

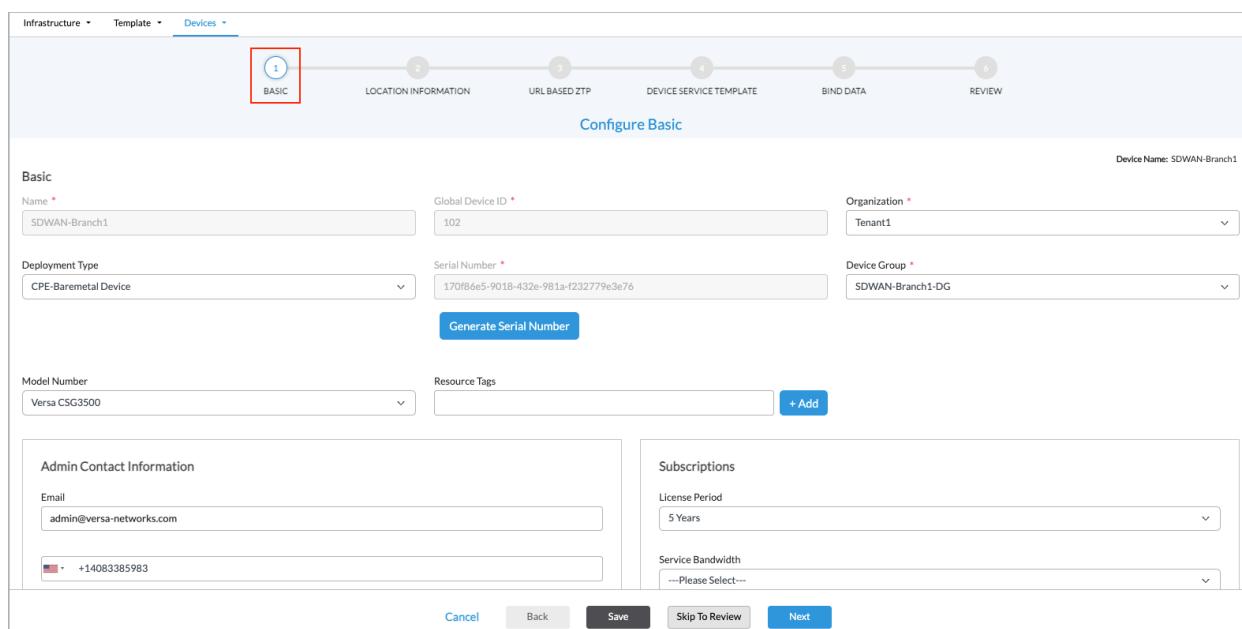
Note: For the Versa Prestaging, Versa Staging, and Versa Staging FQDN templates, you can customize them for a provider if desired. To do so, create a different device group and associate the template with it. You might want to do this if a provider does not use the default local authentication parameter for all its branches or if a provider uses different local authentication parameters at different branches.

- Versa Dummy Post-Staging—This is a placeholder template for devices that do not need to perform post-staging from this Director node with this Controller node.
6. Select Devices > Device Groups in the horizontal menu bar.
 7. Select one of the following standard device groups to use for the VOS devices you are activating:
 - Versa Prestaging DG—Select if the devices use another prestaging Controller node.
 - Versa Staging DG—Select if the devices use a post-staging Controller node whose IP address you know.
 - Versa Staging FQDN DG—Select if the devices use a post-staging Controller node whose FQDN you know.

To view the configuration of the device group, click the name of the group. The Edit Device Group popup window displays the configuration.

8. Select the Workflows tab in the top menu bar.
9. Click the  Add icon. The Add Device popup window displays.

For Releases 22.1.3 and later:



For Releases 21.2.3 and earlier:

Add Device

Basic **Location Information** **URL Based ZTP** **Device Service Template** **Bind Data**

Name*	Global Device ID*	Organization*
Deployment Type	Serial Number	Device Groups*
CPE-Baremetal Device	Generate Serial Number	+Device Group
Admin Contact Information		Subscription
Email	Phone Number	Service Bandwidth Aggregate Bandwidth
		Select options

Cancel **Save** **Continue**

10. Select the Basic tab and enter the serial number of the VOS device as the chassis ID, or click Generate Serial Number to automatically generate a serial number. Note that the device manufacturer provides Versa Networks with a list of serial numbers of the VOS devices that it ships to a provider.
11. Select the Bind Data tab and then select the User Input tab.

a. For Releases 22.1.3 and later:

Configure Bind Data

Device Name: SDWAN-Branch1

User Input Auto Generated

Post Staging Template (11) Service Template (0)

Template: SDWAN-Branch1

Interfaces 4

Variable	Data
LAN1_IPv4_staticaddress	172.16.103.2/24
WAN1_IPv4_staticaddress	192.168.11.101/24
WAN2_IPv4_staticaddress	192.168.112.101/24
WIN-LAN_IPv4_staticaddress	172.16.102.1/24

Cancel **Back** **Save** **Skip To Review** **Next**

1. Click the Post-Staging Template tab, then enter the IPv4 prefix of the interface to use.
2. Click the Virtual Routers tab, then IPv4 address of the default gateway to use to connect to the staging Controller node.



3. Select the Review tab, review and make any necessary edits, then click Deploy.
- b. For Releases 21.2.3 and earlier:
 1. Select the Bind Data tab and then select the User Input tab. Enter the IPv4 prefix of the interface and the IPv4 address of the default gateway to use to connect to the staging Controller node.
 2. Click Deploy.

Add Device

Basic	Location Information	Device Service Template	Bind Data	
User Input	Auto-Generated			
Staging Template - Staging				
Serial	Device Name	Interfaces with Mask	Default Gateway	
	test	vni-0_0_-_Unit_WAN1_IPv4_staticaddress	WAN1-Transport-VR_IPv4_vrHopAddress	
		IPv4 Address/Mask	IPv4 Address	
Post Staging Template - Single_Tenant_PostStaging				
Serial	Device Name	Default Gateway		
	test	WAN1-Transport-VR_IPv4_vrHopAddress	WAN2-Transport-VR_IPv4_vrHopAddress	WAN3-Transport-VR_IPv4_vrHopAddress
		IPv4 Address	IPv4 Address	IPv4 Address
Service Template Variable		Template : Single_Tenant_PostStaging	Device Group : DG-10	
Service Templates :		Tenant1-DataStore		
User Input	Auto-Generated			
<input type="checkbox"/> Serial		Device Name		
<input type="checkbox"/>		test		
Validate Template				
Back		Cancel	Save	Deploy

When the activation of the VOS device completes, the Tasks window reports the status.

Use URL-Based ZTP To Activate VOS Devices

With URL-based ZTP, a site administrator activates a VOS device after receiving an email that includes a link to the staging and post-staging Controller node. The administrator connects to the device using a laptop or mobile phone and

https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Initial_Configuration/

Updated: Wed, 23 Oct 2024 07:22:59 GMT

Copyright © 2024, Versa Networks, Inc.

clicks the link, and then the Controller node completes the device activation. On the Versa Director, you configure the staging Controller node and the contact information for the onsite installer. You can also access the URL from the Director node using REST API calls.

URL-based ZTP decouples a particular hardware device (that is, a particular chassis ID) from a branch location. This means that you can activate any hardware that is running an appropriate version of VOS software. The URL-based ZTP process also allows device activation to be performed using a post-staging Controller node, so you can skip the Versa Networks or provider prestaging process.

You configure URL-based ZTP for a device group.

Before you set up URL-based ZTP, note the following:

- ZTP uses ports 0 and 2 as the WAN ports and ports 1 and 3 as the LAN ports. For CSG700 Series appliances, ZTP uses ports 0 and 1 as the WAN ports and ports 2 and 3 as the LAN ports.
- To use URL-based ZTP on a bare-metal device, run the default configuration script.
- To use URL-based ZTP on a virtual machine (V), load the default-device.cfg file.
- By default, the VOS device runs a DHCP server on its LAN port.

Configure URL-Based ZTP

To create a device group that includes a URL-based ZTP configuration:

1. In Director view, select the Workflows tab in the top menu bar.
2. Select Devices > Devices in the left menu bar.
3. Click the  Add icon.

For Releases 22.1.3 and later, the following screen displays with Step 1, Basic, selected by default.

The screenshot shows the 'Configure Basic' step of a workflow. The 'BASIC' tab is selected. The form includes fields for Name, Global Device ID, Organization, Deployment Type, Serial Number, Model Number, Admin Contact Information, Resource Tags, Subscriptions, and License Period. A 'Device Group' dropdown is highlighted with a red box, showing 'Please Select---' and a '+ Add New' button.

For Releases 21.2.3 and earlier, the Add Device popup window displays.

The 'Add Device' popup window is shown. The 'Basic' tab is selected. The form includes fields for Name, Global Device ID, Organization, Deployment Type, Serial Number, Admin Contact Information (Email and Phone Number), and Device Groups. Buttons at the bottom are 'Cancel', 'Save', and 'Continue'.

- Select the Basic tab, and enter information for the following fields.

Field	Description
Name (Required)	Enter a name for the device. <i>Value:</i> Text string from 1 through 127 characters <i>Default:</i> None
Global Device ID (Required)	Enter the identifier of the device. This value is populated automatically with the next available number. You can change it to a different available

[https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Initial_Configuration/...](https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Initial_Configuration/)

Updated: Wed, 23 Oct 2024 07:22:59 GMT

Copyright © 2024, Versa Networks, Inc.

Field	Description
	value from 1 through 31.
Organization (Required)	Select the organization to which this device belongs.
Deployment Type (Required)	<p>Select the type of deployment:</p> <ul style="list-style-type: none"> ◦ CPE-Bare-metal Device ◦ CPE-Public Cloud
Serial Number	Enter the chassis number of the VOS device. This value must be unique. For Releases 22.1.3 and later, you can click Generate Serial Number to automatically generate a serial number.
Device Groups (Required)	Select the device group to which the device belongs. For the purposes of this procedure, click +Device Group (for Releases 21.2.3 and earlier; for Releases 22.1.3 and later, click + Add New in the Device Group field) and create a new device group, as described in the next step.
Admin Contact Information (Group of Fields)	Enter information about the administrator for the VOS device.
◦ Email	Enter the email address of the administrator associated with the device.
◦ Phone Number	Enter the phone number of the administrator associated with the device.

5. Click +Device Group.

For Release 22.1.3 and later, the Add Device Group screen displays:

Add Device Group

Name *

Description

Tags

Organization *

Enable Two Factor Auth CA In Data Center

Staging Template Post Staging Template

Contact Information

Email

Phone

URL Based ZTP

Pre Staging Staging Controller * VPN Profile * One Time Password

File Upload BW Limit (Kbps)

File Upload Timeout (Min)

[Post Staging Template Association \(0\)](#) [Devices \(0\)](#)

OK Cancel

For Releases 21.2.3 and earlier, the Create Device Group popup window displays:

Create Device Group

Name*	DeviceGroup-1												
Description	Device Group												
Tags													
Organization*	ServiceProvider												
	<input type="checkbox"/> Enable Two Factor Auth												
	<input type="checkbox"/> CA In Data Center												
Staging Template	Post Staging Template												
StagingTemplate	PoststagingTemplate1												
Contact Information	General												
Email	Phone												
(201) 555-5555	(201) 555-5555												
Post Staging Template Association(3) Devices(0) URL Based ZTP													
<table border="1"> <thead> <tr> <th>Tenant</th> <th>Category</th> <th>Template</th> </tr> </thead> <tbody> <tr> <td>ServiceProvider</td> <td>Main</td> <td>PoststagingTemplate1</td> </tr> <tr> <td>ServiceProvider</td> <td>DataStore</td> <td>ServiceProvider-DataStore</td> </tr> <tr> <td>ServiceCustomer1</td> <td>DataStore</td> <td>ServiceCustomer1-DataStore</td> </tr> </tbody> </table>		Tenant	Category	Template	ServiceProvider	Main	PoststagingTemplate1	ServiceProvider	DataStore	ServiceProvider-DataStore	ServiceCustomer1	DataStore	ServiceCustomer1-DataStore
Tenant	Category	Template											
ServiceProvider	Main	PoststagingTemplate1											
ServiceProvider	DataStore	ServiceProvider-DataStore											
ServiceCustomer1	DataStore	ServiceCustomer1-DataStore											
<input type="button" value="OK"/> <input type="button" value="Cancel"/>													

Devices(0) **URL Based ZTP**

<input checked="" type="checkbox"/> URL Based ZTP	<input type="radio"/> Pre Staging	<input checked="" type="radio"/> Staging	Controller	VPN Profile
	<input type="checkbox"/> One Time Password		Controller11	--Select--
<input type="button" value="OK"/> <input type="button" value="Cancel"/>				

6. Select URL-Based ZTP and configure the parameters to enable URL-based ZTP. Enter information for the following fields.

Field	Description
URL-Based ZTP	Click to enable URL-based ZTP.
Prestaging	Click to enable URL-based ZTP during the prestaging state.
Staging	Click to enable URL-based ZTP during the staging state.

Field	Description
Controller	<p>Select the Controller node to use as the staging and post-staging Controller node to activate the VOS devices. A link to this Controller node is sent in email to the site installer.</p> <p>If you upgraded the Director and Controller nodes that were present before the upgrade and they are not listed, check the Controller node status:</p> <ol style="list-style-type: none"> 1. Log in to the Director shell, and enter the following commands: <pre>Administrator@Director> cli Administrator@Director> config Administrator@Director% set provider appliance appliance controller-uuid staging-controller</pre> 2. If the staging-controller value is false for a Controller node that should display in the URL ZTP Controller node list, set the value to true: <pre>Administrator@Director% set show provider appliances appliance controller-uuid staging-controller true</pre> 3. Repeat Step 2 for each Controller node that should display in the list. 4. Commit the changes: <pre>Administrator@Director% commit</pre> <p>Note: The Controller node either must belong to an organization to which the tenant user has access or must be associated with at least one organization that belongs to the device group's organization or parent organization.</p>
VPN Profile	<p>Select the IPsec VPN tunnel to use to reach the staging and post-staging Controller node. In the VPN profile, you define whether the IKE connection between the Controller node and the VOS device uses preshared keys (PSK) or public key infrastructure (PKI).</p>

Field	Description
	<p>If no VPN profile displays in the list for the selected Controller node, do the following:</p> <ol style="list-style-type: none"> 1. Log in to the Director shell, and enter the following commands: <pre>Administrator@Director> cli Administrator@Director> config</pre> 2. Display the provider organization of the selected Controller node: <pre>Administrator@Director% show devices device SDWAN-Controller1 config system sd-wan site provider-org</pre> 3. Based on the name of the Controller organization displayed in the output of Step 2, display a list all VPN profiles: <pre>Administrator@Director% show devices device controller-name SDWAN-Controller1 config orgs org-services controller-org-from- previous-step ipsec vpn-profile vpn- type controller-staging-sdwan</pre> 4. If the output of the show devices command in Step 3 does not display any VPN profiles, contact Versa Networks Customer Support.
One-Time Password	Select to create a password to use only during the URL-based ZTP process.

7. Click OK.

Edit ZTP URL Parameters

After you have deployed a VOS device, you can edit the parameters related to URL-based ZTP:

1. In Director view, select the Administrator tab in the top menu bar.
2. Select Inventory > Hardware in the left menu bar.
3. Select a VOS device from the main pane. The Edit Hardware popup window displays.

For Releases 22.1.3 and later:

Edit Hardware

Basic Location Information **URL Based ZTP**

Authentication Info

PSK PKI

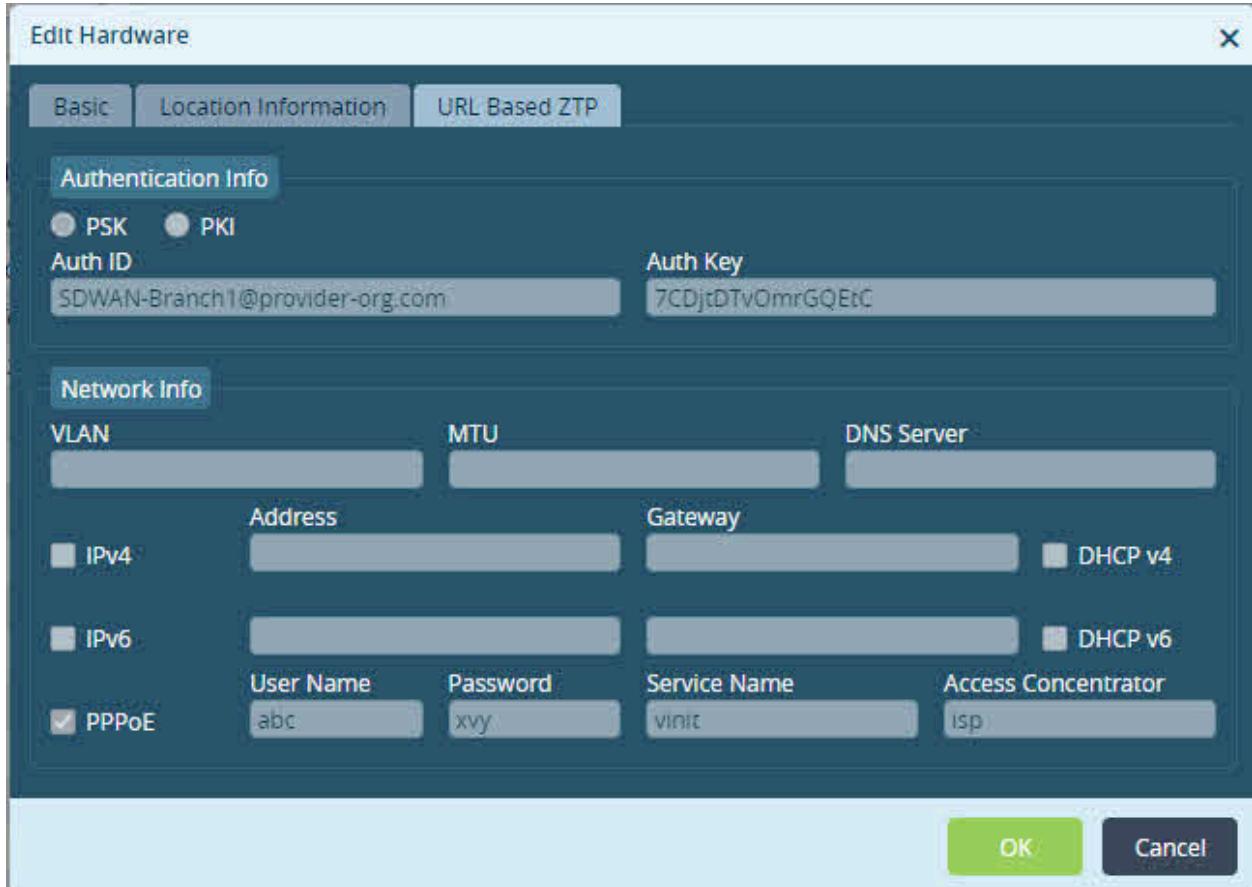
Auth ID	Auth Key
SDWAN-Branch1@provider-org.com	7CDjtDTvOmrGQEtc

Network Info

VLAN	MTU	DNS Server	<input type="checkbox"/> IPv4
Address	Gateway	<input type="checkbox"/> DHCP v4	<input type="checkbox"/> IPv6
		<input type="checkbox"/> DHCP v6	<input checked="" type="checkbox"/> PPPoE
Username	Password	Service Name	Access Concentrator
abc	xvy	vinit	isp
<input type="checkbox"/> DSL	Username	Password	Multiplexing Type
VCI	VPI	VLAN Tag	--Select--

Buttons: OK (Blue) | Cancel (Dark Blue)

For Releases 21.2.3 and earlier:



4. Select the URL-Based TCP tab, and make the desired changes.
5. Click OK.

Access the ZTP URL To Activate a VOS Device

To access the URL to use for ZTP, use one of the following options:

- Connect from the AMQP server that you configured on Versa Director. Note that after you onboard and deploy the VOS device, the URL is posted to the AMQP server.
- Query the URL using the following RESTful API call, where x.x.x.x is the IP address of your Versa Director. For example:

`http://x.x.x.x:9182/vnms/sdwan/device-url-mappings/device-url-mapping/Branch2`

- Copy the URL from the Versa Director Administration > Inventory > Hardware window. On this window, select a VOS device and click the URL-Based ZTP Info icon:

Screenshot of the Versa Networks Director View interface showing the Administration tab selected. The left sidebar is expanded to show the Inventory section, with the Hardware category selected. A red box highlights the "Hardware" link. The main content area displays a table titled "Device Info" listing various network devices. A red box highlights the "SDWAN-Branch2" row, which has a checked checkbox in its first column. The table includes columns for Device Name, Serial Number, RMA Serial Number, Hardware Serial Number, Site Name, Bandwidth (Mbps), Site ID, Location, Longitude, Latitude, Organizations, and Status.

Device Info						Site ID	Location				Organizations	Status
	Device Name	Serial Number	RMA Serial Number	Hardware Serial Number	Site Name	Bandwidth (Mbps)	Location	Longitude	Latitude			
<input type="checkbox"/>	access-switch-4500	463054NPE2326015			access-switch-4500	50000	101	2550 Great America...	-121.9736...	37.414756	Tenant1	shipped
<input type="checkbox"/>	Agg-8300	9803ae4-15fc-4a47-b...			Agg-8300	50000	104	2550 Great America W...	0.000000	0.000000	Tenant1	shipped
<input type="checkbox"/>	Branch3-750	29333fd4-3fb7-4a95...			Branch3-750	1000	105	2550 Great America W...	-121.9736...	37.414756	Tenant1	shipped
<input type="checkbox"/>	SDLAN-B151	a225beb5-235f-4fc-b...		463054NPE2326015	SDLAN-B151	50000	107	2550 Great America W...	-121.9736...	37.414756	Tenant1	claimed
<input type="checkbox"/>	SDLAN-B252	2c9fb685-d371-4222...		463054PE2218116	SDLAN-B252	20000	108	2550 Great America W...	-121.9736...	37.414756	Tenant1	claimed
<input type="checkbox"/>	SDLAN-B353	732656X2220499		732656X2220499	SDLAN-B353	50000	109	2550 Great America W...	-121.9736...	37.414756	Tenant1	claimed
<input type="checkbox"/>	SDLAN-B454	46b2fddc-dcb8-44e5-8...		463054NPE2224023	SDLAN-B454	20000	111	2550 Great America W...	-121.9736...	37.414756	Tenant1	claimed
<input type="checkbox"/>	SDWAN-Branch1	170f86e5-9018-432e-...		AACAA2329004	SDWAN-Branch1		102	2550 Great America W...	-121.9736...	37.414756	Tenant1	claimed
<input checked="" type="checkbox"/>	SDWAN-Branch2	032668d1-15c2-4a16-...		AACAA2326008	SDWAN-Branch2	10000	103	2550 Great America W...	-121.9736...	37.414756	Tenant1	claimed
<input type="checkbox"/>	Switch-4300	144955fc-e9fe-4942-b...		Switch-4300			106	2550 Great America W...	-121.9736...	37.414756	Tenant1	shipped

Activate a VOS Device

To activate a VOS device using URL-based ZTP:

1. Ensure that ICMP is allowed on the VOS device's WAN ports. ICMP is required because, as part of the activation process, the VOS device sends ICMP probes to the Controller node's WAN port to ensure network reachability.
2. If WiFi is enabled on the VOS device, connect to the device from an iPhone or Android device, and skip to Step 4.
3. Otherwise, connect a laptop to the LAN port 2 on the VOS device.
4. Connect the device to the internet:
 - To connect an SD-WAN device, connect WAN port labeled 0 to the internet.



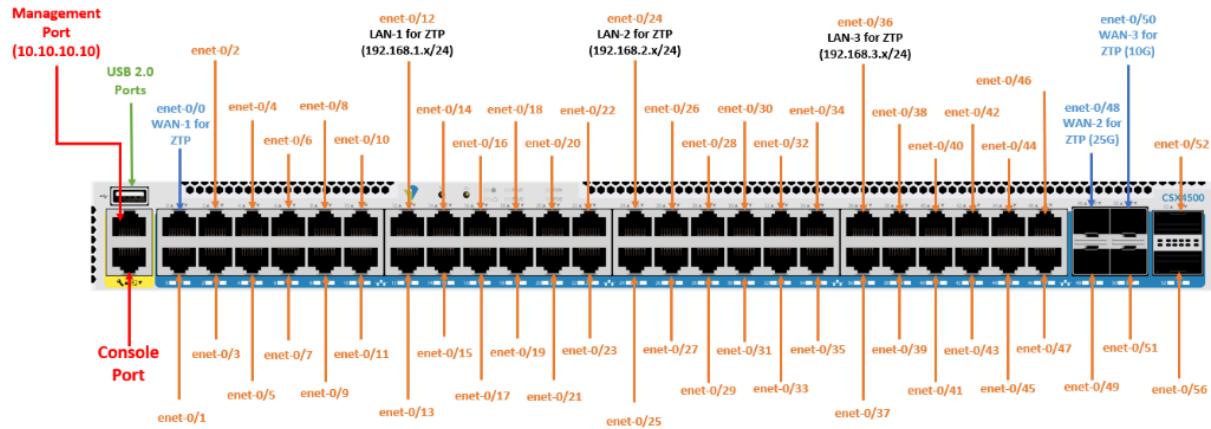
https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Initial_Configuration/...

Updated: Wed, 23 Oct 2024 07:22:59 GMT

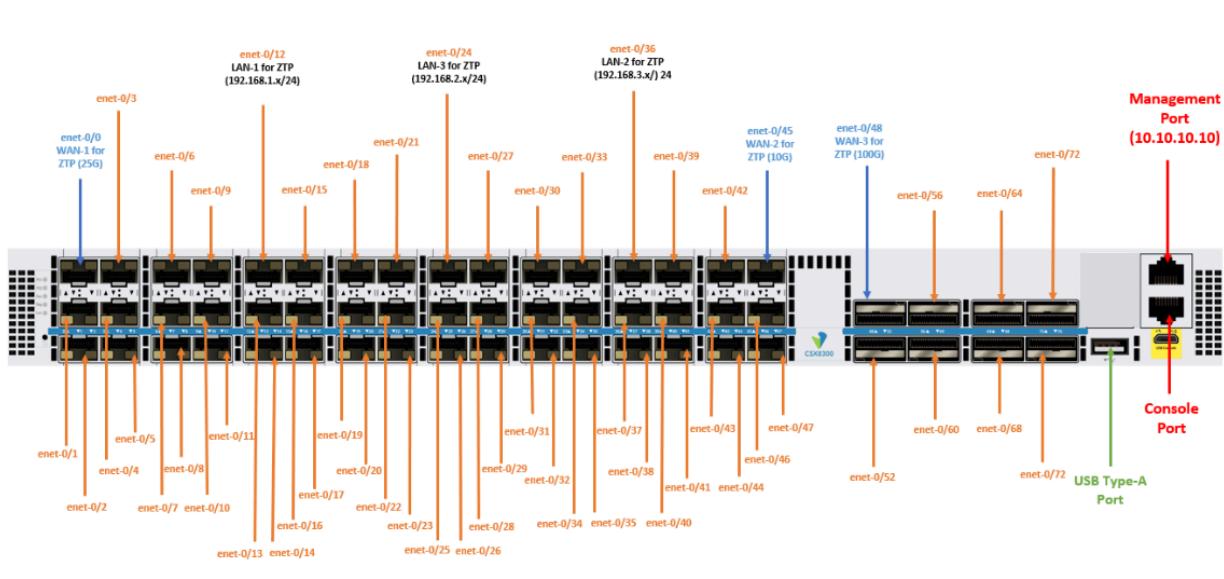
Copyright © 2024, Versa Networks, Inc.

- To connect an SD-LAN device, use the ports indicated for your switch:

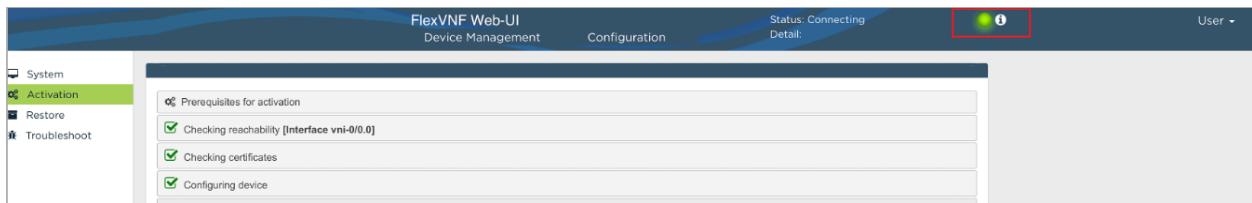
CSX4300 and CSX4500 switches—The default WAN port for ZTP is enet-0/0 WAN-1 (1G). For multigig speeds, you can select enet-0/48 WAN-2 (25G), or enet-0/50 WAN-3 (10G), as shown below.



CSX8300 switches—The default WAN port for ZTP is enet-0/0 WAN-1 (25G). You can also select enet-0/45 WAN-2 (10G) or enet-0/48 WAN-3 (100G), as shown below.



- Click the link in the device activation email that you received. The VOS (FlexVNF) Web-UI screen displays.
- Check the status light in the top menu bar.



If the light is green, proceed to the next step.

If the light is amber, the device configuration was changed and the device no longer has the factory-default settings. As a result, the device might not have been onboarded properly using URL ZTP. To resolve this issue, connect to the device console and issue the following command from the CLI. This command resets the device to the factory-default configuration so that you can use URL-based ZTP and global ZTP.

- ```
request system load-default
```
7. In the Device Management tab, click Start Activation to start the ZTP activation of the VOS device. The VOS device then does the following:
    - a. Check for internet connectivity.
    - b. Fetch valid certificates, and if PKI authentication is selected, check the certificates
    - c. Connect to the configured staging Controller node and receive its configuration.



8. If two-factor authentication is enabled, claim the VOS device:
  - a. When the device boots for the first time, click Claim Device.

## Your device has come up

Device Name      Site-1  
Device ID        JAB12345  
Description

Click on 'Claim Device' to begin auto registration.

Claim Device

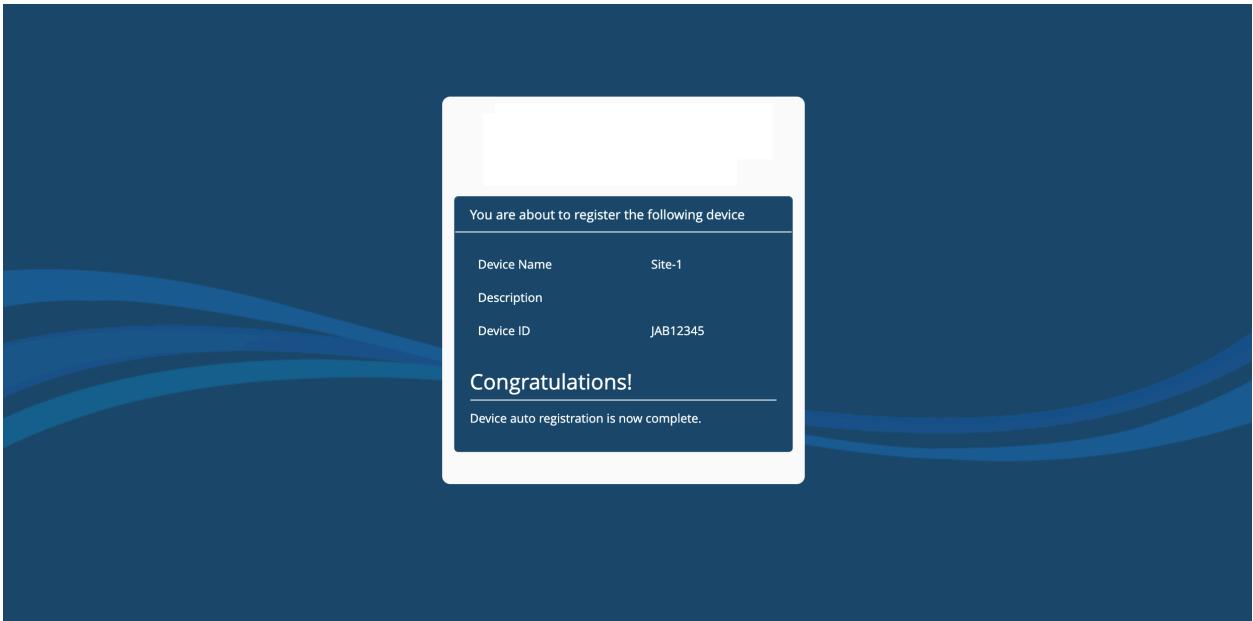
- b. After you claim the device, you receive the device registration code either in an email or as a text message to a mobile phone, depending on the configuration:

## Device Registration Information

Device Name      Site-1  
Device ID        JAB12345  
Registration Code 955883

Registration Code will expire in 15 minutes (2020-04-26 01:33:40 UTC).

- c. Enter the registration code.



- When the ZTP process completes, the VOS device reboots.

```
admin@prague-cli> show interfaces brief
NAME MAC OPER ADMIN TENANT VRF IP
-----+-----+-----+-----+-----+-----+-----+
eth-0/0 00:90:0b:4a:7c:a0 up up 0 global 10.192.74.100/16
tv1-0/0 n/a up up - - -
tv1-0/0.0 n/a up up 1 Versa-Provider-Control-VR
tv1-0/1 n/a up up - - -
tv1-0/1.0 n/a up up 1 Versa-Provider-Control-VR
vni-0/0 00:90:0b:4a:7c:a1 up up - - -
vni-0/0.0 00:90:0b:4a:7c:a1 up up 1 WAN1-Transport-VR 10.113.1.1/24
vni-0/0.1 00:90:0b:4a:7c:a1 up up 1 WAN1-Transport-VR
vni-0/1 00:90:0b:4a:7c:a2 up up - - -
vni-0/1.0 00:90:0b:4a:7c:a2 up up 1 global 192.168.0.1/24
vni-0/2 00:90:0b:4a:7c:a3 down down - - -
vni-0/3 00:90:0b:4a:7c:a4 down down - - -
vni-0/4 00:90:0b:4a:7c:a5 down down - - -

[ok][2017-01-20 01:15:24]
admin@prague-cli>
System message at 2017-01-20 01:15:31...
Commit performed by admin via http using rest.
admin@prague-cli>
System message at 2017-01-20 01:15:38...
Commit performed by admin via http using rest.
admin@prague-cli>
System message at 2017-01-20 01:15:46...
Commit performed by admin via http using rest.
admin@prague-cli>
System message at 2017-01-20 01:16:27...
Commit performed by admin via ssh using netconf.
admin@prague-cli>
System message at 2017-01-20 01:16:30...
Commit performed by admin via console using cli.
```

- On the Director node, verify that the VOS device has been activated.
- If desired, configure static IP addresses and DNS servers in the VOS Web-UI screen. To do this, select the Configuration tab:

| Name       | MAC               | OPER | ADMIN | TENANT | VRF                   | IP                                                       | Type             |
|------------|-------------------|------|-------|--------|-----------------------|----------------------------------------------------------|------------------|
| eth-0/0    | 00:0c:29:e9:bd:b2 | up   | up    | 0      | global                | 10.40.195.208/16<br>2001:192:167:1:20c:29ff:fee9:bdb2/64 | Management - eth |
| ptvi8      | n/a               | up   | up    | 2      | Customer-1-Control-VR | 10.4.64.1/32                                             | Tunnel - ptvi8   |
| tvi-0/16   | n/a               | up   | up    | -      | -                     |                                                          | Tunnel - tvi     |
| tvi-0/16.0 | n/a               | up   | up    | 2      | Customer-1-Control-VR | 10.4.0.112/32                                            | Tunnel - tvi     |
| tvi-0/17   | n/a               | up   | up    | -      | -                     |                                                          | Tunnel - tvi     |
| tvi-0/17.0 | n/a               | up   | up    | 2      | Customer-1-Control-VR | 10.4.64.112/32                                           | Tunnel - tvi     |
| vni-0/0    | 00:0c:29:e9:bd:a8 | up   | up    | -      | -                     |                                                          | Ethernet - vni   |
| vni-0/0.0  | 00:0c:29:e9:bd:a8 | up   | up    | 2      | Internet-Transport-VR | 10.40.195.56/16                                          | Ethernet - vni   |

## Debug URL-Based ZTP

If you are a site administrator, follow these steps to debug URL-based ZTP:

1. Ensure that Port 1 is configured as the eth0 interface.
2. Ensure that a WAN IP address is configured on Port 2.
3. Ensure that the default gateway in the global routing instance is reachable through the WAN port.
4. On Port 3, the LAN IP is received via DHCP. Use <http://192.168.1.1:80> to access the device or directly use the generated URL.
5. Paste the URL in the browser to start the bootstrap process.

You can monitor the progress on Versa Director.

## Prepare for a Demo of URL-Based ZTP

If you are showing a demo of URL-based ZTP, follow these steps to set up the VOS device:

1. Install a new .bin file on the VOS device. Doing this is not required if you are performing the demo on a newly shipped device.
2. Install the factory-default configuration. To do this, run the /opt/versa/scripts/versadevice-factoryreset.sh script on the VOS device. Doing this allows the laptop that you connect to the VOS device to access the internet. Doing this is not required if you are performing the demo on a newly shipped device.
3. Check that the interfaces on the VOS device are operational:

```
admin connected from 10.0.0.27 using ssh on versa-flexvnf
admin@versa-flexvnf-cli> show interfaces brief
NAME MAC OPER ADMIN TENANT VRF IP

eth-0/0 00:90:0b:43:10:42 up up 0 global
vni-0/0 00:90:0b:43:10:43 up up - -
vni-0/0.0 00:90:0b:43:10:43 up up 1 global 10.0.0.23/16
vni-0/1 00:90:0b:43:10:44 up up - -
vni-0/1.0 00:90:0b:43:10:44 up up 1 global 192.168.1.1/24
[ok][2016-08-19 14:50:55]
```

## Use the CLI To Activate VOS Devices

To automatically activate a VOS device from the CLI, run the /opt/versa/scripts/staging.py script.

The following is an example of the options you specify when running the script on an SD-WAN device:

```
admin@VNF:/ $ sudo /opt/versa/scripts/staging.py -I SDWAN-branch@nms-org.com \
-r controller-staging@nms-org.com -c 10.10.10.10 -w 0 -s 10.10.10.20/24 -g 10.10.10.10
```

This example includes the following options:

- Name of the VOS device to activate (`-I SDWAN-branch@nms-org.com`)
- Name of the Controller node to authenticate the VOS device (`-r controller-staging@nms-org.com`)
- IP address of the Controller node (`-c 10.10.10.10`)
- WAN port to use to reach the internet, here, port 0 (`-w 0`)
- Static route to configure (`-s 10.10.10.20/24`)
- Gateway IP address (`-g 10.10.10.10`)

Specify the `-h` option to list all available options for this script:

```
admin@VNF:/ $ sudo /opt/versa/scripts/staging.py -h
[sudo] password for admin:
usage: staging.py [-h] [-l LOCAL_ID] [-r REMOTE_ID] [-c CONTROLLER] [-d] [-w {0,1,2,3}] [-v VLAN]
[-s STATIC] [-g GATEWAY]
Set up branch staging configuration
Optional arguments:
-h, --help Show this help message and exit
-l LOCAL_ID, --local-id LOCAL_ID Local ID string/email
-r REMOTE_ID, --remote-id REMOTE_ID Remote ID string/email
-n SERIAL_NUMBER, --serial-number SERIAL_NUMBER Serial number
-c CONTROLLER, --controller CONTROLLER Controller IPv4 address/FQDN
-c6 CONTROLLER6, --controller CONTROLLER6 Controller IPv6 address/FQDN
-t {prestaging,staging}, --staging {prestaging,staging} Staging type (default=staging)
-wpt {vni,enet}, --wan-port-type {vni,enet} WAN port type [vni | enet] (default=vni)
-w {0,1,2,3}, --wan-port {0,1,2,3} WAN port number
-v VLAN, --vlan VLAN VLAN ID
-s STATIC, --static STATIC Static IPv4/mask for WAN link
-s6 STATIC6, --static6 STATIC6 Static IPv6/mask for WAN link
-g GATEWAY, --gateway GATEWAY Default gateway IP address
-g6 GATEWAY6, --gateway6 GATEWAY6 Default gateway IPv6 address
-d, --dhcp Use DHCP for WAN link
-d6, --dhcp6 Use DHCPv6 for WAN link
-a, --slaac Use SLAAC for IPv6 WAN link
-gt GLOBAL_TENANT_ID, --global-tenant-id GLOBAL_TENANT_ID Global Tenant ID
-lk LOCAL_PSK, --local-psk LOCAL_PSK IPsec Key (default=1234)
-rk REMOTE_PSK, --remote-psk REMOTE_PSK IPsec Key (default=1234)
-lb LOOPBACK, --loopback LOOPBACK IPv4/mask for loopback link; used for staging
-dsl, --dsl_intf Use DSL interface for staging
-vci DSL_VCI, --dsl_vci DSL_VCI VCI value, mandatory for DSL
```

```

-vpi DSL_VPI, --dsl_vpi DSL_VPI VPI value, mandatory for DSL
-multiplex DSL_MULTIPLEX, --dsl_multiplex DSL_MULTIPLEX Multiplex type, mandatory for DSL; multiplex
type can either be llc or vcmux
-vtag DSL_VLAN_TAG, --dsl_vlan_tag DSL_VLAN_TAG VLAN ID for DSL line
-p, --pppoe Use PPPoE interface for staging
-pu PPPOE_USER, --pppoe_user PPPOE_USER PPPoE username, mandatory for PPPoE
-pp PPPOE_PASSWORD, --pppoe-password PPPOE_PASSWORD PPPoE password, mandatory for
PPPoE
-ps PPPOE_SERVICE, --pppoe-service PPPOE_SERVICE PPPoE service name
-pa PPPOE_ACCESS_CONCENTRATOR, --pppoe-access-concentrator PPPOE_ACCESS_
CONCENTRATOR
 PPPoE access concentrator
-wu WWAN_USER, --wwan_user WWAN_USER WWAN username
-wp WWAN_PASSWORD, --wwan-password WWAN_PASSWORD WWAN password
-wapn WWAN_APN, --wwan-apn WWAN_APN WWAN APN name
-wpin WWAN_PIN, --wwan-pin WWAN_PIN WWAN SIM pin
-lmode {auto,full-duplex,half-duplex}, --link-mode {auto,full-duplex,half-duplex}
 Link mode for the interface [auto | half-duplex | full-duplex]
-lspeed {auto,10m,100m,1g}, --link-speed {auto,10m,100m,1g} Link speed for the interface [auto | 10m | 100m | 1g]
-t1e1 {0/0,0/1,0/2,0/3}, --t1e1-iface {0/0,0/1,0/2,0/3} Use T1E1 interface for staging [0/0 | 0/1 | 0/2 | 0/3]
-t1e1-type {t1,e1}, --t1e1-type {t1,e1} T1E1 type (default=t1)
-t1e1-clk-src {internal,external}, --t1e1-clock-source {internal,external}
 T1E1 clock source
-encap {ppp,hdlc,frame-relay}, --encapsulation {ppp,hdlc,frame-relay}
 Encapsulation for T1E1 [ppp | hdlc | frame-relay] (default=ppp)
-dlci DLCI_NUMBER, --dlci-number DLCI_NUMBER DLCI number for frame-relay encapsulation
-auth {psk,cert}, --auth-type {psk,cert} Authentication type [psk | cert] (default=psk)
-bla BGP_LOCAL_AS, --bgp-local-as BGP_LOCAL_AS BGP local autonomous system number
-bpa BGP_PEER_AS, --bgp-peer-as BGP_PEER_AS BGP peer autonomous system number
-bpi BGP_NEIGHBOR, --bgp-neighbor BGP_NEIGHBOR BGP peer IP address

```

To run the script on an SD-LAN device, you must also include the following options, which are shown in the command below:

- Ethernet LAN interface (`-wpt enet`)—Append this option to the WAN port you are using to connect to the internet. The example below uses port 0, so the option is `-w 0 -wpt enet`.
- VLAN (`-v`)—The example below uses VLAN 4091 (`-v 4091`).
- Port group (`-pg`) and port group speed (`-pgspeed`)—For CSX8300 switches, the default port speed is 25 GB. The example below uses port group 0 and sets the speed for ZTP to 10 GB, so the options are `-pg 0` and `-pgspeed 4x10G`.

```

admin@VNF:/ $ sudo /opt/versa/scripts/staging.py -I SDLAN-branch@nms-org.com -r controller-
staging@nms-org.com \
-c 10.10.10.10 -w 0 -wpt enet -s 10.10.10.20/24 -g 10.10.10.10 -pg 0 -pgspeed 4x10G -v 4091

```

If you want to use two-factor authentication in the device activation process, enable it as described in [Use URL-Based ZTP To Activate a VOS Device](#), above.

To verify that the VOS device has been deployed, check the Tasks window in Versa Director:

| Tasks     |   |           |               |                        |                          |                          |                        |          |
|-----------|---|-----------|---------------|------------------------|--------------------------|--------------------------|------------------------|----------|
| Failed 10 |   | Pending 0 |               | In Progress 0          |                          | Success 43   Total 53    |                        |          |
|           | > | ID        | User          | Activity               | Time                     |                          | Description            | Progress |
|           |   |           |               |                        | Start Time               | End Time                 |                        |          |
|           | > | 53        | Administrator | Delete template -Te... | Thu, Feb 20 2020, 1...   | Thu, Feb 20 2020, 1...   | Deleting template ...  | ✓        |
|           | > | 52        | System        | Apply-Post Staging ... | Wed, Feb 05 2020, ...    | Wed, Feb 05 2020, ...    | Apply post-staging ... | !        |
|           | > | 51        | System        | Apply-Post Staging ... | Wed, Feb 05 2020, ...    | Wed, Feb 05 2020, ...    | Apply post-staging ... | !        |
|           | > | 50        | System        | Apply-Post Staging ... | Fri, Jan 31 2020, 22:... | Fri, Jan 31 2020, 22:... | Apply post-staging ... | !        |

## Use a USB Storage Drive To Activate a VOS Device

For Releases 21.2 and later.

If you have physical access to a VOS device, you can stage the SD-WAN CPE device by inserting a USB storage drive into the device. The USB storage drive must contain a file named `staging.params`, which contains input parameters for the `staging.py` script. The USB storage drive can optionally contain a VOS package file and certificates. All these files must be at the root (top level) of the USB drive. They cannot be in subdirectories.

When you install the USB storage drive into the VOS device, the device automatically reads the file and configures itself based on the SD-WAN parameters specified in the `staging.params` file.

The `staging.params` file contains the parameters required as input for the `staging.py` script, in a key-value format. The following example shows an example of the minimum configuration required to configure any device:

```
dhcp
local-id=local@my-company.com
remote-id=remote@remote-site.com
controller=10.1.2.3
```

To ensure that a specific device is being staged, also include the device's service number in the `staging.params` file:

```
serial-number=number
```

The keywords in the `staging.params` file directly map to the long-form command-line arguments of the `staging.py` script, which are shown in [Use the CLI To Activate VOS Devices](#), above. To check the `staging.py` script options supported in the current version of the VOS software, issue the following command:

```
$ vsh show-staging-params
```

In the `staging.params` file, lines starting with a `#` are treated as comments and are skipped, and leading spaces are removed. The file can also be in DOS format.

If the USB drive contains a VOS package file (a file whose name has the format `versa-flexvnf-xxx-yyy-zzz.bin`) or an OS SPack file (a file whose name has the format `versa-flexvnf-osspack-xxxxx.bin`), these files are copied to the appropriate locations on the VOS device.

Note that to activate a VOS device from a USB drive, the device's configuration must be empty or it must be the factory-default configuration. To delete the configuration from the VOS device, issue the **request erase config-file** command from the device's CLI. If the VOS device has the factory-default configuration but has not been staged, the activation process automatically stages the device using the configuration information provided in the staging parameters.

## Configure VOS Devices and ZTP Automatically Using Cloud-Init

When you instantiate a VOS device in a virtual environment, such as KVM, OpenStack, or a cloud, you can use the cloud-init functionality on the VOS device to automatically onboard the device immediately after you finish installing it. Cloud-init is an industry-standard multidistribution method for cross-platform cloud instance initialization. It is supported across all major public cloud providers, provisioning systems for private cloud infrastructure, and bare-metal installations.

If you do not use cloud-init when you install a VOS device as a VM in the cloud or in a virtualization environment, you must manually configure the VOS device after the installation and then you must perform the staging for ZTP manually. If you use cloud-init, you can pass configuration and staging information to the VOS device, and this information is executed when the device first boots. All three operations—installation, configuration and onboarding—are performed automatically.

The following is an example of a cloud-init file you can use to configure the eth0 interface on a VOS device and to stage the VOS device after it boots. Note that you must retain all the spaces at the end of each line for the file to work. JAML is very sensitive to spaces, which serve as an indication of the next action.

```
cloud_init_modules:
 - write-files
 - set_hostname
 - update_hostname
 - users-groups
 - ssh
write_files:
 - content: |
 # This file describes the network interfaces available on your system
 # and how to activate them. For more information, see interfaces(5).
 # The loopback network interface
 auto lo
 iface lo inet loopback
 # The primary network interface
 auto eth0
 iface eth0 inet static
 address 192.168.0.230
 netmask 255.255.255.0
 gateway 192.168.0.1
 path: /etc/network/interfaces
 - content: |
 #!/bin/bash
 logger running staging script
 sudo /opt/versa/scripts/staging.py -I SDWAN-Branch@bk.com -r controller-1-staging@bk.com
 permissions: "0755"
```

```
path: /home/admin/versa.sh
cloud_final_modules:
- runcmd
- scripts-user
runcmd:
- /home/admin/versa.sh
```

---

## Supported Software Information

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

- Releases 21.2 and later support using a USB storage drive to activate a VOS device.
- Releases 22.1.3 and later support configuring and activating an SD-WAN VOS device to manage Layer 2 access and core switches.

---

## Additional Information

[Configure Basic Features](#)