

INTRODUCTION TO VERSA DIRECTOR

The Versa Networks lab environment consists of a fixed, pre-configured topology that will allow you to explore, configure, and manage Versa Networks CPEs by using Versa Director, the central management and orchestration platform for a Versa Secure SD-WAN solution. After completing this lab, you will be able to:

- Identify the functions of the main Versa Director tabs; and
- Navigate through the Versa Director environment to accomplish some basic tasks

In this lab, you will be assigned to a lab environment with 2 CPEs and a hub site. Your user will be a single tenant in a multi-tenant system, so the hub device will be shared device.

The lab environment is accessed through Amazon Workspaces. For instructor-led courses, your instructor will provide information on how to connect to the lab environment.

The remote desktop connection opens a remote workstation, where you will use various tools to navigate and configure the lab environment. The main tool you will use in this lab is Versa Director. Versa Director can be accessed by opening the Google Chrome browser on the Remote Desktop. There is a bookmark to the Versa Director device in the Google Chrome bookmark bar.

During certain lab parts, the lab guide will present sample output from the GUI or the CLI. The sample outputs are SAMPLES and represent the information as it appeared during the lab guide creation. Your output may vary in some ways (some devices may or may not be present, some routes may or may not be the same, etc.) Do not be alarmed if your results vary slightly from the results shown in the lab guide. The important thing is that the lab functions in the desired manner.

This lab guide will step you through some common tasks that are performed on Versa Director. After an introductory set of exercises, you will be asked to perform some basic tasks that will allow you to become more familiar with the environment.

The goal of this and all lab exercises is to help you gain additional skills and knowledge. Because of this, the lab guide contains additional instruction to supplement the student guides.

Now that we've discussed what is expected, let's get started!

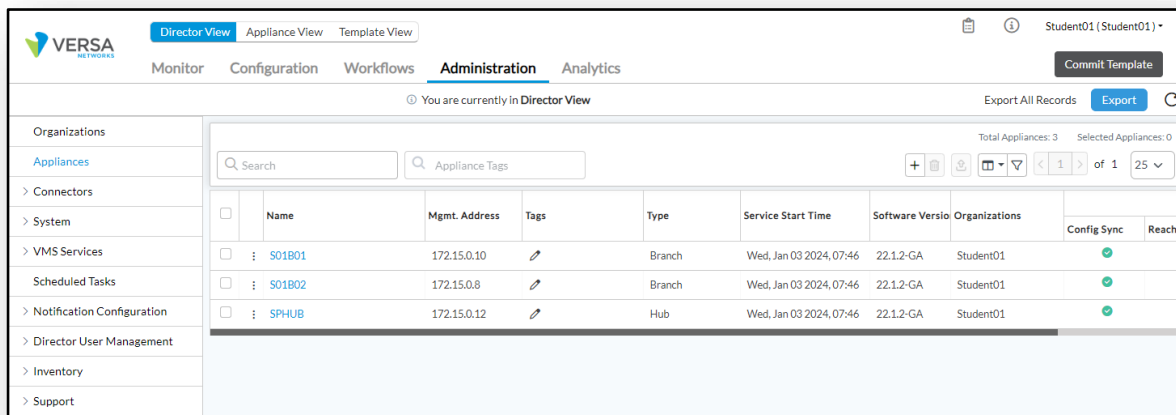
EXERCISE 1: IDENTIFY THE MAIN COMPONENTS OF VERSA DIRECTOR

Please refer to the Lab Access Guide for instructions on how to connect to the remote lab environment.

Step 1. Explore Versa Director

- In the remote landing station, open the *Google Chrome* browser and log into Versa Director. The Versa Director IP address is `https://10.27.1.10` in the remote browser. You should be placed into the *Administration > Appliances* dashboard of Versa Director.

There are 5 tabs at the top of the Versa Director user interface. Each of the tabs represents a set of dashboards to perform certain tasks, such as monitoring devices, managing configuration components on Versa Director, and creating and managing different components. The currently selected tab is highlighted automatically:



The screenshot shows the Versa Director Administration dashboard. The 'Administration' tab is selected, and the 'Appliances' sub-tab is active. The main content area displays a table of appliances with columns for Name, Mgmt. Address, Tags, Type, Service Start Time, Software Versio, Organizations, Config Sync, and Recha. Three appliances are listed: S01B01 (Branch), S01B02 (Branch), and SPHUB (Hub). The left sidebar shows a navigation menu with options like Organizations, Appliances, Connectors, System, VMS Services, Scheduled Tasks, Notification Configuration, Director User Management, Inventory, and Support. The top navigation bar includes tabs for Director View, Appliance View, and Template View, along with a 'Commit Template' button and a 'You are currently in Director View' indicator.

Name	Mgmt. Address	Tags	Type	Service Start Time	Software Versio	Organizations	Config Sync	Recha
S01B01	172.15.0.10		Branch	Wed, Jan 03 2024, 07:46	22.1.2-GA	Student01	✓	
S01B02	172.15.0.8		Branch	Wed, Jan 03 2024, 07:46	22.1.2-GA	Student01	✓	
SPHUB	172.15.0.12		Hub	Wed, Jan 03 2024, 07:46	22.1.2-GA	Student01	✓	

The *Appliances* table of the Administration dashboard lists all of the deployed appliances in your SD-WAN environment. You can click on a device in the list to navigate directly to that device's configuration and monitoring dashboard. You can also navigate to the individual device configuration and management dashboard by clicking the Monitor tab.

The primary tabs are:

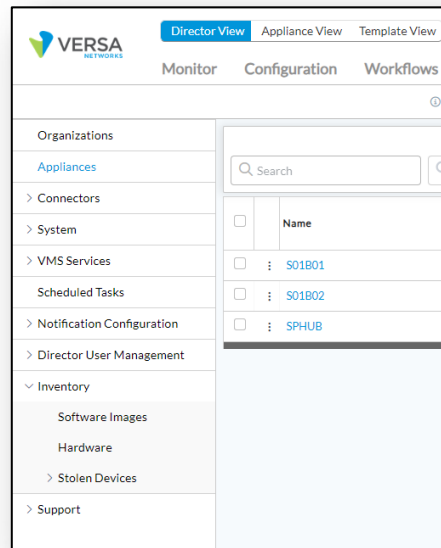
- **Director View:** Access to Versa Director configuration and management
- **Appliance View:** Access to individual appliances
- **Template View:** Access to the configuration templates

The primary Director View tabs are:

- **Monitor:** Provides access to device specific statistics, status, and configurations
- **Configuration:** Provides access to configuration components stored on Versa Director, including Device Groups, Bind Data, and Device and Service Templates
- **Workflows:** Provides access to create new workflows and to view and update existing workflows
- **Administration:** Provides access to SD-WAN environment configuration, including device inventory, deployment information, overlay configuration, external connectors, organization definition and configuration, user management, and licensing. It also provides access to the software management features, such as downloaded OS packages, Security Packages (Spacks), etc.
- **Analytics:** Opens the Versa Analytics GUI within Versa Director

Because you're already here, let's explore the *Administration* tab.

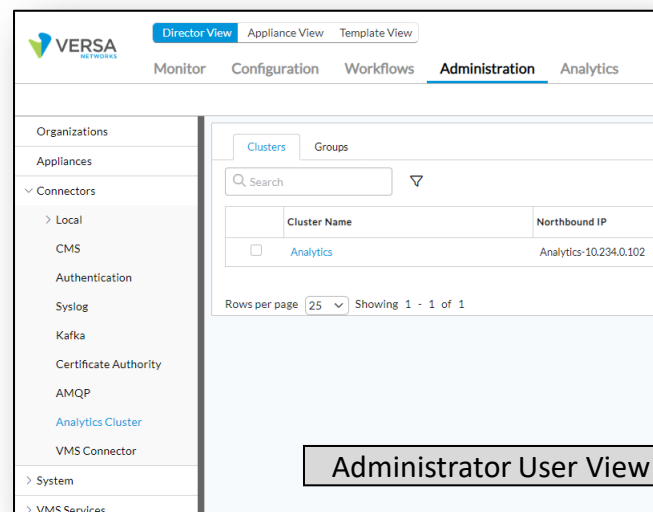
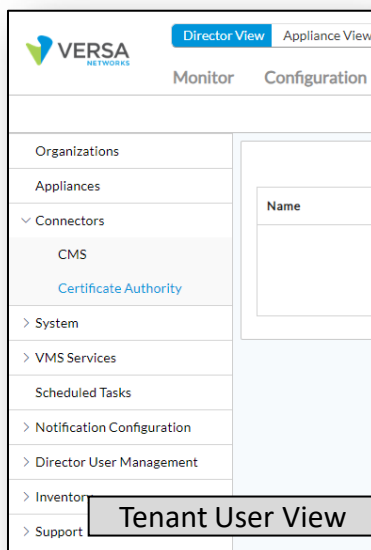
The menu on the left displays the main categories of administration information. Wherever you see a > symbol, this means that the category can be expanded:



b. Expand the *Connectors* menu.

The *Connectors* menu lists the different types of connections that are available to other systems, such as Analytics clusters, authentication servers, syslog servers, and so forth.

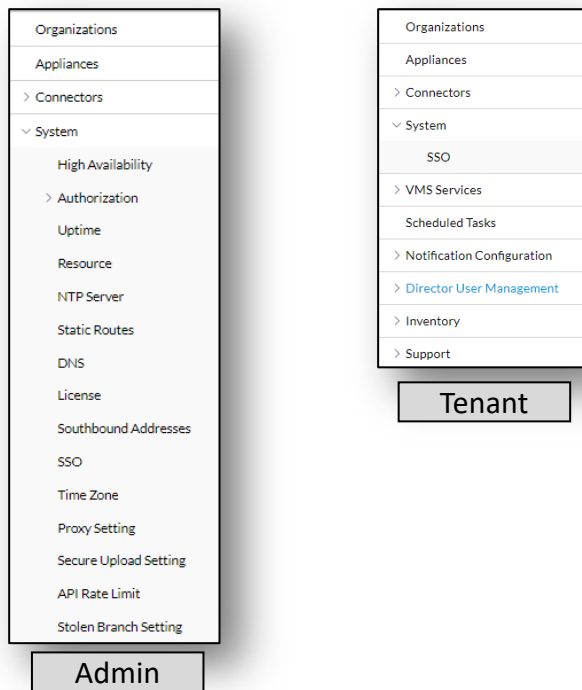
As a tenant of a managed system, Versa Director hides many of these options from the tenant user and only displays configuration components that can be managed by the sub-tenant. This prevents sub-tenants from making configuration changes that could have a negative impact on other tenants. However, from an administrator login, all of the options for Analytics and connector configuration are present.



- c. Next expand the *System* menu.

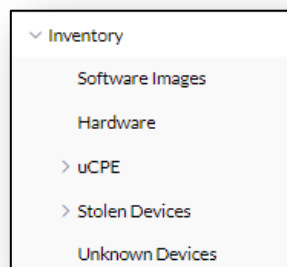
The *System* menu is where Versa Director system information is configured, including Versa Director High Availability, NTP servers, the Versa Director license, DNS settings, Time Zone settings, and so forth. It's important to remember that the Versa Director is a computer system that may need to perform functions for the local processes, including DNS lookups and local routing. These settings are NOT for the SD-WAN systems. These settings are for the local Versa Director system.

Because Versa Director is owned and managed by the provider (in a multi-tenant system), only a provider administrator has access to the server settings. The system properties that can be managed by the tenants include Single Sign On features for authentication to Versa Director.



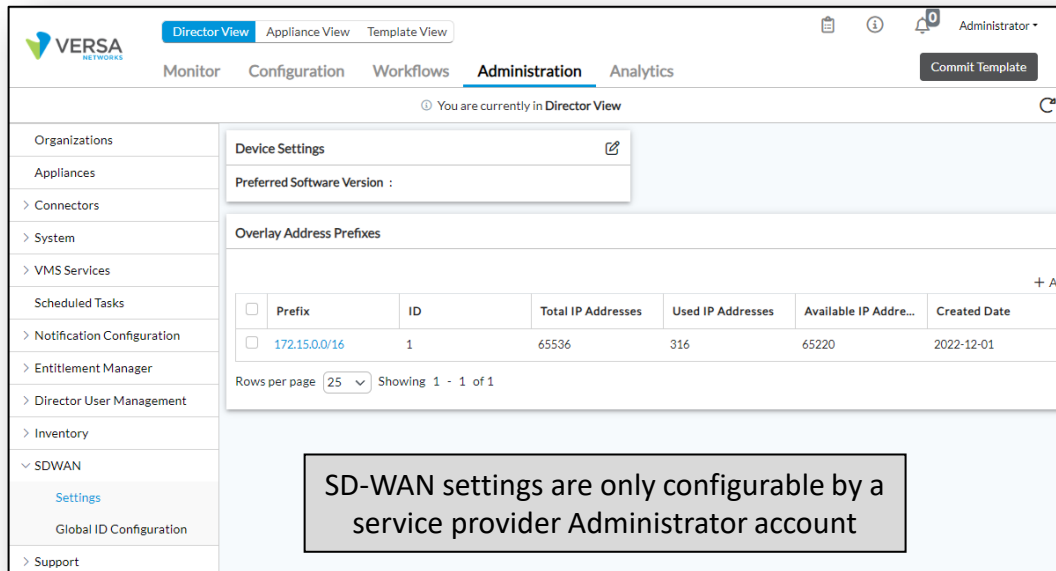
- d. Expand the Inventory menu.

Here you will see dashboards to manage the software images stored on Versa Director, the current device inventory, which includes devices that have been created in the Versa Director database (Hardware), Security Package management, OS Security package management, and uCPE images. The Unknown Devices dashboard lists appliances that have been onboarded but that have a serial number that does not match a device serial number in the Hardware table. Again, depending on whether the user is connected as a provider admin, or a tenant admin, the options are displayed.



- e. Expand the *SDWAN > Settings* menu.

The *SDWAN Settings* dashboard is where the SD-WAN overlay address scheme is defined.

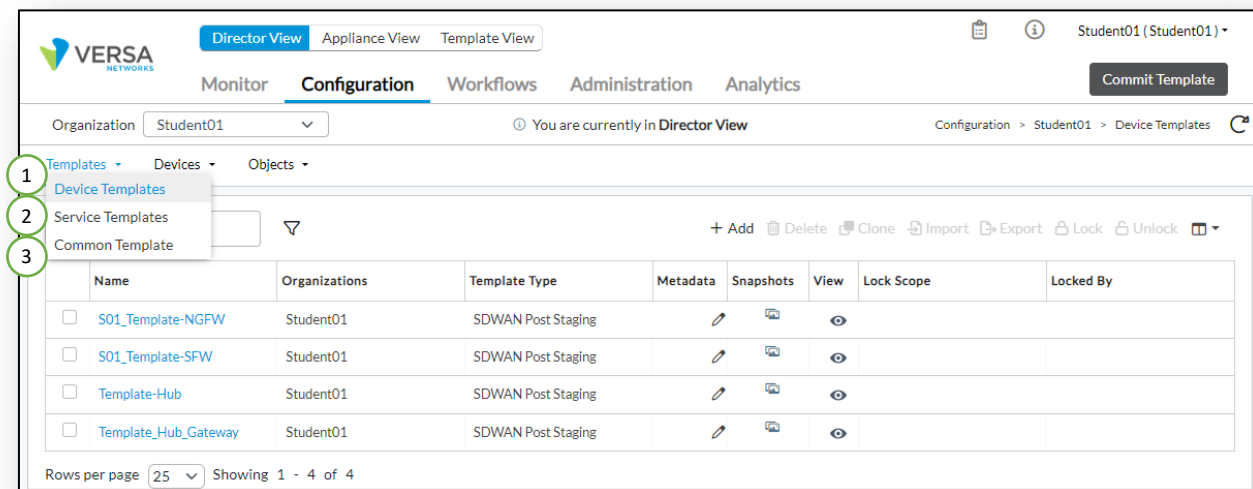


Step 2. Explore Versa Director

In this lab exercise, you will explore various dashboards of the Versa Director platform and answer questions related to the areas that you explore. This exploration is from the perspective of a tenant in a multi-tenant system. Your user ID is assigned a role of TenantSuperAdmin.

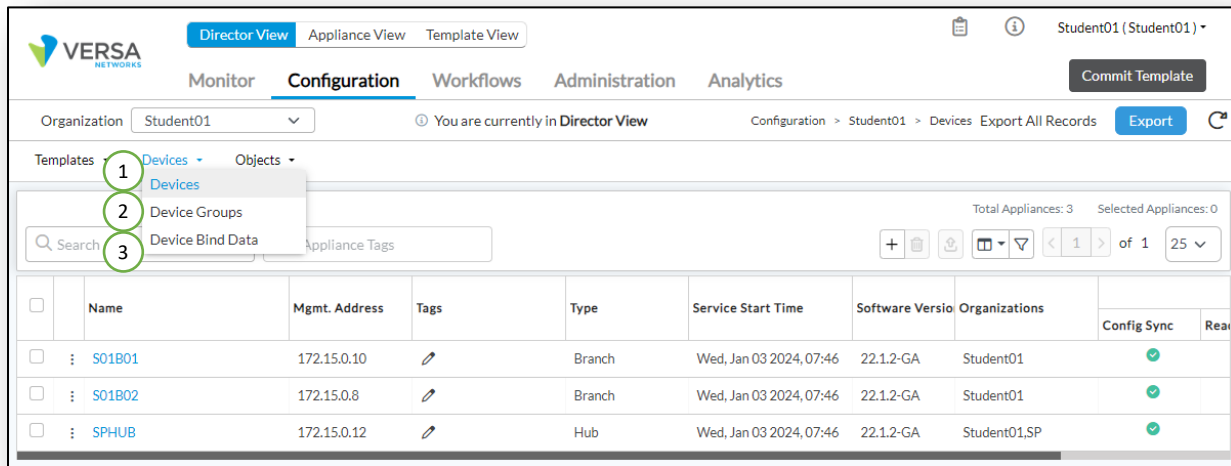
- a. Navigate to the *Configuration* tab.

Use the GUI to find where configuration templates are stored.



- b. Open the *Devices > Devices* menu

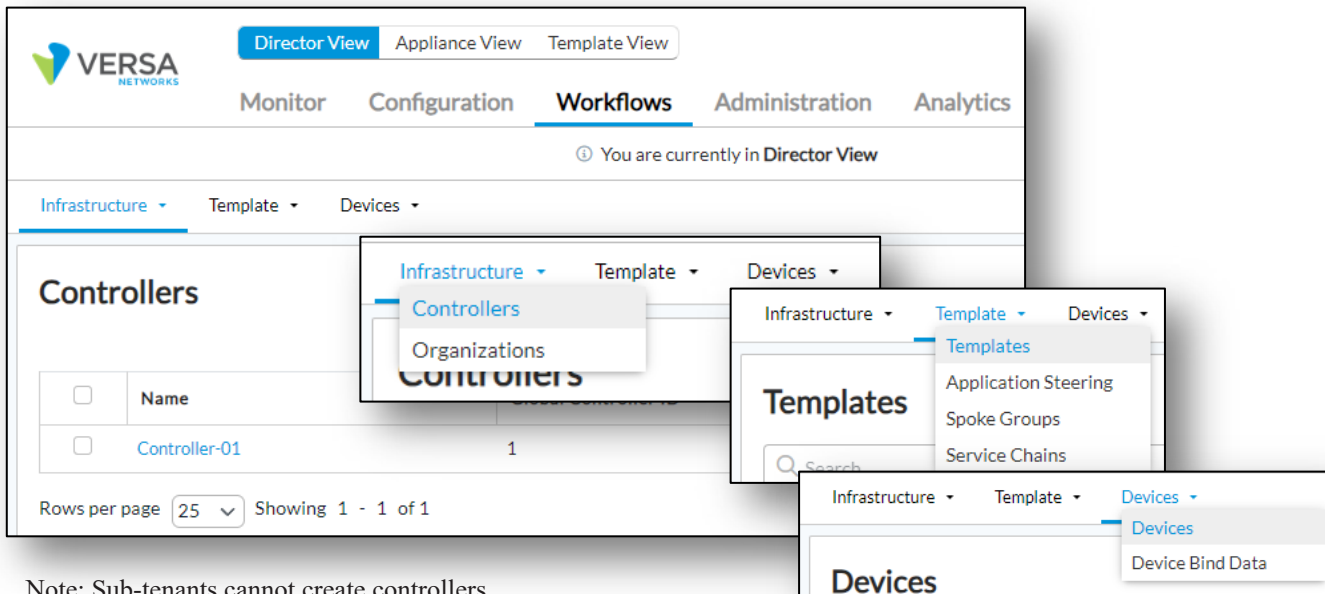
Use the GUI to show where the device related configuration is stored.



- c. Open the *Workflows* dashboard

A workflow is a step-by-step process to perform a task. In Versa Director, a workflow is a step-by-step process to create something, similar to a configuration wizard. The process or settings used are saved so that the process can be repeated, or so that settings in the original process can be changed and re-used to update or modify the object that the workflow created.

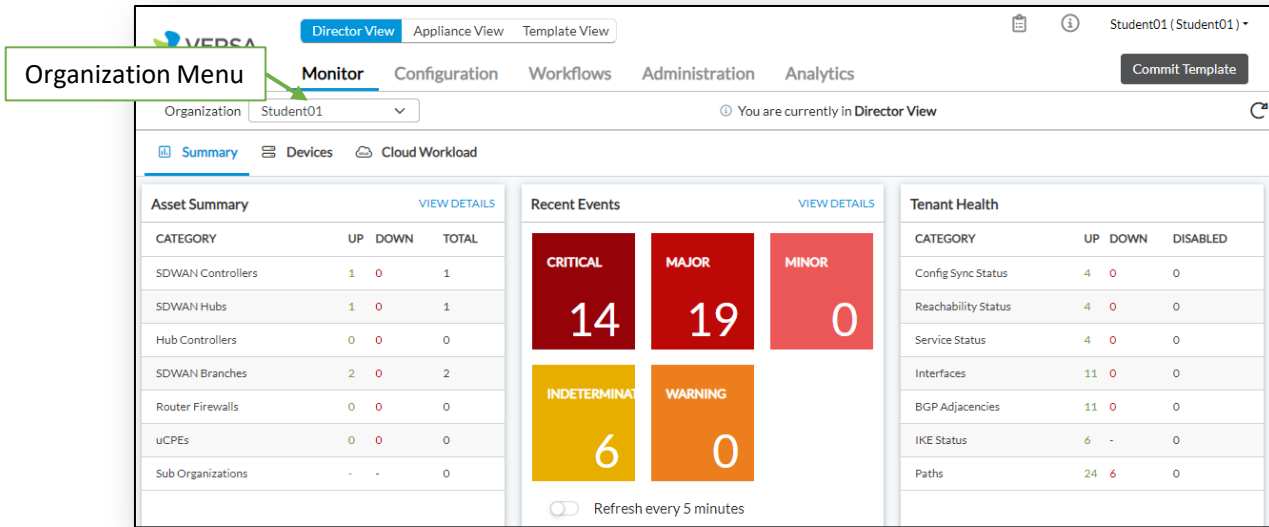
Navigate to the *Workflows* tab. In the *Workflows* tab, examine the different types of workflows that can be used to create configuration components.



Note: Sub-tenants cannot create controllers, as controllers are part of the provider organization.

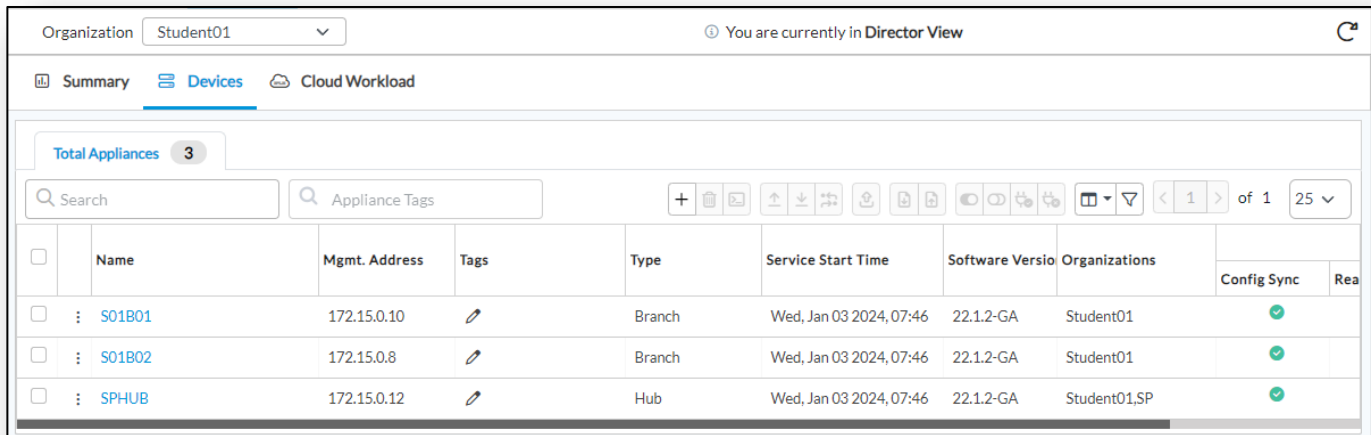
d. Open the *Monitor* tab.

In the *Monitor* tab there is a left-side menu and a sub-menu at the top of the table displayed on the page.

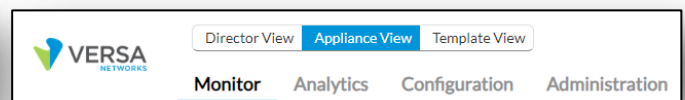
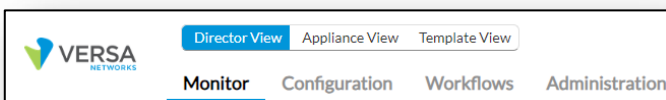


e. Open the *Devices* tab.

The *Devices* tab displays the devices that are managed by your organization.

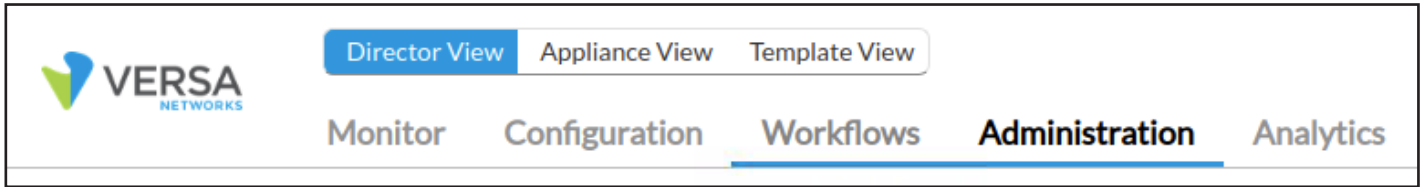


Note that when you click on a device, the top level menu changes to Appliance View. If you click on the “Total Appliances” tab, the top level menu changes back to Director View.



f. Open the *Administration* panel in Director View.

Click the *Director View* button at the top of the administration panel.

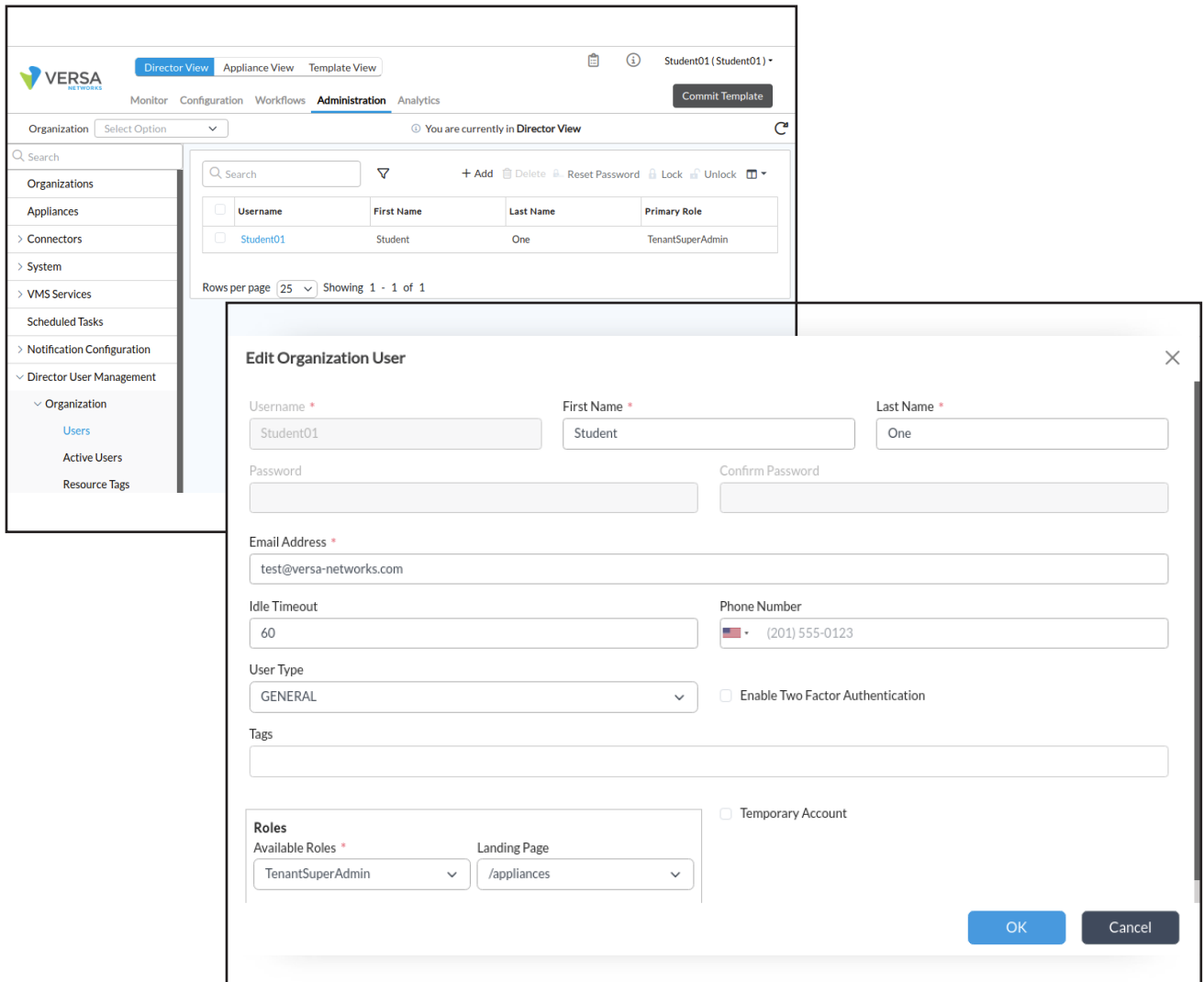


g. Navigate to the *Director User Management* dashboard.

In the *Administration* tab, locate the *Director User Management* menu on the left side and expand the menu. Select the *Organization > Users* from the menu.

Organization users are users that have permission to log into Versa Director and view/configure information associated with the specific organization. Provider users are available to users that are logged in with a provider administrator account.

Tenants can manage their own users and access, and providers can manage all users and access to the system.



From the user menu, user accounts can be locked or unlocked. A user account may become locked because of unsuccessful login attempts, or because the administrator manually locks the account. You can use the *Lock/Unlock* buttons to set the user account mode.

The screenshot shows the Director User Management interface. The organization is set to 'Student01'. A table lists users, with 'Student01' selected. The 'Lock' and 'Unlock' buttons are highlighted with a red box.

Username	First Name	Last Name	Primary Role
Student01	Student	One	TenantSuperAdmin

h. Explore the *Inventory* menu.

Expand the *Inventory* menu, then select *Software Images* from the list. This is where software images are stored when they are downloaded to Versa Director. Software images are placed in their proper categories: OS Security Packages, Security Packages, and VOS/Director images. The software packages in the libraries can be used for appliance and director upgrades.

Tenants cannot download software packages, as that may affect system storage. Providers in a multi-tenant system can download software packages, and those software packages are available to tenants for installation.

The screenshot shows the Director Inventory - Software Images page. The 'Appliance Upgrades' tab is selected. A table lists appliance upgrades with columns for Appliance Name, Management Address, Tags, Appliance Type, OS Type, Owner Org, and OS Security I Package Vers.

Appliance Name	Management Addr...	Tags	Appliance Type	OS Type	Owner Org	OS Security I Package Vers
S01B01	172.15.0.4		branch	Bionic	Student01	OSSPACK Not
S01B02	172.15.0.6		branch	Bionic	Student01	OSSPACK Not
SP-HUB-New	172.15.0.30		hub	Bionic		OSSPACK Not

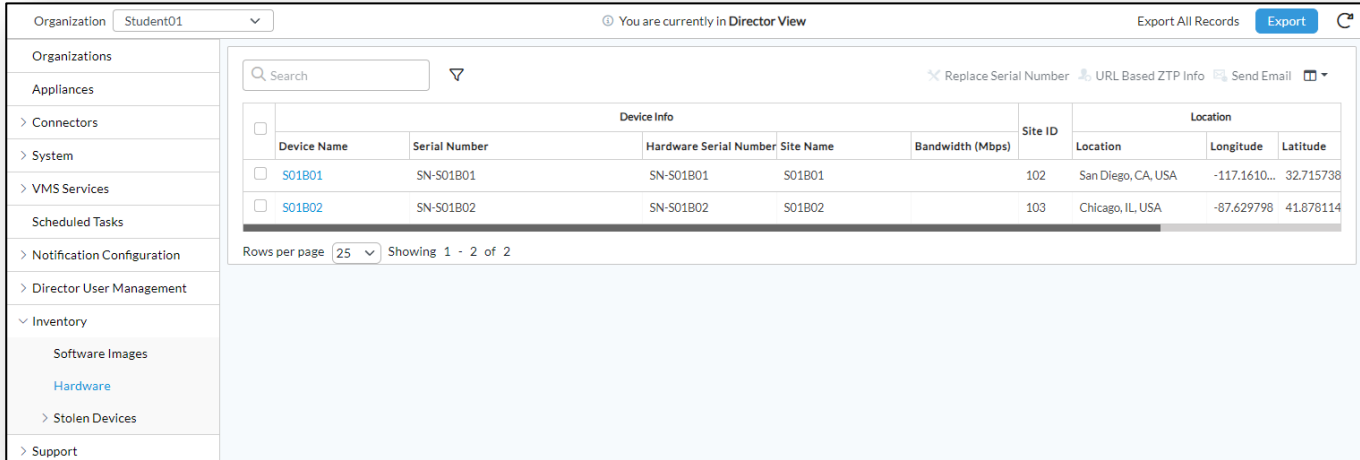
The screenshot shows the Director Inventory - Software Images page. The 'Security (SPack)' tab is selected. A table lists security packages with columns for Package Name, Package Version, Download Type, Flavor, Size, Day & Time Downl..., and Stat.

Package Name	Package Version	Download Type	Flavor	Size	Day & Time Downl...	Stat
versa-security-package-2226.tbz2	2226	Full	Premium	823 MB	Sun, Jan 12 2025, 20:47	DOW
versa-security-package-2220.tbz2	2220	Full	Premium	870 MB	Sun, Jan 12 2025, 20:55	INSTA
versa-security-package-2119.tbz2	2119	Full	Definitions	79 MB	Thu, Feb 15 2024, 17:24	PREV
versa-security-package-2014.tbz2	2014	Full	Premium	711 MB	Tue, Dec 20 2022, 09:23	DOW

- i. Select the *Inventory > Hardware* menu.

The *Inventory > Hardware* dashboard is where devices that have been created in Versa Director are stored. It's important to remember that when you create a device in Versa Director, it is stored as an object in the Versa Director database.

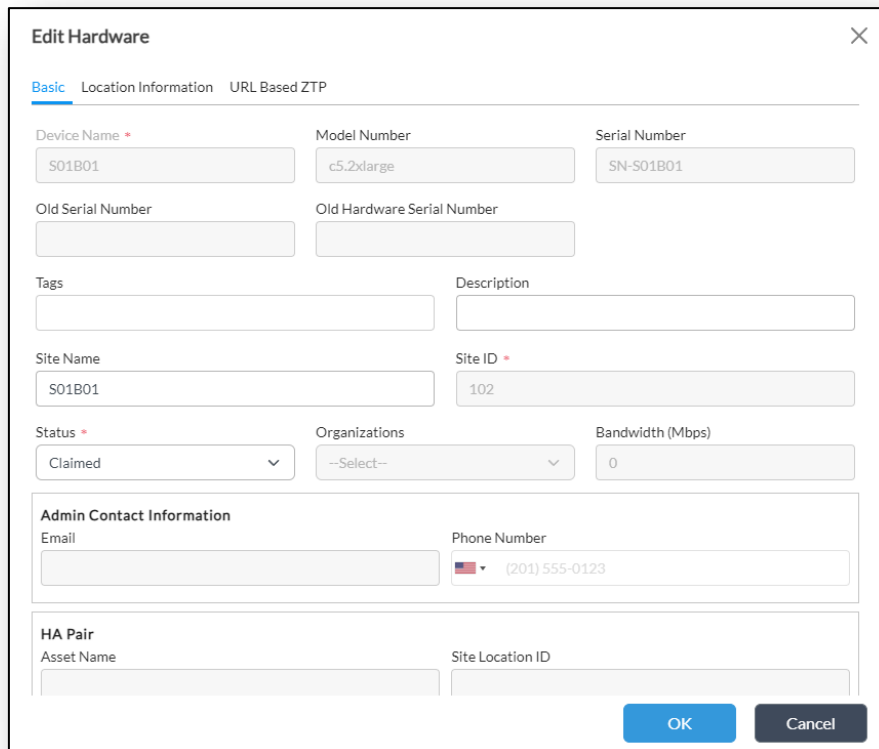
The *Hardware* table lists devices that have been created in Versa Director. The *Appliances* menu table lists devices that have been deployed and are active in the network. When a device in the *Hardware* table is onboarded or deployed in the network, a corresponding Appliance is created in the *Appliance* table – but only AFTER the device is successfully onboarded and is live.



Device Info					Location			
Device Name	Serial Number	Hardware Serial Number	Site Name	Bandwidth (Mbps)	Site ID	Location	Longitude	Latitude
<input type="checkbox"/> S01B01	SN-S01B01	SN-S01B01	S01B01		102	San Diego, CA, USA	-117.1610...	32.715738
<input type="checkbox"/> S01B02	SN-S01B02	SN-S01B02	S01B02		103	Chicago, IL, USA	-87.629798	41.878114

Rows per page: 25 | Showing 1 - 2 of 2

You can click on an item in the hardware table to view the properties associated with the device.



Edit Hardware

Basic | Location Information | URL Based ZTP

Device Name: S01B01 | Model Number: c5.2xlarge | Serial Number: SN-S01B01

Old Serial Number: | Old Hardware Serial Number: |

Tags: | Description: |

Site Name: S01B01 | Site ID: 102

Status: Claimed | Organizations: --Select-- | Bandwidth (Mbps): 0

Admin Contact Information

Email: | Phone Number: (201) 555-0123

HA Pair

Asset Name: | Site Location ID: |

OK | Cancel

Key Point: The Organization drop-down controls the information displayed in the dashboards. Information displayed is associated with the selected organization. This is consistent across all dashboards.

Organization: Student01

Device Info			
	Device Name	Serial Number	Hardware Serial
<input type="checkbox"/>	S01B01	SN-S01B01	SN-S01B01
<input type="checkbox"/>	S01B02	SN-S01B02	SN-S01B02

Rows per page: 25 Showing 1 - 2 of 2

Organization: Student01

Templates		
	Name	Status
<input type="checkbox"/>	S01_Template-NGFW	Deployed
<input type="checkbox"/>	S01_Template-SFW	Deployed

Rows per page: 25 Showing 1 - 2 of 2

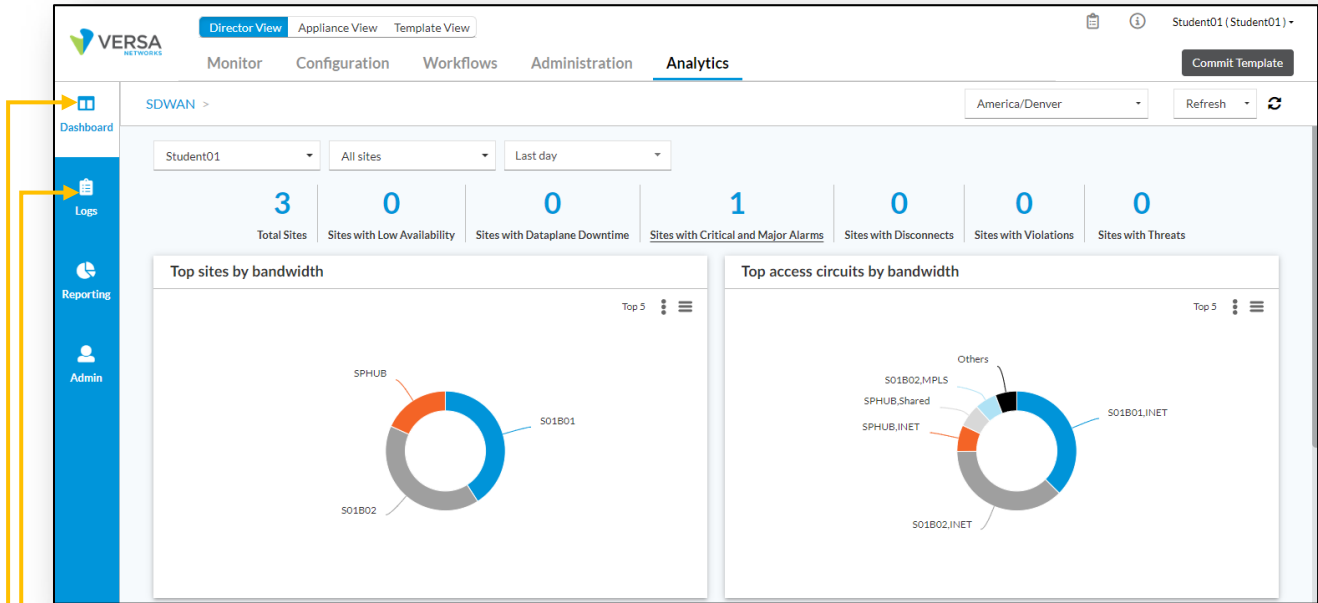
Organization: Student01

Devices		
	Name	Global Device ID
<input type="checkbox"/>	S01B01	102
<input type="checkbox"/>	S01B02	103

Rows per page: 25 Showing 1 - 2 of 2

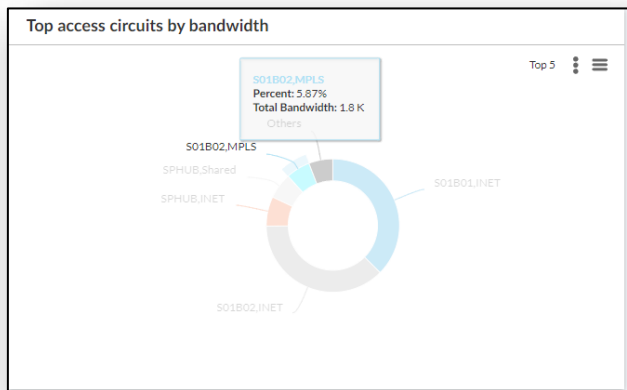
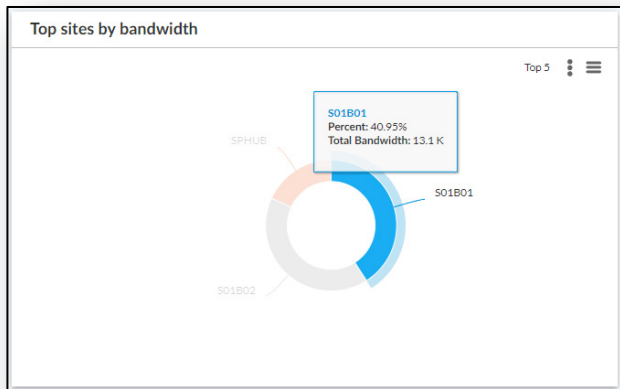
j. Open the *Analytics* dashboard.

Analytics stores recorded information from the environment and can be accessed directly from the Analytics tab in Versa Director, or through the Analytics GUI directly.

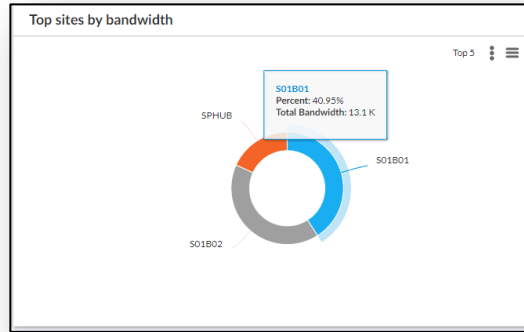


- Logs: Logging and triggered events from VOS devices
- Dashboard: Statistics gathered from devices and reported to Versa Analytics

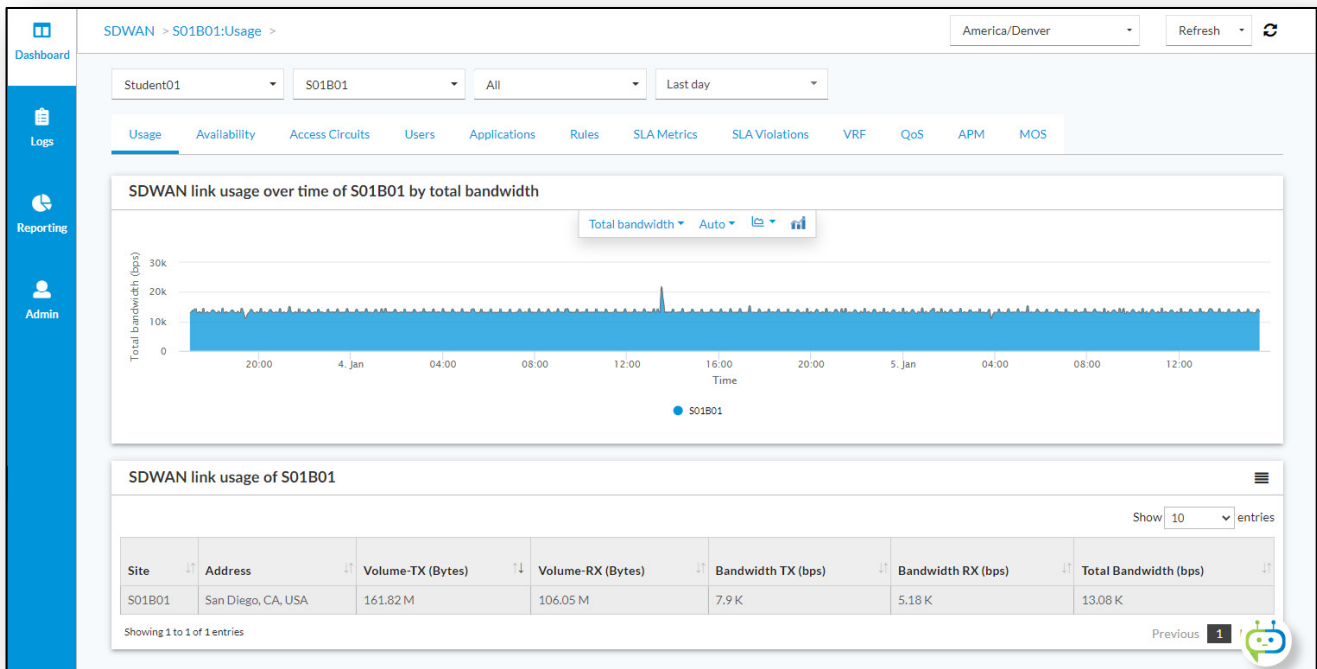
On many of the dashboards you can hover your mouse over a chart or device name and further details will be displayed:



- k. Hover your mouse over the *B01* device in the *Top sites by bandwidth* chart to view the bandwidth information for the B01 branch.

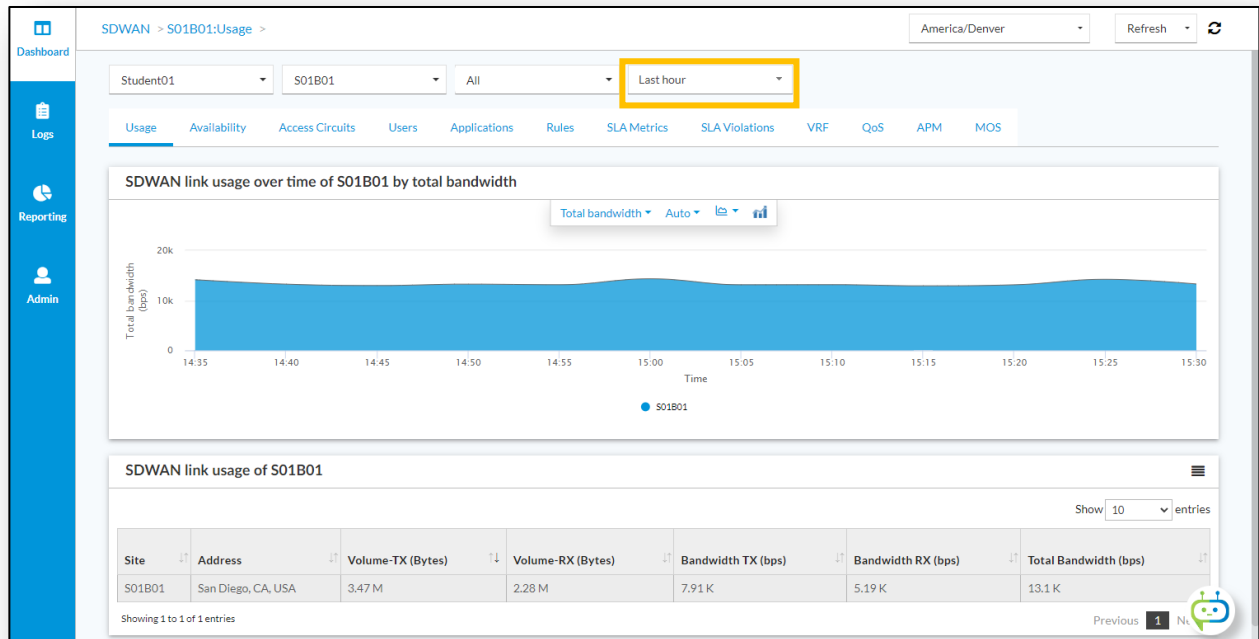


- l. Click the *B01* chart section to open the B01 bandwidth analysis dashboard.

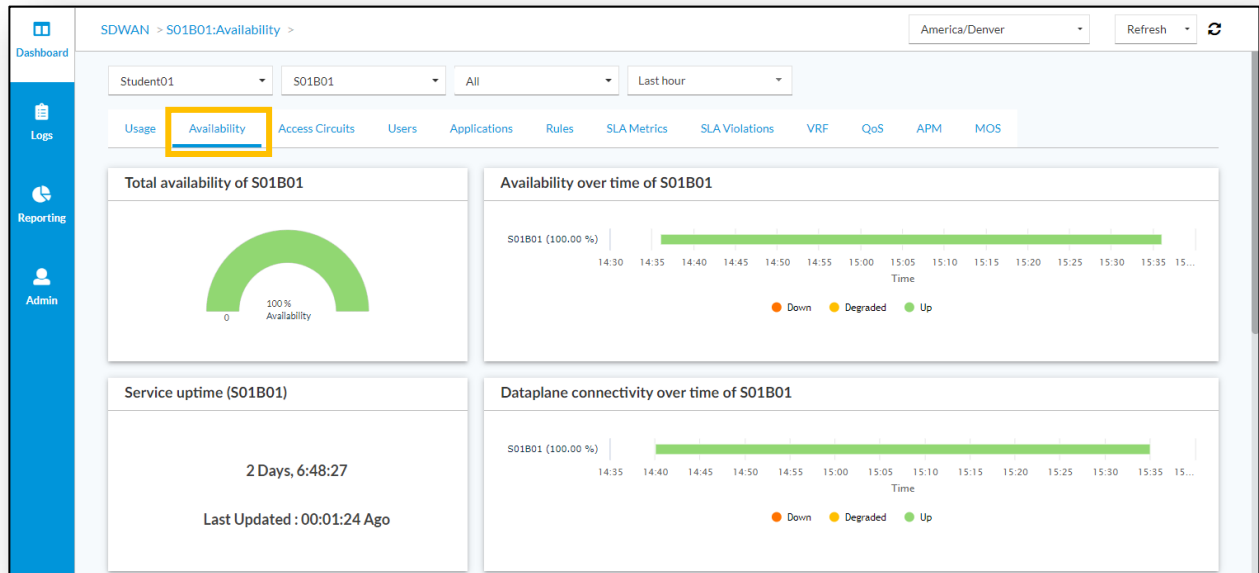


You can see the link usage over time in the chart. The time can be adjusted for different time periods.

m. Change the time frame from *Last day* to *Last hour* to view how the time display changes.



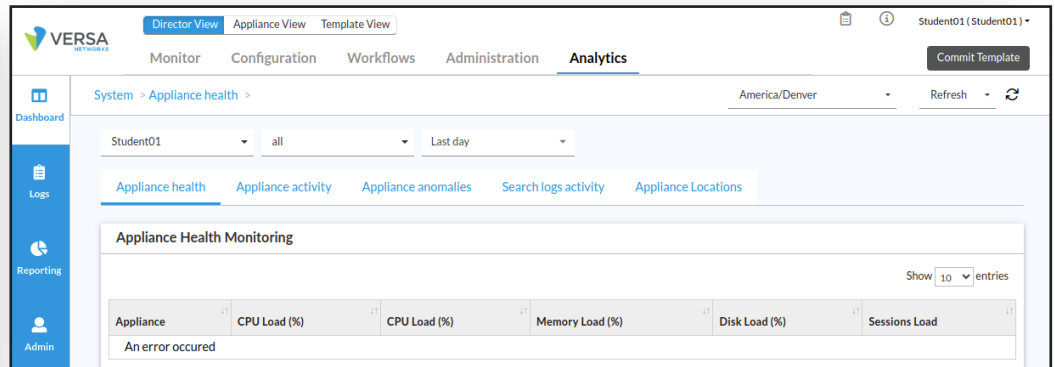
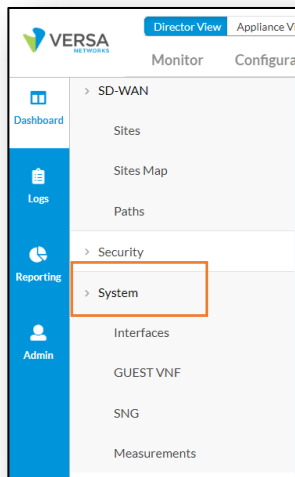
n. Click the *Availability* tab to view the site’s availability over time.



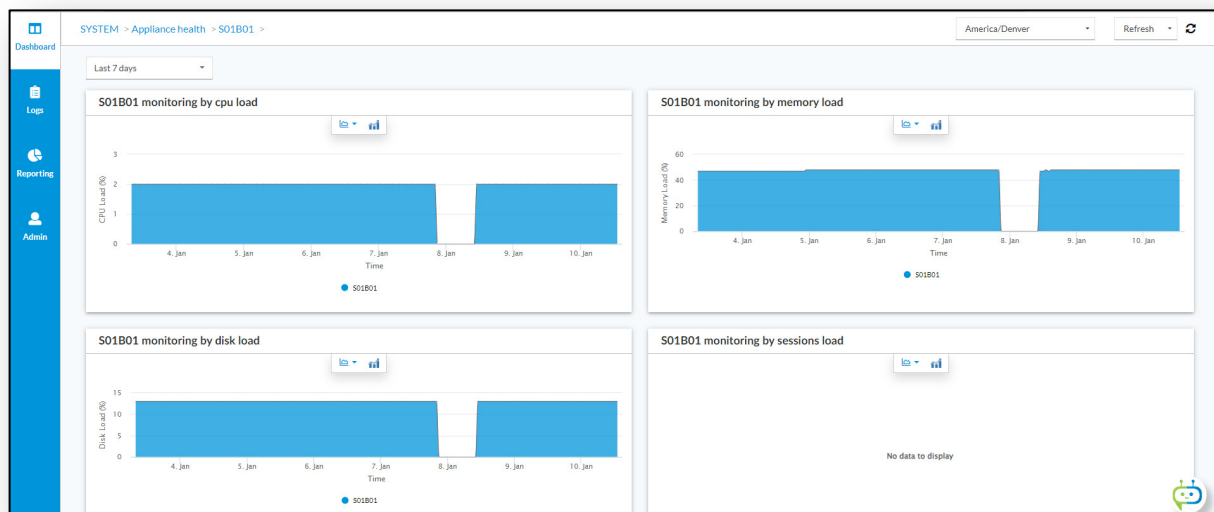
Take a few minutes to navigate through each of the site’s statistics tabs to see what information is stored on each tab.

Note: Some charts may display “No data to display” because this is a lab environment, and traffic is not actively passing between sites. As labs proceed, more information may be available in the dashboards.

- o. Select the *System* dashboard to view information about the appliance health.



- p. Click on an appliance name to see more details about that appliance.



STOP! Notify your instructor that you have completed this lab.

VERSA WORKFLOWS AND TEMPLATES

The Versa Networks lab environment consists of a fixed, pre-configured topology that will allow you to explore, configure, and manage Versa Networks CPEs by using Versa Director, the central management and orchestration platform for a Versa Secure SD-WAN solution. After completing this lab, you will be able to:

- Create a configuration template using template workflows;
- Create a new device group;
- Re-assign your devices to the new device group, thereby re-assigning your devices to a new device template;
- Commit the new template to your devices;
- Verify the services enabled in a configuration template and on the devices;
- Clone a template workflow and verify the creation of a corresponding device template; and
- Clone a device template and verify the creation of a corresponding template workflow.

In this lab you will be assigned two CPE devices (Branch devices) for configuration and monitoring. The branch devices are named after the student ID that you have been assigned.

The lab environment is accessed through Amazon Workspaces. Your student ID and workspace will be assigned by the instructor.

The remote desktop connection opens a remote workstation, where you will use various tools to navigate and configure the lab environment. The main tool you will use in this lab is Versa Director. Versa Director can be accessed by opening the Google Chrome browser on the Remote Desktop. The IP address of the Versa Director (from the remote workstation) is 10.27.1.10. Once you begin the lab, you may want to create a bookmark to Versa Director in the web browser on the remote desktop.

During certain lab parts, the lab guide will present sample output from the GUI or the CLI. The sample outputs are SAMPLES and represent the information as it appeared during the lab guide creation. Your output may vary in some ways (some devices may or may not be present, some routes may or may not be the same, etc.) Do not be alarmed if your results vary slightly from the results shown in the lab guide. The important thing is that the lab functions in the desired manner.

This lab guide will step you through some common tasks that are performed on Versa Director. After an introductory set of exercises, you will be asked to perform some basic tasks that will allow you to become more familiar with the environment.

The goal of this and all lab exercises is to help you gain additional skills and knowledge. Because of this, the lab guide contains additional instruction to supplement the student guides.

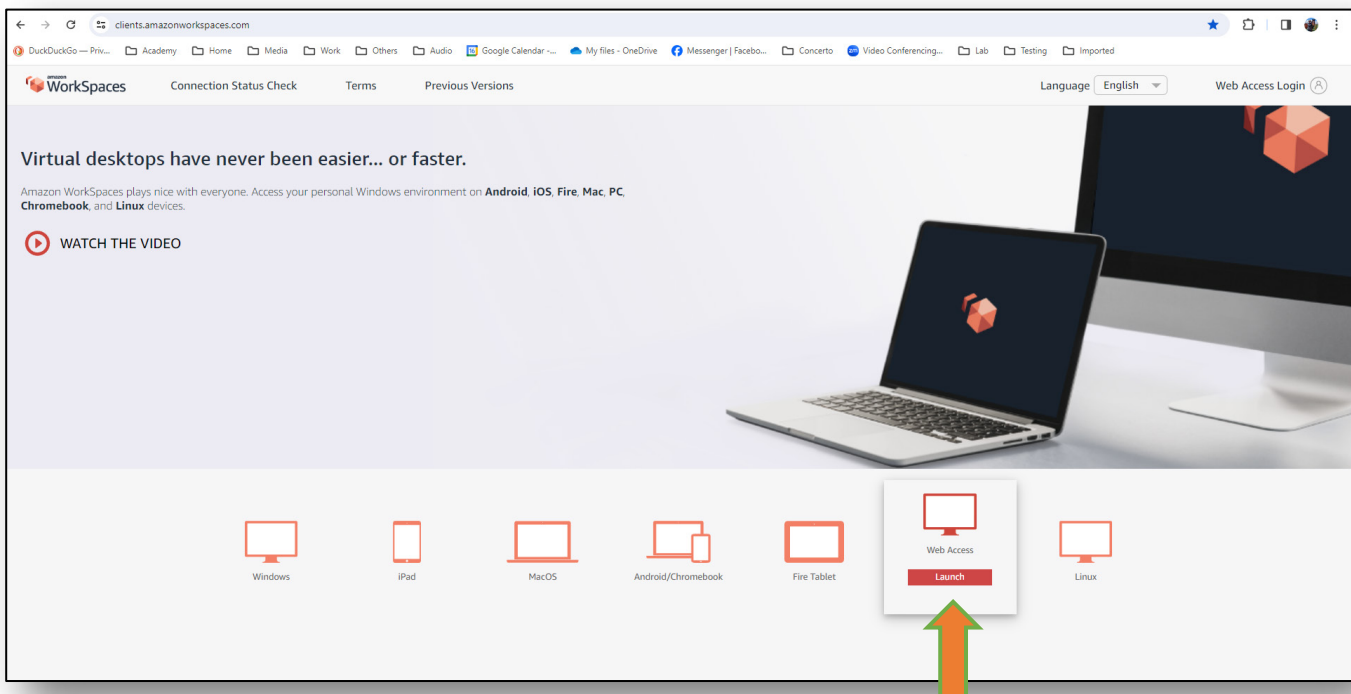
Now that we've discussed what is expected, let's get started!

Step 1. Connect to the Remote Desktop

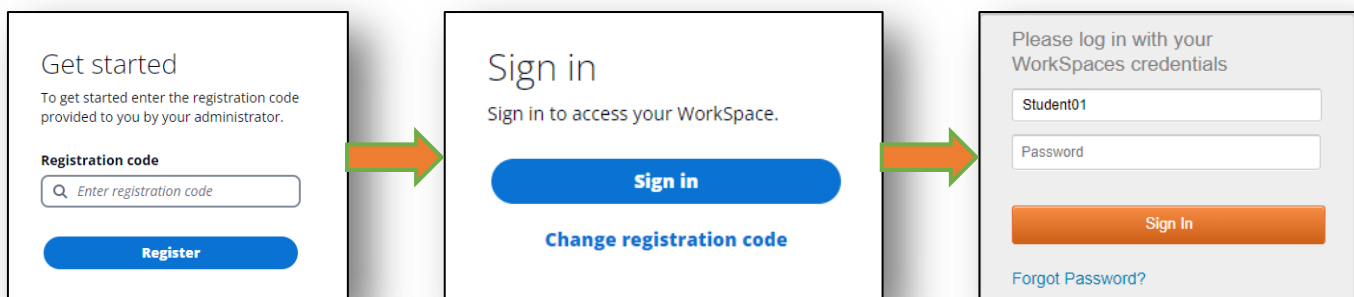
In the following lab exercises, you will:

- Connect to the AWS workspace to launch the remote desktop connection;
- Launch the Google Chrome browser in the remote desktop; and
- Log into Versa Director on the remote desktop.
 - a. Connect to the remote desktop.

Open your local browser and connect to: <https://clients.amazonworkspaces.com/> In the Amazon WorkSpaces window, select the Web Access link to open a web-based remote desktop session.

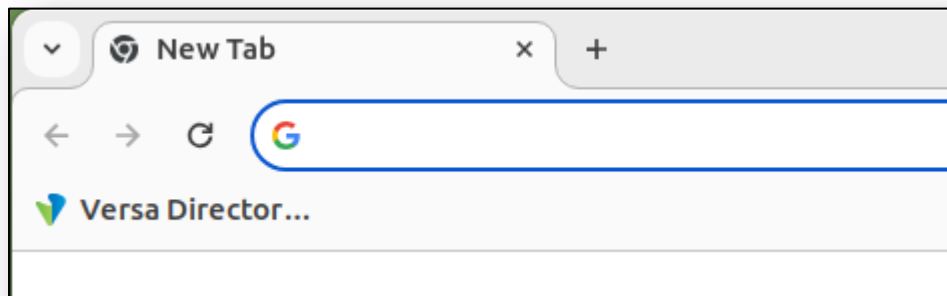
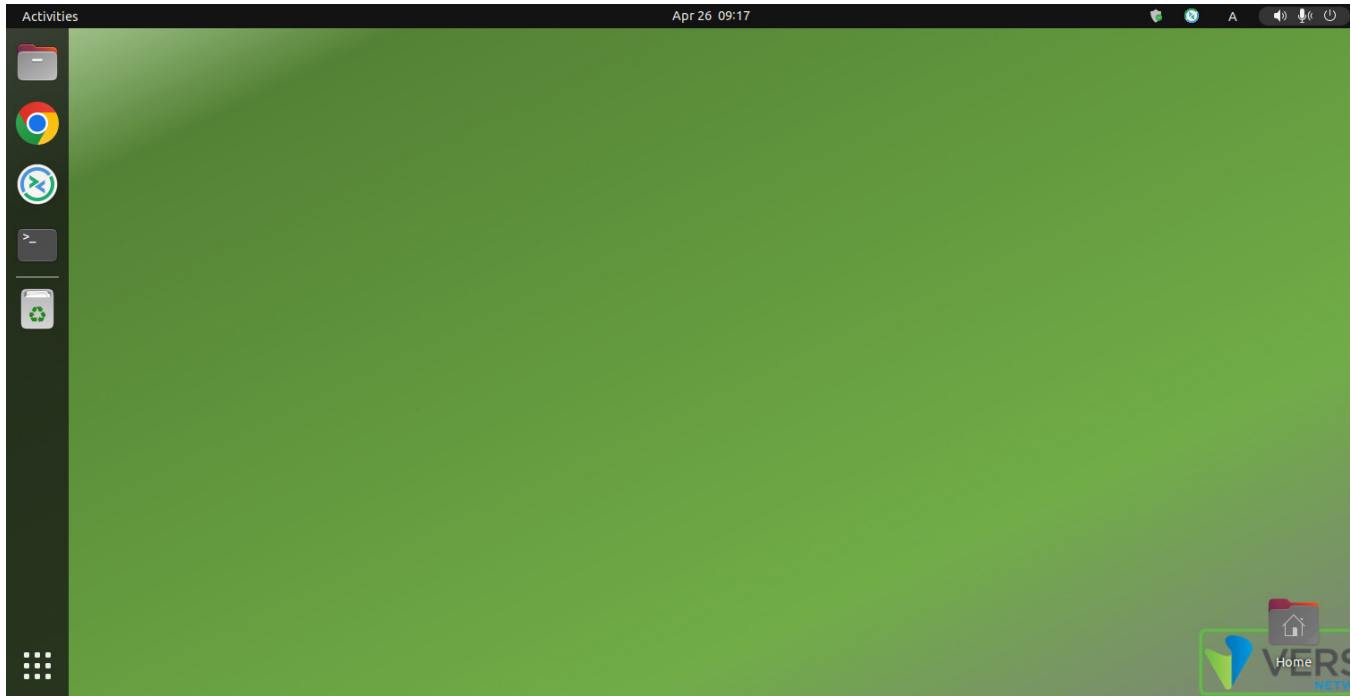


- b. Enter the registration code provided by your instructor, then click Register.
- c. Once registered, click the Sign In button to log into the workspace and start the remote desktop session.



- d. Open *Google Chrome* on the remote desktop.

On the remote desktop, locate and double-click the *Google Chrome* icon on the desktop to start the browser. You can start the browser from the icon on the desktop or from the icon on the task bar.

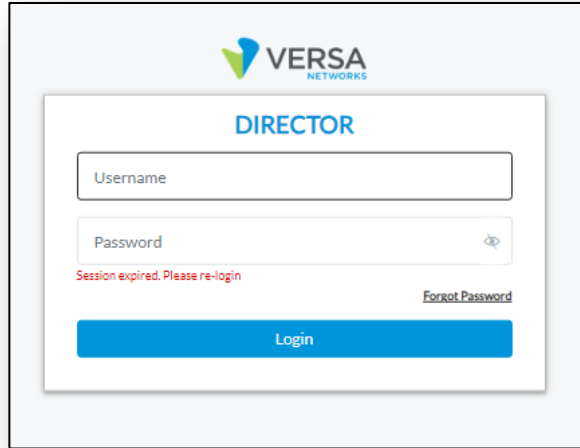


There may be a bookmark in the remote browser window. If there is a bookmark, use the bookmark to connect to Versa Director. If there is not a bookmark, the IP address of Versa Director is 10.27.1.10.

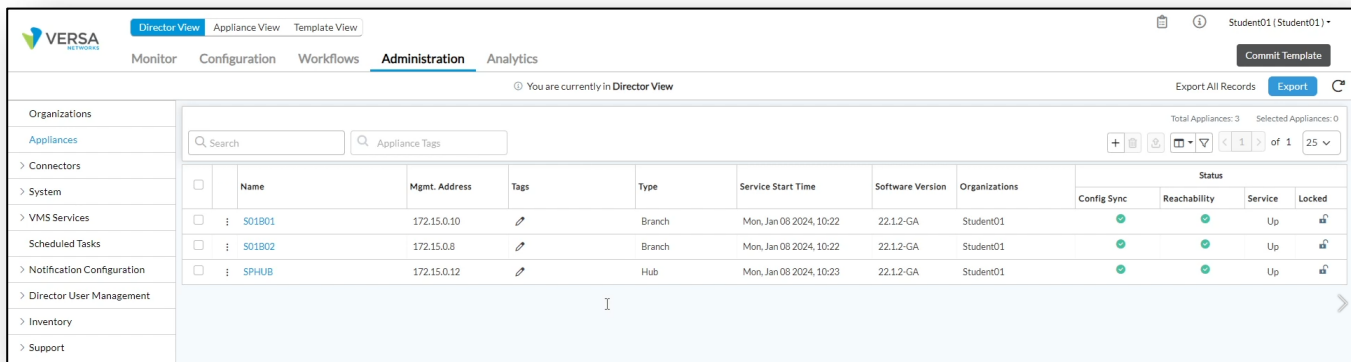
Step 2.

a. Log Into Versa Director

Log into Versa Director with the username and password provided by the instructor. The default login is your student ID (e.g. Student01, Student02, Student03, etc.) with the password *Versa@123*.

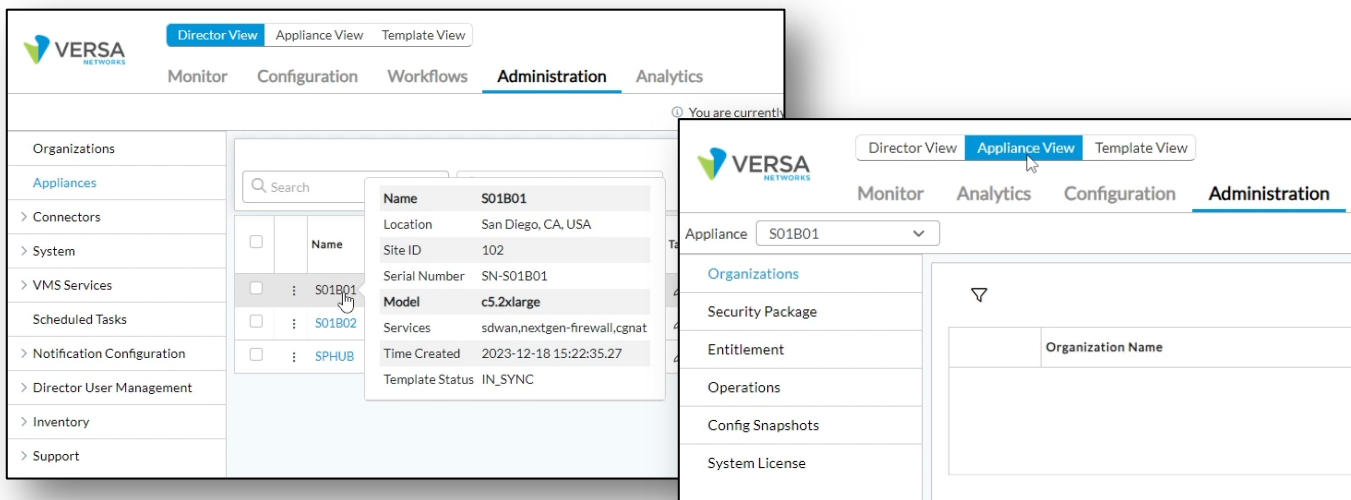


You should be placed on the *Administration > Appliances* dashboard, where the appliances in your organization are displayed.



b. Open your Branch01 device (B01)

In the *Administration > Appliances* tab, locate your SxxB01 branch device (where Sxx is your tenant ID assigned by your instructor.)

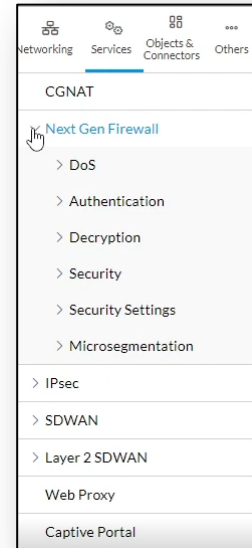
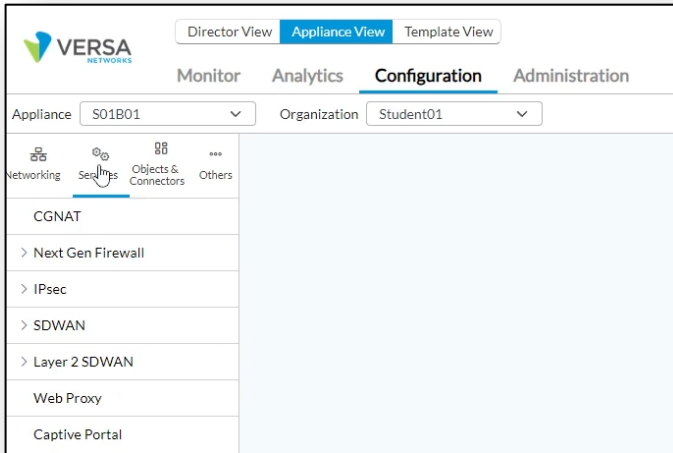


- c. Verify the security services enabled on the device.

Open the *Configuration > Services* dashboard to view the type of security services that are enabled on the device. You should see that *Next Gen Firewall* is the security service available on this device.

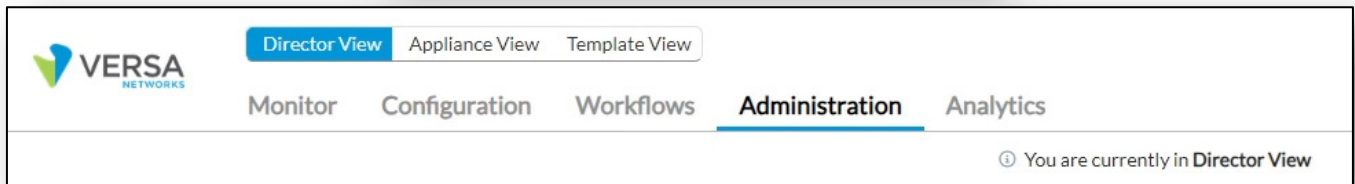
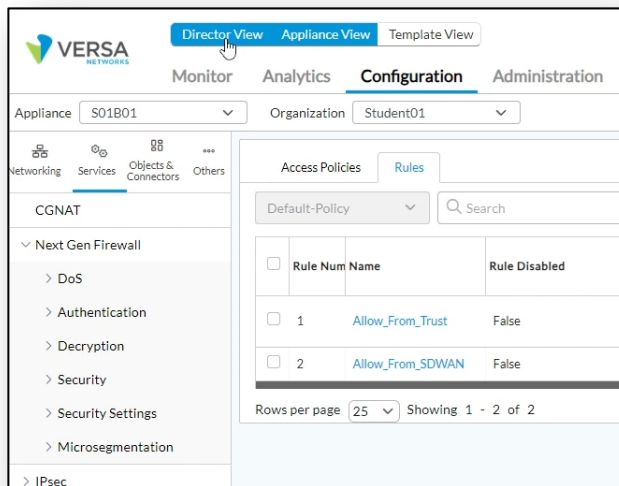
- d. Expand the *Security* services menu.

Click on the arrow next to Next Gen Firewall to expand the list of services currently available on the device.



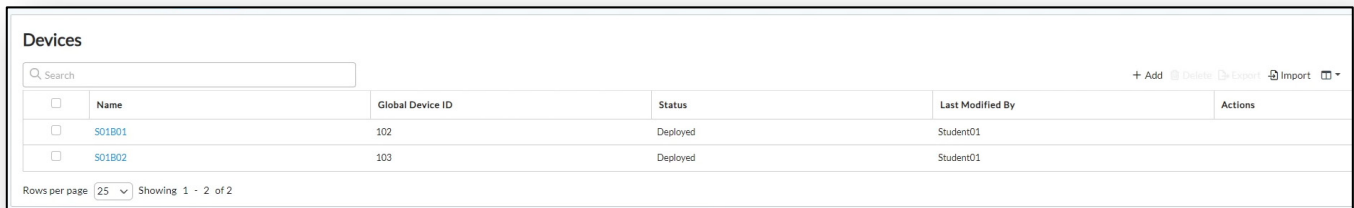
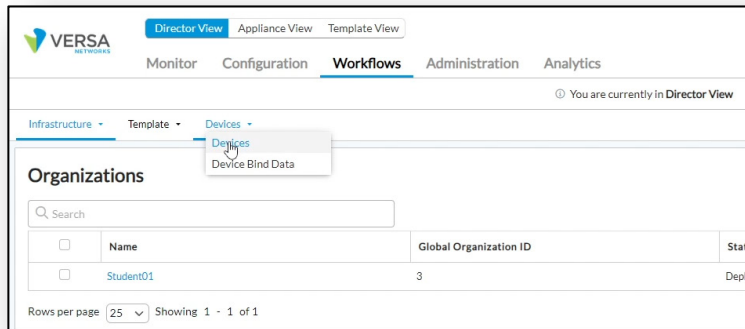
- e. Click the *Director View* button to exit *Appliance View* and return to *Director View*.

To exit appliance mode, click on the *Director View* tab. This will take you back to the main view that allows you to perform centralized management tasks. Note how the top menu bar changes when you change back to Director view.



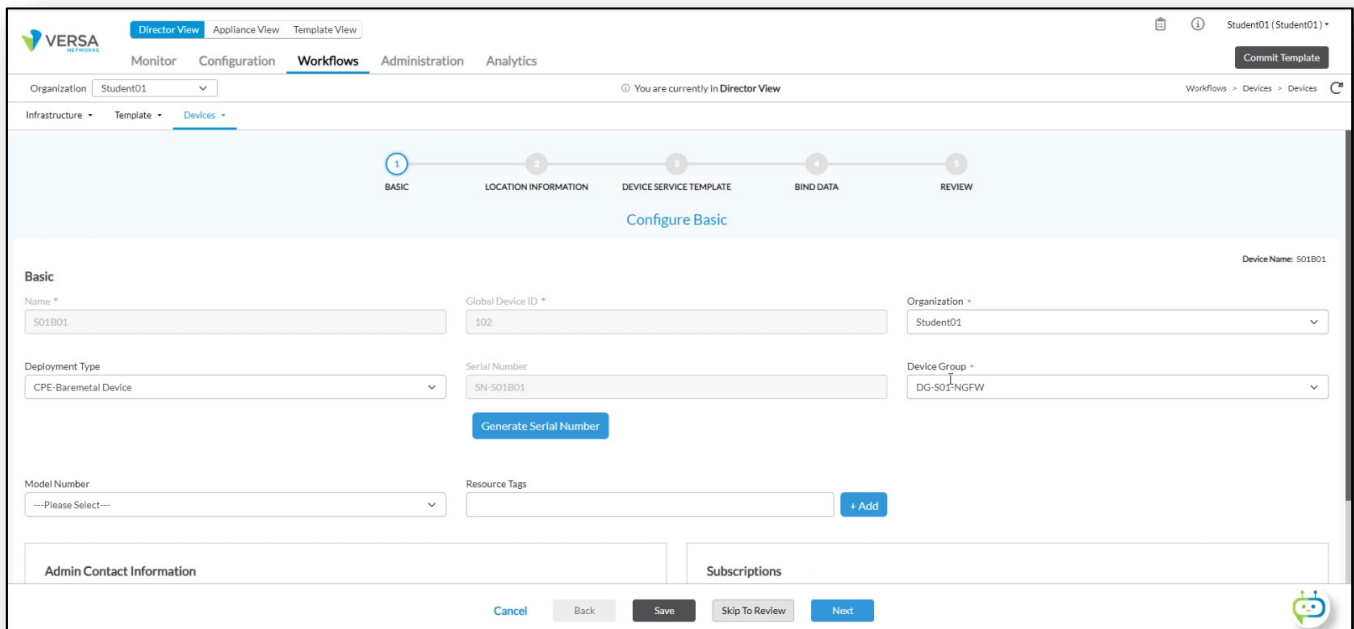
Step 3. View the Device Workflows

- a. From Director View, navigate to *Workflows > Devices > Devices* to view the device workflows that have been created in Versa Director.



- b. View the Branch B01 Device Workflow.

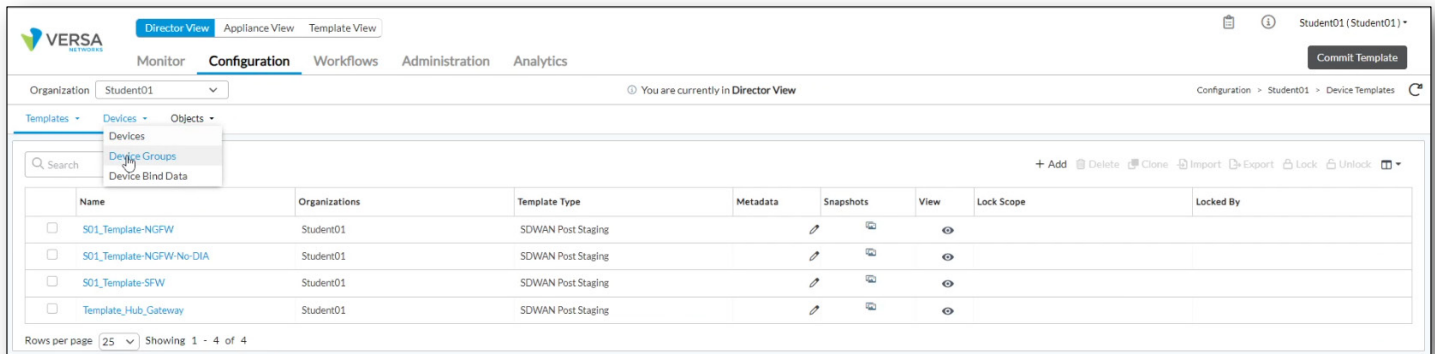
Click on the workflow associated with Branch 01 (B01)



The workflow has a set of steps that are designed to walk you through the process of defining a device. These steps are: *Basic > Location Information > Device Service Template > Bind Data > Review*. For this lab, we will focus on the *Basic* tab, as that is where the device group association is configured. The device should be associated with the *DG-Sxx-NGFW* device group, as shown.

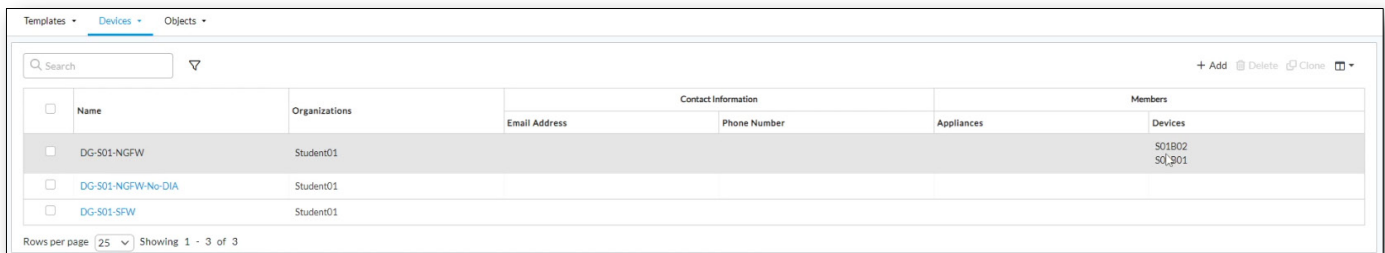
Step 4. View the Configuration database

- a. Navigate to the Configure dashboard to view the configuration components stored in Versa Director.
- b. In the Configuration dashboard, navigate to *Devices > Device Groups* to view the configured device groups.



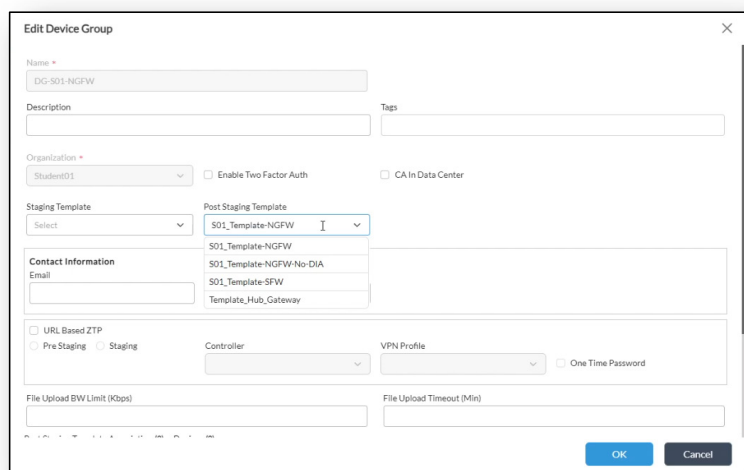
The device groups are displayed. The devices that are associated with each device group are displayed on the right-hand side. You can see that both devices are assigned to the *DG-Sxx-NGFW* device group.

Note: Although you can re-assign devices to different device groups within the configuration dashboard, the re-assignment of a device to a different device group does NOT change the device group assignment within the device workflow. It is recommended to make device group assignments through the corresponding device workflow to maintain consistency.



Click on the DG-Sxx-NGFW device group to see its properties.

Within the device group, locate the Post Staging Template drop-down menu. The device group is linked to the *Sxx_Template_NGFW* device template.



- c. Click Cancel to close the device group window.

Step 5. Create a new template using a Template Workflow

- a. Navigate to *Workflows > Template > Templates* dashboard to view the device template workflows that were used to create the existing device configuration templates.

Organization: Student01

Infrastructure > Template > Devices

Dropdown menu: Templates (selected), Application Steering, Spoke Groups, Service Chains

	Name	Global Device ID
<input type="checkbox"/>	S01B01	102
<input type="checkbox"/>	S01B02	103

Rows per page: 25 Showing 1 - 2 of 2

- b. Add a new Template Workflow

In the *Template Workflow* dashboard, click the + Add button to create a new template workflow. Name the new workflow *Sxx-Template-New*, where Sxx is the student ID that was assigned to you.

Organization: Student01

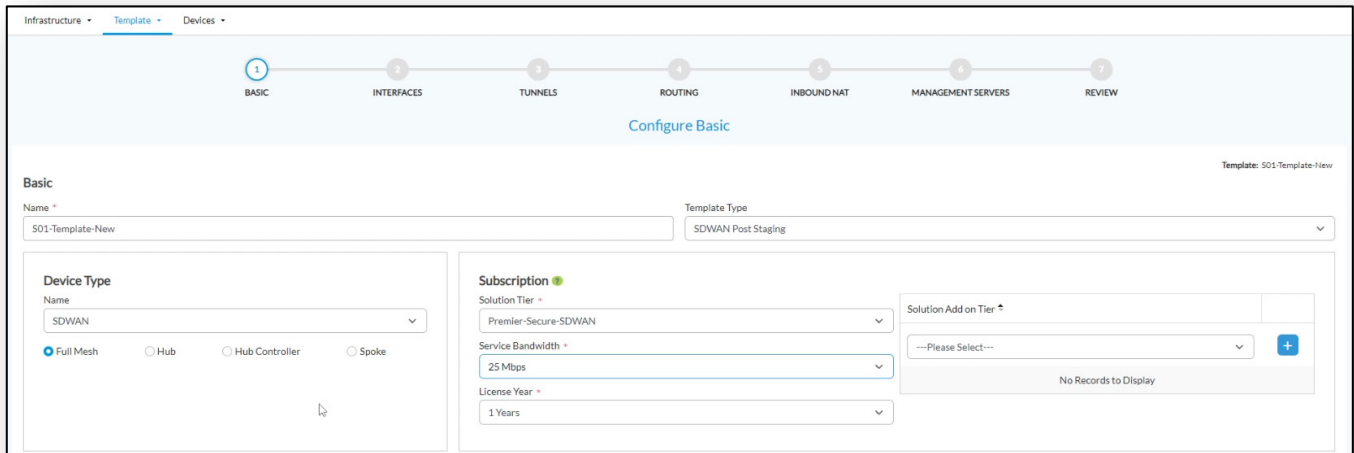
Infrastructure > Template > Templates

Buttons: + Add, Commit Template

	Name	Status	Last Modified Date	Last Modified By	Actions
<input type="checkbox"/>	S01_Template-NGFW	Deployed	2024-01-08 22:34:35	Administrator	
<input type="checkbox"/>	S01_Template-NGFW-No-DIA	Deployed	2024-01-09 23:02:00	Administrator	
<input type="checkbox"/>	S01_Template-SFW	Deployed	2024-01-03 17:24:52	Administrator	

Rows per page: 25 Showing 1 - 3 of 3

c. Assign the Name, Solution Tier, and Service Bandwidth as shown:



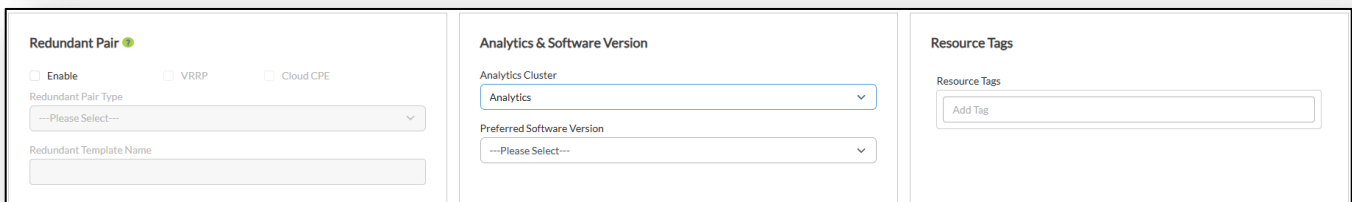
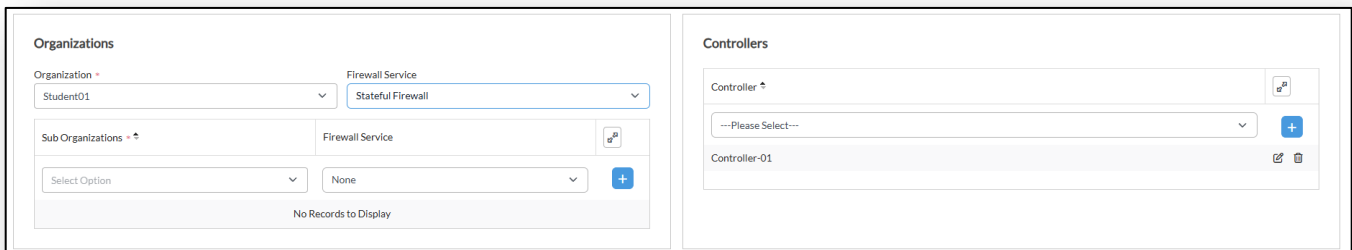
d. Set the Organization and Firewall Services

Scroll down to the *Organizations* box and select your organization (student number) in the drop-down menu, then select *Stateful Firewall* in the *Firewall Services* drop-down menu.

When you select the organization, the list of controllers available to that organization automatically populate in the *Controllers* dialog next to the *Organizations* dialog. You should see *Controller-01* auto-populate in the *Controllers* list.

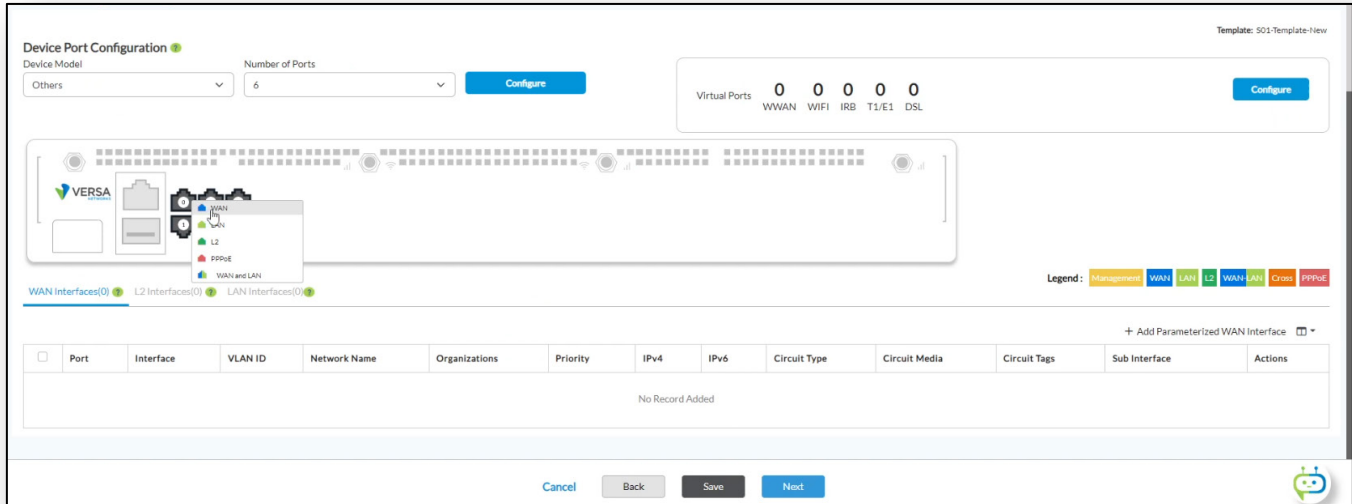
e. Select the Analytics Cluster

Locate the *Analytics & Software Version* box. In the *Analytics Cluster* drop-down, select *Analytics*. This will configure the template to send all statistics and log messages on the VOS devices to the Analytics cluster.



Step 6. Assign Port Roles

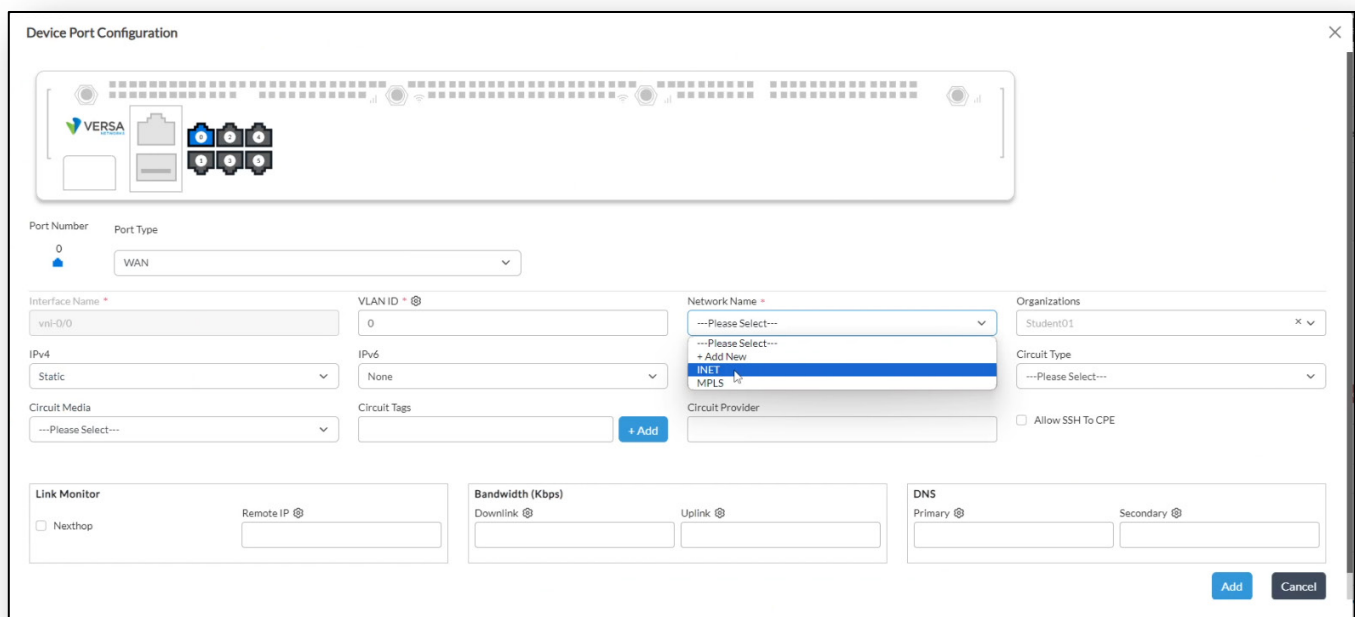
- Click the *Next* button to continue to the *Device Port Configuration* dashboard.
- In the *Device Port Configuration* dialog, you will configure ports 0, 1, and 2. Ports 0 and 1 will be WAN ports, and port 2 will be a LAN port. Click on a port icon to assign the port a role.



c. Assign Port Roles

When a role is assigned to a port, the port configuration dialog appears. Assign the following roles to the ports:

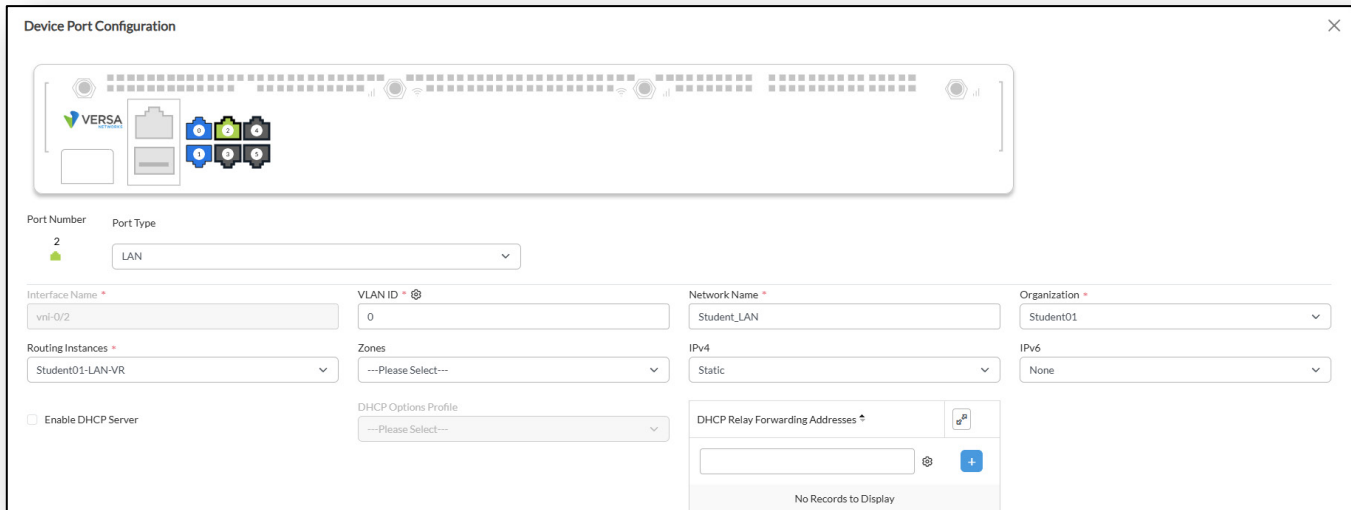
- Port 0: WAN port; Assigned to network INET
- Port 1: WAN port; Assigned to network MPLS
- Port 2: LAN port; Assigned to network Student_LAN



Note: Variables for bind data are created based on the names of the networks. If you use the same network name for the LAN port in all of your sample configurations in the lab, the existing bind data associated with the LAN port will be applied to the LAN port regardless of what template is used. If a template has a different name for the Network name, you will have to re-enter the LAN IP addresses for all of the devices to fill in the new bind-data variable. If you have a question about what the LAN name is, you can cancel the workflow process, open an existing workflow, and copy the LAN network name. Then restart the device template configuration and paste the same network name on the LAN port.

d. Configure the LAN port

The LAN port configuration should associate the LAN port with your student LAN VR (e.g. Student01-LAN-VR, Student02-LAN-VR, etc.). The name of the LAN network should be Student_LAN.



The screenshot shows the 'Device Port Configuration' window with the following settings:

- Port Number: 2
- Port Type: LAN
- Interface Name: vni-0/2
- VLAN ID: 0
- Network Name: Student_LAN
- Organization: Student01
- Routing Instances: Student01-LAN-VR
- Zones: ---Please Select---
- IP4: Static
- IPv6: None
- Enable DHCP Server:
- DHCP Options Profile: ---Please Select---
- DHCP Relay Forwarding Addresses: (Empty list)

e. Verify the port role configuration

Verify the final port role configuration. Your results should resemble the below configuration examples.

Port	Interface	VLAN ID	Network Name	Organizations	Priority	IPv4	IPv6	Circuit Type	Circuit Media	Circuit Tags	Sub Interface	Actions
<input type="checkbox"/>	0	vni-0/0	0	INET		Static					+Add Sub Interface	
<input type="checkbox"/>	1	vni-0/1	0	MPLS		Static					+Add Sub Interface	

WAN Ports

Port	Interface	VLAN ID	Network Name	Organization	Zones	Routing Instance	IPv4	IPv6	Sub Interface	Actions
<input type="checkbox"/>	2	vni-0/2	0	Student_LAN	Student01	Student01-LAN+VR	Static		+Add Sub Interface	

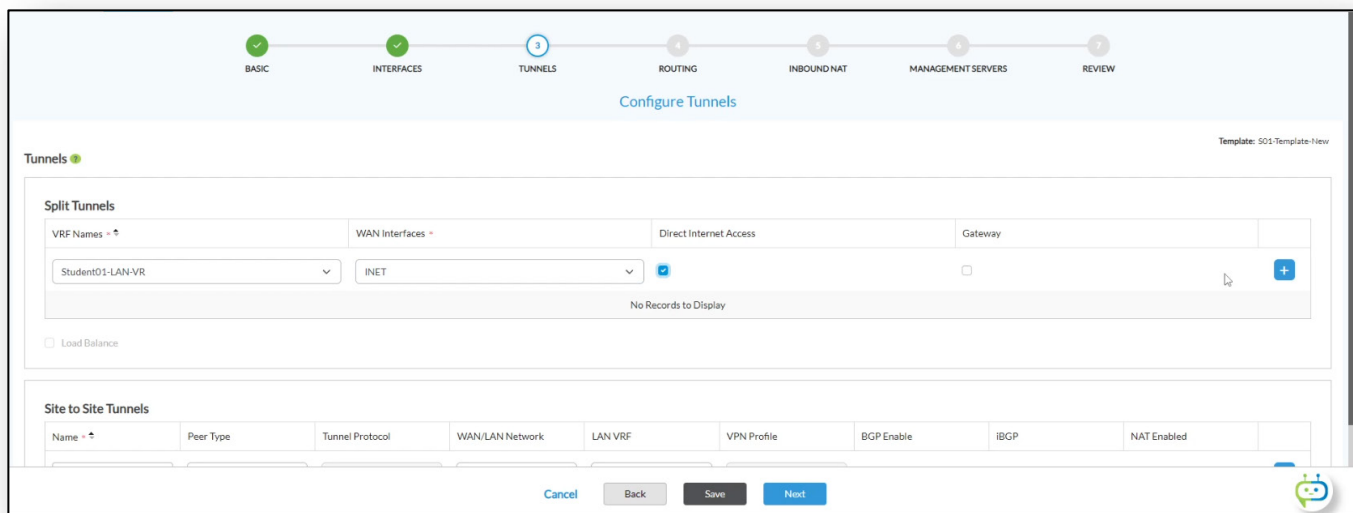
LAN Port

Step 7. Create a DIA connection in the Tunnels dashboard

- a. Click the *Next* button to continue to the *Tunnels* dialog.
- b. In the *Tunnels* dialog, locate the *Split Tunnels* section. The Split Tunnels section allows you to create a bridge between a LAN VRF and a WAN Virtual Router.
- c. Bridge the LAN VRF to the INET WAN

To create a DIA bridge between the INET WAN and the LAN VRF:

- Select the *StudentXX-LAN-VR* from the VRF Names drop-down.
- Select *INET* in the WAN Interfaces drop-down.
- Mark the *Direct Internet Access* check box
- Click the blue + button on the far right

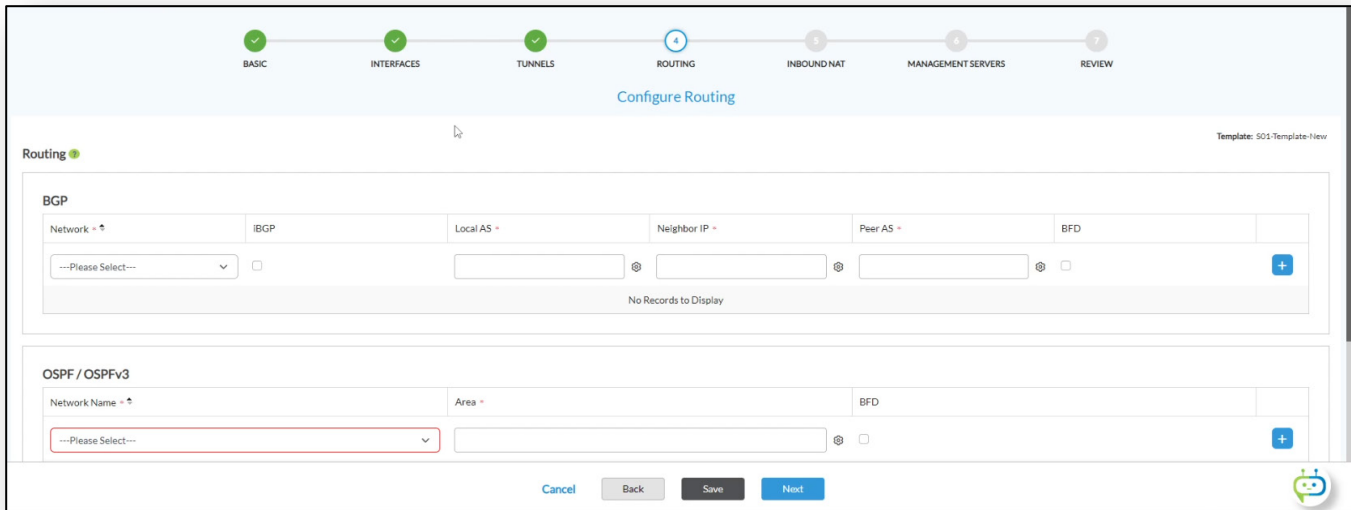


Step 8. Examine the Routing Dialog

- a. Click the *Next* button to continue to the *Routing* dialog.

The Routing dialog allows you to create basic routing protocol configuration within virtual routers. The options are BGP, OSPF, and Static routing. This creates a basic routing configuration and basic policies to advertise locally learned routes to the SD-WAN, and SD-WAN learned routes into the routing protocols that are configured here. While the Workflow routing protocol configuration is basic, once the protocols are configured you can modify the protocol configuration within the device template for more advanced configurations.

Do not configure any routing protocols in this lab.

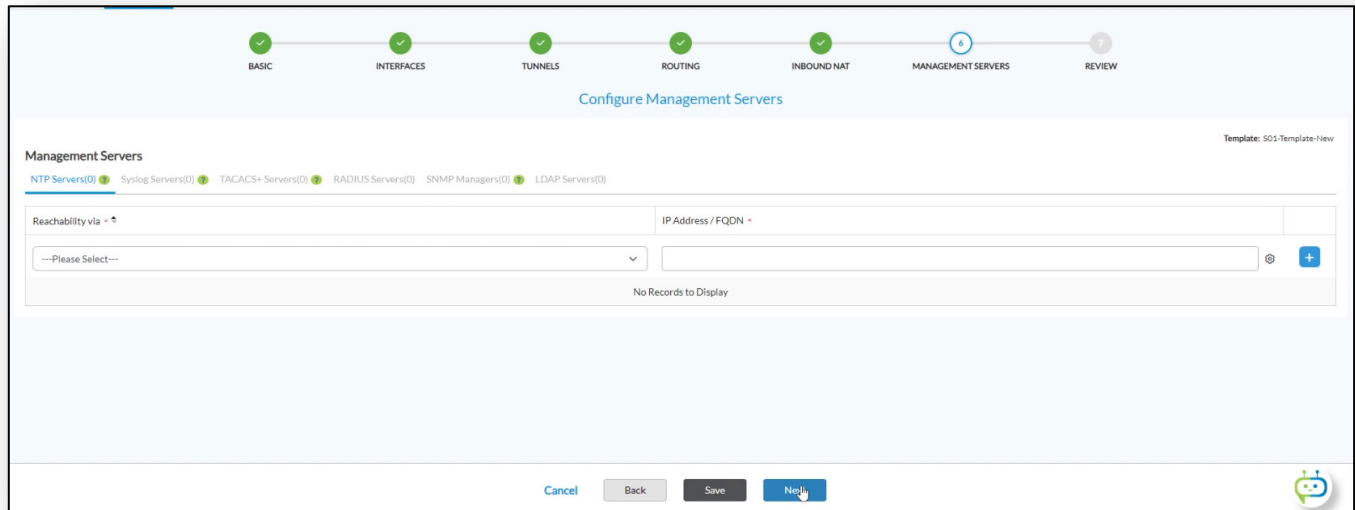


The screenshot displays the 'Configure Routing' dialog box. At the top, a progress bar indicates the current step is 'ROUTING' (step 4), with previous steps 'BASIC', 'INTERFACES', and 'TUNNELS' completed, and subsequent steps 'INBOUND NAT', 'MANAGEMENT SERVERS', and 'REVIEW' pending. The main area is titled 'Routing' and contains two sections: 'BGP' and 'OSPF / OSPFv3'. The 'BGP' section has fields for 'Network', 'IBGP', 'Local AS', 'Neighbor IP', 'Peer AS', and 'BFD'. The 'OSPF / OSPFv3' section has fields for 'Network Name' and 'Area'. At the bottom of the dialog, there are buttons for 'Cancel', 'Back', 'Save', and 'Next'. A chatbot icon is visible in the bottom right corner.

Step 9. Examine the Inbound NAT dialog

- a. Click the *Next* button to navigate to the *Inbound NAT* dialog.

The *Inbound NAT* dialog allows you to configure static inbound (destination) NAT, which can be useful if you have internal resources that must be made available to public networks. Inbound traffic will be translated to the private IP address specified.

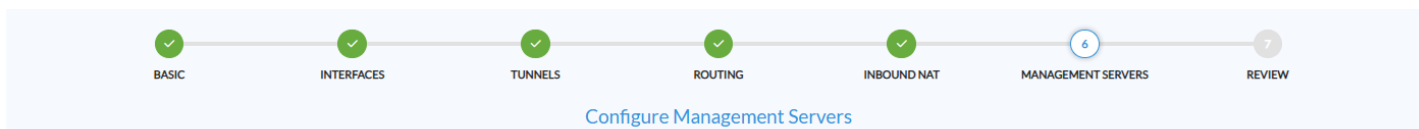


Do not configure any Inbound NAT settings.

Step 10. Examine the Management Servers dialog.

- a. Click *Next* to navigate to the *Management Servers* dialog.






The *Management Servers* dialog allows you to configure connections to additional management processes, such as NTP servers, authentication servers, SNMP managers, etc.



Management Servers

Template: S01-Template-New

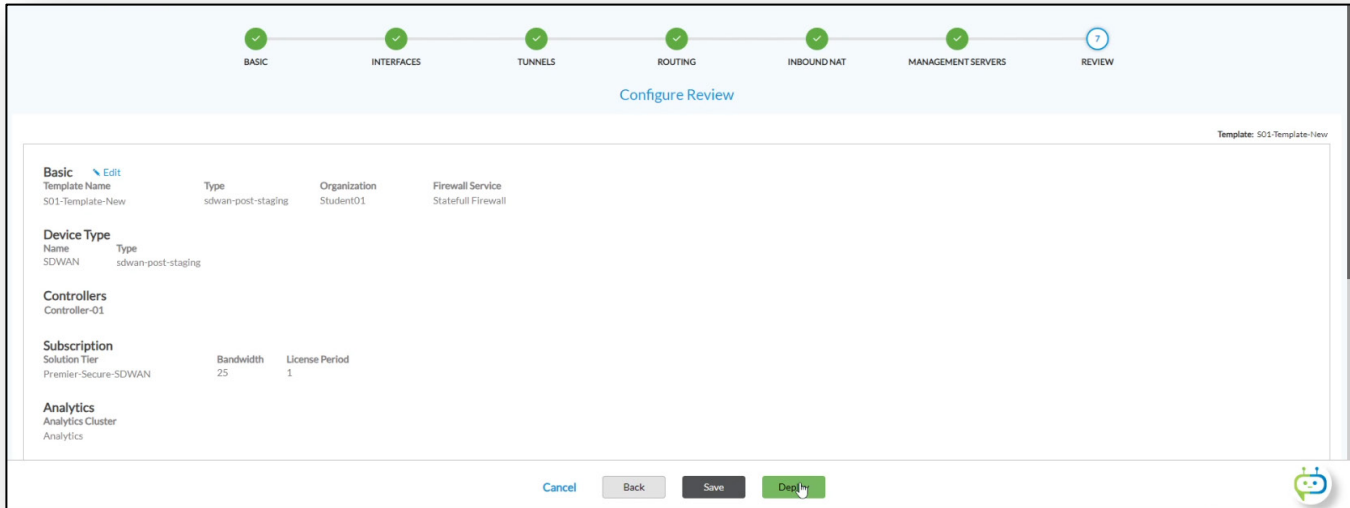
NTP Servers(0) Syslog Servers(0) TACACS+ Servers(0) RADIUS Servers(0) SNMP Managers(0) LDAP Servers(0)

Reachability via 	IP Address / FQDN 	
<input type="text" value="---Please Select---"/>	<input type="text"/>	 
No Records to Display		

Do not configure any management servers settings.

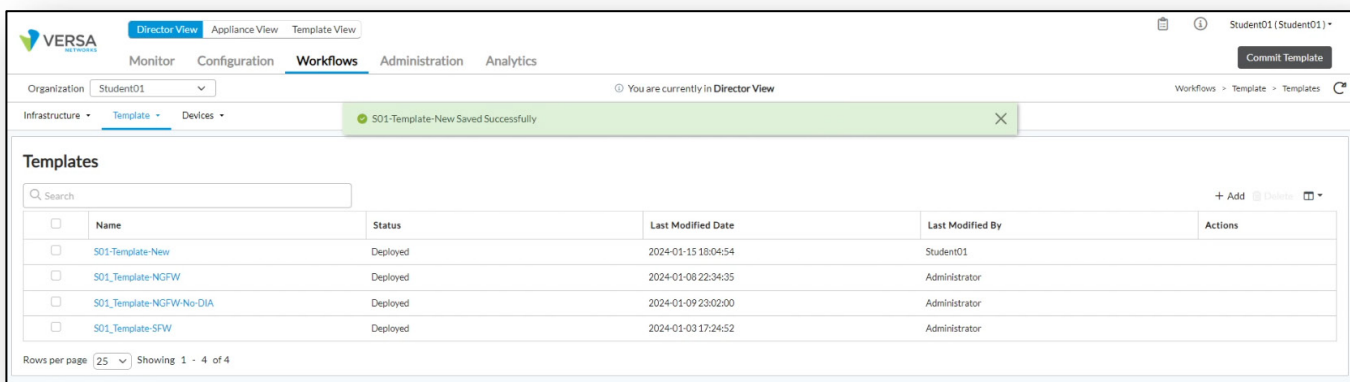
Step 11. Review the Template Workflow and Deploy

- a. Click the *Next* button to navigate to the *Review* window.
- b. The *Review* dialog displays a review of the parameters that have been configured for the template.



Step 12. Deploy the Workflow

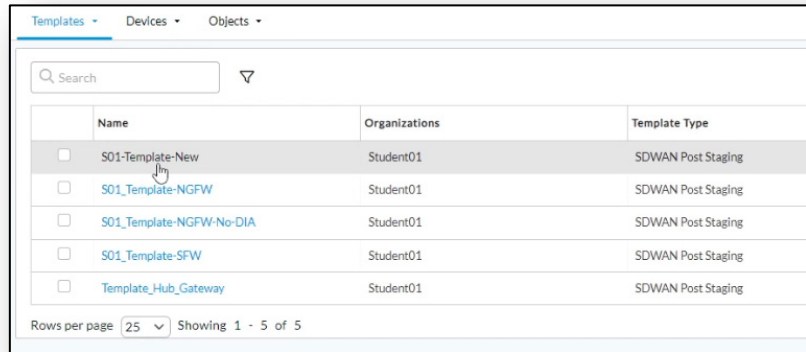
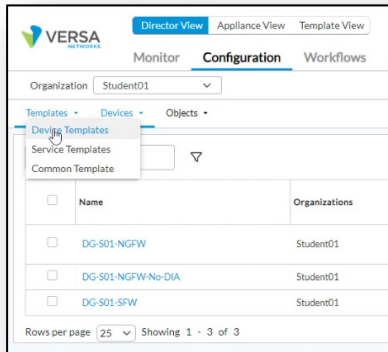
Click the *Deploy* button to save and deploy the workflow. A workflow that has been saved only does not create a corresponding template. A workflow that has been deployed has created a corresponding template.



A deployed workflow appears in the list of template workflows. A workflow can be re-opened to make modifications to a template if needed.

Step 13. Locate the template that was created by the Template Workflow.

- a. Navigate to the *Configuration > Templates > Device Templates* dashboard, then locate the new template that was created by the workflow.



- b. Open the new template.

Click the new template to open the template in Template View.

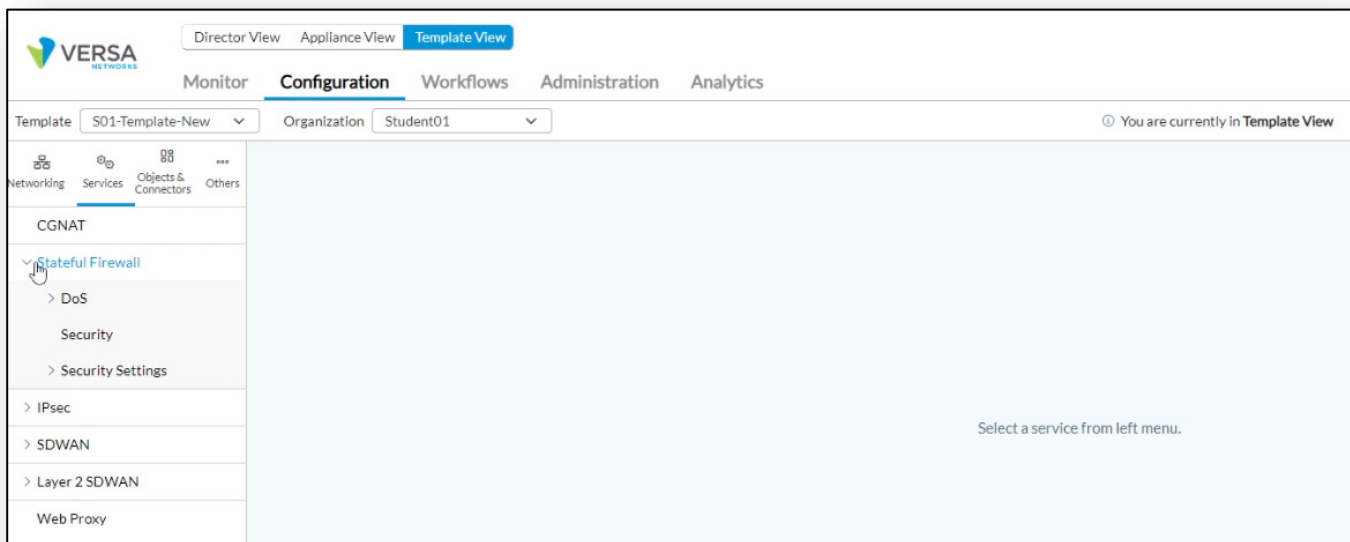
The main view changes to Template View, and the template configuration is displayed.

- c. Navigate to the *Stateful Firewall* services

In the template, click on the *Services* tab on the left side menu. This will display the services configuration hierarchy.

- d. Expand the *Stateful Firewall* service menu

In the *Services* menu on the left side, locate and click on the *Stateful Firewall* menu entry to expand the list of stateful firewall services available in the template.



Step 14. Create a new Device Group

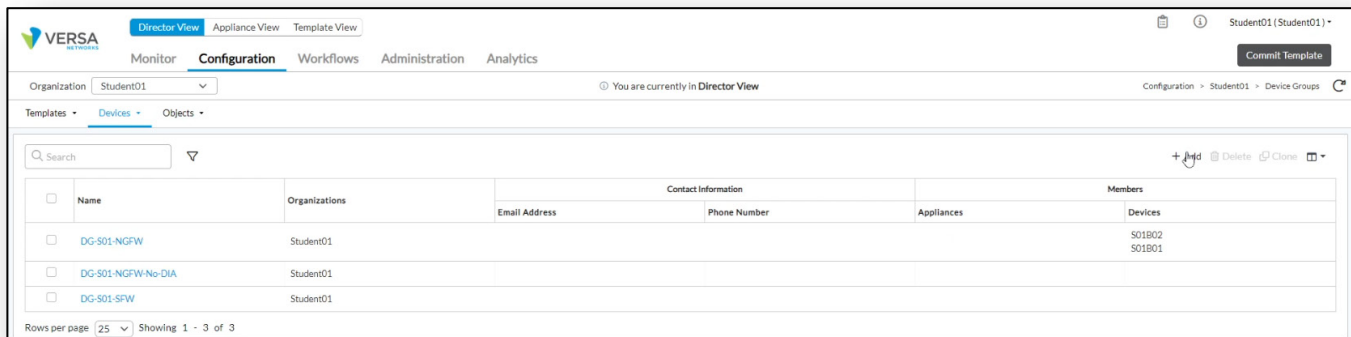
Next you will create a device group that uses the new template.

- a. Switch to *Director View*

Click on the *Director View* button at the top of the window to exit the Template View.

- b. Open the *Device Groups* menu

In Director View, navigate to *Configuration > Devices > Device Groups*. This will display a list of device groups that are pre-configured in the system.



Name	Organizations	Contact Information			Members	
		Email Address	Phone Number	Appliances	Devices	
<input type="checkbox"/> DG-501-NGFW	Student01				S01B02 S01B01	
<input type="checkbox"/> DG-501-NGFW-No-DIA	Student01					
<input type="checkbox"/> DG-501-SFW	Student01					

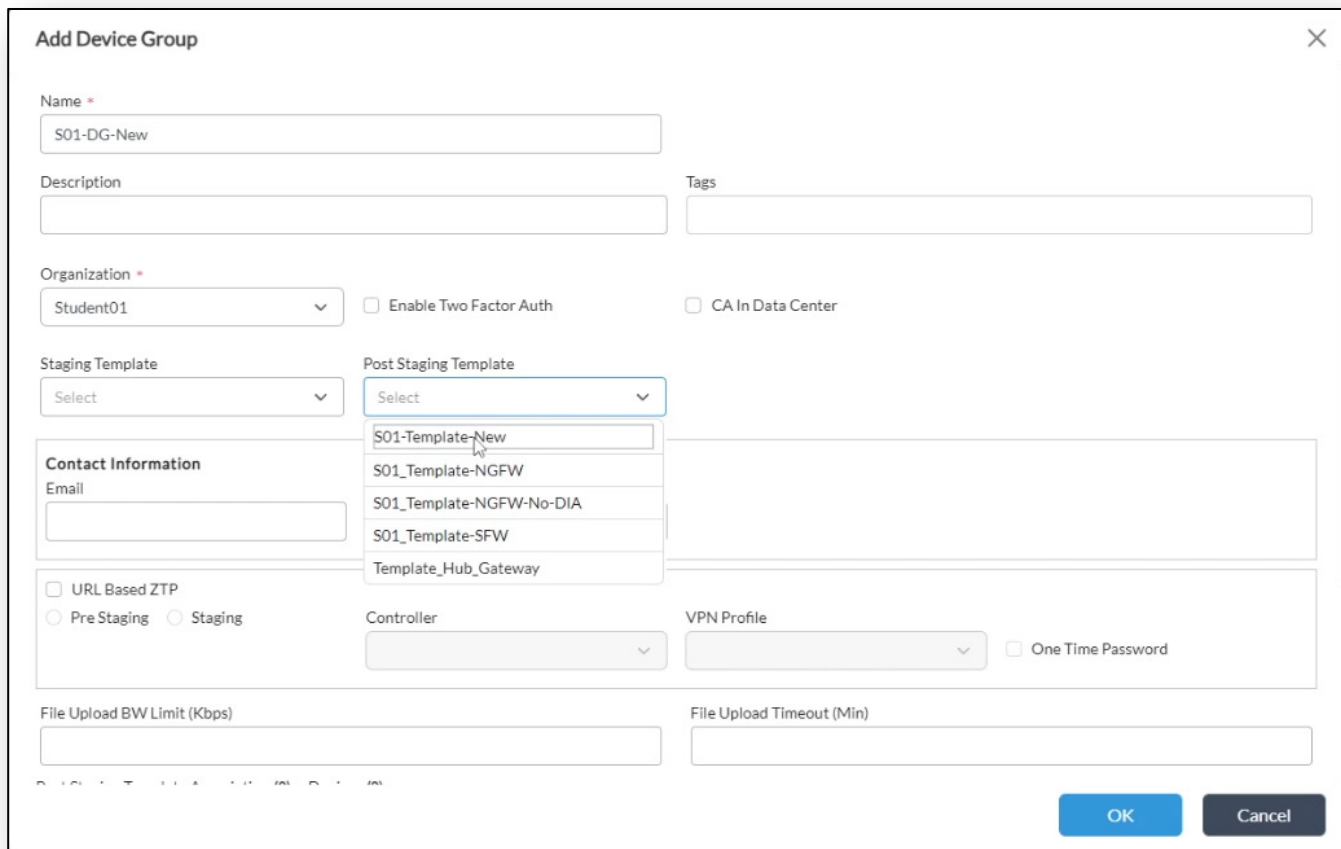
- c. Add a Device Group

Click on the +Add button to create a new device group.

- d. Assign the main template and device group settings

- Provide a name for the new device group based on your student: Sxx-DG-New.
- Select your student ID (organization name) from the Organizations drop-down menu.
- Select the Sxx-Template-New template from the Post Staging Template drop-down menu.

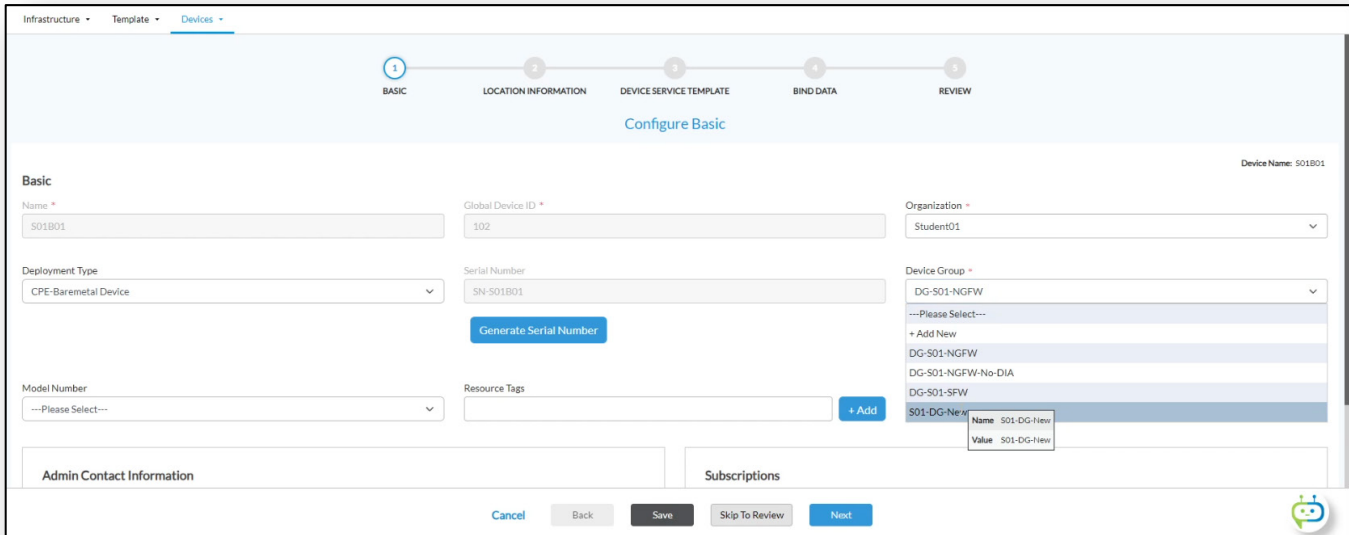
Refer to the image on the following page for an example of the Device Group configuration.



- e. Scroll to the bottom of the device group window. Note that the Sxx-Template-New template is listed as the Main template for the device group. The Datastore template is an organization level template that is automatically applied to all templates in the organization.
- f. Click *OK* to finish creating the device group.

Step 15. Assign your branches to the new Device Group

- Navigate to *Workflows > Devices > Devices*.
- Open the *SxxB01* device workflow.
- In the *BASIC* dashboard, change the Device Group to the *Sxx-DG-New* device group you just created.



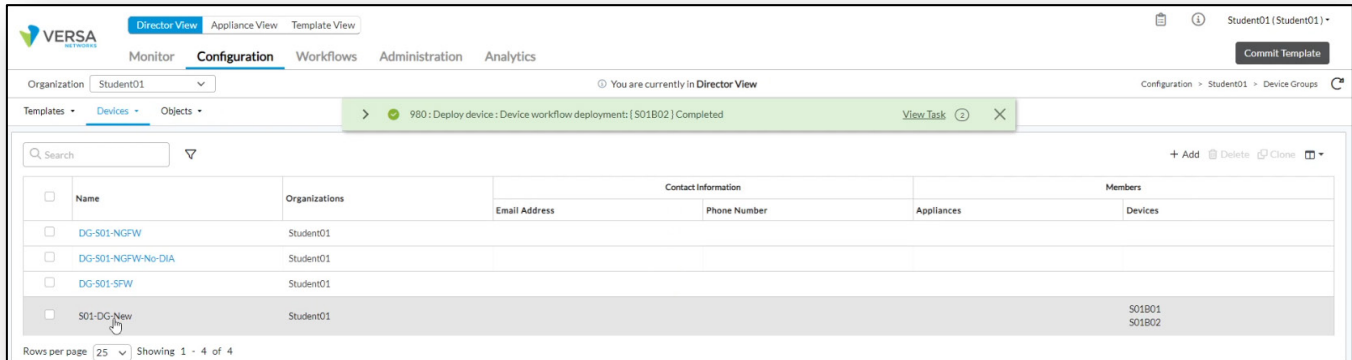
- Click the *Next* button until you reach the Review dashboard.

Note: In the Bind Data tab, ensure that the LAN address is present. If the LAN network name in the new template is different from the LAN name in the previous template, it will require that you re-add the LAN IP addresses to the devices (because the new LAN variable name will be different from the old LAN variable name). If the bind data needs to be re-entered, please notify your instructor for guidance.

- Click the *Re-Deploy* button in the *Review* dashboard to reconfigure the device parameters.
- In the *Device Workflows* window, open the *Sxx_B02* device workflow.
- Repeat steps b, c, d, and e for the S02 device.

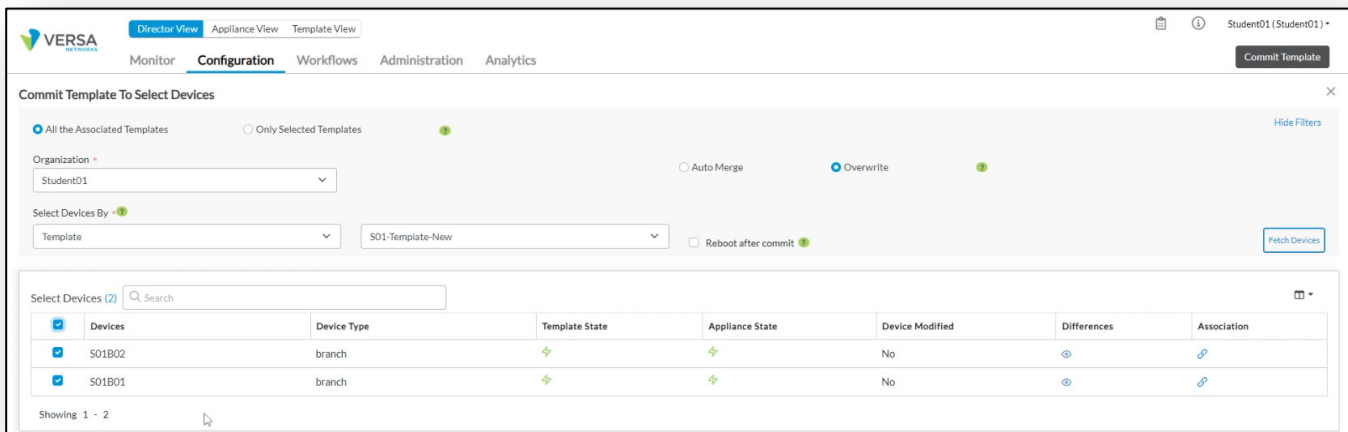
Step 16. Verify the Device Group assignments.

- a. Navigate to the *Configuration > Devices > Device Groups* dashboard.
- b. In the Device Groups dashboard, locate the *Sxx-DG-New* device group. On the right hand side, verify that both of your branches are members of the device group.

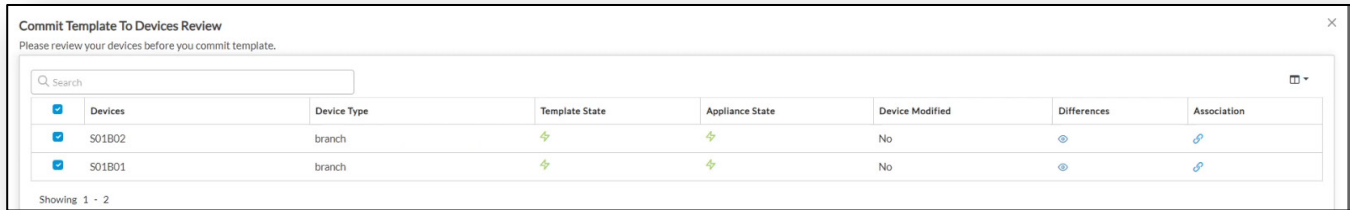


Step 17. Commit the template to the devices

- a. Click the *Commit Template* box in the top right corner of the main dashboard.



- b. In the *Commit Template to Select Devices* dialog, ensure that your organization is listed in the *Organization* drop-down menu.
- c. In the *Select Devices By* box, select *Template*.
- d. In the *Template* drop-down menu, select the new template that you created (e.g. *Sxx-Template-New*).
- e. Click the *Fetch Devices* button to query a list of devices that use the selected template. Your two branch devices should be displayed.



f. Check the boxes next to your two devices.

g. Click the *Review* button.

The review dialog should show that both devices are selected for updates.

h. Click the *Commit* button.

The commit button will recreate the device configurations using the newly assigned template and copy the configurations to the devices.

Step 18. Verify the changes.

a. Navigate to the *Administration > Appliances* dashboard, or click *Appliance View* from the top of the dashboard.

b. Click on your *B01* device to open the device.

c. Open the *Monitor* dashboard

d. In the *B01 Appliance View*, open the *Monitor* dashboard. Open the *System* sub-tab.

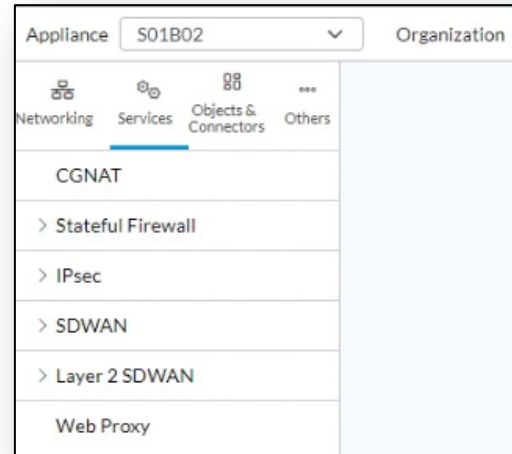
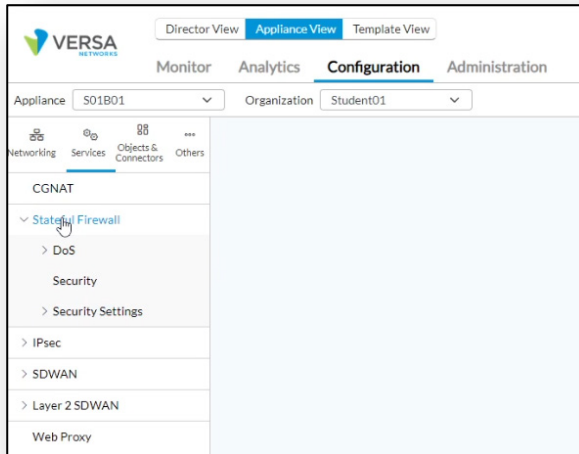
You can view the template association in the System dashboard. You may have to scroll down on the device Monitor dashboard to view the Associate Templates block.



Step 19. Verify the device services configuration

- a. Navigate to *Configuration > Services*

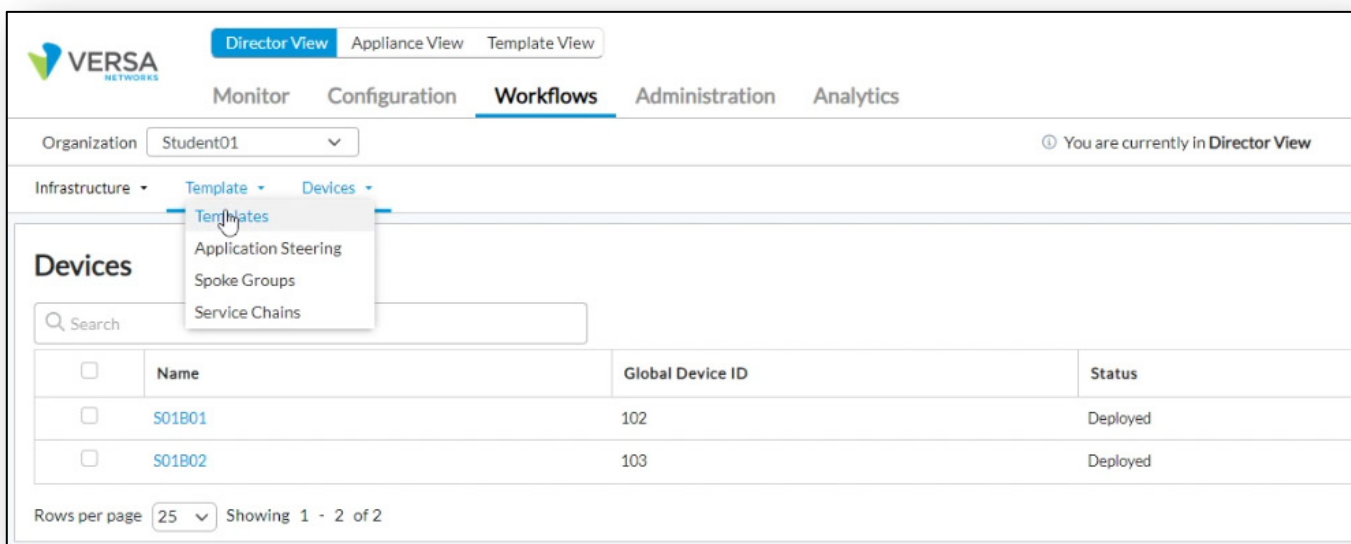
While in Appliance view, click on the *Configuration* tab to view the device configuration. Navigate to the *Services* tab and expand the *Stateful Firewall* item. You can see that the Stateful Firewall services are configurable on the device. If you click on the *Appliance* drop down menu and select the B02 branch, you will see that the services are synchronized on both devices, as they are in the same device group.



Step 20. Clone the new Template Workflow

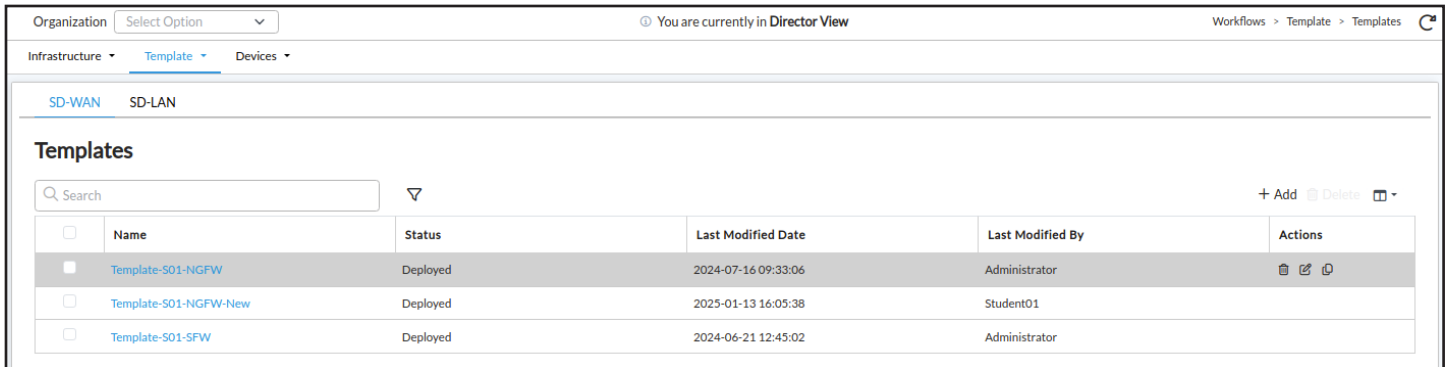
- a. Open the *Configuration > Workflows > Template > Templates* dashboard

Workflows can be cloned, which allows you to create a copy of an existing workflow with a new name. This allows you to create a new workflow and template, with a different name, that inherits the same properties as the original. You can then make adjustments to the properties that you want to change without the requirement of rebuilding the workflow from the beginning.



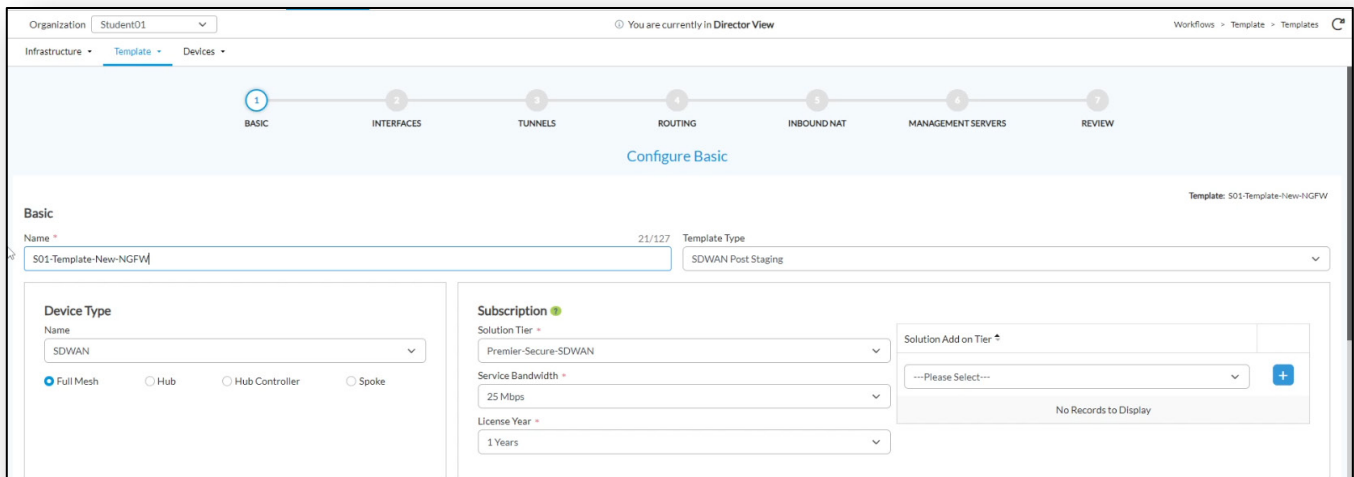
b. Clone the Sxx-Template-New workflow

Mouse over the *Template-Sxx-Template* workflow. Once highlighted, a menu appears on the right side of the row. Click on the *Clone* button to create a clone of the workflow. A new workflow process appears.



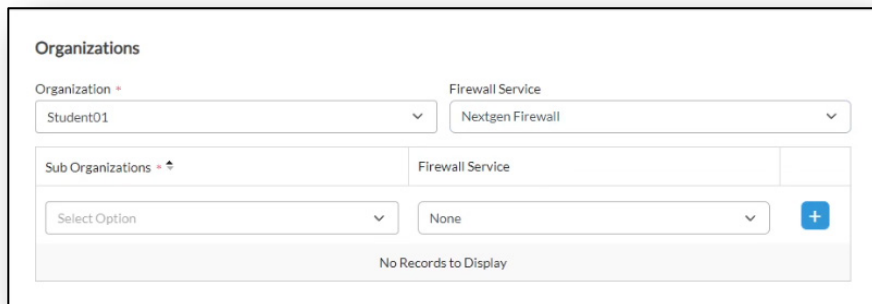
c. Rename the cloned Workflow Template

The new workflow name includes the word *Copy_of_* followed by the original workflow name. Rename the new workflow to *Sxx-Template-New-NGFW*, where *xx* is your student number (e.g. *S01-Template-New-NGFW*).



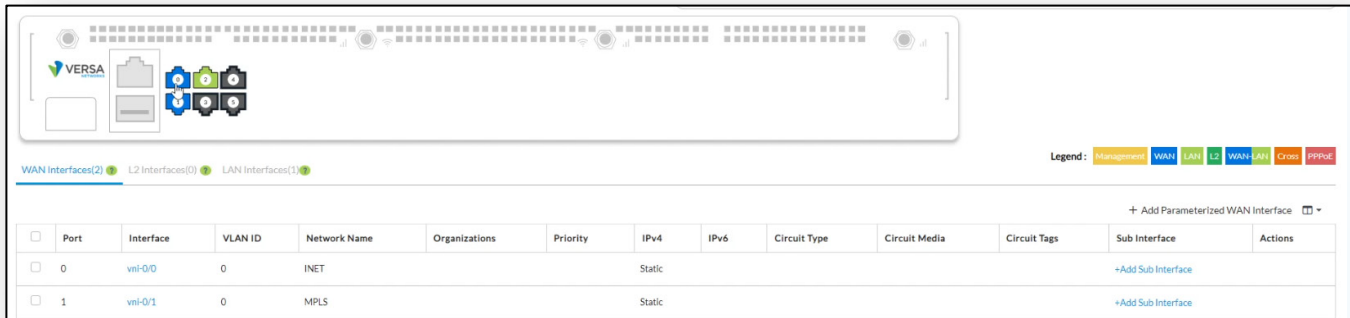
d. Change the enabled firewall service

Scroll down to the *Organizations* box and change the *Firewall Service* to *Nextgen Firewall*.



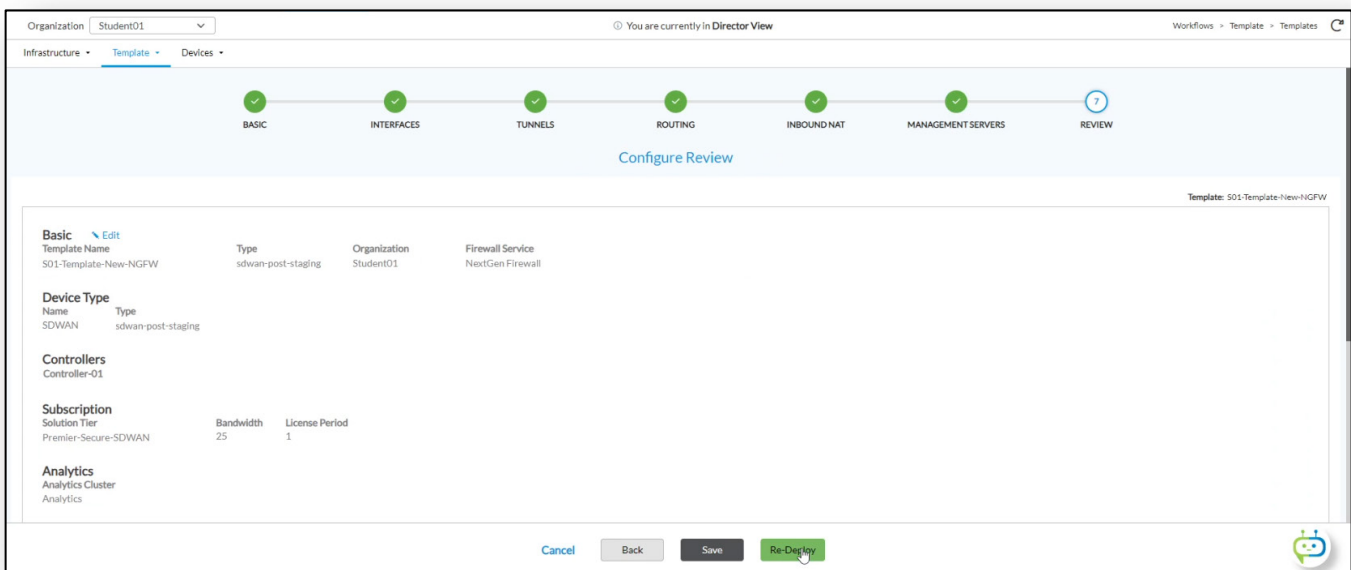
e. View the port configuration

Click the *Next* button to continue to the *Device Port Configuration* dialog. Note that the port information from the original workflow remains, which means you do not have to reconfigure the ports.



f. Deploy the template workflow.

Click the *Next* button until you reach the *Review* dashboard. In the *Review* dashboard, click the *Re-Deploy* button to deploy the new workflow and create the new template.



g. Verify the new template creation

To verify that the workflow clone created a new template, navigate to the *Configuration > Templates > Device Templates* dashboard. You should see your new template in the template table.

Name	Organizations
S01-Template-New	Student01
S01-Template-New-NGFW	Student01
S01_Template-NGFW	Student01
S01_Template-NGFW-No-DIA	Student01
S01_Template-SFW	Student01
Template_Hub_Gateway	Student01

h. Open the new template

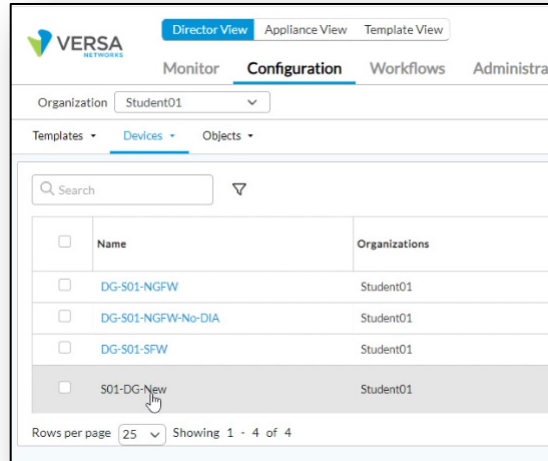
Click on the *Sxx-Template-New-NGFW* template to open the template.

i. Verify the Next Gen Firewall security settings

Navigate to the *Configuration > Services* dashboard. The Next Gen Firewall services are configurable in the new template.

j. Return to Director View

Click on the *Director View* button at the top of the dashboard to return to Director View



To use the new template, it has to be assigned to devices in a device group. You will change the new device group you just created so that the template used by the device group is the new NGFW based template.

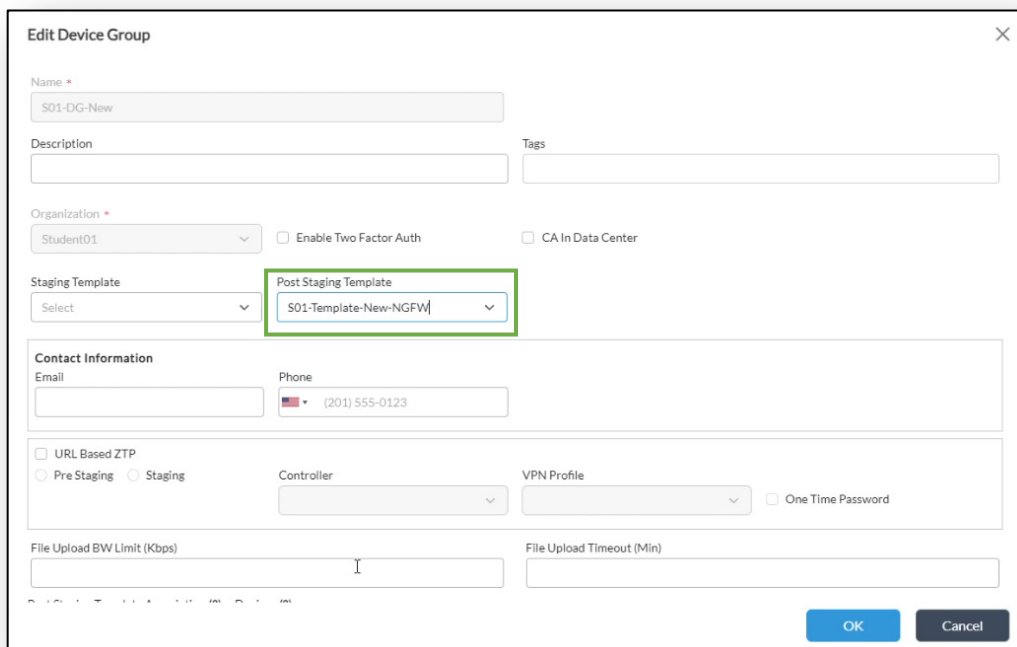
k. Navigate to the Device Group dashboard

Navigate to the *Configuration > Devices > Device Group* dashboard.

l. Open the *Sxx-DG-New* device group

m. Assign the NGFW template to the device group.

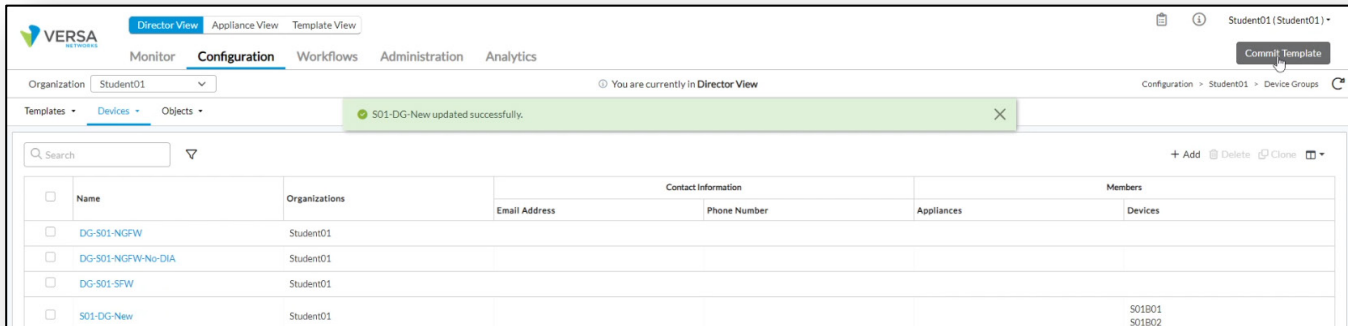
Change the *Post Staging Template* to the new template that you just created with the Clone tool.



- n. Click *OK* to complete the change.

You just changed the post staging template associated with the device group that contains your two devices. It is now time to apply that configuration change.

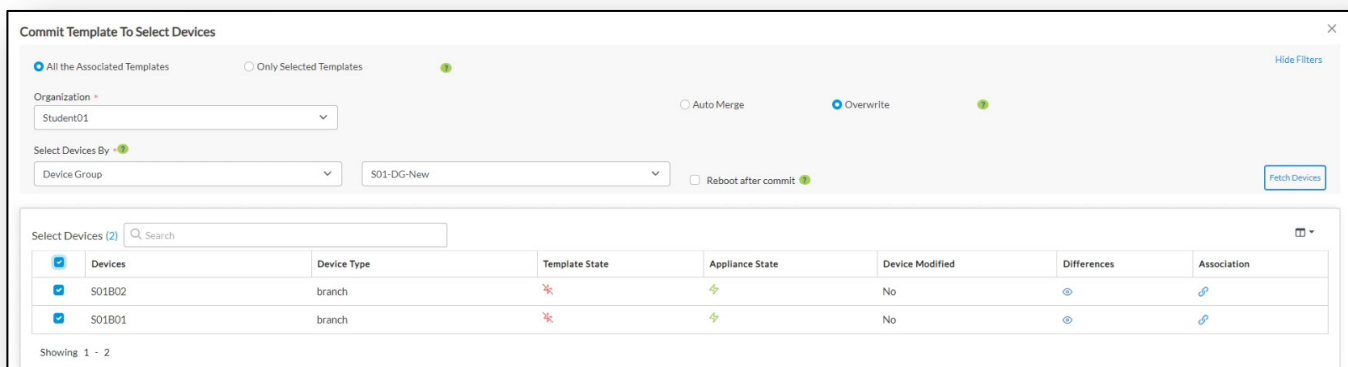
- o. Click the *Commit Template* button



In the *Commit Template* dialog, ensure that your *Studentxx* organization is selected. You can search for devices by device group or by template. In this exercise we will search for devices that are associated with the device group.

- p. Fetch devices based on device group

Select *Device Group* in the *Select Devices By* drop down menu. In the drop down menu next to it, select the *Sxx-DG-New* device group (the device group your devices are members of), then click the *Fetch Devices* button. Your devices should appear in the list.



- q. Commit the changes

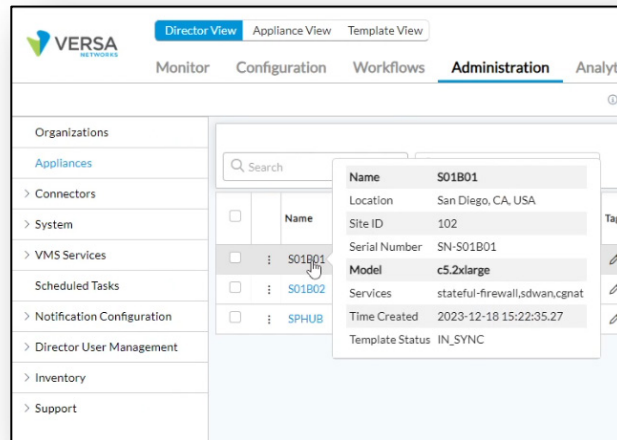
Check the boxes next to your devices, then click the *Review* button at the bottom of the window.

Click the *Commit* button at the bottom of the review window to create new configurations for the devices and apply the configurations to the devices.

Step 21. Verify the configuration changes on the appliances

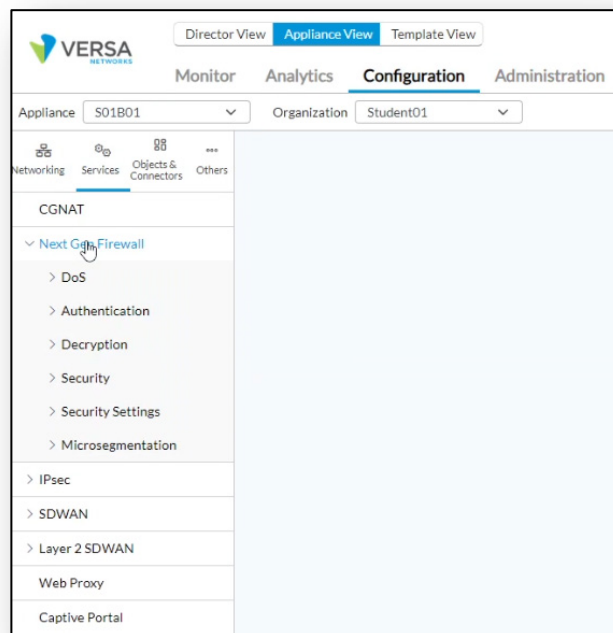
- a. Navigate to the *Administration > Appliances* dashboard and open your B01 appliance.

To verify that the configuration changes have been applied, navigate to *Administration > Appliances* and select the SxxB01 device from the appliance list. Alternatively, click on the Appliance View and select the SxxB01 device from the list. This will open the *Appliance View* of the device.



- b. Verify the Next Gen Firewall services are available

Open the Services menu on the left side menu. Verify that the *Next Gen Firewall* services now appear in the services list of the device configuration.



Step 22. Clone a Template

In the next steps you will clone a template from the *Configuration > Templates* database. This will create a copy of an existing template and it will create a basic Template Workflow associated with the cloned template.

- In Director View, navigate to *Configuration > Templates > Device Templates*.
- From the device templates, locate and click on the box next to the Sxx-Template-New-NGFW template that you previously created. After you check the box next to the template, the actions menu in the top-right of the panel will activate.
- Locate and click on the *Clone* button to create a copy of the template.

Name	Organizations	Template Type	Metadata	Snapshots	View	Lock Scope	Locked By
<input type="checkbox"/> S01-Template-New	Student01	SDWAN Post Staging					
<input checked="" type="checkbox"/> S01-Template-New-NGFW	Student01	SDWAN Post Staging					
<input type="checkbox"/> S01_Template-NGFW	Student01	SDWAN Post Staging					
<input type="checkbox"/> S01_Template-NGFW-No-DIA	Student01	SDWAN Post Staging					
<input type="checkbox"/> S01_Template-SFW	Student01	SDWAN Post Staging					
<input type="checkbox"/> Template_Hub_Gateway	Student01	SDWAN Post Staging					

After you click the *Clone* button, the *Clone Template* dialog will appear. For the purposes of this exercise, you can leave the auto-generated name of the template.

Clone Template ✕

Selected Template Name *

New Template Name *

Redundant Template Name

New Redundant Template Name

Organizations

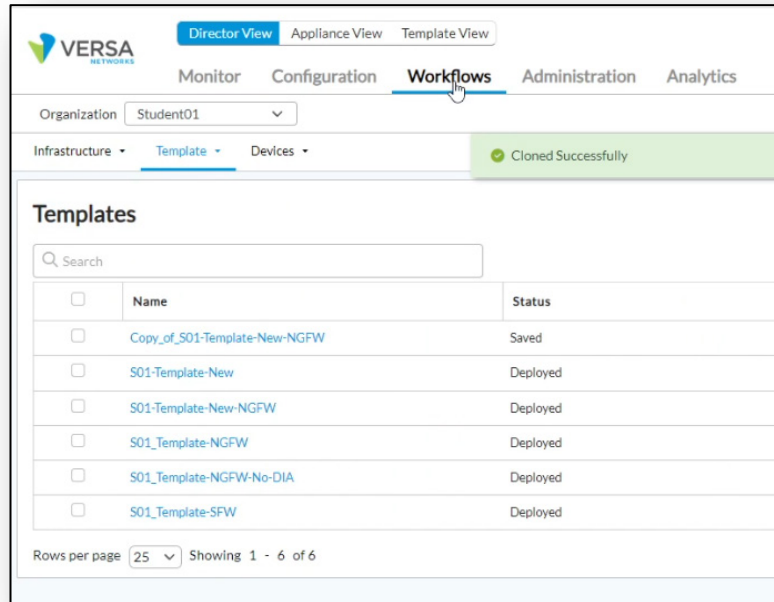
Existing Organizations	New Organizations
Student01	<input type="text" value="Student01"/>
Student01-LAN-VR	<input type="text" value="Student01-LAN-VR"/>

- Click *OK* to create the clone (copy) of the template.

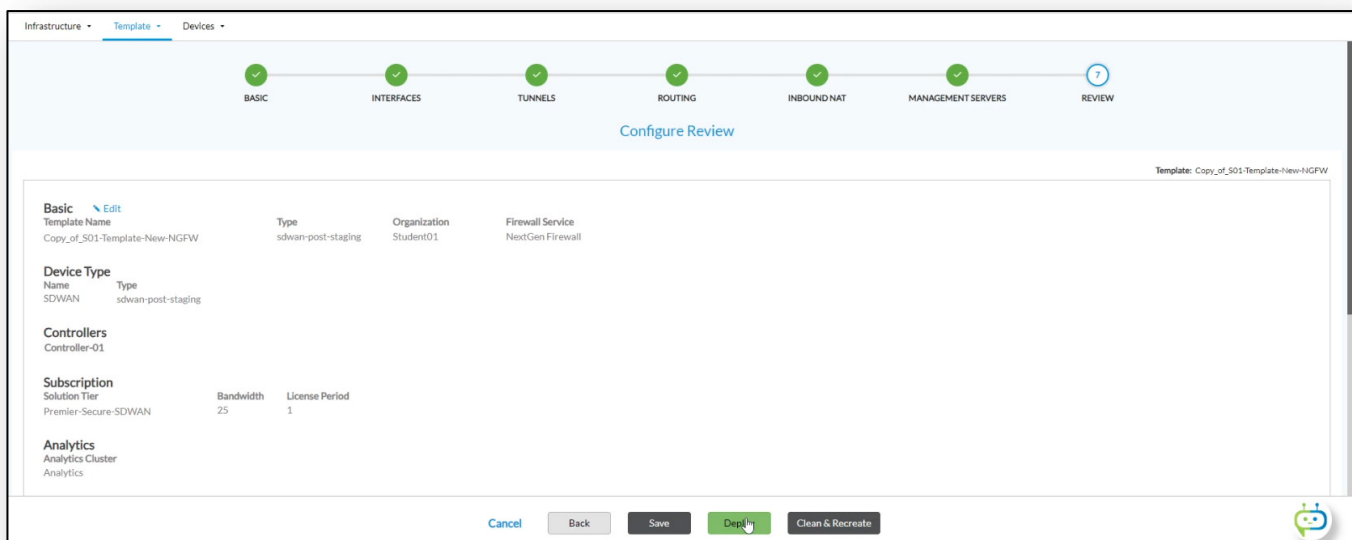
When you create a copy or clone of a template, a corresponding template workflow is created in the Workflows dashboard.

- e. Verify the workflow for the cloned template

Navigate to *Workflows > Template > Templates*. Verify that a workflow has been created with the same name as the cloned template.



It is important to remember the following when cloning workflows and templates. If you clone a workflow, the properties of the workflow are copied, and the template that is created contains those properties. If you clone a template, only the properties of the template that have corresponding workflow properties are copied to the workflow. For example, if you created a template using a workflow and you have modified the template by adding properties such as class of service rules, security rules, or traffic steering rules, the customized properties will be copied to the template, but the workflow will only contain the basic properties that are available to the workflow, so care must be taken when deploying the workflow (use the Deploy option instead of Clean & Recreate when deploying the workflow in the future to prevent erasing custom template properties – unless you intend to erase any customizations in the template and to start with a clean, new template).



DEVICE WORKFLOWS

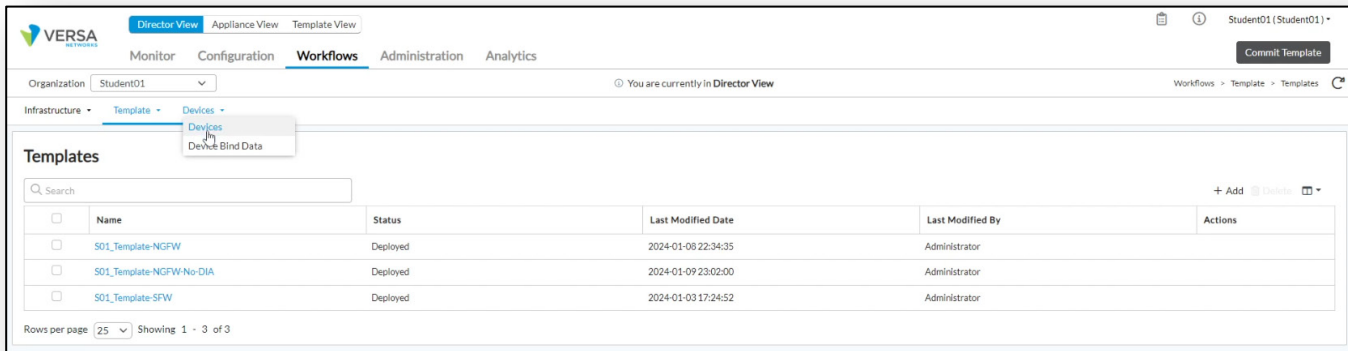
In the next exercises you will create a new device with a device workflow. However, you will not go through the process of onboarding an appliance that references this device.

In this exercise you will:

- Create a device by using a Device Workflow;
- Create a workflow spreadsheet with the workflow Export process;
- Update the exported spreadsheet with information for a new device; and
- Import device workflows from a spreadsheet.

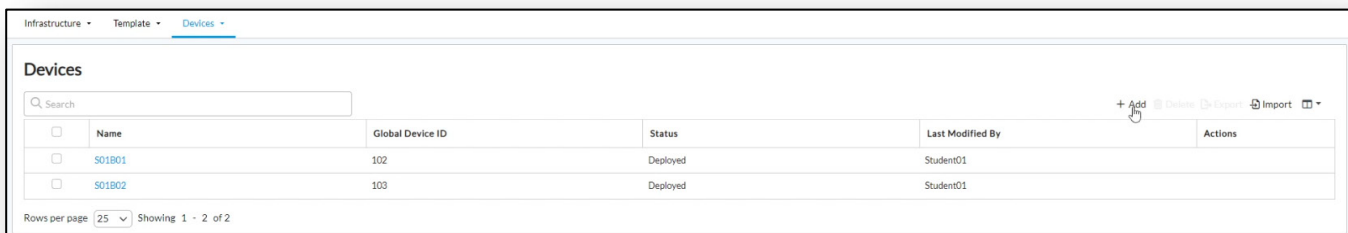
Step 1. Open the Device Workflows dashboard

- In Versa Director navigate to the *Workflows > Devices > Devices* dashboard.



- Create a new Device Workflow

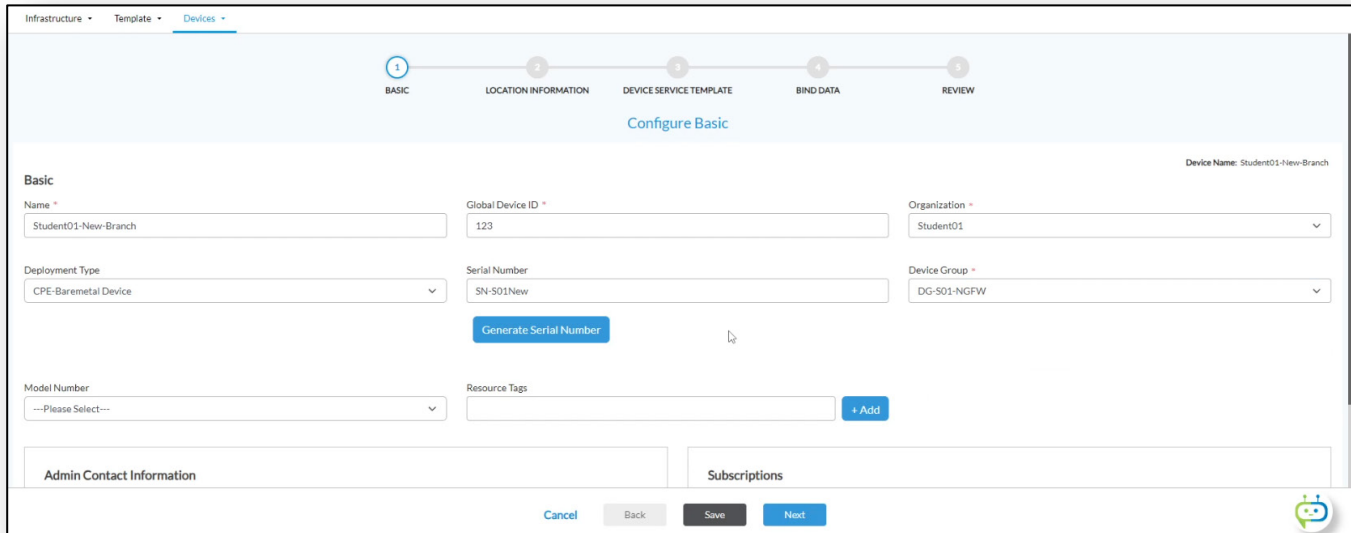
Click the + Add button to create a new device workflow.



c. Configure the Basic properties

For each of the following, the xx value represents your assigned student number (e.g. Studentxx would be Student01, Student02, etc.)

- Name: Studentxx-New-Branch
- Organization: Studentxx
- Serial Number: SN-SxxNew
- Device Group: DG-Sxx-NGFW

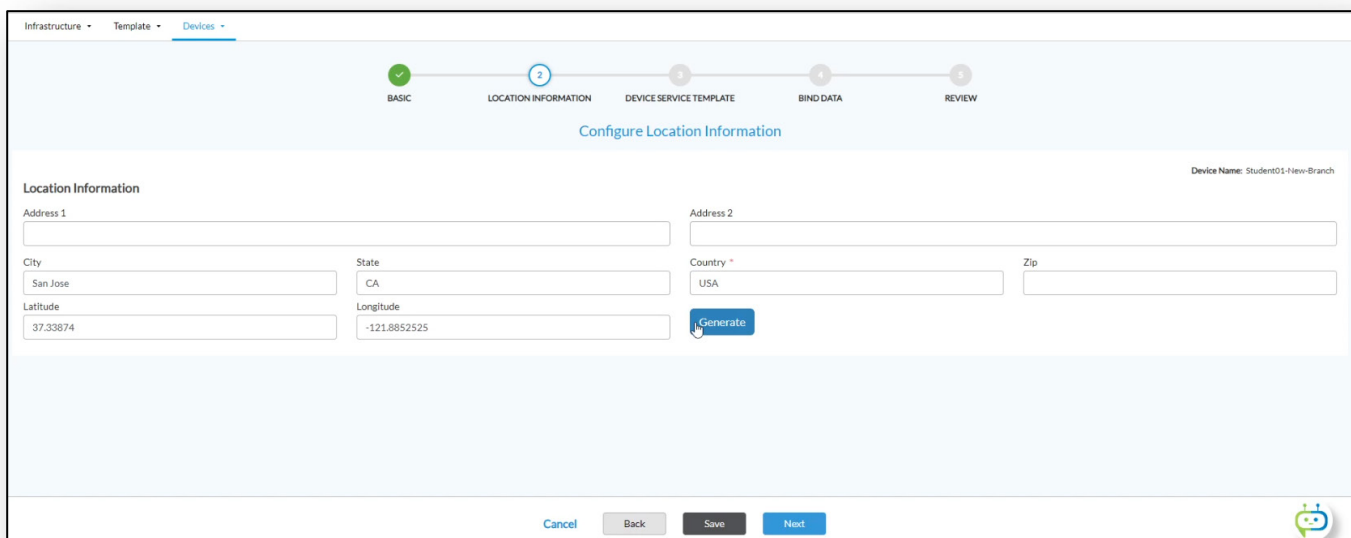


The screenshot shows the 'Configure Basic' dialog in the Versa SD-WAN configuration tool. The dialog is titled 'Configure Basic' and has a progress bar at the top with five steps: BASIC (1), LOCATION INFORMATION (2), DEVICE SERVICE TEMPLATE (3), BIND DATA (4), and REVIEW (5). The 'BASIC' step is currently active. The dialog contains the following fields and controls:

- Name:** Student01-New-Branch
- Global Device ID:** 123
- Organization:** Student01
- Deployment Type:** CPE-Baremetal Device
- Serial Number:** SN-S01New
- Device Group:** DG-S01-NGFW
- Model Number:** ---Please Select---
- Resource Tags:** + Add
- Generate Serial Number:** A blue button to generate a serial number.
- Admin Contact Information:** A section for administrative contact details.
- Subscriptions:** A section for subscription information.
- Buttons:** Cancel, Back, Save, and Next.

d. Configure the Location

- Click the *Next* button to continue to the Location dialog. Enter the City as San Jose, the state as CA, and the country as USA
- Click the Generate to get the coordinates of the address



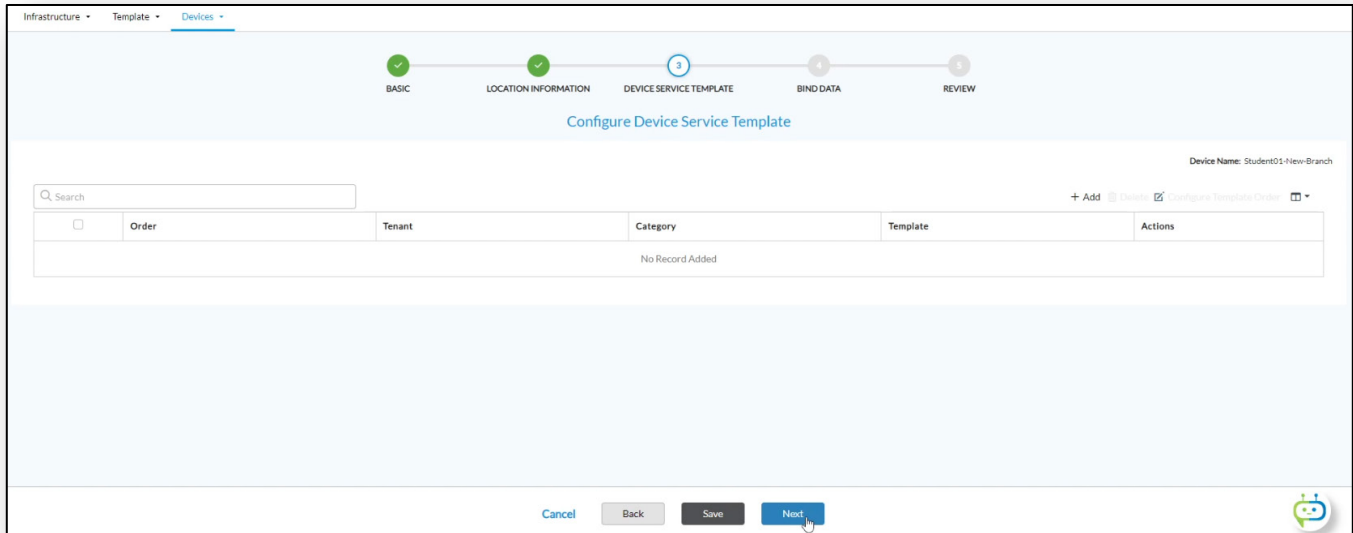
The screenshot shows the 'Configure Location Information' dialog in the Versa SD-WAN configuration tool. The dialog is titled 'Configure Location Information' and has a progress bar at the top with five steps: BASIC (1), LOCATION INFORMATION (2), DEVICE SERVICE TEMPLATE (3), BIND DATA (4), and REVIEW (5). The 'LOCATION INFORMATION' step is currently active. The dialog contains the following fields and controls:

- Address 1:** An empty text field.
- Address 2:** An empty text field.
- City:** San Jose
- State:** CA
- Country:** USA
- Zip:** An empty text field.
- Latitude:** 37.33874
- Longitude:** -121.8852525
- Generate:** A blue button to generate coordinates.
- Buttons:** Cancel, Back, Save, and Next.

- e. Navigate to the Device Service Template window.

Click *Next* to navigate to the *Device Service Template* window. If you have configured service templates you can apply them to a group of devices through the device group, or you can apply service templates directly to a device in the device workflow.

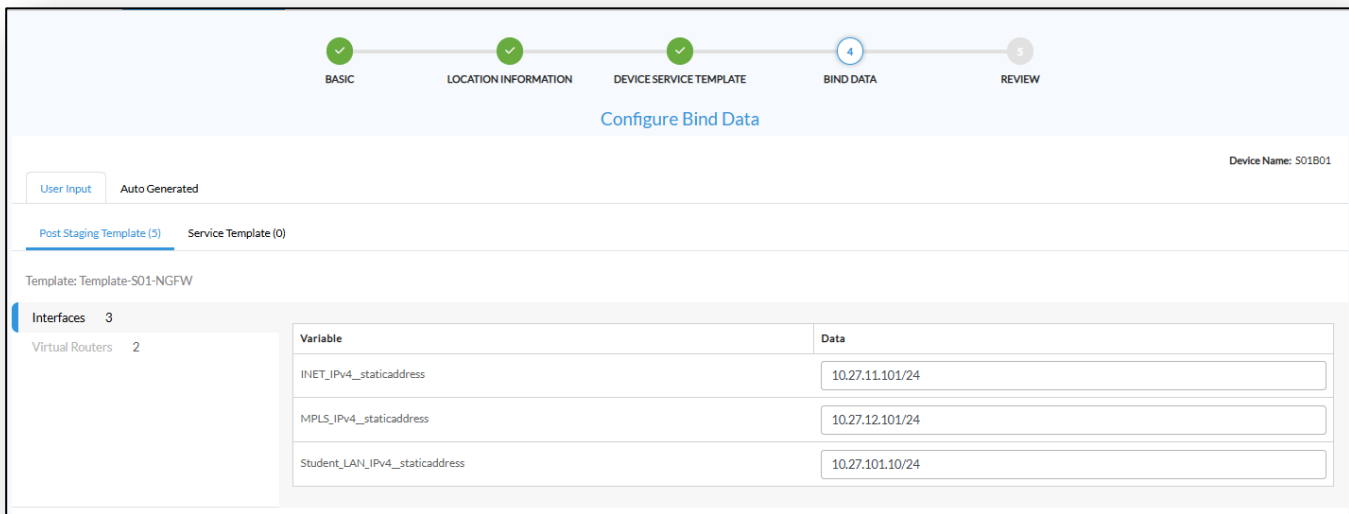
For our example we will not add any service templates to the device directly.



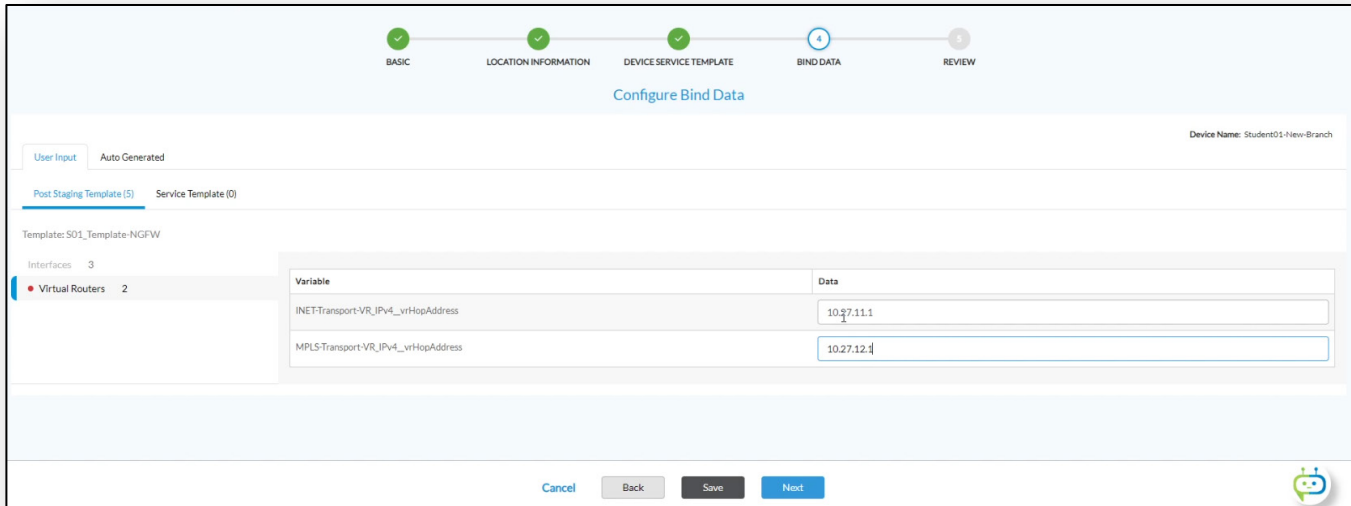
- f. Click the *Next* button to move to the Bind Data window.

You may notice a brief delay when the Bind Data window is opened. This is because Versa Director scans the templates associated with this device for variables and automatically generates system-assigned values to those variables. The user-defined variables, such as IP addresses and gateway addresses, are presented in forms for user input.

Bind data variables are sorted according to their type. In our example there are interface variables and virtual router variables, as shown on the left side of the window.



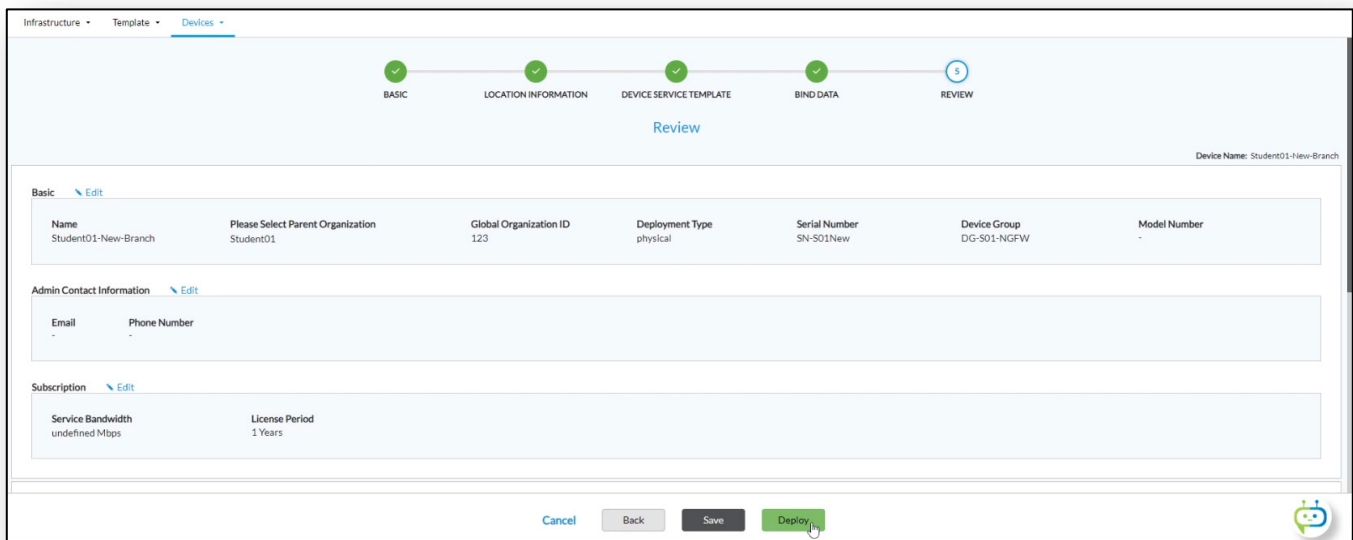
Interfaces Bind Data



Virtual Router bind data (default gateway routes, etc.)

- g. Enter the following values (also shown in the diagram). Because we will not be onboarding the device, all students can enter the same information without causing any IP conflicts.
- INET_IPv4_staticaddress: 10.27.11.201/24
 - MPLS_IPv4_staticaddress: 10.27.12.201/24
 - Student_LAN_IPv4_staticaddress: 10.27.201.10/24
 - INET-Transport-VR_IPv4_vrHopAddress: 10.27.11.1
 - MPLS-Transport-VR_IPv4_vrHopAddress: 10.27.12.1
- h. Click *Next* to go to the Review dashboard.

In the review window you can view the properties that have been defined for this device. You can scroll down the window to see more properties, including the bind data values you provided.



The Save button saves the workflow in its current state, but does not create the device object in the hardware inventory. To create the device in the hardware inventory, click the Deploy button.

- i. Click the Deploy button to deploy the workflow and create the device in the hardware inventory.

You can see the workflow status in the Devices workflow table, as shown below.

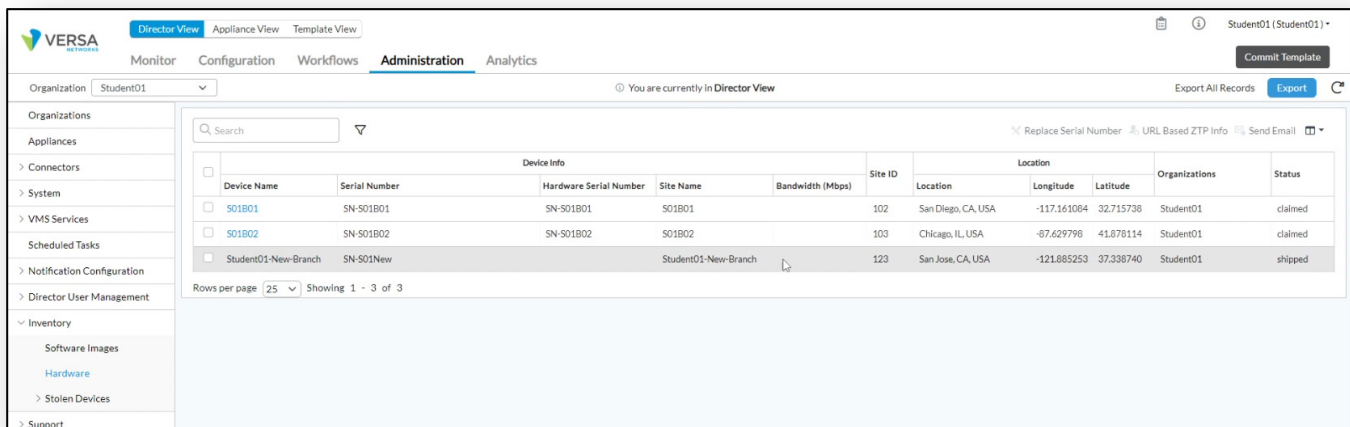
Devices					
Search					
<input type="checkbox"/>	Name	Global Device ID	Status	Last Modified By	Actions
<input type="checkbox"/>	S01B01	102	Deployed	Student01	
<input type="checkbox"/>	S01B02	103	Deployed	Student01	
<input type="checkbox"/>	Student01-New-Branch	123	Deployed	Student01	

Rows per page: 25 | Showing 1 - 3 of 3

Verify the new device in the Hardware Inventory

- j. Navigate to *Administration > Inventory > Hardware* to view the hardware inventory.

In the hardware inventory you should see your new device. There is not a Hardware Serial Number value attached, as the new device has not been associated with a physical appliance.



Hardware Inventory											
Search											
<input type="checkbox"/>	Device Name	Serial Number	Hardware Serial Number	Site Name	Bandwidth (Mbps)	Site ID	Location			Organizations	Status
<input type="checkbox"/>	S01B01	SN-S01B01	SN-S01B01	S01B01		102	San Diego, CA, USA	-117.161084	32.715738	Student01	claimed
<input type="checkbox"/>	S01B02	SN-S01B02	SN-S01B02	S01B02		103	Chicago, IL, USA	-87.629798	41.878114	Student01	claimed
<input type="checkbox"/>	Student01-New-Branch	SN-S01New		Student01-New-Branch		123	San Jose, CA, USA	-121.885253	37.338740	Student01	shipped

Rows per page: 25 | Showing 1 - 3 of 3

At this point the device is ready for onboarding. With the onboarding process (not covered in this lab), the appliance is connected to the WAN and the onboarding process starts with either the URL based onboarding, by running the onboarding script, or through the global ZTP process. When the appliance contacts the controller, it will provide the hardware serial number to the headend. The hardware serial number will then be listed in the hardware table (as it will be associated with the device), and the appliance will be placed in the Appliances table.



STOP! Notify your instructor that you have completed this lab.

TOPOLOGIES

The Versa Networks lab environment consists of a fixed, pre-configured topology that will allow you to explore, configure, and manage Versa Networks CPEs by using Versa Director, the central management and orchestration platform for a Versa Secure SD-WAN solution. After completing this lab, you will be able to:

- Analyze the configuration components of full mesh and hub-and-spoke topologies
- Configure and analyze the following topologies:
 - Spoke-to-Hub-Only
 - Spoke-to-Spoke-via-Hub
 - Spoke-to-Spoke-Direct

In this lab you will be assigned two CPE devices (Branch devices) for configuration and monitoring. The branch devices are named after the student ID that you have been assigned.

The lab environment is accessed through Amazon Workspaces. Your student ID and workspace will be assigned by the instructor.

The remote desktop connection opens a remote workstation, where you will use various tools to navigate and configure the lab environment. The main tool you will use in this lab is Versa Director. Versa Director can be accessed by opening the Google Chrome browser on the Remote Desktop. The IP address of the Versa Director (from the remote workstation) is 10.27.1.10. Once you begin the lab, you may want to create a bookmark to Versa Director in the web browser on the remote desktop.

During certain lab parts, the lab guide will present sample output from the GUI or the CLI. The sample outputs are SAMPLES and represent the information as it appeared during the lab guide creation. Your output may vary in some ways (some devices may or may not be present, some routes may or may not be the same, etc.) Do not be alarmed if your results vary slightly from the results shown in the lab guide. The important thing is that the lab functions in the desired manner.

This lab guide will step you through some common tasks that are performed on Versa Director. After an introductory set of exercises, you will be asked to perform some basic tasks that will allow you to become more familiar with the environment.

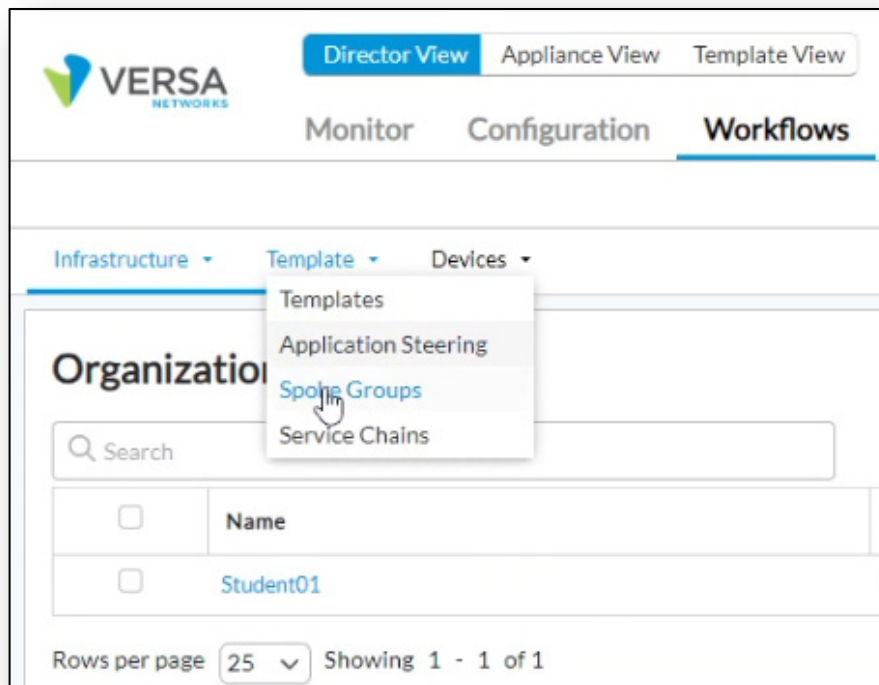
The goal of this and all lab exercises is to help you gain additional skills and knowledge. Because of this, the lab guide contains additional instruction to supplement the student guides.

Now that we've discussed what is expected, let's get started!

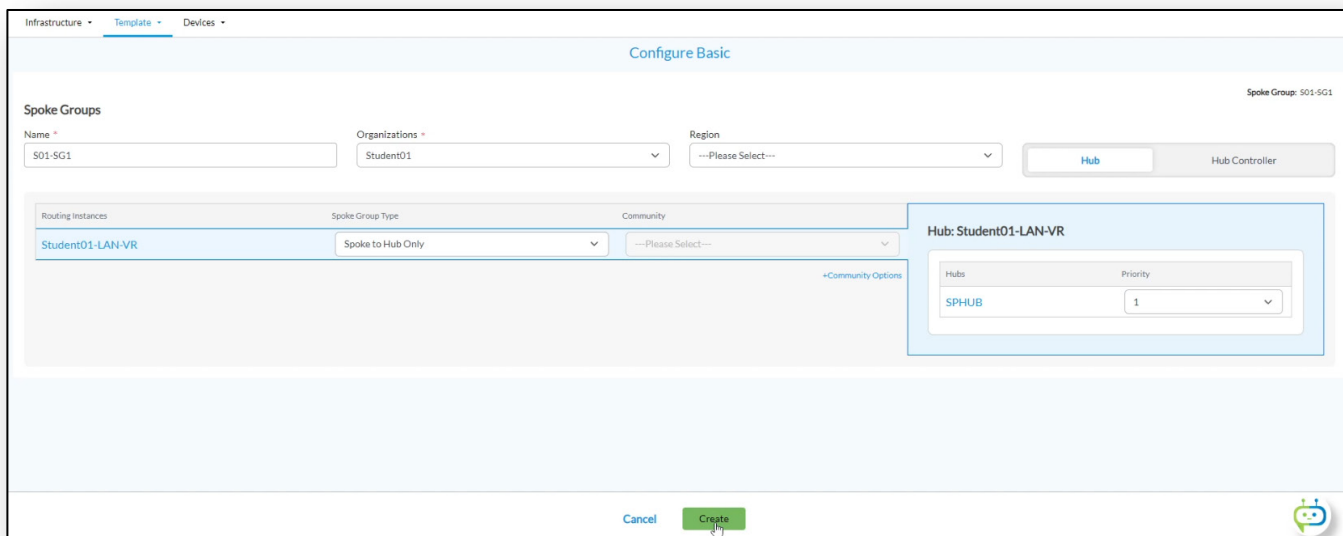
Step 1. Create a Spoke Group

In this exercise you will create 2 spoke groups. As we move through the lab you will change the type of spoke group in order to change the behavior of the routing policies and traffic forwarding. The spoke groups that you will create are based on the student ID that you were assigned.

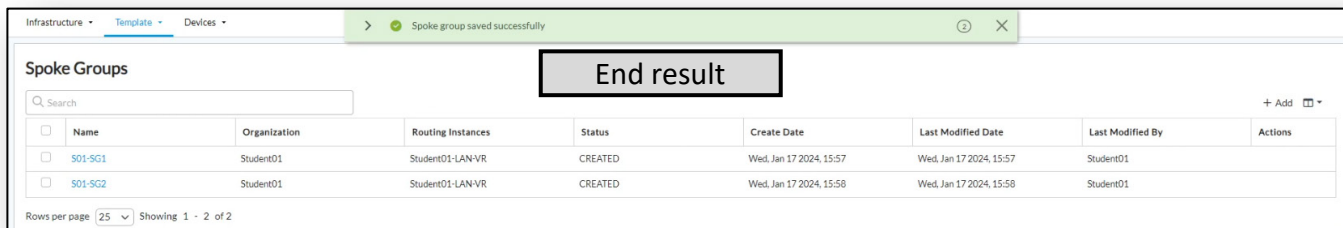
- a. Log into Versa Director
- b. In Versa Director, navigate to *Workflows > Template > Spoke Groups*.



- c. In the Spoke Groups workflow, create a spoke group with the name Sxx-SG01, where xx is your student number.
- d. Set the LAN-VR spoke group type to Spoke to Hub Only.
- e. In the Hub dropdown you should see SPHUB-NEW. This is the shared hub for all tenants.
- f. Set the hub priority to 1.



- g. Click Create to create the spoke group.
- h. Repeat steps c through g process to create a spoke group named Sxx-SG02 with the same properties.



Before you add the devices to a hub and spoke topology, we'll analyze the policies that exist in the default full-mesh topology.

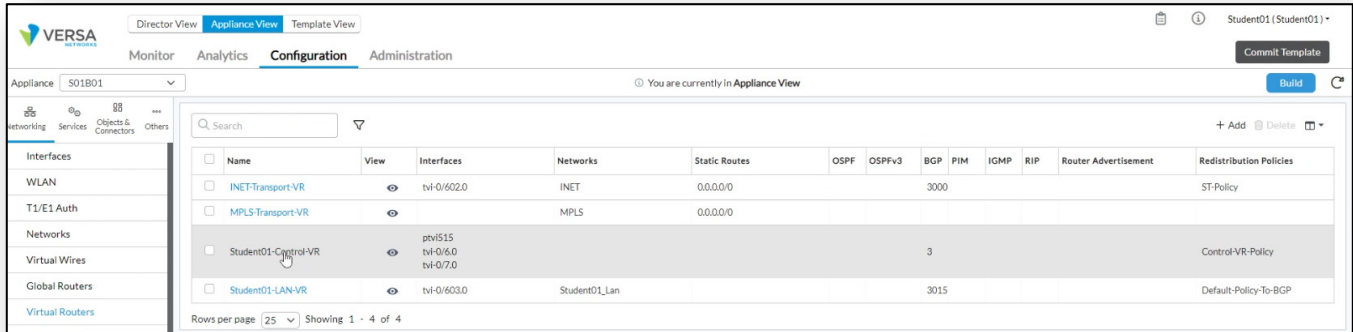
Step 2. Examine BGP Policies

- a. Open your SxxB01 Branch Device to view the configuration

Click the Appliance View at the top of the dashboard, and then click on the SxxB01 branch device, where xx is the student ID that has been assigned to you.

- b. Open the Control Router

In the Appliance view, navigate to *Configuration > Networking > Virtual Routers* and locate the Studentxx-Control-VR virtual router. Click on the *Control* router to open its configuration.



The control router runs the primary BGP instance for the Layer 3 VPN (SD-WAN) connections.

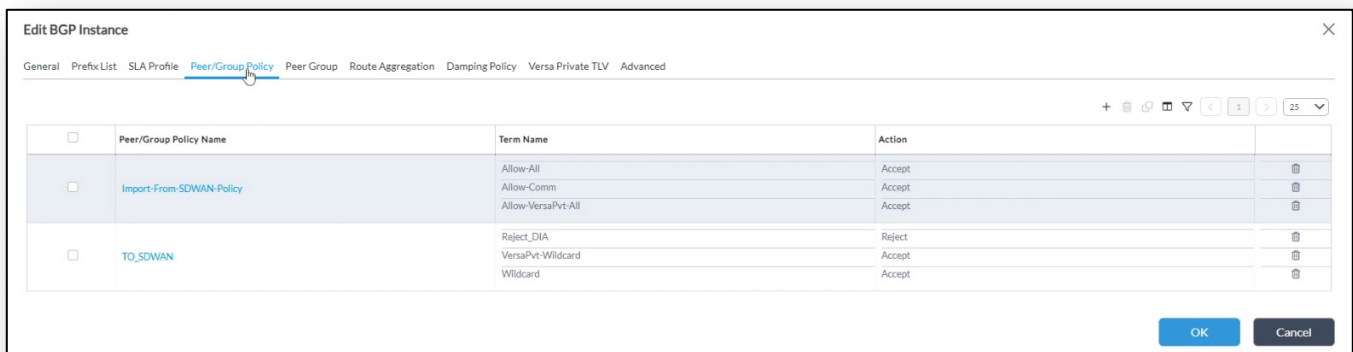
- c. Open the BGP Routing Instance in the Control Router

BGP advertises and receives routes to and from the controller. Navigate to the BGP tab of the control router, then click on the instance ID of the BGP process to open the BGP configuration.



- d. View the BGP Peer and Peer Group Policies

The BGP peer and BGP peer group policies are located in the Peer/Group policies. There are 2 default policies created. Navigate to the Peer/Group Policy tab. In a full mesh topology, the default Import-From-SDWAN-Policy allows all routes received from the controller.



- e. Click Cancel to exit the Policy window.
- f. Click Cancel to exit out of the BGP window.
- g. Click Cancel to exit out of the Control VR configuration window.
- h. Open the Student-LAN-VR

From the Virtual Routers table, locate and click on the Student-LAN-VR to open the LAN facing virtual routing instance. The LAN virtual router contains the LAN facing port and the local LAN routes. It also has policies that add routes from the LAN routing tables to the BGP updates sent by the Control router.

<input type="checkbox"/>	Name	View	Interfaces
<input type="checkbox"/>	INET-Transport-VR		tvi-0/602.0
<input type="checkbox"/>	MPLS-Transport-VR		
<input type="checkbox"/>	Student01-Control-VR		ptvi515 tvi-0/6.0 tvi-0/7.0
<input type="checkbox"/>	Student01-LAN-VR		tvi-0/603.0

Rows per page: 25 Showing 1 - 4 of 4

The Redistribution Policies search for routes in the LAN routing table that should be added to the BGP updates.

- i. Click on the Redistribution Policies tab in the LAN VR.

Edit Student01-LAN-VR ✕

Virtual Router Details Static Routing OSPF RIP BGP PIM IGMP Router Advertisement Prefix Lists Redistribution Policies Instance Import Policies

General | Redistribute To

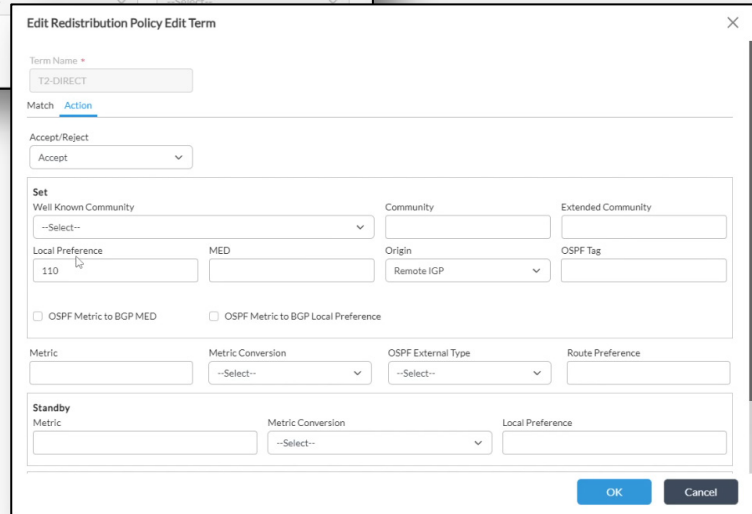
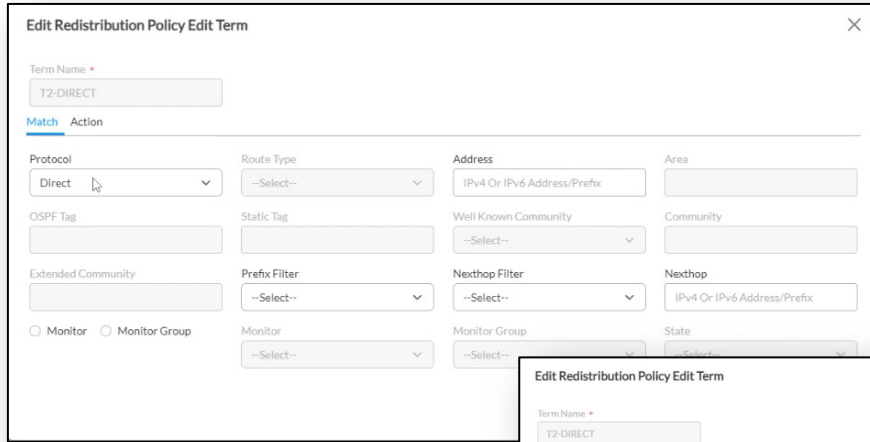
Redistribution Policies + 25

<input type="checkbox"/>	Name	View	Term
<input type="checkbox"/>	Default-Policy-To-BGP		T1-Paired-TVI-Direct T2-DIRECT T4-BGP

OK Cancel

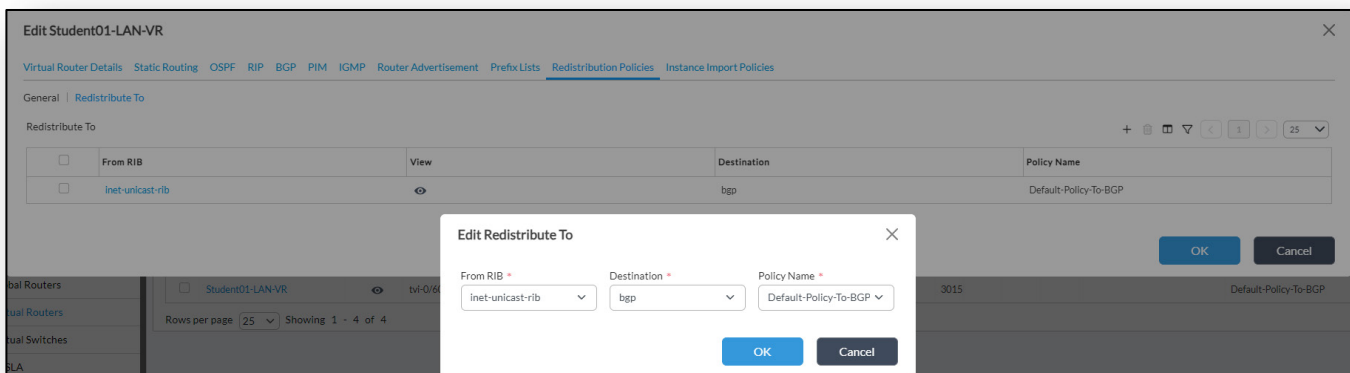
The default redistribution policy rejects the IP addresses that are used for local processes on the device, so that they are not advertised to remote devices. The term T2-DIRECT matches the Direct type of route, or the local LAN link, and adds it to the update. The T4-BGP policy adds any LAN VR BGP routes to the Control router BGP updates and allows them to migrate from one routing domain to another. You can open the policy to view more details.

- j. Open and Examine the T2-DIRECT policy term.



- k. Click on the Redistribute To tab in the Redistribuition Policies window.

The Redistribute To tab identifies from where the routes come, and to where the routes should be moved according to the terms in the rules.



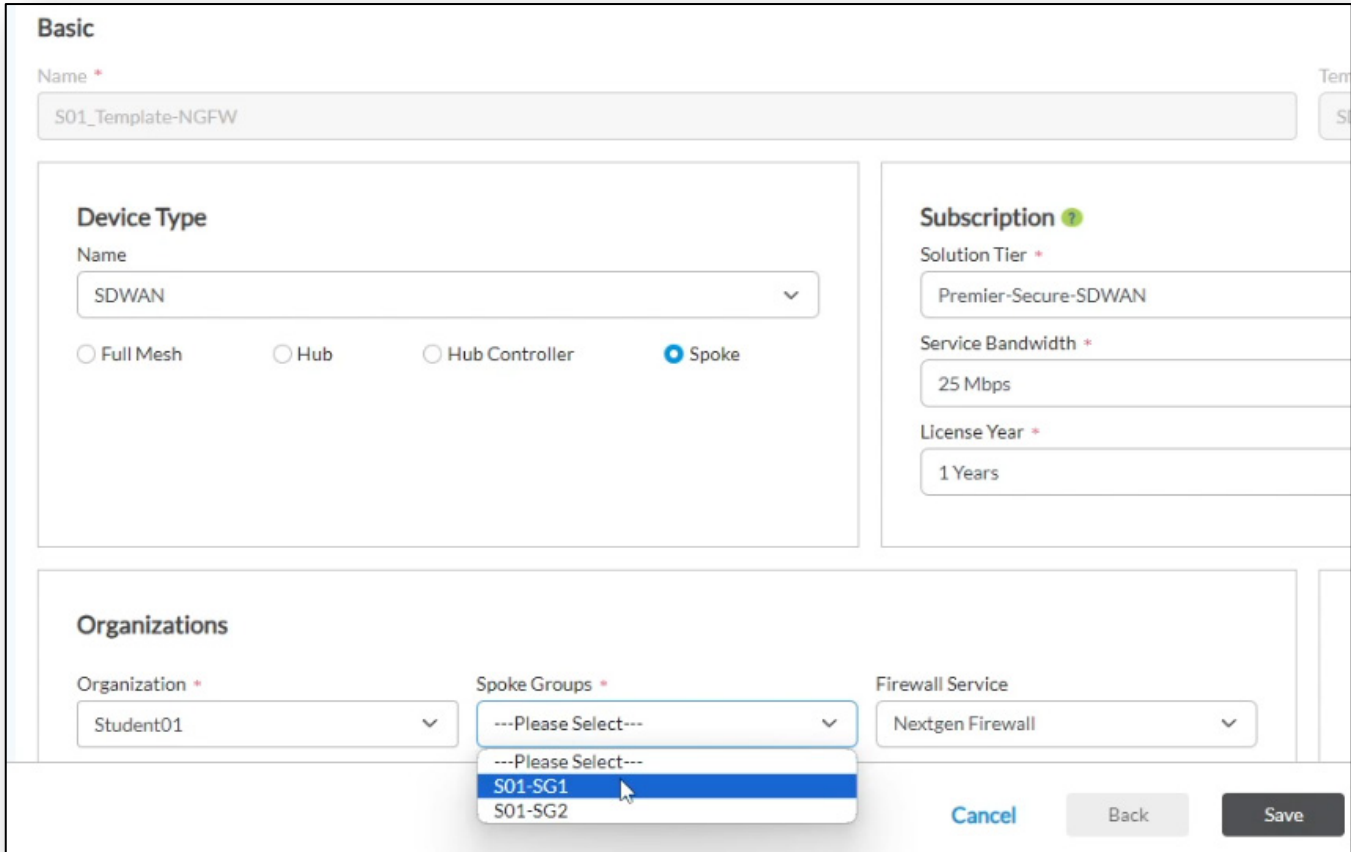
With this configuration, the routes move from the LAN VR unicast table to the main BGP process routing updates according to the rules in the defined policy name.

- l. Click Cancel until you have exited the LAN-VR configuration and exit without making any changes.

Step 3. Apply Spoke Groups

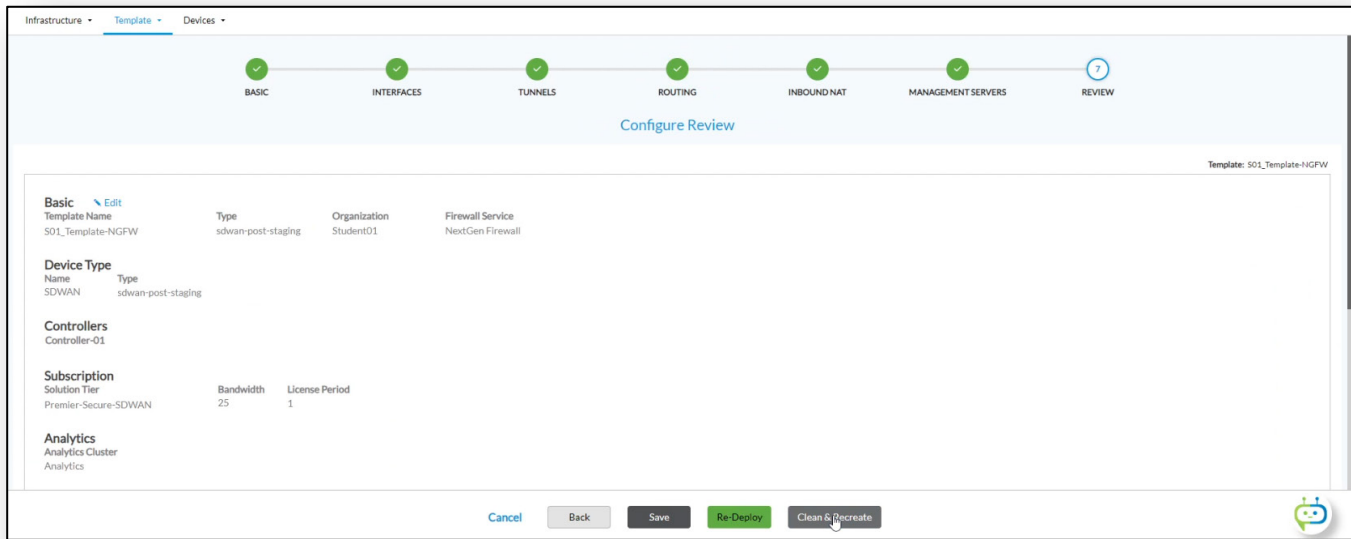
Next you will modify the main NGFW template so that it is a spoke template associated with the Sxx-SG1 spoke group.

- a. Click the Director View button at the top of the window.
- b. In Director View navigate to *Workflows > Template > Templates*.
- c. Locate the Sxx_Template-NGFW workflow, where Sxx is the student number assigned to you.
- d. In the Template-NGFW workflow, select Spoke in the Device Type. Note that when you select Spoke as the device type, a new field is created in the Organizations section to select the spoke group.



- e. Select the Sxx-S01 spoke group.
- f. Click the *Next* button until you arrive at the Review page.

g. In the Review page, click Clean & Recreate to rebuild the template with the new spoke group assignment.



h. Click Confirm when prompted.

To apply the changes, you will need to commit the template to rebuild the device configurations with the new template settings and copy the configurations to the devices.

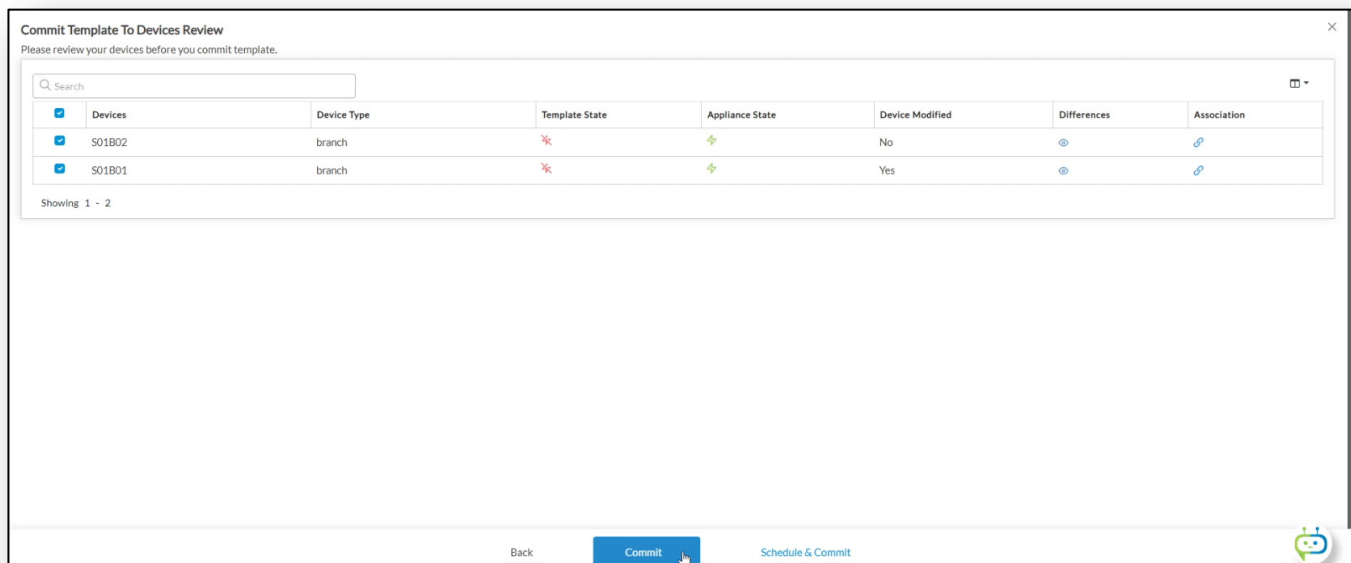
i. Click the Commit button

j. In the Commit Template to Select Devices page, select your organization in the Organization menu, select Template in the Select Devices By menu. Select the Sxx_Template-NGFW as the template, then click the Fetch Devices button. Your devices should be displayed in the table.

k. Check the boxes next to all of the devices.

l. Click the Review button.

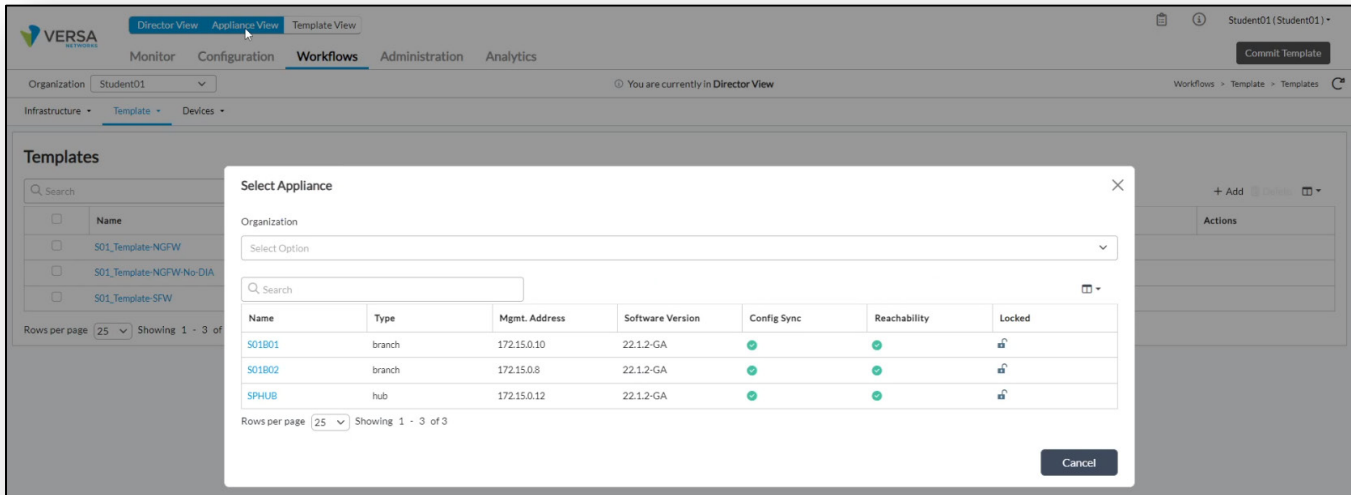
m. In the Review page, click Commit to apply the changes.



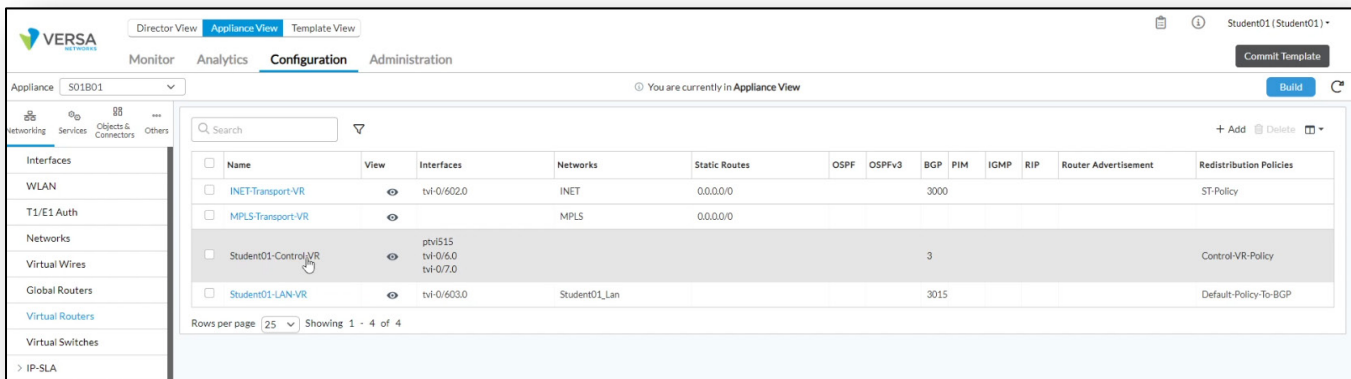
Step 4. Identify changes made by the Spoke Group configuration

Next we will identify and verify the changes that were made when the topology type was changed.

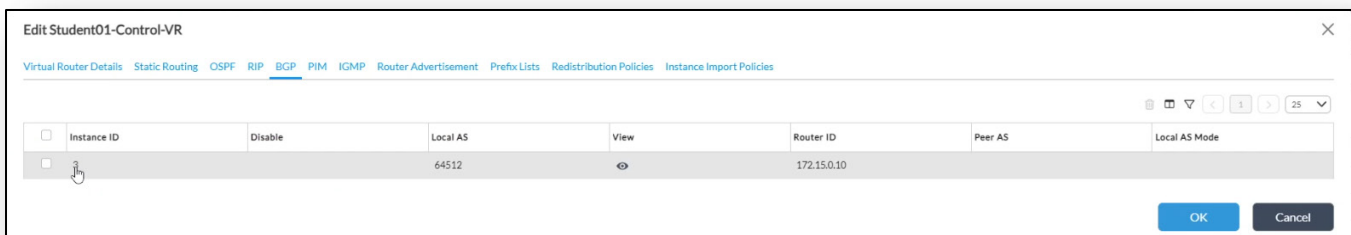
- Click on Appliance View, then locate your SxxB01 branch in the table.
- Click on the branch name to open the branch in Appliance View mode.



- In Appliance view of your SxxB01 device, navigate to *Configuration > Networking > Virtual Routers*.
- Locate the Studentxx-Control-VR and click on the control router to open its configuration.

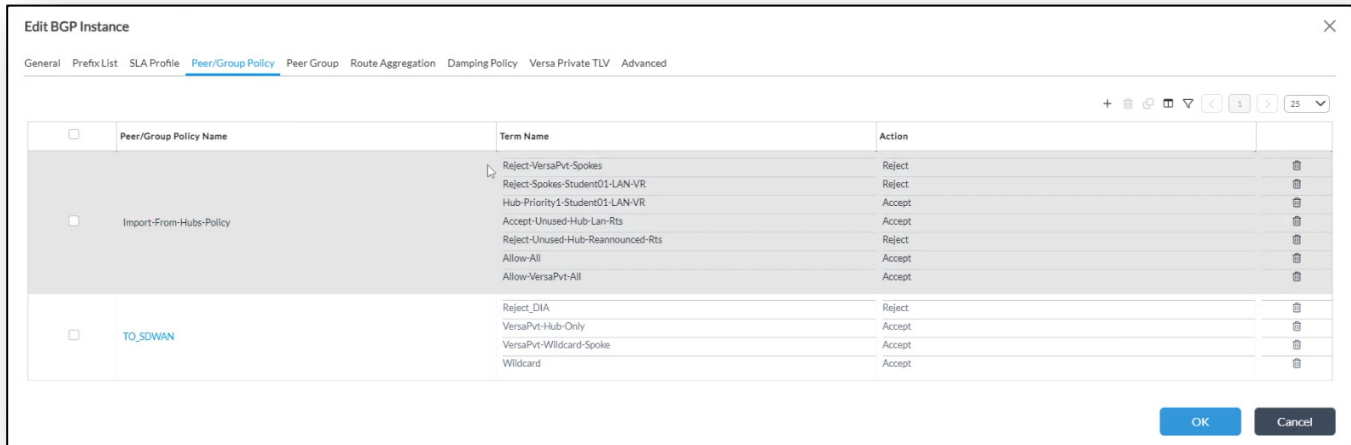


- Navigate to BGP and click on the BGP instance to open the BGP configuration.



- f. Click on the Peer/Group Policy tab.

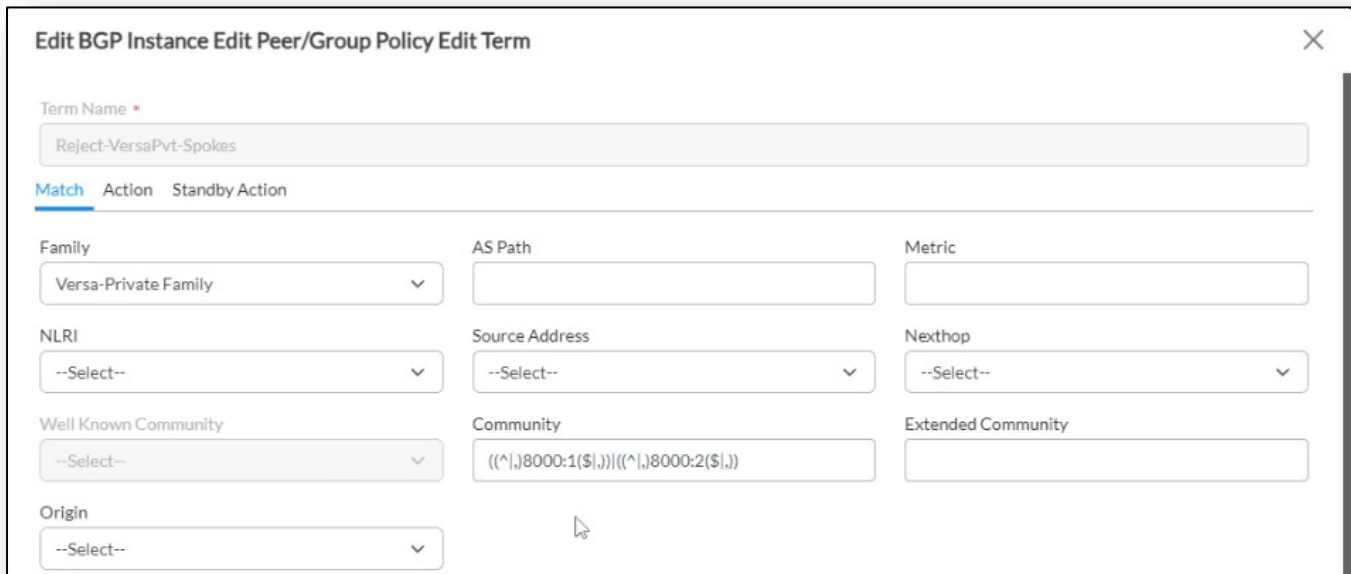
Note the addition of multiple terms to the policies.



- g. Open the Import-From-Hubs-Policy

- h. In the Import-From-Hubs-Policy, click on the Reject-VersaPvt-Spokes term to open the term.

Note that the match conditions search for specific community values. These values are values associated with a specific spoke group. Depending on your environment the values you see may be different from the example. Take a note of the values in the Community field. The same communities are matched in the Reject-Spokes-Student-LAN-VR term.



- i. Click Cancel to close the term without making changes.
- j. Locate and click on the Hub-Priority1-Student-LAN-VR term.

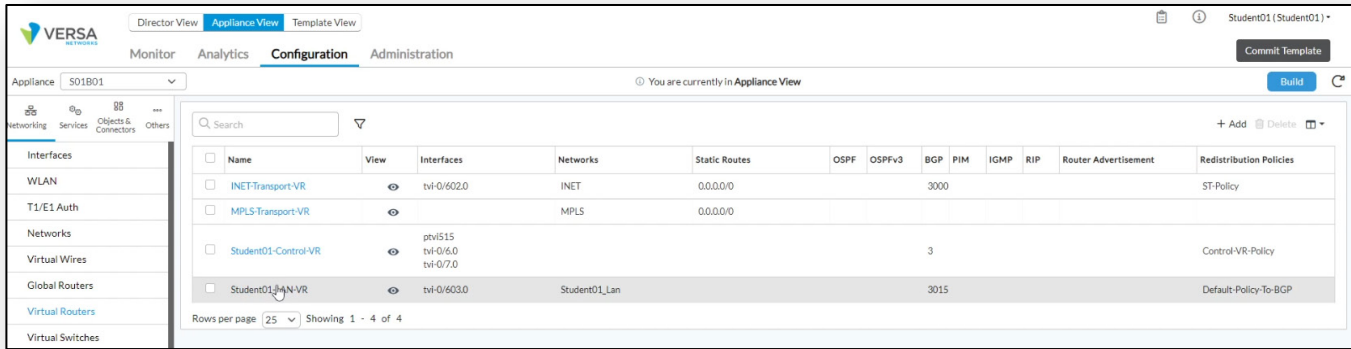
This term matches based on an Extended Community value that is associated with the hub device.

- k. Click on the Action tab of the term.

In the action tab, the route is set to Accept, and the Local Preference of 108 is assigned. This is the value assigned to the routes received from the hub to make them more preferred. In a topology with multiple hubs, each hub will have a different Local Preference assigned to ensure that routes from the highest available hub are preferred in the routing table.

- l. Click Cancel until you exit the virtual router configuration and return to the main branch configuration page.

m. In the main configuration page, under Virtual Routers, locate and click on the Student-LAN-VR routing instance.

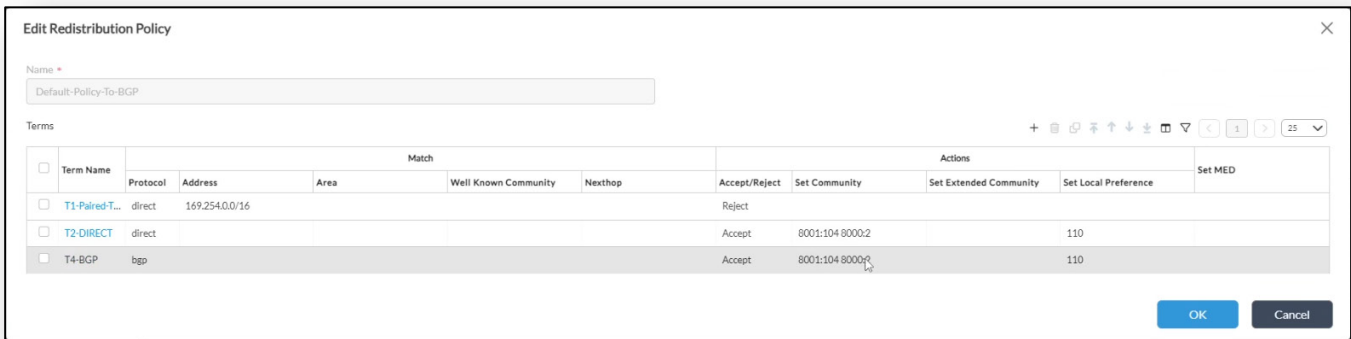


In the Student-LAN-VR routing instance, open the Redistribution Policies tab.



The terms in the redistribution policy appear to be the same, but upon closer inspection of the terms we can see that a Set Community property has been added.

n. Click on the Default-Policy-To-BGP policy to see an overview of the change.



Note that one of the community values that is added to the redistributed routes matches the BGP community value that we saw in the BGP import policy (in this case, 8000:2). This allows remote sites to identify the source of these routes, what spoke group the routes are part of, and allows the BGP policies on other devices to filter the advertisements.

o. Click the Cancel button until you have exited the virtual router configuration. When asked to confirm, click Yes.

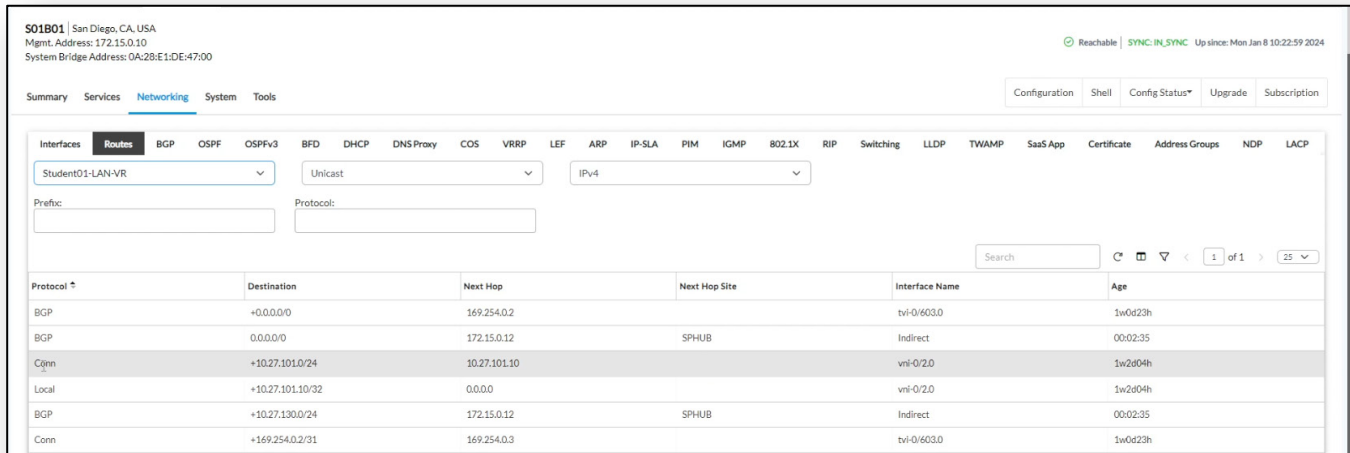
Step 5. Verify the Routing Changes

Next we will verify the routing changes that were made in the topology by examining the routing tables of the two branch devices.

- a. Navigate to the Monitor tab in Appliance view.

In the Monitor dashboard, ensure that the SxxB01 branch is selected, where Sxx is the student ID assigned to you.

- b. Navigate to the *Networking > Routes* dashboard
- c. Select the Student_LAN-VR routing table from the dropdown to view the routes in that virtual router.



Protocol *	Destination	Next Hop	Next Hop Site	Interface Name	Age
BGP	+0.0.0/0	169.254.0.2		tv1-0/603.0	1w0d23h
BGP	0.0.0/0	172.15.0.12	SPHUB	Indirect	00:02:35
Cqnn	+10.27.101.0/24	10.27.101.10		vni-0/2.0	1w2d04h
Local	+10.27.101.10/32	0.0.0		vni-0/2.0	1w2d04h
BGP	+10.27.130.0/24	172.15.0.12	SPHUB	Indirect	00:02:35
Conn	+169.254.0.2/31	169.254.0.3		tv1-0/603.0	1w0d23h

There are 2 main routes you will focus on in this lab exercise. The LAN route for branch B01 and the LAN route for branch B02. The routes for those branches will depend on your organization (Student) number.

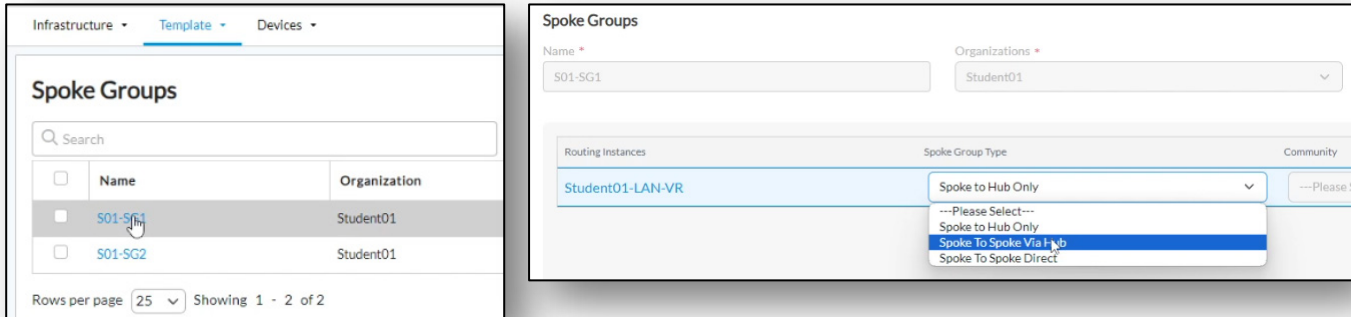
Because this is a spoke-to-hub only topology, the routes to the other spokes are not present in the routing table. However, the route to the hub LAN is present (10.27.130.0/24). If you choose to do so, you can open the SxxB02 device and view the LAN routing table to see the same behavior on branch B02.

Step 6. Change the Spoke Group to Spoke to Spoke via Hub.

Next we will change the spoke group type to Spoke to Spoke via Hub and examine the effects.

- a. Navigate to *Director View > Workflows > Template > Spoke Groups* to open the Spoke Group configuration workflows dashboard.
- b. Locate and click on spoke group Sxx-SG1 to open Spoke Group 1.

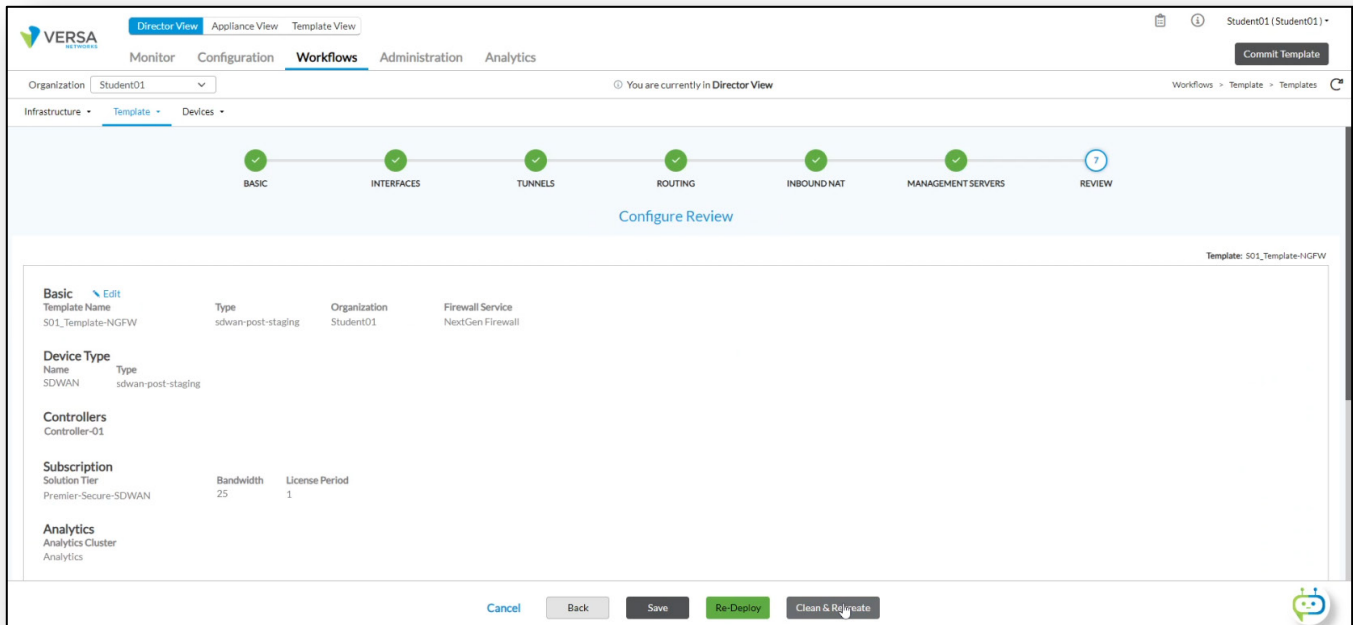
- c. Change the Spoke Group Type to *Spoke to Spoke Via Hub*. Leave all other parameters the same.



- d. Click **Recreate** to rebuild the spoke group settings.

Because the spoke group is part of the template settings, we need to rebuild the template using the template workflow.

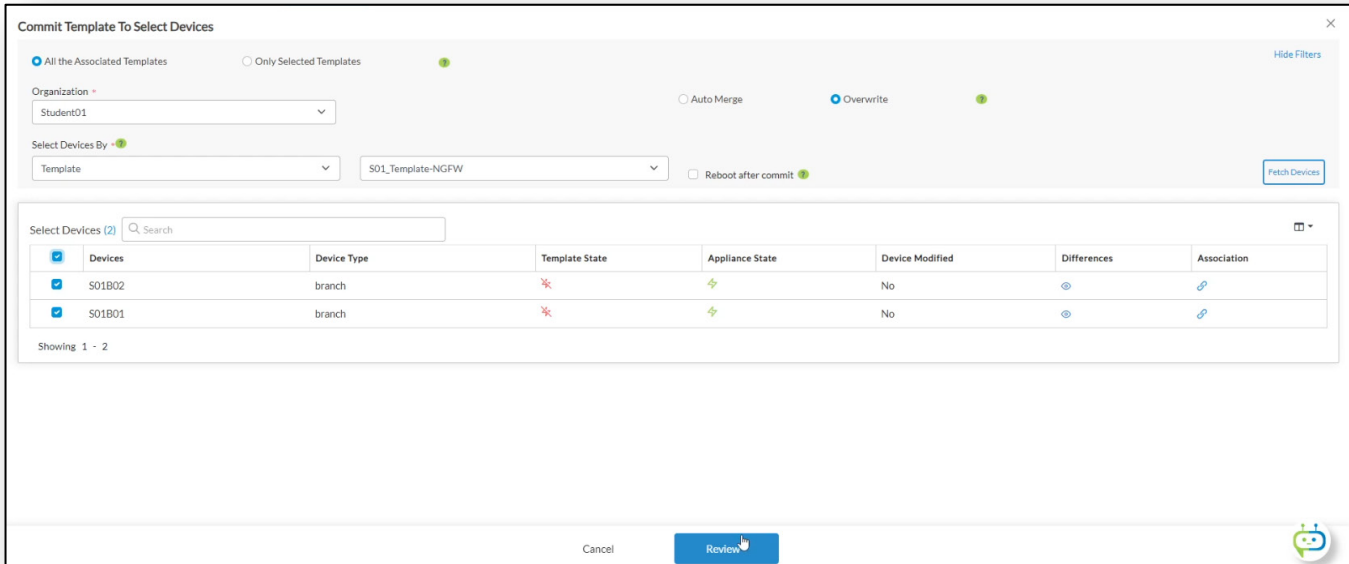
- e. Navigate to *Workflows > Template > Templates*. Locate the *Sxx_Template-NGFW* workflow.
- f. Open the *Sxx_Template-NGFW* workflow
- g. Click the *Next* button until you reach the *Review* page.
- h. On the *Review* page, click *Clean & Recreate* to rebuild the template with the new spoke group settings.



- i. Click *Confirm* to allow the recreation of the template.

The template has been updated. Now the changes in the template need to be committed to the devices.

- j. Click the Commit Template button.
- k. In the Commit Template to Select Devices, select your organization in the Organization drop down. Select the devices by Template, and select the Sxx_Template-NGFW template from the template list.
- l. Click Fetch Devices. Your branch devices should display in the table.
- m. Click the boxes next to your devices, then click Review.



Commit Template To Select Devices

All the Associated Templates
 Only Selected Templates
 Hide Filters

Organization: Student01
 Auto Merge
 Overwrite
 Reboot after commit

Select Devices By: Template
 S01_Template-NGFW
 Fetch Devices

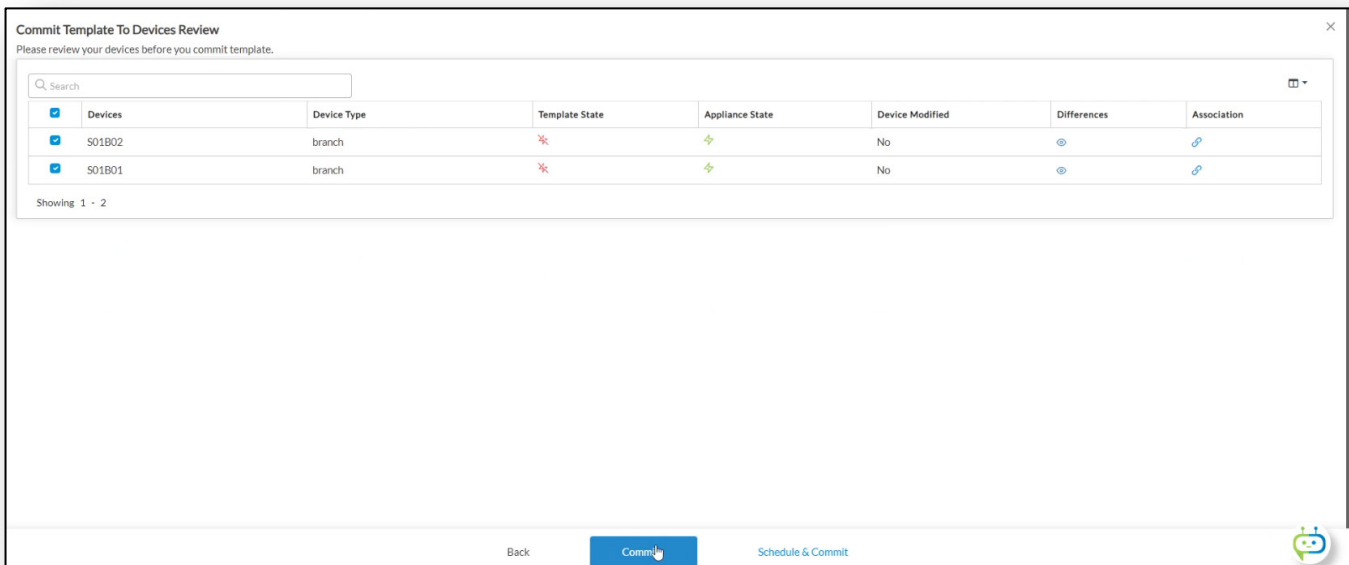
Select Devices (2)

Devices	Device Type	Template State	Appliance State	Device Modified	Differences	Association
<input checked="" type="checkbox"/> S01B02	branch	*	↔	No	👁	🔗
<input checked="" type="checkbox"/> S01B01	branch	*	↔	No	👁	🔗

Showing 1 - 2

Cancel Review

- n. In the Review window, click Commit to apply the changes.



Commit Template To Devices Review

Please review your devices before you commit template.

Devices	Device Type	Template State	Appliance State	Device Modified	Differences	Association
<input checked="" type="checkbox"/> S01B02	branch	*	↔	No	👁	🔗
<input checked="" type="checkbox"/> S01B01	branch	*	↔	No	👁	🔗

Showing 1 - 2

Back Commit Schedule & Commit

Step 7. Verify the policy and routing changes

Next we will verify the policy changes and routing changes.

- Navigate to *Appliance View* and select device SxxB01 from the device list.
- In the SxxB01 dashboard, navigate to *Monitor > Networking > Routes*.
- Select the LAN-VR routing instance from the drop down menu.

This will display the routes in the B01 LAN routing table.

Protocol	Destination	Next Hop	Next Hop Site	Interface Name	Age
BGP	+0.0.0/0	169.254.0.2		tv1-0/603.0	1w0d23h
BGP	0.0.0/0	172.15.0.12	SPHUB	Indirect	00:07:36
Conn	+10.27.101.0/24	10.27.101.10		vni-0/2.0	1w2d04h
Local	+10.27.101.10/32	0.0.0.0		vni-0/2.0	1w2d04h
BGP	+10.27.102.0/24	172.15.0.12	SPHUB	Indirect	00:03:25
BGP	+10.27.130.0/24	172.15.0.12	SPHUB	Indirect	00:07:36
Conn	+169.254.0.2/31	169.254.0.3		tv1-0/603.0	1w0d23h
Local	+169.254.0.3/32	0.0.0.0		tv1-0/603.0	1w0d23h
BGP	+169.254.0.6/31	172.15.0.12	SPHUB	Indirect	00:07:36

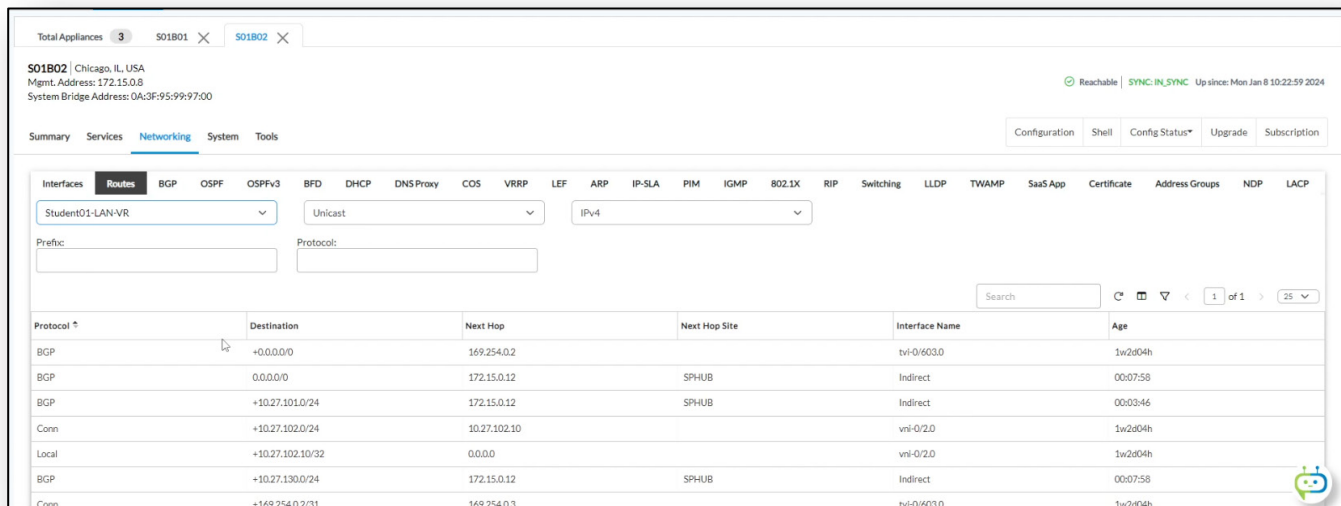
Note that the LAN route from branch B02 is now present, but that it has a next hop site of the SPHUB-NEW device and NOT the B02 branch device.

- Click on the *Total Appliances* tab to view a list of all of the appliances.
- From the appliances table, click on the B02 branch device.

Name	Tags
S01B01	
S01B02	
SPHUB	

Name	Value
Name	S01B02
Location	Chicago, IL, USA
Site ID	103
Serial Number	SN-S01B02
Model	c5.2xlarge
Services	sdwan,nextgen-firewall,cgnat
Time Created	2023-12-18 15:23:24.153
Template Status	

- f. In the SxxB02 appliance window, navigate to *Networking > Routes*.
- g. Select the LAN-VR virtual router from the drop down menu.



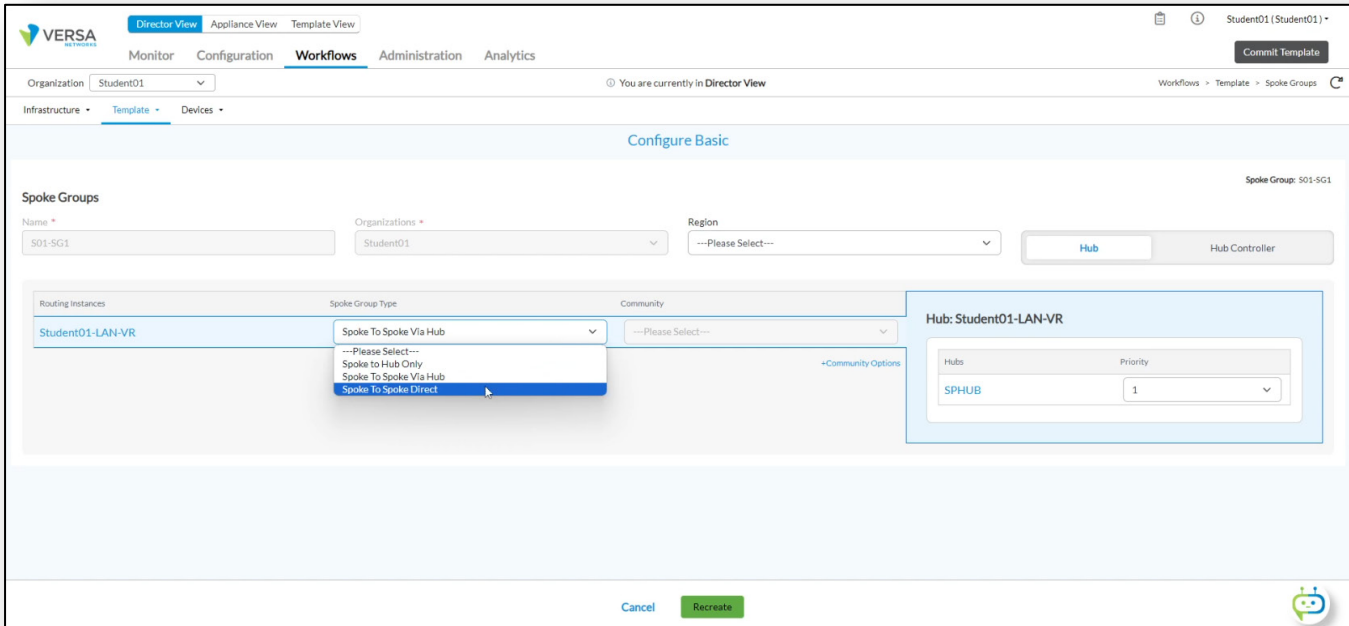
Note that the LAN route from branch B01 has a next hop site of the SPHUB-NEW device, and NOT the B01 device.

Because of this topology type, the branch LANs can communicate, but all traffic is relayed through the hub, and branches do not have direct tunnels between them.

Step 8. Configure Spoke to Spoke Direct

In the next exercise you will change your devices to Spoke to Spoke Direct in the spoke group. In the first part you will place both devices in the same spoke group and examine the routing tables.

- From Director View, navigate to *Workflows > Template > Spoke Groups*.
- From the Spoke Groups table, click on Sxx-SG1 to open Spoke Group 1.
- Change the Spoke Group type to *Spoke to Spoke Direct*. Note how the Community dropdown is activated with the Spoke to Spoke Direct spoke group type.

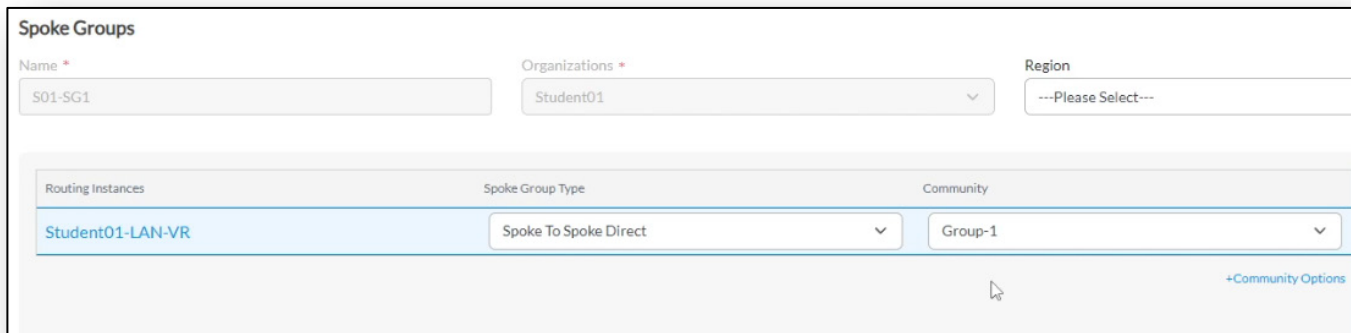


- Click the *+Community Options* link below the Community drop down menu. The Community dialog opens.
- In the Community dialog, click the *+* button to add a community. Name the Community *Group-1* and assign a community ID of 1.
- Click the *+* button again and add a second community called *Group-2*. Assign the community ID of 2.

Your communities should look like the example below.

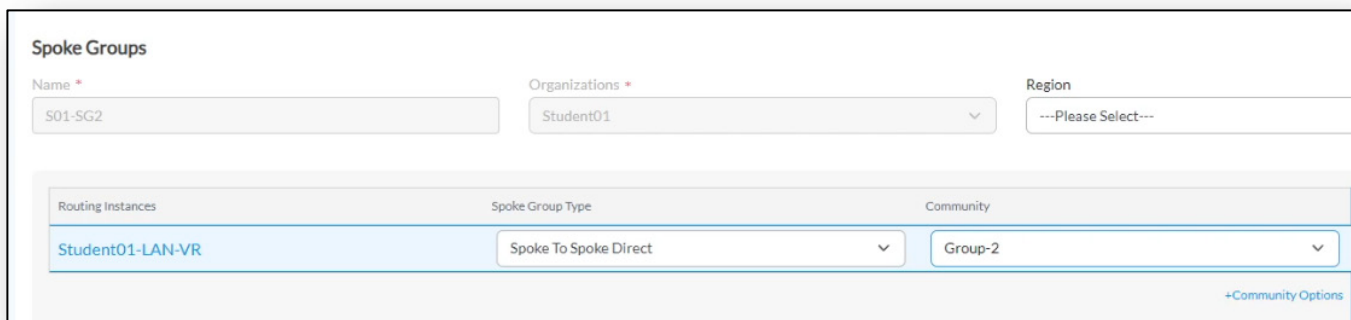


- g. Assign community Group-1 to the spoke group.



Routing Instances	Spoke Group Type	Community
Student01-LAN-VR	Spoke To Spoke Direct	Group-1

- h. Click the Recreate button to apply the changes to the spoke group.
- i. Open Spoke Group 2 (Sxx-SG2)
- j. Change Spoke Group 2 to Spoke to Spoke Direct.
- k. Assign community Group-2 to spoke group 2.



Routing Instances	Spoke Group Type	Community
Student01-LAN-VR	Spoke To Spoke Direct	Group-2

- l. Click Recreate to apply the changes to spoke group 2.

Next you will open the Sxx_Template-NGFW template workflow and re-create the template to ensure that the new spoke group settings are applied.

- m. Navigate to *Workflows > Template > Templates*.
- n. In the Template workflow table, locate and click on the Sxx_Template-NGFW workflow to open the workflow.

<input type="checkbox"/>	Name	Status	Last Modified Date	Last Modified By	Actions
<input checked="" type="checkbox"/>	S01_Template-NGFW	Deployed	2024-01-17 23:03:56	Student01	
<input type="checkbox"/>	S01_Template-NGFW-No-DIA	Deployed	2024-01-09 23:02:00	Administrator	
<input type="checkbox"/>	S01_Template-SFW	Deployed	2024-01-03 17:24:52	Administrator	

Rows per page: 25 | Showing 1 - 3 of 3

The proper settings are already in place for the workflow. However, because the properties of the spoke group assigned to the template have changed, we will re-create the template again to ensure that the spoke group settings are re-copied into the template.

- o. Click the *Next* button until you reach the review page.
- p. On the *Review* page, click the *Clean & Recreate* button to rebuild the template.

Template: S01_Template-NGFW

Basic [Edit](#)

Template Name	Type	Organization	Firewall Service
S01_Template-NGFW	sdwan-post-staging	Student01	NextGen Firewall

Device Type

Name	Type
SDWAN	sdwan-post-staging

Controllers

Controller-01

Subscription

Solution Tier	Bandwidth	License Period
Premier-Secure-SDWAN	25	1

Analytics

Analytics Cluster
Analytics

Buttons: [Cancel](#) [Back](#) [Save](#) [Re-Deploy](#) [Clean & Recreate](#)

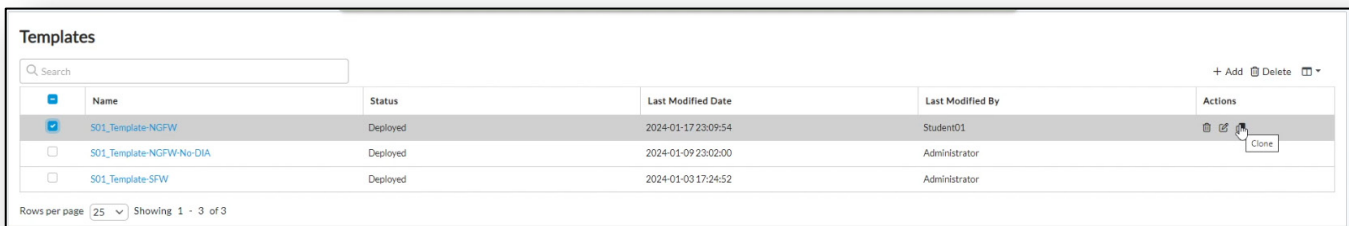
Step 9. Clone the Sxx_Template-NGFW workflow.

Next you will create a clone of the Sxx_Template-NGFW. The cloned workflow will have the same properties as the original workflow.

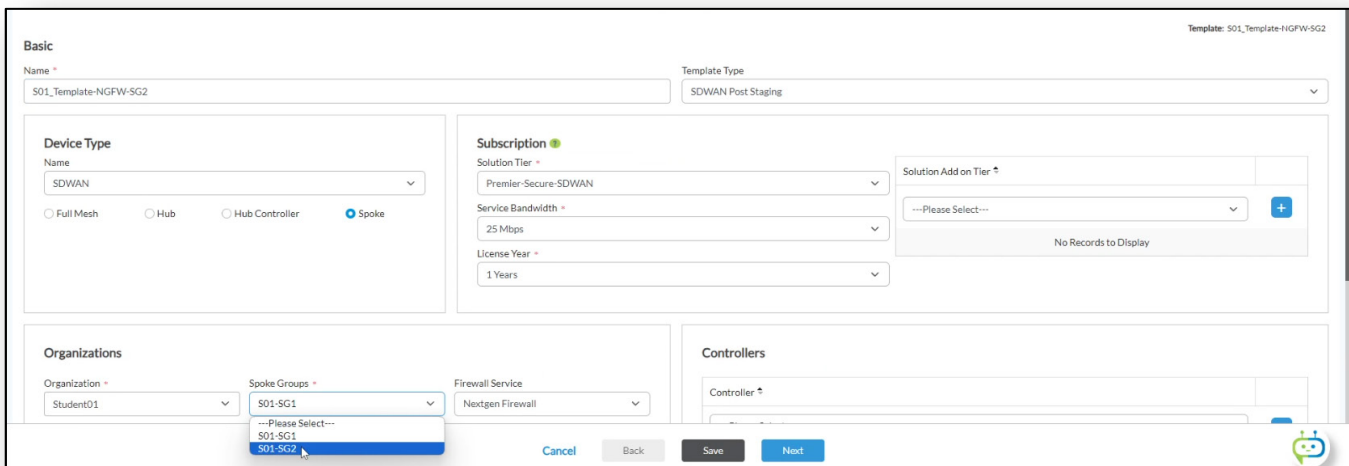
- a. Navigate to *Director View > Workflows > Template > Templates*.
- b. In the Template Workflow table, check the box next to the Sxx-Template-NGFW.

Note the Actions buttons that appear on the right side of the table.

- c. Click the *Clone* button to create a clone of the workflow.



- d. Rename the cloned workflow to Sxx_Template-NGFW-SG2, where Sxx refers to your assigned student number.
- e. In the *Organizations* settings, change the spoke group to Sxx-SG2.

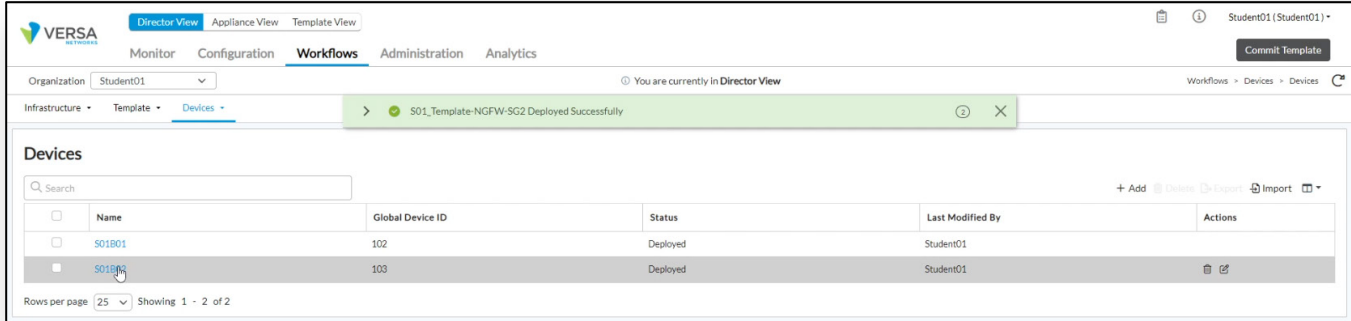


- f. Click the *Next* button until you reach the *Review* page.
- g. In the *Review* page, click *Deploy* to save the workflow and create the new template.

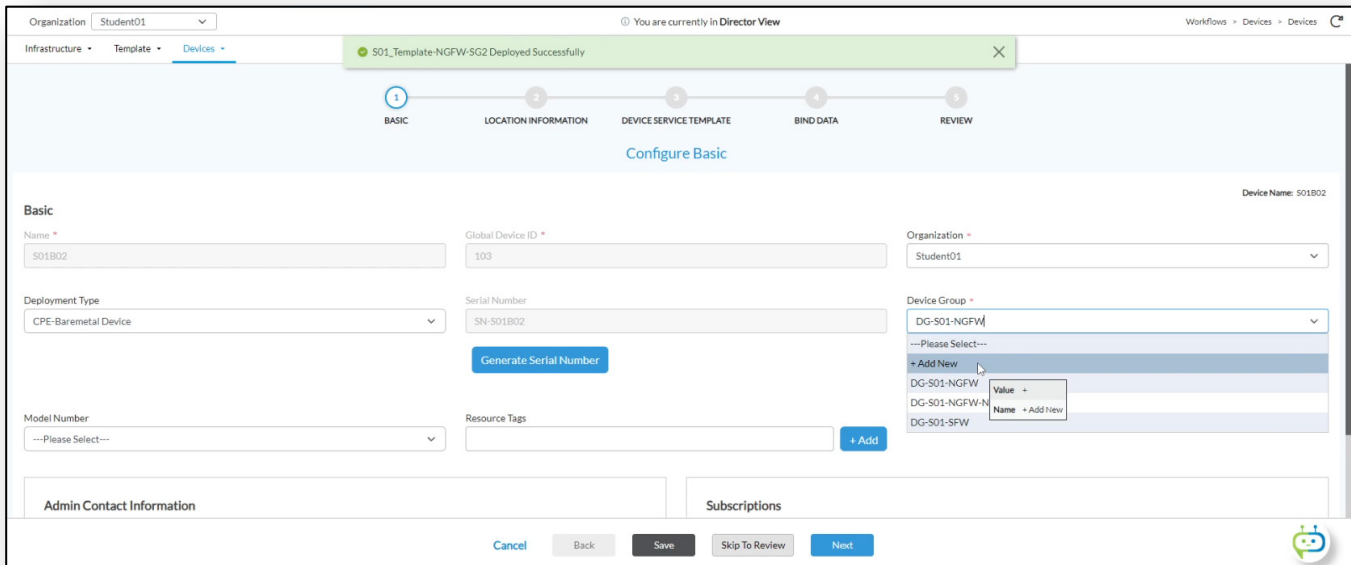
You should now have two templates for spoke groups. The only difference between the templates is the spoke group to which they are assigned.

Next you will re-assign branch B02 to a new device group. The new device group will reference the SG2 template.

- h. Navigate to *Workflows > Devices > Devices*.
- i. From the *Devices* workflow table, click on branch SxxB02 to modify the B02 device.



- j. In the Basic page, add a new device group.



- k. Name the new device group Sxx-DG-SG2, where Sxx is the student number you have been assigned.
- l. Select the Sxx_Template-NGFW-SG2 template as the main device template.

- m. Click the *OK* button to finish creating the device group.

This will take you back to the device workflow and set the new device group as the assigned device group.

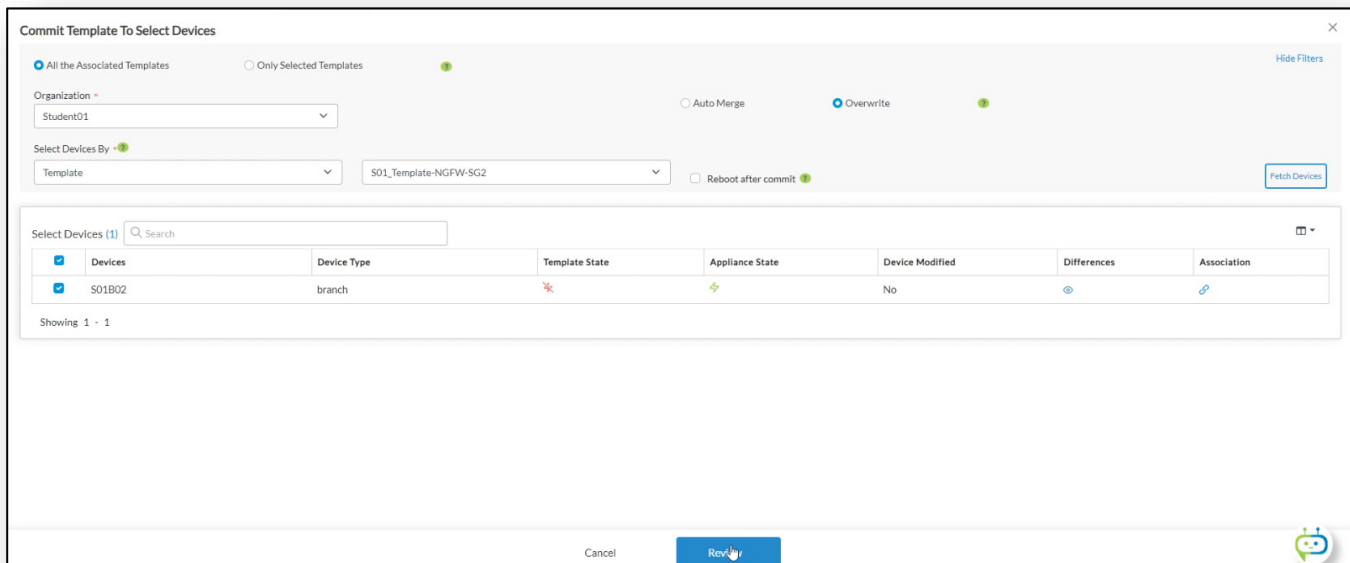
- n. Click the *Next* buttons until you reach the *Review* page.
- o. On the *Review* page, click the *Re-Deploy* button to update the device properties.

Commit the Sxx_Template-NGFW-SG2 template

- p. Click the *Commit Template* button.
- q. In the *Commit Template to Select Devices* page:
 - Select your organization in the Organization drop down
 - Choose Select Devices By: Template
 - Choose template Sxx_Template-NGFW-SG2
 - Click the Fetch Devices button

Your B02 device should be listed.

- r. Check the box next to your B02 device and click *Review*.



Commit Template To Select Devices

All the Associated Templates Only Selected Templates Hide Filters


Organization Auto Merge Overwrite +

Select Devices By Reboot after commit Fetch Devices

Select Devices (1) ⌵

Devices	Device Type	Template State	Appliance State	Device Modified	Differences	Association
<input checked="" type="checkbox"/> S01B02	branch	*	+	No	⊕	🔗

Showing 1 - 1

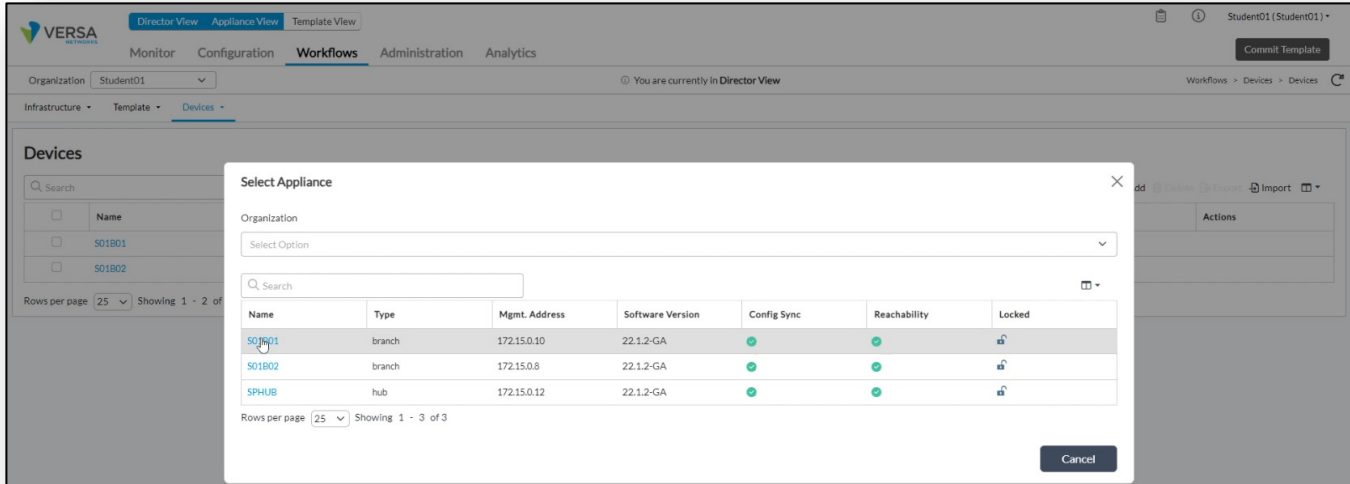
Cancel 

- s. On the Review Page, click the *Commit* button to reprogram the device with the new settings.

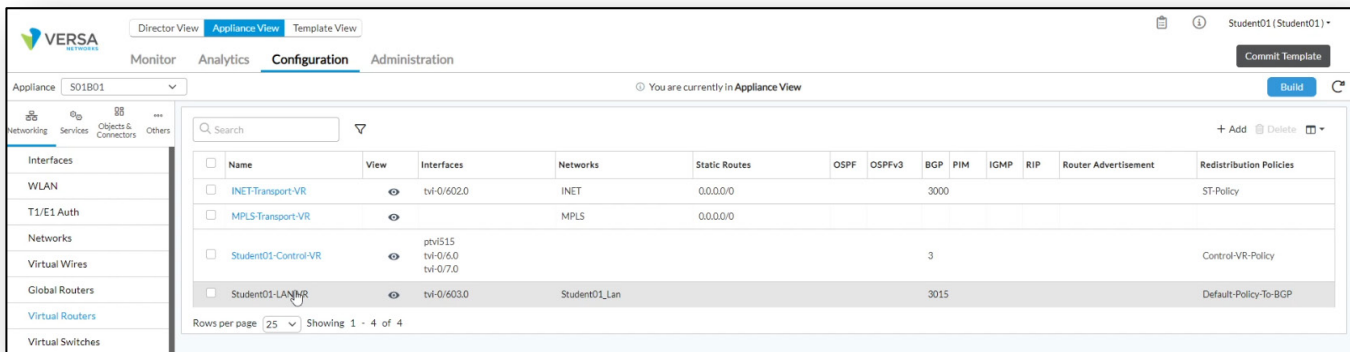
Step 10. Review the Spoke to Spoke Direct Results

In the next exercise you will review the routing results of placing 2 devices in different spoke groups with Spoke to Spoke Direct.

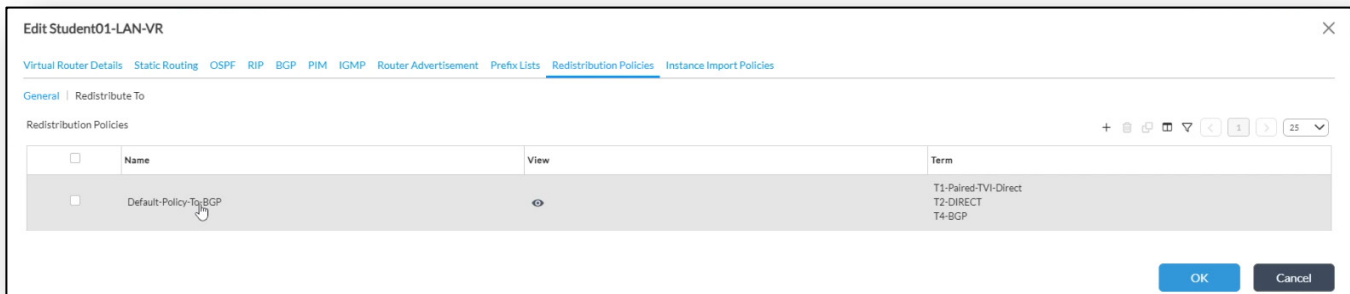
- a. Navigate to Appliance View and select your B01 device from the device list.



- b. In the B01 branch device, navigate to *Configuration > Networking > Virtual Routers > Student-LAN-VR*.



- c. In the LAN-VR virtual router, click the *Redistribution Policies* tab
- d. Click on the *Default-Policy-To-BGP* policy.



Identify the extra community value added to the BGP and Direct routes. This is the community value that you set in the spoke groups.

Note: To avoid community value overlaps in a multi-tenant system, Versa Director only asks for the 2nd part of the community value in the spoke group. The first part (in this case the 8020: prefix) is assigned by Versa Director to ensure that your spoke group communities remain unique in the system.

Edit Redistribution Policy ✕

Name *
Default-Policy-To-BGP

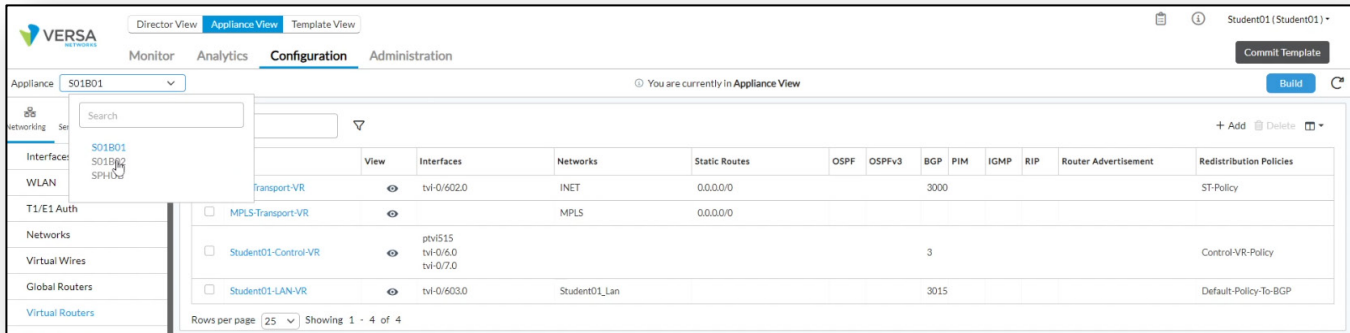
Terms + ✕ ↺ ↻ ↕ ↴ ↵ ↶ ↷ ⏪ 1 ⏩ 25 ▾

<input type="checkbox"/>	Term Name	Match				Actions				
		Protocol	Address	Area	Well Known Community	Nexthop	Accept/Reject	Set Community	Set Extended Community	Set Local Preference
<input type="checkbox"/>	T1-PairedT...	direct	169.254.0.0/16				Reject			
<input type="checkbox"/>	T2-DIRECT	direct					Accept	8001:104 8000:1 8010:1		110
<input checked="" type="checkbox"/>	T4-BGP	bgp					Accept	8001:104 8000:1 8010:1		110

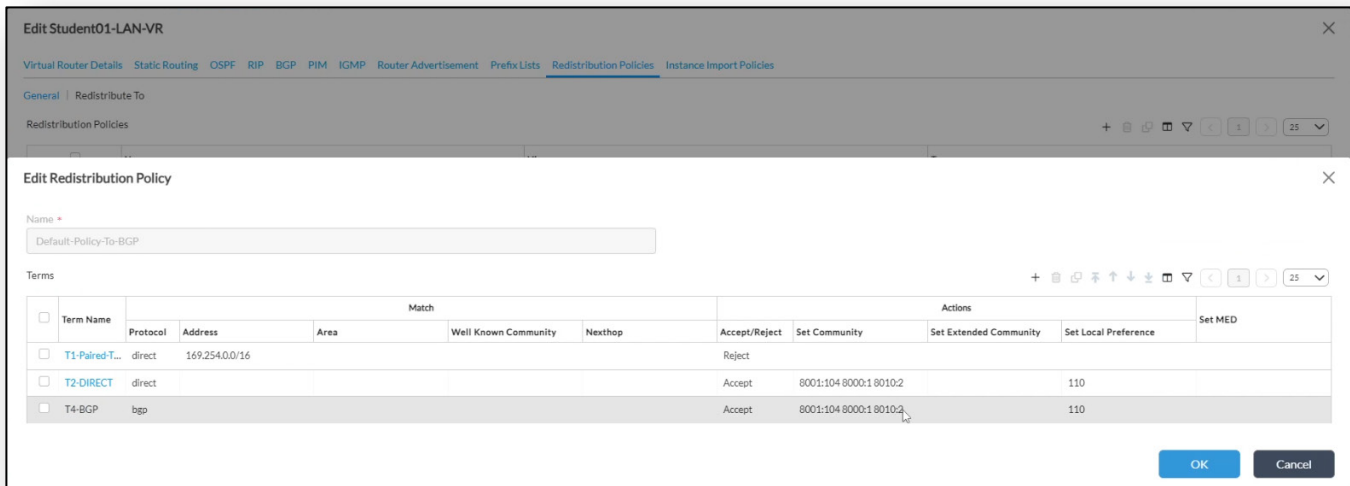
OK
Cancel

- e. Click the *Cancel* button until you have exited the virtual router configuration.
- f. Click *Yes* to the cancel prompt when prompted.

- g. Switch to the B02 branch device by selecting the B02 device from the *Appliance* drop down menu.

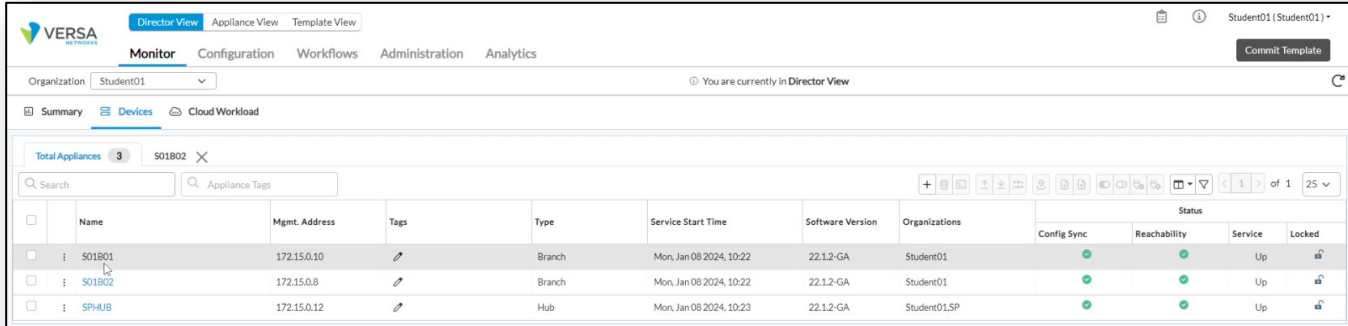


- h. Open the LAN virtual router on the B02 device.
- i. In the LAN virtual router, open the *Redistribution Policies* tab
- j. Click on the *Default-Policy-To-BGP* policy to view the communities assigned on branch B02. Branch B02 should have the community associated with spoke group 2.

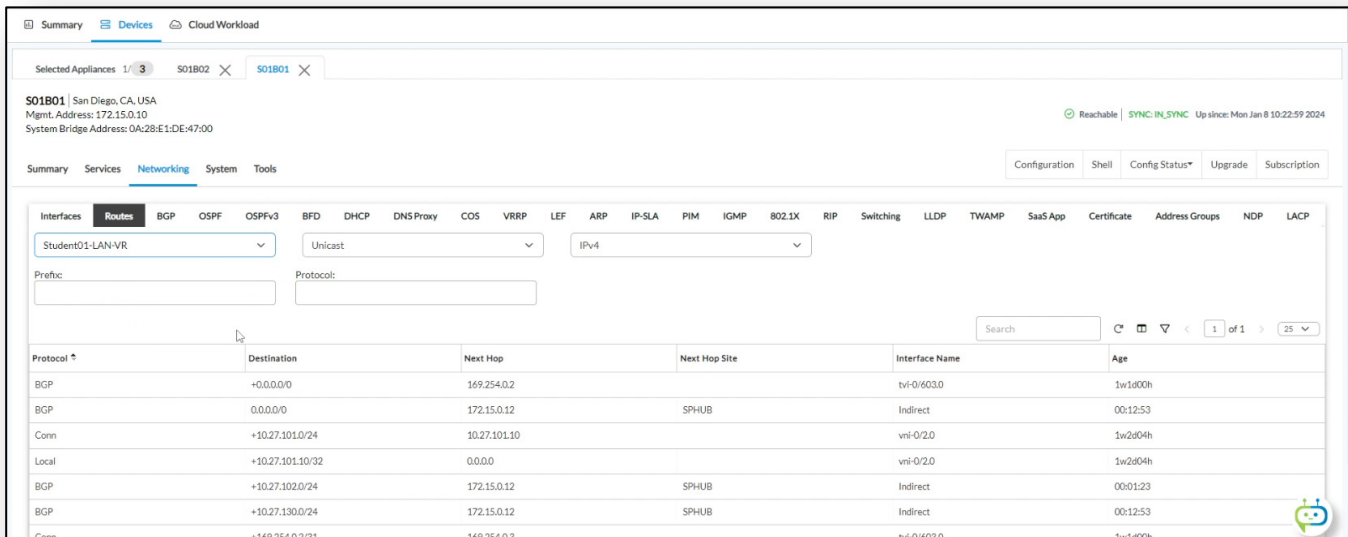


- k. Click the *Cancel* button until you exit the virtual router configuration.

- l. Navigate to *Monitor > Total Appliances*.
- m. In the appliance list, select the B01 branch device. The B02 device should already be opened in a tab.



- n. In the SxxB01 device Monitor dashboard, navigate to *Networking > Routes*.
- o. Select the LAN-VR virtual router from the drop down menu.



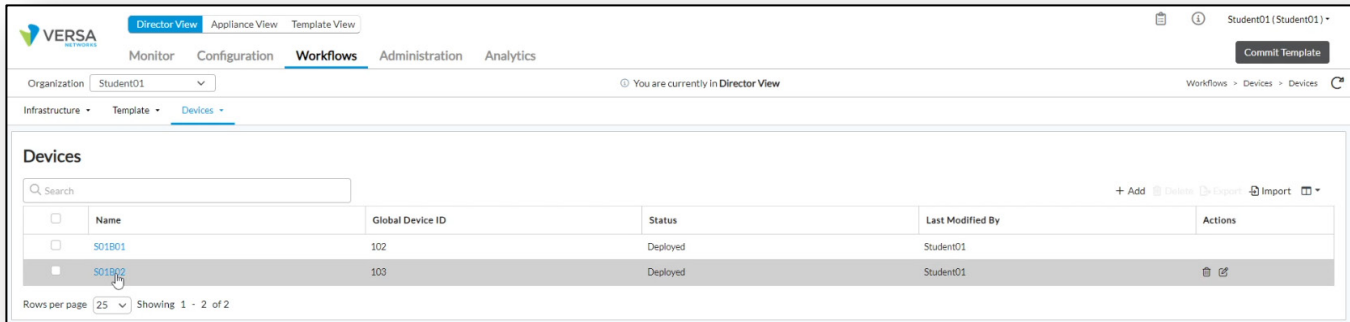
Note that the LAN routes associated with branch B02 list the SPHUB-NEW as the next-hop device, as the B02 device is in a different spoke group.

Protocol	Destination	Next Hop	Next Hop Site	Interface Name	Age
BGP	+0.0.0/0	169.254.0.2		tv1-0/603.0	1w1d00h
BGP	0.0.0/0	172.15.0.12	SPHUB	Indirect	00:12:53
Conn	+10.27.101.0/24	10.27.101.10		vni-0/2.0	1w2d04h
Local	+10.27.101.10/32	0.0.0.0		vni-0/2.0	1w2d04h
BGP	+10.27.102.0/24	172.15.0.12	SPHUB	Indirect	00:01:23
BGP	+10.27.130.0/24	172.15.0.12	SPHUB	Indirect	00:12:53
Conn	+169.254.0.2/31	169.254.0.3		tv1-0/603.0	1w1d00h

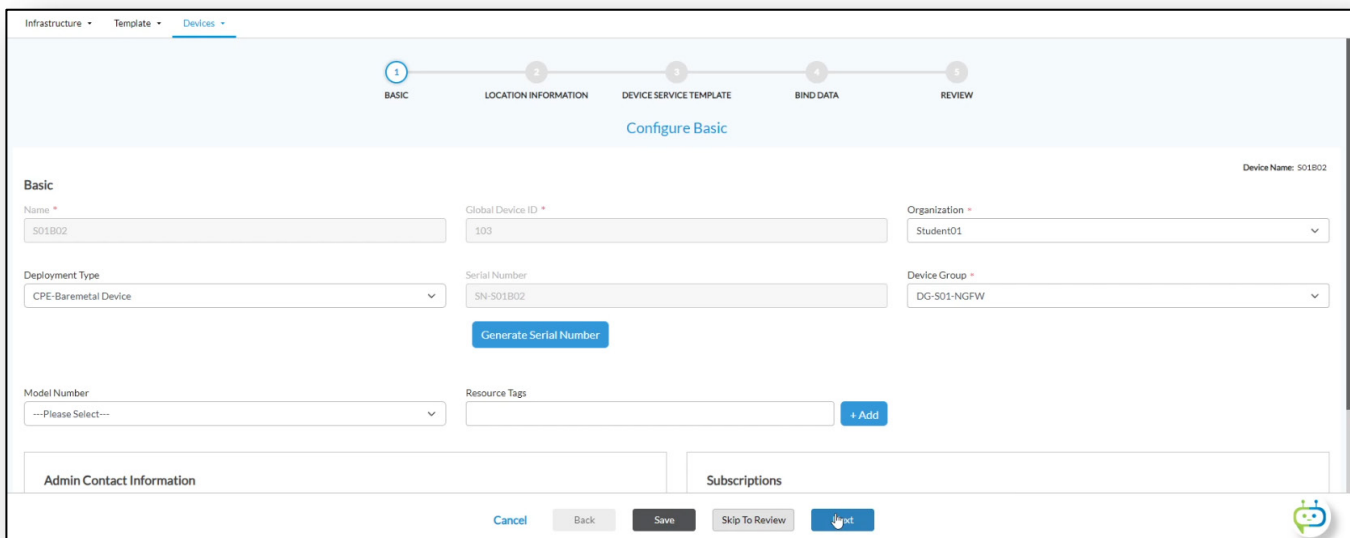
Step 11. Spoke to Spoke Direct - Devices in the same Spoke Group

Next you will place both devices in the same spoke group. Because both devices are in the same spoke group, and the topology is set to Spoke to Spoke Direct, the devices should form direct tunnels to each other (full mesh between devices in the same group).

- a. Navigate to *Director View > Workflows > Devices > Devices* and locate your B02 branch device in the device list.
- b. Click on the B02 device to open its properties.



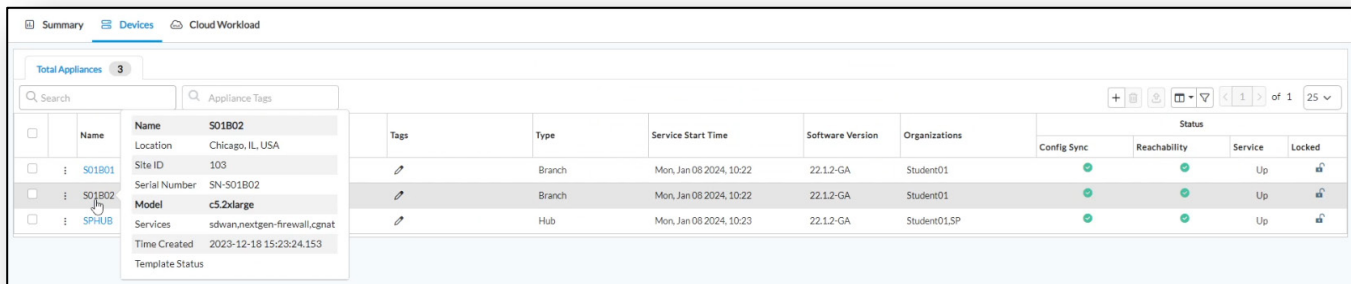
- c. Assign branch B02 to the DG-Sxx-NGFW device group.



- d. Click the *Next* button until you reach the Review page.
- e. In the *Review* page, click the *Re-Deploy* button to assign the new properties to the B02 device.

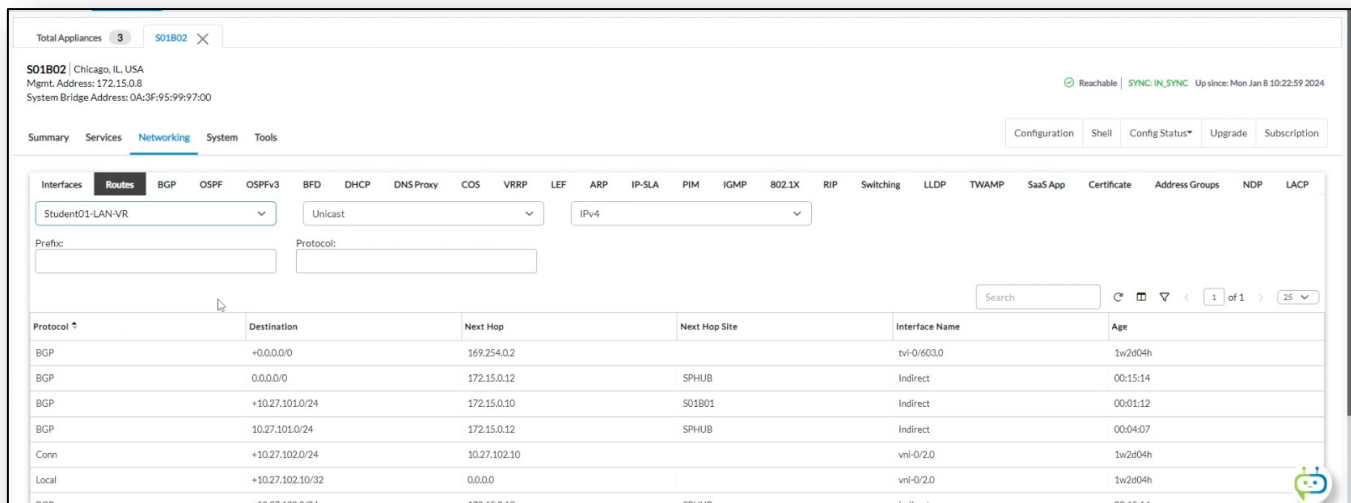
Next you will commit the template to the devices.

- f. Click *Commit Template*.
- g. From the *Commit Template to Select Devices* dialog:
 - Set the Organization to your organization value
 - Select Devices By: Template
 - Choose the Sxx_Template-NGFW template
 - Click *Fetch Devices*
 - Select the SxxB02 device from the list (or select both devices)
 - Click the *Review* button
- h. On the Review page, click the *Commit* button to apply the changes.
- i. Navigate to *Monitor > Devices > Total Appliances*.
- j. Click on your B02 branch device.



- k. Navigate to *Networking > Routes*.
- l. Select the LAN-VR routing instance from the drop-down menu.

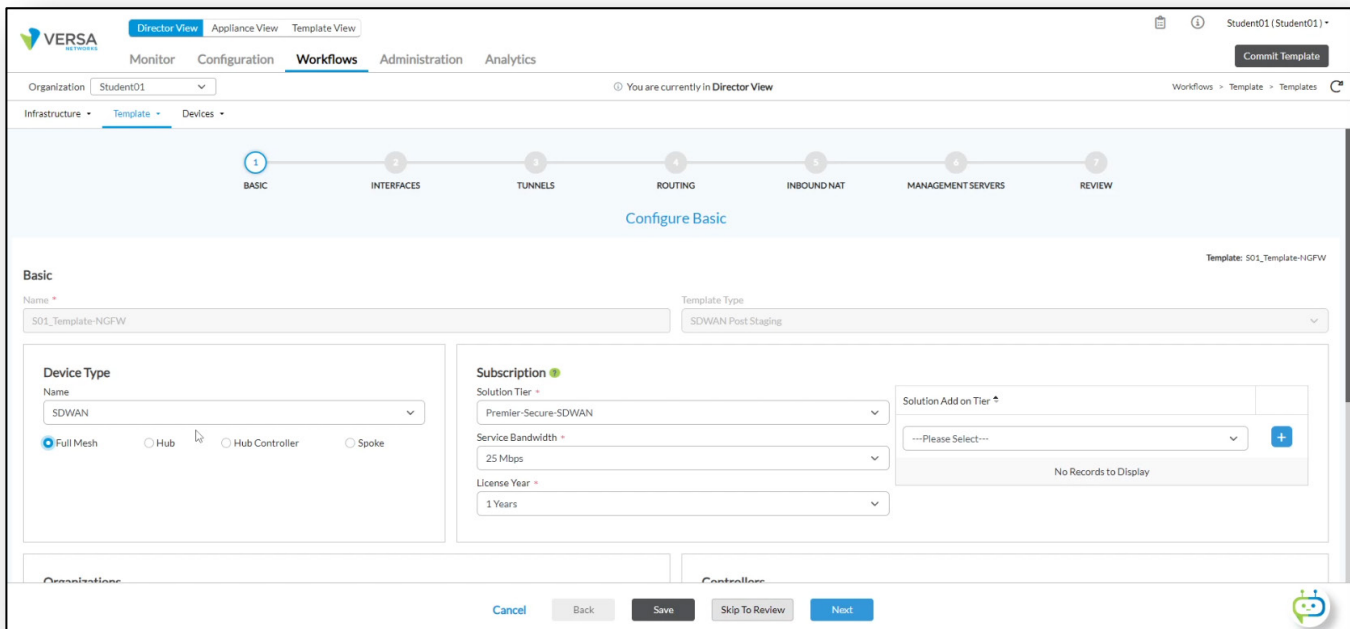
Note that there are 2 routes to the branch B01 LAN (one direct route to the B01 device, and another route to the SPHUB-NEW device). The + symbol in front of one of the routes indicates that it is the active route. The other route is a backup route.



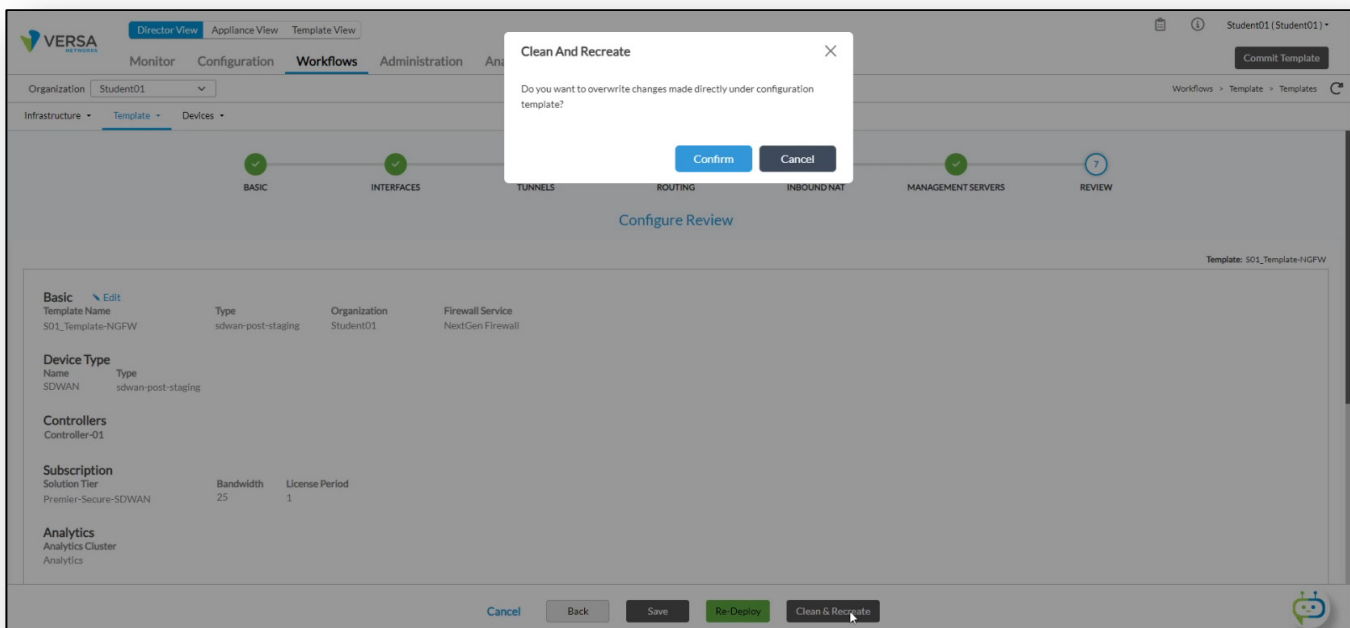
Step 12. Reset the lab environment

In the next steps you will reset the lab environment, which includes resetting the Sxx_Template-NGFW workflow back to the Full Mesh topology type. You will then commit the template to your devices to configure them in a full mesh topology.

- a. Navigate to *Workflows > Template > Templates*.
- b. Locate the Sxx_Template-NGFW template workflow, then click on the workflow to open it.
- c. In the Sxx_Template-NGFW workflow, change the Device Type to *Full Mesh*.

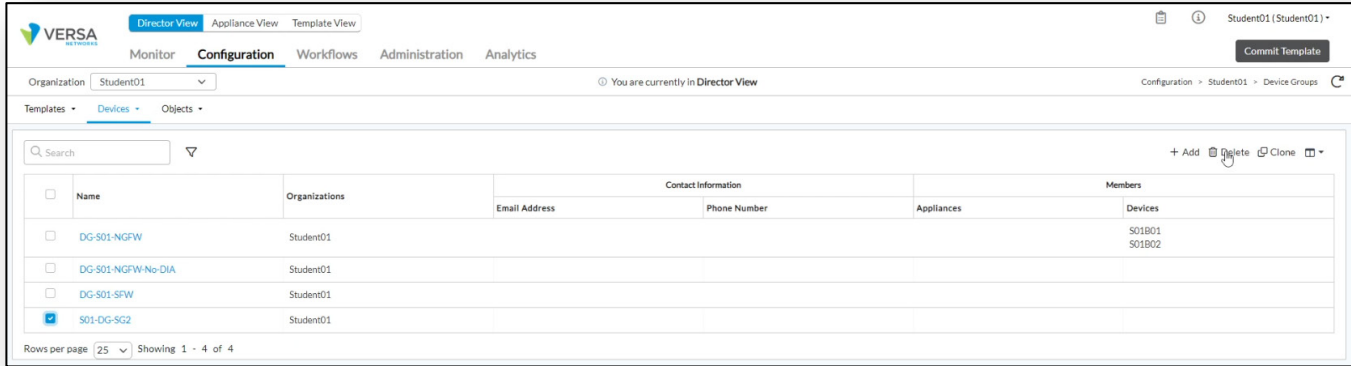


- d. Click the *Next* button until you reach the *Review* page.
- e. In the *Review* page, click on the *Clean & Recreate* button to save the workflow and rebuild the template.
- f. Click *Confirm* when prompted.



Next you will remove the Sxx-DG-SG2 device group.

- g. Navigate to *Configuration > Devices > Device Groups*.
- h. Locate the Sxx-DG-SG2 spoke group and check the box next to the spoke group to select it.

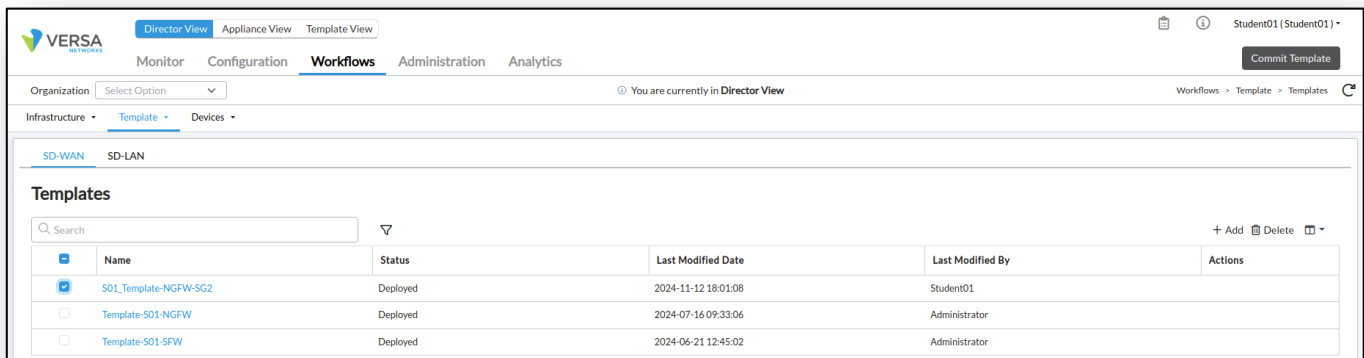


- i. Click on the *Delete* button in the top right to delete the device group.

IMPORTANT: Ensure that you are deleting the device group that you added for this lab exercise!

Next you will remove the Sxx_Template-NGFW-SG2 template workflow, which will also remove the associated template.

- j. Navigate to *Workflows > Template > Templates*.
- k. Locate the Sxx_Template-NGFW-SG2 workflow, where Sxx refers to the student ID assigned to you.
- l. Check the box next to the template to select it, and then click the *Delete* button in the top right corner.



- m. Confirm the deletion when prompted.

Finally, you will commit the Sxx_Template-NGFW template to your devices to rebuild and apply their configurations.

- n. Click the *Commit Template* button.
- o. In the Commit Template to Select Devices dashboard:
 - Select your organization from the Organization drop down;
 - Select Devices By: Template;
 - Select the Sxx_Template-NGFW template from the template drop down;
 - Click *Fetch Devices* – your two branch devices should be displayed;
 - Check the boxes next to the devices to select both branch devices
- p. Click the *Review* button.
- q. In the Review page, click *Commit*.

Commit Template To Select Devices

Organization: Student01

Select Devices By: Template (S01_Template-NGFW)

Devices	Device Type	Template State	Appliance State	Device Modified	Differences	Association
<input checked="" type="checkbox"/> S01B02	branch	*	+	No	👁	🔗
<input checked="" type="checkbox"/> S01B01	branch	*	+	No	👁	🔗

Showing 1 - 2

Buttons: Cancel, Review

Commit Template To Devices Review

Please review your devices before you commit template.

Devices	Device Type	Template State	Appliance State	Device Modified	Differences	Association
<input checked="" type="checkbox"/> S01B02	branch	*	+	No	👁	🔗
<input checked="" type="checkbox"/> S01B01	branch	*	+	No	👁	🔗

Showing 1 - 2

Buttons: Back, Commit, Schedule & Commit



STOP! Notify your instructor that you have completed this lab.

DIRECT INTERNET ACCESS

The Versa Networks lab environment consists of a fixed, pre-configured topology that will allow you to explore, configure, and manage Versa Networks CPEs by using Versa Director, the central management and orchestration platform for a Versa Secure SD-WAN solution. After completing this lab, you will be able to:

- Configure Direct Internet Access, or DIA for Internet Breakout on a branch device
- Verify the routing tables and default routes for DIA configured devices.

In this lab you will be assigned two CPE devices (Branch devices) for configuration and monitoring. The branch devices are named after the student ID that you have been assigned.

The lab environment is accessed through Amazon Workspaces. Your student ID and workspace will be assigned by the instructor.

The remote desktop connection opens a remote workstation, where you will use various tools to navigate and configure the lab environment. The main tool you will use in this lab is Versa Director. Versa Director can be accessed by opening the Google Chrome browser on the Remote Desktop. The IP address of the Versa Director (from the remote workstation) is 10.27.1.10. Once you begin the lab, you may want to create a bookmark to Versa Director in the web browser on the remote desktop.

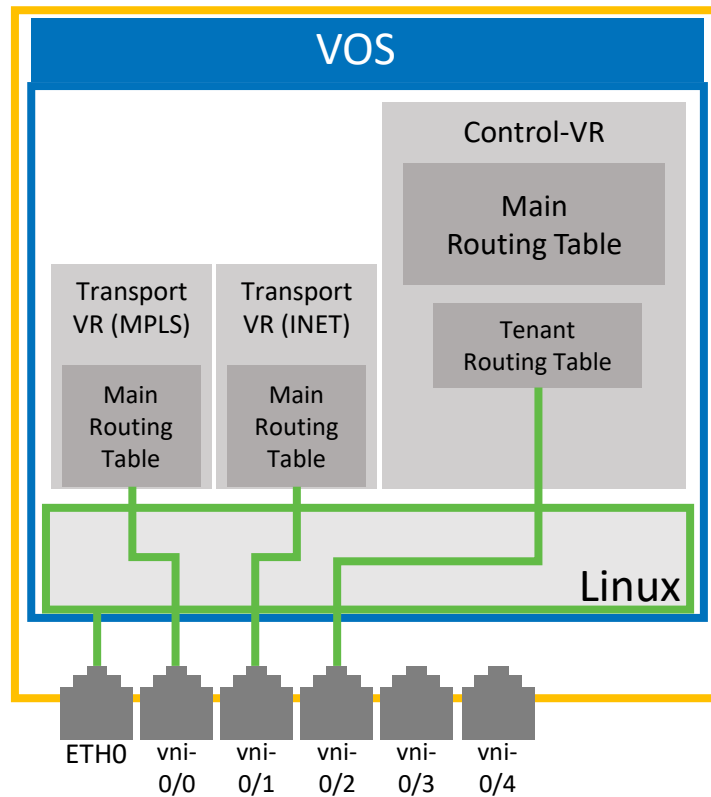
During certain lab parts, the lab guide will present sample output from the GUI or the CLI. The sample outputs are SAMPLES and represent the information as it appeared during the lab guide creation. Your output may vary in some ways (some devices may or may not be present, some routes may or may not be the same, etc.) Do not be alarmed if your results vary slightly from the results shown in the lab guide. The important thing is that the lab functions in the desired manner.

This lab guide will step you through some common tasks that are performed on Versa Director. After an introductory set of exercises, you will be asked to perform some basic tasks that will allow you to become more familiar with the environment.

The goal of this and all lab exercises is to help you gain additional skills and knowledge. Because of this, the lab guide contains additional instruction to supplement the student guides.

Now that we've discussed what is expected, let's get started!

Direct Internet Access, also referred to as Split Tunnel, allows data sessions from a private network to “break out” of the private network at a branch site, so Internet destined traffic does not have to cross a tunnel to reach a public destination. It does this by creating a bridge between a customer VRF routing table and the Public Internet facing virtual router. A default route is advertised from the public Internet router to the Tenant routing table that directs public-destined traffic to the INET routing table, where the traffic is forwarded to the public Internet after having basic Interface NAT applied.



All of the functions of basic DIA are implemented when a DIA tunnel is configured in a template workflow. A template workflow performs the following tasks:

- Two Tunnel interfaces are created. One is placed in the Tenant routing table, the other is placed in the INET routing table. The tunnel interfaces are created as “paired” tunnel interfaces, meaning they are logically connected to each other (like a virtual wire). The default security rules allow all traffic from a branch DTVI tunnel (ptvi zone) to be forwarded, so by default changes to the security policies are not required for traffic to pass. However, if you wish to restrict or monitor traffic that exits a DIA connection, the proper security policies should be put in place.
- An EBGp session is created between the two tunnel endpoints, which allows a default route to be advertised from the Internet virtual router to the tenant VRF routing table.
- A CGNAT policy is created which performs Interface NAT on all traffic that leaves the INET interface, so that traffic that is directed to the INET virtual router has a translated address when it leaves the device.

tvi-0/602	WAN side Split Tunnel interface betwe...	169.254.0.2/31	paired
tvi-0/603	LAN side Split Tunnel Interface betwe...	169.254.0.3/31	paired

In this lab exercise you will examine the routing tables that are present on the B01 device. You will modify the NGFW template associated with your organization to remove the existing DIA configuration. You will deploy the workflow, which will update the device template. You will commit the modified device template to your branch devices. You will examine the changes in the routing and interfaces. You will re-enable the DIA tunnel in the template workflow and commit the workflow to re-add the DIA functions to the device template. You will commit the updated template to your branch devices.

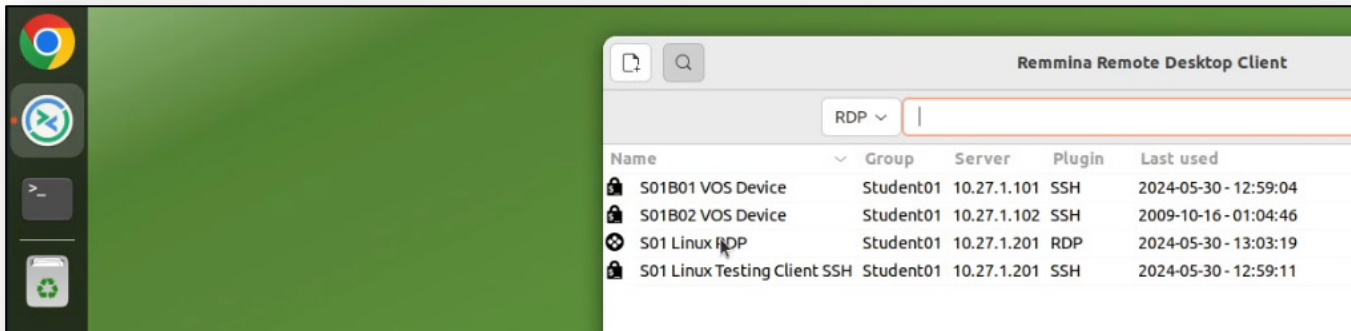
Step 1. Open a remote desktop session to the testing client

Begin the lab by connecting to the remote desktop in AWS. You will use two main applications: Google Chrome (to connect to Versa Director) and Remmina.

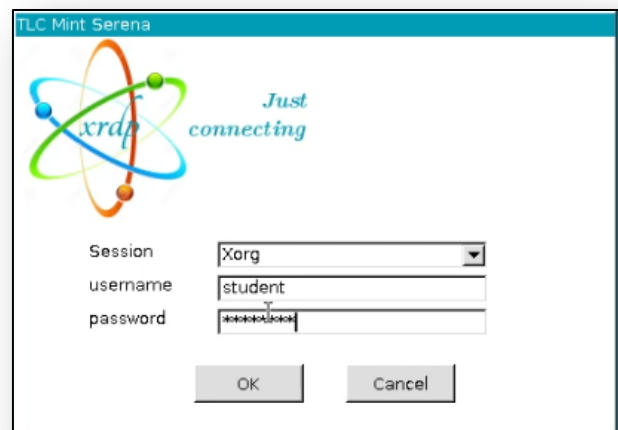
- a. In the remote desktop, open the Remmina application.

In the Remmina application you will use the Linux RDP connection to connect to the testing client and generate web sessions to the Internet. The password for the RDP session is versa123.

- b. In the Remmina application, open the Linux RDP connection.



If you see a Connection Log window appear, click the OK button to continue. Enter the password versa123 when Prompted.

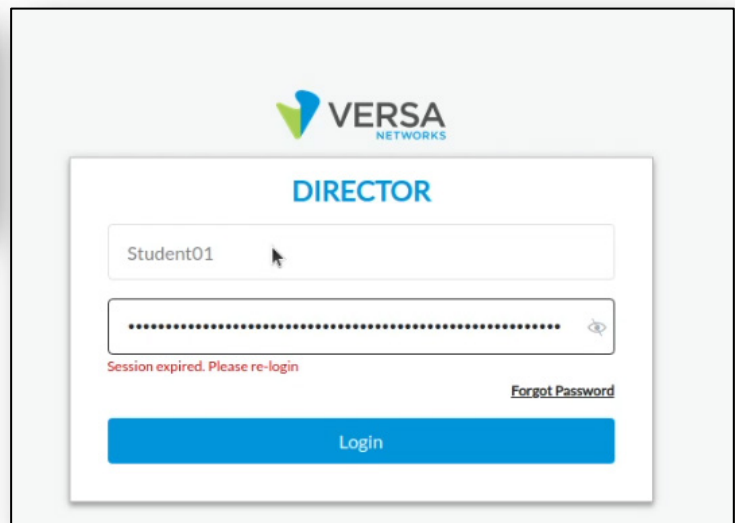
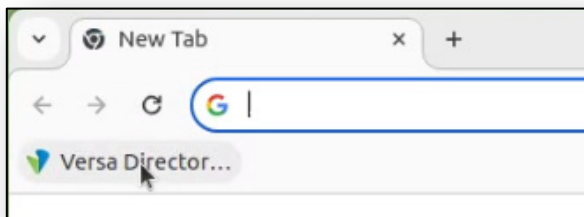


- c. In the testing client, open the Chromium browser.

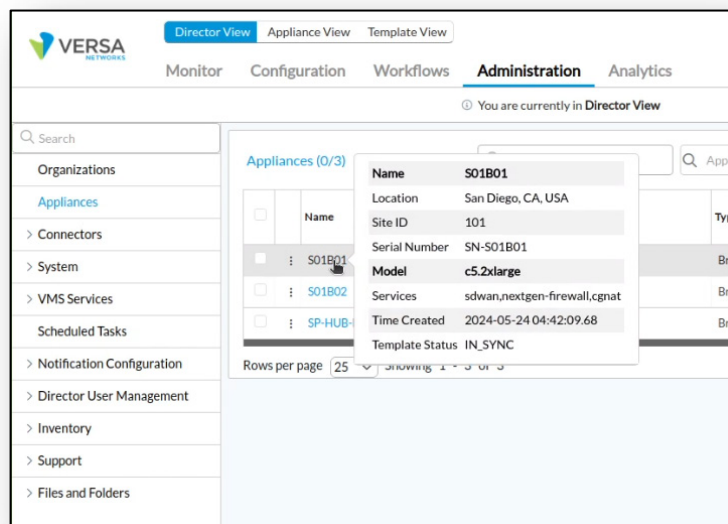
Note that depending on your environment, it may take up to 30 seconds for the remote browser to start properly.

Note the bookmarks in the bookmark bar.

- d. Click on two or more bookmarks to open pages to those destinations. It does not matter which you choose. You should be able to open the sites.
- e. Minimize the Remmina application window to return to the remote desktop.
- f. On the main remote desktop (not the Linux testing client), open the Google Chrome browser.
- g. In the Google Chrome browser, locate the bookmark to the Versa Director.
- h. Click the bookmark to open the Login page for Versa Director, then login using your Versa Director student name and password.



- i. In Versa Director, navigate to *Administration* > *Appliances* and click on your B01 device to open the Appliance context where you can examine statistics and configuration of the device.



- j. Navigate to *Monitor > Devices > SxxB01 > Networking > Routes*.
- k. Select the student LAN-VR from the dropdown table to view the routes in your LAN VR.

You should see 2 default routes. One route is associated with the TVI tunnel interface, and the other route is associated with the hub. The route associated with the tunnel interface should be the active route (as indicated by the + symbol next to the route). This is because the route received over the tunnel interface is preferred over the route received from the hub.

The screenshot shows the 'Routes' configuration page for the 'Student01-LAN-VR' interface. The 'Routes' tab is selected, and the 'Unicast' and 'IPv4' options are chosen. The route count is 80. The table below shows the following routes:

Protocol	Destination	Next Hop	Next Hop Site	Interface Name	Age
BGP	+0.0.0.0/0	169.254.0.2		tvi-0/603.0	00:17:47
BGP	0.0.0.0/0	172.15.0.30	SP-HUB-New	Indirect	00:14:06

- l. Select the INET-Transport-VR routing table from the drop-down.

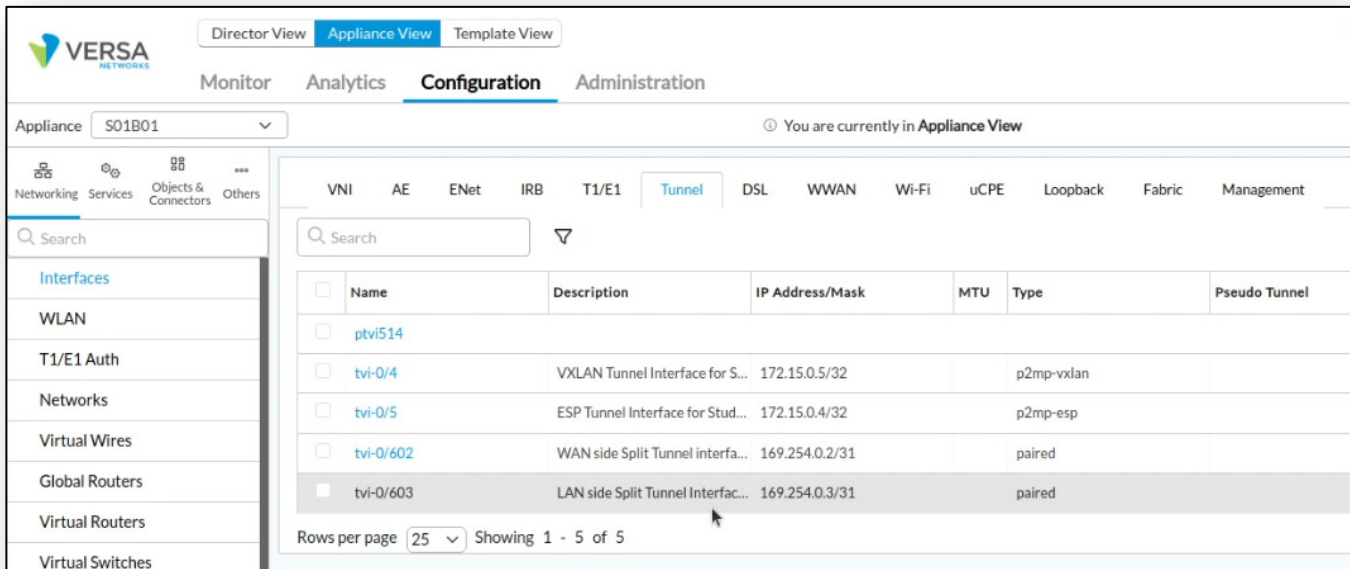
The INET-Transport-VR routing table should have a default route towards the public IP address of the service provider (in this case it is a private address 10.27.11.1).

The screenshot shows the 'Routes' configuration page for the 'INET-Transport-VR' interface. The 'Routes' tab is selected, and the 'Unicast' and 'IPv4' options are chosen. The route count is 17. The table below shows the following routes:

Protocol	Destination	Next Hop	Next Hop Site	Interface Name	Age
Static	+0.0.0.0/0	10.27.11.1		vni-0/0.0	00:18:20
Connected	+10.27.11.0/24	10.27.11.101		vni-0/0.0	00:18:20

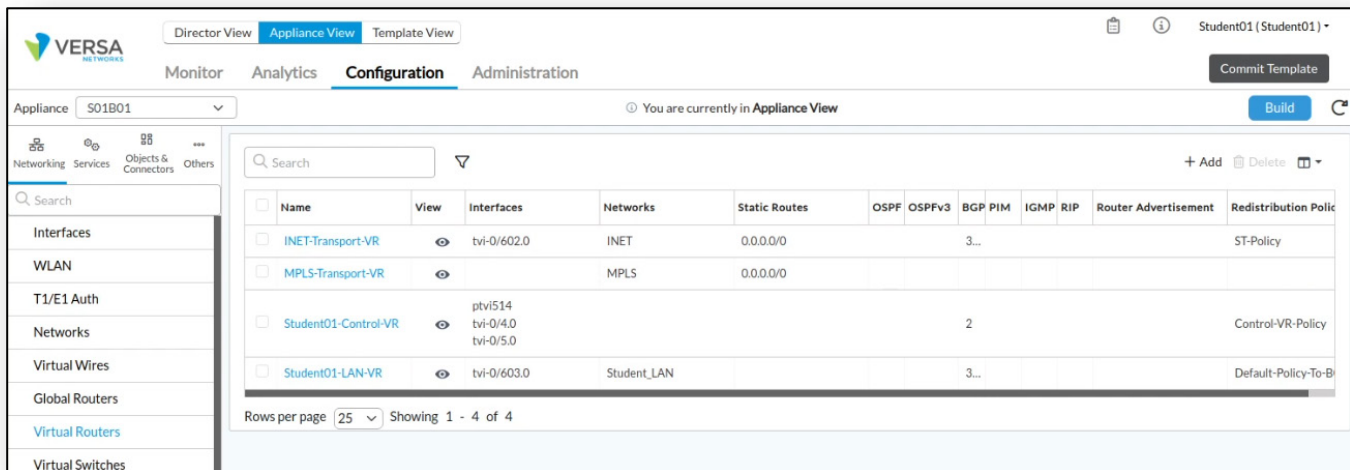
m. Navigate to *Configuration > Networking > Interfaces > Tunnel* to view the pre-configured tunnel interfaces.

Note the interfaces that are of type “paired” and their descriptions.



n. Navigate to *Configuration > Networking > Virtual Routers* and identify where the tunnel interfaces are placed.

You should see one of the tunnel interfaces in the INET-Transport-VR and one in your student LAN-VR routing table.



This allows the two routing tables (in different virtual routers) to communicate.

- o. Navigate to *Services > CGNAT > Rules* to view the CGNAT rules information. Note that you should have multiple hits on the DIA-Rule CGNAT rule.

Name	Hit Count	Forward Packet Count	Forward Byte Count	Reverse Packet Count	Reverse Byte Count
DIA-Rule-Student01-LAN-VR-INET	1129	9778	1483001	36198	45496744
RFC_1918_NoTranslate	4	0	0	0	0
Speed-Test-INET	0	0	0	0	0
Speed-Test-MPLS	0	0	0	0	0

- p. Navigate to the *Services > NGFW > Sessions* dashboard and locate one of the sessions. Note that you may have to scroll to the right on the NGFW tab to locate the Sessions tab.

- q. Click on the Session Count number to display the session list:

Scroll through the session list until you locate a session associated with the browser pages that you opened. If you do not see a session associated with the pages you opened (normally due to session timeout), you can return to the RDP client and click more bookmarks to refresh the session list.

VSN ID	Session Count	Session Created	Session Closed
0	276	1406	1130

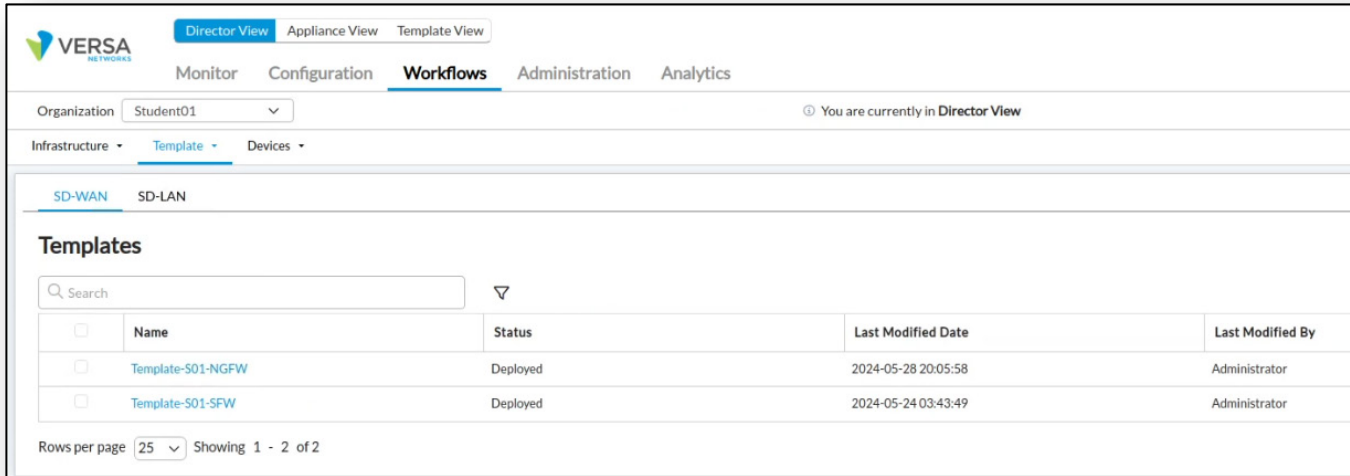
- r. After you locate an active session to one of the web pages, click on the > symbol next to the session to expand the view. Note that the session is marked with *SDWAN: No*, as the session does not cross the SD-WAN due to the Internet Breakout.

Application	Source IP	Destination IP	Protocol	Source Port
foxsports/(predef)	10.27.101.20	151.101.2.132	TCP	51914

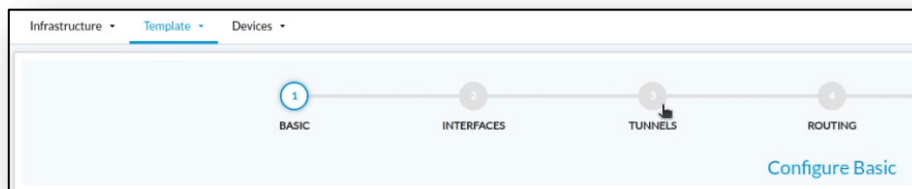
Application: foxsports/(predef)	Destination IP: 151.101.2.132	Destination Port: 443
Natted: Yes	Protocol: TCP	SDWAN: No
Session ID: 841	Source IP: 10.27.101.20	Source Port: 51914
VSN ID: 0	VSN Vid: 2	

Step 2. Remove the DIA connection

- a. Click the *Director View* button at the top of the page to return to Director View.
- b. In Director View, navigate to *Workflows > Template > Templates* to view the Template Workflows.
- c. Locate and click on the *Template-Sxx-NGFW* workflow to view the workflow configuration.



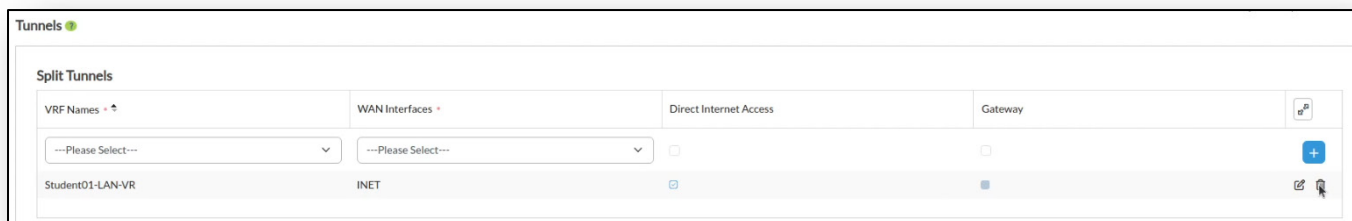
- d. In the NGFW template workflow, click on the *TUNNELS* button to go to the tunnels tab.



- e. In the TUNNELS tab, locate the *Split Tunnels* section.

Note that there is a split tunnel between the Student LAN-VR and the INET WAN interface, and the Direct Internet Access box is checked.

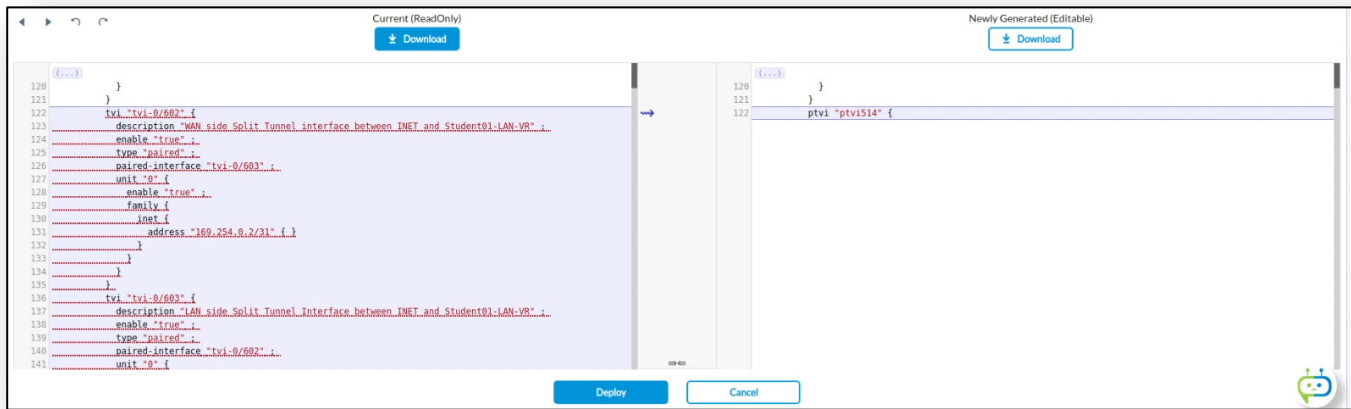
- f. Click the *Delete* icon next to the split tunnel to remove the split tunnel from the workflow.



- g. Click the *Skip to Review* button at the bottom of the page.
- h. In the Review page, click the *Re-Deploy* button to view and apply the changes to the workflow and template.
DO NOT CLICK THE CLEAN & RECREATE BUTTON!

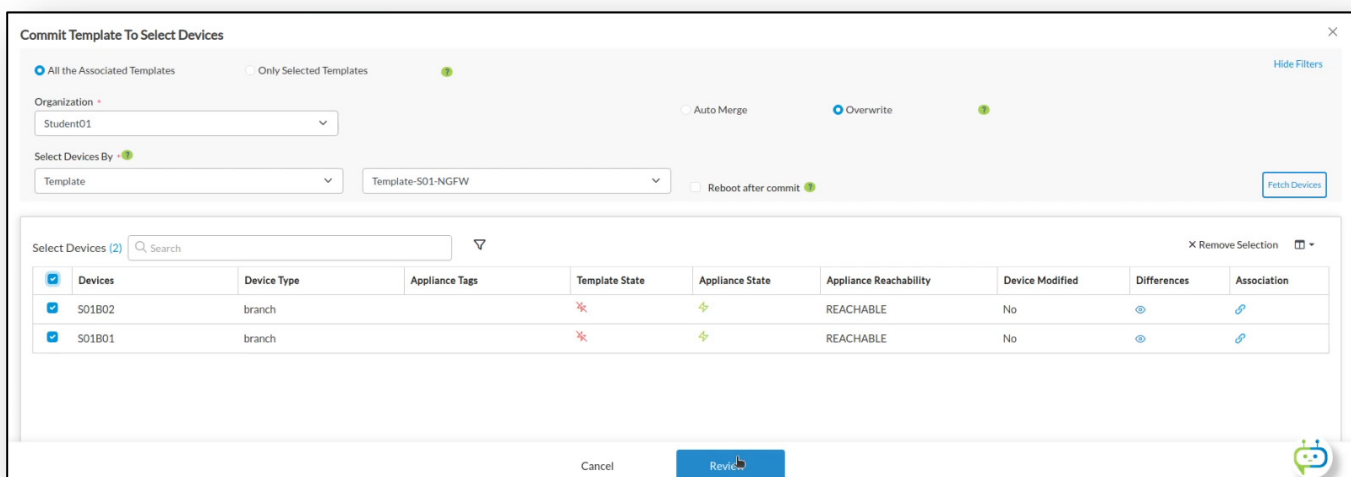
You will be presented with a review/compare window that shows the changes that will be applied to the template. The information on the left is what exists in the current template, and the information on the right is what will be present in the template after the deploy operation. Note that the TVI interfaces will be removed, as will many other parts of the configuration.

- i. Click the Deploy button to accept the changes and update the template.

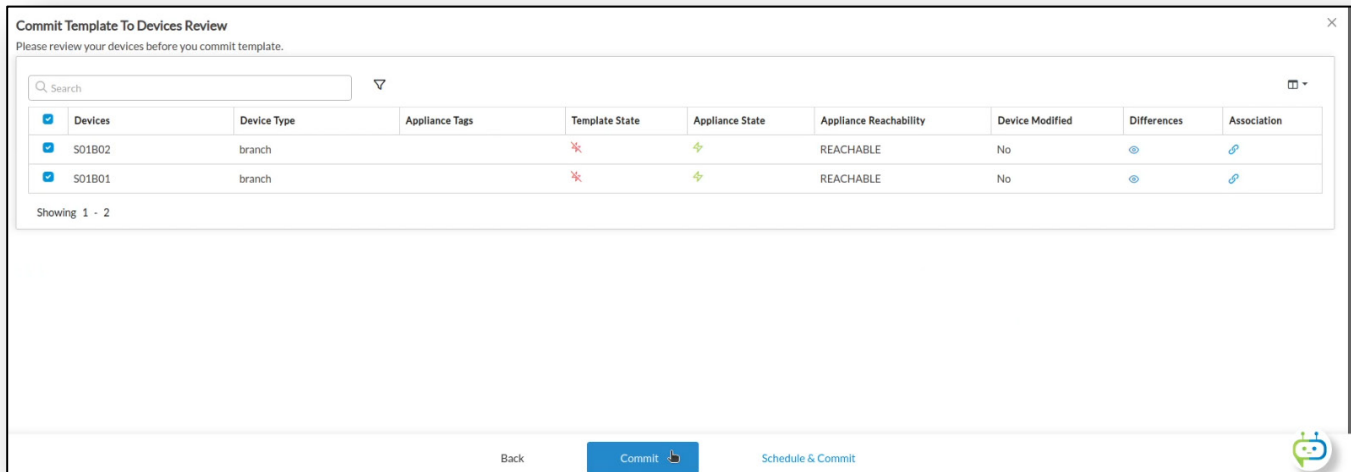


You have updated the NGFW device template. The next step is to apply those changes to your devices.

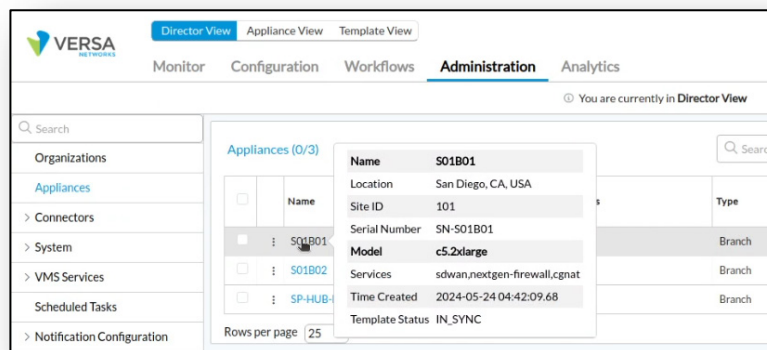
- j. Click the *Commit Template* button in the top right corner of the window.
- k. In the Commit Template to Select Devices window:
 - select your organization from the dropdown menu;
 - select the NGFW template in the Select Devices By field;
 - and click Fetch Devices to retrieve a list of devices that are associated with the template. Both of your branch devices should appear in the device list.
- l. Click the boxes next to the branch devices to select them.
- m. Click the *Review* button at the bottom of the window.



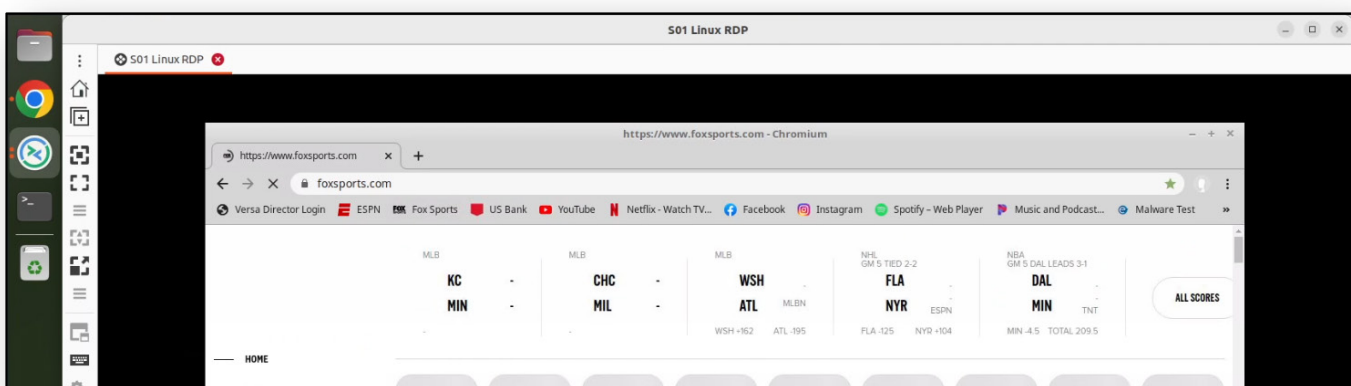
- n. In the *Review* page, click the *Commit* button to apply the changes to the devices.



- o. After the commit operation completes, navigate to the *Director View > Administration > Appliances* dashboard.
- p. Click on the B01 branch device to open the device in Appliance View.



- q. Locate and activate the Remmina application (RDP to the testing client) and click on some of the bookmarks in the remote browser to initiate new sessions.



- r. Return to the Versa Director window.
- s. In Versa Director Appliance View, navigate to *Devices > SxxB01 > Monitor > Services > SDWAN*.
- t. Click on the *Sessions* tab. The sessions to the web sites are now listed as SD-WAN sessions because they are routed through the Hub site (not DIA).

Application	Source IP	Destination IP	Protocol	Source Port	Destination Port	TX WAN Ckt	RX WAN Ckt	Remote Branch
unknown_tcp/(predef)	10.27.101.20	172.253.63.155	TCP	58786	443	MPLS:MPLS	--	SP-HUB-New
unknown_tcp/(predef)	10.27.101.20	108.138.85.73	TCP	37132	443	INET:INET	--	SP-HUB-New
unknown_tcp/(predef)	10.27.101.20	23.201.170.207	TCP	34488	443	MPLS:MPLS	--	SP-HUB-New
unknown_tcp/(predef)	10.27.101.20	146.75.32.84	TCP	33290	443	INET:INET	--	SP-HUB-New
dns/(predef)	10.27.101.20	8.8.8.8	UDP	50795	53	MPLS:MPLS	--	SP-HUB-New
dns/(predef)	10.27.101.20	8.8.8.8	UDP	56771	53	INET:INET	--	SP-HUB-New
dns/(predef)	10.27.101.20	8.8.8.8	UDP	35836	53	MPLS:MPLS	--	SP-HUB-New

- u. Navigate to the *Networking > Routes > Student-LAN-VR* dashboard.

There should only be one default route present in the Student LAN VR, and that route lists the SP-HUB as the next hop.

SO1B01 | San Diego, CA, USA
Mgmt. Address: 172.15.0.4
System Bridge Address: 0A:6D:DC:C8:25:00

Reachable | SYNC:IN_SYNC Up since: Thu May 30 11:54:47 2024

Summary Services **Networking** System Tools

Configuration Shell Config Status Upgrade Subscription

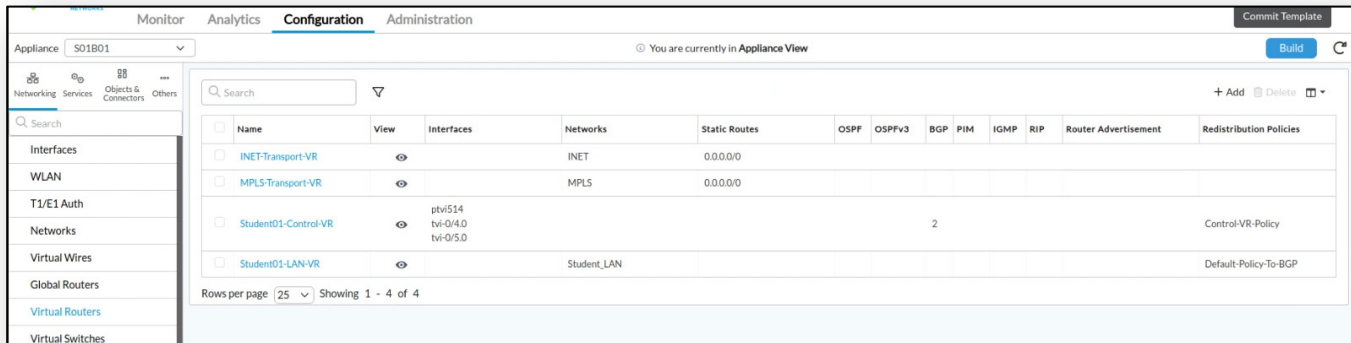
Interfaces **Routes** BGP OSPF OSPFv3 BFD DHCP DNS Proxy COS VRRP LEF ARP IP-SLA PIM IGMP 802.1X RIP Switching LLDP TWAMP SaaS App Certificate Ad

Student01-LAN-VR Unicast IPv4 Route Count: 72

Prefix: Protocol: --Select--

Protocol	Destination	Next Hop	Next Hop Site	Interface Name	Age
BGP	+0.0.0.0	172.15.0.30	SP-HUB-New	Indirect	00:19:11
BGP	+10.27.13.0/24	172.15.0.30	SP-HUB-New	Indirect	00:19:11

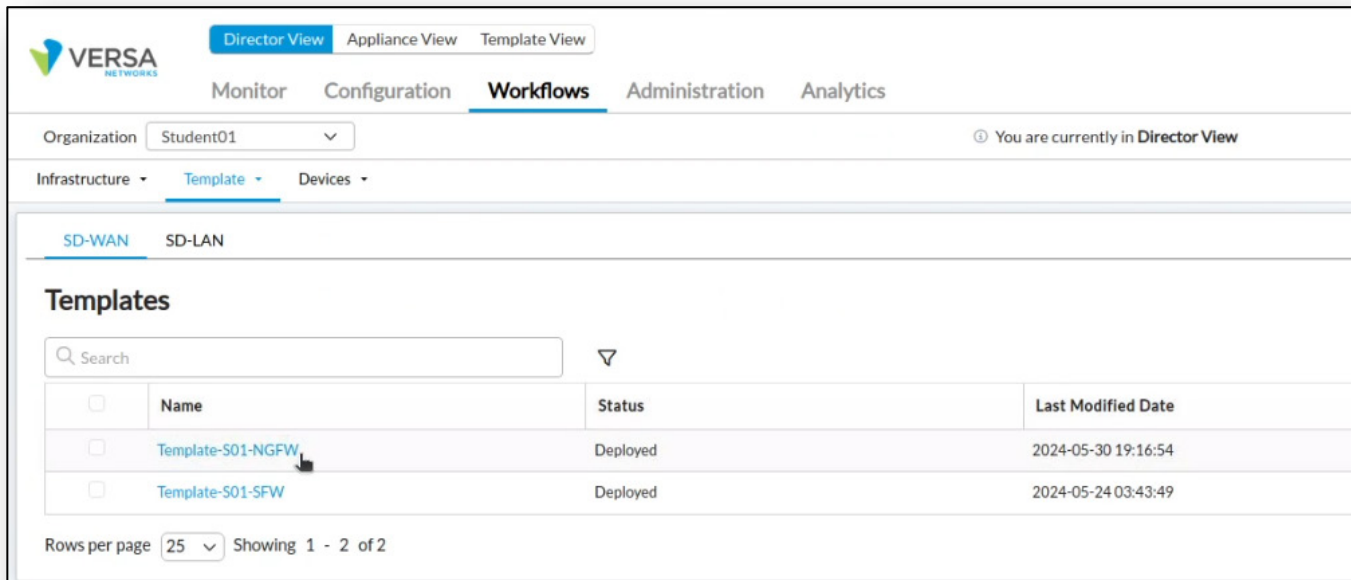
- v. Navigate to *Configuration > Networking > Virtual Routers* and view the virtual router interface assignments. Note that the two paired TVI interfaces are no longer present in the configuration.



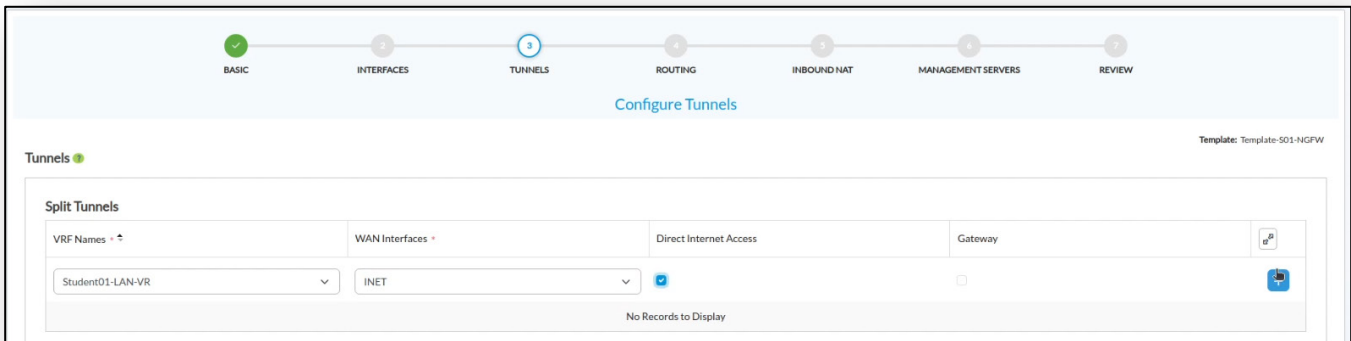
Step 3. Re-add the DIA

Next you will re-add the DIA configuration to the device template by using the Template Workflow.

- a. Return to Director *View > Workflows > Template > Templates*
- b. Click on the *Template-Sxx-NGFW* template workflow to open the workflow.



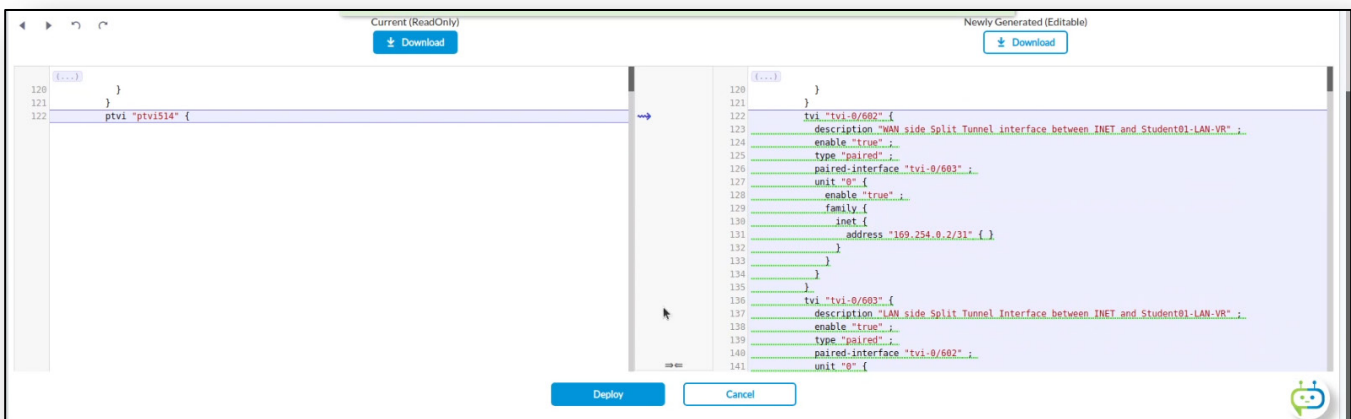
- c. Navigate to the Tunnels tab.
- d. In the Split Tunnels section, select your student LAN-VR in the VRF Names drop-down menu.
- e. Select the INET WAN interface.
- f. Select the Direct Internet Access check box.
- g. Click the blue + button to add the split tunnel to the workflow.



- h. Click *Skip to Review*.
- i. Click *Re-Deploy (DO NOT CLICK Clean & Recreate!)*

A window will display the changes that will be made to the existing template. Note that by adding the split tunnel to the workflow, many configuration items are created to provide the split tunnel features, including the addition of TVI interfaces, BGP sessions, and routing policies.

- j. Click the *Deploy* button to apply the changes to the template.



Step 4. Apply the changes

You have changed the device template. Now you must commit the changes to the devices to reprogram the branch devices.

- a. Click the Commit Template button
- b. In the Commit Template to Select Devices dialog, select your organization, the *Template-Sxx-NGFW* template, and then click the *Fetch Devices* button. Your branch devices should appear in the table.
- c. Check the boxes next to your branch devices.
- d. Click the Review button.

Commit Template To Select Devices

All the Associated Templates
 Only Selected Templates
 Hide Filters

Organization: Student01
 Auto Merge:
 Overwrite:

Select Devices By: Template
 Template: S01-NGFW
 Reboot after commit:
 Fetch Devices

Select Devices (2) X Remove Selection

<input checked="" type="checkbox"/>	Devices	Device Type	Appliance Tags	Template State	Appliance State	Appliance Reachability	Device Modified	Differences	Association
<input checked="" type="checkbox"/>	S01B02	branch		✖	⚡	REACHABLE	No	👁	🔗
<input checked="" type="checkbox"/>	S01B01	branch		✖	⚡	REACHABLE	No	👁	🔗

Cancel **Review**

- e. In the Review window, click the Commit button to reprogram the devices.

Commit Template To Devices Review

Please review your devices before you commit template.

X Remove Selection

<input checked="" type="checkbox"/>	Devices	Device Type	Appliance Tags	Template State	Appliance State	Appliance Reachability	Device Modified	Differences	Association
<input checked="" type="checkbox"/>	S01B02	branch		✖	⚡	REACHABLE	No	👁	🔗
<input checked="" type="checkbox"/>	S01B01	branch		✖	⚡	REACHABLE	No	👁	🔗

Showing 1 - 2

Back **Commit** Schedule & Commit

You have completed this lab. If you choose you can go back to the branch device in Appliance View and verify that the interfaces have been re-added to the device, the additional default route has been added to the LAN VR routing table, and that the preferred next-hop is the TVI interface, with the Hub device as a backup default route.



STOP! Notify your instructor that you have completed this lab.

VERSA APPLIANCE MANAGEMENT

The Versa Networks lab environment consists of a fixed, pre-configured topology that will allow you to explore, configure, and manage Versa Networks CPEs by using Versa Director, the central management and orchestration platform for a Versa Secure SD-WAN solution. After completing this lab, you will be able to:

- Identify when a device configuration is in sync or out of sync with Versa Director
- Import and Export device configurations
- Create device snapshots
- Restore device snapshots
- Manage operations on individual devices
- Manage security packages on individual devices
- Monitor system resources on an individual device

In this lab you will be assigned two CPE devices (Branch devices) for configuration and monitoring. The branch devices are named after the student ID that you have been assigned.

The lab environment is accessed through Amazon Workspaces. Your student ID and workspace will be assigned by the instructor.

The remote desktop connection opens a remote workstation, where you will use various tools to navigate and configure the lab environment. The main tool you will use in this lab is Versa Director. Versa Director can be accessed by opening the Google Chrome browser on the Remote Desktop. The IP address of the Versa Director (from the remote workstation) is 10.27.1.10. Once you begin the lab, you may want to create a bookmark to Versa Director in the web browser on the remote desktop.

During certain lab parts, the lab guide will present sample output from the GUI or the CLI. The sample outputs are SAMPLES and represent the information as it appeared during the lab guide creation. Your output may vary in some ways (some devices may or may not be present, some routes may or may not be the same, etc.) Do not be alarmed if your results vary slightly from the results shown in the lab guide. The important thing is that the lab functions in the desired manner.

This lab guide will step you through some common tasks that are performed on Versa Director. After an introductory set of exercises, you will be asked to perform some basic tasks that will allow you to become more familiar with the environment.

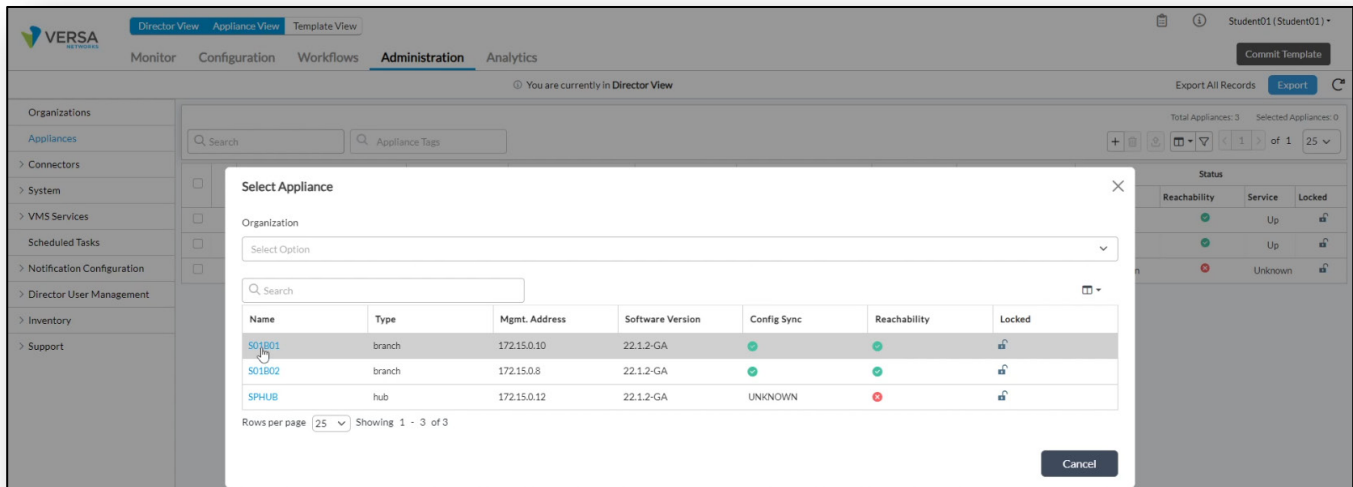
The goal of this and all lab exercises is to help you gain additional skills and knowledge. Because of this, the lab guide contains additional instruction to supplement the student guides.

Now that we've discussed what is expected, let's get started!

The first exercise will identify when a device configuration becomes out of sync with the configuration in Versa Director. To do this, you will log into the shell of one of your branch devices and enable configuration mode through the CLI. You will then enter configuration mode, commit the configuration, and then exit configuration mode. Note that you do not have to make a change to the configuration to bring the device out of sync, as the act of enabling CLI configuration mode is sufficient to flag it as out of sync.

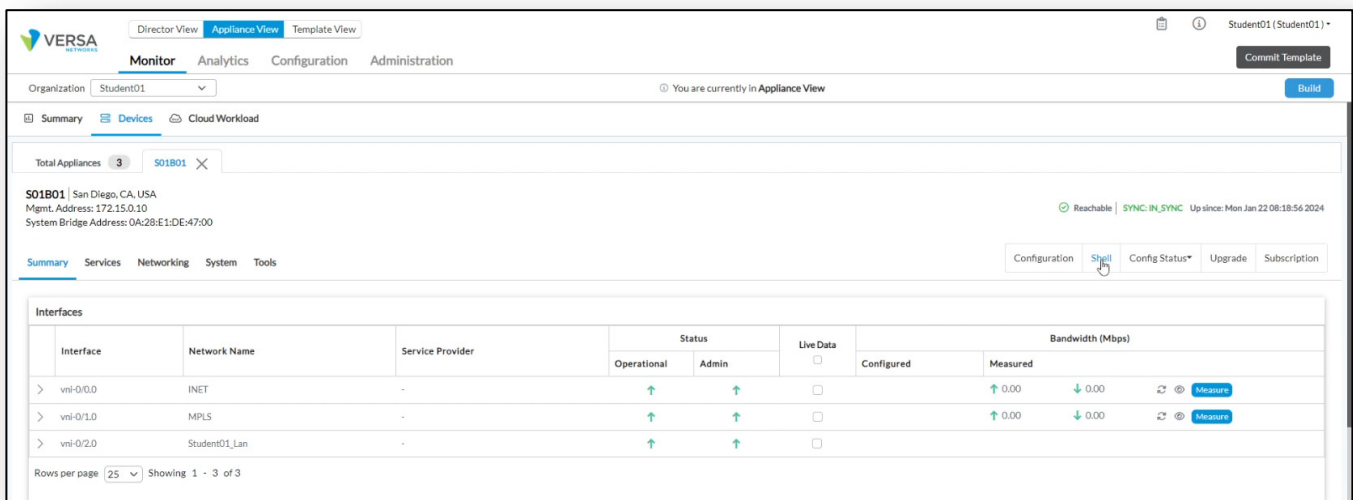
Step 1. Device Configuration Synchronization

- a. From Versa Director, navigate to *Appliance View*
- b. Click on your SxxB01 device to open it in Appliance View.

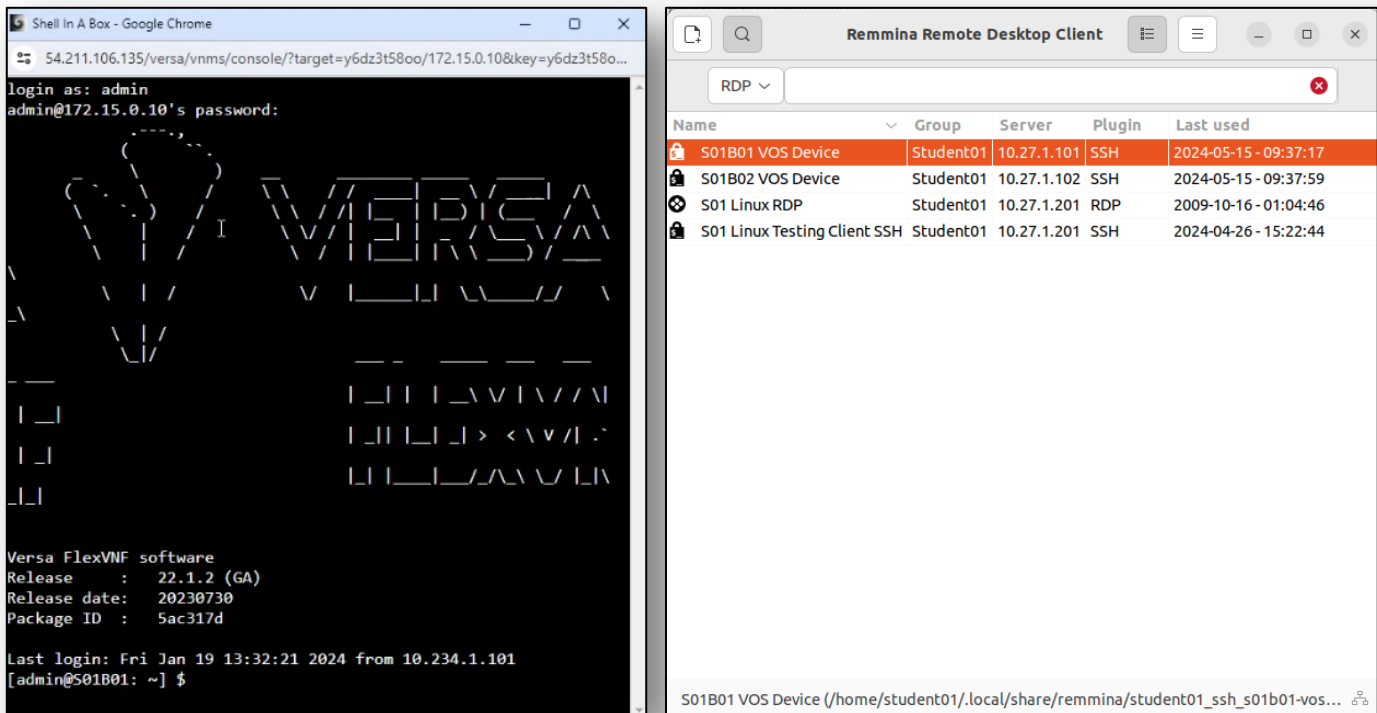


- c. From your SxxB01 device in Appliance View, navigate to the Monitor tab.
- d. Click the Shell button on the right side of the dashboard. This will open the shell.

Alternatively you can connect to the shell using the Remmina Remote Desktop Client on the remote desktop.



- e. Log into the shell of the B01 device with the username *admin* and password *versa123*.



By default configuration mode is disabled from the shell, as the device should be managed and configured by Versa Director.

- f. Enable the CLI configuration on the device. From the shell enter the command *vsh allow-cli*. Enter the admin password of *versa123* when prompted.
- g. After CLI mode has been enabled, type *cli* to start the command line interface.

```
Last login: Fri Jan 19 13:32:21 2024 from 10.234.1.101
[admin@S01B01: ~] $ vsh allow-cli
Enter password:

CLI now allowed
[admin@S01B01: ~] $ cli
```

- h. From the CLI, enter the command `configure` (or `config`) to enter configuration mode.
- i. From configuration mode, enter the command `commit`.

```
admin connected from 10.234.1.101 using ssh on S01B01
admin@S01B01-cli> config
Entering configuration mode private
[ok][2024-01-22 08:30:04]

[edit]
admin@S01B01-cli(config)% commit
No modifications to commit.
[ok][2024-01-22 08:30:07]

[edit]
admin@S01B01-cli(config)%
```

- j. Enter the exit command to leave configuration mode.
- k. Enter the exit command again to leave the CLI. Enter the exit command once more to log out of the device.

```
[edit]
admin@S01B01-cli(config)% exit
[ok][2024-01-22 08:30:08]
admin@S01B01-cli> exit
[admin@S01B01: ~] $ exit
logout
```

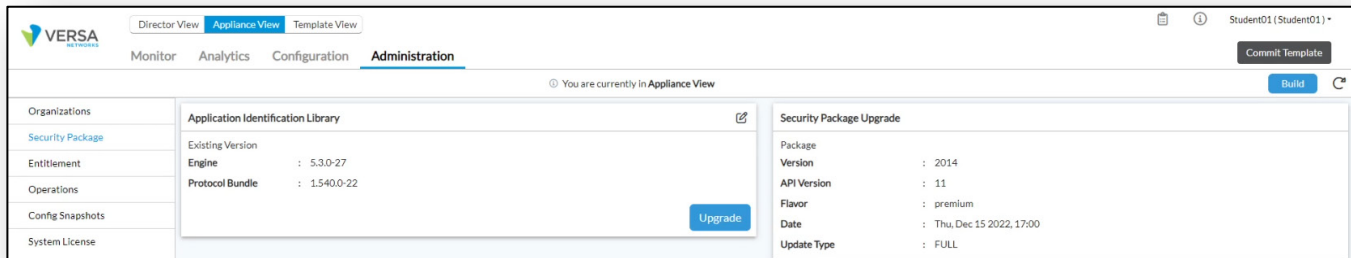
- l. After you log out, you may close the Shell In A Box window or Remmina window.

Versa Director checks the status of the device at regular intervals to verify the configuration synchronization status. It may take a few minutes for Versa Director to notice the changes. While we wait, let's visit the Application Identification database.

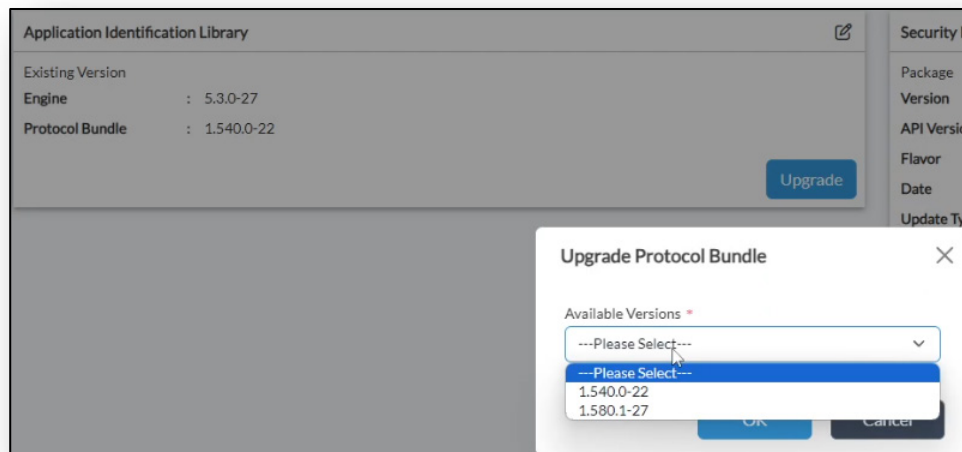
Step 2. Examine the Application Database

- a. Navigate to *Administration > Security Package* to view the application identification library information. You will see a version for Application Identification Library, and another version for Security Package Upgrade.

The Application Identification Library can be updated from the Administration page. We will look at the Security Package Upgrade option later in the lab exercises.



- b. Click on the *Edit* button in the top right corner of the Application Identification Library to open the *Upgrade Protocol Bundle* dialog.



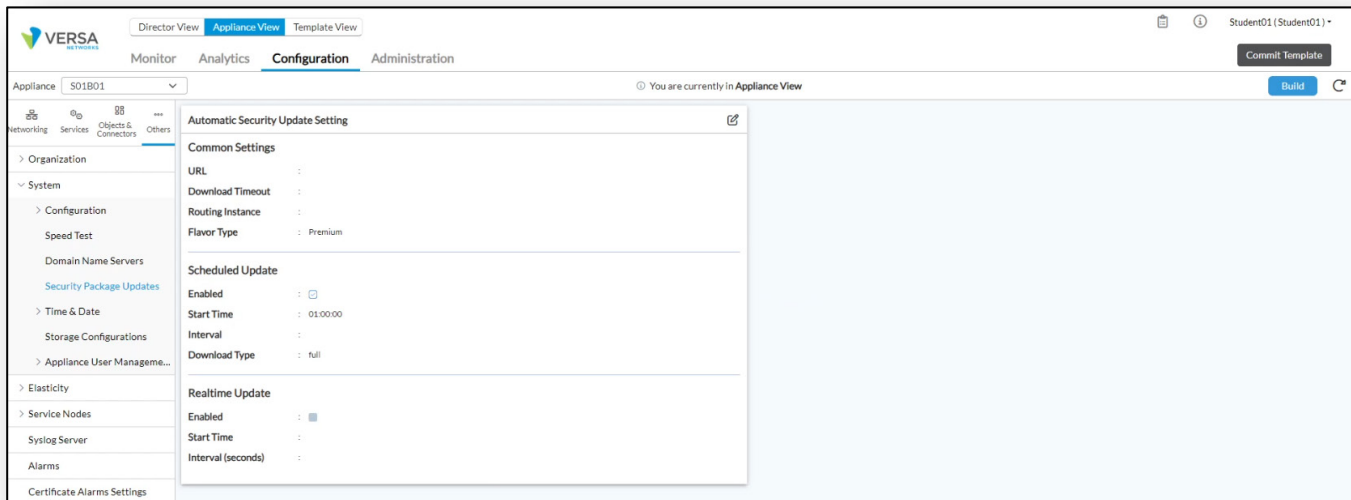
DO NOT UPGRADE THE APPLIANCE, as this will force a reboot of the device. The purpose of this exercise is to view where the upgrade process takes place.

- c. Click the *Cancel* button to exit the dialog.

Step 3. Verify the Security Package (SPACK)

Next you will view where the security package updates can be configured.

- a. Navigate to *Configuration > Others > System > Security Package Updates*.



The current Automatic Security Update Settings are displayed.

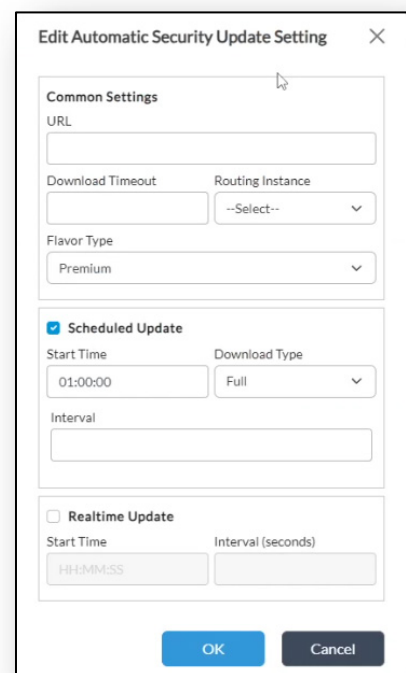
If you want the branch devices to automatically install the most current security package updates when they are released, you can configure the auto-update settings here.

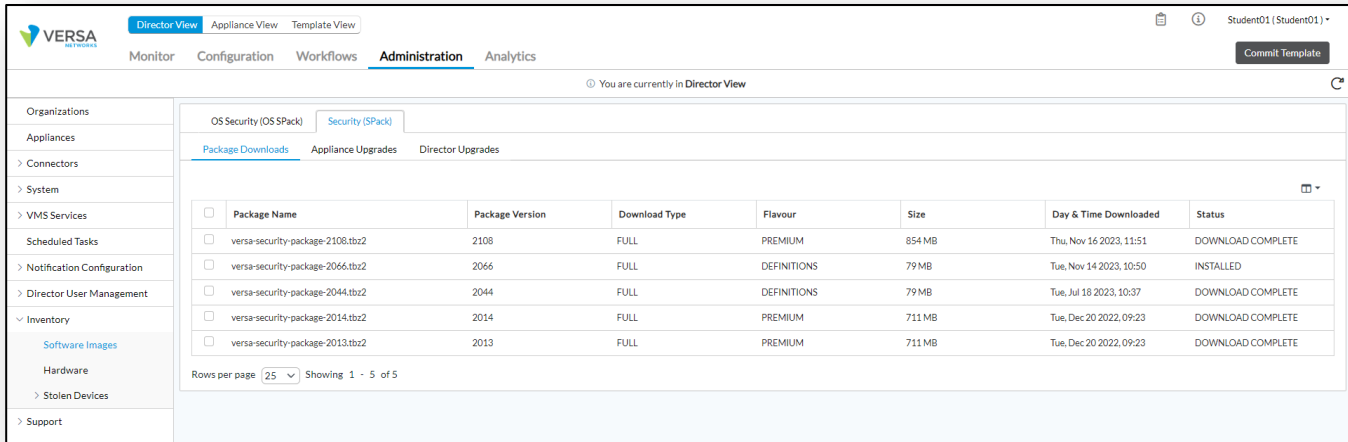
- b. Click the *Edit* button in the top right of the dialog to open the configuration settings.

Configuration settings allow you to specify the Versa Networks URL where the security packages are made available, the routing instance (virtual router) that has connectivity to the download URL, and other parameters.

Some organizations choose to enable automatic updates. Other organizations choose to manage the updates centrally from Versa Director, and to apply security package updates manually. This may be the case when the administrator wants to test the functionality of a security package update prior to placing it in production.

Security packages are centrally managed from Versa Director in the *Administration > Inventory > Software Images* library. Download of security packages is only allowed by the provider organization, as it affects storage on the Versa Director platform. For a sub-organization (as in the lab environment), packages that have been downloaded by the provider account are visible in the Package Downloads window.

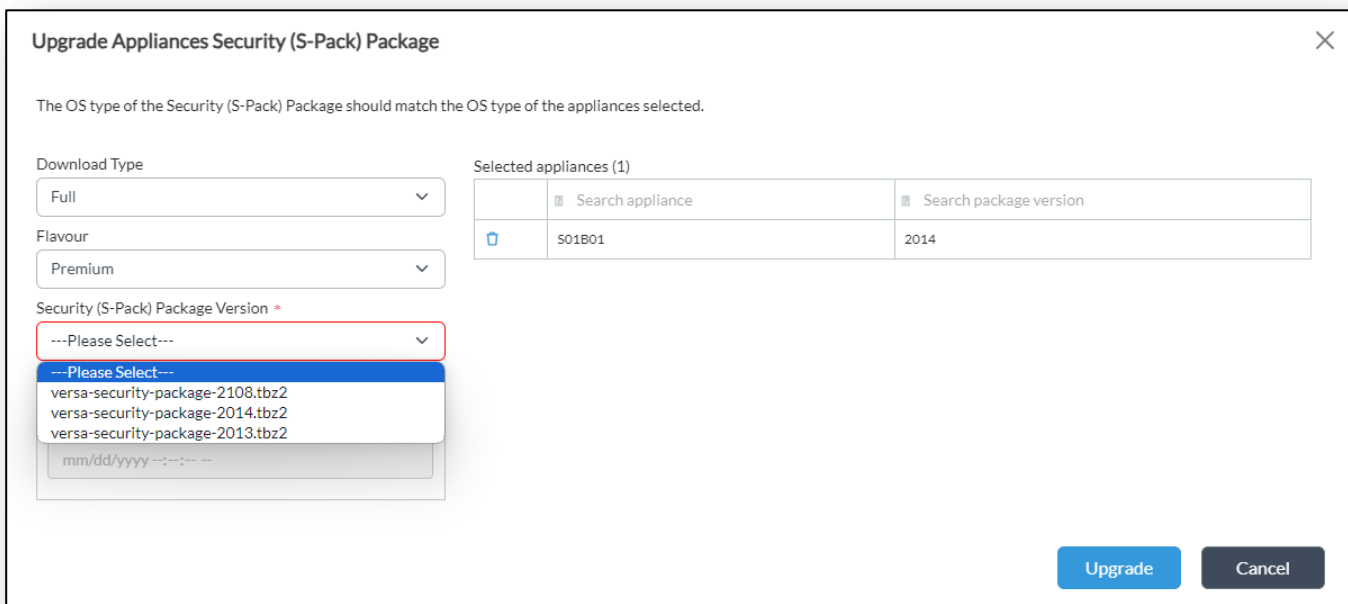




c. Navigate to the Appliance Upgrade tab.

Note: **DO NOT UPGRADE THE APPLIANCE!** The following steps will show you the location of the upgrade process and the steps involved. An upgrade is not needed.

- d. From the Appliance Upgrade window, check the box or boxes next to the appliance or appliances that you want to upgrade.
- e. Click the Upgrade Appliances button in the top right.
- f. From the Upgrade Appliances Security (S-Pack) Package dialog, choose the type of download, the flavour, and the package version.



g. **Do NOT perform an update on the devices.** Click the *Cancel* button to exit the upgrade dialog without making any changes.

Enough time should have passed to allow Versa Director to discover the configuration synchronization differences.

Step 4. Check the Configuration Sync status

- a. Navigate to *Administration* > *Appliances*. You should see a red alert in the Config Sync row of branch SxxB01.

The screenshot shows the Versa Director Administration interface. The 'Appliances' section is active, displaying a table of devices. The first device, SxxB01, has a red 'X' in the 'Config Sync' column, indicating a synchronization issue. The other two devices, SxxB02 and SP-HUB-New, show green checkmarks in the 'Config Sync' column.

	Name	Mgmt. Address	Tags	Type	Service Start Time	Software Version	Organizations	Status			
								Config Sync	Reachability	Service	Locked
<input checked="" type="checkbox"/>	SxxB01	172.15.0.4		Branch	Wed, Dec 11 2024, 09:57	22.1.4-GA	Student01	✗	✓	Up	🔒
<input type="checkbox"/>	SxxB02	172.15.0.6		Branch	Wed, Dec 11 2024, 09:57	22.1.4-GA	Student01	✓	✓	Up	🔒
<input type="checkbox"/>	SP-HUB-New	172.15.0.30		Hub	Wed, Dec 11 2024, 09:57	22.1.4-GA	Student01	✓	✓	Up	🔒

To view the reason for the configuration synchronization issue, you can compare the configuration that is applied to the appliance with the configuration in the Versa Director database.

- b. Check the box next to the SxxB01 branch device, then locate and click on the Compare button.

This screenshot is identical to the previous one, but the 'Compare' button in the top right corner of the appliance table is highlighted with a green box. The 'SxxB01' row is also selected with a blue checkmark in the first column.

A dialog will appear with the differences between the configurations highlighted.

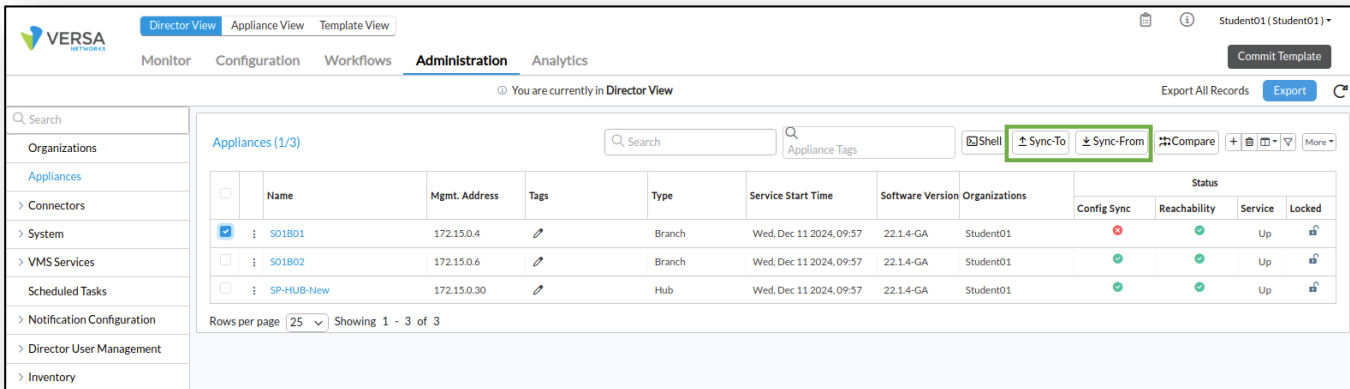


A + symbol indicates that the configuration statement is present on the appliance, but not in Versa Director. A - symbol indicates that a configuration statement is present in Versa Director, but is missing on the appliance.

You can see in the example that the allow-cli command added a statement to the configuration.

- c. Click the X in the top corner of the dialog to close the window.

To synchronize the configuration you can choose one of two options. You can “Sync Config from Appliance” or you can “Sync Config to Appliance”.



The Sync Config from Appliance option copies the appliance configuration into the Versa Director database and replaces the previous version of the configuration in the database. Use this option if you want to keep the changes that are on the appliance.

The Sync Config to Appliance option copies the configuration in the Versa Director database to the appliance and removes the changes made locally on the appliance. This is the option that you will perform.

- d. Click the Sync To button to synchronize the configuration and to remove the changes you made from the CLI.
- e. Click Yes when asked to confirm.

<input type="checkbox"/>	Name	Mgmt. Address	Tags	Type	Service Start Time	Software Version	Organizations	Status			
								Config Sync	Reachability	Service	Locked
<input type="checkbox"/>	: S01B01	172.15.0.10		Branch	Mon, Jan 22 2024, 08:32	22.1.2-GA	Student01			Up	
<input type="checkbox"/>	: S01B02	172.15.0.8		Branch	Mon, Jan 22 2024, 08:18	22.1.2-GA	Student01			Up	
<input type="checkbox"/>	: SPHUB	172.15.0.12		Hub	Mon, Jan 22 2024, 08:31	22.1.2-GA	Student01			Up	

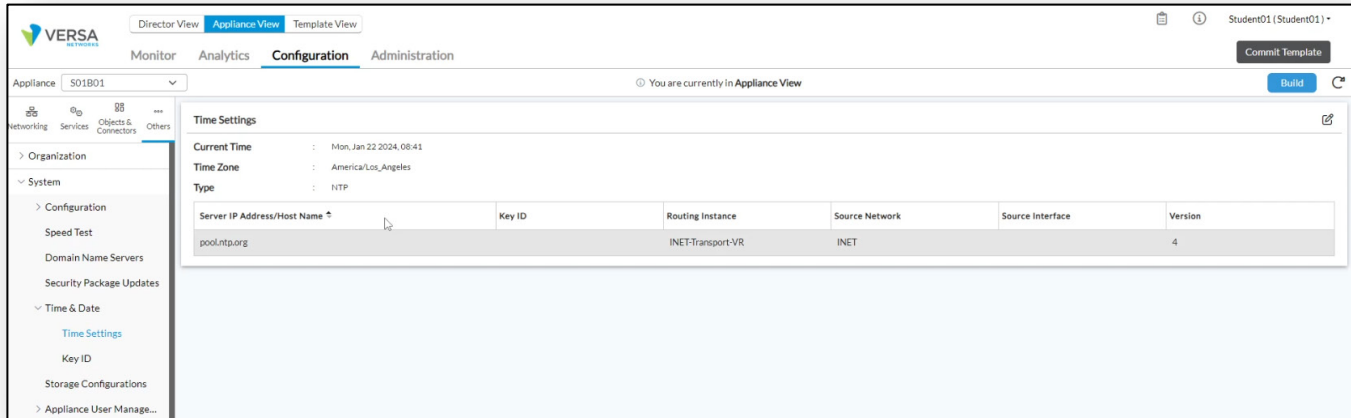
Once finished, the Config Sync status should change to a green check mark.

Step 5. System Settings

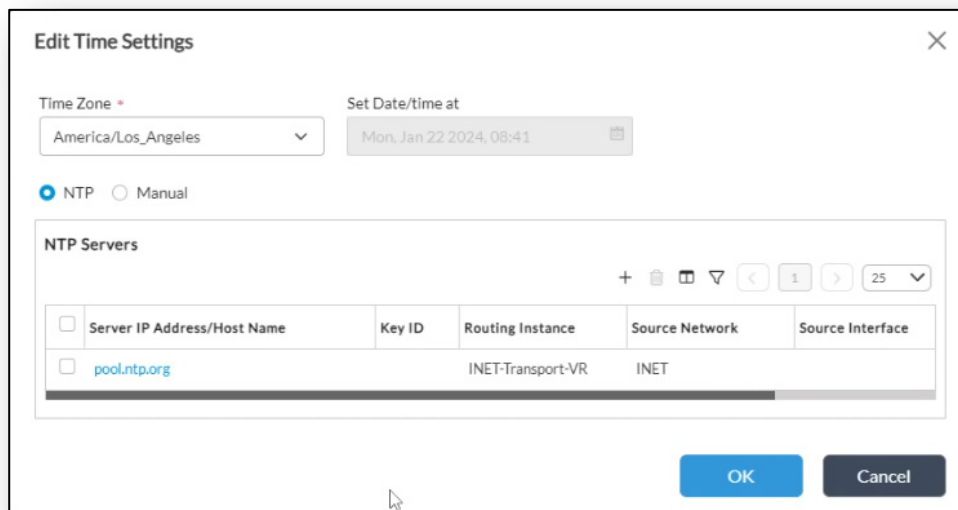
Network Time Protocol is used to synchronize date and time on a device with a centralized clock source. This is important for authentication services, as well as logging and event tracking.

The NTP server settings are located in the *Configuration > Others > System > Time & Date > Time Settings* dashboard.

- a. Ensure you are in the *SxxB01 Appliance View*.
- b. In the SxxB01 Appliance View, navigate to *Configuration > Others > System > Time & Date > Time Settings*.



- c. Click on the Edit button in the top right to open the NTP settings.

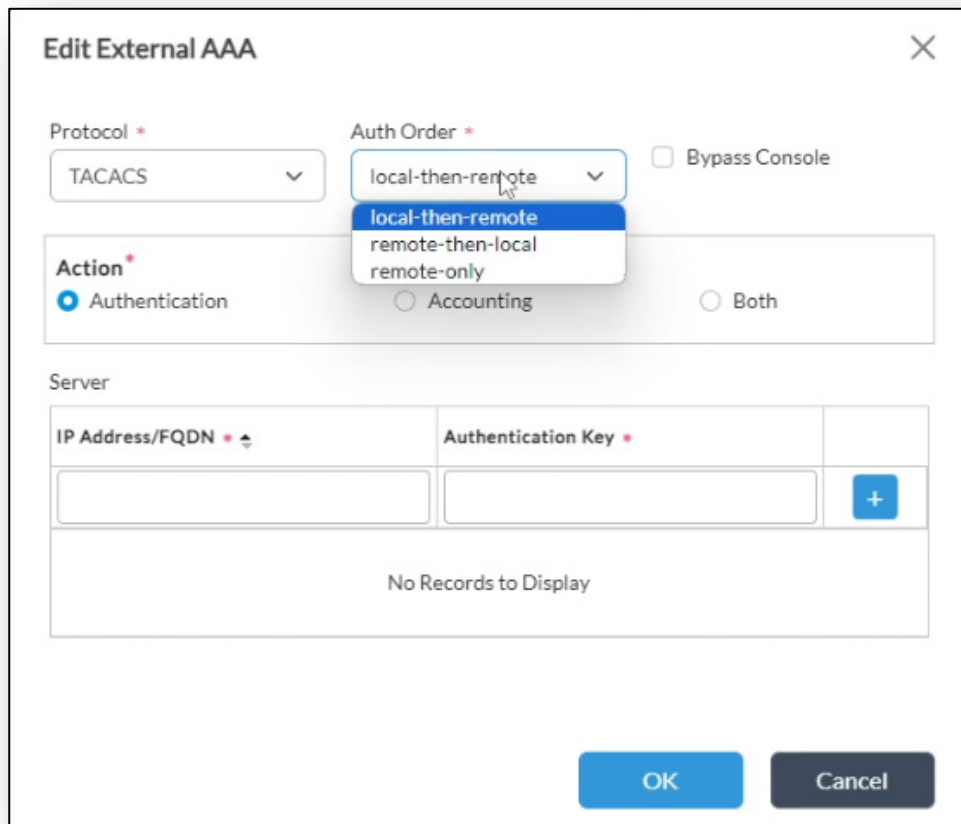
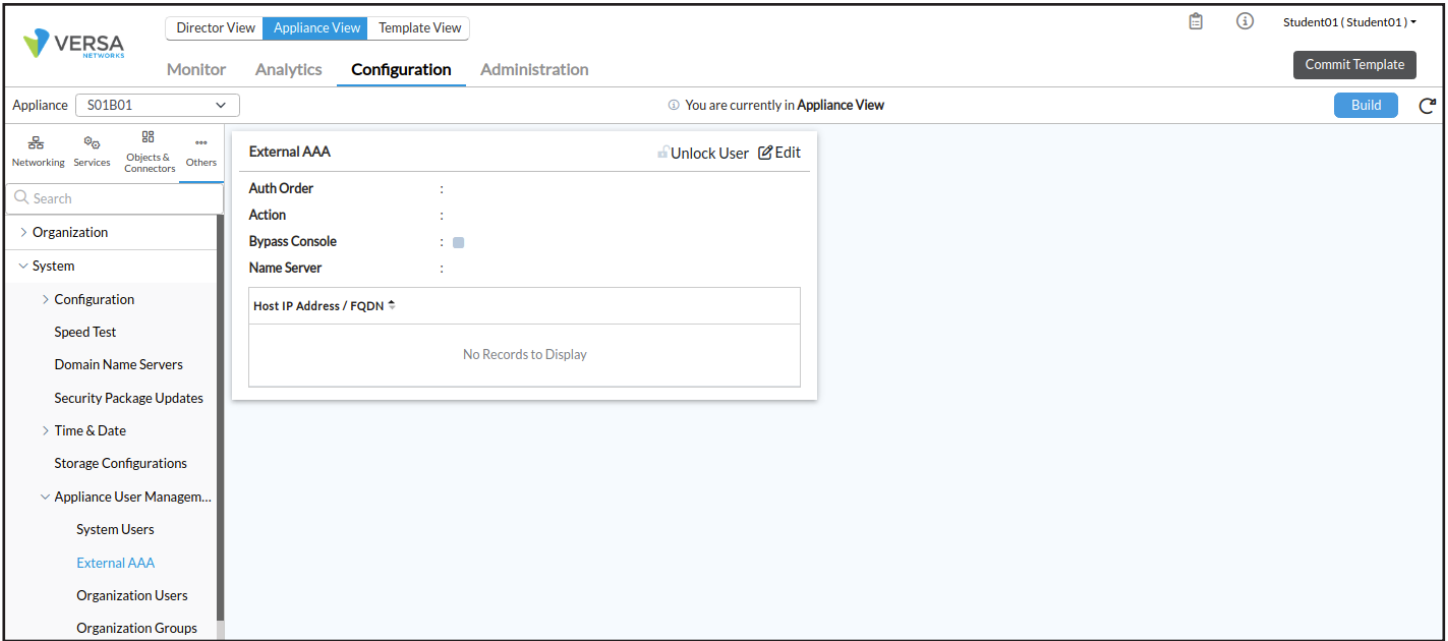


The NTP servers can be added by IP address or FQDN. The routing instance and source network that have reachability to the NTP server are assigned.

Local login parameters can be configured on the devices. It is recommended to change the default login information (admin/versa123) for improved security.

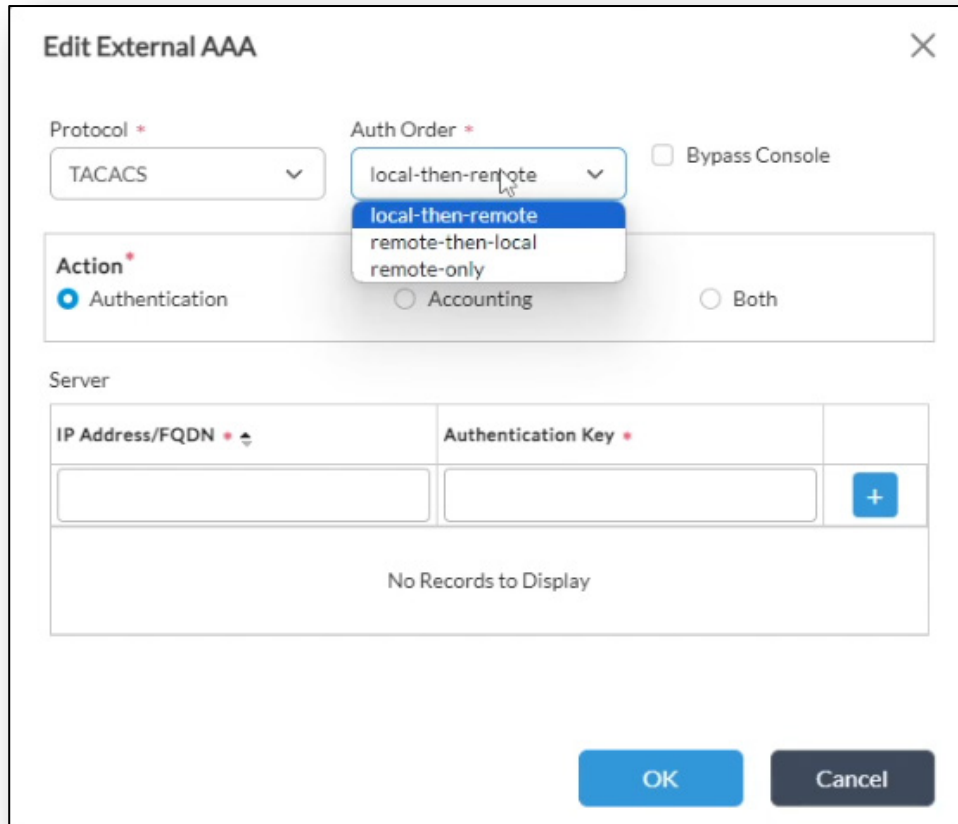
External authentication can be configured with TACACS+ or RADIUS authentication. You can set the appliance user authentication in the *Configuration > Others > System > Appliance User Management > External AAA* dashboard.

- d. Navigate to *Configuration > Others > System > Appliance User Management > External AAA*.



The Auth Order determines the order that the system queries authentication databases when a user attempts to log into the device. The options are:

- local-then-remote: The authentication system will compare the username and password to the local user database first. If the username/password does not match a local username and password, the device will query the remote server for username/password. If the username and password entered by the user does not match either database, login is denied.
- Remote-then-local: The authentication system compares the username and password to the remote server first, and only queries the local database if the username/password does not match the information in the authentication server.
- Remote-only: This option will only use the remote server information for authentication. If the remote authentication server is not reachable or offline, then the local database will be used as a failover.



Edit External AAA

Protocol *
TACACS

Auth Order *
local-then-remote
remote-then-local
remote-only

Bypass Console

Action *
 Authentication
 Accounting
 Both

Server

IP Address/FQDN * ↕	Authentication Key *	
		+

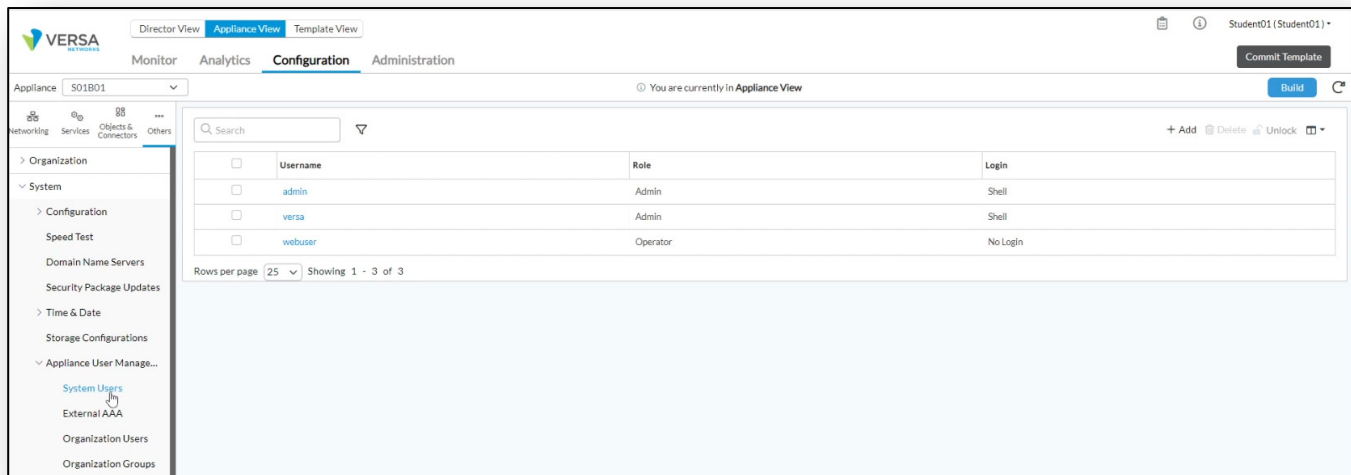
No Records to Display

OK Cancel

- f. Click the Cancel button to exit the dialog without making any changes.

The System Users is where the local users are created with their corresponding authentication parameters.

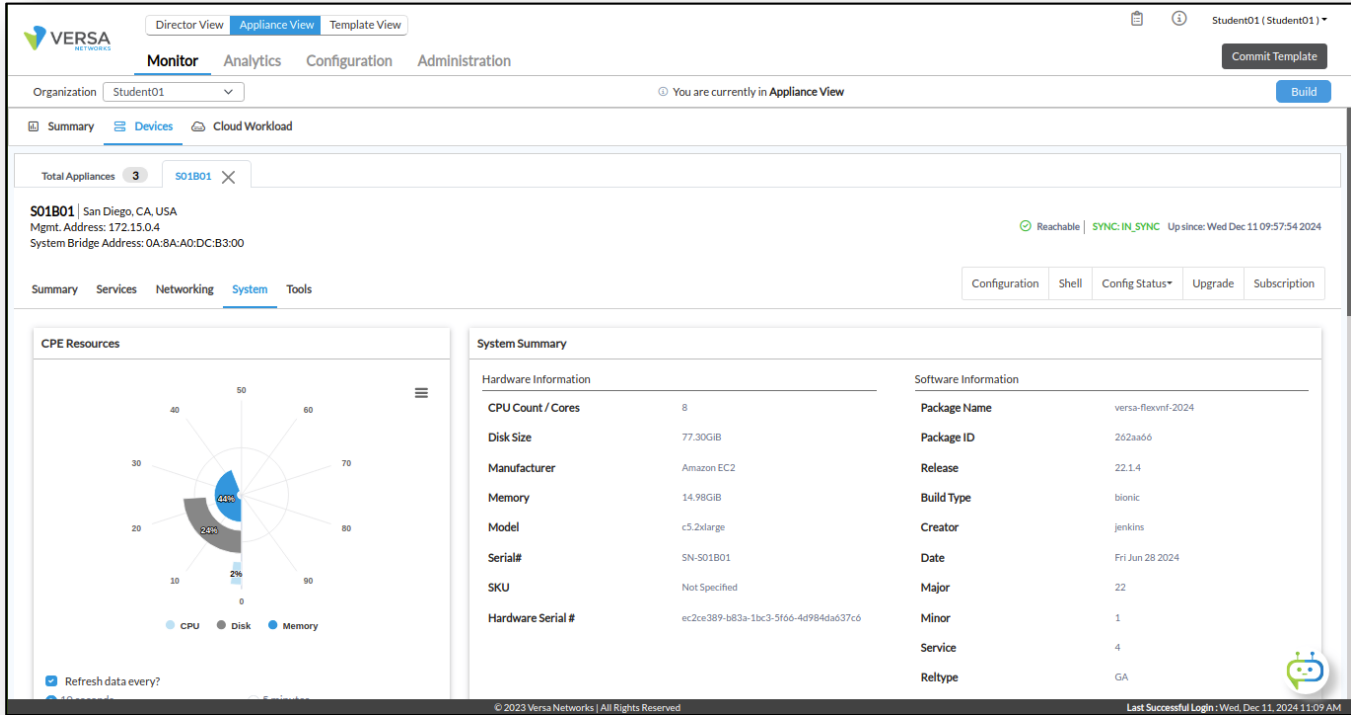
- g. Navigate to *Configuration > Others > System > Appliance User Management > System Users* to view the current users. Note that these are the default users in the system.



Do not make any changes to the local users.

The system resources are tracked through the Monitor dashboard in Versa Director. Individual device resources are viewed through the Monitor dashboard of Appliance View.

- h. In the Appliance View of your SxxB01 device, navigate to *Monitor > System*.

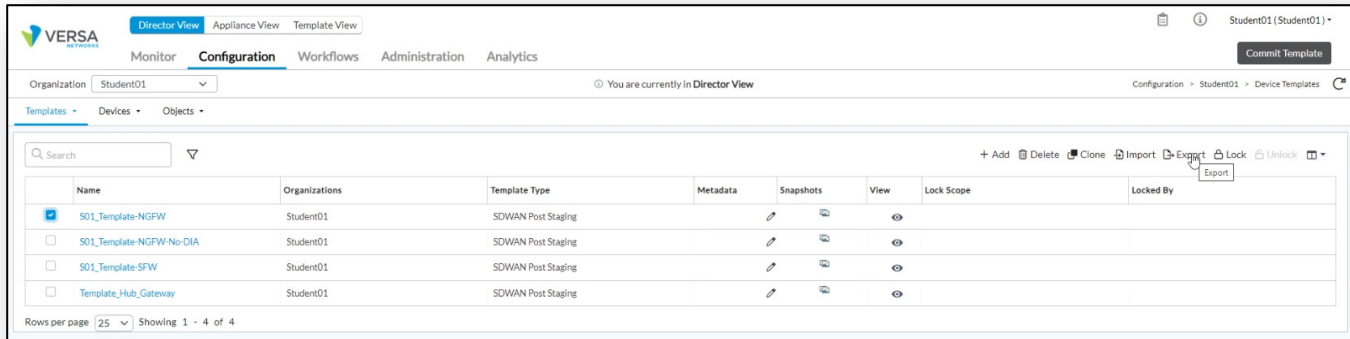


- i. Explore the resource utilization of your branch device, including the software version, hardware configuration, templates and device group associated with the device, location, and overall system status.

Step 6. Exporting Configuration Elements

Device templates can be exported to a text format for archival, to copy between Versa Directors, or to import into the system at a later time.

- a. Navigate to *Director View > Configuration > Templates > Device Templates* to view the device templates database.



- b. In the Device Templates dashboard, check the box next to the Sxx_Template-NGFW template. This will activate the tools in the top of the panel.
- c. Locate and click on the Export button to export a text copy of the configuration template. It will be saved in the local Downloads folder of the remote desktop workstation.
- d. Click OK to confirm the export function.
- e. After you download the template, open the downloads folder (or click on the downloads button in the web browser) and open the template file. Its file extension is .cfg, but you can view the file with the Notepad application or a text editor.

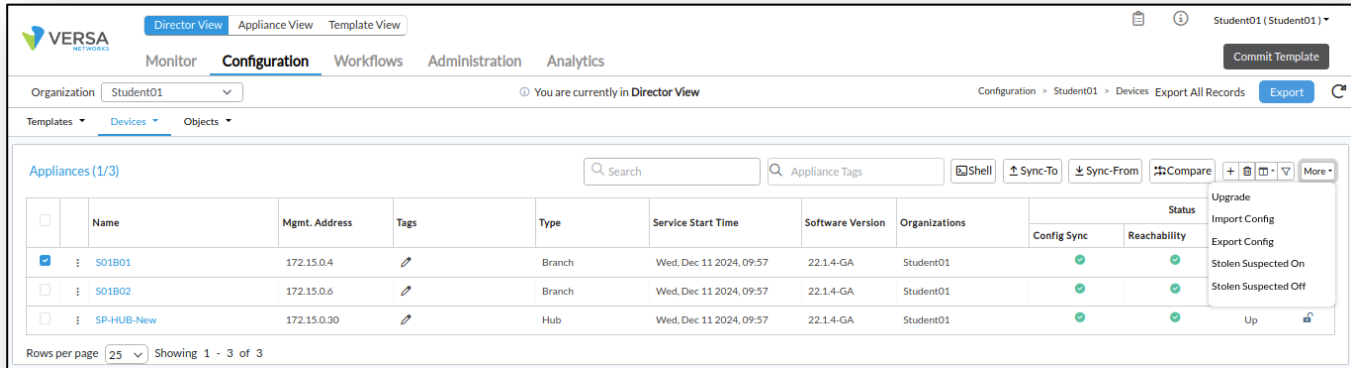
```

1 devices {
2   template Template-S01-NGFW {
3     config {
4       /* Tags: replace */
5       snmp {
6         agent {
7           enabled      false;
8           ip           127.0.0.1;
9           udp-port     161;
10          extra-listen ::1 161;
11          /* Tags: replace */
12          version {
13            v1;
14            v2c;
15          }
16          max-message-size 50000;
17        }
18        system {
19          name      "${Sv_Student01_Site_Name_sitesSiteName}";
20          location "${Sv_location_IdLocation}";
21        }
22        notify std_v1_trap {
23          tag std_v1_trap;
24          type trap;
25        }
26        notify std_v2_inform {
27          tag std_v2_inform;
28          type inform;
29        }
30        notify std_v2_trap {
31          tag std_v2_trap;
32          type trap;
33        }
34        notify std_v3_inform {
35          tag std_v3_inform;
36          type inform;
37        }

```

Device configurations can be exported in a text format.

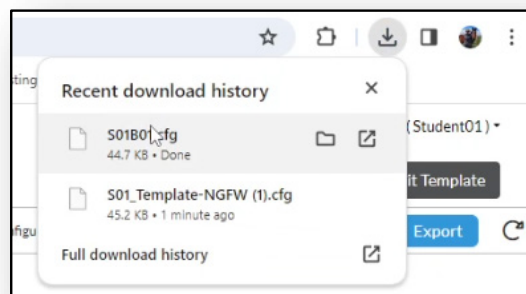
- f. Navigate to *Configuration > Devices > Devices*, or navigate to *Administration > Appliances*.
- g. In either location, locate your SxxB01 device and check the box next to the device to select it. In the *Administration > Appliances* view, you will need to click on the More dropdown in the top right corner to see the *Import Config* and *Export Config* options. The example below is the view from the *Configuration > Devices > Devices* dashboard.



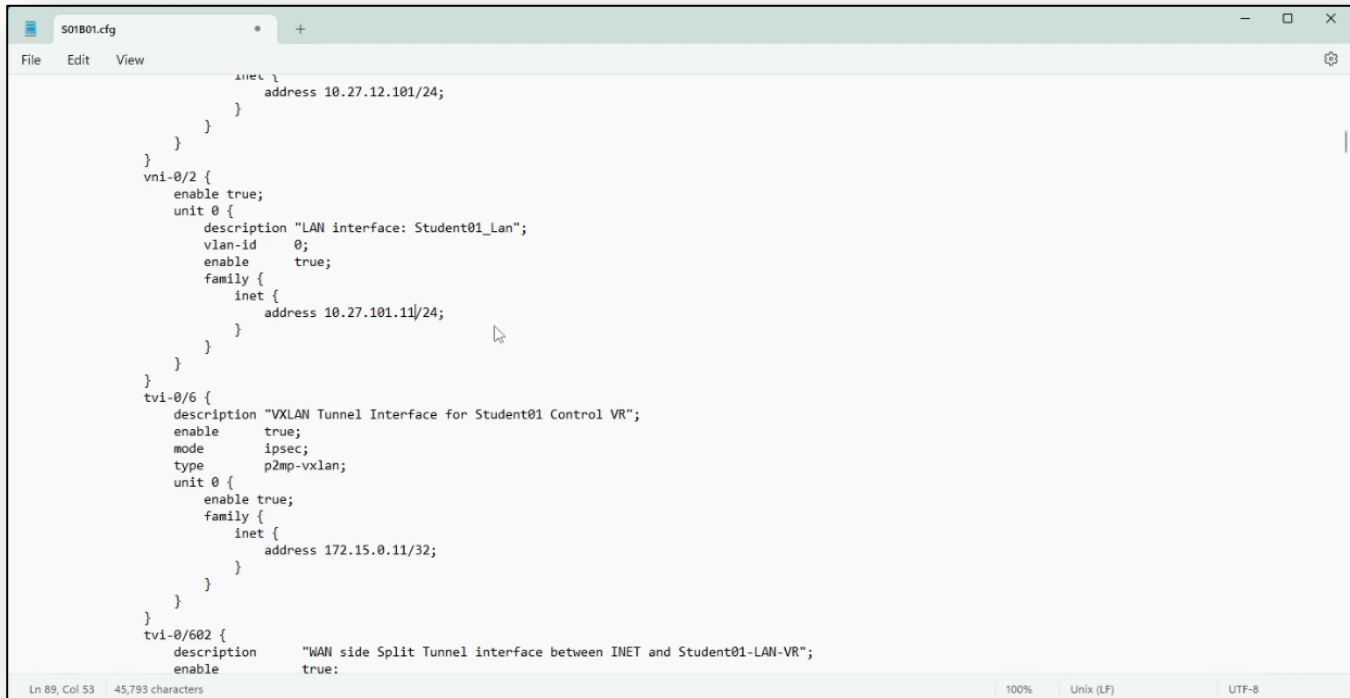
- h. Click the Export Config menu item.

After export, the configuration file will be saved in the Downloads folder of the remote desktop.

- i. Open the Downloads folder on the remote desktop, or click on the Downloads button in the web browser to locate the SxxB01.cfg configuration file.
- j. Open the file with the Notepad or a text editor application.



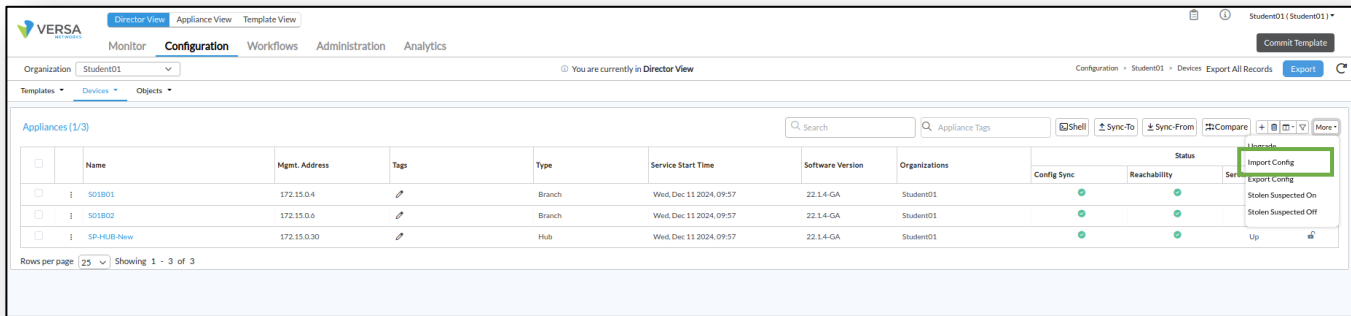
Scroll down in the configuration file and locate the vni-0/2 configuration statement. It should have a description of “LAN interface: Studentxx_Lan”.



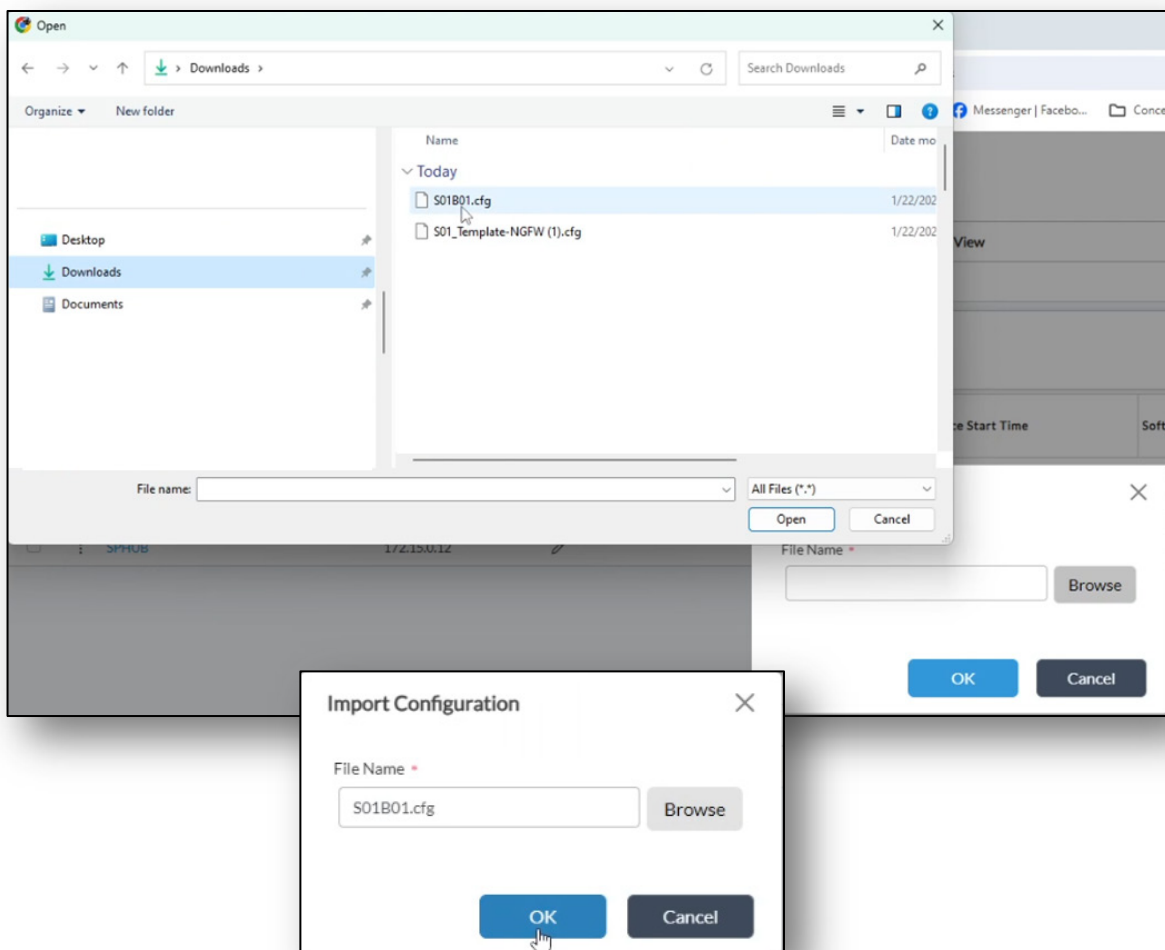
```
File Edit View
S01B01.cfg
inet {
  address 10.27.12.101/24;
}
}
}
vni-0/2 {
  enable true;
  unit 0 {
    description "LAN interface: Student01_Lan";
    vlan-id 0;
    enable true;
    family {
      inet {
        address 10.27.101.11/24;
      }
    }
  }
}
tvl-0/6 {
  description "VXLAN Tunnel Interface for Student01 Control VR";
  enable true;
  mode ipsec;
  type p2mp-vxlan;
  unit 0 {
    enable true;
    family {
      inet {
        address 172.15.0.11/32;
      }
    }
  }
}
tvl-0/602 {
  description "WAN side Split Tunnel interface between INET and Student01-LAN-VR";
  enable true;
}
Ln 89, Col 53 | 45,793 characters | 100% | Unix (LF) | UTF-8
```

- k. Change the address 10.27.1xx.10/24 to 10.27.1xx.11/24, then save the file. The xx values will vary depending on your student ID.

- l. Return to Versa Director. In Versa Director, ensure that your SxxB01 device is selected in the devices list.
- m. Locate and click on the *Import Configuration* button.

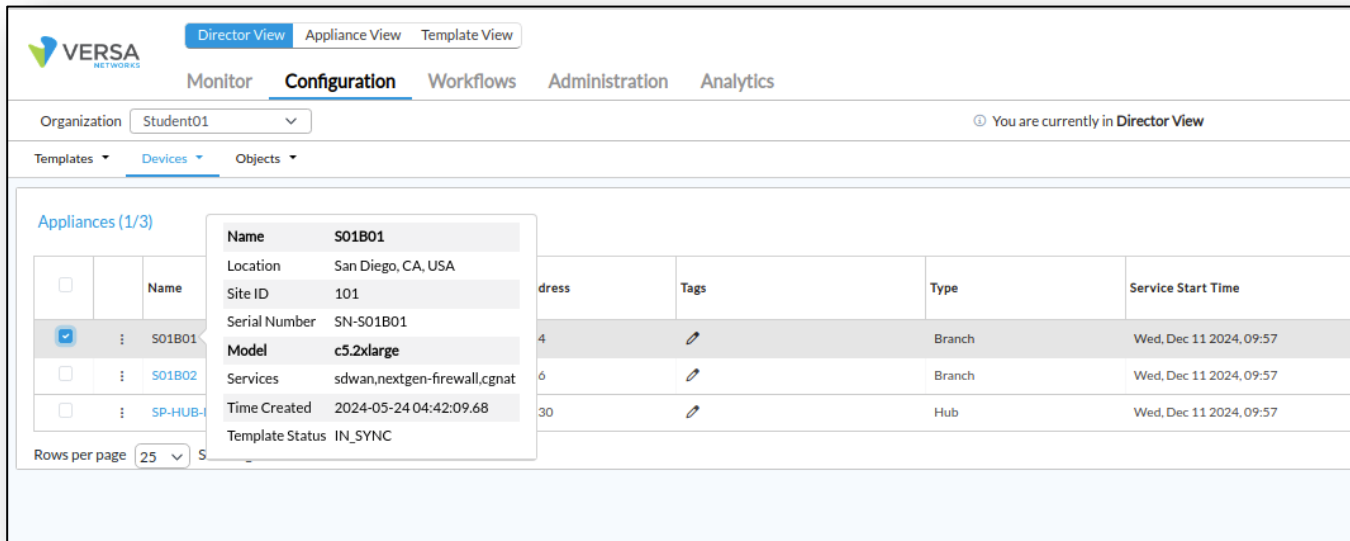


- n. In the Import dialog, locate the SxxB01.cfg file in the remote desktop Downloads folder.
- o. Select the file and click *Open* to load the configuration into Versa Director.
- p. Click the *OK* button to apply the configuration to the device (imported configuration files are automatically applied/committed to the devices).



Next you will verify how the configuration of the SxxB01 device changed when you imported the modified configuration file.

- q. In the Devices window, click on the SxxB01 device to open the device in Appliance View.

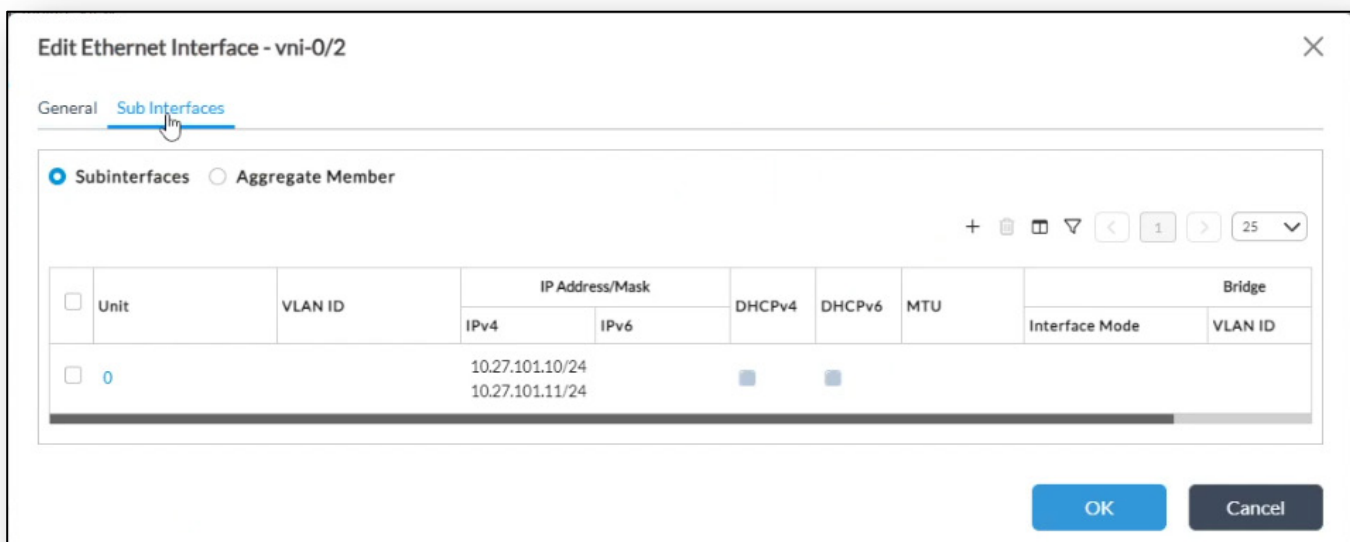


- r. In the Appliance View of the device, navigate to *Configuration > Networking > Interfaces* to view the IP addresses assigned to the interfaces. You should see two IP addresses assigned to interface vni-0/2.

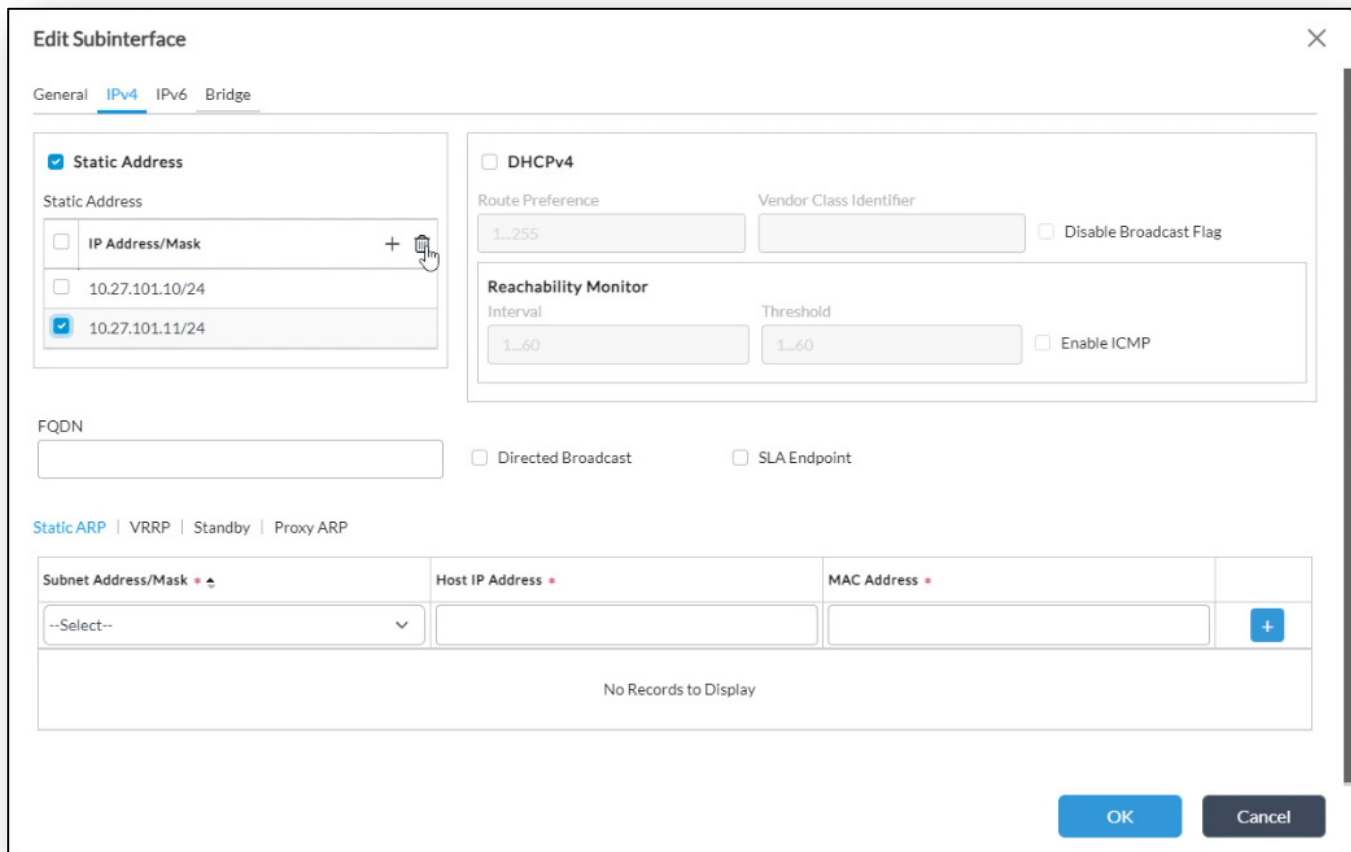
A device configuration action performs a configuration merge with the existing configuration (not a configuration replace). The old IP address that ends in .10/24 is still in place, but the modified .11/24 is added to the configuration.

Next you will remove the added IP address from the configuration.

- s. Click on *interface vni-0/2* to open the interface configuration.
- t. Click on the *Sub Interfaces* tab to view the sub interfaces configuration.



- u. Click on *sub interface 0* and navigate to the IPv4 tab.
- v. In the IPv4 tab of the sub interface, check the box next to the 10.27.xxx.11/24 IP address in the Static Address box.



Edit Subinterface

General **IPv4** IPv6 Bridge

Static Address

Static Address

IP Address/Mask	
<input type="checkbox"/> IP Address/Mask	+
<input type="checkbox"/> 10.27.101.10/24	
<input checked="" type="checkbox"/> 10.27.101.11/24	

DHCPv4

Route Preference: 1..255 Vendor Class Identifier:

Disable Broadcast Flag

Reachability Monitor

Interval: 1..60 Threshold: 1..60

Enable ICMP

FQDN:

Directed Broadcast SLA Endpoint

Static ARP | VRRP | Standby | Proxy ARP

Subnet Address/Mask	Host IP Address	MAC Address	
--Select--	<input type="text"/>	<input type="text"/>	+

No Records to Display

OK Cancel

- w. Click the Delete button to remove the unwanted IP address.
- x. Click *OK* in the Edit Subinterface dialog, then click *OK* to exit the interface dialog.

This will update the configuration in the database, and also push the new configuration to the branch device automatically.



STOP! Notify your instructor that you have completed this lab.

STATISTICS AND MONITORING

The Versa Networks lab environment consists of a fixed, pre-configured topology that will allow you to explore, configure, and manage Versa Networks CPEs by using Versa Director, the central management and orchestration platform for a Versa Secure SD-WAN solution. After completing this lab, you will be able to:

- Monitor the traffic on individual devices in real time
- Monitor the interface and service statistics per-device to view counters and metrics
- Monitor the status of Versa Director
- Monitor the status of the SD-WAN environment as a whole
- Navigate the Versa Analytics platform
- Display and interpret historical data in Versa Analytics
- View logging information in Versa Analytics
- Generate reports using Versa Analytics

In this lab you will be assigned two CPE devices (Branch devices) for configuration and monitoring. The branch devices are named after the student ID that you have been assigned.

The lab environment is accessed through Amazon Workspaces. Your student ID and workspace will be assigned by the instructor.

The remote desktop connection opens a remote workstation, where you will use various tools to navigate and configure the lab environment. The main tool you will use in this lab is Versa Director. Versa Director can be accessed by opening the Google Chrome browser on the Remote Desktop. The IP address of the Versa Director (from the remote workstation) is 10.27.1.10. Once you begin the lab, you may want to create a bookmark to Versa Director in the web browser on the remote desktop.

During certain lab parts, the lab guide will present sample output from the GUI or the CLI. The sample outputs are SAMPLES and represent the information as it appeared during the lab guide creation. Your output may vary in some ways (some devices may or may not be present, some routes may or may not be the same, etc.) Do not be alarmed if your results vary slightly from the results shown in the lab guide. The important thing is that the lab functions in the desired manner.

This lab guide will step you through some common tasks that are performed on Versa Director. After an introductory set of exercises, you will be asked to perform some basic tasks that will allow you to become more familiar with the environment.

The goal of this and all lab exercises is to help you gain additional skills and knowledge. Because of this, the lab guide contains additional instruction to supplement the student guides.

Now that we've discussed what is expected, let's get started!

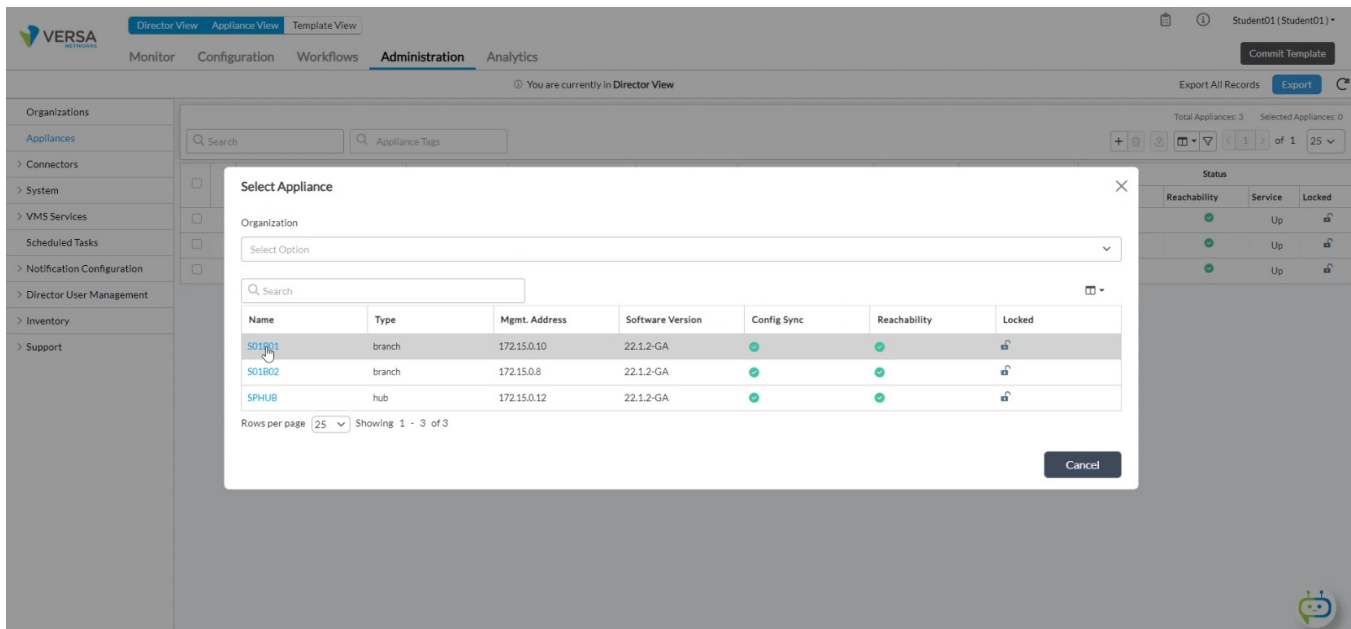
Step 1. Realtime Statistics

Versa Director provides real-time information about the network environment, as well as traffic, service, and policy statistics. In this exercise you will:

- Generate traffic from the host connected to the B01 branch; and
- View live traffic statistics on the B01 device and the SPHUB-NEW device.

To assist with this lab you will run a script that generates ICMP traffic between the B01 branch and the SPHUB-NEW device. This will help to populate the traffic statistics.

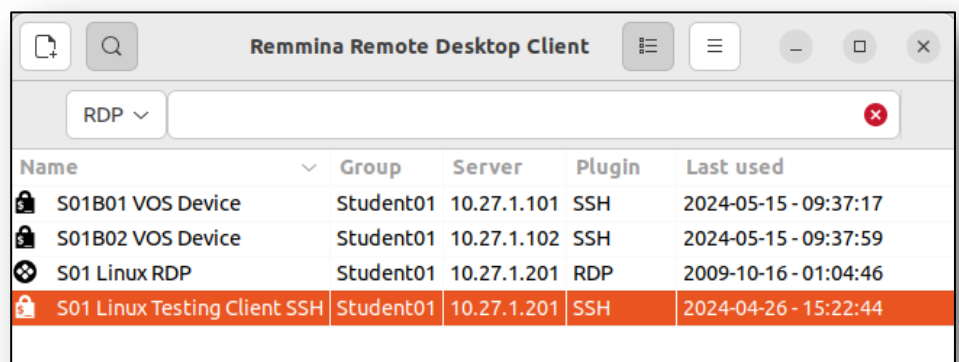
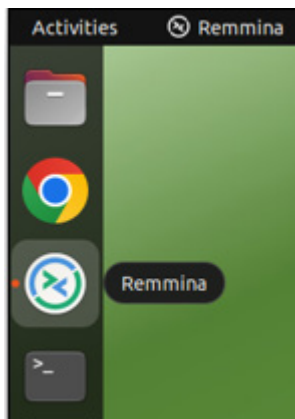
- In Versa Director, navigate to the *Appliance View* and click on your SxxB01 branch device, where Sxx is the student number assigned to you. This will open the B01 Appliance.



- In the B01 Appliance View, navigate to the *Monitor* tab.

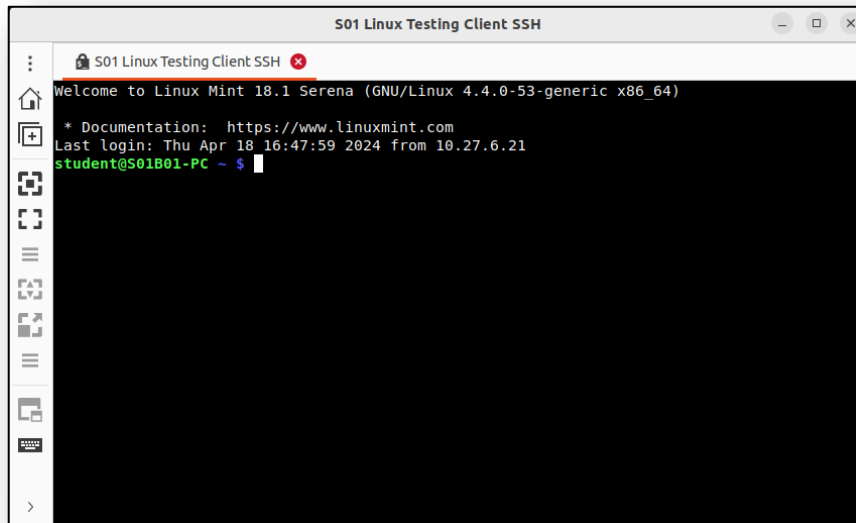
This will allow you to open a console shell to the device.

- Locate and open the Remmina Remote Desktop Client on the remote desktop.



- d. Open the SSH session to the Linux Testing Client.

If prompted for a password, enter the username *student* and password *versa123* when prompted.



You are now connected to the Linux testing host.

- e. From the Linux testing host shell prompt, issue the command *ls* to list the files in the local directory.

You should see a file called *pinghub.sh*.

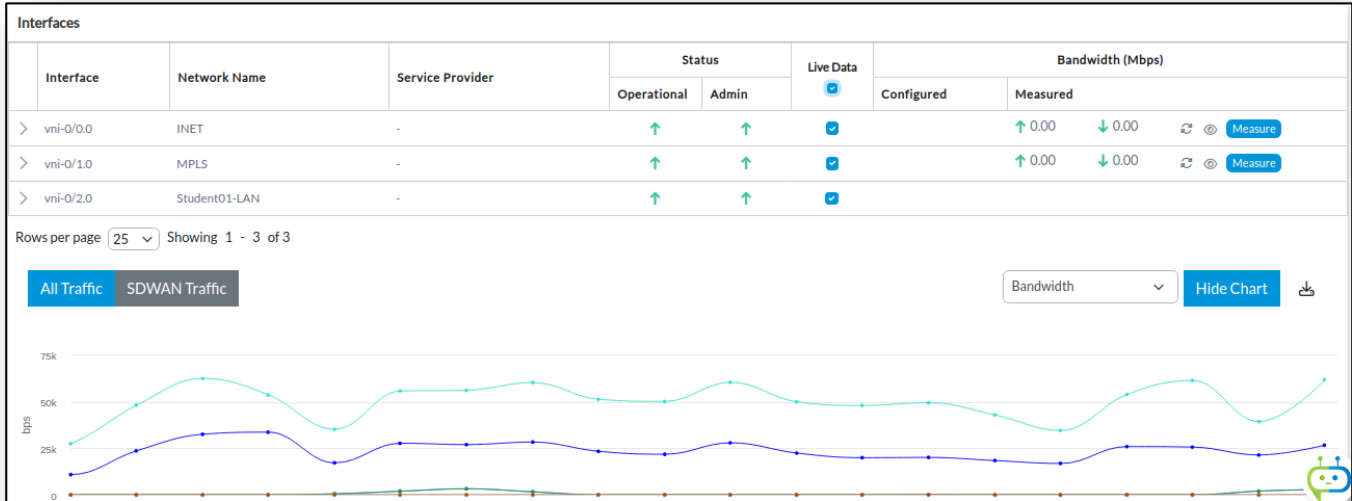
- f. Execute the *pinghub.sh* script by entering the command *./pinghub.sh*. This will initiate a ping of 1500 packets towards the hub-connected host.

```
student@student01-pc ~ $ ./pinghub.sh
PING 10.27.130.98 (10.27.130.98) 1000(1028) bytes of data.
1008 bytes from 10.27.130.98: icmp_seq=1 ttl=63 time=1.76 ms
1008 bytes from 10.27.130.98: icmp_seq=2 ttl=63 time=1.45 ms
1008 bytes from 10.27.130.98: icmp_seq=3 ttl=63 time=1.70 ms
1008 bytes from 10.27.130.98: icmp_seq=4 ttl=63 time=1.42 ms
1008 bytes from 10.27.130.98: icmp_seq=5 ttl=63 time=1.22 ms
1008 bytes from 10.27.130.98: icmp_seq=6 ttl=63 time=11.0 ms
1008 bytes from 10.27.130.98: icmp_seq=7 ttl=63 time=1.60 ms
1008 bytes from 10.27.130.98: icmp_seq=8 ttl=63 time=1.34 ms
1008 bytes from 10.27.130.98: icmp_seq=9 ttl=63 time=1.60 ms
1008 bytes from 10.27.130.98: icmp_seq=10 ttl=63 time=7.57 ms
1008 bytes from 10.27.130.98: icmp_seq=11 ttl=63 time=1.32 ms
1008 bytes from 10.27.130.98: icmp_seq=12 ttl=63 time=1.19 ms
```

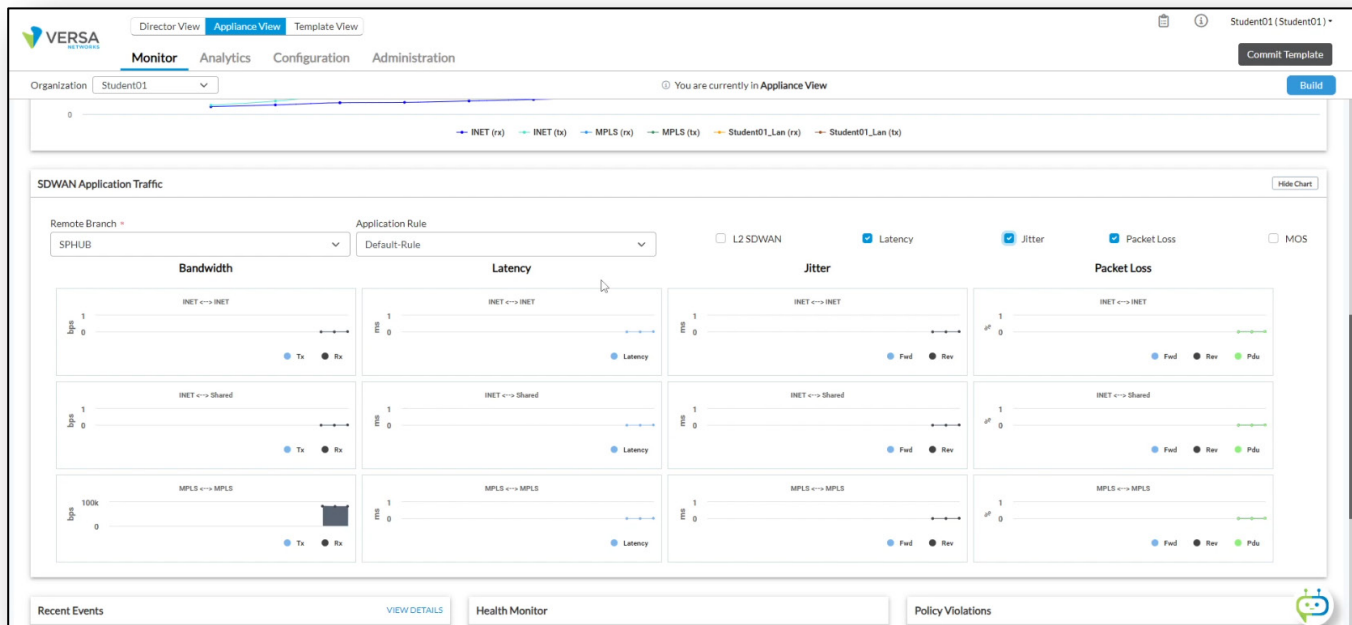
- g. Minimize (do not close) the shell window and return to Versa Director.

- h. Return to the Versa Director *Monitor* dashboard.
- i. In the Versa Director Monitor dashboard click the *Live Data* box to activate the live traffic tracking.

The Live Data box is in the Summary tab. After a few seconds the chart should begin to populate so that you can view the traffic flow.

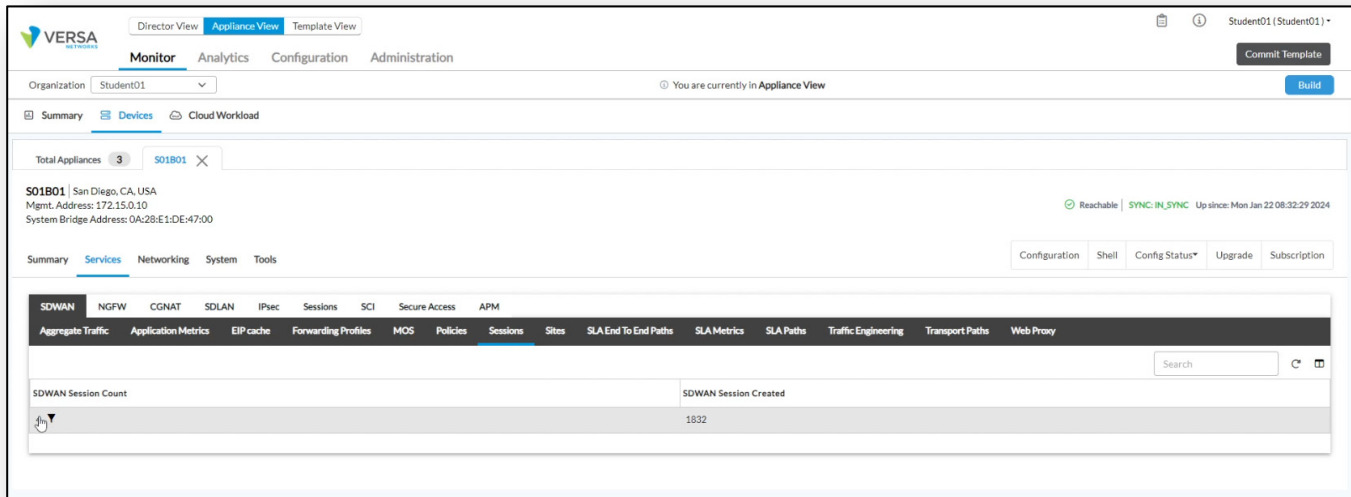


- j. In the Application Traffic window, select Remote Branch SPHUB-NEW to view traffic statistics towards the hub site.
- If desired, you can click the Latency, Jitter, and Packet Loss boxes to turn on/off the charts associated with each statistic.

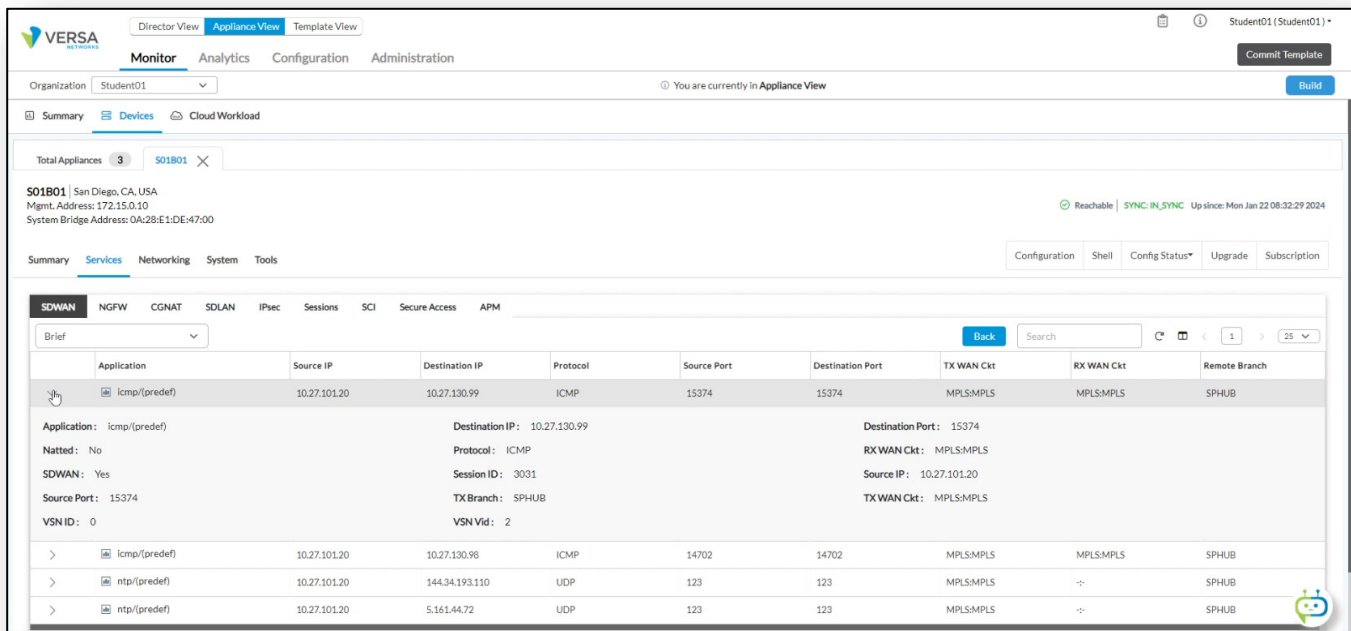


Data points will be added to the charts about every 2 seconds.

- k. Navigate to the *Monitor > Services > SDWAN* dashboard.
- l. Click on the Sessions tab. You should see a session count table for sessions that cross the SD-WAN circuits.

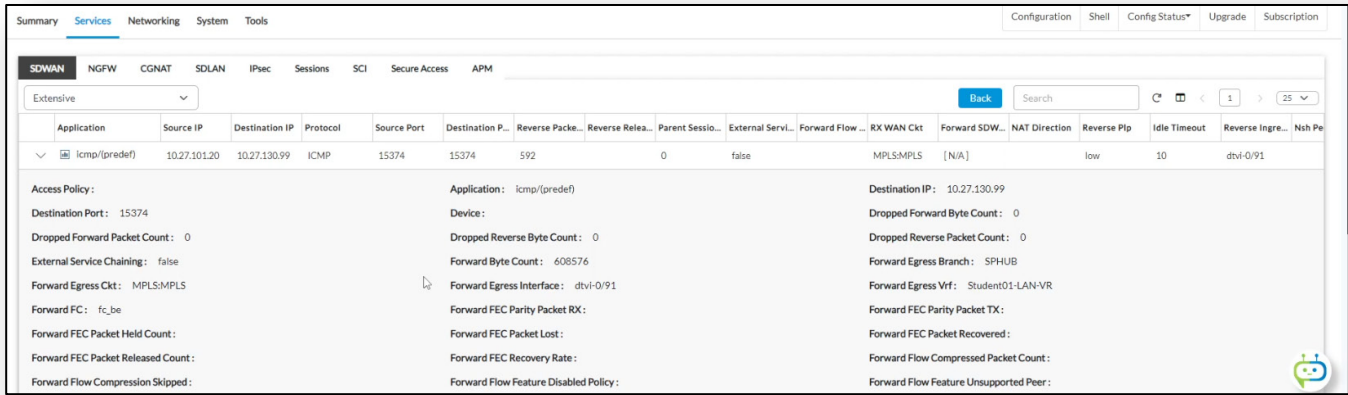


- m. Click on the number next to the session count to view the individual sessions that are active on the device.
- n. Locate the ICMP session and click on the session to view the session details. You can see the transmit and receive WAN circuit information.



- o. In the drop down menu at the top of the table, change the display from *brief* to *extensive* to view the extra information about the sessions.

p. Expand the information displayed by selecting *Detail* or *Extensive* from the drop down menu.



Application	Source IP	Destination IP	Protocol	Source Port	Destination P...	Reverse Packe...	Reverse Relea...	Parent Sessio...	External Servl...	Forward Flow ...	RX WAN Ckt	Forward SDW...	NAT Direction	Reverse Plp	Idle Timeout	Reverse Ingre...	Nsh Pe
icmp/(predef)	10.27.101.20	10.27.130.99	ICMP	15374	15374	592	0	false			MPLS/MPLS	[N/A]		low	10	dtvi-0/91	

Access Policy:

- Destination Port: 15374
- Dropped Forward Packet Count: 0
- External Service Chaining: false
- Forward Egress Ckt: MPLS/MPLS
- Forward FC: fc_be
- Forward FEC Packet Held Count:
- Forward FEC Packet Released Count:
- Forward Flow Compression Skipped:

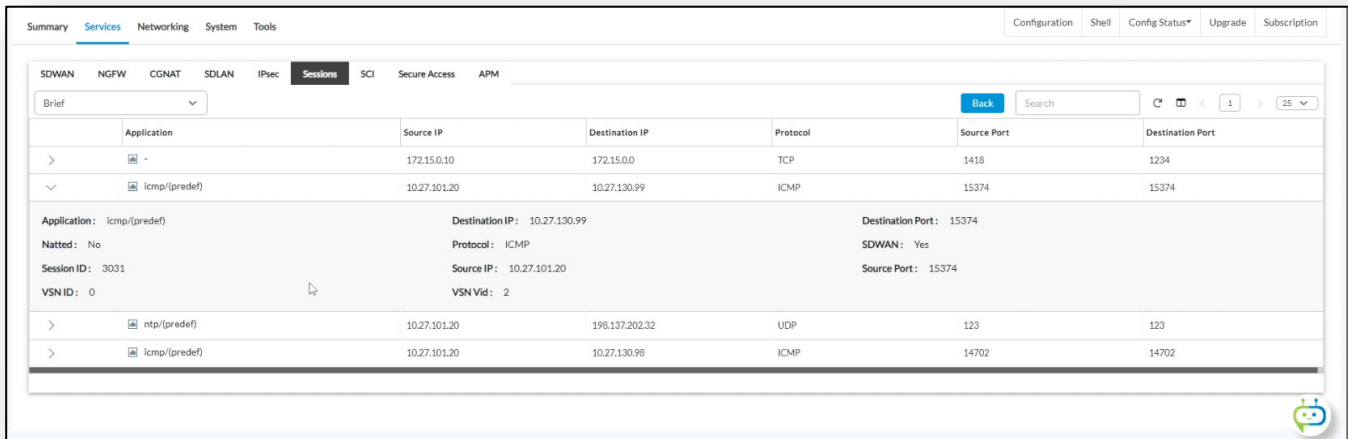
Application: icmp/(predef)

- Device:
- Dropped Reverse Byte Count: 0
- Forward Byte Count: 608576
- Forward Egress Interface: dtvi-0/91
- Forward FEC Parity Packet RX:
- Forward FEC Packet Lost:
- Forward FEC Recovery Rate:
- Forward Flow Feature Disabled Policy:

Destination IP: 10.27.130.99

- Dropped Forward Byte Count: 0
- Dropped Reverse Packet Count: 0
- Forward Egress Branch: SPHUB
- Forward Egress Vrf: Student01-LAN-VR
- Forward FEC Parity Packet TX:
- Forward FEC Packet Recovered:
- Forward Flow Compressed Packet Count:
- Forward Flow Feature Unsupported Peer:

q. Navigate to the main *Sessions* dashboard. This displays all session on the device.



Application	Source IP	Destination IP	Protocol	Source Port	Destination Port
-	172.15.0.10	172.15.0.0	TCP	1418	1234
icmp/(predef)	10.27.101.20	10.27.130.99	ICMP	15374	15374
ntp/(predef)	10.27.101.20	198.137.202.32	UDP	123	123
icmp/(predef)	10.27.101.20	10.27.130.98	ICMP	14702	14702

Application: icmp/(predef)

- Natted: No
- Session ID: 3031
- VSN ID: 0

Destination IP: 10.27.130.99

- Protocol: ICMP
- Source IP: 10.27.101.20
- VSN Vid: 2

Destination Port: 15374

- SDWAN: Yes
- Source Port: 15374

- r. Navigate to *Monitor > Services > SDWAN > Aggregate Traffic*.
- s. Select the SPHUB-NEW device from the drop down.

This shows the aggregate traffic to the SPHUB-NEW device. Here you can view the sent/received packets, and over which tunnels the traffic was sent.

Pvtl Index	Encap Type	RX Packets	RX Bytes	TX Packets	TX Bytes
1055	plaintext	247	169565	247	225644
1056	encrypted	241652	94994996	337026	154079040

- t. Navigate to *Monitor > Services > SDWAN > Policies*.
- u. From the menus, select *Default-Policy* to view the statistics.
- v. Expand the *Default Rule*.
- w. In the Default Rule select *Statistics > Remote Branch > SPHUB-NEW*.

Rule Name	Hit Count	TX Packets Tunnel	TX Bytes Tunnel	RX Packets Tunnel	RX Bytes Tunnel
Default-Rule	2945	69329	66544380	20890	20154256

Local Circuit	Remote Circuit	Hit Count	TX Packets Tunnel	TX Bytes Tunnel	RX Packets Tunnel	RX Bytes Tunnel
INET	Shared	0	0	0	0	0
INET	INET	0	10	10280	0	0
MPLS	MPLS	1841	101453	100727396	53814	55022576

The display should indicate that almost all traffic from the local site to the SPHUB-NEW site is through the MPLS transport.

- x. Change the drop down to *Path State*. This will show the path state information between the local site and the SPHUB-NEW site.

The screenshot shows the Versa SD-WAN management console interface. At the top, it displays system information for site 501B01 in San Diego, CA, USA, including management and system bridge addresses. The main navigation bar includes sections like Summary, Services, Networking, System, and Tools. The 'Services' section is active, showing various service categories such as SDWAN, NGFW, CGNAT, and SDLAN. The 'Forwarding Profiles' section is selected, displaying a table of path states for the 'Default-Policy' rule. The 'Path State' dropdown is set to 'SPHUB', and the 'Detail' view is selected. The table below shows the path list with columns for Local Circuit, Remote Circuit, Forwarding Class, Priority, Two Way Delay, Forward Delay Var, Rev Delay Var, Forward Loss Percentage, Rev Loss Percentage, and PDU Loss Percentage. The 'INET Shared' path is highlighted in grey and marked as 'Down', indicating it is not configured on the local site.

Local Circuit	Remote Circuit	Forwarding Class	Priority	Two Way Delay	Forward Delay Var	Rev Delay Var	Forward Loss Percentage	Rev Loss Percentage	PDU Loss Percentage
INET	INET	fc_ef	Priority 2	0	0	0	0.00	0.00	0.00
INET	Shared	fc_ef	Down	0	0	0	0.00	0.00	0.00
MPLS	MPLS	fc_ef	Priority 1	0	0	0	0.00	0.00	0.00

You can see that the path state for the INET Shared transport is currently down. This is because the local site does not have the Shared transport configured. It is only configured on the SPHUB-NEW site.

- y. Navigate to the *Monitor > Services > SDWAN > Sites* dashboard. This will display the sites that have been discovered by the B01 device.
- z. Click the arrow next to the Controller-01 device to view site information.

SDWAN Sites

Site Name	Management IP	Type	Up Time	Connectivity Status	Controller
Controller-01	172.15.0.2	remote	2d:5h:30m:31s	Connected	yes

Expanded Site Information:

- Connectivity Status: Connected
- Management IP: 172.15.0.2
- Site Name: Controller-01
- Site Type: controller
- VXLAN Remote IP: 172.15.0.3
- ESP Local IP: 172.15.0.10
- Site Chassis ID: Controller-01
- Site Network ID: 3
- Up Time: 2d:5h:30m:36s
- ESP Remote IP: 172.15.0.2
- Site ID: 1
- Site SA: no
- VXLAN Local IP: 172.15.0.11

Link	Circuit Family	Circuit Name	Link ID	Endpoint IP	NAT Status	Public IP	Public Port	Datapath IP	Datapath Port	Link Encryption	Shaping Rate
link1	ipv4	INET	1	10.234.2.103	false	10.234.2.103	4790	10.234.2.103	4790	optional	0

- aa. Expand the *SPHUB-NEW* site to view information about the SPHUB-NEW site.

Expanded Site Information:

- Connectivity Status: Connected
- Management IP: 172.15.0.12
- Site Name: SPHUB
- Site Type: branch
- VXLAN Remote IP: 172.15.0.13
- ESP Local IP: 172.15.0.10
- Site Chassis ID: SN-SP_HUB
- Site Network ID: 3
- Up Time: 2d:5h:30m:45s
- ESP Remote IP: 172.15.0.12
- Site ID: 104
- Site SA: yes
- VXLAN Local IP: 172.15.0.11

Link	Circuit Family	Circuit Name	Link ID	Endpoint IP	NAT Status	Public IP	Public Port	Datapath IP	Datapath Port	Link Encryption	Shaping Rate	Mir
link1	ipv4	MPLS	2	10.27.12.130	false	10.27.12.130	4790	10.27.12.130	4790	optional	0	0
link2	ipv4	Shared	3	10.27.130.98	false	10.27.130.98	4790	10.27.130.98	4790	optional	0	0
link3	ipv4	INET	1	10.27.11.130	false	10.27.11.130	4790	10.27.11.130	4790	optional	0	0

ab. Navigate to the *Monitor > Services > SDWAN > SLA Metrics* dashboard.

ac. Select site *SPHUB-NEW* from the drop down menu.

The screenshot shows the SDWAN SLA Metrics dashboard for site SPHUB. The table displays the following data:

Path Handle	Remote Site Na...	Forward Class	Local WAN Link	Remote WAN LL...	Local WAN Link...	Remote WAN LL...	Two Way Delay...	Forward Delay ...	Rev Delay Var...	PDU Loss Ratio...	Forward Loss R...	Rev Loss Ratio...	Forward Loss	Rev Loss	PDU Sent	PDU Received
6820100	SPHUB	fc_ef	INET	INET	1	1	0	0	0	0.0	0.0	0.0	0	0	5	5
6820612	SPHUB	fc_ef	INET	Shared	1	3	0	0	0	100.0	0.0	0.0	0	0	4	0
6824452	SPHUB	fc_ef	MPLS	MPLS	2	2	0	0	0	0.0	0.0	0.0	0	0	5	5

This displays the SLA statistics for each path. Note that many values are 0 because the lab environment has very low delay, jitter, and latency.

ad. Select the *SLA Paths* tab to display path information.

ae. Select the *SPHUB-NEW* device from the drop down menu.

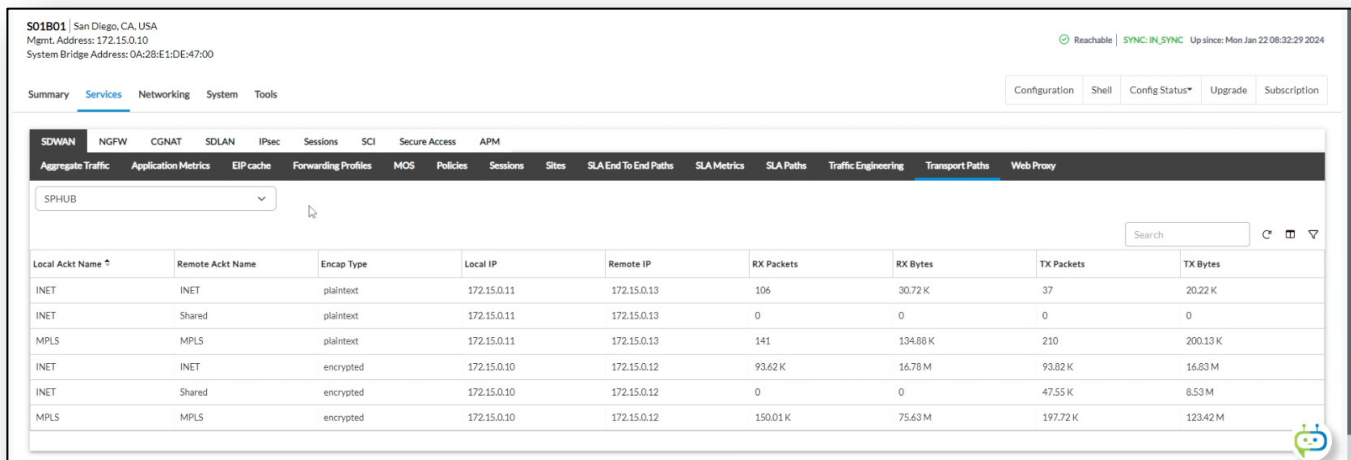
The screenshot shows the SDWAN SLA Paths dashboard for site SPHUB. The table displays the following data:

Path Handle	Remote Site Name	Forward Class	Local WAN Link	Remote WAN Link	Local WAN Link ID	Remote WAN Link ID	Path Mtu	Adaptive Monitoring	Damp State	Damp Flaps	Connection State	Flaps	Last Flapped
6820100	SPHUB	fc_ef	INET	INET	1	1	1500	active	disable	0	up	3	07:01:22
6820612	SPHUB	fc_ef	INET	Shared	1	3		active	disable	0	down	1	2:05h31m
6824452	SPHUB	fc_ef	MPLS	MPLS	2	2	1500	active	disable	0	up	5	07:01:21

This displays the current path properties between the local site and the SPHUB-NEW site.

af. Navigate to *Monitor > Services > SDWAN > Transport Paths*.

ag. Select the *SPHUB-NEW* device from the drop down menu.



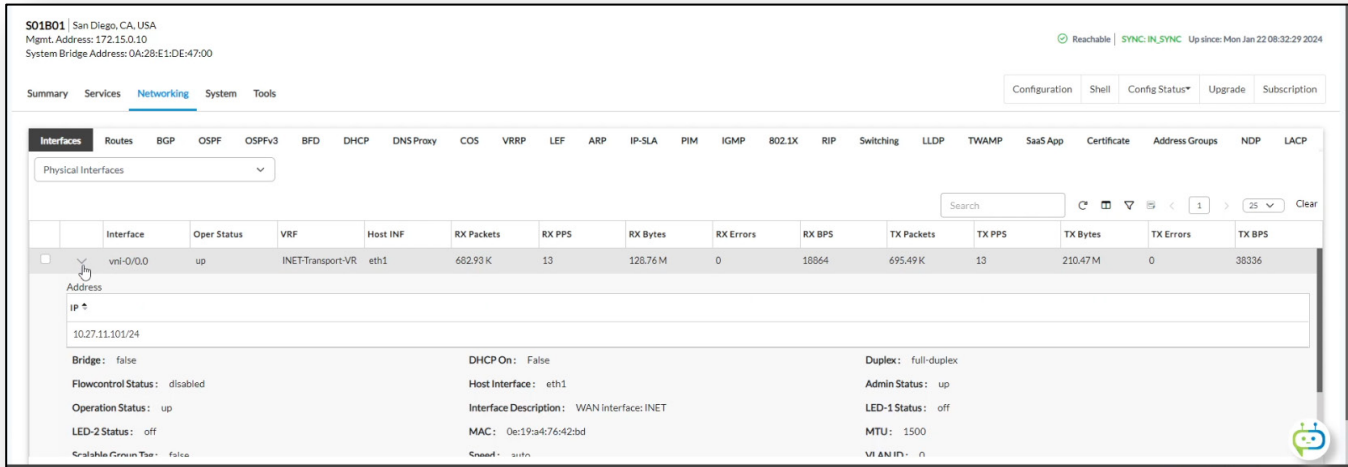
The screenshot shows the Versa SD-WAN management interface for device SPHUB. The 'Transport Paths' section is active, displaying a table of transport paths between sites. The table includes columns for Local Ackt Name, Remote Ackt Name, Encap Type, Local IP, Remote IP, RX Packets, RX Bytes, TX Packets, and TX Bytes. The data is as follows:

Local Ackt Name	Remote Ackt Name	Encap Type	Local IP	Remote IP	RX Packets	RX Bytes	TX Packets	TX Bytes
INET	INET	plaintext	172.15.0.11	172.15.0.13	106	30.72 K	37	20.22 K
INET	Shared	plaintext	172.15.0.11	172.15.0.13	0	0	0	0
MPLS	MPLS	plaintext	172.15.0.11	172.15.0.13	141	134.88 K	210	200.13 K
INET	INET	encrypted	172.15.0.10	172.15.0.12	93.62 K	16.78 M	93.82 K	16.83 M
INET	Shared	encrypted	172.15.0.10	172.15.0.12	0	0	47.55 K	8.53 M
MPLS	MPLS	encrypted	172.15.0.10	172.15.0.12	150.01 K	75.63 M	197.72 K	123.42 M

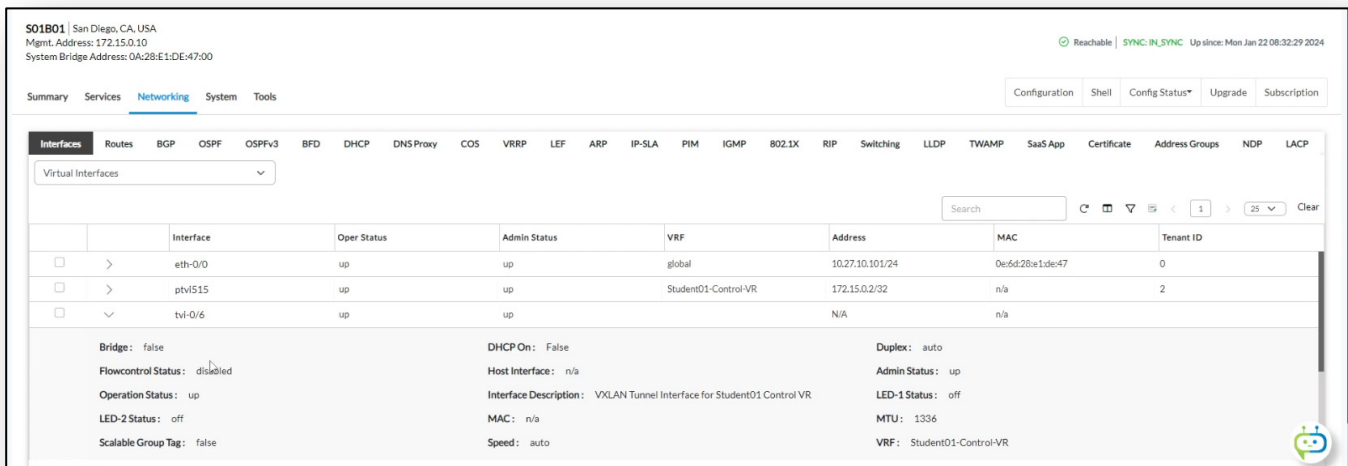
This displays all of the transport paths between the sites and the type of tunnel encapsulation on each path.

ah. Navigate to *Monitor > Networking > Interfaces*. The Physical Interfaces should be selected by default.

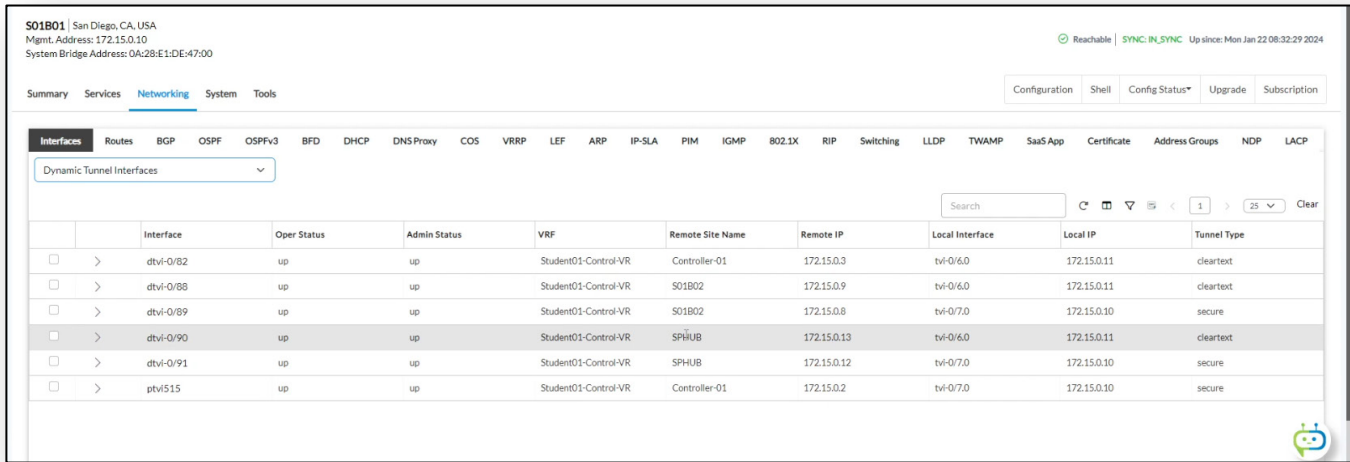
ai. In the interfaces table, expand the *vni-0/0.0* interface to view the interface properties.



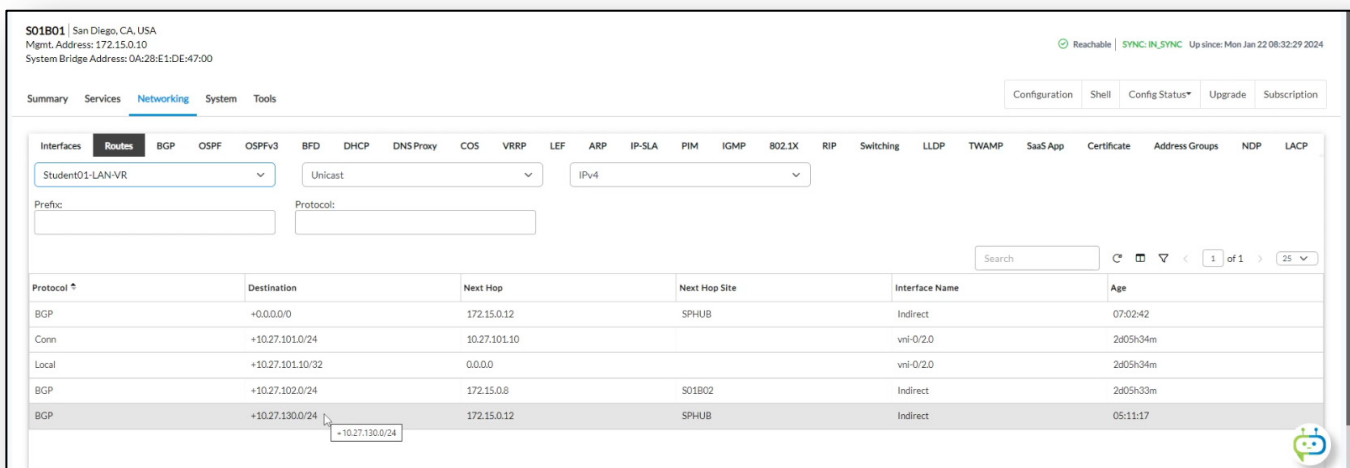
aj. Select *Virtual Interfaces* from the drop down menu. This displays the tunnel interfaces on the system.



ak. Select *Dynamic Tunnel Interfaces* from the drop down menu. This displays the dynamic tunnels that have been created between sites.



al. Navigate to *Monitor > Networking > Routes*, then select the *Student-LAN-VR* from the drop down. This will display the routes in the Student-LAN-VR routing table.



Note the routes and next hops of the following:

- 10.27.13.0/24 > Network connected to the hub site
- 10.27.1xx.0/24 > LAN connected to the B02 branch. This will vary depending on your organization.
- 10.27.1xx.0/24 > LAN connected to the local site. This will vary depending on your organization.

am. Navigate to the *Monitor > System* dashboard. This displays information about the appliance, its licensing, and the processes running on the appliance.

System Summary

Hardware Information		Software Information	
CPU Count / Cores	8	Package Name	versa-fleevnf-2023
Disk Size	77.30GiB	Package ID	5ac317d
Manufacturer	Amazon EC2	Release	22.1.2
Memory	14.99GiB	Build Type	bionic
Model	c5.2xlarge	Creator	jenkins
Serial#	SN-S01B01	Date	Sun Jul 30 2023
SKU	Not Specified	Major	22
Hardware Serial #	ec2a8c6f-a27a-1462-71b3-42e6843324f3	Minor	1
		Service	2
		Reltype	GA

an. Scroll down to view the site summary, location, and templates that are associated with the device.

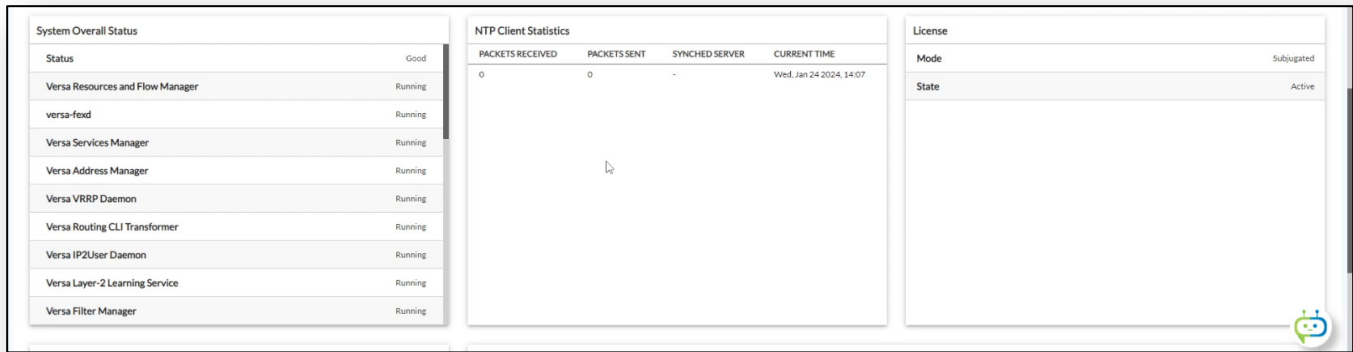
S01B01 - Summary

Configured Address: San Diego, CA, USA
 Mgmt. Address: 172.15.0.10
 Coordinates: Configured
 Source: 117.16108
 Longitude: 32.71573
 Latitude: -
 Altitude: -
 System Bridge Address: 0A:2B:E1:DE:47:00

Associate Templates

Device Group	DG-S01-NGFW-No-DIA
Post Staging Template	S01_Template-NGFW-No-DIA
Service Templates	Student01-DataStore Category: DataStore

ao. Scroll down to view the overall system status and the license information.



The screenshot displays three panels from the Versa SD-WAN management interface:

- System Overall Status:** Shows a 'Status' of 'Good' and a list of services running.
- NTP Client Statistics:** A table showing 0 packets received and sent, with the current time as Wed, Jan 24 2024, 14:07.
- License:** Shows the license mode as 'Subjugated' and the state as 'Active'.

System Overall Status	
Status	Good
Versa Resources and Flow Manager	Running
versa-foxd	Running
Versa Services Manager	Running
Versa Address Manager	Running
Versa VRRP Daemon	Running
Versa Routing CLI Transformer	Running
Versa IP2User Daemon	Running
Versa Layer-2 Learning Service	Running
Versa Filter Manager	Running

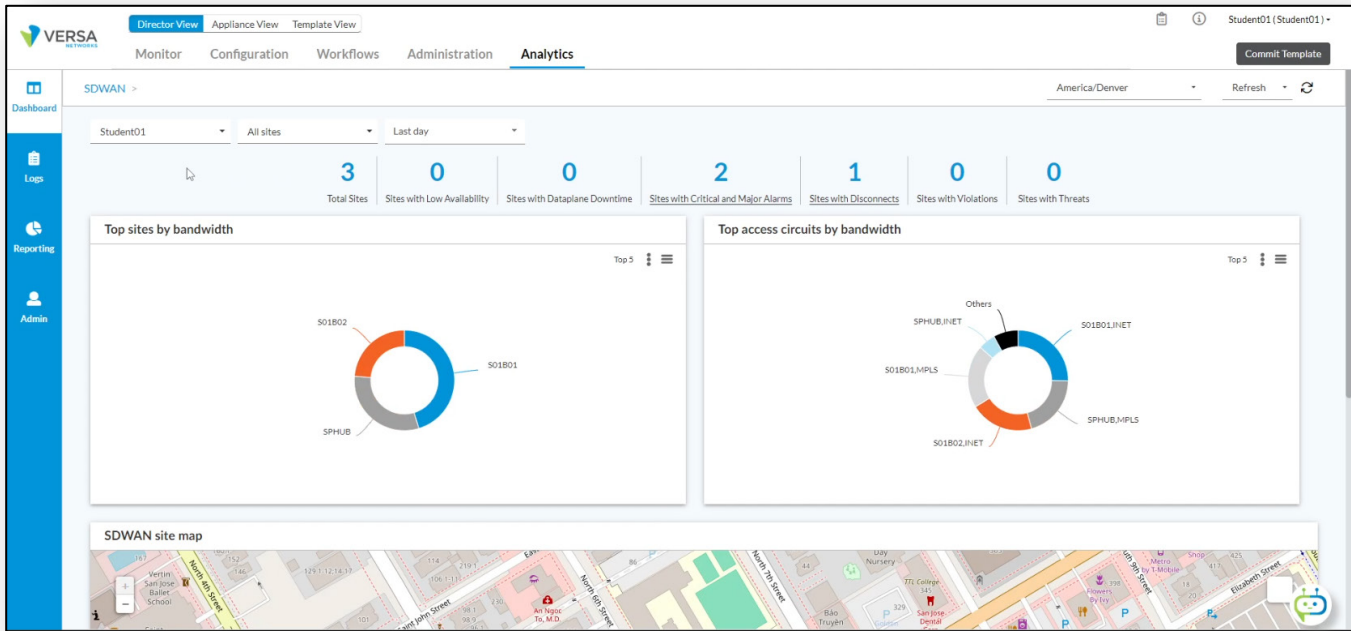
NTP Client Statistics			
PACKETS RECEIVED	PACKETS SENT	SYNCHED SERVER	CURRENT TIME
0	0	-	Wed, Jan 24 2024, 14:07

License	
Mode	Subjugated
State	Active

Note that the Mode is Subjugated. This means that the device is attached to and controlled by Versa Director.

Step 2. Explore Versa Analytics

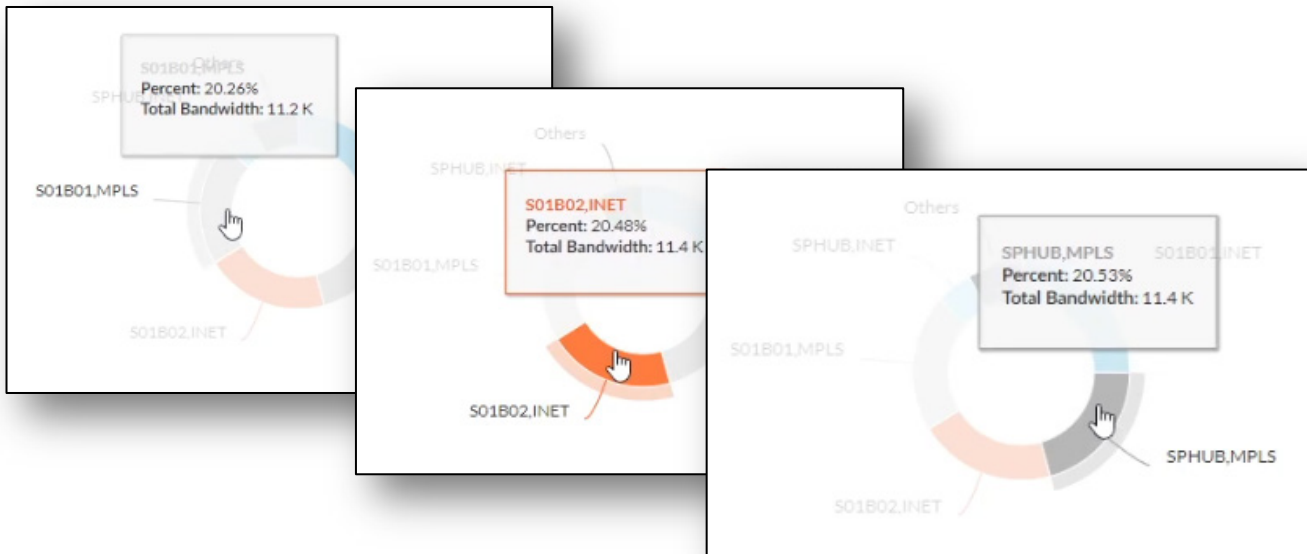
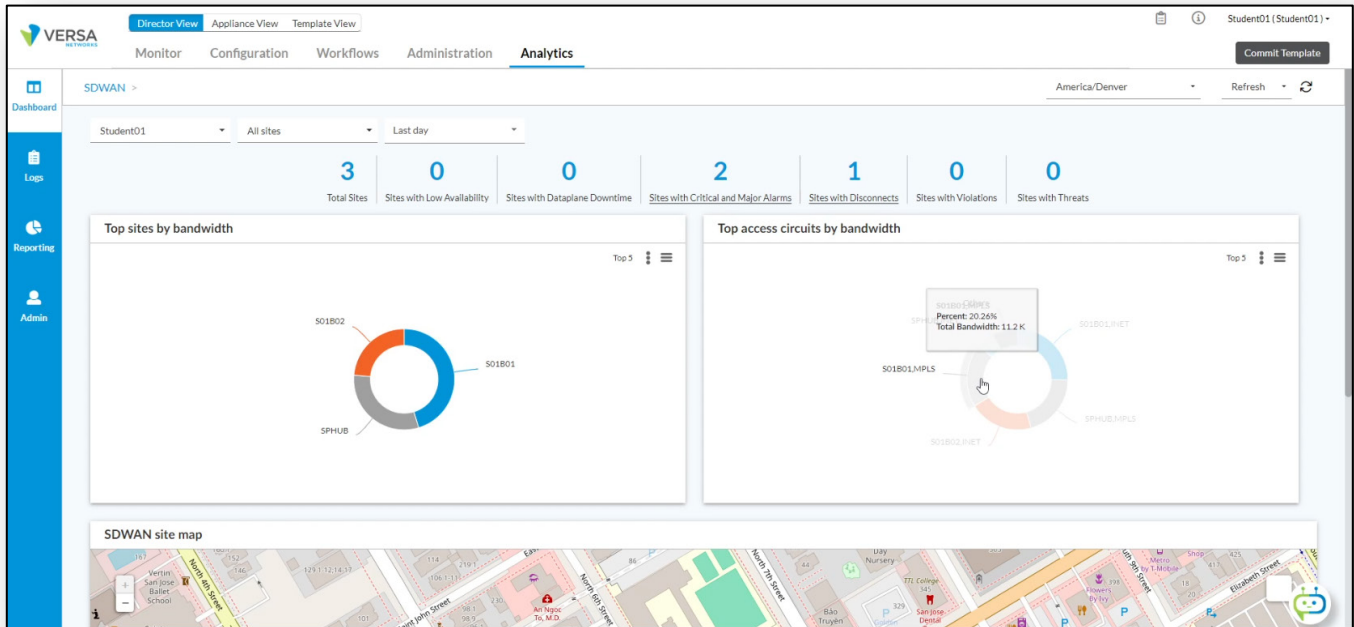
- a. Navigate to *Director View > Analytics* to open the main Analytics dashboard.



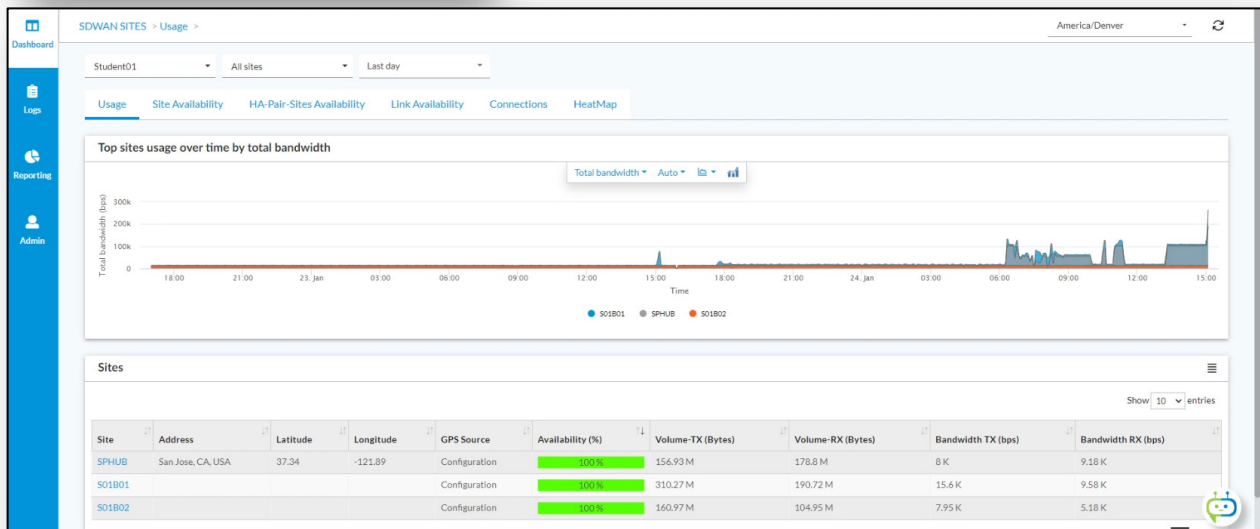
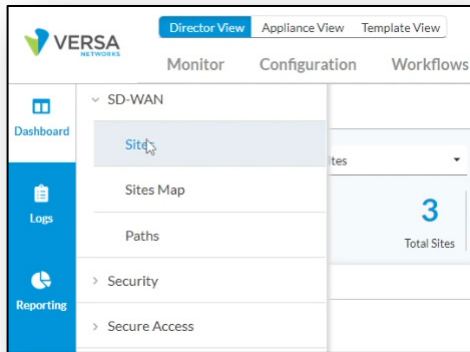
- b. In the main Analytics dashboard, hover over the chart in the Top sites by bandwidth dashboard. Information about each site will pop up in a small chart.



- c. In the main Analytics dashboard, hover over the chart in the Top access circuits by bandwidth. Information about each circuit will be displayed.

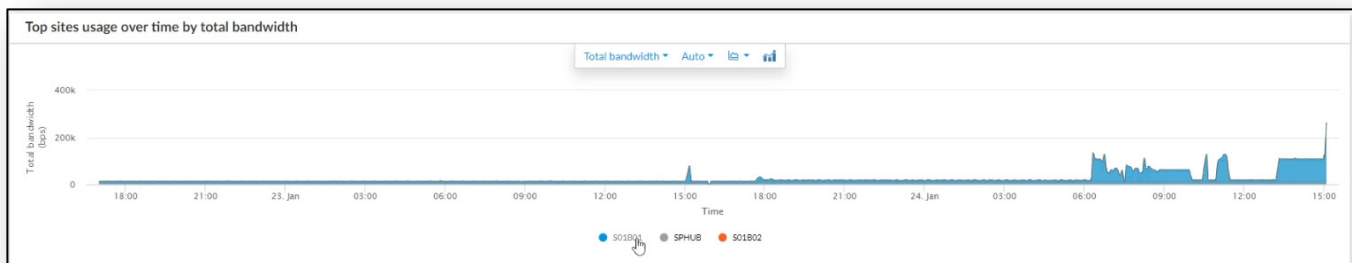


d. Navigate to *Dashboard > SD-WAN > Sites* to view site information. This will display information about the sites.

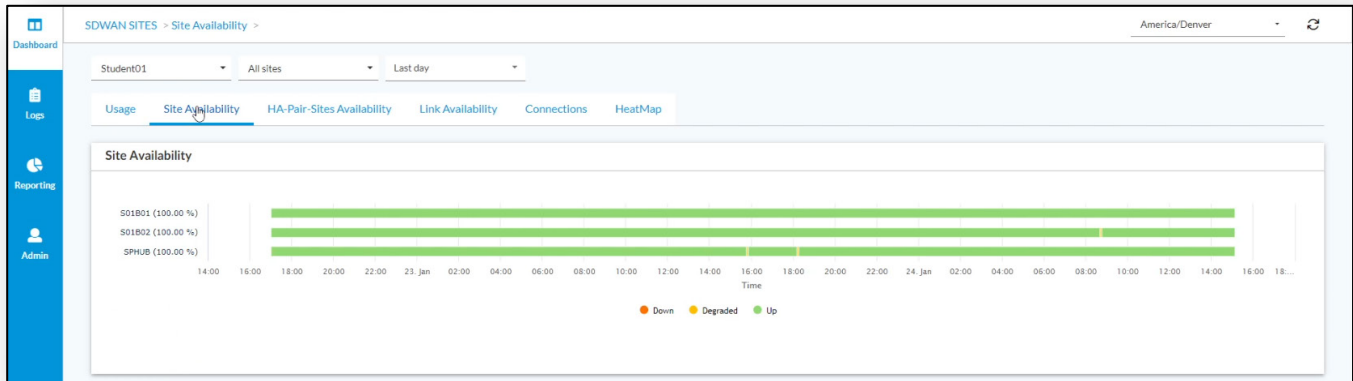


You have the ability to filter or display information by selecting organization, site, and time frame from the drop downs at the top of the dashboard.

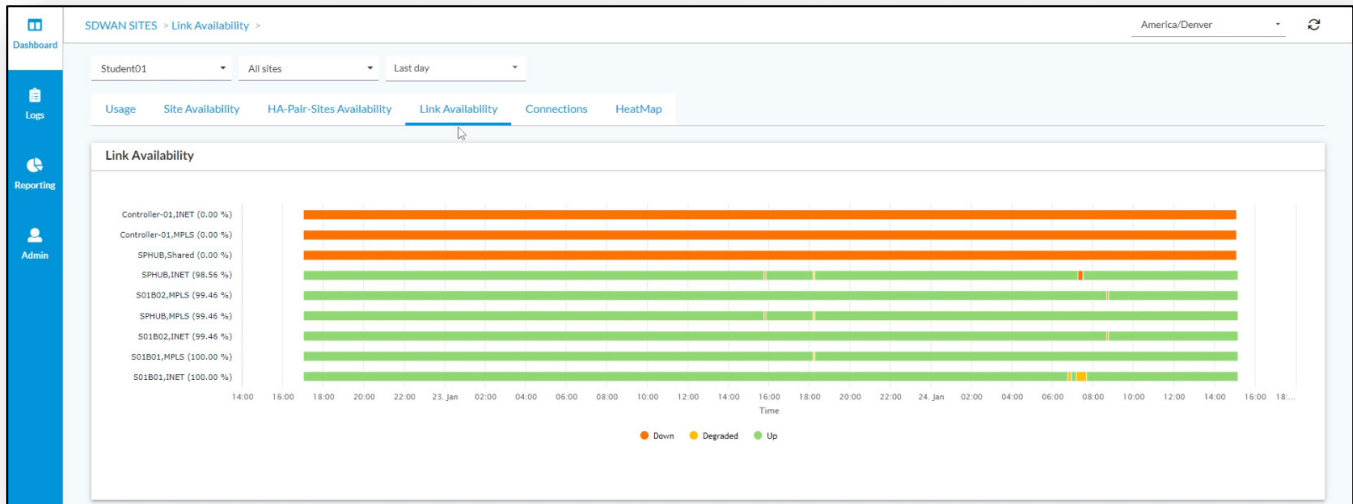
On charts, you can hover your mouse over the legend items to highlight them, and to grey-out the other items. You can click on the items in the legend to activate/deactivate them in the chart.



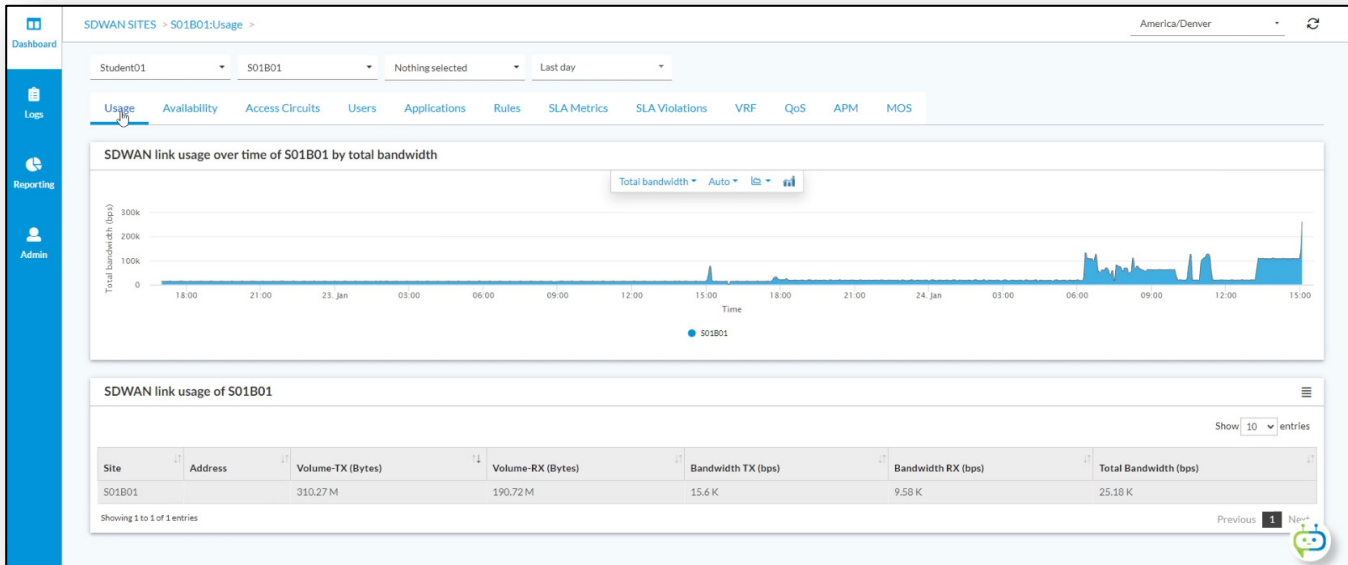
- e. Select *Site Availability* to view a history of the site status and availability.



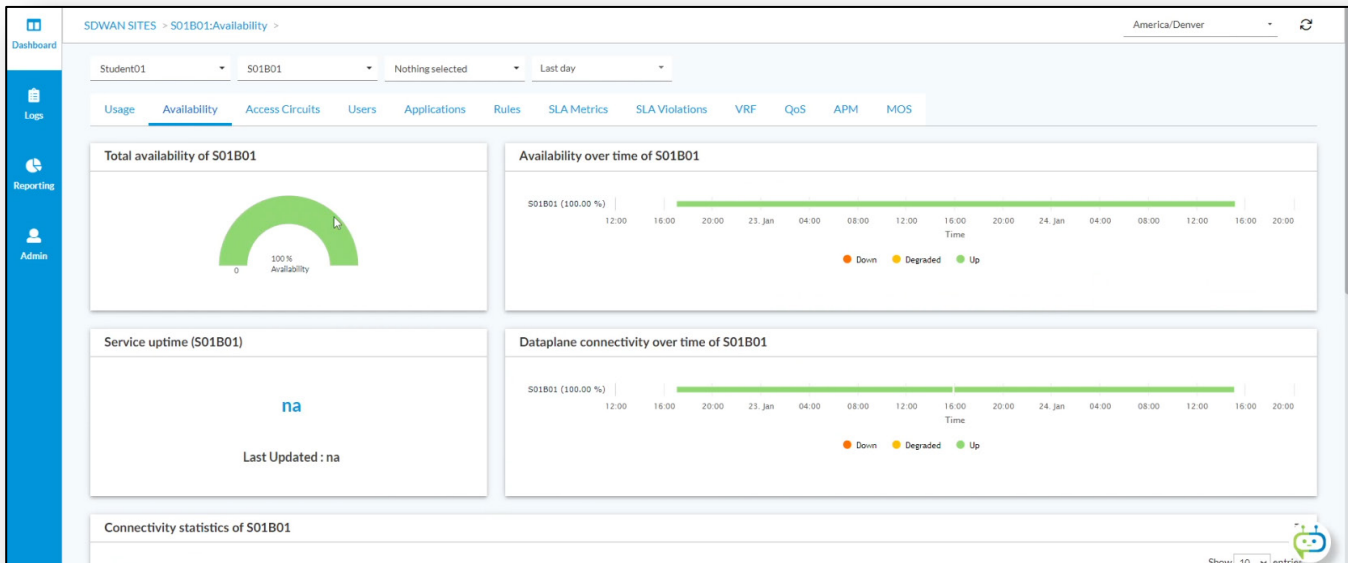
- f. Navigate to the *Link Availability* chart. This shows the link availability in the environment.



g. In the *Sites* menu, select SxxB01 to view site specific information, then click on the *Usage* tab to view site usage.



h. Navigate to the *Availability* tab. This will display the site availability over time.



- i. Navigate to *Access Circuits*. This will display historical statistics about the access circuits on branch SxxB01.

SDWAN SITES > S01B01:Access Circuits > America/Denver

Student01 | S01B01 | Nothing selected | Last day

Usage | Availability | **Access Circuits** | Users | Applications | Rules | SLA Metrics | SLA Violations | VRF | QoS | APM | MOS

SDWAN overall usage over time of S01B01 by total bandwidth

SDWAN overall traffic usage of S01B01

Site	Access circuit	Uplink Bandwidth (bps)	Downlink Bandwidth (bps)	Type	Media	IP	ISP	Volume-TX (Bytes)	Volume-RX (Bytes)	Bandwidth TX (bps)	Bandwidth RX (bps)
S01B01	INET	NaN undefined	NaN undefined	N/A	N/A	N/A	N/A	176.04 M	104.68 M	8.75 K	5.2 K
S01B01	MPLS	NaN undefined	NaN undefined	N/A	N/A	N/A	N/A	134.23 M	86.04 M	6.85 K	4.38 K

Showing 1 to 2 of 2 entries

SDWAN application traffic usage over time of S01B01 by total bandwidth

DIA application traffic usage over time of S01B01 by total bandwidth

SDWAN application traffic usage summary of S01B01

Site	Access circuit	IP	Volume-TX (Bytes)	Volume-RX (Bytes)	Bandwidth TX (bps)	Bandwidth RX (bps)
S01B01	MPLS	N/A	96.83 M	53.15 M	11.45 K	6.28 K
S01B01	INET	N/A	580.26 K	0	15.47 K	0

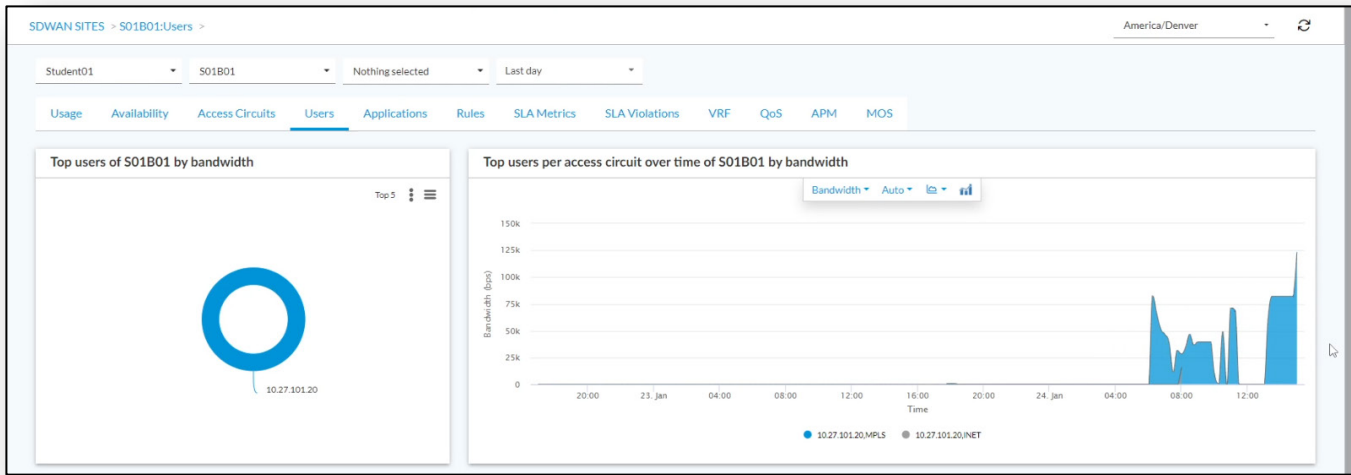
Showing 1 to 2 of 2 entries

DIA application traffic usage summary of S01B01

Site	Access circuit	IP	Volume-TX (Bytes)	Volume-RX (Bytes)	Bandwidth TX (bps)	Bandwidth RX (bps)
S01B01	INET	N/A	31.32 K	30.28 K	4	4

Showing 1 to 1 of 1 entries

- j. Navigate to *Users*. This will display historical statistics about user sessions. When active directory integration is not active, users are displayed by IP address.



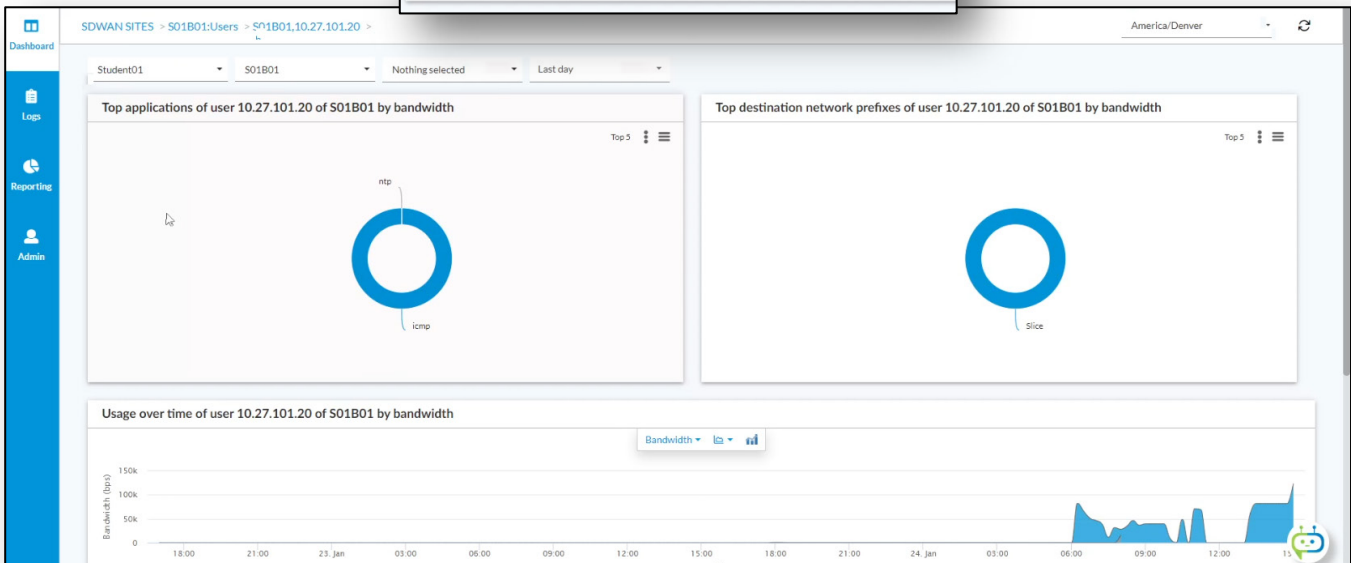
- k. Click on the magnifying glass next to a user to see more details about that user’s usage. You can scroll down the page to see more information about the site.

Users usage (S01B01)

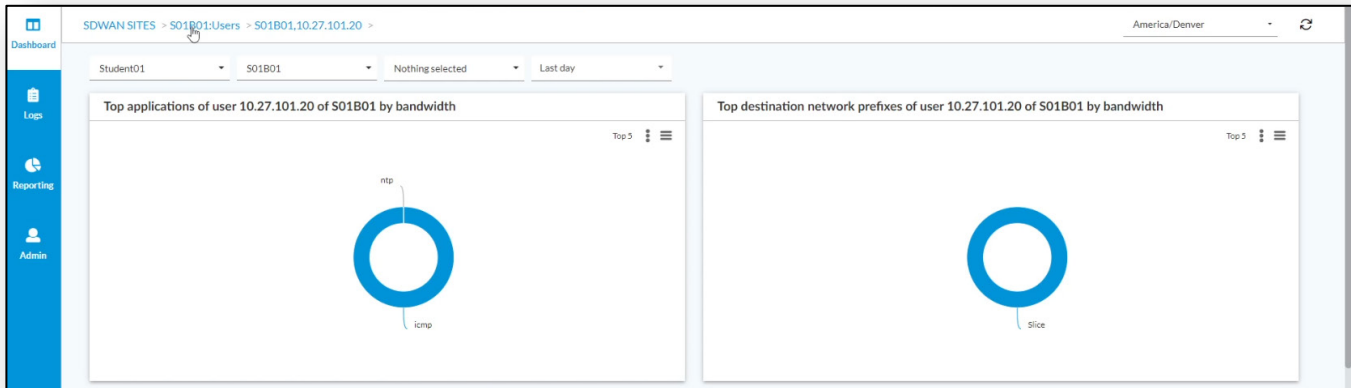
Set filters here... Apply | Clear | Copy Filter

Site	User	Sessions	Volume-TX (Bytes)
S01B01	10.27.101.20	2.27 K	97.43 M

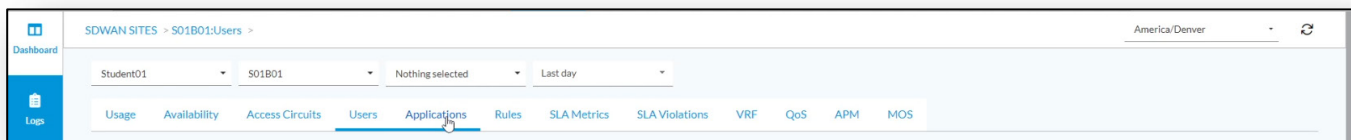
Showing 1 to 1 of 1 entries



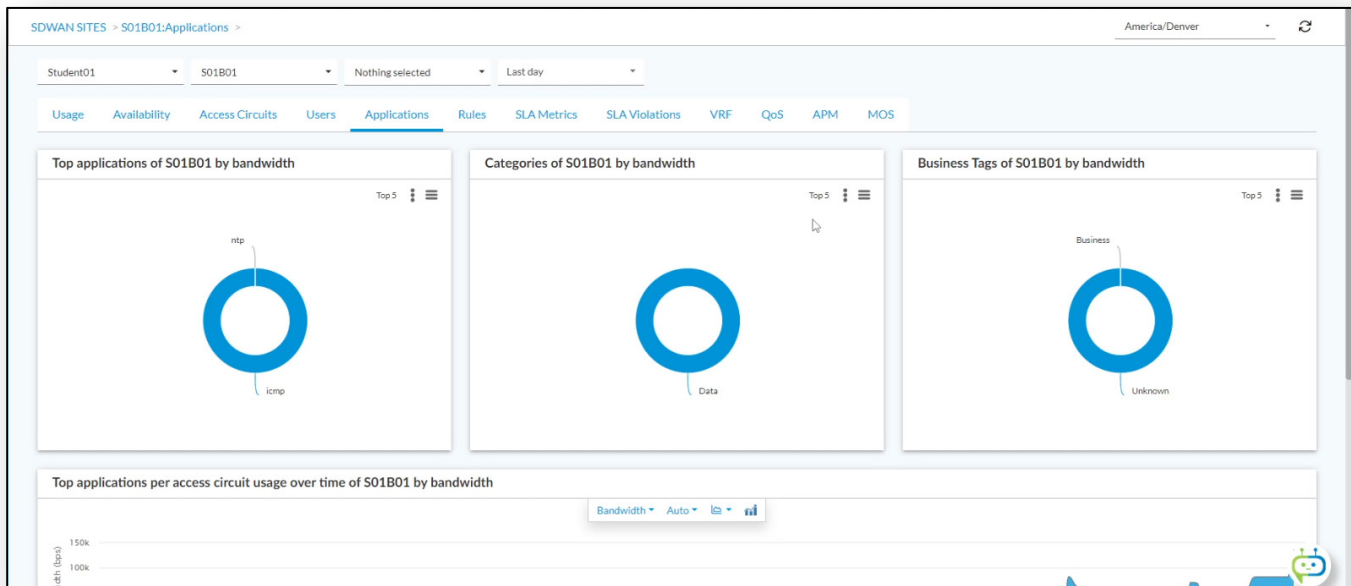
When you navigate into a specific set of data, you will have the navigation path listed at the top of the dashboard. You can jump back to a previous level by clicking on that level in the navigation path.



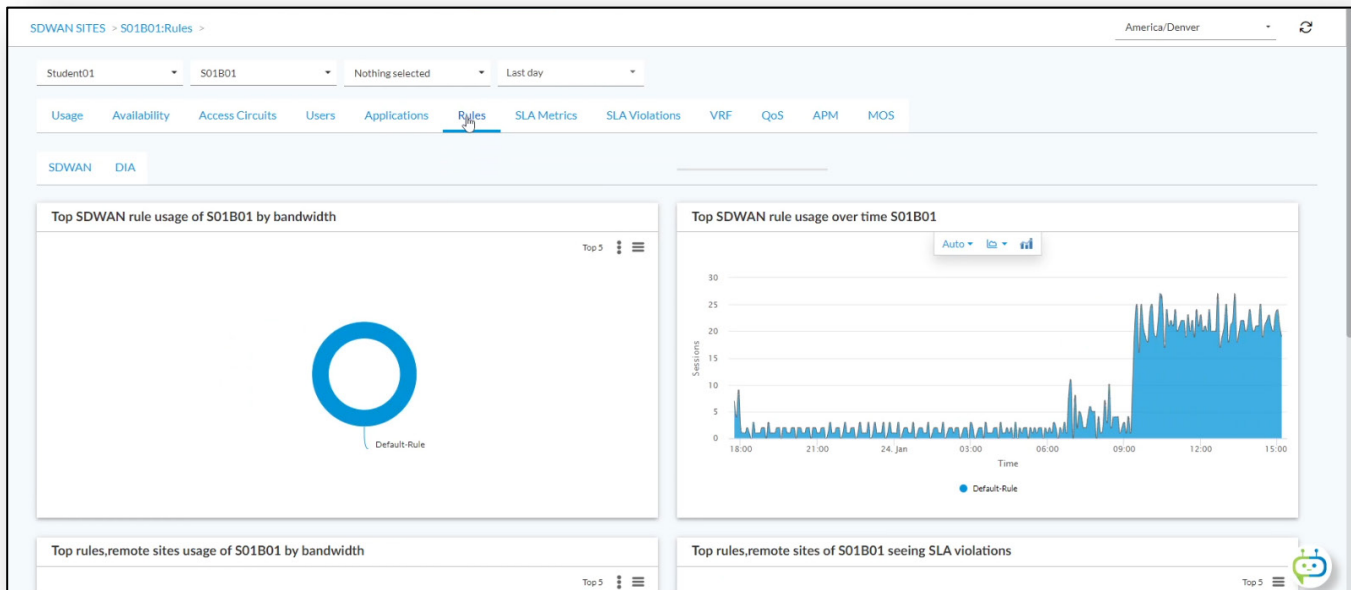
- l. Click on the *SxxB01:Users* level of the navigation path to return to the main Users dashboard.
- m. Navigate to the *Applications* dashboard of the SxxB01 site.



This dashboard displays the applications that the user has accessed over time.



- n. Navigate to the Rules tab. If you have SD-WAN traffic rules in place, the rule usage will be displayed. In the lab environment there is only a default rule in place.

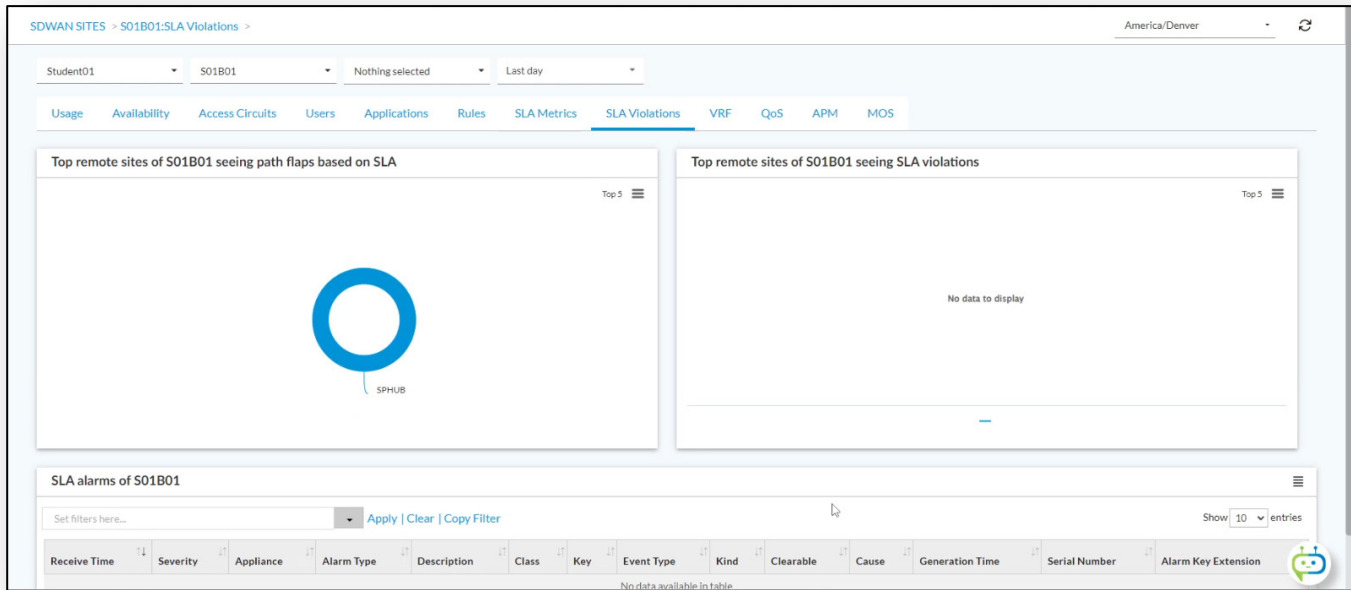


The SLA Metrics table displays the SLA information between the sites. Note that in the lab environment many of the values are listed at 0, as there is very little delay and jitter within the lab network.

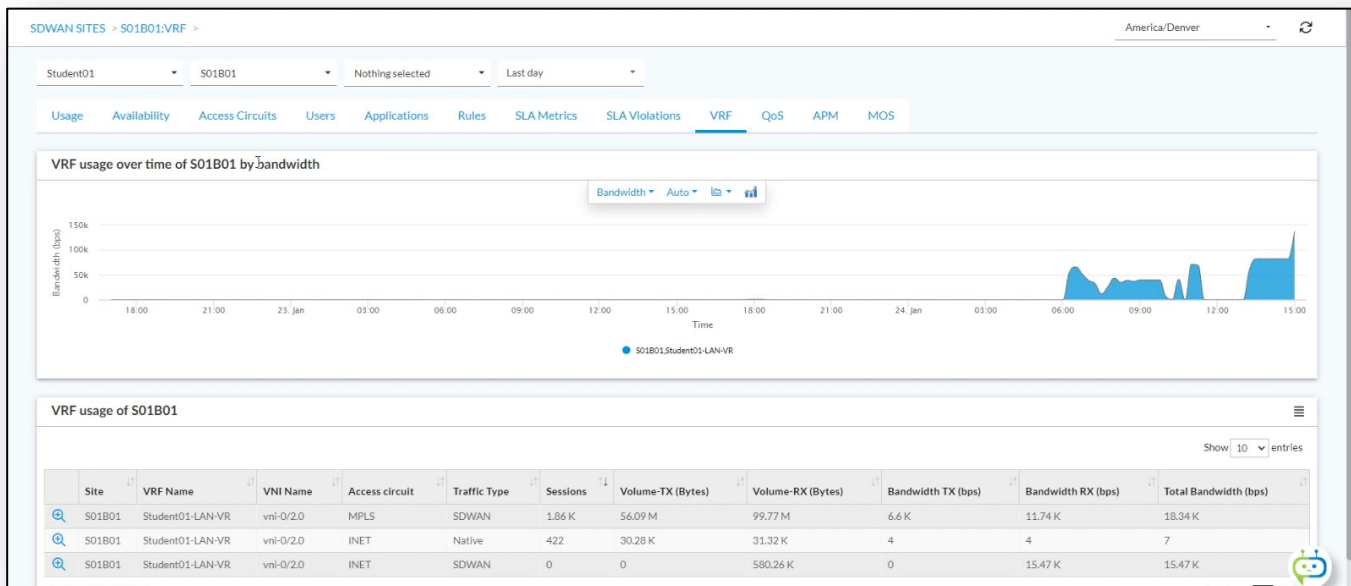
The screenshot shows the 'SLA Metrics' tab for site S01B01. The 'Top SLA measurement of S01B01 by delay' chart shows 'No data to display'. Below it is a table titled 'SLA measurement of S01B01' with 12 columns: Local Site, Remote Site, Local Access Circuit, Remote Access Circuit, Forwarding class, Logs count, Delay (ms), Forward Delay Variation (ms), Reverse Delay Variation (ms), Forward Loss Ratio (%), PDU Loss Ratio (%), and Reverse. The table contains three rows of data.

Local Site	Remote Site	Local Access Circuit	Remote Access Circuit	Forwarding class	Logs count	Delay (ms)	Forward Delay Variation (ms)	Reverse Delay Variation (ms)	Forward Loss Ratio (%)	PDU Loss Ratio (%)	Reverse
S01B01	SPHUB	MPLS	MPLS	fc_ef	233	0ms	0ms	0ms	0.25%	0.37%	0.00%
S01B01	SPHUB	INET	Shared	fc_ef	233	0ms	0ms	0ms	0.00%	100.00%	0.00%
S01B01	SPHUB	INET	INET	fc_ef	228	0ms	0ms	0ms	0.25%	0.38%	0.00%

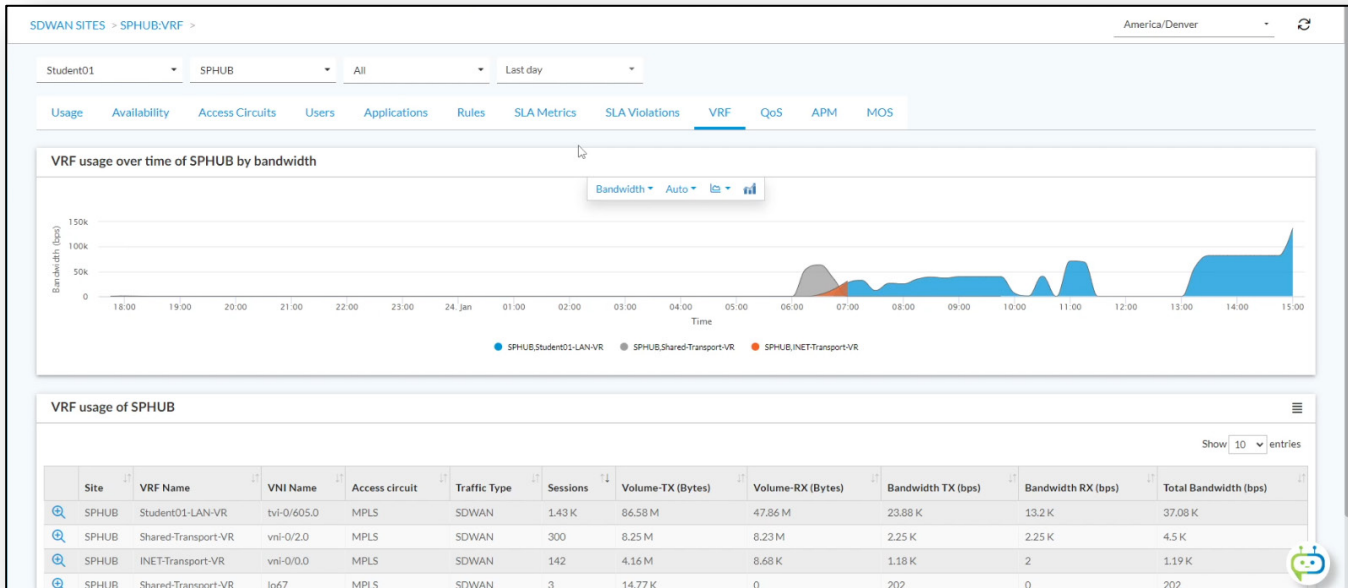
SLA violations are registered whenever the path parameters between sites fall below configured performance thresholds. The SLA Violations dashboard shows an historical view of any SLA path violations.



VRF usage monitors the resources used by each VRF in the system. For each tenant, there is currently a single VRF configured (the LAN facing VR).

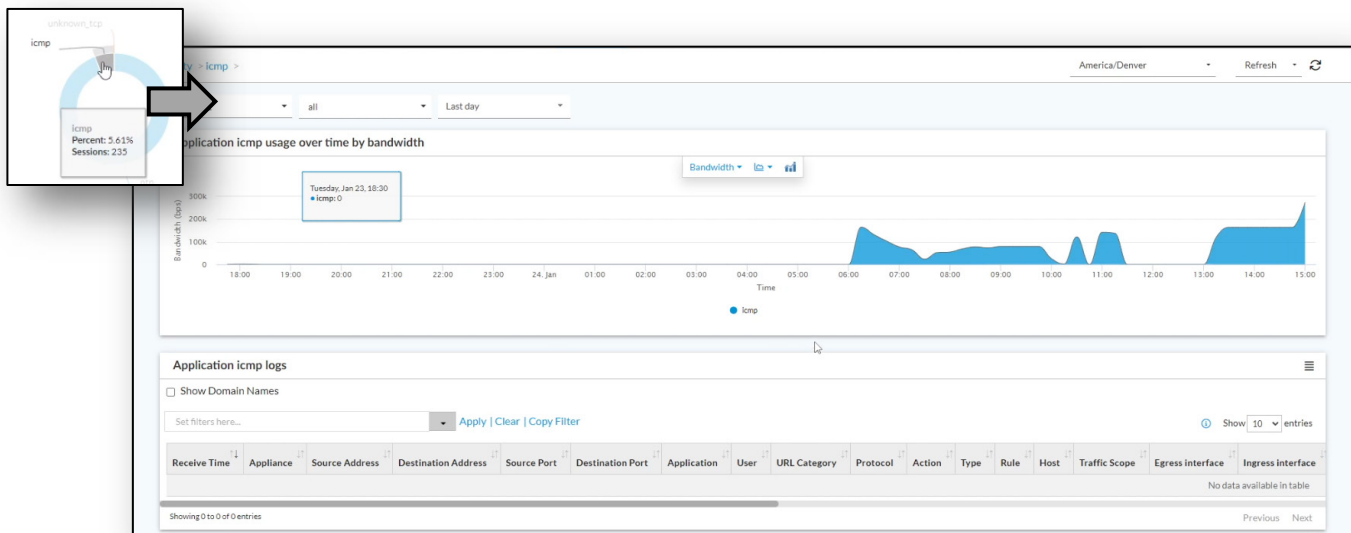
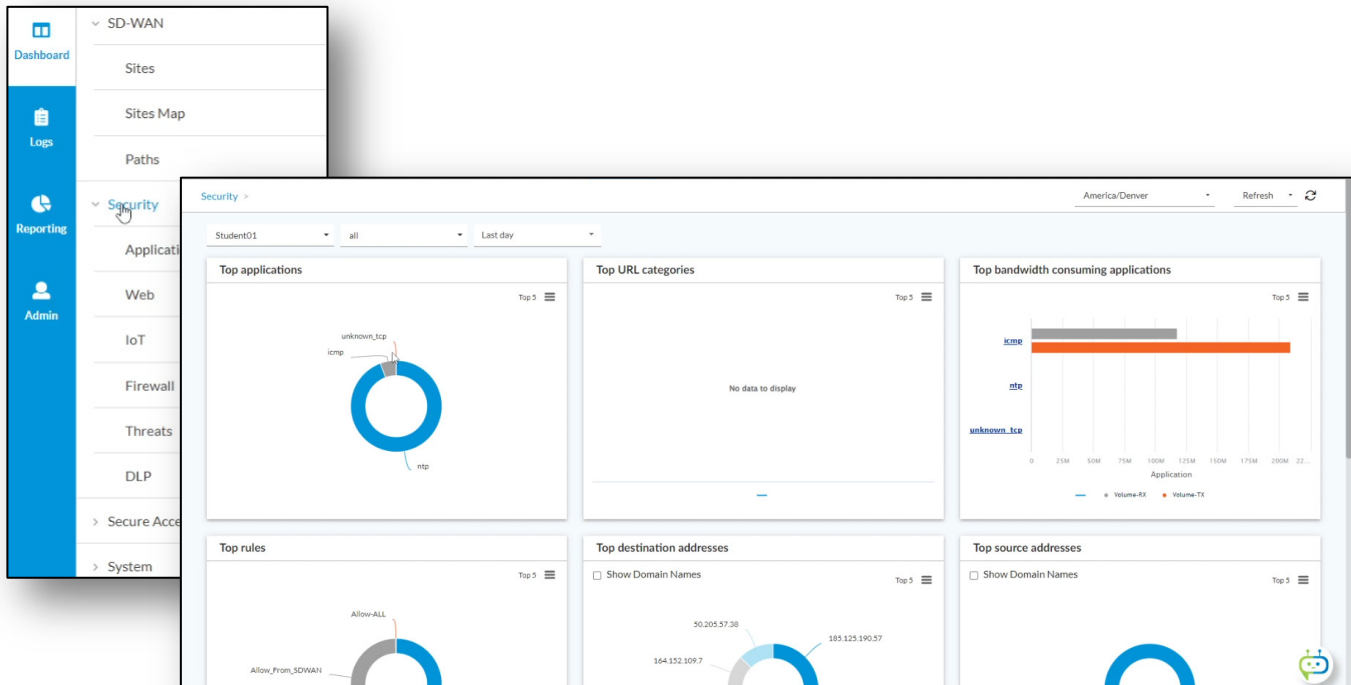


- o. Select the *SPHUB-NEW* device from the device drop down menu. This will display the VRF usage information on the hub site.



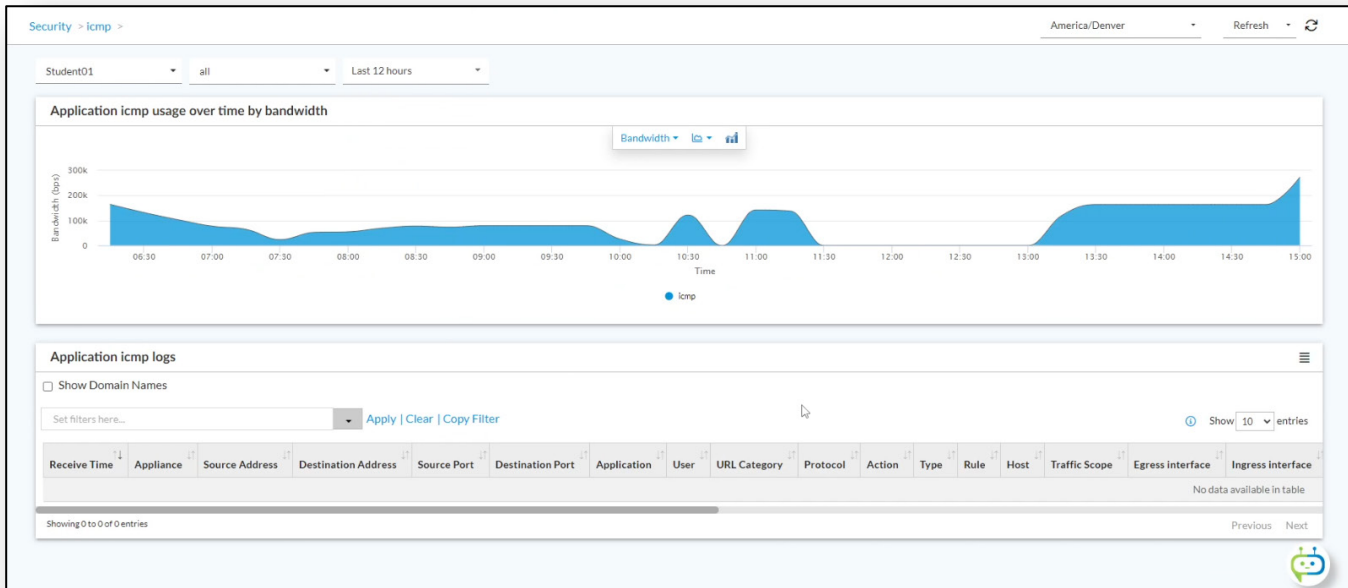
There are multiple VRFs available to the Studentxx organization on the hub site, including the WAN transport networks.

p. Navigate to the *Dashboard* > *Security* to view the main security dashboard.

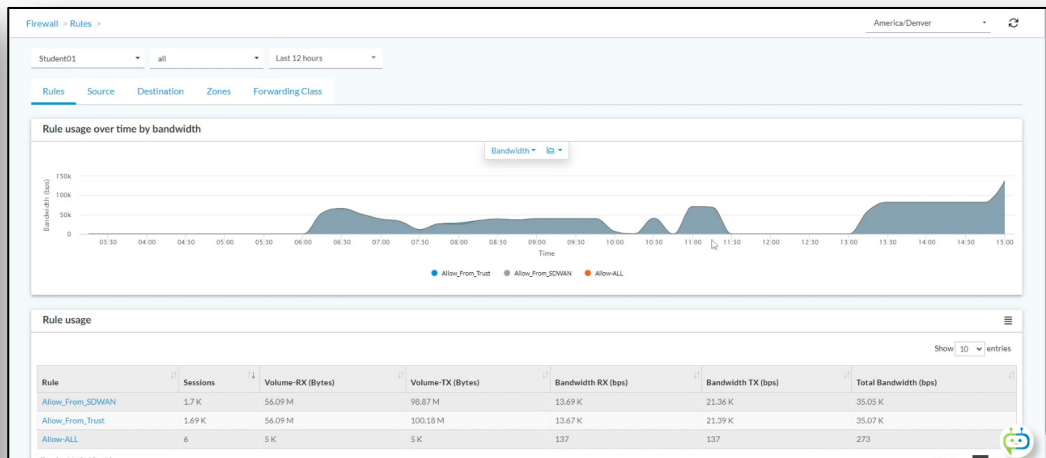
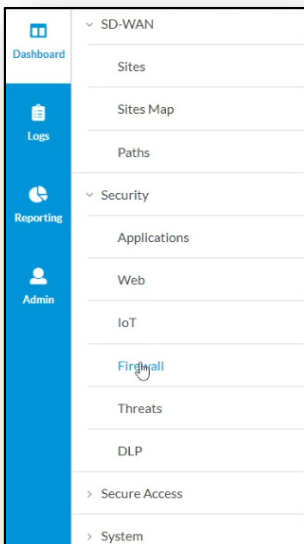


The main security dashboard displays charts of the top activity in the system from a security perspective. You can hover your mouse over different charts to see more information, or click on many charts to expand that information. Hover over and click on the icmp data in the chart. If you click on the icmp data in the chart, a window opens with more information about the chart entry.

The application specific charts display information about the selected application. Because this is a lab environment, and you just started to generate new traffic across the SD-WAN, select Last 12 hours in the time filter.



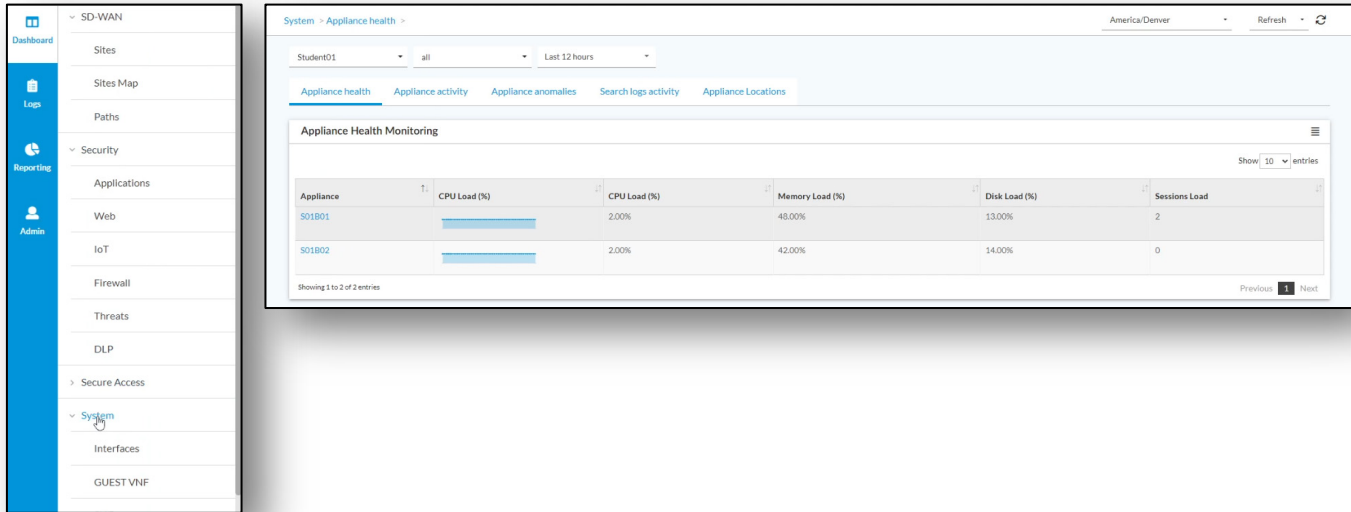
q. To view firewall information, navigate to the *Dashboard > Security > Firewall* dashboard.



Firewall information can be displayed based on rules, source and destination addresses and zones, and the forwarding class of traffic. Take a few moments to view some of the information available in the Firewall dashboard.

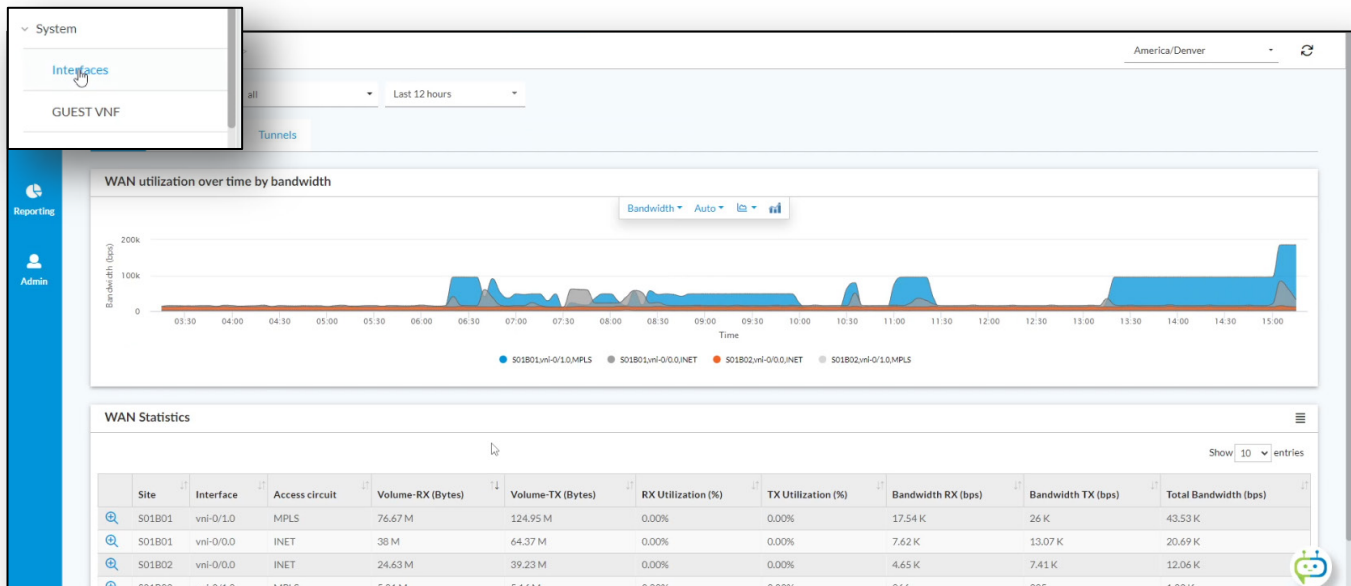
Historical system health information is displayed in the *Dashboard > System* dashboards. Subcategories of system information include interfaces and the guest VNF information.

- r. Navigate to *Dashboard > System* to view the main system dashboard.



The main appliance health dashboard displays the CPU, memory, disk, and session load over time.

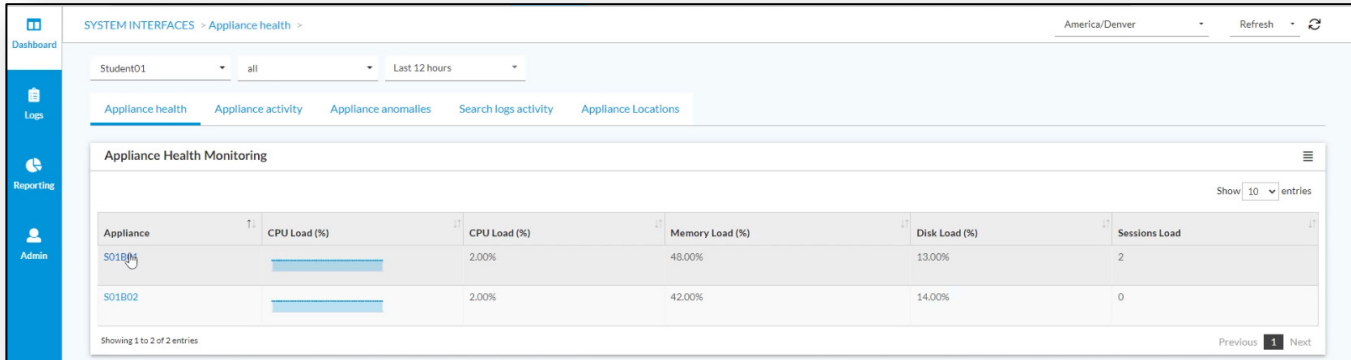
The *System > Interfaces* dashboard displays historical interface activity over a period of time.



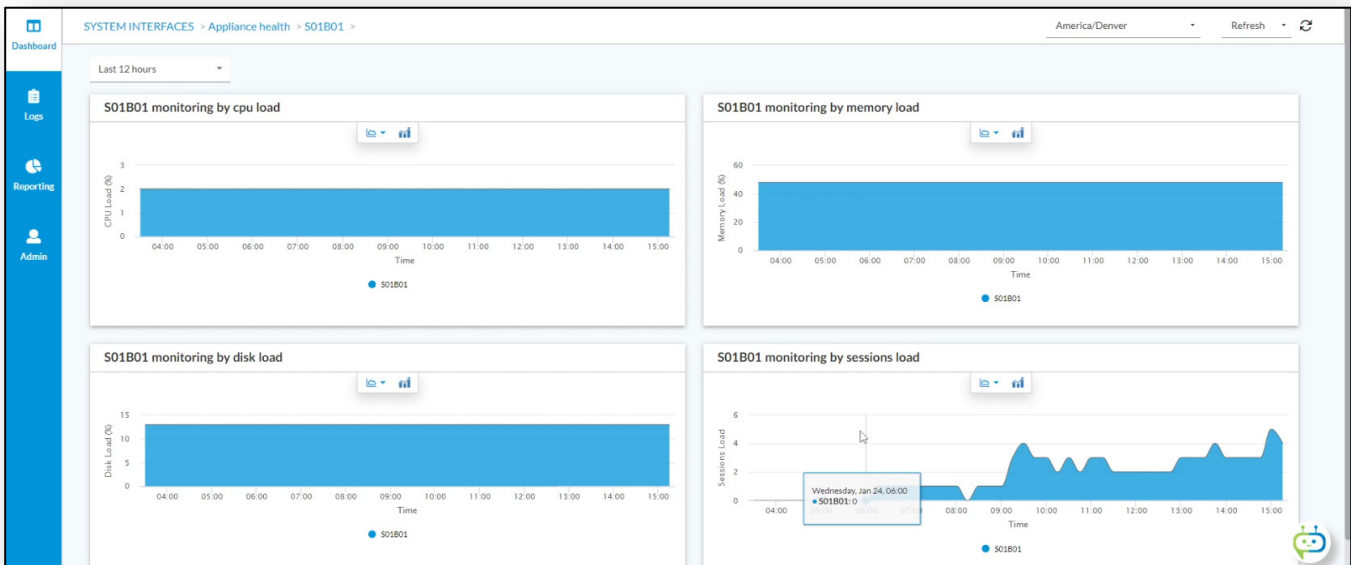
- s. Return to the main *System* dashboard.

When you click on an appliance name, detailed information about that appliance will be displayed.

- t. In the *Dashboard* > *System* main dashboard, click on the SxxB01 device in the appliance list.

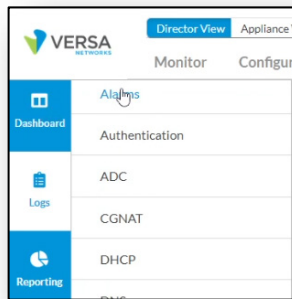


Detailed information about the appliance health and activity (over time) is displayed.



System logs, alerts, and alarms are sent to Versa Analytics from VOS devices.

- u. Navigate to the *Logs > Alarms* dashboard.



Alarm > Logs > America/Denver

Student01 | all | Last 12 hours

Logs | Charts | Summary

Alarms

Set filters here... Apply | Clear | Copy Filter Show 10 entries

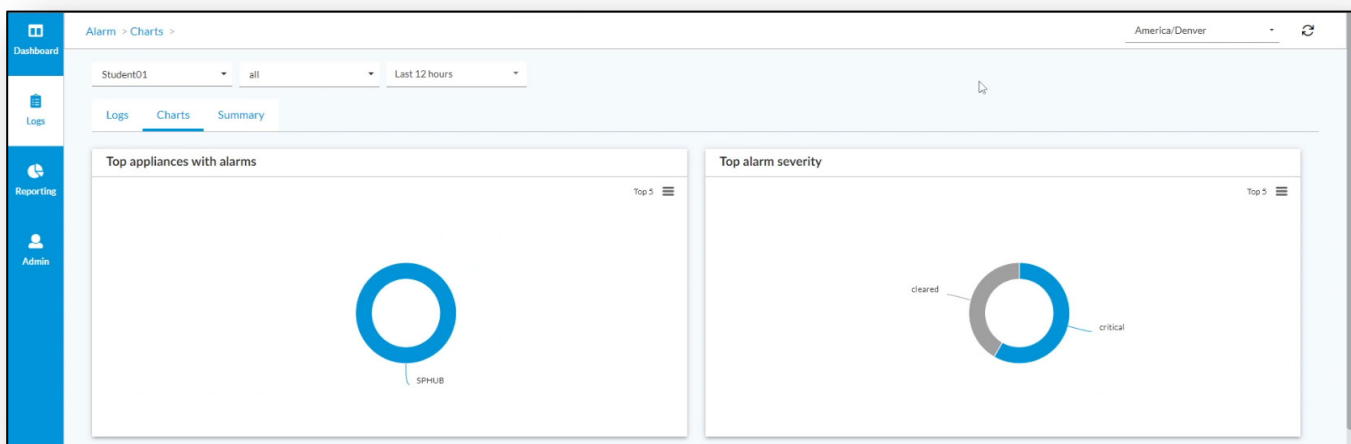
Receive Time	Severity	Appliance	Alarm Type	Description	Class	Key	Event Type	Kind	Clearable	Cause	Generation Time
Jan 24th 2024, 9:54:22 AM MST	critical	SPHUB	bgp-nbr-state-change	BGP Instance 3015: Peer 169.254.0.10 transitioned to Active state	new	3015 169.254.0.10	communicationsAlarm	symptom	no	causeOther	Jan 24th 2024, 9:5
Jan 24th 2024, 7:32:22 AM MST	cleared	SPHUB	interface-down	Interface vni-0/0 is up (n/a)	cleared	vni-0/0	equipmentAlarm	symptom	yes	outOfService	Jan 24th 2024, 7:3
Jan 24th 2024, 7:32:20 AM MST	cleared	SPHUB	interface-down	Interface vni-0/0 is up (n/a)	cleared	vni-0/0	equipmentAlarm	symptom	yes	outOfService	Jan 24th 2024, 7:3
Jan 24th 2024, 7:32:19 AM MST	critical	SPHUB	bgp-nbr-state-change	BGP Instance 3015: Peer 169.254.0.8 transitioned to Active state	new	3015 169.254.0.8	communicationsAlarm	symptom	no	causeOther	Jan 24th 2024, 7:3
Jan 24th 2024, 7:14:17 AM MST	critical	SPHUB	interface-down	Interface vni-0/0 is down (n/a)	new	vni-0/0	equipmentAlarm	symptom	yes	outOfService	Jan 24th 2024, 7:1
Jan 24th 2024, 7:14:15 AM MST	critical	SPHUB	interface-down	Interface vni-0/0 is down (n/a)	new	vni-0/0	equipmentAlarm	symptom	yes	outOfService	Jan 24th 2024, 7:1
Jan 24th 2024, 7:09:18 AM MST	cleared	SPHUB	bgp-nbr-state-change	BGP Instance 3015: Peer 169.254.0.8 transitioned to Established state	new	3015 169.254.0.8	communicationsAlarm	symptom	no	causeOther	Jan 24th 2024, 7:0
Jan 24th 2024, 7:02:51 AM MST	critical	SPHUB	bgp-nbr-state-change	BGP Instance 3015: Peer 169.254.0.8 transitioned to Active state	new	3015 169.254.0.8	communicationsAlarm	symptom	no	causeOther	Jan 24th 2024, 7:0
Jan 24th 2024, 6:54:07 AM MST	cleared	SPHUB	interface-down	Interface vni-0/0 is up (n/a)	cleared	vni-0/0	equipmentAlarm	symptom	yes	outOfService	Jan 24th 2024, 6:5
Jan 24th 2024, 6:54:05 AM MST	cleared	SPHUB	interface-down	Interface vni-0/0 is up (n/a)	cleared	vni-0/0	equipmentAlarm	symptom	yes	outOfService	Jan 24th 2024, 6:5

Showing 1 to 10 of 12 entries Previous 1 2 Next

The alarms and their active/cleared states are listed.

The Charts dashboard displays top alarms and severity in a chart format.

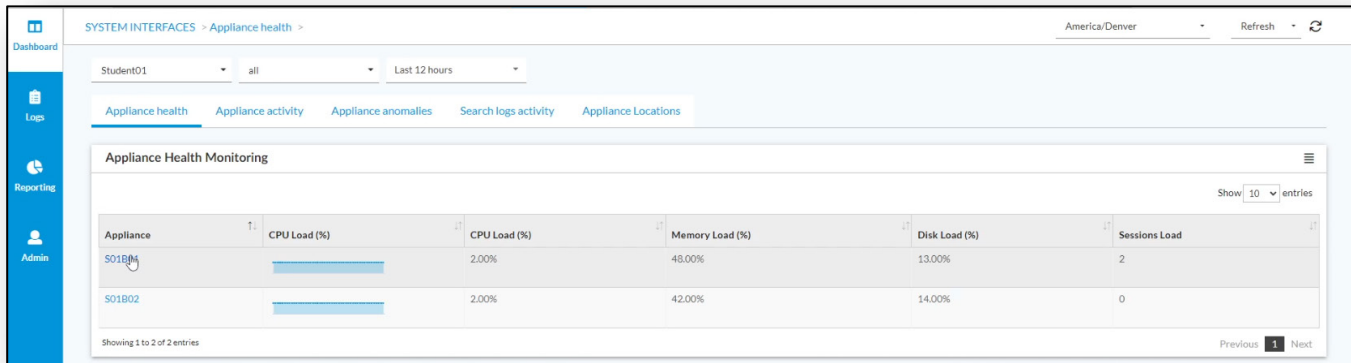
- v. Click the Charts tab to view the alarms charts.



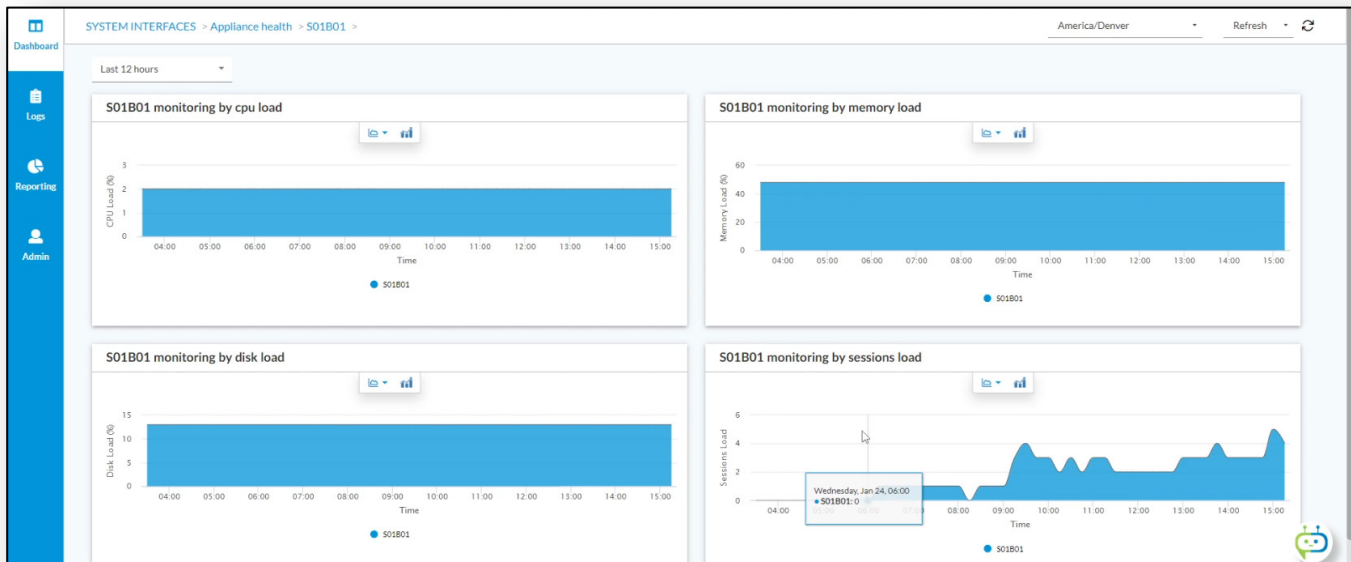
w. Return to the main System dashboard.

When you click on an appliance name, detailed information about that appliance will be displayed.

x. In the *Dashboard* > *System* main dashboard, click on the *SxxB01* device in the appliance list.

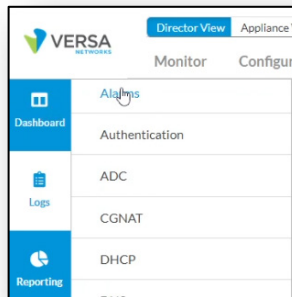


Detailed information about the appliance health and activity (over time) is displayed.



System logs, alerts, and alarms are sent to Versa Analytics from VOS devices.

- y. Navigate to the *Logs > Alarms* dashboard.



Alarm > Logs > America/Denver

Student01 | all | Last 12 hours

Logs | Charts | Summary

Alarms

Set filters here... Apply | Clear | Copy Filter Show 10 entries

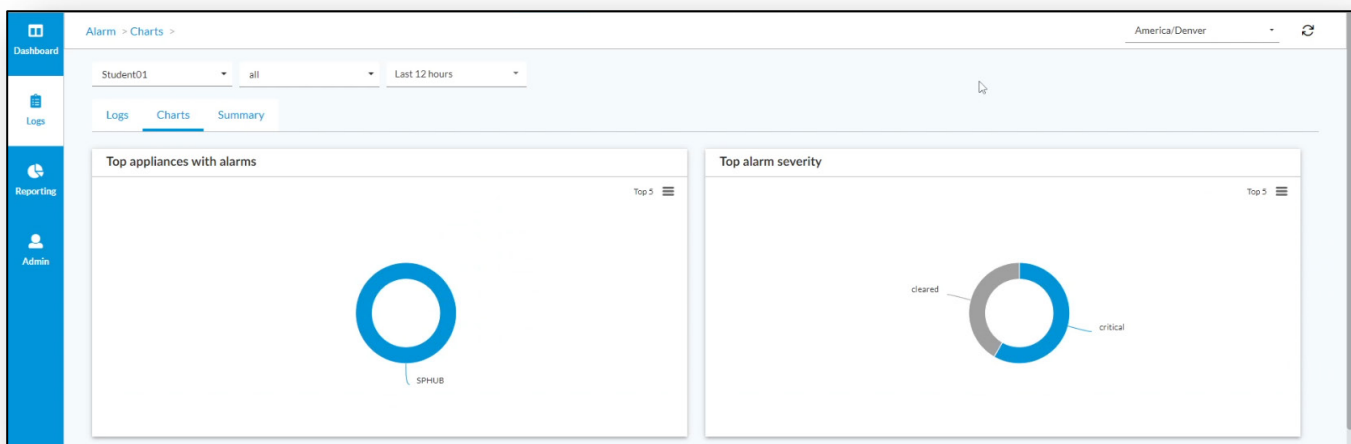
Receive Time	Severity	Appliance	Alarm Type	Description	Class	Key	Event Type	Kind	Clearable	Cause	Generation Time
Jan 24th 2024, 9:54:22 AM MST	critical	SPHUB	bgp-nbr-state-change	BGP Instance 3015: Peer 169.254.0.10 transitioned to Active state	new	3015 169.254.0.10	communicationsAlarm	symptom	no	causeOther	Jan 24th 2024, 9:5
Jan 24th 2024, 7:32:20 AM MST	cleared	SPHUB	interface-down	Interface vni-0/0 is up (n/a)	cleared	vni-0/0	equipmentAlarm	symptom	yes	outOfService	Jan 24th 2024, 7:3
Jan 24th 2024, 7:32:20 AM MST	cleared	SPHUB	interface-down	Interface vni-0/0 is up (n/a)	cleared	vni-0/0	equipmentAlarm	symptom	yes	outOfService	Jan 24th 2024, 7:3
Jan 24th 2024, 7:32:19 AM MST	critical	SPHUB	bgp-nbr-state-change	BGP Instance 3015: Peer 169.254.0.8 transitioned to Active state	new	3015 169.254.0.8	communicationsAlarm	symptom	no	causeOther	Jan 24th 2024, 7:3
Jan 24th 2024, 7:14:17 AM MST	critical	SPHUB	interface-down	Interface vni-0/0 is down (n/a)	new	vni-0/0	equipmentAlarm	symptom	yes	outOfService	Jan 24th 2024, 7:1
Jan 24th 2024, 7:14:15 AM MST	critical	SPHUB	interface-down	Interface vni-0/0 is down (n/a)	new	vni-0/0	equipmentAlarm	symptom	yes	outOfService	Jan 24th 2024, 7:1
Jan 24th 2024, 7:09:18 AM MST	cleared	SPHUB	bgp-nbr-state-change	BGP Instance 3015: Peer 169.254.0.8 transitioned to Established state	new	3015 169.254.0.8	communicationsAlarm	symptom	no	causeOther	Jan 24th 2024, 7:0
Jan 24th 2024, 7:02:51 AM MST	critical	SPHUB	bgp-nbr-state-change	BGP Instance 3015: Peer 169.254.0.8 transitioned to Active state	new	3015 169.254.0.8	communicationsAlarm	symptom	no	causeOther	Jan 24th 2024, 7:0
Jan 24th 2024, 6:54:07 AM MST	cleared	SPHUB	interface-down	Interface vni-0/0 is up (n/a)	cleared	vni-0/0	equipmentAlarm	symptom	yes	outOfService	Jan 24th 2024, 6:5
Jan 24th 2024, 6:54:05 AM MST	cleared	SPHUB	interface-down	Interface vni-0/0 is up (n/a)	cleared	vni-0/0	equipmentAlarm	symptom	yes	outOfService	Jan 24th 2024, 6:5

Showing 1 to 10 of 12 entries Previous 1 2 Next

The alarms and their active/cleared states are listed.

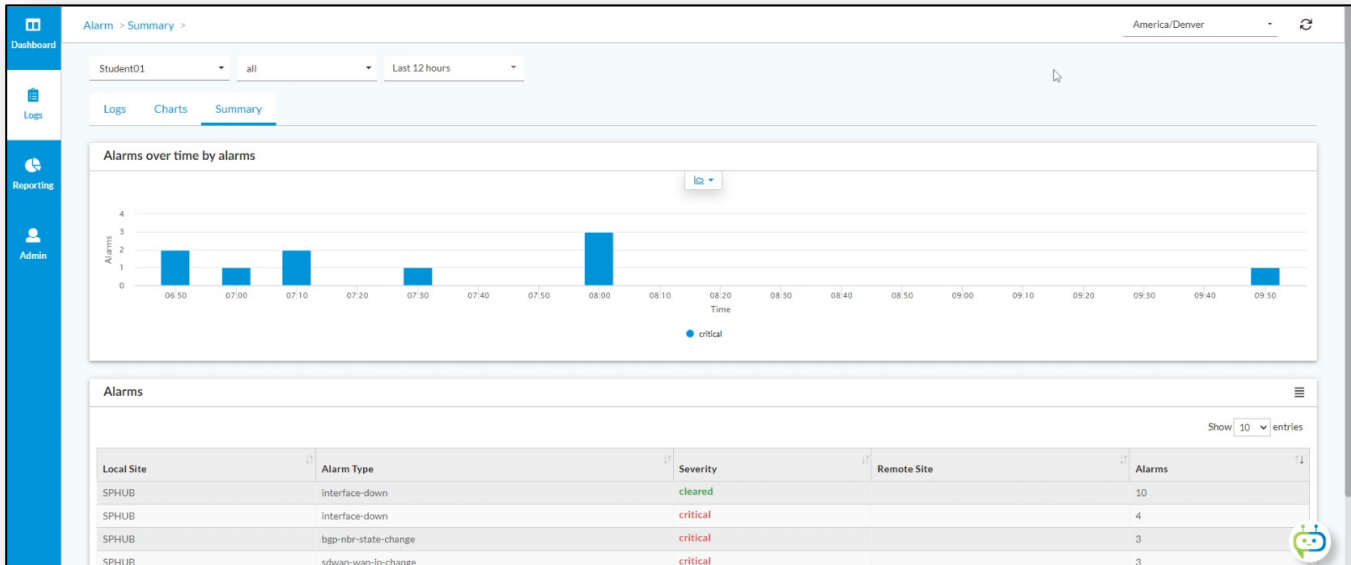
The Charts dashboard displays top alarms and severity in a chart format.

- z. Click the Charts tab to view the alarms charts.



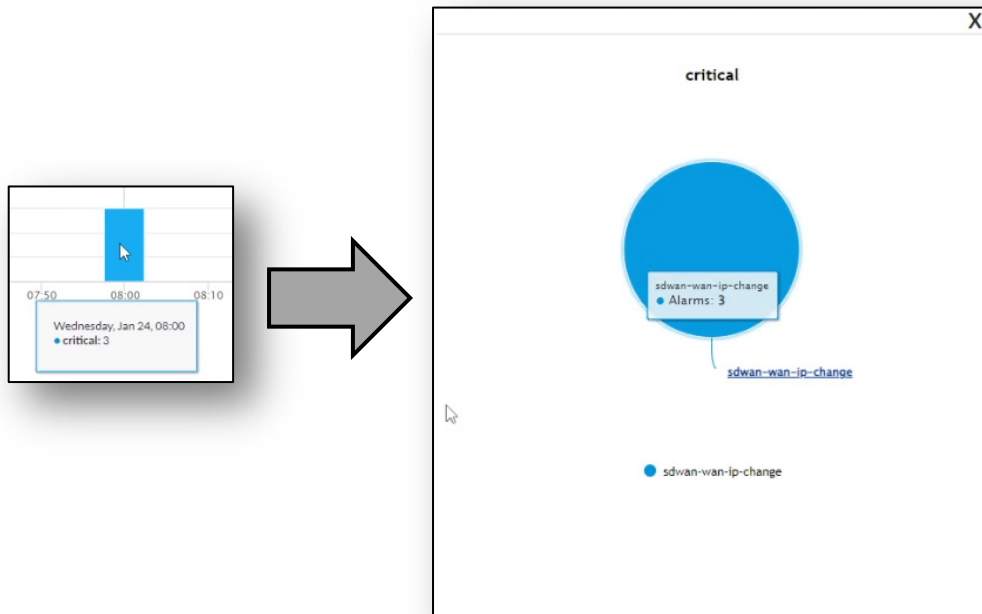
The Alarm Summary dashboard displays a summary of alarms over time.

aa. Click the *Summary* tab to open the *Alarm Summary* dashboard.



ab. Hover the mouse over alarms in the chart to see more details.

ac. Click on the item in the chart to see further details.

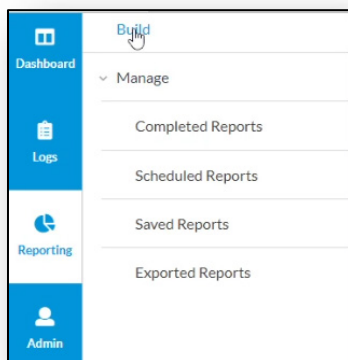


Step 3. Analytics Reporting

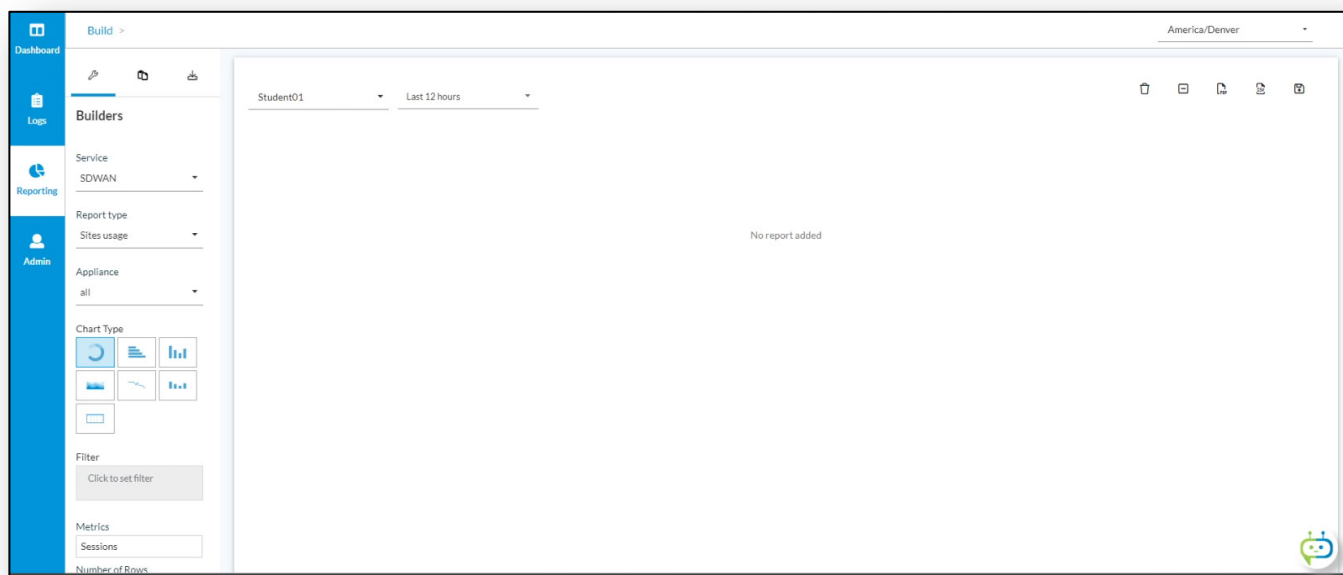
Versa Analytics has a report building system built into the platform to generate reports on the data found in Analytics. There are 2 main functions of the Reporting process: Build and Manage.

Build is used to create reports. Manage is used to view and sort reports and report storage.

- a. Navigate to the *Reporting > Build* dashboard in the left-side menu.



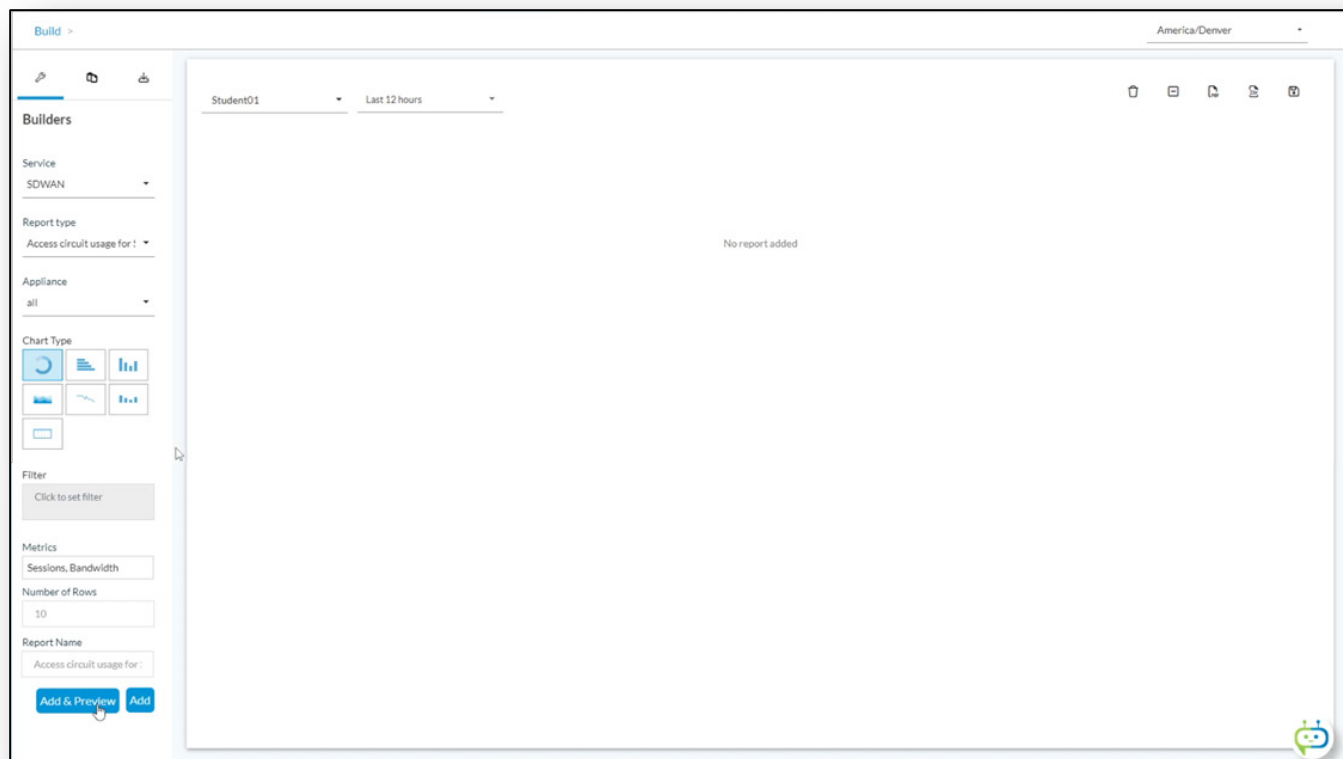
The left side of the Build dashboard allows you to select the type of information you want to add to a report, as well as the way you want it displayed.



Let's go through the process of building a report template. Each data entry is considered a report that can be added to the final report document. The report template can have one or more reports included, which will all be displayed.

b. Start by adding a report that includes the following information:

- Service: SDWAN
- Report type: Access circuit usage for SDWAN
- Chart type: Circle graph
- Metrics: Sessions and Bandwidth
- Report name: Access circuit usage for SDWAN



Note: Although the pie chart button is highlighted, you will have to click on it directly to activate that chart type.

c. Click the *Add & Preview* button to add the report and add create preview of the data in the report dashboard.

d. Let's add another report with the following information:

- Service: Security
- Report type: Top applications
- Chart type: Column chart
- Metrics: Sessions and Bandwidth
- Report name: Top applications

The screenshot shows the 'Build' interface for a report titled 'Access circuit usage for SDWAN'. The report is configured with the following settings:

- Service: Security
- Report type: Top applications
- Appliance: all
- Chart Type: Pie chart (highlighted)
- Filter: Click to set filter
- Metrics: Sessions, Bandwidth
- Number of Rows: 10
- Report Name: Top applications

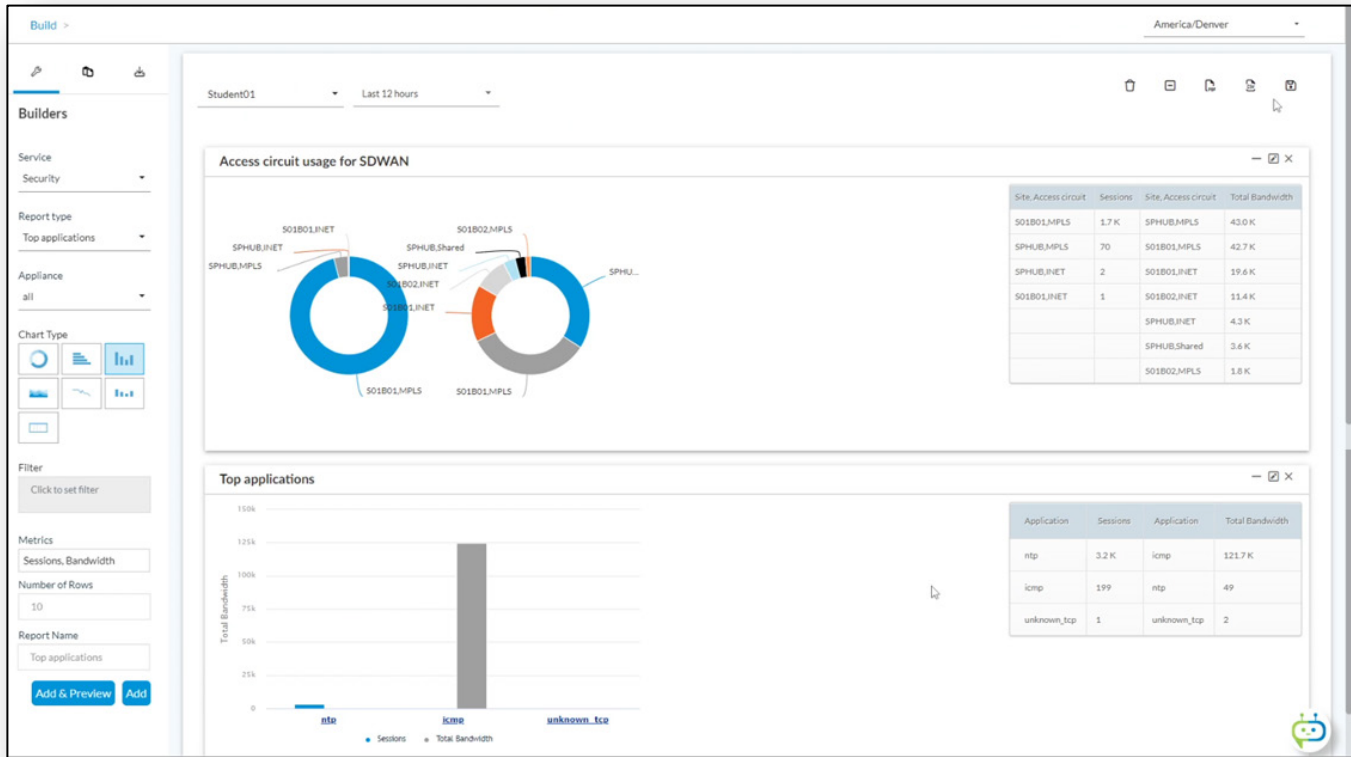
The main area displays two donut charts and a data table. The data table is as follows:

Site, Access circuit	Sessions	Site, Access circuit	Total Bandwidth
S01B01,MPLS	1.7 K	SPHUB,MPLS	43.0 K
SPHUB,MPLS	70	S01B01,MPLS	42.7 K
SPHUB,INET	2	S01B01,INET	19.6 K
S01B01,INET	1	S01B02,INET	11.4 K
		SPHUB,INET	4.3 K
		SPHUB,Shared	3.6 K
		S01B02,MPLS	1.8 K

Note: Although the pie chart button is highlighted, you will have to click on it directly to activate that chart type.

e. Click the *Add & Preview* button to add the report and add a preview of the data in the report dashboard.

Your results should look similar to the example below.



The two reports are combined in a single main report that can be saved and scheduled.

- f. Click the *Save* button in the top right corner to save the report format. This will open the save dialog.



Save the report with the following settings:

- Name: Generic Usage Report
- Access: Private
- PDF Template: Default
- Schedule: every 1 hours

- g. Click *OK* when finished to save and schedule the report.

Note that scheduled reports can automatically be emailed to one or more user by including their email address in the Email notification recipients dialog. For reports to be emailed, the email functions must be enabled in the Admin settings.

The 'Save and Schedule' dialog box contains the following settings:

- Name:** Generic Usage Report
- Access:** Private
- PDF Template:** Default
- Schedule:** (checked)
- Now(1time)
- Hourly every 1 hours
- Daily at 10:00 AM
- Weekly on Sunday at 10:00 AM
- Monthly on the 1st at 10:00 AM
- Expiration:** 01/24/2024
- Email notification recipients:** (empty field)

Buttons: Cancel, Ok

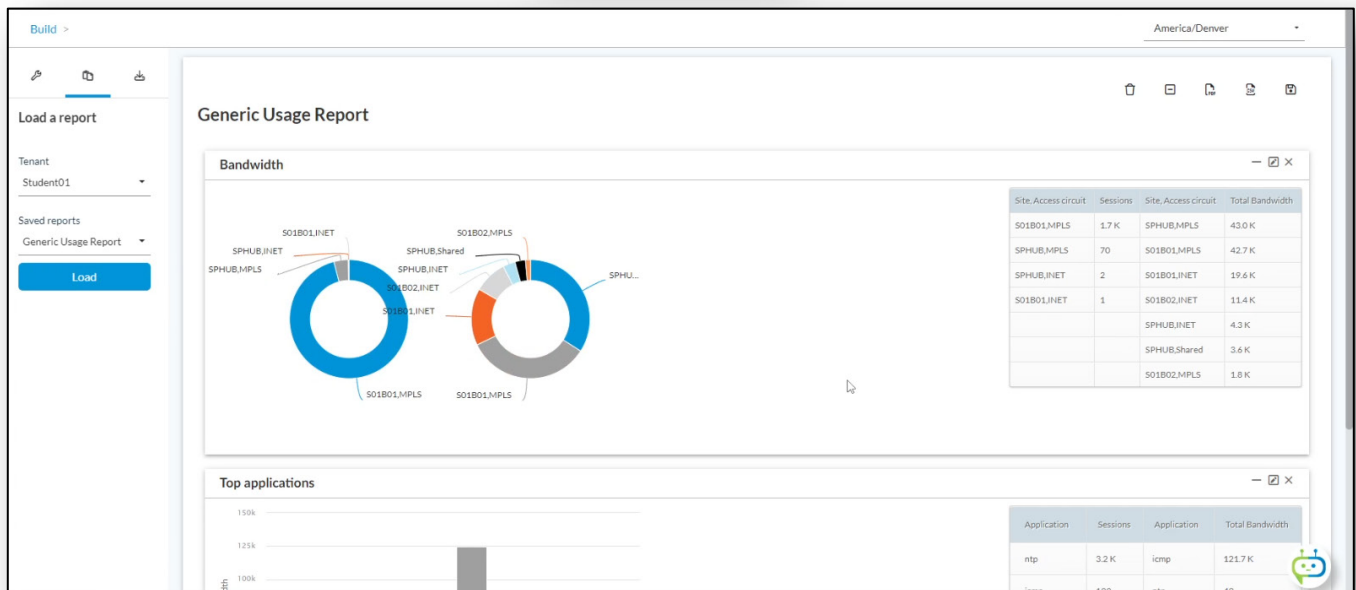
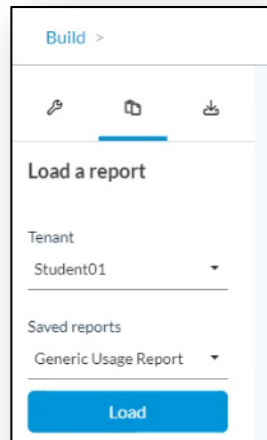
Single reports can be reloaded in the load of report dialogue.

- h. Click on the Load a report button in the build menu.

When you select a tenant, all of the saved reports for that tenant become available in the dropdown.

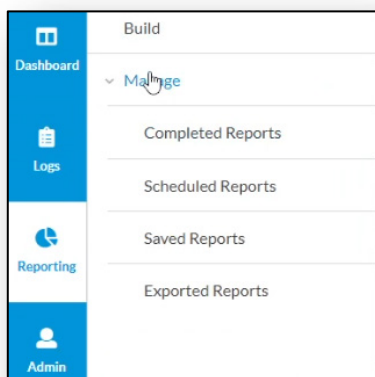
Note that the saved report is the layout of the report, not the information within the report. In other words, when you load a report, the information in the charts and graphs will be updated to reflect current information.

- i. Click the Load button to pull the new information into the dashboard. The formatting and layout options will be the same as when you built the report.



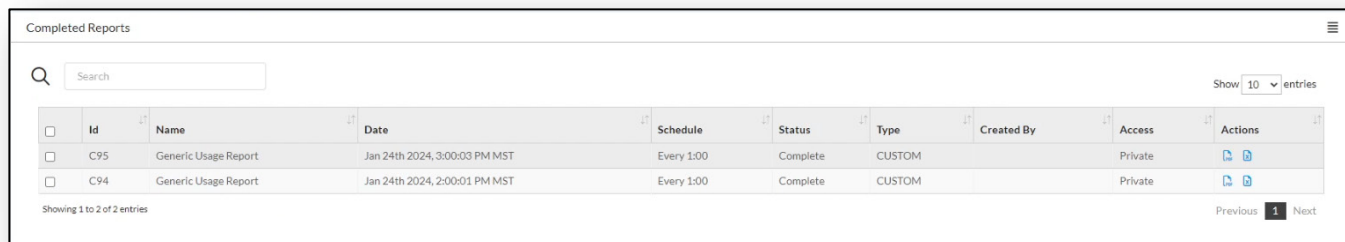
- j. For a soft copy of the information, click the PDF or CSV buttons in the top right. A soft copy will download to your Downloads folder.

k. To view copies of previous reports, open the *Reporting > Manage* dashboard.



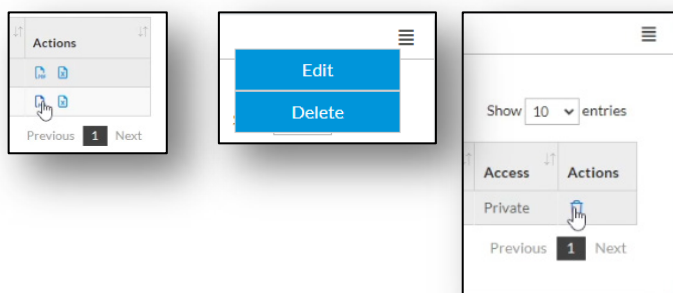
Completed reports are reports that have been previously run, or that have run according to a report schedule.

l. Click on Completed Reports to see if any reports are present in the system. There should be at least one report (the one that you ran).

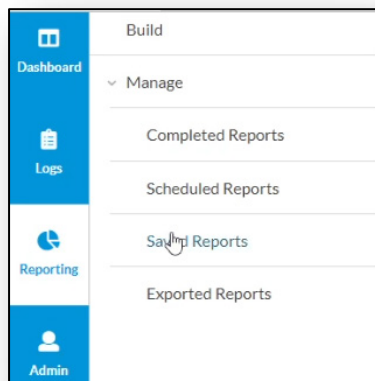


You can delete the reports by clicking on the menu button on the top right, or by clicking the Delete button next to the report.

m. Click the Delete button next to the report that you created to remove it from the system.



The Saved Reports dashboard contains the saved report layouts that you can load in the Load Report screen. You can manage the different layouts from the Saved Reports dashboard.

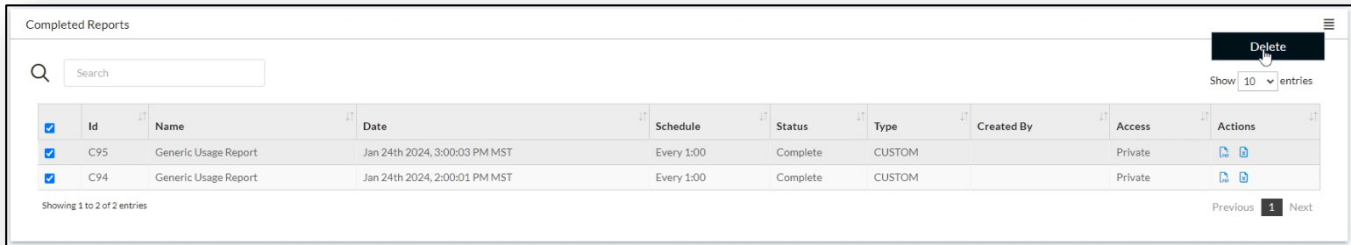


You can schedule or delete the reports by clicking the menu button at the top right of the dashboard.

- n. Check the box next to your saved report, then click the *Menu* button and select *Delete* to delete the report.



- o. Return to the *Completed Reports* page and ensure that any completed reports in the system are removed.



Completed Reports

Search

Show 10 entries

<input checked="" type="checkbox"/>	Id	Name	Date	Schedule	Status	Type	Created By	Access	Actions
<input checked="" type="checkbox"/>	C95	Generic Usage Report	Jan 24th 2024, 3:00:03 PM MST	Every 1:00	Complete	CUSTOM		Private	🔗 🔗
<input checked="" type="checkbox"/>	C94	Generic Usage Report	Jan 24th 2024, 2:00:01 PM MST	Every 1:00	Complete	CUSTOM		Private	🔗 🔗

Showing 1 to 2 of 2 entries

Previous 1 Next



STOP! When you have finished exploring the Monitor and Analytics dashboards, notify your instructor that you have completed this lab.

DIAGNOSTIC TOOLS

The Versa Networks lab environment consists of a fixed, pre-configured topology that will allow you to explore, configure, and manage Versa Networks CPEs by using Versa Director, the central management and orchestration platform for a Versa Secure SD-WAN solution. After completing this lab, you will be able to:

- Use the PING tool from Versa Director to perform connectivity tests;
- Use the Trace tool from Versa Director to perform connectivity tests;
- Use the Versa Speedtest function to verify circuit speeds.

In this lab you will be assigned two CPE devices (Branch devices) for configuration and monitoring. The branch devices are named after the student ID that you have been assigned.

The lab environment is accessed through Amazon Workspaces. Your student ID and workspace will be assigned by the instructor.

The remote desktop connection opens a remote workstation, where you will use various tools to navigate and configure the lab environment. The main tool you will use in this lab is Versa Director. Versa Director can be accessed by opening the Google Chrome browser on the Remote Desktop. The IP address of the Versa Director (from the remote workstation) is 10.27.1.10. Once you begin the lab, you may want to create a bookmark to Versa Director in the web browser on the remote desktop.

During certain lab parts, the lab guide will present sample output from the GUI or the CLI. The sample outputs are SAMPLES and represent the information as it appeared during the lab guide creation. Your output may vary in some ways (some devices may or may not be present, some routes may or may not be the same, etc.) Do not be alarmed if your results vary slightly from the results shown in the lab guide. The important thing is that the lab functions in the desired manner.

This lab guide will step you through some common tasks that are performed on Versa Director. After an introductory set of exercises, you will be asked to perform some basic tasks that will allow you to become more familiar with the environment.

The goal of this and all lab exercises is to help you gain additional skills and knowledge. Because of this, the lab guide contains additional instruction to supplement the student guides.

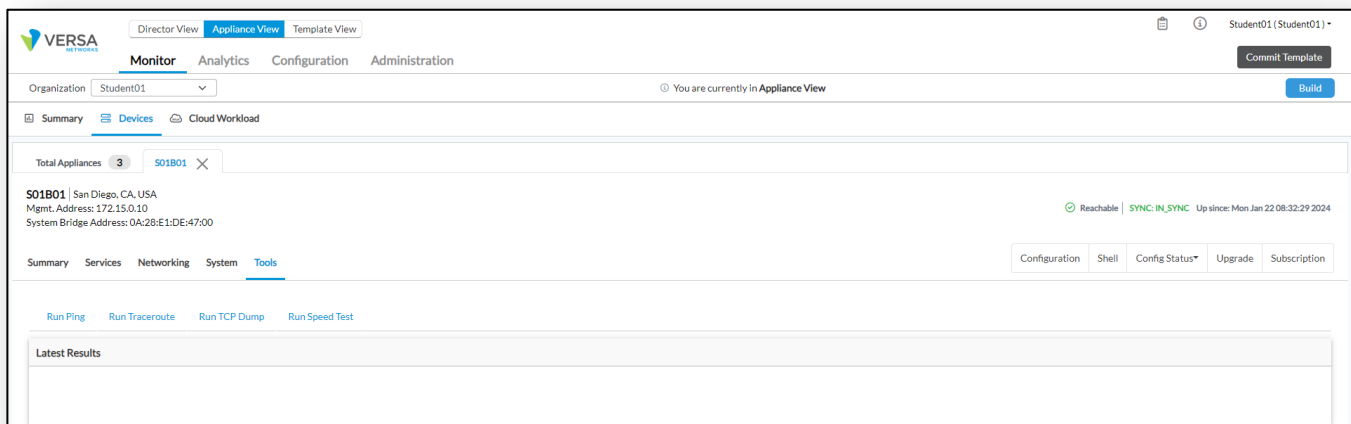
Now that we've discussed what is expected, let's get started!

Step 1. The Ping Utility

The PING utility is a tool used to verify IP connectivity between devices. It works by sending an ICMP echo request packet to a remote system, which the remote system responds to. Information such as reachability and delay metrics can be gathered. It should be noted that the PING utility is used for basic connectivity verification and is not used for more complex troubleshooting scenarios, although it is frequently one of the first connectivity tests used to verify if a remote host is reachable.

In this exercise you will use the built-in PING utility in the Versa Operating System.

- a. In Versa Director, navigate to *Appliance View*.
- b. In *Appliance View*, click on your *SxxB01* device
- c. In the *Appliance View* of your *SxxB01* device, navigate to *Monitor > Tools*.
- d. It is located in the *Appliance View > Monitor > Tools* dashboard.



You will use the PING tool to test connectivity to the LAN segment attached to the SPHUB-NEW device, and to test connectivity to the WAN interface on the SPHUB-NEW device.

- e. In the *Tools* dashboard, click on the *Run Ping* tab.
- f. In the *Run Ping* tab, enter:
 - Host Name/Address: 10.27.13.10 (the IP address connected to the SPHUB-NEW Shared network);
 - Routing Instance: Student-LAN-VR (your local LAN VRF); and
 - Source Address: This will populate automatically as the local LAN address.
- g. Click the *Start* button. The Latest Results box will not populate until the PING test is finished (about 10 seconds).

Run Ping

Run Traceroute

Run TCP Dump

Run Speed Test

Host Name/Address

Routing Instance

Student01-LAN-VR
▼

Source Address [Input a different address](#)

10.27.101.10
▼

Packet-size

Count

Start

Latest Results

```

PING 10.27.13.100 (10.27.13.100) from 10.27.101.10 : 56(84) bytes of data.
64 bytes from 10.27.13.100: icmp_seq=1 ttl=64 time=1.77 ms
64 bytes from 10.27.13.100: icmp_seq=2 ttl=64 time=1.57 ms
64 bytes from 10.27.13.100: icmp_seq=3 ttl=64 time=1.55 ms
64 bytes from 10.27.13.100: icmp_seq=4 ttl=64 time=25.2 ms
64 bytes from 10.27.13.100: icmp_seq=5 ttl=64 time=1.50 ms
64 bytes from 10.27.13.100: icmp_seq=6 ttl=64 time=1.23 ms
64 bytes from 10.27.13.100: icmp_seq=7 ttl=64 time=1.72 ms
64 bytes from 10.27.13.100: icmp_seq=8 ttl=64 time=1.22 ms
64 bytes from 10.27.13.100: icmp_seq=9 ttl=64 time=1.01 ms
64 bytes from 10.27.13.100: icmp_seq=10 ttl=64 time=1.54 ms
--- 10.27.13.100 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9009ms
rtt min/avg/max/mdev = 1.012/3.842/25.266/7.145 ms
                    
```

Next you will test reachability to the WAN port on the hub device.

h. Enter the following information in the *Run Ping* dialog:

- Host Name/Address: 10.27.11.100
- Routing Instance: INET-Transport-VR
- Source Address: This will auto-populate

i. Click the *Start* button to begin the test.

Run Ping
Run Traceroute
Run TCP Dump
Run Speed Test

Host Name/Address

Source Address
 [Input a different address](#)

Count

Routing Instance

Packet-size

Start

Latest Results

```

PING 10.27.11.100 (10.27.11.100) from 10.27.11.101 : 56(84) bytes of data.
64 bytes from 10.27.11.100: icmp_seq=1 ttl=64 time=2.09 ms
64 bytes from 10.27.11.100: icmp_seq=2 ttl=64 time=1.09 ms
64 bytes from 10.27.11.100: icmp_seq=3 ttl=64 time=0.711 ms
64 bytes from 10.27.11.100: icmp_seq=4 ttl=64 time=0.708 ms
64 bytes from 10.27.11.100: icmp_seq=5 ttl=64 time=0.720 ms
64 bytes from 10.27.11.100: icmp_seq=6 ttl=64 time=0.813 ms
64 bytes from 10.27.11.100: icmp_seq=7 ttl=64 time=0.702 ms
64 bytes from 10.27.11.100: icmp_seq=8 ttl=64 time=0.817 ms
64 bytes from 10.27.11.100: icmp_seq=9 ttl=64 time=0.973 ms
64 bytes from 10.27.11.100: icmp_seq=10 ttl=64 time=0.727 ms
--- 10.27.11.100 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9133ms
rtt min/avg/max/mdev = 0.702/0.935/2.091/0.406 ms
                    
```

Next you will use the Traceroute tool to check reachability to a public destination.

- j. Click on the *Run Traceroute* tab.
- k. In the *Run Traceroute* dialog, enter the following information:
 - Target Host Name/Address: 8.8.8.8
 - Routing Instance: INET-Transport-VR
 - Source IP: This will auto-populate
- l. Click the *Start* button to begin the test.

Run Ping
Run Traceroute
Run TCP Dump
Run Speed Test

Target Host Name/Address

Routing Instance

Source IP

Protocol

Start

Latest Results

```

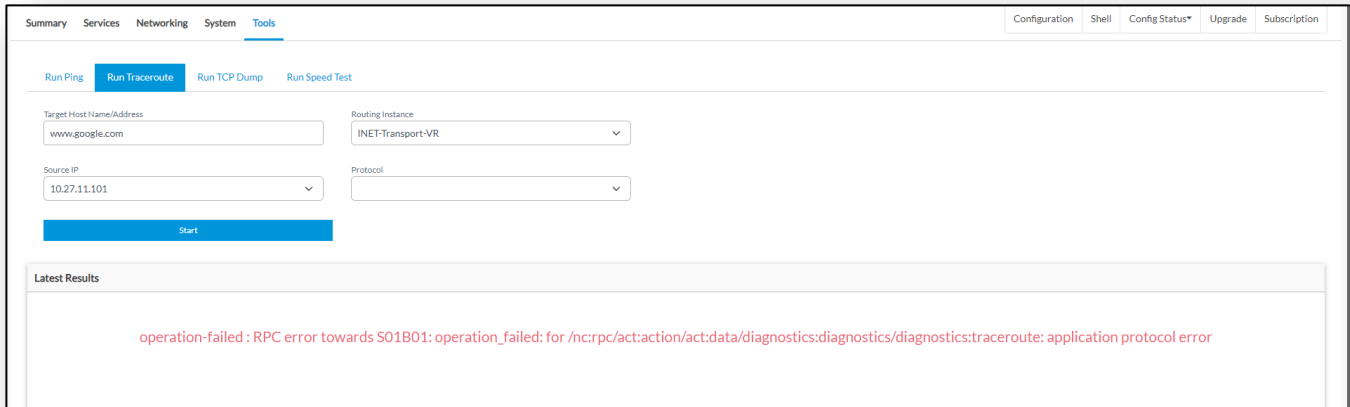
tracert to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1 10.27.9.137 1.787 ms 1.748 ms 1.710 ms
 2 216.182.231.86 20.266 ms 3.236.63.119 6.896 ms 3.236.60.1 32.634 ms
 3 240.4.112.69 2.697 ms 100.65.90.192 11.562 ms 240.0.224.97 2.678 ms
 4 242.8.90.21 4.237 ms 242.2.113.71 4.237 ms 242.7.27.5 3.694 ms
 5 100.100.2.38 3.652 ms * 241.0.4.75 2.614 ms
 6 241.0.4.90 2.589 ms * 99.83.115.173 3.039 ms
 7 72.14.203.158 3.550 ms 99.83.65.1 2.862 ms 100.66.4.215 13.583 ms
 8 108.170.240.97 3.321 ms 100.65.111.132 6.419 ms *
 9 8.8.8.8 2.743 ms 2.770 ms 2.750 ms
                    
```

Next you will use a domain name to run the traceroute function.

m. In the *Run Traceroute* dialog, enter the following information:

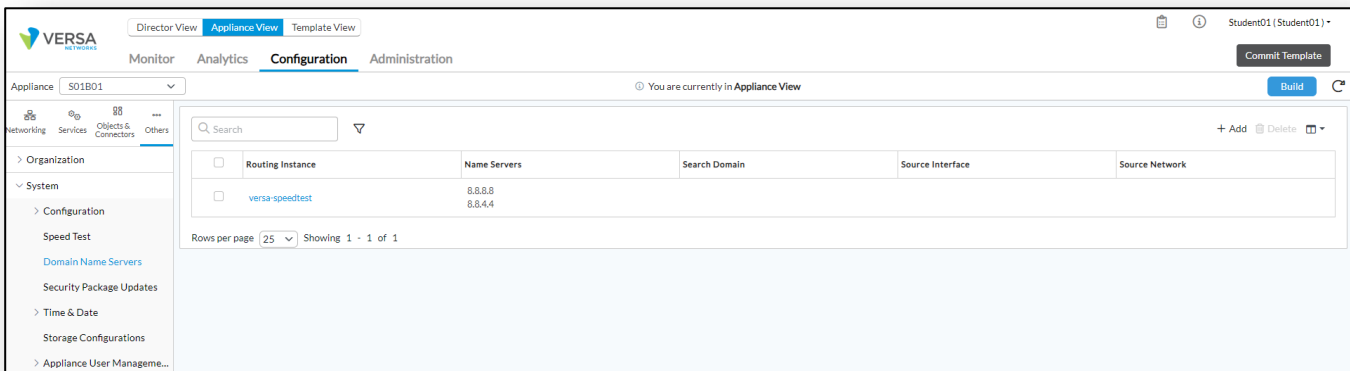
- Target Host Name/Address: `www.google.com`
- Routing Instance: `INET-Transport-VR`
- Source IP: This will auto-populate

Click the *Start* button to begin the test. This test should fail with an error.



This failure is because the virtual router (INET-Transport-VR) does not have a DNS server configured and therefore cannot look up the FQDN of `www.google.com`. We will now resolve this issue and run the test again.

n. Navigate to *Configuration > Others > System > Domain Name Servers*.



The current DNS server entry is only for the `versa-speedtest` routing instance. You need to add a DNS server to the `INET` virtual router if you are going to request DNS lookups in that router.

- o. Click on the *+Add* button to add a new DNS server. Use the information below.

Add Name Servers ✕

Routing Instance *

Source Interface Source Network

	Name Servers *		Search Domain
<input type="checkbox"/>	<input type="text" value="8.8.8.8"/>	<input type="checkbox"/>	Search Domain Not Configured

- p. Click the *OK* button to add the DNS server to the INET-Transport-VR.
- q. After you have added a DNS server to the INET-Transport-VR, return to the *Monitor > Tools > Run Traceroute* dialog.
- r. Run the Traceroute function again with the hostname *www.google.com*. The test should succeed now.

Configuration Shell Config Status* Upgrade Subscription

Summary Services Networking System **Tools**

Run Ping **Run Traceroute** Run TCP Dump Run Speed Test

Target Host Name/Address Routing Instance

Source IP Protocol

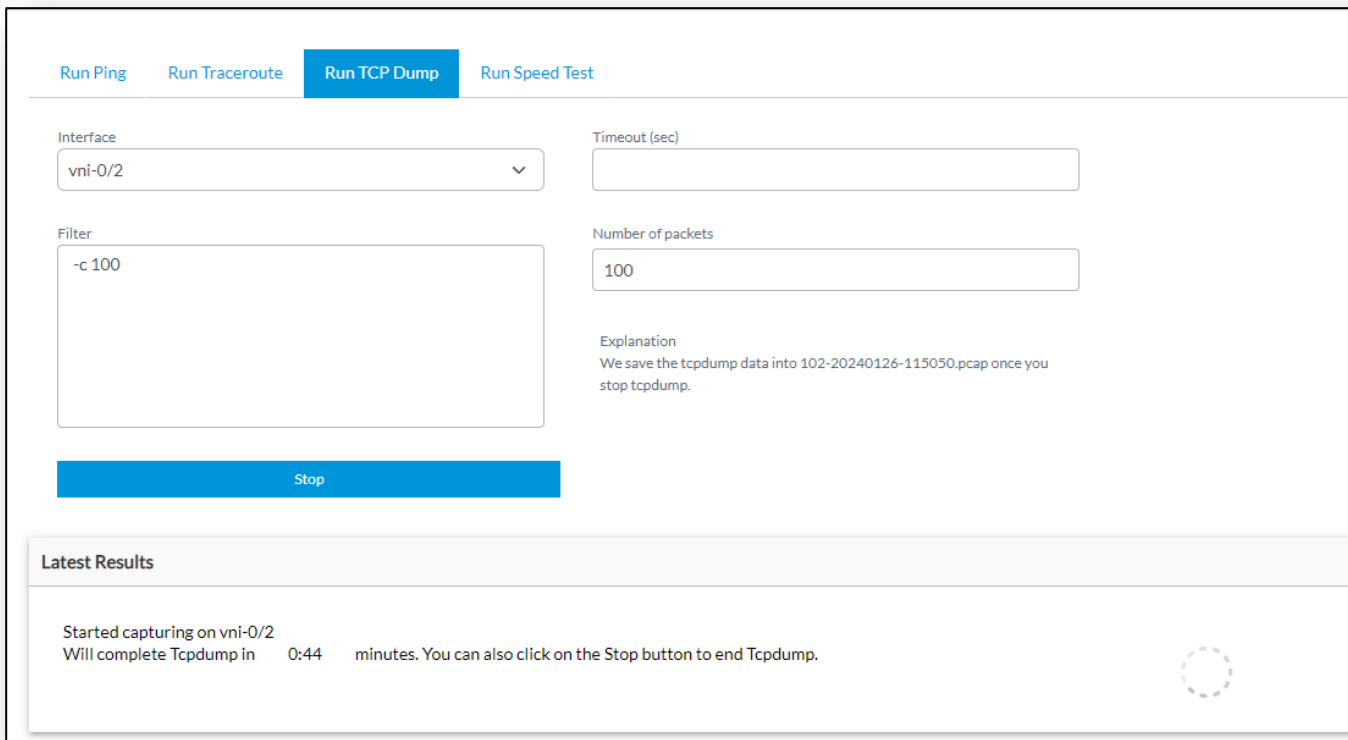
Latest Results

```

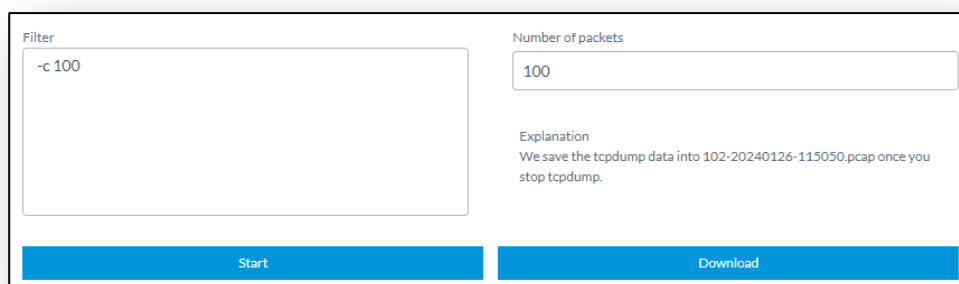
traceroute to www.google.com [172.253.122.147], 30 hops max, 60 byte packets
 1 10.27.10.212 0.830 ms 1.350 ms 1.349 ms
 2 244.5.5.229 4.512 ms 3.236.60.53 9.863 ms 3.236.62.107 10.890 ms
 3 240.4.112.64 2.348 ms * 240.0.56.97 2.328 ms
 4 240.0.236.3 3.866 ms 240.0.236.1 3.863 ms *
 5 100.100.36.98 3.298 ms 100.66.47.76 15.401 ms 100.100.4.80 3.896 ms
 6 69.29.136.21 3.847 ms 69.29.136.1 3.322 ms 2.791 ms
                    
```

Next you will run the TCP Dump application to perform a packet capture. The remote testing host does not have an application that can read the packet capture files, so you will not be able to view the data. An application such as Wireshark is able to read the files in a production environment.

- s. Navigate to the *Run TCP Dump* tab.
- t. In the *Run TCP Dump* dialog, enter interface vni-0/2. The number of packets should be pre-populated with a count of 100. This translates to the Filter in the Filter dialog (-c 100). You can also specify a timeout in seconds. Use the pre-configured capture filter of 100 packets.
- u. Click the *Start* button to begin the packet capture on the LAN interface.

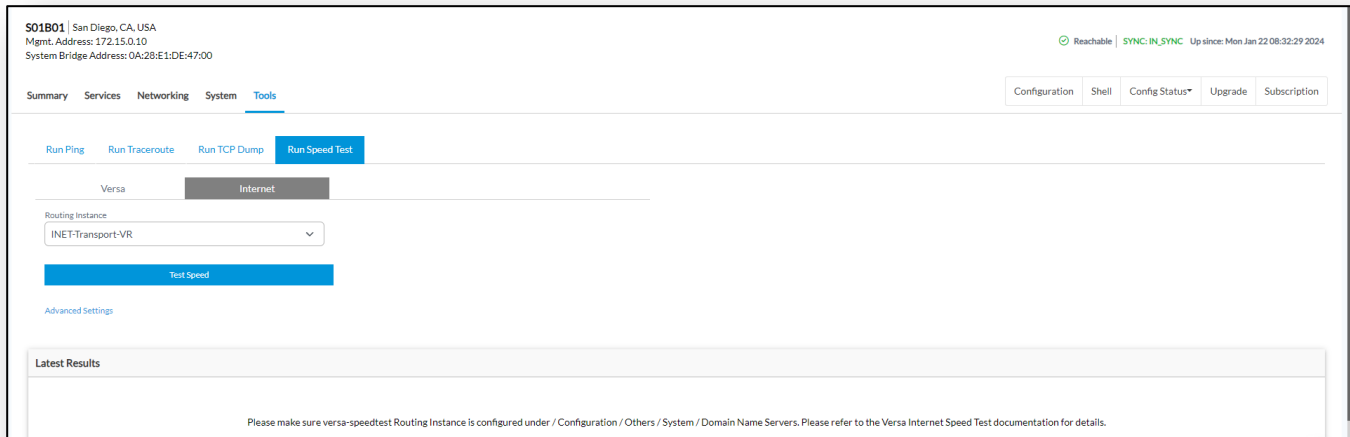


A default 60 second timer will begin. Once the timer is complete, the dashboard will allow you to download the captured packets.



Next you will run a speedtest function to test circuit speed.

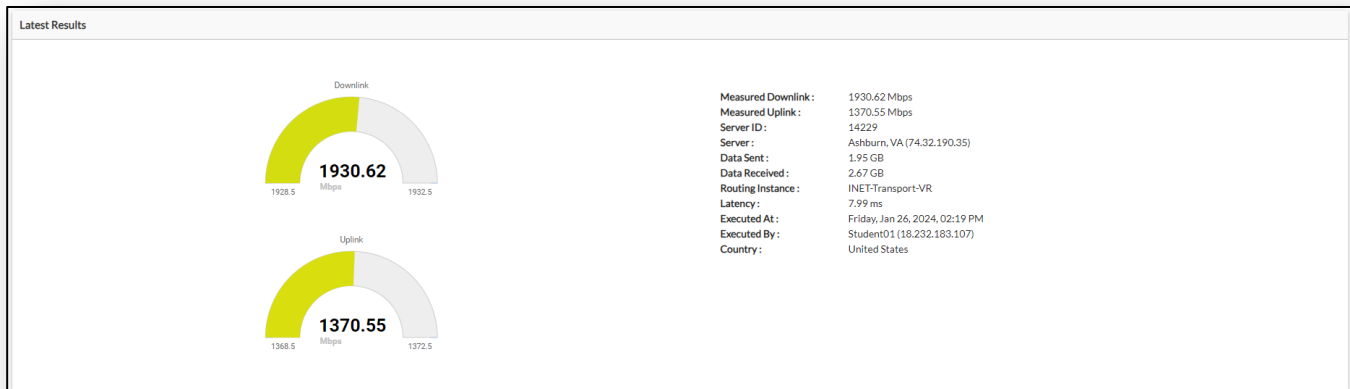
- v. Click on the *Run Speed Test* tab to open the speedtest dialog.



Speedtest can be run between the VOS device and a Versa Appliance, or to a public speedtest server (if public Internet access is available). To use a VOS device as a speedtest server, you must enable the speedtest server function in the appliance *Configuration > Others > System > Speedtest* dashboard.

For this lab you will do a speedtest to a public speedtest server.

- w. In the *Run Speed Test* dialog, click the *Internet* tab.
- x. In the *Routing Instance* field, enter *INET-Transport-VR*.
- y. Click the *Test Speed* button to begin the test. The test will take up to 30 seconds to complete.



- z. Return to the *Summary* screen. In the summary screen you can measure the speed of circuits using the Measure button.
- aa. In the *Summary* screen, click the *Measure* button on the INET link.

Interface	Network Name	Service Provider	Status		Live Data	Bandwidth (Mbps)		Measure
			Operational	Admin		Configured	Measured	
> vni-0/0.0	INET	-	↑	↑	<input type="checkbox"/>	↑ 990.00	↓ 990.00	Measure
> vni-0/1.0	MPLS	-	↑	↑	<input type="checkbox"/>	↑ 0.00	↓ 0.00	Measure
> vni-0/2.0	Student01_Lan	-	↑	↑	<input type="checkbox"/>			

- ab. Enter the *SPHUB-NEW* as the Remote Destination, then click OK.

Bandwidth Measurement

Local WAN Interface
vni-0/0.0

Remote Destination *
SPHUB

Remote Circuit Name
---Please Select---

Remote Circuit Media
---Please Select---

Remote Circuit Type
---Please Select---

After the test is complete, the results will display in the Bandwidth column.

Interface	Network Name	Service Provider	Status		Live Data	Bandwidth (Mbps)		Measure
			Operational	Admin		Configured	Measured	
> vni-0/0.0	INET	-	↑	↑	<input type="checkbox"/>	↑ 990.00	↓ 990.00	Measure
> vni-0/1.0	MPLS	-	↑	↑	<input type="checkbox"/>	↑ 0.00	↓ 0.00	Measure
> vni-0/2.0	Student01_Lan	-	↑	↑	<input type="checkbox"/>			



STOP! Notify your instructor that you have completed this lab.