Configure for NIAP Common Criteria (Version 1.0, March 29 2024)

Install Initial Headend Components

Before you install Versa headend components, design an IP addressing schema for the following networks:

- Management network—For example: 192.168.0.0/24
- Control plane network—For example: 192.168.1.0/24
- WAN network as provisioned by the service provider
- Overlay network—For example: 10.0.0.0/24

To install the initial headend components:

1. Download the following images from download.versa-networks.com and manually verify the hash of each image. SHA-256 checksums are published along with the installation images. To manually verify the installation file, use a tool such as shasum to calculate the digest and compare to the published value. If the values do not match, you must not use it as the image has been tampered with. Contact Versa Support to obtain the correct installation image:
    - versa-director-4a087e1-22.1.3-B.ova
    - versa-analytics-fips-95f9b00-22.1.3-B.ova
    - versa-flexvnf-67ff6c7-21.2.3.ova
    - versa-flexvnf-20221202-122502-1aace6d-21.2.3.bin
    - versa-flexvnf-67ff6c7-21.2.3.qcow2.tbz2
2. Deploy the Versa Director, Versa Analytics, and Versa Operating System^{TM} (VOS^{TM}) images on an ESXi host. Create at least one Director node, two Analytics nodes, and one VOS virtual machine (VM).
3. Create two ESXi virtual port groups, one for the control plane network, and the other for the WAN.
4. By default, a VM network port group should be present. However, you can use any existing network for the management network.

For more information, see Headend Installation and Perform Initial Software Configuration.

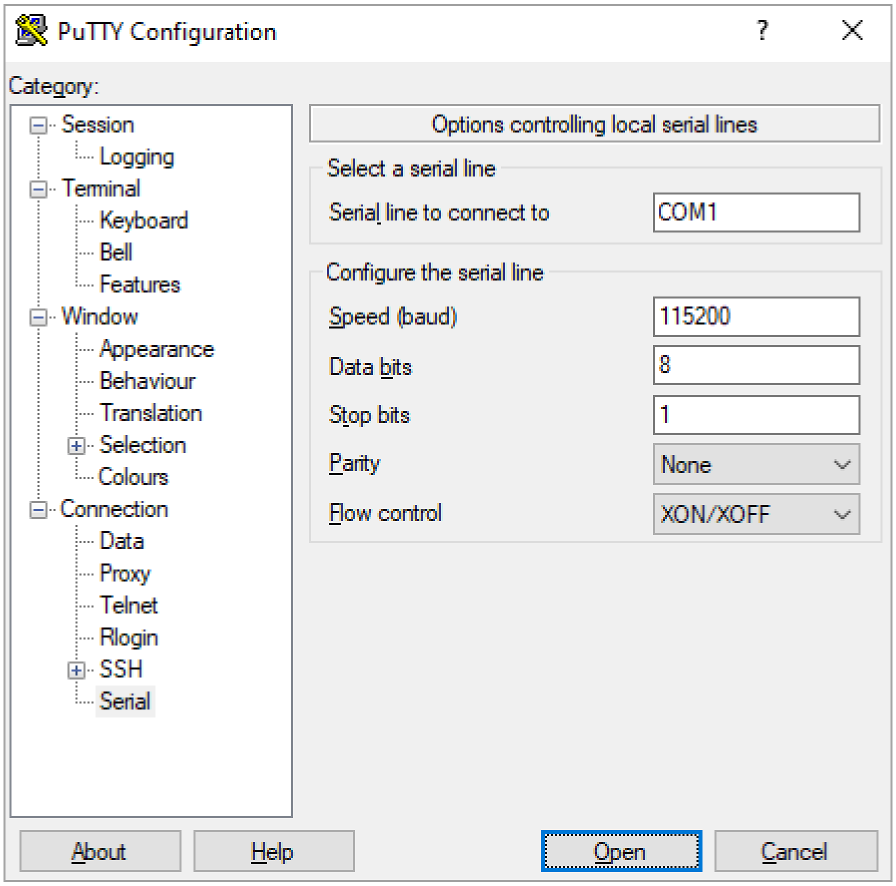
Log In from a Local Console

Before you log in to a VOS device from a local console:

- Install a terminal emulator software (PuTTY or SecureCRT) on your computer.
- Ensure that you have the following:
  - Rollover console cable
  - DB9 female to RJ-45 adapter
  - USB to DB9 serial adapter cable
  - Adapter cable driver

To configure a local serial connection:

1. Connect the rollover console cable with the USB-to-serial adapter cable to your computer.
2. Plug in the RJ45 connector to the console port of your computer.
3. Plug in the USB connector to the USB port of your computer.
4. Connect an Ethernet cable from the management port on the VOS device to the Ethernet port of your computer.
5. Open Device Manager on your computer and check which COM that displays for this USB serial connection.
6. Open the terminal emulator software (here, PuTTY), and select Connection > Serial in the left menu bar.



Options controlling local serial lines

Select a serial line

Serial line to connect to: COM1

Configure the serial line

Speed (baud): 115200

Data bits: 8

Stop bits: 1

Parity: None

Flow control: XON/XOFF

7. In the Select a Serial Line field, enter the COM Port number.
8. In the Speed field, enter 115200 baud.
9. Click Open to open a console session to the VOS device. Use the default username and password, either admin/versa123 or versa/versa123.

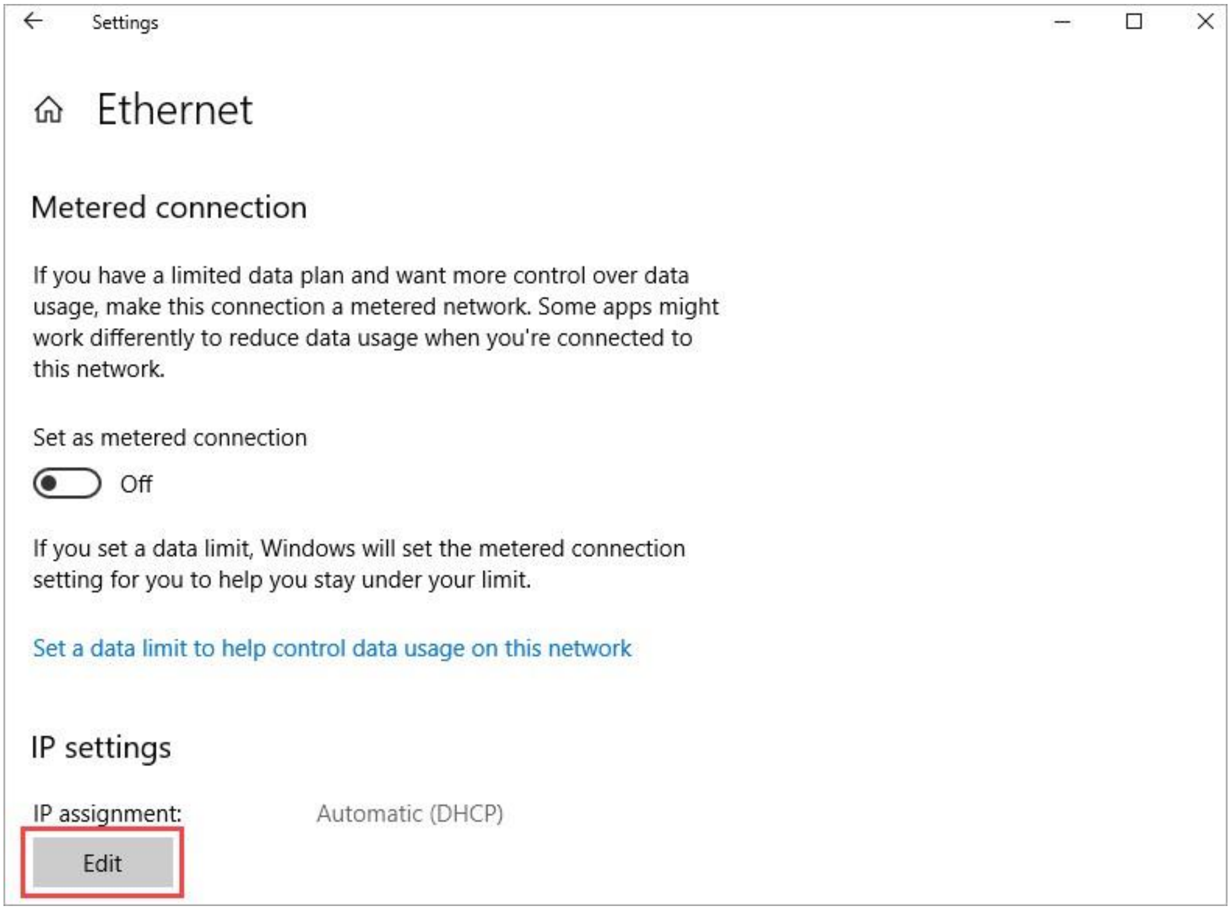
Upgrade VOS Device Manually

Before you manually upgrade your VOS device, if your VOS device is not shipped with CC certified version, do the following:

1. After configuring the local serial connection as described in Log In via Local Console, change your computer Ethernet connection IP settings from DHCP to Static. For example, in Windows 10:

   a. Open Settings on Windows 10 and click Network & Internet.

   b. Click Ethernet and click on the current network connection.



Ethernet

Metered connection

If you have a limited data plan and want more control over data usage, make this connection a metered network. Some apps might work differently to reduce data usage when you're connected to this network.

Set as metered connection

○ Off

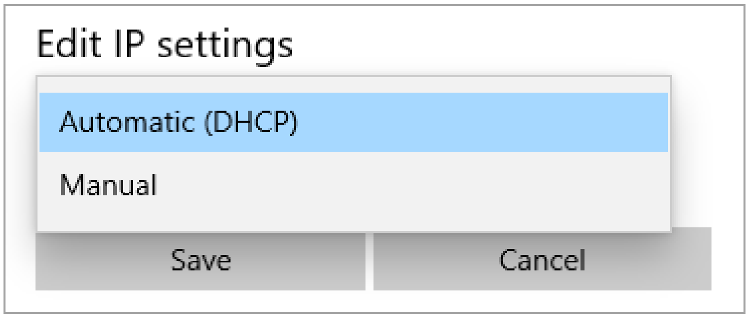
If you set a data limit, Windows will set the metered connection setting for you to help you stay under your limit.

Set a data limit to help control data usage on this network

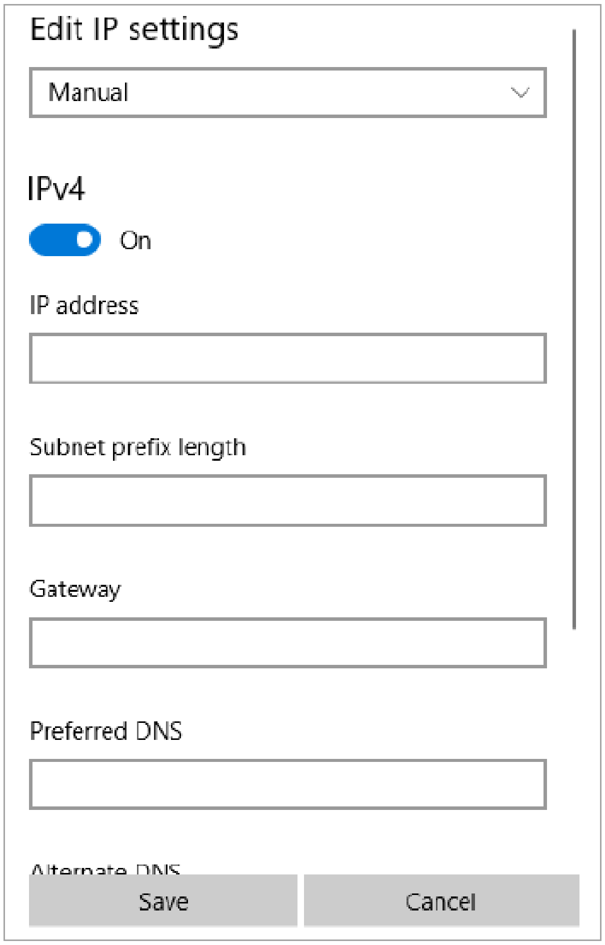
IP settings

IP assignment: Automatic (DHCP)

   c. In the Ethernet pop-up screen, click Edit under IP assignment.



d. In the Edit IP Settings screen, select Manual from the drop-down list and click Save.



e. Enable IPv4 and/or IPv6 and enter the static IP address and prefix as 10.10.10.11/8. The default management port IP address for Versa is 10.10.10.10/8 and this allows you to connect your computer to the Versa network and copy software packages from the Versa network to your computer using WinSCP.

To manually upgrade your VOS device:

1. Ensure that you can ping 10.10.10.10.

2. Open WinSCP and create a new site with host name 10.10.10.10, admin as user name and versa123 as password to log in.
3. Navigate to the folder in your computer where you have saved VOS Release 20.2.3 code.
4. Navigate to the package directory on the Versa device: /home/versa/packages/ and transfer the code from your computer to Versa's Packages directory.
5. Open a Versa console session, run the following CLI command to upgrade:

   ```
   Request system package upgrade versa-flexvnf-20221202-122502-1aace6d-21.2.3.bin
   ```

6. Type Yes after the question prompt to restart the device. The device reboots after upgrade. It takes approximately 7 to 10 minutes to complete the upgrade and for services to be active after the restart.
7. Issu the **vsh details** CLI command to verify the software version.

Configure Basic Network

1. Log on to each appliance via the console using serial port or VMware console, with the default credentials (versa/versa123). Assign an IP address in the Management network to each on the eth0 interface, for example:

   ```
   sudo ifconfig eth0 10.0.0.50/16 up
   ```

2. Make sure to remove any DHCP addresses after eth0 has been assigned a static IP. Ping the management interface to ensure that each device is now reachable.

Enable FIPS Mode

For Director and Analytics, you must use a FIPS-compatible image. The certified Versa Director and Versa Analytics images are in FIPS mode by default.

To check if the FIPS mode is enabled in Director or Analytics, issue the **cat /proc/sys/crypto/fips_enabled** CLI command. If FIPS is enabled, value 1 displays.

FIPS mode is disabled on VOS appliances by default.

1. To enable FIPS mode on the VOS device, issue the following command:

   ```
   % request system fips-mode enable
   Restart all Versa services. Are you sure? [no,yes] yes
   ```

2. To enable FIPS mode, you must restart all Versa services. If you want to delay the restarting of Versa services to complete the FIPS mode change, answer **no** to the prompt and manually restart the Versa services at a later time.
3. To enable FIPS mode and automatically restart all services without being prompted, issue the following command:

   ```
   % request system fips-mode enable no-confirm
   ```

4. To disable FIPS mode, issue the following command:

   ```
   % request system fips-mode disable
   Restart all Versa services. Are you sure? [no,yes] yes
   ```

5. To disable FIPS mode, you must restart all Versa services. If you want to delay the restarting of Versa services to complete the FIPS mode change, answer **no** to the prompt and manually restart the Versa services at a later time.
6. To disable FIPS mode and automatically restart all services without being prompted, issue the following command:

> % **request system fips-mode disable no-confirm**

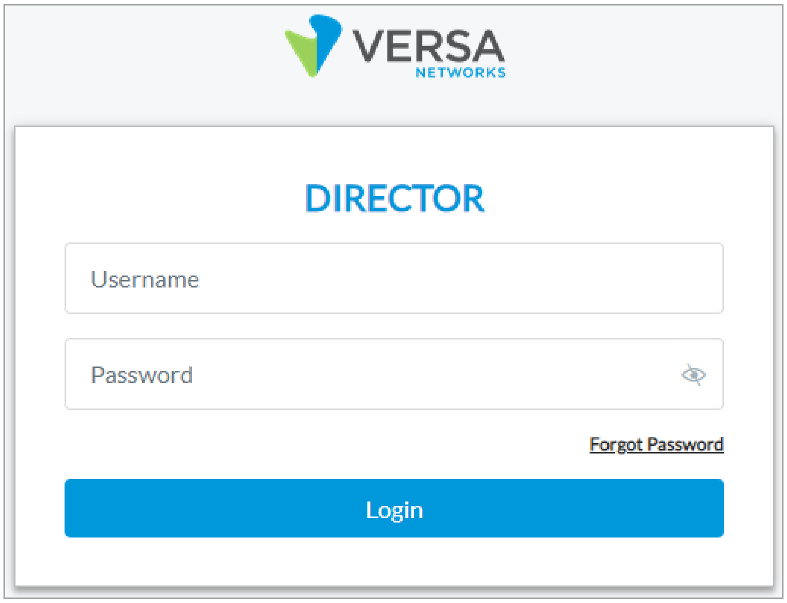
Initialize Versa Director

To initialize Versa Director:

1. Issue the **cd /opt/versa/vnms/scripts vnms-startup.sh** initialization script on the Director node.
2. Follow the prompts and on Setup Network Interfaces, set eth0 field to the same IP address as on the Director configured above.
3. If required, specify a default gateway for outside connectivity.
4. Under eth1, assign an IP address from the Control plane network.
5. Set eth0 as the northbound interface and eth1 as the southbound interface.
6. Say no for “Enable secure mode for Director HA ports” and “Secure Director HA communication” prompts. If you are configuring Director with high availability (HA), you can perform this this step later.
7. Say yes to “Prompt to set new password at first time UI login”. Director services restart and, if required, you can return to this script any time to reinitialize Director.

Log In Remotely to Director

1. You can access the Director GUI or SSH CLI by navigating to the IP address configured on eth0 from a web browser or using an SSH client. The default credentials are as follows:
2. Versa Director GUI: Administrator/versa123
3. Versa Director SSH: admin/versa123 or Administrator/versa123
4. To log in to Versa Director:
5. To log on to SSH, use a client such as PuTTY or use the ssh command, **ssh Administrator@10.0.0.50**, on MacOS and Linux systems.
6. Enter the password when prompted and press Enter. The Versa CLI displays when you enter valid login credentials.
7. To log on to Director UI, open a browser and enter the Director IP address. The login screen displays.



8. Enter the user name and password and click Login. The Director UI displays.

Perform Manual Hardening for SSH

Note that you cannot configure the SSH re-keying thresholds. They are hard-coded and occur approximately after an hour or after 1GB of data has been transmitted, whichever occurs first.

1. To perform manual hardening on the Director host:
2. To set the SSH cipher configuration, issue the following CLI command to set the SSH cipher configuration. After this, SSH only allows ciphers as defined in the Common Criteria Security Target and you do not require any additional cipher configuration.

```
vsh niap enable
sudo  /opt/versa/vnms/scripts/vnms-config.sh  --configure-niap
```

3. To generate the Director SSH host key, issue the following CLI command:

```
sudo ssh-keygen -f /etc/ssh/ssh_host_ecdsa_key -N ‘’ -t ecdsa -b 384 -C “Director SSH hostkey”
```

4. To enable public key authentication, issue the following CLI command from the management workstation:

```
ssh-keygen -t ecdsa -b 384 -C “admin”
ssh-copy-id -I ~/.ssh/id_ecdsa.pub admin@<director host>
```

Install Director License Key

1. Install the Director license by issuing the following CLI commands from the Administrator account. If you are installing multiple Directors for HA, issue these commands on each node:
2. To get the node ID file on a running Director node:

```
Administrator@vd> request system gen-nodeid
Written to /home/versa/keys/vsnodeid.v
```

3. Send the generated node ID to Versa Networks customer support. A key is generated and shared with to you.
4. On each Director node, upload the key to /home/versa/keys and issue the following CLI command.

```
admin@vd:~$ vsh load-key /home/admin/vs-hostname.key
Key accepted
```

5. To verify if the key status on a running Director node:

```
Administrator@vd> show system trial-info
Mode: internal Active
```

Generate Director X.509 Certificate and Configure TLS Ciphers

To generate the private key and certificate signing request (CSR), and to configure TLS ciphers:

1. Log on to SSH as Administrator.
2. Run the following command to create the CSR by replacing each field with organization-specific details:

```
sudo -u versa /opt/versa/vnms/scripts/vnms-csrgen.sh
--domain domain-name --country country --state state --locality location
-–organization organization-name --organizationalunit company-department
--email contact-email --keypass password –-validity validity-period --san domain-name
```

The following example creates a CSR with a SAN containing both the primary and backup director (when deploying in HA):

```
sudo -u versa /opt/versa/vnms/scripts/vnms-csrgen.sh --domain vd01.versa-networks.com
--country US --state CA --locality SC –-organization versa-networks.com
--organizationalunit IT --email admin@versa-networks.com --keypass versa123 –-validity 365
–-san vd01,DNS:vd02,DNS:vd01.versa-networks.com,DNS:vd02.versa-networks.com,DNS:10.0.0.
50,DNS:10.0.0.60
```

The CSR and private key are created in /var/versa/vnms/certs directory

3. Create a directory called certs under /home/versa by issuing the CLI commands below:

```
sudo su – versa
mkdir certs
chmod 700 certs
```

4. Copy the CSR and private key file to /home/versa/certs.
5. Upload the root and intermediate CA certificate files to /home/versa/certs.
6. Combine the root and intermediate CA certs into a single file, replacing the filenames in the example below with your CA files:

```
~# cat intermediate-certificate.pem root-certificate.pem > CA-certificate.pem
```

7. Have your PKI administrator or third-party certificate authority sign the Director certificate.
8. Upload the certificate to /home/versa/certs and issue the following CLI commands to set the permissions:

   ```
   admin@vd:~# cd /home/versa/certs
   sudo chown -R versa:versa *
   ```

9. Issue the **service vnms stop** command to stop Director services.
10. Issue the following CLI command to install the new Director certificate:

    ```
    sudo -u versa /opt/versa/vnms/scripts/vnms-import-key-cert.sh --key private-key-filename
    --cert CA-signed-cert-filename cafile ca-root-certificate-filename
    --keypass private-key-password –storepass keystore-password
    ```

    For example:

    ```
    sudo -u versa /opt/versa/vnms/scripts/vnms-import-key-cert.sh --key
    /home/versa/certs/vd01.key --cert /home/versa/certs/vd01.pem cafile
    /home/versa/certs/ca.pem --keypass versa123 --storepass versa123
    ```

11. If you are setting up a secondary Director node for HA, copy the files in the /home/versa/certs directory to the secondary node and run the command above again on the secondary Director (do not create a new CSR or private key).
12. Change the ownership of the key store and trust store files, and start the Director services:

    ```
    Admin@VersaDirector:~# cd /var/versa/vnms/data/certs
    sudo chown -R versa:versa *
    vsh start
    ```

13. Back up the /home/versa/certs directory and delete it from each node.
14. To configure HTTPS ciphers, stop the Director services by issuing the **vsh stop** CLI command.
15. Issue the following CLI command to edit the Tomcat configuration file to restrict cipher suites:

    ```
    sudo vi /opt/versa/vnms/apache-tomcat/conf/server.xml
    ```

16. Replace the following lines:

    ```
    <SSLHostConfig protocols="TLSv1.2+TLSv1.3"
       ciphers="TLS_AES_128_GCM_SHA256,
             TLS_AES_256_GCM_SHA384,
             TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,
             TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,
             TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
             TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
             TLS_AES_128_GCM_SHA256,
             TLS_AES_256_GCM_SHA384,
             TLS_CHACHA20_POLY1305_SHA256,
             TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256,
             TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256,
             TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256">
    ```

With these lines:

```
<SSLHostConfig protocols="TLSv1.2"
        ciphers="TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,
               TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,
               TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
               TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
               TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
               TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384">
```

17. Issue the following CLI command to edit /var/versa/vnms/data/conf/application.properties:

```
sudo  vi  /var/versa/vnms/data/conf/application.properties
```

18. Then, replace the following lines:

```
server.ssl.enabled-protocols=TLSv1.2,TLSv1.3
server.ssl.ciphers=TLS_AES_128_GCM_SHA256,TLS_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_
AES_128_GCM_SHA256,
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_
SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_AES_128_GCM_SHA256,TLS_AES_256_GCM_SHA384, \TLS_CHACHA20_POLY1305_
SHA256,TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256,
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256,TLS_DHE_RSA_WITH_CHACHA20_
POLY1305_SHA256
```

With the following lines:

```
server.ssl.enabled-protocols=TLSv1.2
server.ssl.ciphers=TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_
AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_
SHA256,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
```

19. Issues the **vsh start** CLI command to start the Director services.

Change Default Password

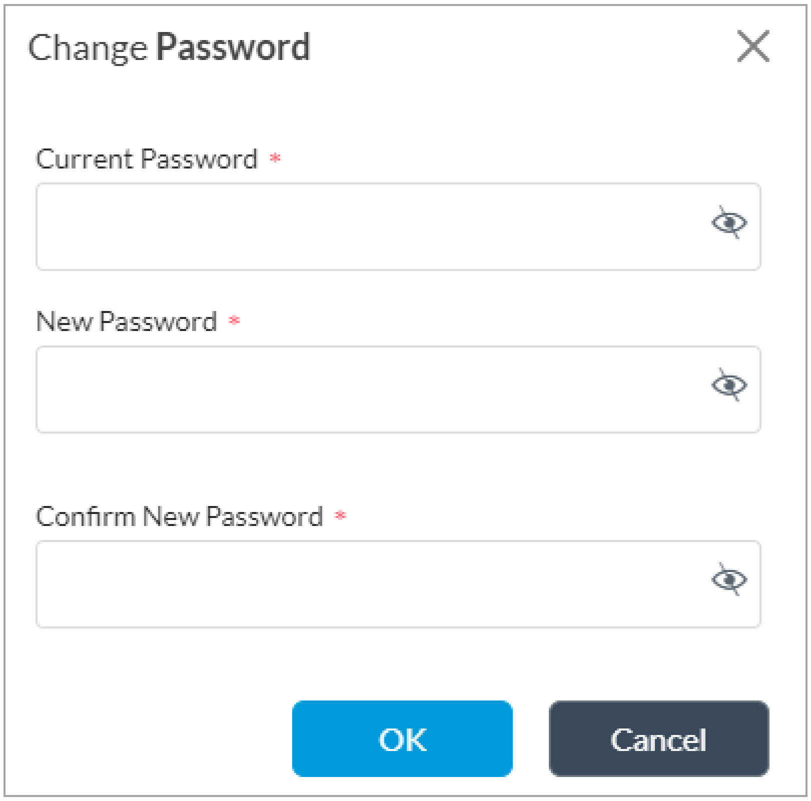
Versa recommends that you change the passwords for the following default user accounts:

- versa
- admin
- Administrator
- aaauser
- aaaadmin

To change passwords:

1. In Director view, click the Administrator drop-down menu on the top right corner of the screen.

2. Select Change Password from the drop-down list. The Change Password popup window displays.



3. Type the current password and the new password.
4. Confirm the new password and click OK.
5. To change the logged in user's password, issue the **request nms actions change-password** CLI command.
6. To change another user's password, issue the following CLI command:

   ```
   request nms actions reset-password-by-admin username username newpassword password
   ```

7. To change system-level passwords using CLI, issue the **passwd** command.
8. To switch to another user account, use the **su** command. For example:

   ```
   sudo su -u versa
   passwd
   ```

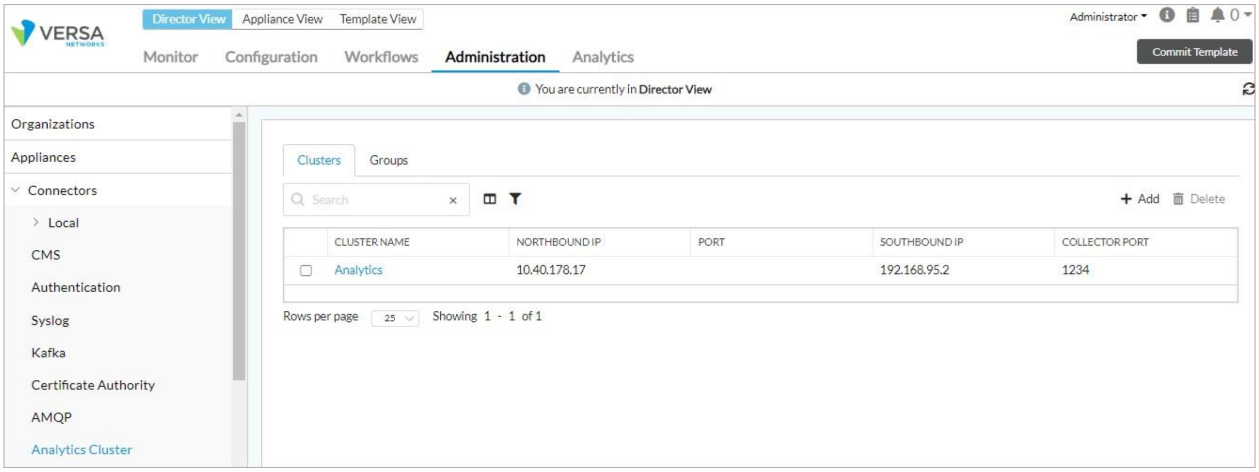
Configure an Analytics Cluster

Before you set up and Analytics cluster, you must configure an Analytics connector in Versa Director.

To configure an Analytics Connector:

1. Log in to the Director node.
2. In Director view, select the Administration tab in the top menu bar.

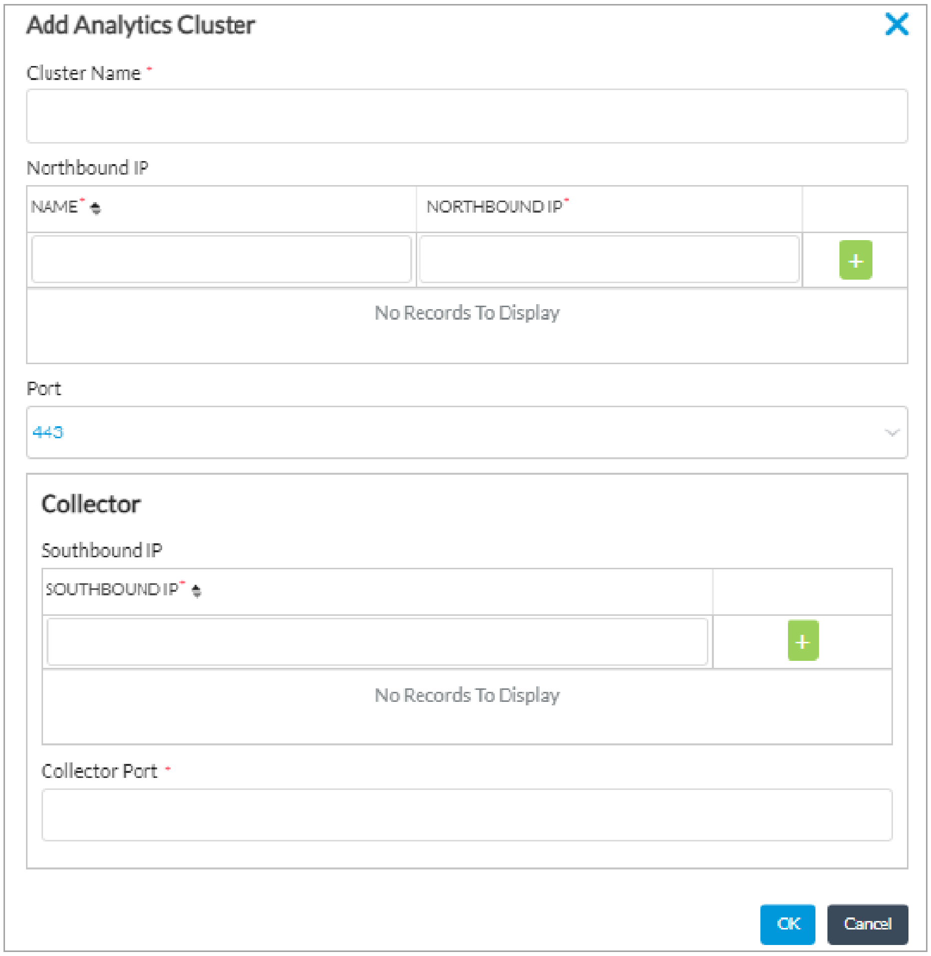
3. Select Connectors > Analytics Cluster in the left menu bar.



	CLUSTER NAME	NORTHBOUND IP	PORT	SOUTHBOUND IP	COLLECTOR PORT
□	Analytics	10.40.178.17		192.168.95.2	1234

Rows per page 25 Showing 1 - 1 of 1

4. Click the ⊞ Add icon. In the Add Analytics Cluster popup window, enter information for the following fields.


Add Analytics Cluster

Cluster Name *

Northbound IP

NAME *	NORTHBOUND IP *	
		+
No Records To Display		

Port: 443

Collector

Southbound IP

SOUTHBOUND IP *	
	+
No Records To Display	

Collector Port *

Parameter	Description
Cluster Name (Required)	Enter a name for the cluster.
Northbound IP (Table)	Enter information about the northbound interface on the Analytics cluster.
◦ Name (Required)	Enter a name for the northbound interface. For example, van01.
◦ Northbound IP (Required)	Enter the IP address of the northbound interface. For example, 10.0.0.70.
◦ + Add icon	Click the + Add icon to add the northbound IP address.
Connector Port	Select the port number to use for the northbound connection.
Collector (Table)	Enter information about the Versa Analytics cluster collector.
◦ Southbound IP (Required)	Enter the IP address of the southbound interface. For example, 172.16.0.70.
◦ ⊞ Add icon	Click the ⊞ Add icon to add the IP address.
Collector Port (Required)	Enter the port number to use on the Analytics log collector. For example, 8080.

5. Click OK.
6. To set up an analytics cluster:
7. Log in to the shell on the primary Director node.
8. Issue the following CLI command.

```
Administrator@Director01:~$ cd /opt/versa/vnms/scripts/van-cluster-config/van_cluster_install
Administrator@Director01:~$ nano clustersetup.conf
```

9. Edit the clustersetup.conf file, adding values for the parameters listed below. This file contains other parameters that are for internal use only. Do not modify the values for these parameters, and do not delete them from the file. If you use Director HA, add a block for [VERSA-DIR-2] mirroring the fields shown below in [VERSA-DIR-1].

```
[VAN_CLUSTER_SETUP_CONF]
cluster_size: 2
cluster_name: name_of_the_cluster
forwarder_count: 0

[VERSA_DIRECTOR]
```

```
director_count: 1

[VERSA-DIR-1]
username: Administrator
rpc_address: director_northbound_IP_address
listen_address: director_southbound_IP_address

[VAN-NODE-1]
username: versa
mode: cluster
hostname: hostname_of_primary_analytics_node
personality: analytics
rpc_address: northbound_IP_address_of_primary_analytics_node
listen_address: southbound_IP_address_of_primary_analytics_node
collector_address: collector_address
collector_port: collector_port

[VAN-NODE-2]
username: versa
mode: cluster
hostname: hostname_of_secondary_analytics_node
personality: search
rpc_address: northbound_IP_address_of_secondary_analytics_node
listen_address: southbound_IP_address_of_secondary_analytics_node
collector_address: collector_address
collector_port: collector_port
```

Parameter	Description
cluster_name	Name for the cluster. This same name is used for all the nodes of the cluster.
cluster_size	Number of nodes in the cluster, either 2, 4, or 6.
forwarder_count	Number of log forwarders in the cluster. In default mode, this value is 0.
director_count	Number of Director nodes that are communicating with the Analytics nodes. If the Director is operating in standalone mode, enter 1. If the Director is in active-standby mode, enter 2.
rpc_address	IP address of the management (northbound) interface, which is the eth0 interface.
listen_address	IP address of the internal network (southbound) interface, which is the eth1 interface.
username	Name of an admin user who is authorized to log in to the Analytics nodes from the Director node. When you generate the Analytics configuration in the next step, you are prompted for a password. The default username is versa, and the default password is versa123.
password	(In Releases 20.2.3 and later, and Releases 21.1.1 and later.) Enter a password associated with the username. If you configure a password and include the **--force** option when you run the cluster installation script, the script skips the password request prompt.

Parameter	Description
mode	Enter the string "cluster" (without the quotation marks) to indicate that the Analytics node is operating as a cluster. (If you are setting up an Analytics node for a proof of concept (POC), you can set the mode to "standalone" to set up a standalone Analytics node.)
hostname	Name to use as the base name to identify the Analytics nodes in the cluster. Each of the nodes is identified by this name followed by a number. For example, if you specify the hostname "Analytics," the script names the first node "Analytics01," the second node "Analytics02," and so on.
personality	Role of the Analytics node, either analytics or search. Based on the number of nodes in the cluster (specified with the cluster_size parameter), the script configures the first half of the nodes with the analytics personality and the second half of the nodes with the search personality. So in a four-node cluster, node01 and node02 are analytics nodes, and node03 and node04 are search nodes. (If you are setting up an Analytics node for a proof of concept (POC), you can set the personality to standalone.)
collector_address	IP address of the Analytics log collector.
collector_port	Port number to use to connect to the log collector.

10. Save the file and exit, then issue the following CLI command**.**

```
Administrator@Director01:~$ sudo ./van_cluster_installer.py
```

This script does the following:

- Based on the parameters values you configured in the clustersetup.conf file, generates one Analytics configuration setup file, vansetup.conf, for each node in the cluster. Do not modify the contents of the vansetup.conf files.

- Copies the vansetup.conf file and all required installation files to each Analytics node in the cluster.
- Installs the Analytics certificate on the Director node.
- Executes the vansetup.py installation script on each Analytics node.

11. Run the cluster installation script a second time, including the **--post-setup** option, to complete the setup of the Analytics cluster.

```
Administrator@Director01:~$ sudo ./van_cluster_installer.py --post-setup
```

12. Run the cluster installation script a third time with the **--secure** option to enable encrypted communication between various database components. This option is required when the Analytics node is exposed to public networks.

```
Administrator@Director01:~$ sudo -u versa ./van_cluster_installer.py --secure
```

The script enables secure communication on the following components:

- Cassandra
  - Client communication secure port: 9042
  - Internode communication secure port: 7001
- Solr
  - Client communication secure port: 8983
  - Internode communication secure port: 8983
- Versa Analytics driver
  - REST API secure port: 5000
- Versa Analytics monitor
  - REST API secure port: 5010
- Versa LCED
  - REST API secure port: 8008
- Zookeeper
  - Internode communication secure ports: 2888, 3888

The following steps must be run any time the Director certificates are re-generated or replaced.

1. Ensure all VAN nodes are configured in the Analytics Cluster Connector from the Director UI.
2. Run the following commands:

```
sudo su – versa /opt/versa/vnms/scripts/vd-van-cert-upgrade.sh
```

Or

```
su - versa -c "/opt/versa/vnms/scripts/vd-van-cert-upgrade.sh --pull"
```

3. Restart the Versa services by issuing the **vsh restart** CLI command.
4. Pull the Director Certificate from the Analytics node. Before you do this, ensure that the hostname is resolvable via DNS or /etc/hosts entry. The from which to pull the certificates must be open and accessible from the Analytics nodes. Also, if IP address is specified, the certificate must contain the IP address as SAN. Run the following command.

   > sudo /opt/versa/scripts/van-scripts/van-cert-pull.sh --host VERSA_DIRECTOR_HOSTNAME/IP_Address --port [Default is 8443]

5. To pull the Director certificate again from the REST API port 9183 and add it to the trust-store, issue the following command.

   > sudo /opt/versa/scripts/van-scripts/van-cert-pull.sh --host VERSA_DIRECTOR_HOSTNAME/IP_Address --port 9183

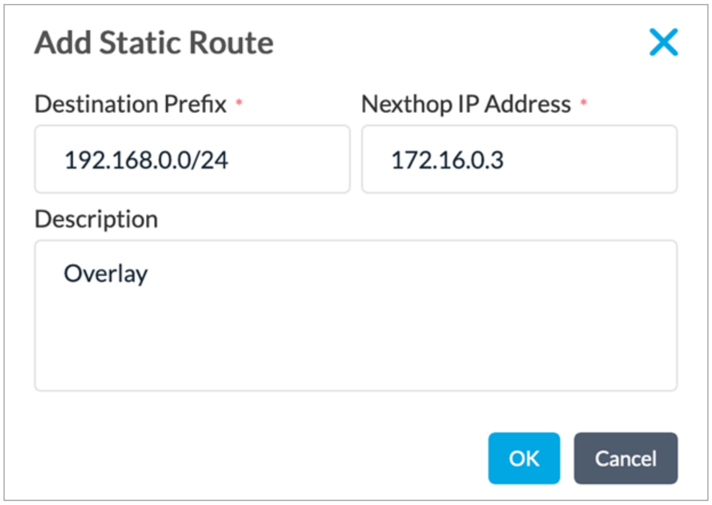
   This script automatically restarts the analytic services.
6. Restart Analytics services if they do not restart.
7. Register the Versa Director hostname in Analytics Configuration > Authentication screen. The hostname must match the host provided Step 2.

Configure an SD-WAN Controller

Before you configure an SD-WAN controller, define a static route on the active Versa Director to provide an exit from the device when no other routes are available. Then, configure an overlay address prefix.

To define a static route:

1. In Director view, select the Administration tab in the top menu bar.
2. Select System > Static Routes. The Static Routes window display the configured statis routes.
3. Click + Add. The Add Static Route popup window displays. Enter information for the following fields.


Add Static Route

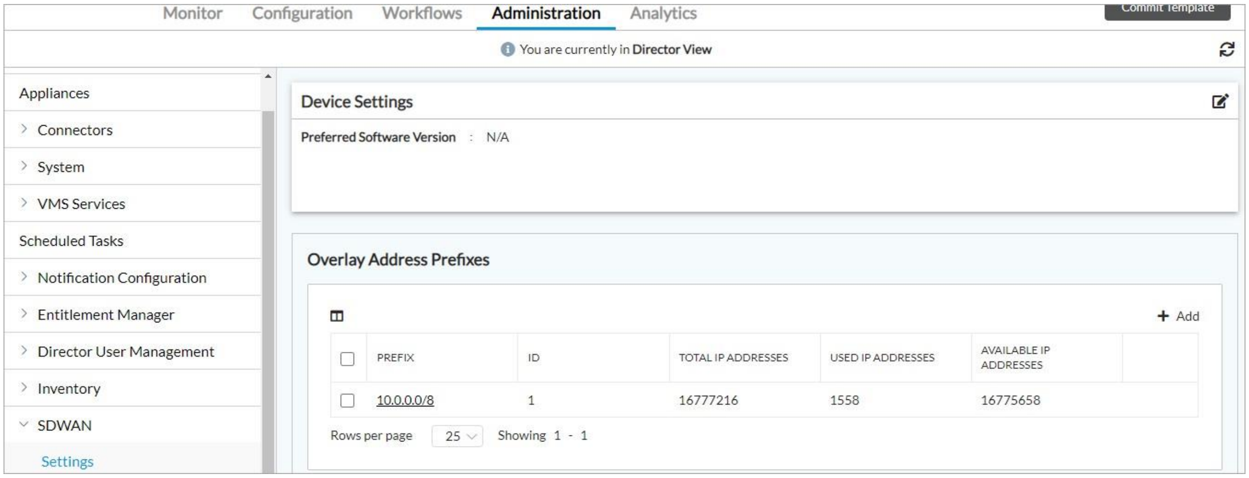
Destination Prefix *: 192.168.0.0/24

Nexthop IP Address *: 172.16.0.3

Description: Overlay

Parameter	Description
Destination Prefix (Required)	Enter the IP address and prefix that is reachable using the static route.
Nexthop IP Address (Required)	Enter the IP address of the router or gateway to reach the destination.
Description	Enter a description for the static route.

4. Click OK.
5. To configure an overlay address prefix:
6. In Director view, select the Administration tab in the menu bar.
7. Select SD-WAN > Settings in the left menu bar. The main pane displays the Device Settings and Overlay Address Prefixes panes.



Device Settings

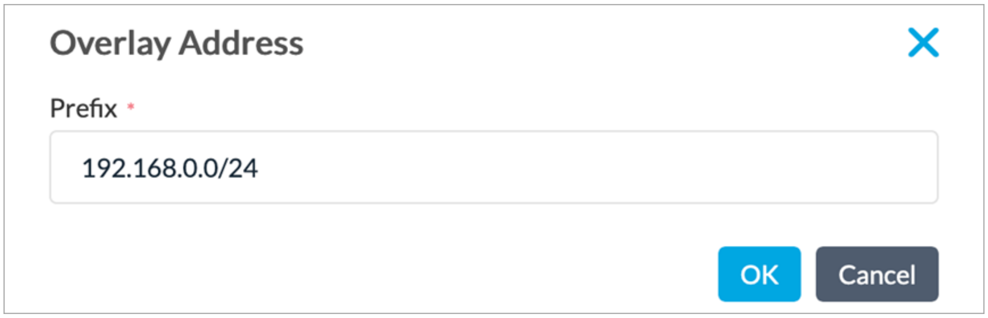
Preferred Software Version : N/A

Overlay Address Prefixes

PREFIX	ID	TOTAL IP ADDRESSES	USED IP ADDRESSES	AVAILABLE IP ADDRESSES
10.0.0.0/8	1	16777216	1558	16775658

Rows per page 25 Showing 1 - 1

8. Click + Add. The Overlay Address popup window displays.

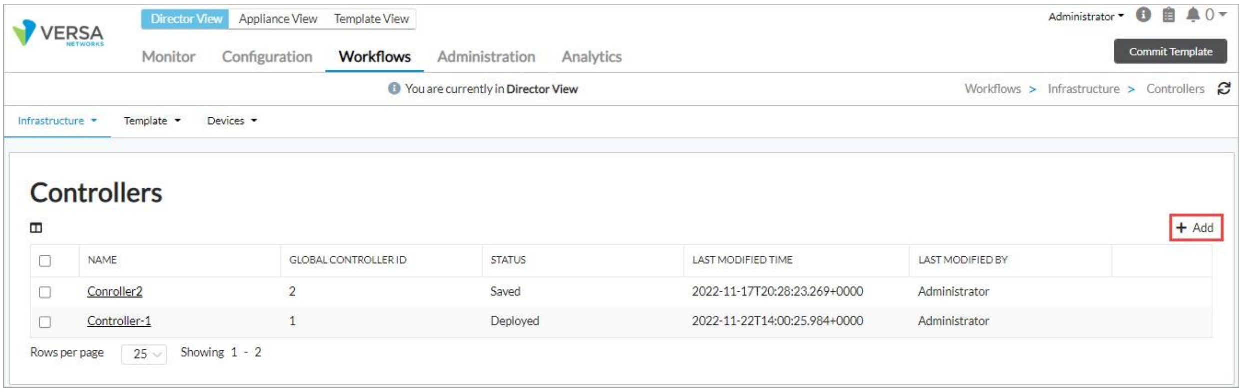


Overlay Address

Prefix *

192.168.0.0/24

9. Enter the overlay address prefix in the Prefix field. For example, 192.168.0.0/24.
10. Click OK.
11. To add an SD-WAN Controller:
12. In Director view, select the Workflows tab in the top menu bar.
13. Select Infrastructure > Controllers in the left menu bar.

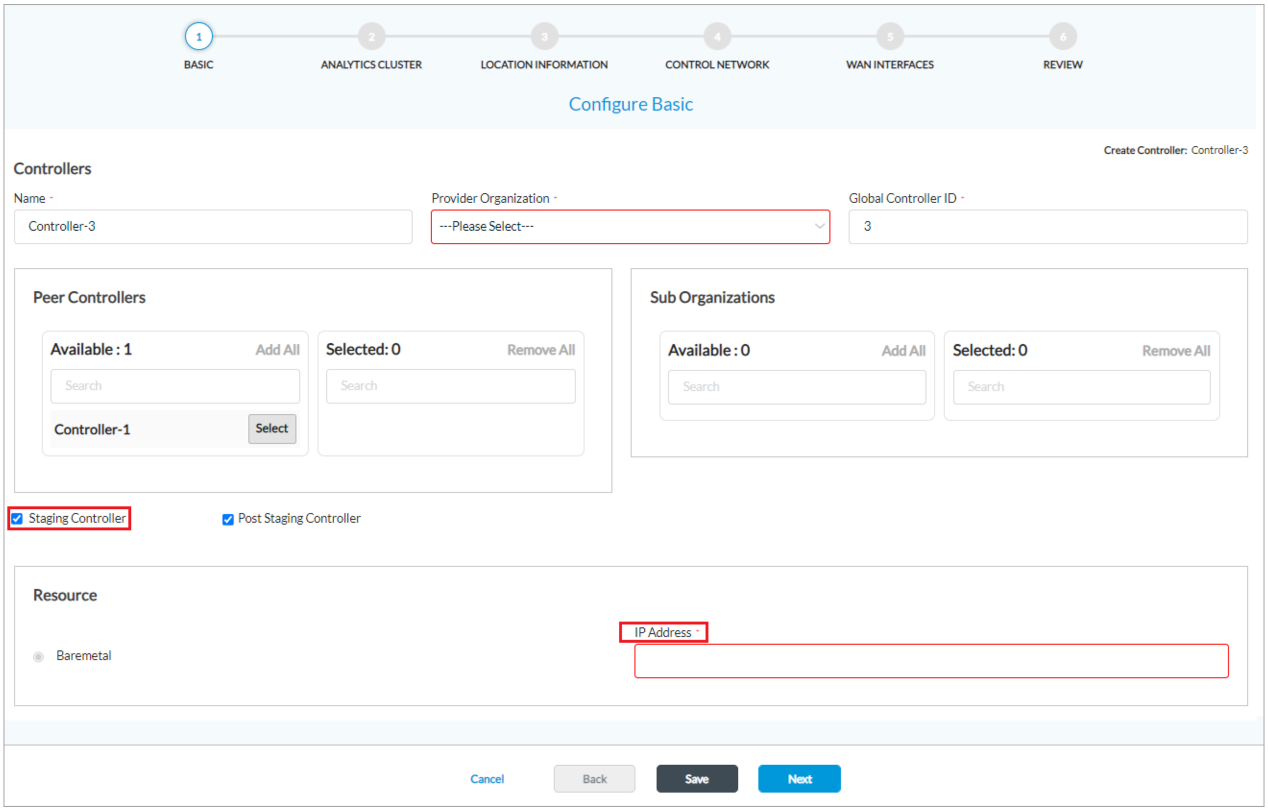


Controllers

NAME	GLOBAL CONTROLLER ID	STATUS	LAST MODIFIED TIME	LAST MODIFIED BY
Conroller2	2	Saved	2022-11-17T20:28:23.269+0000	Administrator
Controller-1	1	Deployed	2022-11-22T14:00:25.984+0000	Administrator

Rows per page 25 Showing 1 - 2

14. Click the + Add icon. The Create Controller Configure Basic tab displays.



Create Controller: Controller-3

Controllers

Name * Controller-3

Provider Organization * ---Please Select---

Global Controller ID * 3

Peer Controllers

Available : 1 — Controller-1

Selected: 0

Sub Organizations

Available : 0

Selected: 0

☑ Staging Controller

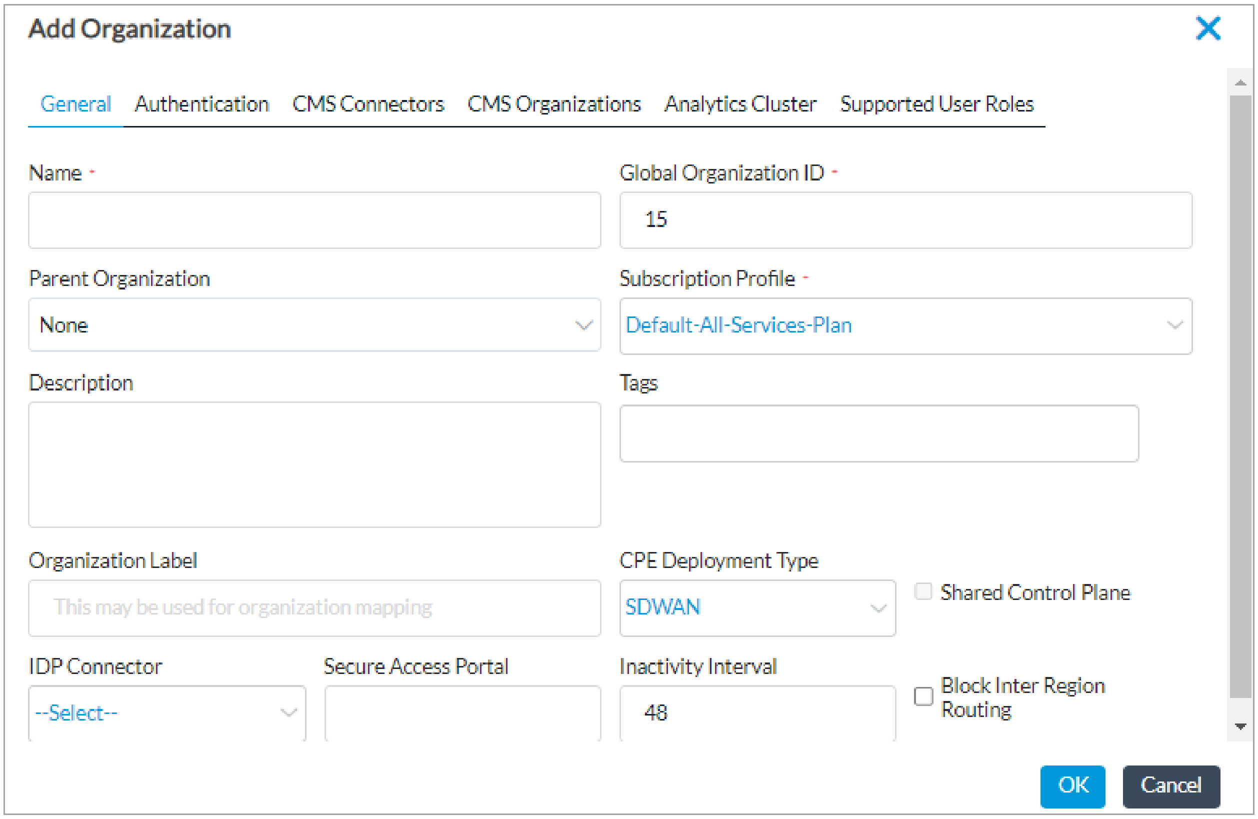
☑ Post Staging Controller

Resource

○ Baremetal

IP Address *

15. Enter a name for the controller.
16. Select + Add New from the Provider Organization drop-down list. The Add Organization > General tab displays.



Add Organization

Name *

Global Organization ID * 15

Parent Organization: None

Subscription Profile *: Default-All-Services-Plan

Description

Tags

Organization Label: This may be used for organization mapping

CPE Deployment Type: SDWAN

□ Shared Control Plane

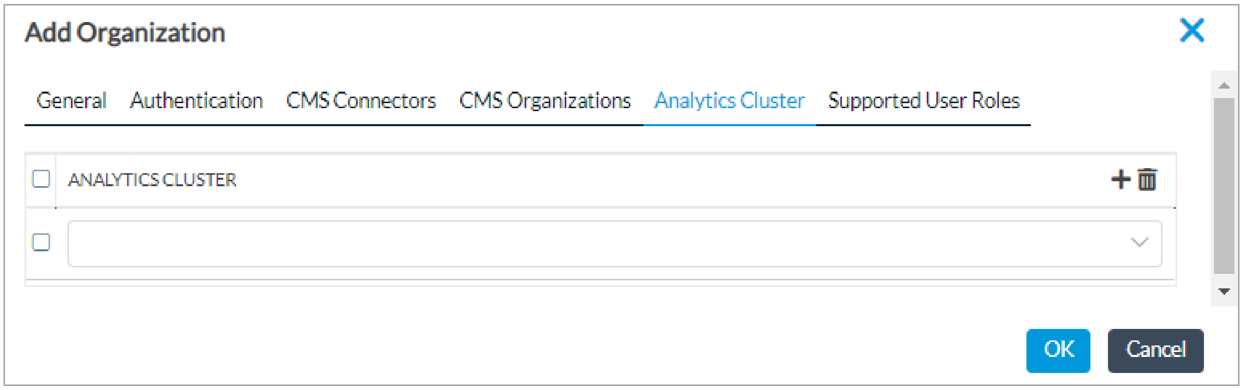
IDP Connector: --Select--

Secure Access Portal

Inactivity Interval: 48

□ Block Inter Region Routing

- Enter a name for the organization.
- If this is the first organization, enter 1 in the Global Organization ID field. Enter a name for the organization.
- Select the Analytics tab and click + to select the analytics cluster you created in Configure an Analytics Cluster.



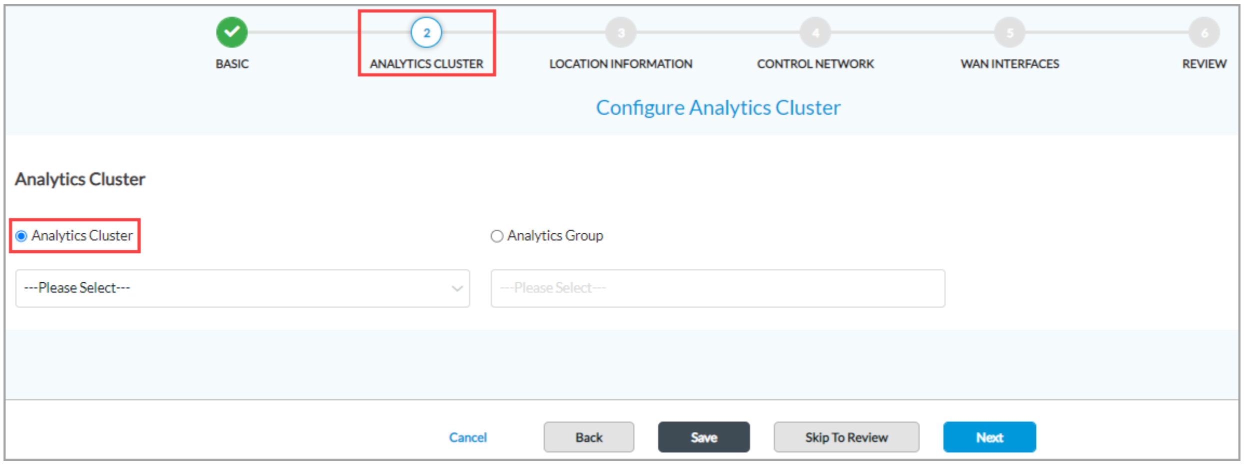
Add Organization

□ ANALYTICS CLUSTER

□

- For information about configuring other parameters, see Add a Provider Organization.
- Click OK.

17. In the Create Controller > Basic tab, select Staging Controller and enter the northbound IP address of the controller.
18. Select Analytics Cluster tab.
19. Select Analytics Cluster and select the cluster you created in Configure an Analytics Cluster from the drop-down list.

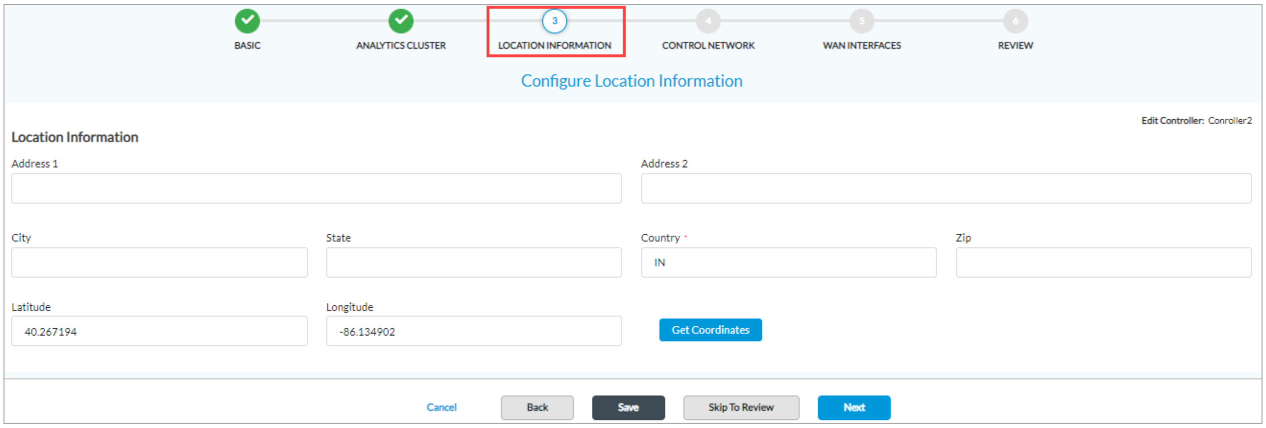


Analytics Cluster

● Analytics Cluster ○ Analytics Group

---Please Select--- ---Please Select---

20. Select the Location Information tab and enter the geographical coordinates.

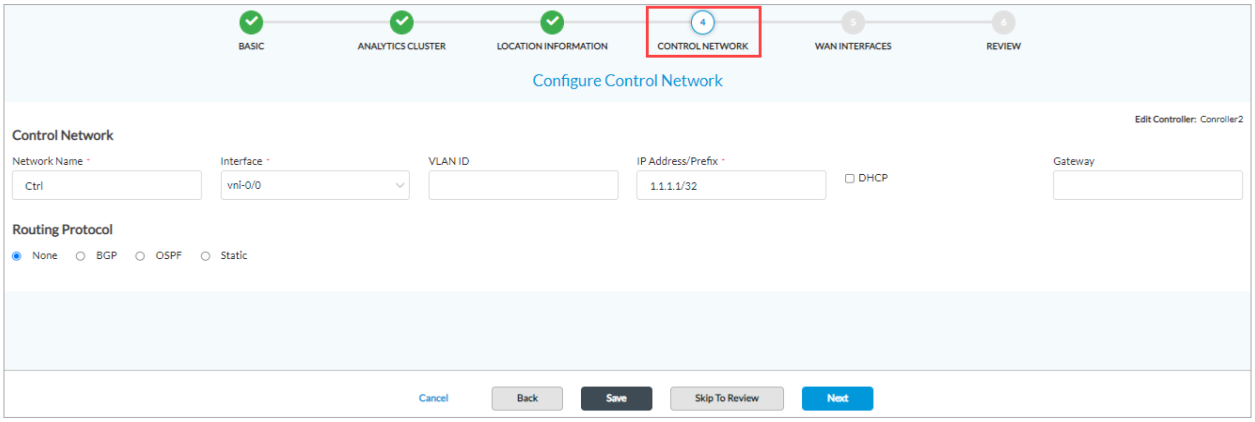


Edit Controller: Conroller2

Location Information

Address 1		Address 2	
City	State	Country *	Zip
		IN	
Latitude	Longitude		
40.267194	-86.134902		

21. Select the Control Network tab and enter values for Network Name, Interface, VLAN ID, and IP Address/Prefix.



Edit Controller: Conroller2

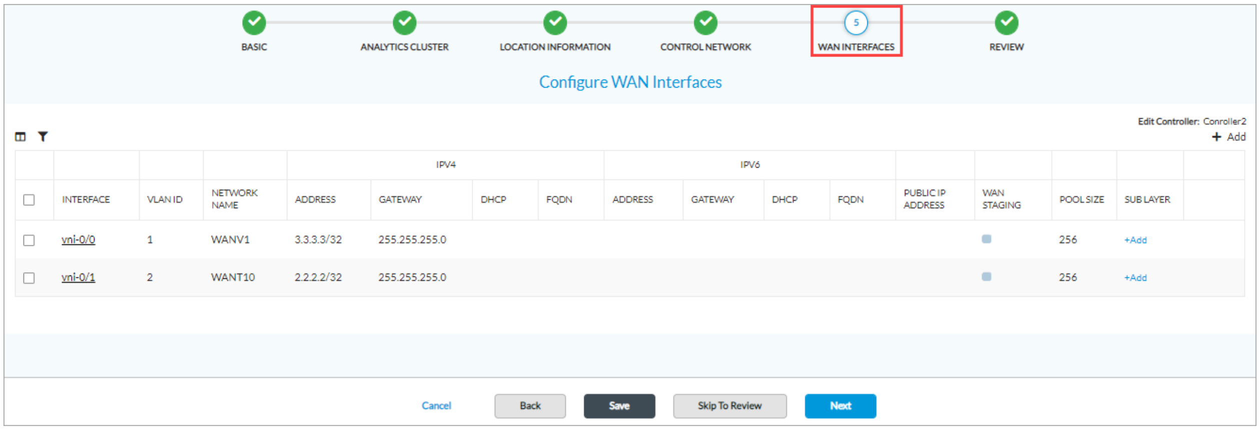
Control Network

Network Name *	Interface *	VLAN ID	IP Address/Prefix *		Gateway
Ctrl	vni-0/0		1.1.1.1/32	□ DHCP	

Routing Protocol

● None ○ BGP ○ OSPF ○ Static

22. Select the WAN Interfaces tab.



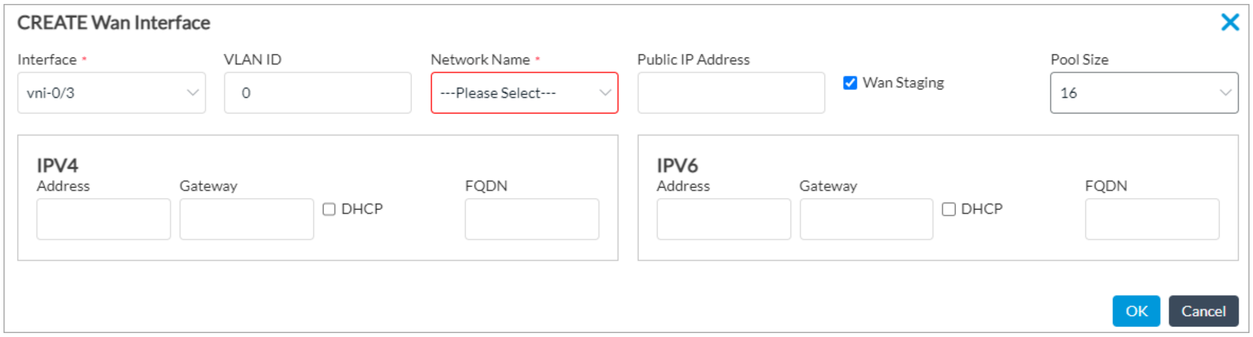
Configure WAN Interfaces

Edit Controller: Conroller2

+ Add

				IPV4				IPV6							
□	INTERFACE	VLAN ID	NETWORK NAME	ADDRESS	GATEWAY	DHCP	FQDN	ADDRESS	GATEWAY	DHCP	FQDN	PUBLIC IP ADDRESS	WAN STAGING	POOL SIZE	SUB LAYER
□	vni-0/0	1	WANV1	3.3.3.3/32	255.255.255.0								■	256	+Add
□	vni-0/1	2	WANT10	2.2.2.2/32	255.255.255.0								■	256	+Add

- Click + Add to add a WAN interface. The Create WAN Interface popup window displays.



CREATE Wan Interface

Interface * vni-0/3

VLAN ID 0

Network Name * ---Please Select---

Public IP Address

☑ Wan Staging

Pool Size 16

IPV4

Address

Gateway

□ DHCP

FQDN

IPV6

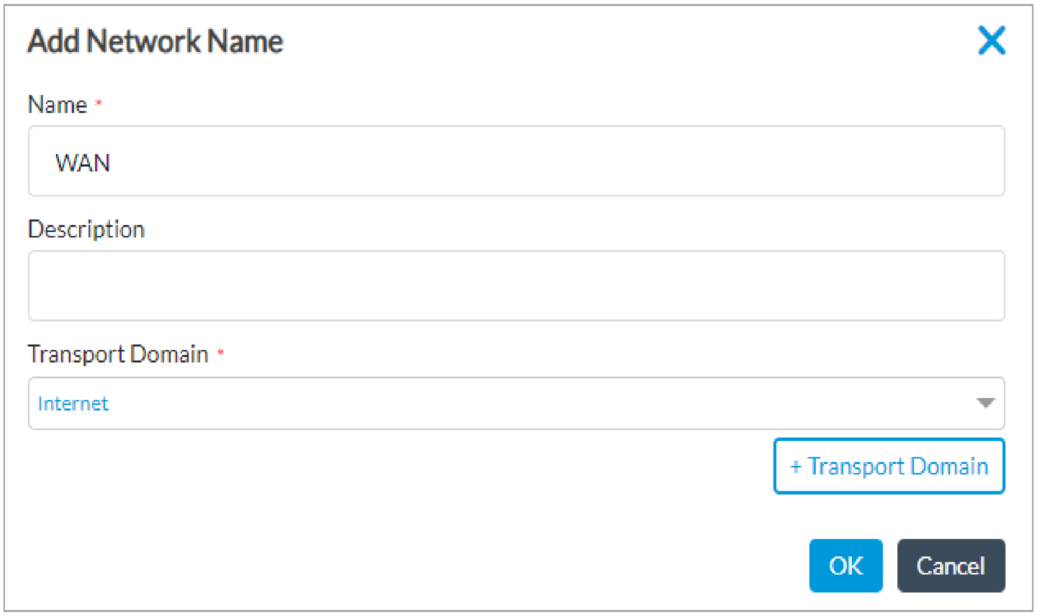
Address

Gateway

□ DHCP

FQDN

- Under Network Name, select + Add New. The Add Network Name window displays.



Add Network Name

Name * WAN

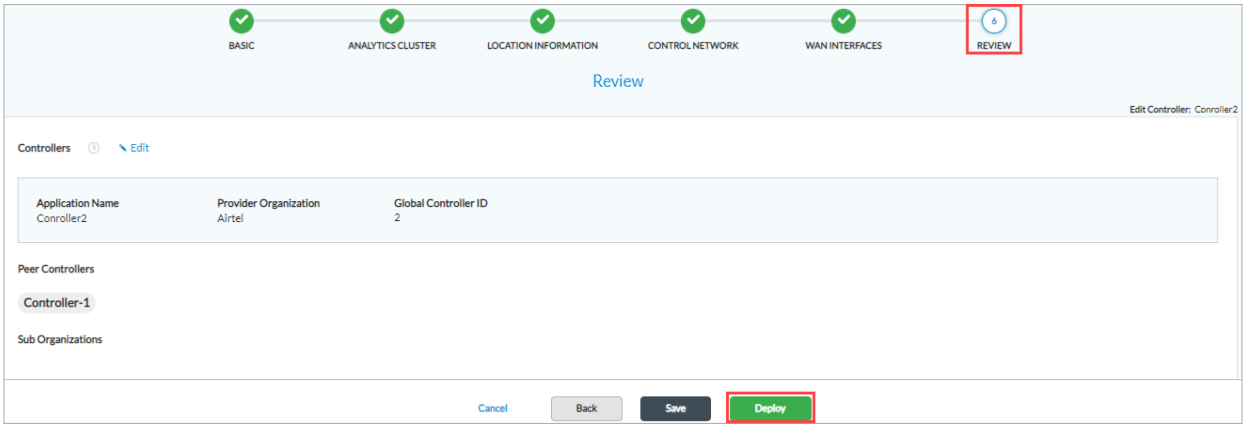
Description

Transport Domain * Internet

- Enter a name for the network and select a transport domain from the drop-down list. For example, Internet.

- Select the network interface, enter a VLAN ID, IPv4/IPv6 Address and Gateway.
- Select WAN Staging.
- Select Pool Size. For testing purposes, a pool size of 16 is recommended.
- Click OK.

23. For information about configuring other parameters, see Add a Controller Node.
24. Select the review tab and click Deploy. After deploying, the Status field displays Deployed.



Edit Controller: Conroller2

Controllers

Application Name	Provider Organization	Global Controller ID
Conroller2	Airtel	2

Peer Controllers

Controller-1

Sub Organizations

Configure a DNS Server

You can configure Domain Name System (DNS) servers for individual routing instances. For any DNS configuration, you must configure either source interface or source network. You can configure explicit DNS servers when you want to avoid non-routable interfaces (paired TVIs) or when a DNS server is not present in a VPN and the DNS request must traverse a tunnel.

For more information about configuring DNS servers from the Director UI, see Configure DNS Servers.

To configure DNS servers using CLI:

1. Edit the resolvconf file in each headend node by issuing the following CLI command:

```
sudo vi /etc/resolvconf/resolv.conf.d/base
nameserver name-server-name
```

   An example for name server is 1.1.1.1.
2. Save the file and issue the **sudo resolvconf -u** CLI command.
3. Ping and external host to test connectivity. For example, **ping google.com**.

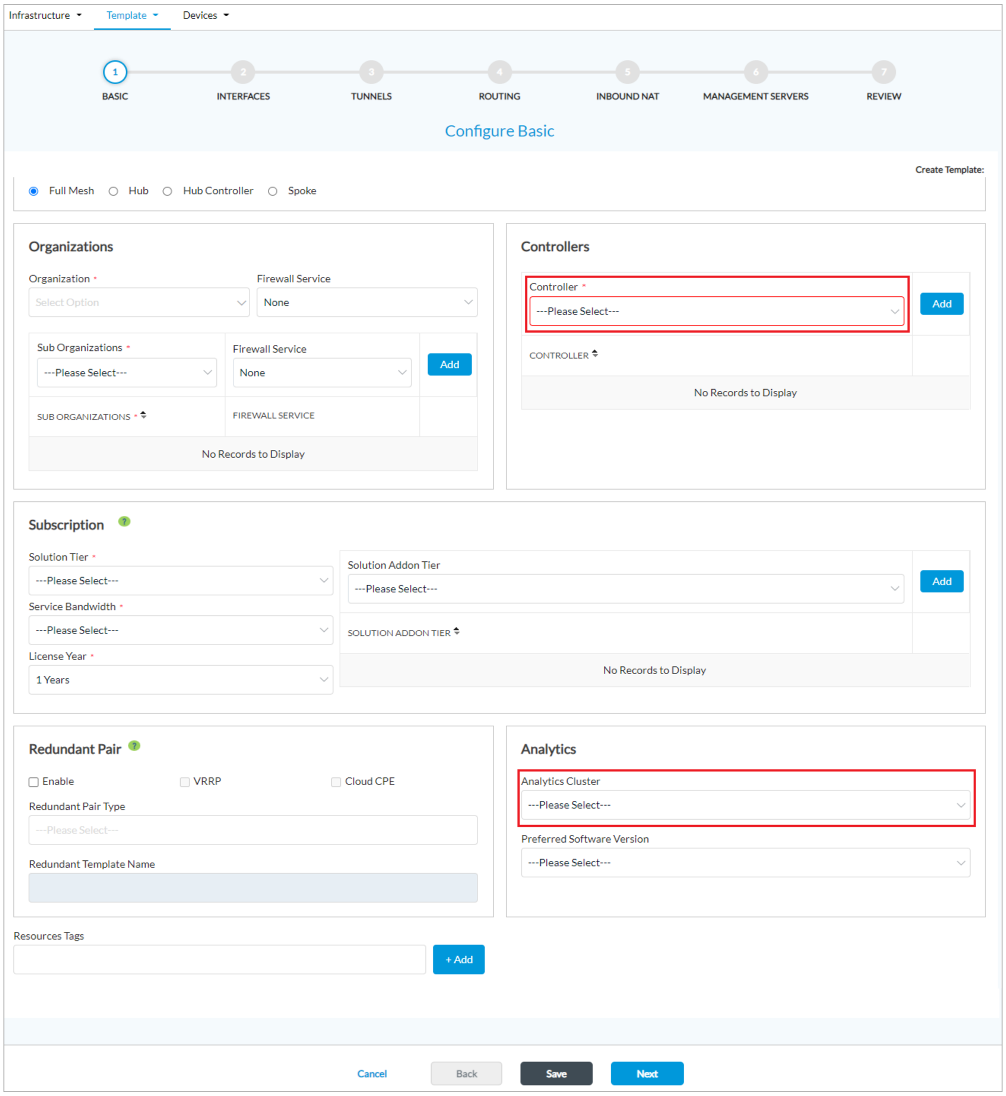
Deploy a VOS Branch Device

To deploy a branch device, do the following:

Add a Post-Staging Template

First, add a template:

1. In Director view, select the Workflows tab in the top menu bar.
2. Select Template > Templates in the horizontal menu bar.
3. Click the + Add icon. The Create Template screen displays. In the Basic tab, enter information for the following fields.



● Full Mesh ○ Hub ○ Hub Controller ○ Spoke

Organization *: Select Option
Firewall Service: None
Sub Organizations *: ---Please Select---
Firewall Service: None
SUB ORGANIZATIONS * | FIREWALL SERVICE
No Records to Display

Controller *: ---Please Select---
CONTROLLER
No Records to Display

Solution Tier *: ---Please Select---
Service Bandwidth *: ---Please Select---
License Year *: 1 Years
Solution Addon Tier: ---Please Select---
SOLUTION ADDON TIER
No Records to Display

□ Enable □ VRRP □ Cloud CPE
Redundant Pair Type: ---Please Select---
Redundant Template Name:

Analytics Cluster: ---Please Select---
Preferred Software Version: ---Please Select---

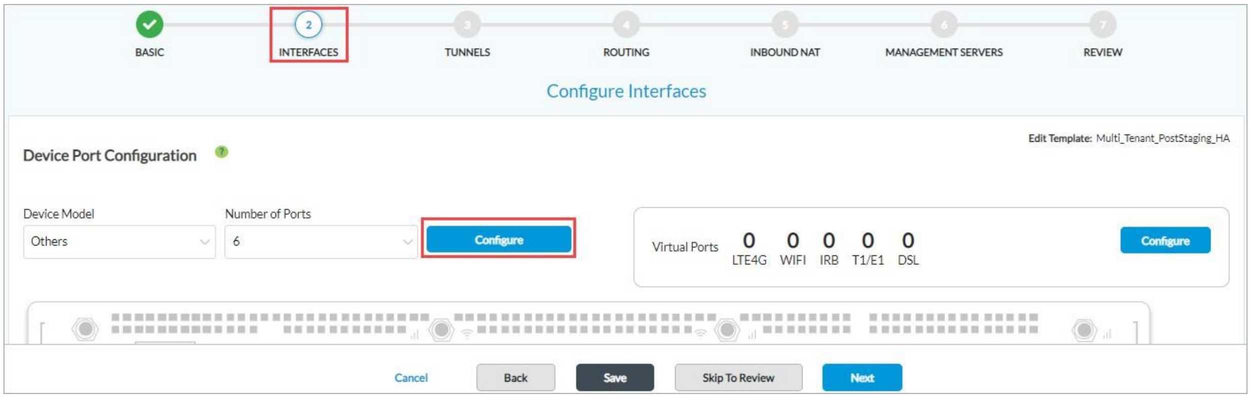
Resources Tags:

- Enter a name for the template.
- Select a organization, solution tier, and service bandwidth and enter other mandatory information.
- Under Controller, select the SD-WAN controller you created in Configure an SD-WAN Controller from the drop-down list.
- Under Analytics, select the analytics cluster you created in Configure an Analytics Cluster from Analytics

Cluster the drop-down list.

- Click Next.

4. In the Interfaces tab, select the device model and number of ports and click Configure.



Configure Interfaces

Device Port Configuration

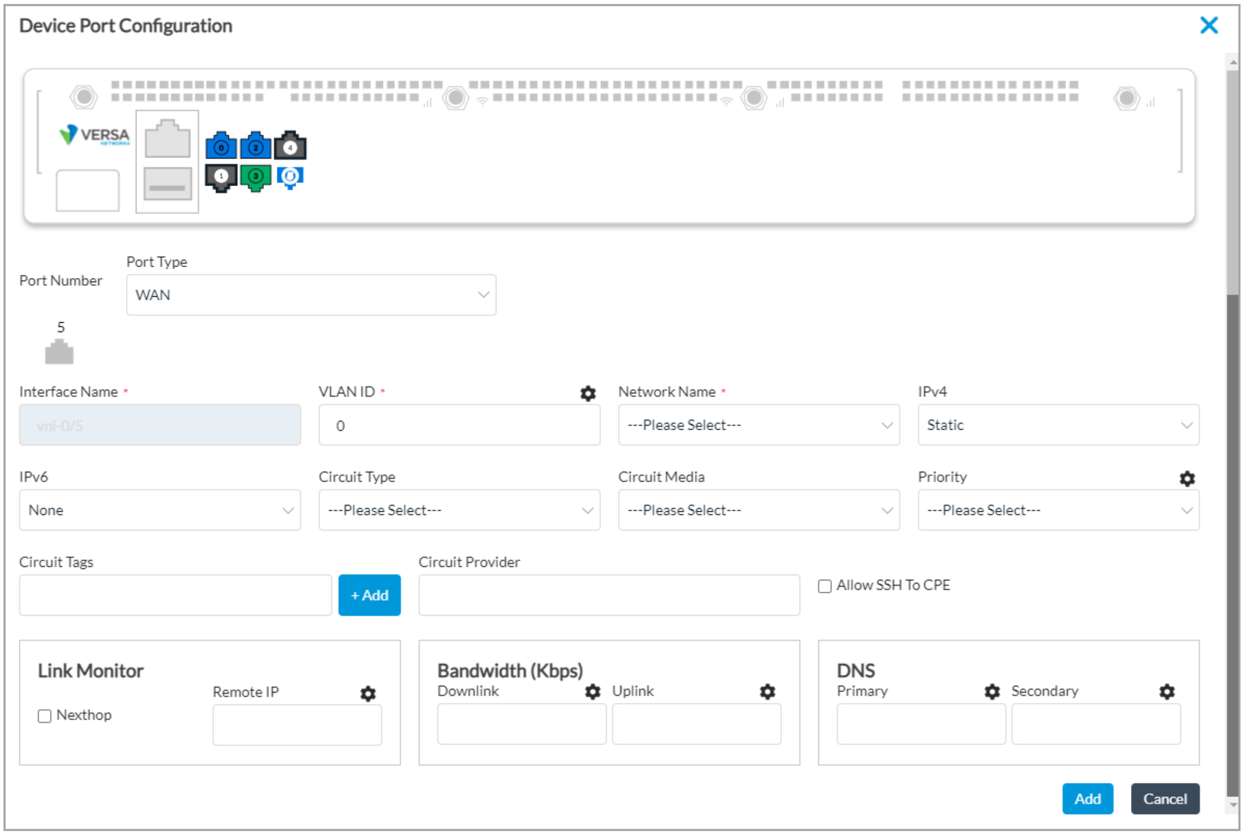
Edit Template: Multi_Tenant_PostStaging_HA

Device Model: Others

Number of Ports: 6

Virtual Ports: 0 LTE4G, 0 WIFI, 0 IRB, 0 T1/E1, 0 DSL

5. Configure the details for a WAN and a LAN port. The screenshot below shows an example for WAN port configuration.



Device Port Configuration

Port Number: 5

Port Type: WAN

Interface Name *: vni-0/5

VLAN ID *: 0

Network Name *: ---Please Select---

IPv4: Static

IPv6: None

Circuit Type: ---Please Select---

Circuit Media: ---Please Select---

Priority: ---Please Select---

Circuit Tags:

Circuit Provider:

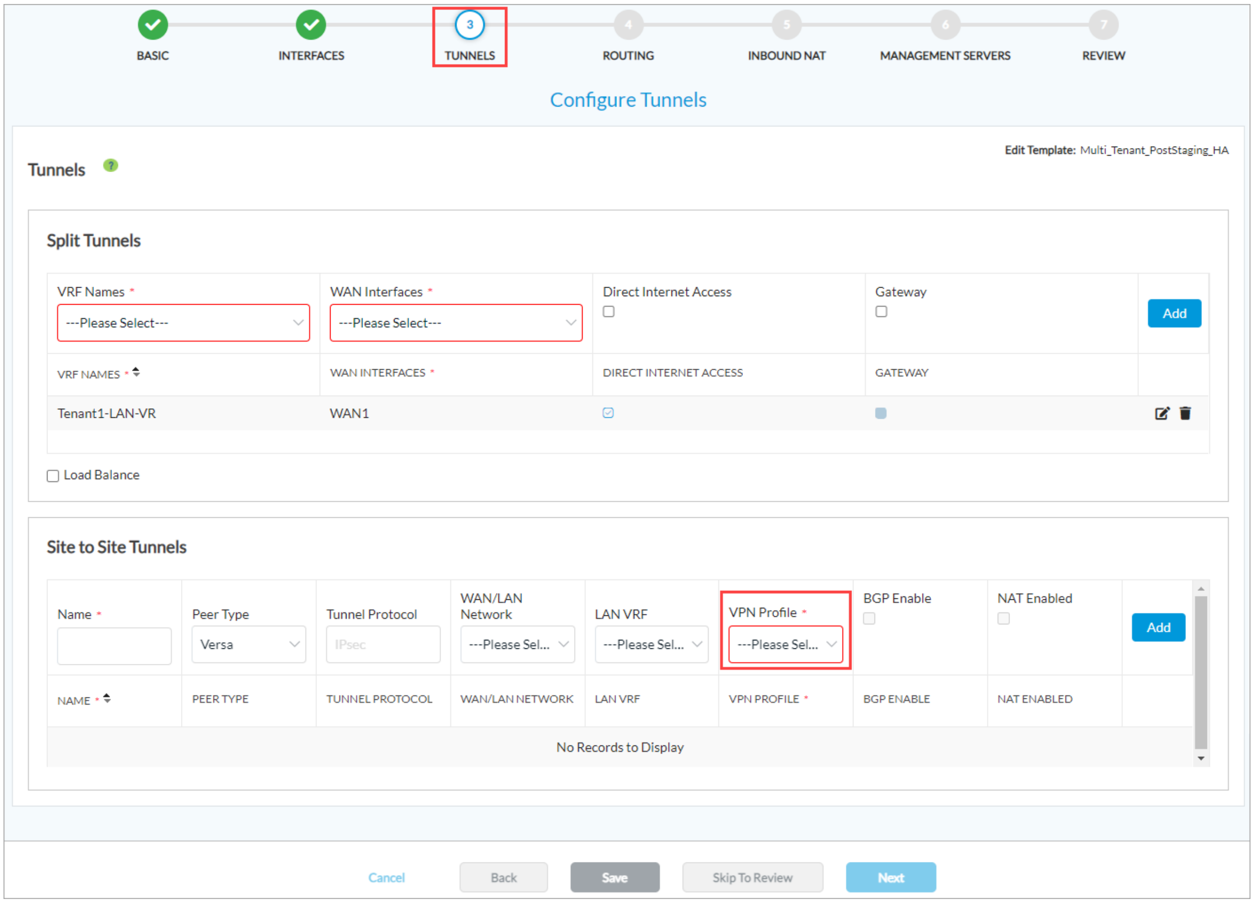
□ Allow SSH To CPE

Link Monitor: Remote IP:; □ Nexthop

Bandwidth (Kbps): Downlink:; Uplink:

DNS: Primary:; Secondary:

6. In the Tunnels tab, enter details for LAN or WAN split tunnel.



Configure Tunnels

Tunnels

Edit Template: Multi_Tenant_PostStaging_HA

Split Tunnels

VRF Names *	WAN Interfaces *	Direct Internet Access	Gateway	
---Please Select---	---Please Select---	□	□	Add
VRF NAMES *	WAN INTERFACES *	DIRECT INTERNET ACCESS	GATEWAY	
Tenant1-LAN-VR	WAN1	☑	■	

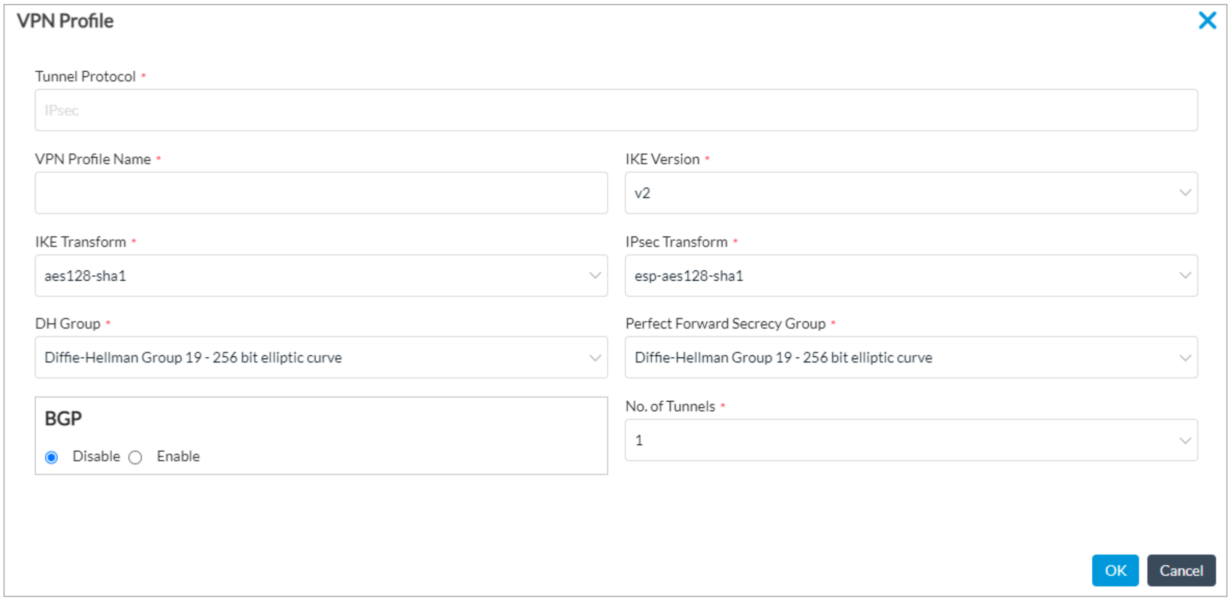
□ Load Balance

Site to Site Tunnels

Name *	Peer Type	Tunnel Protocol	WAN/LAN Network	LAN VRF	VPN Profile *	BGP Enable	NAT Enabled	
	Versa	IPsec	---Please Sel...	---Please Sel...	---Please Sel...	□	□	Add
NAME *	PEER TYPE	TUNNEL PROTOCOL	WAN/LAN NETWORK	LAN VRF	VPN PROFILE *	BGP ENABLE	NAT ENABLED	

No Records to Display

7. In the Site-to-Site Tunnels section, select + Add New from the VPN Profile drop-down list. The VPN Profile window displays.
8. Enter the information to add a VPN profile.



VPN Profile

Tunnel Protocol *
IPsec

VPN Profile Name *

IKE Version *
v2

IKE Transform *
aes128-sha1

IPsec Transform *
esp-aes128-sha1

DH Group *
Diffie-Hellman Group 19 - 256 bit elliptic curve

Perfect Forward Secrecy Group *
Diffie-Hellman Group 19 - 256 bit elliptic curve

BGP
● Disable ○ Enable

No. of Tunnels *
1

Note that you must use the following ciphers to comply with the configuration evaluated by CC:

IKE:
aes128-sha1
aes256-sha1
aes128-sha256
aes256-sha256
aes128-sha384
aes256-sha384
aes128-sha512
aes256-sha512
aes256-gcm

IPsec:

esp-aes128-sha1
esp-aes256-sha1
esp-aes128-sha256
esp-aes256-sha256
esp-aes128-sha384
esp-aes256-sha384
esp-aes128-sha512
esp-aes256-sha512
esp-aes256-gcm

Diffie-Hellman:

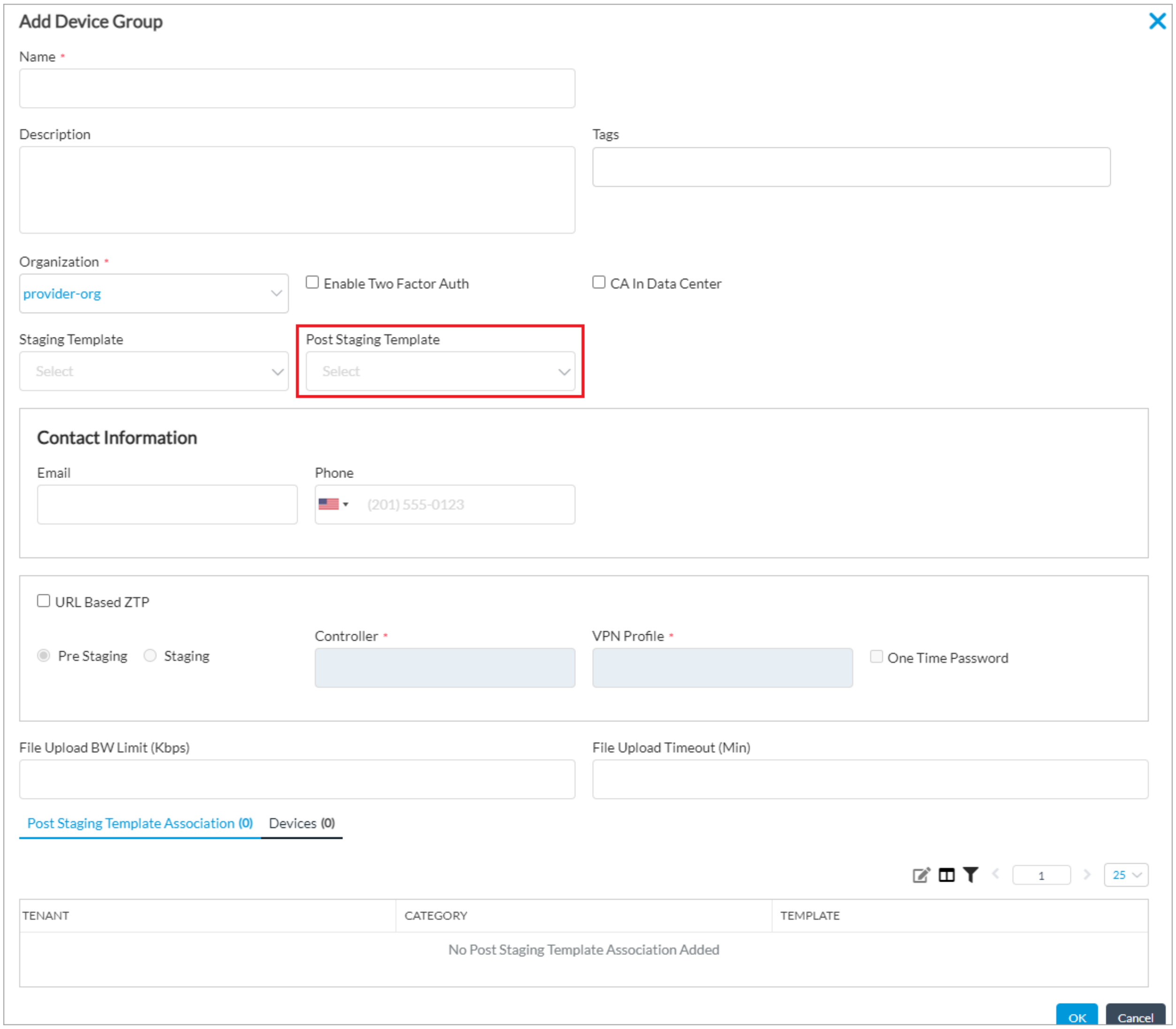
Group 19
Group 20

9. In the Review screen, click Create.

Create a Device Group

To create a device group:

1. In Director view:
    a. Select the Configuration tab in the top menu bar.
    b. Select Devices > Device Groups in the horizontal menu bar.
2. Click + Add. The Add Device Group window displays.
3. Enter the required information such as Name and Organization.



Organization *: provider-org

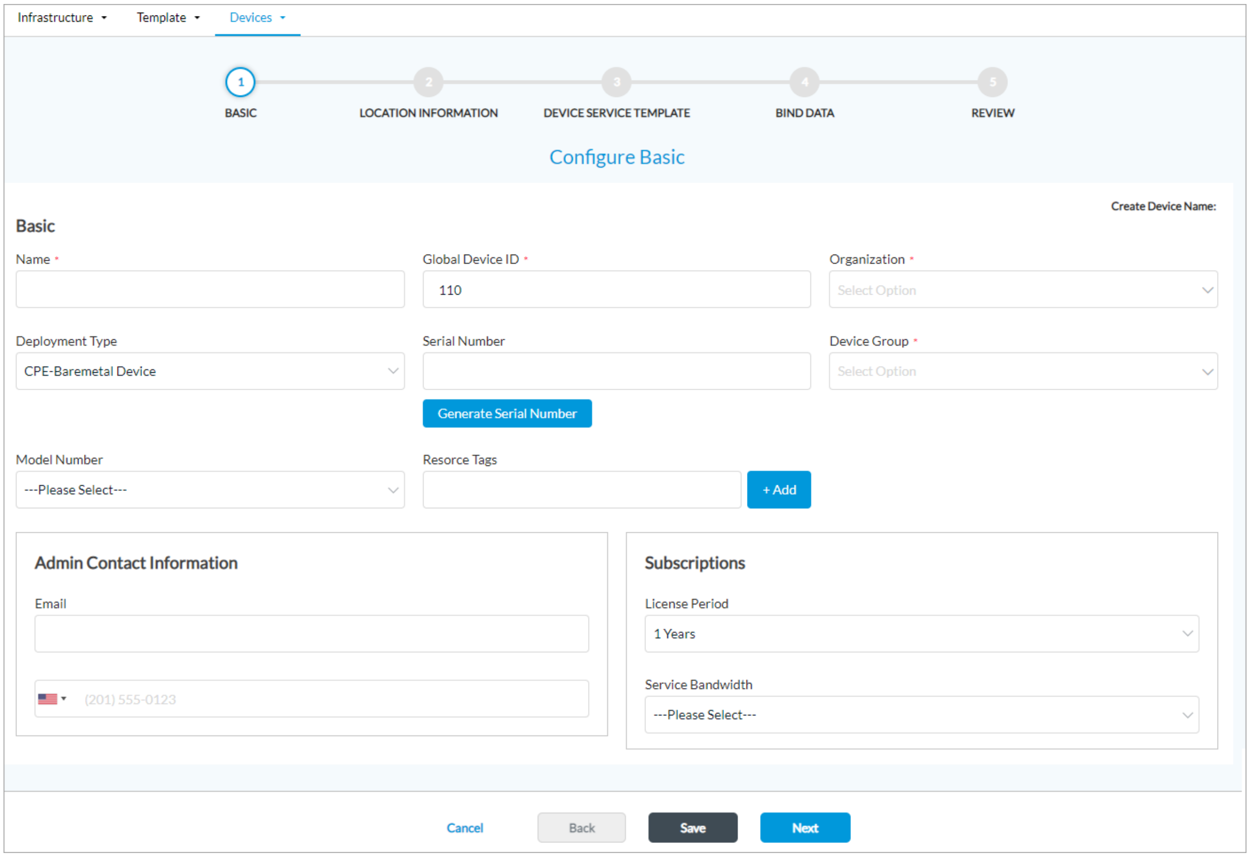
TENANT	CATEGORY	TEMPLATE
	No Post Staging Template Association Added	

4. Select the post-staging template you created in Add a Post-Staging Template from the Post-Staging Template drop-down list.
5. For information about configuring other parameters, see Create Devices and Device Groups.
6. Click OK.

Create a Device

To add a device:

1. In Director view:
    a. Select the Workflows tab in the top menu bar.
    b. Select Devices > Devices in the horizontal menu bar.
2. Click + Add. The Add Device Group window displays.



Configure Basic

Create Device Name:

Basic

Name *	Global Device ID *	Organization *
	110	Select Option
Deployment Type	Serial Number	Device Group *
CPE-Baremetal Device		Select Option
Model Number	Resorce Tags	
---Please Select---		

Admin Contact Information

Email:

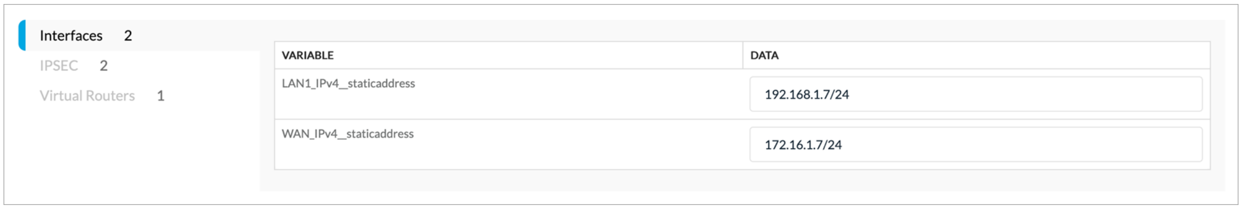
(201) 555-0123

Subscriptions

License Period: 1 Years

Service Bandwidth: ---Please Select---

3. In the Basic tab, select the Device group you configured in Create a Device Group.
4. Enter a Name, and Post Staging Template. Click Next. Enter the Location information as you did for the Controller. Click Next.
5. Select the Branch Tunnel and Peer Type and click Next.
6. Enter the Location Information and click Continue.
7. Under Bind Data, enter the WAN, LAN, and Gateway addresses with their prefixes.



VARIABLE	DATA
LAN1_IPv4__staticaddress	192.168.1.7/24
WAN_IPv4__staticaddress	172.16.1.7/24

8. In the Review tab, click Deploy.

Log on to the VOS branch device console and run the following script:

sudo ./staging.py -n 1234 -w 0 -s 172.16.1.2/24 -g 172.16.1.254 -c 172.16.1.1 -r Controller1-staging@Provider.com -l SDWAN-Branch@Provider.com

- Here:

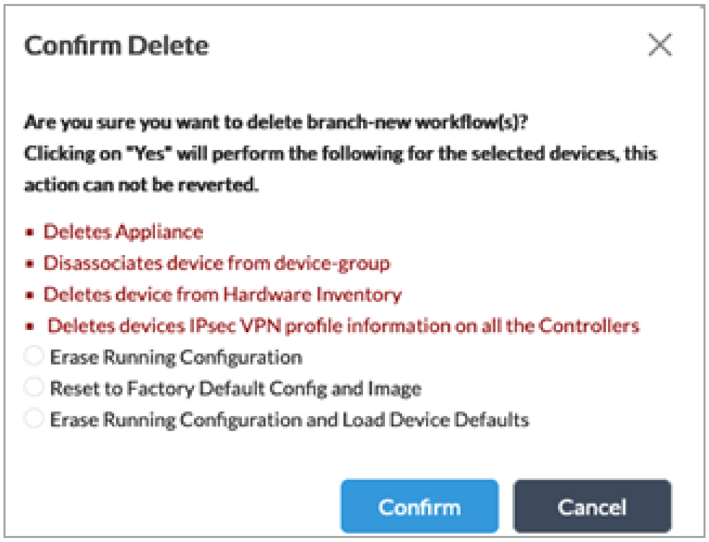
- -n is the serial number of the branch device
- -w is the WLAN interface. For example, vni-0/0.0
- -s is the IP address with prefix of the WLAN interface
- -g is the IP address of the WAN gateway
- -c is the WAN IP address of the controller
- -r is the remote ID of the controller
- -l is the local ID of the branch

Run this script for additional branch devices, as required.

Delete a Device

To delete an SD-WAN branch device:

1. In Director view, select Workflows > Devices.
2. Select the device to delete and click Delete. The following message displays.



Confirm Delete

Are you sure you want to delete branch-new workflow(s)?
Clicking on "Yes" will perform the following for the selected devices, this action can not be reverted.

- Deletes Appliance
- Disassociates device from device-group
- Deletes device from Hardware Inventory
- Deletes devices IPsec VPN profile information on all the Controllers

○ Erase Running Configuration
○ Reset to Factory Default Config and Image
○ Erase Running Configuration and Load Device Defaults

3. Click Confirm. When you delete a device, communications between the Director and the deleted device are disabled and you cannot push policies to that device. Essentially, you cannot manage that device using Director, unless you redeploy if from an existing configuration backup.

Post-Installation Configurations

After installing the headend, configure the following:

Configure NTP Servers

To configure NTP servers for time synchronization using CLI command, issue the following CLI commands on each headend node:

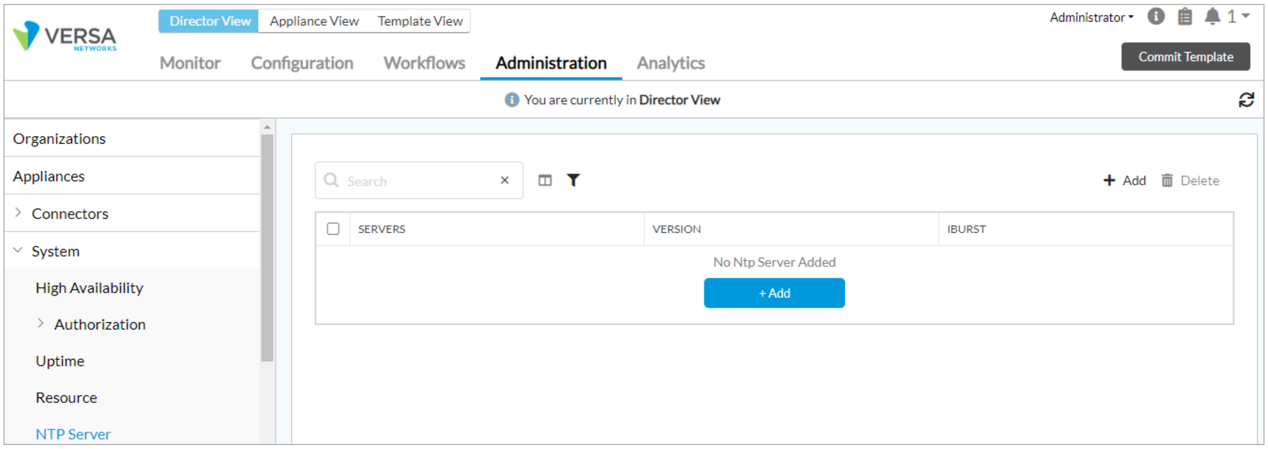
1. To set the timezone, Issue the **sudo timedatectl set-timezone** CLI command. For example:

   ```
   sudo timedatectl set-timezone America/Los_Angeles
   ```

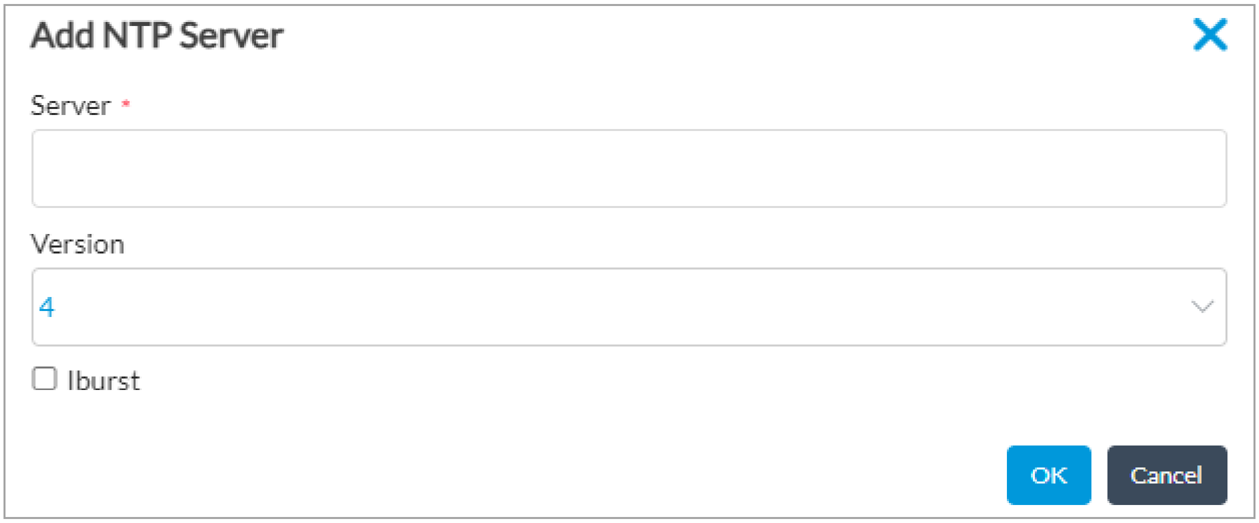
2. To verify time synchronization, issue the **timedatectl** CLI command.
3. To update the time manually from Director or VOS CLI, issue the **request system set date-time** CLI command.
4. To edit time synchronization, issue the following CLI command:

   ```
   sudo nano /etc/ntp/ntp.servers
   server first.ntp.server.local
   server second.ntp.server.local
   server third.ntp.server.local
   ```

5. To verify, issue the **ntpq -pn** CLI command.
6. To configure NTP servers using Director UI:
7. In Director view, select the Administration tab in the top menu bar.
8. Select System > NTP Server in the left menu bar.



9. Click the + Add icon. In the Add NTP Server popup window, enter information for the following fields.



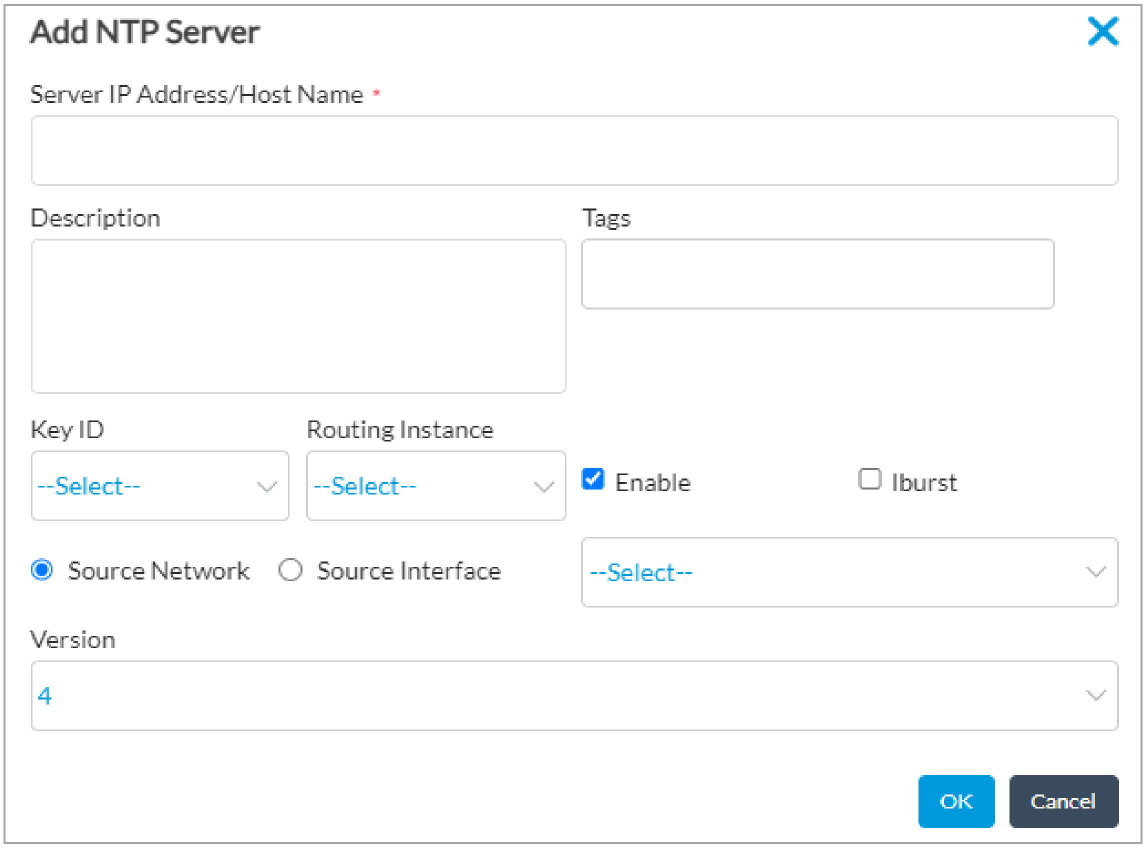
Server *

Version: 4

□ Iburst

Field	Description
Server	Enter a name for the server.
Version	Enter the version NTP running on the server.
iburst	Click to enable iburst on the server. Using iburst improves the time required for initial synchronization. With iburst, when the NTP server is unreachable, a burst of eight packets is sent instead of the usual one packet.

10. Click OK.
11. To manage the time settings on VOS devices:
12. In Director view, select the Configuration tab in the top menu bar.
13. Select Templates > Device Templates. Select the branch template you created in Add a Post-Staging Template.
14. Select Others > System > Time & Date > Time Settings in the left menu.
15. Click the Edit icon. The Edit Time Settings window displays. For more information, see Configure Time Settings.
16. Under NTP Servers, click the **+** icon to add an NTP server. In the Add NTP Server popup window, enter information for the following fields.



Add NTP Server

Server IP Address/Host Name *

Description

Tags

Key ID: --Select--

Routing Instance: --Select--

☑ Enable

□ Iburst

● Source Network ○ Source Interface --Select--

Version: 4

Field	Description
Server IP Address/Host Name (Required)	Enter the IP address or host name of the NTP server.
Description	Enter a text description the server.
Key ID	Select the ID of the authentication key. For more information, see Configure an Authentication Key ID, below.
Routing Instance	Select the routing instance to use to reach the NTP server.
Source Network Source Interface	Click to select either the network or interface to use to reach the NTP server.
Version	Select the version of the NTP server. The current version is 4, which is compatible with version 3.

Field	Description
Enable	Click to activate the NTP server.
iburst	Click to enable iburst on the server. Using iburst improves the time required for initial synchronization. With iburst, when the NTP server is unreachable, a burst of eight packets is sent instead of the usual one packet.

17. Click OK.
18. To configure time setting for each VOS device:
19. In Director view, select the Configuration tab in the top menu bar.
20. Select Devices > Devices in the horizontal menu.
21. Select the device you want to configure.
22. Repeat the steps to manage time settings on VOS devices.

Secure Management and Control Plane Ports

Use the following IP table rules to secure host ports on Versa headend.

1. To secure the Controller:

```
sudo iptables -A INPUT -s ip-address -j ACCEPT

sudo iptables -A INPUT -m state –state ESTABLISHED,RELATED -j ACCEPT
sudo iptables -P OUTPUT ACCEPT
sudo iptables -P FORWARD DROP
```

```
sudo iptables -P INPUT DROP

sudo iptables -A INPUT -s ip-address-of-ssh-source -p tcp -m tcp –dport 22 -j ACCEPT

root@Controller-1:~# iptables-save > /opt/versa/etc/rules.v4
root@Controller-1:~# echo -e  “#Restore iptables  rules\niptables-restore < /opt/versa/etc/rules.v4”
>>
/opt/versa/scripts/setup_versa_env.sh
```

2. To secure Director:

```
sudo iptables -A INPUT -s ip-address -p tcp -m tcp --dport 9182 -j ACCEPT
sudo iptables -A INPUT -s ip-address -p tcp -m tcp --dport 9183 -j ACCEPT
sudo iptables -A INPUT -s ip-address -p tcp -m tcp --dport 20514 -j ACCEPT

sudo iptables -A INPUT -s 127.0.0.1 -j ACCEPT

sudo iptables -A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
sudo iptables -A INPUT -p tcp -m tcp --dport 8443 -j ACCEPT

sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
sudo iptables -P OUTPUT ACCEPT
sudo iptables -P FORWARD DROP
sudo iptables -P INPUT DROP
sudo iptables -A INPUT -s ip-address-of-ssh-source -p tcp -m tcp --dport 22 -j ACCEPT

root@director1:~# iptables-save > /etc/iptables/rules.v4
```

3. To secure Analytics:

```
sudo iptables -A INPUT -s ip-address -p tcp -m tcp --dport 8443 -j ACCEPT

sudo iptables -A INPUT -s cross-connect-ip-address -j ACCEPT

sudo iptables -A INPUT -p tcp -m tcp --dport 1234 -j ACCEPT
sudo iptables -A INPUT -p udp --dport 123 -j ACCEPT

sudo iptables -A INPUT -p icmp --icmp-type 8 -s  <controller north ip-address>  -j ACCEPT

sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
sudo iptables -P OUTPUT ACCEPT
sudo iptables -P FORWARD DROP
sudo iptables -P INPUT DROP

iptables-save > /opt/versa/etc/rules.v4

echo -e  "#Restore iptables  rules\niptables-restore < /opt/versa/etc/rules.v4" >> /etc/init.d/versa-analytics
```

Disable Eth0 on Devices

To disable eth0 interface of each controller and branch device, run the following CLI command:

```
sudo sed -I ‘s/auto eth0/manual eth0/g’ /etc/network/interfaces
```

Configure X.509 Certificate

For additional information on configuring X.509 certificates to use with IPsec authentication, see the following articles:

- Configure CSR Objects
- Configure CA Certificates, Key File, and CA Chains
- Configure Certificate Servers

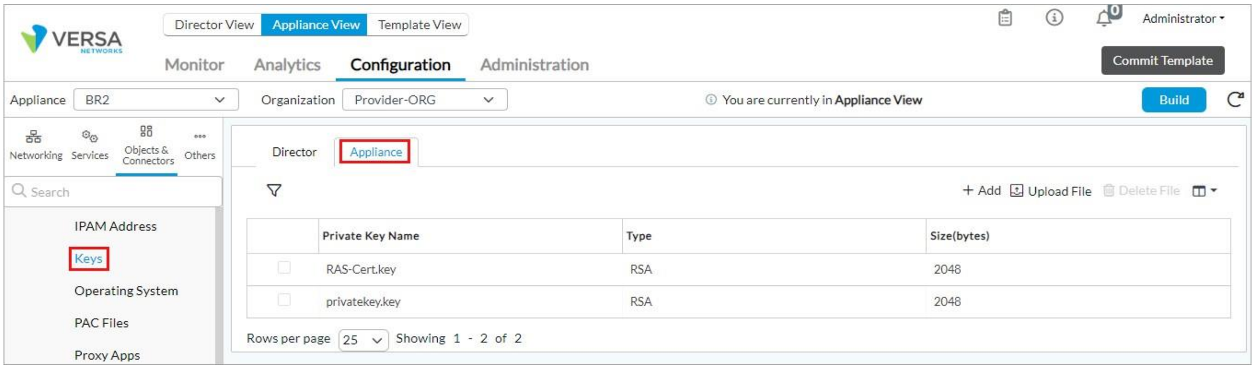
It is recommended to use a certificate server to handle automatic enrollment of IPsec certificates. To manually set up X.509 certificates for IPSec authentication, you do the following:

- Generate private key
- Generate certificate signing request (CSR)
- Sign the CSR with a trusted CA

- Import the CA chain
- Import the certificate

Generate a Private Key

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects > Custom Objects > Keys in the left menu bar.

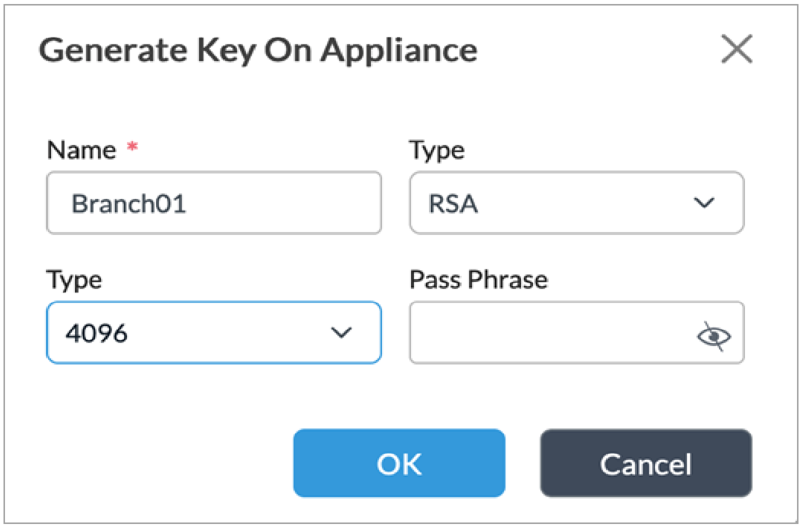


Appliance: BR2
Organization: Provider-ORG

	Private Key Name	Type	Size(bytes)
□	RAS-Cert.key	RSA	2048
□	privatekey.key	RSA	2048

Rows per page 25 Showing 1 - 2 of 2

4. Select the Appliance tab and click + Add. In the Generate Key on Appliance popup window, enter information for the following fields.


Generate Key On Appliance

Name *: Branch01
Type: RSA
Type: 4096
Pass Phrase:

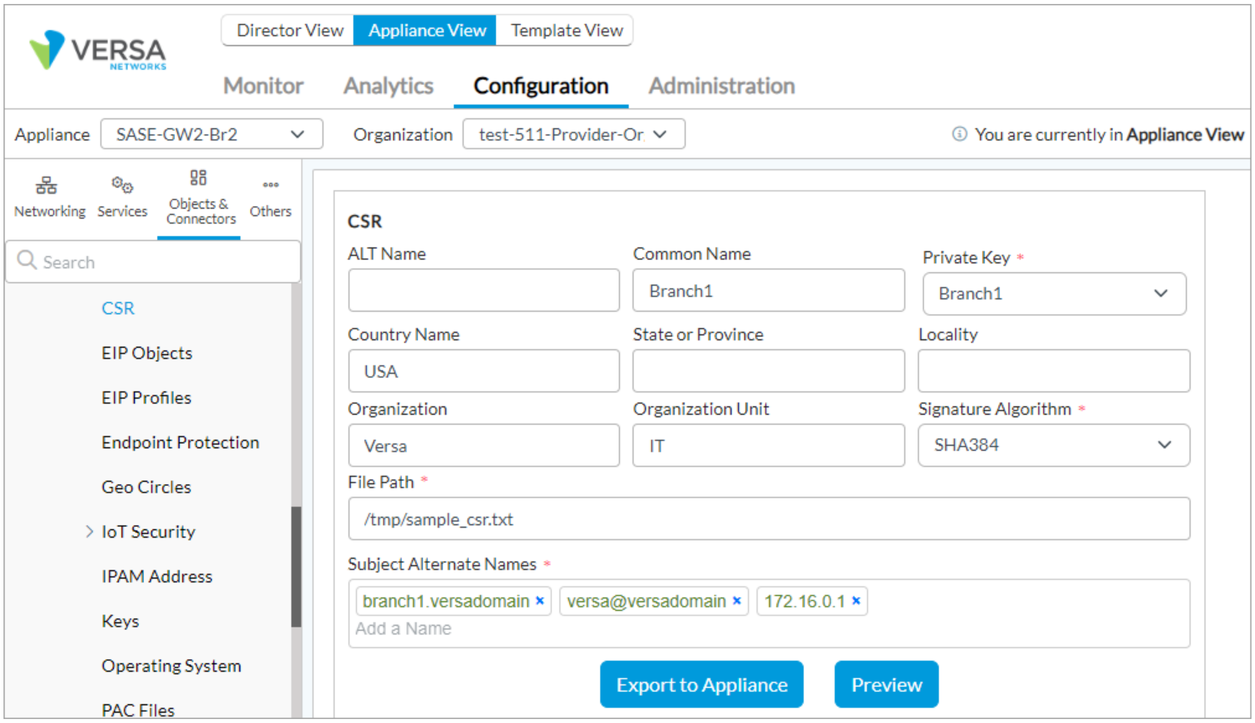
Field	Description

Name	Enter a name for the certificate key.
Type	Select the encryption type, RSA or ECDSA, to use to securely encode and decode the information.
Size	Enter the RSA key size. For RSA select 2048 or 4096 for RSA. For ECDSA select 256, 384, or 521 for ECDSA. For CSfC compliance, use RSA 4096 and ECDSA 384 or 521.
Pass Phrase	Enter the pass-phrase key, or password, to use to encrypt the file that contains the RSA key.

5. Click OK.

Generate a CSR

1. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliances in the left menu bar.
    c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects > Custom Objects > CSR in the left menu bar.



Appliance: SASE-GW2-Br2

Organization: test-511-Provider-Or

CSR

ALT Name:	Common Name: Branch1	Private Key *: Branch1
Country Name: USA	State or Province:	Locality:
Organization: Versa	Organization Unit: IT	Signature Algorithm *: SHA384

File Path *: /tmp/sample_csr.txt

Subject Alternate Names *: branch1.versadomain × versa@versadomain × 172.16.0.1 ×

4. In the CSR pane, enter information for the following fields.

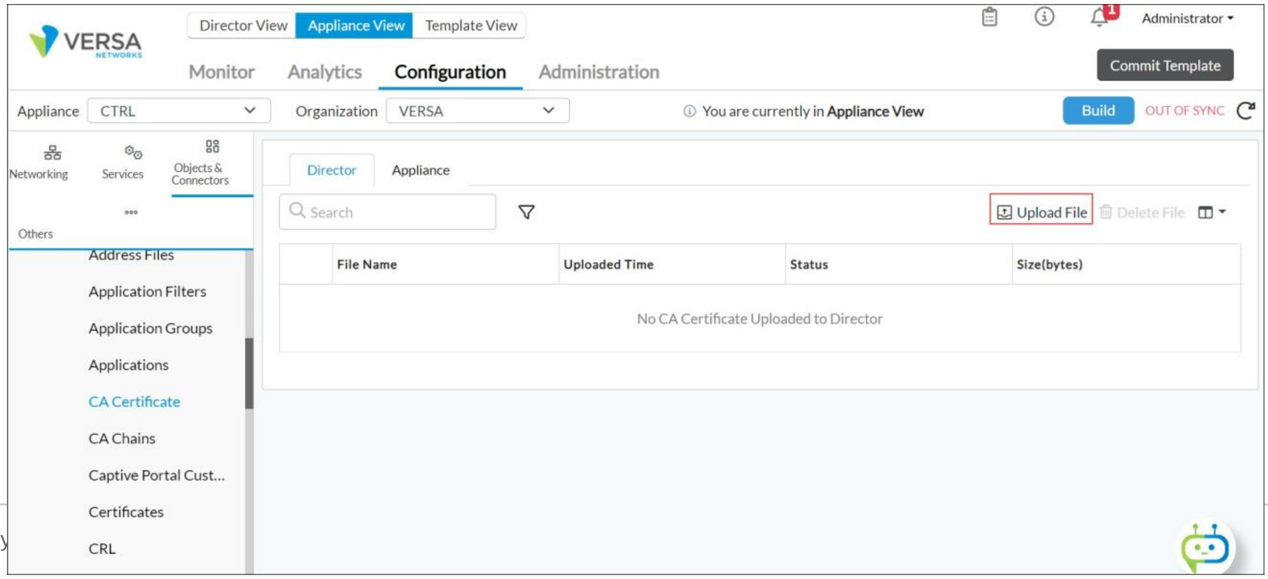
Field	Description
ALT Name	Enter the alternative name for the domain name.
Common Name	Enter the name of the certificate. The name is an identity that also you also must configure on the certificate authority server. Both names must match so that the CA server issue the certificate.
Private Key (Required)	Select the private key to access secured traffic using a certificate. For more information, see Create a Private Key for a CA Certificate.
Country Name State or Province Locality Organization Organization Unit	Enter information about the location of the certificate server and the organization to which it belongs.

Field	Description
Signature Algorithm (Required)	Select SHA-256 or SHA-384. For CSfC, select SHA-384.
File Path	Enter the path on the VOS device where you want to save the generated CSR file. When you click Export to Appliance, the CSR certificate is exported to this directory.
Subject Alternate Names (Required)	Enter the subject alternative names (SANs) to be secured by the certificate. These can be FQDNs, IP addresses, or email addresses. You can enter a maximum of 20 SANs.

5. Click Export to Appliance to export the CSR certificate to the VOS device directory specified in File Path field. Retrieve this file and submit a request to a Certificate Authority to sign. Before you import the signed certificate, you must import the CA chain.

Import CA Chain

1. In the Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Devices > Devices in the horizontal menu bar.
   c. Select a device in the dashboard. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects > Custom Objects > CA Certificate in the left menu bar.



Appliance: CTRL

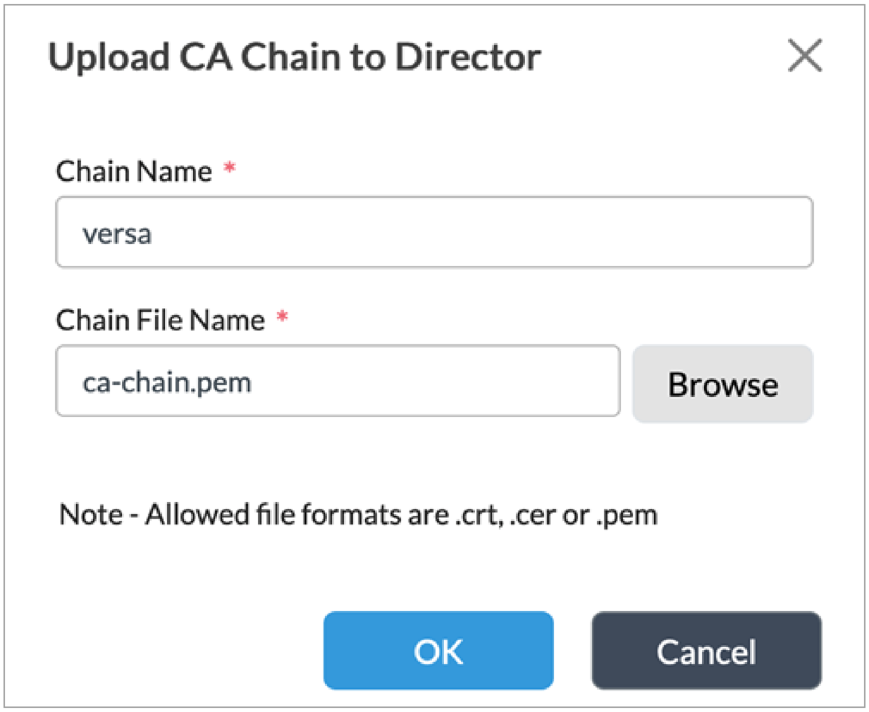
Organization: VERSA

You are currently in Appliance View

File Name	Uploaded Time	Status	Size(bytes)

No CA Certificate Uploaded to Director

4. In the Director tab, click the Upload File icon to upload a CA certificate file to the Director node. The Upload CA Certificate to Director popup window displays.



Upload CA Chain to Director

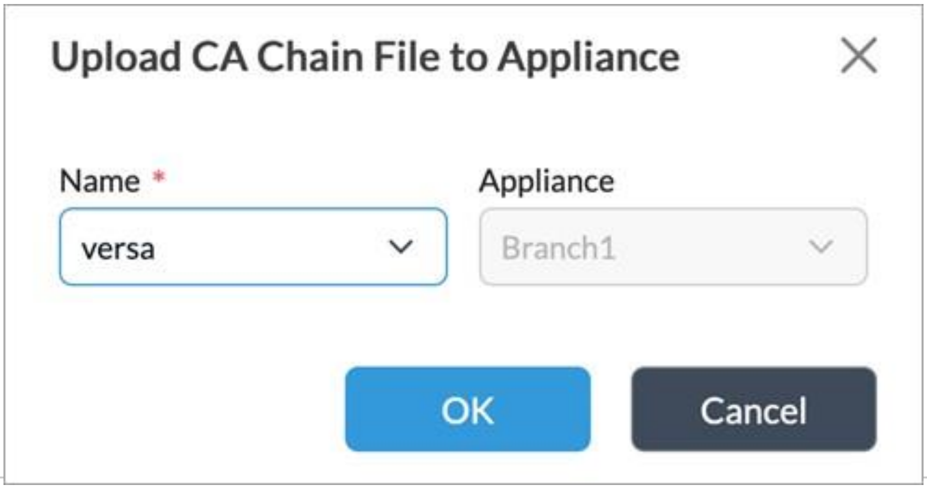
Chain Name *: versa

Chain File Name *: ca-chain.pem

Note - Allowed file formats are .crt, .cer or .pem

5. Enter a name for the CA chain.
6. Click Browse, and then select the CA certificate file to upload to the Director node. The supported file formats are.crt, .cer or .pem. The CA chain file must contain the trusted root and all intermediate CAs, starting with the root followed by each subordinate CA.
7. Select the Appliance tab.

8. Click the Upload File icon to upload a CA certificate file to the selected VOS device. The Upload CA Certificate to Appliance popup window displays.



Upload CA Chain File to Appliance

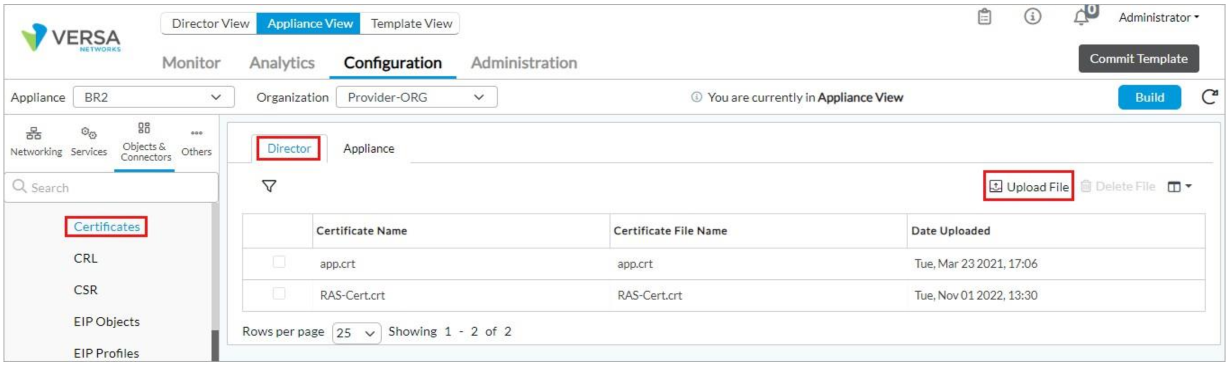
Name *: versa

Appliance: Branch1

9. In the Name field, select the CA certificate file to upload to the VOS device.
10. In the Appliance field, select the VOS device to upload the CA certificate file.

Import Signed Certificate

1. In the Director view:
    a. Select the Configuration tab in the top menu bar.
    b. Select Devices > Devices in the horizontal menu bar.
    c. Select a device in the dashboard. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects > Custom Objects > Certificates in the left menu bar.

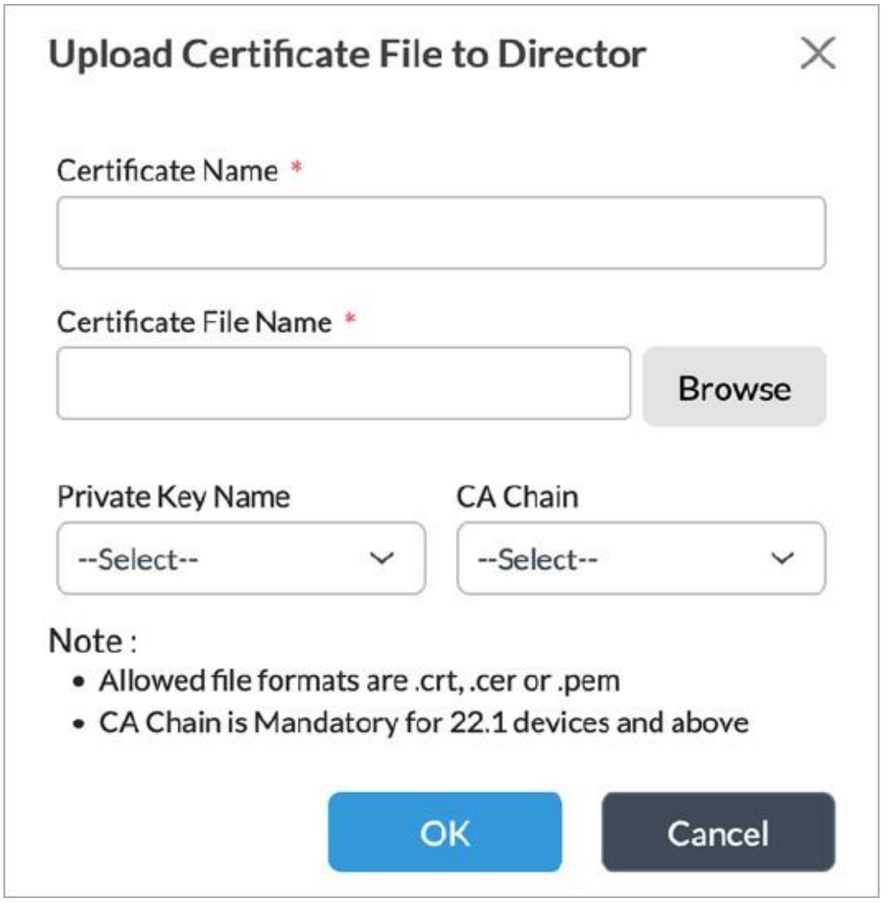


Appliance BR2 | Organization Provider-ORG | You are currently in **Appliance View**

	Certificate Name	Certificate File Name	Date Uploaded
□	app.crt	app.crt	Tue, Mar 23 2021, 17:06
□	RAS-Cert.crt	RAS-Cert.crt	Tue, Nov 01 2022, 13:30

Rows per page 25 Showing 1 - 2 of 2

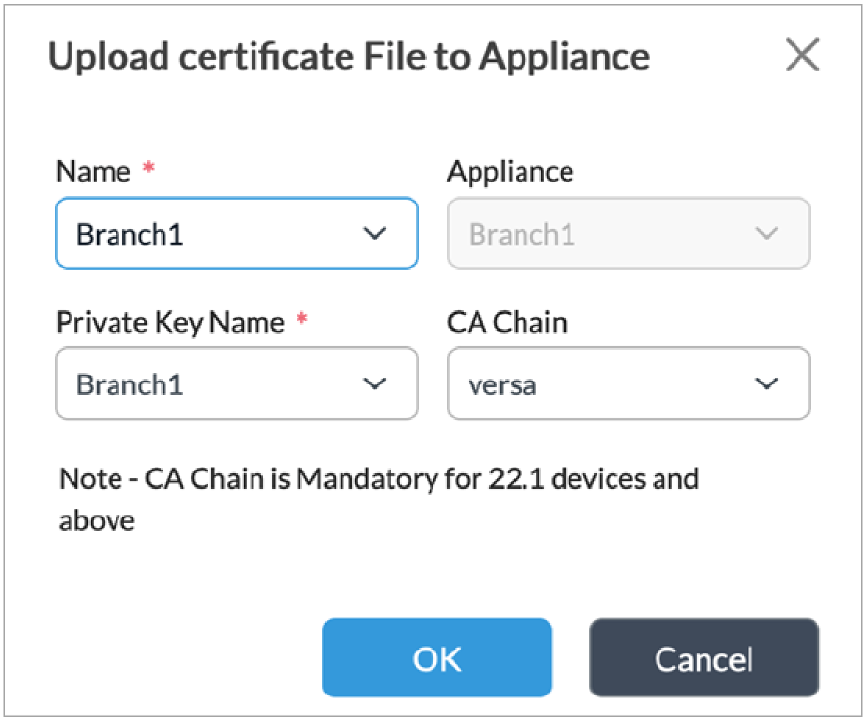
4. In the Director tab, click the Upload File icon to upload a CA certificate file to the Director node. The Upload Certificate File to Director popup window displays.



Note :

- Allowed file formats are .crt, .cer or .pem
- CA Chain is Mandatory for 22.1 devices and above

5. Enter a name for the certificate in the Certificate Name field.
6. Click Browse, and then select the certificate file to upload to the Director node.
7. Select a CA chain. The import fails if you do not select a CA chain.
8. Click OK.
9. Select the Appliance tab.
10. Click the Upload File icon to upload a CA certificate file to the selected VOS device. The Upload CA Certificate to Appliance popup window displays.



Upload certificate File to Appliance

Name * Branch1

Appliance Branch1

Private Key Name * Branch1

CA Chain versa

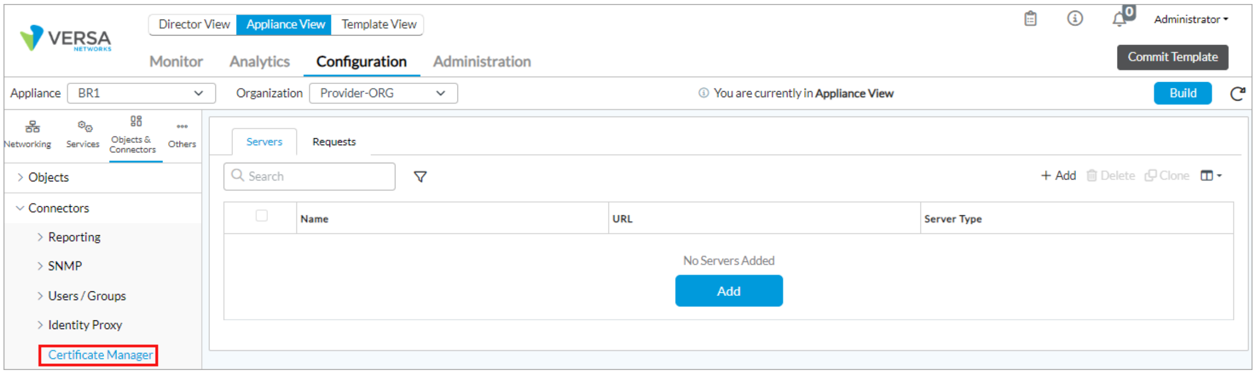
Note - CA Chain is Mandatory for 22.1 devices and above

11. Select a name for the certificate file.
12. Select the private key.
13. Select CA chain. The import fails if you do not select a CA chain.
14. Click OK. The certificate is now ready for use with an IPsec VPN profile.

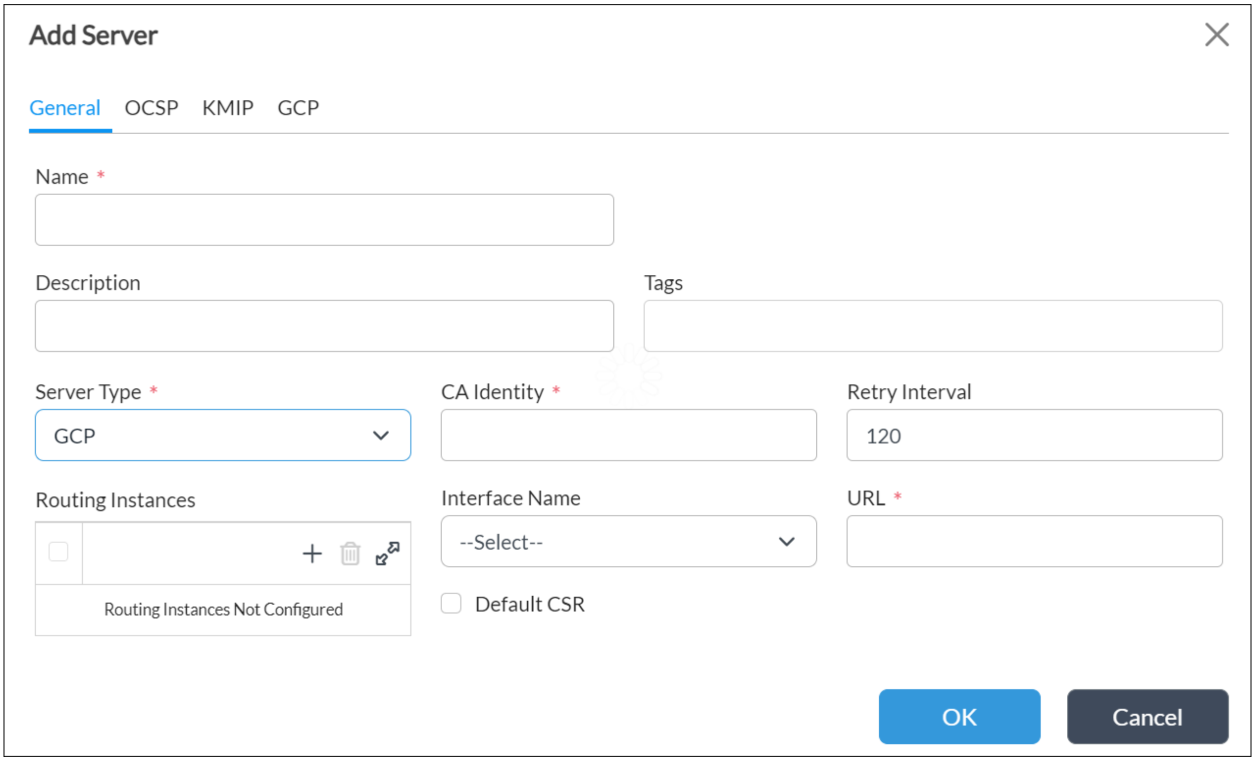
Configure Certificate Revocation Method

You must also configure a certificate revocation method:

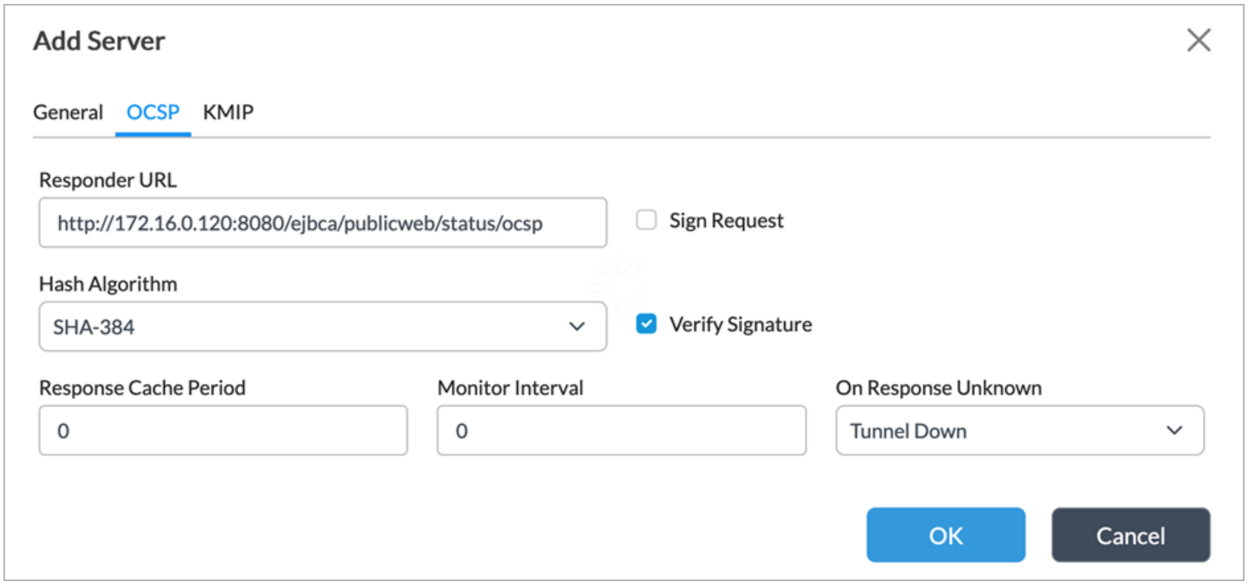
1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Devices > Devices in the horizontal menu bar.
   c. Select an organization in the left menu bar.
   d. Select a device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Connectors > Certificate Manager in the left menu bar.



4. Select the Servers tab in the horizontal menu bar, and then click + Add. In the Add Server popup window, select the General tab.



5. Enter a name, which must match the name of the CA chain you imported in Import CA Chain above.
6. Select Server Type as GCP.
7. Select CA Identity. If you are not using an automated certificate enrollment protocol, other values are ignored, but you must specify them to configure OCSP.
8. For information about configuring other parameters, see Configure Certificate Servers.
9. Select the OCSP tab.



Add Server

General OCSP KMIP

Responder URL: http://172.16.0.120:8080/ejbca/publicweb/status/ocsp

□ Sign Request

Hash Algorithm: SHA-384

☑ Verify Signature

Response Cache Period: 0

Monitor Interval: 0

On Response Unknown: Tunnel Down

10. Enter the responder URL and select the hash algorithm.
11. Select Tunnel Down from the On Response Unknown field.
12. For information about configuring other parameters, see Configure Certificate Servers.
13. Click OK. Note that each CA chain supports only one OCSP responder. Ensure that a delegate responder certificate is issued for each CA in the chain.

X.509 Certificate Validation

X.509 certificate validation checks occur on the following certificates during the following conditions:

- While importing CA certificates into the trust store:
  - BasicConstraints flag is present and set to True.
  - Intermediate CA certificates are properly chained.
- While Importing end-entity certificates into the trust store:
  - Valid CA chain is installed and terminated at the root CA.
  - CA certificates contain BasicConstraints flag and is set to True.
- During IPsec session establishment:
  - Can verify peer certificate signatures up to the root of trust.
  - Peer certificates are not expired.
  - OCSP response indicates a non-revoked peer certificate, and OCSP responder certificate is valid and contains the OCSP signing extended key usage.
  - Peer certificate chains contain EC certificates use named elliptic curves
  - Peer reference identifier matches the expected identifier.

Configure IPsec

You can create additional tunnels from Versa Director. You can also create additional staging and post-staging VPN profiles or configure VOS for a site-to-site tunnel or remote access server. For more information, see Configure IPsec VPN Profiles. Note that the NIAP-evaluated configuration supports only tunnel mode.

When you configure VPN profiles, follow these guidelines to ensure compliance with the evaluated configuration:

- Use IKEv2 for CSfC conformance, though IKEv1 is also supported.
- Use RSA or ECDSA certificates for authentication with IKEv2 or IKEv1. For more information about configuring X.509 certificates to use with IPsec, see Configure X.509 Certificate above.
- The configuration evaluation by NIAP does not support pre-shared keys.

- The evaluated configuration supports only the following encryption algorithms and hashes. FIPS mode supports only single transforms and does not support multiple transforms. The values highlighted in bold font face are required for CSfC. Note that setting an IKE encryption cipher that is weaker than the strength of the ESP cipher is not supported.
    - AES128-SHA1
    - AES128-SHA256
    - AES128-SHA384
    - AES128-SHA512
    - AES256-SHA1
    - AES256-SHA256
    - **AES256-SHA384**
    - **AES256-SHA512**
    - **AES256-GCM**
- You can use the following DH groups:
    - Diffie-Hellman Group 19—256-bit elliptic curve
    - **Diffie-Hellman Group 20—384-bit elliptic curve**
- Set the Revocation Check field to OCSP.
- Set the Authentication Type field to Certificate.
- Supported peer identifier types are email, FQDN, and IP address (CN and SAN).
- Set IKE rekey time between 2 minutes and 24 hours. The default value is 8 hours (28800 seconds).
- The evaluated configuration supports the following IPsec transforms. The values in bold are required for CSfC:
    - ESP-AES128-SHA1
    - ESP-AES128-SHA256
    - ESP-AES128-SHA384
    - ESP-AES128-SHA512
    - ESP-AES256-SHA1
    - ESP-AES256-SHA256

    - **ESP-AES256-SHA384**
    - **ESP-AES256-SHA512**
    - **ESP-AES256-GCM**
- You can use the following DH groups:
    - Diffie-Hellman Group 19—256-bit elliptic curve
    - **Diffie-Hellman Group 20—384-bit elliptic curve**
- IPsec rekey time between 2 minutes and 24 hours. The default value is 8 hours (28800 seconds).

Use following configure mode commands to set the certificate parameters for authentication:

> **set orgs org-services** *Organization* **ipsec vpn-profile** *VPN profile* **local-auth-info auth-type certificate ca-chain** *CA chain*
> **cert-domain tenant id-type** *IP address|email|FQDN* **id-string** *local ID* **cert-name** *local cert*

> **set orgs org-services** *Organization* **ipsec vpn-profile** *VPN profile* **per-auth-info auth-type certificate ca-chain** *CA chain*
> **cert-domain tenant id-type** *IP address|email|FQDN* **id-string** *peer ID*

VOS supports the construction of an SPD consisting of BYPASS (for example, no encryption), DISCARD (for example, drop the packet), and PROTECT (for example, encrypt the packet) rules through a combination of IPsec SAs, IP forwarding rulesets and traffic filters. The packet processing algorithm is described as follows:

- A packet is received on an interface and is placed into an outbound queue for processing.
- If the packet does not violate any inspection policies or default firewall rules, the packet is matched against a set of rules in a top-down order until a match is found.
- If the packet matches a rule marked as Drop, the packet is immediately discarded.
- If the packet matches a rule marked as Permit, it is forwarded and transmitted from the destination interface. If the packet is not flagged by the IPsec VPN policy or is not part of an existing SA, the packet flows in plain text.
- If the packet matches an IPsec VPN policy, it is forwarded and encrypted according to the SA, if the packet matches an existing SA. If the packet does not match an existing SA, a new one is established and upon completion of the SA, the packet is forwarded encrypted.
- If the packet does not match any of the configured rules, it is dropped by a default deny rule

To define a security policy that protects data traffic, configure appropriate virtual routers and define static routes for IP addresses or subnets that can be accessed through the VPN Tunnel.

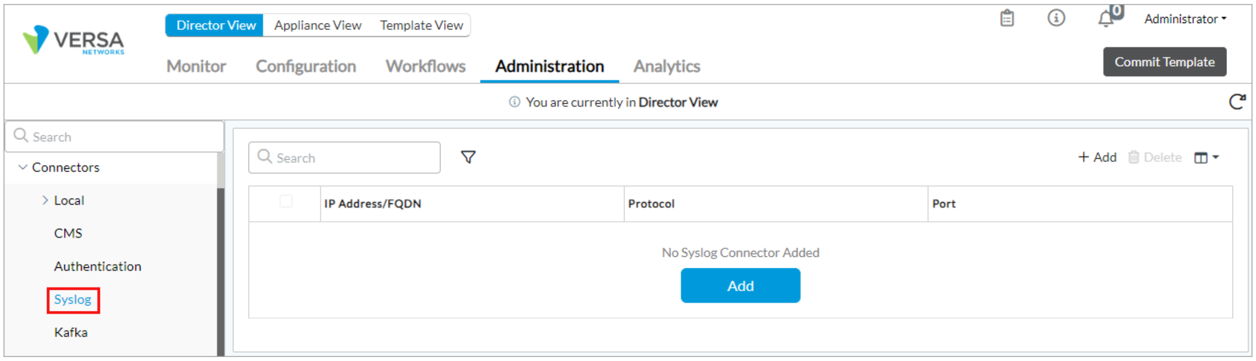
To allow certain traffic between hosts connected to the VPN, configure granular NGFW access policy rules. To reject certain traffic destined for the VPN, apply an NGFW access policy rule with Reject action to or from hosts, networks, interfaces, or ports that must not be allowed. For more information, see Configure NGFW.

To bypass the tunnel, use virtual routers and define static routes to route traffic to interfaces or networks that are not associated with VPN tunnels.

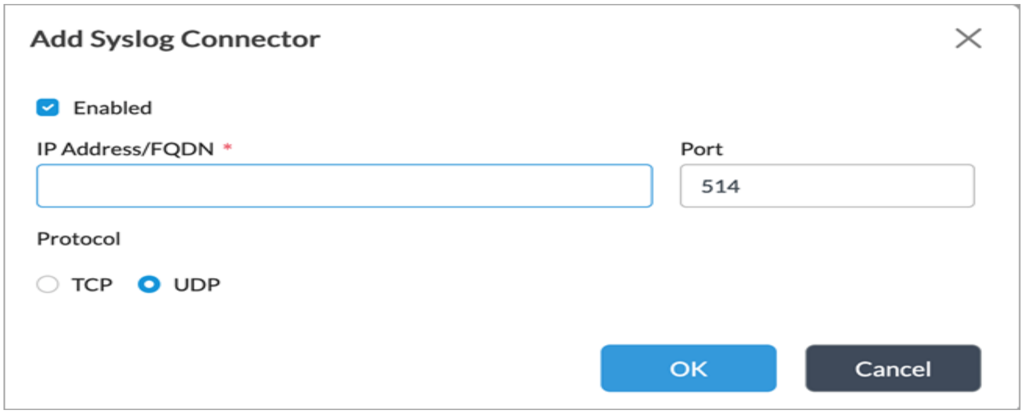
Configure Syslog Server

To configure the syslog server address:

1. In Director view, select the Administration tab in the top menu bar.
2. In the left navigation bar, select Connectors > Syslog.



3. Click Add. In the Add Syslog Connector popup window, enter the following information.



Add Syslog Connector

☑ Enabled

IP Address/FQDN *

Port: 514

Protocol: ○ TCP ● UDP

Field	Description
Enabled	Check to enable the syslog connector.
IP Address/ FQDN	Enter the IP address or the fully qualified domain name of the syslog server.
Port	Enter the port number used to connect to the syslog server. The default port number is 514.
Protocol	Select TCP or UDP as the protocol for the syslog connector.

4. Click OK.

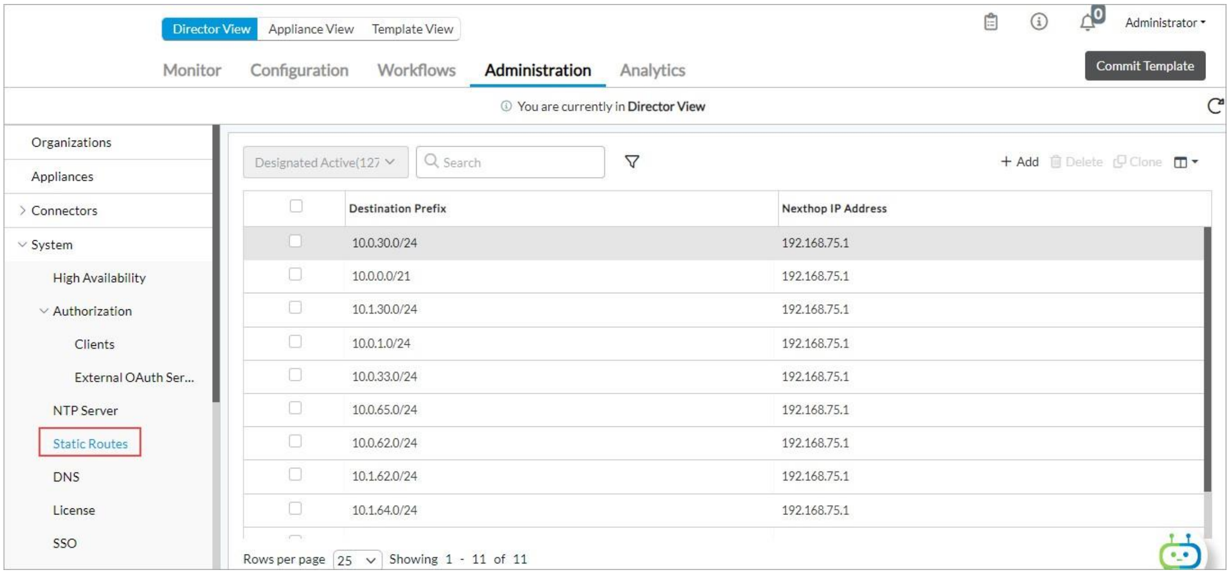
To define a static route for traffic to be diverted through the Controller IPsec tunnel, define a static route as defined in the following sections. You must use the defined routes direct both NTP and Syslog traffic from each TOE component through the associated IPSec tunnel(s) to the management server endpoints.

To configure audit and system events so that they are captured by the syslog daemon and forwarded externally, run the **set system enable-syslog-event-logging true** CLI command on the Director CLI.

Add a Static Route

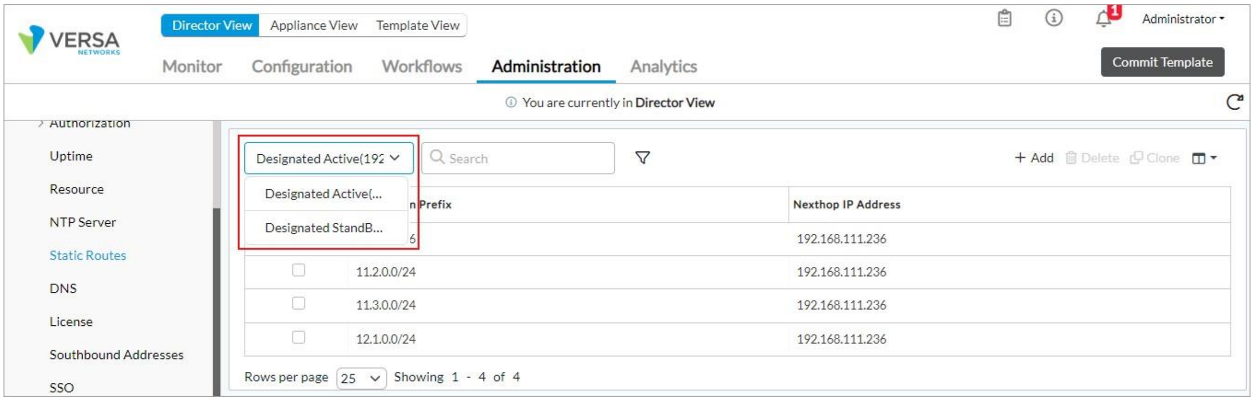
Define a static route on the active Versa Director to provide an exit from the device when no other routes are available:

1. In the active Director node, select the Administration tab in the top menu bar.
2. In the left navigation bar, select System > Static Routes.



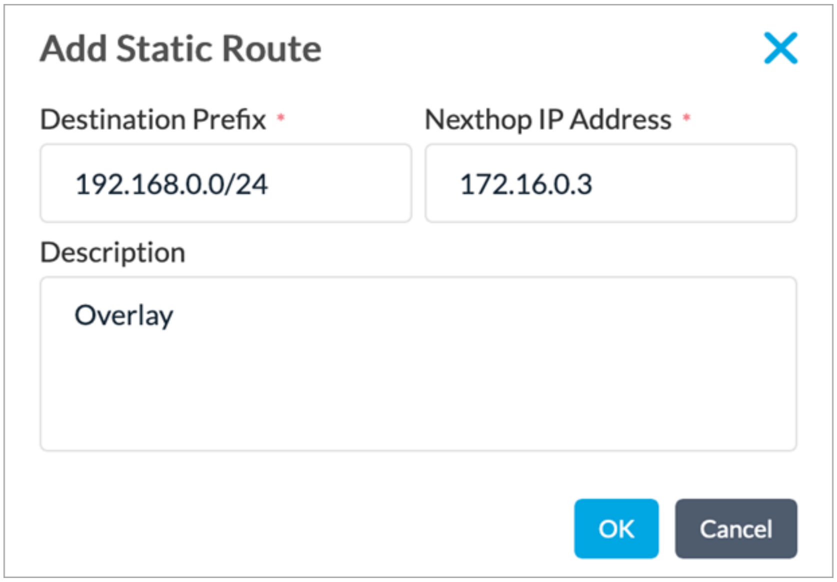
Destination Prefix	Nexthop IP Address
10.0.30.0/24	192.168.75.1
10.0.0.0/21	192.168.75.1
10.1.30.0/24	192.168.75.1
10.0.1.0/24	192.168.75.1
10.0.33.0/24	192.168.75.1
10.0.65.0/24	192.168.75.1
10.0.62.0/24	192.168.75.1
10.1.62.0/24	192.168.75.1
10.1.64.0/24	192.168.75.1

3. Click the drop-down menu in the main pane, and then select a node.



n Prefix	Nexthop IP Address
6	192.168.111.236
11.2.0.0/24	192.168.111.236
11.3.0.0/24	192.168.111.236
12.1.0.0/24	192.168.111.236

4. Click the + Add icon. In the Add Static Route popup window, enter information for the following fields:



Add Static Route

Destination Prefix *: 192.168.0.0/24

Nexthop IP Address *: 172.16.0.3

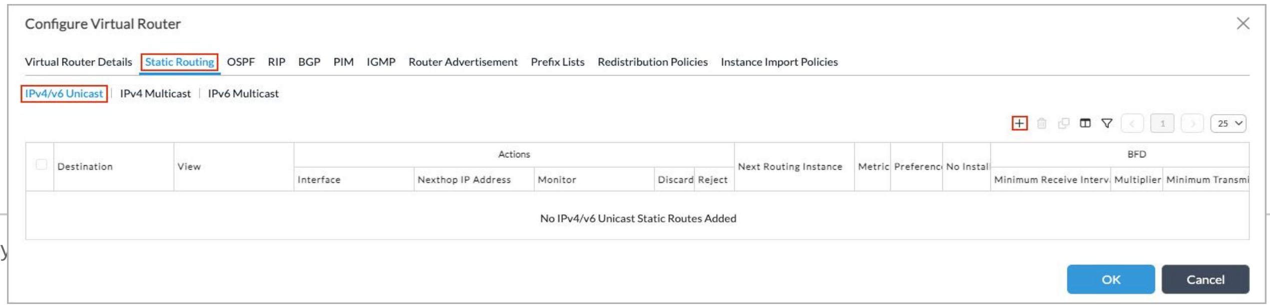
Description: Overlay

Field	Description
Destination Prefix	IP address and prefix that is reachable using the static route.
Next-Hop IP Address	IP address of the router or gateway to reach the destination.

5. Click OK.

Configure Static Routes

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select an appliance in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Virtual Routers in the left menu bar.
4. Click the + Add icon. The Configure Virtual Router popup window displays.
5. Select Static Routing in the horizontal menu bar in the Configure Virtual Router window.

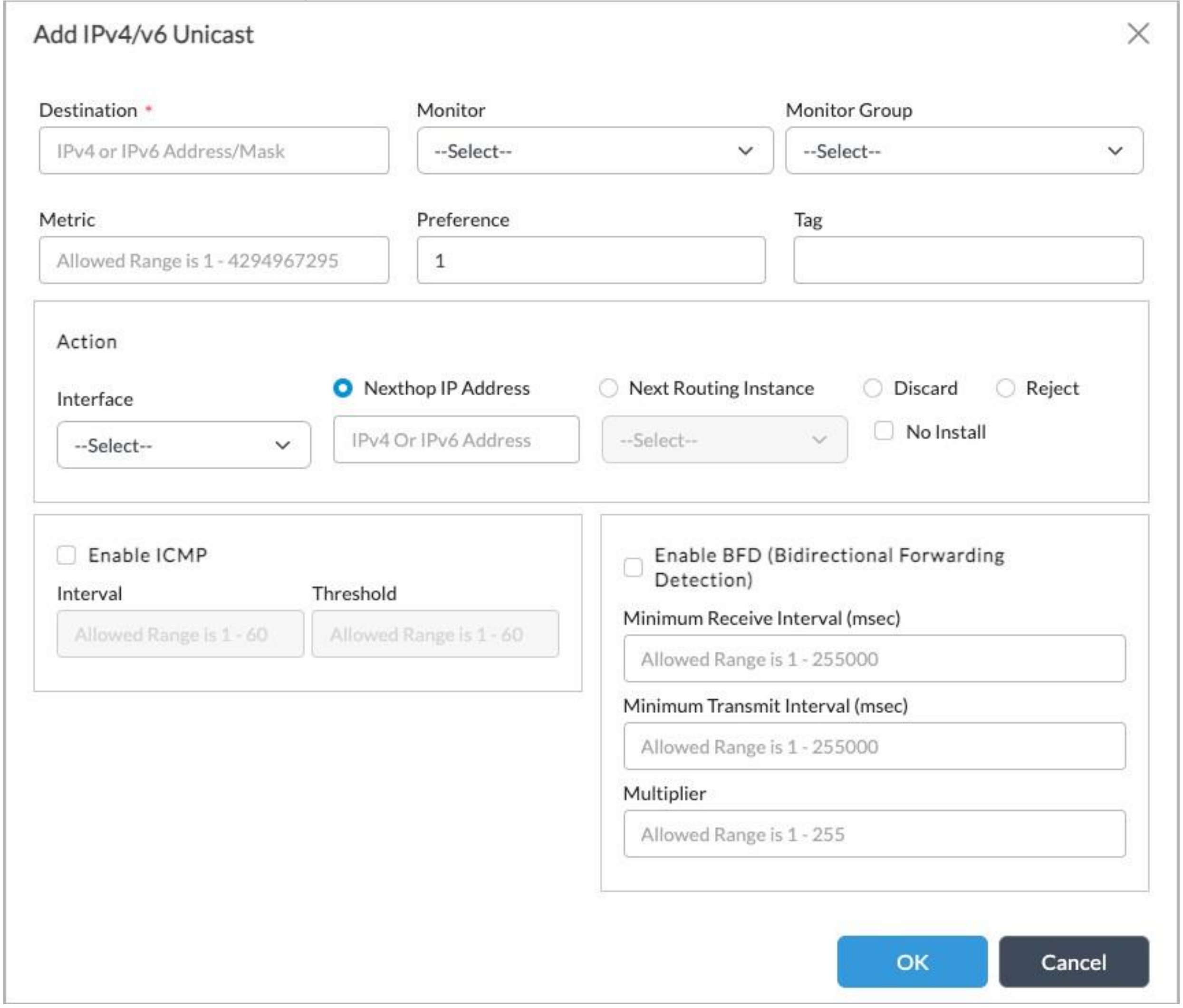


Configure Virtual Router

□	Destination	View	Actions					Next Routing Instance	Metric	Preferenc	No Install	BFD		
			Interface	Nexthop IP Address	Monitor	Discard	Reject					Minimum Receive Interv	Multiplier	Minimum Transmi

No IPv4/v6 Unicast Static Routes Added

6. To add an IPv4 or IPv6 unicast static route, select the IPv4/IPv6 Unicast tab and then click the + Add icon. Enter information for the following fields.



Add IPv4/v6 Unicast

Destination * IPv4 or IPv6 Address/Mask

Monitor --Select--

Monitor Group --Select--

Metric Allowed Range is 1 - 4294967295

Preference 1

Tag

Action

Interface --Select--

● Nexthop IP Address IPv4 Or IPv6 Address

○ Next Routing Instance --Select--

○ Discard

○ Reject

□ No Install

□ Enable ICMP

Interval Allowed Range is 1 - 60

Threshold Allowed Range is 1 - 60

□ Enable BFD (Bidirectional Forwarding Detection)

Minimum Receive Interval (msec) Allowed Range is 1 - 255000

Minimum Transmit Interval (msec) Allowed Range is 1 - 255000

Multiplier Allowed Range is 1 - 255

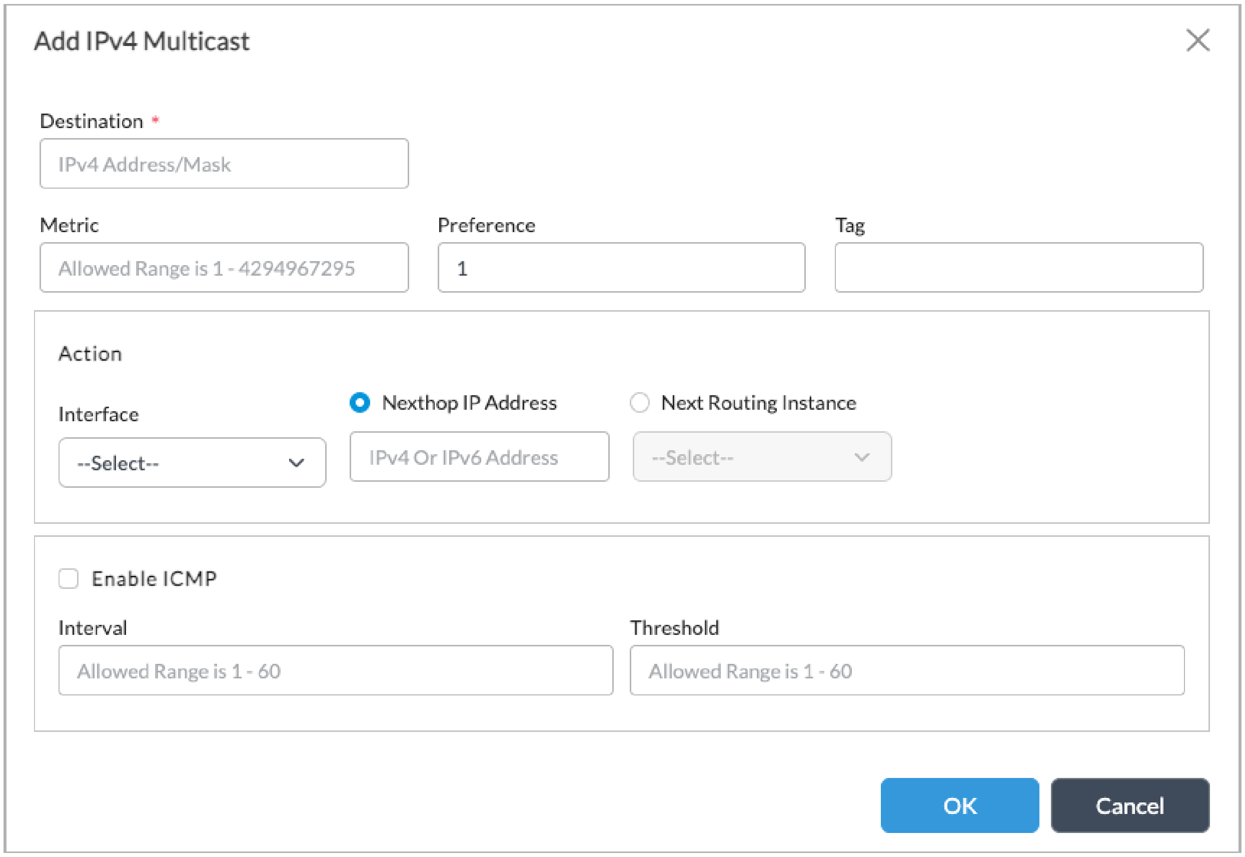
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Destination</td><td>Enter the destination IP address or network.</td></tr>
<tr><td>Action (Group of Fields)</td><td></td></tr>
<tr><td>◦ Next-Hop Interface</td><td>Select the next-hop interface towards the destination network.</td></tr>
<tr><td>◦ Next-Hop IP Address</td><td>Click to specify the IP address to use to reach the destination network.</td></tr>
<tr><td>◦ Next Routing Instance</td><td>Click to select the routing instance to use to reach the destination network.</td></tr>
<tr><td>◦ Discard</td><td>Install the route in both the control plane and the data plane. In the data plane, the traffic is installed with the Discard option.
For example, if there is a static route to 172.16.0.0/16 for which the Discard option is selected, a more specific route to 172.16.1.0/24 for which the Forward action is selected, and a default route (0.0.0.0/0), the data plane actions are as follows:
<table>
<tr><th>Route</th><th>Data Plane Action</th></tr>
<tr><td>0.0.0.0/0 (default forwarding)</td><td>Forward</td></tr>
<tr><td>172.16.0.0/16</td><td>Discard</td></tr>
<tr><td>172.16.1.0/24</td><td>Forward</td></tr>
</table>
The following examples illustrate how packets are handled:
◦ A packet to 172.16.1.10 is forwarded to the next hop.
◦ A packet to 172.16.5.10 is silently dropped.
◦ A packet to 8.8.8.8 is forwarded through the default gateway next hop.</td></tr>
<tr><td>◦ Reject</td><td>Install the route in both the control plane and the data plane. In the data plane, the traffic is installed with the Reject option.
For example, if there is a static route to 172.16.0.0/16 for which the Reject option selected, a</td></tr>
</table>

<table>
<tr><td></td><td>more specific route to 172.16.1.0/24 for which the Forward action selected,and a default route (0.0.0.0/0), the data plane actions are as follows:
<table><tr><th>Route</th><th>Data Plane Action</th></tr><tr><td>0.0.0.0/0 (default forwarding)</td><td>Forward</td></tr><tr><td>172.16.0.0/16</td><td>Reject</td></tr><tr><td>172.16.1.0/24</td><td>Forward</td></tr></table>
The following examples illustrate how packets are handled:
◦ A packet to 172.16.1.10 is forwarded to the next hop.
◦ A packet to 172.16.5.10 is dropped, and an ICMP message is sent to the sender reporting that the destination is unreachable.
◦ A packet to 8.8.8.8 is forwarded through the default gateway next hop.</td></tr>
<tr><td>◦ No Install</td><td>Install the route in the control plane only, and do not install the route in the data plane.
For example, if there is a static route to 172.16.0.0/16 for which the No Install option selected and a default route (0.0.0.0/0), a packet destined to 172.16.0.10 is sent using the default route if the data plane has no matching routes that are longer.</td></tr>
<tr><td>Enable ICMP (Group of Fields)</td><td>Click to enable ICMP monitoring of the next hop configured for the static route. If the ICMP monitoring fails, the route is withdrawn from the routing table. Note that if you configure one or more of the Enable ICMP, Monitor, and Enable BFD fields simultaneously, and if any one of the monitors fails, the static route is withdrawn from the routing table.</td></tr>
<tr><td>◦ Interval</td><td>Enter the time interval between ICMP packets.
<i>Range:</i> 1 through 60 seconds</td></tr>
<tr><td>◦ Threshold</td><td>Enter the the number of ICMP probes to be missed before setting the state of the ICMP monitor as down and withdrawing the static route.
<i>Range:</i> 1 through 60</td></tr>
<tr><td>Metric</td><td>Enter the cost to reach the destination network. The metric is used to choose between multiple paths learned with the same routing protocol.
<i>Range:</i> 1 through 4294967295</td></tr>
</table>

Preference	Enter the administrative distance (AD) or route preference value of the static route. You can assign a preference for each route. The preference is used to choose between multiple paths learned from different routing protocols. *Range:* 1 through 255
Tag	Enter a tag for the static route.
Monitor	Select the name of a liveness detection monitor that must be up for the static route to become active. To configure a monitor, see Configure IP SLA Monitor Objects. Note that if you configure one or more of the Enable ICMP, Monitor, and Enable BFD fields simultaneously, and if any one of the monitors fails, the static route is withdrawn from the routing table.
Enable BFD (Group of Fields)	Click to enable Bidirectional Forwarding Detection monitoring of the next hop configured for the static route. If the BFD monitoring fails, the route is withdrawn from the routing table. Note that if you configure one or more of the Enable ICMP, Monitor, and Enable BFD fields simultaneously, and if any one of the monitors fails, the static route is withdrawn from the routing table.
◦ Minimum Receive Interval	Enter the minimum time interval to receive routes, in milliseconds. *Range:* 1 through 255000 milliseconds
◦ Multiplier	Enter the multiplier value to use to calculate the final minimum receive interval and minimum transmit interval. *Range:* 1 through 255
◦ Minimum Transmit Interval	Enter the time after which routes can be retransmitted, in milliseconds. *Range:* 1 through 255000 milliseconds

7. Click OK

8. To add an IPv4 multicast static route, select the IPv4 Multicast tab and then click the + Add icon. Enter information for the following fields.



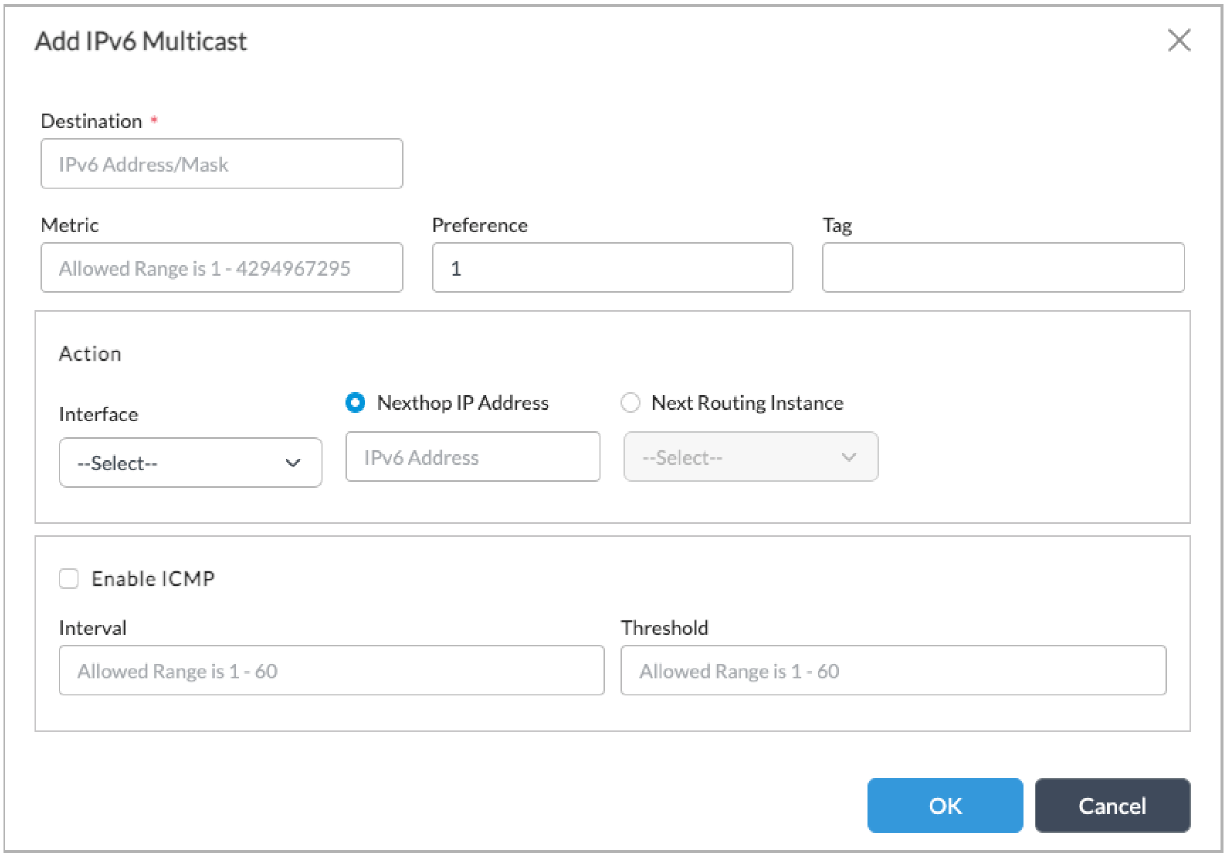
Preference: 1

● Nexthop IP Address

Field	Description
Destination	Enter the destination IP address or network.
Action (Group of Fields)	
◦ Interface	Select the interface towards the destination network.
◦ Next-Hop IP Address	Click to specify the IP address to use to reach the destination network.
◦ Next Routing Instance	Click to select the routing instance to use to reach the destination network.
Metric	Enter the cost to reach the destination network. The metric is used to choose between multiple paths learned with the same routing protocol. *Range:* 1 through 4294967295
Preference	Enter the preference value of the IPv4 route. *Range:* 1 through 255
Tag	Enter a tag for the IPv4 route.

9. Click OK.

10. To add an IPv6 multicast static route, select the IPv6 Multicast tab and then click the + Add icon. Enter information for the following fields.



Add IPv6 Multicast

Destination *

IPv6 Address/Mask

Metric: Allowed Range is 1 - 4294967295

Preference: 1

Tag

Action

Interface: --Select--

● Nexthop IP Address: IPv6 Address

○ Next Routing Instance: --Select--

□ Enable ICMP

Interval: Allowed Range is 1 - 60

Threshold: Allowed Range is 1 - 60

Field	Description
Destination	Enter the destination IP address or network.
Action (Group of Fields)	
◦ Interface	Select the interface towards the destination network.
◦ Next-Hop IP Address	Click to specify the IP address to use to reach the destination network.
◦ Next Routing Instance	Click to select the routing instance to use to reach the destination network.
Metric	Enter the cost to reach the destination network. The metric is used to choose between multiple paths learned with the same routing protocol. *Range:* 1 through 4294967295

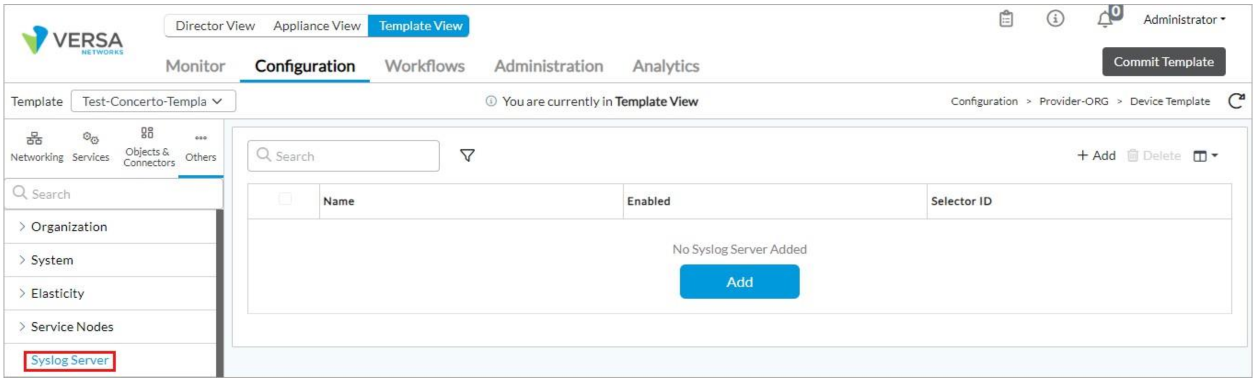
Field	Description
Preference	Enter the preference value of the IPv6 route. *Range:* 1 through 255
Tag	Enter a tag for the IPv6 route.

11. Click OK. The static route displays in the Configure Virtual Router popup window.

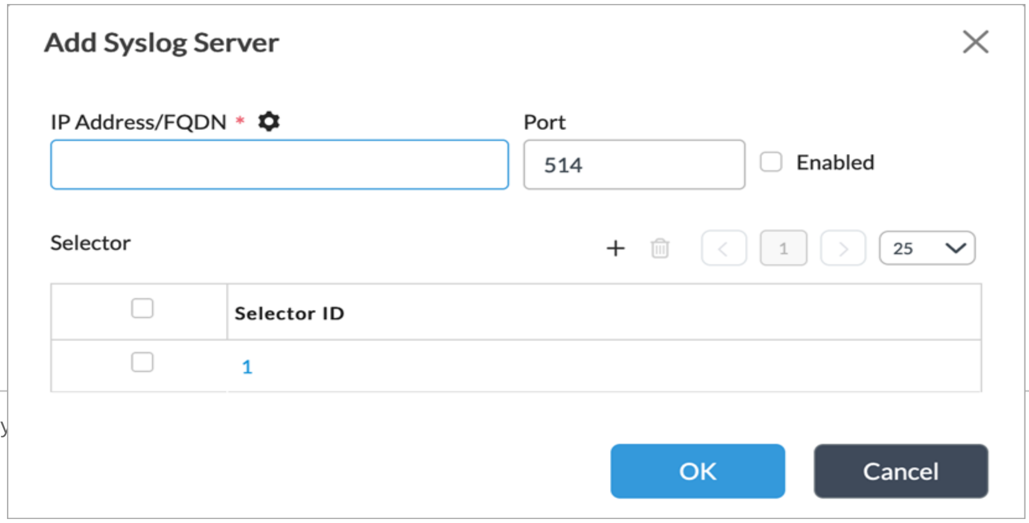
Manage Syslog Server

To manage the syslog server settings on your VOS devices:

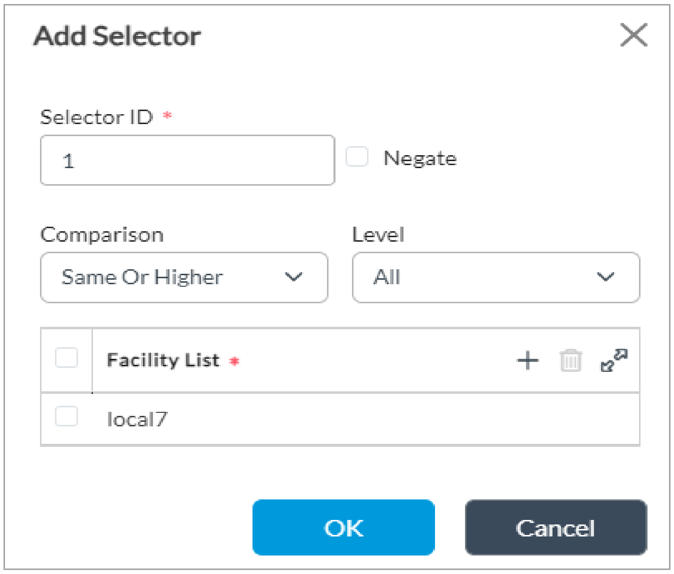
1. In Director view, select the Configure tab in the top menu bar.
2. Select Template > Device Templates in the horizontal menu bar and select the template you created in [Deploy a VOS Branch Device]() above.
3. Select Others > Syslog Server in the left menu bar.



4. Click Add to configure a new syslog server. In the Add Syslog Server popup window, enter information for the following fields.



5. Enter the IP address or FQDN of the server in the IP Address/FQDN field.
6. Enter the server port number in the Port field.
7. Check Enabled.
8. Click the + Add icon in the Selector field. In the Add Selector popup window, enter the following information.



Add Selector

Selector ID * 1 □ Negate

Comparison: Same Or Higher

Level: All

□	Facility List *
□	local7

9. Enter the the ID, Level, and Facility.
10. For more information about configuring other parametere, see Configure a Syslog Server.
11. Click OK and click OK on the Add Syslog Server window to save the syslog server.

To direct additional log files, such as IPsec daemon logs, to a remote server, you can redirect them to the syslog file. The *rsyslog* file captures this information after you configure the remote syslog server. To redirect log files to the syslog file, run the **set debug ipsec send to syslog** CLI command from the VOS CLI.

You can also use **set debug ipsec level** and **set debug ipsec flags** CLI commands to direct certain feature log types and to capture logging levels.

Audit Log Protection

Each TOE component is configured to send log data to the Analytics node over an internal IPsec tunnel in real-time. The Analytics node performs data analysis and provides reports and data visualization on syslog received from other TOE components and is configured to export all TOE logs to an external syslog receiver via IPsec in realtime.
TSF restricts access to audit logs stored on each component to authorized security administrators. Audit logs are configured to automatically archive and rotate log files via cron job, based on size limit specified by logrotate.d parameters. Administrator with admin role can delete audit log files, while administrators with super user privileges can manually delete the audit logs. Only authorized security administrators can read audit records.

Configure Log Exports

VOS data plane logs and other auditable events such as device alarms, are forwarded via IPFIX or syslog formats over an IPsec encrypted tunnel to Versa Analytics using Log Export Functionality (LEF). You can apply LEF profiles to inspection policies, firewall rules, and other configuration elements that forward logs specific to a security function. For example, you can apply LEF profiles to a firewall access policy that logs packets triggering an action such as drop or allow. This also applies to IPS or IDS actions, and VPN traffic logs.

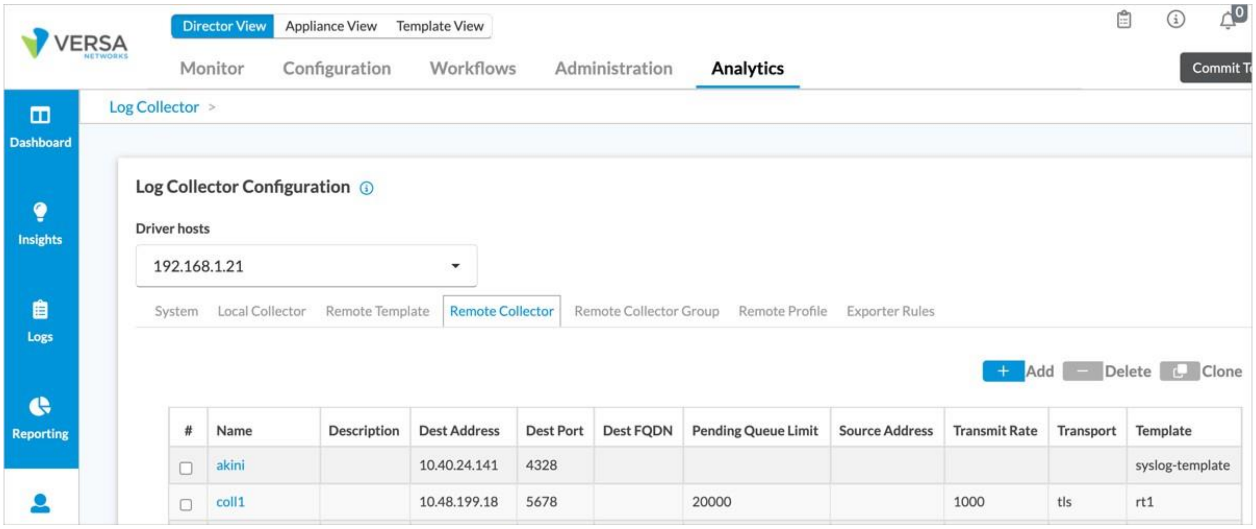
To define LEF profiles and log collectors, see the following articles to define LEF profiles and log collectors.

- Analytics Log Collector Types Overview
- Configure Log Export Functionality
- Apply Log Export Functionality
- Configure Log Collectors and Log Exporter Rules

After you enable forwarding of logs to Analytics, you must use a log collector exporter to reflect logs to an external syslog server.

To configure a remote collector:

1. In Director view, select the Analytics tab in the top menu bar.
2. Select Administration > Configurations > Log Collector Exporter in the left menu bar.
3. Click the Remote Collector tab. The following screen displays.



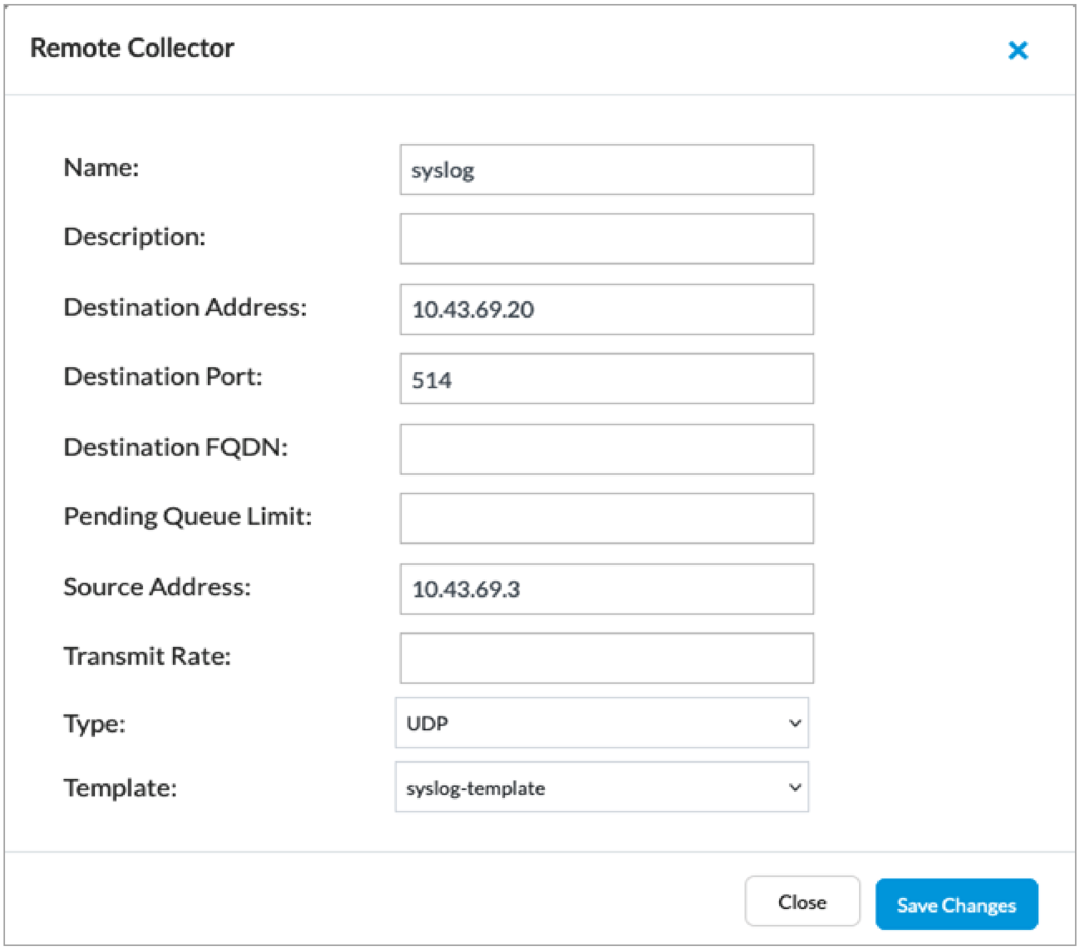
Log Collector Configuration

Driver hosts: 192.168.1.21

#	Name	Description	Dest Address	Dest Port	Dest FQDN	Pending Queue Limit	Source Address	Transmit Rate	Transport	Template
□	akini		10.40.24.141	4328						syslog-template
□	coll1		10.48.199.18	5678		20000		1000	tls	rt1

4. In the Driver Hosts field, select the Analytics log collector node.

5. Click the + Add icon. The Remote Collector popup window displays. Enter information for the following fields.



Remote Collector

Name: syslog

Description:

Destination Address: 10.43.69.20

Destination Port: 514

Destination FQDN:

Pending Queue Limit:

Source Address: 10.43.69.3

Transmit Rate:

Type: UDP

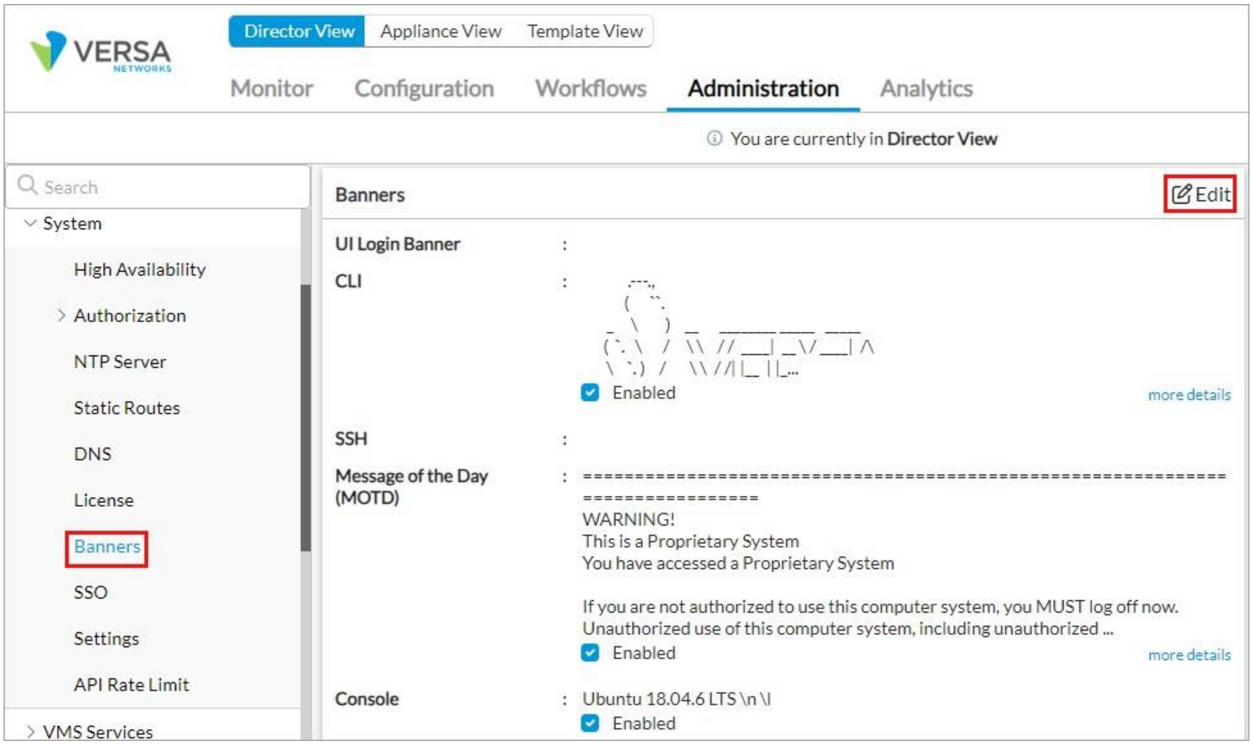
Template: syslog-template

6. Enter Name, Destination Address, Destinaton Port, and Destination FQDN (if applicable).
7. Select Type as UDP or TCP depending on the syslog server. VOS supports any RFC 5424-compatible syslog server.
8. Select syslog-template from the Template field, unless you configure another remote template during installation.
9. For more information about configuring other parameters, see Configure a Remote Collector.

Configure Login Banners

To set the banner displayed on the Versa Director login window, Director CLI, SSH, message of the day, and console:

1. In Director view, select the Administration tab in the top menu bar.
2. Select System > Banners in the left menu bar. The following screen displays.



Banners

UI Login Banner :

CLI :

```
     .---.
    (     `.
  _  \     )  __   ______ ___  ____
 ( `. \   /   \\ // ___| _\/ ___| /\
  \  `.)  /    \\ //| |__ | |_...
```

☑ Enabled

SSH :

Message of the Day (MOTD) :

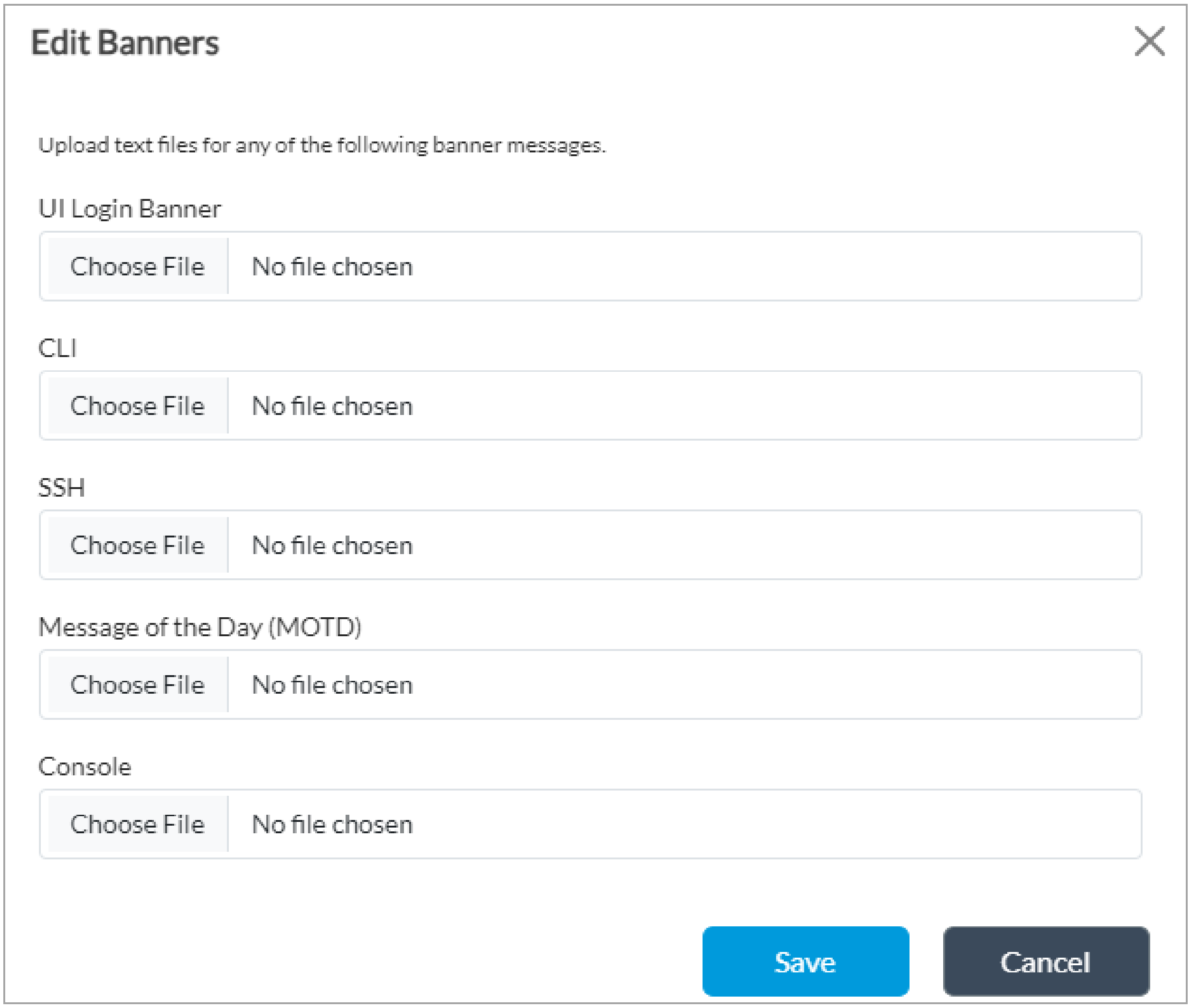
```
=================================================================
=================
WARNING!
This is a Proprietary System
You have accessed a Proprietary System

If you are not authorized to use this computer system, you MUST log off now.
Unauthorized use of this computer system, including unauthorized ...
```

☑ Enabled

Console : Ubuntu 18.04.6 LTS \n \l

☑ Enabled

3. Click Edit. The Edit Banners window displays. To change the banner, ensure that create a text file containing the banner text you wish to display at login.



Edit Banners

Upload text files for any of the following banner messages.

UI Login Banner

Choose File No file chosen

CLI

Choose File No file chosen

SSH

Choose File No file chosen

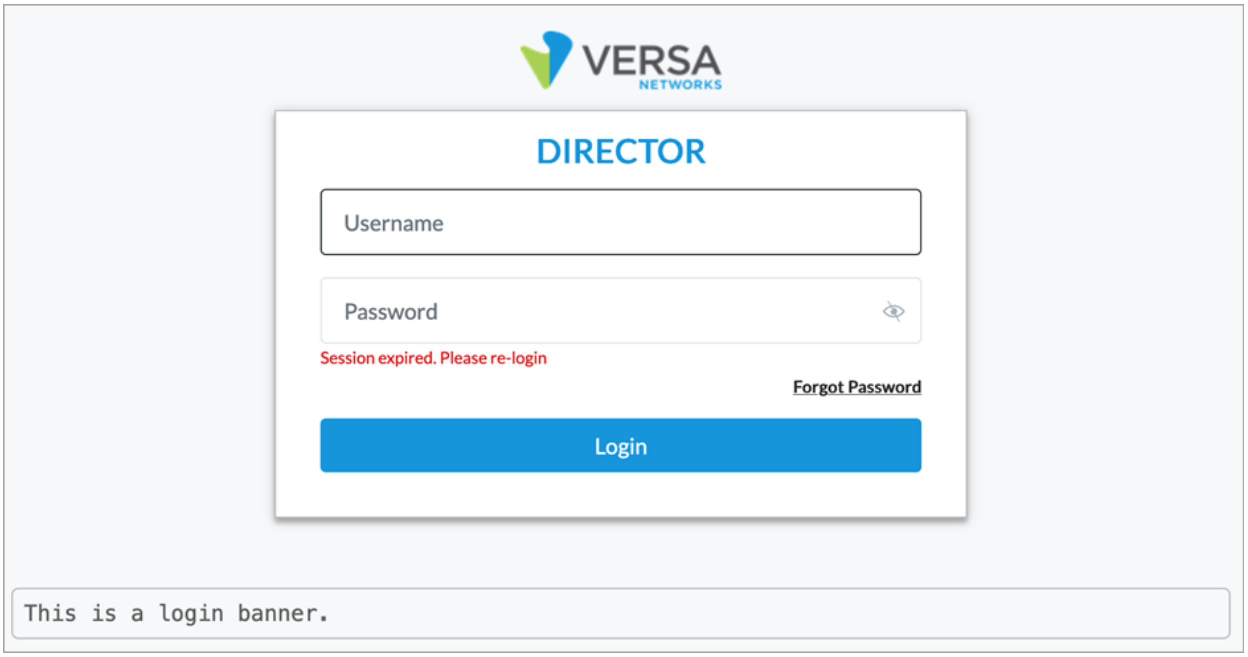
Message of the Day (MOTD)

Choose File No file chosen

Console

Choose File No file chosen

4. Click Choose File and select the text file with the message you want to display at login.
5. Repeat this for CLI, SSH, MOTD, and Console to change the login banner text for these options.
6. Click Save. The login banner displays the next time you log in. For example, for Versa Director:



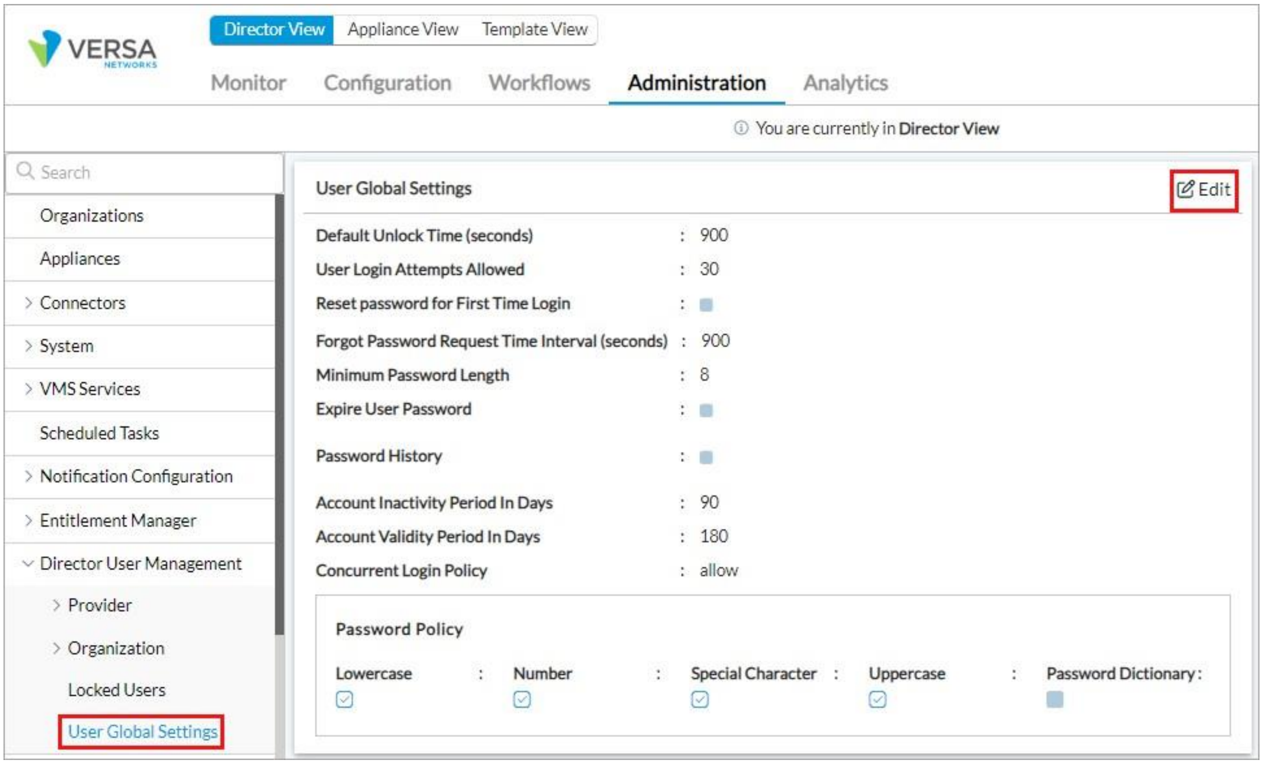
Session expired. Please re-login

This is a login banner.

Configure Director and System User Authentication

Use the User Global Settings menu to define user security enforcements such as authentication failure threshold, unlock time period, and minimum password length for Director users.

1. In Director view, select the Administration tab in the top menu bar.
2. Select Director User Management > User Global Settings in the left menu bar. The following screen displays.



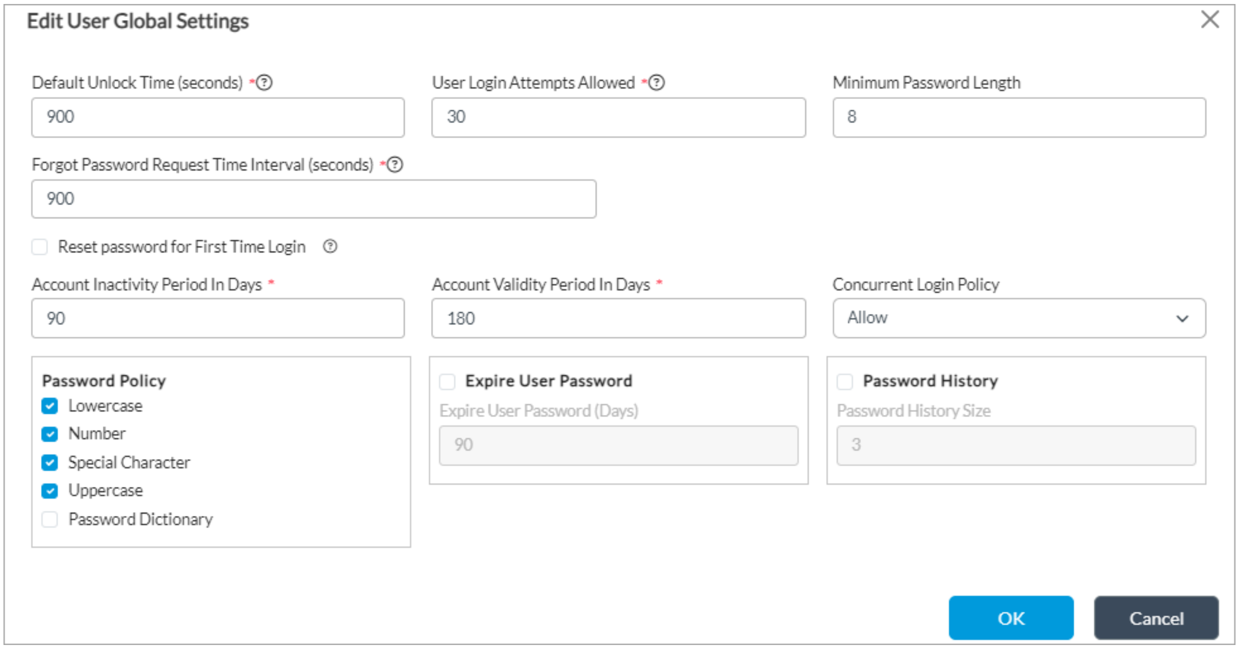
User Global Settings

Default Unlock Time (seconds)	:	900
User Login Attempts Allowed	:	30
Reset password for First Time Login	:	□
Forgot Password Request Time Interval (seconds)	:	900
Minimum Password Length	:	8
Expire User Password	:	□
Password History	:	□
Account Inactivity Period In Days	:	90
Account Validity Period In Days	:	180
Concurrent Login Policy	:	allow

Password Policy

Lowercase :	Number :	Special Character :	Uppercase :	Password Dictionary :
☑	☑	☑	☑	□

3. Click ✎ Edit and make the required changes in the Edit User Global Settings popup window.



Edit User Global Settings

Default Unlock Time (seconds) * 900

User Login Attempts Allowed * 30

Minimum Password Length 8

Forgot Password Request Time Interval (seconds) * 900

□ Reset password for First Time Login

Account Inactivity Period In Days * 90

Account Validity Period In Days * 180

Concurrent Login Policy Allow

Password Policy
☑ Lowercase
☑ Number
☑ Special Character
☑ Uppercase
□ Password Dictionary

□ Expire User Password
Expire User Password (Days) 90

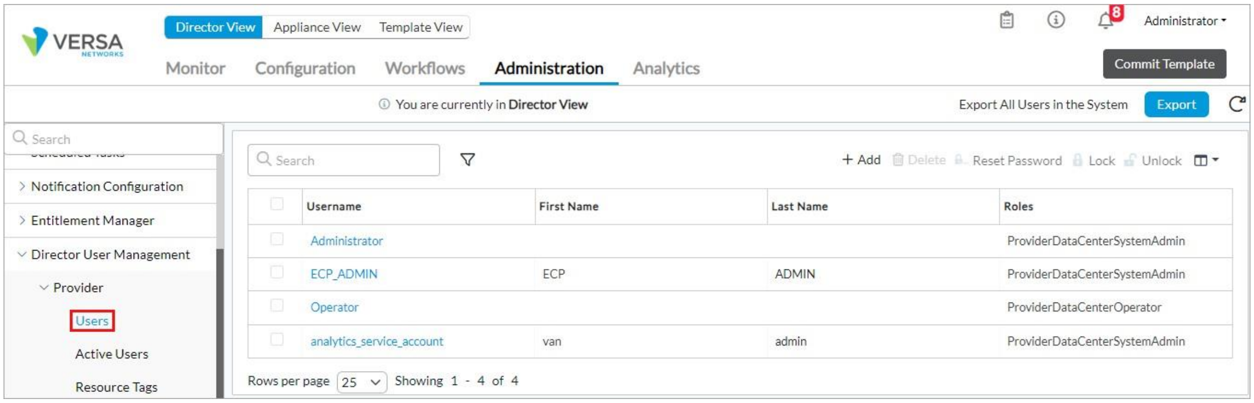
□ Password History
Password History Size 3

4. Click OK.

To add administrative users to Director,

1. In Director view, select the Administration tab in the top menu bar.

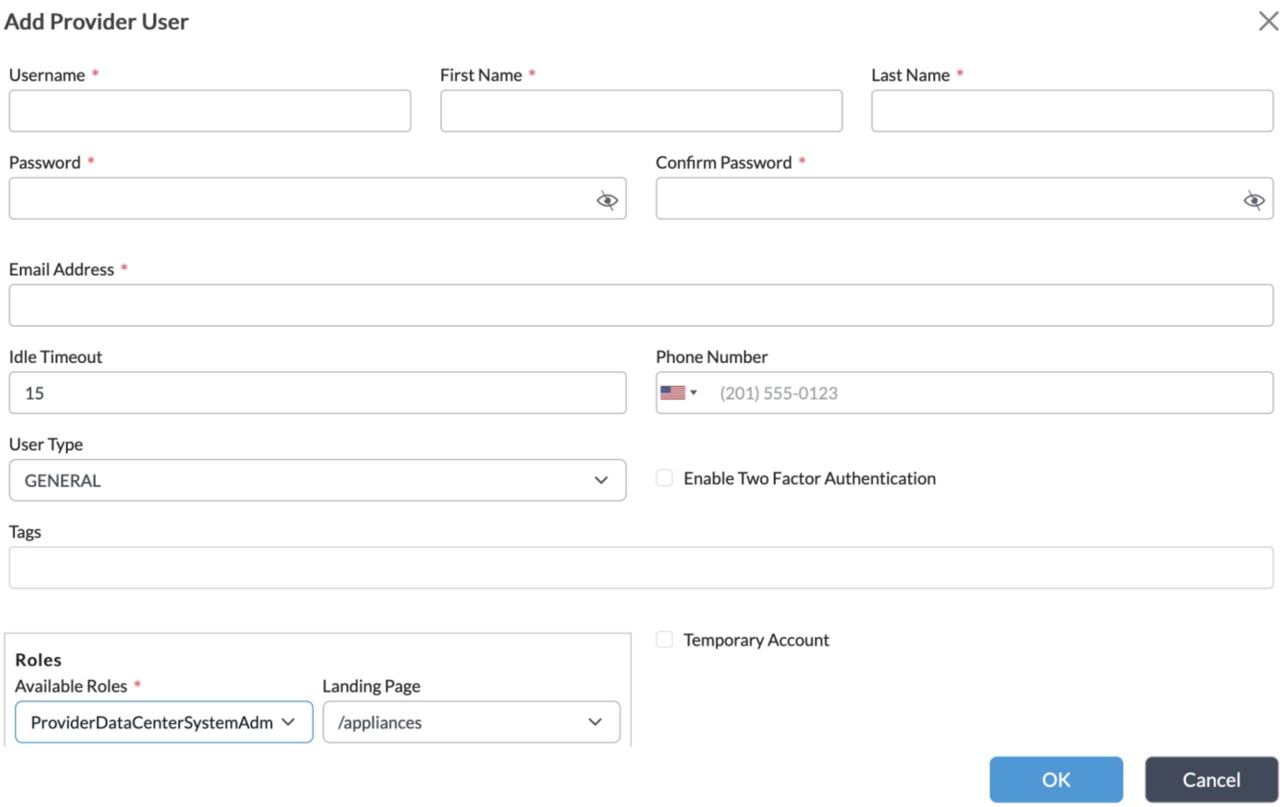
2. Select Director User Management > Provider > Users in the left menu bar. The following screen displays.



Username	First Name	Last Name	Roles
Administrator			ProviderDataCenterSystemAdmin
ECP_ADMIN	ECP	ADMIN	ProviderDataCenterSystemAdmin
Operator			ProviderDataCenterOperator
analytics_service_account	van	admin	ProviderDataCenterSystemAdmin

Rows per page 25 Showing 1 - 4 of 4

3. Click the “+ Add” button. The following screen displays:



Username *

First Name *

Last Name *

Password *

Confirm Password *

Email Address *

Idle Timeout: 15

Phone Number: (201) 555-0123

User Type: GENERAL

□ Enable Two Factor Authentication

Tags

□ Temporary Account

Roles

Available Roles *: ProviderDataCenterSystemAdm

Landing Page: /appliances

4. Enter at least the Username, First Name, Last Name, Password, Email Address, and the Role for the user, and click OK. See below section for requirements on password strength.

Set Password Complexity

You must set the Minimum Password Length parameter User Global Settings window to a positive integer. The acceptable minimum password length values are between 8 and 25.

To define the minimum password length for system users, set the **PASS_MIN_LENGTH=15** parameter in in /opt/versa/etc/niap.env.

Re-run the **sudo /opt/versa/vnms/scripts/vnms-config.sh --configure-niap** script for the setting to take effect.

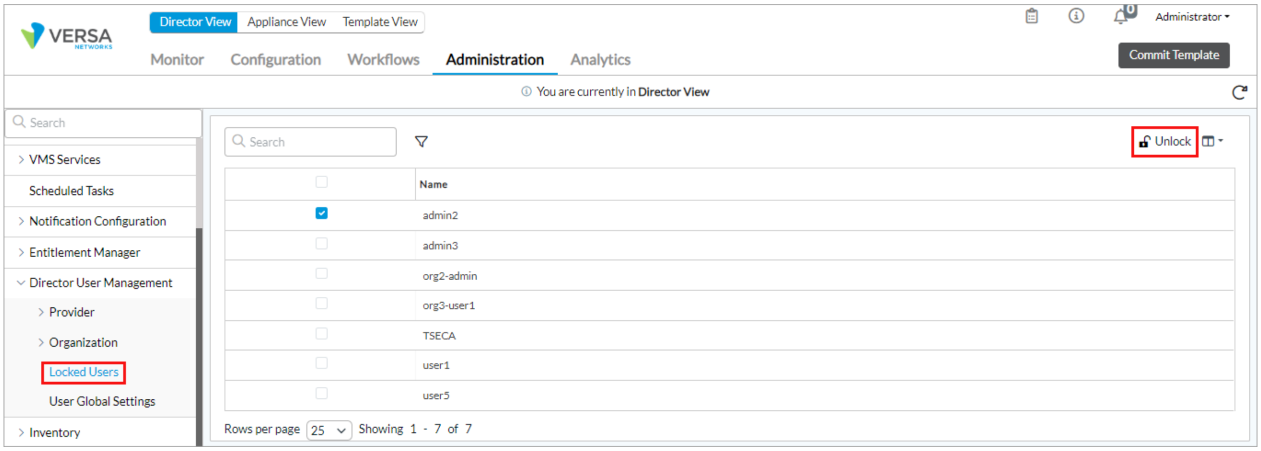
Passwords must be a combination of lowercase, uppercase, numeric, and these special characters:
! @ # $ % ^ & * ( ) " ' + , - . / : ; < = > ? @ [\ ] _ ` { | } ~

Set User Account Unlock Time

Set the User Login Attempts Allowed parameter in the User Global Settings window to a positive integer along with the Default Unlock Time, which is the time in seconds after which the locked account unlocks automatically.

To manually unlock a user account:

1. In Director view, select the Administration tab in the top menu bar.
2. Select Director User Management > Locked Users in the left menu bar. The following screen displays.



	Name
☑	admin2
□	admin3
□	org2-admin
□	org3-user1
□	TSECA
□	user1
□	user5

Rows per page 25 Showing 1 - 7 of 7

3. Select the user account you want to unlock and click Unlock.

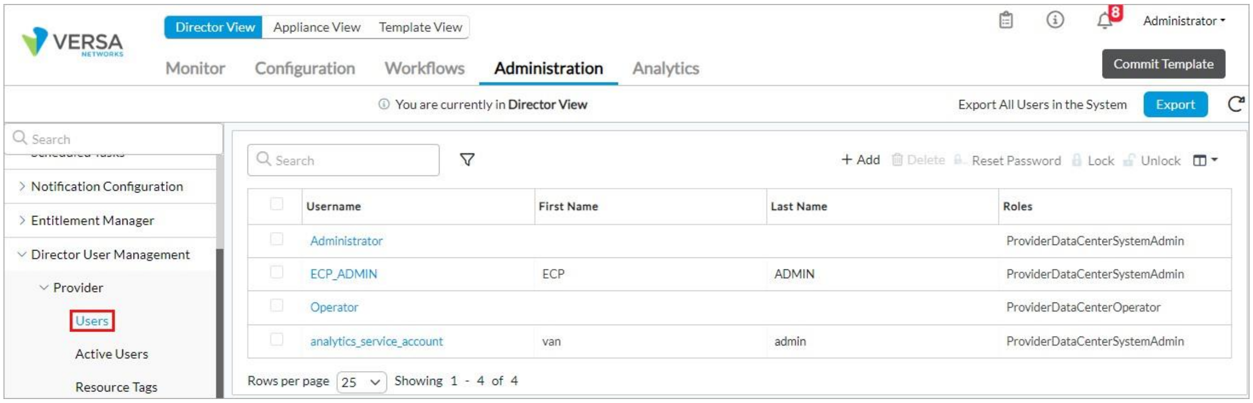
To unlock a user account from the Director CLI, run the **request nms actions unlock-user-by-admin username** *user name* CLI command.

Set Director GUI and CLI Idle Timeout

To set the Director GUI the session timeout:

5. In Director view, select the Administration tab in the top menu bar.

6. Select Director User Management > Provider > Users in the left menu bar. The following screen displays.



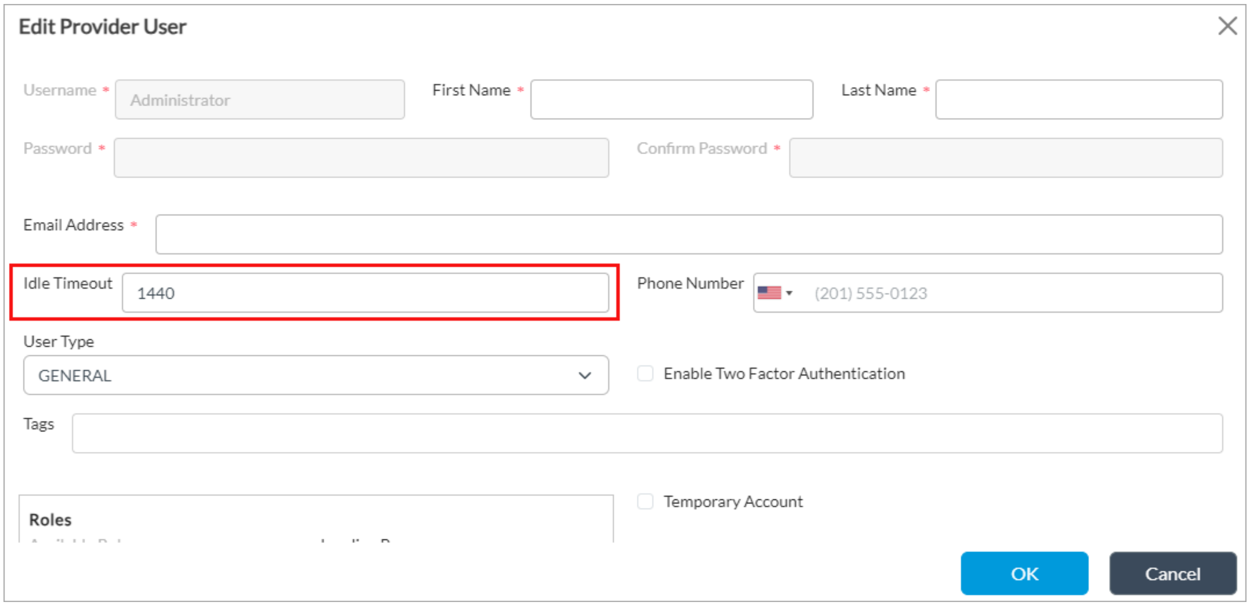
You are currently in Director View

Export All Users in the System

Username	First Name	Last Name	Roles
Administrator			ProviderDataCenterSystemAdmin
ECP_ADMIN	ECP	ADMIN	ProviderDataCenterSystemAdmin
Operator			ProviderDataCenterOperator
analytics_service_account	van	admin	ProviderDataCenterSystemAdmin

Rows per page 25 Showing 1 - 4 of 4

7. Select a user and the Edit Provider User window displays.



Edit Provider User

Username * Administrator

First Name *

Last Name *

Password *

Confirm Password *

Email Address *

Idle Timeout 1440

Phone Number (201) 555-0123

User Type GENERAL

□ Enable Two Factor Authentication

Tags

Roles

□ Temporary Account

8. Set the value for the Idel Timeout field. The value range is 15 through 1440 minutes.

To set idle timeout from the Director CLI, run the **set idle-timeout** *seconds* CLI command. The value can be between 0 and 8192.

Set Director User Timeout and Authentication Lockout

You use the following APIs to configure and use auth-lockout and shell-timeout to secure administrator user access to Director CLI.

To check whether authentication lockout or shell timeout is enabled:

curl -k https://<Director-IP>:9182/vnms/system/bash-config -u Administrator:*password* **-H 'Content-Type:**

application/json' -H 'Accept: application/json'

Response:

```
{
"shell-timeout-in-sec": 900,
"is-shell-timeout-enabled": false,
"is-auth-lockout-enabled": false,
“auth-lockout-time-in-sec": 600,
"retries-before-lockout": 3
}
```

In the example above:

- **is-shell-timeout-enabled** and **is-auth-lockout-enabled** are set to False, indicating that shell time out and authentication lockout are not enabled.
- **shell-timeout-in-sec** indicates the time in seconds of user inactivity after which shell timeout logs out the user.
- **auth-lockout-time-in-sec** is the period in seconds for which a user is locked after the number of unsuccessful authentication attempts specified in **retries-before-lockout.**

To enable authentication lockout or shell timeout, run the following command or modify the parameters for either **function:**

```
curl -X PUT -k https://<Director-IP-address>:9182/vnms/system/bash-config -u Administrator:password
-H 'Content-Type: application/json' -H 'Accept: application/json' -d
'{"shell-timeout-in-sec":900,"is-shell-timeout-enabled":true,"is-auth-lockout-enabled":true,
"auth-lockout-time-in-sec":600,"retries-before-lockout":3}'
```

If successful, the **Applied system configuration successfully** response message displays.

To prevent situations where all users are locked out, add certain “break-glass” emergency accounts or system accounts to /var/lib/vs/.lockout_excluded_users, which are excluded from authentication lockout. To add a user to this exclusion list, run the following command:

```
curl -X PUT -k https://<Director-IP>:9182/vnms/system/bash-config/exclude-user/user-name -u
Administrator:password -H
Content-Type: application/json' -H 'Accept: application/json'
```

If successful, the **User:** *user-name* **excluded from lockout successfully** response message displays.

To remove a user from the exclusion list, run the following command:

```
curl -X PUT -k https://<Director-IP>:9182/vnms/system/bash-config/exclude-user/user-name -u
Administrator:password -H
'Content-Type: application/json' -H 'Accept: application/json'
```

If successful, the **User:** *user-name* **included for lockout successfully** response message displays.

To manually unlock a locked-out user, run the following command:

```
curl -X PUT -k https://<Director-IP>:9182/vnms/system/bash-config/reset-failure/user-name -u
Administrator:password -H 'Content-Type: application/json' -H 'Accept: application/json'
```

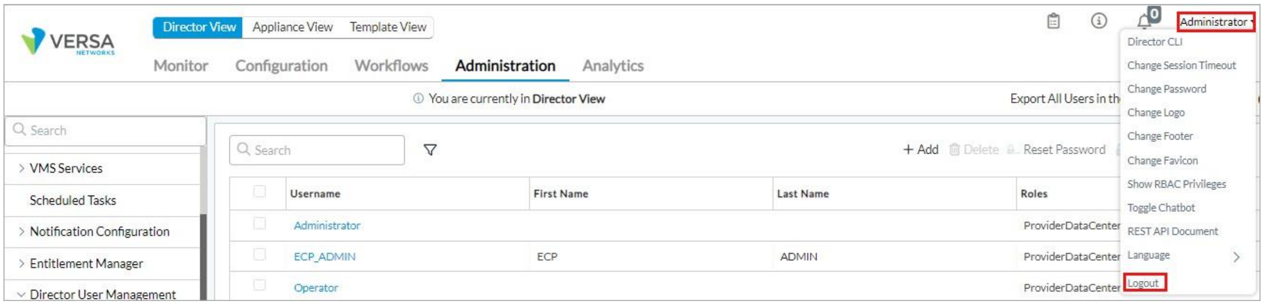
If successful, the **User:** *user-name* **auth failures reset successfully** response message displays.

Local console is not subject to user lockout.

Log Out Manually from an Administrator Session

To exit an administrator session from the Director CLI, type **exit** or **logout** and press the Enter key.

To log out of the Director GUI, select the username in the top right corner, and click Logout:



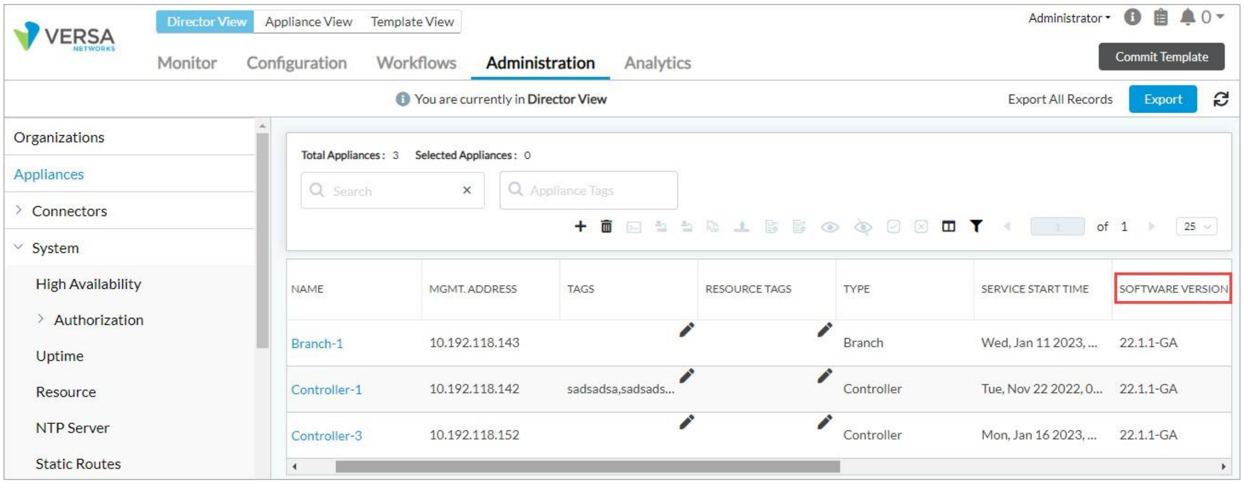
Username	First Name	Last Name	Roles
Administrator			ProviderDataCenter
ECP_ADMIN	ECP	ADMIN	ProviderDataCenter
Operator			ProviderDataCenter

Verify the Installation and Perform Upgrades

Verify Software Version

To verify the base software versions of appliances:

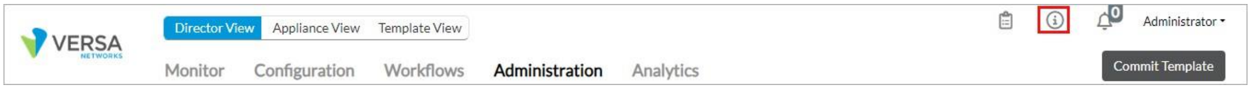
1. Select the Administration in the top menu bar.
2. Select Appliances in the left menu. The Appliances window displays and the Software Version column displays the appliance software version. For more information, see Verify Software Installation.



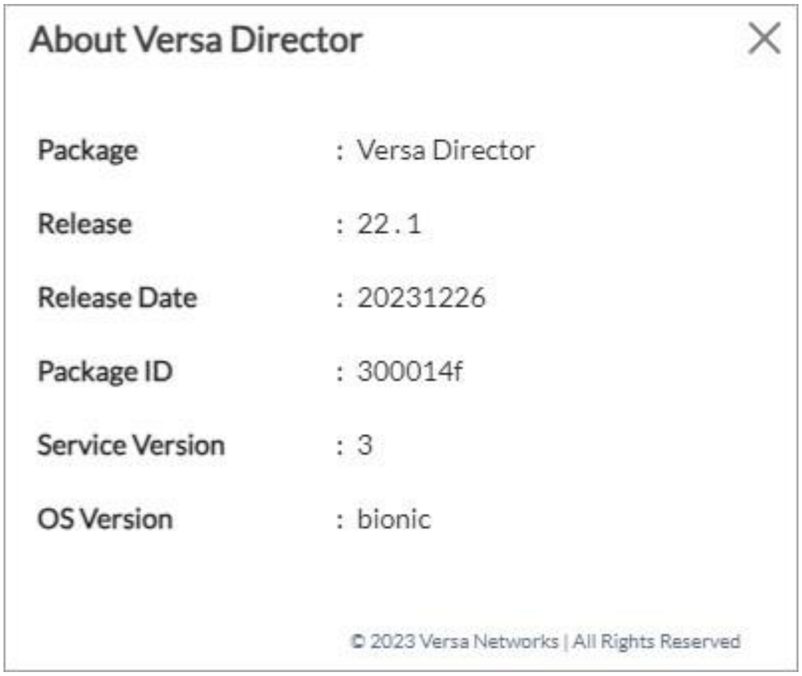
Total Appliances : 3 Selected Appliances : 0

NAME	MGMT. ADDRESS	TAGS	RESOURCE TAGS	TYPE	SERVICE START TIME	SOFTWARE VERSION
Branch-1	10.192.118.143			Branch	Wed, Jan 11 2023, ...	22.1.1-GA
Controller-1	10.192.118.142	sadsadsa,sadsads...		Controller	Tue, Nov 22 2022, 0...	22.1.1-GA
Controller-3	10.192.118.152			Controller	Mon, Jan 16 2023, ...	22.1.1-GA

3. To verify the Director software version, click the Information icon on the top right corner:



The About Versa Direcor popup window displays:

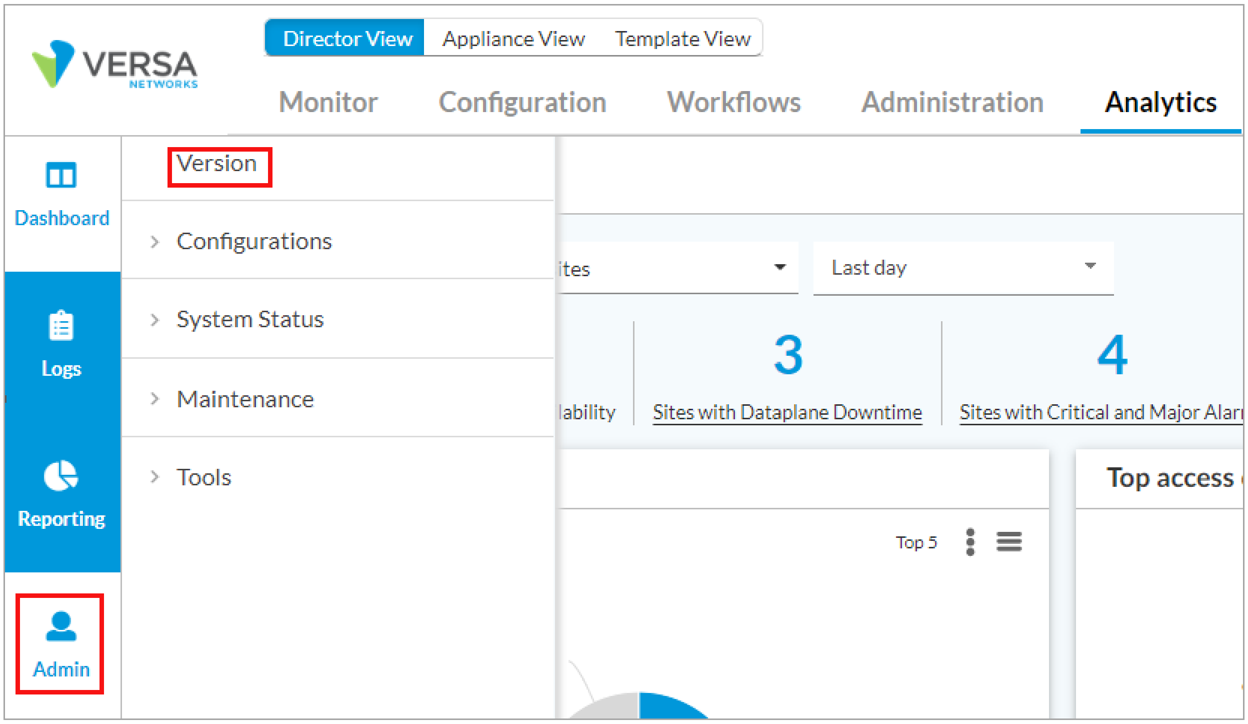


About Versa Director

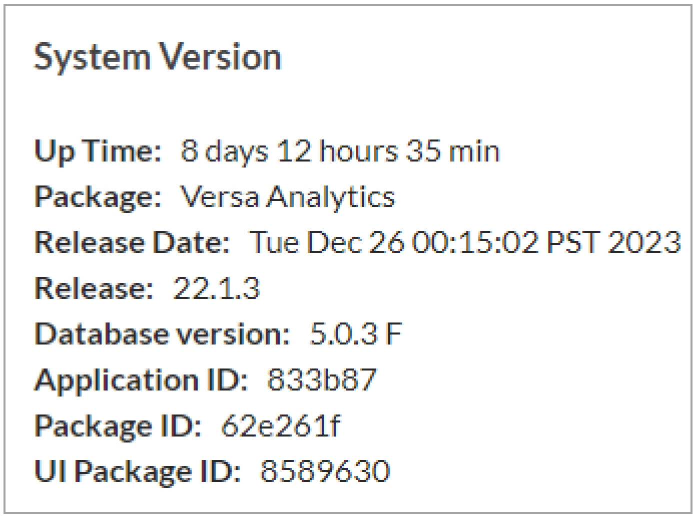
Package	: Versa Director
Release	: 22.1
Release Date	: 20231226
Package ID	: 300014f
Service Version	: 3
OS Version	: bionic

© 2023 Versa Networks | All Rights Reserved

4. To verify the Analytics software version, from Analytics UI, select Admin > Version in the left menu.



The System Version popup window displays:



System Version

Up Time: 8 days 12 hours 35 min
Package: Versa Analytics
Release Date: Tue Dec 26 00:15:02 PST 2023
Release: 22.1.3
Database version: 5.0.3 F
Application ID: 833b87
Package ID: 62e261f
UI Package ID: 8589630

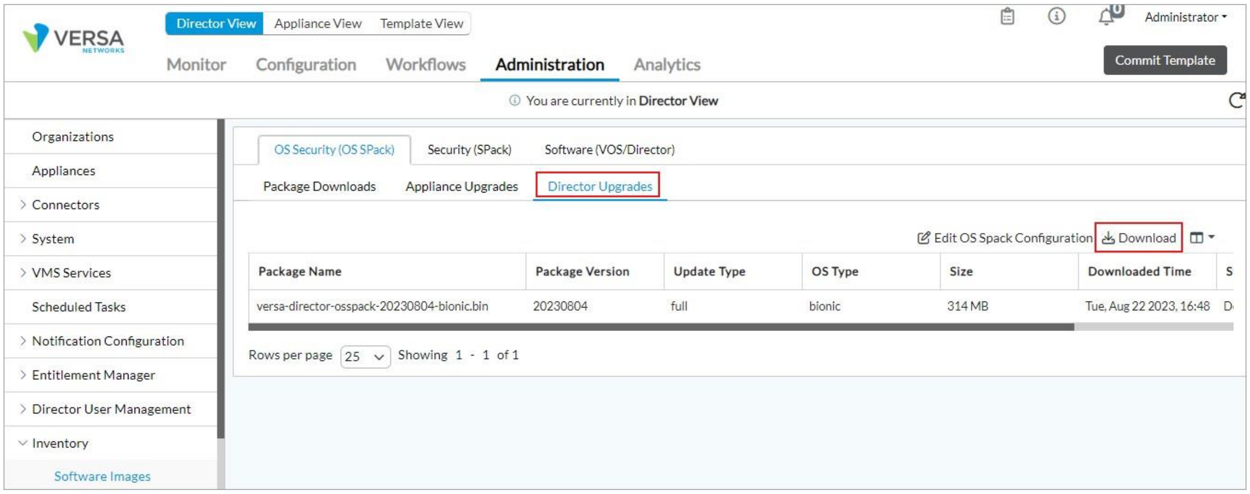
5. To verify the software version using CLI, issue the **show system package-info** CLI command from the Director or Analytics CLI.

Apply OS Security Packages

Before you upgrade a Versa operating system security package (OS SPack), backup iptables rules by issuing the **sudo iptables-save > iptables.rules** CLI command.

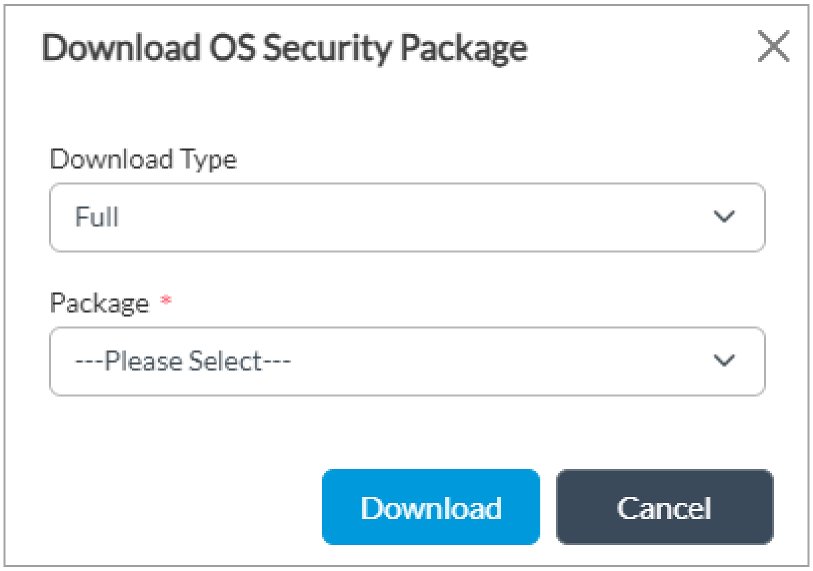
To download an OS SPack to a Director node and then install it:

1. In Director view, select the Administration tab in the top menu bar.
2. Select Inventory > Software Images in the left menu bar. The OS Security (OS SPack) tab display by default.
3. In the OS Security (OS SPack) tab, select the Director Upgrades tab. The table in the main pane lists the OS SPacks that have been downloaded.



Package Name	Package Version	Update Type	OS Type	Size	Downloaded Time	S
versa-director-osspack-20230804-bionic.bin	20230804	full	bionic	314 MB	Tue, Aug 22 2023, 16:48	D

4. Click the Download icon to download the OS Security package. In the Download OS Security Package popup window, enter the following information.



Download OS Security Package

Download Type: Full

Package *: ---Please Select---

Field	Description
Download Type	Select the type of download: ◦ Full—Select to download a new OS SPack to Director. Select this option if an OS SPack is not already installed on the Director node. ◦ Incremental—Select to upgrade the OS SPack on a Director node.
Package (Required)	Select the name of the OS SPack.

5. Click Download. The downloaded file is saved in the /var/versa/packages/osspack/versa-director/ directory. For more information, see [Download and Install an OS SPack on a Director Node]().

To install the OS Spack:

1. Install the OS security pack update by executing the following Linux commands from a bash shell:

```
cd  /var/versa/packages/osspack/versa-director/
~$ chmod  a+x filename.bin
~$ sudo ./filename.bin
```

To display a list of OS SPack versions that are present on a Director node, SSH into the node and issue the following shell command:

```
cat /opt/versa/etc/osspack/manifest.json | grep '"version":'
```

Note that in this command, the text string **version** is preceded by a single quotation mark followed by a double quotation mark.

To download and install an OS SPack on an Analytics node, follow the to download the OS SPack on a Directore node. Ensure that the binary file that you download and use to install the security update is the binary file for Analytics.

You can also download the OS SPack by issuing the following commands from the CLI:

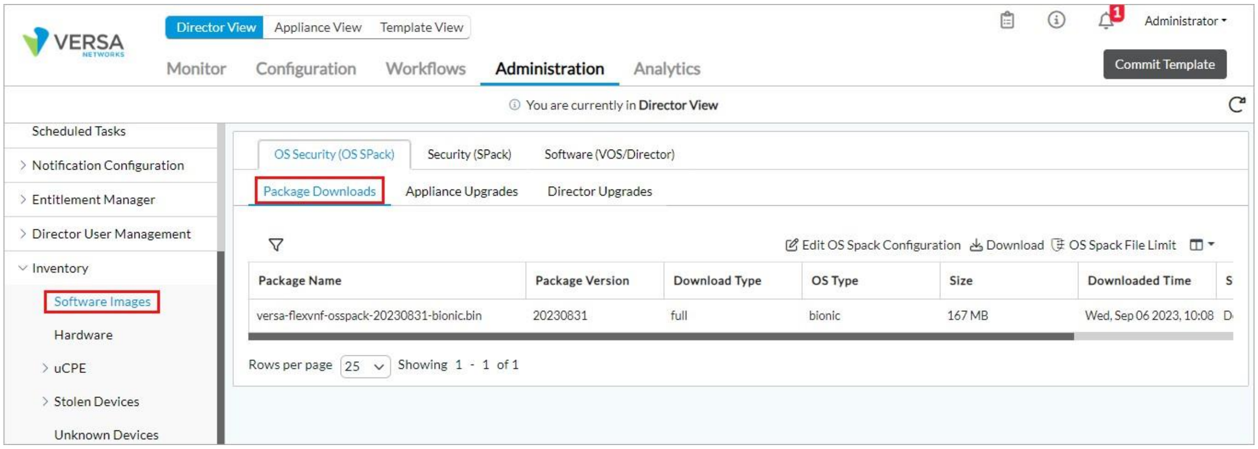
> request security osspack check updates
> request security osspack download bundle version
> request security osspack download file *filename* (for Releases 21.1.4 and later)
> request security osspack install bundle *bundle-name*

To display a list of OS SPack versions that are present on an Analytics node, for Releases 21.1.1 and later, issue the following CLI command:

> analytics-cli> **show security osspack info**

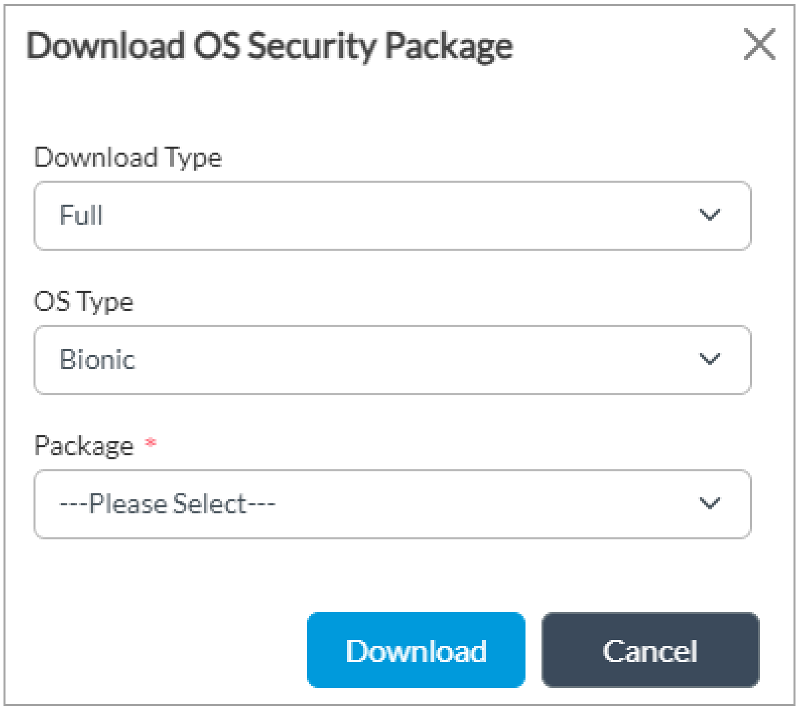
To download the OS SPack for a VOS device:

1. Before you download and install the OS SPack, configure DNS settings so that the Director node can locate the server from which to download the OS SPack. For more information, see Configure DNS Settings.
2. In Director view, select the Administration tab in the top menu bar.
3. Select Inventory > Software Images in the left menu bar.
4. Select the OS Security (OS SPack) tab in the horizontal menu bar, and then select the Package Downloads tab. The table in the main pane lists the OS SPacks that have already been downloaded.



Package Name	Package Version	Download Type	OS Type	Size	Downloaded Time	S
versa-flexvnf-osspack-20230831-bionic.bin	20230831	full	bionic	167 MB	Wed, Sep 06 2023, 10:08	D

5. Click the 📥 Download icon to download the OS Security package. In the Download OS Security Package popup window, enter information for the following.



Download OS Security Package

Download Type: Full

OS Type: Bionic

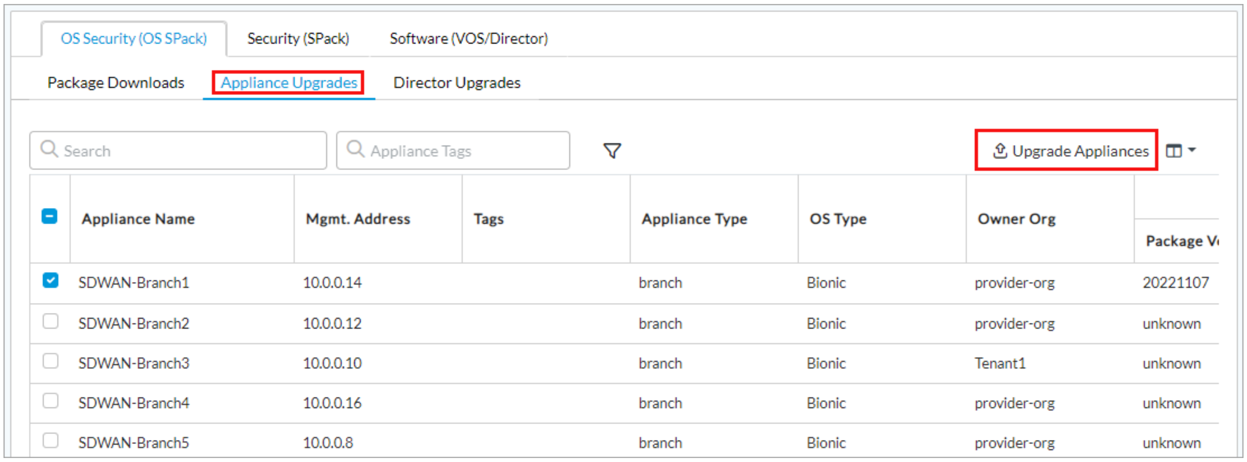
Package *: ---Please Select---

Field	Description
Download Type	Select the type of download: ◦ Full—Download the complete OS SPack to the Director node. Select this option if an OS SPack is not already installed on the Director node. ◦ Incremental—Select to upgrade the OS SPack on a Director node with only the changes that have been made to the OS SPack.
OS Type	Select the OS type Bionic (Ubuntu 18.04).
Package (Required)	Select the name of the OS SPack.

6. Click Download. The OS SPack is downloaded, and it is then listed in the table in the main pane. For more information, see Download the OS SPack for a VOS Device.

To install the OS SPack on a VOS device:

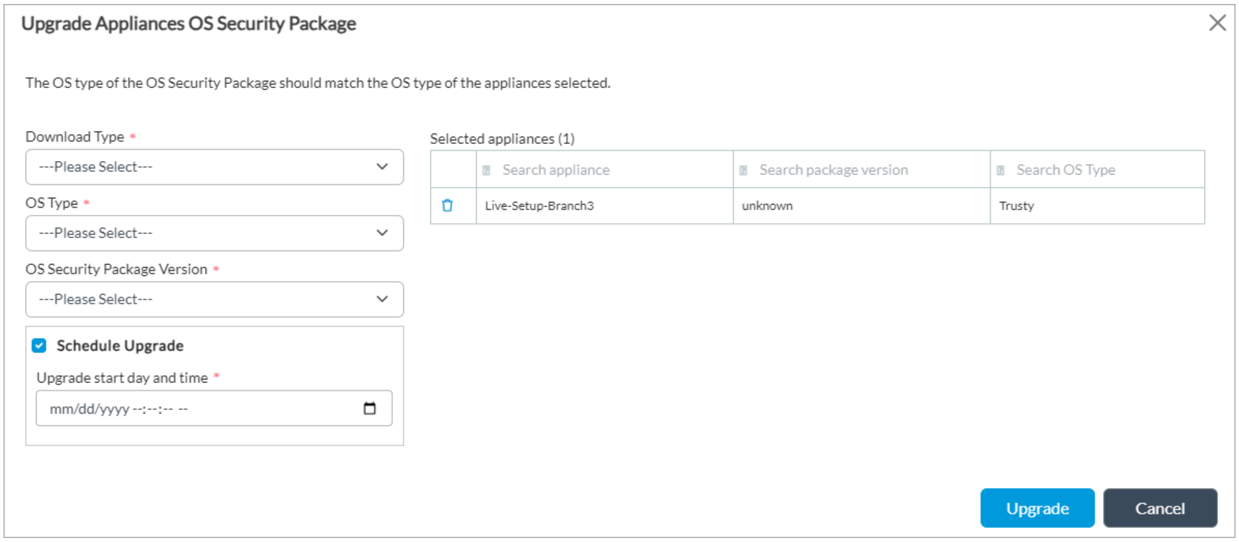
1. In the OS Security (OS SPack) tab, select the Appliance Upgrades tab.



☐	Appliance Name	Mgmt. Address	Tags	Appliance Type	OS Type	Owner Org	Package V
☑	SDWAN-Branch1	10.0.0.14		branch	Bionic	provider-org	20221107
☐	SDWAN-Branch2	10.0.0.12		branch	Bionic	provider-org	unknown
☐	SDWAN-Branch3	10.0.0.10		branch	Bionic	Tenant1	unknown
☐	SDWAN-Branch4	10.0.0.16		branch	Bionic	provider-org	unknown
☐	SDWAN-Branch5	10.0.0.8		branch	Bionic	provider-org	unknown

2. Select the VOS device or devices on which to install the OS SPack, or select the box next to the Appliance Name column to select all devices.

3. Click Upgrade Appliances. The Upgrade Appliances OS Security Package popup window displays. Enter the following information.



Upgrade Appliances OS Security Package

The OS type of the OS Security Package should match the OS type of the appliances selected.

Download Type *
---Please Select---

OS Type *
---Please Select---

OS Security Package Version *
---Please Select---

☑ Schedule Upgrade

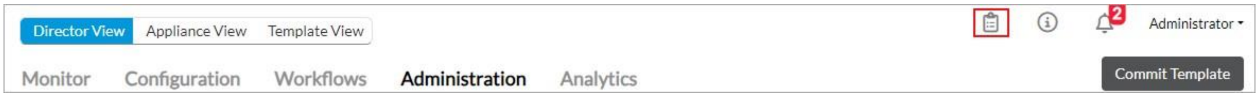
Upgrade start day and time *
mm/dd/yyyy --:--:-- --

Selected appliances (1)

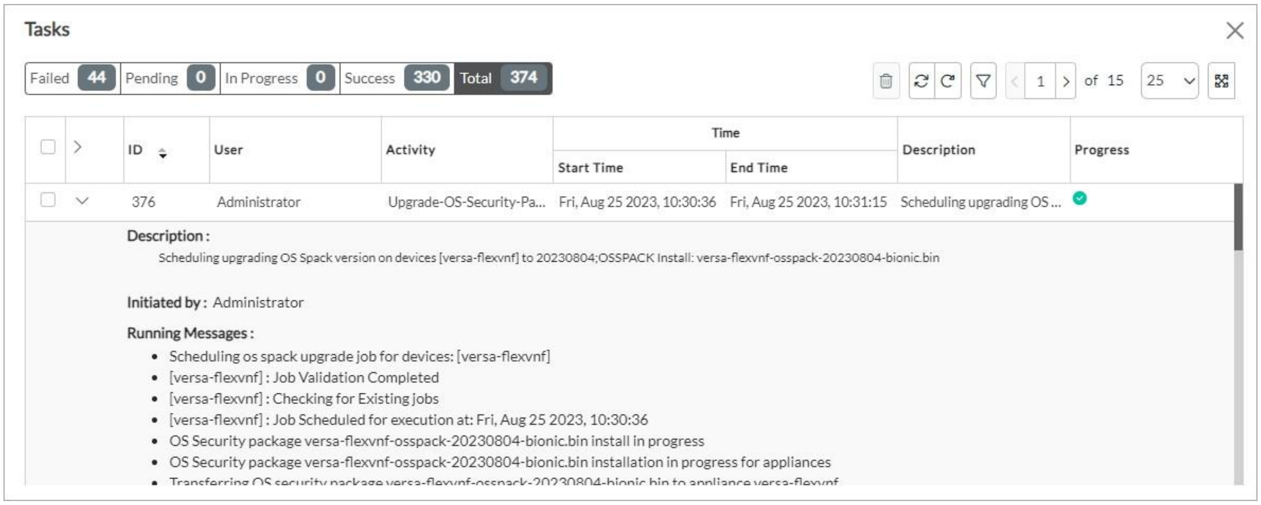
	Search appliance	Search package version	Search OS Type
🗑	Live-Setup-Branch3	unknown	Trusty

Field	Description
Download Type (Required)	Select the type of downloaded package: ◦ Full—Select a new OS SPack. Select this option if an OS SPack is not already installed on the VOS device. ◦ Incremental—Select to upgrade the device.
OS Type	Select the OS type running on the VOS node.
OS Security Package Version (Required)	Select the OS SPack from the list of downloaded SPacks.
Schedule Upgrade	Click to schedule a date and time for the upgrade to occur. Enter the date in the format *mm*/*dd*/*yyyy* (month/date/year), and enter the time in the format *hh*:*mm*:*ss* (hours:minutes:seconds, using 24-hour format for the hours).
Selected Appliances	Displays the device or devices you selected for upgrade.

4. Click Upgrade. If you have not set a schedule for upgrade, the OS SPack is upgraded immediately.
5. To check the status of the download and installation of the OS SPack, click the Tasks icon in the horizontal menu bar.



The Tasks popup window displays details of the OS SPack download tasks, including failed, pending, in progress, successful, and total tasks. For more information see, Install the OS SPack.



ID	User	Activity	Time		Description	Progress
			Start Time	End Time		
376	Administrator	Upgrade-OS-Security-Pa...	Fri, Aug 25 2023, 10:30:36	Fri, Aug 25 2023, 10:31:15	Scheduling upgrading OS ...	✓

Description :
Scheduling upgrading OS Spack version on devices [versa-flexvnf] to 20230804;OSSPACK Install: versa-flexvnf-osspack-20230804-bionic.bin

Initiated by : Administrator

Running Messages :

- Scheduling os spack upgrade job for devices: [versa-flexvnf]
- [versa-flexvnf] : Job Validation Completed
- [versa-flexvnf] : Checking for Existing jobs
- [versa-flexvnf] : Job Scheduled for execution at: Fri, Aug 25 2023, 10:30:36
- OS Security package versa-flexvnf-osspack-20230804-bionic.bin install in progress
- OS Security package versa-flexvnf-osspack-20230804-bionic.bin installation in progress for appliances
- Transferring OS security package versa-flexvnf-osspack-20230804-bionic.bin to appliance versa-flexvnf

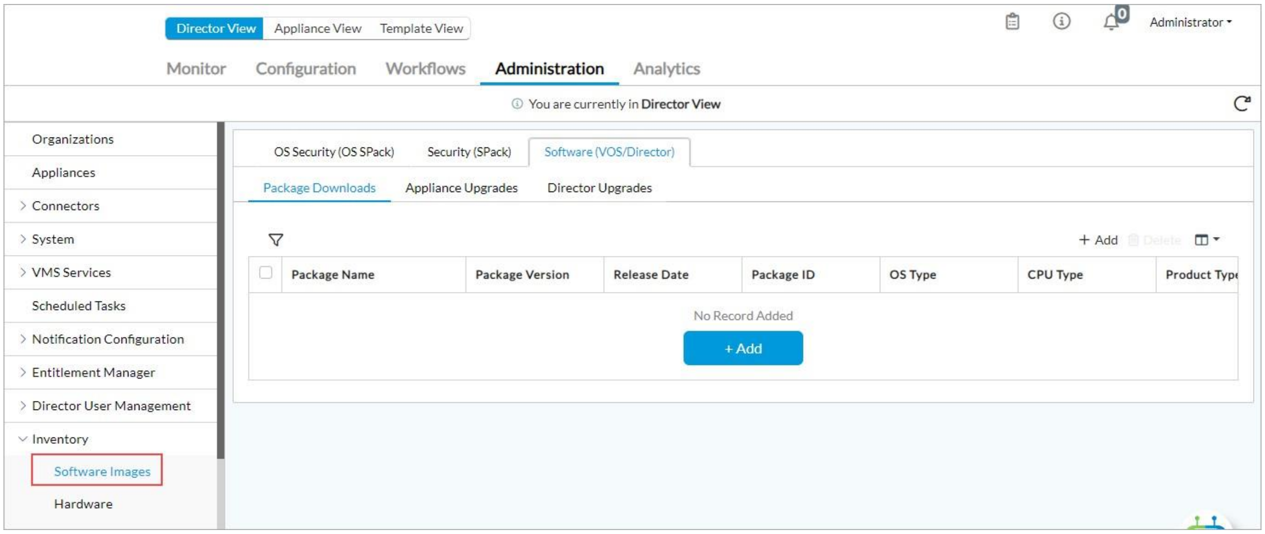
To display a list of OS SPack versions that are present on a VOS device, issue the following CLI command:

```
vos-cli> show security osspack info
```

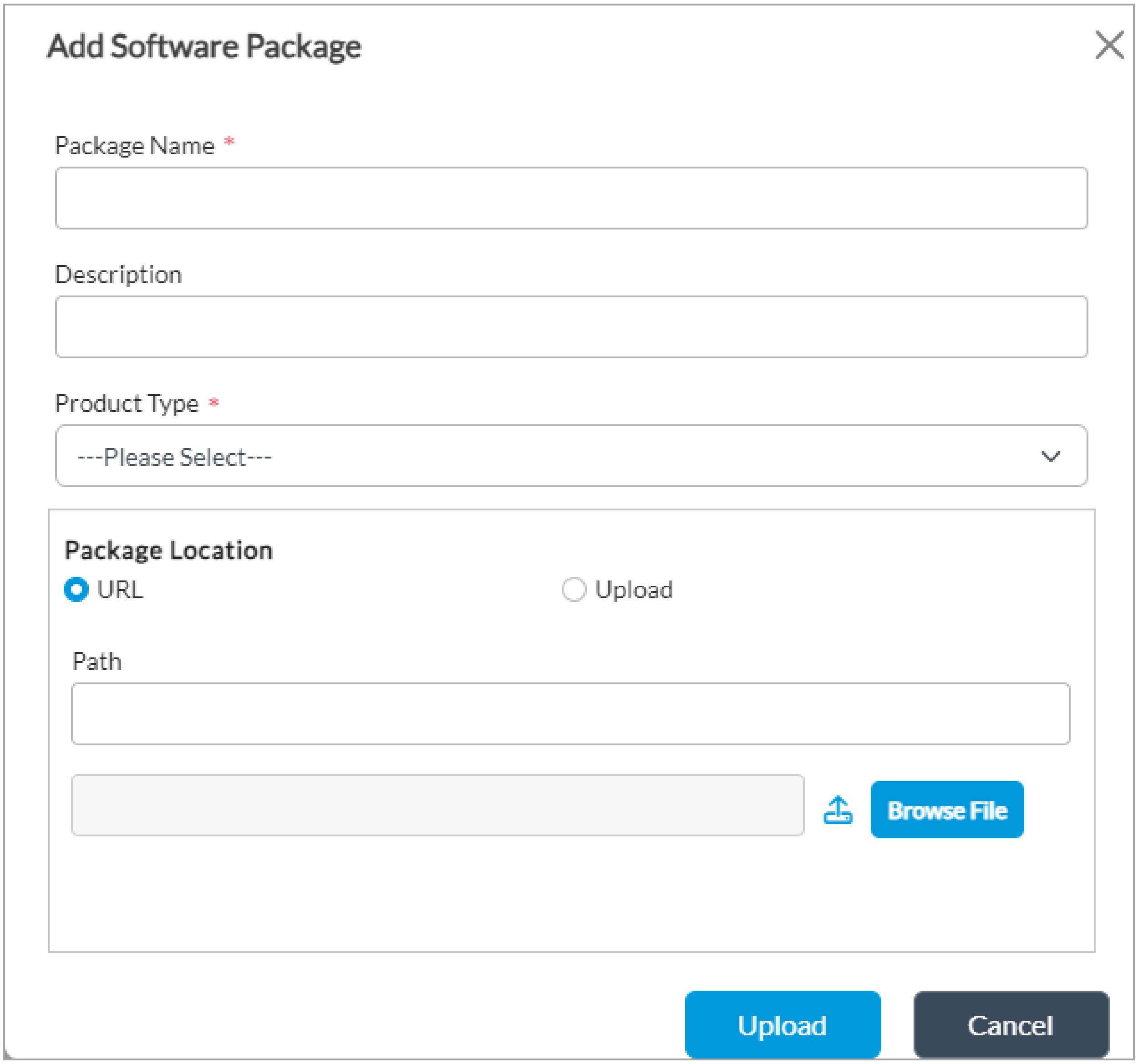
Upgrade Director and VOS

To upgrade the VOS software on a Director node:

1. In Director view, select the Administration tab in the top menu bar.
2. Select Inventory > Software Images in the left menu bar.
3. Select the Software (VOS/Director) tab, and then select the Package Downloads tab. The following screen displays.



4. Click the + Add icon. In the Add Software Package popup window, enter information for the following fields.



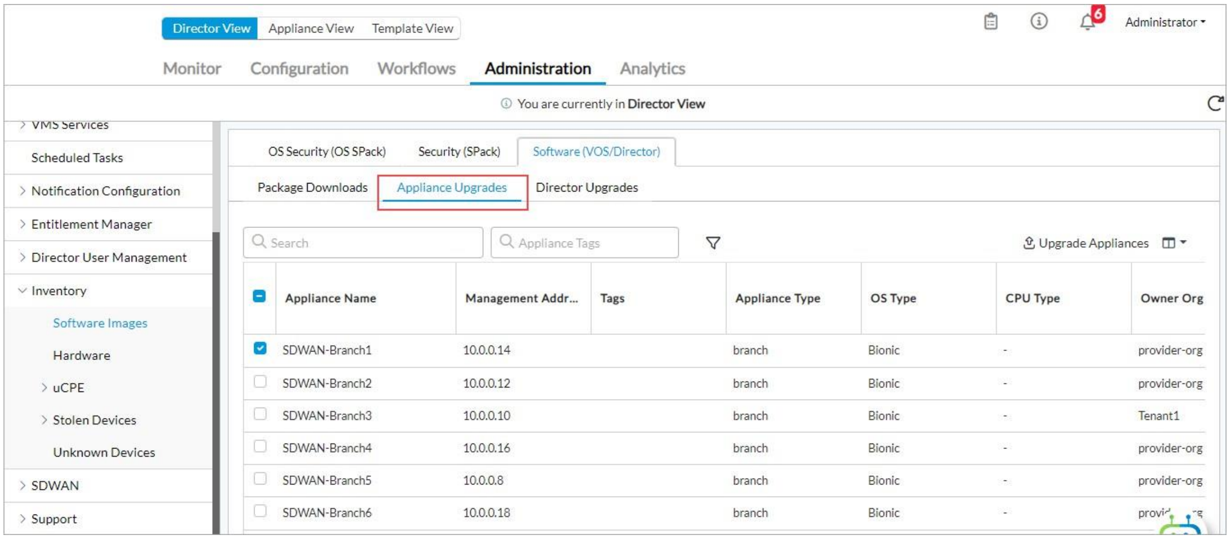
Field	Description
Package Name (Required)	Enter the name of the software package.
Description	Enter a text description for the software package.
Product Type (Required)	Select the product type: ◦ Director—Select for a Director node. ◦ FlexVNF —Select for a VOS device or Controller node.

Package Location (Group of Fields)	Select the location of the software package.
◦ URL	Click, and then enter the URL in the Path field from which to download the software package.
◦ Upload	Click Browse, and then select the software package file.

5. Click Upload. For more information, see Download Controller and VOS Software Image to Director Node.

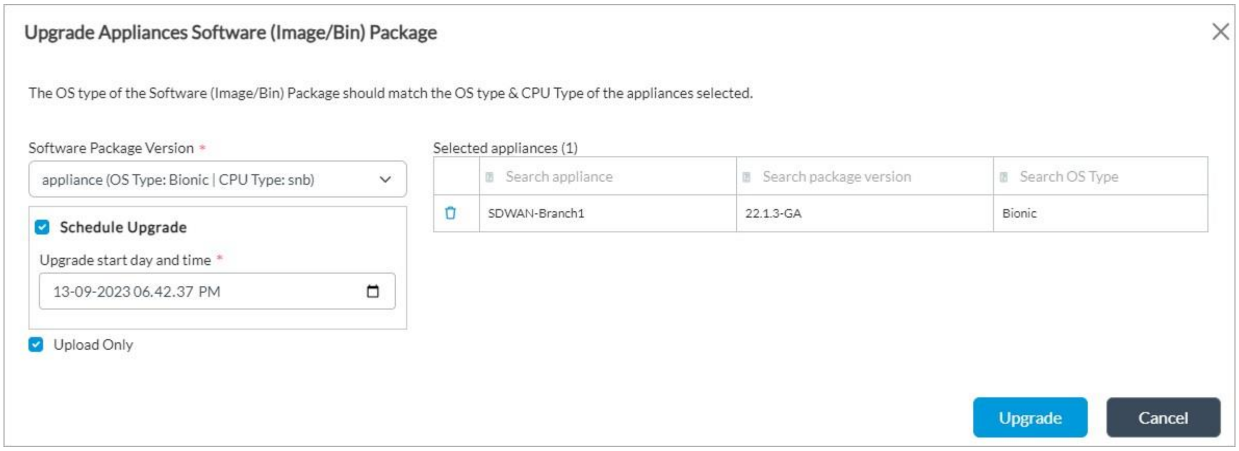
To upgrade a software image on a VOS device:

1. In Director view, select the Administration tab in the top menu bar.
2. Select Inventory > Software Images in the left menu bar.
3. Select the Software (VOS/Director) tab, and then select the Appliance Upgrades tab.



⊟	Appliance Name	Management Addr...	Tags	Appliance Type	OS Type	CPU Type	Owner Org
☑	SDWAN-Branch1	10.0.0.14		branch	Bionic	-	provider-org
☐	SDWAN-Branch2	10.0.0.12		branch	Bionic	-	provider-org
☐	SDWAN-Branch3	10.0.0.10		branch	Bionic	-	Tenant1
☐	SDWAN-Branch4	10.0.0.16		branch	Bionic	-	provider-org
☐	SDWAN-Branch5	10.0.0.8		branch	Bionic	-	provider-org
☐	SDWAN-Branch6	10.0.0.18		branch	Bionic	-	provi rg

4. Select the VOS device or devices on which to upgrade the software, or select the box next to the Appliance Name column to select all devices. The Package Version column in the table displays the current software version installed on the device.
5. Click Upgrade Appliances. The Upgrade Appliances Software Package popup window displays. Enter information for the following fields.



Upgrade Appliances Software (Image/Bin) Package

The OS type of the Software (Image/Bin) Package should match the OS type & CPU Type of the appliances selected.

Software Package Version *: appliance (OS Type: Bionic | CPU Type: snb)

☑ Schedule Upgrade

Upgrade start day and time *: 13-09-2023 06.42.37 PM

☑ Upload Only

Selected appliances (1)

	Search appliance	Search package version	Search OS Type
🗑	SDWAN-Branch1	22.1.3-GA	Bionic

Field	Description
Software Package Version (Required)	Select the software package from the list of downloaded software packages.
Schedule Upgrade (Required)	Click to schedule a date and time for the upgrade to occur. Enter the date in the format *mm/dd/yyyy* (month/date/year), and enter the time in the format *hh*:*mm*:*ss* (hours:minutes:seconds, using 24-hour format for the hours).
Upload Only	Click to upload the software package without upgrading it.
Selected Appliances	Displays the device or devices you selected to upgrade

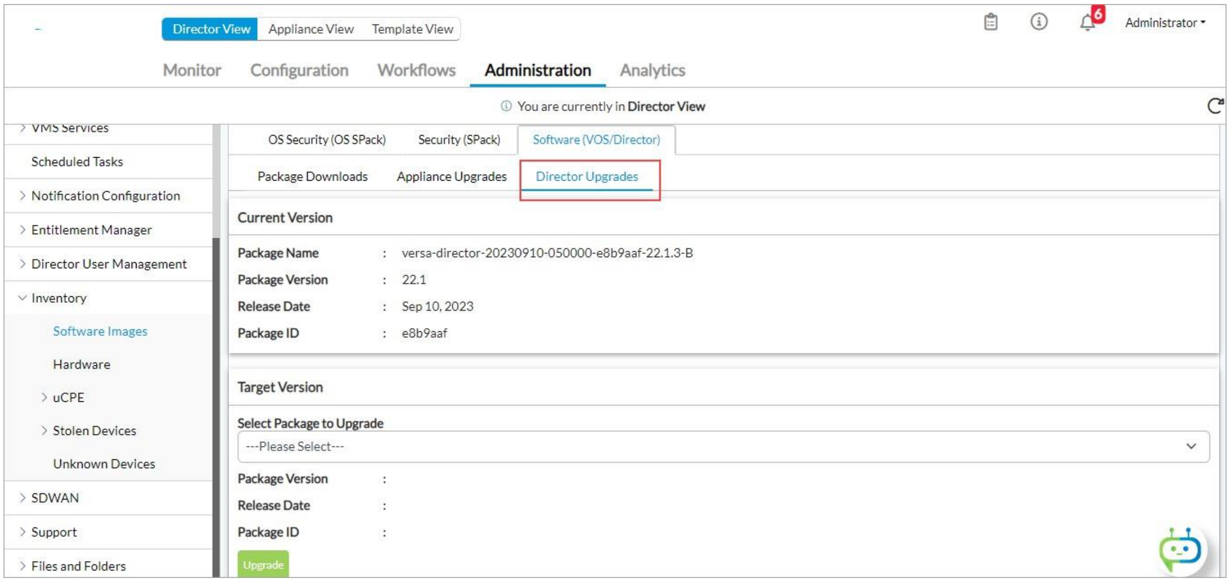
6. Click Upgrade. If you have not set a schedule for upgrade, the software package is upgraded immediately. For more information, see Upgrade a Software Image on a VOS Device.

To update the VOS device using CLI, run the following CLI command:

```
admin@Director$ request system package upgrade filename.bin
```

To install the upgrade on a Director node:

1. In Director view, select the Administration tab in the top menu bar.
2. Select Inventory > Software Images in the left menu bar.
3. Select the Software (VOS/Director) tab, and then select the Director Upgrades tab. The Package Version column in the table displays information about the software package that is installed on the Director node.



Current Version

Package Name : versa-director-20230910-050000-e8b9aaf-22.1.3-B
Package Version : 22.1
Release Date : Sep 10, 2023
Package ID : e8b9aaf

Target Version

Select Package to Upgrade
---Please Select---
Package Version :
Release Date :
Package ID :

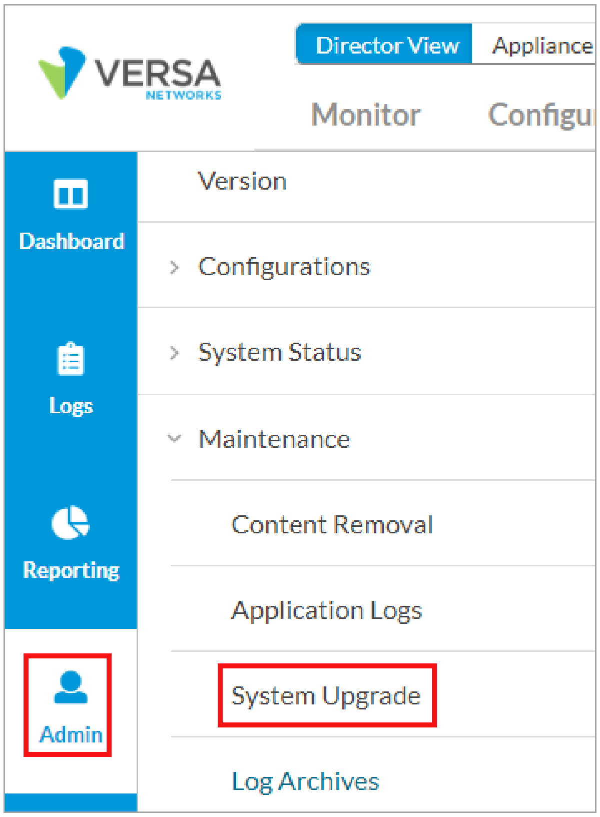
4. In the Target Version box, in the Select Package to Upgrade field, select the package to which to upgrade the Director node.
5. Click Upgrade.

To update the Director node using CLI, run the following CLI command:

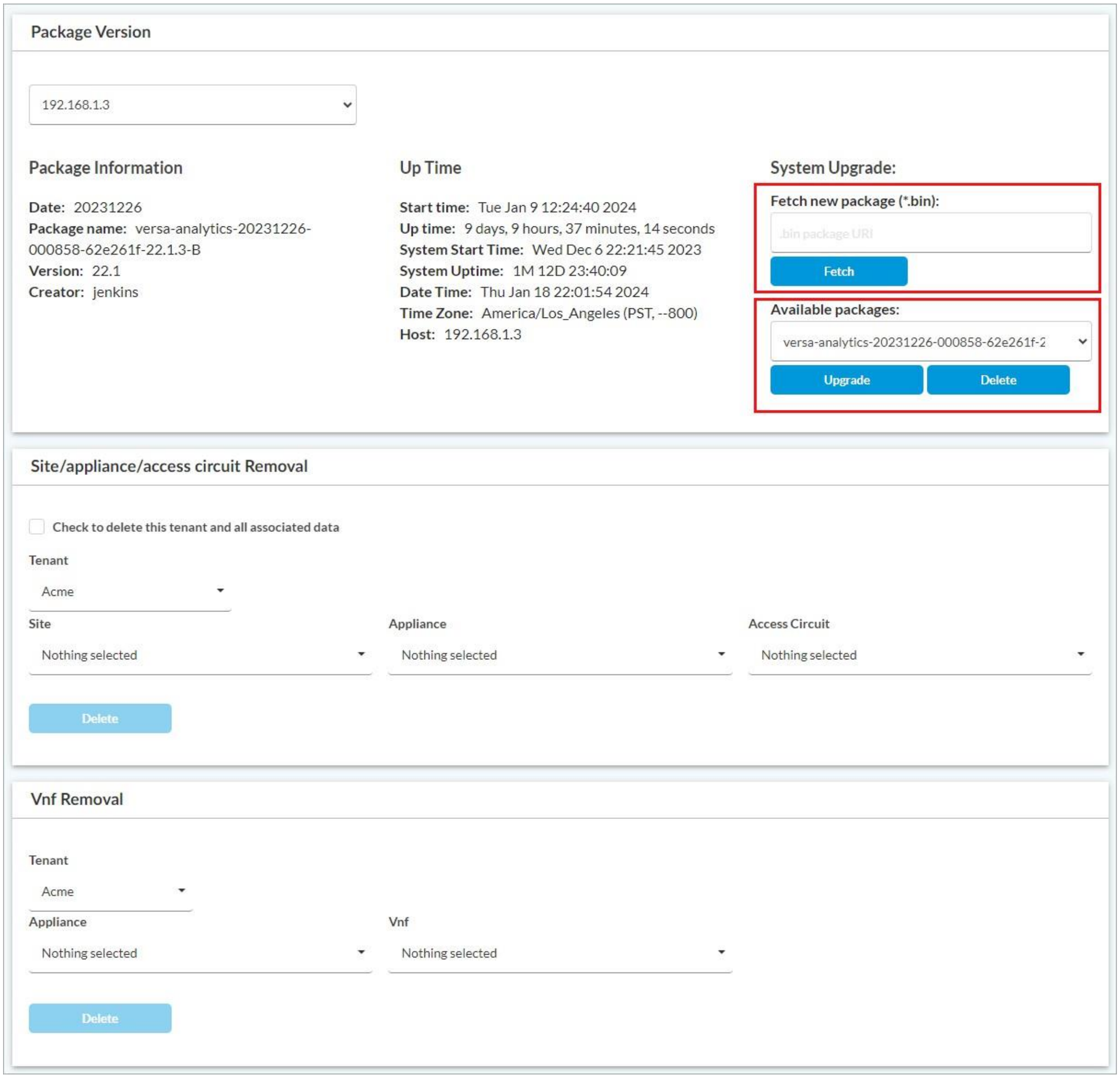
> admin@Director2> **request system package upgrade** *image-filename*

To upgrade an Analytics node:

1. From Director UI Analytics screen, select Admin > Maintenance > System Upgrade in the left menu.



The Package Version window displays.



Package Version

192.168.1.3

Package Information

Date: 20231226
Package name: versa-analytics-20231226-000858-62e261f-22.1.3-B
Version: 22.1
Creator: jenkins

Up Time

Start time: Tue Jan 9 12:24:40 2024
Up time: 9 days, 9 hours, 37 minutes, 14 seconds
System Start Time: Wed Dec 6 22:21:45 2023
System Uptime: 1M 12D 23:40:09
Date Time: Thu Jan 18 22:01:54 2024
Time Zone: America/Los_Angeles (PST, --800)
Host: 192.168.1.3

System Upgrade:

Fetch new package (*.bin): .bin package URI

Available packages: versa-analytics-20231226-000858-62e261f-2

Site/appliance/access circuit Removal

□ Check to delete this tenant and all associated data

Tenant: Acme
Site: Nothing selected
Appliance: Nothing selected
Access Circuit: Nothing selected

Vnf Removal

Tenant: Acme
Appliance: Nothing selected
Vnf: Nothing selected

2. To download an upgrade, specify the package URI in the Fetch new Package (*.bin) field under System Upgrade, and click Fetch.
3. To deploy the upgrade, select the package from the Available Packages field and click Upgrade.

To upgrade the Analytics node using CLI, run the following CLI command:

> admin@Analytics> **request system package upgrade** *filename***.bin**

Configure Intrusion Detection and Prevention

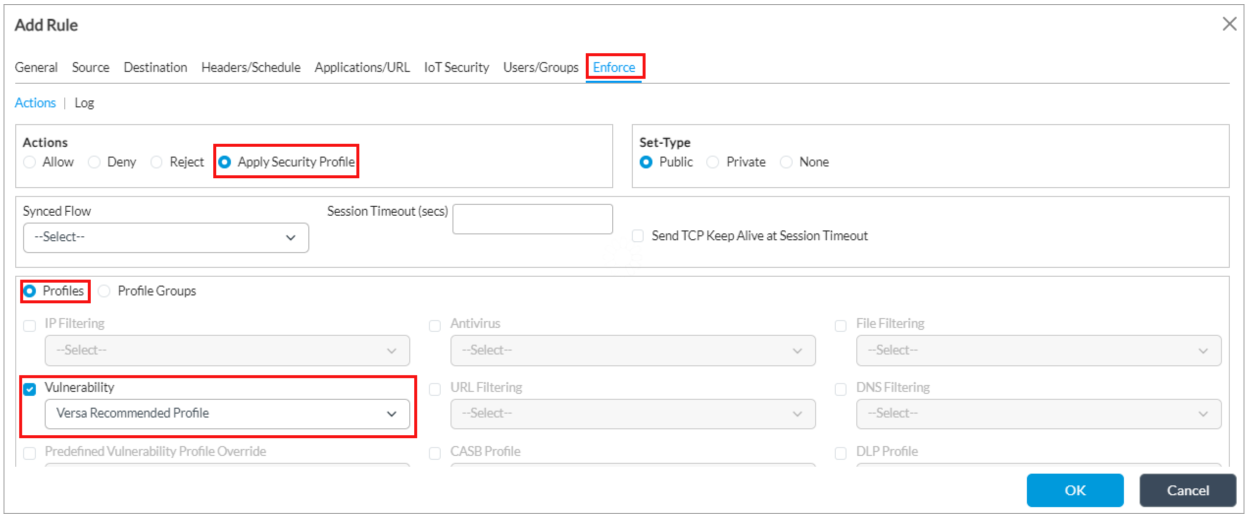
To install the latest set of signatures, you must install the latest security pack security pack (SPack). To set the download settings for SPacks, run the following CLI commands:

```
set security security-package url https://spack.versanetworks.com/versa-updates
set security security-package flavor premium
set security security-package download-type full
```

For more information, see Use Security Packages.

To associate a vulnerability profile with an access policy:

1. Configure an NGFW security access policy. For more information, see Configure a Security Access Policy.
2. Configure an NGFW security rule and apply an vulnerability security profile from the Enforce tab. For more information see, Associate Vulnerability Profiles with Access Policy Profiles.
   a. In Director view:
      I. Select the Administration tab in the top menu bar.
      II. Select Appliance in the left menu bar.
      III. Select an appliance in the main pane. The view changes to Appliance view.
   b. Select Configuration in the top menu bar.
   c. Select Services > Next Gen Firewall > Security > Policies in the left menu bar.
   d. Click the Rules tab to display the access policy rules.
   e. Select a rule or click Add to add a new rule. The Add/Edit Rule popup window displays.
   f. Select the Enforce tab.



Actions: ○ Allow ○ Deny ○ Reject ● Apply Security Profile

Set-Type: ● Public ○ Private ○ None

Synced Flow: --Select--

Session Timeout (secs)

□ Send TCP Keep Alive at Session Timeout

● Profiles ○ Profile Groups

□ IP Filtering: --Select--

□ Antivirus: --Select--

□ File Filtering: --Select--

☑ Vulnerability: Versa Recommended Profile

□ URL Filtering: --Select--

□ DNS Filtering: --Select--

□ Predefined Vulnerability Profile Override

□ CASB Profile

□ DLP Profile

   g. In the Actions section, select Apply Security Profile. When you select this field, the Profiles section, on the lower part of the popup window, is then selected.
   Click Vulnerability and select the vulnerability profile to associate with the security access policy rule. The drop-down includes both predefined and custom vulnerability profiles. It is recommended to use the Versa-

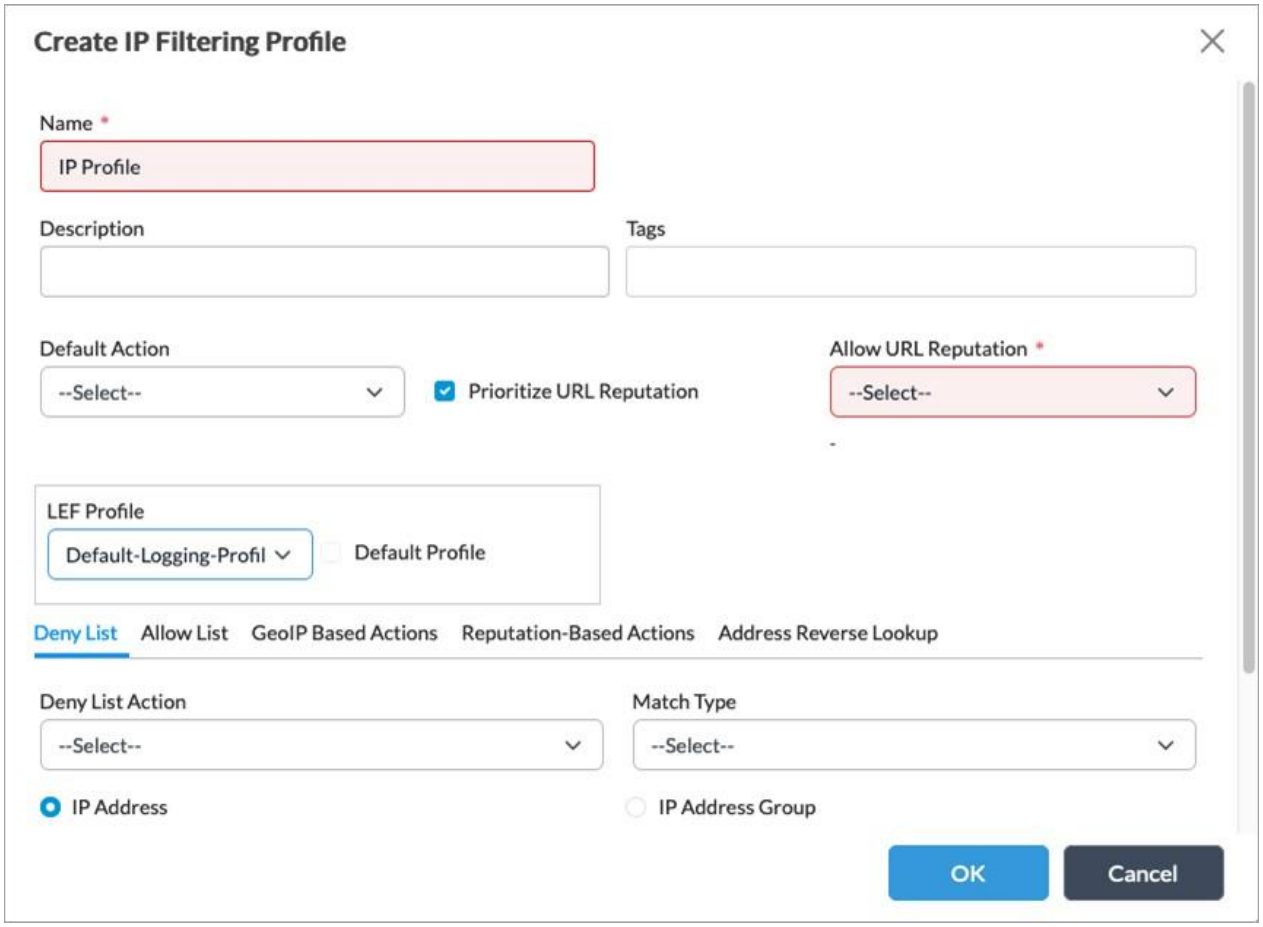
Recommended vulnerability profile.

h. To configure a custom vulnerability rule, see Create Custom Vulnerability Profiles. These rules are displayed in the Vulnerability field drop-down list , under User Defined Profiles.

i. Click OK.
When you configure an NGFW policy with a vulnerability profile, configure the logging profile and log action to ensure that IDS or IPS actions are forwarded to Versa Analytics.

To create access rules based on IP allow and deny lists:

1. Select Services > Next Gen Firewall > Security > Policies in the left menu bar.
2. Click the Rules tab to display the access policy rules.
3. Select a rule or click Add to add a new rule. The Add/Edit Rule popup window displays.
4. Select the Enforce tab.
5. In the Actions section, select Apply Security Profile.
6. From the IP Filtering field, select Add New. In the Create IP Filtering Profile popup window, enter the following information.



Create IP Filtering Profile

Name *: IP Profile

Description:

Tags:

Default Action: --Select--

☑ Prioritize URL Reputation

Allow URL Reputation *: --Select--

LEF Profile: Default-Logging-Profil

□ Default Profile

Deny List | Allow List | GeoIP Based Actions | Reputation-Based Actions | Address Reverse Lookup

Deny List Action: --Select--

Match Type: --Select--

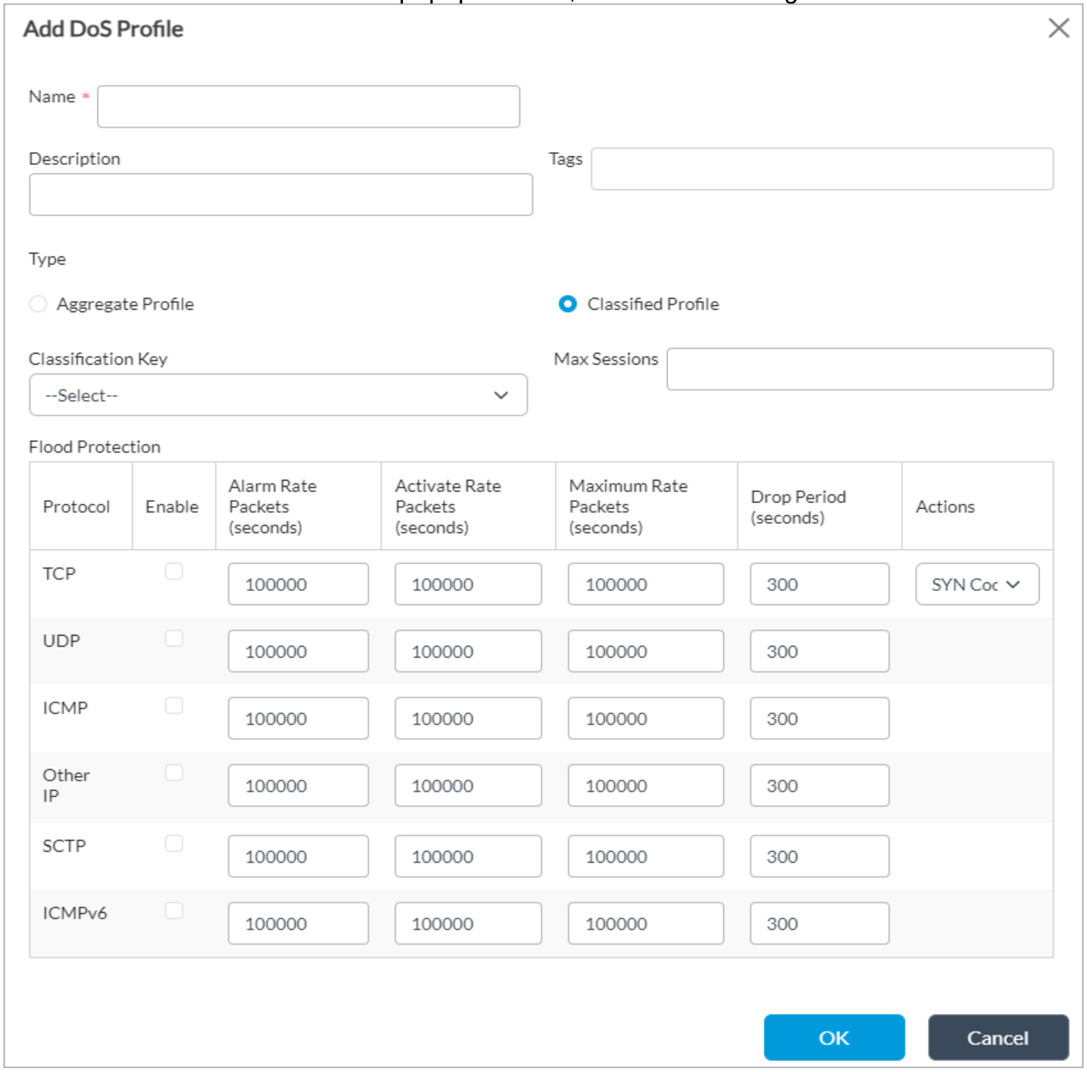
● IP Address ○ IP Address Group

7. Select the LEF Profile.
8. In the Deny List tab, configure the IP deny list by selecting the Deny List Action, Match Type, and IP addresses or groups.
9. In the Allow List tab, configure the IP allow list. For more information, see Configure IP Filtering.

10. Click OK.

To configure DoS protection settings:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliance in the left menu bar.
   c. Select the device from the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Next-Gen Firewall > DoS > Profiles in the left menu bar, or select Services > Stateful Firewall > DoS > Profiles in the left menu bar.
4. Click Add. In the Add DoS Profile popup window, enter the following information.



Add DoS Profile

Name *

Description

Tags

Type

○ Aggregate Profile

● Classified Profile

Classification Key: --Select--

Max Sessions

Flood Protection

Protocol	Enable	Alarm Rate Packets (seconds)	Activate Rate Packets (seconds)	Maximum Rate Packets (seconds)	Drop Period (seconds)	Actions
TCP	□	100000	100000	100000	300	SYN Coc
UDP	□	100000	100000	100000	300	
ICMP	□	100000	100000	100000	300	
Other IP	□	100000	100000	100000	300	
SCTP	□	100000	100000	100000	300	
ICMPv6	□	100000	100000	100000	300	

5. Configure thresholds for the Alarm Rate, Activate Rate, Maximum Rate, Drop Period, and Action (drop method) for TCP, UDP and ICMP protocols. For more information, see Configure DoS Protection.
6. Click OK.

Custom IPS

NGFW provides network protection beyond the protection based on ports, protocols, and IP addresses. In addition to traditional firewall capabilities, NGFW includes filtering functions such as intrusion prevention system (IPS).

IP filtering and vulnerability policies are applied to NGFW security access policies. In the policy, administrators define the traffic to match based on various parameters, such as zones and applications, and configure the policy to enforce the action defined in vulnerability profile.

It is recommended to use the predefined vulnerability profiles, however administrators may create custom vulnerability profiles. Then, the administrator must associate the vulnerability profiles with a next-generation firewall (NGFW) security profile (also called an access policy profile) in an NGFW policy. An NGFW security profile comprises an ordered set of one or more policy rules. Each policy rule comprises a set of match criteria and enforcement actions.

The following protocols are supported for NGFW and IDP inspection policies:

- IPv4
- IPv6
- ICMPv4
- ICMPv6
- TCP
- UDP

Management Ethernet interfaces are logically separated from the Ethernet data ports and cannot be used as a sensor interface. The TSF supports both in-line and promiscuous modes on any available Ethernet data port. A minimum of two Ethernet data ports is required for in-line mode.

Rules may be associated with distinct network interfaces, or groups of interfaces, referred to as zones. A zone profile defines flood protection, scan protection, and traffic anomaly protection information, and it is applied to all traffic flows that enter the zone through the interfaces associated with the zone.

The zone protection profile can detect and prevent the following types of traffic from entering the networks in the zone:

- Traffic floods of various protocols, such as TCP, UDP, and ICMP
- Port scans, host sweeps, and other types of reconnaissance traffic
- Malicious or spoofed packets

Signature based detection applies a set of pre-defined rules or custom rules. Rules are based on the snort rule format. Snort rules are divided into two logical sections, the rule header and the rule options. The rule header contains the rule's action, protocol, source and destination IP addresses and netmasks, and the source and destination ports information, and a series of customizable rule options which cover all the fields described in IPS_SBD_EXT.1.5.

The TSF also supports anomaly detection, which monitors a network for unusual events or trends. Vulnerability profiles

may be configured to compare an observed event with the baseline of the normal traffic. Anomaly detection detects patterns that are normally not present in the traffic, so it is useful for detecting new attacks.
The following actions may be configured in a vulnerability profile which are taken on matching anomaly rules:

- Allow
- Alert
- Drop packet
- Drop session
- Reject
- Reset client
- Reset server

Throughput rates are configured within a DoS protection profile. Time of day settings are configured via Schedule Objects which are applied to NGFW security policies. Frequency options are set under Thresholds within a vulnerability profile. Thresholds may be defined for each Security Scanner, or protocol parser.

Within a zone protection profile, the following options may be selected in order to drop packets involved in attacks as defined in IPS_SBD_EXT.1. These include:

- Fragmented IP packets
- Spoofed IP packets
- Fragmented ICMP packets
- Large ICMP packets
- Packets with improper TCP flags
- Malformed UDP packets

DoS Flood thresholds may be defined for ICMP, IP, TCP, and UDP. For TCP, packets may be randomly dropped or SYN cookies may be used to ensure that valid connections are not dropped during a SYN flood attack. SYN cookies are the default behavior.

IP address filters are based on the following IP address attributes:

- IP reputation—Administrators can create IP-filtering profiles with the following predefined IP reputations:
  - BotNets
  - Denial of service
  - Phishing
  - Proxy
  - Reputation
  - Scanners
  - Spam sources
  - Web attacks
  - Windows exploits

- Geolocation—Versa Networks provides a list of predefined regions that you can use to create IP-filtering profiles based on geolocation.

Administrators define IP-filtering profiles to filter traffic based on the IP address attributes. Each IP-filtering profile object can specify the following:

- Allow lists for IP addresses
- Deny lists for IP addresses
- DNS reverse lookup configurations
- Rules for geolocation-based actions
- Rules for IP reputation–based actions

Administrators can configure rules to match the IP address based on the following match criteria:

- Destination IP address
- Source IP address
- Source and destination IP address
- Source or destination IP address

Administrators can enforce the following actions when a session's IP address matches the conditions in an IP-filtering profile:

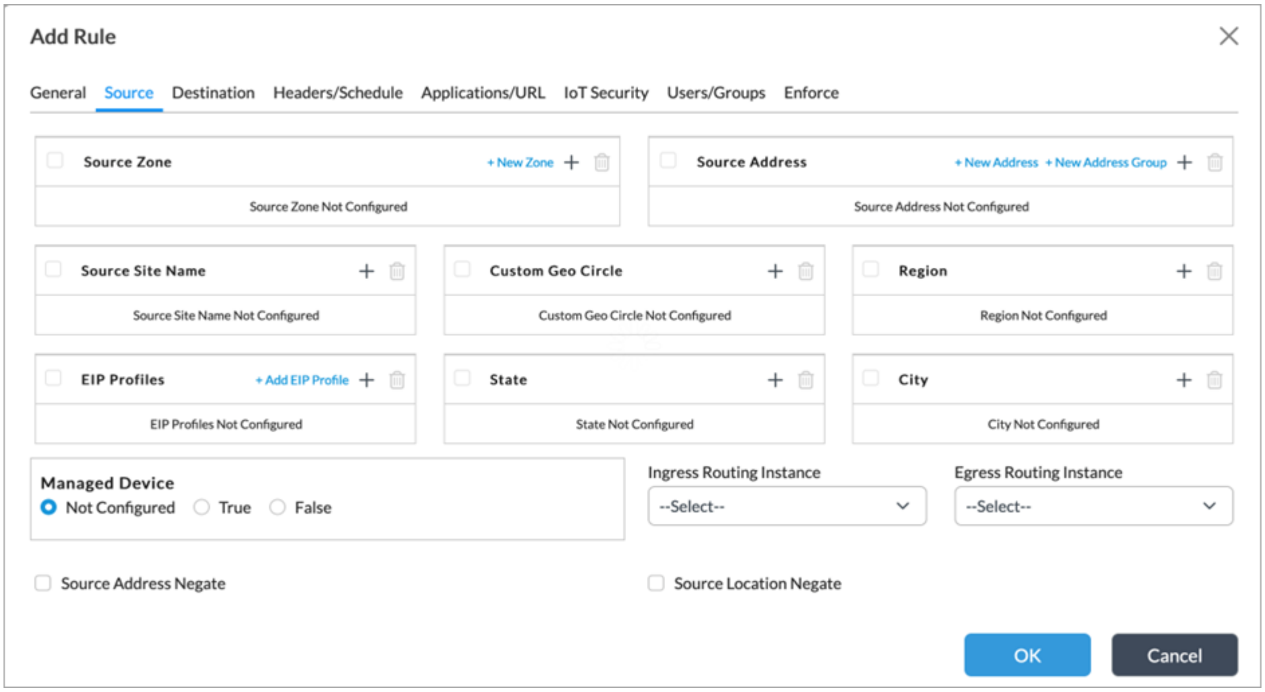
- Allow
- Alert
- Drop packet
- Drop session
- Reset

Configure Stateful and Next-Generation Firewall

To create an NFGW access policy and rule:

1. Or, in Director view:
    1. Select the Administration tab in the top menu bar.
    2. Select Appliance in the left menu bar.
    3. Select the device from the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Next Gen Firewall > Security > Policies in the left menu bar.
4. Click the Add icon to define a policy. For more information, see Configure Access Policies (ACLs).
5. Select the Rules tab.
6. Click the Add icon to define rules for the policy. The Add Rule popup window displays. For more information, see Configure Access Policy Rules (ACL Rules).

7. If you already added one or more rules, the Add popup window displays. VOS processes rules in a top-down order, meaning the top-most applies first, followed by the seconds, until it finds a match. The matching rule action is applied on the network traffic. It is recommended that you order rules from permissive to restrictive to prevent blocking of legitimate traffic. You can add a deny rule to the bottom to handle traffic that does not match any other rules.
8. In the Add Rules screen, select Source tab.



Add Rule

□ Source Zone: Source Zone Not Configured

□ Source Address: Source Address Not Configured

□ Source Site Name: Source Site Name Not Configured

□ Custom Geo Circle: Custom Geo Circle Not Configured

□ Region: Region Not Configured

□ EIP Profiles: EIP Profiles Not Configured

□ State: State Not Configured

□ City: City Not Configured

Managed Device: ● Not Configured ○ True ○ False

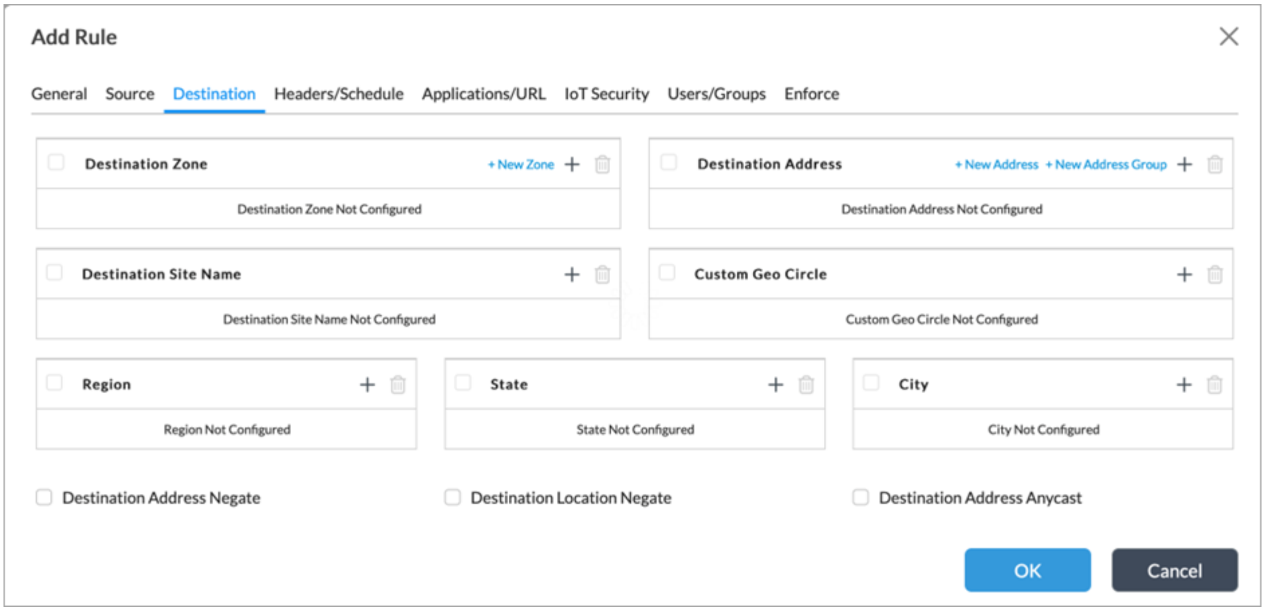
Ingress Routing Instance: --Select--

Egress Routing Instance: --Select--

□ Source Address Negate

□ Source Location Negate

9. Enter a source IP address or address group, or other source details for filtering.
10. To apply the rule to an interface or set of interfaces, add interfaces to a zone and select it in the Source Zone field.
11. Select the Destination tab.


Add Rule
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce
Destination Zone + New Zone
Destination Address + New Address + New Address Group
Destination Site Name
Custom Geo Circle
Region
State
City
OK
Cancel

Destination Zone Not Configured

Destination Address Not Configured

Destination Site Name Not Configured

Custom Geo Circle Not Configured

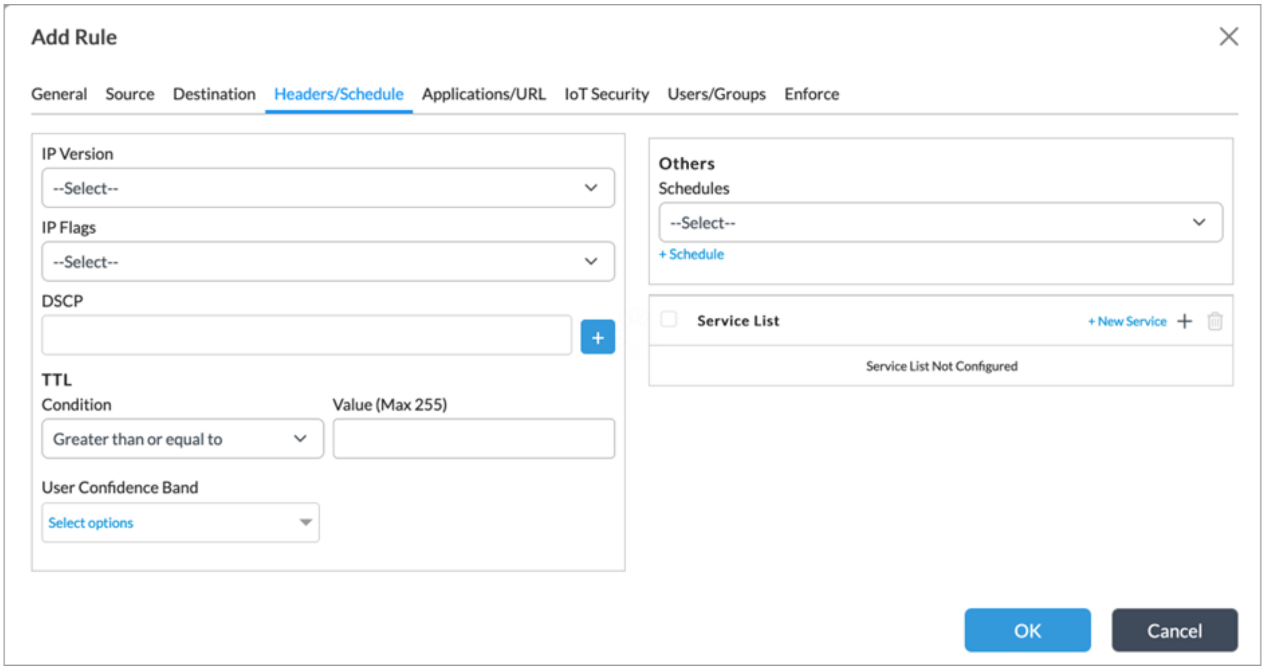
Region Not Configured

State Not Configured

City Not Configured

□ Destination Address Negate □ Destination Location Negate □ Destination Address Anycast

12. Enter destination address or address group and other details for filtering, as required.
13. To apply the rule to an interface or set of interfaces, add interfaces to a zone and select it in the Destination Zone field.
14. Select the Headers/Schedule tab.


Add Rule
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce
Others
+ Schedule
Service List + New Service
TTL
OK
Cancel

IP Version: --Select--

IP Flags: --Select--

DSCP:

Condition: Greater than or equal to

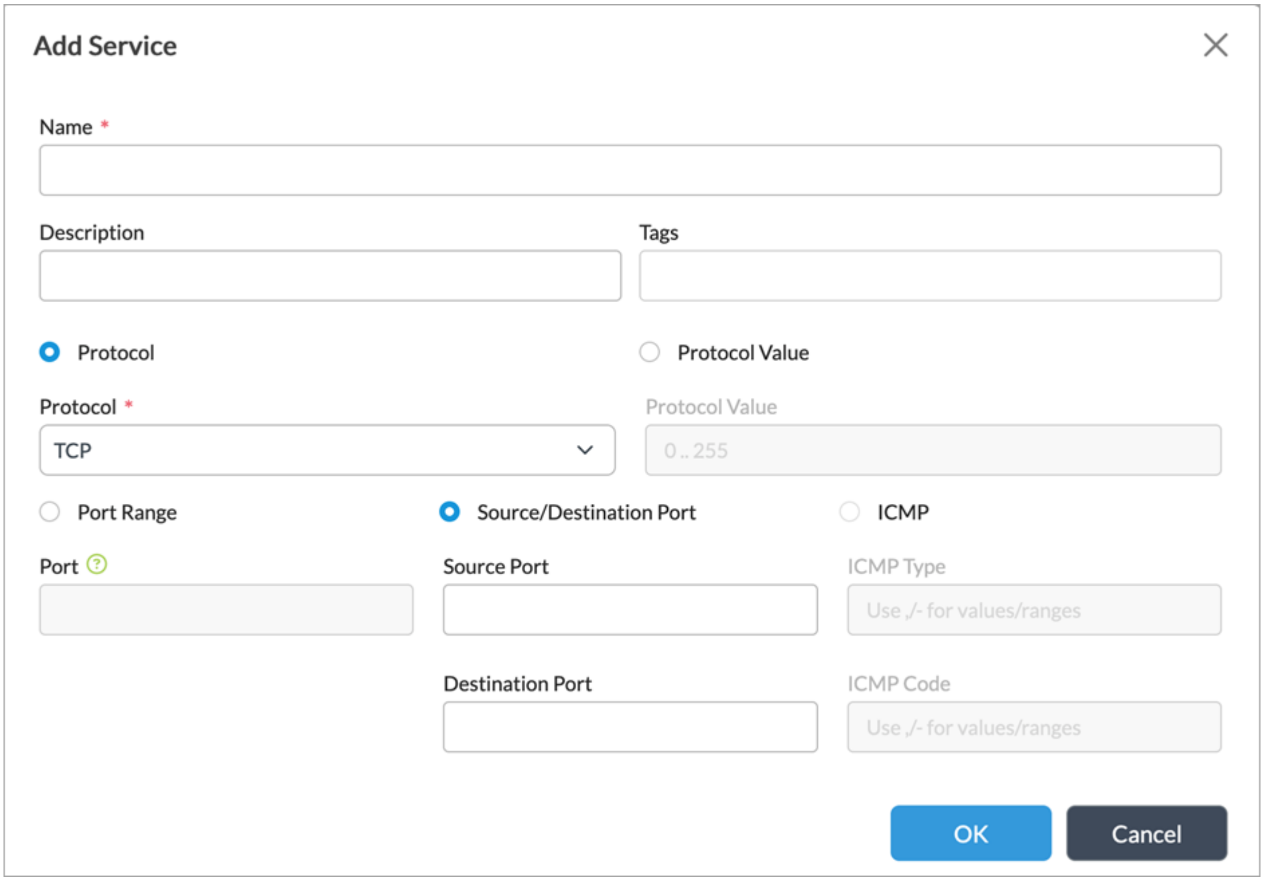
Value (Max 255):

User Confidence Band: Select options

Schedules: --Select--

Service List Not Configured

15. Enter filtering details such as IP version, IP flags, and services.
16. To add a new service, click + New Service. Enter the following information in the Add Service popup window.



Add Service

Name *

Description

Tags

● Protocol ○ Protocol Value

Protocol *: TCP

Protocol Value: 0 .. 255

○ Port Range ● Source/Destination Port ○ ICMP

Port

Source Port

ICMP Type: Use ,/- for values/ranges

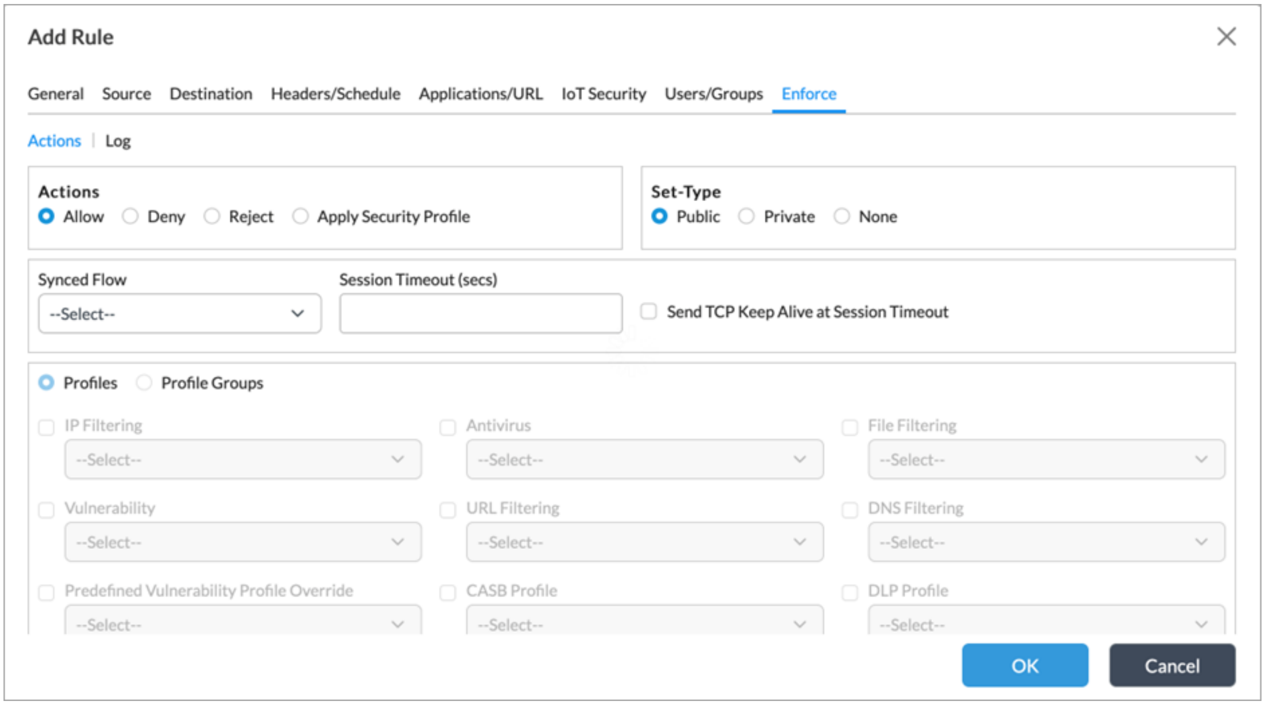
Destination Port

ICMP Code: Use ,/- for values/ranges

a. Enter source and destination ports, along with the protocol and specific type or code values for ICMP.

b. Click OK

17. Select the Enforce tab.



Actions
● Allow ○ Deny ○ Reject ○ Apply Security Profile

Set-Type
● Public ○ Private ○ None

Synced Flow: --Select--

Session Timeout (secs):

□ Send TCP Keep Alive at Session Timeout

● Profiles ○ Profile Groups

□ IP Filtering: --Select--
□ Antivirus: --Select--
□ File Filtering: --Select--
□ Vulnerability: --Select--
□ URL Filtering: --Select--
□ DNS Filtering: --Select--
□ Predefined Vulnerability Profile Override: --Select--
□ CASB Profile: --Select--
□ DLP Profile: --Select--

18. Specify an action (Allow, Deny, Reject, or Apply Security Profile). Apply Security Profile enables application of additional filtering and inspection policies for IDS/IPS.
19. In the Log tab, to generate a log when a rule action applies, select whether the log must be at the start or end of a traffic flow, or both.
20. Then select the logging profile.
21. Click OK.

Certain default or implicit rules automatically filter and, where applicable, log packet drops on most types of malformed or unexpected packets. Most of these implicit rules do not require any configuration. However, apply the following configurations to enforce all mandatory default filtering rules.

To filter out-of-sequence TCP control packets, run the **set system parameters stream-tcp-async-oneside true** CLI command. You must also have a vulnerability profile associated with an access rule governing the traffic.

To log unknown dropped packets destined for the host, run the following **set system session log-unknown-hostbound-packets disable false** CLI command.

Stateful Session Behaviors

VOS devices support routed, or Layer 3, interfaces. The interface associated with each physical network interface (PNIC) or virtual network interface (VNIC) is configured with an IP address. Based on the routing configuration, the traffic from the tenant is forwarded to the interfaces on the VOS device. The VOS device supports several routing instances or virtual routing functions (VRFs). Each VRF is associated with one or more interfaces on the VOS device, and the VOS device supports static routing, BGP, and OSPF.

The traffic of a particular tenant enters a VOS device because the IP address of the routed interface is the next-hop address of the tenant traffic's final destination. Firewall policies can be applied on the traffic entering a VOS device, and the traffic is routed to the next hop (based on routing configuration) only if the security policy allows the traffic to be forwarded.

A VOS firewall device can be installed as a bare metal or a virtual machine (VM). The security policies are applied to the traffic that enters the firewall through physical or virtual interfaces. The VOS firewall recognizes VLAN tags for incoming traffic and adds the appropriate VLAN tags to the outbound traffic.

The following are typical scenarios for configuring traffic on a PNIC:

- Non-VLAN Traffic—Traffic that is not tagged with VLAN and enters the firewall using PNIC is mapped to a single tenant.
- VLAN Traffic—Traffic tagged with VLAN is mapped to one or more tenant. The VOS device creates a unique subinterface for each VLAN. Use one or more VLAN to configure the traffic identification for each tenant hosted on the VOS device.

The following are typical scenarios for configuring traffic on a VNIC:

- VLAN-mapped VNIC— If the VNIC is mapped by the hypervisor to a specific VLAN for the traffic that enters through the PNIC, then when the traffic enters the firewall through the VNIC, the VLAN is already stripped by the hypervisor. Therefore, all the traffic that enters through the VNIC is mapped to a single tenant. In this scenario, a single VNIC cannot support traffic from multiple tenants.
- PNIC-mapped VNIC with non-VLAN traffic—When the hypervisor directly maps the VNIC to the PNIC without any VLAN stripping and if the traffic that enters the firewall through the VNIC is not VLAN tagged, all traffic that enters through the VNIC is mapped to a single tenant.
- PNIC-mapped VNIC with VLAN traffic—When the hypervisor directly maps the VNIC to the PNIC without any VLAN stripping and if the traffic that enters the firewall through the VNIC is VLAN tagged, traffic that belongs to different VLANs is mapped to one or more tenants.
- You create a unique subinterface for each VLAN. You can configure the traffic identification using one or more VLANs for each tenant hosted on the VOS device.

The TSF supports a stateful packet filtering policy, and the following attributes are configurable within stateful traffic filtering rules for the associated protocols:

ICMPv4	Type
	Code
ICMPv6	Type
	Code

IPv4 (RFC 791)	Source address
	Destination Address
	Transport Layer Protocol
IPv6 (RFC 8200)	Source address
	Destination Address
	Transport Layer Protocol
TCP (RFC 793)	Source Port
	Destination Port
UDP (RFC 768)	Source Port
	Destination Port

Versa uses industry-standard network traffic generators to perform interoperability testing to ensure RFC compliance with the above standards.

All interfaces of the TOE are subject to processing rules which can be applied to each distinct network interface or sub-interface as described above.

TSF can classify traffic according to stateful TCP and UDP sessions. To classify traffic, stateful firewall verifies its destination port and then tracks the state of the traffic and monitors every interaction of each connection until it is closed. Stateful firewall grants or rejects access based not only on port and protocol but also on the packet history in the state table. When stateful firewall receives a packet, it checks the state table for an established connection or for a request for the incoming packet from an internal host. If nothing is found, the packet's access is subject to the access policy rule. Connections are removed after administrator-defined protocol timeout values and applied on the next received packet. If the session has been closed, the next received packet would be rejected.

For stateful firewall, Security administrators configure a security access policy to classify traffic using a security access policy. A security access policy includes the stateful firewall rule that collates the defined objects and assigns an action to take based on the match conditions.

Stateful firewall focuses on examining the information in Layer 2 (link layer), Layer 3 (network), and Layer 4 (transport) packets. For these packets, their Layer 3 and 4 information (IP address and TCP/UDP port number) is verified against the information stored in the state table to confirm that they are part of the current exchange. This method increases overall firewall performance because only the initiating packets must be unencapsulated for these layers and all layers up to the application layer (Layer 7).

For more advanced inspection capabilities, stateful targets vital packets for Layer 7 (application) examination, such as the packet that initializes a connection. If the inspected packet matches an existing firewall rule that permits it, the packet is passed and an entry is added to the state table. From this point forward, because the packets in that communication session match an existing state table entry, they are allowed access without a call for further application layer inspection.

Each security access policy consists of one or more rules. Each rule consists of match criteria and enforcement actions. You can use one or more of these traffic attributes to specify the match criteria:

- IP headers
- Domain names
- Services, based on port and protocol
- Source and destination geographic location
- Source and destination IP addresses
- Source and destination zones
- Time-of-day scheduling

For TCP, TSF uses the following attributes to determine if packets are associated with an existing session: source and destination addresses, source and destination ports, sequence number, and individual flags.

While UDP is a stateless protocol, TSF uses the following attributes to determine if packets are associated with an existing session: source and destination addresses, source and destination ports.

ICMP is also a stateless protocol however TSF uses the following attributes to determine if packets are associated with an existing session: source and destination addresses, type, and code.

A rule matches when all match criteria defined in the rule matches. All rules in the security access policy are evaluated starting with the first rule in the policy. The first rule that matches is selected and the corresponding security actions are enforced. No other rules are evaluated once a match is found.

It is recommended that in a security policy to configure more specific rules first and then configure generic rules, followed by a final deny-all rule. The TOE does not prevent administrators from applying conflicting rules.

For a stateful firewall policy, administrators may configure the following enforcement actions:

- Logging
  - Start
  - End

    - Both
    - Never
- Action
    - Allow—Allow sessions that match the configured rule to pass.
    - Deny—Drop sessions that match the rule.
    - Reject—Drop sessions that match the rule and sends a TCP reset (RST) or a UDP ICMP port unreachable message.

You may configure TSF to automatically drop the following packet types within an access policy (which in turn may associated with a LEF profile for logging):

- All fragmented packets (counters)
- Loose-source routing
- Strict-source routing
- Record route
- Broadcast source
- Multicast source
- Loopback source address
- Unspecified or reserved IP (RFC 5735, RFC 3513)
- Packets where the source address is equal to the address of the network interface where the network packet was received
- Packets where the source or destination address of the network packet is a link-local address
- Packets where the source address does not belong to the networks associated with the network interface where the network packet was received – the access policy will determine which zones the rules are associated with and therefore the networks associated with each zone.

TSF implements TCP SYN flood protection under DoS Protection or zone protection profiles. DoS protection is applied where the TOE is deployed at the perimeter of a network on which services are accessed externally through the VOS, where Zone Protection is applicable to an entire zone. Thresholds may be set for the number of TCP packets per second across three levels:

- Alarm rate—The rate at which a log is generated
- Action rate—The rate at which TOE drops packets. By default, the firewall uses SYN Cookies to track valid connections, but may be configured to randomly drop packets.
- Maximum rate—The rate at which all packets are dropped for a configurable duration.

Stale connections (including half-open connections) are removed after the defined protocol timeout value.

Self-Test Errors

Versa products perform a suite of FIPS 140-2 self-tests during power-up and re-boot. If any of the self-test fails, the product does not enter operational state and the serial console CLI and system logs display an error message indicating a self-test failure. If this occurs, you must reboot the device. If the product still does not enter operational state, contact Versa Support.

The following errors that can occur during self-tests:

- Failure to verify integrity of Versa application binaries.
- Failure to satisfy cryptographic self-test condition (for example, known-answer test failure).
- Failure of entropy source.
- Failure to instantiate a system service.
- Hardware or virtualization platform related errors.

You can clear most error conditions by issuing the **vsh restart** CLI command to restart Versa applications. If the error condition persists, ensure that the product has been installed according to Versa documentation. Contact Versa Support if you require further assistance.

Audit Events

Each Versa appliance generates an audit event for each user interaction with the applicable interface. Each event includes at least a timestamp, the username of the user whose action generated the event, a source IP address, and text describing the event.

The device stores each audit log record and only an authorized administrator can view it. Apart from storing records locally, you can configure the device to transmit audit log records to a remote auditing server over a trusted channel using IPsec.

Audit Events

The following table describes the audit events.

Requirement	Audit Event	Additional Audit Content	Example Audit Record
FAU_GEN.1 and FAU_GEN.1/VPN	Startup and shutdown of the audit function	None.	**Start up:** YYYY-MM-DD HH:MM:SS Director1 systemd[1]: Starting Security Auditing Service... **Shut down:** YYYY-MM-DD HH:MM:SS Director1 systemd[1]: Stopped Security Auditing Service.

Requirement	Audit Event	Additional Audit Content	Example Audit Record
	Indication that TSF self-test was completed		YYYY-MM-DD HH:MM:SS INFO FIPS Integrity test for openssl-lib passed. 1s YYYY-MM-DD HH:MM:SS INFO Invoking versa-vsmd prestart AES Selftest PASSED
	Failure of self-test		YYYY-MM-DD HH:MM:SS INFO Starting FIPS integrity test for: versa-vsmd Signature match for /opt/versa/bin/versa-vsmd Failed! YYYY-MM-DD HH:MM:SS INFO FIPS Integrity test for versa-vsmd failed

FCO_CPC_EXT.1	•Enabling communications between a pair of components.
	•Disabling communications between a pair of components.
		Identities of the endpoints pairs enabled or disabled.	**Enable:**
			[DD-MM-YYYY HH:MM:SS][INFO] Administrator@ ProviderDataCenterSystemAdmin, 172.16.16.253:18292, create, , appliances: SDWAN-Branch2 , changeset:devices { device{SDWAN-Branch2} { _operations } }
			Disable:
			[DD-MM-YYYY HH:MM:SS][INFO] Administrator@ ProviderDataCenterSystemAdmin, 172.16.16.253:13399, delete, appliance:32e09cdc-26fa-40f6-9ac2-c70e8d66ffaa , changeset:{"delete-appliance":{"applianceuuid":"32e09cdc-26fa-40f6-9ac2-c70e8d66ffaa","clean-config":false,"reset-config":false,"load-defaults":false}}

FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Reason for failure.	**Refer to FCS_TLSS_EXT.1**
FCS_IPSEC_EXT.1	Failure to establish an IPSec SA.	Reason for failure.	**Valid connection:** YYYY-MM-DD HH:MM:SS Controller1 ipsec-log 2023-10-05 10:20:31.202 INFO [0x200] IKE-Event: IKEv2 SA [Initiator] negotiation completed: YYYY-MM-DD HH:MM:SS Controller1 ipsec-log IKE (Done) : local: 172.1.1.3, peer: 172.1.1.254, role: [initiator] YYYY-MM-DD HH:MM:SS Controller1 ipsec-log YYYY-MM-DD HH:MM:SS INFO [0x200] IKE-Event: IPsec SA [Initiator, tunnel, auto] negotiation completed: YYYY-MM-DD HH:MM:SS Controller1 ipsec-log IPSEC (Done) : local: 172.1.1.3, peer: 172.1.1.254, role: [initiator]

Requirement	Audit Event	Additional Audit Content	Example Audit Record
			YYYY-MM-DD HH:MM:SS Controller1 ipsec-log local spi: 0xce926891 remote spi: 0x2006c88 **No Proposal Chosen / IKE weaker than ESP:** YYYY-MM-DD HH:MM:SS Controller1 ipsec-log IKE (Failed) : local: 172.1.1.3, peer: 172.1.1.254, role: [initiator] YYYY-MM-DD HH:MM:SS Controller1 ipsec-log Error: No proposal chosen **Invalid Certificate:** YYYY-MM-DD HH:MM:SS INFO [0x200] IKE-Event: Validation failed for remote identity '172.1.1.254 (ipv4)' and remote certificate 'C=US, ST=MD, L=Catonsville, O=GSS, CN=tl18-16x.example.com' (S/N=157) against trust anchor 'C=US, ST=MD, L=Catonsville, O=GSS, CN=rootca-rsa' (S/N=65537) YYYY-MM-DD HH:MM:SS ERROR [0x200] IKE-Event: Reason: Certificate was not found **Mismatched Identifier:** YYYY-MM-DD HH:MM:SS Controller1 ipsec-log IKE (Failed) : local: 172.1.1.3, peer: 172.1.1.254, role: [initiator] YYYY-MM-DD HH:MM:SS Controller1 ipsec-log Error: Authentication failed YYYY-MM-DD HH:MM:SS Controller1 versa-vmod: [ipsec] [ipsecIkeAuthFailure] [YYYY-MM-DD HH:MM:SS] versa: IKE authentication with peer 172.1.1.254 (routing-instance WAN1-Transport-VR, interface tvi-0/20.0, vpn Reference-Identifiers) failed

FCS_NTP_EXT.1	• Configuration of a new time server
	• Removal of configured time server
		Identity of new/removed time server.	**Configuration:**
			[DD-MM-YYYY HH:MM:SS][INFO] Administrator@ProviderDataCenterSystemAdmin, 172.16.16.253:58683, create, server:172.16.16.254 , changeset:system { ntp { + server{172.16.16.254} } }
			[DD-MM-YYYY HH:MM:SS][INFO] Administrator@ProviderDataCenterSystemAdmin, 172.16.16.253:59366, modify, server:172.16.16.254 , changeset:system { ntp { server{172.16.16.254} { - version 4 } } }

Requirement	Audit Event	Additional Audit Content	Example Audit Record
			Removal: [DD-MM-YYYY HH:MM:SS][INFO] Administrator@ProviderDataCenterSystem Admin, 172.16.16.253:20263, delete, server:172.1.1.200 , changeset:system { ntp { - server{172.1.1.200} { - version 4} } }
FCS_SSHS_EXT .1	Failure to establish an SSH session.	Reason for failure.	**Valid connection:** YYYY-MM-DD HH:MM:SS Director1 sshd[5024]: Accepted password for admin from 172.16.16.254 port 48398 ssh2 YYYY-MM-DD HH:MM:SS Director1 sshd[5024]: pam_unix(sshd:session): session opened for user admin by (uid=0) YYYY-MM-DD HH:MM:SS Director1 systemd-logind[4058]: New session 2286 of user admin. YYYY-MM-DD HH:MM:SS Director1 sshd[12168]: Accepted publickey for admin from 172.16.16.254 port 43788 ssh2: RSA SHA256:CHOqCdF3BT4v2NAlWL78B1z+YVg1UzBy4YhETEYuGng **Bad Cipher:** YYYY-MM-DD HH:MM:SS Director1 sshd[2264]: Unable to negotiate with 172.16.16.254 port 47186: no matching cipher found. Their offer: aes128-cbc [preauth] **Bad Auth Alg:** YYYY-MM-DD HH:MM:SS Director1 sshd[2610]: Unable to negotiate with 172.16.16.254 port 47560: no matching host key type found. Their offer: ssh-rsa [preauth] **Bad MAC Alg:** YYYY-MM-DD HH:MM:SS Director1 sshd[2629]: Unable to negotiate with 172.16.16.254 port 47806: no matching MAC found. Their offer: hmac-sha1 [preauth] **Bad Kex Alg:** YYYY-MM-DD HH:MM:SS Director1 sshd[2648]: Unable to negotiate with 172.16.16.254 port 47870: no matching key exchange method found. Their offer: diffie-hellman-group14-sha1,ext-info-c [preauth]
FCS_TLSS_EXT. 1	Failure to establish a TLS Session.	Reason for failure.	**No Shared Cipher / Invalid Key Exchange:** javax.net.ssl|ERROR|38|https-jsse-nio-

Requirement	Audit Event	Additional Audit Content	Example Audit Record
			127.0.0.1-8443-exec-13|YYYY-MM-DD HH:MM:SS TZ|TransportContext.java:352|Fatal (HANDSHAKE_FAILURE): no cipher suites in common **Wrong Version:** javax.net.ssl|ERROR|3B|https-jsse-nio-127.0.0.1-8443-exec-16| YYYY-MM-DD HH:MM:SS TZ |TransportContext.java:352|Fatal (PROTOCOL_VERSION): Client requested protocol TLSv1.1 is not enabled or supported in server context **Modified Finished Message:** javax.net.ssl|ERROR|68|https-jsse-nio-127.0.0.1-8443-exec-61|YYYY-MM-DD HH:MM:SS TZ|TransportContext.java:352|Fatal (DECRYPT_ERROR): The Finished message cannot be verified.
FIA_AFL.1	Unsuccessful login attempt limit is met or exceeded.	Origin of the attempt (e.g., IP address).	**WebUI:** [DD-MM-YYYY HH:MM:SS][INFO] GSS-Test-User, 172.16.16.253:9183, Login Failed, Invalid Username or Password, : [DD-MM-YYYY HH:MM:SS][INFO] GSS-Test-User, 172.16.16.253:9183, Login Failed, GSS-Test-User is Locked, : **SSH:** YYYY-MM-DD HH:MM:SS Director1 sshd[3077]: Failed password for gsstestuser from 172.16.16.254 port 44576 ssh2 YYYY-MM-DD HH:MM:SS Director1 sshd[3077]: error: maximum authentication attempts exceeded for gsstestuser from 172.16.16.254 port 44576 ssh2 [preauth] YYYY-MM-DD HH:MM:SS Director1 sshd[3077]: Disconnecting authenticating user gsstestuser 172.16.16.254 port 44576: Too many authentication failures [preauth] YYYY-MM-DD HH:MM:SS Director1 sshd[3077]: pam_listfile(sshd:auth): Refused user gsstestuser for service sshd YYYY-MM-DD HH:MM:SS Director1 sshd[3077]: pam_faillock(sshd:auth): Consecutive login failures for user gsstestuser account temporarily locked
FIA_UAU_EXT.2	All use of identification and authentication	Origin of the attempt (e.g., IP address).	**Refer to FIA_UIA_EXT.1**

Requirement	Audit Event	Additional Audit Content	Example Audit Record
	mechanism.		
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	**Console Login Success:** YYYY-MM-DD HH:MM:SS Director1 login[3735]: pam_unix(login:session): session opened for user admin by LOGIN(uid=0) YYYY-MM-DD HH:MM:SS Director1 systemd-logind[4058]: New session 2266 of user admin. **Console Login Failure:** YYYY-MM-DD HH:MM:SS Director1 login[3500]: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=/dev/tty1 ruser= rhost= user=admin YYYY-MM-DD HH:MM:SS Director1 login[3500]: FAILED LOGIN (1) on '/dev/tty1' FOR 'admin', Authentication failure **SSH Login Success:** YYYY-MM-DD HH:MM:SS Director1 sshd[5024]: Accepted password for admin from 172.16.16.254 port 48398 ssh2 YYYY-MM-DD HH:MM:SS Director1 sshd[5024]: pam_unix(sshd:session): session opened for user admin by (uid=0) YYYY-MM-DD HH:MM:SS Director1 systemd-logind[4058]: New session 2286 of user admin. **SSH Login Failure:** YYYY-MM-DD HH:MM:SS Director1 sshd[4779]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.16.16.254 user=admin YYYY-MM-DD HH:MM:SS Director1 sshd[4779]: Failed password for admin from 172.16.16.254 port 48378 ssh2 **SSH Public Key Success:** YYYY-MM-DD HH:MM:SS Director1 sshd[12168]: Accepted publickey for admin from 172.16.16.254 port 43788 ssh2: RSA SHA256:CHOqCdF3BT4v2NAlWL78B1z+YVg1UzBy4YhETEYuGng **SSH Public Key Failure:** YYYY-MM-DD HH:MM:SS Director1 sshd[4779]: pam_unix(sshd:auth): authentication failure; logname= uid=0

Requirement	Audit Event	Additional Audit Content	Example Audit Record
			euid=0 tty=ssh ruser= rhost=172.16.16.254 user=admin **WebUI Success:** [DD-MM-YYYY HH:MM:SS][INFO] Administrator, 172.16.16.253:9183, Login, : **WebUI Failure:** [DD-MM-YYYY HH:MM:SS][INFO] Administrator, 172.16.16.253:9183, Login Failed, Invalid Username or Password, :
FIA_X509_EXT.1 / Rev	•Unsuccessful attempt to validate a certificate •Any addition, replacement or removal of trust anchors in the TOE's trust store	•Reason for failure of certificate validation •Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store	**Trust Anchor Addition:** [DD-MM-YYYY HH:MM:SS][INFO] Administrator@ProviderDataCenterSystemAdmin, 172.16.16.253:64587, upload-to-vd, security:rootca-ecdsa.pem,32febf11-3ab5-46e2-95ea-dcd8f90705ba,ca-chain **Trust Anchor Deletion:** [DD-MM-YYYY HH:MM:SS][INFO] Administrator@ProviderDataCenterSystemAdmin, 172.16.16.253:64625, delete-from-vd, security:rootca-ecdsa.pem,32febf11-3ab5-46e2-95ea-dcd8f90705ba,ca-chain **Expired cert:** YYYY-MM-DD HH:MM:SS INFO [0x200] IKE-Event: Validation failed for remote identity '172.1.1.254 (ipv4)' and remote certificate 'C=US, ST=MD, L=Catonsville, O=GSS, CN=tl18-16x.example.com' (S/N=135) against trust anchor 'C=US, ST=MD, L=Catonsville, O=GSS, CN=rootca-rsa' (S/N=65537) YYYY-MM-DD HH:MM:SS ERROR [0x200] IKE-Event: Reason: Certificate is not valid at this time **Corrupt ASN.1:** YYYY-MM-DD HH:MM:SS WARN [0x200] IKE-Event: Could not decode certificate. The certificate may be corrupted or it was given in unrecognized format (file format may be wrong) **Invalid Signature:** YYYY-MM-DD HH:MM:SS INFO [0x200] IKE-Event: Validation failed for remote identity '172.1.1.254 (ipv4)' and remote certificate 'C=US, ST=MD, L=Catonsville, O=GSS, CN=tl18-16x.example.com' (S/N=364) against trust anchor 'C=US, ST=MD, L=Catonsville, O=GSS,

Requirement	Audit Event	Additional Audit Content	Example Audit Record
			CN=rootca-rsa' (S/N=65537) YYYY-MM-DD HH:MM:SS ERROR [0x200] IKE-Event: Reason: Certificate signature verification failed **Invalid CA:** YYYY-MM-DD HH:MM:SS INFO [0x200] IKE-Event: Validation failed for remote identity '172.1.1.254 (ipv4)' and remote certificate 'C=US, ST=MD, L=Catonsville, O=GSS, CN=tl18-16x.example.com' (S/N=157) against trust anchor 'C=US, ST=MD, L=Catonsville, O=GSS, CN=rootca-rsa' (S/N=65537) YYYY-MM-DD HH:MM:SS ERROR [0x200] IKE-Event: Reason: Certificate was not found **OCSP Revoked cert:** DEBUG: YYYY-MM-DD HH:MM:SS L-0 SshIkev2StatePkAuth/ikev2-pk-auth.c:448/vs_ikev2_check_ocsp_revocation_cb: [7f6a89421108/7f6b66809f48] OCSP: [REPLY] Error: Peer certificate is Revoked! TID 2 VRF 9 DEBUG: YYYY-MM-DD HH:MM:SS L-3 SshIkev2State/ikev2-state.c:353/ikev2_state_error: [7f6a89421108/7f6b66809f48] Negotiation failed because of error Authentication failed (24) TID 2 VRF 9 **No OCSP Signing Purpose:** YYYY-MM-DD HH:MM:SS VsOcspClient/vs_ocsp.c:984/vs_ocsp_public_key_add: OCSP: EKU ocsp-signing is false! **Explicit EC Certificate:** YYYY-MM-DD HH:MM:SS INFO [0x200] IKE-Event: Validation failed for remote identity '172.1.1.254 (ipv4)' and remote certificate 'C=US, ST=MD, L=Catonsville, O=GSS, CN=tl18-16x.example.com' (S/N=157) against trust anchor 'C=US, ST=MD, L=Catonsville, O=GSS, CN=rootca-ecdsa' (S/N=65537) YYYY-MM-DD HH:MM:SS ERROR [0x200] IKE-Event: Reason: Certificate path construction did not succeed
FMT_MOF.1/ ManualUpdate	Any attempt to initate a manual update.		**Refer to FPT_TUD_EXT.1**

Requirement	Audit Event	Additional Audit Content	Example Audit Record
FMT_MTD.1/CryptoKeys	Management of cryptographic keys		**Refer to FIA_X509_EXT.1 for Trust Anchor Addition and Deletion**
FMT_SMF.1	All management activities of TSF data.		**Refer to FMT_SMF.1 Management Functions below**
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure).		**Initiation:** [DD-MM-YYYY HH:MM:SS][INFO] Administrator, CLI 'request system package upgrade versa-director-20240110-220801-4a087e1-22.1.3-B-fips.bin' DD-MM-YYYY, HH:MM:SS __main__ [INFO] Pre-Upgrade-Validation Successful DD-MM-YYYY, HH:MM:SS __main__ [INFO] Upgrading Versa Director from versa-director-20231022-050000-45aaddd-22.1.3-B-fips.bin to versa-director-20240110-220801-4a087e1-22.1.3-B-fips.bin **Success:** DD-MM-YYYY, HH:MM:SS __main__ [INFO] Upgrade to versa-director-20240110-220801-4a087e1-22.1.3-B-fips.bin successful! **Failure:** DD-MM-YYYY, HH:MM:SS __main__ [INFO] Failed to initiate upgrade to versa-director-20230504-172406-5317a45-22.1.1-B-fips.bin
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).	YYYY-MM-DD HH:MM:SS Director1 admin: admin [19798]: YYYY-MM-DD HH:MM:SS sudo timedatectl set-time YYYY-MM-DD HH:MM:SS' [0] YYYY-MM-DD HH:MM:SS Director1 systemd-timedated[20044]: Changed local time to dd MM DD HH:MM:SS YYYY
FTA_SSL_EXT.1 (if 'terminate the session' is selected)	The termination of a local session by the session locking mechanism.		YYYY-MM-DD HH:MM:SS Director1 login[16126]: pam_unix(login:session): session closed for user admin YYYY-MM-DD HH:MM:SS Director1 systemd-logind[4161]: Removed session 418.

Requirement	Audit Event	Additional Audit Content	Example Audit Record
FTA_SSL.3	The termination of a remote session by the session locking mechanism.		**WebUI Session Lock:** [DD-MM-YYYY HH:MM:SS][INFO] Administrator, 127.0.0.1:9183, Logout, : **SSH Session Lock:** YYYY-MM-DD HH:MM:SS Director1 sshd[10955]: Timeout, client not responding from user gsstestuser 172.16.16.254 port 46382
FTA_SSL.4	The termination of an interactive session.		**WebUI Logout:** [DD-MM-YYYY HH:MM:SS][INFO] Administrator, 127.0.0.1:9183, Logout, : **Console Logout:** YYYY-MM-DD HH:MM:SS Director1 login[3735]: pam_unix(login:session): session closed for user admin YYYY-MM-DD HH:MM:SS Director1 systemd-logind[4058]: Removed session 2266. **SSH Logout:** YYYY-MM-DD HH:MM:SS Director1 sshd[5031]: Received disconnect from 172.16.16.254 port 48398:11: disconnected by user YYYY-MM-DD HH:MM:SS Director1 sshd[5031]: Disconnected from user admin 172.16.16.254 port 48398 YYYY-MM-DD HH:MM:SS Director1 sshd[5024]: pam_unix(sshd:session): session closed for user admin YYYY-MM-DD HH:MM:SS Director1 systemd-logind[4058]: Removed session 2286.
FTP_ITC.1	•Initiation of the trusted channel. •Termination of the trusted channel. •Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.	**Refer to FCS_IPSEC_EXT.1**
FTP_TRP.1/Admin	•Initiation of the trusted channel. •Termination of the trusted channel. •Failure of the trusted channel functions.		**Audits for the initiation of SSH and TLS protected WebUI sessions are shown in FIA_UIA_EXT.1.** **Termination of SSH and TLS protected WebUI sessions are shown in FTA_SSL.4.** **SSH remote administration session failures are shown in FCS_SSHS_EXT.1.**

Requirement	Audit Event	Additional Audit Content	Example Audit Record
			TLS protected WebUI remote administration connection failures are shown in FCS_TLSS_EXT.1.

Management Functions (FMT_SMF.1)

The following table describes the audit events for management function FMT_SMF.1.

Requirement	Audit Event	Audit Content
FMT_SMF.1	Ability to administer the TOE locally and remotely.	**Refer to FIA_UIA_EXT.1**
	Ability to configure the access banner.	[DD-MM-YYYY HH:MM:SS][INFO] Administrator@ProviderDataCenterSystemAdmin, 172.16.16.253:63977, enable- banner, settings
	Ability to configure the session inactivity time before session termination or locking.	**WebUI:** [DD-MM-YYYY HH:MM:SS][INFO] Administrator@ProviderDataCenterSystemAdmin, 172.16.16.253:63995, UpdateUser, user , changeset:{"update-user":{"user":{"name":"Administrator","idle- time-out":"15"}}} **SSH and Console:** [DD-MM-YYYY HH:MM:SS][INFO] Administrator@ProviderDataCenterSystemAdmin, 172.16.16.254:55086, update- bash-shell-settings, settings
	Ability to update the TOE, and to verify the updates using [digital signature, hash comparison] capability prior to installing those updates.	**Refer to FPT_TUD_EXT.1**

Requirement	Audit Event	Audit Content
	Ability to configure the authentication failure parameters for FIA_AFL.1	**WebUI:** [DD-MM-YYYY HH:MM:SS][INFO] Administrator@ProviderDataCenterSystemAdmin, 172.16.16.253:39161, update, UserGlobalSettings **SSH:** [DD-MM-YYYY HH:MM:SS][INFO] Administrator@ProviderDataCenterSystemAdmin, 172.16.16.254:55086, update-bash-shell-settings, settings
	Ability to start and stop services	YYYY-MM-DD HH:MM:SS Director1 admin: admin [10807]: YYYY-MM-DD HH:MM:SS vsh start [0] YYYY-MM-DD HH:MM:SS Director1 admin: admin [10807]: YYYY-MM-DD HH:MM:SS vsh stop [0]

	Ability to modify the behavior of the transmission of audit data to an external IT entity	[DD-MM-YYYY HH:MM:SS][INFO] Administrator@ProviderDataCenterSystemAdmin, 172.16.16.253:65268, modify, server:172.16.16.254 , changeset:system { syslog-servers { server{172.16.16.254} { - enabled true - port 6514 - protocol TCP } } }
		[DD-MM-YYYY HH:MM:SS][INFO] Administrator@ProviderDataCenterSystemAdmin, 172.16.16.253:65247, modify, server:172.16.16.254, appliances: SDWAN-Branch2 , changeset:devices { device{SDWAN-Branch2} { config { system { syslog { server{172.16.16.254} { - enabled true - port 514 - selector{2} { - comparison same_or_higher - facility-list syslog,all - level all - negate false} } } } } }

	Ability to manage the cryptographic keys	**Refer to FIA_X509_EXT.1**

Requirement	Audit Event	Audit Content
	Ability to configure the cryptographic functionality	[DD-MM-YYYY HH:MM:SS][INFO] Administrator@versa, 172.16.16.253:65316, modify, vpn-profile:Reference-Identifiers, appliances: SDWAN-Branch2 , changeset:devices { device{SDWAN-Branch2} { config { orgs { org-services{versa} { ipsec { vpn-profile{Reference-Identifiers} { - alarms { - ike-auth-failure enable - ike-state-change enable - ipsec-state-change enable} - hardware-accelerator any - ike { - dpd-timeout 30 - frag-size 576 - group mod19 - lifetime 28800 - operations - transform aes256-sha256 - version v2} - ipsec { - anti-replay enable - force-nat-t disable - fragmentation pre-fragmentation - hello-interval { - send-interval 10} - life { - duration 28800 - volume 512} - mode tunnel - operations - pfs-group mod19 - transform esp-aes256-sha256} - lef-profile-default true - local { - address 172.1.1.5} - local-auth-info { - auth-type certificate - ca-chain rootca-rsa - cert-domain tenant - cert-name server-TOE-rsa-Branch2.crt} - peer { - address 172.1.1.254} - peer-auth-info { - auth-type certificate - ca-chain rootca-rsa} - precedence 0 - revocation-check none - routing-instance WAN1-Transport-VR - tunnel-initiate automatic - tunnel-interface tvi-0/20.0 - tunnel-routing-instance versa-LAN-VR - vpn-type site-to-site } } } } } } }

	Ability to configure the lifetime for IPsec SAs.	**IKE SA lifetime:**
		[YYYY-MM-DD HH:MM:SS][INFO] Administrator@versa, 172.16.16.253:65085, modify, vpn-profile:Reference-Identifiers, appliances: SDWAN-Branch2 , changeset:devices { device{SDWAN-Branch2} { config { orgs { org-services{versa} { ipsec { vpn-profile{Reference-Identifiers} { - alarms { - ike-auth-failure enable - ike- state-change enable - ipsec-state-change enable} - hardware-accelerator any - ike { - dpd-timeout 30 - frag-size 576 - group mod19 - lifetime 86400 - operations - transform aes256-sha256 - version v2} - ipsec { - anti-replay enable - force-nat-t disable - fragmentation pre-fragmentation - hello-interval { - send-interval 10} - life { - duration 21600 - volume 512} - mode tunnel - operations - pfs-group mod19 - transform esp-aes256-sha256} - lef-profile-default true - local { - address 172.1.1.5}
		ESP SA lifetime:
		[YYYY-MM-DD HH:MM:SS][INFO] Administrator@versa, 172.16.16.253:65095, modify, vpn-profile:Reference-Identifiers, appliances: SDWAN-Branch2 , changeset:devices { device{SDWAN-Branch2} { config { orgs { org-services{versa} { ipsec { vpn-profile{Reference-Identifiers} { - alarms { - ike-auth-failure enable - ike- state-change enable - ipsec-state-change enable} - hardware-accelerator any - ike {

Requirement	Audit Event	Audit Content
		- dpd-timeout 30 - frag-size 576 - group mod19 - lifetime 28800 - operations - transform aes256-sha256 - version v2} - ipsec { - anti-replay enable - force-nat-t disable - fragmentation pre-fragmentation - hello-interval { - send-interval 10} - life { - duration 21600 - volume 512} - mode tunnel - operations - pfs-group mod19 - transform esp-aes256-sha256} - lef-profile-default true - local { - address 172.1.1.5} local-auth-info { - auth-type certificate - ca-chain rootca-rsa - cert-domain tenant - cert-name server-TOE-rsa-Branch2.crt} - peer { - address 172.1.1.254} - peer-auth- info { - auth-type certificate - ca-chain rootca-rsa} - precedence 0 - revocation-check none - routing-instance WAN1-Transport-VR - tunnel-initiate responder-only - tunnel-interface tvi-0/20.0 - tunnel-routing-instance versa-LAN-VR - vpn-type site- to-site } } } } } } }
	Ability to configure the interaction between TOE components	**Refer to FCO_CPC_EXT.1**
	Ability to re-enable an Administrator account	[DD-MM-YYYY HH:MM:SS][INFO] Administrator, CLI 'request nms actions unlock-user-by-admin username admin1'

	Ability to configure NTP	[DD-MM-YYYY HH:MM:SS][INFO] Administrator@ProviderDataCenterSystemAdmin, 172.16.16.253:58683, create, server:172.16.16.200 , changeset:system { ntp { + server{172.16.16.200} } }
		[DD-MM-YYYY HH:MM:SS][INFO] Administrator@ProviderDataCenterSystemAdmin, 172.16.16.253:59366, modify, server:172.16.16.200 , changeset:system { ntp { server{172.16.16.200} { - version 4 } } }

	Ability to configure reference identifier for the peer	**Refer to FMT_SMF.1: Ability to configure the cryptographic functionality**
	Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors	**Refer to FIA_X509_EXT.1**
	Ability to import X.509v3 certificates to the TOE's trust store	**Refer to FIA_X509_EXT.1**

Requirement	Audit Event	Audit Content
	Ability to manage the trusted public key database	YYYY-MM-DD HH:MM:SS Director1 root: root [2549]: sudo ssh-keygen -f /etc/ssh/ssh_host_ecdsa_key -N "" -t ecdsa -b 256 -C "Director SSH hostkey" [0]
	Resetting passwords	[DD-MM-YYYY HH:MM][INFO] Administrator@ProviderDataCenterSystemAdmin, 172.16.16.253:34227, ResetPasswordByAdmin, password , changeset:{"reset-password-by-admin":{"newpassword":"******","username":"GSS-Test-User"}}
FMT_SMF.1/ IPS	Enable, disable signatures applied to sensor interfaces, and determine the behavior of IPS functionality	[DD-MM-YYYY HH:MM:SS][INFO] Administrator@ProviderDataCenterSystemAdmin, 172.16.16.253:34178, configure-vulnerability-rule-files, security:SDWAN-Branch2,32febf11-3ab5-46e2-95ea-dcd8f90705ba,ips
	Modify the parameters that define the network traffic to be collected and analyzed: o Source IP addresses (host address and network address) o Destination IP addresses (host address and network address) o Source port (TCP and UDP) o Destination port (TCP and UDP) o Protocol (IPv4 and IPv6) o ICMP type and code	[DD-MM-YYYY HH:MM:SS][INFO] Administrator@versa, 172.16.16.253:34183, modify, access-policy:BYPASS-Rule, appliances: SDWAN-Branch2 , changeset:devices { device{SDWAN-Branch2} { config { orgs { org-services{versa} { security { access-policies { access-policy-group{Default-Policy} { rules { access-policy{BYPASS-Rule} { - match { - destination { - address { - address-list 172.1.1.0/32}} - services { - services-list Any-ICMP} - source { - address { - address-list 172.1.1.0/32} - user { - external-database { - status disabled} - local-database { - status disabled} - user-type any}}} - rule-disable false - set { - action allow - lef { - event start - options { - send-pcap-data { - enable false}} - profile Default-Logging-Profile} - set-type public - tcp-session-keepalive disabled} } } } } } } } } }
	Update (import) signatures	[DD-MM-YYYY HH:MM:SS][INFO] Administrator@ProviderDataCenterSystemAdmin, 172.16.16.253:34190, upload-vulnerability-rule-file, security:SBD.1.1-ip4-2-modified-30.rules,32febf11-3ab5-46e2-95ea-dcd8f90705ba,ips
	Create custom signatures	[DD-MM-YYYY HH:MM:SS][INFO] Administrator@ProviderDataCenterSystemAdmin, 172.16.16.253:34190, upload-vulnerability-rule-file, security:SBD.1.1-ip4-2-modified-30.rules,32febf11-3ab5-46e2-95ea-dcd8f90705ba,ips
	Configure anomaly detection	[DD-MM-YYYY HH:MM:SS][INFO] Administrator@ProviderDataCenterSystemAdmin, 172.16.16.253:34190, upload-vulnerability-rule-file, security:SBD.1.1-ip4-2-modified-30.rules,32febf11-3ab5-46e2-95ea-dcd8f90705ba,ips
	Enable and disable actions to be taken when signature or anomaly matches are detected	[DD-MM-YYYY HH:MM:SS][INFO] Administrator@ProviderDataCenterSystemAdmin, 172.16.16.253:34178, configure-vulnerability-rule-files, security:SDWAN-Branch2,32febf11-3ab5-46e2-95ea-dcd8f90705ba,ips

Requirement	Audit Event	Audit Content
	Modify thresholds that trigger IPS actions	[DD-MM-YYYY HH:MM:SS][INFO] Administrator@versa, 172.16.16.253:34201, modify, dos-profile:DOS_Profile, appliances: SDWAN-Branch2 , changeset:devices { device{SDWAN-Branch2} { config { orgs { org-services{versa} { security { profiles { dos { classified { dos-profile{DOS_Profile} { - classification-key source-and-destination-ip - flood { - icmp { - enable yes - red { - activate-rate 100000 - alarm-rate 1 - drop-period 10 - maximal-rate 100000}} - icmpv6 { - enable yes - red { - activate-rate 100000 - alarm-rate 10 - drop-period 10 - maximal-rate 100000}} - other-ip { - enable yes - red { - activate-rate 100000 - alarm-rate 10 - drop-period 10 - maximal-rate 100000}} - sctp { - enable no - red { - activate-rate 100000 - alarm-rate 10 - drop-period 10 - maximal-rate 100000}} - tcp { - action random-early-drop - enable yes - red { - activate-rate 100000 - alarm-rate 10 - drop-period 10 - maximal-rate 100000}} - udp { - enable yes - red { - activate-rate 100000 - alarm-rate 10 - drop-period 10 - maximal-rate 100000}}} - max-sessions 1000 } } } } } } } } } }
	Modify the duration of traffic blocking actions	[DD-MM-YYYY HH:MM:SS][INFO] Administrator@versa, 172.16.16.253:34201, modify, dos-profile:DOS_Profile, appliances: SDWAN-Branch2 , changeset:devices { device{SDWAN-Branch2} { config { orgs { org-services{versa} { security { profiles { dos { classified { dos-profile{DOS_Profile} { - classification-key source-and-destination-ip - flood { - icmp { - enable yes - red { - activate-rate 100000 - alarm-rate 1 - drop-period 10 - maximal-rate 100000}} - icmpv6 { - enable yes - red { - activate-rate 100000 - alarm-rate 10 - drop-period 10 - maximal-rate 100000}} - other-ip { - enable yes - red { - activate-rate 100000 - alarm-rate 10 - drop-period 10 - maximal-rate 100000}} - sctp { - enable no - red { - activate-rate 100000 - alarm-rate 10 - drop-period 10 - maximal-rate 100000}} - tcp { - action random-early-drop - enable yes - red { - activate-rate 100000 - alarm-rate 10 - drop-period 10 - maximal-rate 100000}} - udp { - enable yes - red { - activate-rate 100000 - alarm-rate 10 - drop-period 10 - maximal-rate 100000}}} - max-sessions 1000 } } } } } } } } } }
	Modify the known-good and known-bad lists (of IP addresses or address ranges)	[DD-MM-YYYY HH:MM:SS 076][INFO] Administrator@versa, 172.16.16.253:34208, modify, ip-filter-profile:IPS_IPB_EXT_1, appliances: SDWAN-Branch2 , changeset:devices { device{SDWAN-Branch2} { config { orgs { org-services{versa} { security { profiles { ip-filtering { ip-filter-profile{IPS_IPB_EXT_1} { - address-reverse-lookup { - enable false} - allow-url-reputation undefined - black-list { - action { - predefined reject} - ip-addresses { - address-groups Bad_List} - match source-or-destination} - lef-profile Default-Logging-Profile - prioritize-url-reputation enabled - white-list { - ip-addresses { - address-groups Good_List} - log true - match source-or-destination} } } } } } } } } }
	Configure the known-good and known-bad lists to override signature- based IPS policies	[DD-MM-YYYY HH:MM:SS][INFO] Administrator@versa, 172.16.16.253:34208, modify, ip-filter-profile:IPS_IPB_EXT_1, appliances: SDWAN-Branch2 , changeset:devices { device{SDWAN-Branch2} { config { orgs { org-services{versa} { security { profiles { ip-filtering { ip-filter-profile{IPS_IPB_EXT_1} { - address-reverse-lookup { - enable false} - allow-url-reputation undefined - black-list { - action { - predefined reject} - ip-addresses { - address-groups Bad_List} - match source-or-destination} - lef-profile Default-Logging-Profile - prioritize-url-reputation enabled - white-list { - ip-addresses { - address-groups Good_List} - log true - match source-or-destination} } } } } } } } } }

Requirement	Audit Event	Audit Content
FMT_SMF.1/ FFW	All management activities of TSF data (including creation, modification and deletion of firewall rules).	[DD-MM-YYYY][INFO] Administrator@versa, 172.16.16.253:34183, modify, access-policy:BYPASS-Rule, appliances: SDWAN-Branch2 , changeset:devices { device{SDWAN-Branch2} { config { orgs { org-services{versa} { security { access-policies { access-policy-group{Default-Policy} { rules { access-policy{BYPASS-Rule} { - match { - destination { - address { - address-list 172.1.1.0/32}} - services { - services-list Any-ICMP} - source { - address { - address-list 172.1.1.0/32} - user { - external-database { - status disabled} - local-database { - status disabled} - user-type any}}} - rule-disable false - set { - action allow - lef { - event start - options { - send-pcap-data { - enable false}} - profile Default-Logging-Profile} - set-type public - tcp-session-keepalive disabled} } } } } } } } } } }
FMT_SMF.1/ VPN	Definiton of packet filtering rules	[DD-MM-YYYY HH:MM:SS][INFO] Administrator@ProviderDataCenterSystemAdmin, 172.16.16.253:34178, configure-vulnerability-rule-files, security:SDWAN-Branch2,32febf11-3ab5-46e2-95ea-dcd8f90705ba,ips
	Association of packet filtering rules to network interfaces	[DD-MM-YYYY HH:MM:SS][INFO] Administrator@versa, 172.16.16.253:34183, modify, access-policy:BYPASS-Rule, appliances: SDWAN-Branch2 , changeset:devices { device{SDWAN-Branch2} { config { orgs { org-services{versa} { security { access-policies { access-policy-group{Default-Policy} { rules { access-policy{BYPASS-Rule} { - match { - destination { - address { - address-list 172.1.1.0/32}} - services { - services-list Any-ICMP} - source { - address { - address-list 172.1.1.0/32} - user { - external-database { - status disabled} - local-database { - status disabled} - user-type any}}} - rule-disable false - set { - action allow - lef { - event start - options { - send-pcap-data { - enable false}} - profile Default-Logging-Profile} - set-type public - tcp-session-keepalive disabled} } } } } } } } } }
	Ordering of packet rules by priority	**Refer to FMT_SMF.1/IPS and FMT_SMF.1/FFW**

Firewall and IPS Audit Events

The following table describes the firewall and IPS audit events.

Requirement	Audit Event	Audit Content	Example Audit Record
FFW_RUL_EXT.1	Application of rules configured with the 'log' operation	Source and destination address Source and destination ports Transport Layer Protocol	YYYY-MM-DD HH:MM:SS accessLog, applianceName=SDWAN-Branch4, tenantName=versa, flowId=33664378, flowCookie=1689796335, flowStartMilliseconds=1138567999, flowEndMilliseconds=0, sentOctets=60, sentPackets=1, recvdOctets=0, recvdPackets=0, appId=8, eventType=start, tenantId=2, urlCategory=, action=deny, vsnId=0, applianceId=1, appRisk=0, appProductivity=0, appIdStr=not-resolved, appFamily=, appSubFamily=, rule= , forwardForwardingClass=fc_be, reverseForwardingClass=fc_be, host=, deviceKey=Unknown, deviceName=Unknown, sourceIPv6Address=ff05::2, destinationIPv6Address=2001:172:16:8::38, sourceTransportPort=32000, destinationTransportPort=12345, protocolIdentifier=0, fromUser=Unknown, eipProfileName=, traffScope=Unknown, srcSGT=, destSGT=

Requirement	Audit Event	Audit Content	Example Audit Record
IPS_ABD_EXT .1	Inspected traffic matches an anomaly-based IPS policy.	Source and destination IP addresses.The content of the header fields that were determined to match the policy.TOE interface that received the packet.Aspect of the anomaly- based IPS policy rule that triggered the event (for example, throughput, time of day, frequency, etc.).Network-based action by the TOE (for example, allowed, blocked, sent reset to source IP, sent blocking notification to firewall). See application note.	YYYY-MM-DD HH:MM:SS idpLog, applianceName=SDWAN-Branch3, tenantName=versa, flowId=33556413, flowCookie=1694464680, signatureId=1000031, groupId=1, signatureRev=1, vsnId=0, applianceId=1, tenantId=2, moduleId=10, signaturePriority=medium, idpAction=reject, signatureMsg="FTP USER ANOMALY", classMsg="Unknown Traffic", threatType=unknown, packetTime=09/11/ 2023-16:48:34.123277, HitCount=1, ipsProfile=Versa Recommended Profile, ipsProfileRule=Attack Severity Rule Filter, ipsDirection=ToServer, ipsProtocol=TCP, ipsApplication=unknown_tcp, sourceIPv4Address=192.168.144.254, destinationIPv4Address=172.16.8.181, sourceTransportPort=6056, destinationTransportPort=21, protocolIdentifier=6, fromUser=Unknown, traffScope=none
IPS_IPB_EXT.1	Inspected traffic matches a list of known- good or known-bad addresses applied to an IPS policy.	Source and destination IP addresses (and, if applicable, indication of whether the source and/or destination address matched the list).TOE interface that received the packet.Network-based action by the TOE (For example, allowed, blocked, sent reset). See application note.	YYYY-MM-DD HH:MM:SS ipfLog, applianceName=SDWAN-Branch3, tenantName=versa, flowId=33556241, flowCookie=1698429900, tenantId=2, vsnId=0, applianceId=1, profileName=IPS_IPB_EXT_1, match=BlackList, ipfAction=reject, srcWhiteList=, dstWhiteList=, srcBlackList=Yes, dstBlackList=No, srcReputation=, dstReputation=, srcLocation=, dstLocation=, srcDomain=, dstDomain=, ipfActionMessage=, sourceIPv4Address=50.50.50.1, destinationIPv4Address=104.237.139.111, sourceTransportPort=32190, destinationTransportPort=80, protocolIdentifier=6, fromUser=Unknown, threatSeverity=, threatType=

Requirement	Audit Event	Audit Content	Example Audit Record
IPS_NTA_EXT.1	Modification of which IPS policies are active on a TOE interface. Enabling/ disabling a TOE Interface with IPS policies applied. Modification of which mode(s) is/ are active on a TOE interface.	Identification of the TOE interface.The IPS policy and interface mode (if applicable).	**Modification of which policies are active on TOE interface:** [DD-MM-YYYY HH:MM:SS][INFO] Administrator@ProviderDataCenterSystemAdmin , 172.16.16.253:64656, configure-vulnerability-rule- files, security:SDWAN-Branch3,32febf11-3ab5-46e2-95ea-dcd8f90705ba,ips **Enabling/Disabling TOE interface with policy applied // Modification of active mode:** [DD-MM-YYYY HH:MM:SS][INFO] Administrator@ProviderDataCenterSystemAdmin , 172.16.16.253:64692, create, vni:vni-0/3, appliances: SDWAN-Branch3 , changeset:devices { device{SDWAN-Branch3} { config { interfaces { + vni{vni-0/3} } } } } [DD-MM-YYYY HH:MM:SS][INFO] Administrator@ProviderDataCenterSystemAdmin, 172.16.16.253:64713, delete, vni:"vni-0/3", appliances: SDWAN-Branch3 , changeset:devices { device{SDWAN-Branch3} { config { interfaces { - vni{vni-0/3} { - dhcp-trusted false - enable true - promiscuous false - unit{0} { - enable true - family { - inet { - address{100.100.100.1/32}}}}} } } } }
IPS_SBD_EXT.1	Inspected traffic matches a signature-based IPS rule with logging enabled.	Name or identifier of the matched signature.Source and destination IP addresses.The content of the header fields that were determined to match the signature.TOE interface that received the packet.Network-based action by the TOE (e.g. allowed, blocked, sent reset). - See application note.	YYYY-MM-DD HH-MM-SS idpLog, applianceName=SDWAN-Branch4, tenantName=versa, flowId=33554694, flowCookie=1693510734, signatureId=910004, groupId=1, signatureRev=0, vsnId=0, applianceId=1, tenantId=2, moduleId=10, signaturePriority=medium, idpAction=reject, signatureMsg="(ipv4) not IPv4 datagram", classMsg="", threatType=Unknown, packetTime=08/31/2023-15:38:41.495863, HitCount=1, ipsProfile=Versa Recommended Profile, ipsProfileRule=Attack Severity Rule Filter, ipsDirection=ToClient, ipsProtocol=IP4, ipsApplication=unknown_ipv4,

Requirement	Audit Event	Audit Content	Example Audit Record
			sourceIPv4Address=126.115.7.217, destinationIPv4Address=174.25.1.9, sourceTransportPort=0, destinationTransportPort=0, protocolIdentifier=4, fromUser=Unknown, traffScope=none