Configure SNMP

For supported software information, click here.

This article describes Versa Operating System^{TM} (VOS^{TM}) Management Information Base (MIBs) and how to configure the Simple Network Management Protocol (SNMP) on VOS devices.

SNMP MIB Information

The SNMP MIB information is different for each VOS release. To find the MIB list for a specific release, go to the VOS (FlexVNF) software download page, at this link:

https://support.versa-networks.com/support/solutions/articles/23000019109-software-download

Select the desired release, follow the link, and then open the subdirectory named FlexVNF. The Versa-MIB.pdf file in this subdirectory contains a description of the MIBs.

Configure SNMP

To configure SNMP, you do the following:

1. Configure the SNMP manager. You do this with Workflows which you create a post-staging template. For more information, see Create and Manage Staging and Post-Staging Templates.
2. Configure SNMP trap profiles.
3. Configure communities (for SNMPv2 only).
4. Configure SNMP agents.
5. Configure USM for local and remote users.
6. Configure VACM views and groups.
7. Configure the VNF manager.

The following sections describe the procedures for performing Steps 2 through 7.

Configure SNMP Trap Profiles

SNMP traps are alert messages that are sent from one or more remote SNMP-enabled devices to a central device, which is called the SNMP manager. A trap communicates the health and performance warnings to the SNMP manager.

You can configure two types of notifications: traps and informs. For a trap notification, the receiver does not send any acknowledgment when it receives the trap, so the sender cannot determine whether the trap was received. A trap may be lost if a problem occurs during transmission.

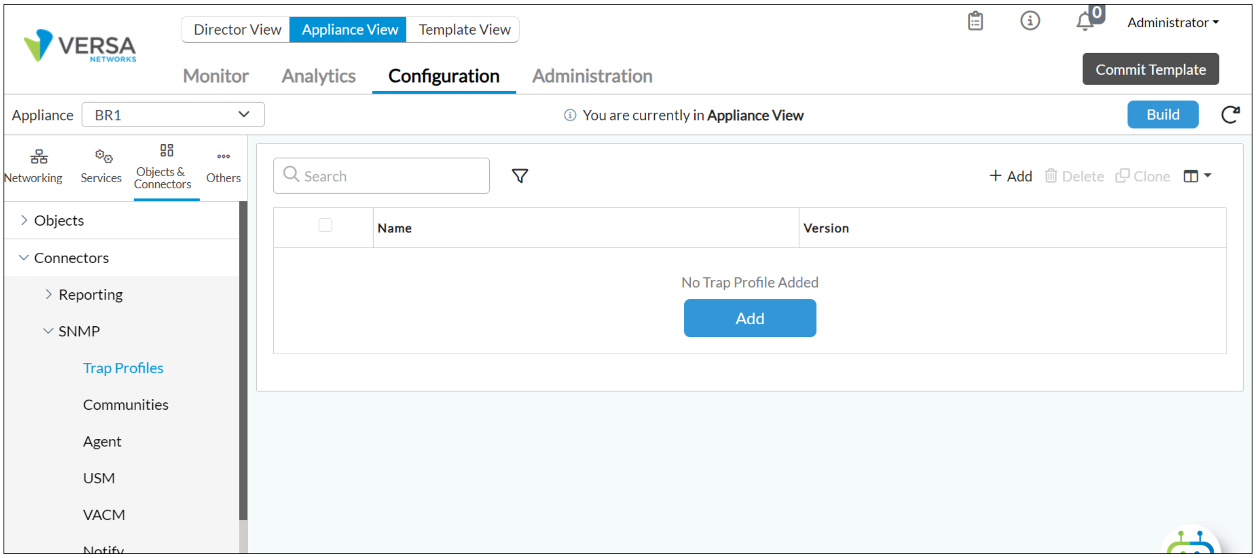
An inform notification is similar to a trap except that the inform is stored and retransmitted at regular intervals until one of the following occurs:

- The receiver (target) of the inform returns an acknowledgment to the SNMP agent.
- A specified number of unsuccessful retransmissions have been attempted, and the agent discards the inform message.

Inform notifications increase the reliability of SNMP notifications. You can configure inform notifications if you are using SNMPv3.

To configure SNMP trap profiles:

1. In Director view:
    a. Select the Configuration tab in the top menu bar.
    b. Select Templates > Device Templates in the left menu bar.
    c. Select an organization in the left menu bar.
    d. Select a template from the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Connectors > SNMP > Trap Profiles in the left menu bar. The table in the main pane lists the trap profiles that are already configured.



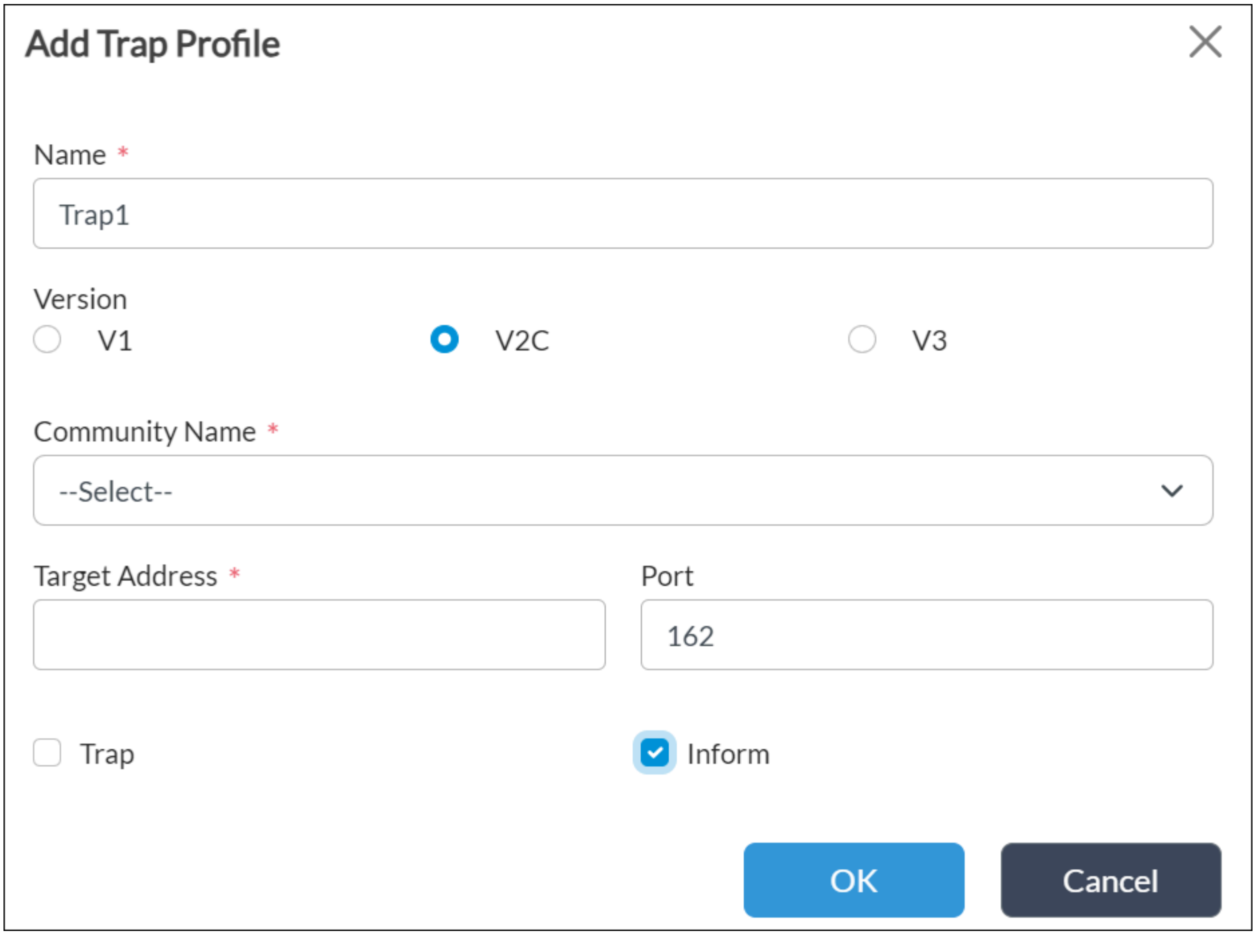
You are currently in Appliance View

	Name	Version
□		

No Trap Profile Added

4. Click the + Add icon to add a profile. The Add Trap Profile popup window displays. Enter information for the following fields.

For SNMPv2:



Add Trap Profile

Name *

Trap1

Version

○ V1 ● V2C ○ V3

Community Name *

--Select--

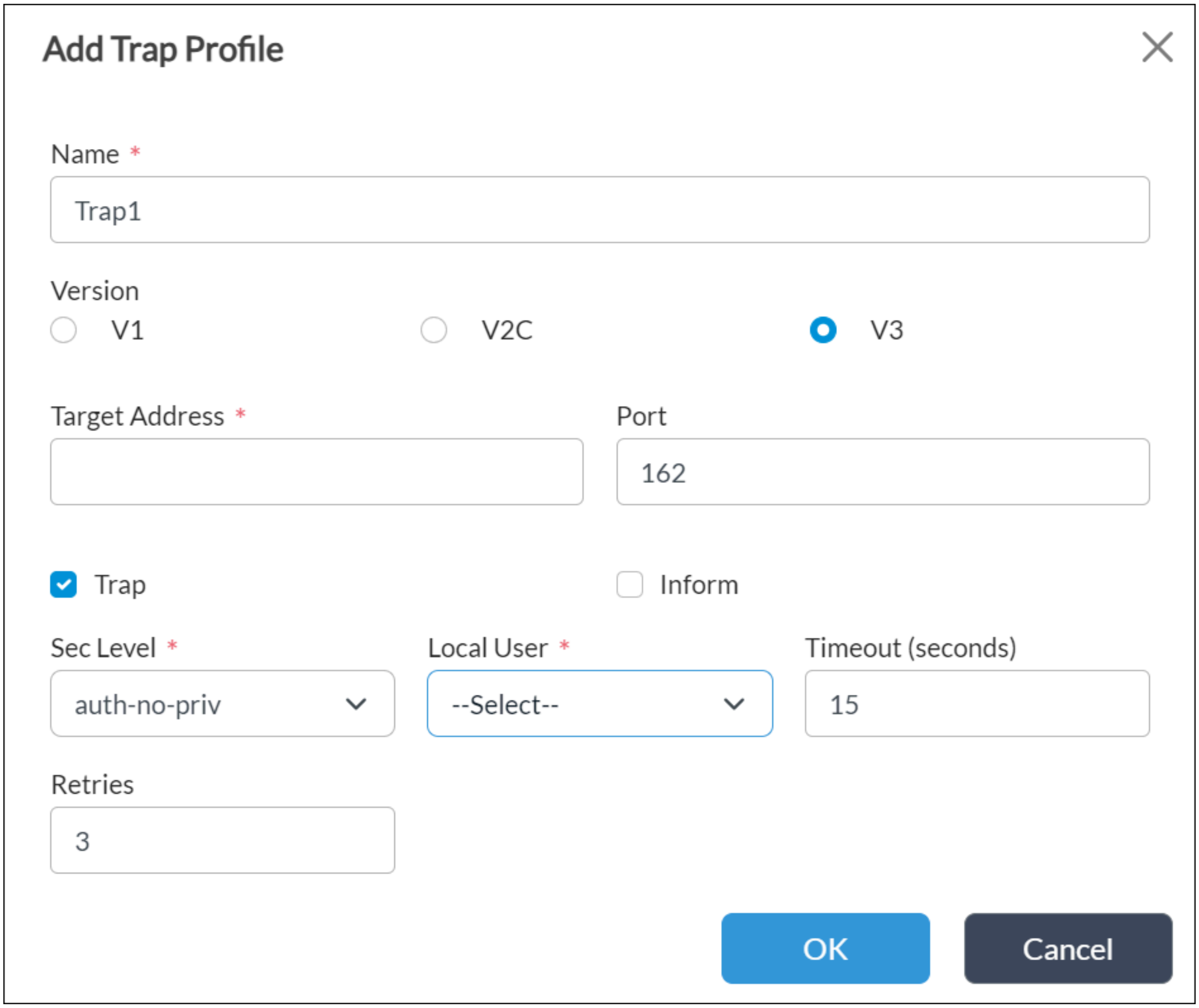
Target Address *

Port

162

□ Trap ☑ Inform

For SNMPv3:



Add Trap Profile

Name *

Trap1

Version

○ V1 ○ V2C ● V3

Target Address *

Port

162

☑ Trap □ Inform

Sec Level *

auth-no-priv

Local User *

--Select--

Timeout (seconds)

15

Retries

3

Field	Description
Name	Enter a name for the trap profile.
Version	Select the SNMP version of the trap notification: ◦ V1 ◦ V2C ◦ V3
Community Name	(For SNMPv2 only.) Select the name of the SNMP community. A community comprises SNMP managers and monitored devices. The name serves as a password to authenticate community members to each other.
Target Address	Enter the IP address of the SNMP manager.
Port	Enter the port number to use to connect to the SNMP manager.
Trap	Select to send trap notifications. For SNMPv3, select the following: ◦ Sec Level—Security level to use when generating SNMP notifications: ▪ authentication—Provide authentication but no encryption. ▪ none—Provide no authentication and no encryption. ▪ privacy—Provide authentication and encryption. ◦ Local user—Select the local username from the drop-down.
Inform	(For Releases 20.2 and later.) For SNMPv3 only, select to send inform notifications to an SNMPv3 user on a remote device: ◦ In the Engine ID field, select the engine ID associated with the remote SNMP user. ◦ In the Remote User field, select the remote username.

Timeout	(For Releases 20.2 and later.) Enter how long, in seconds, to wait for an acknowledgment to an inform notification. If no acknowledgment is received within this period, the inform is retransmitted. *Default:* 1500 seconds
Retries	(For Releases 20.2 and later.) Enter how many times to resend an SNMP inform notification. *Default:* 3

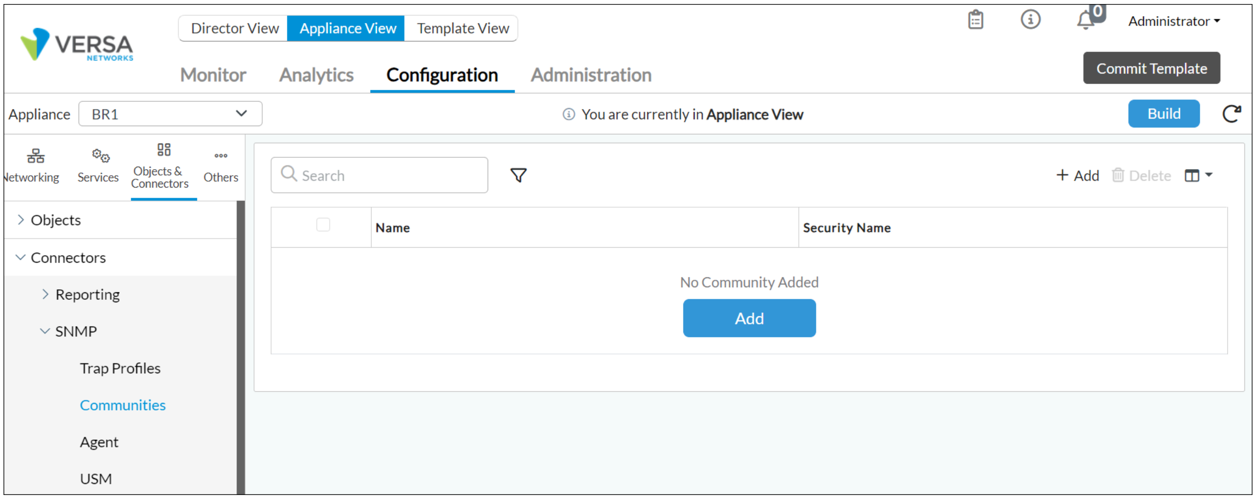
5. Click OK.

Configure Communities

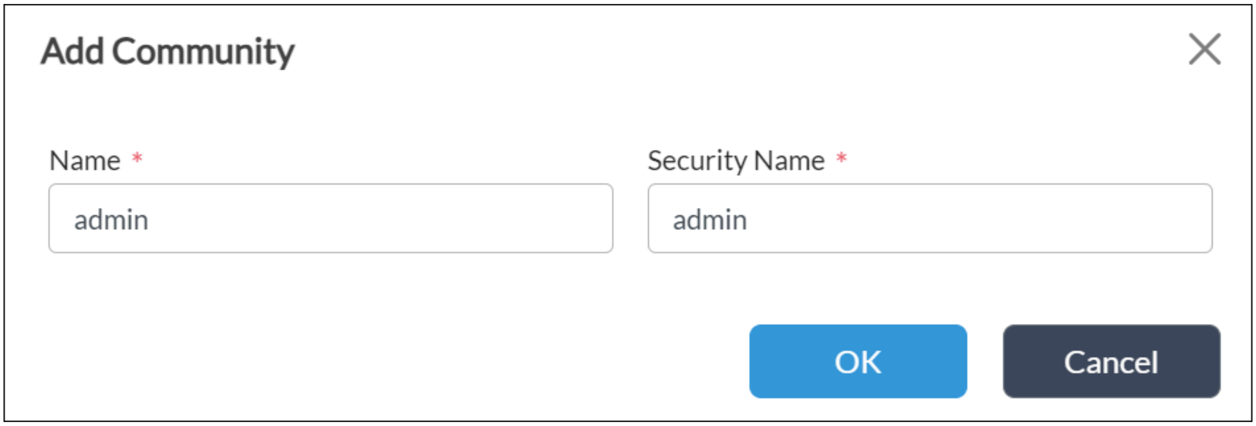
A community is a group of devices that SNMP monitors.

To configure a community:

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the left menu bar.
   c. Select an organization in the left menu bar.
   d. Select a template from the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Connectors > SNMP > Communities in the left menu bar. The table in the main pane lists the communities that are already configured.



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



Add Community

Name *

admin

Security Name *

admin

Field	Description
Name	Enter a name for the community.
Security Name	Enter a security name for the community.

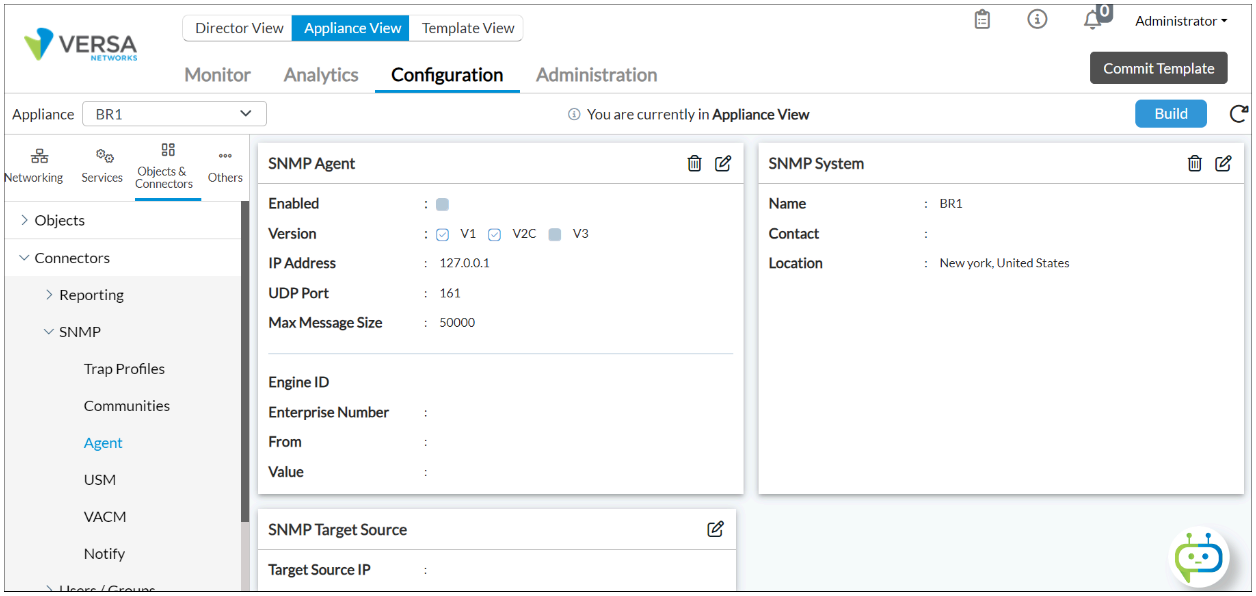
5. Click OK.

Configure SNMP Agents

An agent interacts with SNMP and enables the flow of information between the monitored devices, the applications, and the monitoring device.

To configure an agent:

1. In Director view:
    a. Select the Configuration tab in the top menu bar.
    b. Select Templates > Device Templates in the left menu bar.
    c. Select an organization in the left menu bar.
    d. Select a template from the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Connectors > SNMP > Agent in the left menu bar. The main pane displays the SNMP Agent and SNMP Target Source panes.



Appliance BR1

You are currently in **Appliance View**

SNMP Agent

Enabled	: ■
Version	: ☑ V1 ☑ V2C ■ V3
IP Address	: 127.0.0.1
UDP Port	: 161
Max Message Size	: 50000

Engine ID

Enterprise Number	:
From	:
Value	:

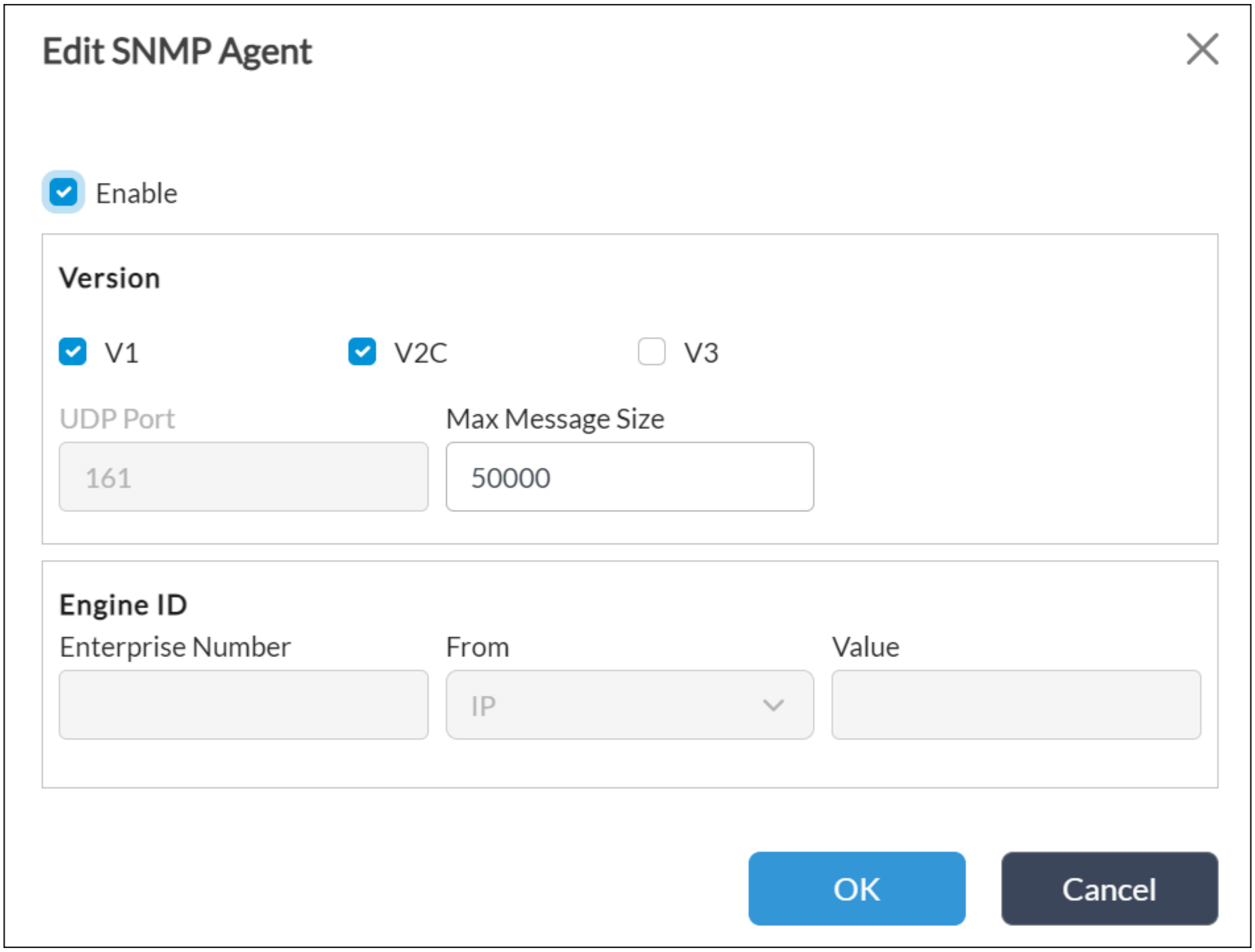
SNMP System

Name	: BR1
Contact	:
Location	: New york, United States

SNMP Target Source

Target Source IP	:

4. Click the ✎ Edit icon in the SNMP Agent pane. In the Edit SNMP Agent popup window, enter information for the following fields.



Edit SNMP Agent

☑ Enable

Version

☑ V1 ☑ V2C □ V3

UDP Port	161
Max Message Size	50000

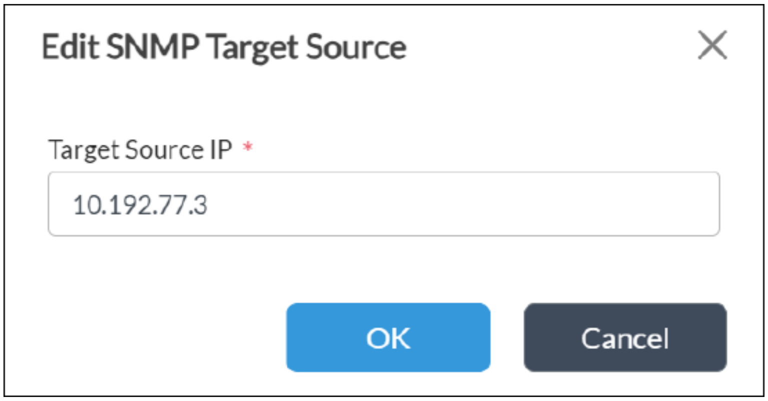
Engine ID

Enterprise Number	
From	IP
Value	

Field	Description
Enable	Click to activate the SNMP agent.
Version	Click to select the version or versions of SNMP: ◦ V1 ◦ V2C ◦ V3
Max Message Size	Enter the maximum size of messages that can be exchanged.

5. Click OK.

6. Click the ✎ Edit icon in the SNMP Target Source pane. In the Edit SNMP Target Source popup window, enter the IP address of the SNMP agent.



Edit SNMP Target Source

Target Source IP *

10.192.77.3

7. Click OK.

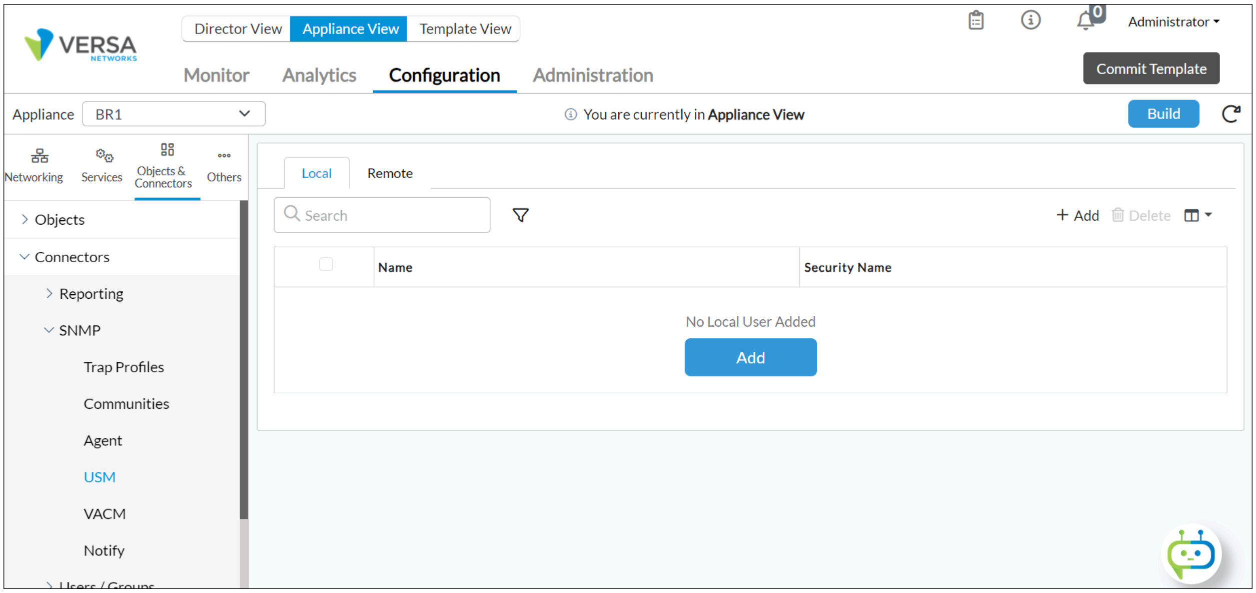
Configure USM

SNMPv3 uses user-based security model (USM) for securing messages. USM uses the concept of a user for which security parameters (levels of security, authentication, privacy protocols, and keys) are configured for both the agent and the manager. Messages sent using USM are highly secure. You configure the security model for local users and remote users.

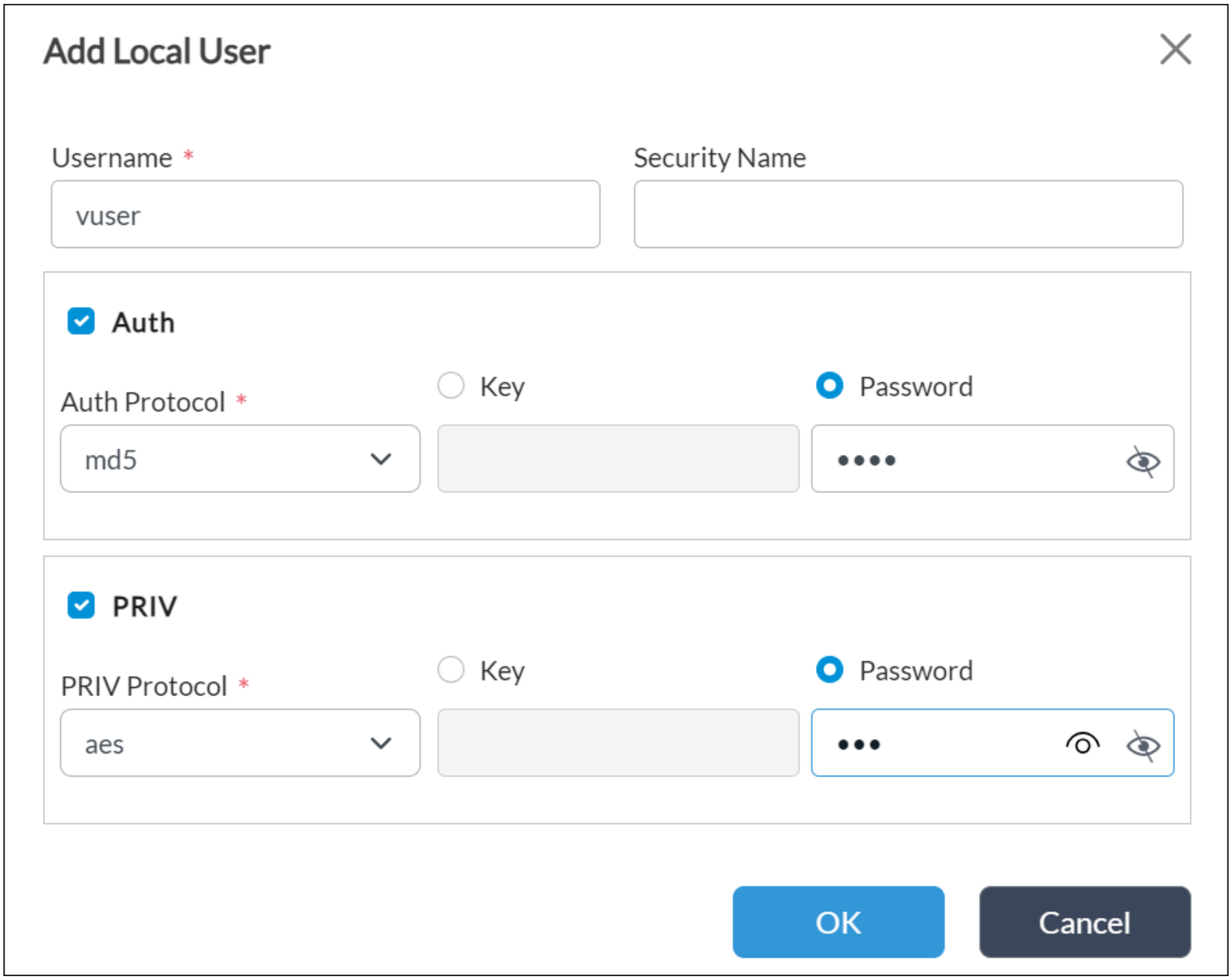
Configure USM for Local Users

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the left menu bar.

    c. Select an organization in the left menu bar.
    d. Select a template from the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Connectors > SNMP > USM in the left menu bar, and select the Local tab in the main pane.



4. Click the + Add icon to add a local user security model. In the Add Local User popup window, enter information for the following fields.



Username * vuser

Security Name

☑ Auth

Auth Protocol * md5

○ Key

● Password ••••

☑ PRIV

PRIV Protocol * aes

○ Key

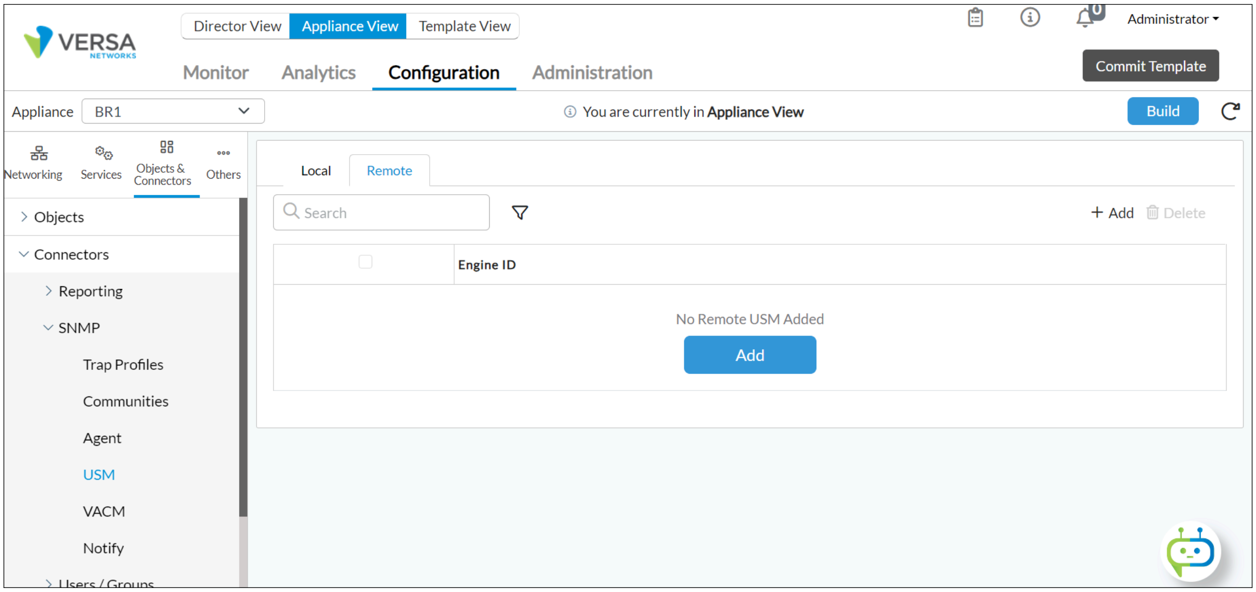
● Password •••

Field	Description
User Name	Enter a name for the local user.
Security Name	Enter a security name for the local user.
Authentication (Group of Fields)	Click to configure the authorization protocol to use for messages.
◦ Authorization Protocol	Select the authorization protocol: ◦ MD5 ◦ SHA
◦ Key	Click and then enter the key to use with the authorization protocol.
◦ Password	Click and then enter the password to use with the authorization protocol.
Privacy (Group of Fields)	Click to configure the privacy protocol to use for messages.
◦ Privacy Protocol	Select the privacy protocol: ◦ AES ◦ DES
◦ Key	Click and then enter the key to use with the privacy protocol.
◦ Password	Click and then enter the password to use with the privacy protocol.

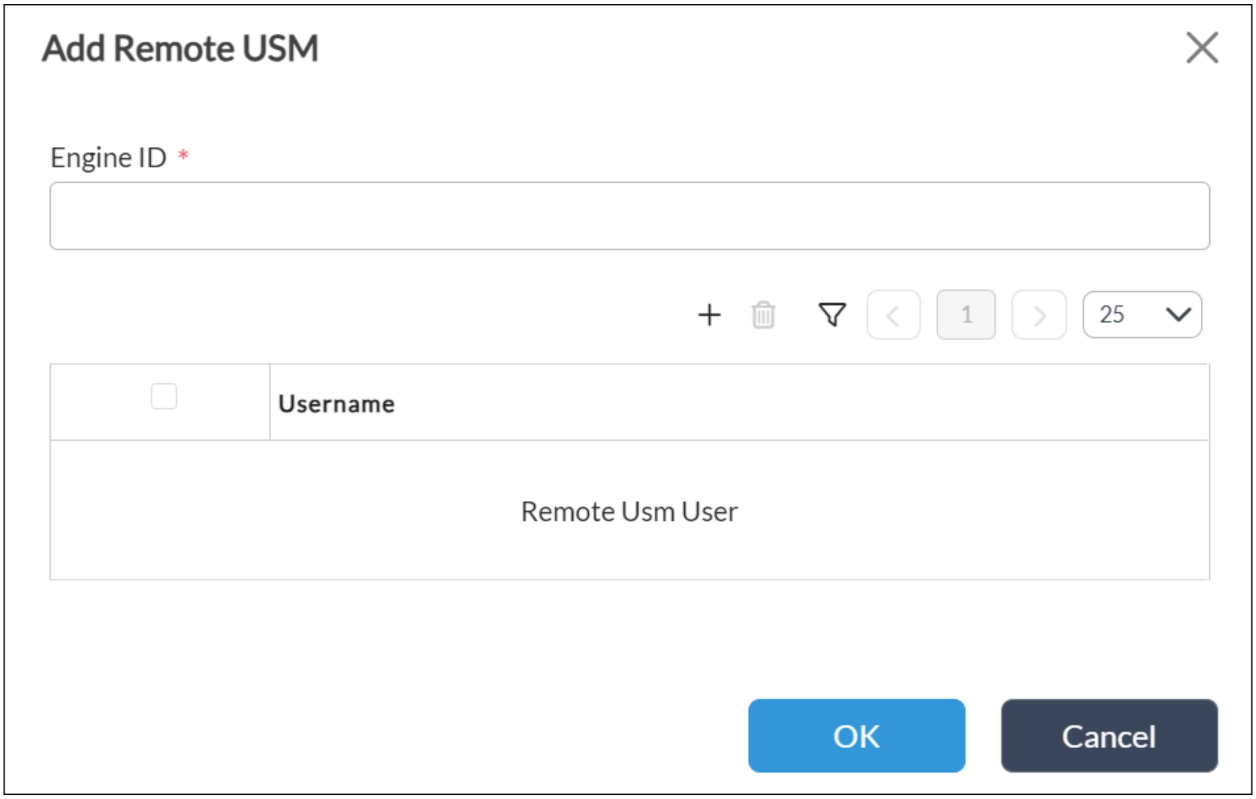
5. Click OK.

Configure USM for Remote Users

1. In Director view:
    a. Select the Configuration tab in the top menu bar.
    b. Select Templates > Device Templates in the left menu bar.
    c. Select an organization in the left menu bar.
    d. Select a template from the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Connectors > SNMP > USM in the left menu bar, and select the Remote tab in the main pane.



4. Click the + Add icon to add a remote user security model. In the Add Remote USM popup window, enter information for the following fields.



Field	Description
Engine ID	Enter the MAC address of the SNMP engine.

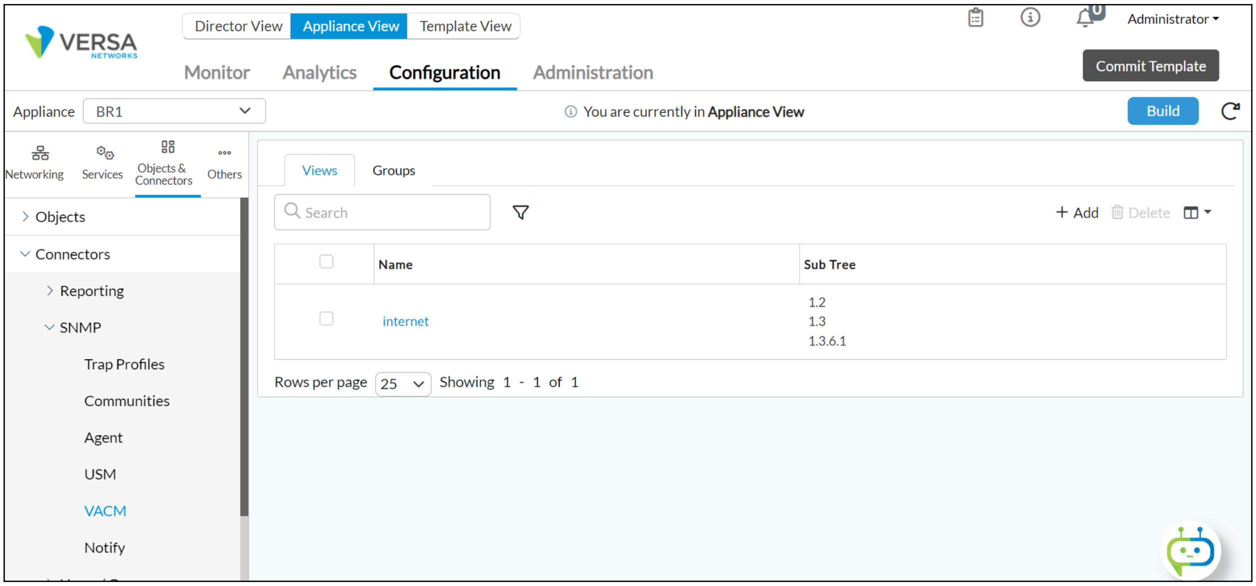
5. Click the + Add icon. In the Add Remote USM User popup window, enter information for the fields, as described in Step 4 of Configure USM for Local Users, above.
6. Click OK.

Configure VACM

SNMPv3 uses view-based access control model (VACM), which allows you to configure the access privileges granted to a group. All access control within VACM operates on groups, which are collections of users defined by USM. You can configure the security model for views and groups.

Configure VACM Views

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the left menu bar.
   c. Select an organization in the left menu bar.
   d. Select a template from the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Connectors > SNMP > VACM in the top menu bar. The table in the main panes displays the VACM views that are already configured.

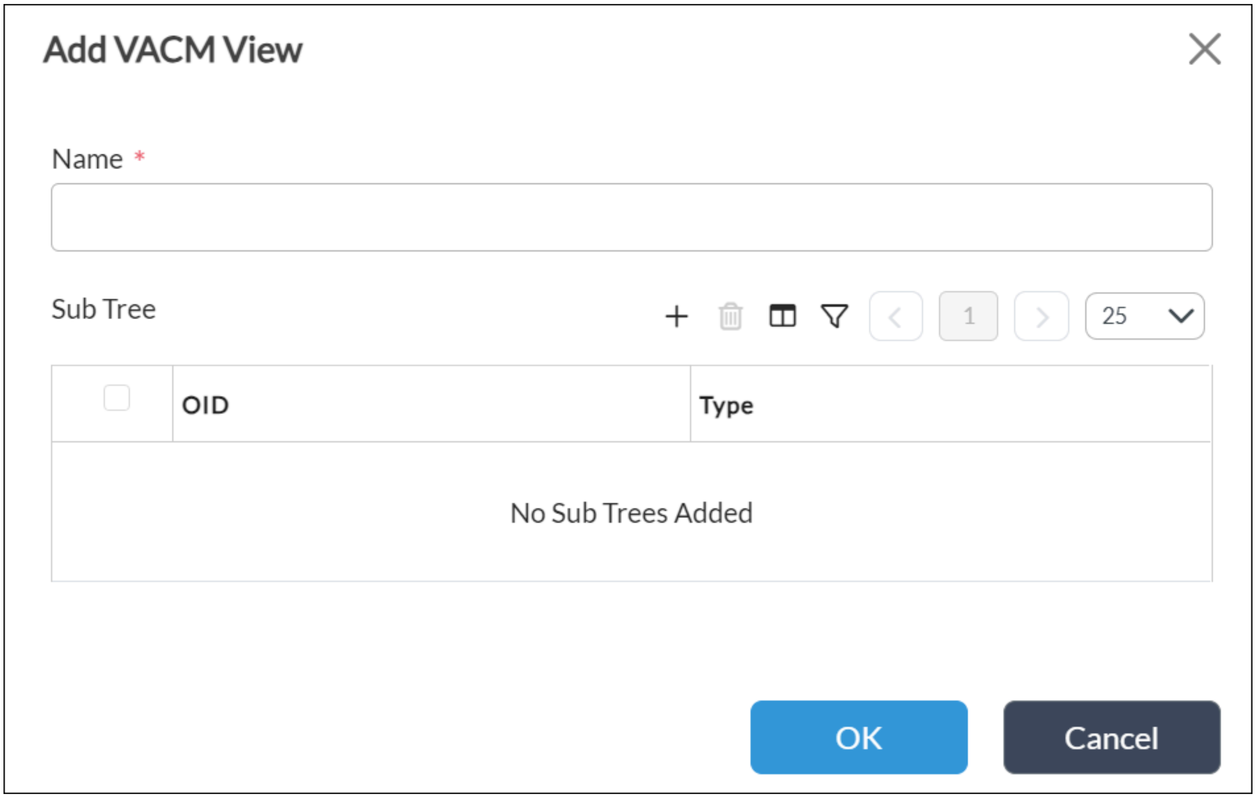


Appliance: BR1

Name	Sub Tree
internet	1.2 1.3 1.3.6.1

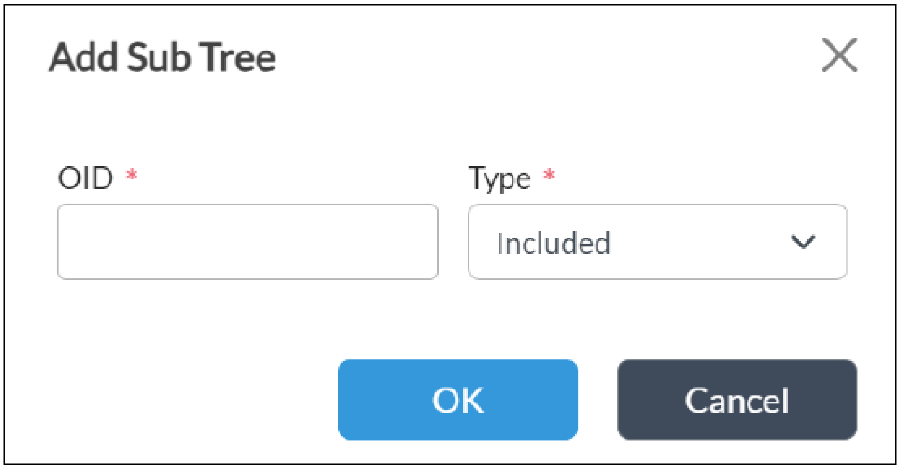
Rows per page 25 Showing 1 - 1 of 1

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



Field	Description
Name	Enter a name for the view.

5. Click the + Add icon. In the Add Subtree popup window, enter information for the following fields.

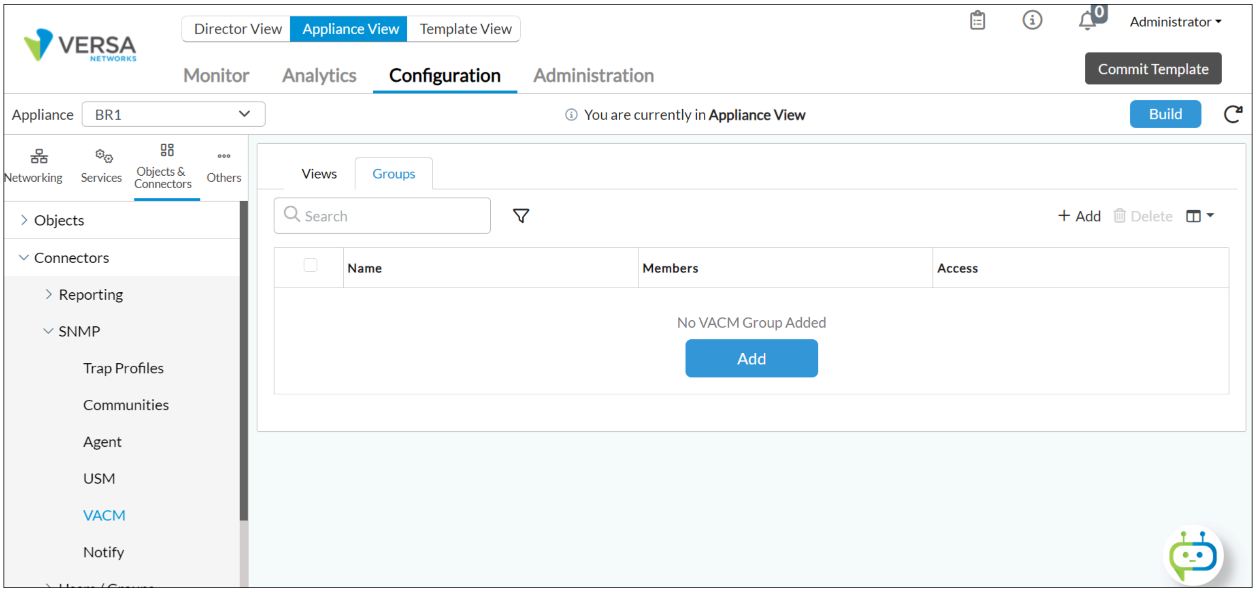


Field	Description
OID	Enter the object identifier.
Type	Select the privilege type: ◦ Excluded ◦ Included

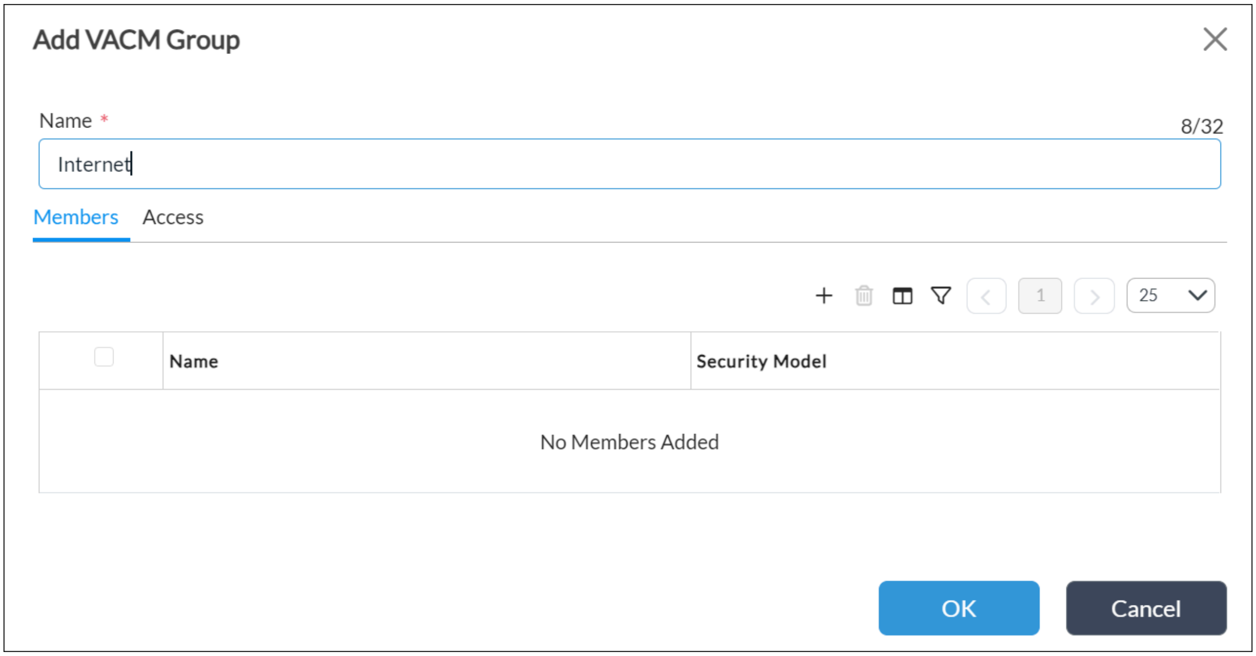
6. Click OK in the Add Subtree popup window.
7. Click OK in the Add VACM View popup window.

Configure VACM Groups

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the left menu bar.
   c. Select an organization in the left menu bar.
   d. Select a template from the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Connectors > SNMP > VACM in the left menu bar.

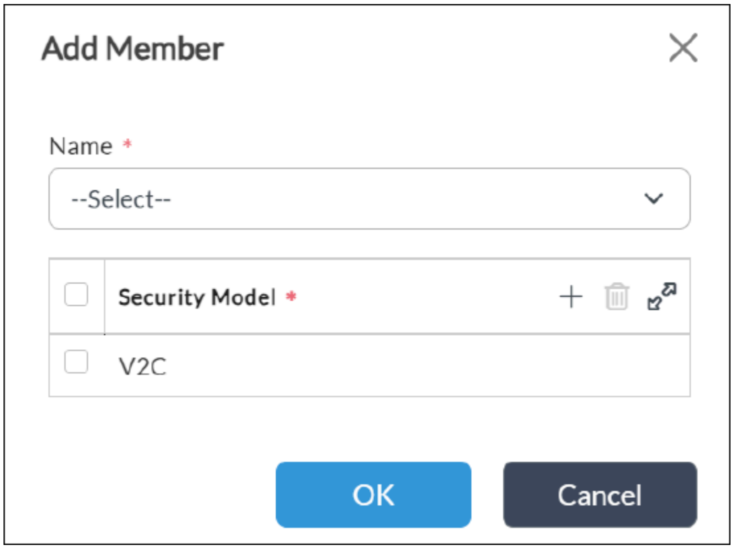


4. Select the Group tab in the main pane, and click the + Add icon. In the Add VACM Group popup window, select the Members tab and enter information for the following fields.



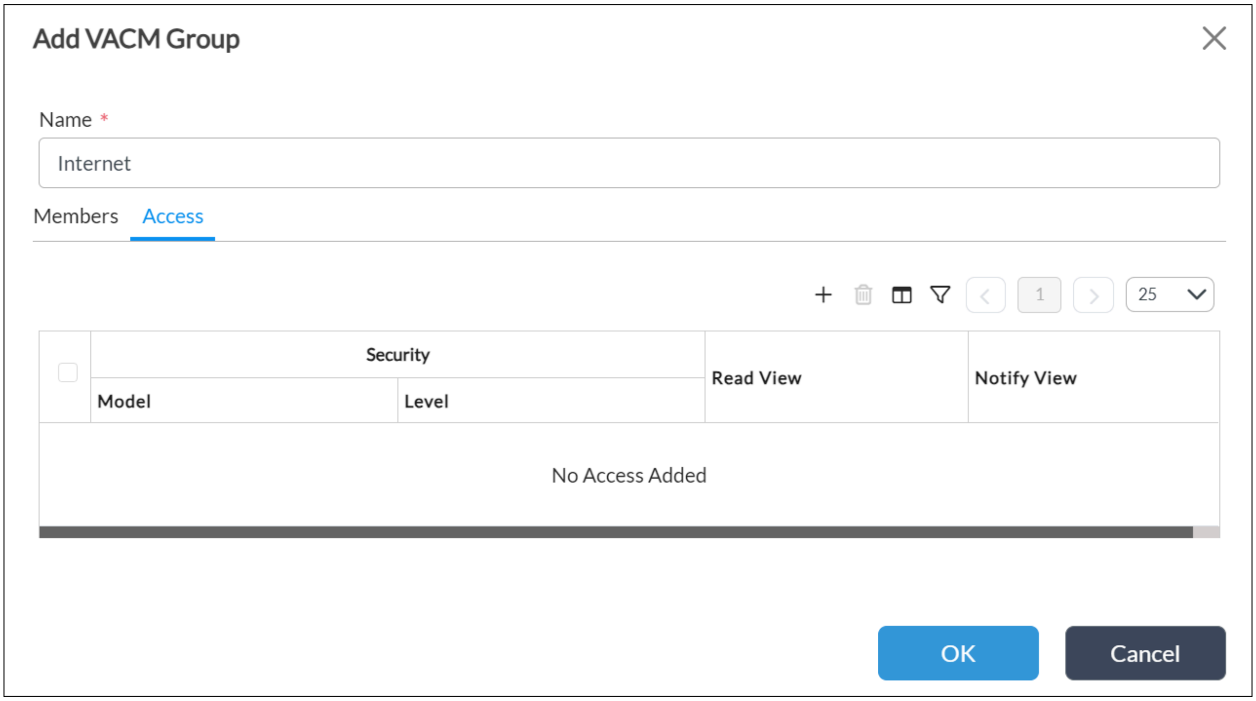
Field	Description
Name	Enter a name for the VACM group.

5. Click the + Add icon to add members to the VACM group. In the Add Member popup window, enter information for the following fields.

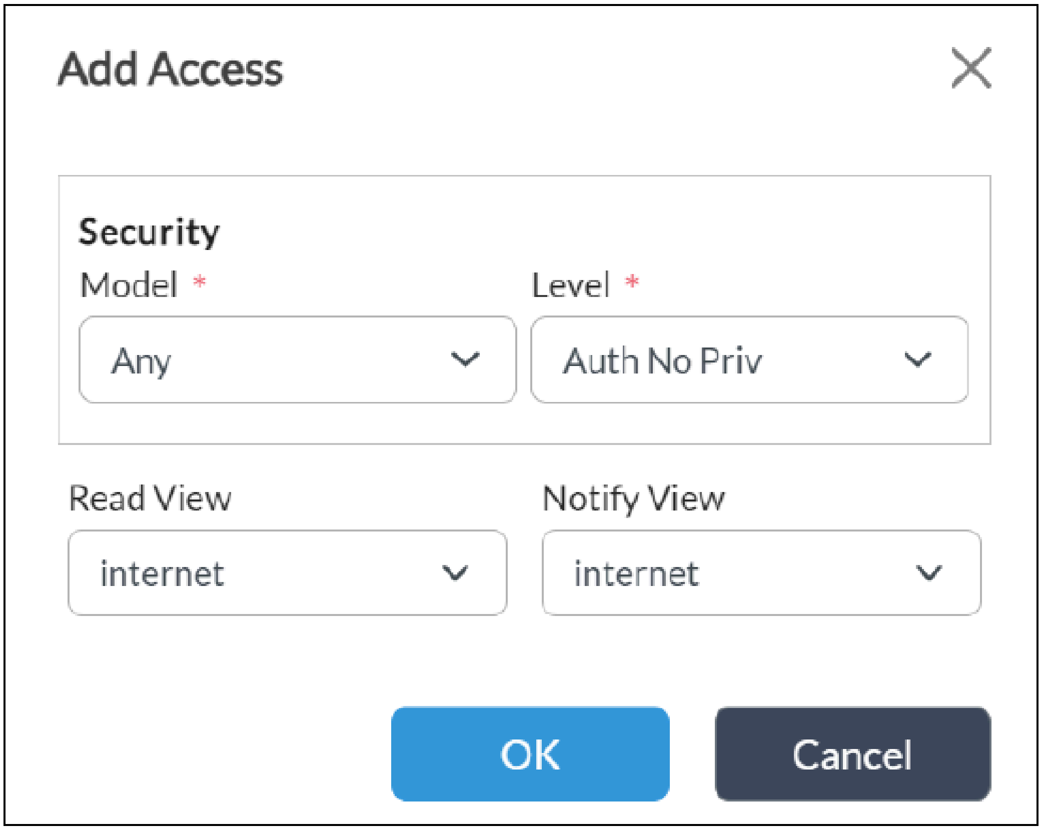


Field	Description
Name	Enter a name for the VACM member.
+ Add icon	Click to select a security model for the VACM member.

6. Click OK.
7. Select the Access tab.



8. Click the + Add icon to add an access model. In the Add Access popup window, enter information for the following fields.



Add Access

Security

Model * Any

Level * Auth No Priv

Read View internet

Notify View internet

Field	Description
Security Model	Select the name of the security model.
Security Level	Select the type of security: ◦ Auth No Priv ◦ Auth Priv ◦ No Auth No Priv
Write View	Select the object for which to grant write permission.
Read View	Select the object for which to grant read permission.
Notify View	Select the object for which to grant notify permission.

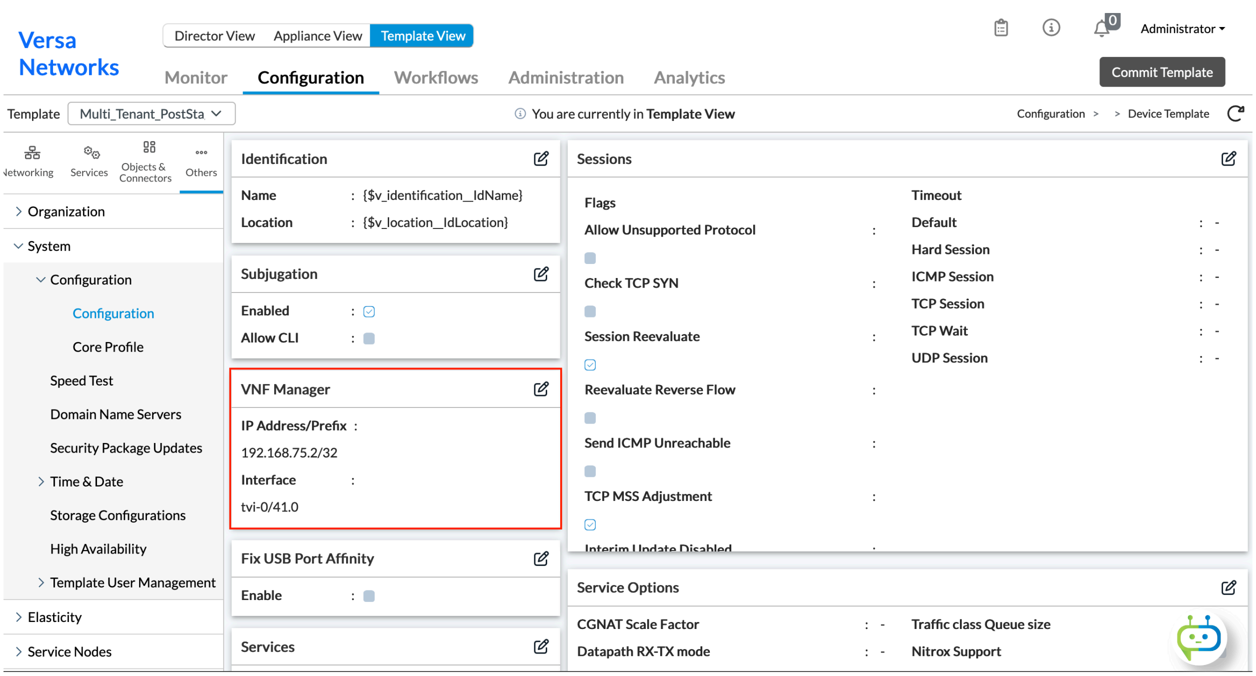
9. Click OK in the Add Access popup window.
10. Click OK in the Add VACM popup window.

Configure VNF Manager Settings

For SNMP server to be able to poll the VOS device and receive its SNMP traps, you need to configure the SNMP server to the VNF manager settings. You also need to configure the VOS interface to use to reach the SNMP server.

To configure the VNF manager:

1. In Director view:
    a. Select the Configuration tab in the top menu bar.
    b. Select Templates > Device Templates in the left menu bar.
    c. Select an organization in the left menu bar.
    d. Select a template from the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Others > System > Configuration > Configuration in the left menu bar. The following screen displays.



Identification

Name	{$v_identification__IdName}
Location	{$v_location__IdLocation}

Subjugation

Enabled	☑
Allow CLI	□

VNF Manager

IP Address/Prefix	192.168.75.2/32
Interface	tvi-0/41.0

Fix USB Port Affinity

Enable	□

Services

Sessions

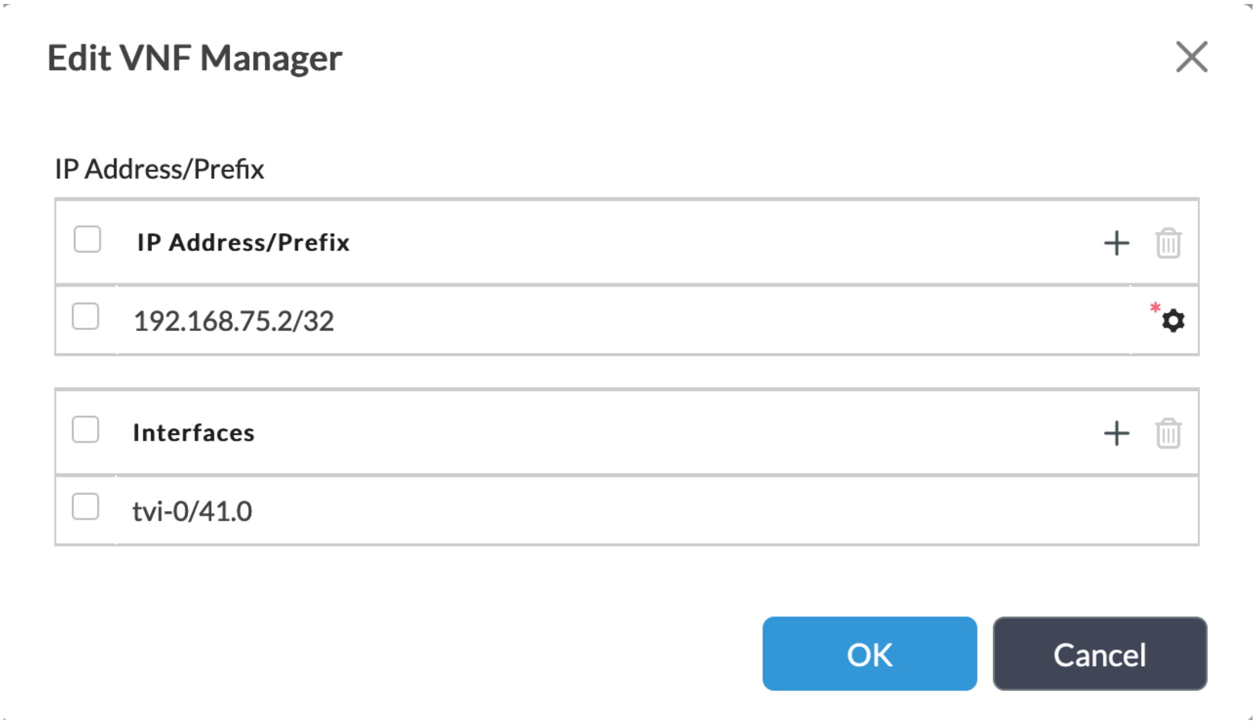
Flags	
Allow Unsupported Protocol	□
Check TCP SYN	□
Session Reevaluate	☑
Reevaluate Reverse Flow	□
Send ICMP Unreachable	□
TCP MSS Adjustment	☑
Interim Update Disabled	

Timeout	
Default	-
Hard Session	-
ICMP Session	-
TCP Session	-
TCP Wait	-
UDP Session	-

Service Options

CGNAT Scale Factor	-	Traffic class Queue size	
Datapath RX-TX mode	-	Nitrox Support	

4. In the VNF Manager pane, click the Edit icon. In the Edit VNF Manager popup window, enter information for the following fields.



Edit VNF Manager

IP Address/Prefix

□	**IP Address/Prefix**
□	192.168.75.2/32

□	**Interfaces**
□	tvi-0/41.0

Field	Description
IP Address/Prefix	Select the IP address of the SNMP server that you want to be able to poll the VOS device and receive its SNMP traps. Click the + Add icon to add an address.
Interfaces	Select the VOS interface to use to reach the SNMP server. Click the + Add icon to add an address.

5. Click OK.

Execute the snmpwalk Command

To execute the **snmpwalk** command, you need to know the SNMP engine ID of the VOS device. To determine the engine ID, issue the **show configuration snmp-notification-receiver** command from the CLI of the VOS device. For example:

```
Administrator@VOS> show configuration snmp-notification-receiver
engine-id 81:01:62:82:81:52:0a:30:96:0f:01:b5:83:55:64;
```

Troubleshoot SNMP Traps

To troubleshoot SNMP traps, you check the VOS device and the SNMP client.

On the VOS device:

1. Verify that target source IP address is configured correctly.
2. Verify that the target UDP port on the VOS device is set to 162.
3. Enable developerLogLevel trace under confdConfig, and check the entries in the devel.log file.
4. Check entries in the snmp.log file with the severity level snmpLogLevel info.

On the SNNMP client:

1. If a trap packet was ignored because of a misconfiguration, issue the **snmptrapd –d** command to do a hexadecimal dump of the sent and received packets.
2. Verify whether the snmptrapd.conf file contains log entries for engineID, execute, net public, doNotFork yes, and authCommunity.

Supported Software Information

Releases 20.2 and later support all content described in this article.

Additional Information

Configure VOS Device Alarms
Create and Manage Post-Staging Templates