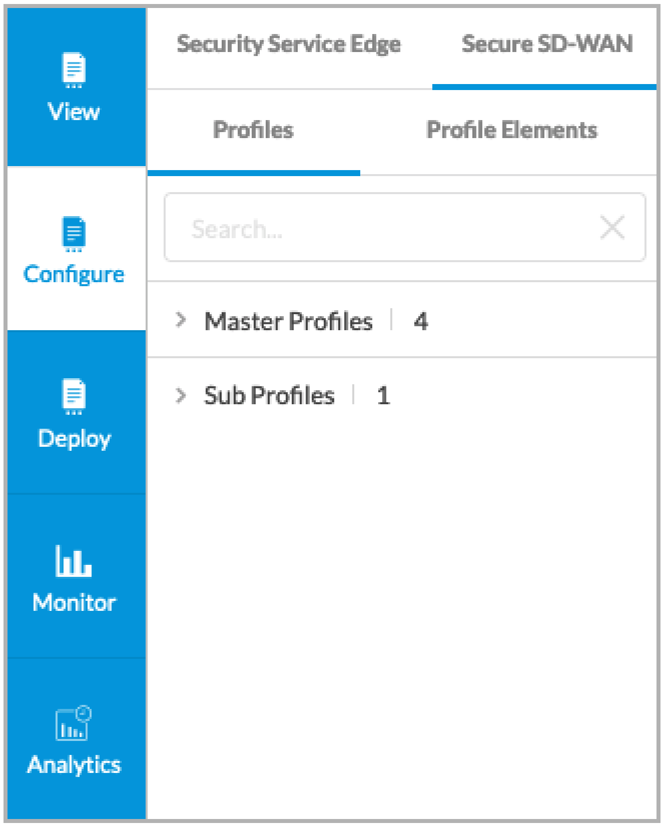
Configure Profiles

For supported software information, click here.

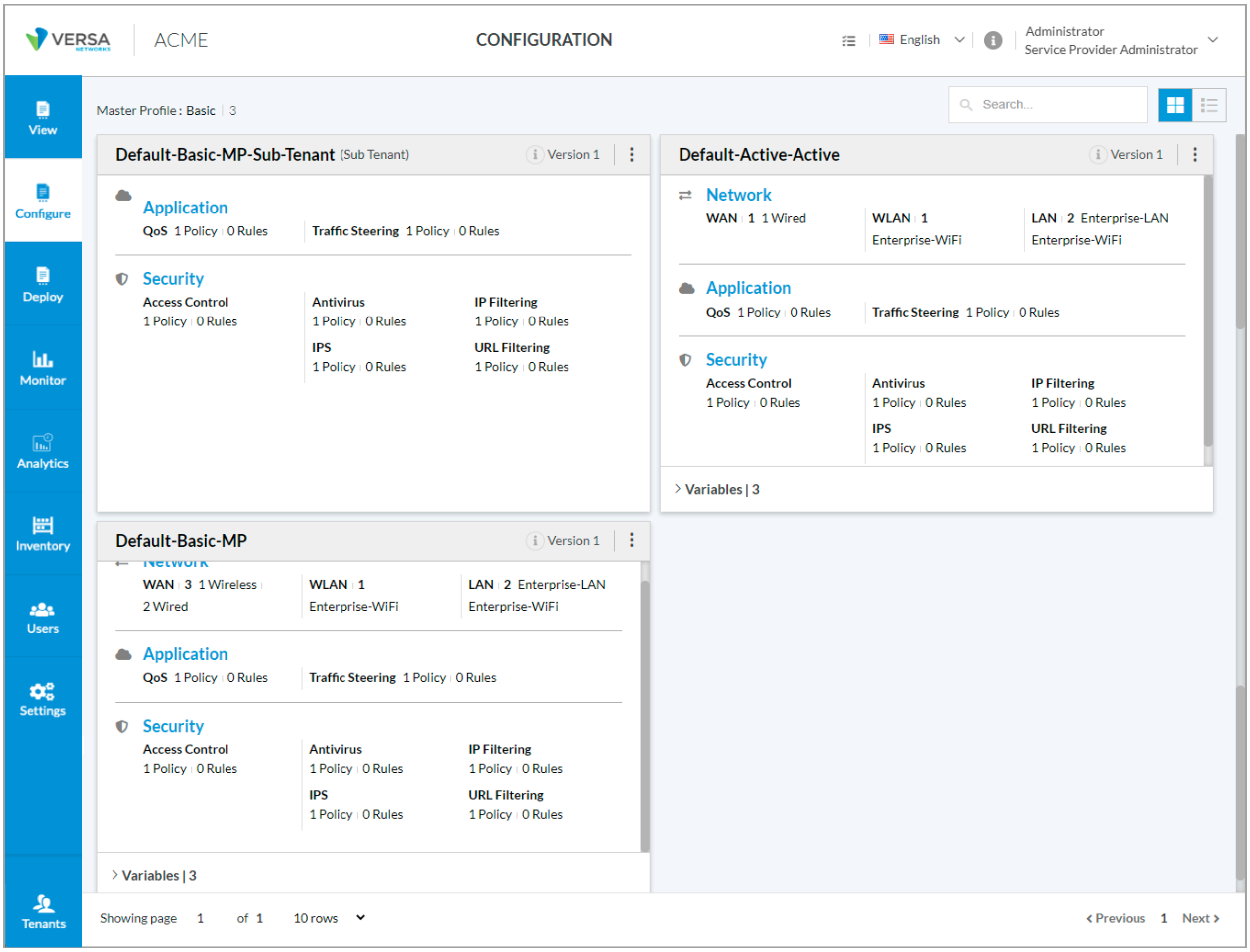
You use the Configure lifecycle to create all configuration objects for Secure SD-WAN deployments. The Concerto configuration objects are hierarchical and consist of master profiles, subprofiles, policies, and rules. A master profile contains one or more subprofiles, a subprofile contains one or more policies, and a policy contains one or more rules. For more information, see Configuration Hierarchies.

To access the Configure lifecycle screen, select Configure in the left menu bar on the Concerto tenant's home screen. Then select Secure SD-WAN > Profiles.



The following figure shows a Configure lifecycle screen that displays the basic master profile (Default-Basic-MP), the default active-active HA profile (Default-Active-Active), and the basic subtenant master profile (Default-Basic-MP-Sub-

Tenant, for Releases 11.2.1 and later).



Master Profile : Basic | 3

Default-Basic-MP-Sub-Tenant (Sub Tenant) Version 1

Application
QoS 1 Policy | 0 Rules — Traffic Steering 1 Policy | 0 Rules

Security
Access Control 1 Policy | 0 Rules — Antivirus 1 Policy | 0 Rules — IP Filtering 1 Policy | 0 Rules
IPS 1 Policy | 0 Rules — URL Filtering 1 Policy | 0 Rules

Default-Active-Active Version 1

Network
WAN | 1 1 Wired — WLAN | 1 Enterprise-WiFi — LAN | 2 Enterprise-LAN Enterprise-WiFi

Application
QoS 1 Policy | 0 Rules — Traffic Steering 1 Policy | 0 Rules

Security
Access Control 1 Policy | 0 Rules — Antivirus 1 Policy | 0 Rules — IP Filtering 1 Policy | 0 Rules
IPS 1 Policy | 0 Rules — URL Filtering 1 Policy | 0 Rules

> Variables | 3

Default-Basic-MP Version 1

Network
WAN | 3 1 Wireless | 2 Wired — WLAN | 1 Enterprise-WiFi — LAN | 2 Enterprise-LAN Enterprise-WiFi

Application
QoS 1 Policy | 0 Rules — Traffic Steering 1 Policy | 0 Rules

Security
Access Control 1 Policy | 0 Rules — Antivirus 1 Policy | 0 Rules — IP Filtering 1 Policy | 0 Rules
IPS 1 Policy | 0 Rules — URL Filtering 1 Policy | 0 Rules

> Variables | 3

Showing page 1 of 1 10 rows — < Previous 1 Next >

Profile Types

The Concerto orchestrator has two types of profiles: master profiles and subprofiles.

Master profiles are configuration templates that you can apply to one or more appliances. Each master profile consists of subprofiles. There are two types of master profiles:

- Basic—Includes a subset of the available configuration objects. You can build most configuration objects in the basic master profile in the same way that you build them in standard master profiles. For Releases 11.2.1 and later, the subtenant basic master profile allows you to configure security and application services. The basic master profile provides a simple user experience and eliminates the subprofiles hierarchy. Instead of creating subprofiles, you create policies and rules and then attach them directly to the basic master profile. For Releases 11.2.1 and later, a master profile can be for a single tenant or for multiple tenants.
- Standard—Includes all available configuration objects and provides more configuration options.

The following types of subprofiles are available:

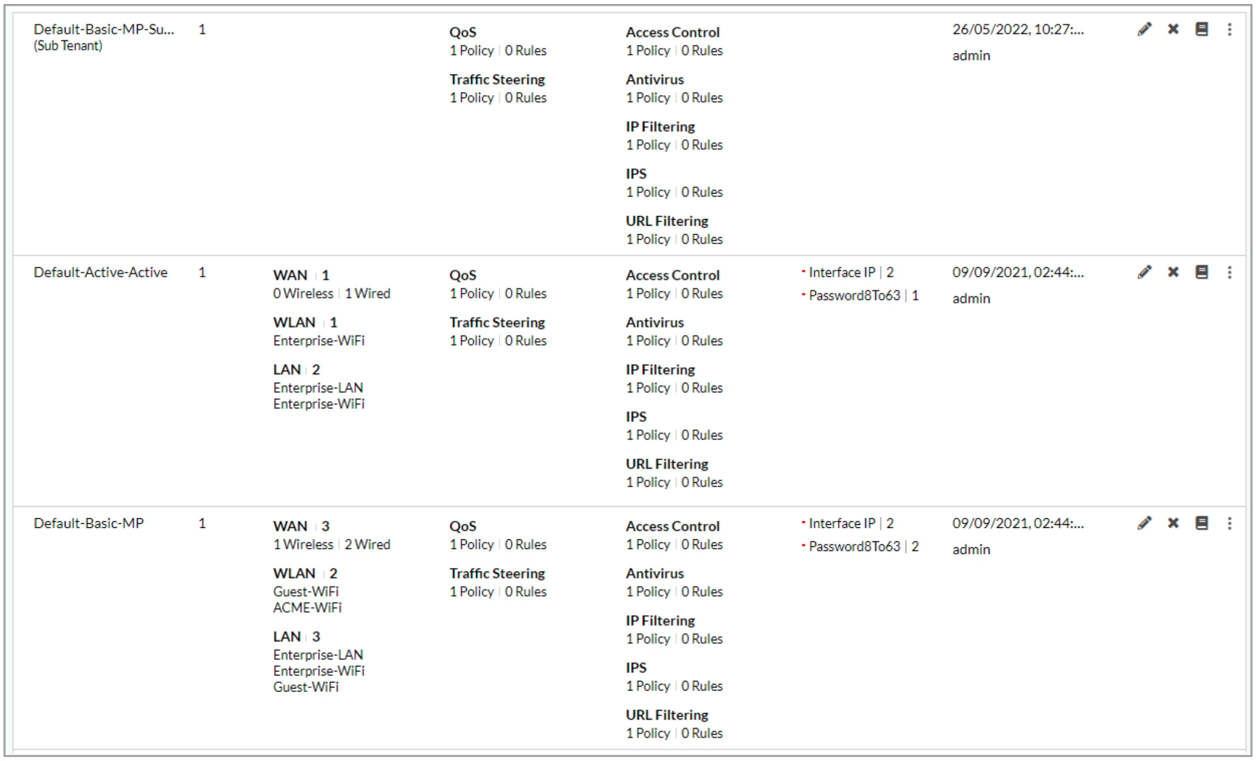
- Application—Use to create QoS and traffic-steering policies.
- Device—Use to create BGP peer, interface, and radio policies.
- Network Services—Use to create CGNAT, DHCP, and WLAN policies.
- Security—Use to create access control, antivirus, IP-filtering, IPS, and URL-filtering policies
- Topology—Use to create VPN policies, including branch and hub policies.

Default Master Profiles

When you install the Concerto software or create a new tenant, Concerto automatically builds three default basic master profiles for the tenant:

- Default-Basic-MP
- Default-Active-Active
- Default-Basic-MP-Sub-Tenant (for Releases 11.2.1 and later)

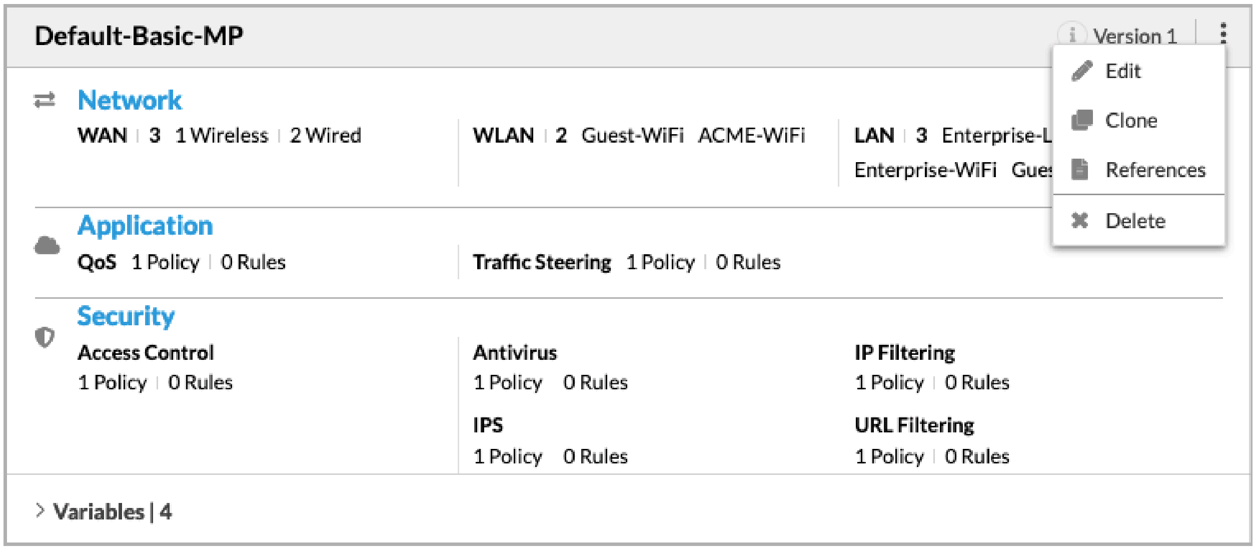
The default master profiles consist of preconfigured network, security, and application objects, as shown below. The default basic subtenent master profile consists of only application and security objects. Concerto creates these basic master profiles automatically for each tenant on Concerto. You can customize the Default-Basic-MP master profile and use it for single-appliance or multitenant site deployments. You can customize the Default-Active-Active master profile and use it for active–active appliance HA site and multitenant deployments.



Default-Basic-MP-Su... (Sub Tenant)	1		**QoS** 1 Policy | 0 Rules **Traffic Steering** 1 Policy | 0 Rules	**Access Control** 1 Policy | 0 Rules **Antivirus** 1 Policy | 0 Rules **IP Filtering** 1 Policy | 0 Rules **IPS** 1 Policy | 0 Rules **URL Filtering** 1 Policy | 0 Rules		26/05/2022, 10:27:... admin
Default-Active-Active	1	**WAN** | **1** 0 Wireless | 1 Wired **WLAN** | **1** Enterprise-WiFi **LAN** | **2** Enterprise-LAN Enterprise-WiFi	**QoS** 1 Policy | 0 Rules **Traffic Steering** 1 Policy | 0 Rules	**Access Control** 1 Policy | 0 Rules **Antivirus** 1 Policy | 0 Rules **IP Filtering** 1 Policy | 0 Rules **IPS** 1 Policy | 0 Rules **URL Filtering** 1 Policy | 0 Rules	- Interface IP | 2 - Password8To63 | 1	09/09/2021, 02:44:... admin
Default-Basic-MP	1	**WAN** | **3** 1 Wireless | 2 Wired **WLAN** | **2** Guest-WiFi ACME-WiFi **LAN** | **3** Enterprise-LAN Enterprise-WiFi Guest-WiFi	**QoS** 1 Policy | 0 Rules **Traffic Steering** 1 Policy | 0 Rules	**Access Control** 1 Policy | 0 Rules **Antivirus** 1 Policy | 0 Rules **IP Filtering** 1 Policy | 0 Rules **IPS** 1 Policy | 0 Rules **URL Filtering** 1 Policy | 0 Rules	- Interface IP | 2 - Password8To63 | 2	09/09/2021, 02:44:... admin

When you click the ⋮ Ellipses icon for a basic master profile or standard master profile, a popup window displays the following options:

- Edit—Click to configure a new version of the the basic master profile. Each version is assigned a new version number, and the original default master profile remains.
- Clone—Click to create a new master profile based on the basic master profile. After you make changes to the configuration objects, save it with a unique name.
- References—Click to view all the appliances using this master profile.
- Propagate—Click to view all the appliances using previous versions of this master profile, and select all appliances or a subset of them to which to apply this master profile version.
- Delete—Click to delete the master profile.



Default-Basic-MP

Version 1

Network

WAN | 3 1 Wireless | 2 Wired

WLAN | 2 Guest-WiFi ACME-WiFi

LAN | 3 Enterprise-L
Enterprise-WiFi Gues

Application

QoS 1 Policy | 0 Rules

Traffic Steering 1 Policy | 0 Rules

Security

Access Control
1 Policy | 0 Rules

Antivirus
1 Policy 0 Rules

IP Filtering
1 Policy | 0 Rules

IPS
1 Policy 0 Rules

URL Filtering
1 Policy | 0 Rules

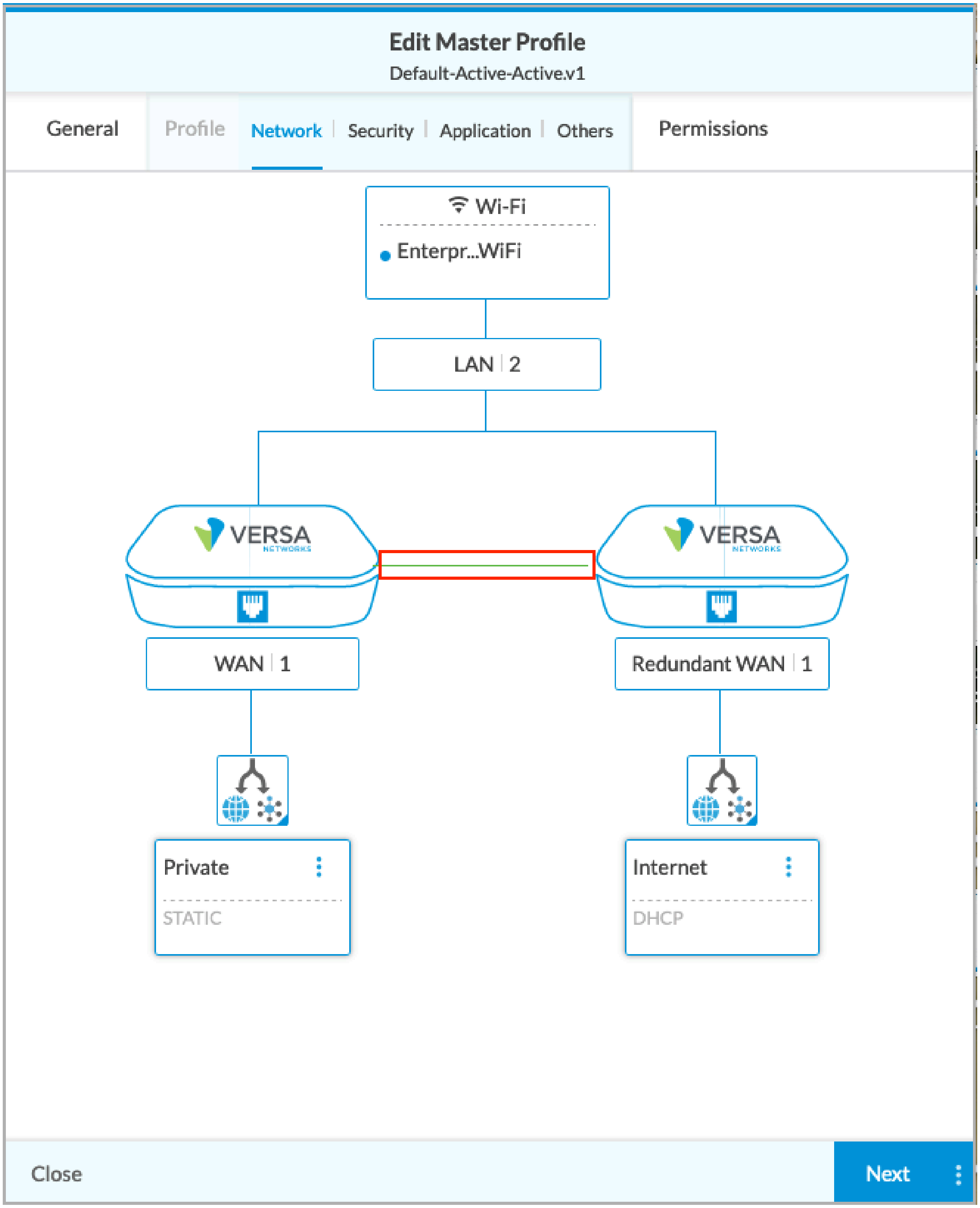
> Variables | 4

For HA, a default active–active HA basic master profile is provided. You can build active-active HA profiles directly in the default active–active HA basic master profile. The following figure below shows the network diagram for the default active–active HA master profile.

Note: Before using the built-in default basic master profiles, do the following:

- Set the connection names on each WAN interface under the Connection tab
- Set the Direct Internet Access connection names under VPN Instances under the Others tab.

If you do not set the connection names used on the appliances in the master profile, when you try to publish the master profile to an appliance, the publish process fails. For more information, see Make Mandatory Updates to the Default Basic Master Profile.

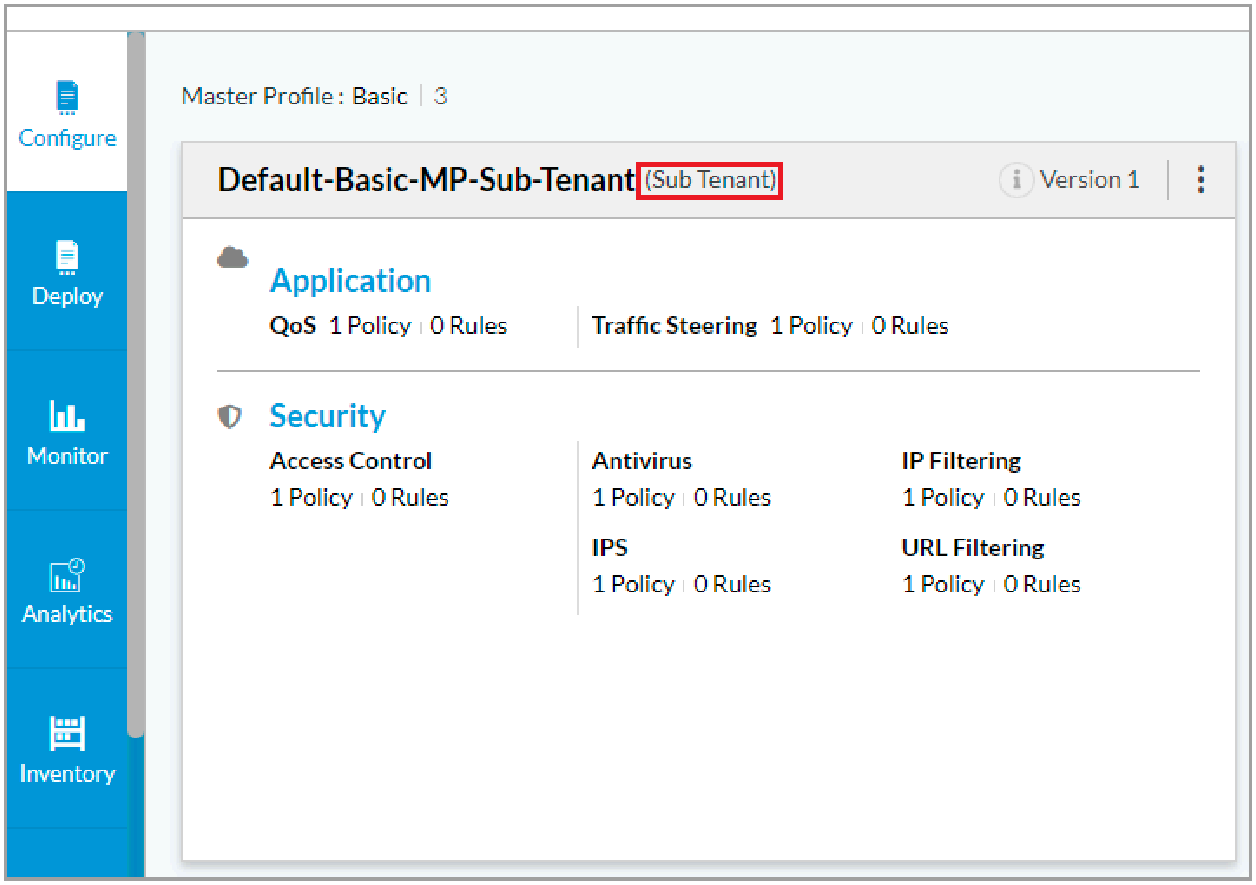


To create an active–active HA deployment, you create a single profile and use it on both the primary and secondary HA appliances. All configuration changes and bind-variable values assignments are made on the primary appliance, even if they are meant for the secondary appliance. After you create the configuration for the primary appliance, Concerto uses that configuration to build the configuration for the secondary appliance in the HA pair. After you configure both HA appliances, you publish each of the appliances separately to create the HA deployment.

The cross-connect interface shown in the figure above is optional. If the WAN interfaces on both the primary and secondary appliances are the same, that is, if the circuits are the same in each WAN interface, you do not need to add the cross-connect interface. If you do need the cross-connect, you configure it in the same way as any other interface type.

You can also convert any non-HA master profile to active–active mode by simply adding a redundant WAN interface to it. Redundant WAN interfaces are attached to the secondary appliance.

For Releases 11.2.1 and later, Concerto provides a default subtenant basic master profile at the subtenant level. You use a subtenant standard master profile to configure security and application services for a subtenant. The subtenant basic master profile does not support other services.



Make Mandatory Updates to the Default Basic Master Profile

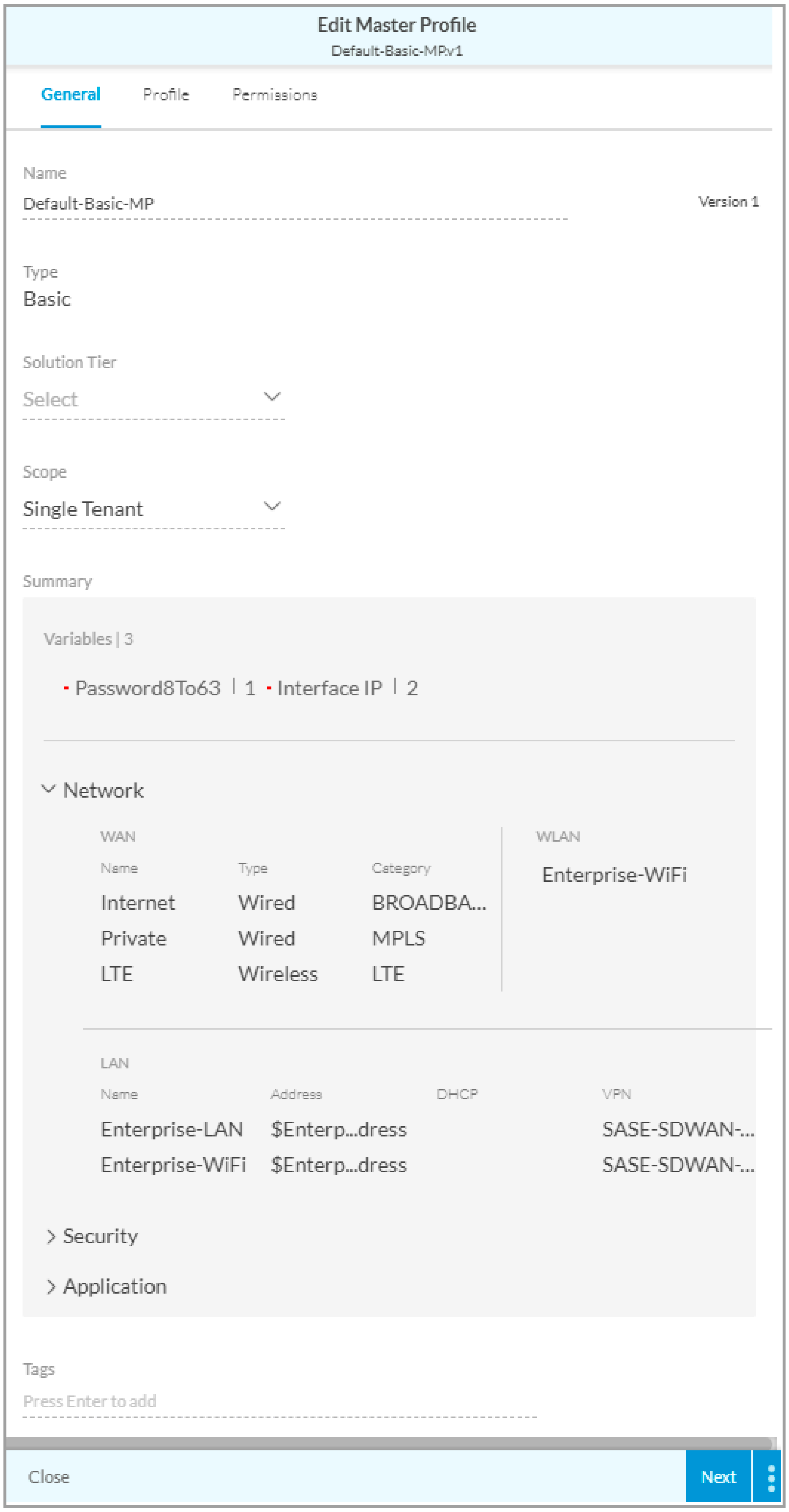
When you create a new tenant in the Concerto orchestrator, several built-in configuration objects are created, and they are packaged with the Concerto software. One of the built-in objects is the default basic master profile, which is named

Default-Basic-MP.v1. You must update this profile before using it on an appliance. You can also clone this basic master profile and modify it before applying it to an appliance.

In the Default-Basic-MP.v1 object, the following interfaces are preconfigured:

- Three WAN interfaces
    - Two wired interfaces, named Private and Internet
    - One LTE interface
- Three LAN interfaces
    - One wired LAN interface
    - One enterprise WiFi interface
    - One guest WiFi interface

The following figure shows the default WAN and LAN interfaces in the default basic master profile. The Type field shows that the master profile is a basic master profile.



Edit Master Profile
Default-Basic-MPv1

Name
Default-Basic-MP
Version 1

Type
Basic

Solution Tier
Select

Scope
Single Tenant

Summary

Variables | 3

- Password8To63 | 1 - Interface IP | 2

Network

WAN

Name	Type	Category
Internet	Wired	BROADBA...
Private	Wired	MPLS
LTE	Wireless	LTE

WLAN
Enterprise-WiFi

LAN

Name	Address	DHCP	VPN
Enterprise-LAN	$Enterp...dress		SASE-SDWAN-...
Enterprise-WiFi	$Enterp...dress		SASE-SDWAN-...

Security

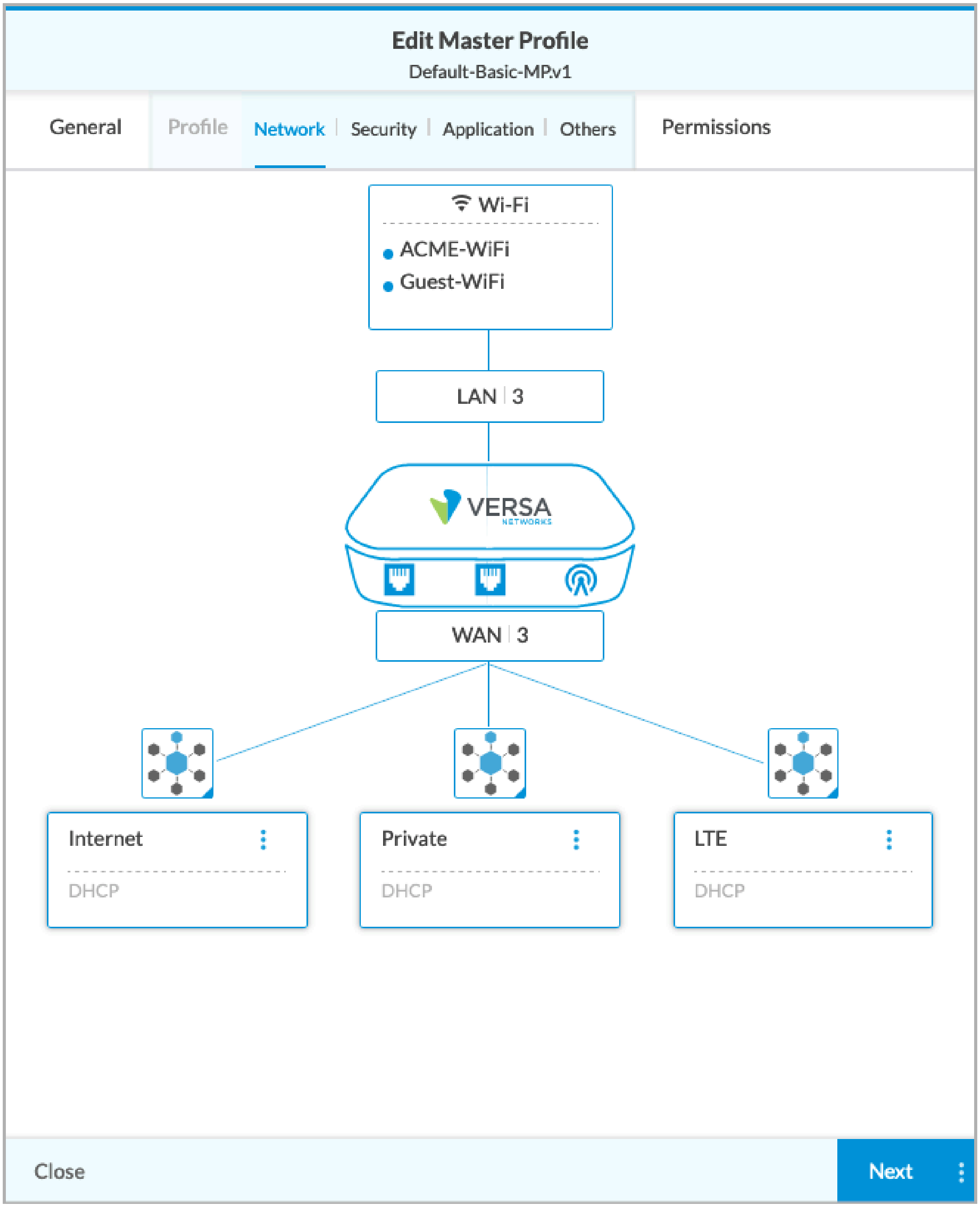
Application

Tags
Press Enter to add

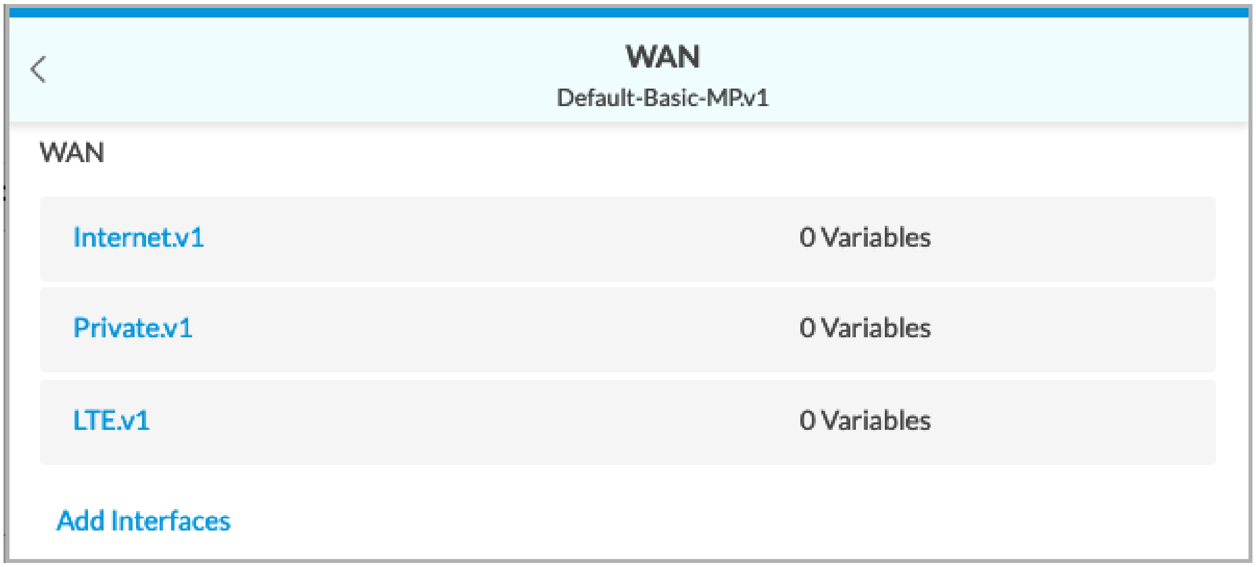
Before you use the default basic master profile on an appliance, you must disable the interfaces that are not required and then associate them with one of the WAN connections (the WAN networks defined on the Director node). You must also set the direct internet access connection names under VPN Instances.

To make the mandatory updates to the default basic master profile:

1. In Tenant view, select the Configure lifecycle in the left menu bar.
2. Select Profiles > Master Profiles.
3. Select the Default-Basic-MP profile in the main pane. The Edit Master Profile screen displays.
4. Select the Profile tab. The Network subtab displays, showing a diagram of the network.



5. Click the WAN box in the network diagram. The WAN screen displays the three WAN interfaces. Because these interfaces are specific to each deployment, the default basic master profile is not preconfigured with connection names for the WAN interfaces.



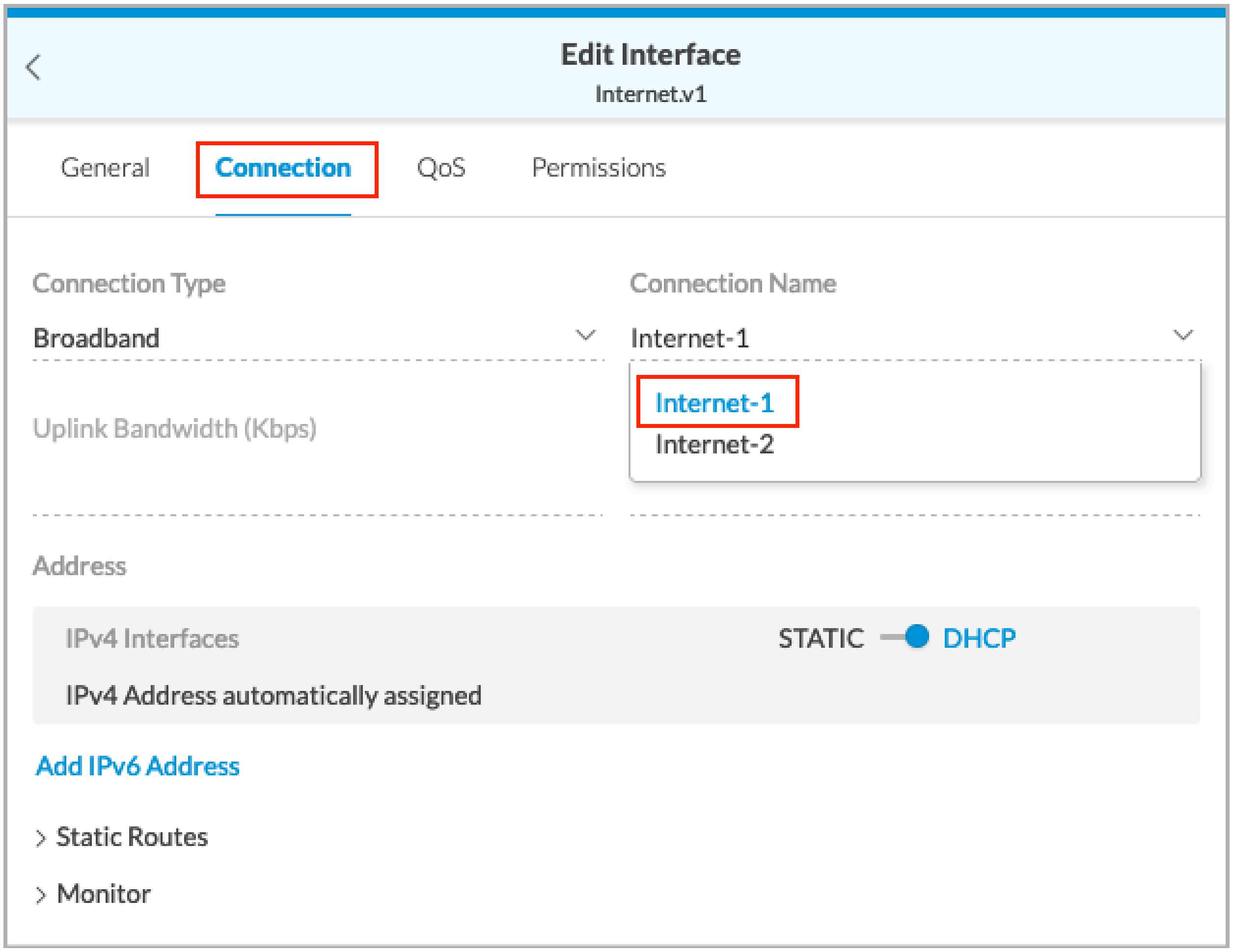
WAN

Default-Basic-MP.v1

WAN

Internet.v1	0 Variables
Private.v1	0 Variables
LTE.v1	0 Variables

6. Click an interface name. The Edit Interface screen displays.
7. Click the Connection tab, and then select a connection in the Connection Name field. The following screenshot shows that the Internet-1 connection is selected.



Edit Interface

Internet.v1

Connection Type: Broadband

Connection Name: Internet-1

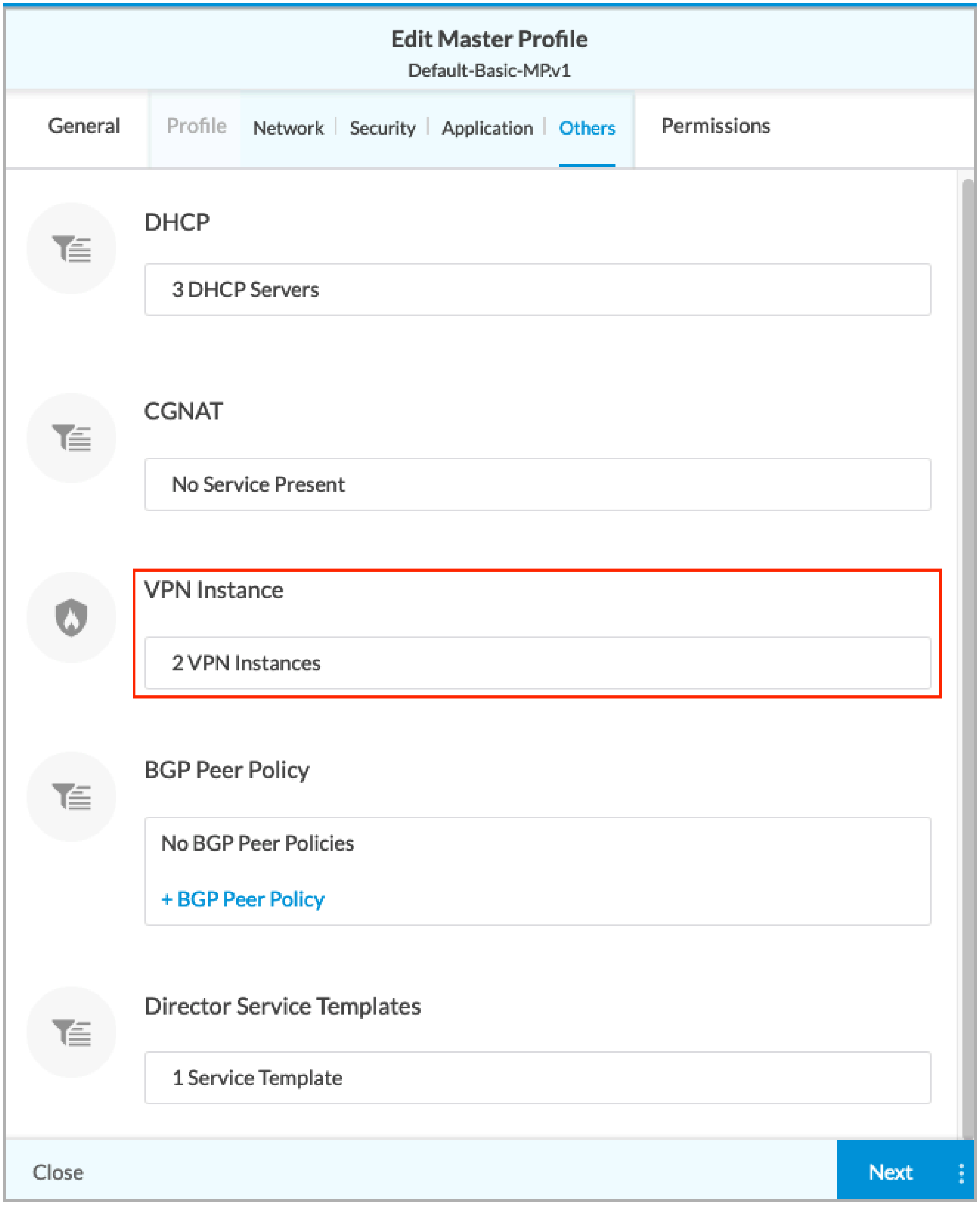
Uplink Bandwidth (Kbps)

Address

IPv4 Interfaces: STATIC / DHCP

IPv4 Address automatically assigned

8. Repeat Step 7 for the other two WAN interfaces.
9. To set the direct internet access connection names, click the Others tab in the Edit Master Profile screen.



DHCP

3 DHCP Servers

CGNAT

No Service Present

VPN Instance

2 VPN Instances

BGP Peer Policy

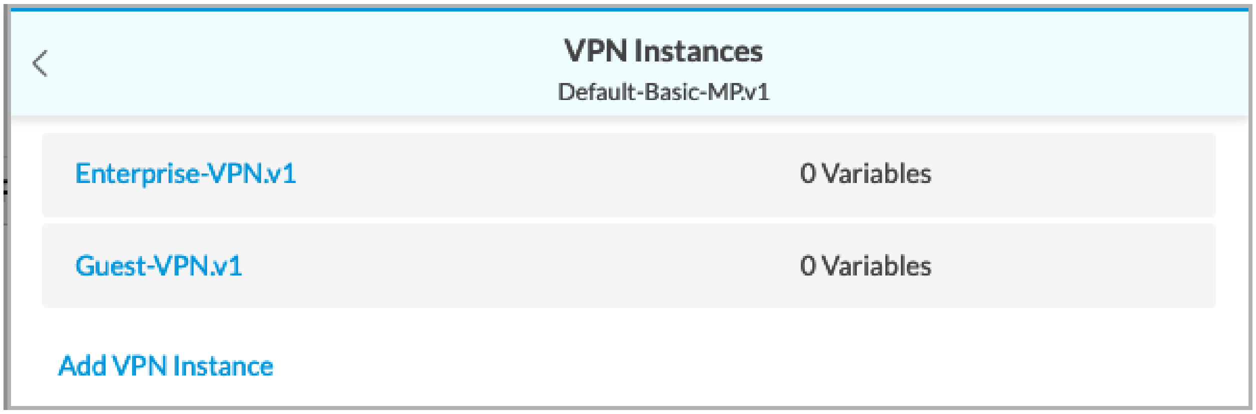
No BGP Peer Policies

+ BGP Peer Policy

Director Service Templates

1 Service Template

10. Click the VPN instances box. The VPN Instances screen displays.



VPN Instances

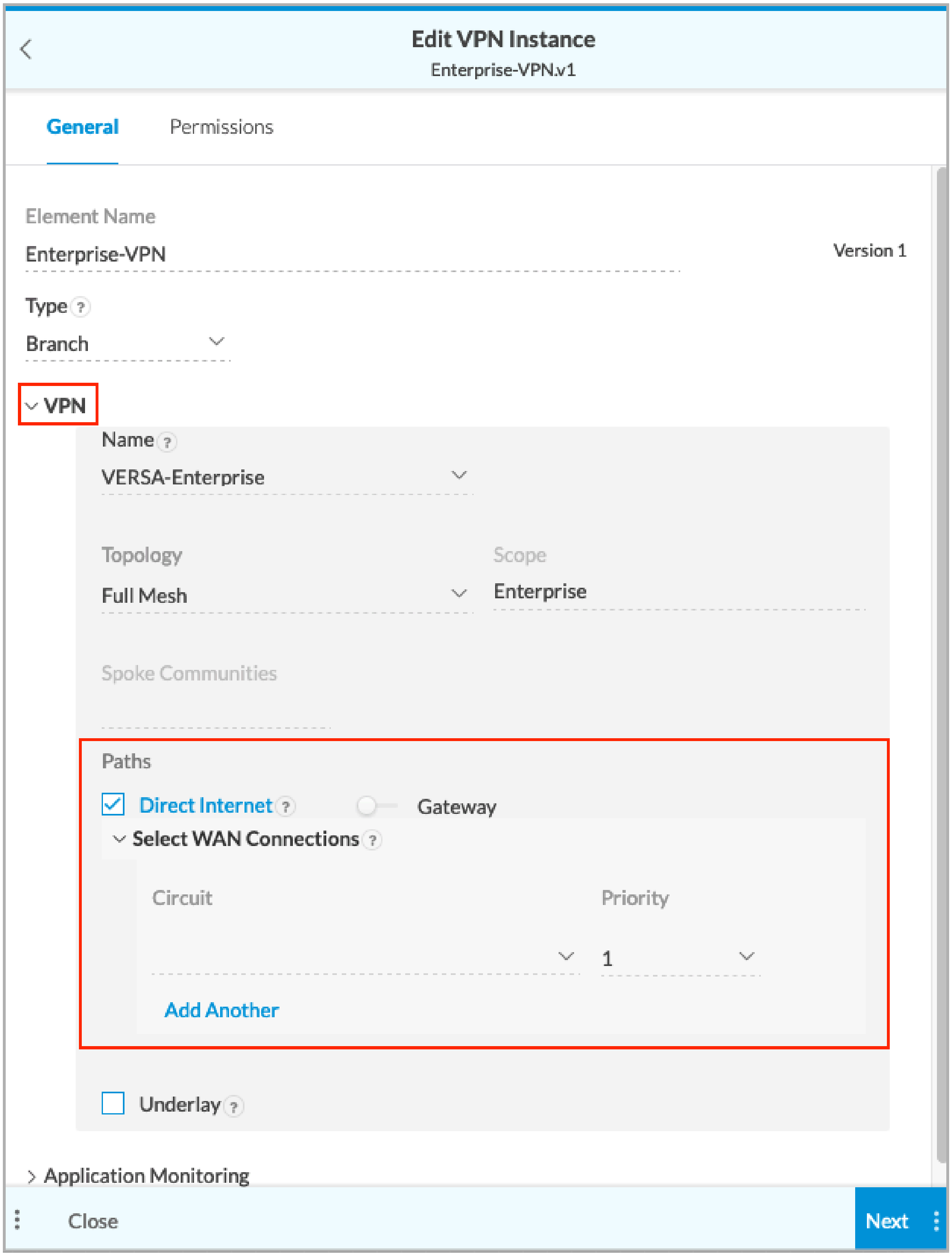
Default-Basic-MP.v1

Enterprise-VPN.v1 0 Variables

Guest-VPN.v1 0 Variables

Add VPN Instance

11. Click a VPN instance. The Edit VPN Instance screen displays.



Edit VPN Instance
Enterprise-VPN.v1

Element Name: Enterprise-VPN
Version 1

Type: Branch

VPN

Name: VERSA-Enterprise

Topology: Full Mesh

Scope: Enterprise

Spoke Communities

Paths

☑ Direct Internet ○ Gateway

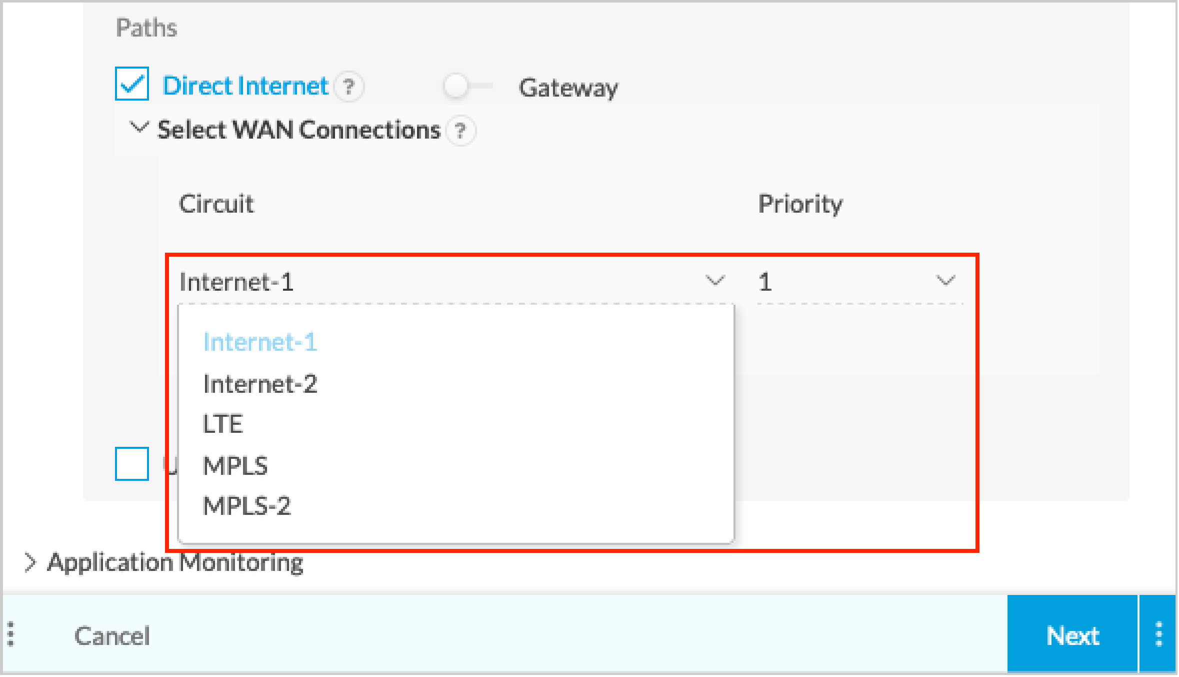
Select WAN Connections

Circuit:

Priority: 1

☐ Underlay

12. Click VPN, and then under Paths, select Direct Internet.
13. Under Circuit, select a connection name, and then under Priority, select a priority for the direct internet access (DIA) connection.



14. Click the Permissions tab, and then click Save. A message displays at the top of the Configuration screen confirming that the basic master profile has been updated successfully.

Make Optional Updates to the Default Basic Master Profile

Based on your site configuration requirements, you may need to create a new basic master profile. To do this, you clone the Default-Basic-MP.v1 master profile and then update it as needed. The following are some of the common changes you can make to the master profile:

- Configure a multitenant master profile.
- Disable the LTE interface.
- Enable or disable DIA.
- Update the authentication protocol for the WiFi interface.
- Add traffic steering, QoS, and security rules.
- Update or add services.

Configure a Multitenant Basic Master Profile

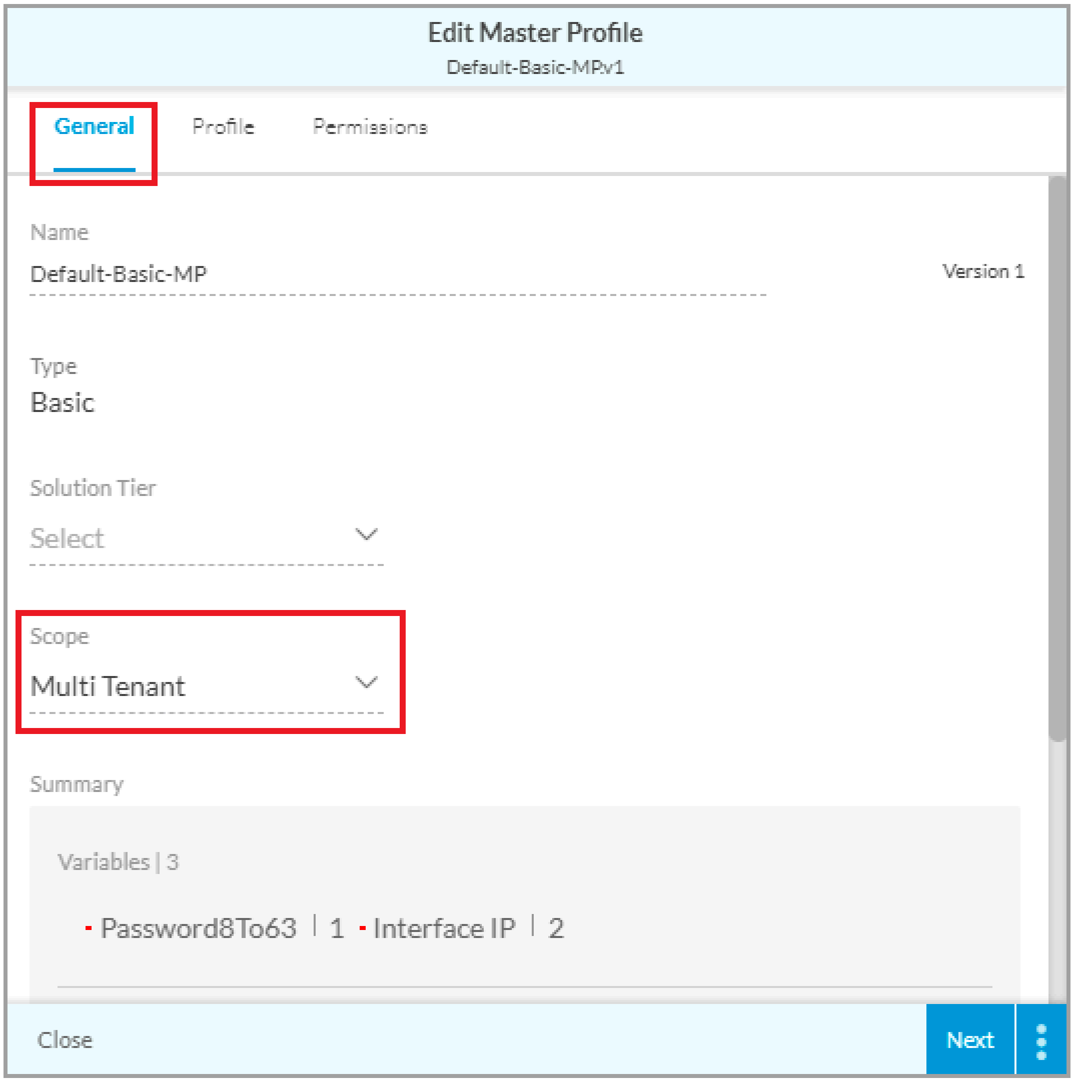
For Releases 11.2.1 and later.

You can edit a default active–active master profile or default basic master profile to allow multitenancy. With a multitenant basic master profile, you can create multitenant appliances for a provider organization. You can create new subtenants, and you can attach existing subtenants while publishing the provider organization appliance that uses the multitenant master profile. Appliances are automatically created in the subtenants associated with a provider appliance that uses a multitenant master profile.

In a multitenant basic master profile, you create interfaces for subtenants in the provider tenant profile. Because interfaces, networks, and routing instances are common appliance resources, configuring them at the provider tenant level avoids overlapping of the configuration among tenants. For example, multiple tenants can use vni-0/0.1 independently on the same appliance. Having shared resources such as interfaces helps to avoid such misconfiguration and simplify the implementation. You configure interfaces and routing on a multitenant appliance at the provider tenant level. The provider user can mark each interface for the subtenant to which it belongs. The remainder of the service configuration, such as security, traffic steering, and application QoS, can be performed at the subtenant level by subtenant or provider tenant users.

To configure a multitenant basic master profile:

1. Configure the scope of the default active–active (Default-Active-Active) or default basic master profile (Default-Basic-MP) to multitenant.
    a. Click the basic master profile.
    b. In Edit Master Profile > General, select Multitenant in the Scope field.



Edit Master Profile
Default-Basic-MPv1

Name
Default-Basic-MP
Version 1

Type
Basic

Solution Tier
Select

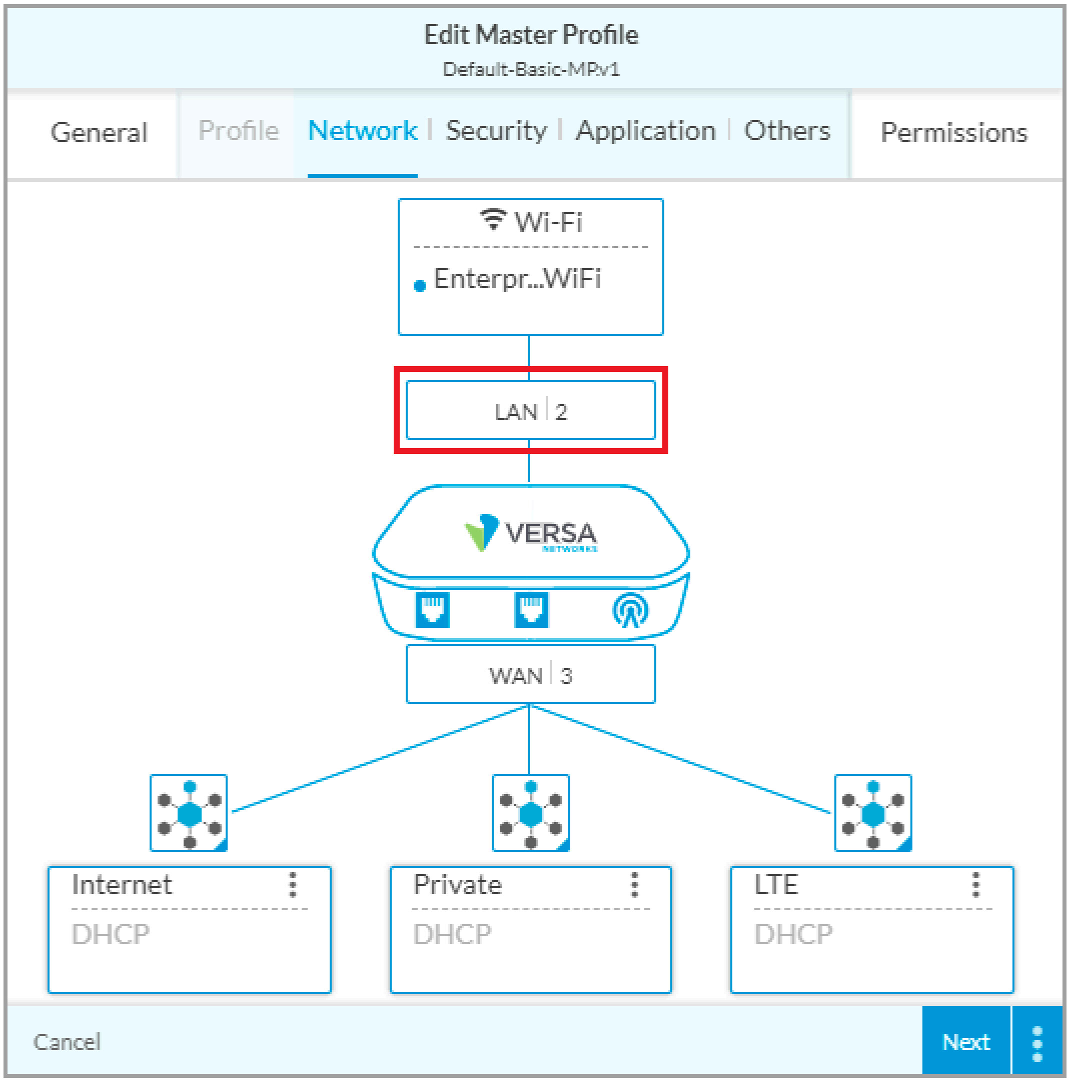
Scope
Multi Tenant

Summary

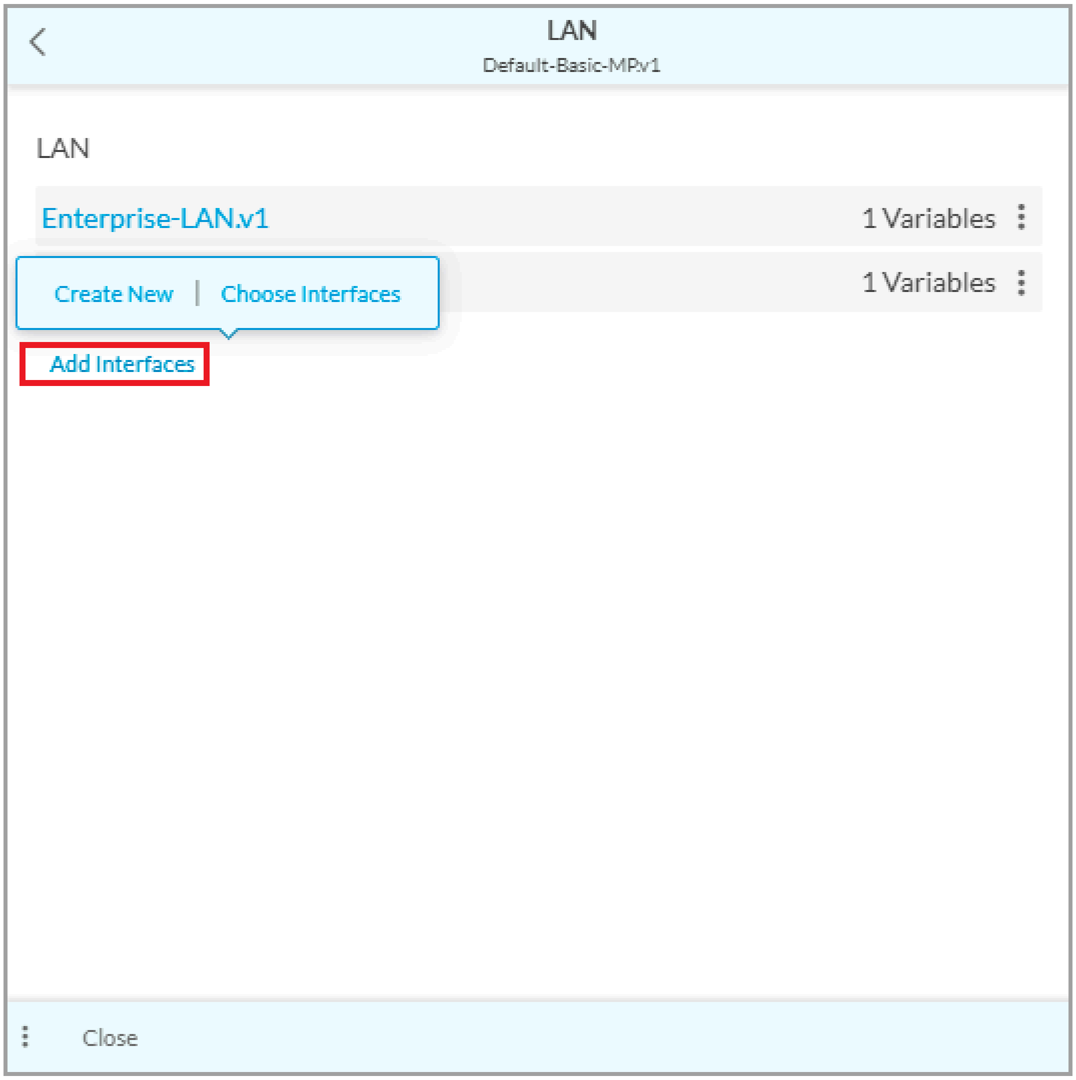
Variables | 3

- Password8To63 | 1 - Interface IP | 2

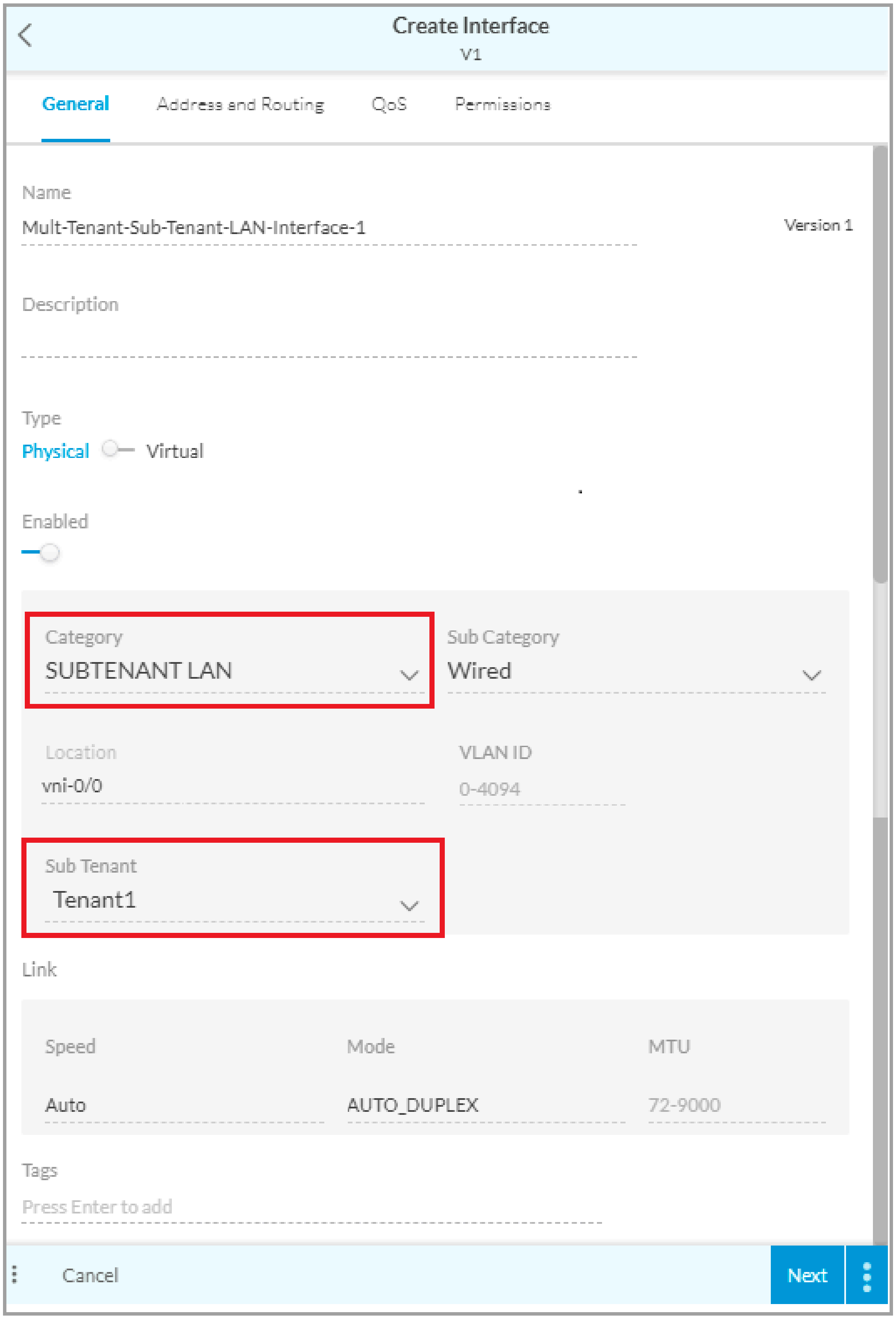
2. Configure subtenant LAN interfaces for subtenants that are associated with the provider organization. By default, the master profile contains a LAN interface. Note that you can create subtenant LAN interfaces only for basic master profiles of type Multitenant.
   a. Select Edit Master Profile > Profile. The Network subtab displays, showing a diagram of the network.
   b. Click LAN.



c. In the LAN screen, click Add Interfaces > Create New. The LAN screen displays the default enterprise LAN interface.



d. In Create Interface screen > General tab, enter a name for the subtenant LAN interface.



Create Interface
V1

General | Address and Routing | QoS | Permissions

Name: Mult-Tenant-Sub-Tenant-LAN-Interface-1 — Version 1

Description:

Type: Physical ○— Virtual

Enabled

Category: SUBTENANT LAN

Sub Category: Wired

Location: vni-0/0

VLAN ID: 0-4094

Sub Tenant: Tenant1

Link

Speed: Auto

Mode: AUTO_DUPLEX

MTU: 72-9000

Tags: Press Enter to add

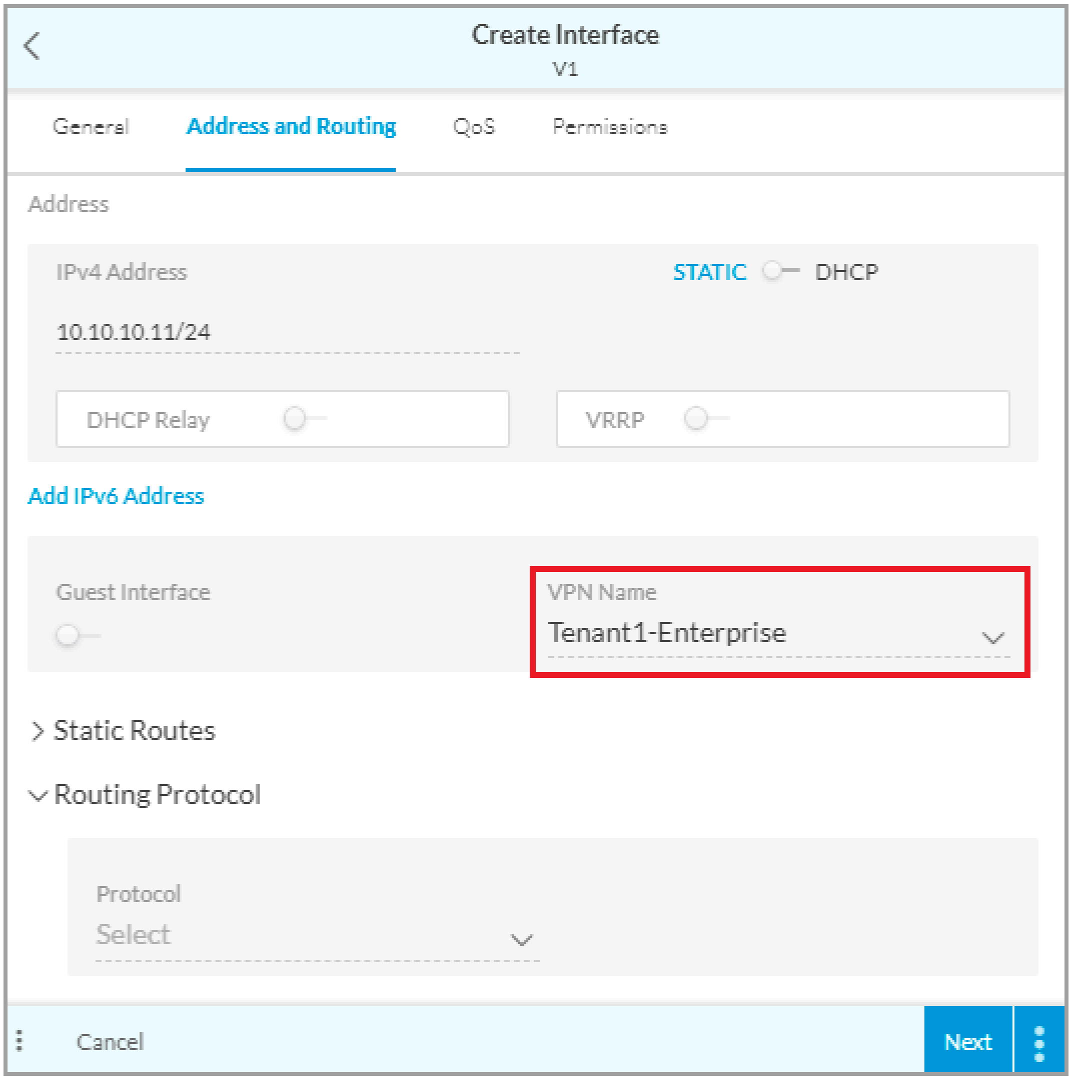
Cancel | Next

e. In the Category field, select Subtenant-LAN.

f. Select the location.

g. In the Subtenant field, select the subtenant for which you are creating the subtenant LAN interface.

h. Click Next. The Address and Routing tab displays.



Create Interface
V1

Address

IPv4 Address: 10.10.10.11/24

STATIC / DHCP

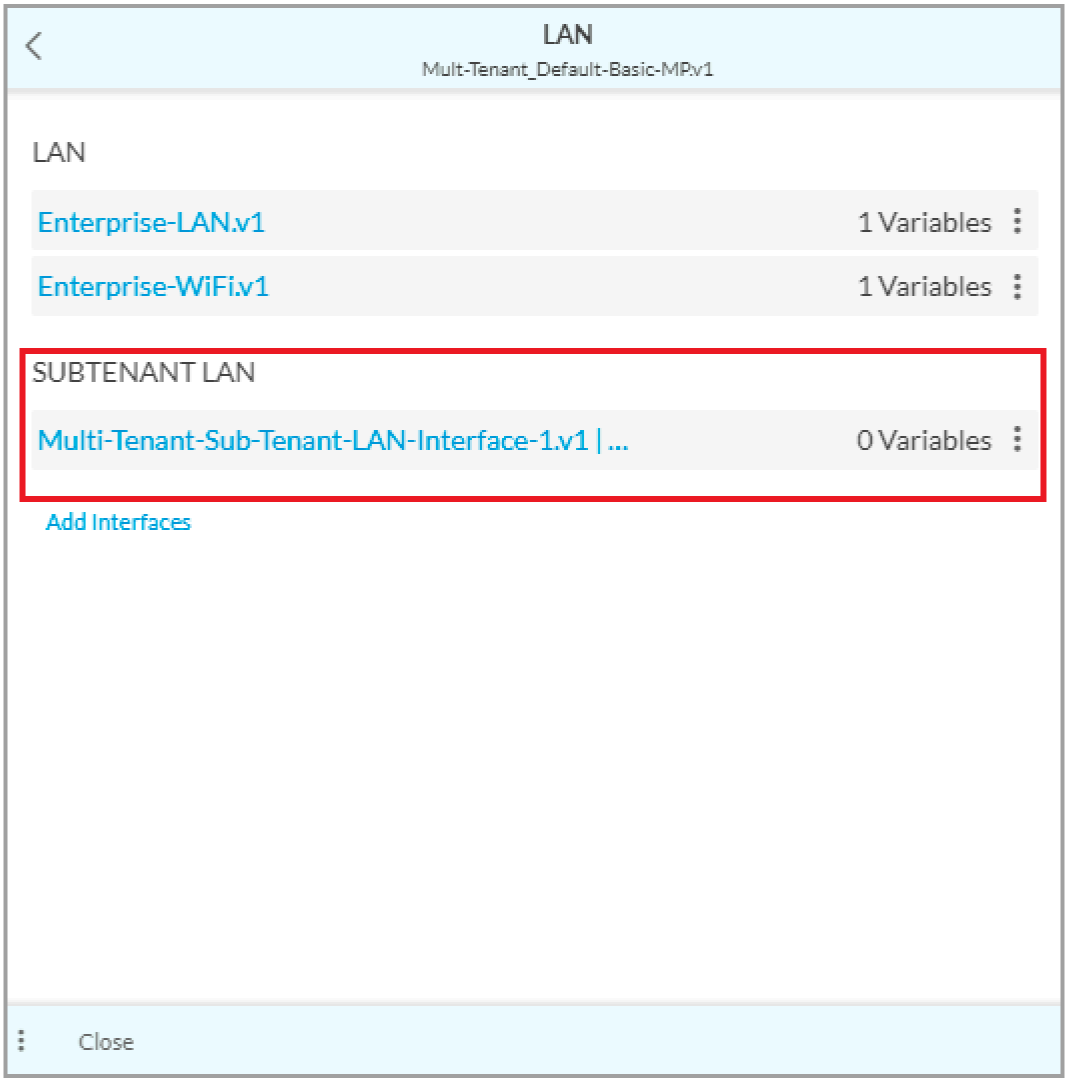
VPN Name: Tenant1-Enterprise

Protocol: Select

i. Enter the IPv4 address for the LAN interface.

j. In the VPN Name field, select the tenant's VPN. By default, the VPN of the tenant you selected in the General tab is displayed

k. Enter information in the other fields, and the save the subtenant LAN interface. The interface that you add displays under Subtenant LAN. For example:



LAN

Mult-Tenant_Default-Basic-MPv1

LAN

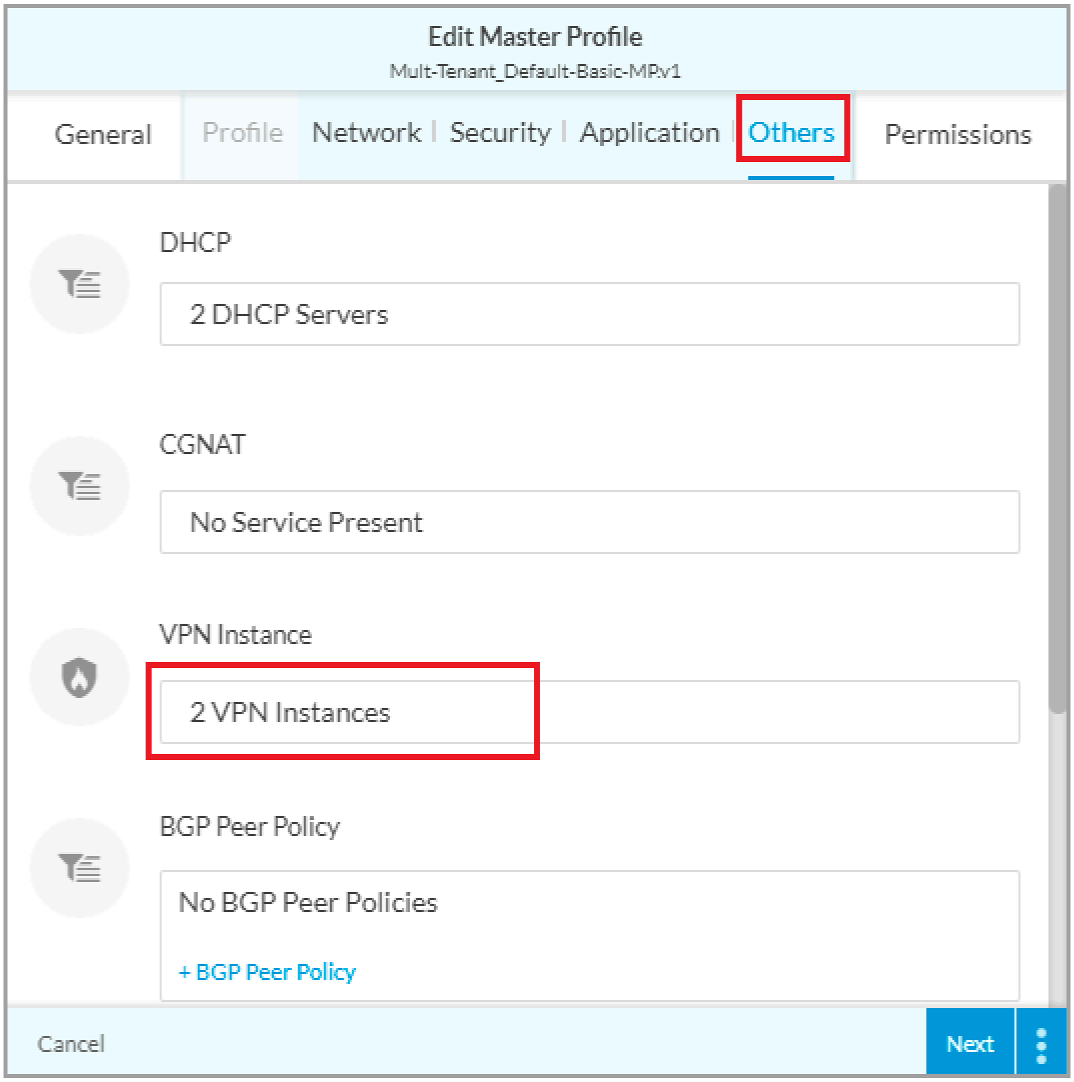
Enterprise-LAN.v1	1 Variables
Enterprise-WiFi.v1	1 Variables

SUBTENANT LAN

Multi-Tenant-Sub-Tenant-LAN-Interface-1.v1 | ...	0 Variables

l. Repeat this step for each subtenant.

3. Create VPN instances to associate subtenant VPNs with the master profile for the provider organization.
   a. In Edit Master Profile > Profile, select the Others tab.



Edit Master Profile

Mult-Tenant_Default-Basic-MPv1

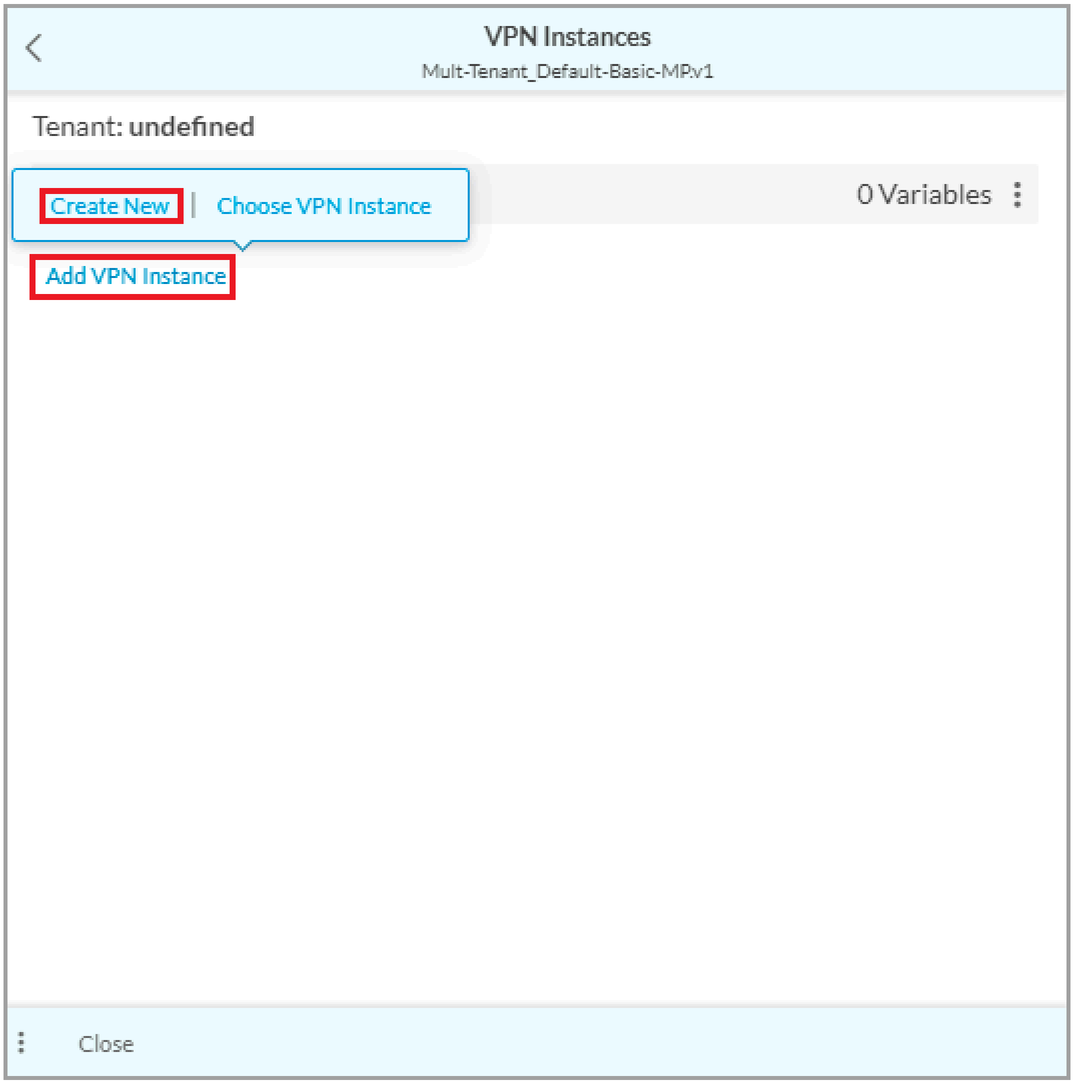
DHCP: 2 DHCP Servers

CGNAT: No Service Present

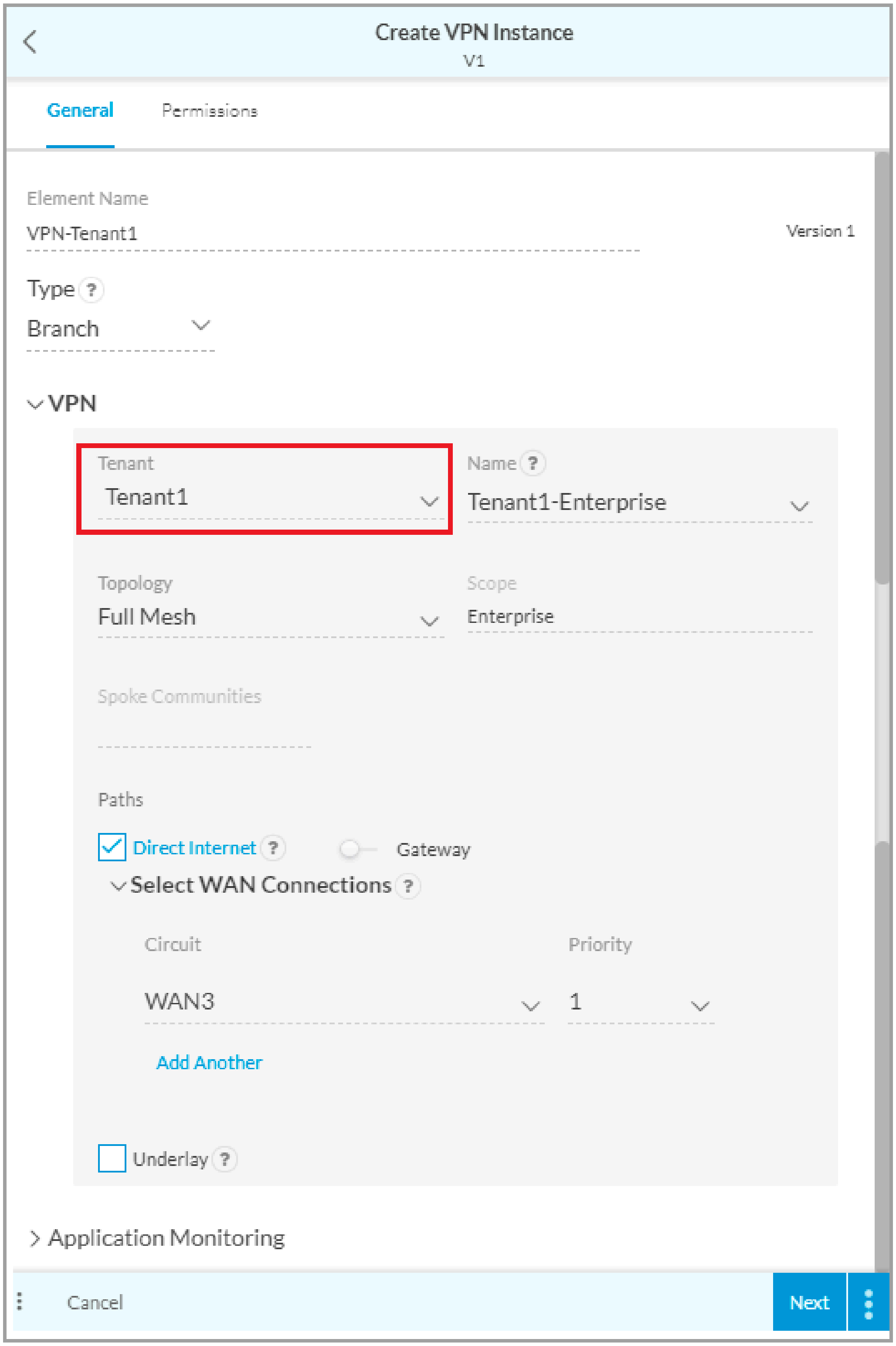
VPN Instance: 2 VPN Instances

BGP Peer Policy: No BGP Peer Policies

b. Click the VPN Instance field. In the VPN Instances screen, click Add VPN Instance, and then click Create New.


VPN Instances
Mult-Tenant_Default-Basic-MPv1
Tenant: undefined
Create New | Choose VPN Instance
0 Variables
Add VPN Instance
Close

c. In the Create VPN Instance screen, select the General tab.



Create VPN Instance
V1

General Permissions

Element Name: VPN-Tenant1 — Version 1

Type: Branch

VPN

Tenant: Tenant1 — Name: Tenant1-Enterprise

Topology: Full Mesh — Scope: Enterprise

Spoke Communities

Paths

☑ Direct Internet — ○ Gateway

Select WAN Connections

Circuit	Priority
WAN3	1

Add Another

□ Underlay

Application Monitoring

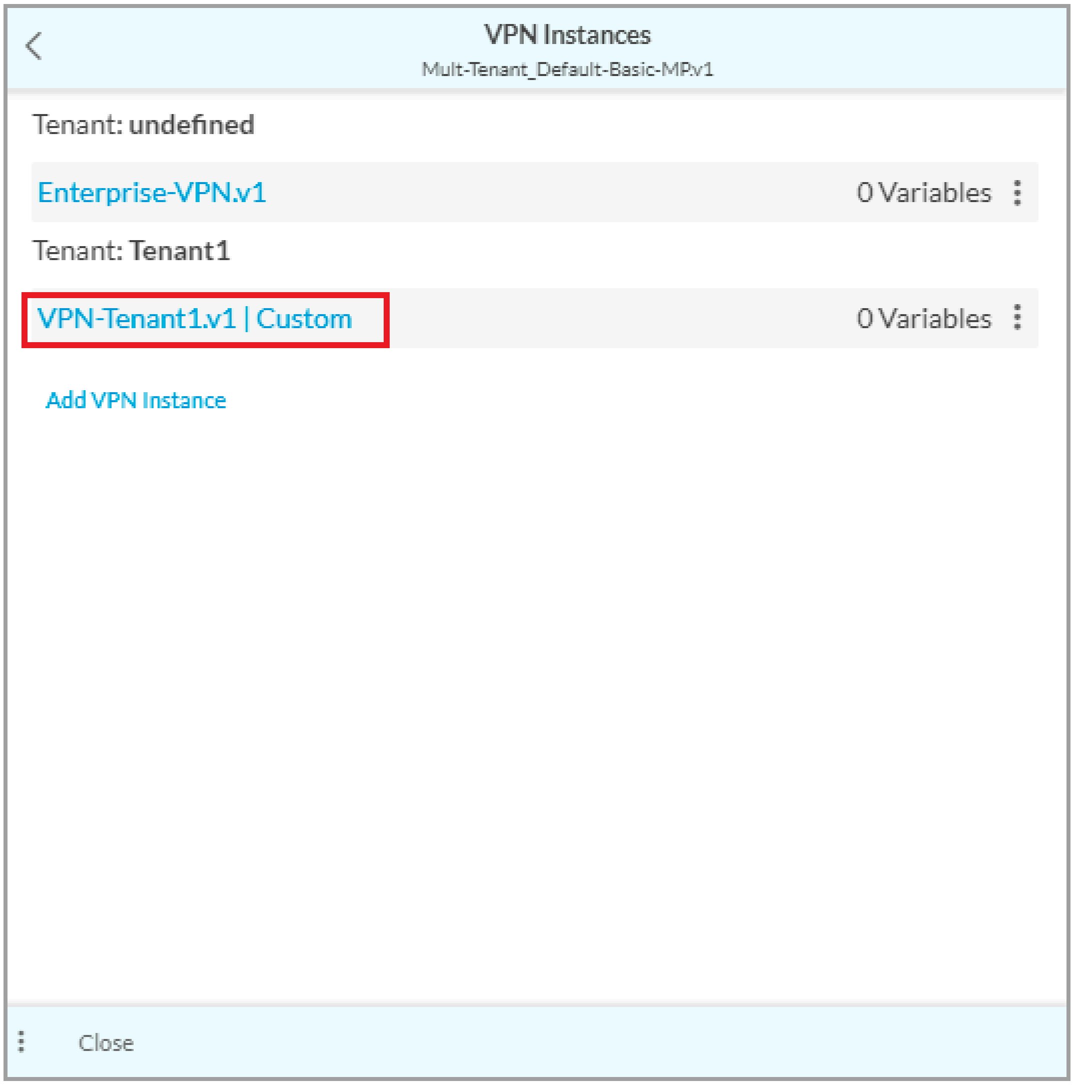
d. Enter a name for the VPN instance for the tenant.

e. Under VPN, select the tenant for which to create VPN instance.

f. Select the name of the VPN connection. By default, the VPN connection of the tenant displays.

g. Enter information in the other fields.

h. Click Next, and then save the VPN instance. The VPN instance displays in the VPN Instances screen.



VPN Instances

Mult-Tenant_Default-Basic-MP.v1

Tenant: undefined

Enterprise-VPN.v1 — 0 Variables

Tenant: Tenant1

VPN-Tenant1.v1 | Custom — 0 Variables

i. Repeat this step for all subtenant VPNs.

4. After you update the master profile, deploy the appliance associated with the master profile. When you publish, Concerto creates a subtenant appliance in each of the subtenants. For more information, see Concerto Deploy Lifecycle Overview.

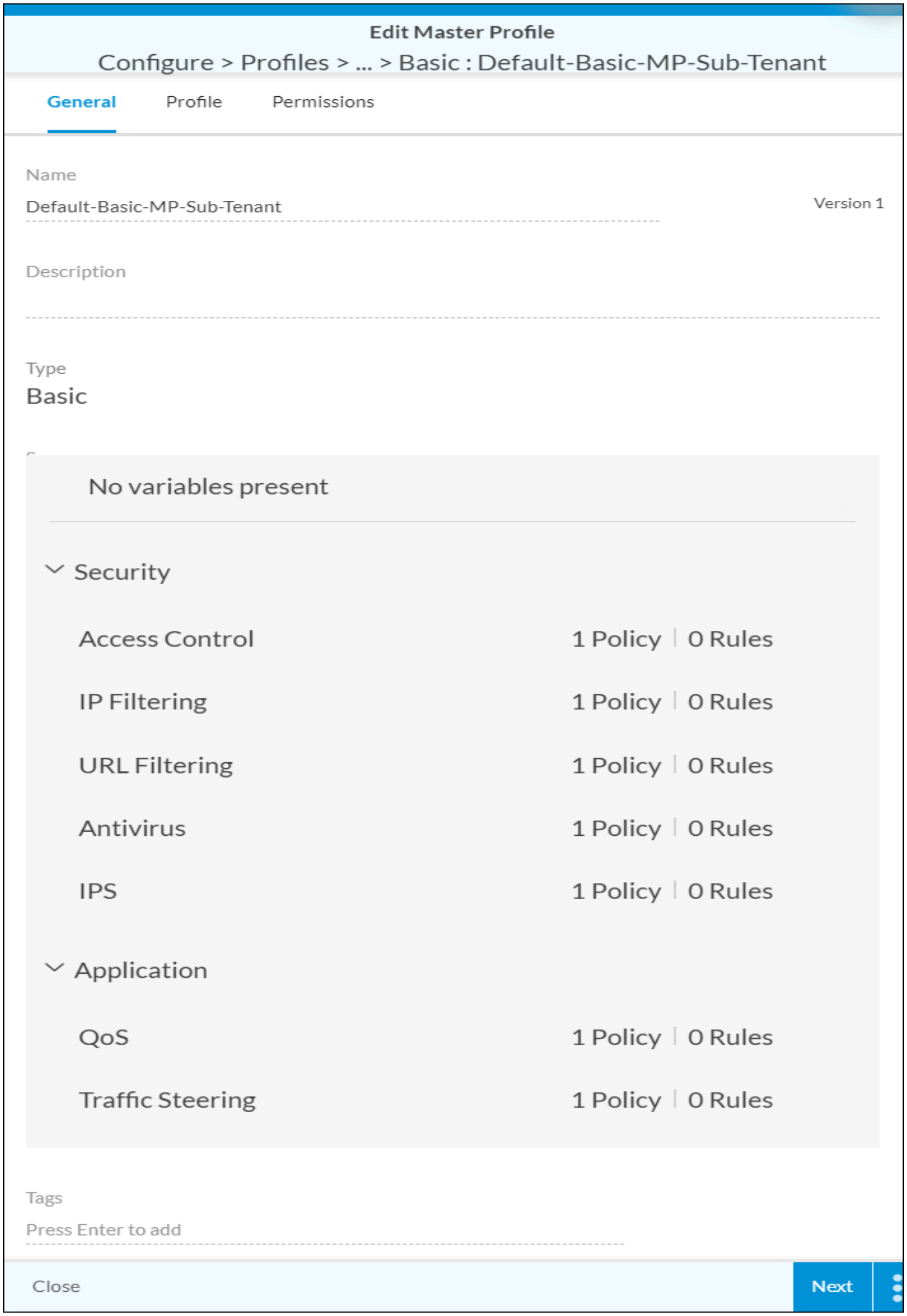
Edit the Subtenant Basic Master Profile

For Releases 11.2.1 and later.

You can use a subtenant standard master profile to configure security and application services for a provider organization.

To edit a subtenant basic master profile:

1. Click the basic subtenant master profile, which the GUI displays as Default-Basic-MP-subtenant. You cannot edit the Type and Scope fields.



Edit Master Profile

Configure > Profiles > ... > Basic : Default-Basic-MP-Sub-Tenant

Name
Default-Basic-MP-Sub-Tenant

Version 1

Description

Type
Basic

No variables present

Security

Access Control	1 Policy	0 Rules
IP Filtering	1 Policy	0 Rules
URL Filtering	1 Policy	0 Rules
Antivirus	1 Policy	0 Rules
IPS	1 Policy	0 Rules

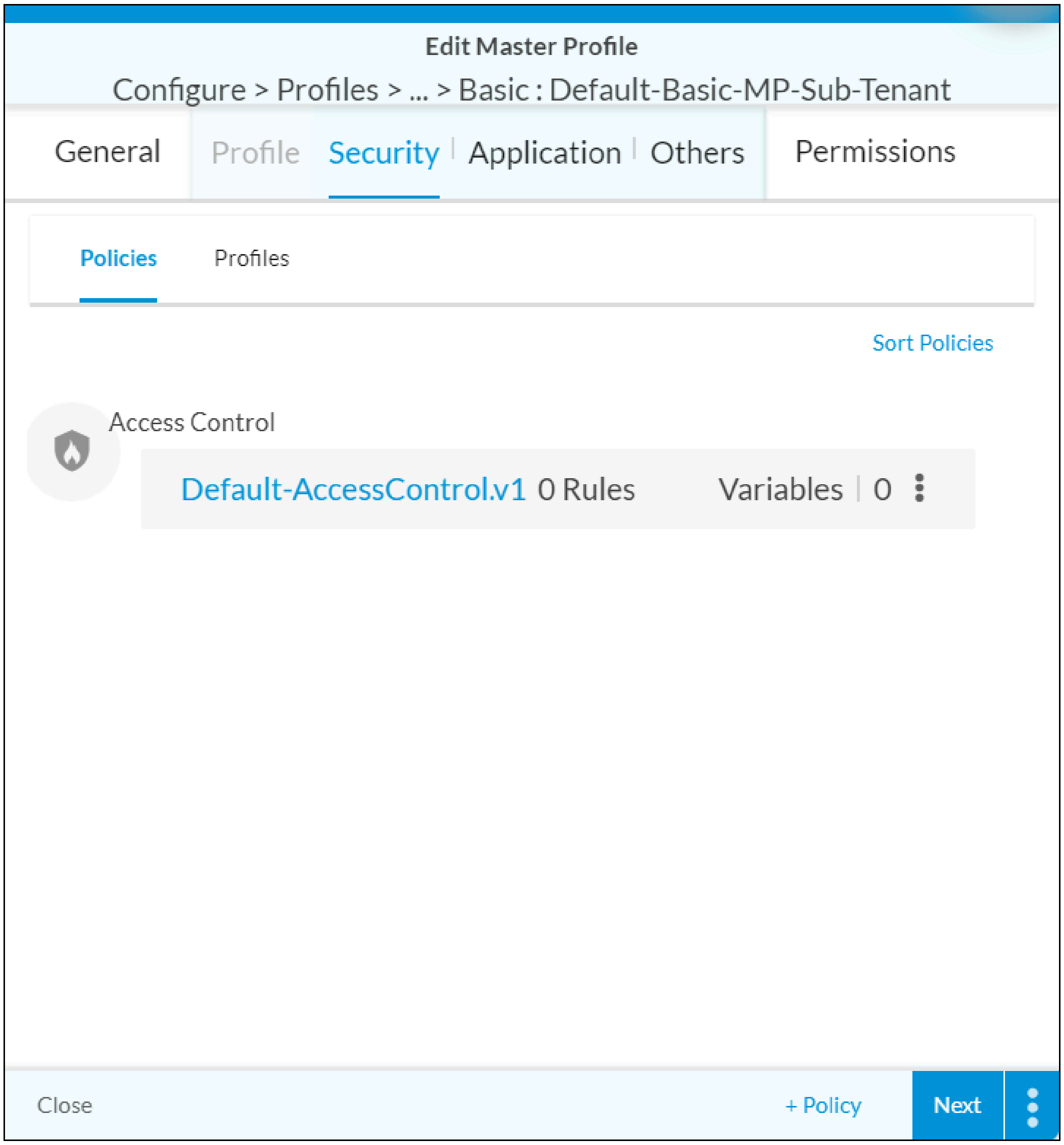
Application

QoS	1 Policy	0 Rules
Traffic Steering	1 Policy	0 Rules

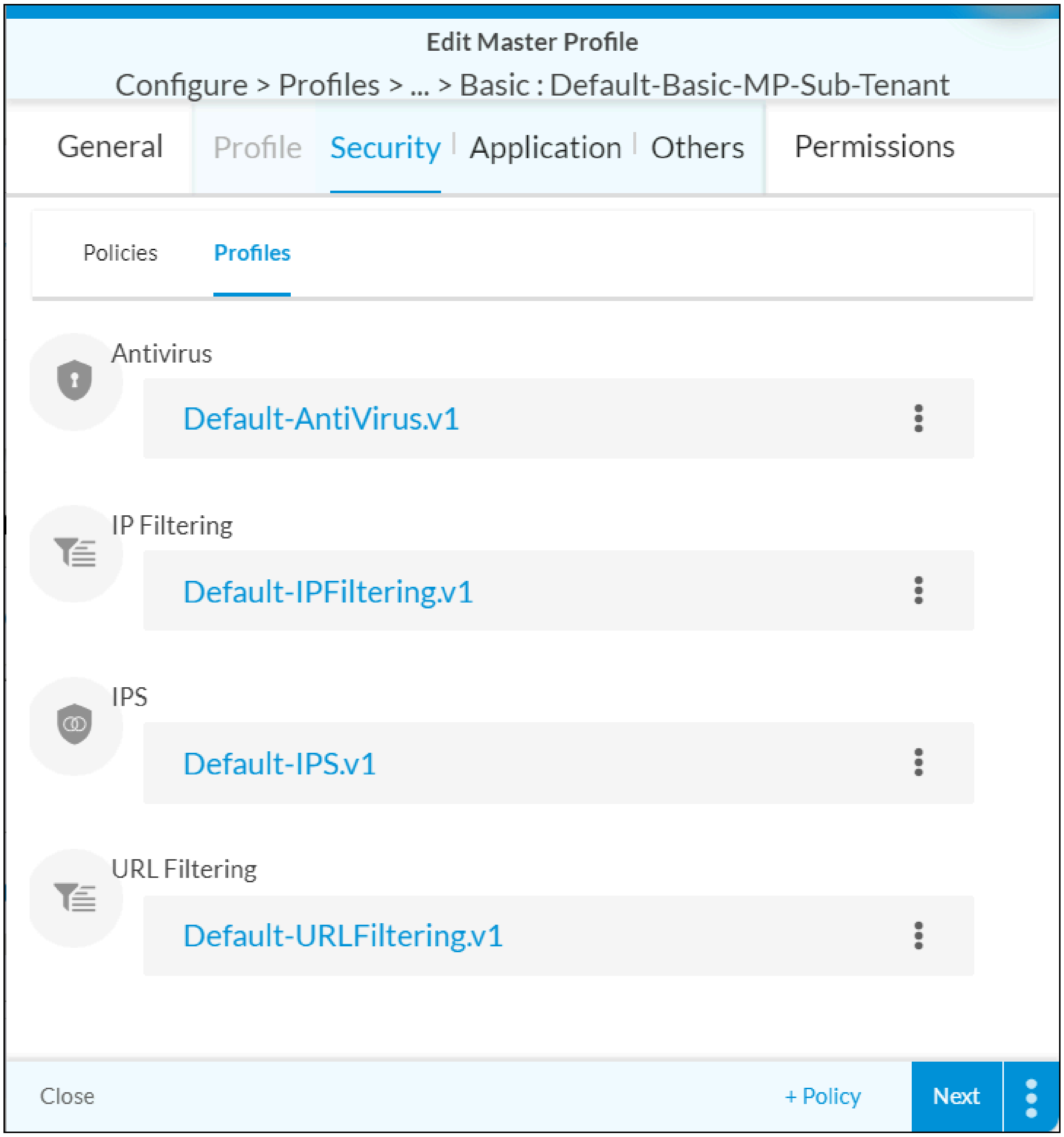
Tags
Press Enter to add

2. Click Next. The Profile > Security tab displays.
    a. Modify the security policies, if required. For more information, see Update Security Policies and Rules, below.

- (For Releases 12.1.1 and later.) To modify the security policy, on the Policies tab, click the policy name.
- (For Releases 11.4.3 and earlier.) To modify the security policy, click the policy name.



b. (For Releases 12.1.1 and later.) Select the Profiles tab, and then modify the security profiles, if required. For more information, see Update Security Policies and Rules, below.



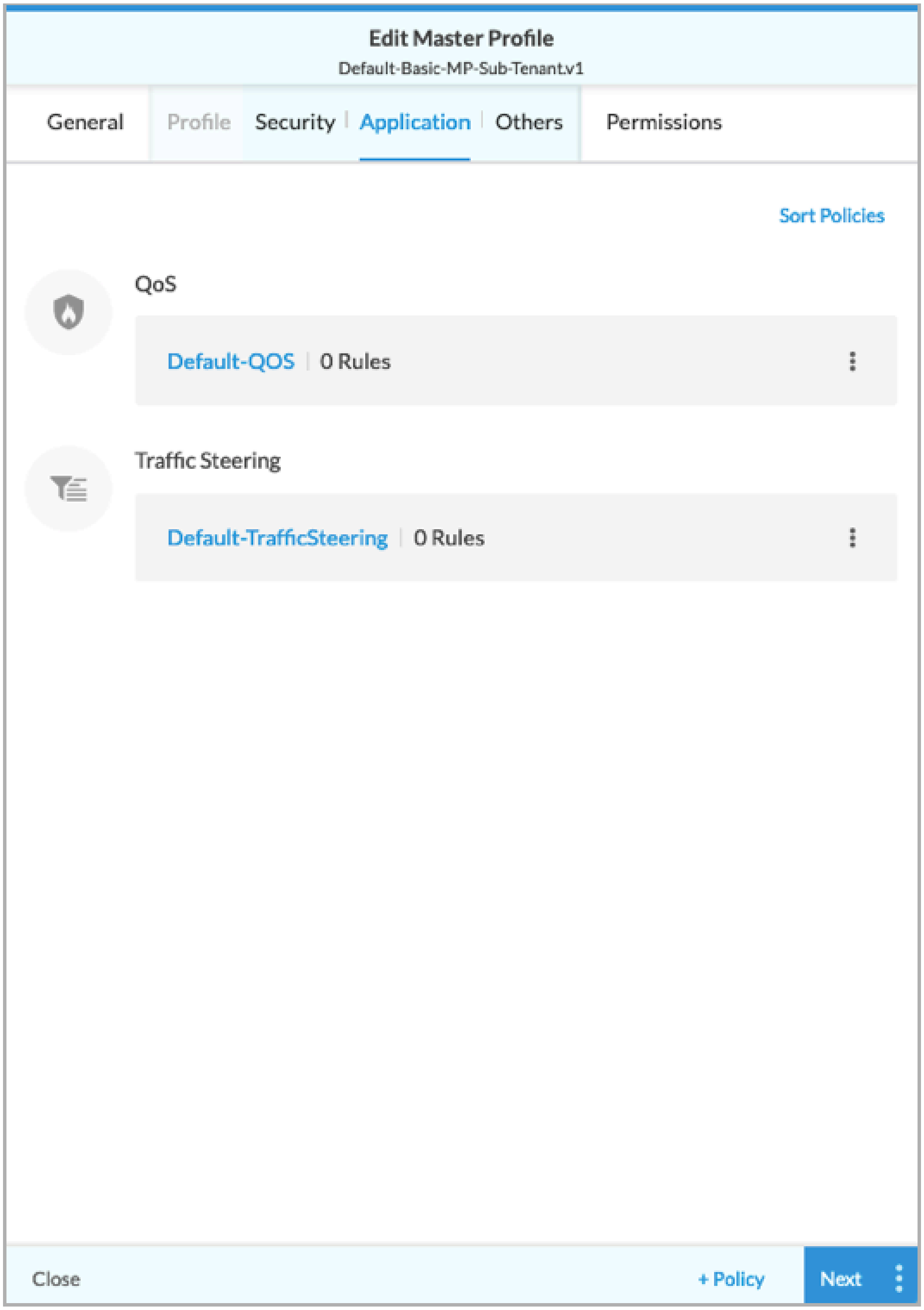
Antivirus: Default-AntiVirus.v1

IP Filtering: Default-IPFiltering.v1

IPS: Default-IPS.v1

URL Filtering: Default-URLFiltering.v1

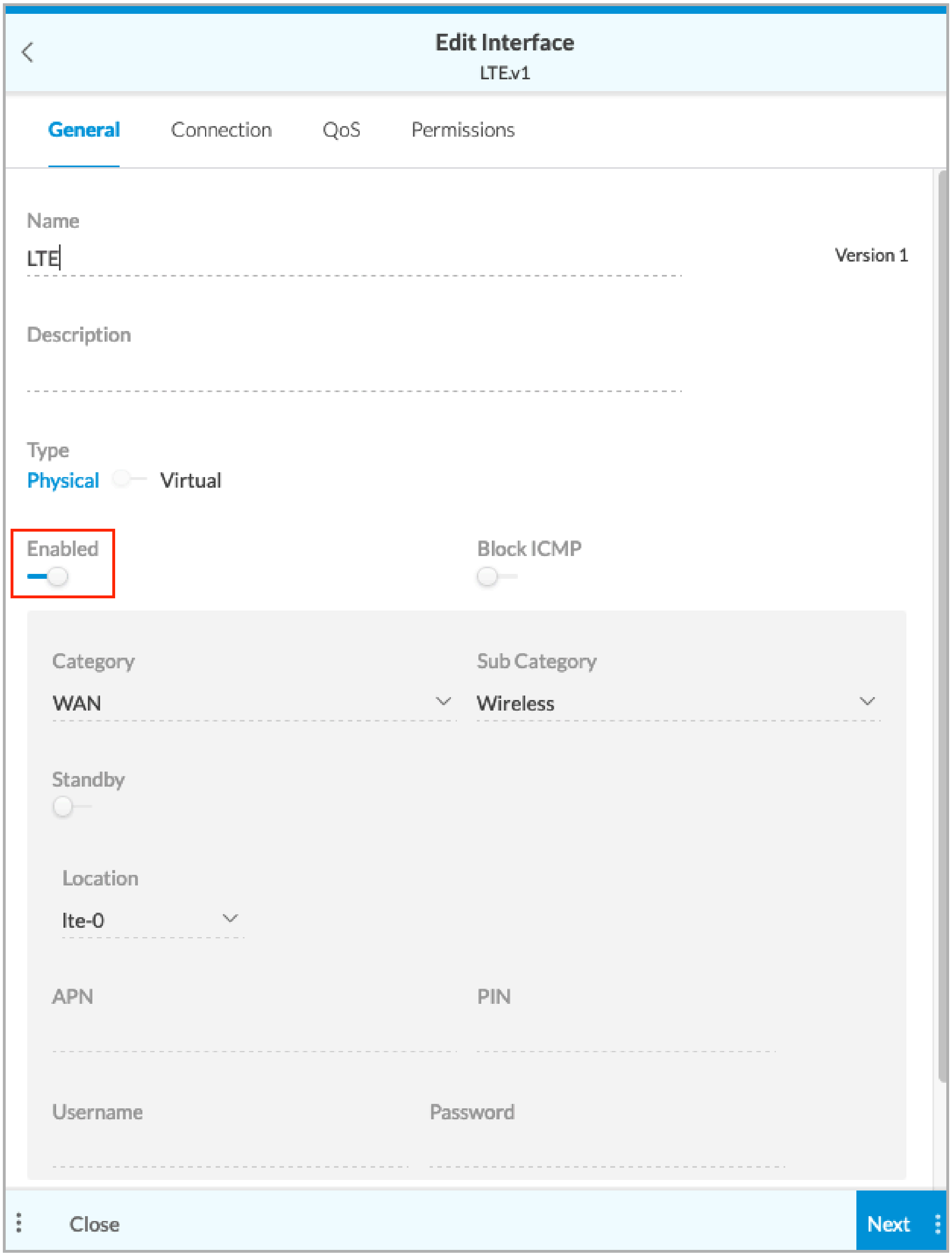
3. Select the Application tab, and then modify the QoS and traffic-steering policies, if required. For more information, see Configure QoS Policies and Rules and Configure Traffic-Steering Policies and Rules, below.



4. Make other changes in the Others and Permissions tabs.
5. Save the subtenant basic master profile.

Disable the LTE Interface

1. In Edit Master Profile > Profile > Network, click the ⋮ Ellipses icon in the LTE box, and then select Edit. The Edit Interface screen displays.



Name
LTE

Version 1

Description

Type
Physical Virtual

Enabled

Block ICMP

Category
WAN

Sub Category
Wireless

Standby

Location
lte-0

APN

PIN

Username

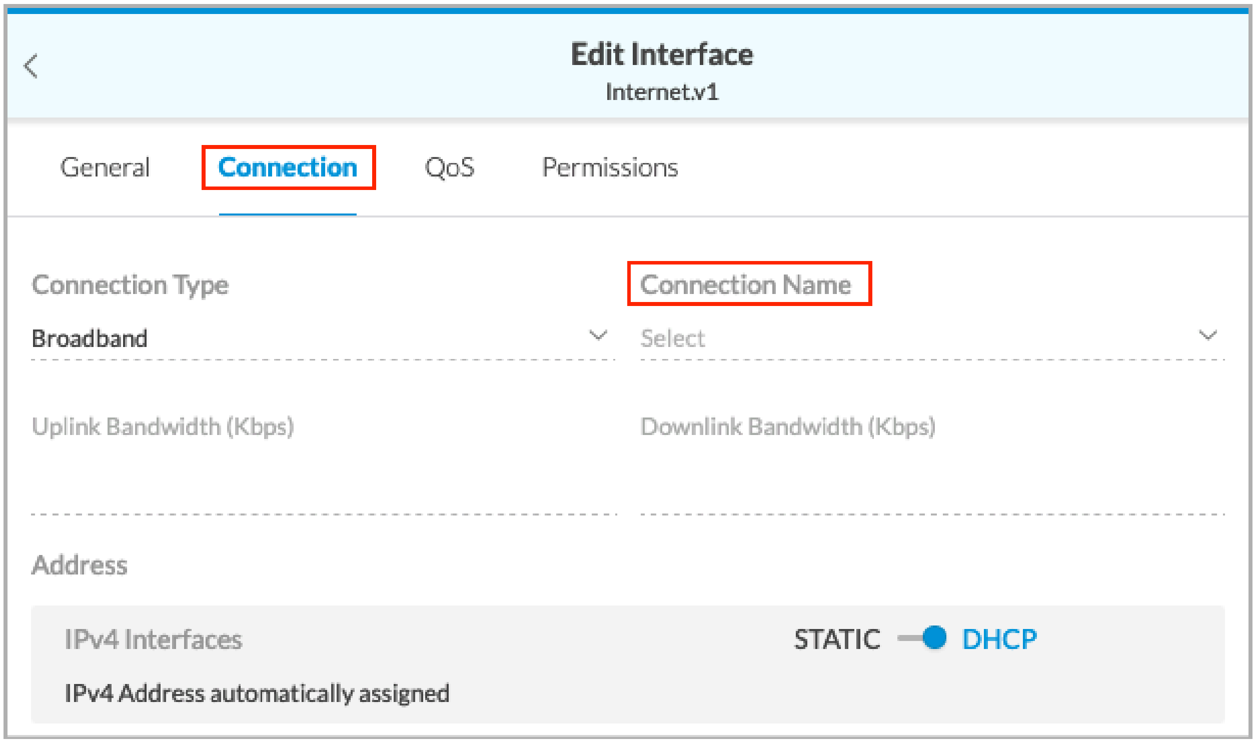
Password

2. Click the Enabled indicator so that it is grayed out. The LTE interface is disabled.

Enabled

Enable or Disable DIA on a WAN Interface

1. In Edit Master Profile > Profile > Network, click the interface on which to enable or disable DIA. The Edit Interface screen displays.



Edit Interface
Internet.v1

Connection Type: Broadband
Connection Name: Select
Uplink Bandwidth (Kbps)
Downlink Bandwidth (Kbps)
Address
IPv4 Interfaces STATIC ● DHCP
IPv4 Address automatically assigned

2. In the Connection Name field, configure a name for the interface. Configure the connection name before you change the connection type.

3. In Edit Master Profile > Profile > Network, click the VPN Only icon for the interface you are changing.

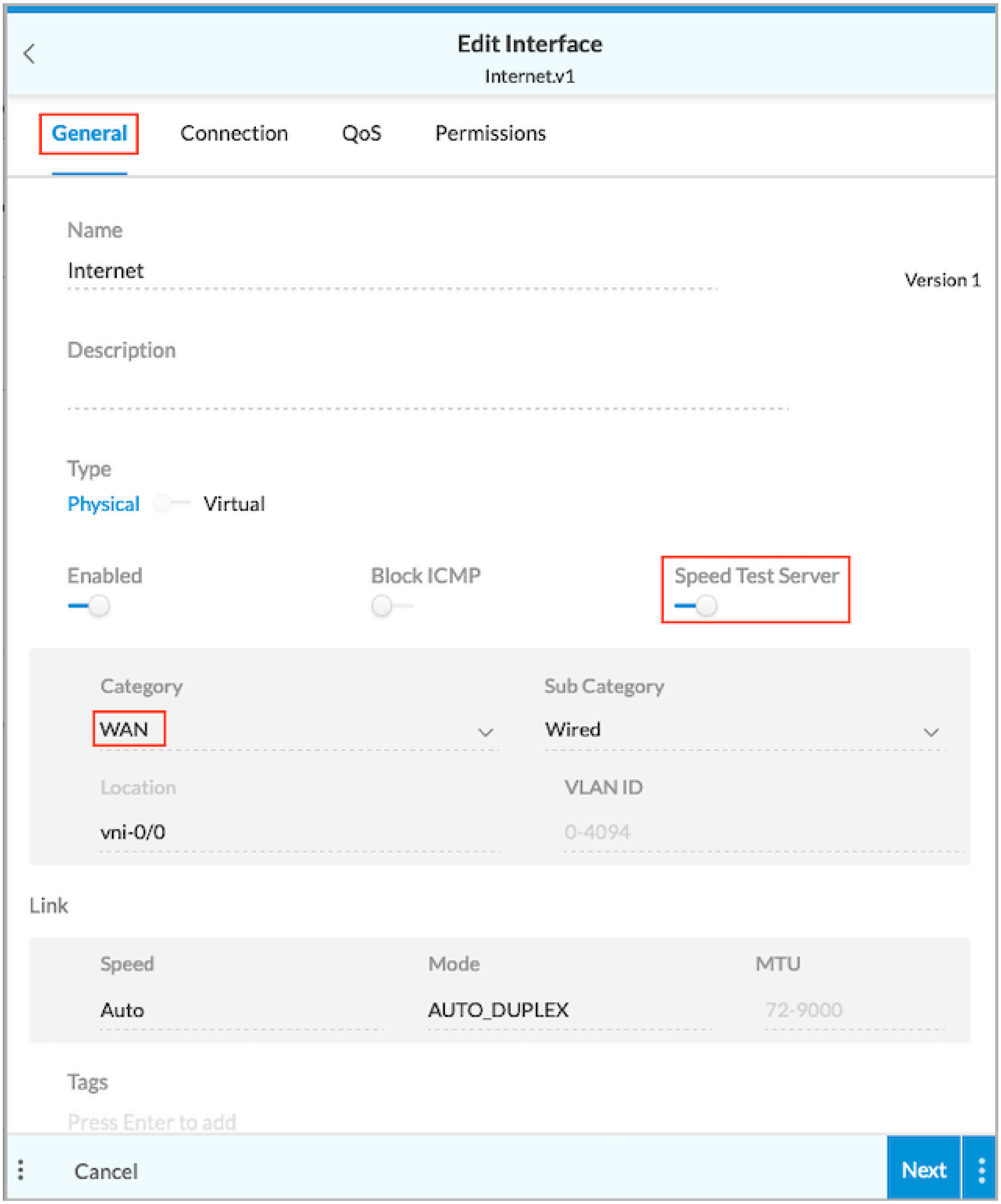
4. To enable DIA, click the Internet and VPN (Split Tunnel) icon. To disable DIA, click the VPN Only icon.
5. Select the Permissions tab, and then click Save.

Enable a Speed-Test Server on a WAN Interface

To troubleshoot link speed issues, you can configure a WAN interface to be a speed-test server.

To configure a WAN interface to be a speed-test server:

1. In Edit Master Profile > Profile > Network, click the interface on which to enable the speed-test server. The Edit Interface screen displays.



Edit Interface
Internet.v1

Name
Internet

Version 1

Description

Type
Physical ○— Virtual

Enabled
Block ICMP
Speed Test Server

Category
WAN

Sub Category
Wired

Location
vni-0/0

VLAN ID
0-4094

Link

Speed
Auto

Mode
AUTO_DUPLEX

MTU
72-9000

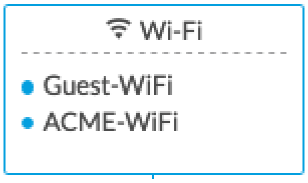
Tags
Press Enter to add

2. Select the General tab.

3. In the Speed-Test Server field, click the slider to enable a server.
4. Ensure that the interface category is WAN.
5. Select the Permissions tab, and then click Save.

Update the WiFi Interface Authentication Protocol

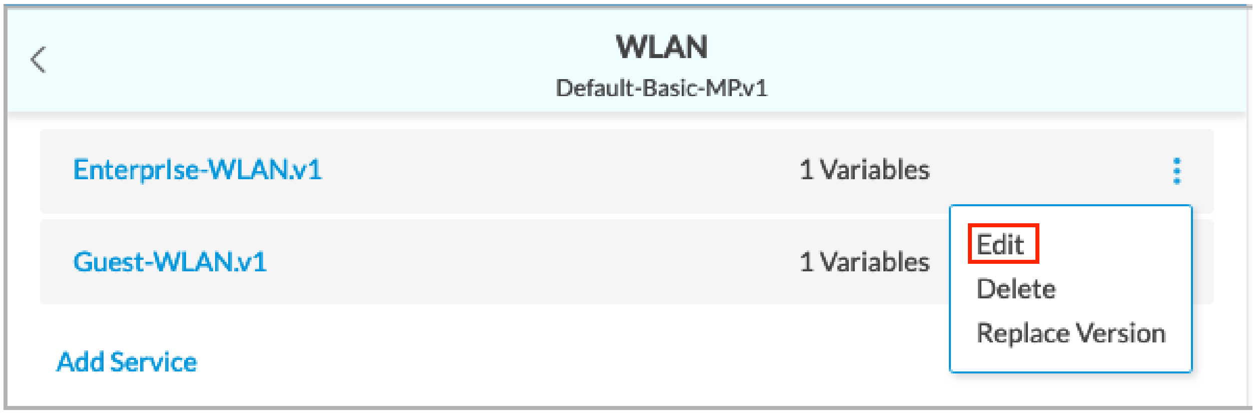
1. In Edit Master Profile > Profile > Network, click the WiFi box.



Wi-Fi

- Guest-WiFi
- ACME-WiFi

The WLAN screen displays.

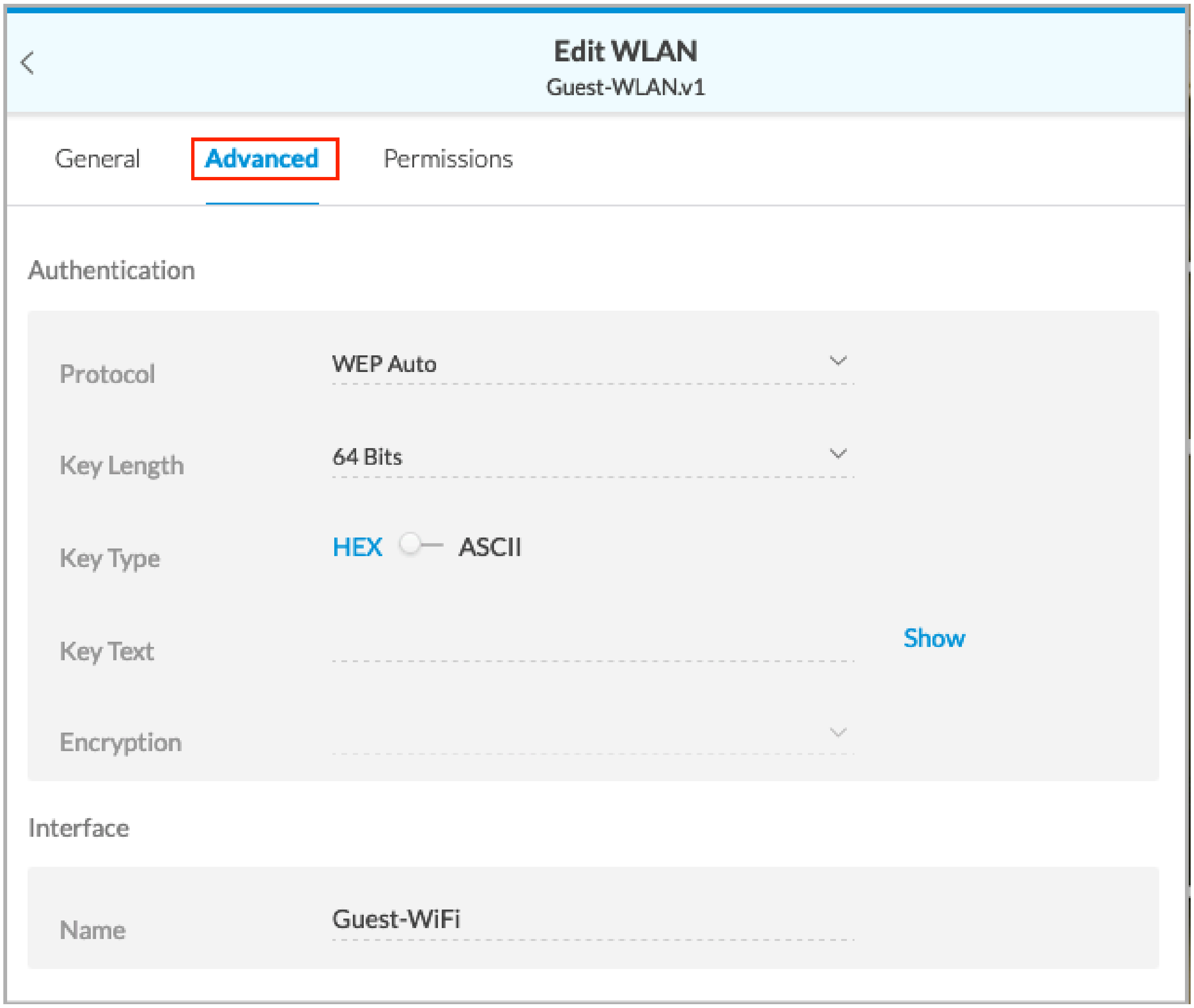


WLAN

Default-Basic-MP.v1

Enterprlse-WLAN.v1	1 Variables
Guest-WLAN.v1	1 Variables

2. Click the ⋮ Ellipses icon of the WLAN network that you want to update, and then click Edit. The Edit WLAN screen displays.
3. Select the Advanced tab. The following screen displays.



Edit WLAN

Guest-WLAN.v1

Authentication

Protocol: WEP Auto

Key Length: 64 Bits

Key Type: HEX ○— ASCII

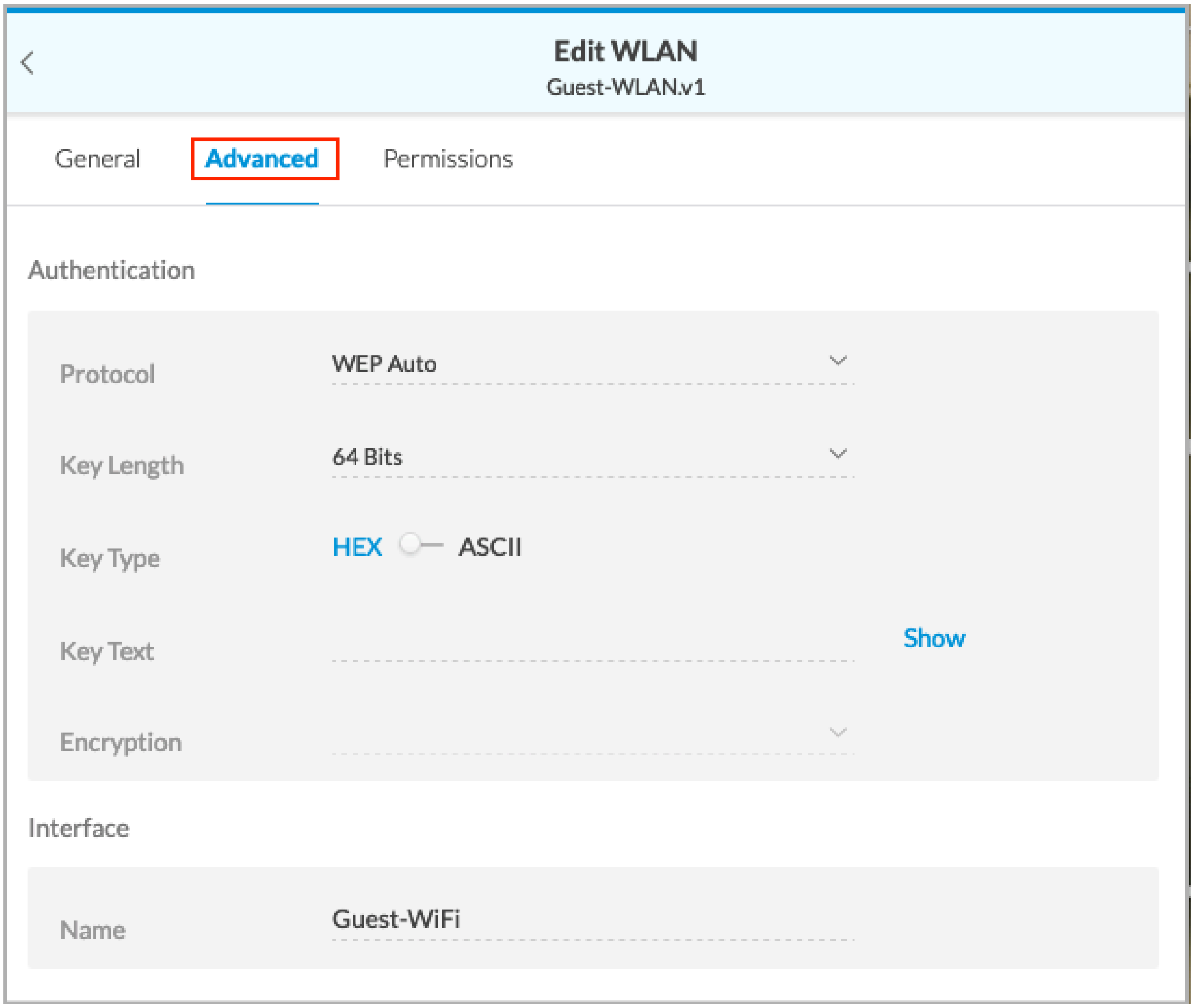
Key Text:

Encryption:

Interface

Name: Guest-WiFi

4. For Wired Equivalent Privacy (WEP)-based authentication, enter information for the following fields.



Edit WLAN

Guest-WLAN.v1

Authentication

Protocol: WEP Auto

Key Length: 64 Bits

Key Type: HEX ASCII

Key Text:

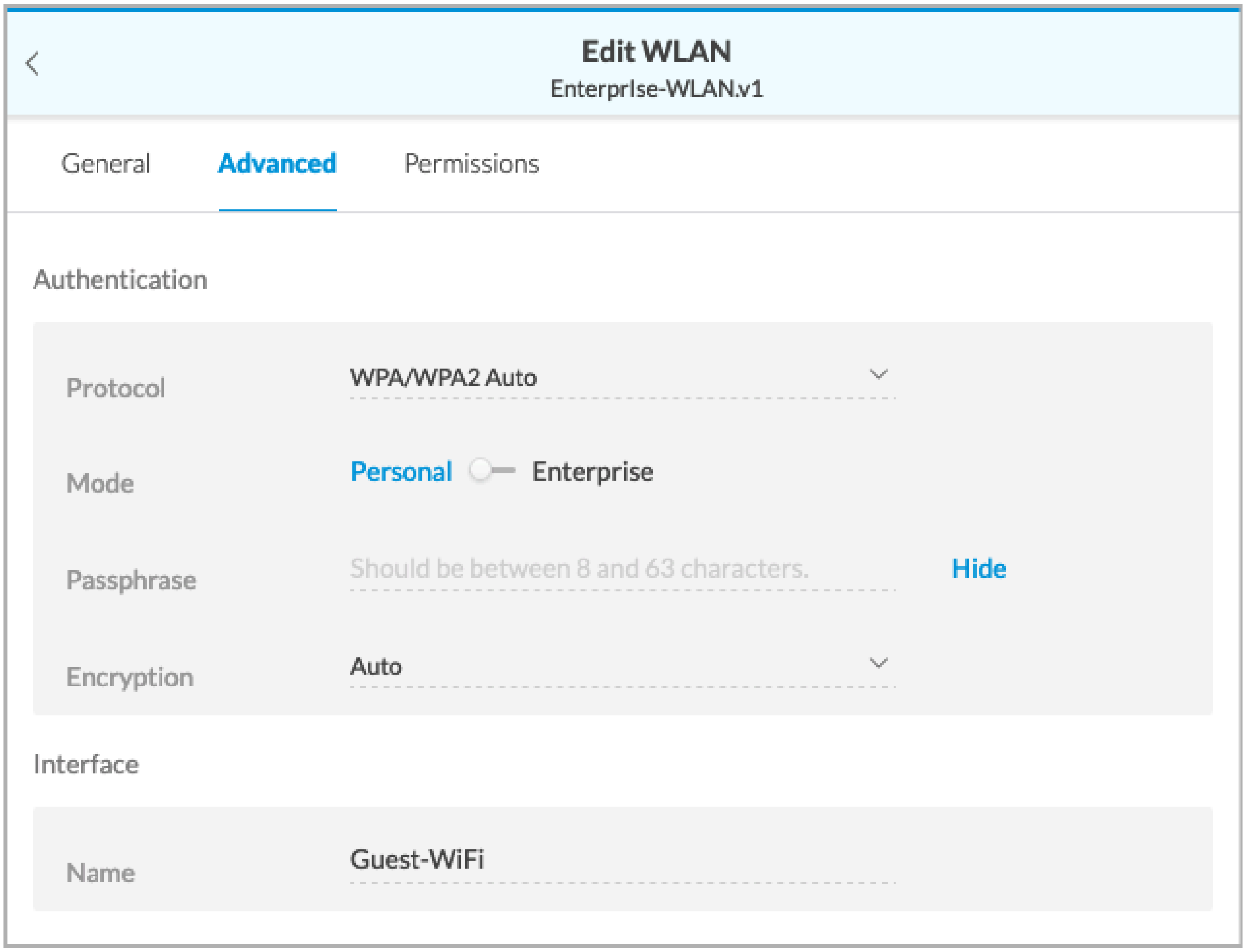
Encryption:

Interface

Name: Guest-WiFi

Field	Description
Authentication (Group of Fields)	
◦ Protocol	Select the protocol: ◦ WEP Auto ◦ WEP Open ◦ WEP Shared Key
◦ Key Length	Select the key length: ◦ 64 bits ◦ 128 bits
◦ Key Type	Use the slider bar to select the key type: ◦ ASCII ◦ HEX
◦ Key Text	For the ASCII as the key type, enter 5 characters for the key text. For the HEX key type, enter 10 characters for the key text.
Interface Name	Click in the Name field, and then select an interface name.

5. For WiFi Protected Access (WPA)-based authentication, enter information for the following fields.



Edit WLAN

Enterprlse-WLAN.v1

Authentication

Protocol: WPA/WPA2 Auto

Mode: Personal / Enterprise

Passphrase: Should be between 8 and 63 characters. Hide

Encryption: Auto

Interface

Name: Guest-WiFi

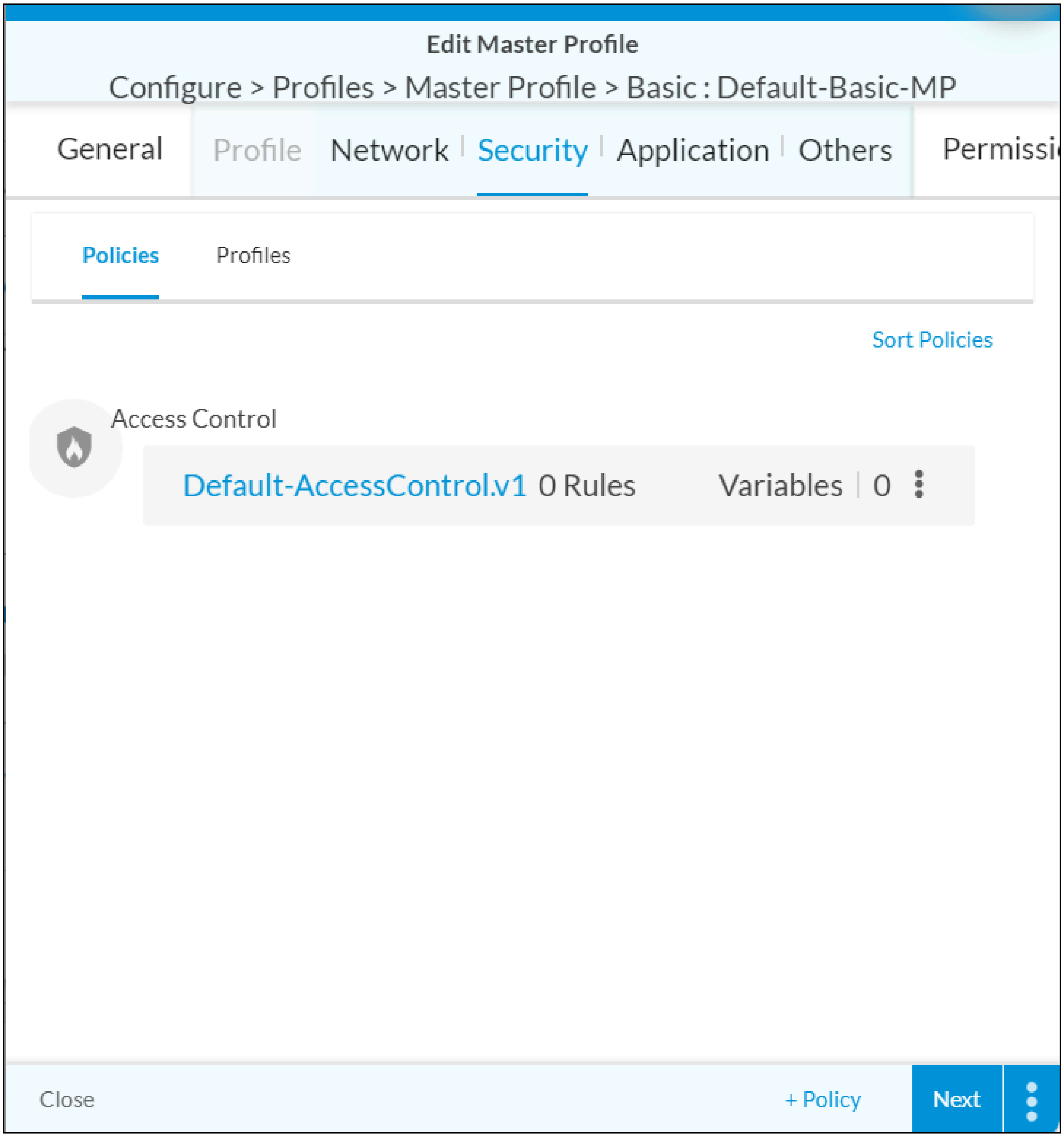
Field	Description
Authentication (Group of Fields)	
◦ Protocol	Select the protocol: ◦ WPA ◦ WPA/WPA2 Auto ◦ WPA2
◦ Mode	User the slider bar to select the mode: ◦ Enterprise ◦ Personal
◦ Passphrase	Enter a passphrase (password), which can be from 8 to 63 characters.

Field	Description
◦ Encryption	Select the encryption type: ◦ Auto ◦ CCMP ◦ Temporal Key Integrity Protocol (TKIT)
Interface Name	Click in the Name field and select an interface name.

6. Click Next, or select the Permissions tab, and then Click Save.

Update Security Policies and Rules

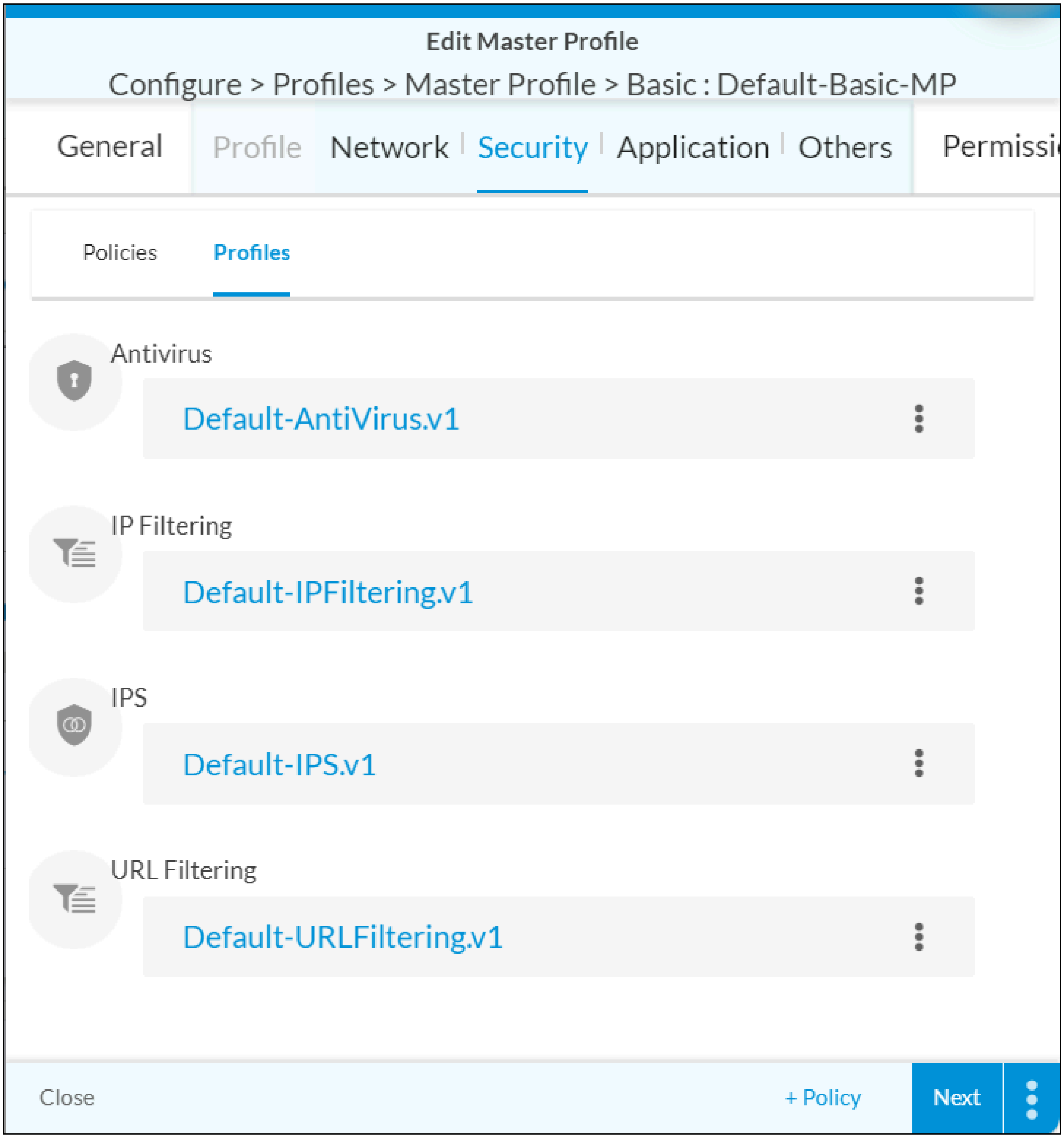
1. In the Edit Master Profile screen, select Profile > Security. The Policies tab displays the security policies, if any, that are associated with them.



Edit Master Profile

Configure > Profiles > Master Profile > Basic : Default-Basic-MP

2. (For Releases 12.1.1 and later.) Select the Profiles tab, and then click a profile name to display information about a profile.



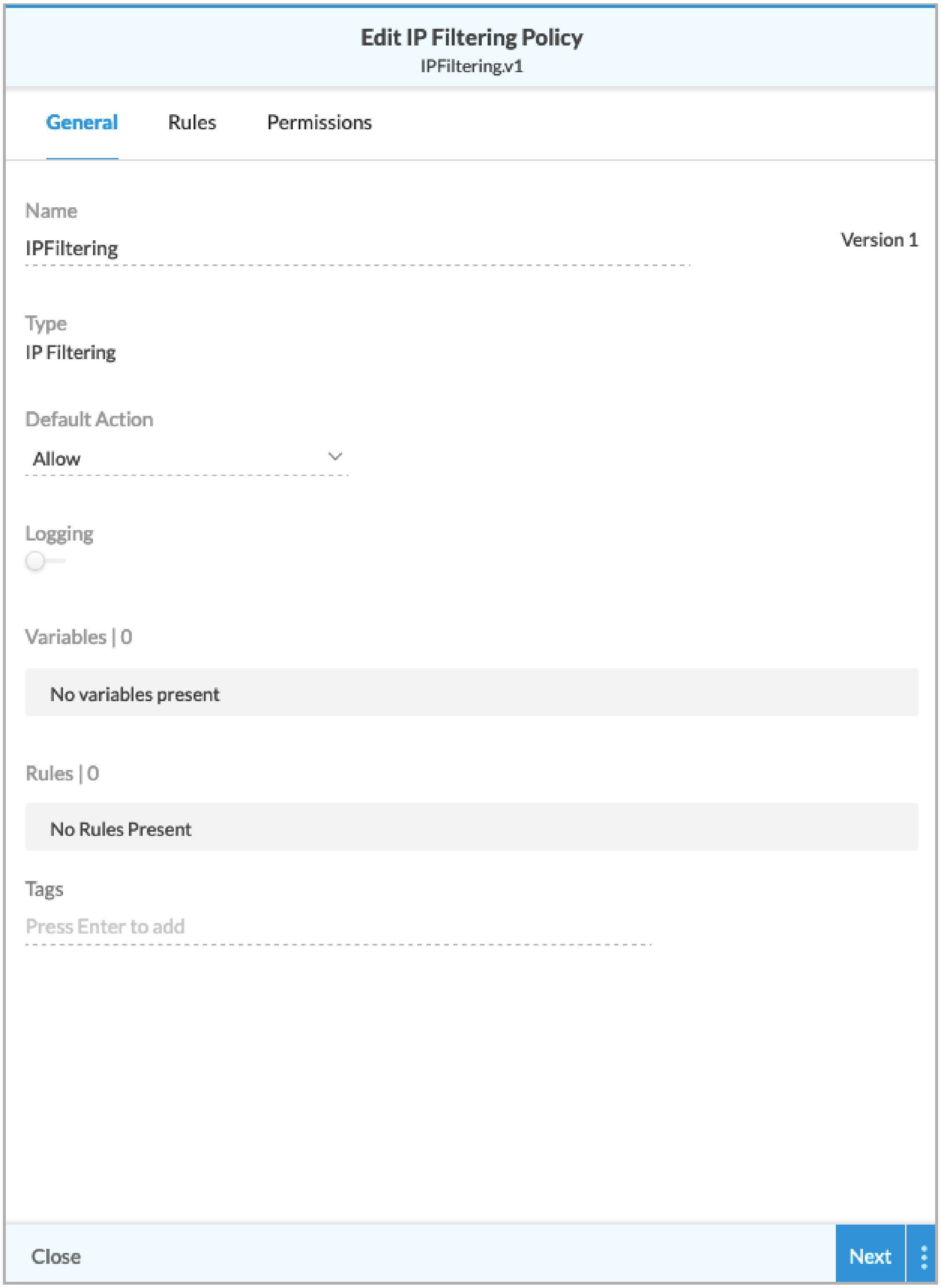
Antivirus: Default-AntiVirus.v1

IP Filtering: Default-IPFiltering.v1

IPS: Default-IPS.v1

URL Filtering: Default-URLFiltering.v1

3. To display information about a policy, click the policy name on the Policies tab. The Edit Policy screen displays. The following screenshot shows the Edit IP Filtering Policy screen.



Name
IPFiltering

Version 1

Type
IP Filtering

Default Action
Allow

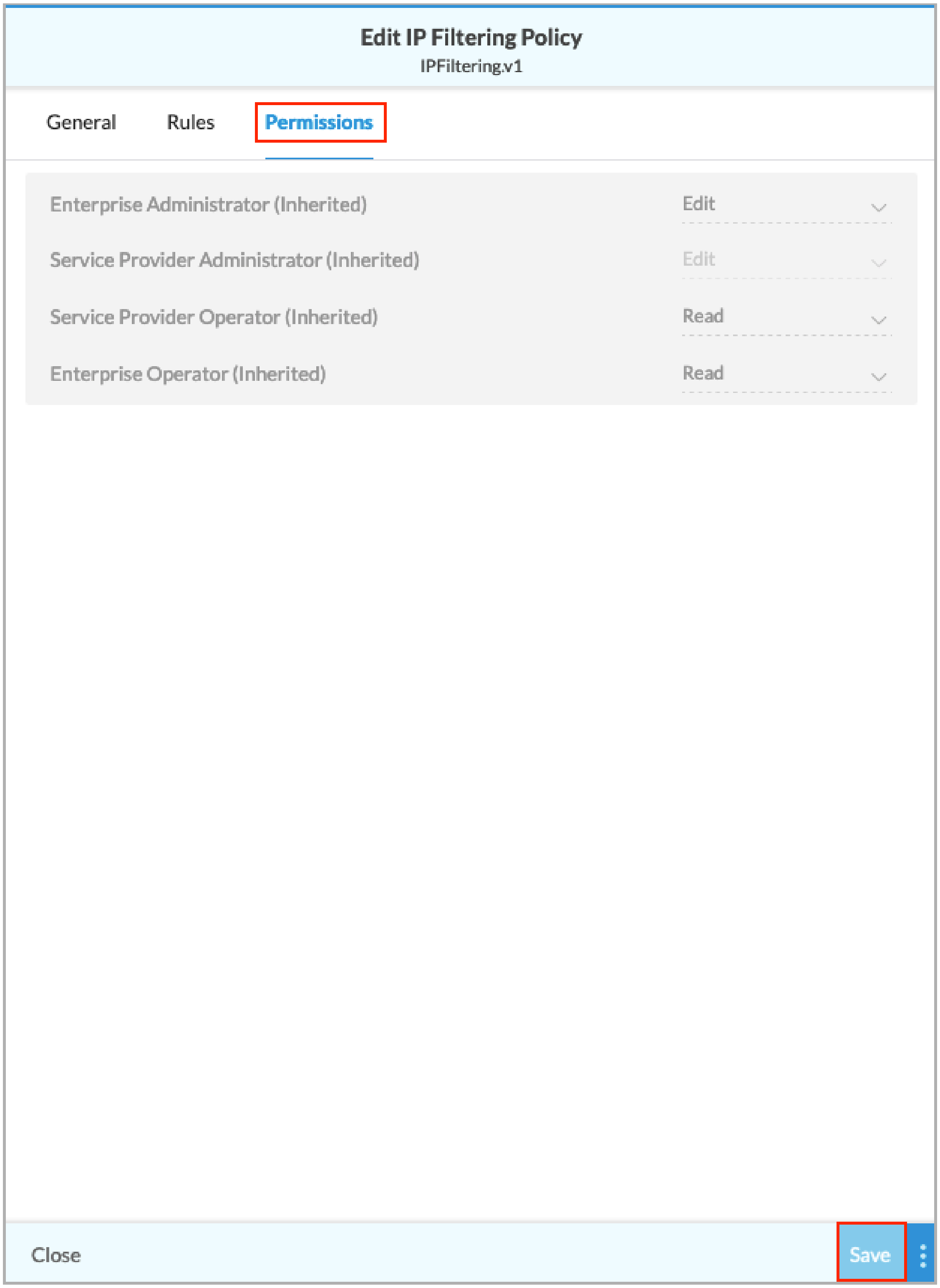
Logging

Variables | 0
No variables present

Rules | 0
No Rules Present

Tags
Press Enter to add

4. To create a new rule or choose an existing rule for the policy, select the Rules tab. For more information, see Create a New Rule, below.
5. To display the inherited permissions for the default roles and change them, if desired, select the Permissions tab.


Edit IP Filtering Policy
IPFiltering.v1

Enterprise Administrator (Inherited)	Edit
Service Provider Administrator (Inherited)	Edit
Service Provider Operator (Inherited)	Read
Enterprise Operator (Inherited)	Read

6. Click Save.

Configure QoS Policies and Rules

For information about configuring QoS policies and rules, see Configure QoS Policies and Rules.

Configure Traffic-Steering Policies and Rules

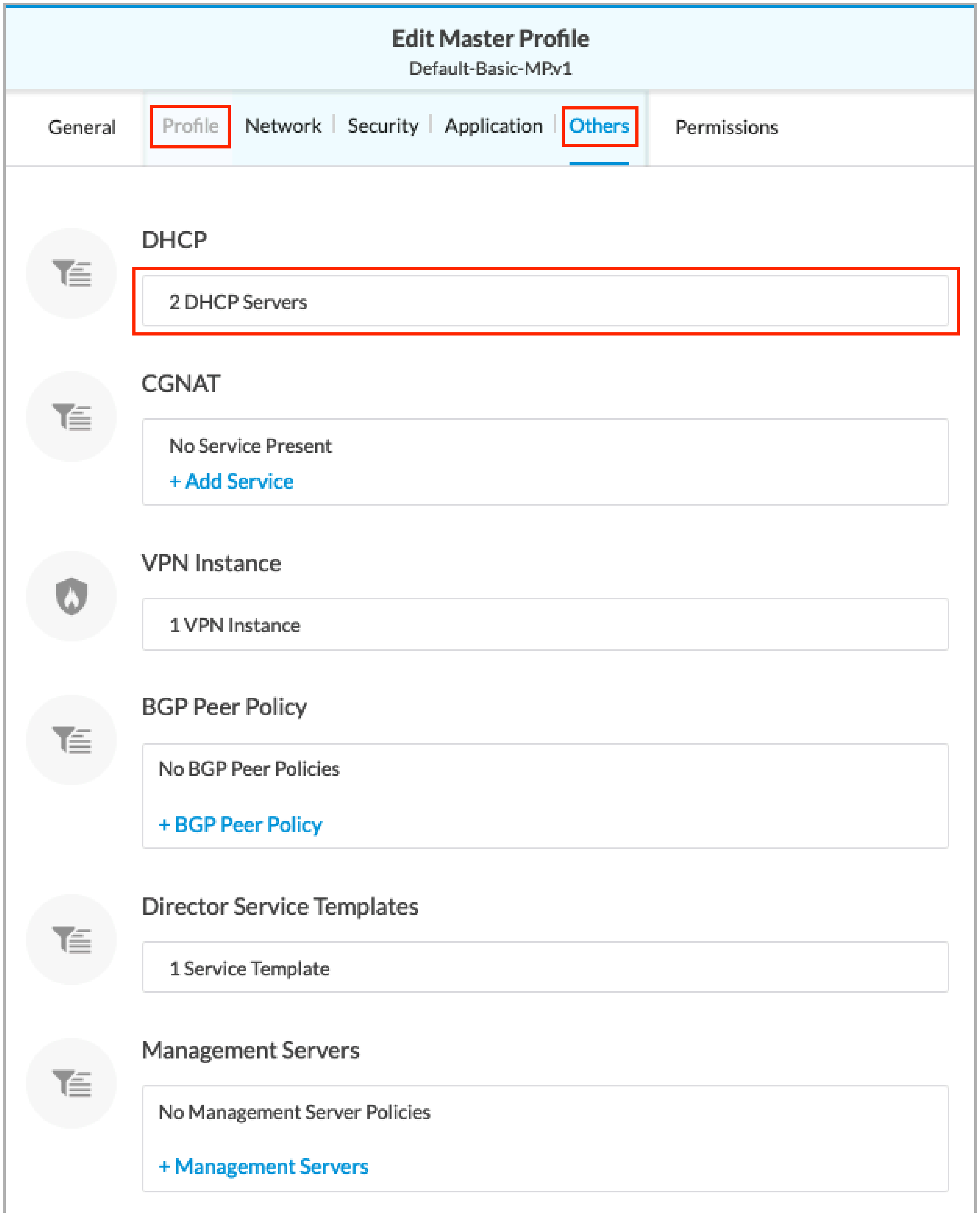
For information about configuring traffic-steering policies and rules, see Configure Traffic-Steering Policies and Rules.

Update or Add Services

You can update or add services, including those for BGP peer policy, CGNAT, DHCP, Director service templates, management server policies, user management policies, and VPN instances.

To update or add services:

1. In the Edit Master Profile screen, select Profile > Others. The following screen displays.



Edit Master Profile

Default-Basic-MP.v1

DHCP

2 DHCP Servers

CGNAT

No Service Present

VPN Instance

1 VPN Instance

BGP Peer Policy

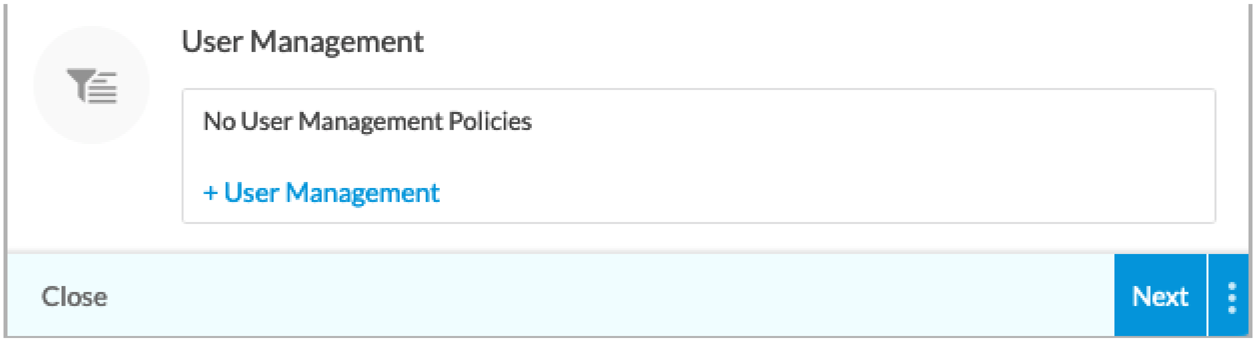
No BGP Peer Policies

Director Service Templates

1 Service Template

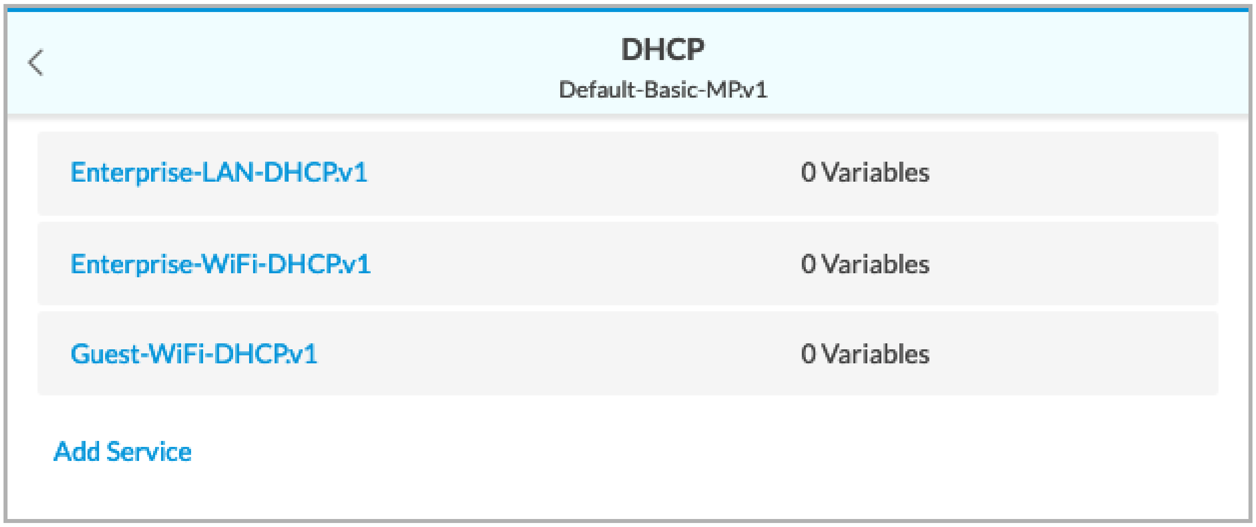
Management Servers

No Management Server Policies



No User Management Policies

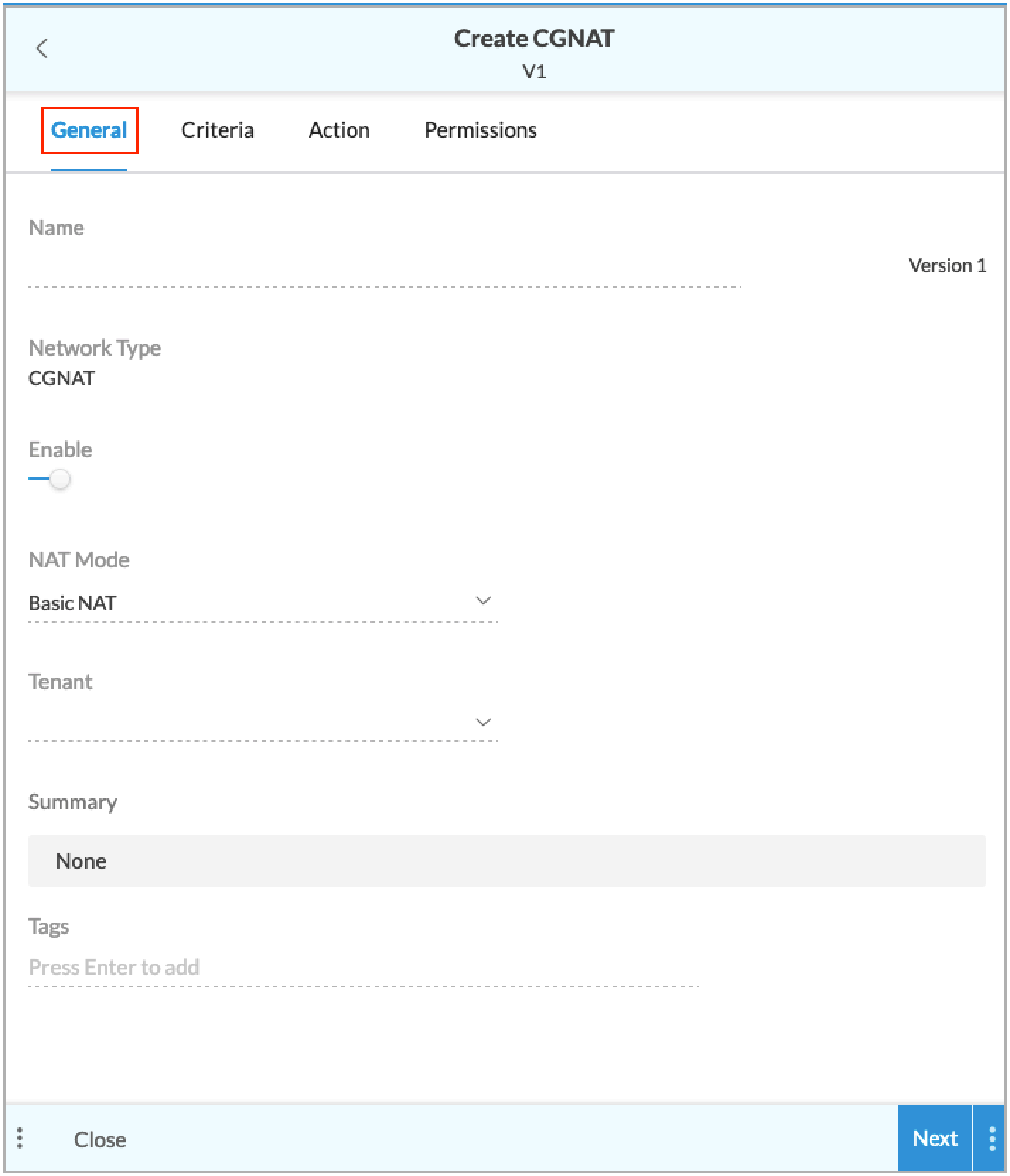
2. To update an existing DHCP service or add a new DHCP service, click the DHCP box. The DHCP screen displays.



Enterprise-LAN-DHCP.v1	0 Variables
Enterprise-WiFi-DHCP.v1	0 Variables
Guest-WiFi-DHCP.v1	0 Variables

   a. To display or update information about the service, click an existing DHCP service, such as Enterprise-LAN-DHCP.v1 in the screenshot above.
   b. To add a new DHCP service, click Add Service. You can create a new service or choose an existing service.

3. To update an existing CGNAT service or add a CGNAT service, click CGNAT. In the CGNAT screen, click Add Service to add a new service. You can create a new service or choose an existing service. The Create CGNAT screen displays. Enter information for the following fields.



Name

Version 1

Network Type
CGNAT

Enable

NAT Mode
Basic NAT

Tenant

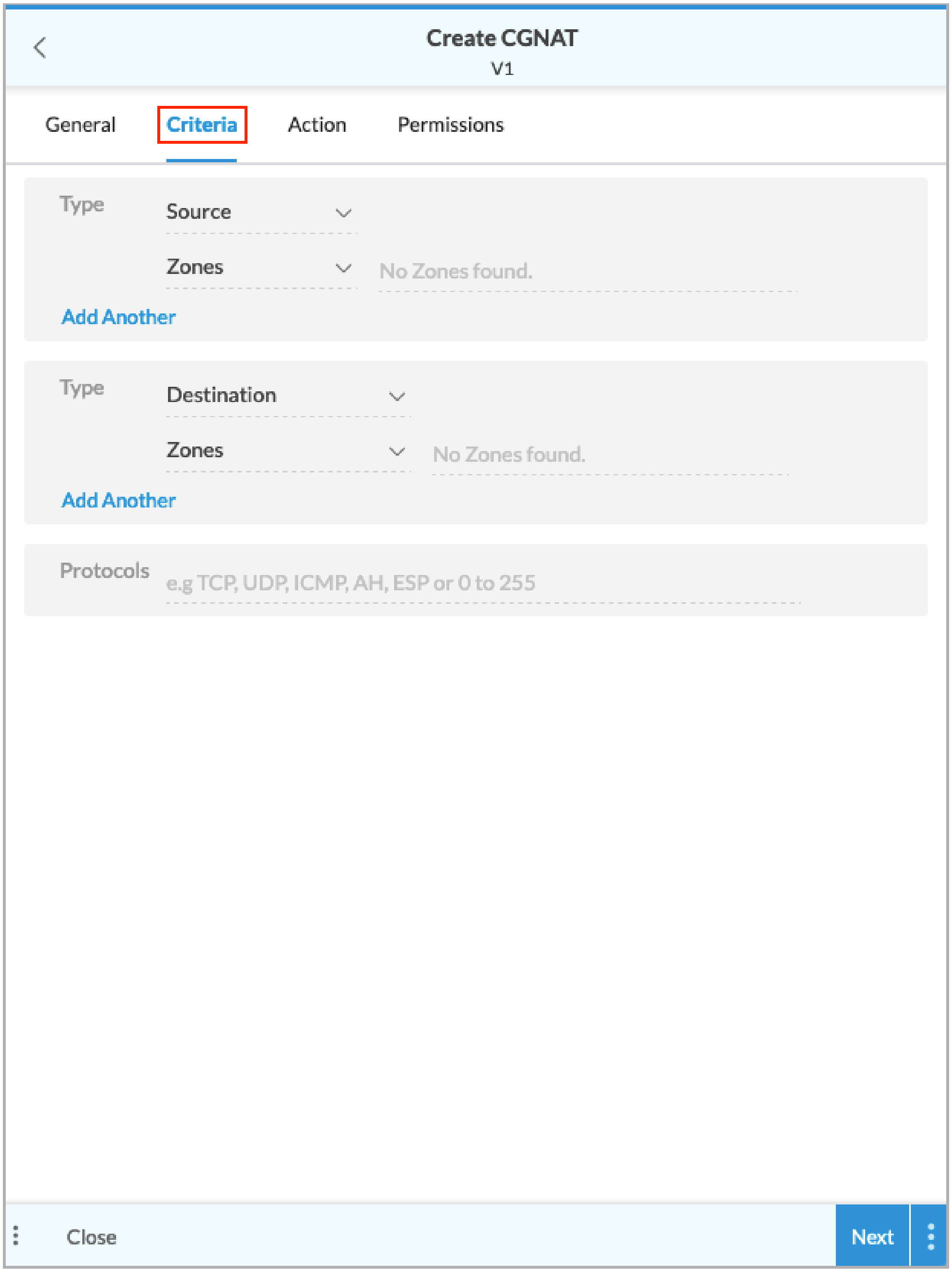
Summary
None

Tags
Press Enter to add

Field	Description
Name	Enter a name for the CGNAT service.

Field	Description
Enable	The slider bar is in the Enabled position by default. To disable the CGNAT service, click the slider bar so that it is grayed out.
NAT Mode	Select the NAT mode: ◦ Basic NAT. This is the default. ◦ Destination NAT ◦ Dynamic NAT ◦ NAPT ◦ Twice Basic NAT ◦ No Translation *Default:* Basic NAT
Tenant	(For Releases 11.4.1 and later.) Select a tenant. The list displays the current tenant and all child tenants. If a tenant is not selected, the system displays the name of the current tenant only, not any child tenants.

a. Select the Criteria tab, and then enter information for the following fields.



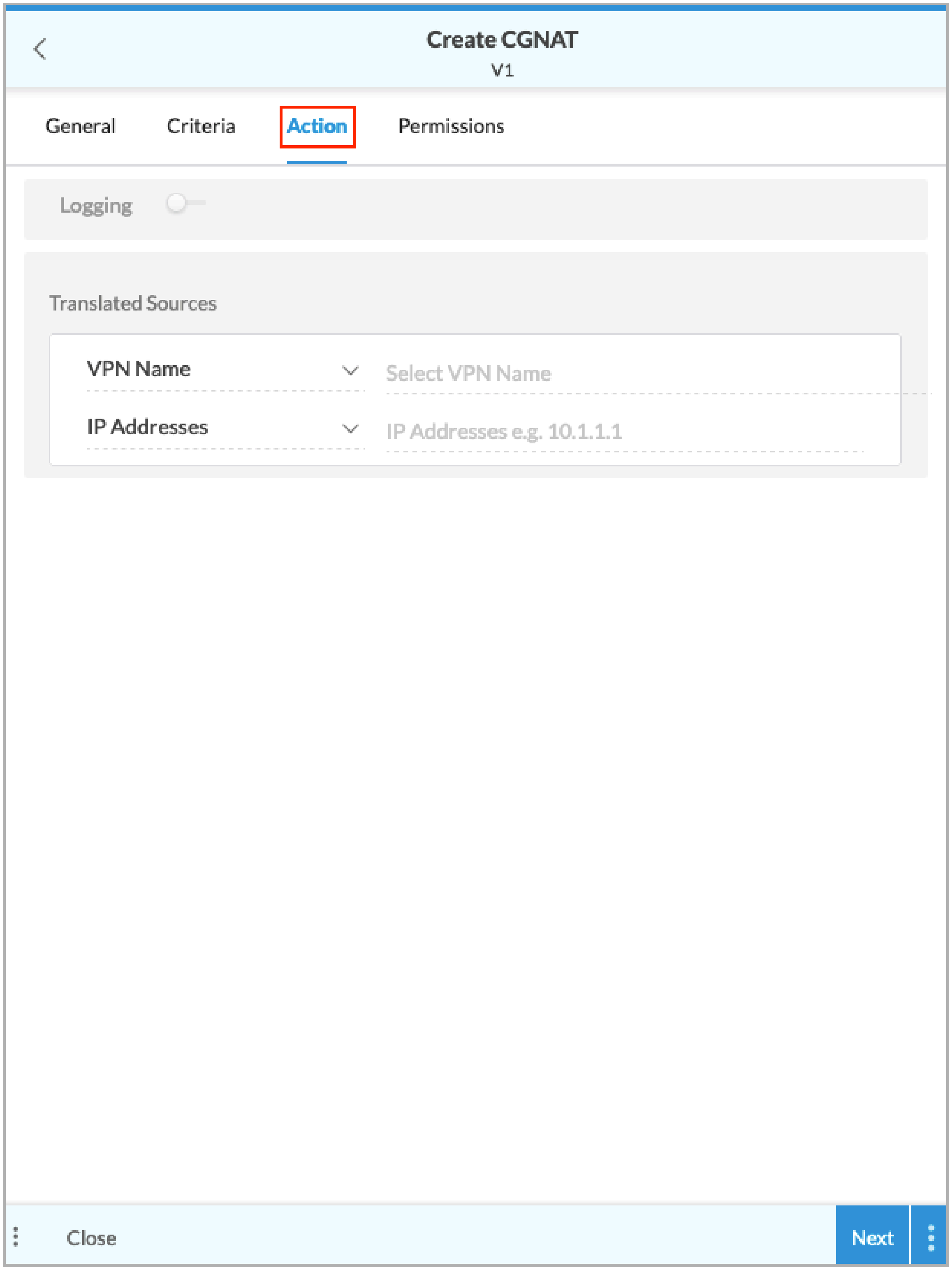
Type Source
Zones No Zones found.

Type Destination
Zones No Zones found.

Protocols e.g TCP, UDP, ICMP, AH, ESP or 0 to 255

Field	Description
Type (Source)	The Source type is selected by default, and you cannot change it. Select the type of source to use: ▪ IP Ranges—Enter an IP address range, such as 10.10.1.1-10.10.1.100, and then click the ✓ Check mark icon or press Enter. You can enter multiple address ranges. ▪ Subnets—Enter an IP address subnet, such as 10.1.1.0/24. ▪ VPN Name—Select a VPN name. ▪ Zones—Select a zone.
Type (Destination)	The Destination type is selected by default, and you cannot change it. Select the type of destination to use: Note: The IP Ranges and Subnets options are mutually exclusive; you can select one or the other, but you cannot select both of them. ▪ IP Ranges—Enter an IP address range, such as 10.10.1.1- 10.10.1.100, then click the Check mark icon or press Enter. You can enter multiple address ranges. ▪ Port—Enter a destination port number. *Range*: 1 through 65535 *Default*: None ▪ Port Range—Enter a destination port range, such as 80-88. ▪ Subnets—Enter an IP address subnet, such as 10.1.1.0/24. ▪ Zones—Select a zone.
Protocols	Select one or more protocols: ▪ ESP ▪ ICMP ▪ UDP ▪ 0 through 255

b. Select the Action tab, and then enter information for the following fields.



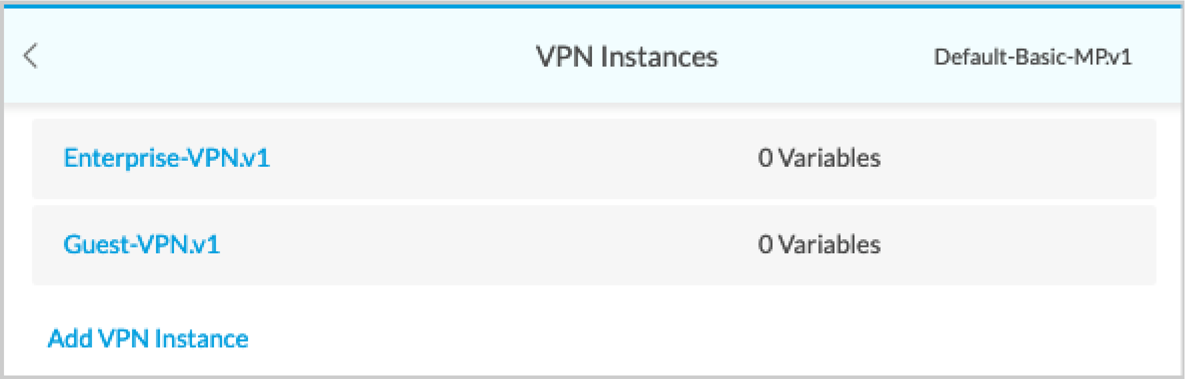
Create CGNAT
V1
General
Criteria
Action
Permissions
Logging
Translated Sources
VPN Name
Select VPN Name
IP Addresses
IP Addresses e.g. 10.1.1.1
Close
Next

Field	Description
Logging	Click the slider bar to enable logging to Versa Analytics.
Translated Sources	Select the translated sources based on VPN names or WAN connections: ▪ VPN Name—Select a VPN name. ▪ WAN Connection—Select a WAN connection. Select the translated sources from IP addresses, subnets, or IP address ranges: ▪ IP Addresses—Enter an IP address, and then click the ✓ Check mark icon or press Enter. You can enter multiple IP addresses. ▪ IP Ranges—Enter an IP address range, and then click the ✓ Check mark icon or press Enter. You can enter multiple IP address ranges. ▪ Subnets—Enter an IP subnet, and then the ✓ Check mark icon or press Enter. You can enter multiple IP subnets.

c. Select the Permissions tab, and revise the permissions, if needed.

d. Click Save to create the CGNAT service.

4. To display existing VPN instances or add new VPN instances, click VPN. The VPN Instances screen displays.

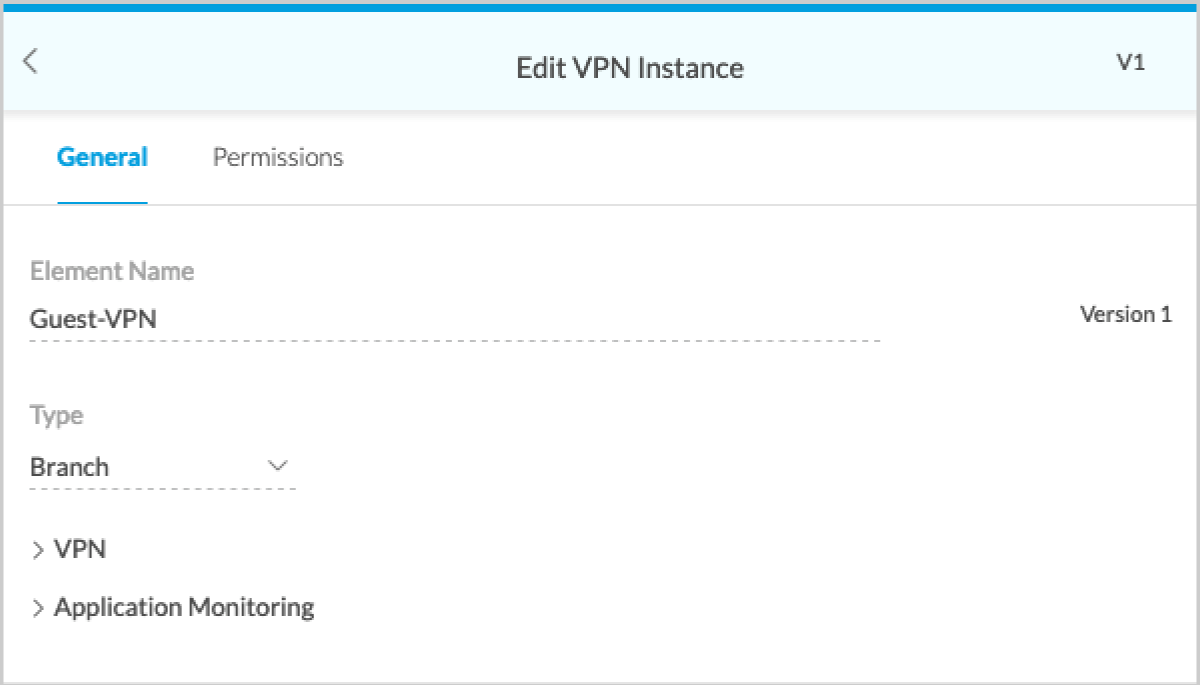


VPN Instances Default-Basic-MP.v1

Enterprise-VPN.v1	0 Variables
Guest-VPN.v1	0 Variables

Add VPN Instance

a. To display or update information about the instance, click an existing VPN instance.



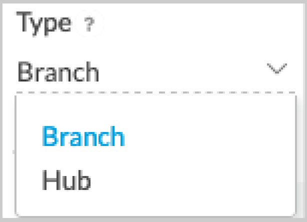
Edit VPN Instance

Element Name: Guest-VPN

Version 1

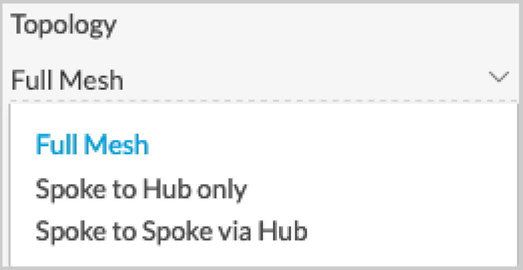
Type: Branch

b. In the Type field, select Branch or Hub.



Type: Branch

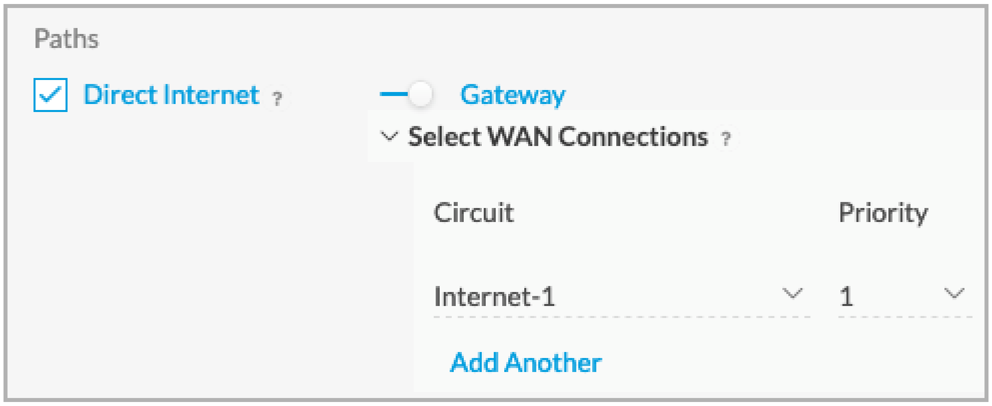
c. To set or update the topology, click VPN and then select a topology. If you selected Hub in the Type field, the topology options are hidden.



Topology: Full Mesh

d. Under Paths, select Direct Internet, Underlay, or both:

Direct Internet—Enable or disable DIA for the VPN. If you enable Gateway, the appliance acts as an internet gateway for the enterprise and re-advertises default routes on the SD-WAN overlay to other appliances.



Paths

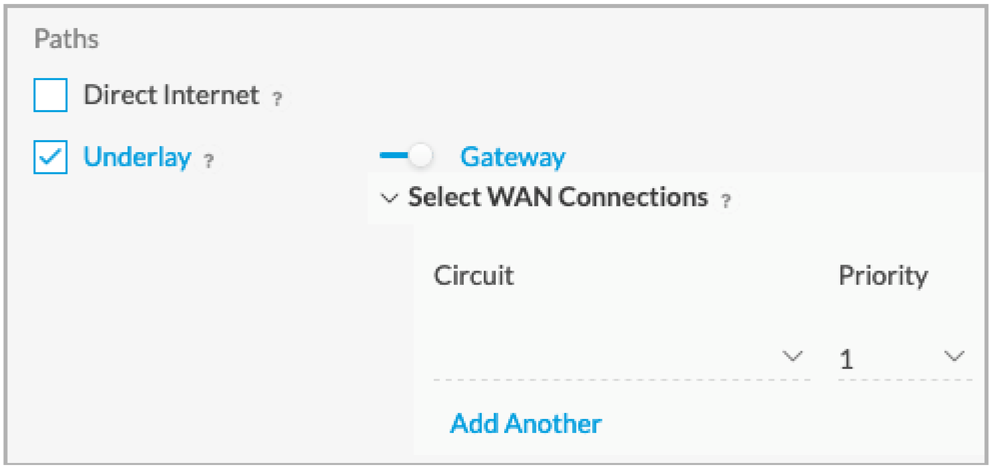
☑ Direct Internet ?

Gateway

Select WAN Connections ?

Circuit	Priority
Internet-1	1

Underlay—Enable or disable underlay routing to non-SD-WAN appliances over the MPLS network without performing NAT on the traffic. If you enable Gateway, the appliance acts as a gateway to non-SD-WAN networks and re-advertises routes from the MPLS underlay to the SD-WAN overlay.



Paths

□ Direct Internet ?

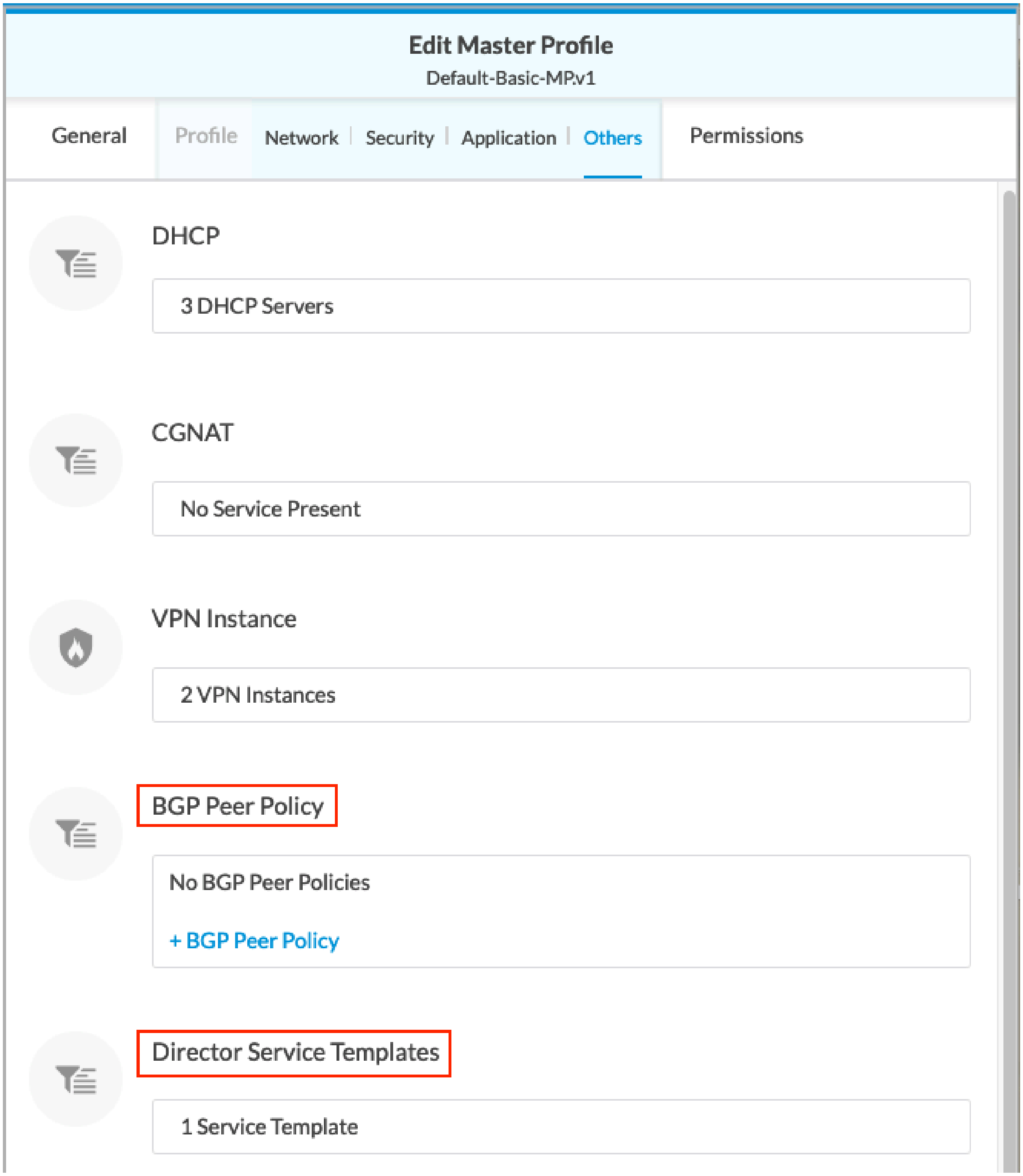
☑ Underlay ?

Gateway

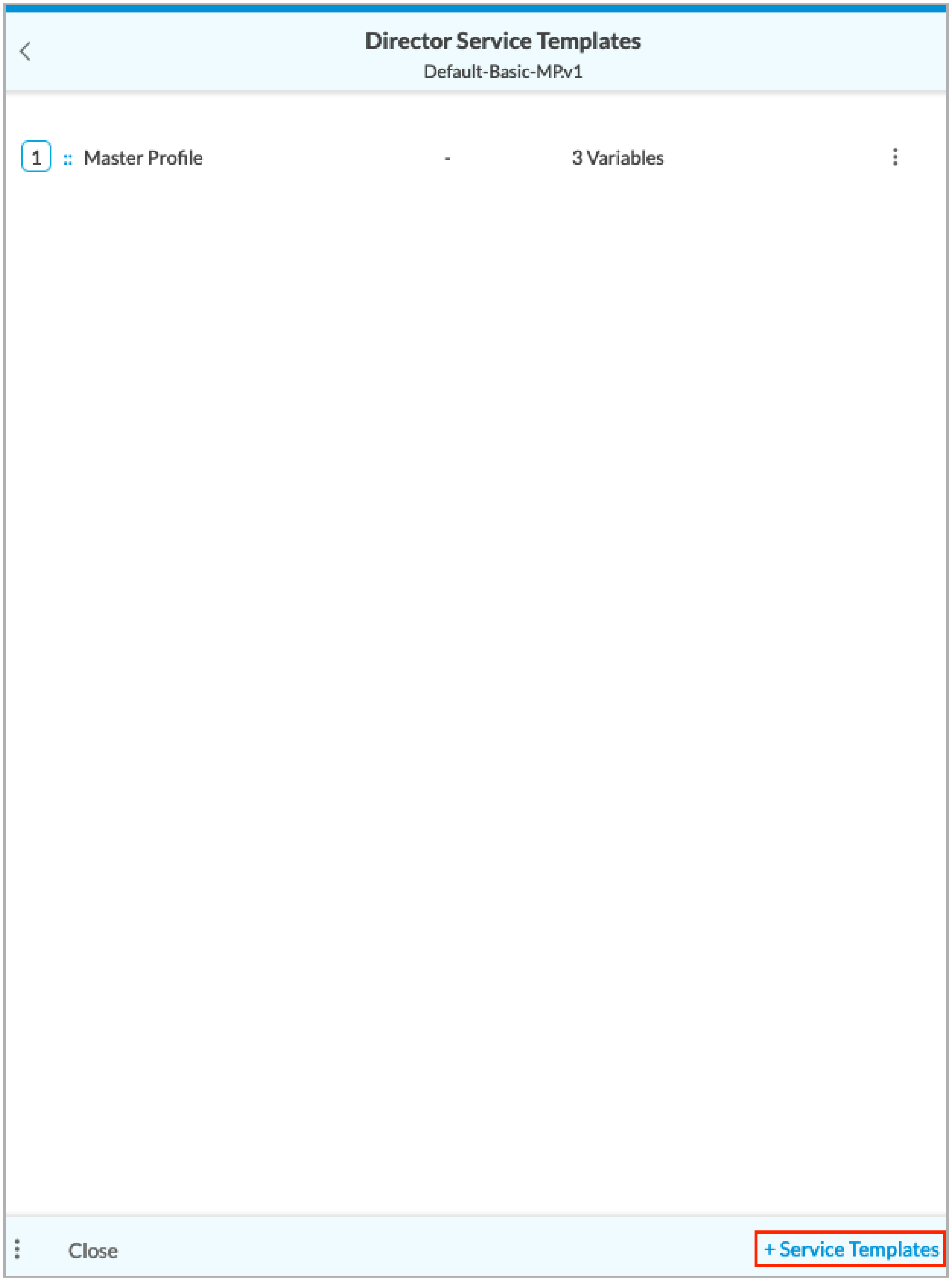
Select WAN Connections ?

Circuit	Priority
	1

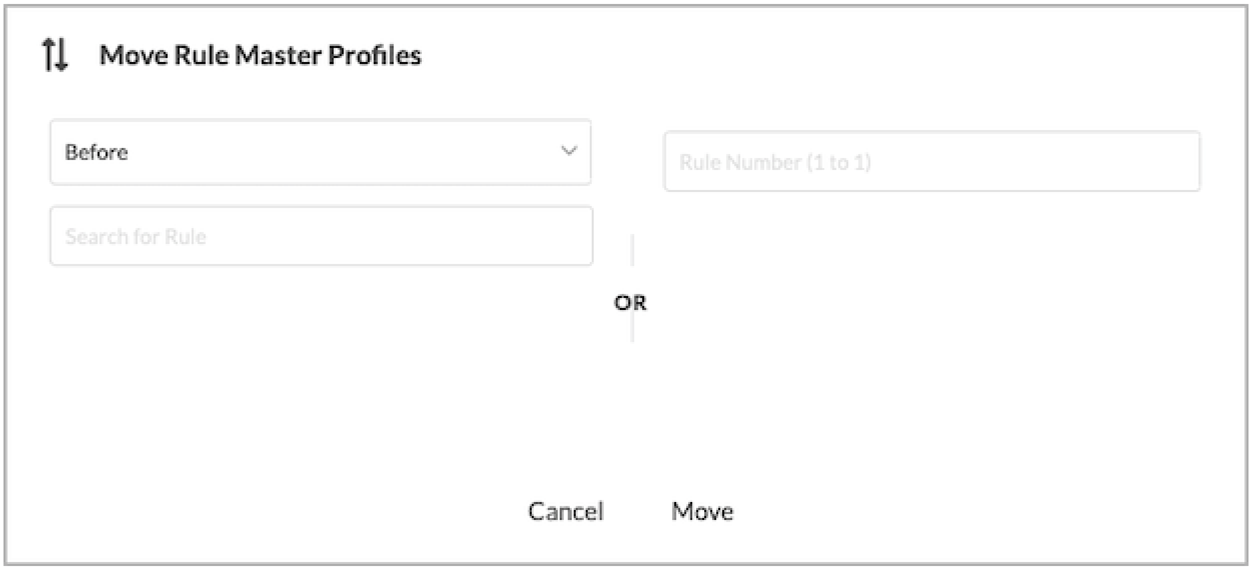
5. To update an existing BGP peer policy or add a new policy, click + BGP Peer Policy. If you refer to a BGP peer policy in the BGP neighbor configuration on a WAN or LAN interface, you should attach the peer policy to the BGP peer policies list. For more information, see Configure SASE BGP Peer Policies.



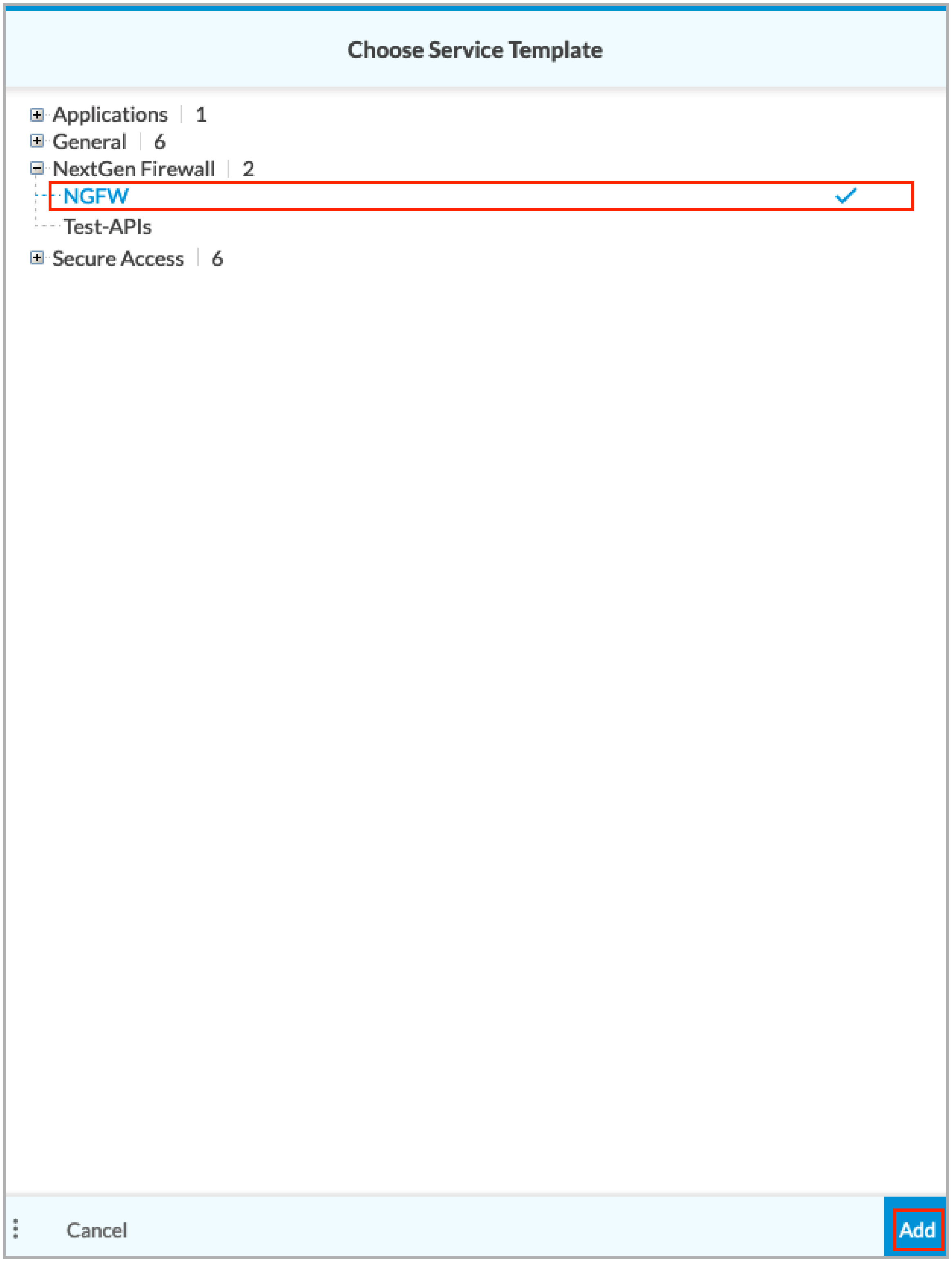
6. To add or move a Director service template, click Director Service Templates. The following screen displays.



a. To move a service template up or down in the list, click Move. The following screen displays.



b. To choose which direction to move the rule, click Before or After.
c. Enter the rule number.
d. Click Move.
e. To add a service template, click + Select Templates. The following screen displays the available templates.



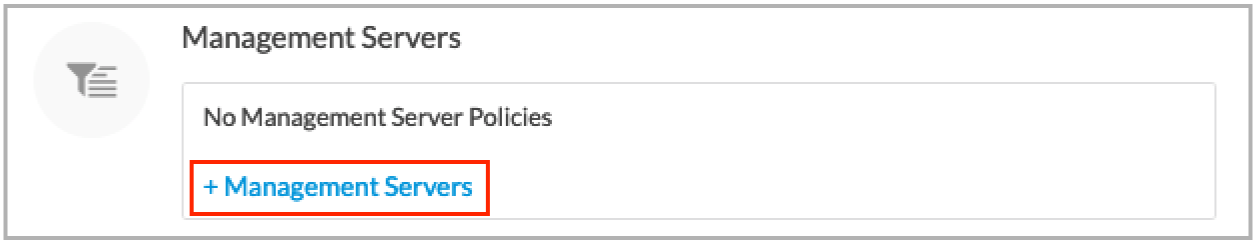
Choose Service Template

- ⊞ Applications | 1
- ⊞ General | 6
- ⊟ NextGen Firewall | 2
  - NGFW ✓
  - Test-APIs
- ⊞ Secure Access | 6

f. Select one or more service templates, and then click Add. The template is added to the Director Service Templates screen.

7. For Releases 11.1.1 and later, to update management server policies for NTP, SNMP, syslog, and TACACS+, or

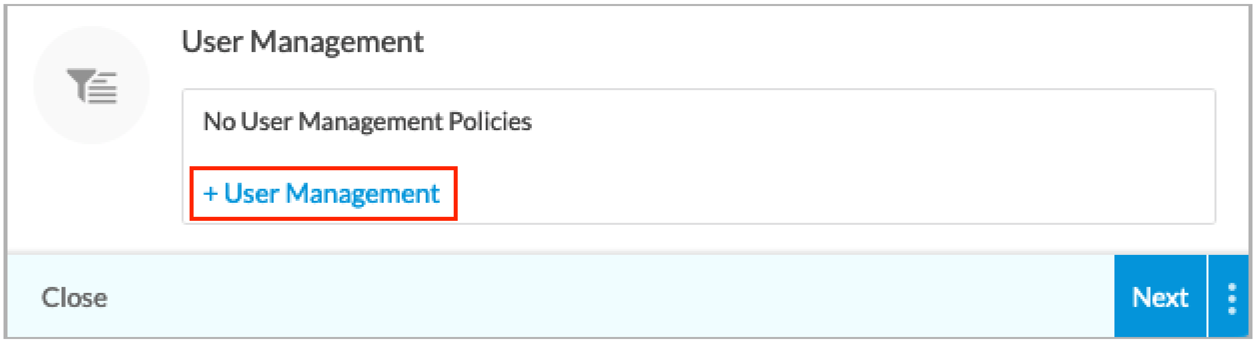
to add a new management server policy, click + Management Servers. For more information, see Configure Management Servers.



Management Servers

No Management Server Policies

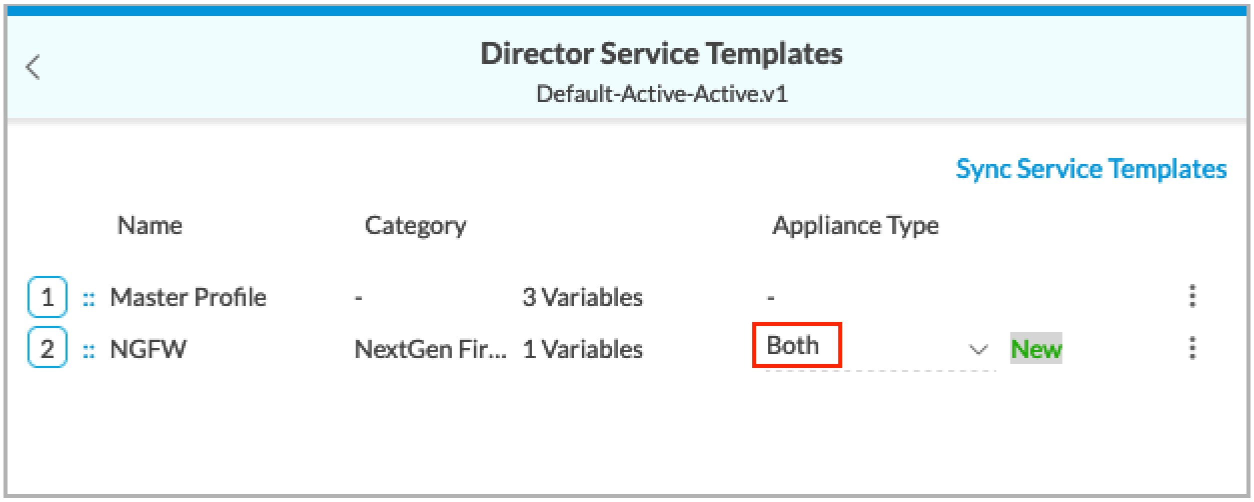
8. For Releases 11.3.1 and later, to create a user management policy or associate an existing user management policy with the master profile to add and manage VOS device users, click + User Management. For more information, see Manage VOS Users.



User Management

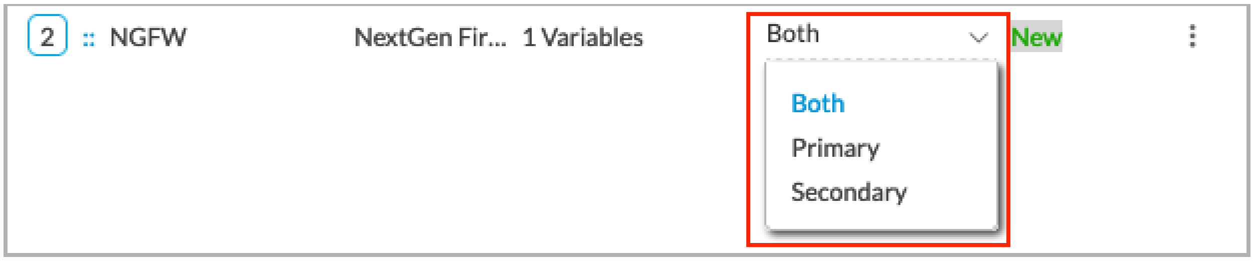
No User Management Policies

9. For Releases 11.3.1 and later, to apply different services templates to the devices in a master profile for redundant devices:
   a. Go to Configure > Profiles > Master Profiles, and select a master profile for redundant devices.
   b. In the Edit Master Profile screen, click Profile > Others.
   c. Under Director Service Templates, click the Service Template box. The Director Service Templates screen displays the tenant's current service templates.
   d. Click + Service Templates in the lower right corner of the screen. The Choose Service Template screen displays the available service templates.
   e. Select one or more service templates, and then click Add. The templates are added to the Director Service Templates screen. By default, the service templates are added to both the primary and secondary devices in the redundant configuration. Note that the Appliance Type column displays only when you are editing a master profile for redundant devices.



	Name	Category		Appliance Type		
1	Master Profile	-	3 Variables	-		
2	NGFW	NextGen Fir...	1 Variables	Both	New	

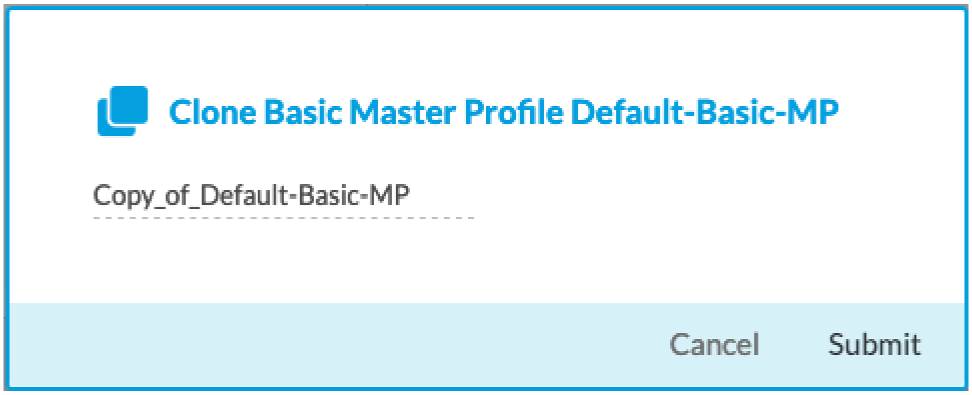
f. To apply the service template to only one of the redundant devices, click the drop-down list and then select either the Primary or Secondary device in the pair.



	Name	Category		Appliance Type	
2	NGFW	NextGen Fir...	1 Variables	Both	New

Clone the Default Basic Master Profile

You can create a new basic master profile by cloning one of the default basic master profiles, changing the configuration objects as needed, and saving the new basic master profile with a unique name. For example, you could create a new master profile to apply to hub appliances, and a second new master profile to apply to spoke appliances.



Clone Basic Master Profile Default-Basic-MP

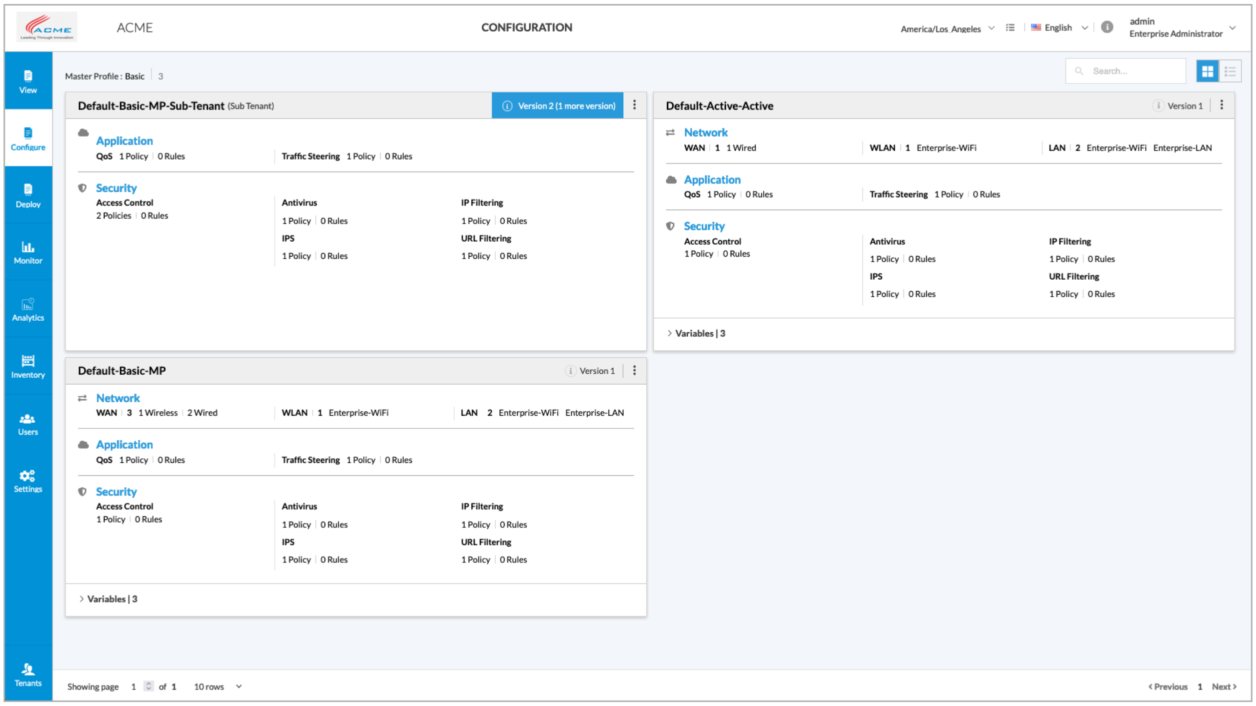
Copy_of_Default-Basic-MP

Enter a new name for the master profile, then click Submit. You can then edit the new basic master profile as needed. For information on the master profile screens, see Add a Standard Master Profile, below.

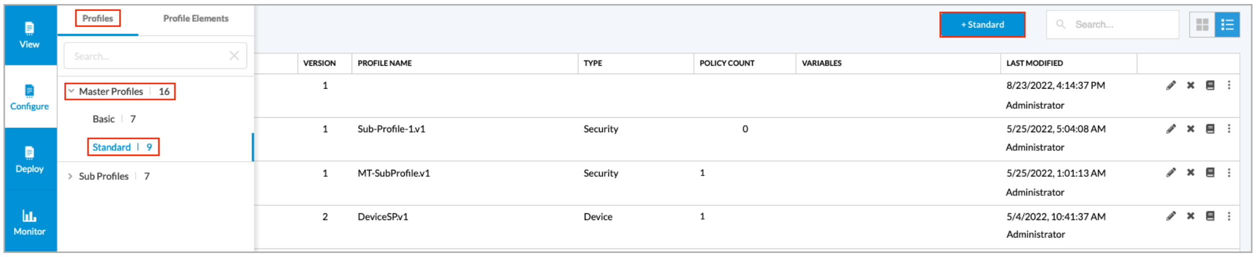
Add a Standard Master Profile

To add a standard master profile:

1. In Tenants view, select the name of a tenant. If the default lifecycle is not the Configure lifecycle, select Configure in the left menu bar. The Configure screen displays.

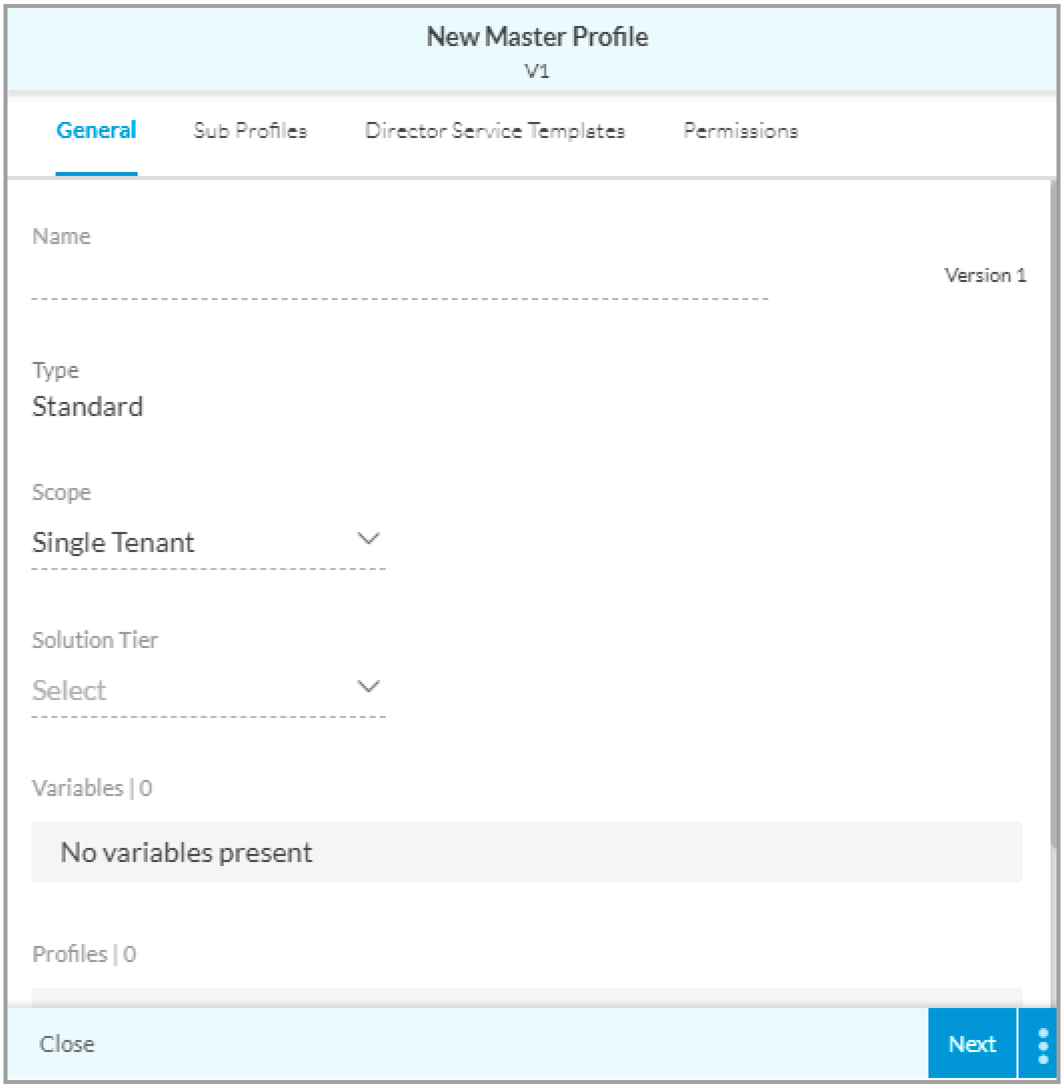

ACME
CONFIGURATION
America/Los_Angeles
English
admin
Enterprise Administrator
View
Configure
Deploy
Monitor
Analytics
Inventory
Users
Settings
Tenants
Master Profile : Basic | 3
Search...
Default-Basic-MP-Sub-Tenant (Sub Tenant)
Version 2 (1 more version)
Application
QoS 1 Policy | 0 Rules
Traffic Steering 1 Policy | 0 Rules
Security
Access Control 2 Policies | 0 Rules
Antivirus 1 Policy | 0 Rules
IPS 1 Policy | 0 Rules
IP Filtering 1 Policy | 0 Rules
URL Filtering 1 Policy | 0 Rules
Default-Active-Active
Version 1
Network
WAN | 1 1 Wired
WLAN | 1 Enterprise-WiFi
LAN | 2 Enterprise-WiFi Enterprise-LAN
Application
QoS 1 Policy | 0 Rules
Traffic Steering 1 Policy | 0 Rules
Security
Access Control 1 Policy | 0 Rules
Antivirus 1 Policy | 0 Rules
IPS 1 Policy | 0 Rules
IP Filtering 1 Policy | 0 Rules
URL Filtering 1 Policy | 0 Rules
Variables | 3
Default-Basic-MP
Version 1
Network
WAN | 3 1 Wireless | 2 Wired
WLAN | 1 Enterprise-WiFi
LAN | 2 Enterprise-WiFi Enterprise-LAN
Application
QoS 1 Policy | 0 Rules
Traffic Steering 1 Policy | 0 Rules
Security
Access Control 1 Policy | 0 Rules
Antivirus 1 Policy | 0 Rules
IPS 1 Policy | 0 Rules
IP Filtering 1 Policy | 0 Rules
URL Filtering 1 Policy | 0 Rules
Variables | 3
Showing page 1 of 1 10 rows
< Previous 1 Next >

2. To create a new master profile of type Standard, click Configure > Profiles > Master Profiles > Standard, and then click + Standard.



VERSION	PROFILE NAME	TYPE	POLICY COUNT	VARIABLES	LAST MODIFIED
1					8/23/2022, 4:14:37 PM Administrator
1	Sub-Profile-1.v1	Security	0		5/25/2022, 5:04:08 AM Administrator
1	MT-SubProfile.v1	Security	1		5/25/2022, 1:01:13 AM Administrator
2	DeviceSP.v1	Device	1		5/4/2022, 10:41:37 AM Administrator

The New Master Profile screen displays.



New Master Profile
V1

Name

Version 1

Type
Standard

Scope
Single Tenant

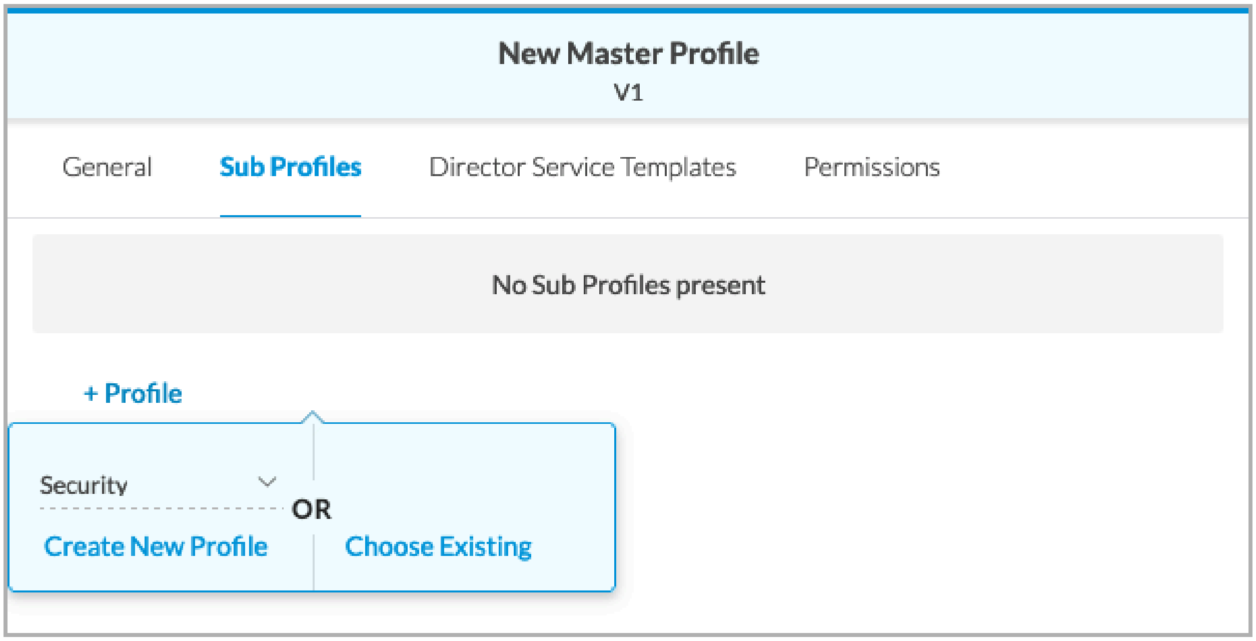
Solution Tier
Select

Variables | 0

No variables present

Profiles | 0

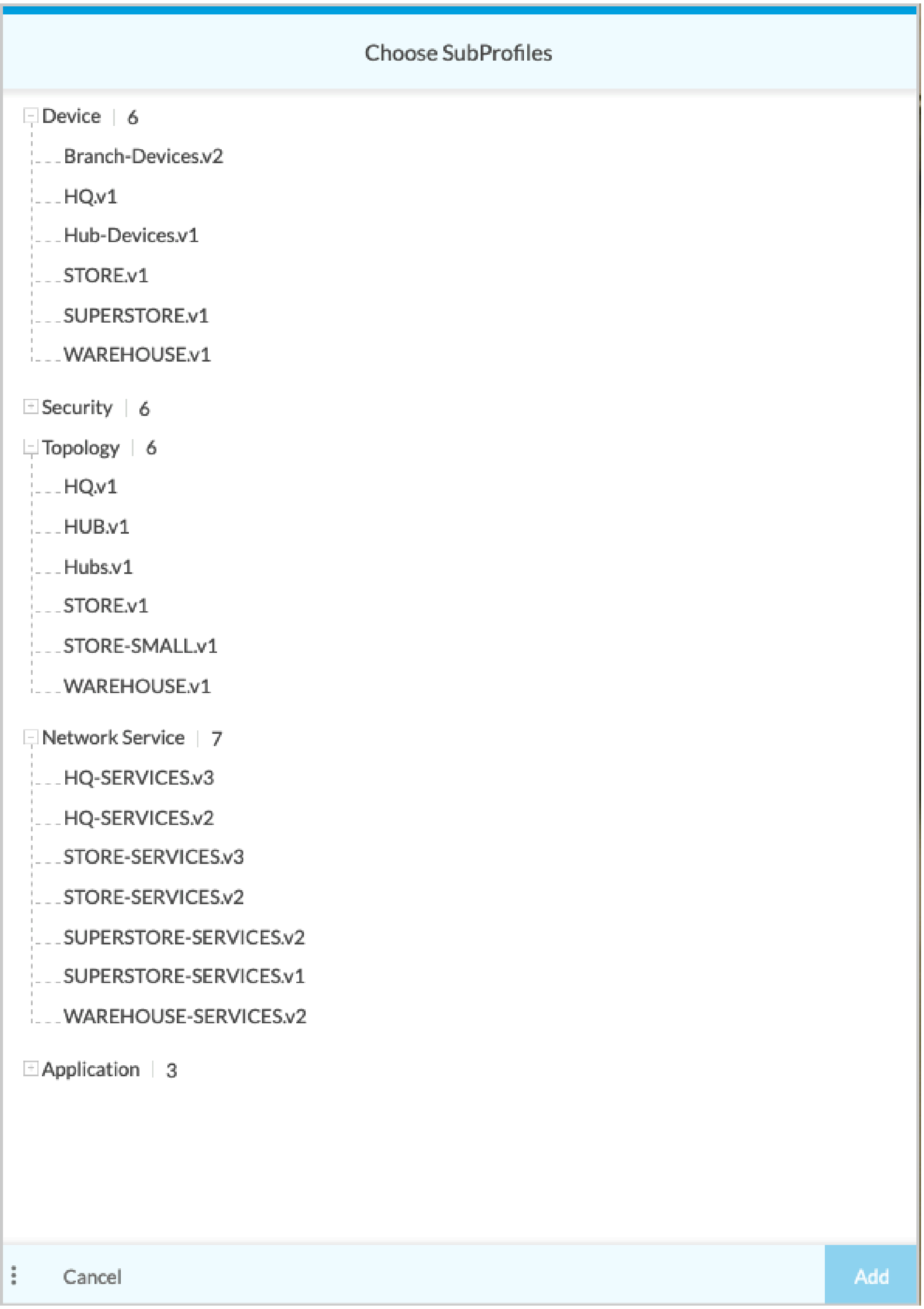
3. In the Name field, enter a name for the new master profile.
4. In the Solution Tier field, select a Versa licensing solution tier.
5. For Releases 11.2.1 and later, in the Scope field, select if the master profile is for single tenant, multitenant, or subtenant. By default, Single Tenant is selected.
6. Click Next. The Subprofiles tab displays.
7. Click + Profile to add a subprofile to the master profile. You can create a new subprofile or reuse an existing one.



Reuse an Existing Subprofile

To reuse an existing subprofile in a new master profile:

1. In New Master Profile > Subprofiles tab, click Choose Existing. The Choose Subprofiles screen displays.



Choose SubProfiles

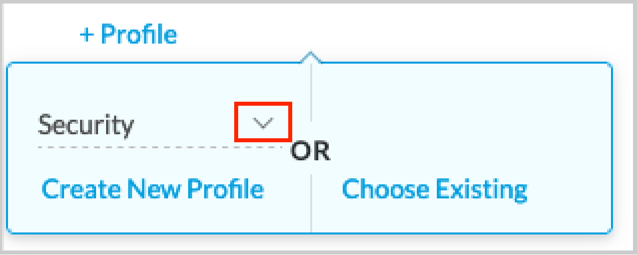
- Device | 6
  - Branch-Devices.v2
  - HQ.v1
  - Hub-Devices.v1
  - STORE.v1
  - SUPERSTORE.v1
  - WAREHOUSE.v1
- Security | 6
- Topology | 6
  - HQ.v1
  - HUB.v1
  - Hubs.v1
  - STORE.v1
  - STORE-SMALL.v1
  - WAREHOUSE.v1
- Network Service | 7
  - HQ-SERVICES.v3
  - HQ-SERVICES.v2
  - STORE-SERVICES.v3
  - STORE-SERVICES.v2
  - SUPERSTORE-SERVICES.v2
  - SUPERSTORE-SERVICES.v1
  - WAREHOUSE-SERVICES.v2
- Application | 3

2. Select one or more existing subprofiles to use in the new master profile.
3. Click Add.

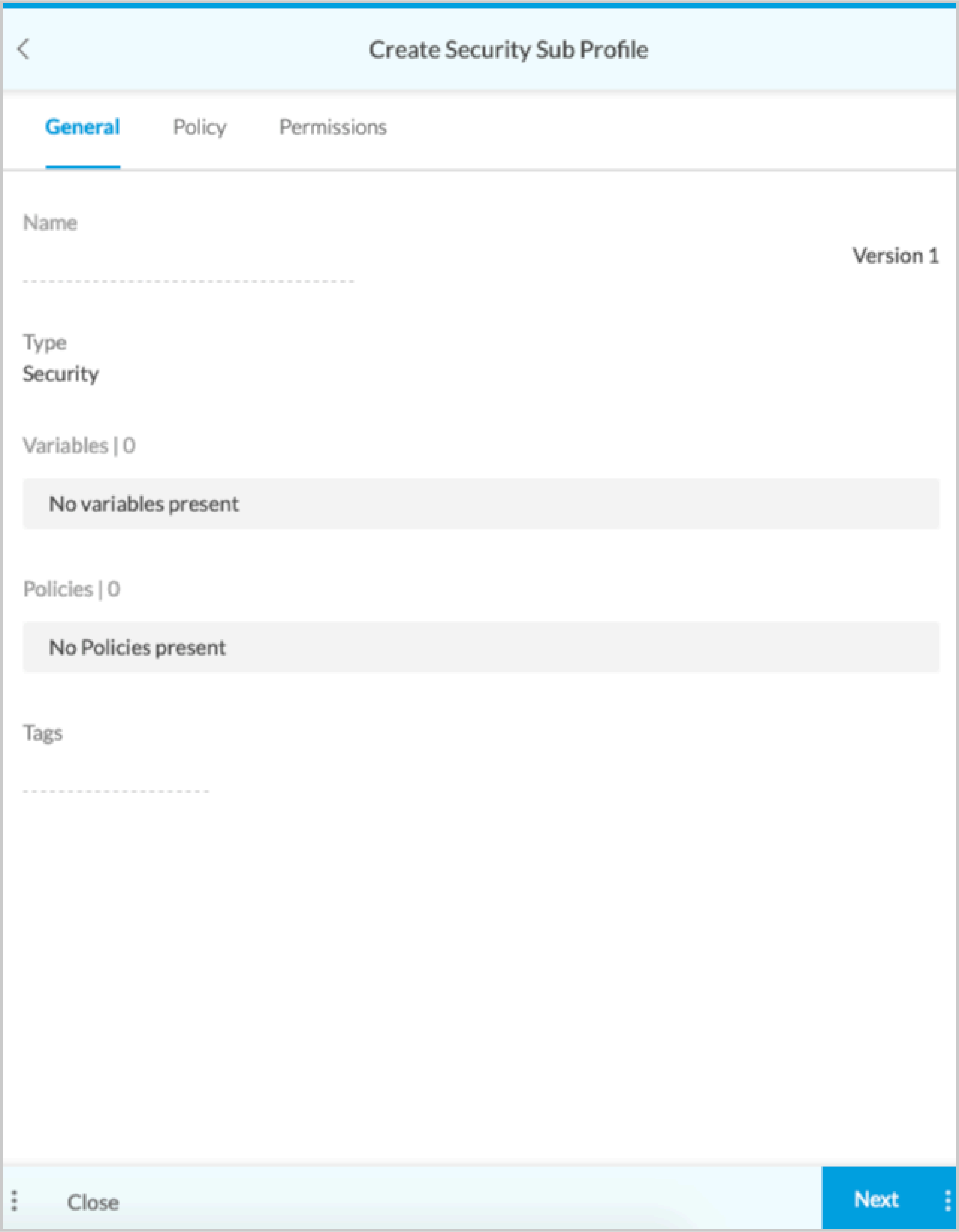
Create a New Subprofile

To create a new subprofile to use in a new master profile:

1. In the New Master Profile > Subprofiles tab, click + Profile. The following popup window displays.



2. Click the down arrow, select a profile type. The profile types are Security, Application, Device, Network Services, Topology, and, for Releases 11.3.1 and later, System.
3. Click Create New Profile. The Create *Type* Subprofile screen displays. The following screenshot shows the Create Security Subprofile screen.



Version 1

Type
Security

Variables | 0

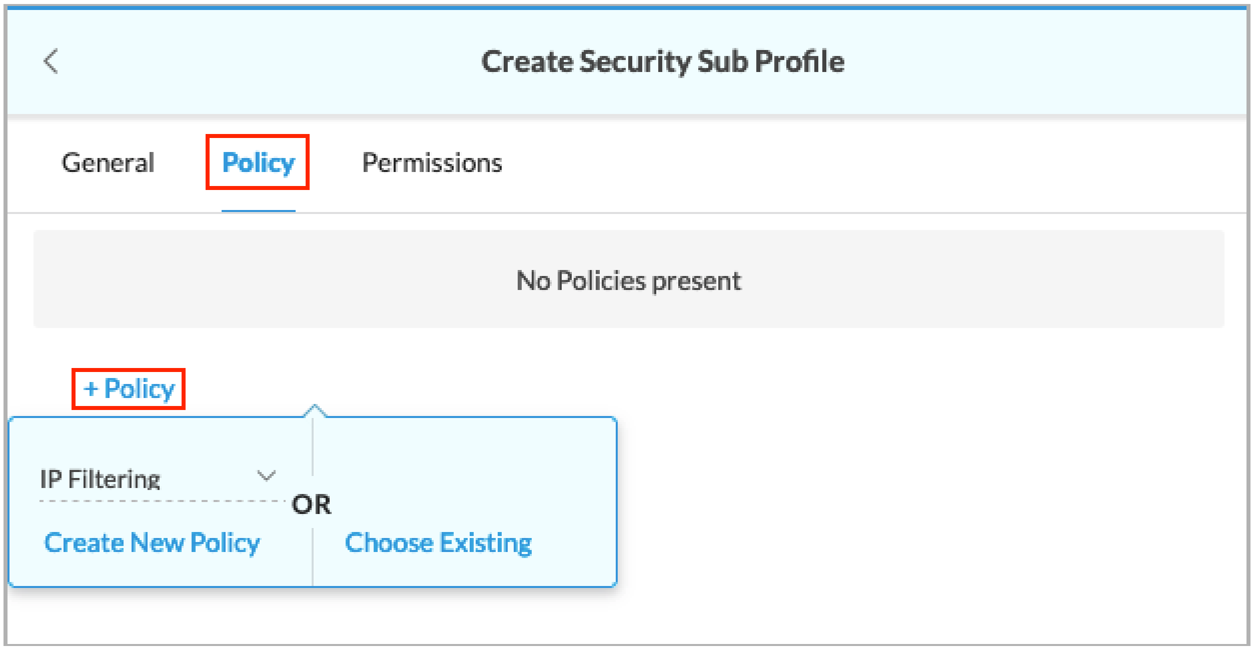
No variables present

Policies | 0

No Policies present

4. Enter a name for the subprofile.
5. Select the Policy tab or click Next. The Policy screen displays.

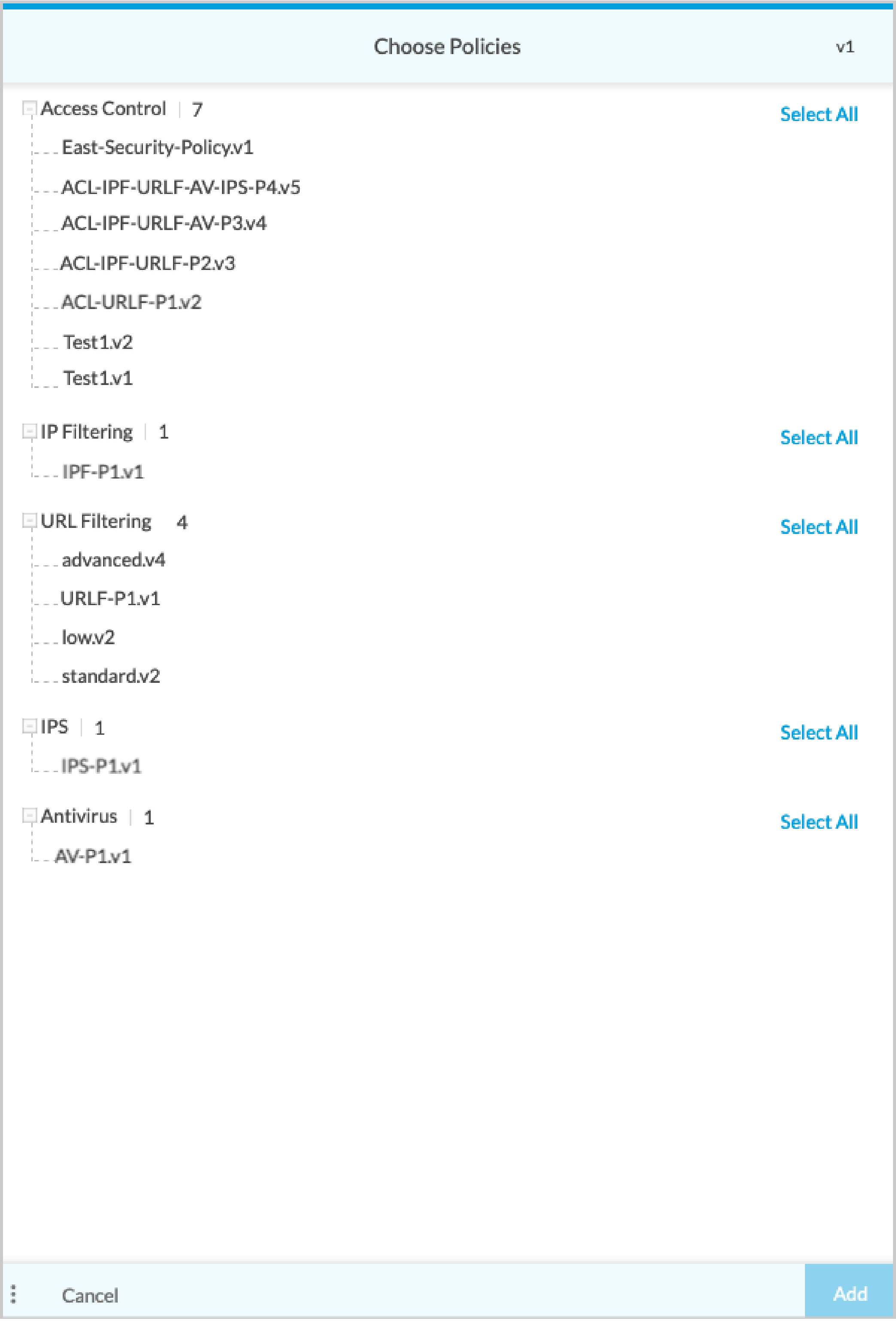
6. Click + Policy to create a new policy or to reuse an existing one.



Reuse an Existing Policy

To reuse an existing policy:

1. Click Choose Existing. The Choose Policies screen displays.



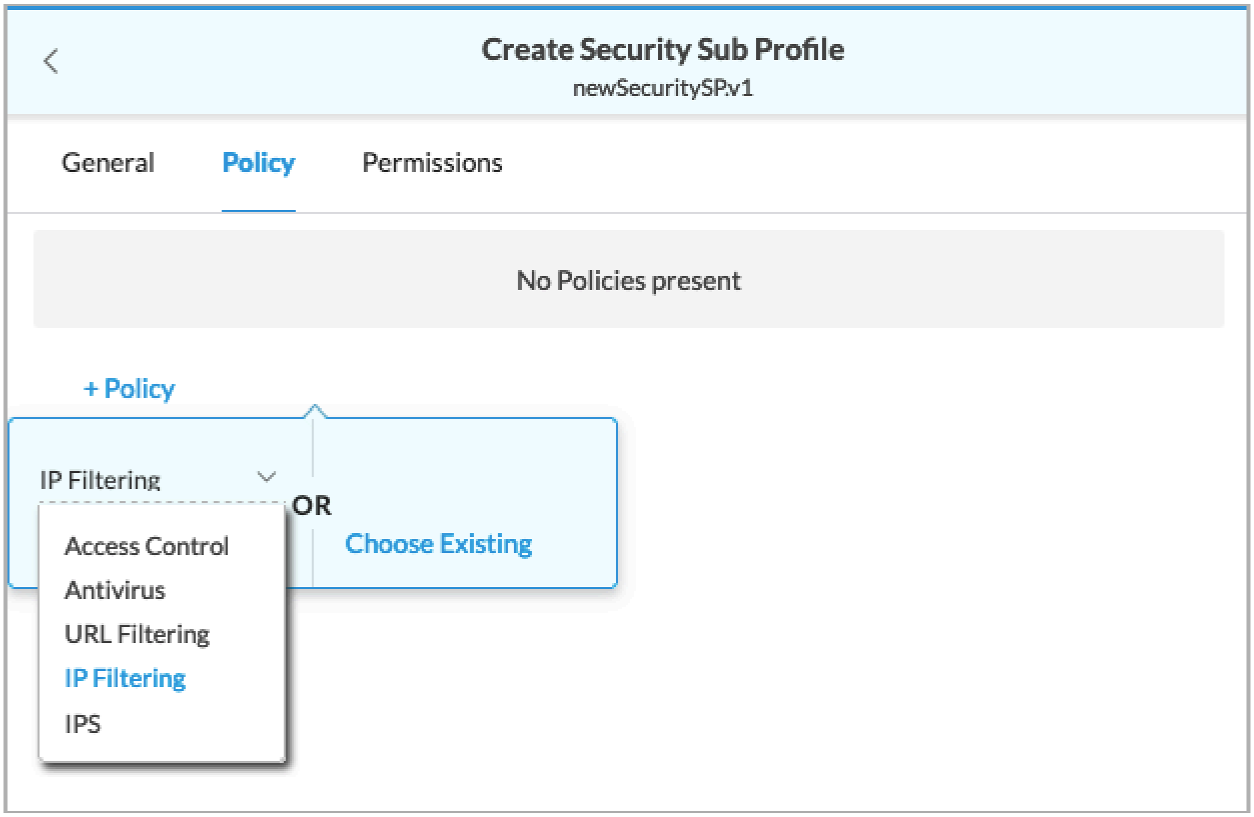
- Access Control | 7
  - East-Security-Policy.v1
  - ACL-IPF-URLF-AV-IPS-P4.v5
  - ACL-IPF-URLF-AV-P3.v4
  - ACL-IPF-URLF-P2.v3
  - ACL-URLF-P1.v2
  - Test1.v2
  - Test1.v1
- IP Filtering | 1
  - IPF-P1.v1
- URL Filtering 4
  - advanced.v4
  - URLF-P1.v1
  - low.v2
  - standard.v2
- IPS | 1
  - IPS-P1.v1
- Antivirus | 1
  - AV-P1.v1

2. Select one or more existing policies.
3. Click Add.

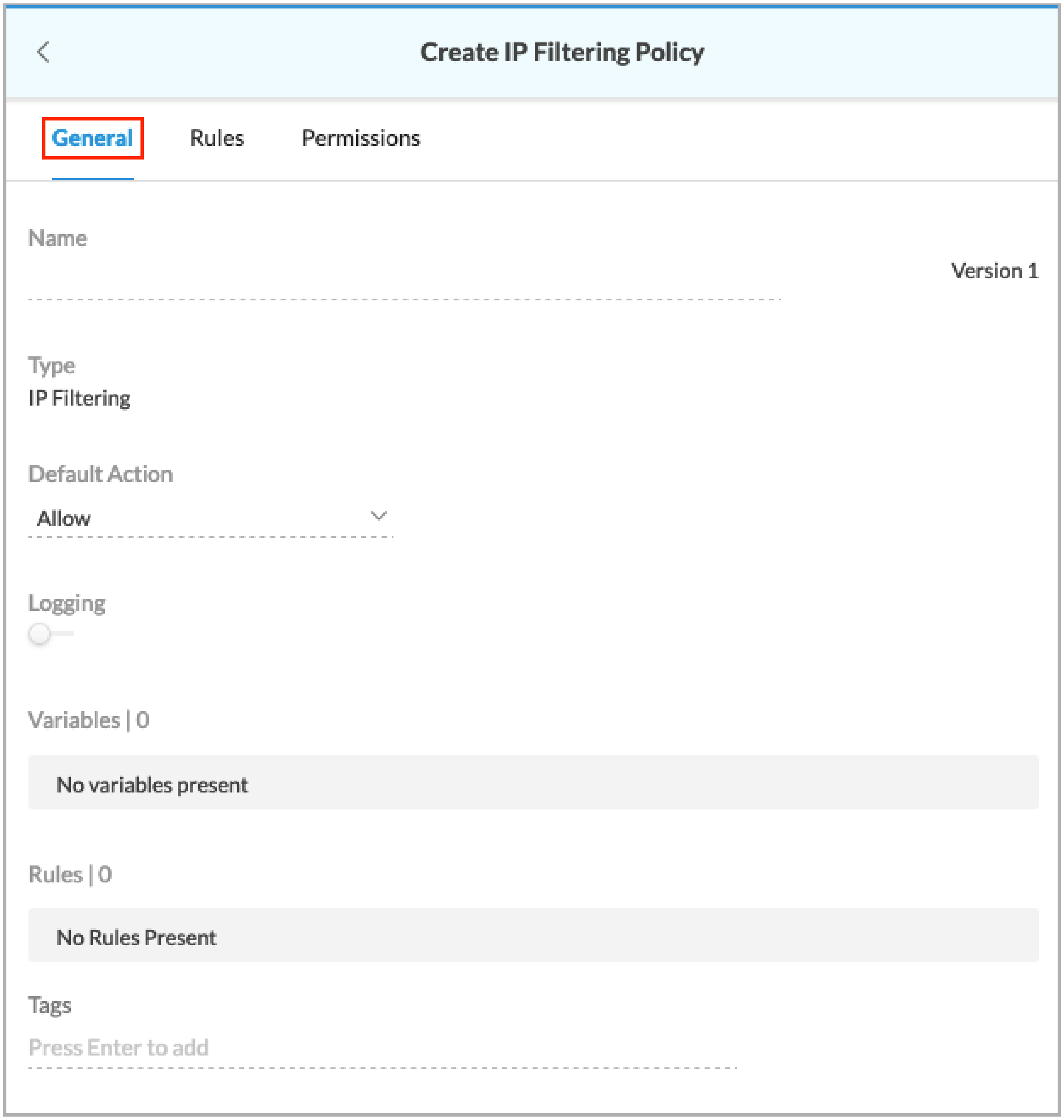
Create a New Policy

To create a new policy:

1. Select a policy type, and then click Create New Policy.



The Create Policy screen displays, and the General tab is selected. The following screenshot shows the Create IP Filtering Policy screen.



Create IP Filtering Policy

Name

Version 1

Type
IP Filtering

Default Action
Allow

Logging

Variables | 0

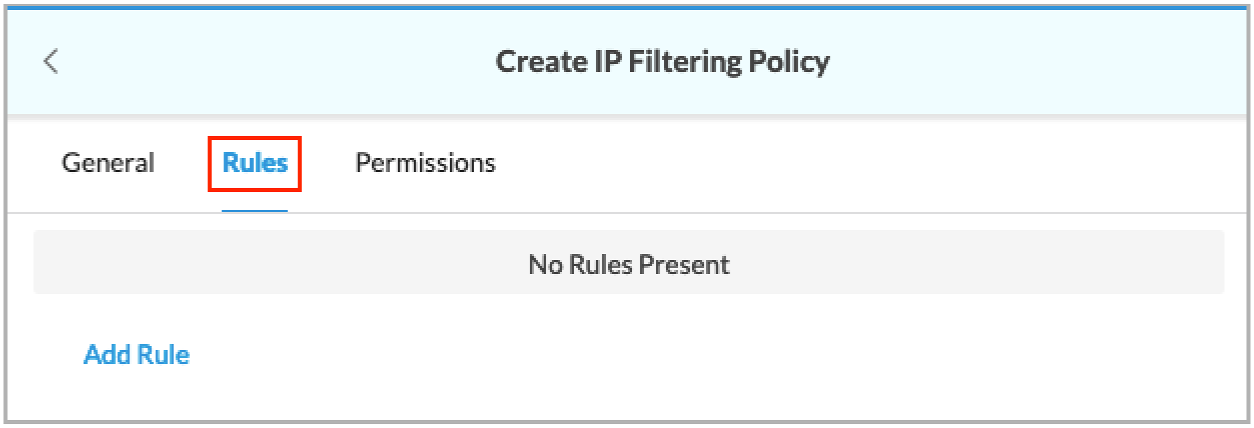
No variables present

Rules | 0

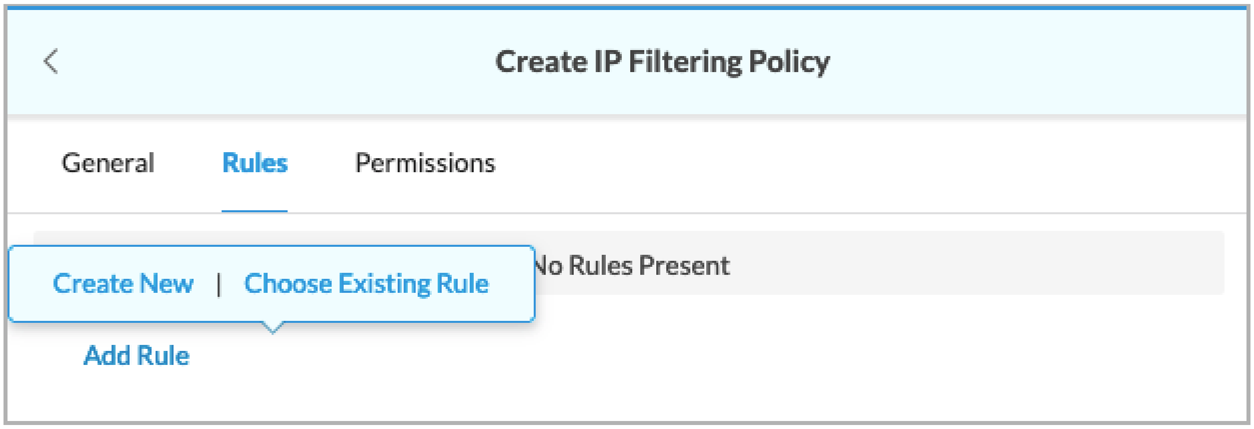
No Rules Present

Tags
Press Enter to add

2. Enter a name for the new policy.
3. Click Next. The Rules tab displays. You can create a new rule or reuse an existing one.



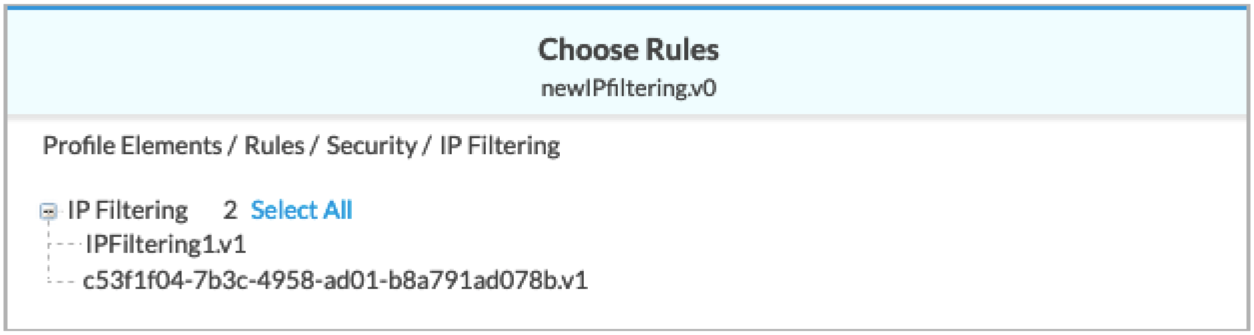
4. Click Add Rule.



Reuse an Existing Rule

To reuse an existing rule:

1. Click Choose Existing Rule. The Choose Rules screen displays.


Choose Rules
newIPfiltering.v0
Profile Elements / Rules / Security / IP Filtering
IP Filtering 2 Select All
IPFiltering1.v1
c53f1f04-7b3c-4958-ad01-b8a791ad078b.v1

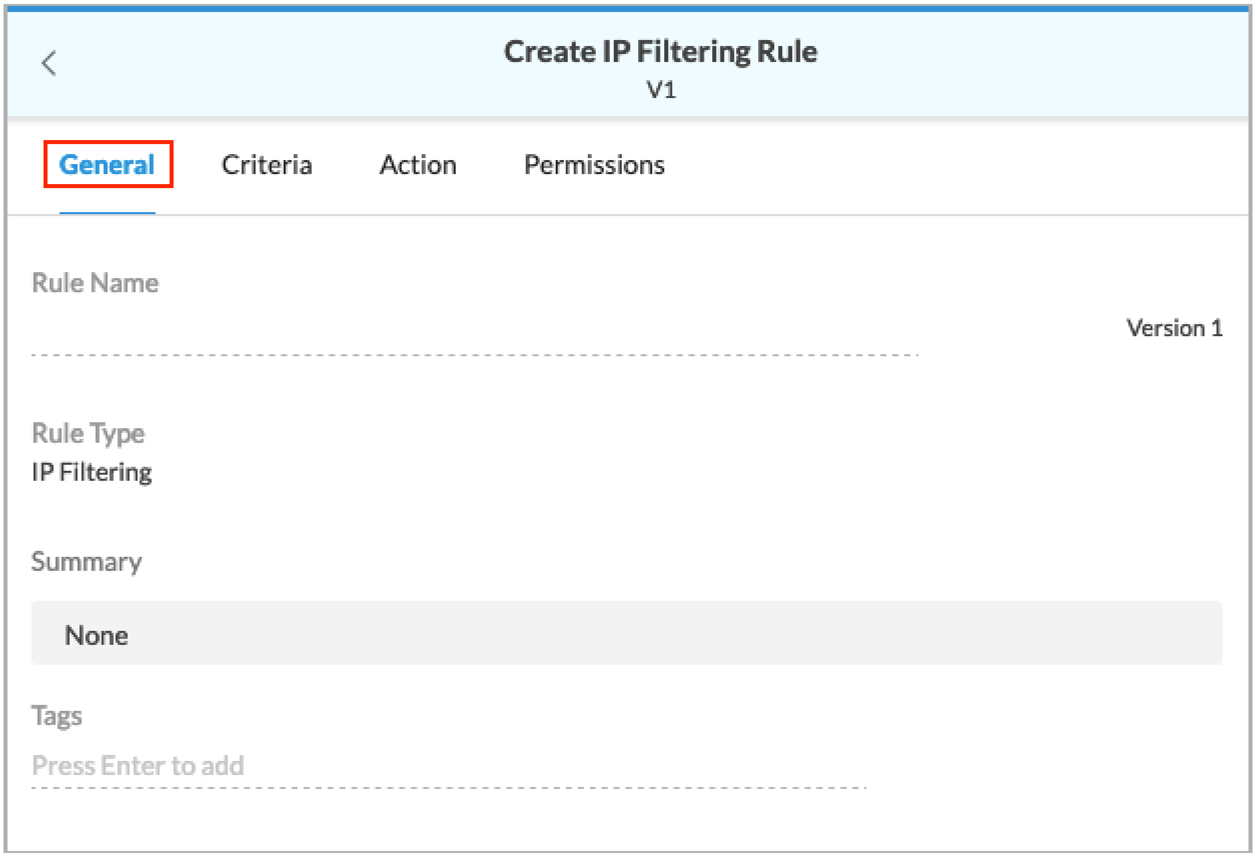
2. Select one or more existing rules.

3. Click Add.

Create a New Rule

To create a new rule:

1. Click Create New. The Create Rule screen displays. The following screenshot shows the Create IP Filtering Rule screen.



Create IP Filtering Rule
V1

General | Criteria | Action | Permissions

Rule Name

Version 1

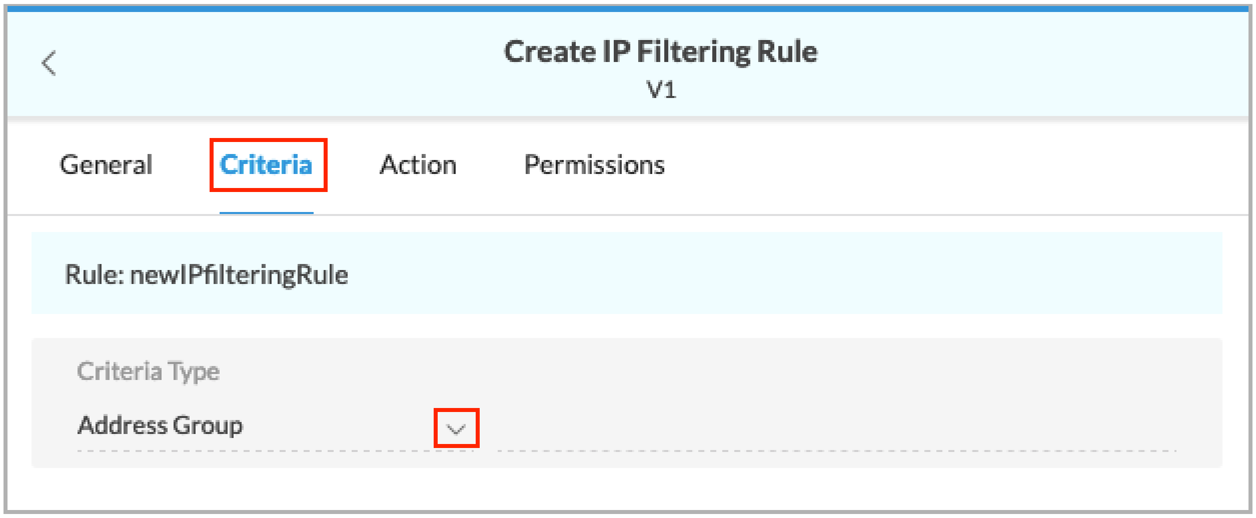
Rule Type
IP Filtering

Summary

None

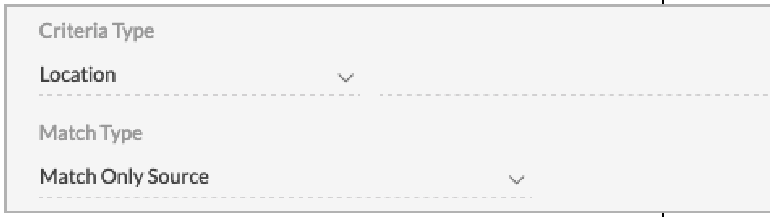
Tags
Press Enter to add

2. Enter a name for the rule.
3. Click Next. The Criteria tab displays. In the Criteria Type field, enter information for the following fields.

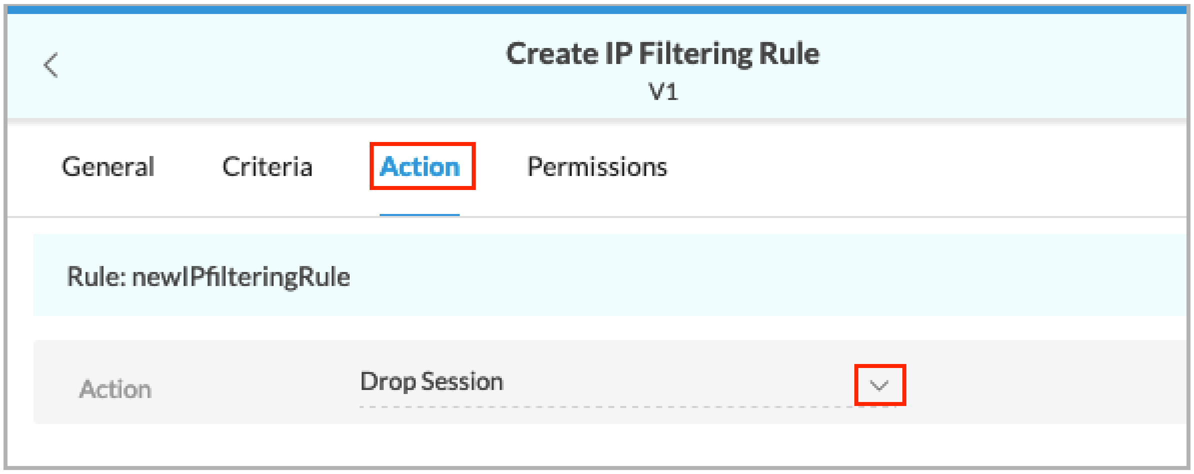


Rule: newIPfilteringRule

Criteria Type: Address Group

Field	Description
Address Group	Click in the field to the right of Address Group and select a group. You can select multiple address groups.
Location	 Criteria Type: Location Match Type: Match Only Source Click in the field to the right of Location, and then select a location. Then, in the Match Type field, select a match type: ◦ Match Only Source ◦ Match Only Destination ◦ Match Source or Destination ◦ Match Source and Destination
Reputation	Click in the field to the right of Reputation, and then select one or more reputations.

4. Click Next. The Actions tab displays.



Create IP Filtering Rule

V1

Rule: newIPfilteringRule

Action: Drop Session

5. In the Action field, select an action:
   - Drop Packet
   - Drop Session
   - Allow
   - Alert
   - Reject
6. Click Save.

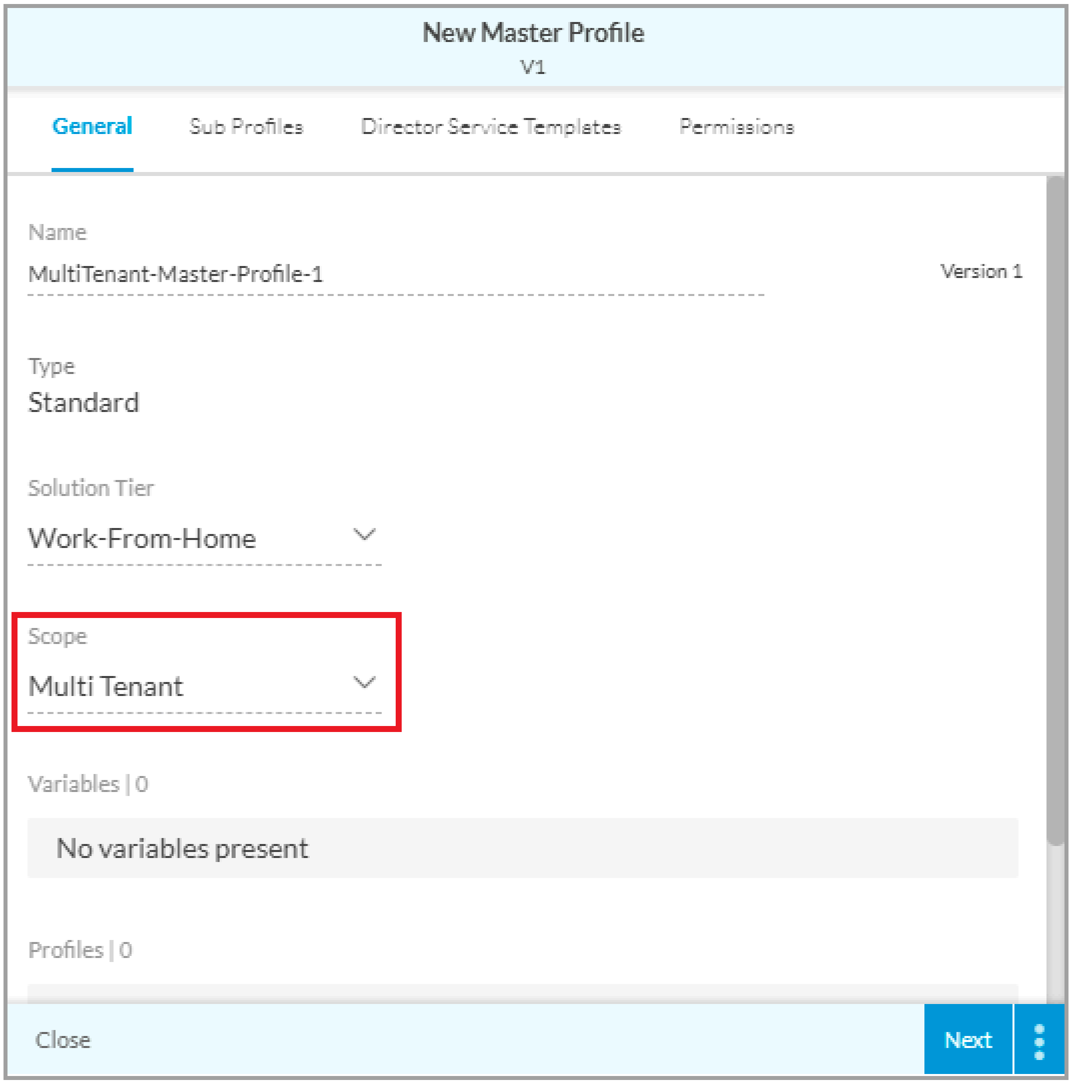
Configure a Multitenant Standard Master Profile

For Releases 11.2.1 and later.

A multitenant master profile allows you to create multitenant appliances for a provider organization. You can create new subtenants and you can attach existing subtenants while publishing the provider organization appliance that uses the multitenant master profile. Appliances are automatically created in the subtenants associated with the provider appliance that uses a multitenant master profile.

To configure a multitenant standard master profile:

1. Configure a standard multitenant with the scope Multitenant. Go to
   a. Go to New Master Profile > General.



New Master Profile
V1

Name: MultiTenant-Master-Profile-1

Version 1

Type: Standard

Solution Tier: Work-From-Home

Scope: Multi Tenant

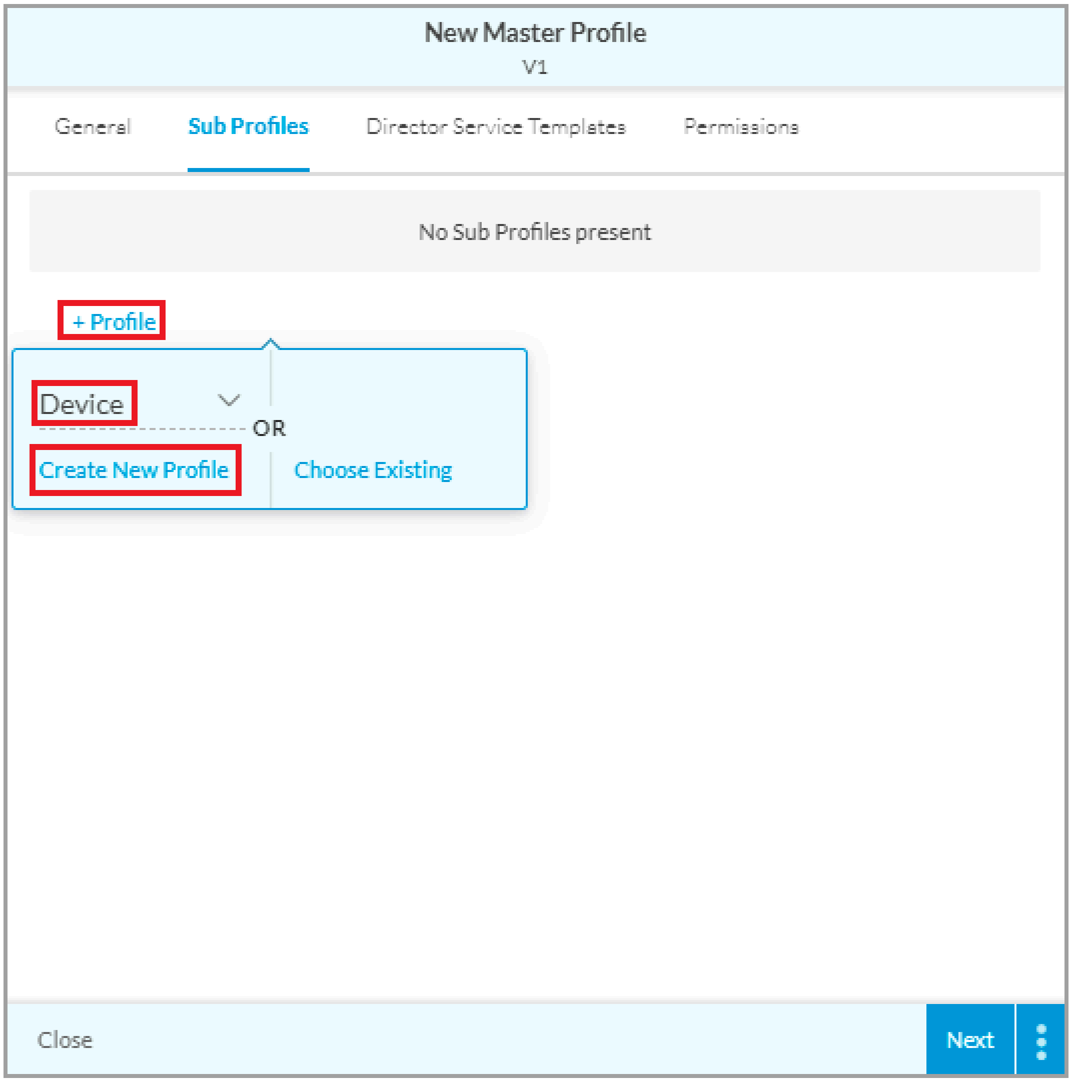
Variables | 0

No variables present

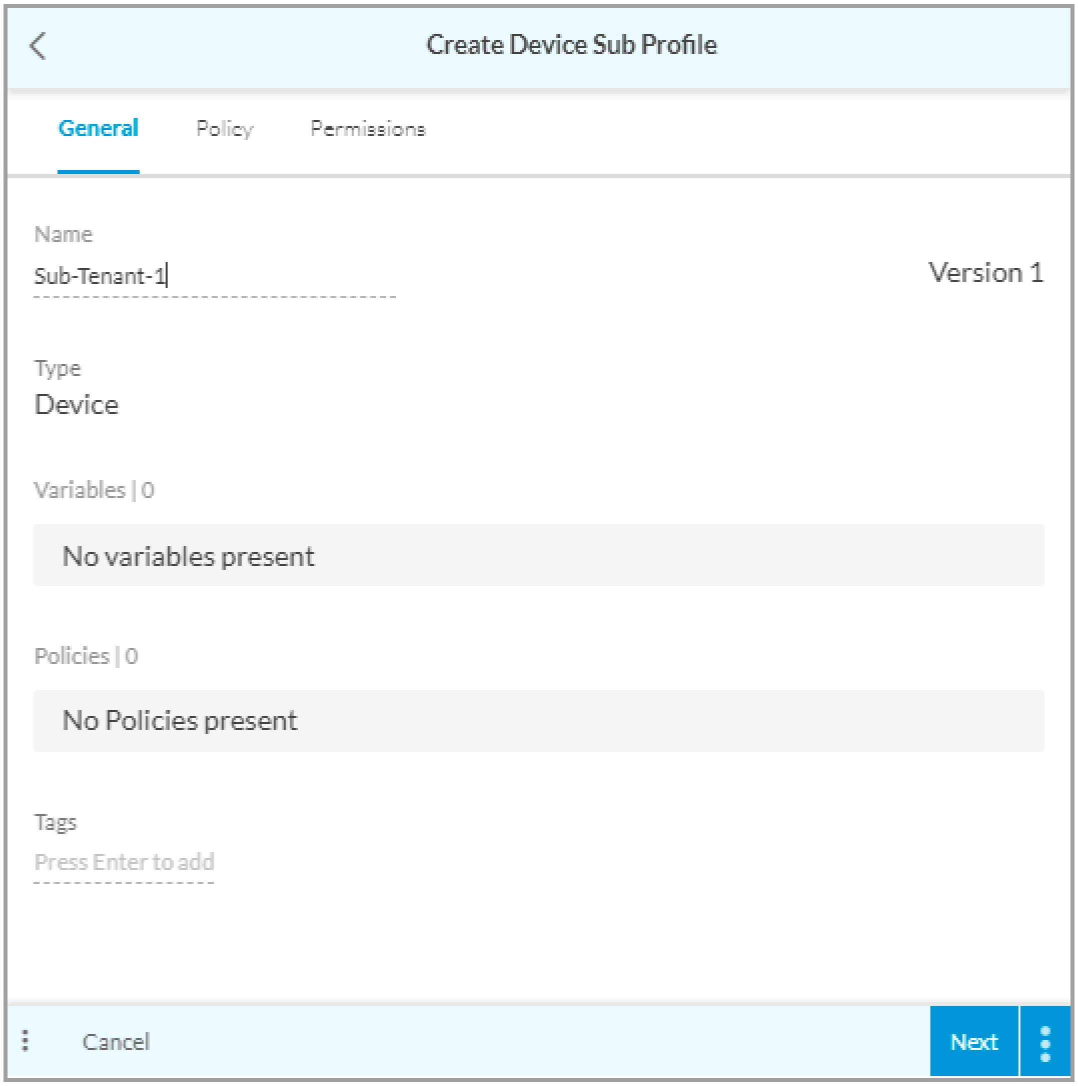
Profiles | 0

b. Enter a name for the profile.
c. Select the solution tier.
d. In the Scope field, select Multitenant.
e. Click Next.

2. Configure a device subprofile to add LAN Interfaces for the subtenants you want to onboard.
    a. Go to New Master Profile > Subprofiles, click + Profile, select Device, and then click Create New Profile.



b. In Create Device Subprofile > General, enter a name for the subprofile.



Name

Sub-Tenant-1

Version 1

Type

Device

Variables | 0

No variables present

Policies | 0

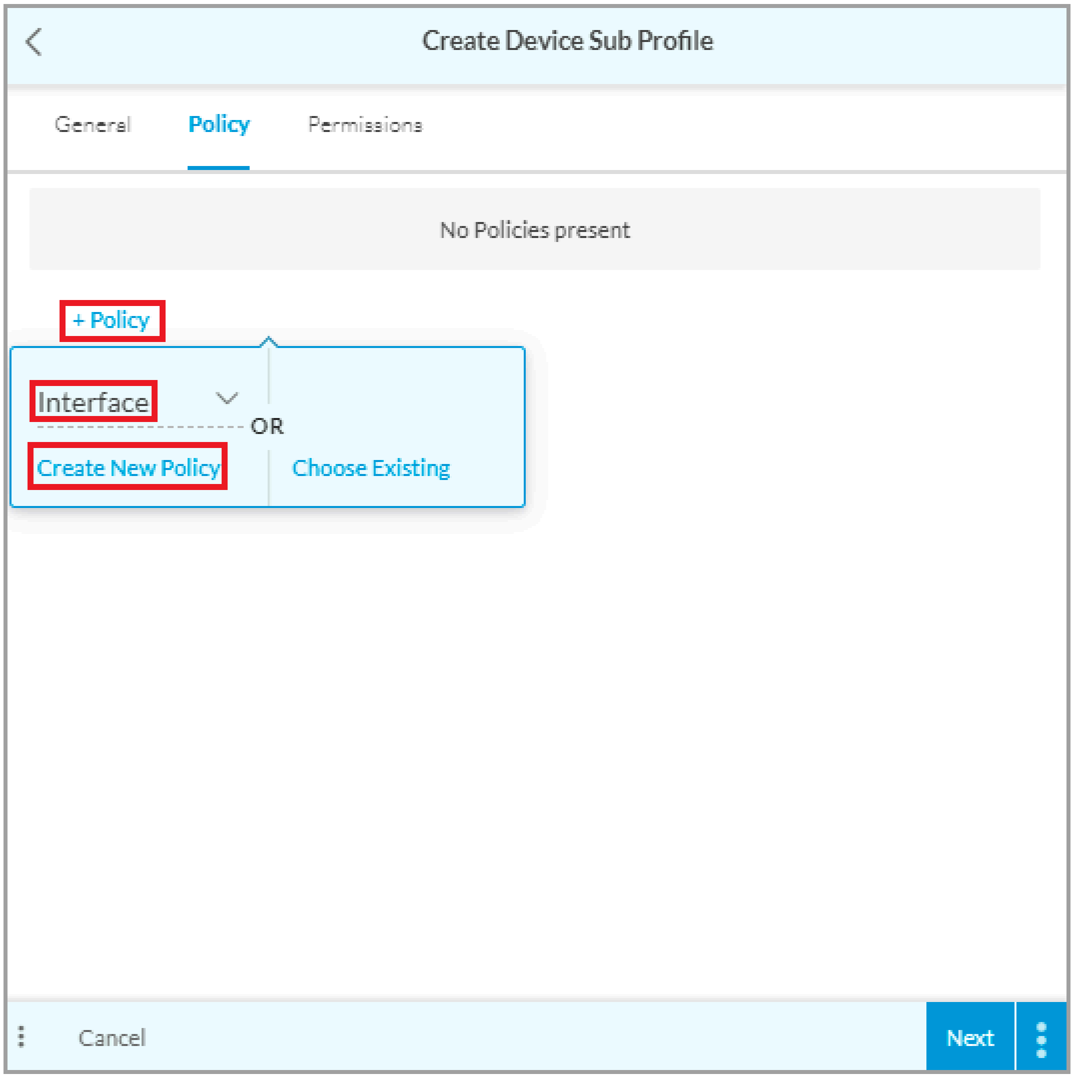
No Policies present

Tags

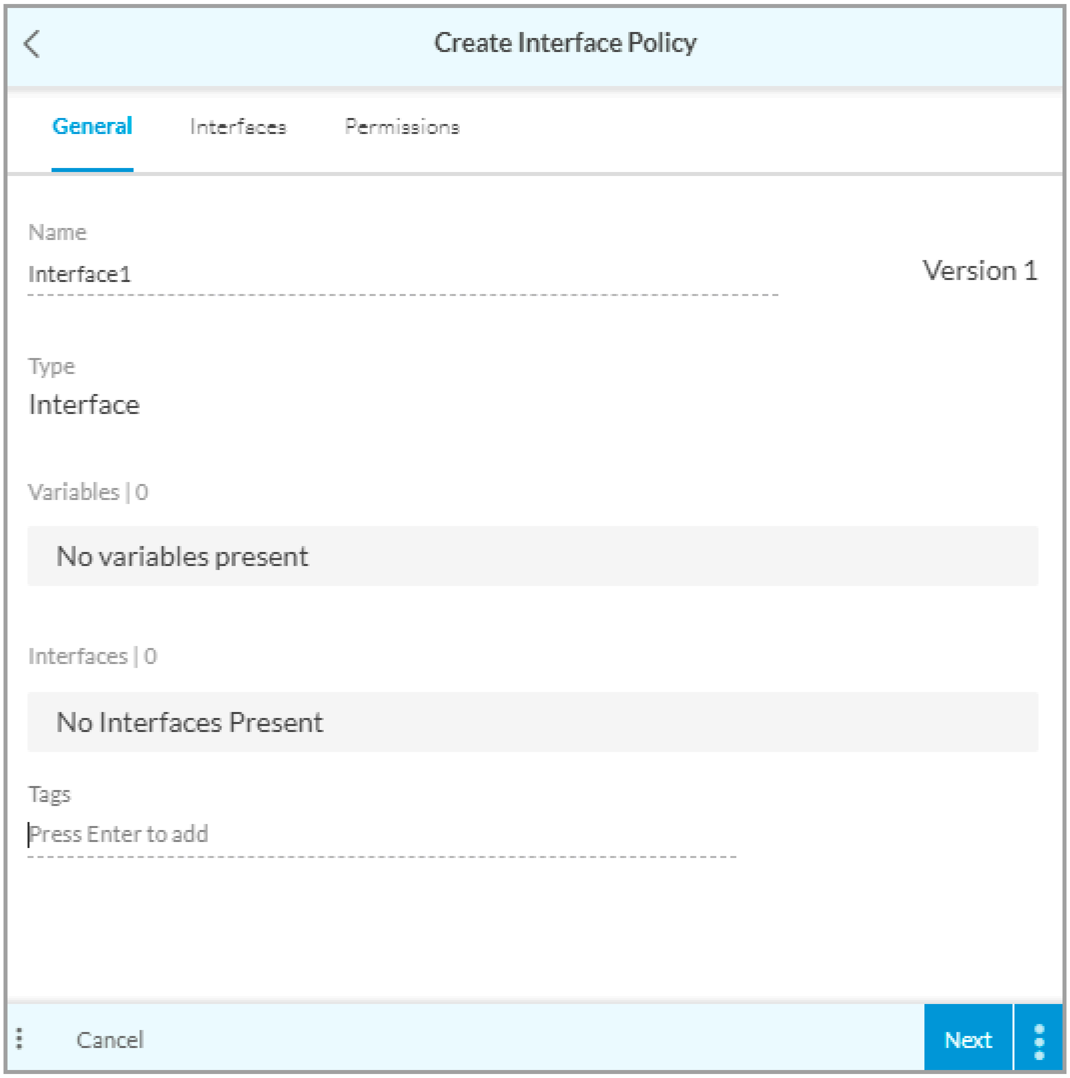
Press Enter to add

c. Click Next.

d. In the Policy tab, click + Policy, select Interface, and then click Create New Policy. The Create Interface Policy screen displays.



e. In Create Interface Policy > General, enter a name for the interface policy.



Name
Interface1

Version 1

Type
Interface

Variables | 0

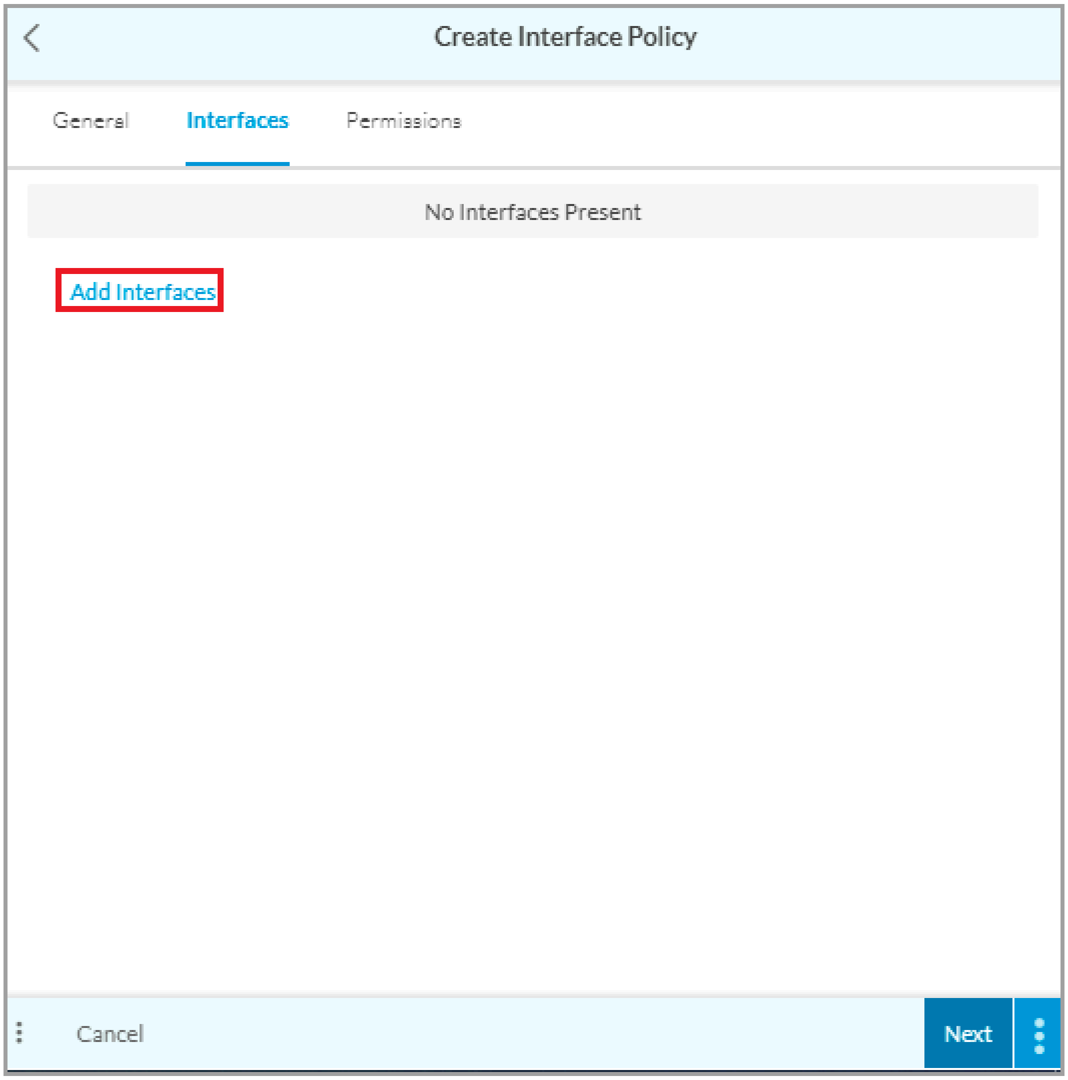
No variables present

Interfaces | 0

No Interfaces Present

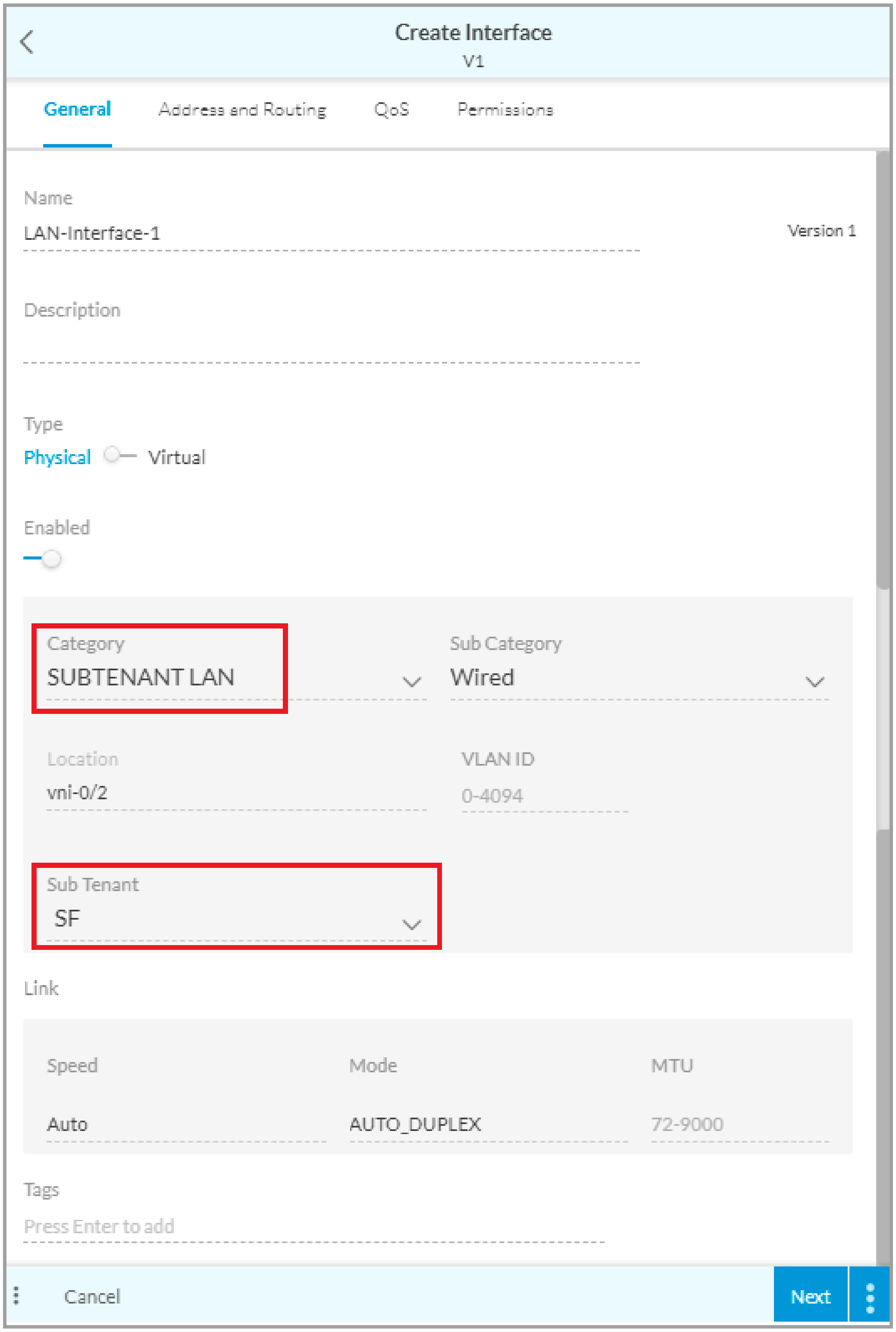
Tags
Press Enter to add

f. Click Next. The Interfaces tab displays.



g. Click Add Interface and then click Create New. The Create Interface screen displays. You can also choose an existing interface.

h. The Create Interface screen displays.



Create Interface
V1

Name
LAN-Interface-1

Version 1

Description

Type
Physical ○— Virtual

Enabled

Category
SUBTENANT LAN

Sub Category
Wired

Location
vni-0/2

VLAN ID
0-4094

Sub Tenant
SF

Link

Speed
Auto

Mode
AUTO_DUPLEX

MTU
72-9000

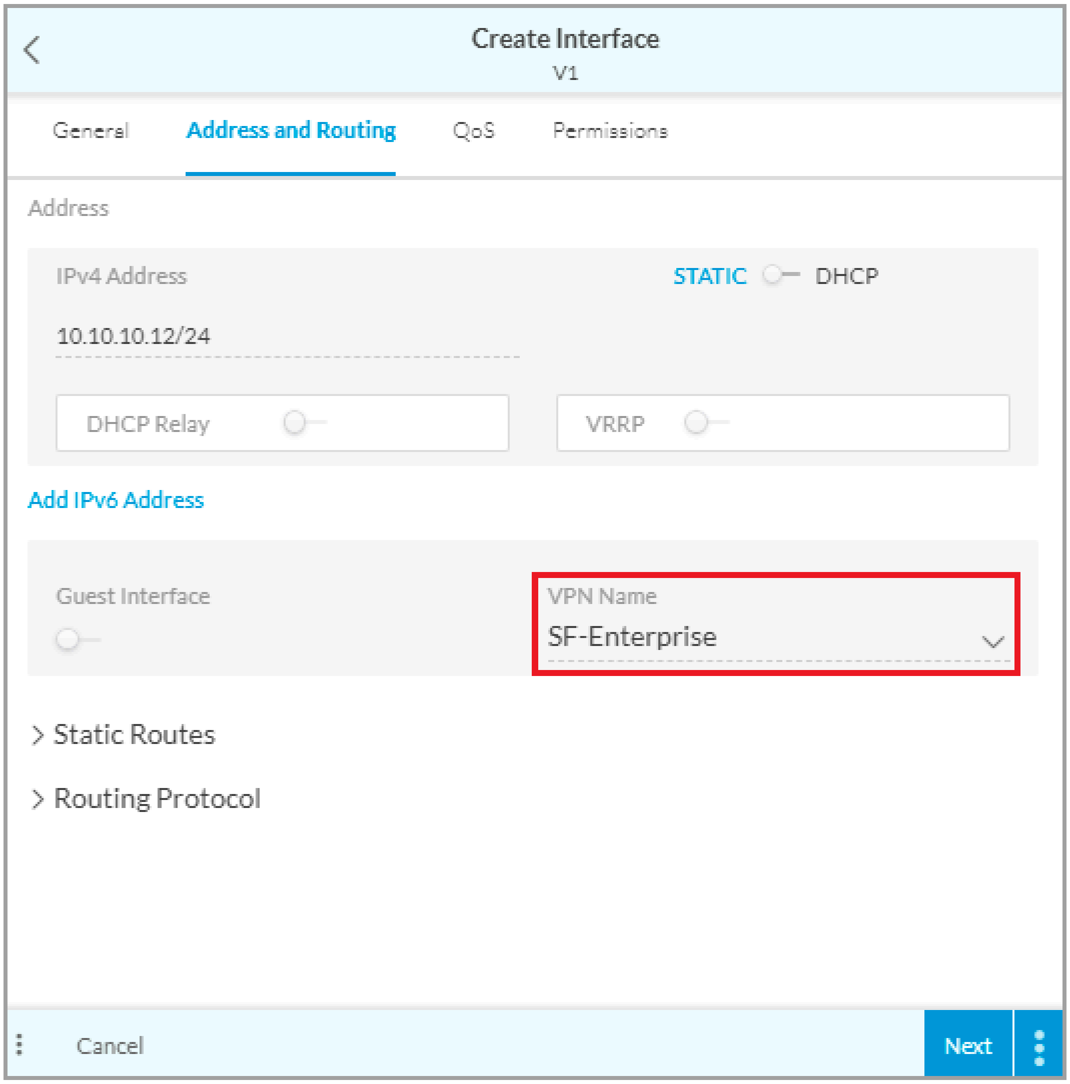
Tags
Press Enter to add

i. Enter a name for the interface.

ii. In the Category field, select Subtenant LAN. Note that to create a LAN for the provider organization, select LAN.

iii. In the Subtenant field, select the subtenant for which you are creating the subtenant LAN interface.
iv. Enter other required information.
v. Click Next.

i. The Address and Routing tab displays.



Create Interface
V1

General | Address and Routing | QoS | Permissions

Address

IPv4 Address: 10.10.10.12/24 (STATIC / DHCP)

DHCP Relay

VRRP

Add IPv6 Address

Guest Interface

VPN Name: SF-Enterprise

Static Routes

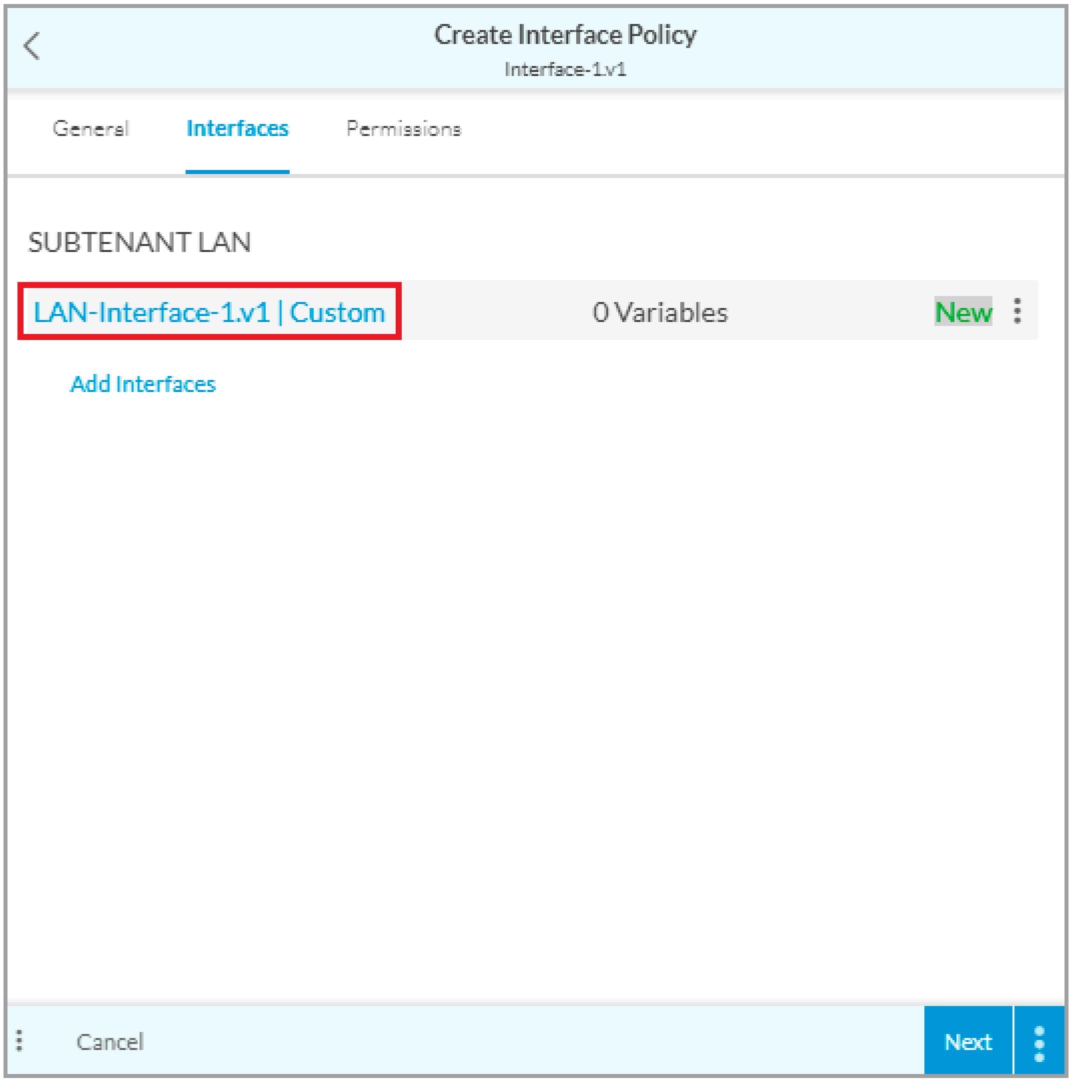
Routing Protocol

Cancel | Next

i. Enter the IPv4 address for the LAN interface.
ii. Select the VPN of the tenant in the VPN Name field. The VPN of the tenant you selected in the General tab is displayed by default.
iii. Click Next

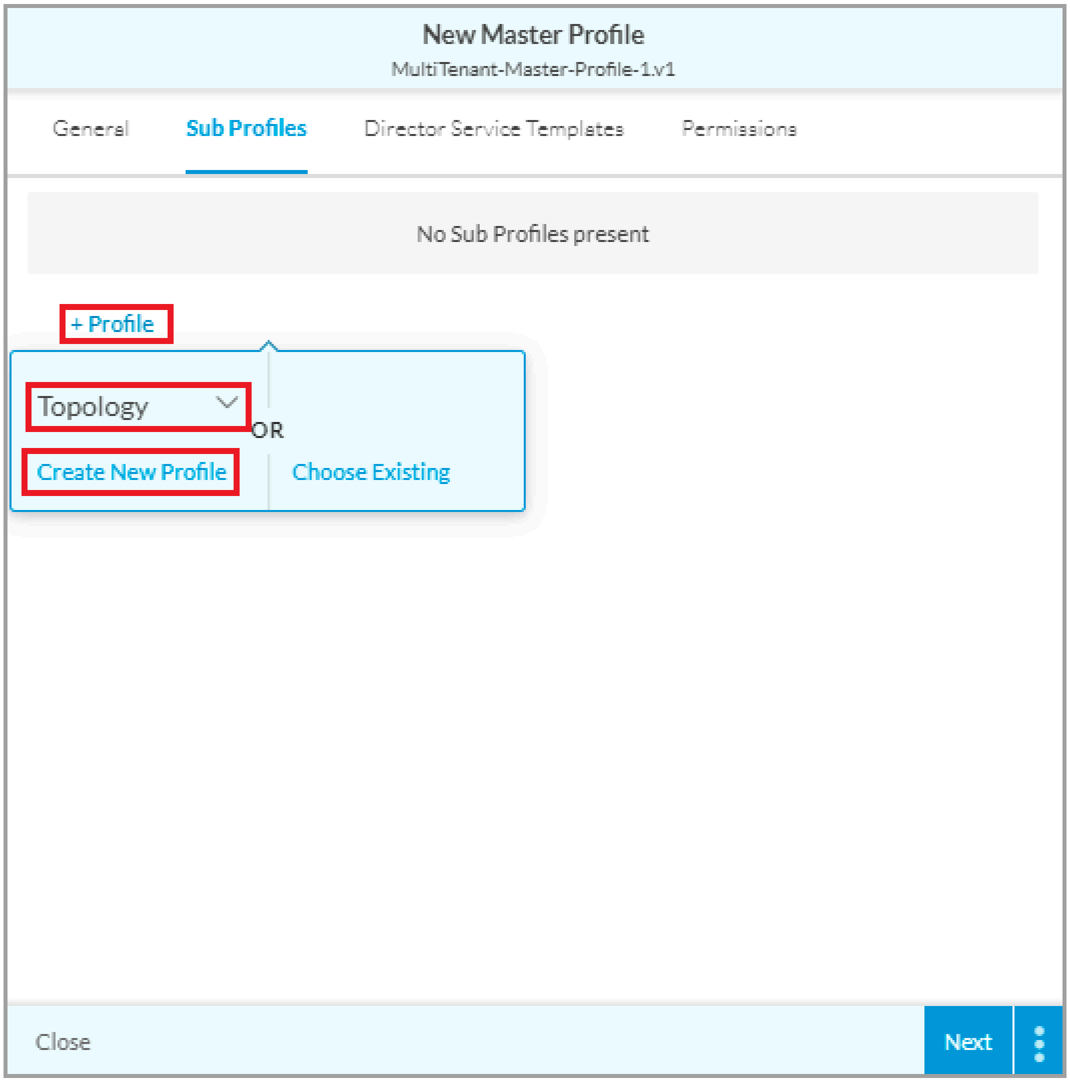
j. Enter other information, if required.

k. Save the subtenant LAN interface. The interface that you added is displayed under subtenant LAN. For example:

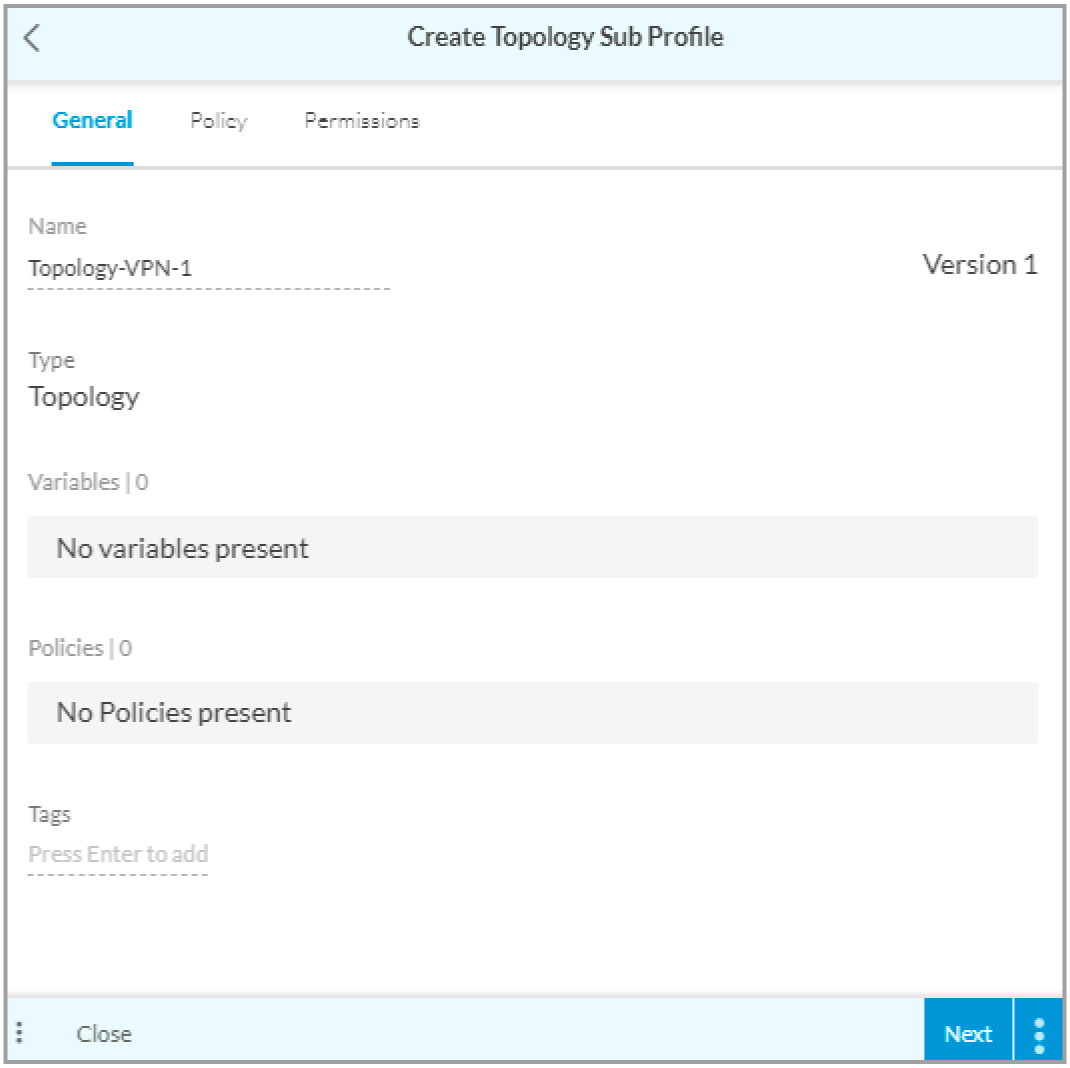


l. Repeat this step for other subtenant LANs.

3. Create a Topology subprofile to add a VPN policy and VPN instances to associate subtenant VPNs with the standard master profile.
    a. In New Master Profile > Subprofiles, click + Profile. Then select Topology, and click Create New Profile. The Create Topology Subprofile screen displays.



b. In Create Topology Subprofile > General, enter a name for the subprofile.



Create Topology Sub Profile

Name
Topology-VPN-1

Version 1

Type
Topology

Variables | 0

No variables present

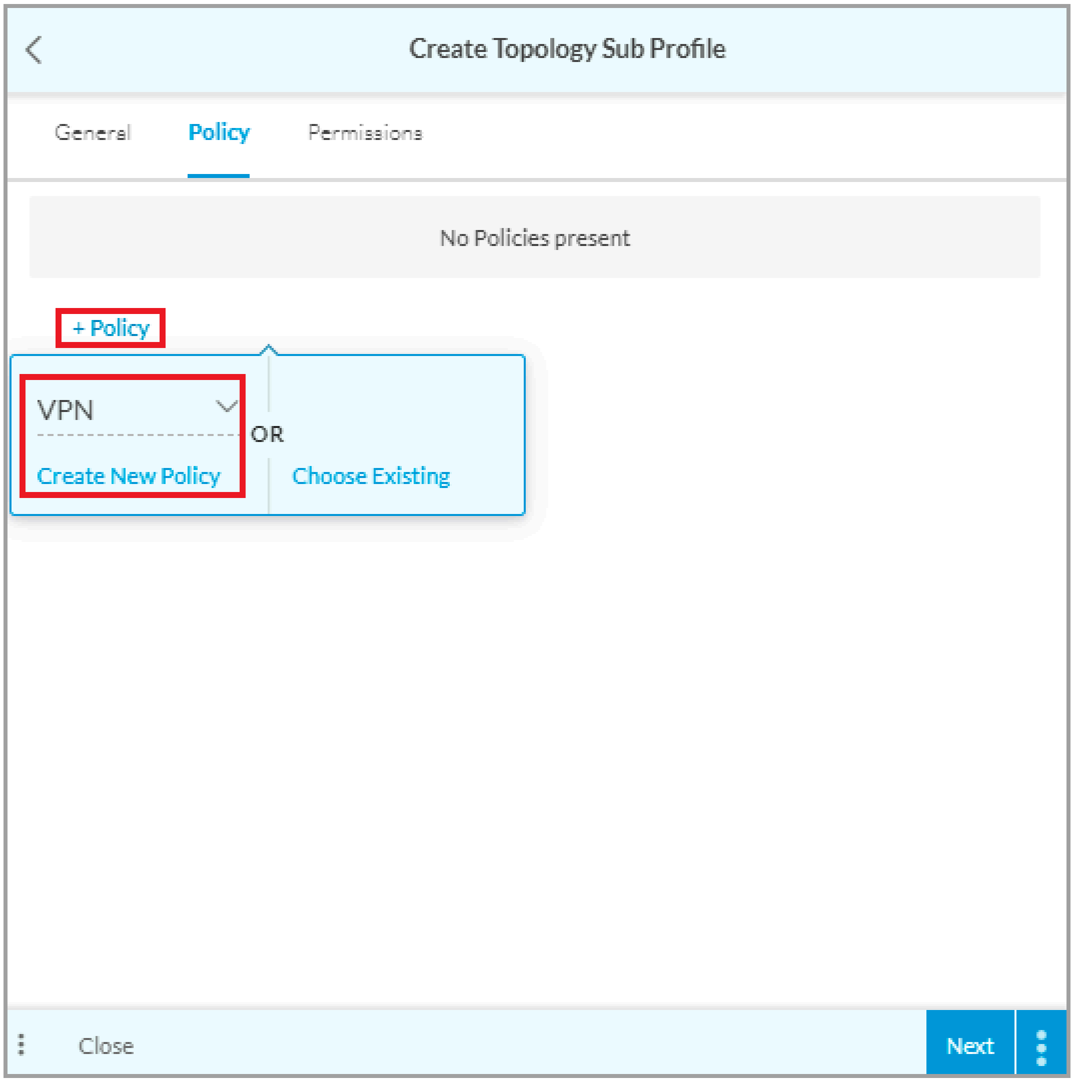
Policies | 0

No Policies present

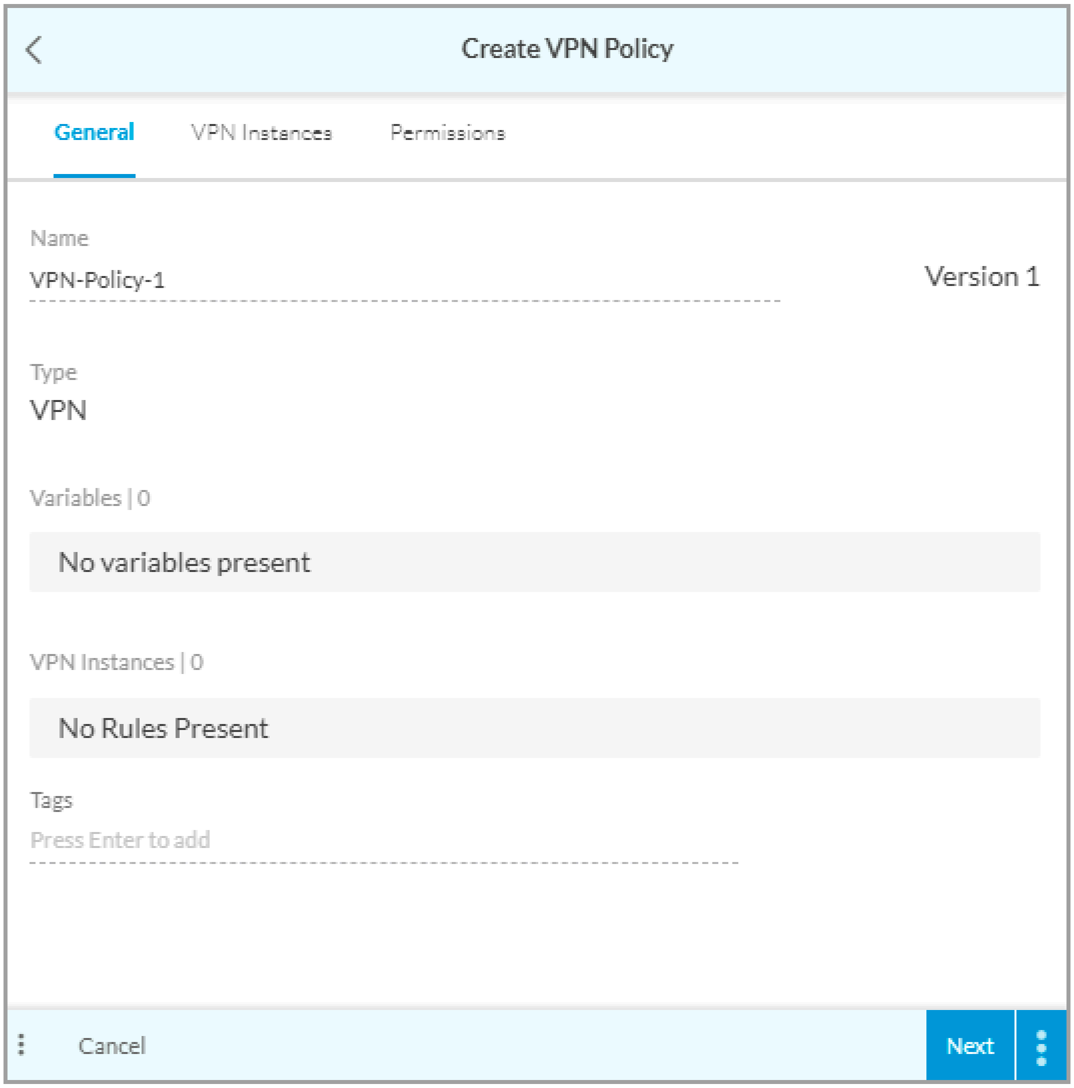
Tags
Press Enter to add

c. Click Next.

d. In the Policy tab, click + Policy, select VPN and click Create New Policy.



e. In Create VPN Policy > General, enter a name for the VPN policy.



Name
VPN-Policy-1

Version 1

Type
VPN

Variables | 0

No variables present

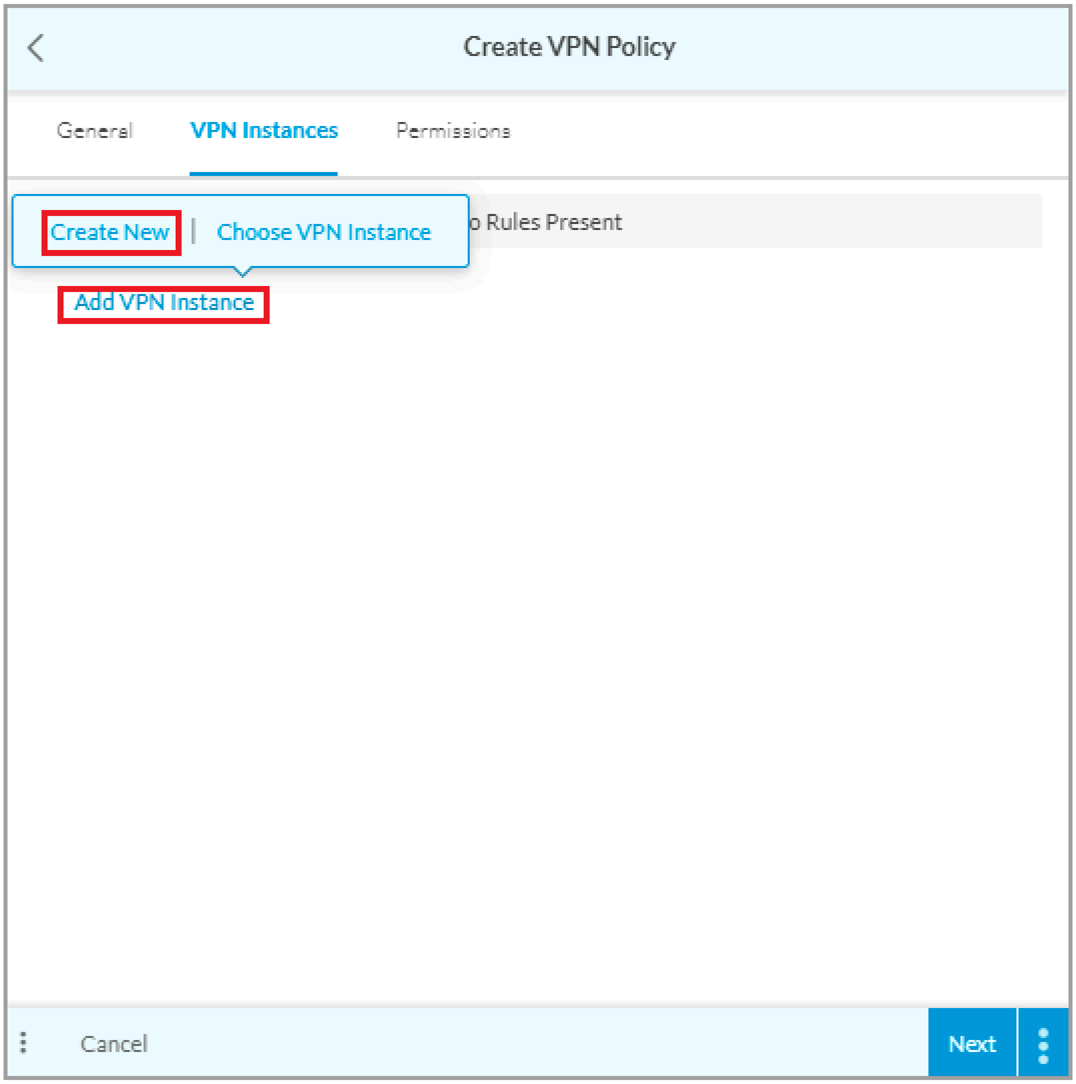
VPN Instances | 0

No Rules Present

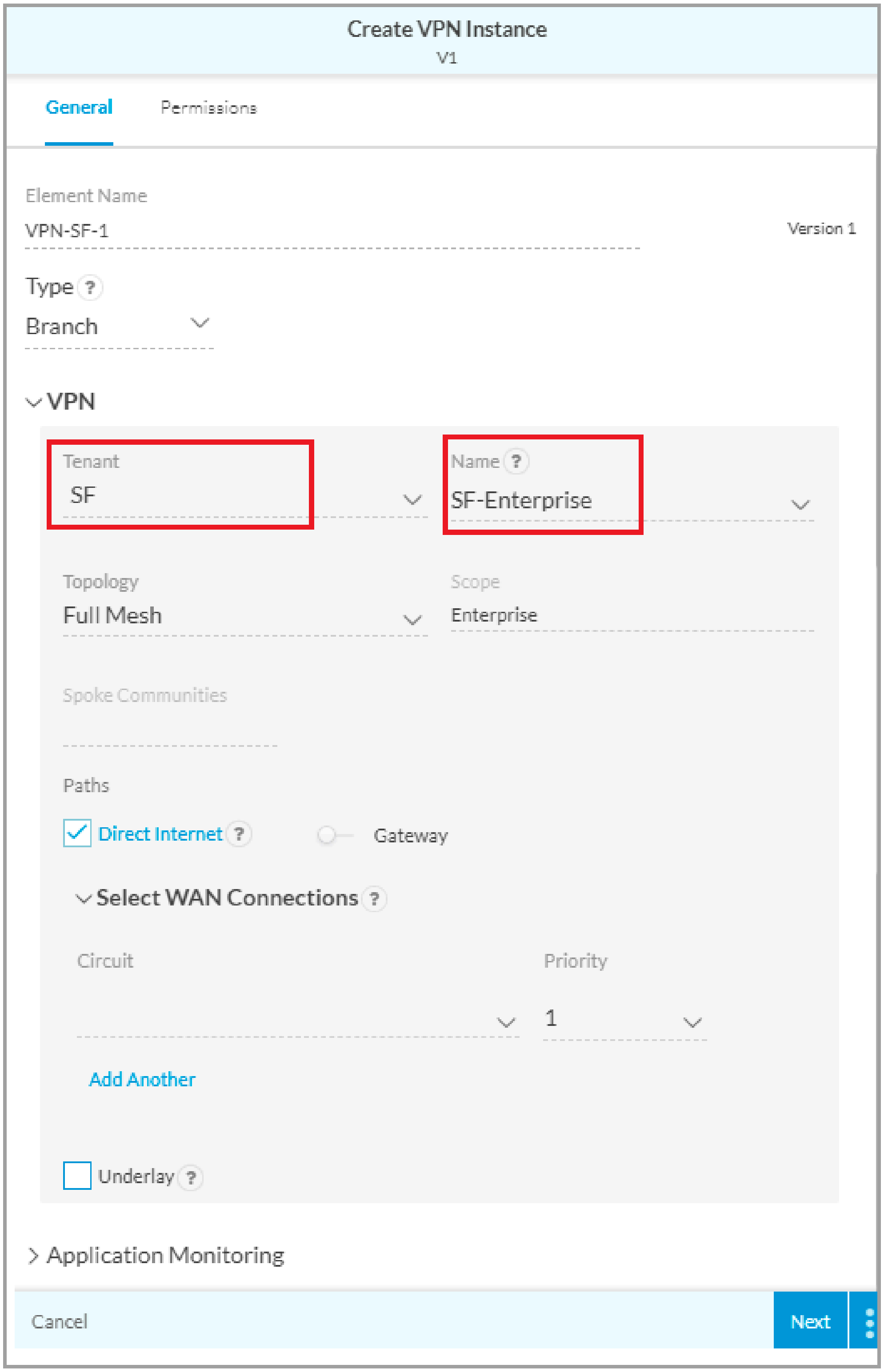
Tags
Press Enter to add

f. Click Next.

g. In the VPN Instances tab, click Add VPN Instance > Create New. To select existing VPN instances, click Choose VPN Instance.



h. Select Create VPN Instance > General.



Element Name
VPN-SF-1
Version 1

Type ?
Branch

VPN

Tenant
SF

Name ?
SF-Enterprise

Topology
Full Mesh

Scope
Enterprise

Spoke Communities

Paths
☑ Direct Internet ?
○ Gateway

Select WAN Connections ?

Circuit
Priority
1

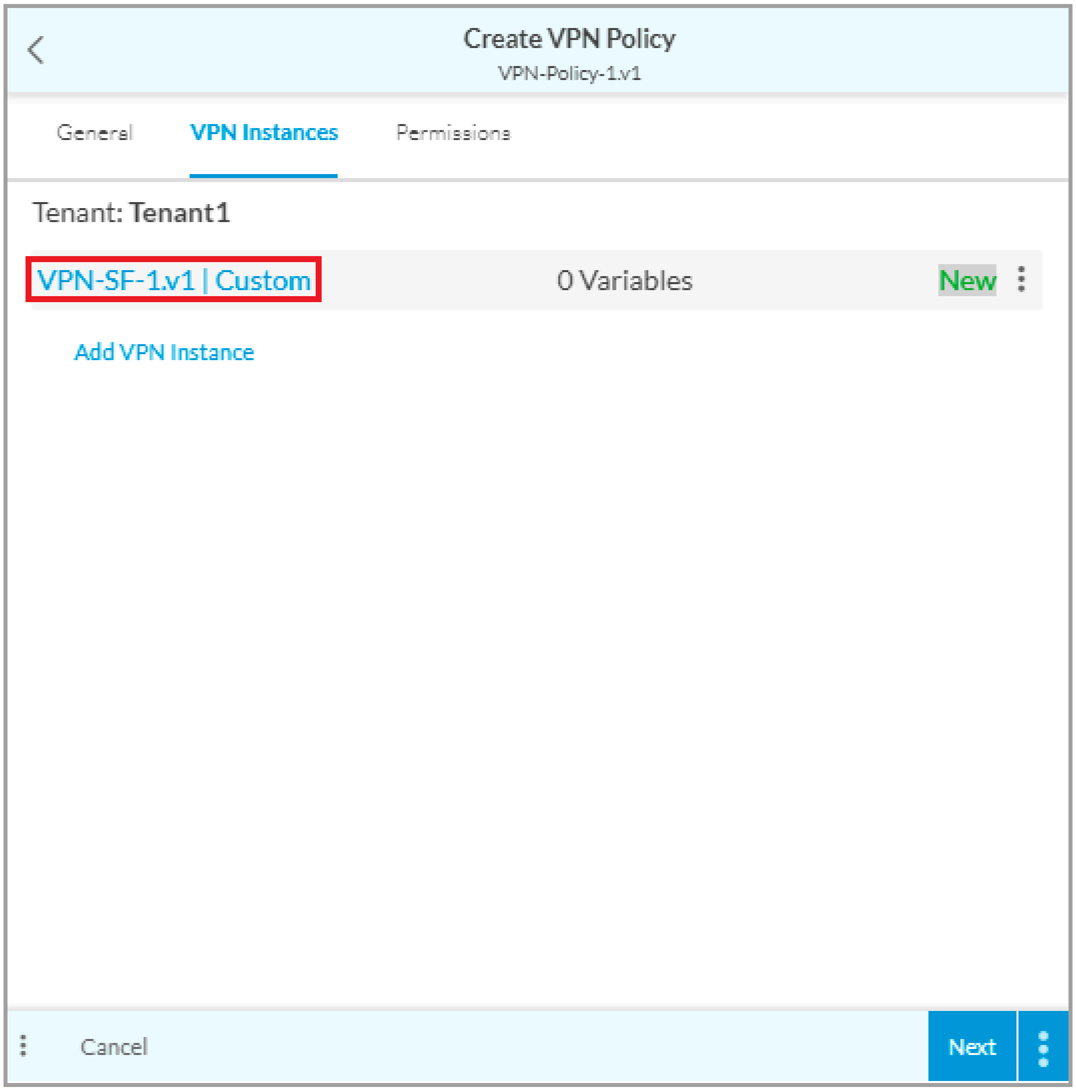
□ Underlay ?

i. Enter a name for the VPN instance for the tenant.
ii. Under VPN, select the subtenant for which to create VPN instance.
iii. Select the name of the VPN connection. The VPN connection of the subtenant selected is displayed by

default.

iv. Enter other required information.

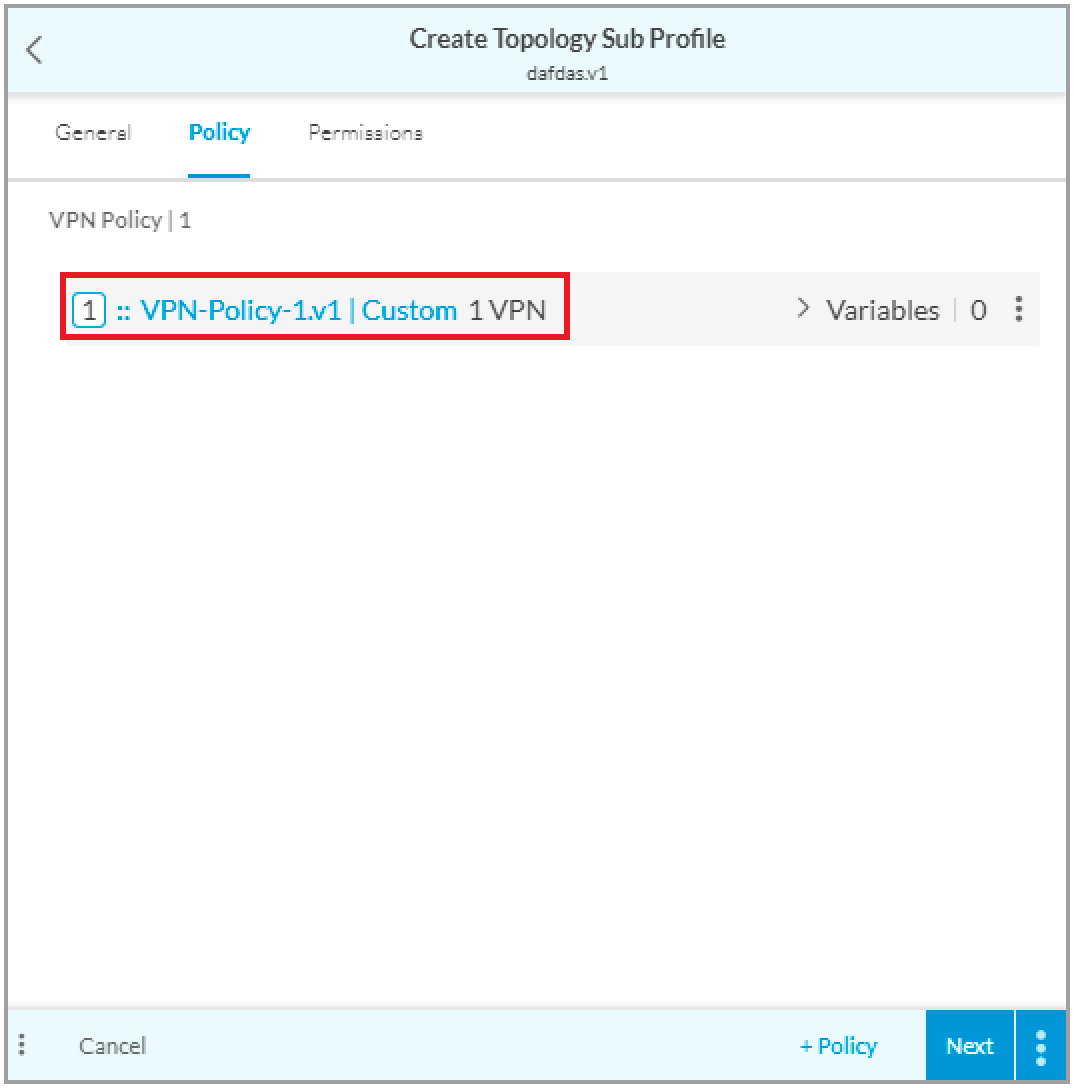
v. Click Next and save the VPN instance. The VPN instance displays in the VPN Instances screen.



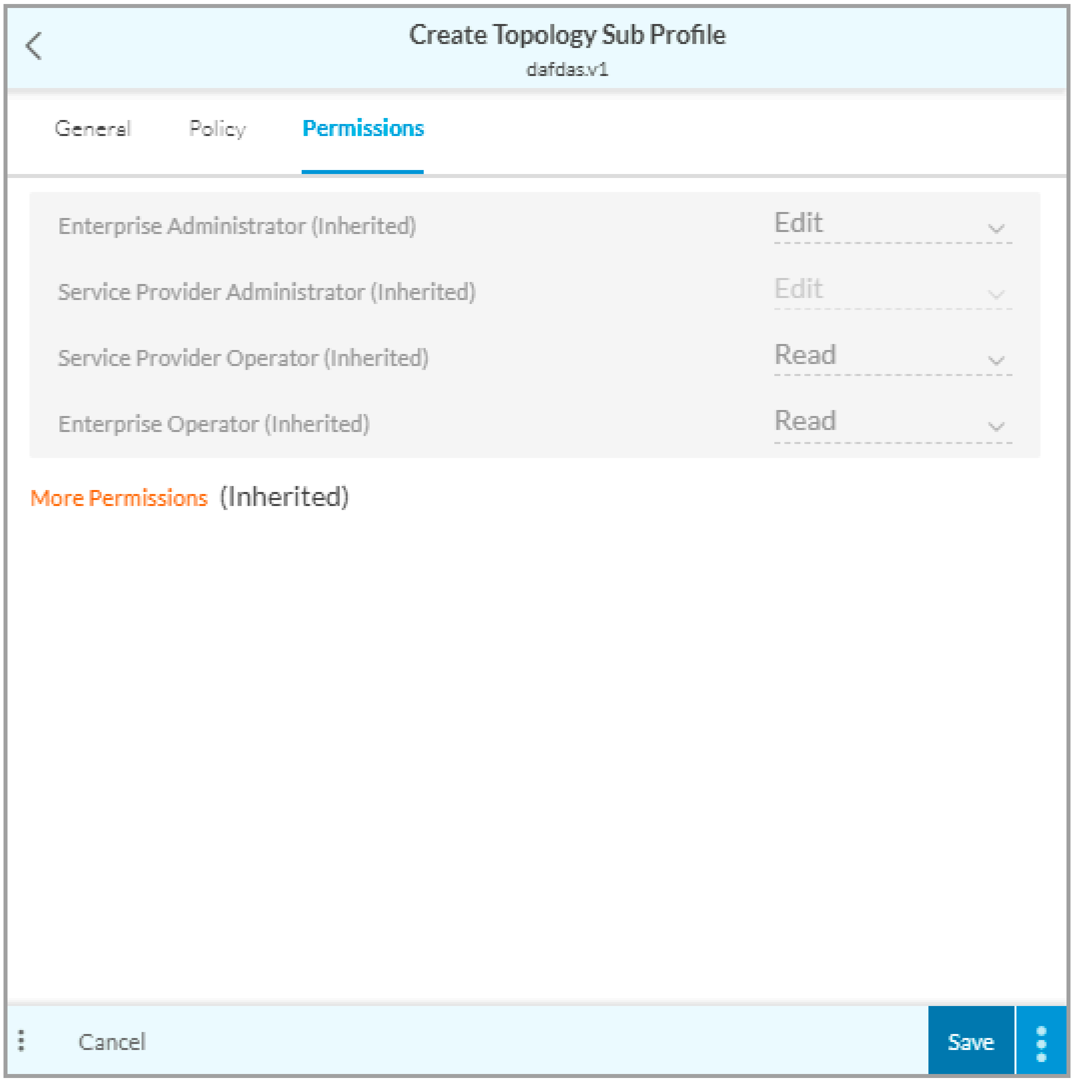
vi. Repeat this step for all subtenant VPNs.

i. Click Next. In the Permissions tab, set the permissions.

j. Save the VPN Policy. The VPN policy displays in the Policy tab.



k. Click Next. In the Permissions tab, set the permissions as required and then save the Topology subprofile.



Create Topology Sub Profile

dafdas.v1

Enterprise Administrator (Inherited)	Edit
Service Provider Administrator (Inherited)	Edit
Service Provider Operator (Inherited)	Read
Enterprise Operator (Inherited)	Read

More Permissions (Inherited)

4. Deploy the appliance associated to the standard master profile. When you publish, Concerto creates a subtenant appliance for each of the subtenants. For more information, see Concerto Deploy Lifecycle Overview.

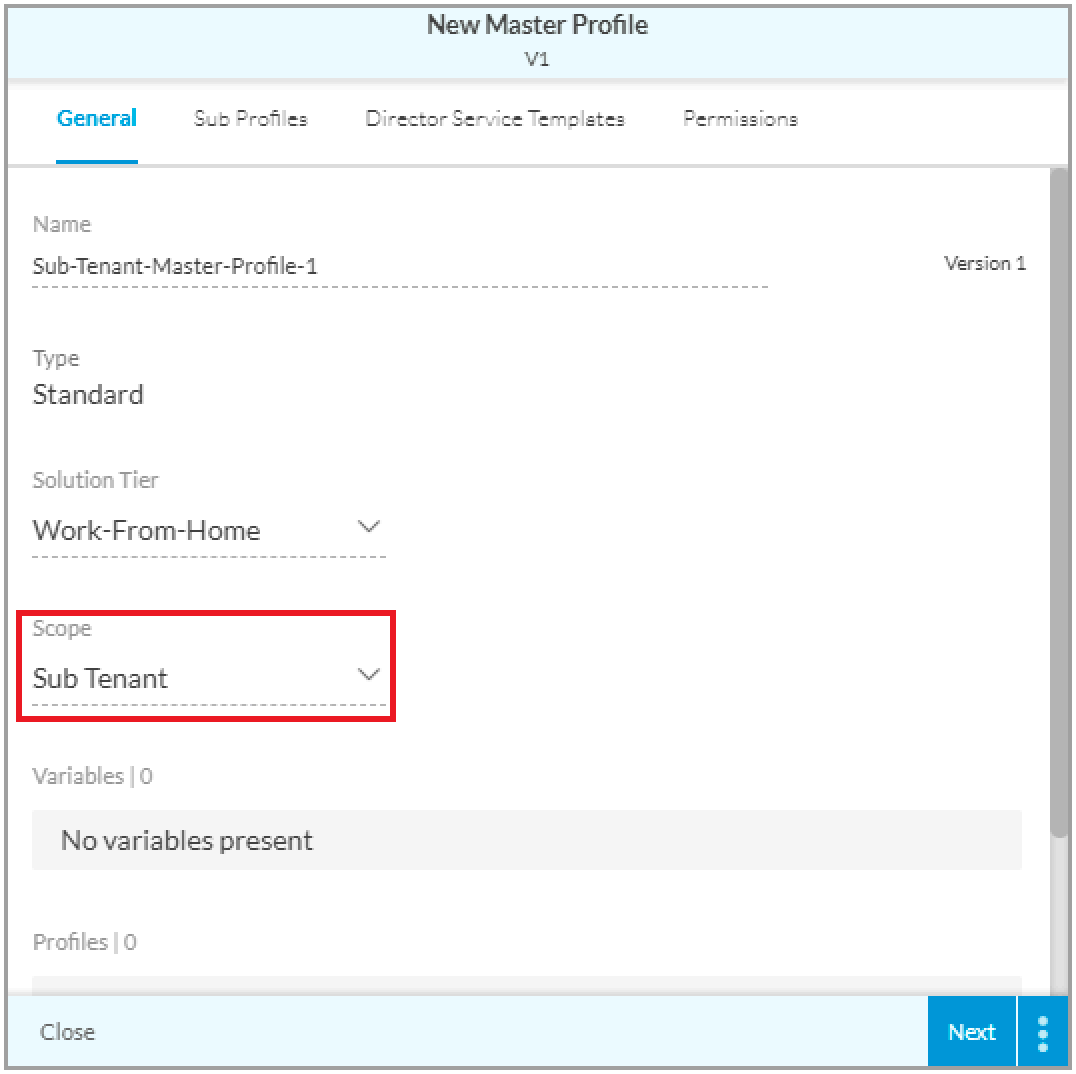
Configure a Subtenant Standard Master Profile

For Releases 11.2.1 and later.

You can use subtenant standard master profile to configure services such as security, traffic steering, and application QoS for a subtenant. You can create application and security subprofiles only for a standard master profile.

To configure a subtenant standard master profile:

1. Go to New Master Profile > General.



New Master Profile
V1

Name
Sub-Tenant-Master-Profile-1
Version 1

Type
Standard

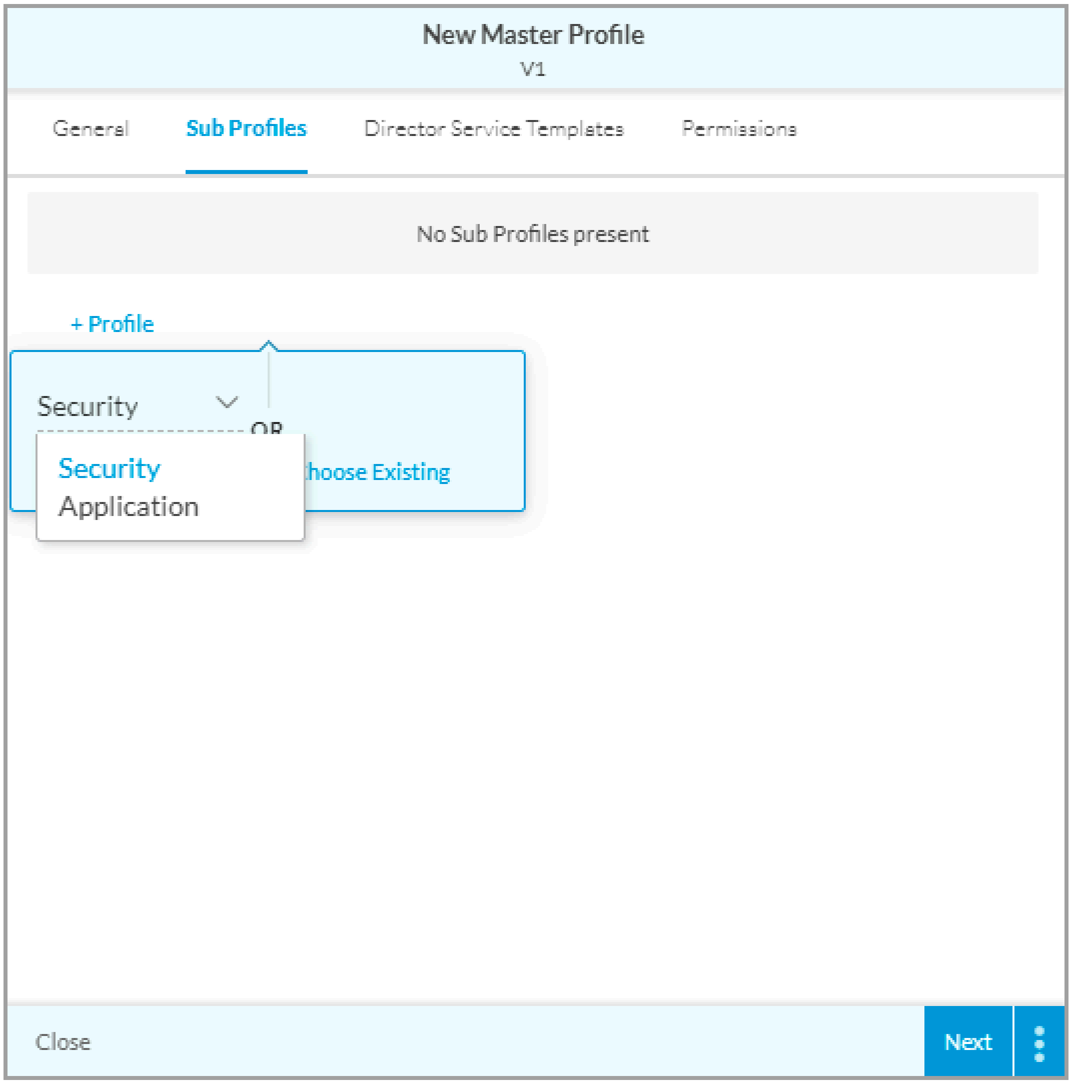
Solution Tier
Work-From-Home

Scope
Sub Tenant

Variables | 0
No variables present

Profiles | 0

2. Enter a name for the profile.
3. Select the solution tier.
4. In the Scope field, select subtenant.
5. Click Next.
6. In the Subprofiles tab, click + Profile, select Application or Security, and then click Create New Profile. Application and Security are the only subprofile options available for a subtenant standard master profile.



7. Enter other required information.
8. Save the subtenant standard master profile.
9. Deploy the appliance associated to the standard master profile. For more information, see Concerto Deploy Lifecycle Overview.

Supported Software Information

Releases 10.2.1 and later support all content described in this article, except:

- Release 11.2.1 adds support for a new default basic master subtenant profile, Default-Basic-MP-Sub-Tenant, and for multitenancy configuration in the Default-Active-Active and Default-Basic-MP basic master profiles.

Additional Information

Configuration Hierarchies
Configure Profile Elements
Configure QoS Policies and Rules
Configure TCP Optimizations
Configure Traffic-Steering Policies and Rules