Configure Management Servers

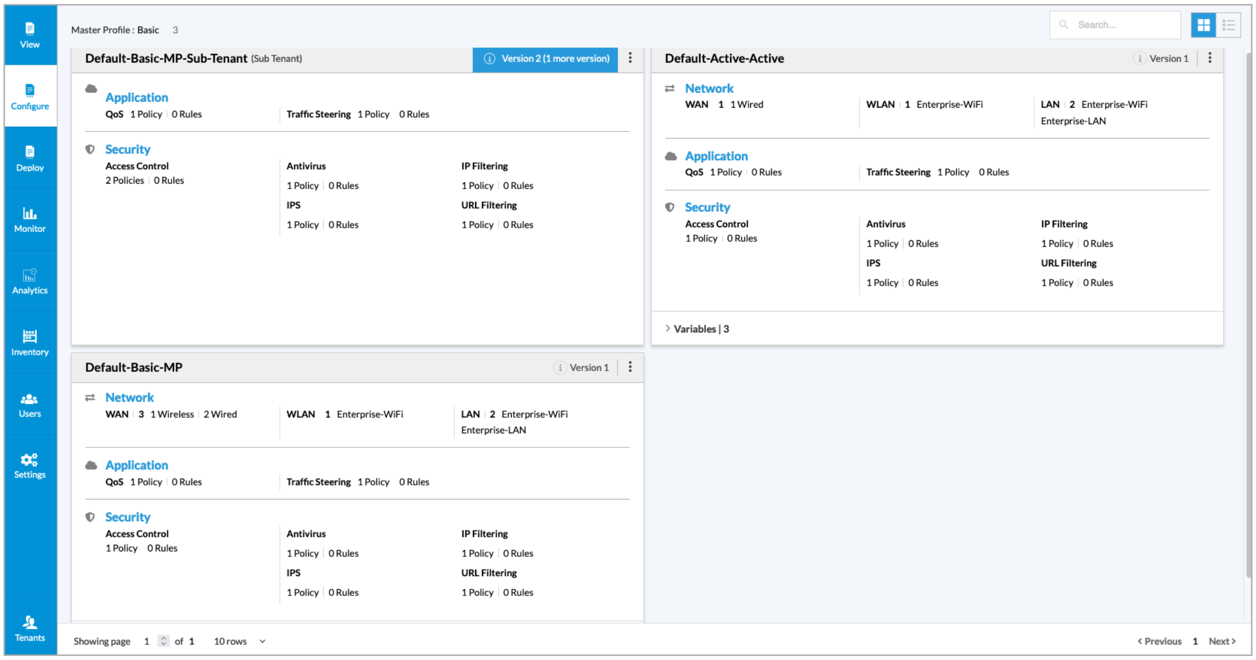
For supported software information, click here.

You can configure various network management servers, including DNS, LDAP, NTP, SNMP, syslog, and TACACS+ servers. The subprofile called System contains global policies that are related to the system. You can configure only one management server policy in the System subprofile, but the policy can contain one or more management servers.

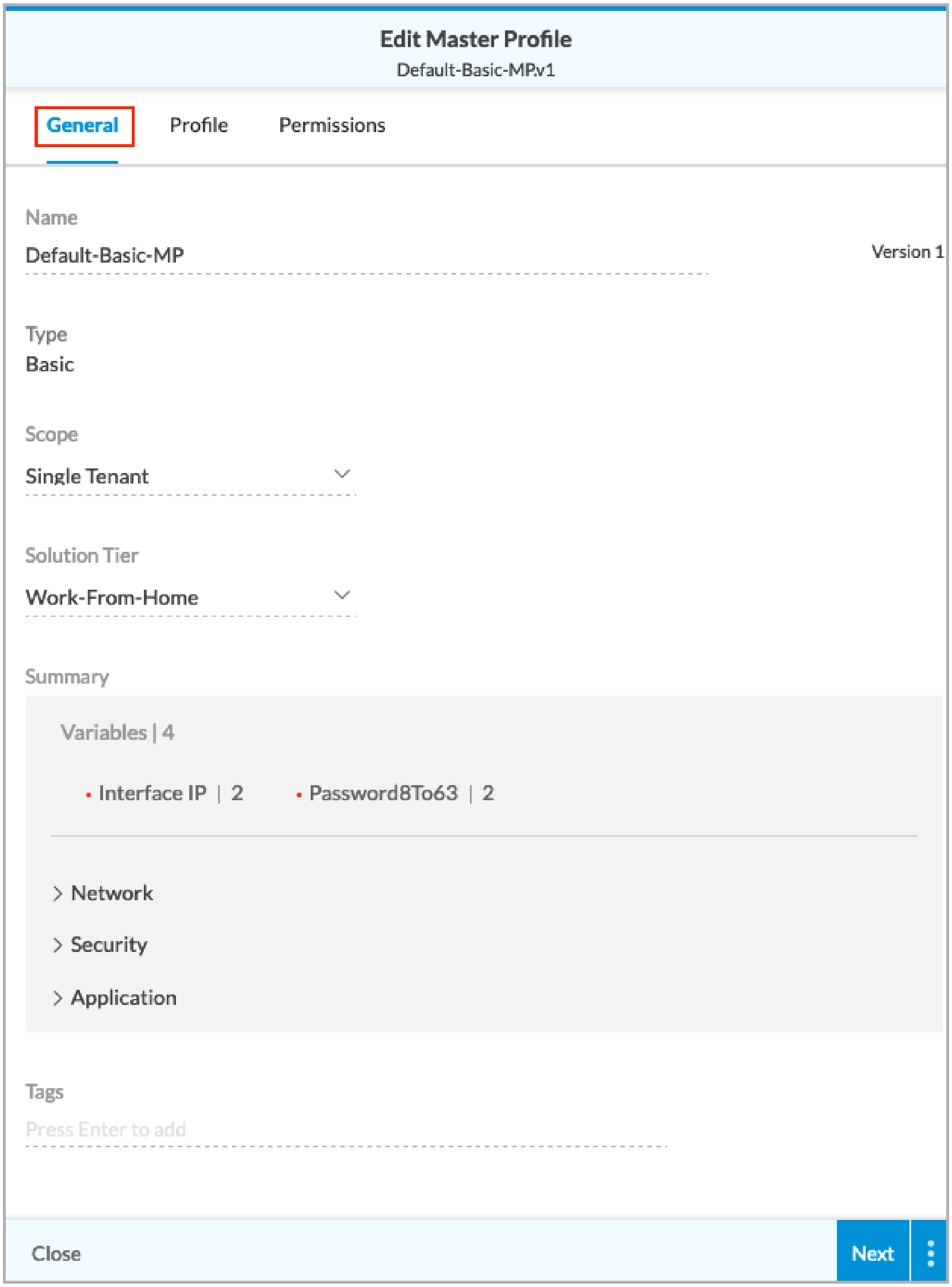
Configure a Profile or Profile Element To Use for Management Servers

To begin configuring management servers, configure a basic master profile, a standard master profile, or a profile element:

1. Go to the Configuration lifecycle screen.
    a. To configure a management server at the basic master profile level:
        i. Select Profiles > Master Profiles > Basic.


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

ii. Click on the Basic master profile to which you want to add a new policy for management servers. The Edit Master Profile screen displays.



Edit Master Profile

Default-Basic-MP.v1

Name

Default-Basic-MP

Version 1

Type

Basic

Scope

Single Tenant

Solution Tier

Work-From-Home

Summary

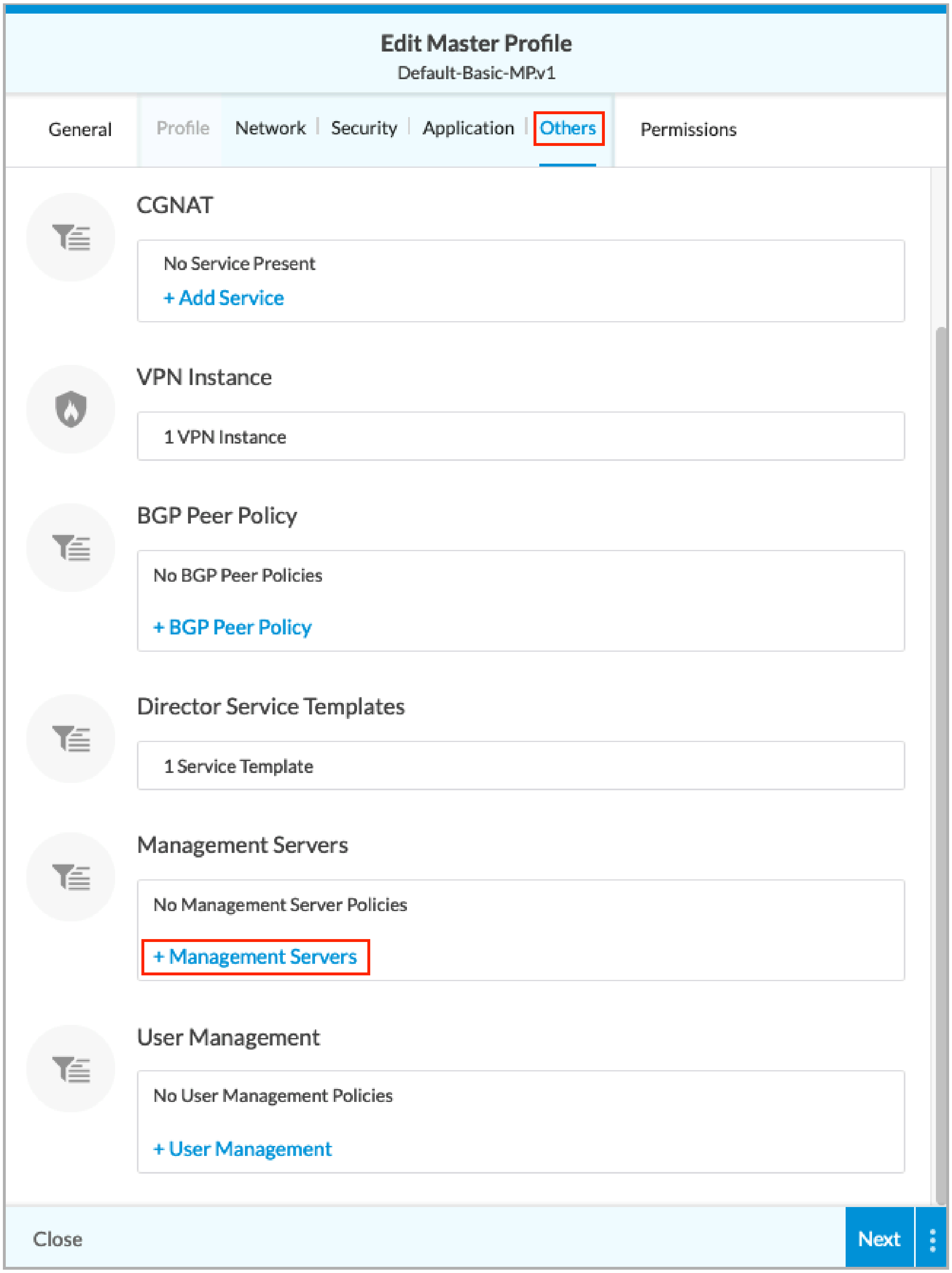
Variables | 4

- Interface IP | 2
- Password8To63 | 2

Tags

Press Enter to add

iii. Select the Profile tab, and then select Others in the top menu bar. The following screen displays.



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

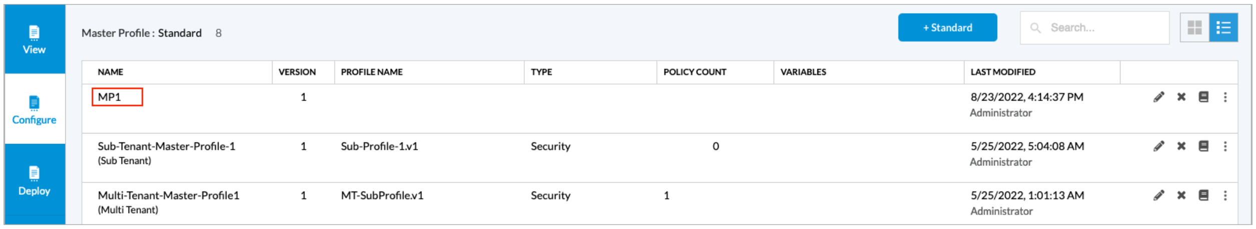
User Management

No User Management Policies

iv. Click + Management Servers. A popup window prompts you to create a new policy or choose an existing policy. Click Create New Policy to create a policy that includes one or more management servers. The Create Management Servers screen displays. Go to Step 2.

b. To configure a management server at the standard master profile level:

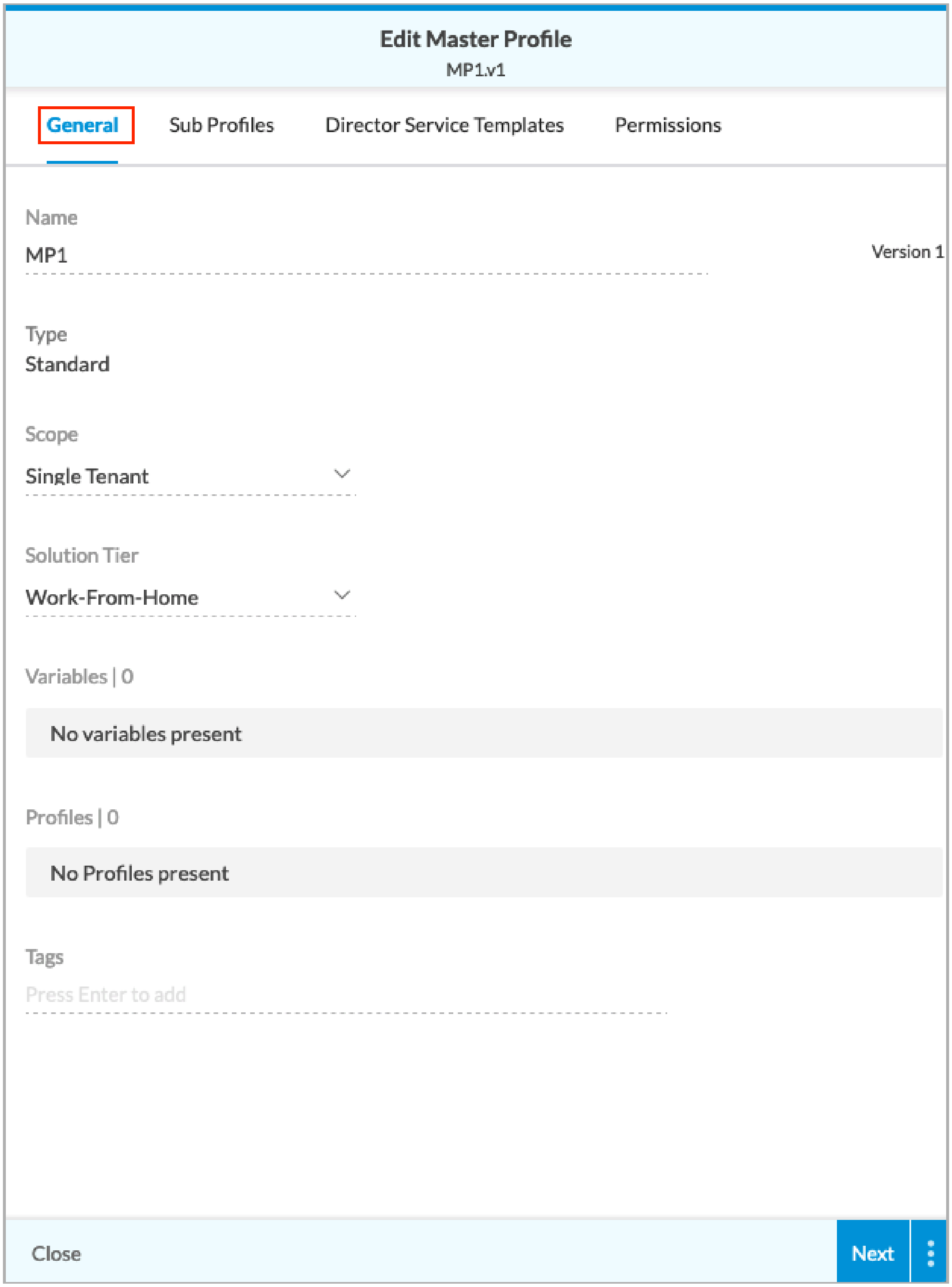
    i. Go to Configure > Profiles > Master Profiles > Standard.



Master Profile : Standard 8

NAME	VERSION	PROFILE NAME	TYPE	POLICY COUNT	VARIABLES	LAST MODIFIED
MP1	1					8/23/2022, 4:14:37 PM Administrator
Sub-Tenant-Master-Profile-1 (Sub Tenant)	1	Sub-Profile-1.v1	Security	0		5/25/2022, 5:04:08 AM Administrator
Multi-Tenant-Master-Profile1 (Multi Tenant)	1	MT-SubProfile.v1	Security	1		5/25/2022, 1:01:13 AM Administrator

    ii. Click the Standard master profile to which you will add a management server. The Edit Master Profile screen displays.



Edit Master Profile

MP1.v1

Name

MP1

Version 1

Type

Standard

Scope

Single Tenant

Solution Tier

Work-From-Home

Variables | 0

No variables present

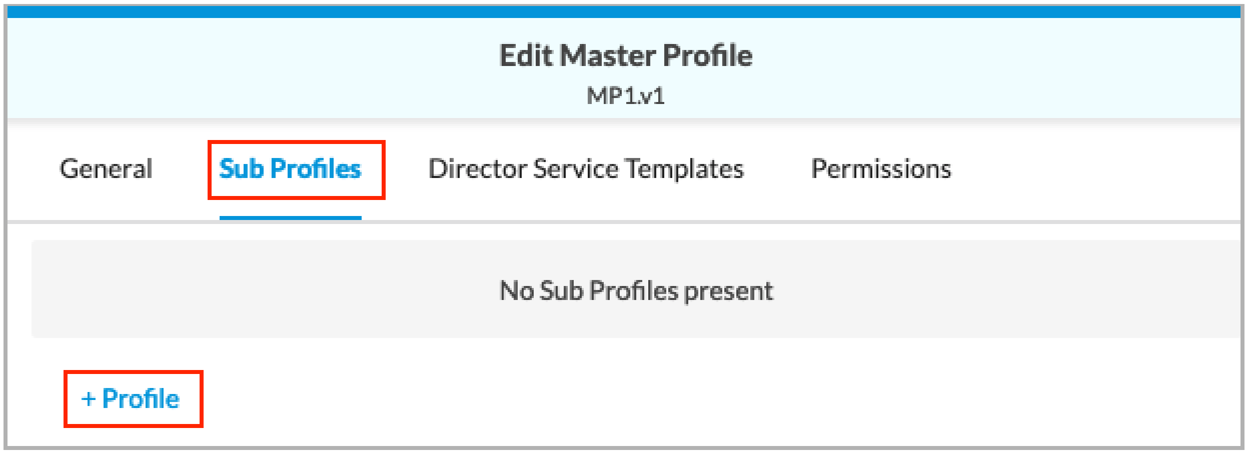
Profiles | 0

No Profiles present

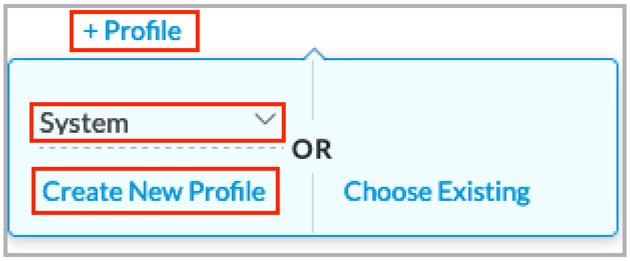
Tags

Press Enter to add

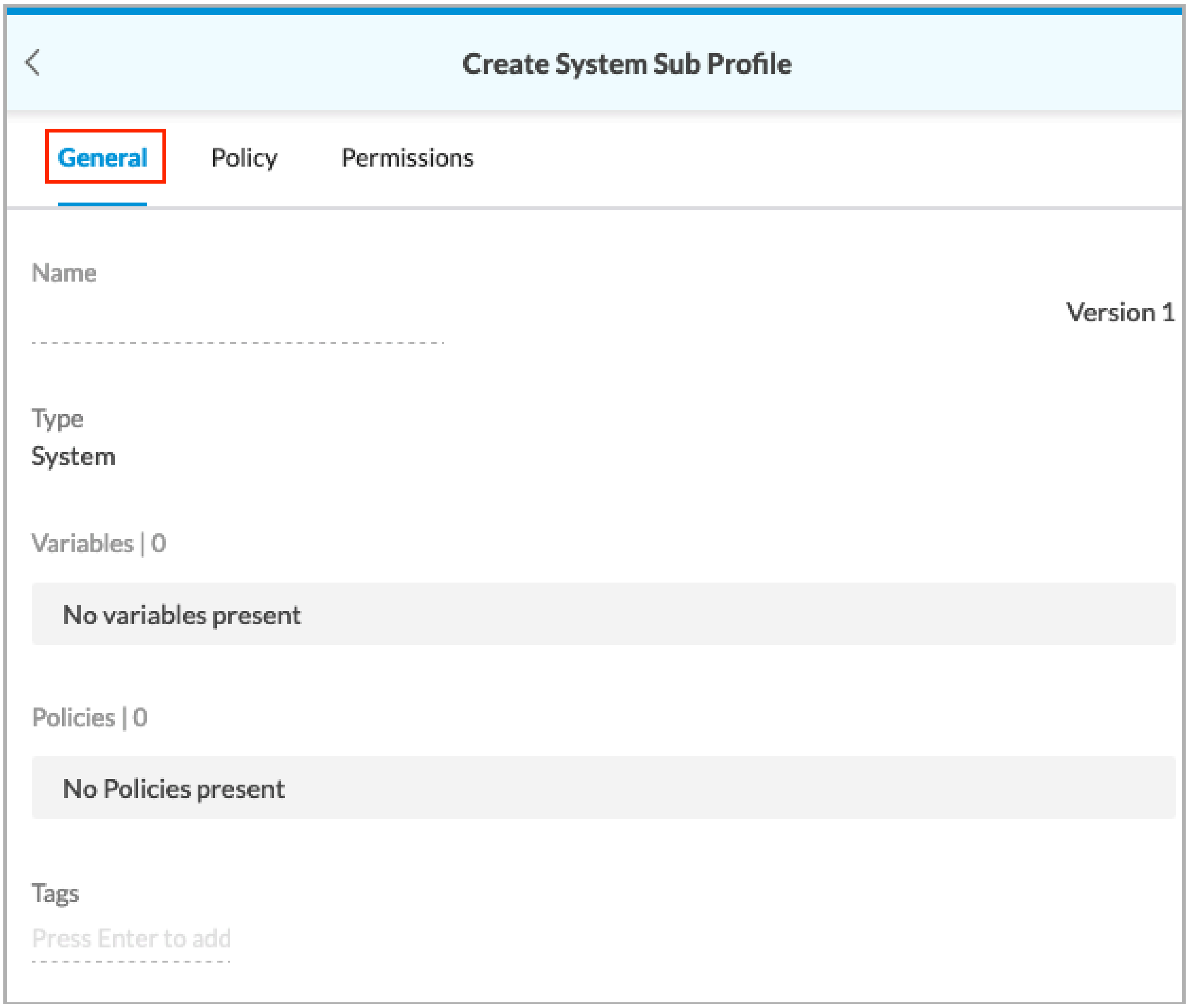
iii. Click the Sub Profiles tab, then click + Profile to add a sub-profile for management servers.



Select System from the drop-down list, and then click Create New Profile. The Create System Sub Profile screen displays.



iv. In the General tab, enter a name for the new sub-profile, then click the Policy tab.



Name

Version 1

Type
System

Variables | 0

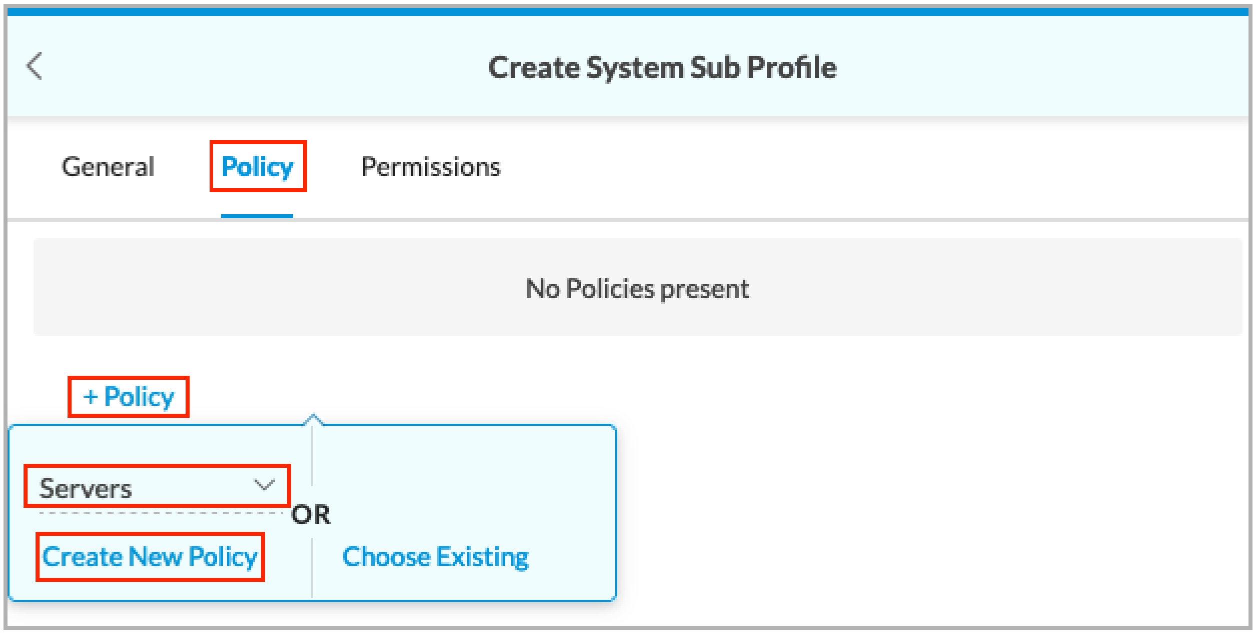
No variables present

Policies | 0

No Policies present

Tags
Press Enter to add

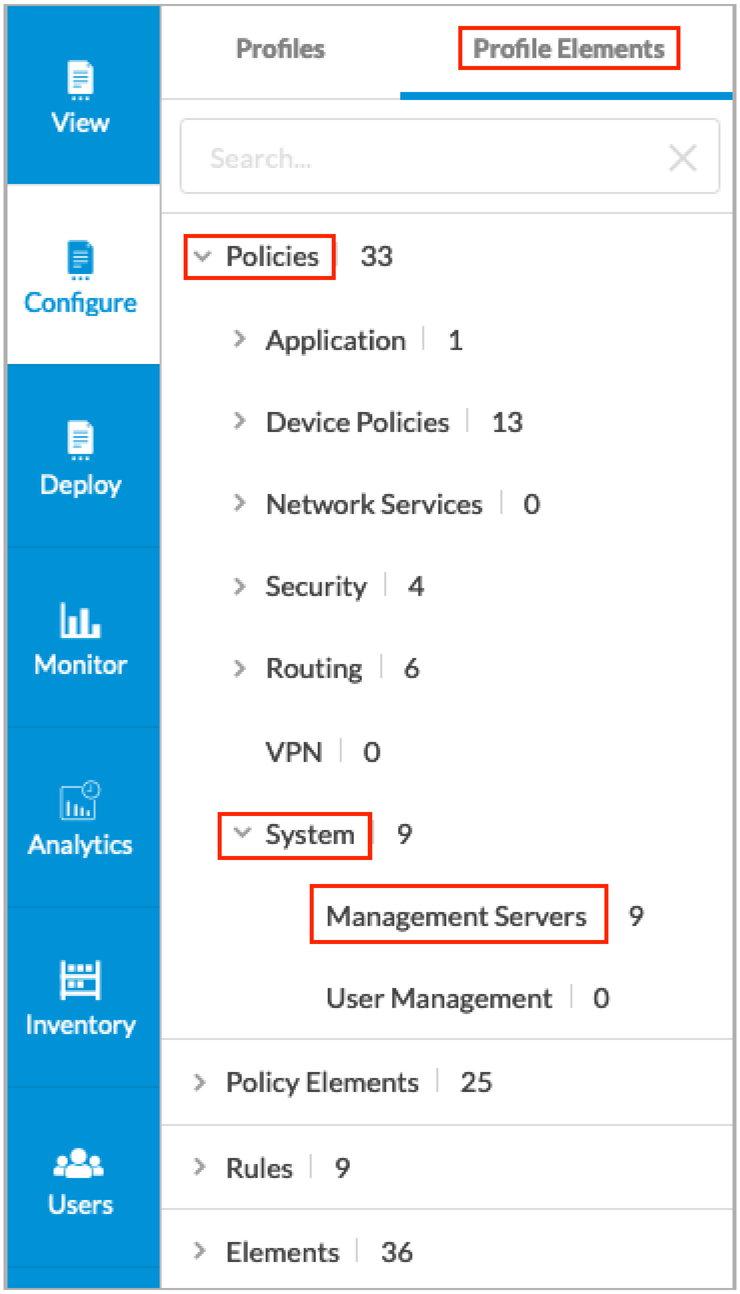
v. In the Policy tab, do the following:
   A. Click + Policy.
   B. Select Servers from the drop-down list.
   C. Click Create New Policy. The Create Management Servers screen displays.



D. Go to Step 2.

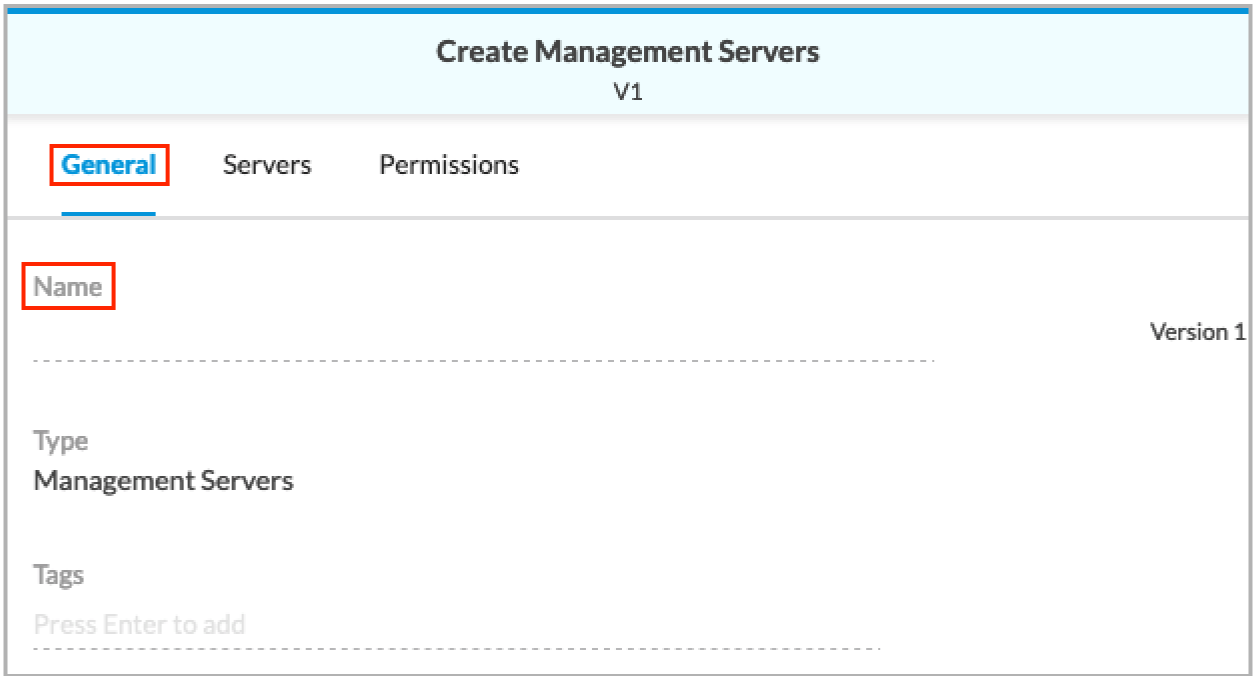
c. To configure a management server at the Profile Elements level:

i. Go to Configure > Profile Elements > Policies > System > Management Servers.

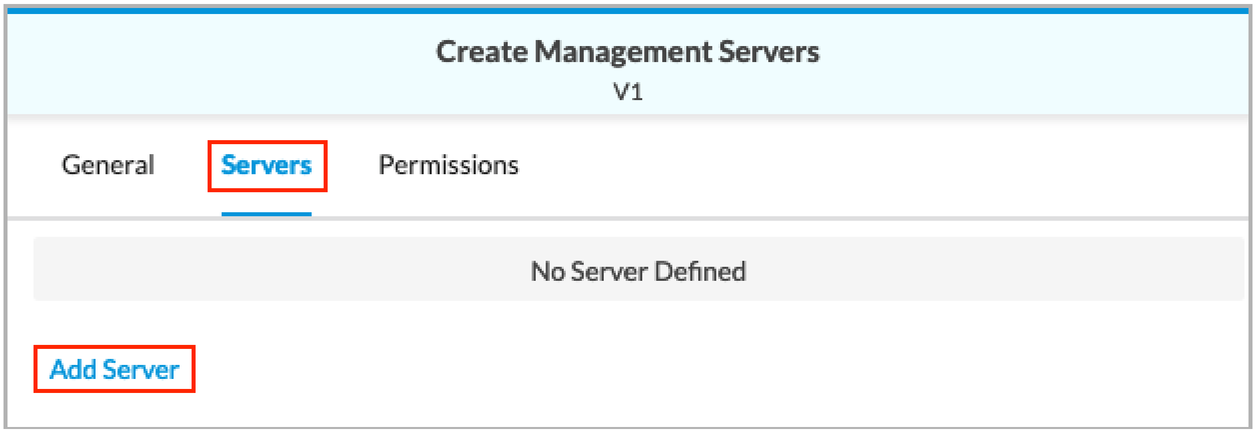


ii. In the Management Servers screen, click + Management Servers. The Create Management Servers screen displays.

2. In the Create Management Servers > General tab, enter a name for the new management server policy.

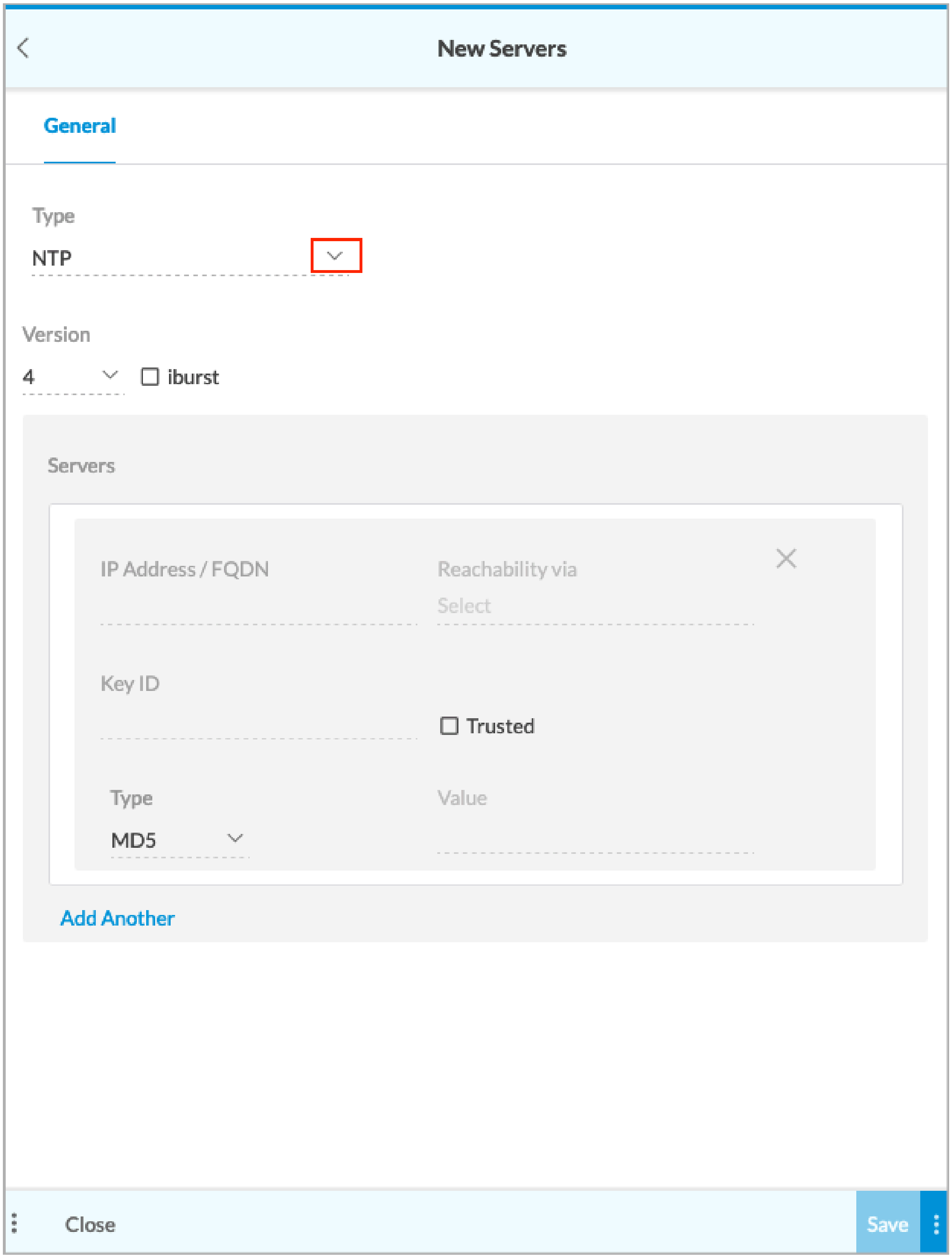


3. Select the Servers tab, then click Add Server. The New Servers screen displays.



4. In the Type field, select the management server type:
   - DNS (for Releases 11.3.1 and later)
   - LDAP
   - NTP
   - RADIUS
   - SNMP
   - Syslog
   - TACACS+

   Note: It is recommended that you configure either a TACACS+ or a RADIUS server, but not both.



Type
NTP

Version
4 □ iburst

Servers

IP Address / FQDN

Reachability via
Select

Key ID

□ Trusted

Type
MD5

Value

5. Configure each management server type, as described in the following sections.

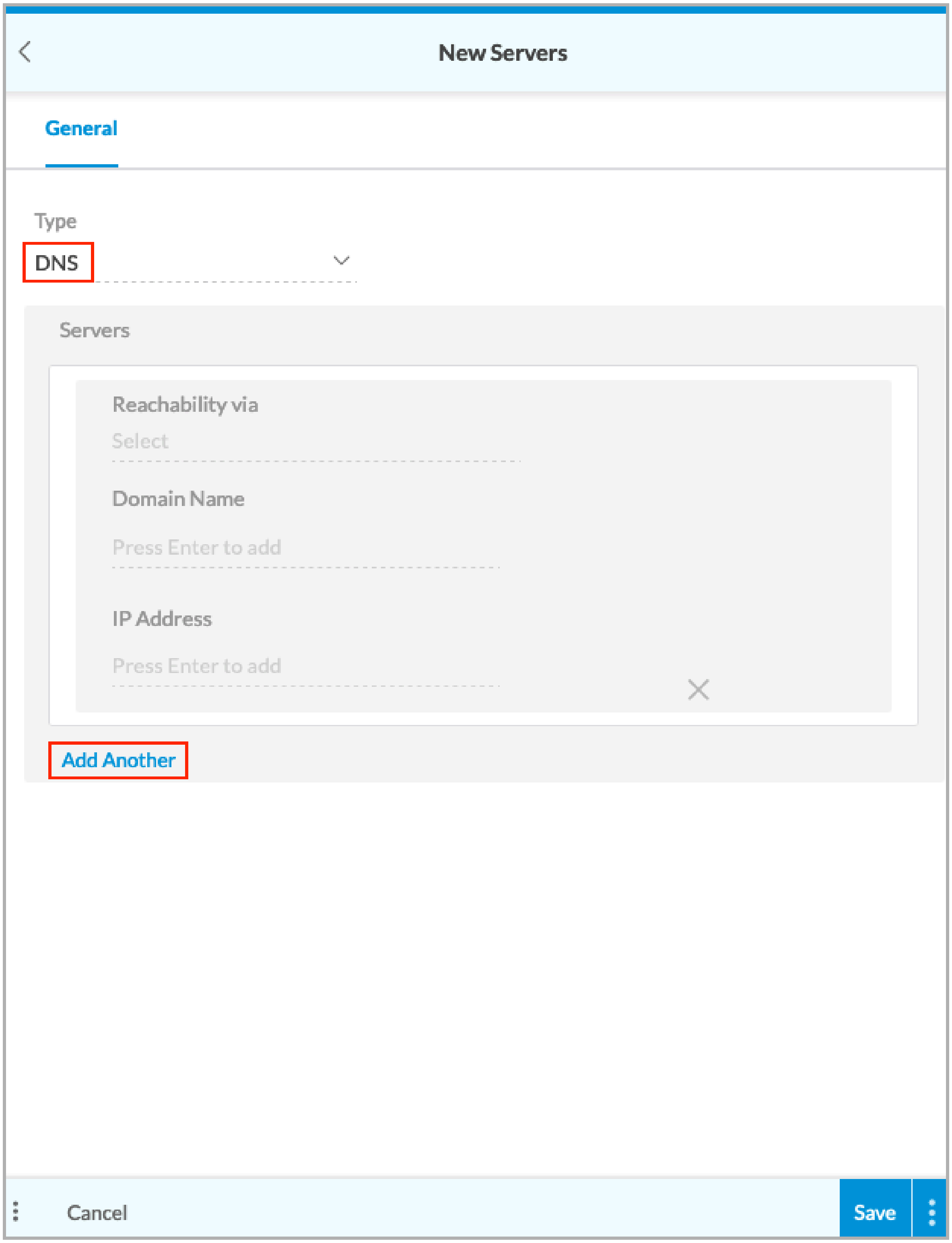
Configure a DNS Server

For Releases 11.3.1 and later.

You can configure DNS servers so that they can be reached when they are located behind Controller nodes in a customer's data center. To do this, you use the overlay network in the control virtual router (VR). Configuring a DNS server in this way allows you to configure redundant DHCP forwarders.

To configure a DNS servers:

1. In the Type field, select DNS.



Type: DNS

Servers

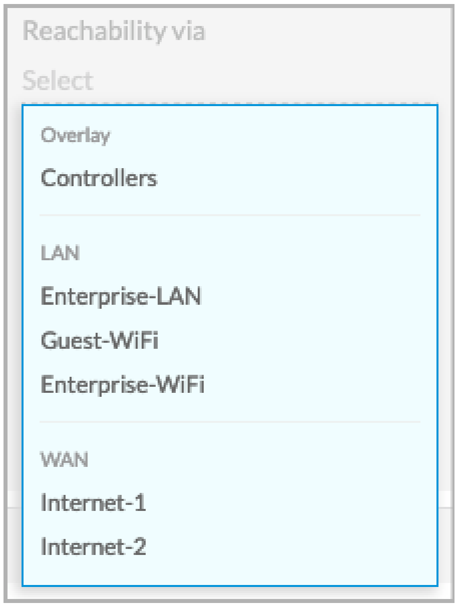
Reachability via: Select

Domain Name: Press Enter to add

IP Address: Press Enter to add

Add Another

2. Enter information for the following fields.

Field	Description
Reachability via	Select the network to use for reachability between the controller and the DNS server.  Reachability via Select Overlay Controllers LAN Enterprise-LAN Guest-WiFi Enterprise-WiFi WAN Internet-1 Internet-2
Domain Name	Enter the name of the domain in which the DNS server resides, and then click Enter to add the domain name. You can enter multiple domain names.
IP Address (Required)	Enter the IP address of the DNS server, and then click Enter to add the IP address. You can enter multiple IP addresses.

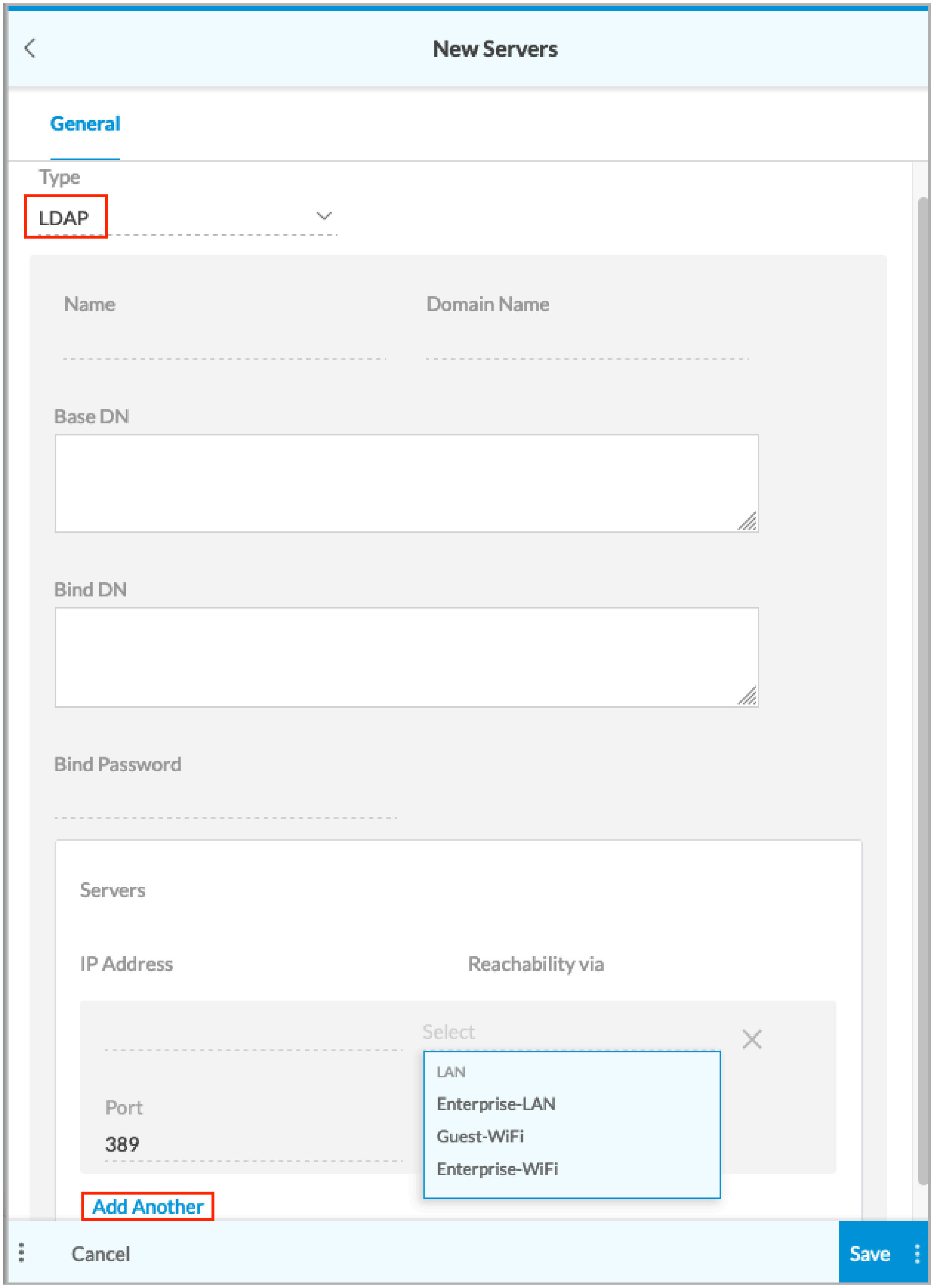
3. Click Add Another to configure additional DNS servers.
4. Click Save.

Configure an LDAP Server

The Lightweight Directory Access Protocol (LDAP) is a standards-based, client-server protocol that allows clients to access an LDAP server to perform a variety of operations, inclucing storing and retrieving data (such as user names, passwords, and email addresses), searching for data matching a given set of criteria, and authenticating clients.

To configure an LDAP server:

1. In the Type field, select LDAP.



Type
LDAP

Port
389

2. Enter information for the following fields.

Field	Description
Name	Enter a name for the LDAP server.
Domain Name	Enter the domain name in which the LDAP server resides.
Base DN	Enter the base DN of the LDAP directory location.
Bind DN	Enter the bind distinguished name (DN) authentication credentials for binding to the LDAP tree.
Bind Password	Enter the bind password.
Servers (Group of Fields)	
◦ IP Address	Enter the IP address of the LDAP server.
◦ Reachability via	Select the network to use for reachability between the controllerand the LDAP server.
◦ Port	Enter the number of the listening port on the LDAP server. This is the port number used to communicate with the LDAP directory service. *Range*: 1 through 65535 *Default*: 389

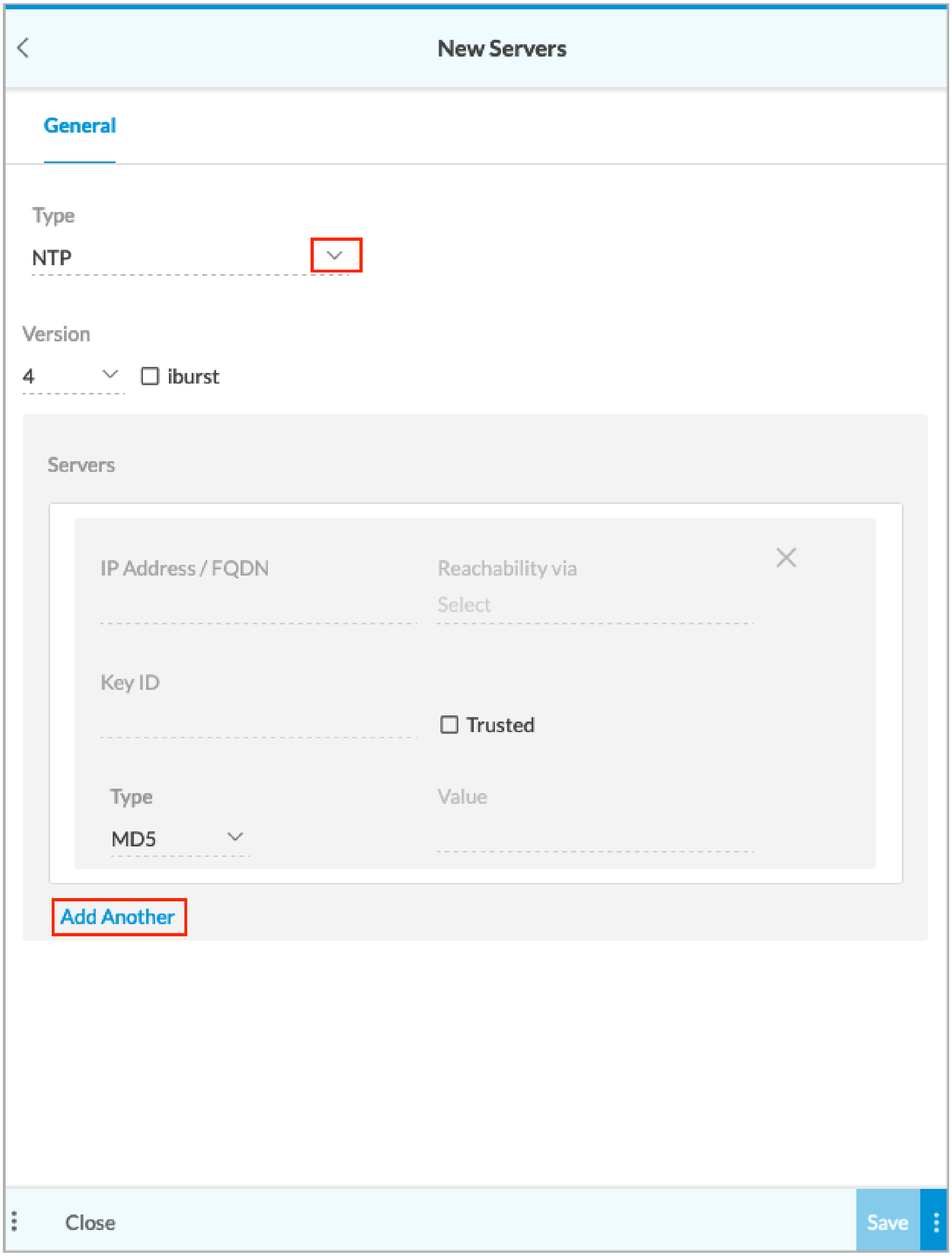
3. Click Add Another to configure additional LDAP servers.
4. Click Save.

Configure an NTP Server

The Network Time Protocol (NTP) synchronizes the clocks running on different computer systems in packet-switched, variable-latency data networks. NTP synchronizes all participating systems to within a few milliseconds of Coordinated Universal Time (UTC). NTP obtains its time by polling an authoritative NTP server.

To configure an NTP server:

1. In the Type field, select NTP, then enter information for the following fields.



New Servers

General

Type
NTP

Version
4 □ iburst

Servers

IP Address / FQDN

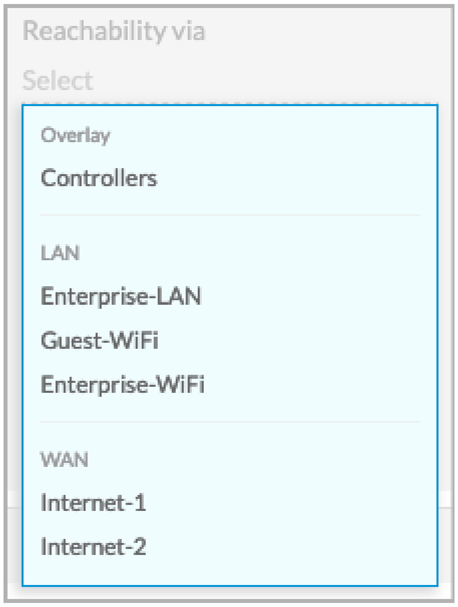
Reachability via
Select

Key ID

□ Trusted

Type
MD5

Value

Field	Description
Version	Select the NTP version.
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. When the server does not respond, packets are sent every 16 seconds. When the server responds, packets are sent every 2 seconds.
Servers (Group of Fields)	
◦ IP Address/FQDN	Enter the IP address or FQDN of the NTP server.
◦ Reachability via	Select the network to use for reachability between the controller and the NTP server.  Reachability via Select Overlay Controllers LAN Enterprise-LAN Guest-WiFi Enterprise-WiFi WAN Internet-1 Internet-2
◦ Key ID	Enter an ID for the authentication key. *Range*: 0 through 4294967295 *Default*: None
◦ Trusted	Click to mark the key as trusted.

Field	Description
◦ Type	Select the key type: ◦ MD5
◦ Value	Enter an MD5 key value, which must be 32 characters .

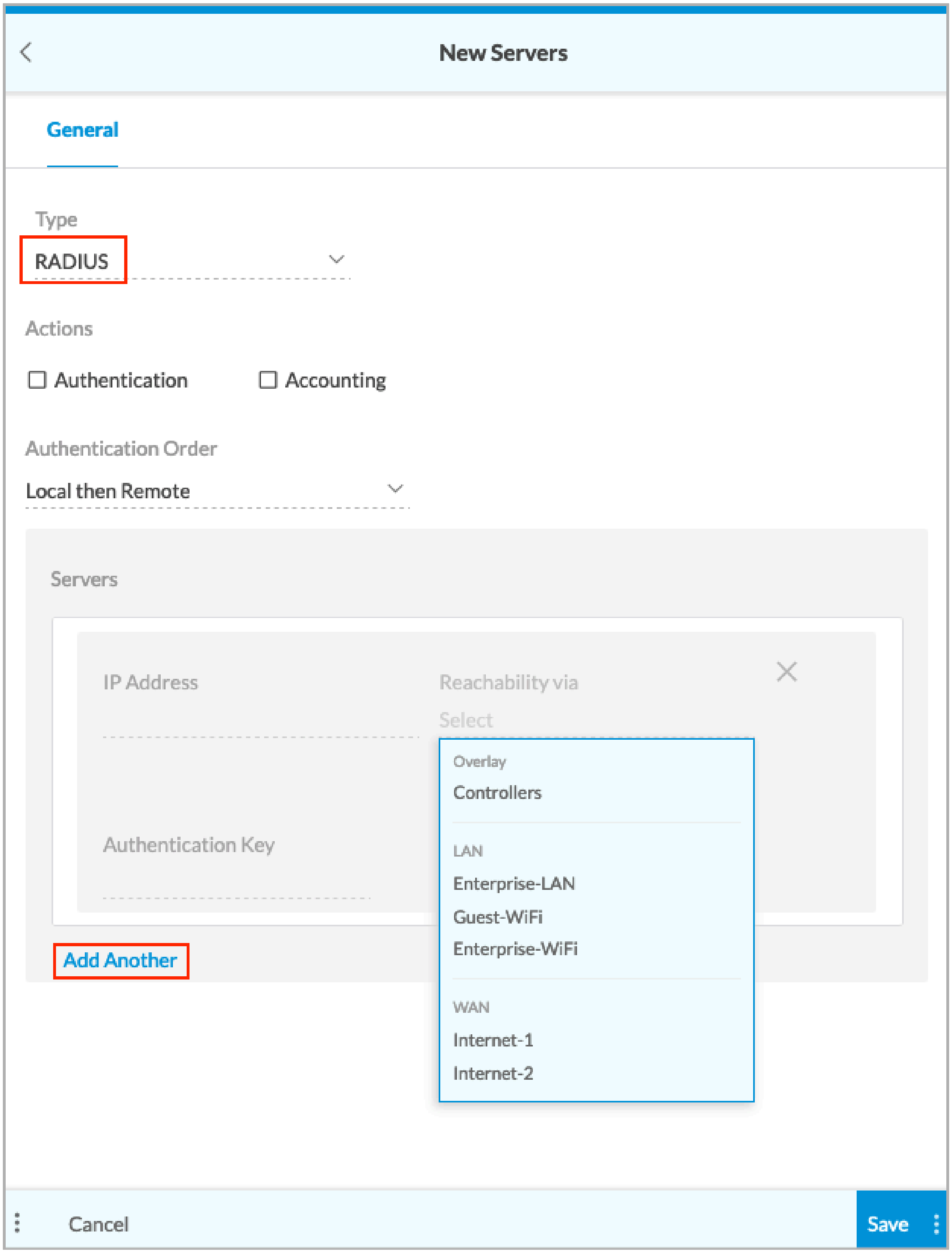
2. Click Add Another to configure additional NTP servers. If you require more than one NTP server, configure them here. You cannot add additional NTP servers from other screens.
3. Click Save.

Configure a RADIUS Server

RADIUS is a distributed client-server system that secures networks against unauthorized access. A RADIUS server provides an external database that you can use to authenticate users before allowing them to access a network, a device, or related services.

To configure a RADIUS server:

1. In the Type field, select RADIUS. It is recommended that you configure either a TACACS+ server or a RADIUS server, but not both.



New Servers

General

Type

RADIUS

Actions

□ Authentication □ Accounting

Authentication Order

Local then Remote

Servers

IP Address

Reachability via

Select

Authentication Key

2. Enter information for the following fields.

Field	Description
Actions (Group of Fields)	
◦ Authentication	Select to enable RADIUS authentication.
◦ Accounting	Select to enable RADIUS accounting.
Authentication Order	Select the authentication order from the drop-down list: ◦ Local-Then-Remote—User is authenticated by checking the local database first, then the remote database. ◦ Remote-Then-Local—User is authenticated by checking the remote database first. If the remote database is unreachable, the local database is then searched. ◦ Remote-Only—User is authenticated by checking the remote database only.
Servers (Group of Fields)	
◦ IP Address	Enter the IP address of the RADIUS server.
◦ Reachability via	Select the network to use for reachability between the controller and the RADIUS server.
◦ Authentication Key	Enter the RADIUS key. The key can consist of both numbers and letters, and it cannot include a hash mark (#) or spaces.

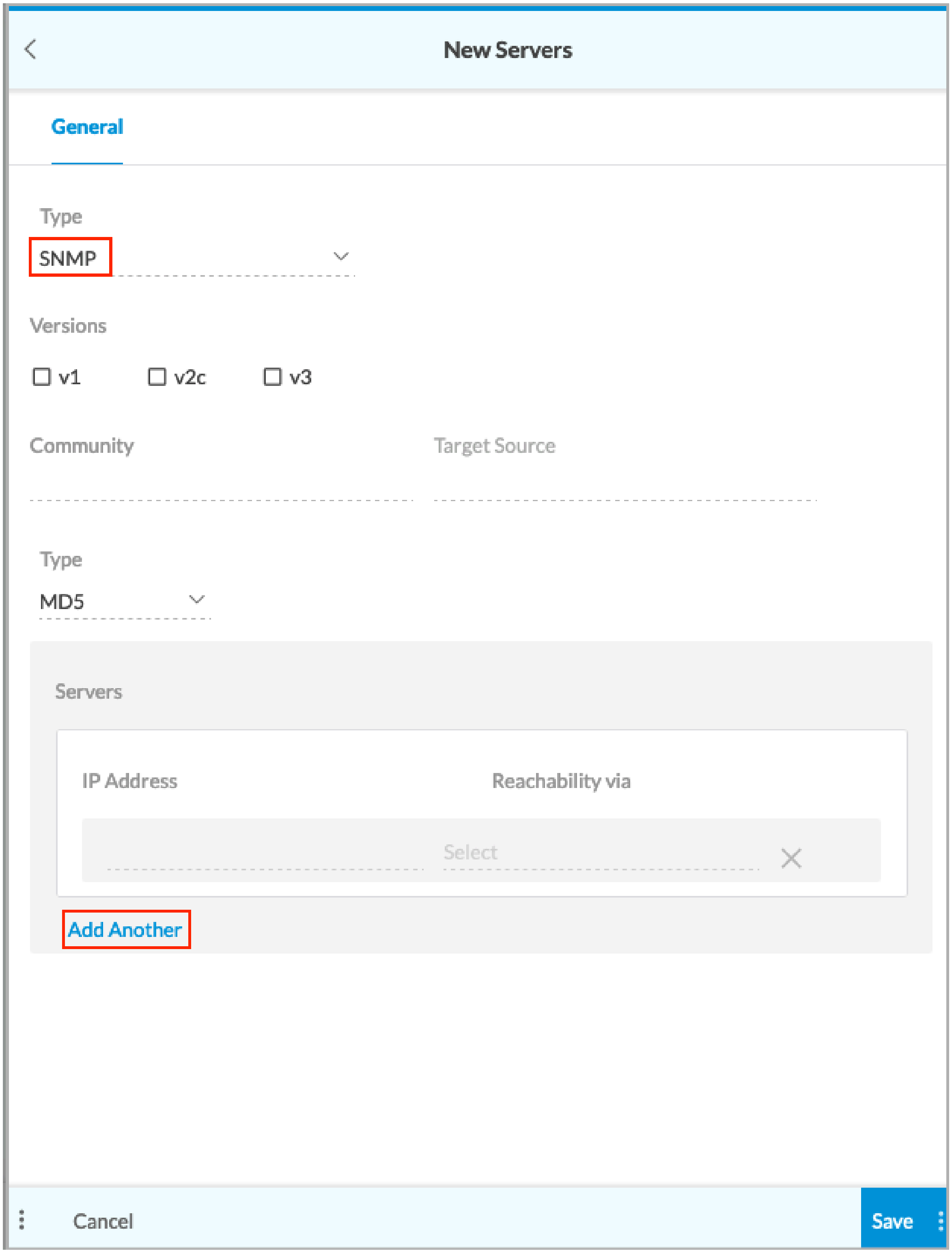
3. Click Add Another to configure additional TACACS+ servers.
4. Click Save.

Configure an SNMP Server

The Simple Network Management Protocol (SNMP) is an open standard networking protocol that is used for managing, monitoring, and organizing data about networking devices on both LANs and WANs.

To configure an SNMP server:

1. In the Type field, select SNMP.


New Servers

General

Type

SNMP

Versions

□ v1 □ v2c □ v3

Community

Target Source

Type

MD5

Servers

IP Address

Reachability via

Select

Add Another

2. Enter information for the following fields.

Field	Description
Versions (Group of Fields)	
◦ v1	Select to enable SNMP version 1.
◦ v2c	Select to enable SNMP version 2c.
◦ v3	Select to enable SNMP version 3.
Community	Enter a community name. A community is a group of devices that SNMP monitors.
Target Source	Enter the IP address of the SNMP manager.
Type	Select the type of authentication protocol: ◦ MD5 ◦ SHA
Servers (Group of Fields)	
◦ IP Address	Enter the IP address of the SNMP server.
◦ Reachability via	Select the network to use for reachability between the controller and the SNMP server.

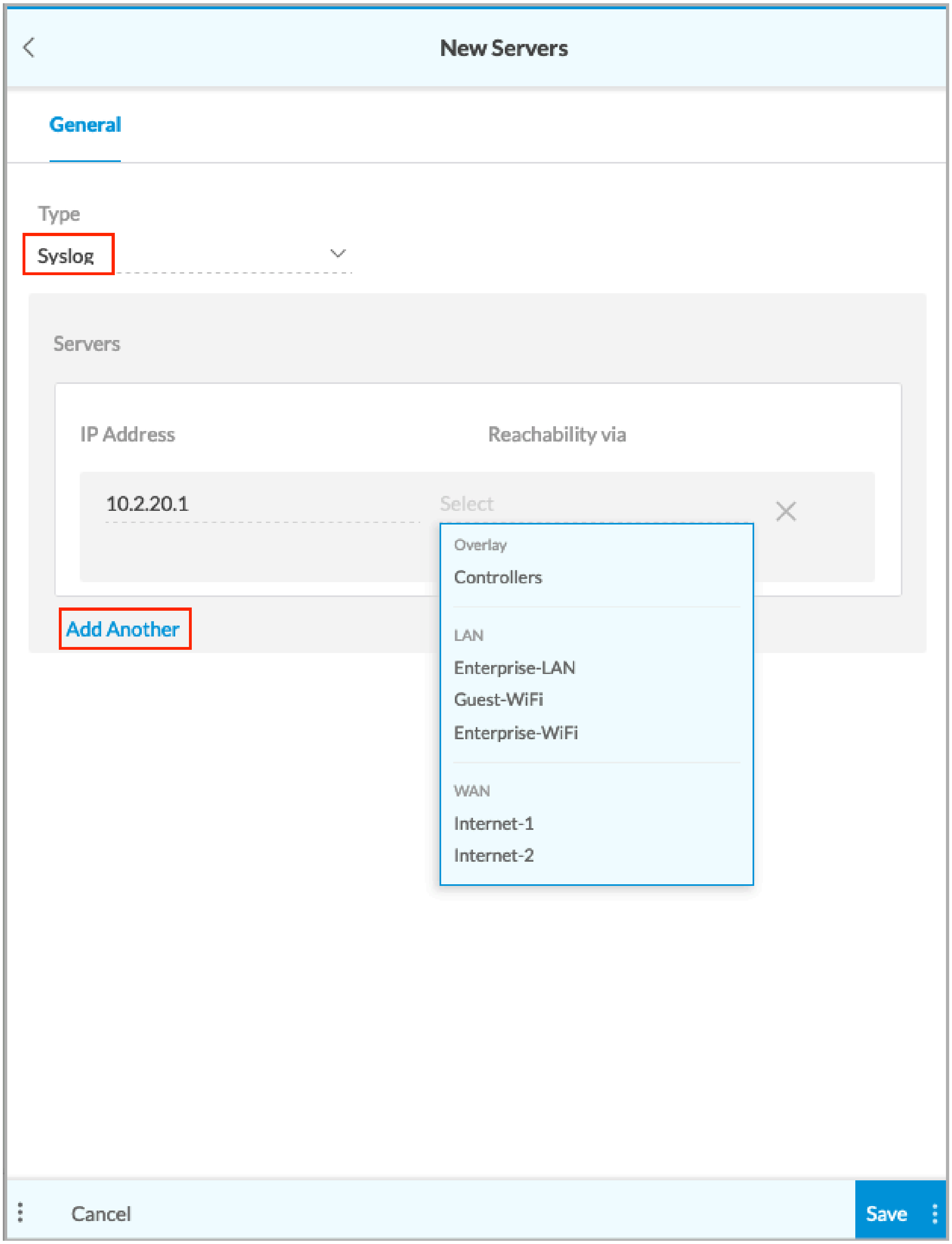
3. Click Add Another to configure additional SNMP servers.
4. Click Save.

Configure a Syslog Server

A syslog server consolidates logs from multiple sources into a single location. Syslog messages report about conditions that occur on a device, and you can use the information they contains to help identify basic information about where, when, and why a condition occurred. A syslog message contains the IP address, timestamp, and a log message. You configure a syslog server for each appliance.

To configure a syslog server:

1. In the Type field, select Syslog.



2. Enter information for the following fields.

Field	Description
IP Address	Enter the IP address of the syslog server.
Reachability via	Select the network to use for reachability between the controller and the syslog server.

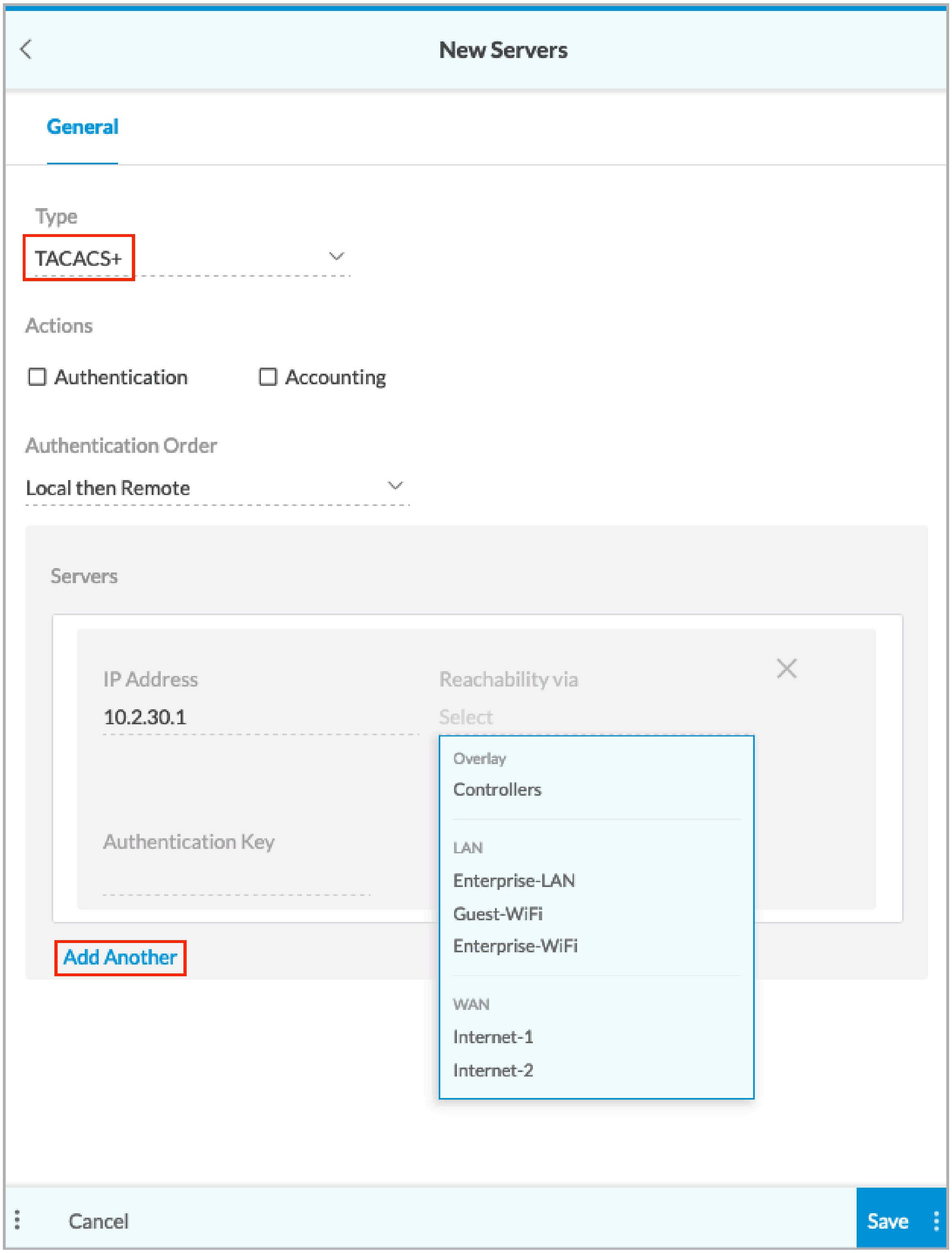
3. Click Add Another to configure additional syslog servers.
4. Click Save.

Configure a TACACS+ Server

TACACS+ provides detailed accounting information and flexible administrative control over authentication and authorization processes. A TACACS+ server provides an external database that you can use to authenticate users before allowing them to access a network, a device, or related services.

To configure a TACACS+ server:

1. In the Type field, select TACACS+. It is recommended that you configure either a TACACS+ server or a RADIUS server, but not both.



New Servers

General

Type

TACACS+

Actions

□ Authentication □ Accounting

Authentication Order

Local then Remote

Servers

IP Address

10.2.30.1

Reachability via

Select

Authentication Key

2. Enter information for the following fields.

Field	Description
Actions (Group of Fields)	
◦ Authentication	Select to enable TACACS+ authentication.
◦ Accounting	Select to enable TACACS+ accounting.
Authentication Order	Select the authentication order: ◦ Local-Then-Remote—User is authenticated by checking the local database first, then the remote database. ◦ Remote-Then-Local—User is authenticated by checking the remote database first. If the remote database is unreachable, the local database is then searched. ◦ Remote-Only—User is authenticated by checking the remote database only.
Servers (Group of Fields)	
◦ IP Address	Enter the IP address of the TACACS+ server.
◦ Reachability via	Select the network to use for reachability between the controller and the TACACS+ server.
◦ Authentication Key	Enter the TACACS+ key. The key can consist of both numbers and letters, and it cannot include a hash mark (#) or spaces.

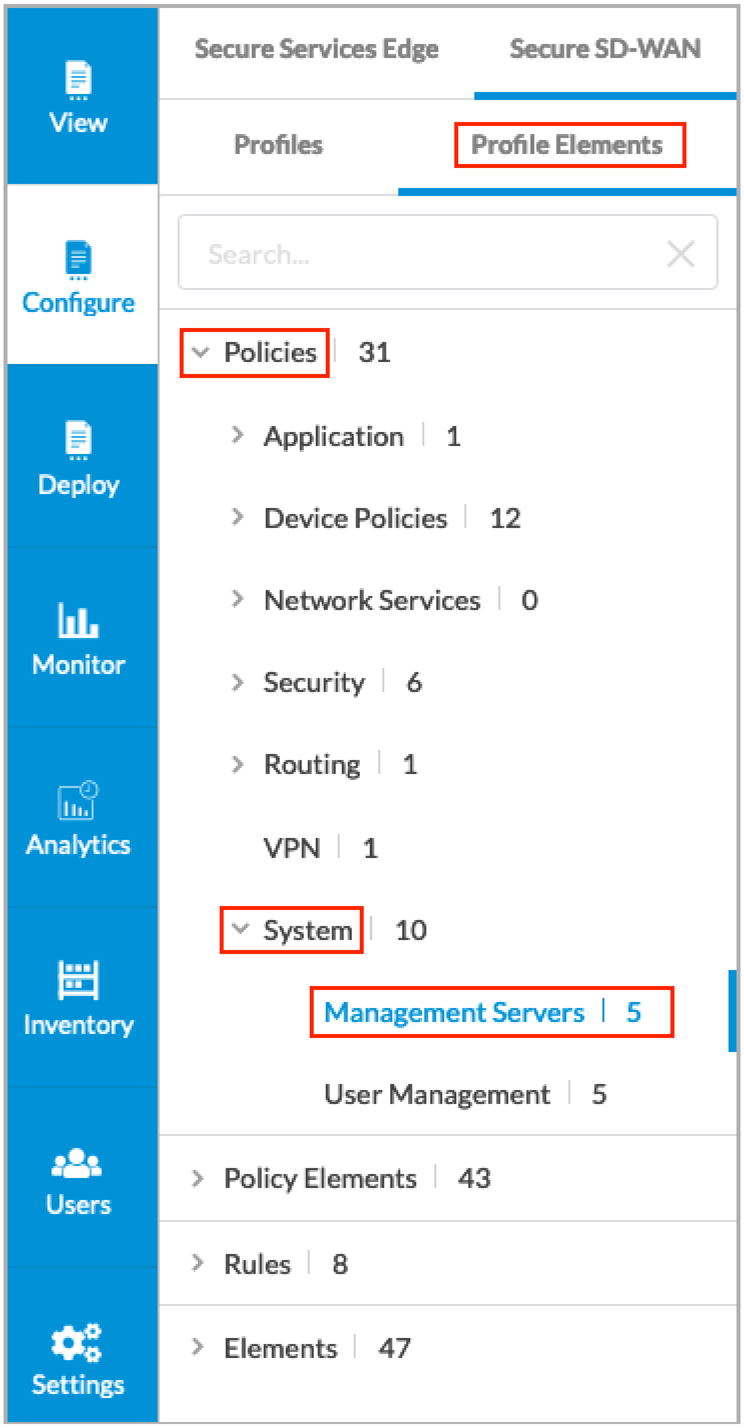
3. Click Add Another to configure additional TACACS+ servers.
4. Click Save.

Add Management Servers

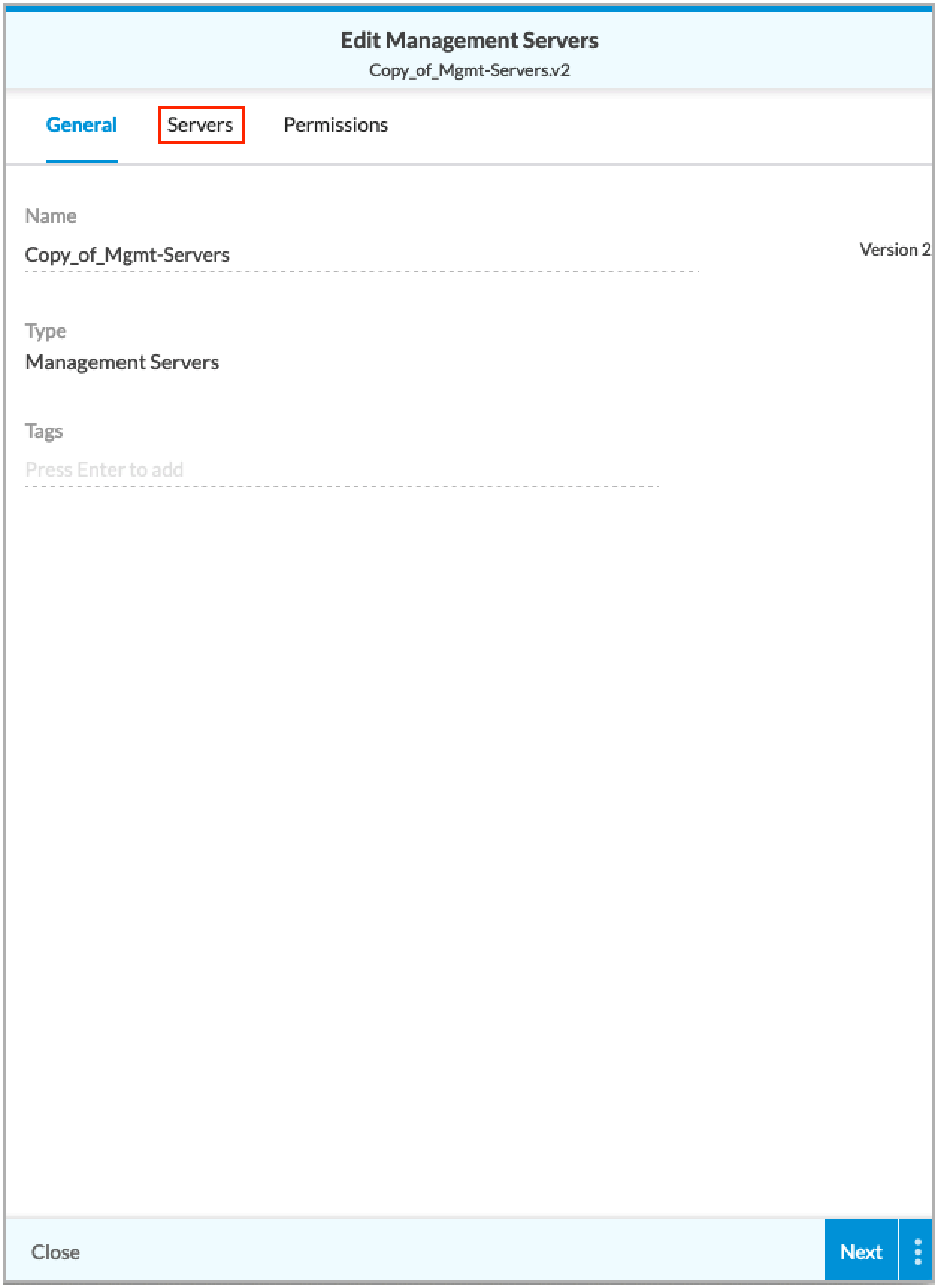
After you have configured one or more management servers, you can configure additional servers as needed.

To configure additional management servers:

1. Go to Configure > Profile > Profile Elements > Policies > System.



2. Click Management Servers, and then select a management server policy. The Edit Management Servers screen displays.


Edit Management Servers

Copy_of_Mgmt-Servers.v2

Name

Copy_of_Mgmt-Servers

Version 2

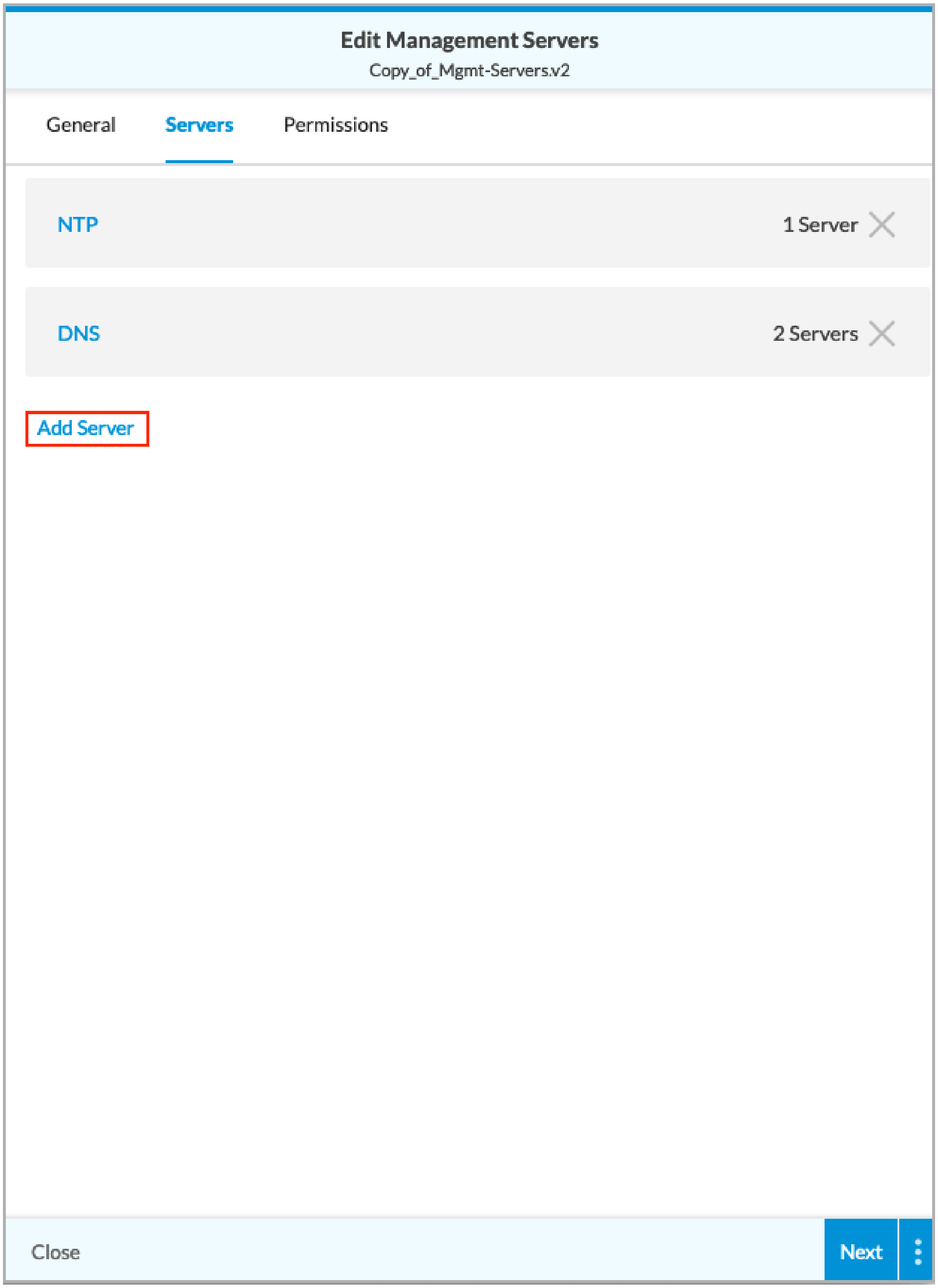
Type

Management Servers

Tags

Press Enter to add

3. Select the Servers tab. The Edit Management Servers screen displays.



Edit Management Servers

Copy_of_Mgmt-Servers.v2

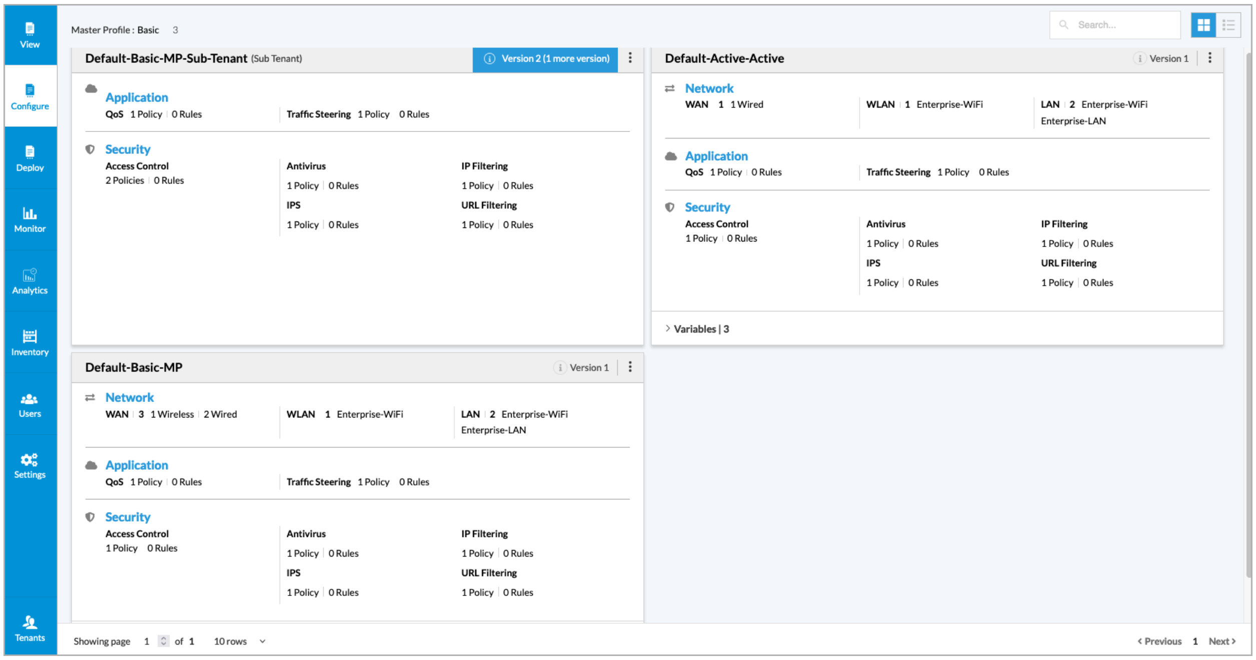
4. Click Add Server. The New Servers screen displays.
5. Depending on which type of management server you want to add, follow the instructions in the preceding sections to add the additional management server or servers.

Delete a Management Server

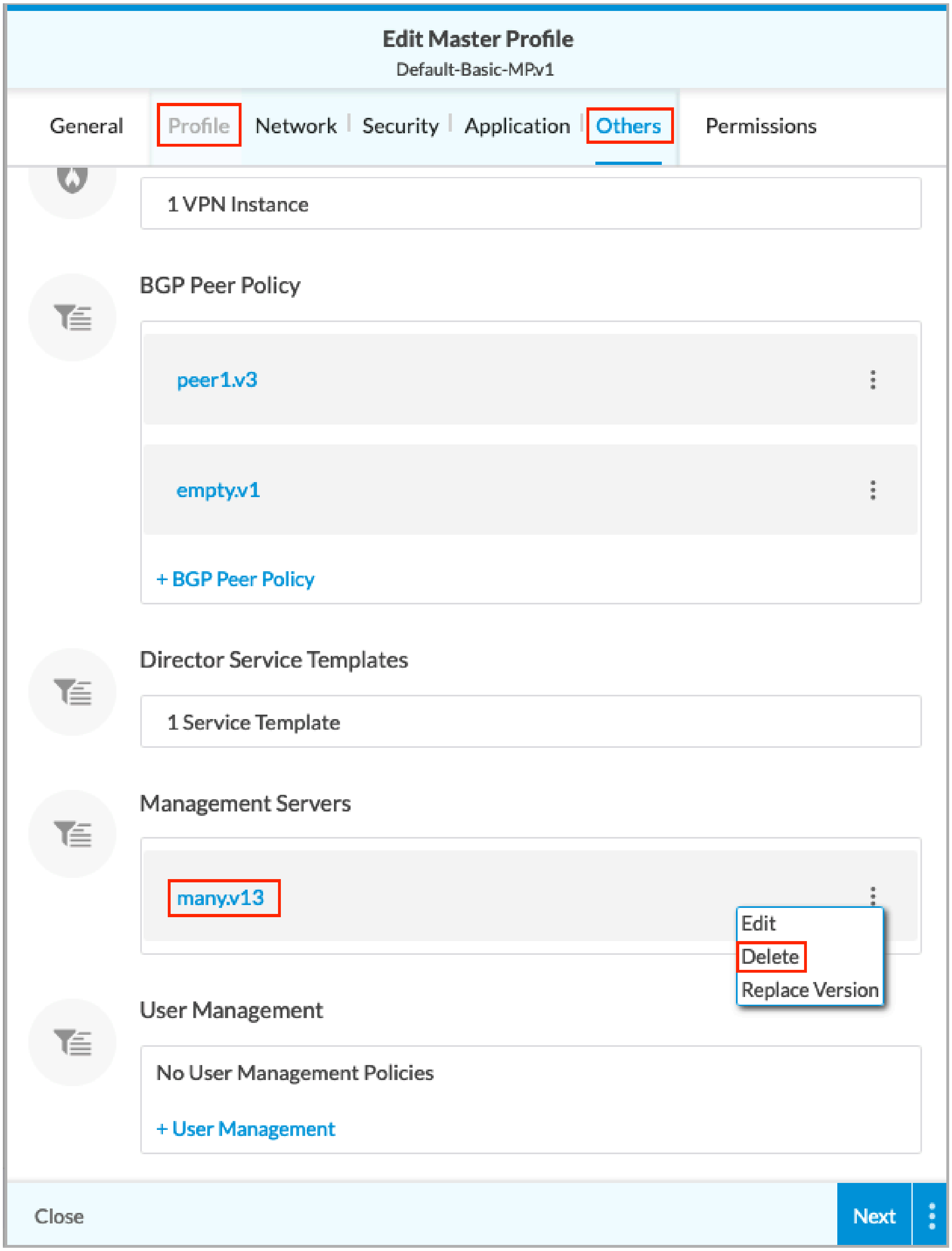
You can attach only one management server policy to a basic master profile or standard master profile. To attach a new management server, first delete the existing management server, then add the new one.

To delete a management server from the basic master profile level:

1. Go to the Configuration lifecycle screen.
   a. To delete a management server at the basic master profile level:
      i. Select Profiles > Master Profiles > Basic.


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

      ii. Click the Basic master profile from which you want to delete a management server policy. The Edit Master Profile screen displays.
      iii. Select the Profile tab, and then select Others in the top menu bar. The following screen displays.



Edit Master Profile

Default-Basic-MP.v1

1 VPN Instance

BGP Peer Policy

peer1.v3

empty.v1

Director Service Templates

1 Service Template

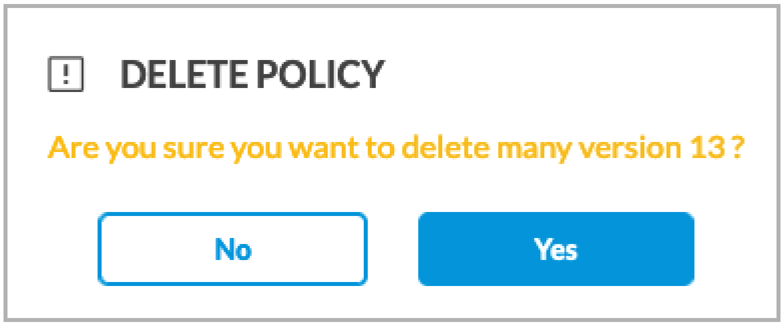
Management Servers

many.v13

User Management

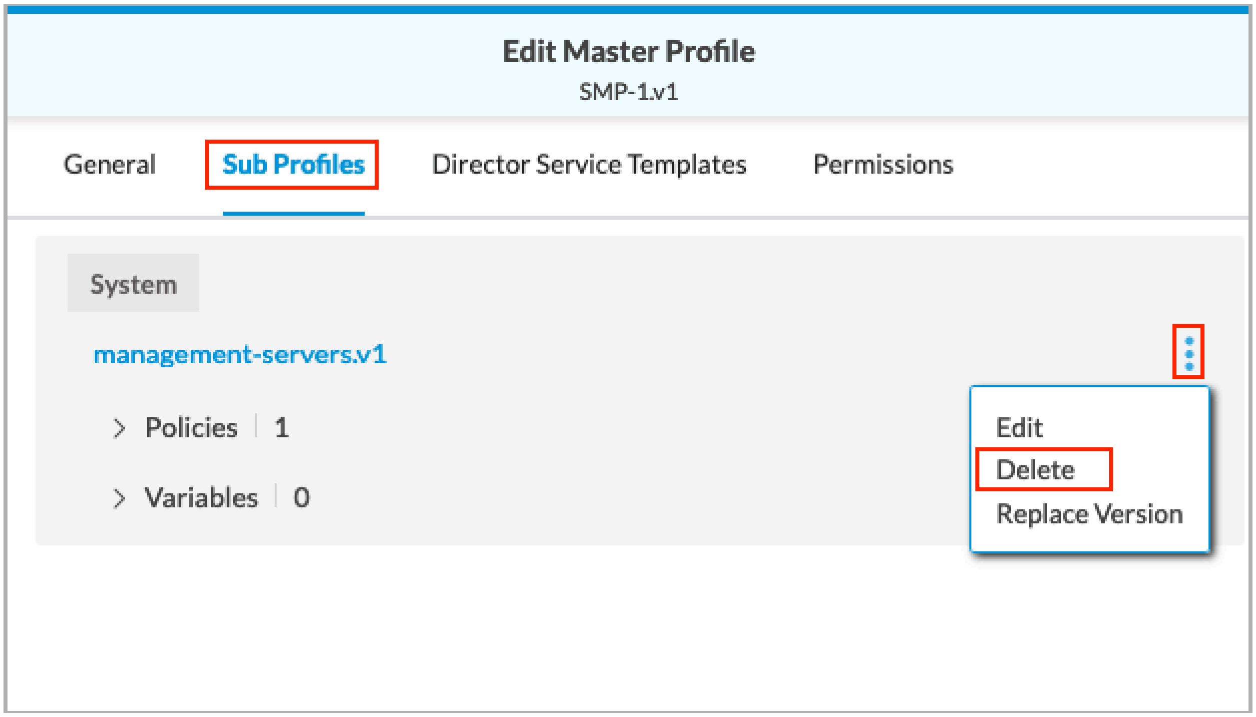
No User Management Policies

iv. In the Management Servers box, click the Vertical Dots icon, then click Delete. The following popup window displays.

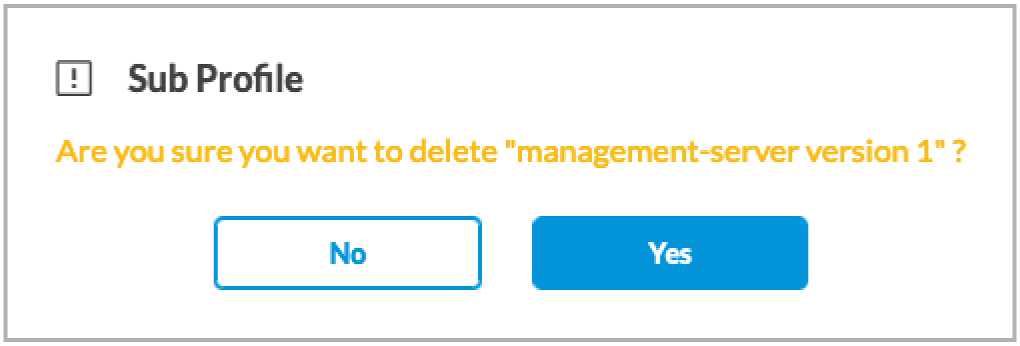


v. Click Yes to delete the management server policy.

2. To delete a management server at the standard master profile level:
   i. Go to Configure > Profiles > Master Profiles > Standard.
   ii. Click the standard master profile from which you want to delete a management server policy. The Edit Master Profile screen displays.
   iii. Click the Sub-Profile tab in the Edit Master Profile screen.



   iv. Click the Vertical Dots icon to the right of the management server subprofile to be deleted, then click Delete. The following screen displays.



Sub Profile

Are you sure you want to delete "management-server version 1" ?

v. In the popup window, click Yes to delete the management server subprofile.

Supported Software Information

Releases 11.1.1 and later support all content described in this article, except:

- Releases 11.3.1 adds support for DNS management servers.

Additional Information

[Configuration Hierarchies](#)
[Object Versioning](#)
[Parameterized Variables with Type](#)