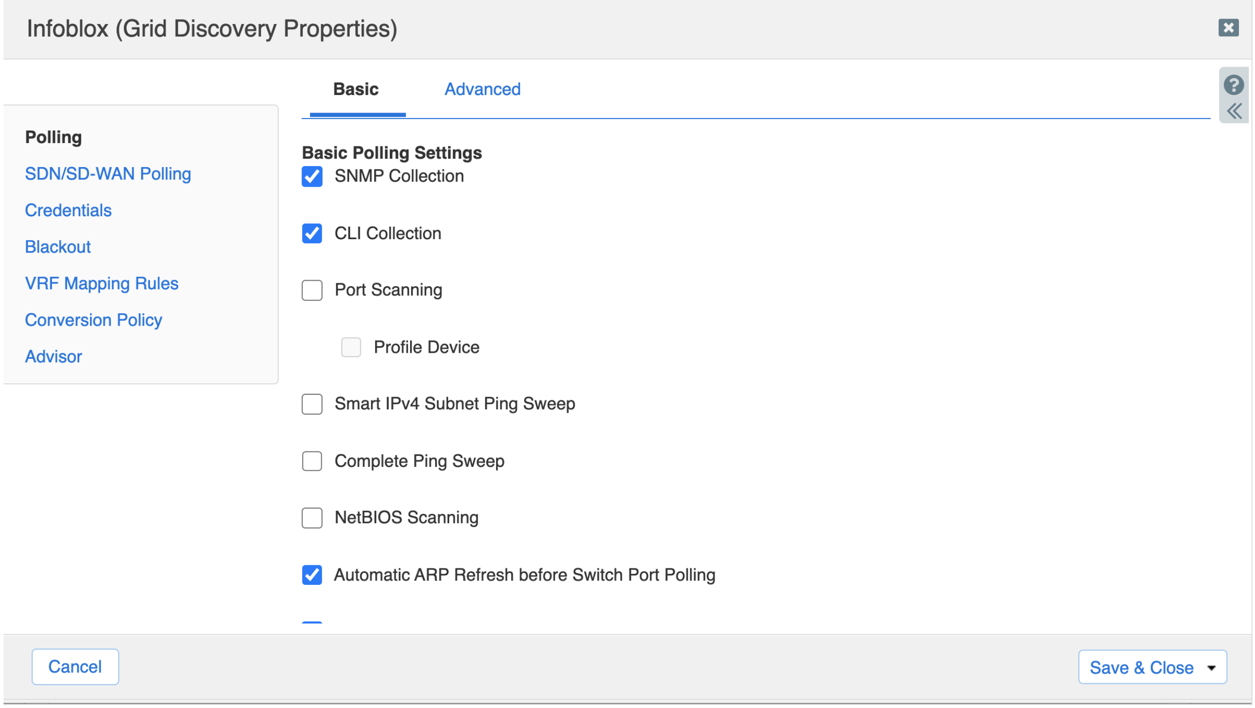
DEPLOYMENT GUIDE

Network Insight

Table of Contents

Best Practices for Configuring Network Insight Discovery

1. Navigate to **Grid** → **Grid Manager** → **Discovery** → **Toolbar** → **Edit** → **Grid Discovery Properties**.



Basic Polling Settings

☑ SNMP Collection

☑ CLI Collection

□ Port Scanning

□ Profile Device

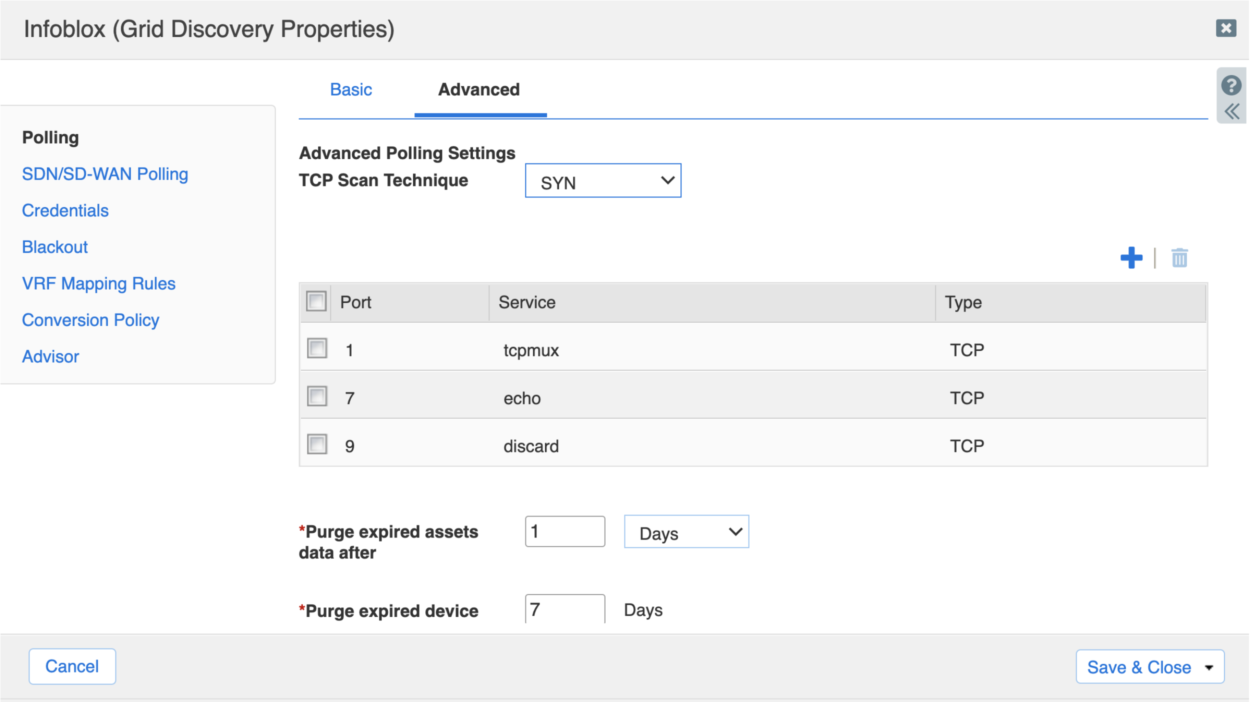
□ Smart IPv4 Subnet Ping Sweep

□ Complete Ping Sweep

□ NetBIOS Scanning

☑ Automatic ARP Refresh before Switch Port Polling

2. Use the enabled default settings which are:
   - **SNMP Collection -** Network Insight uses SNMP to collect traceroute/path information, vendor and model, SNMP credential collection, routing and ARP tables, switch port data, and VLAN configuration data.
   - **CLI Collection -** Network Insight uses SSH or telnet to connect to devices to collect IP configuration, port configuration, and routing tables.
   - **Automatic ARP Refresh before Switch Port Polling -** Refreshes ARP caches on switches and switch-routers in the managed network before NIOS performs polling of switch ports. Enabling this feature applies only to switched Ethernet devices. This feature enables more accurate detection of all endpoint devices on L2 switches. Without ARP refresh, some endpoint devices may not be detected.
   - **Switch Port Data Collection-** this enables the probe to poll l2 enterprise switches. The recommendation is to poll every hour.
   - Disable **Use DHCP routers** as seed routers.
3. Navigate to **Grid** → **Grid Manager** → **Discovery**.
4. In the **Toolbar** click on **Edit** → **Grid Discovery Properties** → **Advanced**.


Infoblox (Grid Discovery Properties)

Advanced Polling Settings

TCP Scan Technique SYN

□	Port	Service	Type
□	1	tcpmux	TCP
□	7	echo	TCP
□	9	discard	TCP

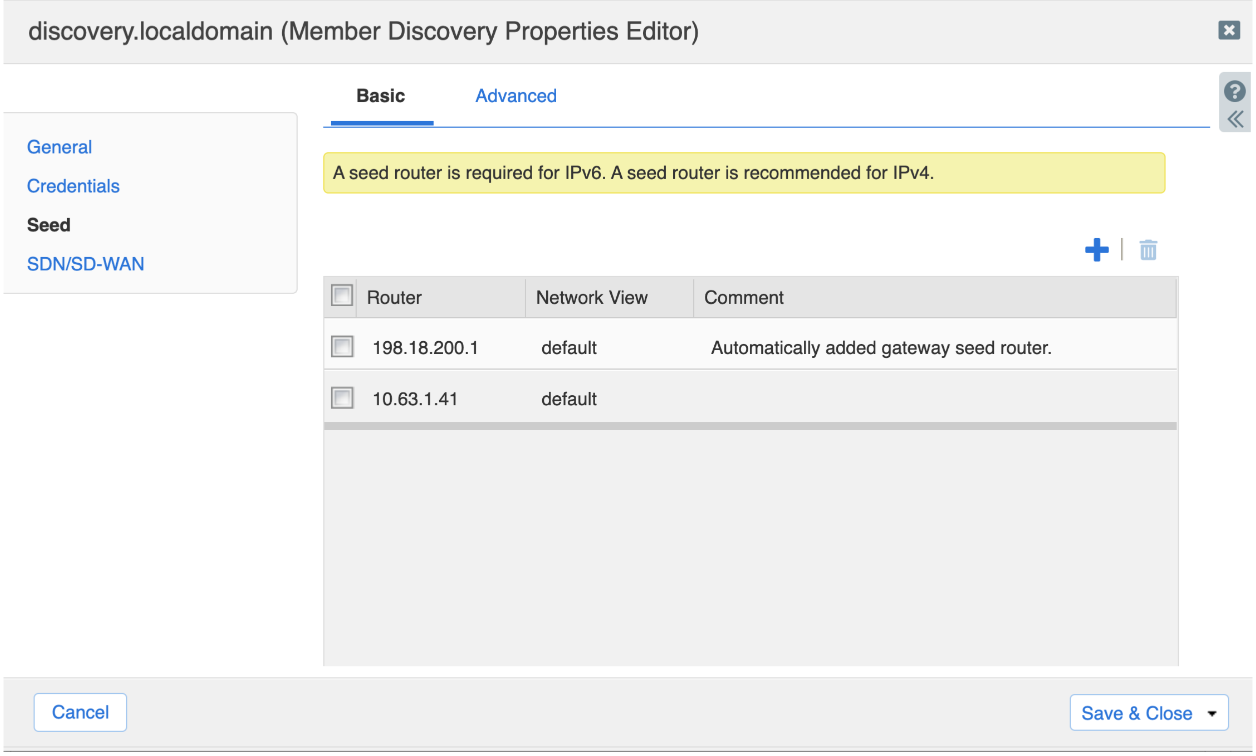
***Purge expired assets data after** 1 Days

***Purge expired device** 7 Days

Use the most minimal amount of network containers as possible. For example, use network containers that use the IP address's natural mask such as 10.0.0/8 to contain your 10 subnets. For sub containers and/or networks, override discovery settings as little as possible. Every time an override is set extra resources are created and used under the covers and could impact performance over time.

Use as few Seed Routers as possible. Using one as close to the core as possible is recommended.

5. Navigate to **Grid** → **Grid Manager** → **Discovery**.
6. Click on a **Discovery Device** and edit the properties.
7. Click on **Seed**.
8. Click on the **+** button to add the IP address of a seed router.



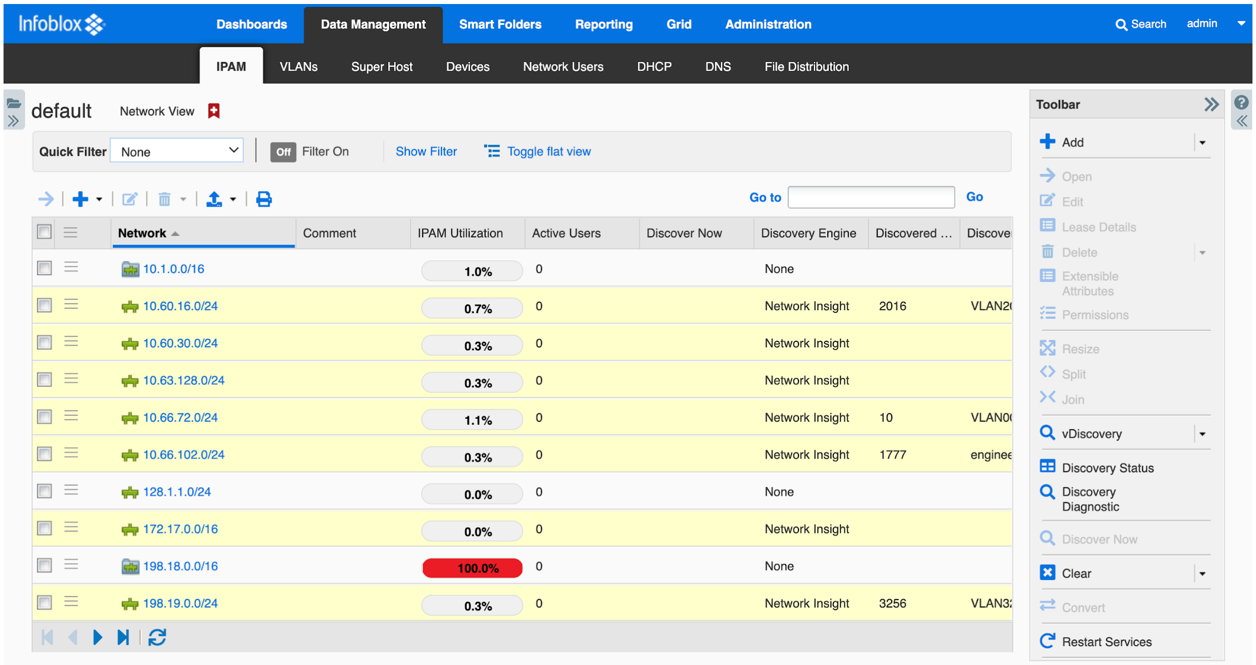
discovery.localdomain (Member Discovery Properties Editor)

A seed router is required for IPv6. A seed router is recommended for IPv4.

Router	Network View	Comment
198.18.200.1	default	Automatically added gateway seed router.
10.63.1.41	default	

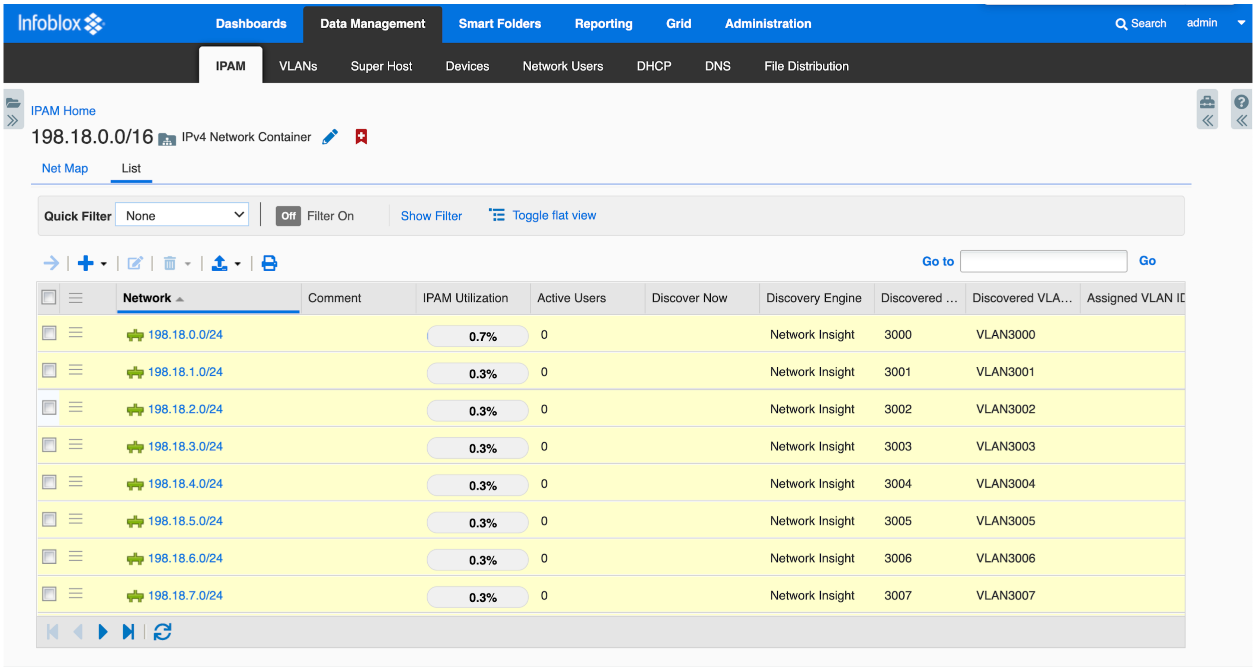
Use Exclusions for IP addresses you want excluded from discovery.

9. Navigate to **Data Management** → **IPAM** → **Network Container**.



Network	Comment	IPAM Utilization	Active Users	Discover Now	Discovery Engine	Discovered ...	Discove
10.1.0.0/16		1.0%	0		None		
10.60.16.0/24		0.7%	0		Network Insight	2016	VLAN2(
10.60.30.0/24		0.3%	0		Network Insight		
10.63.128.0/24		0.3%	0		Network Insight		
10.66.72.0/24		1.1%	0		Network Insight	10	VLAN0(
10.66.102.0/24		0.3%	0		Network Insight	1777	enginee
128.1.1.0/24		0.0%	0		None		
172.17.0.0/16		0.0%	0		Network Insight		
198.18.0.0/16		100.0%	0		None		
198.19.0.0/24		0.3%	0		Network Insight	3256	VLAN3:

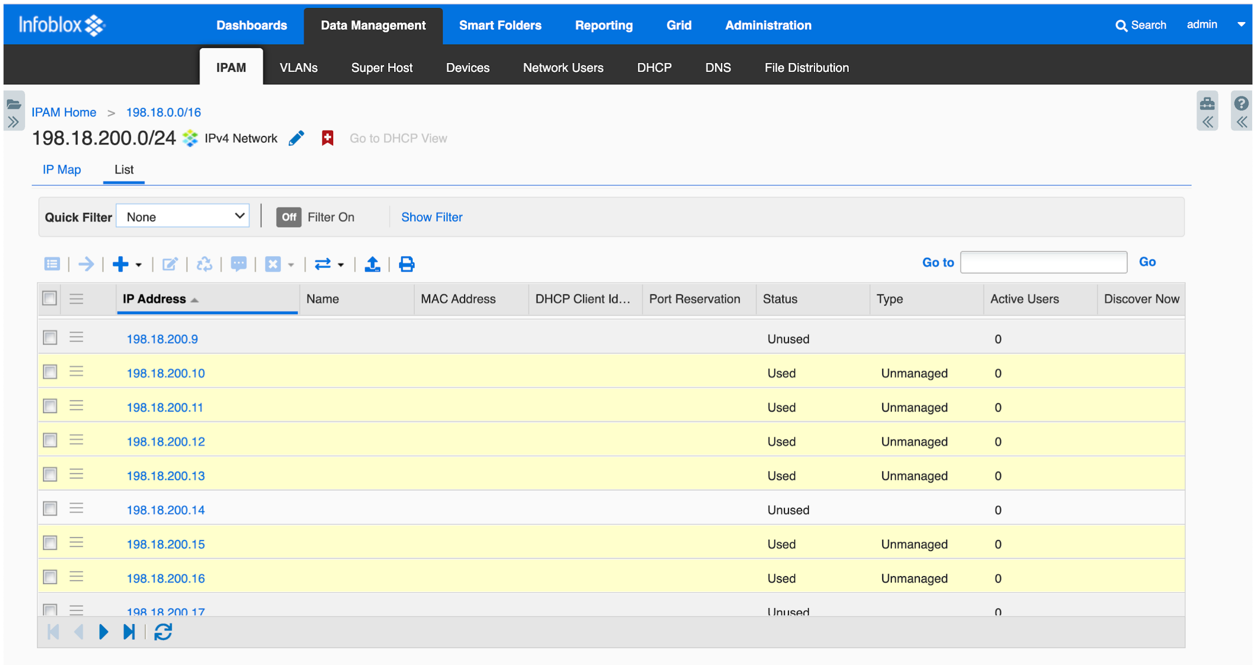
10. Click on the container and the list of IP subnets will appear.



198.18.0.0/16 IPv4 Network Container

Network	Comment	IPAM Utilization	Active Users	Discover Now	Discovery Engine	Discovered ...	Discovered VLA...	Assigned VLAN ID
198.18.0.0/24		0.7%	0		Network Insight	3000	VLAN3000	
198.18.1.0/24		0.3%	0		Network Insight	3001	VLAN3001	
198.18.2.0/24		0.3%	0		Network Insight	3002	VLAN3002	
198.18.3.0/24		0.3%	0		Network Insight	3003	VLAN3003	
198.18.4.0/24		0.3%	0		Network Insight	3004	VLAN3004	
198.18.5.0/24		0.3%	0		Network Insight	3005	VLAN3005	
198.18.6.0/24		0.3%	0		Network Insight	3006	VLAN3006	
198.18.7.0/24		0.3%	0		Network Insight	3007	VLAN3007	

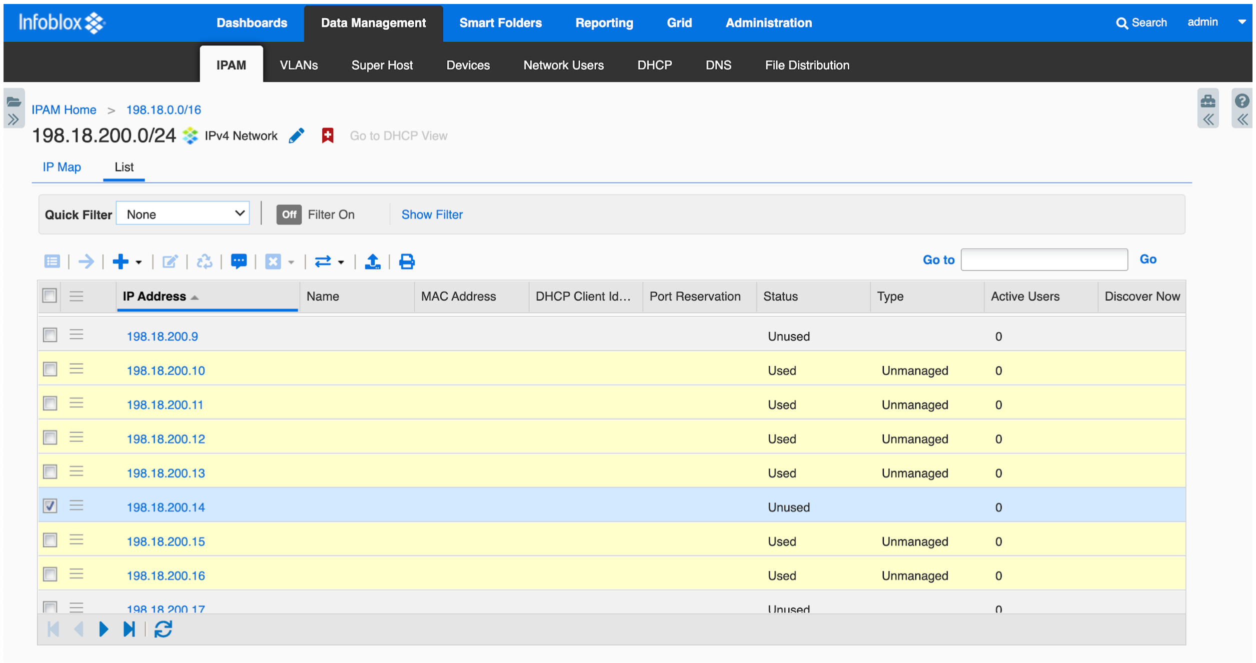
11. Click on the selected IP subnet and the list of IP addresses will appear.



198.18.200.0/24 IPv4 Network

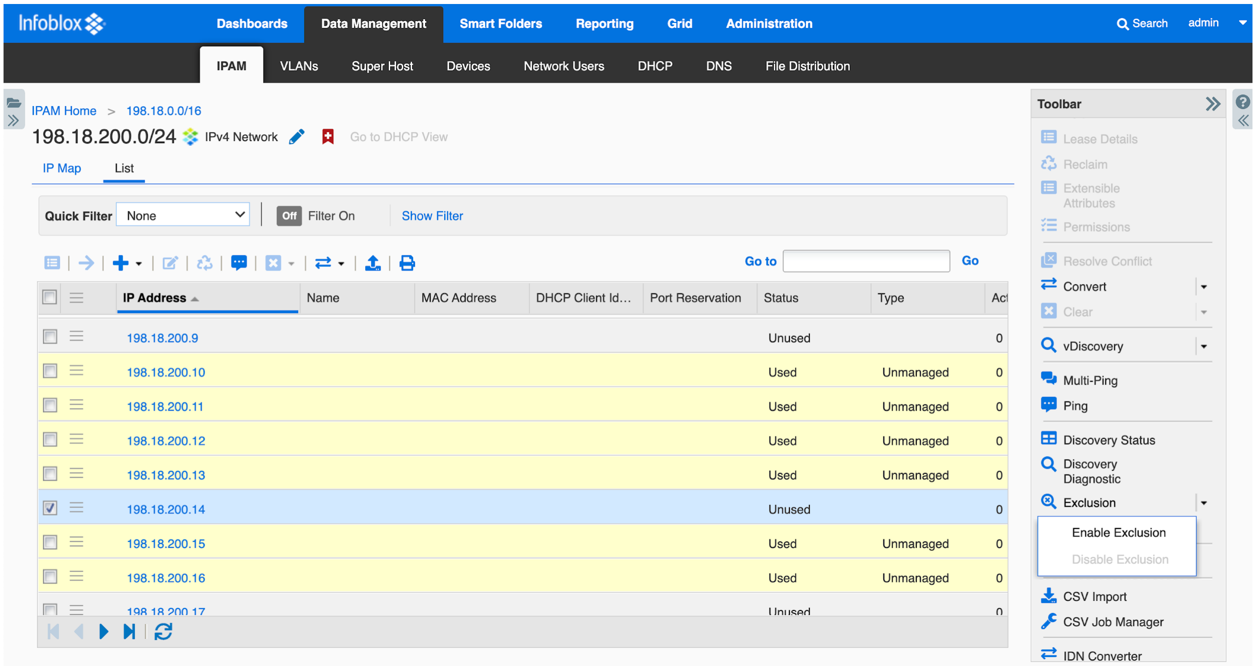
IP Address	Name	MAC Address	DHCP Client Id...	Port Reservation	Status	Type	Active Users	Discover Now
198.18.200.9					Unused		0	
198.18.200.10					Used	Unmanaged	0	
198.18.200.11					Used	Unmanaged	0	
198.18.200.12					Used	Unmanaged	0	
198.18.200.13					Used	Unmanaged	0	
198.18.200.14					Unused		0	
198.18.200.15					Used	Unmanaged	0	
198.18.200.16					Used	Unmanaged	0	
198.18.200.17					Unused		0	

12. Click on the check box for the IP address you wish to exclude from discovery.



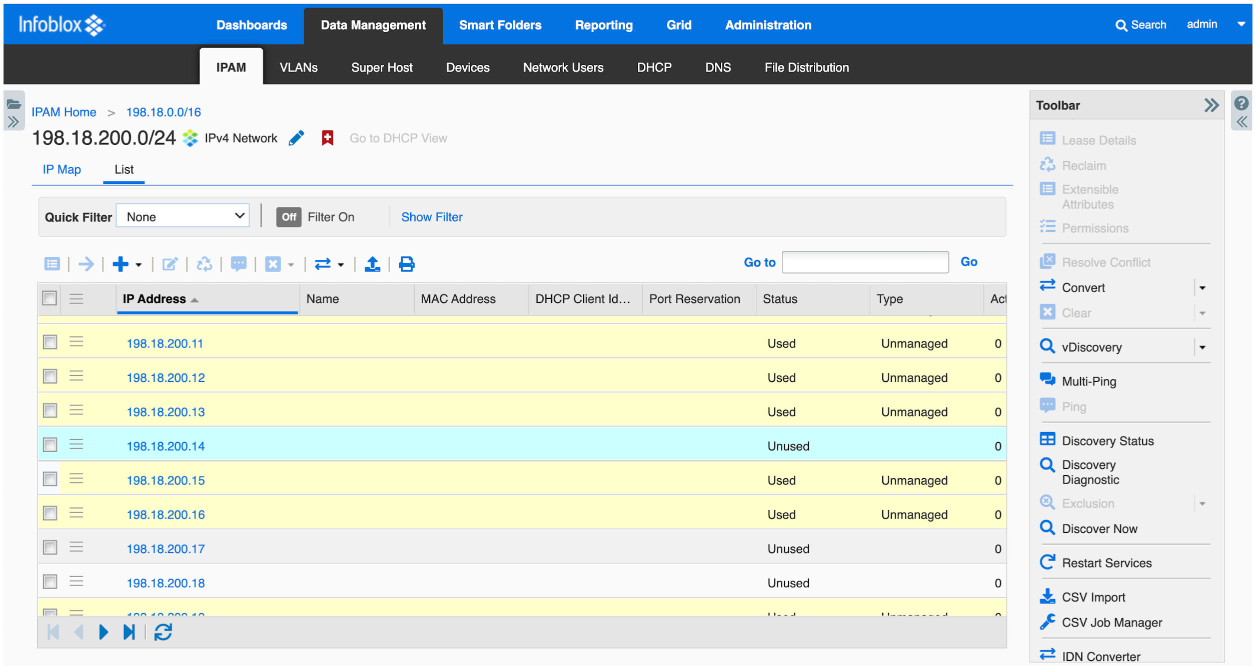
☐	IP Address	Name	MAC Address	DHCP Client Id...	Port Reservation	Status	Type	Active Users	Discover Now
☐	198.18.200.9					Unused		0	
☐	198.18.200.10					Used	Unmanaged	0	
☐	198.18.200.11					Used	Unmanaged	0	
☐	198.18.200.12					Used	Unmanaged	0	
☐	198.18.200.13					Used	Unmanaged	0	
☑	198.18.200.14					Unused		0	
☐	198.18.200.15					Used	Unmanaged	0	
☐	198.18.200.16					Used	Unmanaged	0	
☐	198.18.200.17					Unused		0	

13. Go to the **Toolbar** and click on **Exclusion**.



☐	IP Address	Name	MAC Address	DHCP Client Id...	Port Reservation	Status	Type	Act
☐	198.18.200.9					Unused		0
☐	198.18.200.10					Used	Unmanaged	0
☐	198.18.200.11					Used	Unmanaged	0
☐	198.18.200.12					Used	Unmanaged	0
☐	198.18.200.13					Used	Unmanaged	0
☑	198.18.200.14					Unused		0
☐	198.18.200.15					Used	Unmanaged	0
☐	198.18.200.16					Used	Unmanaged	0
☐	198.18.200.17					Unused		0

The IP address will be highlighted in an aqua color to indicate the IP address is excluded from discovery.



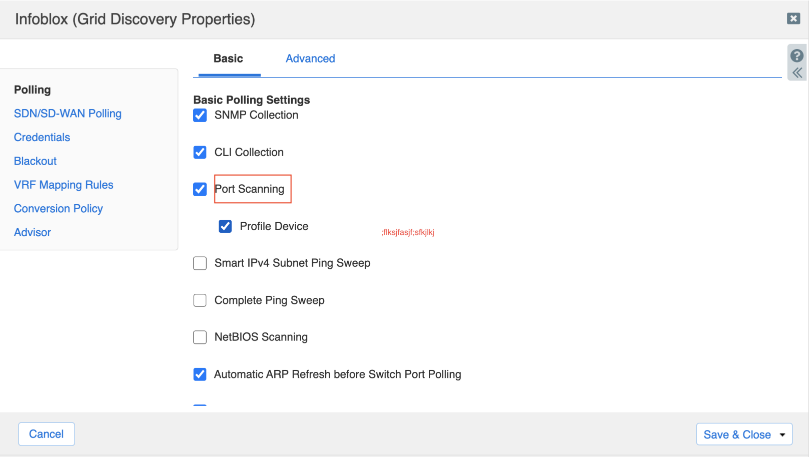
IP Address	Name	MAC Address	DHCP Client Id...	Port Reservation	Status	Type	Act
198.18.200.11					Used	Unmanaged	0
198.18.200.12					Used	Unmanaged	0
198.18.200.13					Used	Unmanaged	0
198.18.200.14					Unused		0
198.18.200.15					Used	Unmanaged	0
198.18.200.16					Used	Unmanaged	0
198.18.200.17					Unused		0
198.18.200.18					Unused		0
198.18.200.19					Used	Unmanaged	0

Description of Optional Parameters

Port Scanning

Port Scanning allows the Network Insight probes to scan for open TCP ports on a device based upon an adjustable TCP port list.

1. Navigate to **Grid** → **Grid Manager** → **Discovery**.
2. In the Toolbar click on **Edit** → **Grid Discovery Properties**.
3. Click on the check box for **Port Scanning** to enable and click on **Save & Close**.



Basic Polling Settings

☑ SNMP Collection

☑ CLI Collection

☑ Port Scanning

☑ Profile Device

□ Smart IPv4 Subnet Ping Sweep

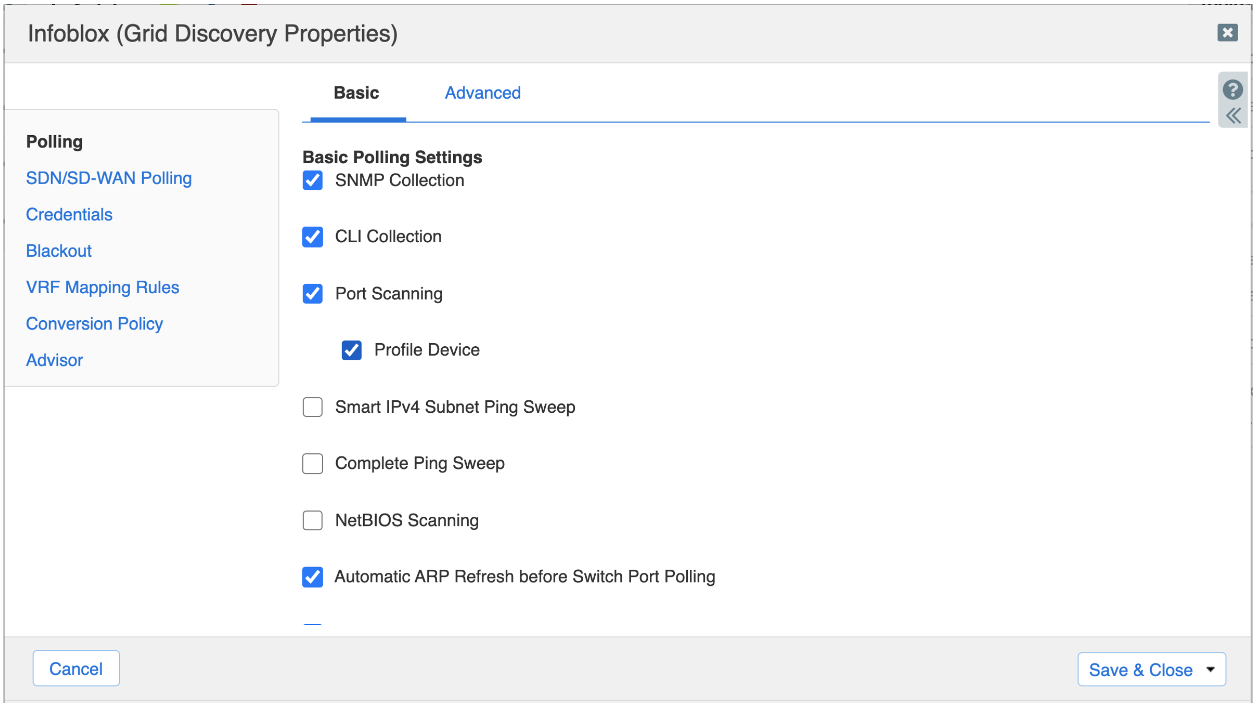
□ Complete Ping Sweep

□ NetBIOS Scanning

☑ Automatic ARP Refresh before Switch Port Polling

An accompanying parameter is called Profile Device. While just enabling port scanning will tell what TCP ports are open, **Profile Device** will try to identify the device by based upon the open TCP port numbers. In the absence of SNMP access, the Profile Device function is usually the only way to identify devices that do not support SNMP. If you disable Profile Device, devices accessible via SNMP are still correctly identified; all other devices are assigned a device type of Unknown.

4. Navigate to **Grid** → **Grid Manager** → **Discovery**.
5. In the **Toolbar** → **Edit** → **Grid Discovery Properties**.
6. Click on the check box for **Port Scanning** and **Profile Device** to enable.
7. Click **Save & Close**.



Infoblox (Grid Discovery Properties)

Basic Polling Settings

☑ SNMP Collection

☑ CLI Collection

☑ Port Scanning

☑ Profile Device

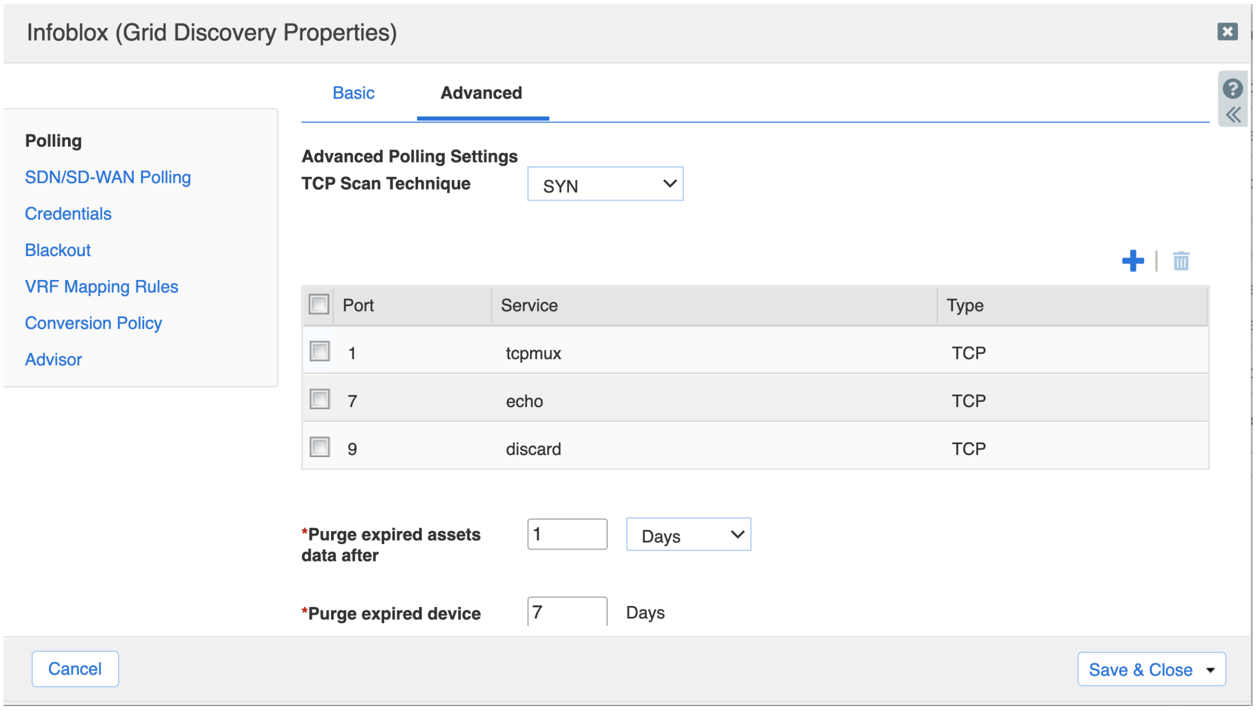
☐ Smart IPv4 Subnet Ping Sweep

☐ Complete Ping Sweep

☐ NetBIOS Scanning

☑ Automatic ARP Refresh before Switch Port Polling

On the Advanced Tab, the screenshot shows the TCP Scan Technique: SYN or Connect. When you use the SYN technique, the discovery sends a TCP SYN packet to establish a connection on a TCP port. If the port is open, the host replies with a SYN ACK response. The discovery does not close the port connection. The CONNECT technique is a three-way TCP handshake. The discovery starts with the same process as the SYN technique by sending the TCP SYN packet. A response containing a RST flag indicates that the port is closed. If the host replies with a SYN ACK response, discovery sends a RST packet to close the connection. If there is no reply, the port is considered filtered. TCP scanning is a deliberate and accurate discovery method, enabling detection of all active hosts on a network provided that there are no firewalls blocking TCP packet exchanges.


Infoblox (Grid Discovery Properties)

Advanced Polling Settings

TCP Scan Technique: SYN

□	Port	Service	Type
□	1	tcpmux	TCP
□	7	echo	TCP
□	9	discard	TCP

*Purge expired assets data after: 1 Days

*Purge expired device: 7 Days

Smart IPv4 Ping Sweep

The ICMP Smart Ping Sweep option enables brute-force subnet Ping sweeps on IPv4 networks. Subnet ping sweeps are used as a last resort in the discovery process. A subnet ping sweep is performed if Network Insight is unable to identify any network devices in a given subnet. Subnet ping sweeps are performed no more than once per day, and will end the ping sweep on a given subnet once Network Insight discovers a network device and is able to collect data from it.

Note: Smart subnet ping sweeps will not be performed on subnets larger than/22.

NetBIOS Scanning

The NetBIOS method queries IP addresses for an existing NetBIOS service. This method detects active hosts by sending NetBIOS queries and listening for NetBIOS replies. It is a fast discovery that focuses on Microsoft hosts or non-Microsoft hosts that run NetBIOS services.

Discovery Procedure

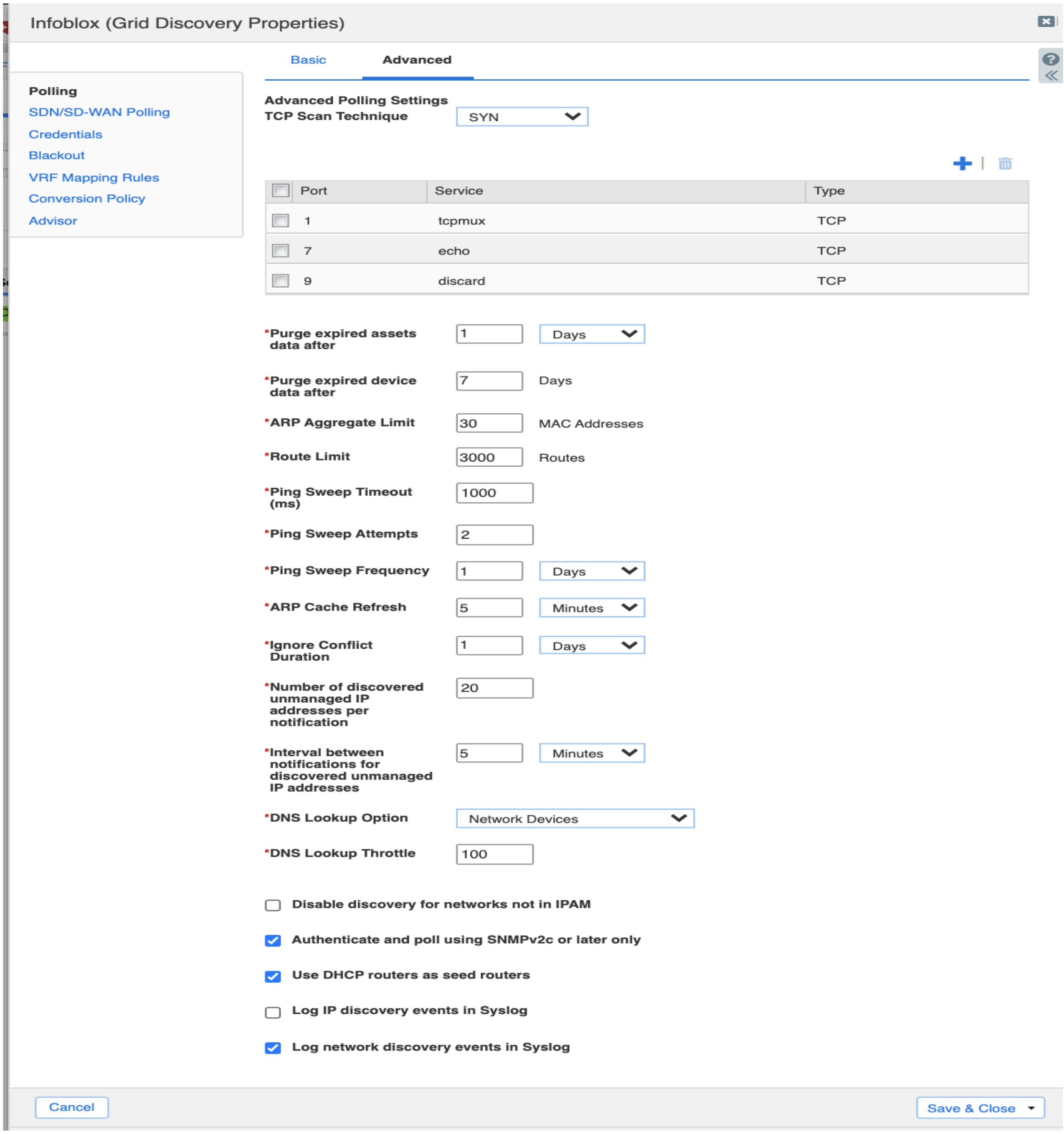
Prerequisite

This deployment guide assumes Network Insight as a standalone, consolidator and/or probes have been installed on the Infoblox Grid. Refer to the NIOS Administrator’s Guide for more information.

Grid and Member Discovery Properties

1. Navigate to **Grid** → **Grid Manager** → **Discovery**
2. In the **Toolbar** click **Edit** → **Grid Discovery Properties**.

Use the default discovery settings as much as possible. The screenshot below shows the default polling discovery settings for both the basic and advanced sections. When done with any adjustments, click on **Save & Close**.



Infoblox (Grid Discovery Properties)

Advanced Polling Settings

TCP Scan Technique: SYN

□	Port	Service	Type
□	1	tcpmux	TCP
□	7	echo	TCP
□	9	discard	TCP

*Purge expired assets data after	1	Days
*Purge expired device data after	7	Days
*ARP Aggregate Limit	30	MAC Addresses
*Route Limit	3000	Routes
*Ping Sweep Timeout (ms)	1000	
*Ping Sweep Attempts	2	
*Ping Sweep Frequency	1	Days
*ARP Cache Refresh	5	Minutes
*Ignore Conflict Duration	1	Days
*Number of discovered unmanaged IP addresses per notification	20	
*Interval between notifications for discovered unmanaged IP addresses	5	Minutes
*DNS Lookup Option	Network Devices	
*DNS Lookup Throttle	100	

□ Disable discovery for networks not in IPAM

☑ Authenticate and poll using SNMPv2c or later only

☑ Use DHCP routers as seed routers

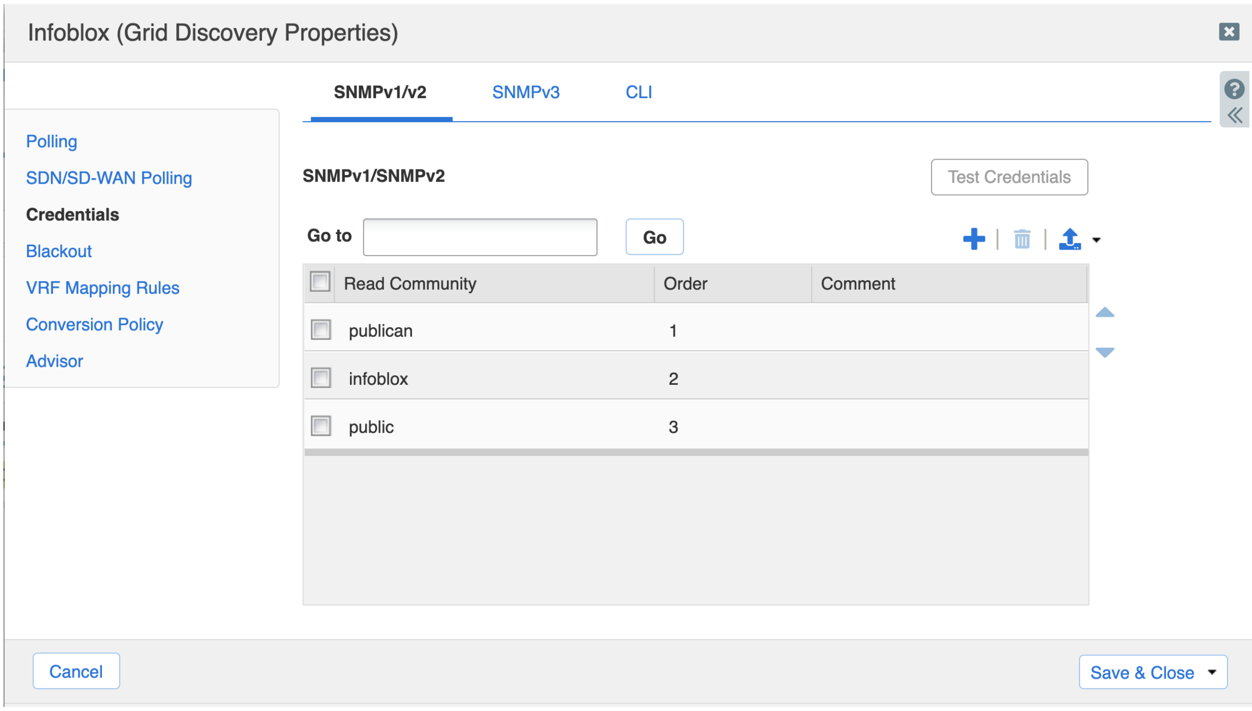
□ Log IP discovery events in Syslog

☑ Log network discovery events in Syslog

Note: Disable Use DHCP routers as seed routers. This feature creates a seed router entry for every DHCP range, which can lead to performance issues.

Credentials

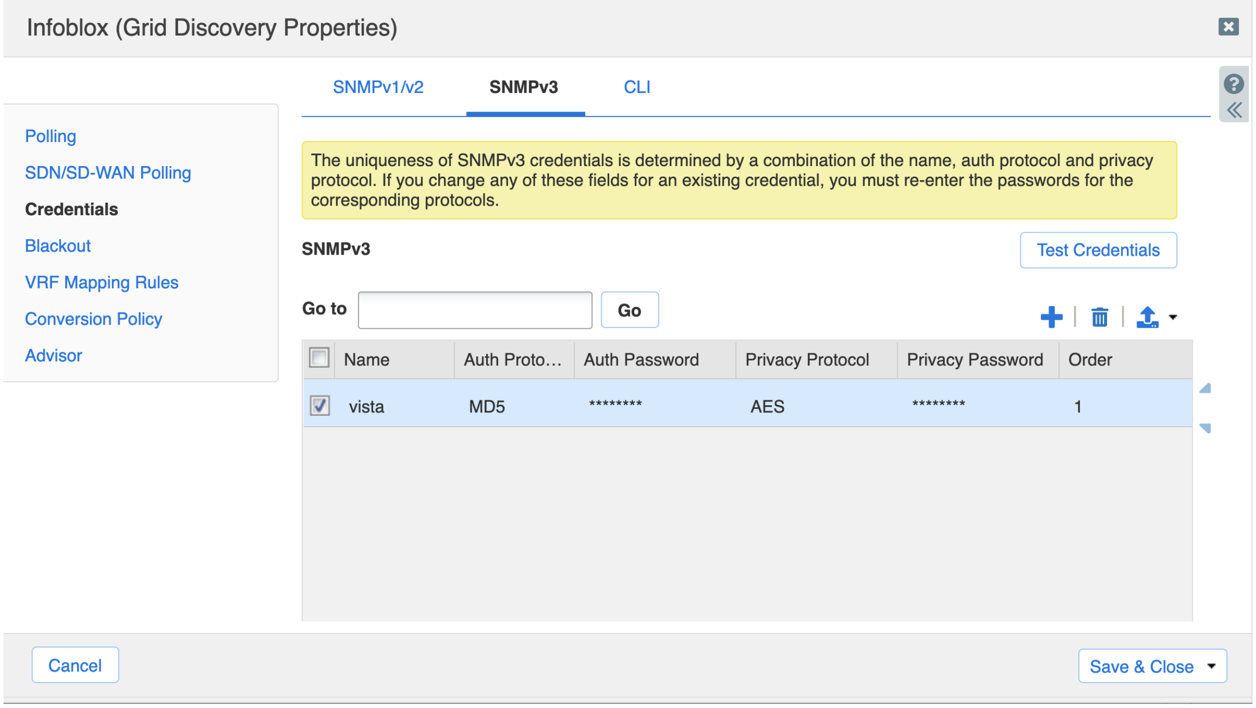
After reviewing the Polling parameters, click on **Credentials** to enter the credentials for the discovered devices. The credential types are SNMP v1/v2, SNMPv3, and CLI. The example screenshots below show SNMP v1/v2, SNMP3, and CLI. When done entering credentials click on **Save & Close**.



Infoblox (Grid Discovery Properties)

SNMPv1/SNMPv2

☐	Read Community	Order	Comment
☐	publican	1	
☐	infoblox	2	
☐	public	3	

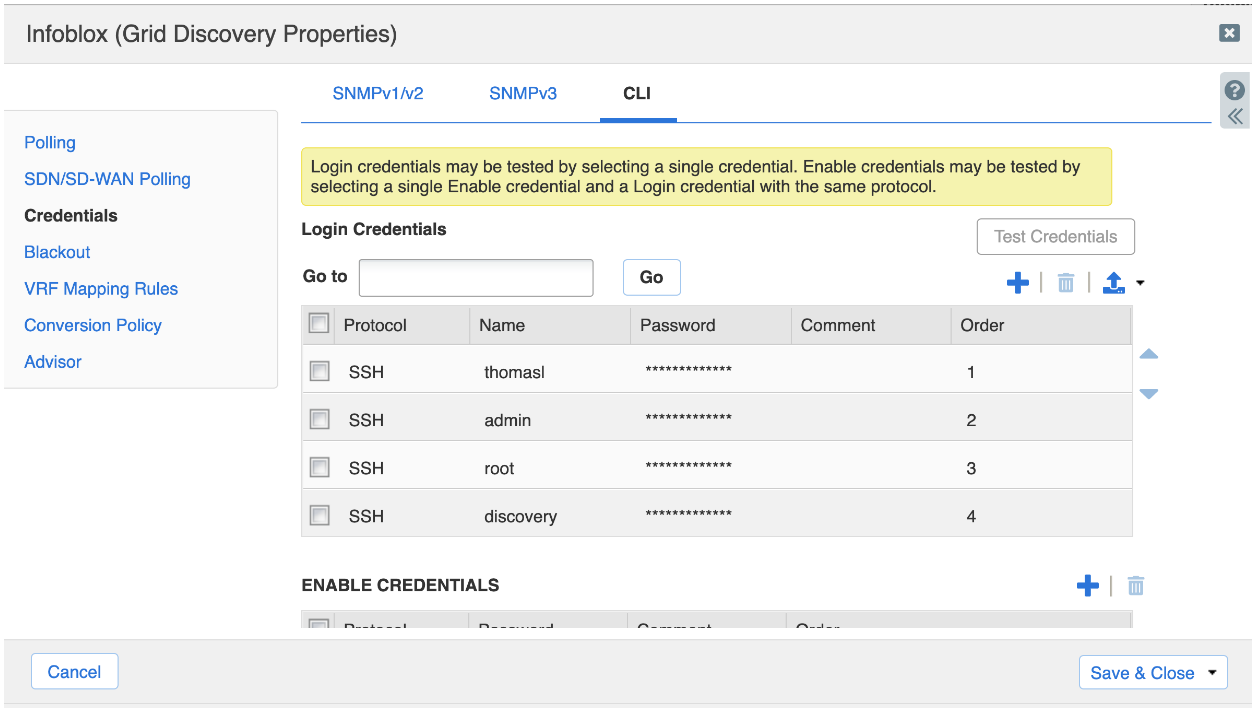


Infoblox (Grid Discovery Properties)

The uniqueness of SNMPv3 credentials is determined by a combination of the name, auth protocol and privacy protocol. If you change any of these fields for an existing credential, you must re-enter the passwords for the corresponding protocols.

SNMPv3

☐	Name	Auth Proto…	Auth Password	Privacy Protocol	Privacy Password	Order
☑	vista	MD5	********	AES	********	1


Infoblox (Grid Discovery Properties)

Login credentials may be tested by selecting a single credential. Enable credentials may be tested by selecting a single Enable credential and a Login credential with the same protocol.

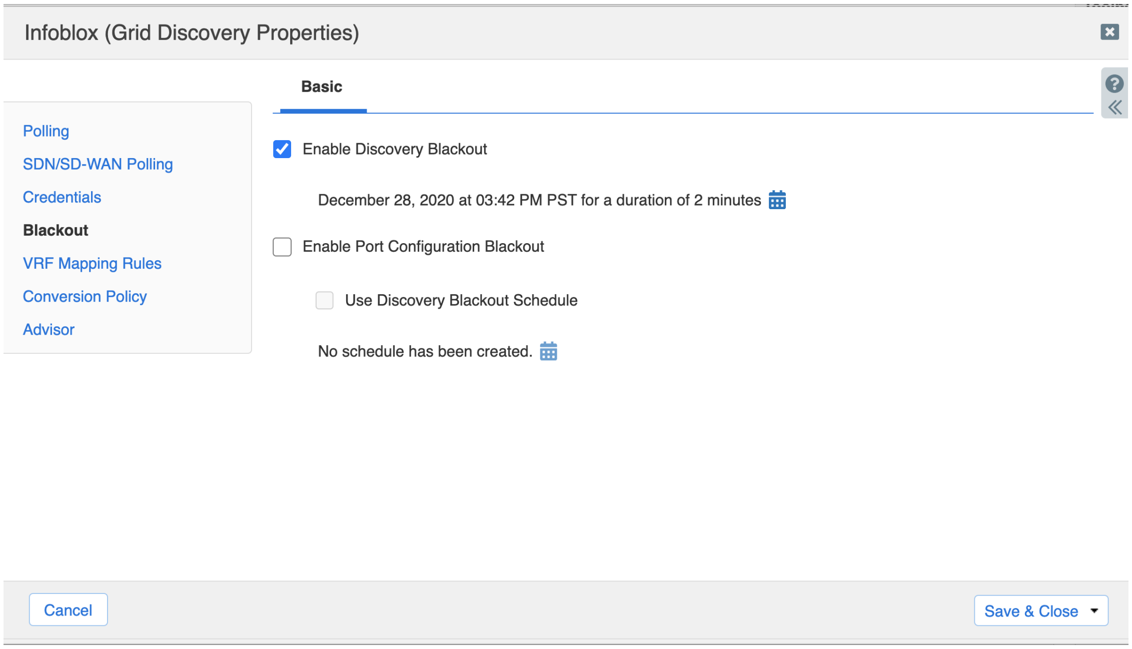
Login Credentials

□	Protocol	Name	Password	Comment	Order
□	SSH	thomasl	**************		1
□	SSH	admin	**************		2
□	SSH	root	**************		3
□	SSH	discovery	**************		4

ENABLE CREDENTIALS

Blackout

Network Insight performs discovery constantly. Each network device is polled roughly once an hour. However, if your network policies dictate a blackout period for non-essential network services, you can define a blackout period. Click on the **Blackout** button. Click on **Save & Close** when done.


Infoblox (Grid Discovery Properties)

☑ Enable Discovery Blackout

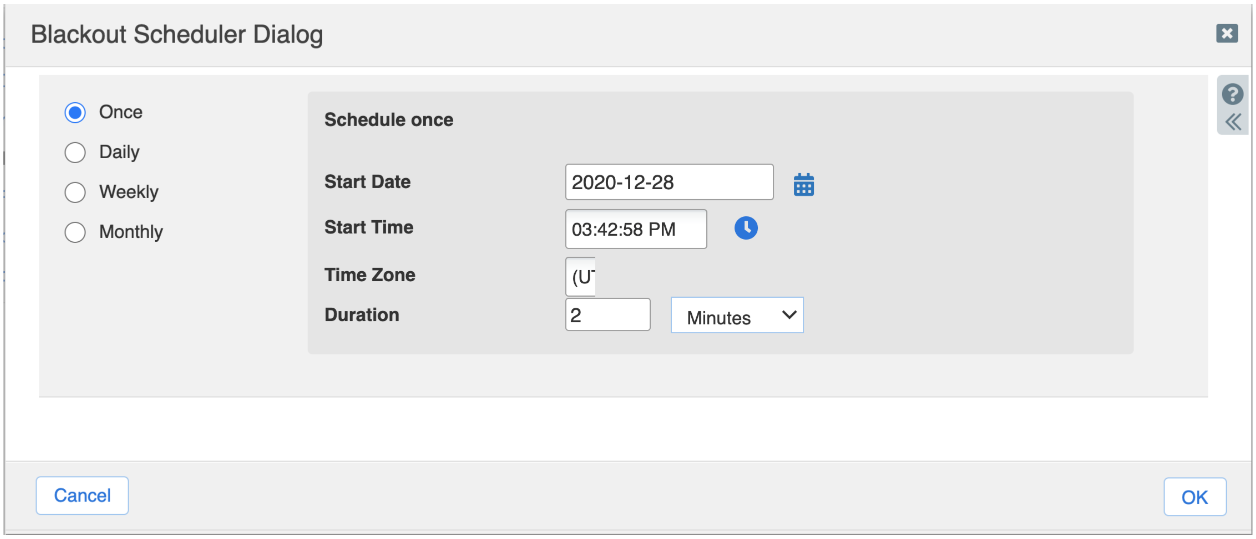
December 28, 2020 at 03:42 PM PST for a duration of 2 minutes

□ Enable Port Configuration Blackout

□ Use Discovery Blackout Schedule

No schedule has been created.

Click on the **Enable Discovery Blackout** box to enable and then click on the calendar below. Click **OK** when done.



Blackout Scheduler Dialog

- ● Once
- ○ Daily
- ○ Weekly
- ○ Monthly

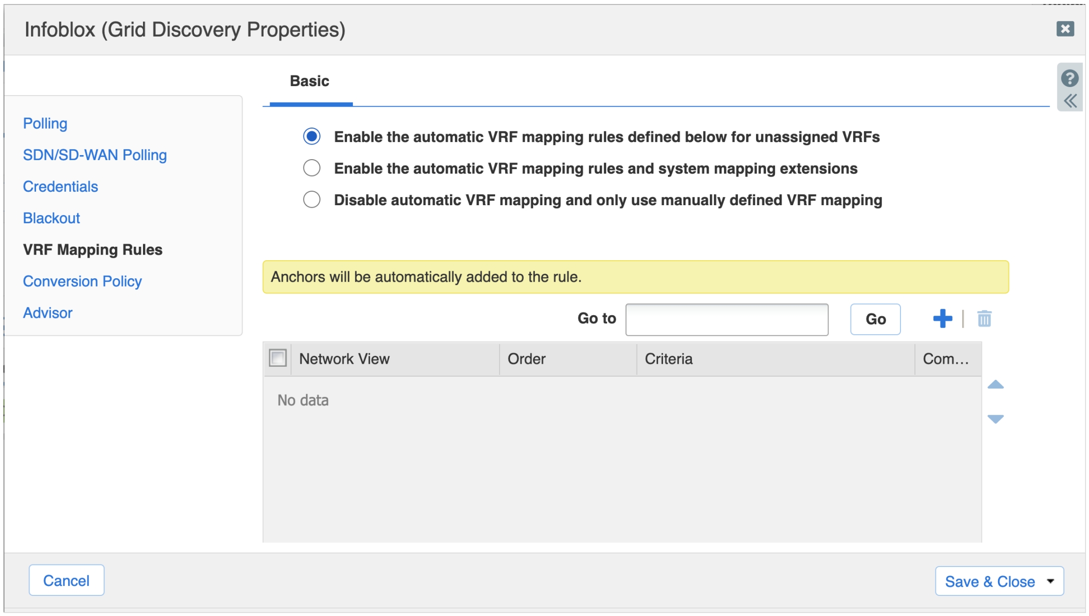
Schedule once

Start Date	2020-12-28
Start Time	03:42:58 PM
Time Zone	(U
Duration	2 Minutes

Note: The duration can be set for X amount of minutes, hours, or days. Click ***OK*** *when done*

VRF Mapping Rules

If you are using Network Insight in a VRF environment, you'll need to map VRFs to Network Views. This can be done manually or you can configure rules to do the mapping automatically.



Infoblox (Grid Discovery Properties)

- ● Enable the automatic VRF mapping rules defined below for unassigned VRFs
- ○ Enable the automatic VRF mapping rules and system mapping extensions
- ○ Disable automatic VRF mapping and only use manually defined VRF mapping

Anchors will be automatically added to the rule.

□ Network View	Order	Criteria	Com...
No data			

- **Enable the automatic VRF mapping rules defined below for unassigned VRFs**: Select this to enable automatic VRF mapping so you can define mapping rules that Network Insight uses to map network views to unassigned VRFs that match the criteria of the rules.
- **Enable the automatic VRF mapping rules and system mapping extensions**: Select this to enable the VRF Mapping Rules table so you can define mapping rules that Network Insight uses to map network views to unassigned VRFs that match the criteria of the rules; and in cases where none of the rules match a VRF name, Network Insight maps the VRF to the network view from which one of the interfaces the unassigned VRF is reached.
- **Disable automatic VRF mapping and only use manually defined VRF mapping**: Select this to disable the VRF Mapping Rules table. When you select this, Network Insight does not perform any evaluation of the VRF mapping rules. You can manually assign or unassign network views to the discovered VRFs.

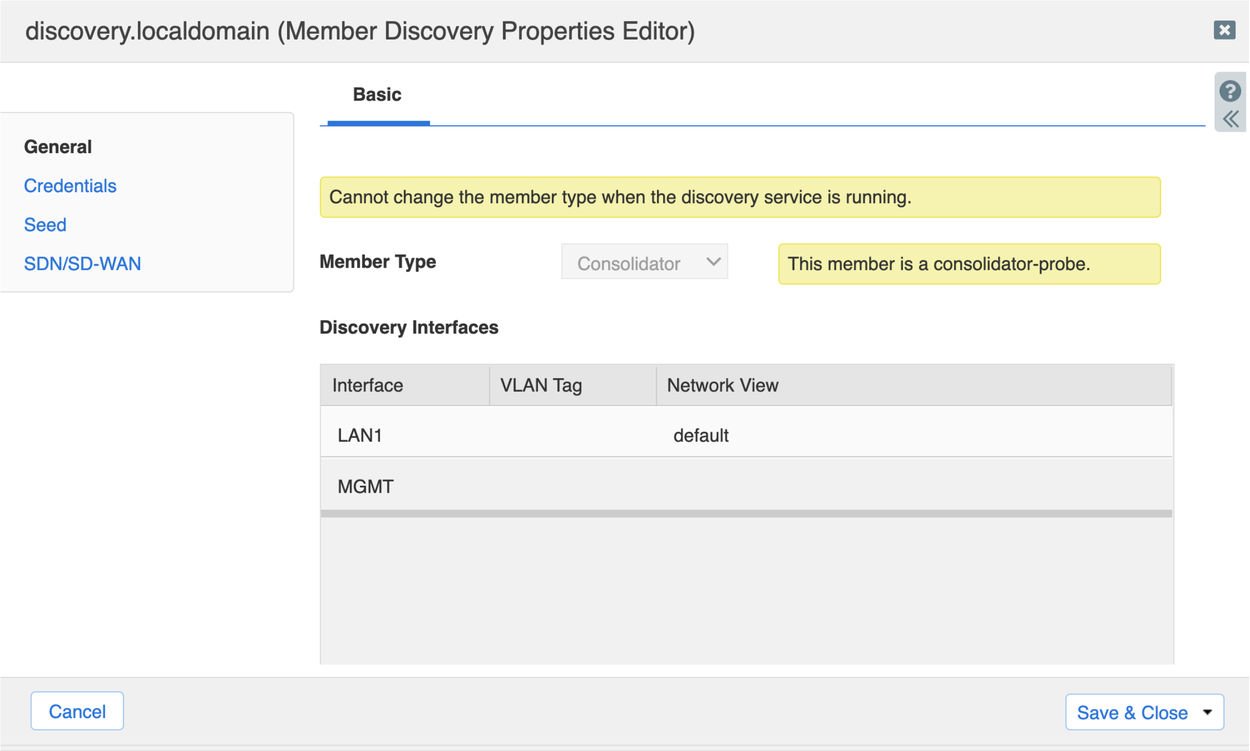
When you enable automatic VRF mapping, you can add mapping rules to the VRF Mapping Rules table, as follows:

1. Click the **Add** icon, and the appliance adds a row to the table.
2. In the table, click each of the following fields and enter the values accordingly:
   - **Network View**: The network view that you want to use for all matching VRFs. You can click this field and select a network view from the drop-down list that displays all the configured network views, including the default network view.
   - **Order**: The order and priority in which Network Insight evaluates the mapping rules. Each time you add a new rule, the appliance automatically appends the rule to the end of the list and assigns the next incremental number to the rule. To reorder the list, you can select a rule and use the up and down arrows next to the table to move the rules to its desired position so you can set the priority for the rule evaluation. Network Insight evaluates the rules based on the order, starting with 1 as the highest priority.
   - **Criteria**: The criteria that Network Insight uses to match the VRF name of an unassigned VRF. You can use POSIX regular expressions to define the mapping criteria. The appliance validates the rule when you save the configuration, and it returns an error message if the criteria is invalid. For more information about regular expressions,
   - **Comment**: Enter a comment about the VRF mapping rule. Click the **Add** icon again to define another mapping rule.
3. **Save** the configuration

Adding a Seed Router

An important item in network discovery is adding a seed router. Network Insight will use the seed router to access the routing table to discover the network. The recommendation is to use a seed router that is in the core of the network or closest to the core of the network. To add a seed router, use the following instructions:

1. Navigate to **Grid** → **Grid Manager** → **Discovery**.



discovery.localdomain (Member Discovery Properties Editor)

Cannot change the member type when the discovery service is running.

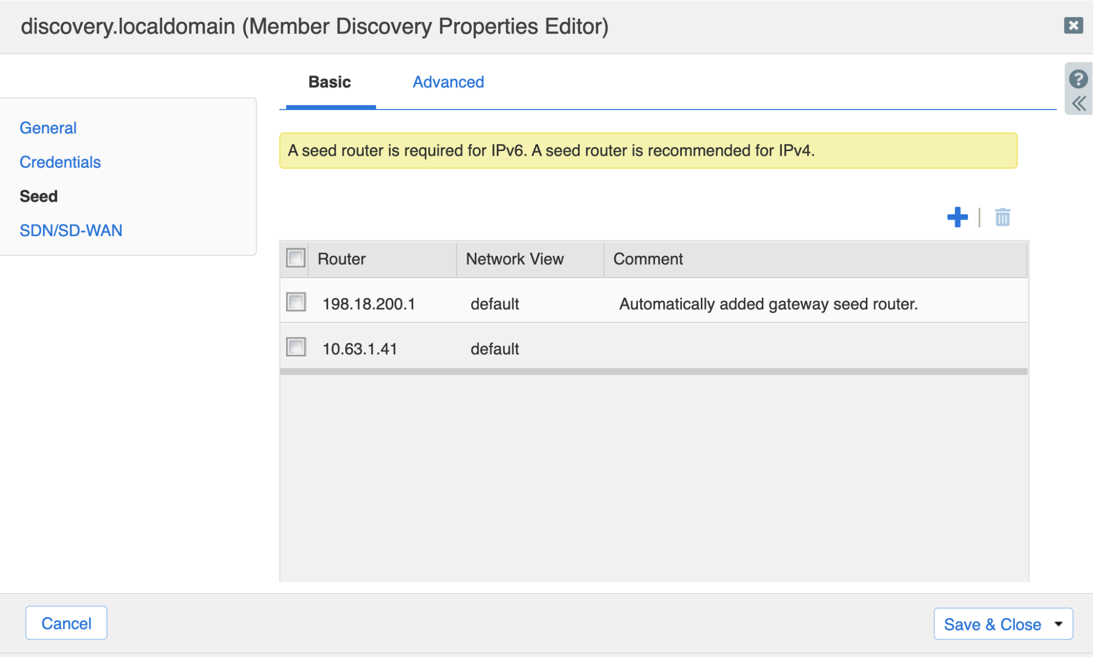
Member Type: Consolidator

This member is a consolidator-probe.

Discovery Interfaces

Interface	VLAN Tag	Network View
LAN1		default
MGMT		

2. Click on the **Seed** button.



discovery.localdomain (Member Discovery Properties Editor)

A seed router is required for IPv6. A seed router is recommended for IPv4.

□	Router	Network View	Comment
□	198.18.200.1	default	Automatically added gateway seed router.
□	10.63.1.41	default	

3. Click on the **+** button to add a seed router and then type in the IP address of the seed router under the router column. Click **Save & Close**.
4. Define a top-level Network Container to consolidate IP subnets. For example, create a network container like 10.0.0.0/8 to contain all of the subnets under the 10 networks.

Conversion Procedures

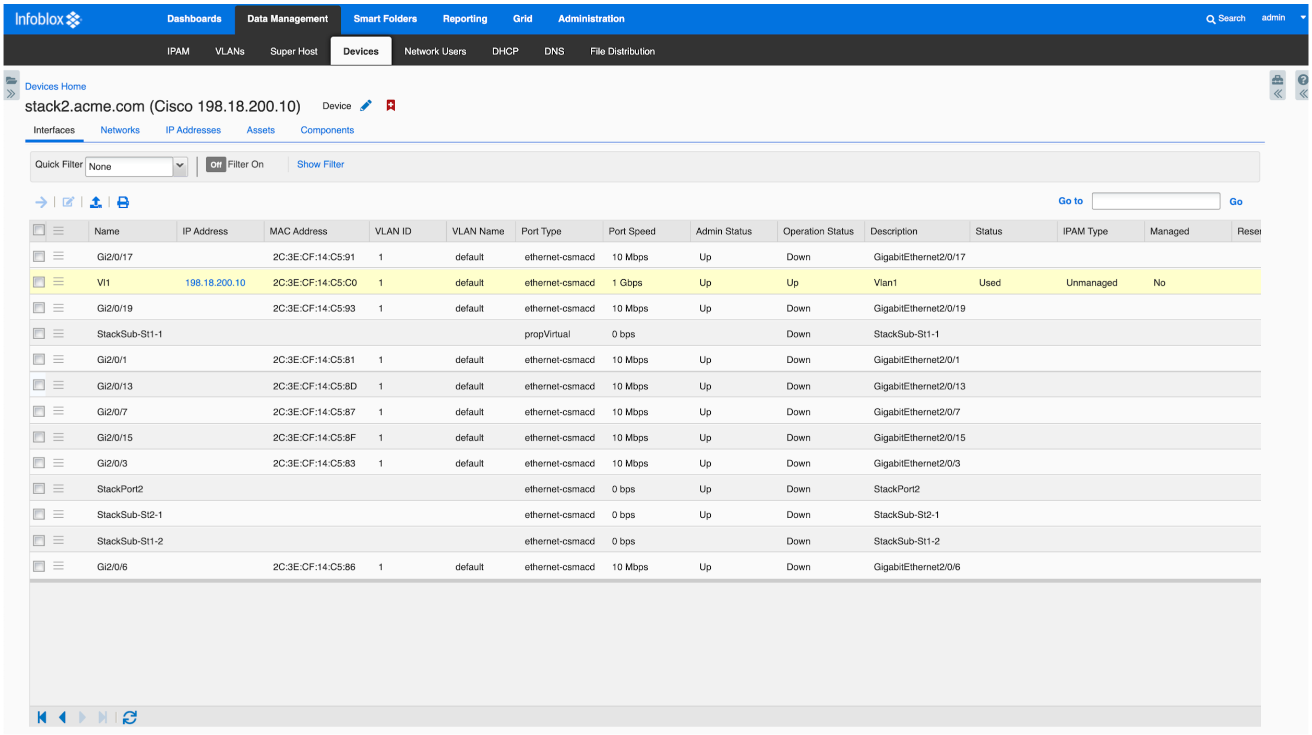
After a discovery, key information is collected and displayed in the **Data Management**, **Devices**, **Interfaces**, **Networks**, **IP Addresses**, and **Assets** tabs of Grid Manager. You can view information about each discovered entity in one of these tabs.

A discovered entity is considered unmanaged if it is discovered in a network for which no information is being stored in the NIOS database. You are not able to configure unmanaged objects in NIOS. Depending on the nature of the discovered entity, you may convert certain unmanaged entities into managed objects so you can manage them through Grid Manager. When an entity is in the managed state, you can configure settings such as applying permissions to it, limiting who can modify the configurations and deployments, and when those changes can be applied. You cannot do so with unmanaged objects. Grid Manager allows you to convert certain unmanaged devices, interfaces, networks, and assets to the following IPAM object types:

- When converting unmanaged entities to managed objects in NIOS, you can choose to convert them one at a time or as a group.
- To convert a single entity, just select a specific entity and perform the conversion. To convert multiple entities to the same IPAM object type, you can select the entities you want to manage and then perform a bulk conversion.

Converting Unmanaged Devices to Managed Devices

1. Navigate to **Data Management** → **Devices.**



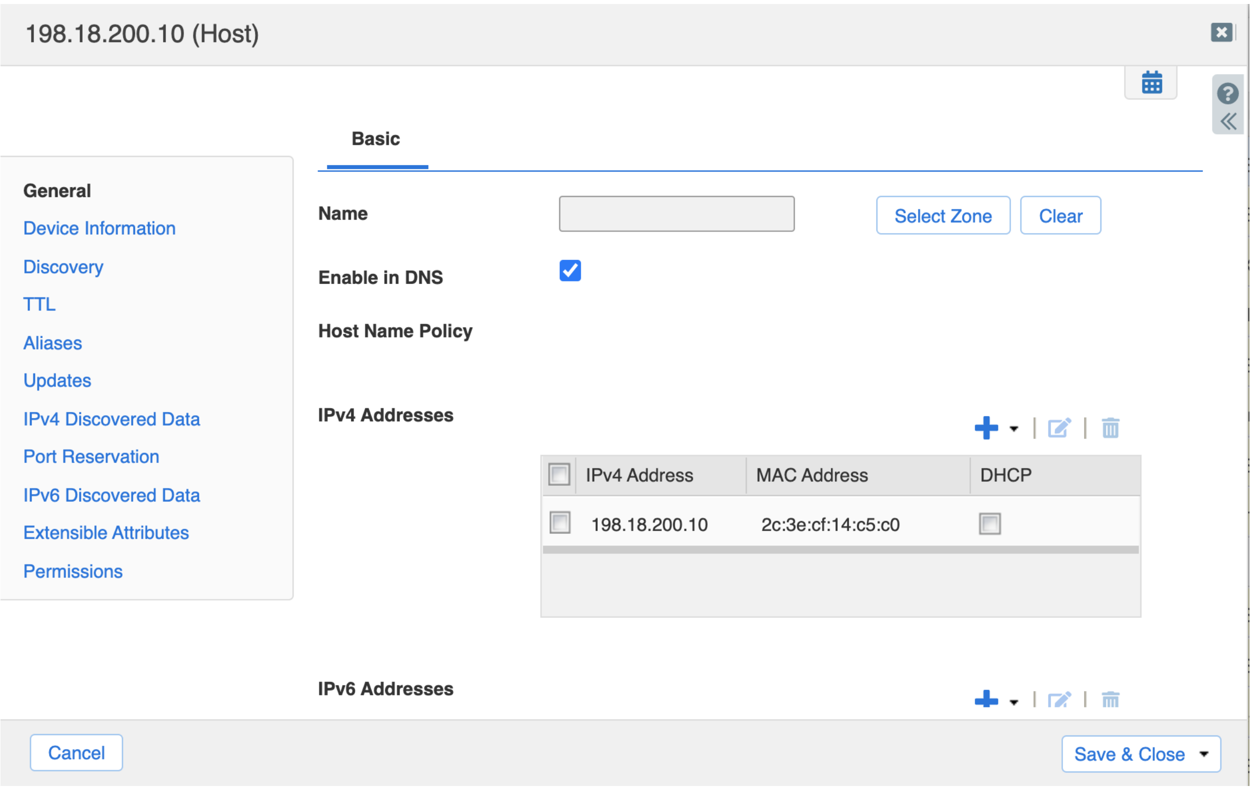
stack2.acme.com (Cisco 198.18.200.10) Device

Quick Filter: None | Off Filter On | Show Filter

Name	IP Address	MAC Address	VLAN ID	VLAN Name	Port Type	Port Speed	Admin Status	Operation Status	Description	Status	IPAM Type	Managed	Reser
Gi2/0/17		2C:3E:CF:14:C5:91	1	default	ethernet-csmacd	10 Mbps	Up	Down	GigabitEthernet2/0/17				
Vl1	198.18.200.10	2C:3E:CF:14:C5:C0	1	default	ethernet-csmacd	1 Gbps	Up	Up	Vlan1	Used	Unmanaged	No	
Gi2/0/19		2C:3E:CF:14:C5:93	1	default	ethernet-csmacd	10 Mbps	Up	Down	GigabitEthernet2/0/19				
StackSub-St1-1					propVirtual	0 bps		Down	StackSub-St1-1				
Gi2/0/1		2C:3E:CF:14:C5:81	1	default	ethernet-csmacd	10 Mbps	Up	Down	GigabitEthernet2/0/1				
Gi2/0/13		2C:3E:CF:14:C5:8D	1	default	ethernet-csmacd	10 Mbps	Up	Down	GigabitEthernet2/0/13				
Gi2/0/7		2C:3E:CF:14:C5:87	1	default	ethernet-csmacd	10 Mbps	Up	Down	GigabitEthernet2/0/7				
Gi2/0/15		2C:3E:CF:14:C5:8F	1	default	ethernet-csmacd	10 Mbps	Up	Down	GigabitEthernet2/0/15				
Gi2/0/3		2C:3E:CF:14:C5:83	1	default	ethernet-csmacd	10 Mbps	Up	Down	GigabitEthernet2/0/3				
StackPort2					ethernet-csmacd	0 bps	Up	Down	StackPort2				
StackSub-St2-1					ethernet-csmacd	0 bps	Up	Down	StackSub-St2-1				
StackSub-St1-2					ethernet-csmacd	0 bps		Down	StackSub-St1-2				
Gi2/0/6		2C:3E:CF:14:C5:86	1	default	ethernet-csmacd	10 Mbps	Up	Down	GigabitEthernet2/0/6				

2. Select a device that has a No in the Managed column. In the screenshot above, we will select the switch name of '**stack2.acme.com**'.
3. Click on the corresponding wheel for switch '**stack2.acme.com**'. Select **Convert** and this expands to another menu. Select either **To Host**, **To A Record**, **To PTR Record** or **To Fixed Address**.

An editor for each of the selections will appear like the following:



Name

Enable in DNS ☑

Host Name Policy

IPv4 Addresses

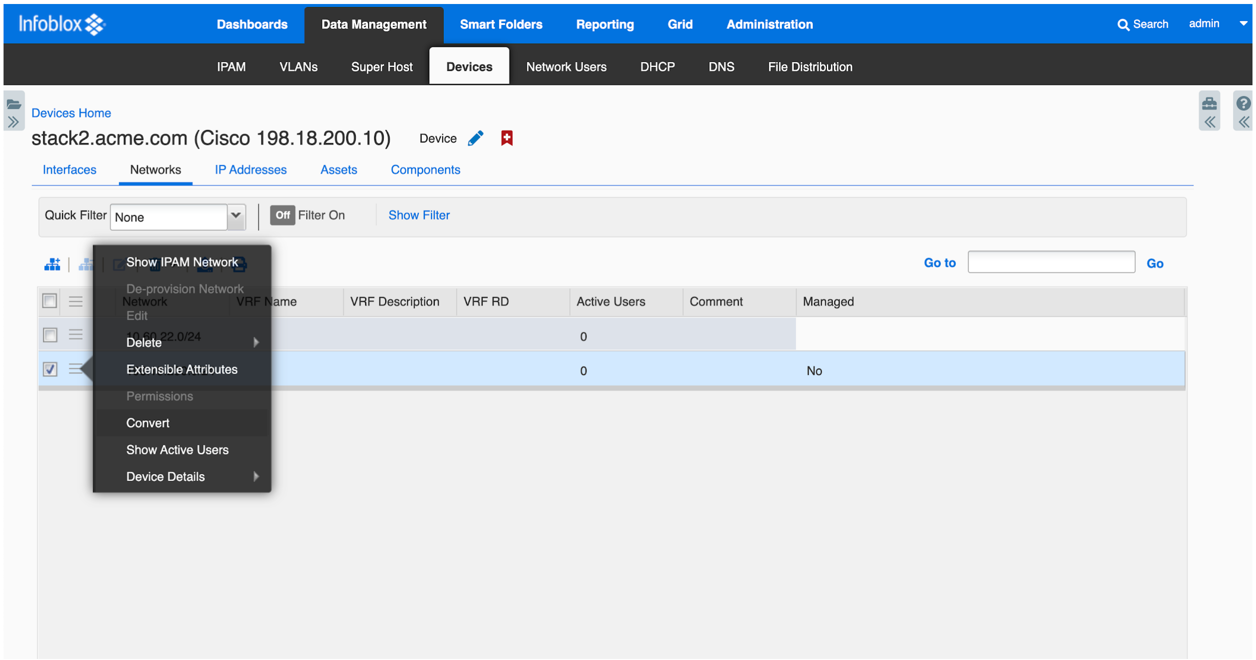
□	IPv4 Address	MAC Address	DHCP
□	198.18.200.10	2c:3e:cf:14:c5:c0	□

IPv6 Addresses

4. Fill in the field for the General tab. You can also define the other settings if needed. Refer to online help for more details.
5. Click **Save & Close**.

Convert Unmanaged Interfaces to Managed Status

Interfaces that appear in the Interfaces table for a device may be converted to managed status, under specific circumstances. If an interface is bound to an IP address that is present in an IPAM network (for example, a leaf network inside a network container under IPAM), that interface can be converted to managed status.



stack2.acme.com (Cisco 198.18.200.10)

Quick Filter: None

Off Filter On

Network	VRF Name	VRF Description	VRF RD	Active Users	Comment	Managed
10.60.22.0/24				0		
				0		No

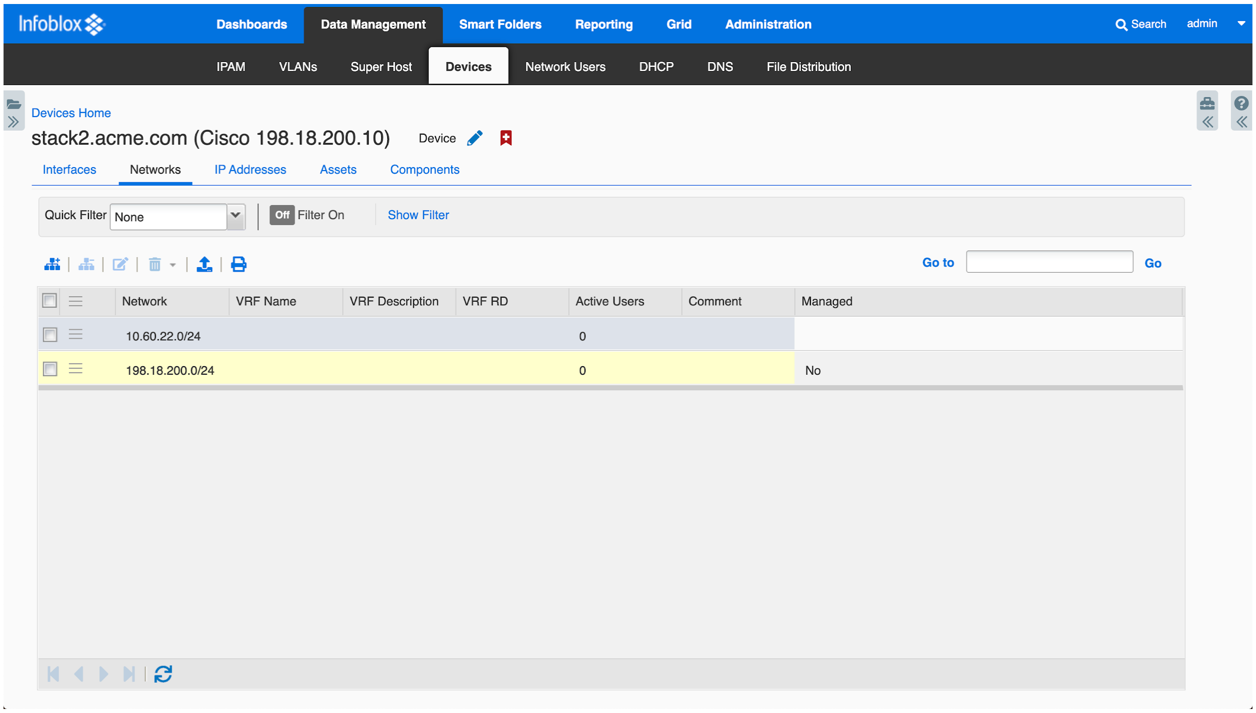
1. From the **Data Management** tab, select the **Devices** tab.
2. Click the **Next Page** and **Last Page** icons to locate the device through which you want to locate the interfaces to convert.
3. Click the **Name** link of the device.
4. Click the **Interfaces** tab for the chosen device. This tab lists all ports discovered on the device.
5. To convert a single interface, click the **Action** icon next to the interface you want to convert (this automatically selects it) select **Convert** → **To Host**, **To A Record**, **To PTR Record**, or **To Fixed Address** from the menu.
6. To convert multiple interfaces (bulk conversion), select the checkboxes of the interfaces you want to convert.
7. From the Toolbar, select **Convert** → **To Host, To A & PTR Record, or To Fixed Address**.
8. **For a single interface**: The respective object editor appears based on the conversion type you have selected. For example, if you select To Host, the Host editor appears.

In the editor, define the required General settings for the new object. You can also define other settings you need from any of the tabs in the editor. For details about how to configure these settings, refer to the online Help in Grid Manager or see the appropriate chapters in this guide.

Convert Unmanaged Networks to Managed Status

Unmanaged networks listed under discovered devices present the same conversion features as networks listed under IPAM.

1. Begin by examining the **Data Management** → **Devices** page,
2. Click a discovered device name's wheel icon and click the device name hotlink.
3. Open the **Networks** tab. The Managed column shows one of three possible states for all discovered networks on each device:
    - **Blank value**–indicates that the network is not known to IPAM, because insufficient information is available to identify and catalog the network at the present time, or because the network listed at the device level is for a loopback interface, a disconnected network, or a network prefix that is overlapped by a larger network encompassing that prefix and defined in IPAM. These are also called non-NIOS networks. At the device level, non-NIOS networks are highlighted in light grey;
    - **No**–indicates that the network is not managed under IPAM/Grid Manager, but enough information is catalogued that the network can be converted to Managed state. This state is required before a network can be converted to managed status. Networks in this state are highlighted in yellow.
    - **Yes**–The network is currently managed under IPAM, converted to an IPAM network. At the device level, managed networks are highlighted in white.
4. Navigate to **Data Management** → **Devices** → **Selected Device** → **Networks**.



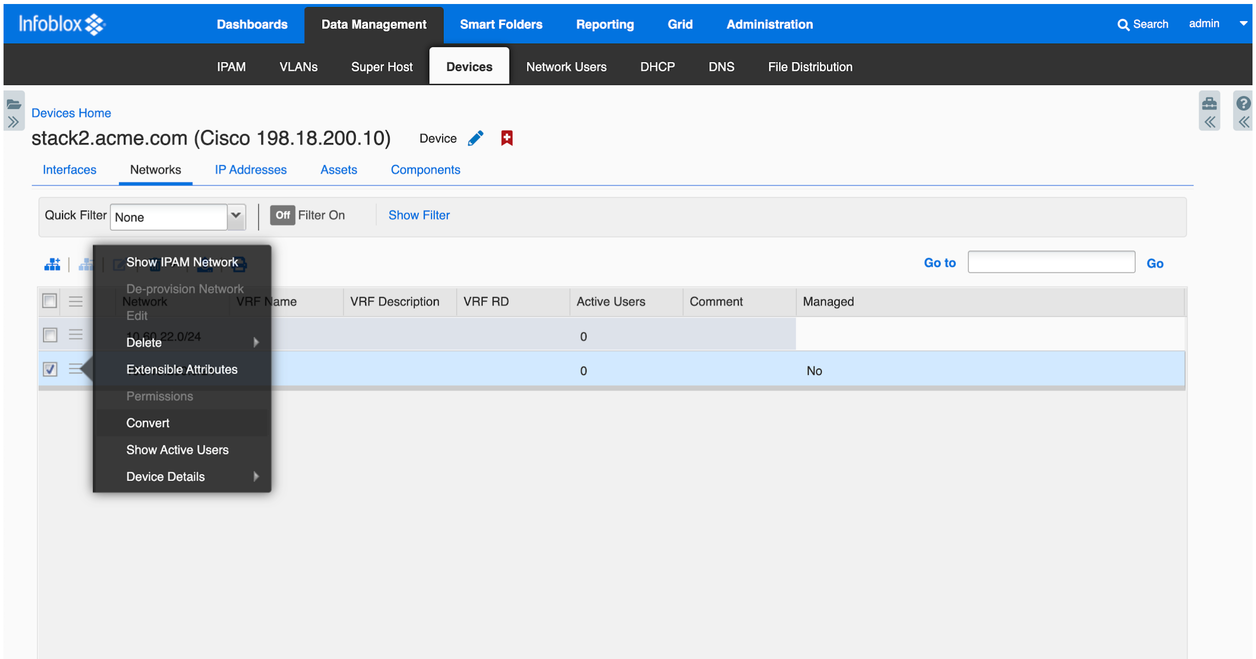
stack2.acme.com (Cisco 198.18.200.10) Device

Quick Filter None

Off Filter On

□	☰	Network	VRF Name	VRF Description	VRF RD	Active Users	Comment	Managed
□	☰	10.60.22.0/24				0		
□	☰	198.18.200.0/24				0		No

5. Click on the **hamburger** icon.

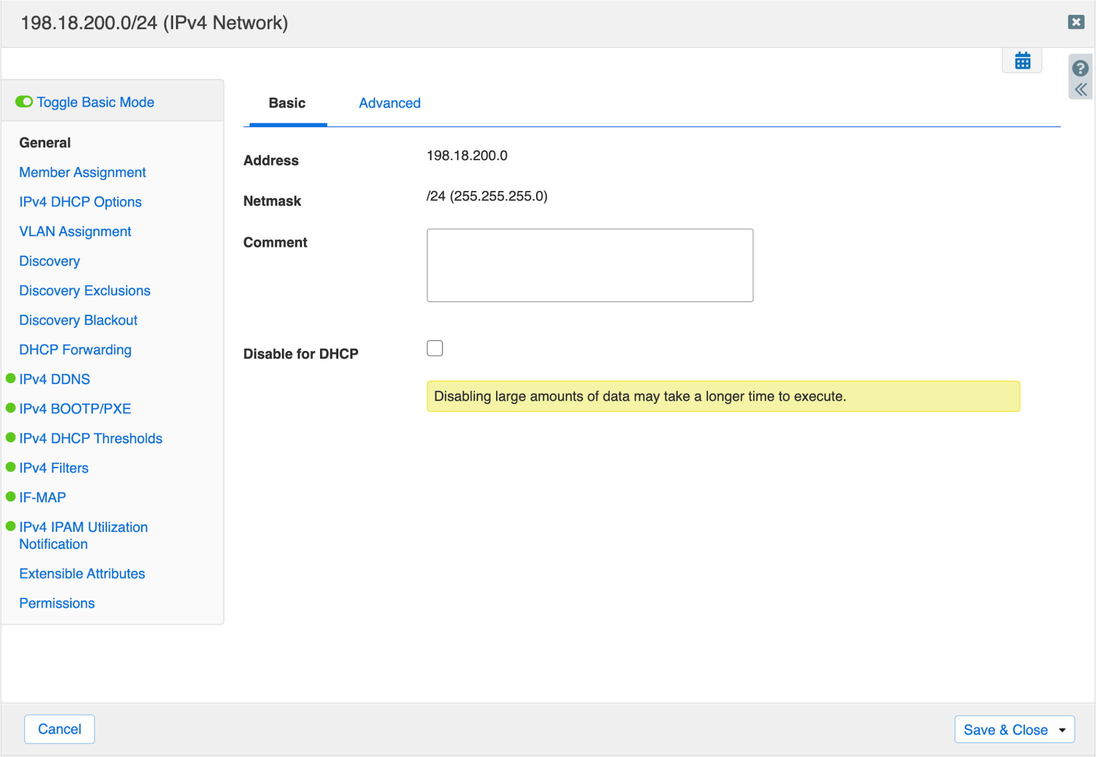


stack2.acme.com (Cisco 198.18.200.10)

Quick Filter: None

Network	VRF Name	VRF Description	VRF RD	Active Users	Comment	Managed
10.60.22.0/24				0		
				0		No

6. Click **Convert**.



198.18.200.0/24 (IPv4 Network)

Address	198.18.200.0
Netmask	/24 (255.255.255.0)
Comment	
Disable for DHCP	□

Disabling large amounts of data may take a longer time to execute.

7. Fill in the General section and any other sections.

8. Click **Save & Close**.

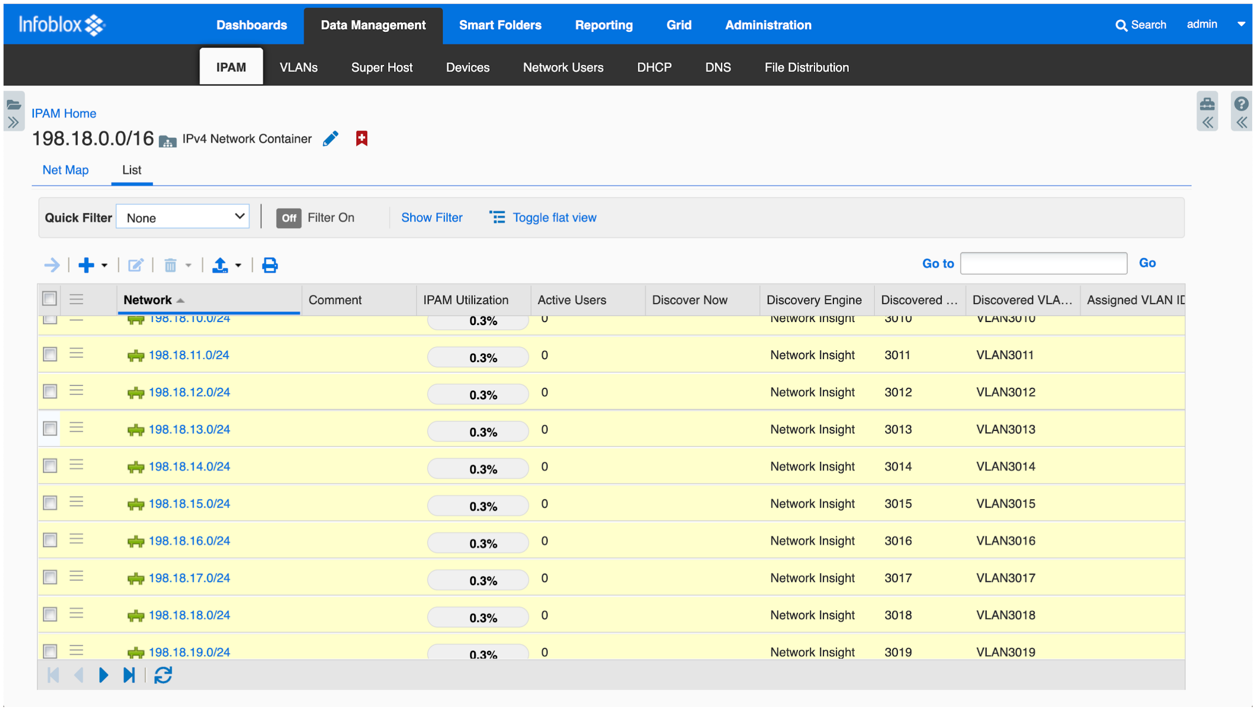
Convert Unmanaged Networks under IPAM to Managed Status

The IPAM tab lists all discovered networks as unmanaged, highlighted in yellow. Administrators cannot apply services or IPAM objects to IP addresses in unmanaged networks until the networks are converted to managed status. You can explore unmanaged networks through the IP Map and IP List views, but many operations cannot be carried out on unmanaged networks, including editing, splitting, resizing, permissions changes and other tasks.

1. Unmanaged networks can be converted at the IPAM main page and at the device level under **Data Management** → **Devices**, selecting a device and opening the Networks page.
2. Under IPAM, the **Managed** column for the Network tables can show one of two possible states for all discovered IPAM networks:
   - ○ **No**–Shows that the network is not managed under IPAM/Grid Manager, but enough information is catalogued that the device can be converted to Managed state. This state is required before a network can be converted to Managed status.

   - ○ **Yes**–The network shown in the table is now Managed under IPAM, converted to an IPAM network.

3. Navigate to **Data Management** → **IPAM** → **selected network container** (if needed)

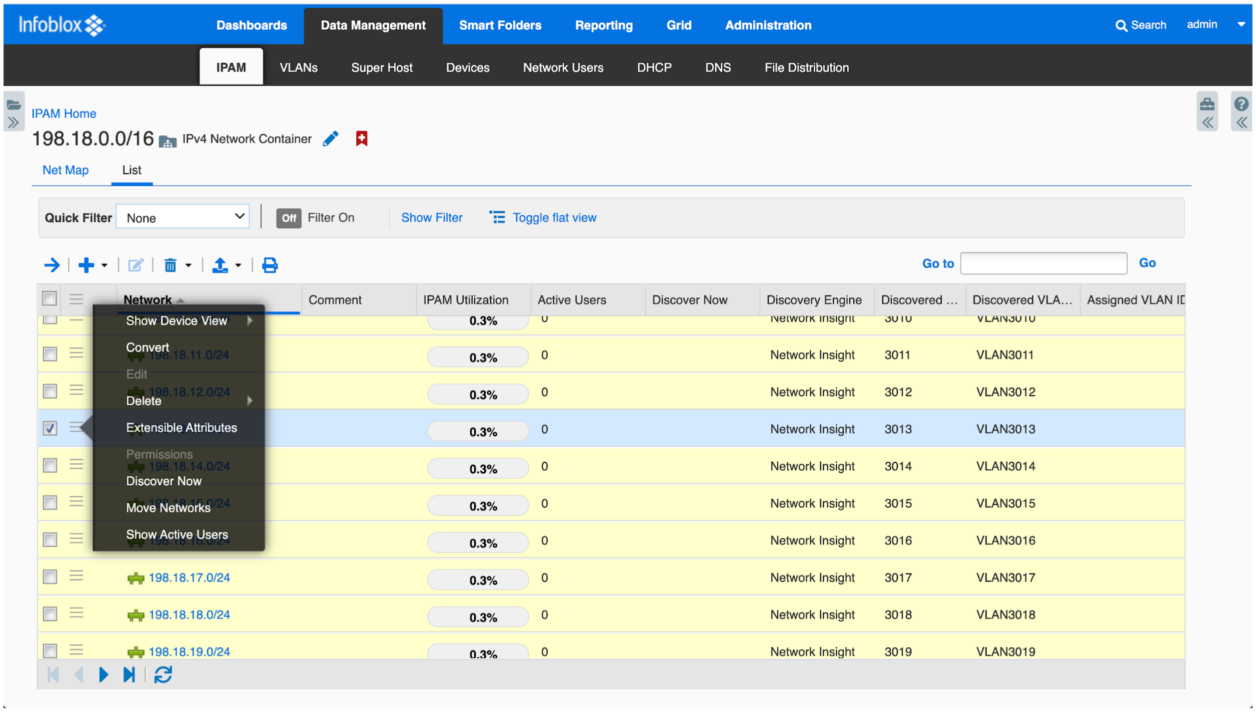


198.18.0.0/16 IPv4 Network Container

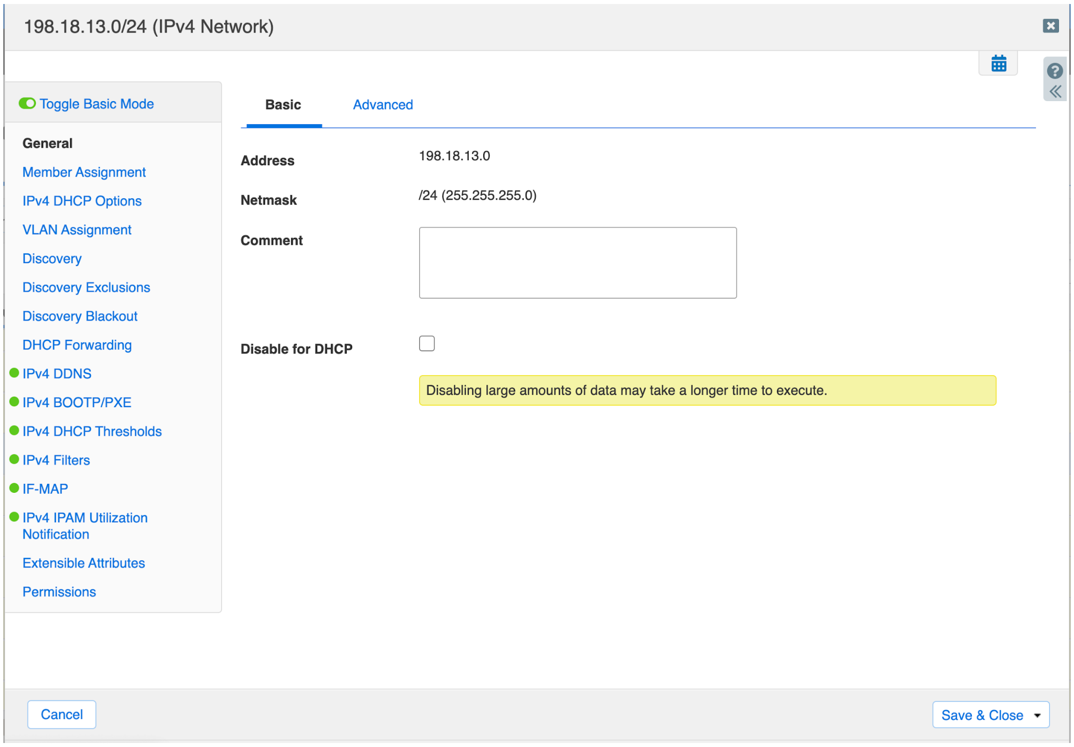
None

Network	Comment	IPAM Utilization	Active Users	Discover Now	Discovery Engine	Discovered ...	Discovered VLA...	Assigned VLAN ID
198.18.10.0/24		0.3%	0		Network Insight	3010	VLAN3010	
198.18.11.0/24		0.3%	0		Network Insight	3011	VLAN3011	
198.18.12.0/24		0.3%	0		Network Insight	3012	VLAN3012	
198.18.13.0/24		0.3%	0		Network Insight	3013	VLAN3013	
198.18.14.0/24		0.3%	0		Network Insight	3014	VLAN3014	
198.18.15.0/24		0.3%	0		Network Insight	3015	VLAN3015	
198.18.16.0/24		0.3%	0		Network Insight	3016	VLAN3016	
198.18.17.0/24		0.3%	0		Network Insight	3017	VLAN3017	
198.18.18.0/24		0.3%	0		Network Insight	3018	VLAN3018	
198.18.19.0/24		0.3%	0		Network Insight	3019	VLAN3019	

4. Select a network and click on the corresponding hamburger icon.
5. Click **Convert**.



☐	Network	Comment	IPAM Utilization	Active Users	Discover Now	Discovery Engine	Discovered ...	Discovered VLA...	Assigned VLAN ID
☐			0.3%	0		Network Insight	3010	VLAN3010	
☐	198.18.11.0/24		0.3%	0		Network Insight	3011	VLAN3011	
☐	198.18.12.0/24		0.3%	0		Network Insight	3012	VLAN3012	
☑			0.3%	0		Network Insight	3013	VLAN3013	
☐	198.18.14.0/24		0.3%	0		Network Insight	3014	VLAN3014	
☐	198.18.15.0/24		0.3%	0		Network Insight	3015	VLAN3015	
☐	198.18.16.0/24		0.3%	0		Network Insight	3016	VLAN3016	
☐	198.18.17.0/24		0.3%	0		Network Insight	3017	VLAN3017	
☐	198.18.18.0/24		0.3%	0		Network Insight	3018	VLAN3018	
☐	198.18.19.0/24		0.3%	0		Network Insight	3019	VLAN3019	


198.18.13.0/24 (IPv4 Network)

Address	198.18.13.0
Netmask	/24 (255.255.255.0)
Comment	
Disable for DHCP	☐

Disabling large amounts of data may take a longer time to execute.

6. Fill in the **General Section** and any other sections.
7. Click **Save & Close.**

Automating Converting Unmanaged Networks to Managed Status

To automate the conversion of IP addresses of discovered entities from “unmanaged” to “managed” in a specific network view, you can configure conversion rules that Network Insight uses to automatically create new DNS records or update existing data for the discovered IP addresses. Network Insight automatically converts newly discovered IP addresses to host records, A and PTR records, or fixed addresses based on your configuration. You can define templates that Network Insight uses to create new records by using supported variables and functions.

Note that corresponding DNS zones in a selected network view must already exist in order for Network Insight to add DNS records during the conversion. Otherwise, Network Insight does not add any DNS records and it logs a message to the syslog.

Network Insight automatically adds DNS records based on the following conditions:

- The corresponding DNS zones must already exist in the NIOS database. Network Insight does not automatically create DNS zones for the records.

- To create a PTR record, the corresponding reverse-mapping zone must exist.

- A DNS zone cannot be associated with more than one DNS view. Network Insight does not create DNS records for zones that are associated with multiple DNS views.

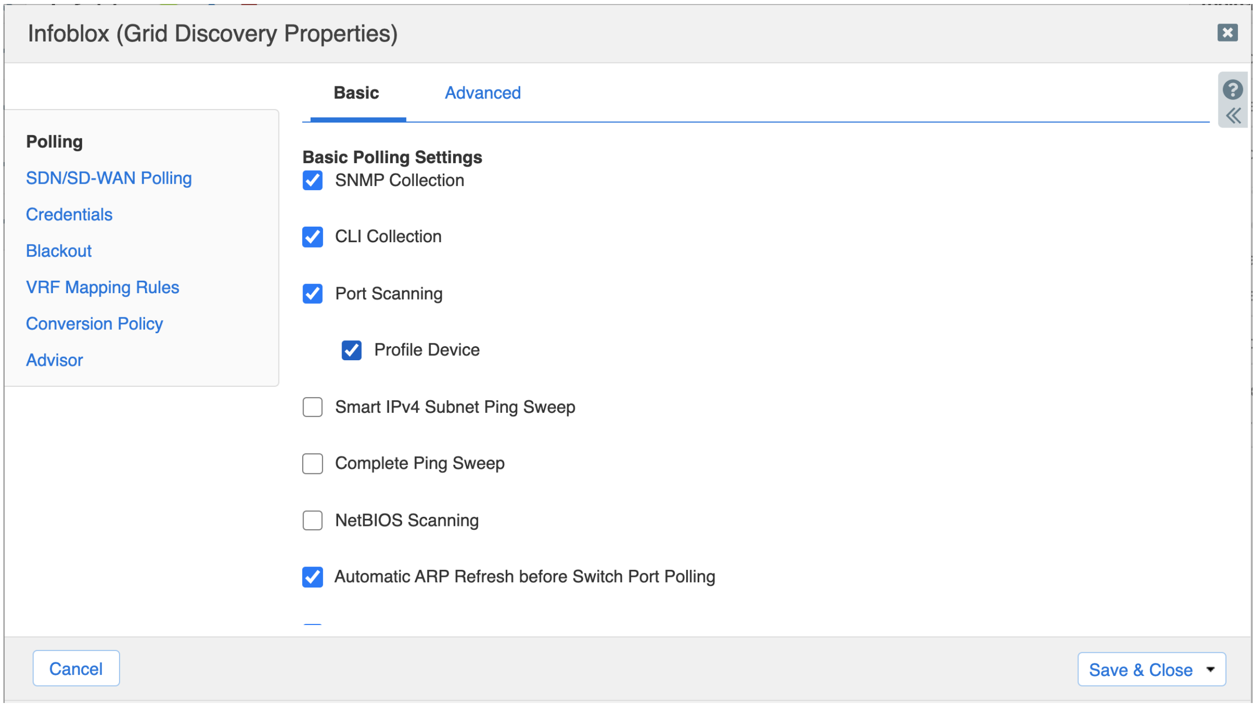
- NIOS adds new DNS records only if the discovered_name for the discovered IP address is available and there is no conflict with information about the associated network view.

On subsequent discovery jobs, if an IP for a VM is removed, the corresponding DNS records are removed accordingly. If the IP for a VM is changed, the IP address in the corresponding DNS record is changed accordingly. If the DNS record name template is changed, all the DNS records are replaced with the DNS records using the new template. All administrative actions for these changes are recorded in the audit log. Summary of the changes are logged in the syslog.

Note: Network Insight updates only records that are created by the Network Insight process. It does not create or update DNS records that are originally created by other admin users.

To add automatic conversion rules:

1. Navigate to **Grid** → **Grid Manager**.
2. In the **Toolbar** → **Edit** → **Grid Discovery Properties**.



Infoblox (Grid Discovery Properties)

Basic | Advanced

Polling
SDN/SD-WAN Polling
Credentials
Blackout
VRF Mapping Rules
Conversion Policy
Advisor

Basic Polling Settings

☑ SNMP Collection

☑ CLI Collection

☑ Port Scanning

☑ Profile Device

□ Smart IPv4 Subnet Ping Sweep

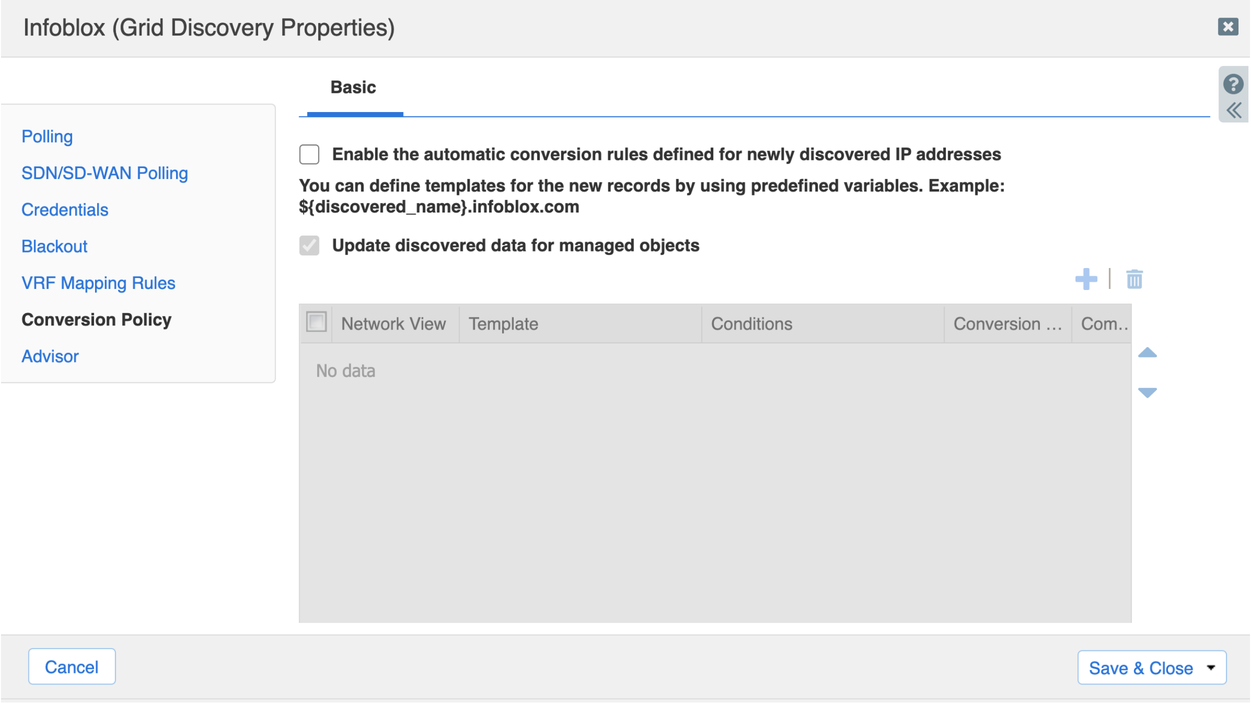
□ Complete Ping Sweep

□ NetBIOS Scanning

☑ Automatic ARP Refresh before Switch Port Polling

Cancel | Save & Close

3. Click on the **Conversion Policy** tab.



Infoblox (Grid Discovery Properties)

Basic

Polling
SDN/SD-WAN Polling
Credentials
Blackout
VRF Mapping Rules
Conversion Policy
Advisor

□ **Enable the automatic conversion rules defined for newly discovered IP addresses**

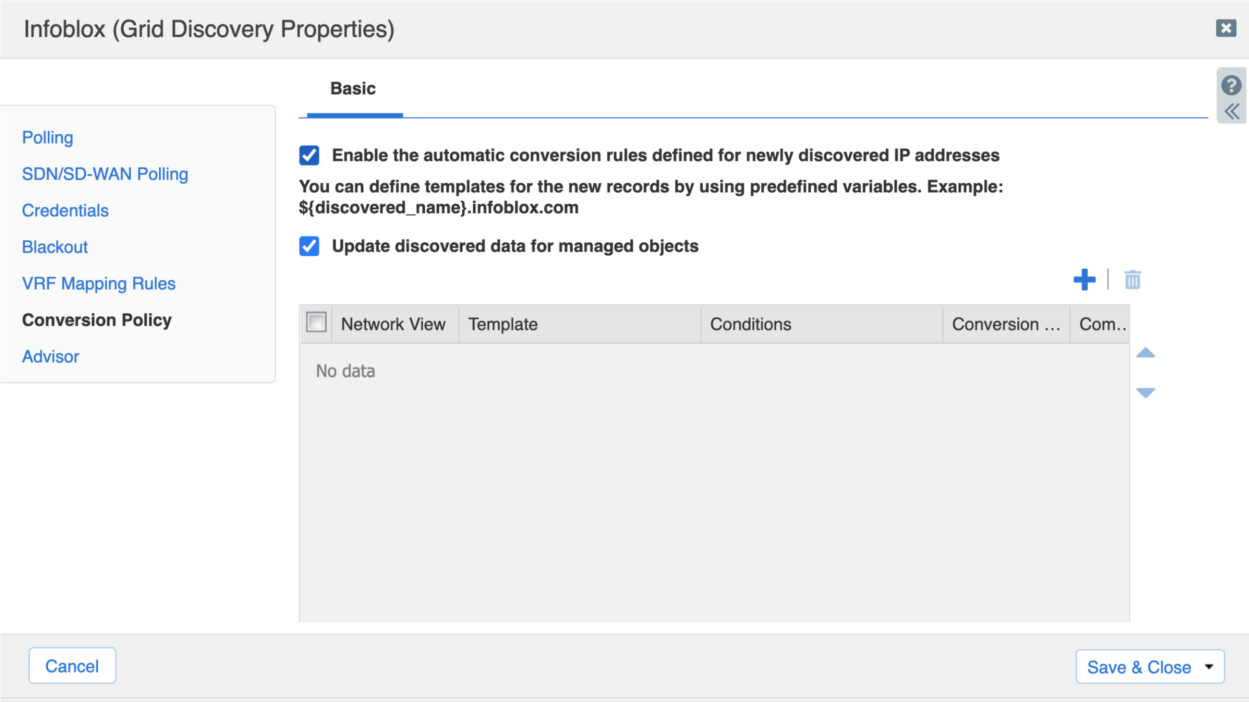
You can define templates for the new records by using predefined variables. Example: ${discovered_name}.infoblox.com

☑ **Update discovered data for managed objects**

□	Network View	Template	Conditions	Conversion ...	Com..
No data					

Cancel | Save & Close

4. Click on **Enable the automatic conversion rules defined for newly discovered IP addresses**.



☑ Enable the automatic conversion rules defined for newly discovered IP addresses

You can define templates for the new records by using predefined variables. Example: ${discovered_name}.infoblox.com

☑ Update discovered data for managed objects

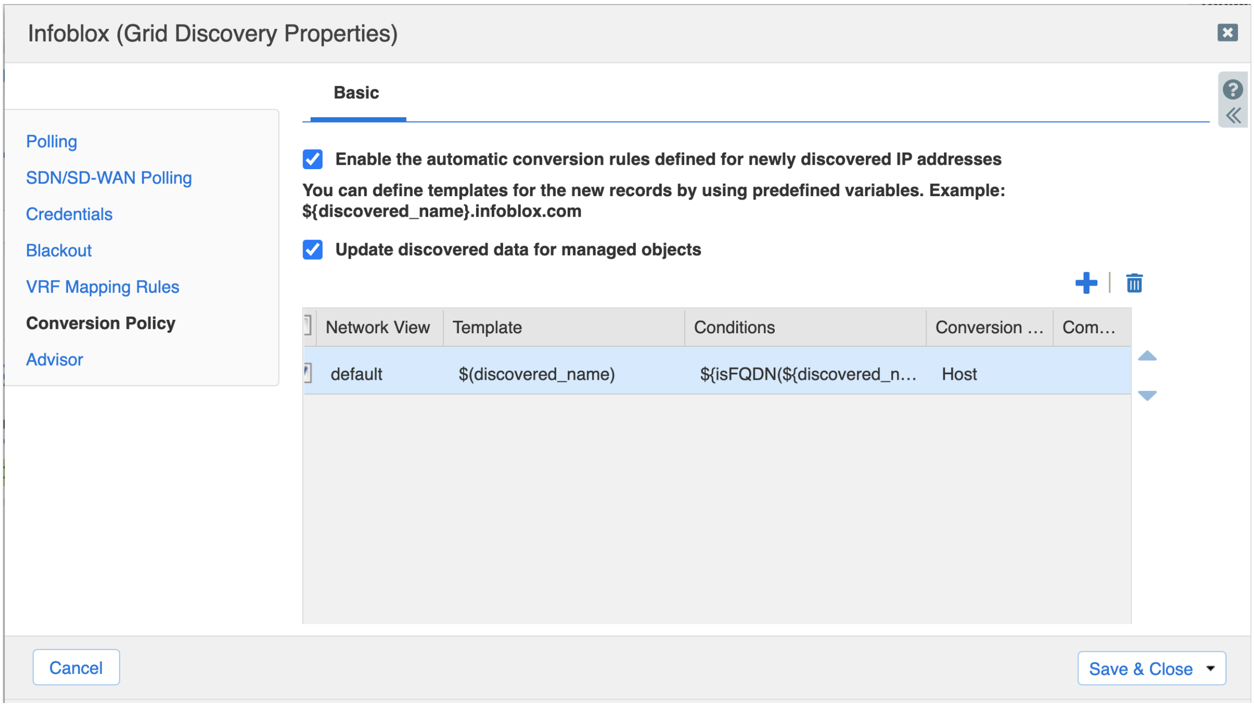
□	Network View	Template	Conditions	Conversion ...	Com..
No data					

The Update discovered data for managed objects is enabled by default. Enter the following:

- **Network View** - From the drop-down list, select the network view in which your conversion rule will take effect. Note that this rule applies only to objects in the selected network view. If you have multiple network views, you must configure a separate policy for each network view.
- **Template** - Define a naming template that Network Insight uses to automatically create DNS records for the unmanaged IP addresses in the network view. You can use the following syntax: ${substitution}, where substitution can be a supported variable or function. Note that each IPv6 address substitution is unwrapped into dotted presentation. For example, when you enter ${discovered_name}.corp100.com and the discovered_name for the asset is XYZ, the DNS name for this IP becomes XYZ.corp100.com. When you enter $dev-{ip_address_octet3}.corp100.com and the IP for the asset is2dba::db8::1, the DNS name for this IP becomes dev-3.corp100.com. When you enter ${ip_address[7]}.corp100.com for an IPv6 address and if the IP for the asset is 2001:db8:acad::1, the DNS name becomes b.corp100.com. You can also use the following functions in the naming template: dashed, reversed, and underscored. For example, when you enter ${dashed(${ip_address})}-corp100.com and the IP is 1.2.3.4, the DNS name becomes 1-2-3-4-corp100.com. When you enter ${reversed(${ip_address})}-corp100.com and the IP is 1.2.3.4, the DNS name becomes 4.3.2.1-corp100.com.
- **Conditions** - Enter the matching conditions for the conversion rule. You can use magic variables, supported variables, operators, and functions in the condition. When Network Insight finds IP addresses that match this condition, it will convert the IP addresses into DNS records (Hosts, A/PTR records, or fixed addresses) based on your selected conversion type. For example, if you want to match IP addresses that do not have an FQDN in the discovered_name, you can enter

this condition: ${isFQDN(${discovered_name})} == false AND ${discovered_name} == 'unknown'. If you want to match devices from the network 137.65.75.0/24 with the name starting with "Serial0", you can enter this condition: ${ip_belongs_to("137.65.75.0/24")} == true AND ${discovered_name} like "Serial0".

- **Conversion Type** - From the drop-down list, select the DNS record type that you want Network insight to convert the unmanaged IP addresses into. You can convert an unmanaged IP into Host, A/PTR, or Fixed Address. When you select A/PTR, Network Insight converts each IP into A and PTR records simultaneously.
- **Comment** (optional) - Enter description about this policy to distinguish it from others. For example, if the policy is used to identify and convert IP addresses with discovered_name that does not contain an FQDN, you can enter "No FQDN in discovered_name." as the comment to remind yourself about this conversion rule.



☑ Enable the automatic conversion rules defined for newly discovered IP addresses

You can define templates for the new records by using predefined variables. Example: ${discovered_name}.infoblox.com

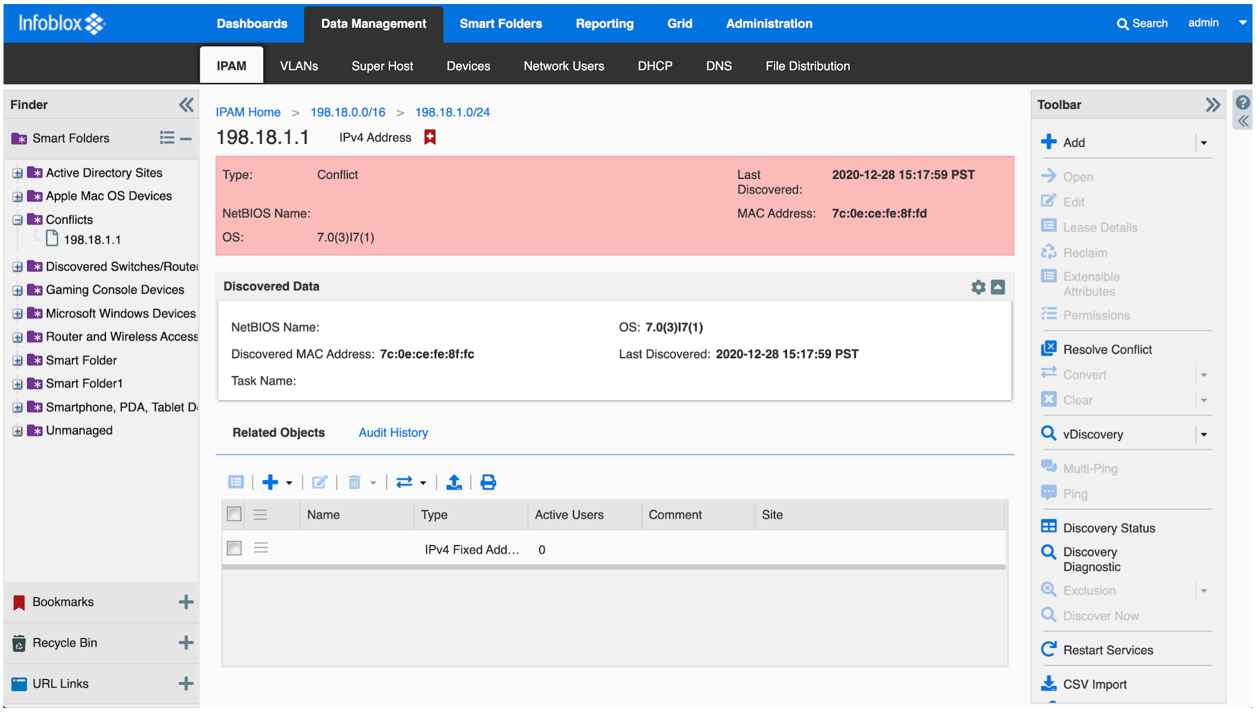
☑ Update discovered data for managed objects

Network View	Template	Conditions	Conversion ...	Com...
default	$(discovered_name)	${isFQDN(${discovered_n...	Host	

Note: For more information on Conversion Parameters, refer to the 'Supported Conversion Parameter' section in the Infoblox NIOS Administrator Guide.

Conflict Resolution in Network Insight

You can sometimes encounter conflicts when defining port reservations for IPAM-managed objects such as Fixed IP addresses or host records. The quickest way to locate any conflicts in Grid Manager is to open the Conflicts Smart Folder as noted in the screenshot below.



Type: Conflict

Last Discovered: 2020-12-28 15:17:59 PST

NetBIOS Name:

MAC Address: 7c:0e:ce:fe:8f:fd

OS: 7.0(3)I7(1)

Discovered Data

NetBIOS Name:

OS: 7.0(3)I7(1)

Discovered MAC Address: 7c:0e:ce:fe:8f:fc

Last Discovered: 2020-12-28 15:17:59 PST

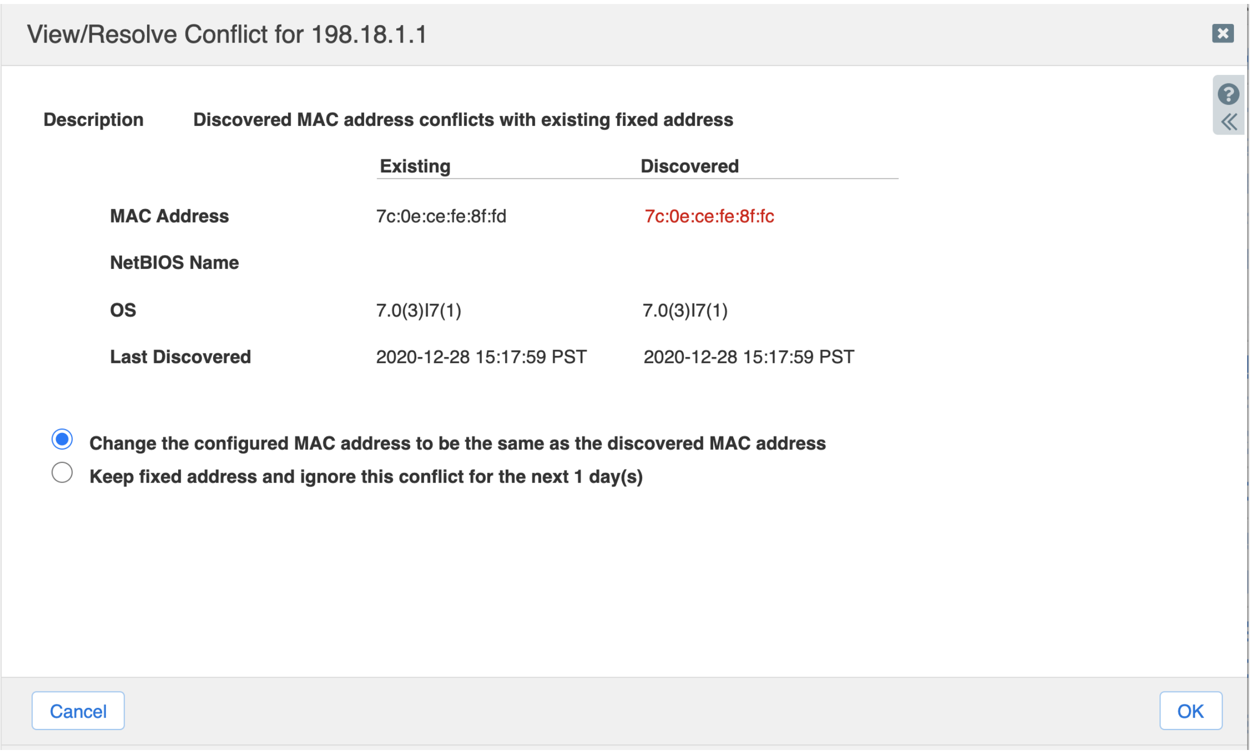
Task Name:

Name	Type	Active Users	Comment	Site
	IPv4 Fixed Add...	0		

Numerous types of conflicts are possible:

- Device Information conflict;
- Port Reservation conflict, including Used Port Reservation conflicts (usually resulting from a request to reserve a port that has already been assigned to another IPAM object);
- Fixed address conflict;
- IP Address conflicts;
- DHCP Range conflicts (such as: Discovered address is within an existing DHCP range but does not match an existing lease, fixed address, or exclusion range);
- MAC Address conflict (such as: Discovered MAC Address conflicts with existing fixed address). Note: When you execute discovery (**Discovery** → **Discovery Now** from the Toolbar), the appliance does not send an SNMP trap if it finds any conflicting information between the NIOS data and the discovered data.

The Conflict Resolution wizard automatically recognizes the object associated with the conflict and ensures that changes you make during resolution are applied correctly to the object. An example appears below.



View/Resolve Conflict for 198.18.1.1

Description Discovered MAC address conflicts with existing fixed address

	Existing	Discovered
MAC Address	7c:0e:ce:fe:8f:fd	7c:0e:ce:fe:8f:fc
NetBIOS Name		
OS	7.0(3)I7(1)	7.0(3)I7(1)
Last Discovered	2020-12-28 15:17:59 PST	2020-12-28 15:17:59 PST

● Change the configured MAC address to be the same as the discovered MAC address

○ Keep fixed address and ignore this conflict for the next 1 day(s)

Resolving Port Reservation Conflicts

Sometimes, administrators may accidentally request a device port to be reserved for an IP address when the port is already reserved for another object, or try to apply a different port to an object that already has a port reservation. When these cases arise, Grid Manager reports a conflict.

To resolve port reservation conflicts:

1. Click the link provided in the **Conflicts Smart Folder**.
2. Expand the Toolbar and click **Resolve Conflict**. The Resolve Port Reservation Conflict dialog opens, showing the differences between the reserved and discovered information.
3. Choose from the following options:
   - Change the reserved port to be the same as the discovered port.
   - Keep the configured port reservation and clear the conflict for the next 1 day(s).

*Note: In the **Grid Discovery Properties** → **Advanced** tab, the Ignore Conflict Duration setting governs the default time duration to ignore (clear) certain types of conflicts that may occur when defining IPAM objects that are associated with discovered and managed devices, interfaces, or IP addresses. Increments can be defined in Hours or Days.*

4. Click **OK** to save changes.

Another category of conflicts involves incorrectly defined device information for the object:

- The reserved Device Type information provided is different from the discovered vendor and device type (Router vs. Switch, for example).
- The defined Device Vendor information does not match with the discovered information.
- A User Port Reservation conflict occurs when an unmanaged IP address attempts to use a port that is already reserved by an IPAM object on a different IP address.

You can choose from the following options:

- Change configured information to discovered information.
- Keep the current device configuration and clear the conflict for the next 1 day(s).

In virtually all cases, replacing the configured information with the discovered information successfully clears the conflict; click **OK** to commit changes or to temporarily clear the conflict.

Resolving Multiple Conflicts

You can define objects for IP addresses, attempt to apply a port reservation, or incorrectly specify a value such as a MAC address or a vendor name, and accidentally cause multiple conflicts after creating the new object. When multiple conflicts need to be resolved for a particular IP address, you use a Resolve Multiple Conflicts wizard:

1. To quickly locate any conflicts, open the **Smart Folders** panel and open the **Conflicts** list.
2. Click the IP address for any entry in the Conflicts list. The IPAM page opens for the selected IP address, with the top panel highlighted in pink to indicate the conflict.
3. Open the vertical toolbar and click **Resolve Conflict**.

*Note: If multiple issues are involved with the conflict entry, the Resolve Conflicts wizard lists each of them. Select the conflict that you want to resolve first and click **Next**. For example, consider choosing to resolve the MAC Address conflict as shown above. The second step of the wizard appears, listing the differences between the Existing and Discovered information for the conflict as shown below.*

In this case, the MAC address specified in the last fixed address object configuration, for that object, conflicts with the MAC address associated with the IP. (You can verify this by checking the Related Objects tab in the IPAM page for the IP address.) Choose from one out of two options:

- Change the configured MAC address to be the same as the discovered MAC address;
- Keep a fixed address and ignore this conflict for the next 1 day(s).

In this example, the Discovered information for the MAC address associated with the Fixed Address object is one digit off from the Existing MAC information, which was entered incorrectly by the administrator. The discovered MAC, shown in red, is the correct value and should be used to overwrite the record for the conflict.

Select the **'Update... with discovered data'** option and click **Resolve**. The wizard updates with a return to the first step, in which you select the next conflict to resolve. A banner shows the result of the first resolution.

Select the next conflict to resolve and click **Next**. To resolve the conflict, the Configured information must be overwritten with the Discovered information:

- Change configured device type and vendor to be the same as the discovered device type and vendor;

- Keep current device configuration and clear the conflict for the next 1 day(s). Other conflict types have similar language.

Select from the above choices and click **Resolve**.

Continue through the wizard to resolve the last conflict associated with the IP address.

infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054
+1.408.986.4000
www.infoblox.com