Technical Guide

Device Discovery and Monitoring using SNMP

Feature Overview and Configuration Guide

Introduction

SNMP Device Discovery uses SNMP to discover devices which are then displayed on the network map in Vista Manager mini, or can be listed through the CLI. SNMP traps can then be received for these SNMP discovered devices. Alerts for any problems or notable events with these devices are shown on the map. This enables real-time monitoring of third party devices.

This document describes using SNMP Device Discovery and Monitoring from Vista Manager mini and SNMP Device Discovery from the AlliedWare Plus CLI.

Products and software version that apply to this guide

This guide applies to all AlliedWare Plus™ products that are AMF capable, running version **5.5.0-0.3** or later, and to Vista Manager mini on Device GUI version **2.5.2** or later.

For the latest information, see the following documents:

- The product's Datasheet
- The AlliedWare Plus Datasheet
- The product's Command Reference

These documents are available from the above links on our website at alliedtelesis.com.

Related documents

See the following documents for more detailed information about how to configure SNMP, SNMP MIBs, AMF, and Vista Manager mini:

- For more information about SNMP, see the SNMP Feature Overview and Configuration Guide.
- For more information about SNMP Management Information Base traps, see the Support for Allied Telesis Enterprise MIBs in AlliedWare Plus Technical Guide.
- This feature makes use of an existing AMF network to supply this information to the device GUI. For more information about AMF, see the AMF Feature Overview and Configuration Guide.
- For more information about how to configure Vista Manager mini, see the User Guide: Vista Manager mini.

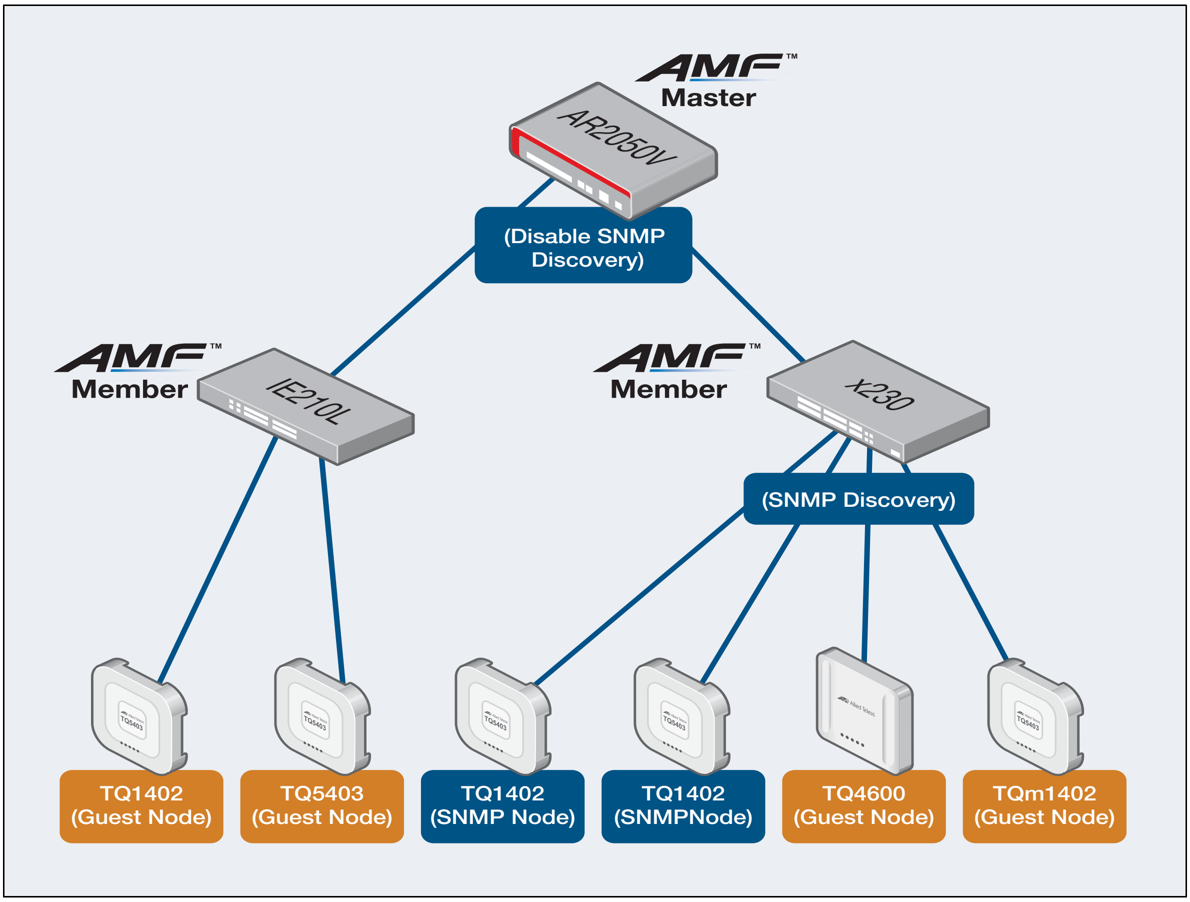
Content

How does SNMP Discovery and Monitoring work?

This is the process that SNMP Device Discovery and Monitoring uses to operate:

1. The administrator enables SNMP discovery on an AMF node.
2. ARP requests are sent out to all VLAN interfaces with prefixes with less than 256 members.
3. Any device that sends an ARP response is detected and its address is stored in ARP discovery.
4. SNMP discovery takes these detected IP addresses and does an SNMP 'get' request based on SNMP configured information. SNMP discovery stores the SNMP responses.
5. Discovered device details are sent to the AMF master across the AMF network.
6. This information is written to the AMF topology tree as a discovered node.
7. Vista Manager mini accesses this information to display devices.
8. Vista Manager mini receives trap information from the discovered devices.

The following diagram shows two discovered nodes:



What can you configure using SNMP Discovery?

These are the things you can configure for SNMP Discovery:

- Enable SNMP Discovery.
- Set the SNMP version to version v1, version v2c or version v3 (version v2c is the default).
- Set a specified list of IP addresses to poll SNMP MIB values.
- Deny or permit IP addresses.
- Deny interfaces.
- Set the 'community' string to use when making SNMPv1/v2c requests.
- Set the 'user name' and security settings to use when making SNMPv3 requests.
- Configure the polling intervals for each stage of device discovery.

Supported SNMP Monitoring information and traps

SNMP Discovery and Monitoring uses a trap receiver to allow the CLI and Vista Manager mini to display discovered devices. SNMP Monitoring allows you to report notable events from third party vendor devices.

This feature allows you to display third party vendor device information in real time. It makes use of an existing AMF network to supply this information to the Device GUI. The following information is provided via SNMP Discovery when this information is available:

NAME	EXAMPLE
Area Name	Area1
Node Name	Node1
Name	AT-TQ5403
Serial Number	AB123456
IP Address	192.168.55.2
MAC Address	001a.ebdc.f4c0
Local Interface	port1.0.5
Description	Access point 1
State	Up
Location	Main building 3rd floor

In the Device GUI, the following SNMP traps are displayed on the device icon in the Network MAP, and show up in the Recent Events List in the SNMP Monitoring window:

- atFiberMonAlarmSetNotify
  This alarm activates if fiber monitoring detects an issue.
- atLoopProtectDetectedLoopBlockedTrap
  This alarm is generated when the Loop Protection feature blocks an interface with a loop.
- atLoopProtectDetectedByLoopDetectionTrap
  This alarm is generated when the Loop Protection feature detects a loop by its Loop Detection method.
- atLoopProtectDetectedByThrashLimitTrap
  This alarm is generated when the Loop Protection feature detects a loop by its MAC address-table Thrash-Limiting method.
- newRoot Trap
  This event indicates that the sending agent has become the new root of the Spanning Tree. The trap is sent by a bridge soon after its election as the new root, for example, upon expiration of the Topology Change Timer, immediately subsequent to its election.
- topologyChange Trap
  This trap is sent when a spanning tree group receives a topology change notification.
- linkDown Trap
  A linkDown trap means that a link has gone down.
- linkUp Trap
  A linkDown trap means that a link has come up.
- coldStart Trap
  A coldStart trap means that a device has restarted after a power cycle.
- pethPsePortOnOff
  This notification indicates if a PSE (Power Sourcing Equipment) port is delivering power or not.
- pethMainPowerUsageOn
  The PSE Threshold usage indicator is on and power usage is above the threshold.
- pethMainPowerUsageOff
  The PSE Threshold usage indicator is off and power usage is below the threshold.

In the Device GUI, the following SNMP traps show as recent events on the SNMP Monitoring window. These are not displayed on the device icon in the Network MAP.

- atFiberMonAlarmClearedNotify
  A notification is generated when the monitored received optical power of an SFP returns to an acceptable value. This can occur because the power has returned to its previous level or the comparison baseline has adjusted to the new level.
- atLoopProtectRecoverLoopBlockedTrap
  This alarm is generated when the Loop Protection feature blocks an interface with a loop.

Restrictions

The following restrictions apply to SNMP Discovery:

- SNMP Discovery can find up to 30 nodes on the AMF master. These 30 nodes can be spread across AMF members.
- The maximum number of denied/permitted interfaces is 30 on each node.
- Discovery addresses are not supported on Ethernet ports or tunnel interfaces.
- SNMP Discovery does not discover IPv4 interfaces for AMF nodes, including AMF guest nodes. These nodes are discovered through AMF.
- Stacking VLANs are not used in the SNMP discovery process.
- In the Device GUI, you can only configure SNMP Discovery on AMF members that support Vista Manager mini. You can use the CLI to configure other AMF members if needed. For more information, see "SNMP Discovery through the AlliedWare Plus CLI" on page 28.

SNMP Discovery and Monitoring through Vista Manager mini

You can configure SNMP Discovery from Vista Manager mini so that SNMP can discover nodes and display them in the Network MAP. You can monitor SNMP traps to see if there any problems with any of the devices connected to your AMF network.

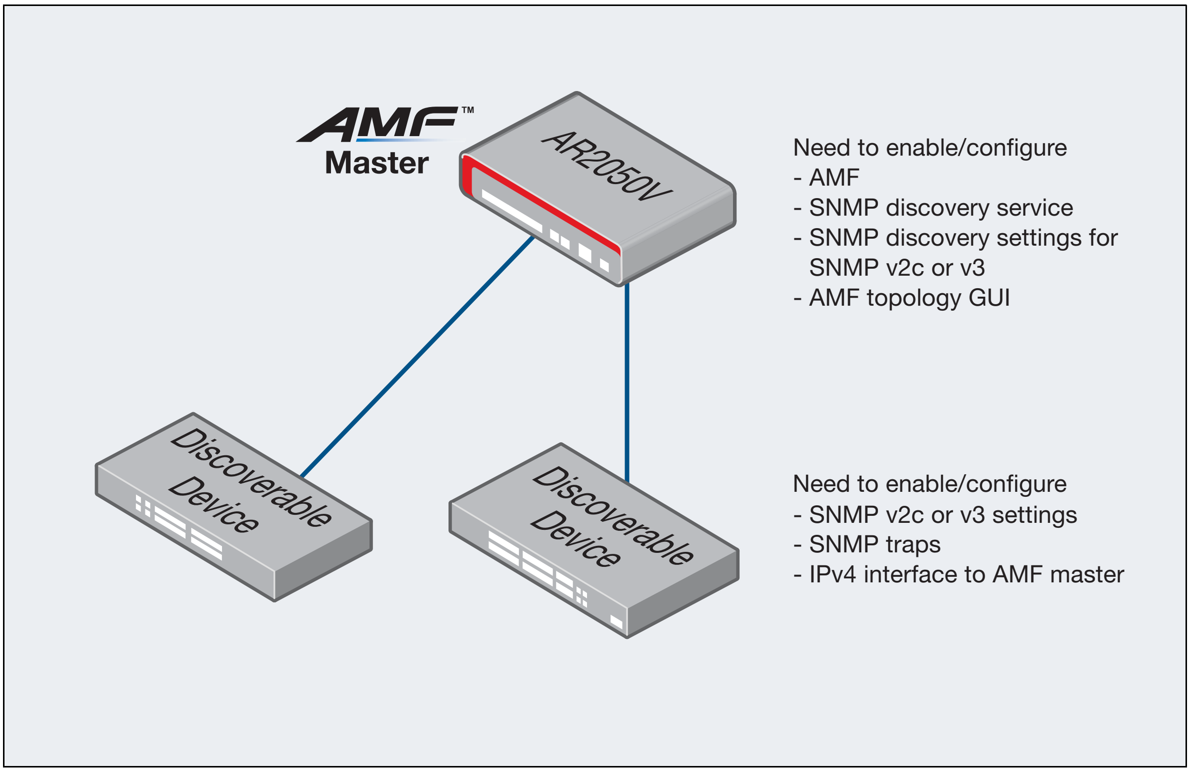
What to configure

The roles that can to be configured for SNMP Discovery and Monitoring are:

- AMF master
- AMF members, if not all discoverable devices are directly connected to the AMF master, and
- discoverable devices.

The following diagram shows the simplest network design, where discoverable devices are directly connected to the AMF master. For a more complex design, see "How to configure a multi-member network" on page 14.

This is an example of a simple network design:



Need to enable/configure
- AMF
- SNMP discovery service
- SNMP discovery settings for SNMP v2c or v3
- AMF topology GUI

Need to enable/configure
- SNMP v2c or v3 settings
- SNMP traps
- IPv4 interface to AMF master

How to configure SNMP Discovery on a simple network

Before you start

Before you configure SNMP Discovery, you must first complete the following tasks:

On the AMF master:

- Run AlliedWare Plus version 5.5.0-0.3 or later.
- Have the Device GUI version 2.5.2 or later running Vista Manager mini. The Device GUI only enables you to configure SNMP Discovery on AMF masters that support Vista Manager mini.
- Configure your AMF network. For more information about AMF, see the AMF Feature Overview and Configuration Guide.
- Enable the AMF topology GUI using the command **atmf topology-gui enable**.
- Have an IPv4 interface to the discoverable device and be able to ping the device.

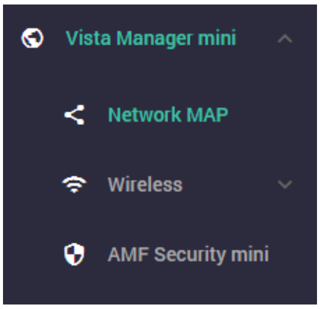
On the discoverable devices:

- Configure a trap destination of the AMF master.
- Set up SNMP v2c or v3.
- Make sure that the devices will respond to SNMP ‘get’ requests.
- Enable traps that you want to display. See "Supported SNMP Monitoring information and traps" on page 5.

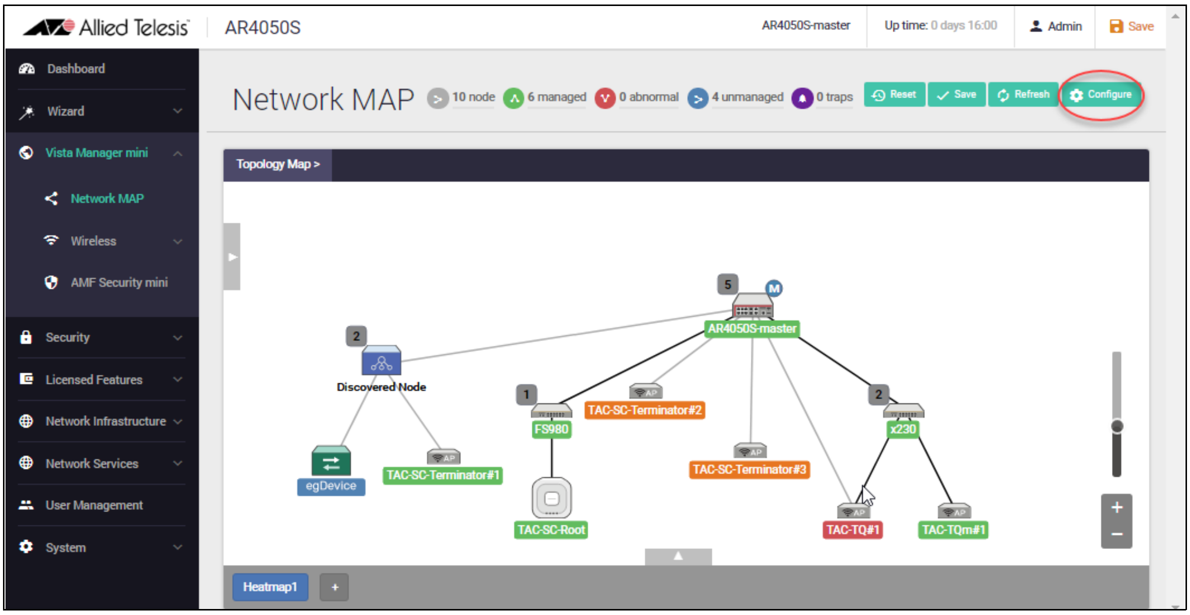
Configuration on a simple network

Perform the following steps to configure SNMP Discovery for your network:

1. Select **Vista Manager mini > Network MAP**:

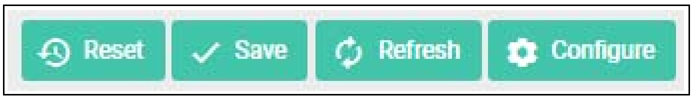


The Network MAP displays the topology map of the devices in your network. The following is an example of a network topology:

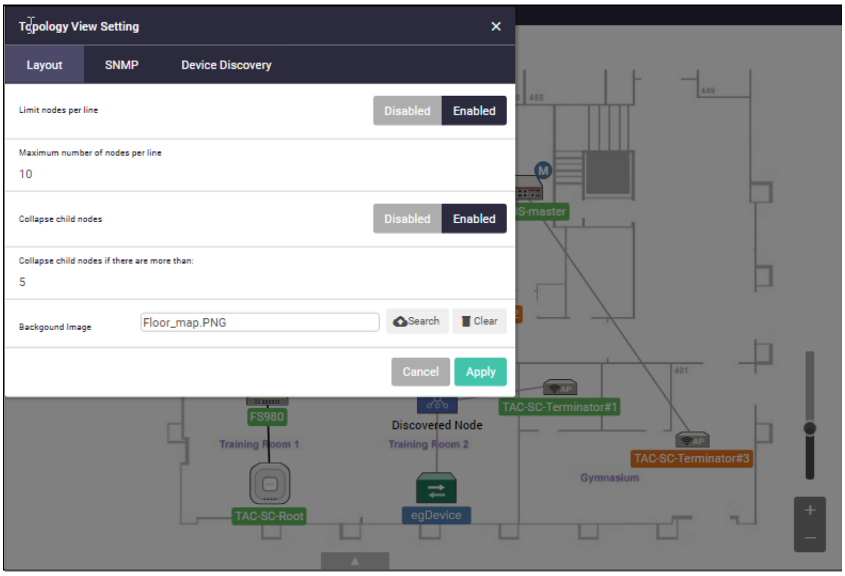


2. Click on the **master** node that appears in the Network MAP.

3. Click **Configure** from the top right hand side of the Network MAP window:



The following **Topology View Setting** dialog appears showing three tabs: the **Layout** tab, the **SNMP** tab and the **Device Discovery** tab. The Layout tab is displayed by default, for example:



Limit nodes per line: Disabled [✓ Enabled]

Maximum number of nodes per line: 10

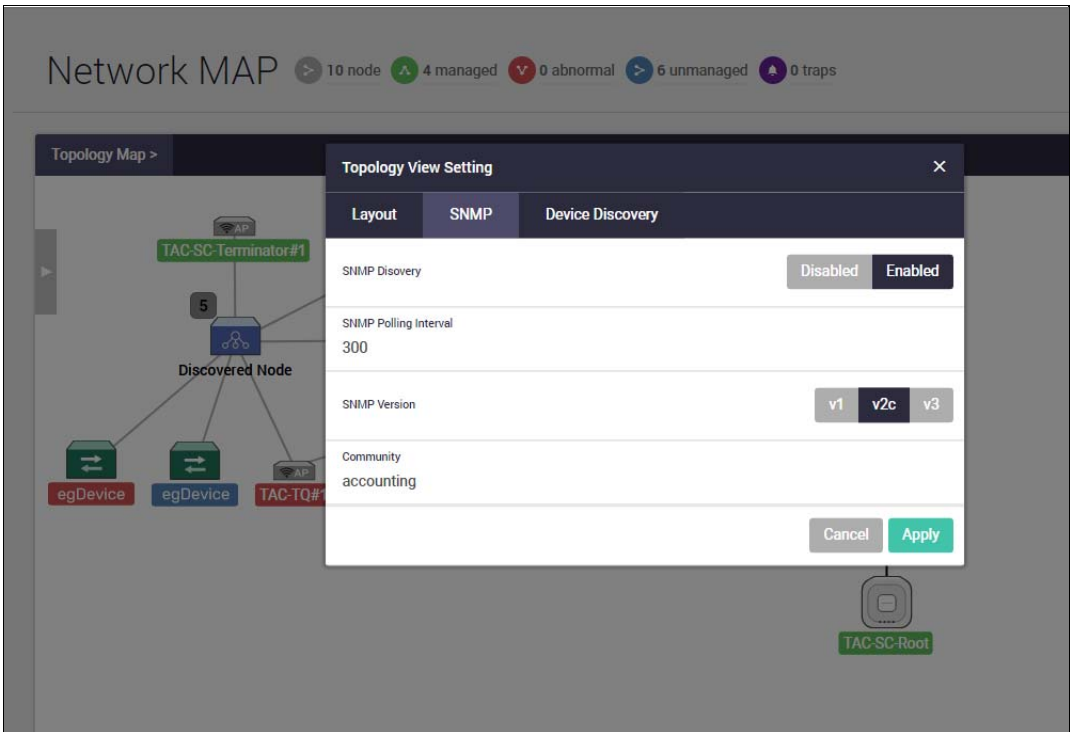
Collapse child nodes: Disabled [✓ Enabled]

Collapse child nodes if there are more than: 5

Backgound Image: Floor_map.PNG

From the **Layout** tab you can optionally set up an existing network topology to do things like: limit the nodes that appear per line, set a maximum number of nodes per line, collapse the child nodes or add a background image. A child node is a node that is connected to a node above it (a parent node). The example above shows a layout floor map that has been added.

4. Click on the **SNMP** tab from the **Topology View Setting** dialog:



Network MAP 10 node 4 managed 0 abnormal 6 unmanaged 0 traps

Topology View Setting

SNMP Disovery: Disabled **Enabled**

SNMP Polling Interval: 300

SNMP Version: v1 **v2c** v3

Community: accounting

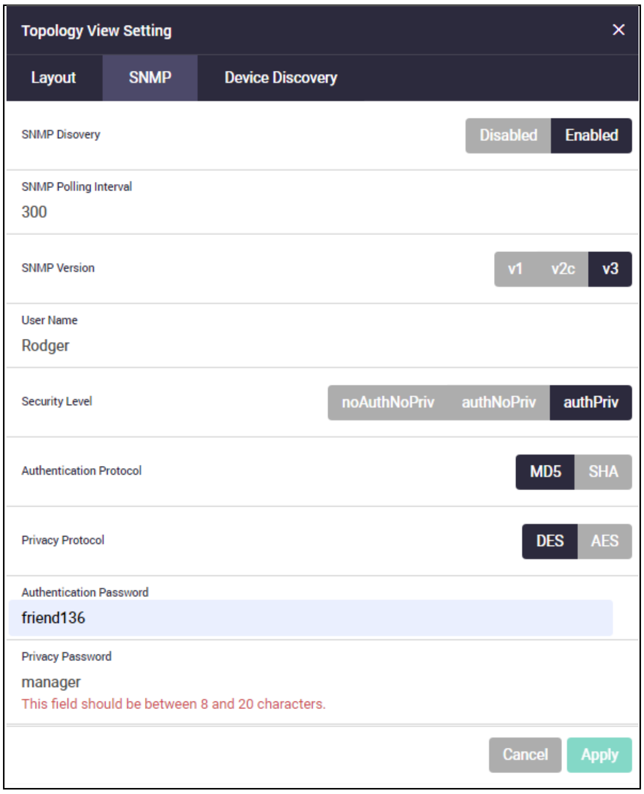
5. Click **Enabled** to the right of the phrase 'SNMP Discovery'.

6. Set the SNMP version (the default is version v2c).

   If you use SNMP version v2c, enter the community name. The example above shows the version set at version v2c with a community named ‘accounting’.

If you use SNMP v3 you can set a User Name, a Security Level, an Authentication Protocol, a Privacy Protocol, an Authentication Password and Privacy Password.

For example, settings for SNMP version v3:



Topology View Setting

SNMP Disovery: Disabled | **Enabled**

SNMP Polling Interval
300

SNMP Version: v1 | v2c | **v3**

User Name
Rodger

Security Level: noAuthNoPriv | authNoPriv | **authPriv**

Authentication Protocol: **MD5** | SHA

Privacy Protocol: **DES** | AES

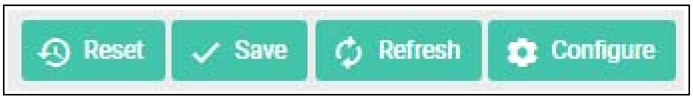
Authentication Password
friend136

Privacy Password
manager
This field should be between 8 and 20 characters.

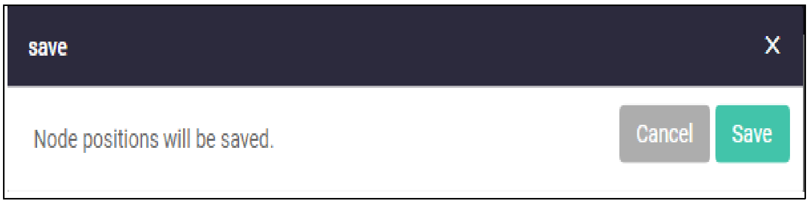
7. Click **Apply**.

   Once you have applied the configuration, the **Topology View Setting** dialog closes.

8. Click **Save**.



After saving your configuration, the following message displays:

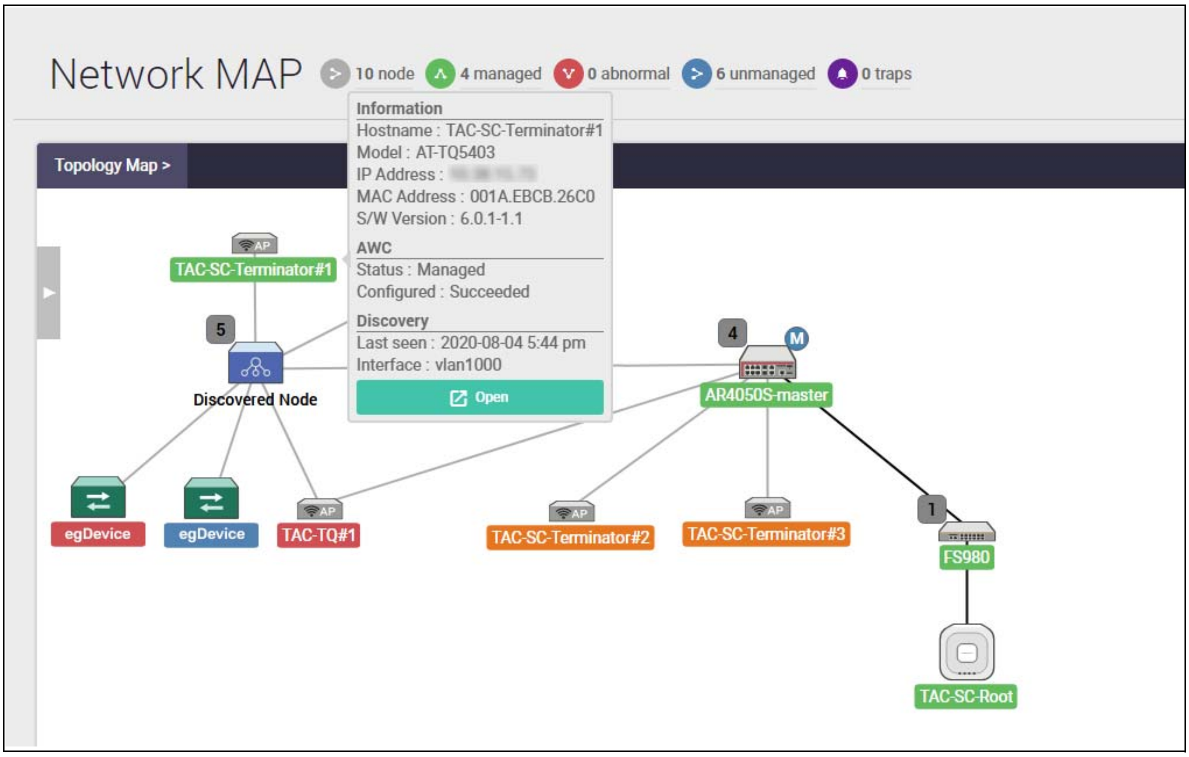


save

Node positions will be saved.

9. Click **Save**.

Once configured, you can see discovered devices under a discovered node. If you want to see details about SNMP Discovery nodes from the Network MAP, click on the discovered node's device icon:



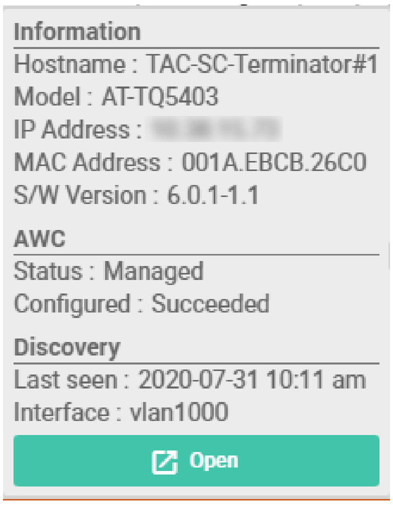
Information
Hostname : TAC-SC-Terminator#1
Model : AT-TQ5403
IP Address : [redacted]
MAC Address : 001A.EBCB.26C0
S/W Version : 6.0.1-1.1

AWC
Status : Managed
Configured : Succeeded

Discovery
Last seen : 2020-08-04 5:44 pm
Interface : vlan1000

Open

You can see the information about a discovered node, such as Hostname, IP Address, MAC Address, when it was last seen and what interface the device is on, for example:



Information
Hostname : TAC-SC-Terminator#1
Model : AT-TQ5403
IP Address : [redacted]
MAC Address : 001A.EBCB.26C0
S/W Version : 6.0.1-1.1

AWC
Status : Managed
Configured : Succeeded

Discovery
Last seen : 2020-07-31 10:11 am
Interface : vlan1000

Open

How to configure a multi-member network

The instructions above describe how to configure a network where the discoverable devices are directly connected to the AMF master. If your discoverable devices are instead connected to an AMF member, you need to configure SNMP Discovery on the member as well as on the master.

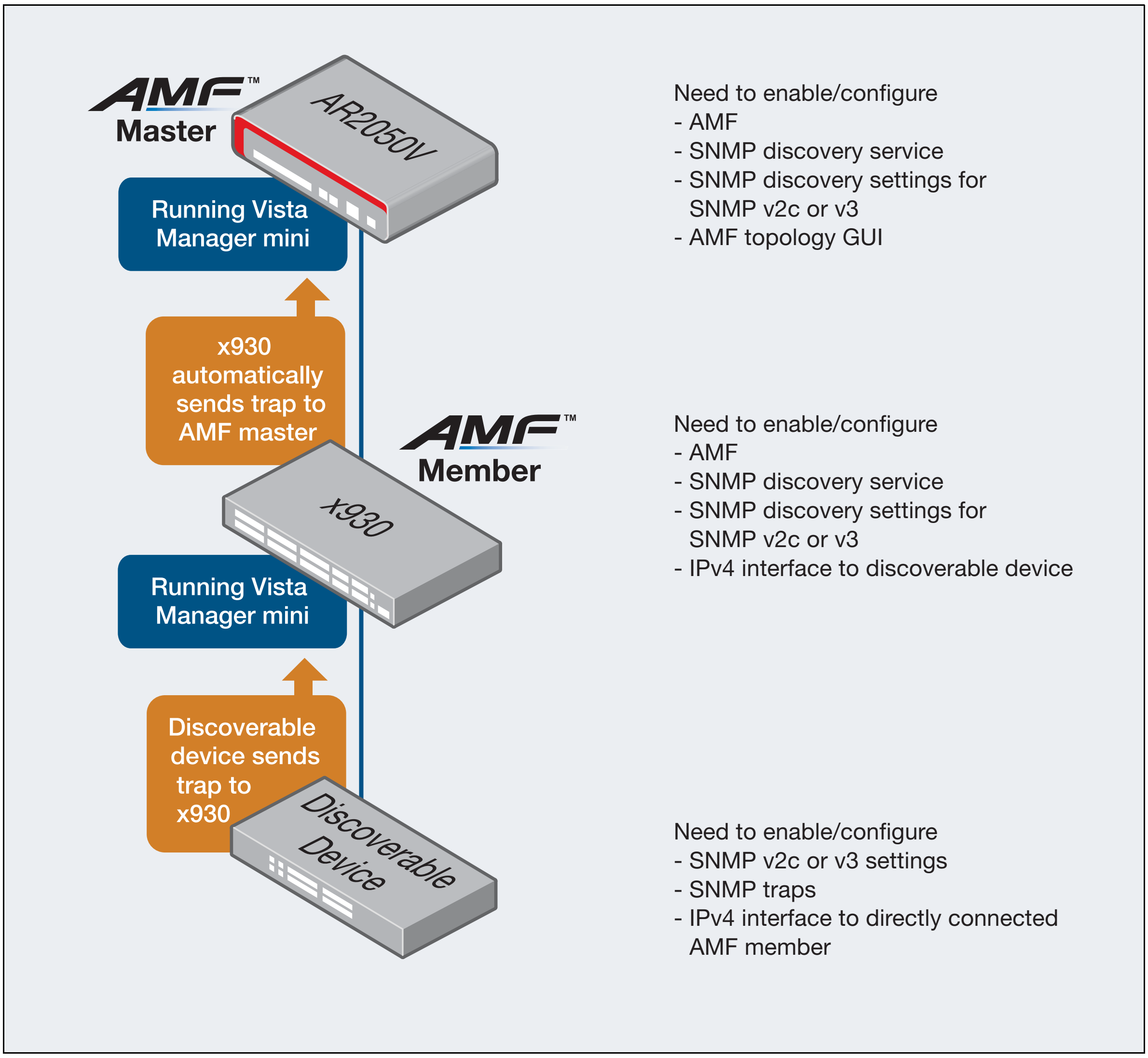
You also need to choose one of two approaches for SNMP Monitoring:

- Distributed trap receiving, where SNMP Monitoring receives the traps on the directly-attached member and automatically forwards them to the AMF master, or
- Centralized trap receiving, where SNMP Monitoring receives the traps on the AMF master.

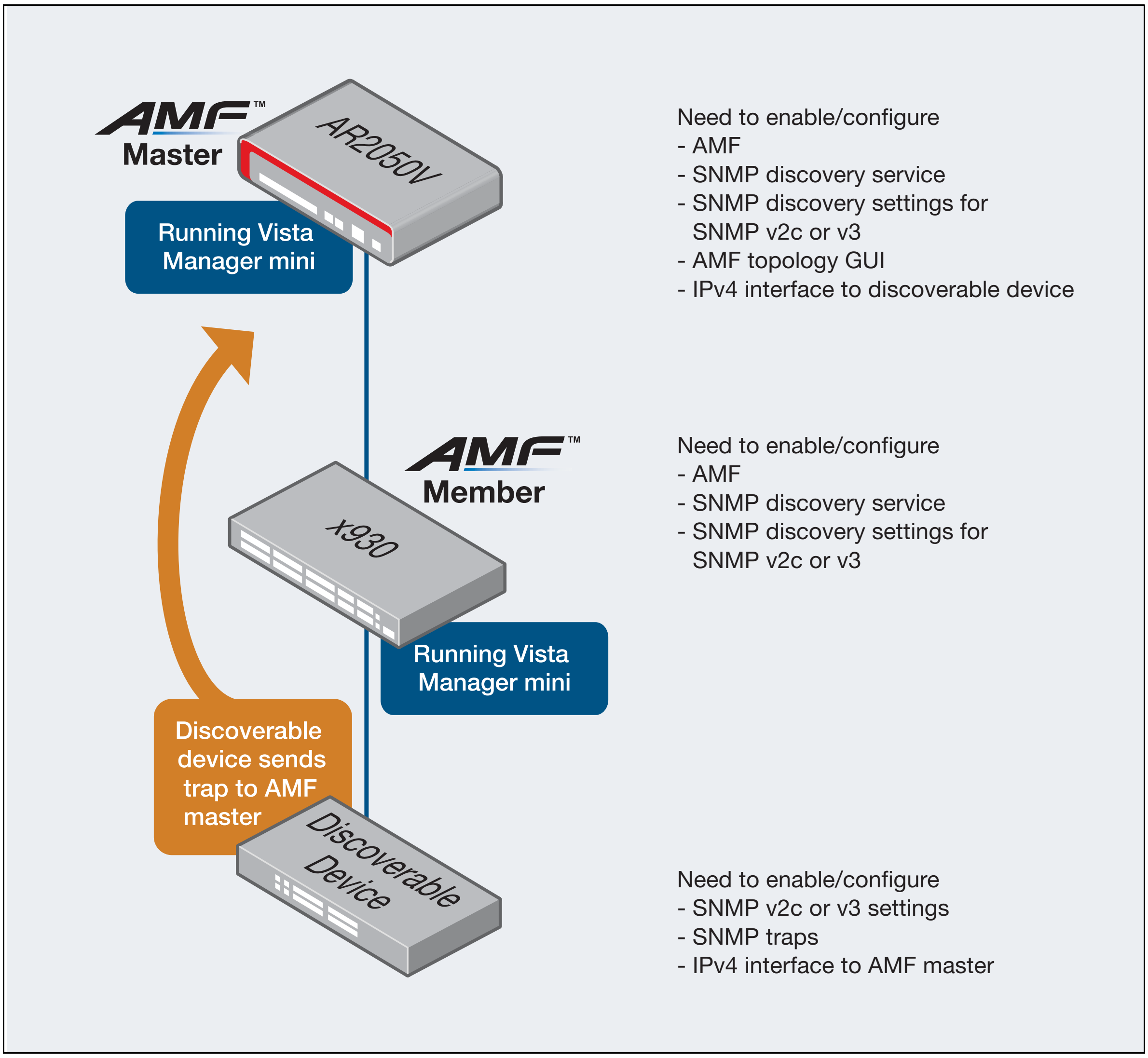
The best approach will depend on your network configuration.

The following diagrams shows both these approaches and what you need to configure in each approach.

This is an example of distributed trap receiving:


AMF™
Master
AR2050V
Running Vista Manager mini
Need to enable/configure
- AMF
- SNMP discovery service
- SNMP discovery settings for SNMP v2c or v3
- AMF topology GUI
x930 automatically sends trap to AMF master
AMF™
Member
x930
Running Vista Manager mini
Need to enable/configure
- AMF
- SNMP discovery service
- SNMP discovery settings for SNMP v2c or v3
- IPv4 interface to discoverable device
Discoverable device sends trap to x930
Discoverable Device
Need to enable/configure
- SNMP v2c or v3 settings
- SNMP traps
- IPv4 interface to directly connected AMF member

This is an example of centralized trap receiving:


AMF™
Master
AR2050V
Running Vista Manager mini
Need to enable/configure
- AMF
- SNMP discovery service
- SNMP discovery settings for SNMP v2c or v3
- AMF topology GUI
- IPv4 interface to discoverable device
AMF™
Member
x930
Running Vista Manager mini
Need to enable/configure
- AMF
- SNMP discovery service
- SNMP discovery settings for SNMP v2c or v3
Discoverable device sends trap to AMF master
Discoverable Device
Need to enable/configure
- SNMP v2c or v3 settings
- SNMP traps
- IPv4 interface to AMF master

Before you start

Before you configure SNMP Discovery, you must first complete the following tasks:

On the AMF master:

- Run AlliedWare Plus version 5.5.0-0.3 or later.
- Have the Device GUI version 2.5.2 or later running Vista Manager mini. The Device GUI only enables you to configure SNMP Discovery on AMF masters that support Vista Manager mini.
- Configure your AMF network. For more information about AMF, see the AMF Feature Overview and Configuration Guide.
- Enable the AMF topology GUI using the command **atmf topology-gui enable**.
- Have an IPv4 interface to the discoverable device and be able to ping the device, if using centralised trap receiving as described in the diagram above.

And on AMF members connected to discoverable devices:

- Run AlliedWare Plus version 5.5.0-0.3 or later.
- Have the Device GUI version 2.5.2 or later running Vista Manager mini. The Device GUI only enables you to configure SNMP Discovery on AMF members that support Vista Manager mini.
- Have an IPv4 interface to the discoverable device and be able to ping the device, if using distributed trap receiving as described in the diagram above.

And on the discoverable devices

- Configure a trap destination of the AMF master or member.
- Set up SNMPv2 or v3.
- Make sure that the devices will respond to SNMP ‘get’ requests.
- Enable traps that you want to display. See "Supported SNMP Monitoring information and traps" on page 5.

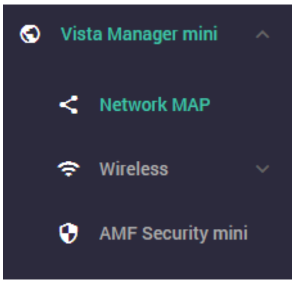
Configuration on a multi-member network

If your AMF members support Vista Manager mini, simply follow steps 1-9 of "How to configure SNMP Discovery on a simple network" on page 9 on every AMF member that has a discoverable device connected to it.

If your AMF members do not support Vista Manager mini, use the CLI to configure them, as described in "SNMP Discovery through the AlliedWare Plus CLI" on page 28.

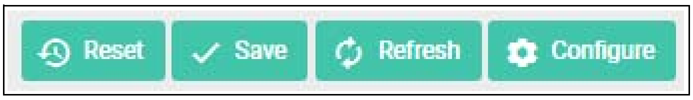
How to optionally configure polling intervals

1. Click **Vista Manager mini > Network MAP**:



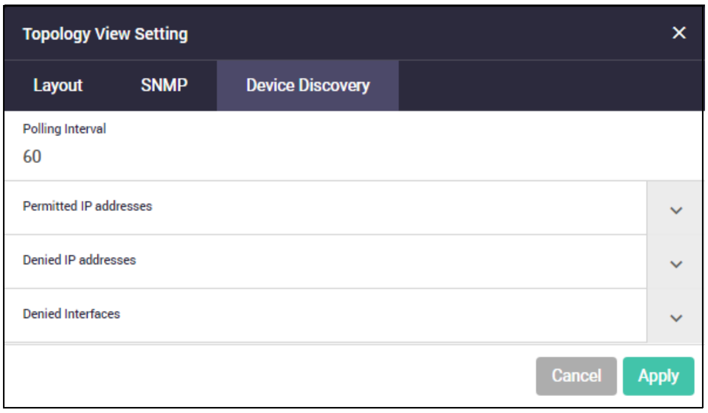
This displays the topology map of your configured network.

2. To change the configuration, click **Configure**:



3. Click the **Device Discovery** tab.

   SNMP Discovery first uses ARP to discover subnets that are reachable from the AMF node. This polling happens every 60 seconds by default. To change this polling interval, change the **Device Discovery Polling Interval** on the **Device Discovery** tab.



Polling Interval
60

Permitted IP addresses

Denied IP addresses

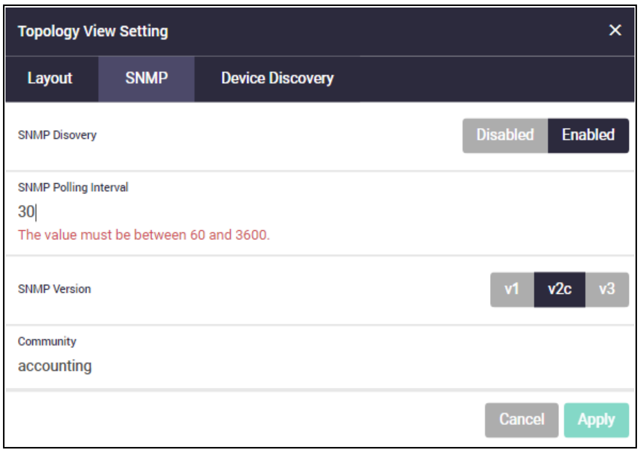
Denied Interfaces

   This polling happens on each Layer 3 interface with a subnet of 256 members or less. If you need SNMP Discovery on nodes with subnets of greater than 256 members, see "How to optionally deny interfaces or deny or permit IP addresses" on page 18.

   If an IPv4 address responds to an ARP request, the IP address and MAC address are added to a list which is available to SNMP discovery to contact.

4. Click the **SNMP** tab.

   SNMP Discovery uses SNMP 'get' requests to poll the devices discovered by the ARP polling. This polling happens every 300 seconds (5 minutes) by default. To change this polling interval, change the **SNMP Polling Interval** on the **SNMP** tab.



SNMP Discovery: Disabled [✓ Enabled]

SNMP Polling Interval
30
The value must be between 60 and 3600.

SNMP Version: v1 [✓ v2c] v3

Community
accounting

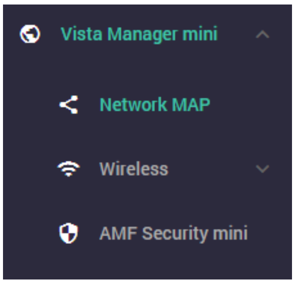
5. Once you have chosen your configuration, click **Apply**.

   When you click Apply, you are returned to the main screen. Save your configuration with the Save button.

How to optionally deny interfaces or deny or permit IP addresses

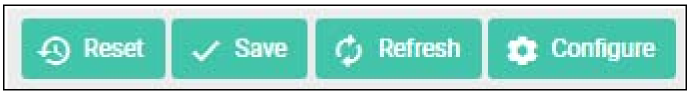
In some network situations, you may need to turn SNMP Discovery on or off for specific IP addresses or interfaces. This enables you to control which devices appear on the Network MAP, and therefore focus on the devices you want to monitor.

1. Click **Vista Manager mini > Network MAP**:



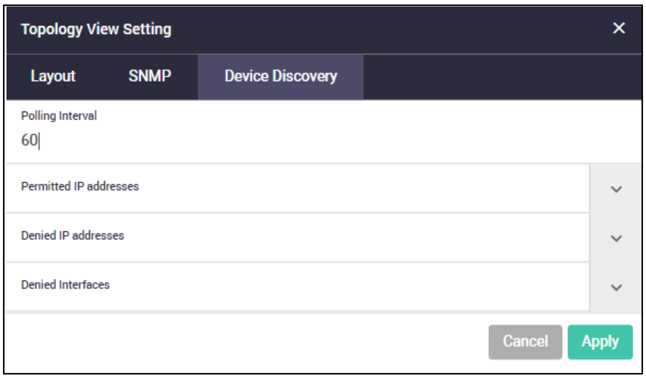
This displays the topology map of your configured network.

2. To change the configuration, click **Configure**:



3. Click the **Device Discovery** tab.

From this tab you can set permitted IP addresses, denied IP addresses and denied Interfaces:



Polling Interval
60

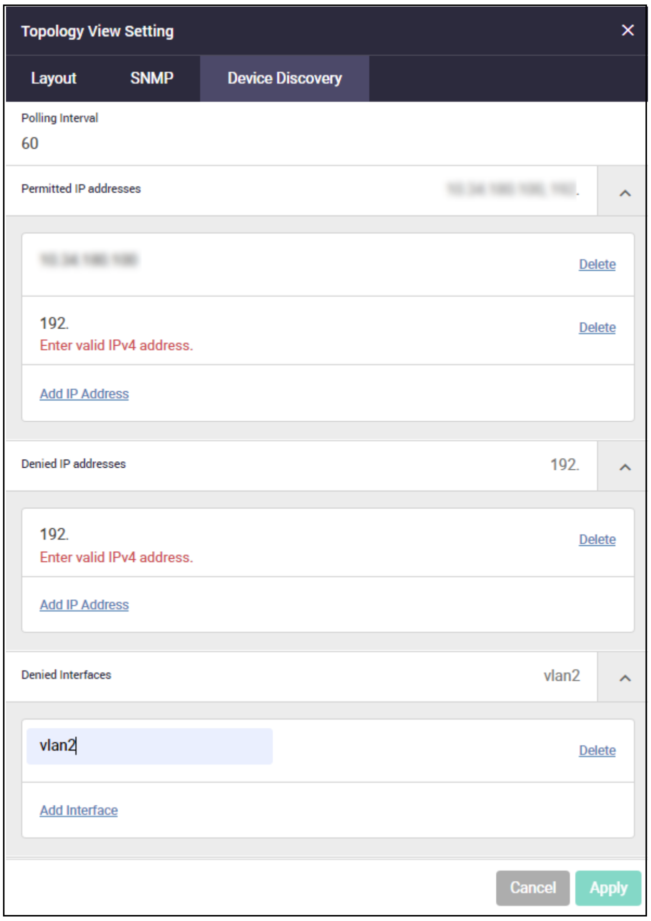
Due to dynamic learning of IP addresses, it is possible for SNMP Discovery to report duplicate entries to the AMF master. In that case, the Network MAP will show multiple connections to the discovered device. You can prevent this by finding out which IP address has reported the unwanted link and denying that IP address on this tab.

By default, all IPv4 interfaces with prefixes of 256 members or less are included in SNMP Discovery. If you want to allow SNMP Discovery to do requests on interfaces with greater than 256 members, you can configure a permit on an IP address.

The AMF and stacking management VLANs are denied by default.

Expand the Permitted IP addresses, Denied IP addresses and Denied Interfaces fields with the down arrow icon to the right if you want to enter IP addresses or interfaces.

The example below shows IP addresses being entered to deny and permit, and an interface being entered to deny:



Topology View Setting

Polling Interval
60

Permitted IP addresses [redacted]

[redacted]

192.
Enter valid IPv4 address.

Denied IP addresses 192.

192.
Enter valid IPv4 address.

Denied Interfaces vlan2

vlan2

4. Once you have chosen your configuration, click **Apply**.

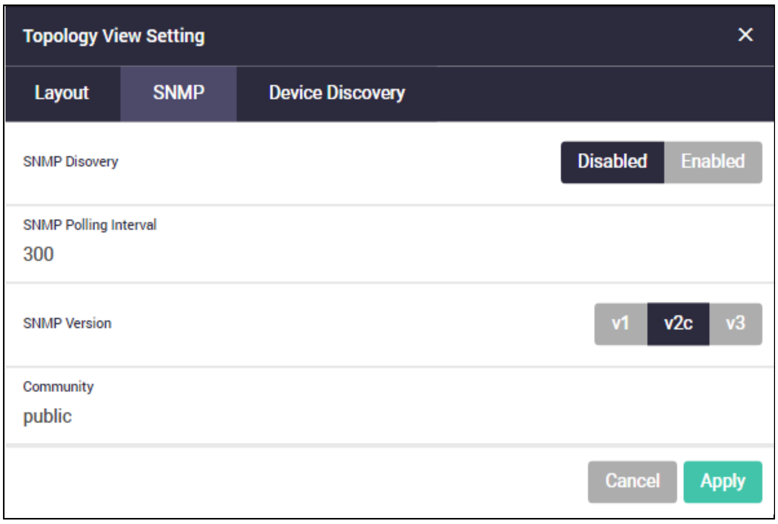
   When you click Apply, you are returned to the main screen. Save your configuration with the Save button.

How to disable SNMP Discovery

To disable SNMP discovery, from the **Network MAP** click **Configure**.

1. Click on the **SNMP** tab.
2. Click **Disabled**.
3. Click on the SNMP version.
4. Click **Apply**.

This removes the SNMP Discovery configuration from your network. This stops automatic discovery of nodes on your network and removes discovered nodes from the Network MAP. The following example shows disabling SNMP Discovery for v2c:



SNMP Disovery: Disabled

SNMP Polling Interval
300

SNMP Version: v2c

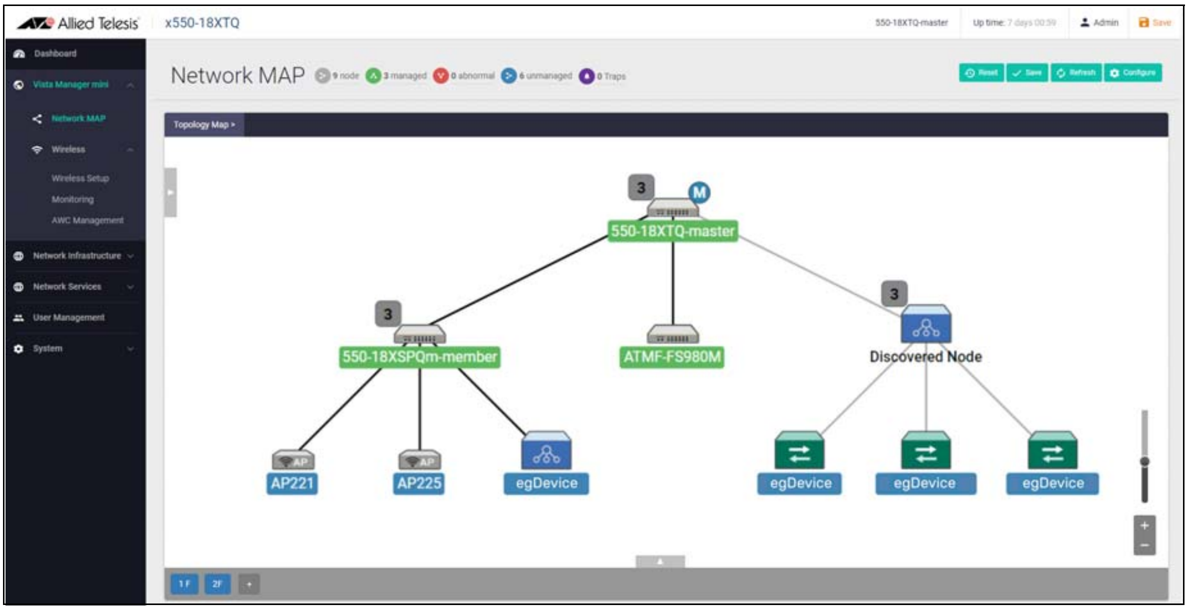
Community
public

How to see information about discovered devices

All SNMP nodes are automatically displayed in positions where are they located on the topology map. If the discovered node is located under an AMF member, it will automatically display under that AMF member.

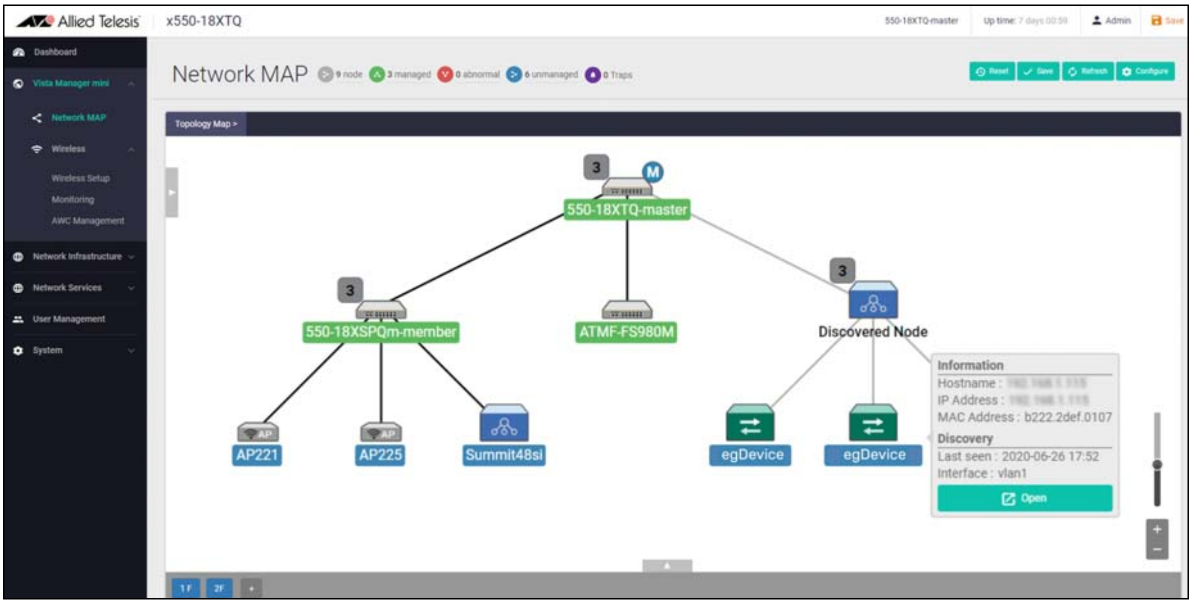
Child devices display under a discovered device

The following example shows a discovered device (node), with child devices displayed under it:



Node information

The following example shows a discovered device and its detailed information. Click on the device icon to see this information:

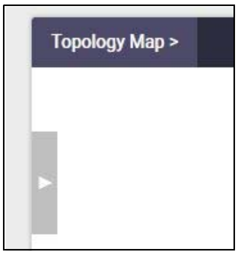


Information
Hostname : [redacted]
IP Address : [redacted]
MAC Address : b222.2def.0107

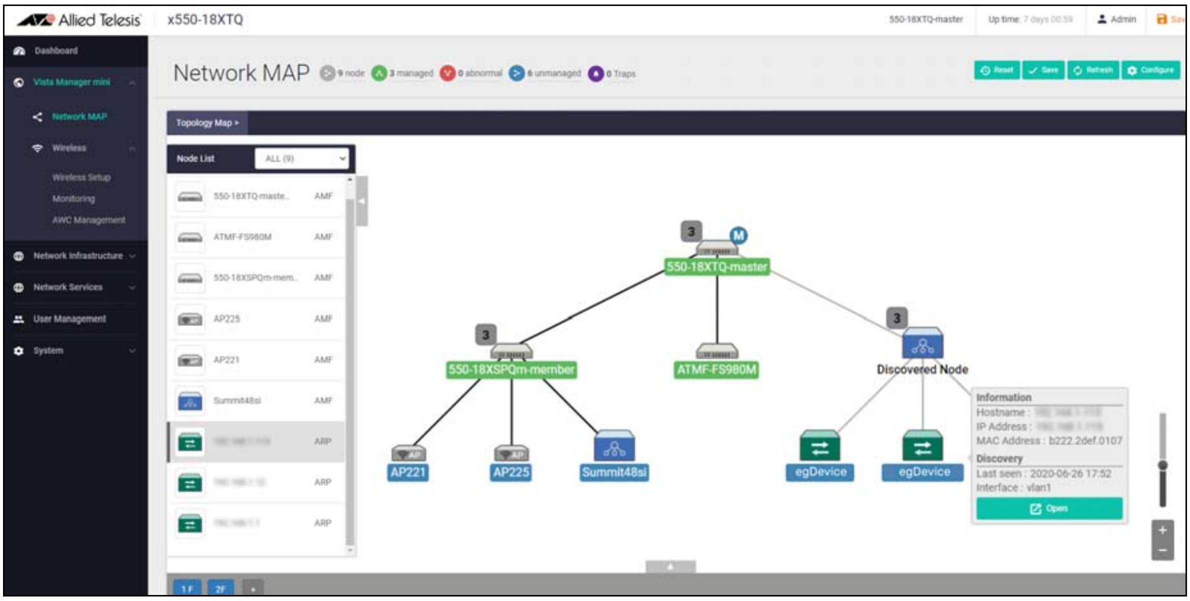
Discovery
Last seen : 2020-06-26 17:52
Interface : vlan1

Node List information

SNMP nodes are displayed in the **Node List**. Click on the arrow bar under the Topology Map heading to display the Node List:



The following example shows detected nodes in the Node List:

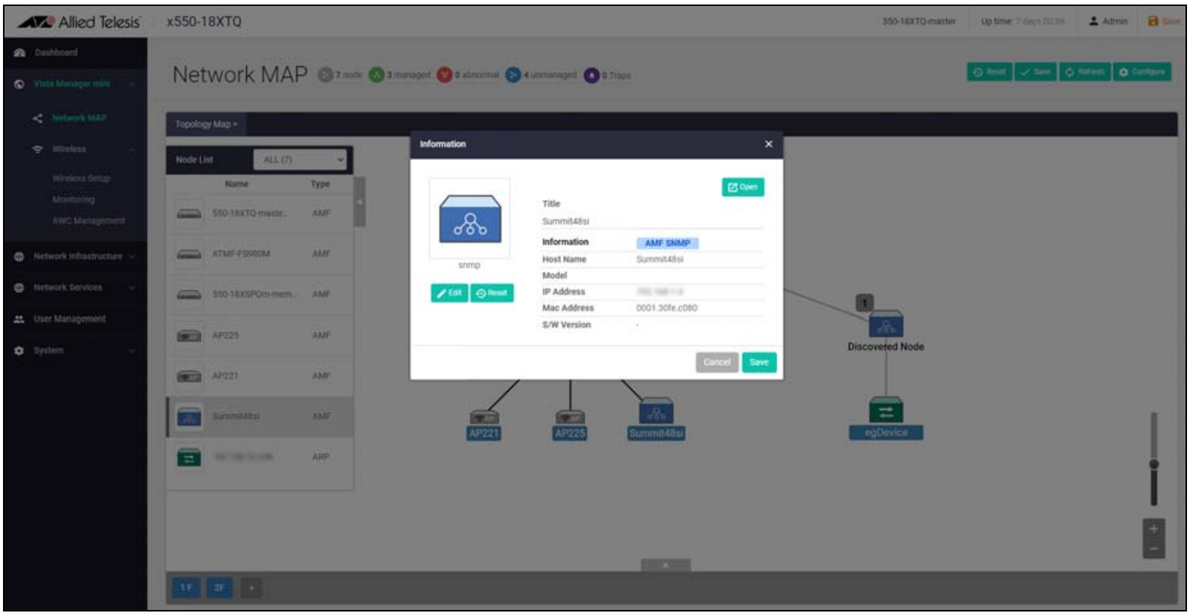


Node List ALL (9)

550-18XTQ-maste...	AMF
ATMF-FS980M	AMF
550-18XSPQm-mem...	AMF
AP225	AMF
AP221	AMF
Summit48si	AMF
[redacted]	ARP
[redacted]	ARP
[redacted]	ARP

Information
Hostname : [redacted]
IP Address : [redacted]
MAC Address : b222.2def.0107
Discovery
Last seen : 2020-06-26 17:52
Interface : vlan1

Click on the device icon in the Node List to display more detailed information:



Node List ALL (7)

Name	Type
550-18XTQ-maste...	AMF
ATMF-FS980M	AMF
550-18XSPQm-mem...	AMF
AP225	AMF
AP221	AMF
Summit48si	AMF
[redacted]	ARP

Information

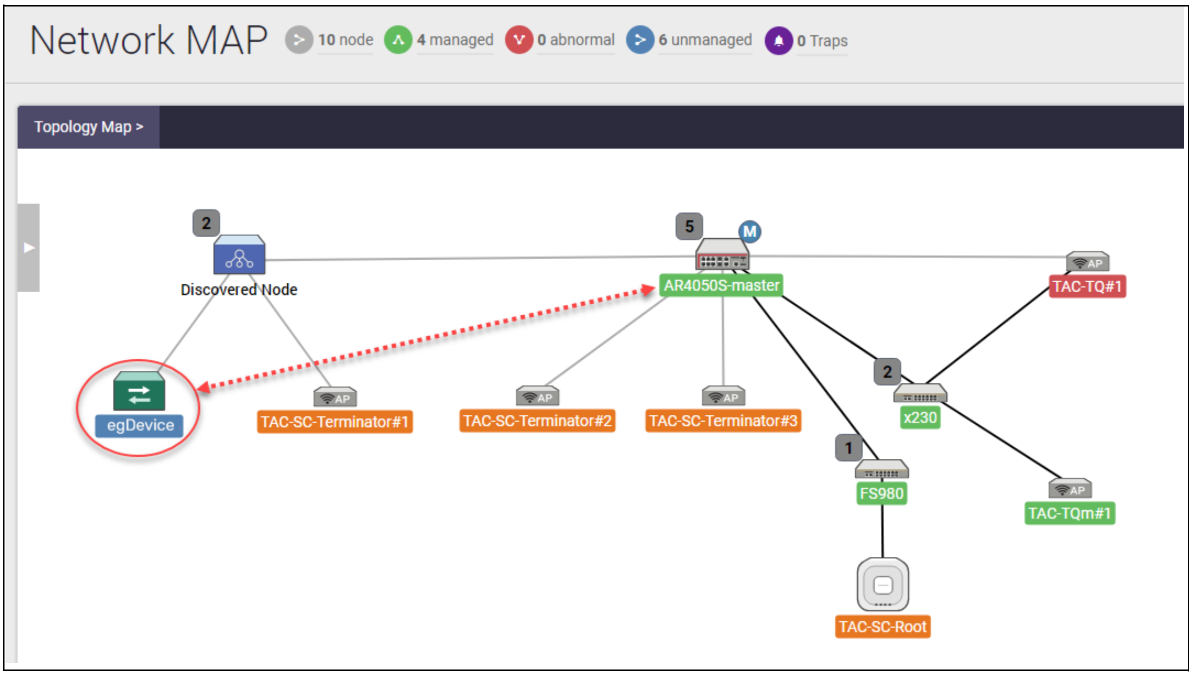
Title
Summit48si

Information	AMF SNMP
Host Name	Summit48si
Model	
IP Address	[redacted]
Mac Address	0001.30fe.c080
S/W Version	-

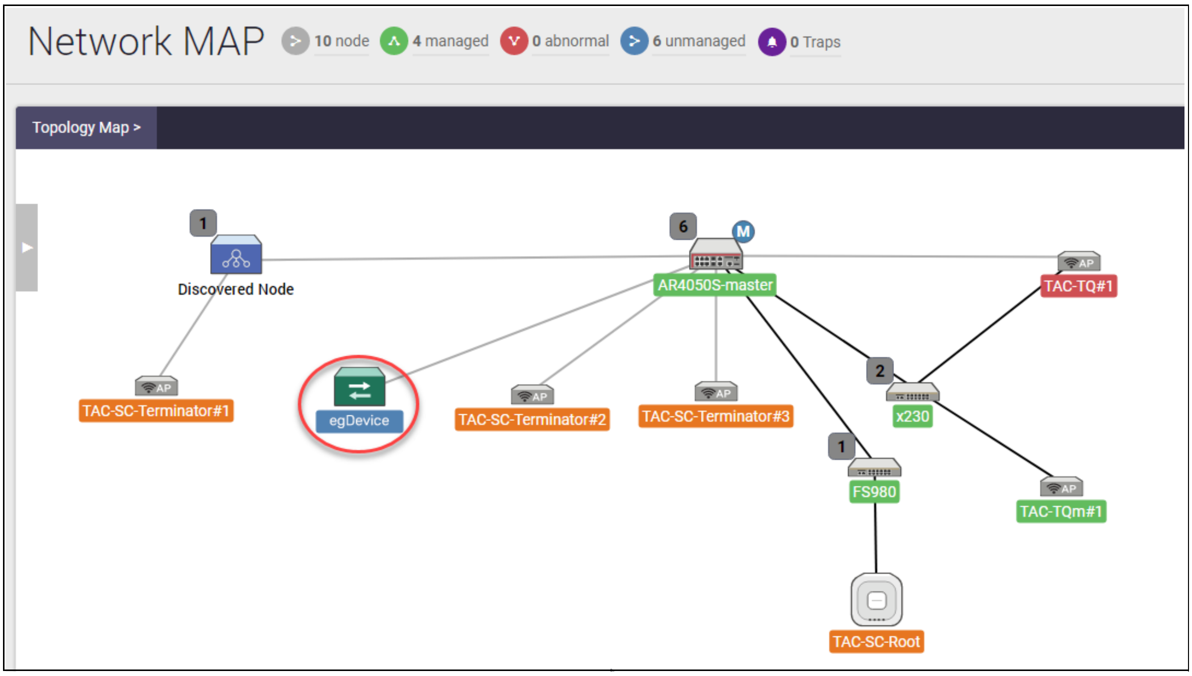
Drag and drop feature

If you want to move a node to a different location in the Network MAP you can use the **drag and drop** feature. For example, to move the discovered node Host ‘egDevice’ from its current location to the AR4050S-master node click on the node to move and drag it to its new location.

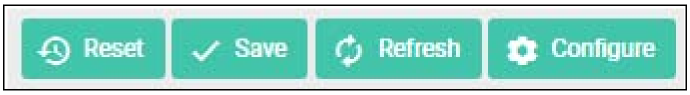
1. Click on the node and drag it to the new location, for example:



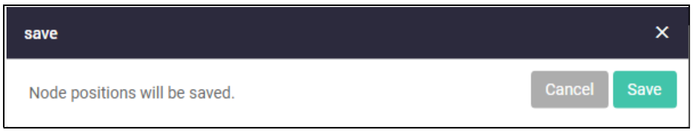
The result below shows that the node is now repositioned from where you clicked on it and then dragged it to its new position:



2. To save the Network MAP node positions and locations click **save**:



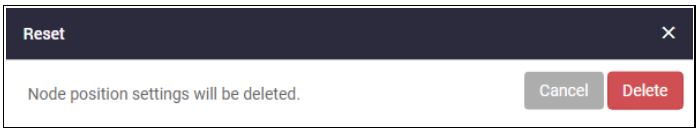
3. Click on the **save** button if you want to save the new position settings:


save

Node positions will be saved.

Or if you want to reset your Network Map nodes back to the original positions to the way they were before you changed it, choose the reset option.

4. Click on the **reset** button if you want to put the node positions settings back to how they were before you moved them:


Reset

Node position settings will be deleted.

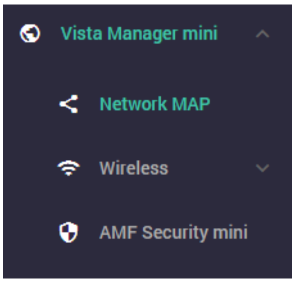
Now you can see your Network Map as it was before you changed it.

How to see SNMP Monitoring trap data

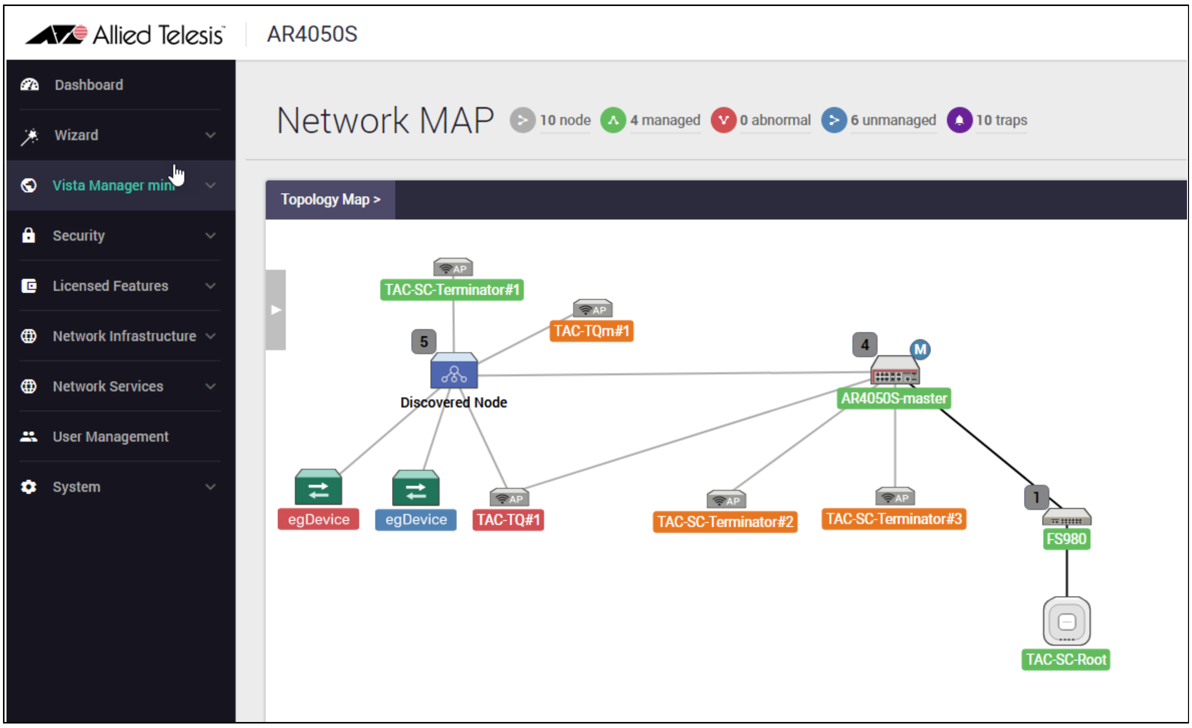
You need to use the CLI to enable traps that you want Vista Manager mini to display. See "Before you start" on page 9.

To display SNMP Monitoring trap notifications and trap counts for devices in your network, follow the steps below:

1. Click **Vista Manager mini > Network MAP**:

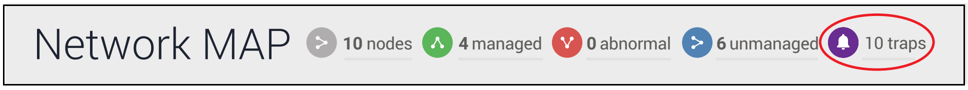


The Network MAP topology is displayed. You can monitor SNMP trap events from the Network MAP menu bar. All SNMP node trap counts display at the top of the Network MAP page, as 'x traps' (where ‘x’ is the number of traps). If there are new trap alarms, you will see this by a wobble effect on the bell icon beside the number of traps.



Trap icon

2. Click on the **traps** icon that appears on a the Network MAP menu bar as shown below:

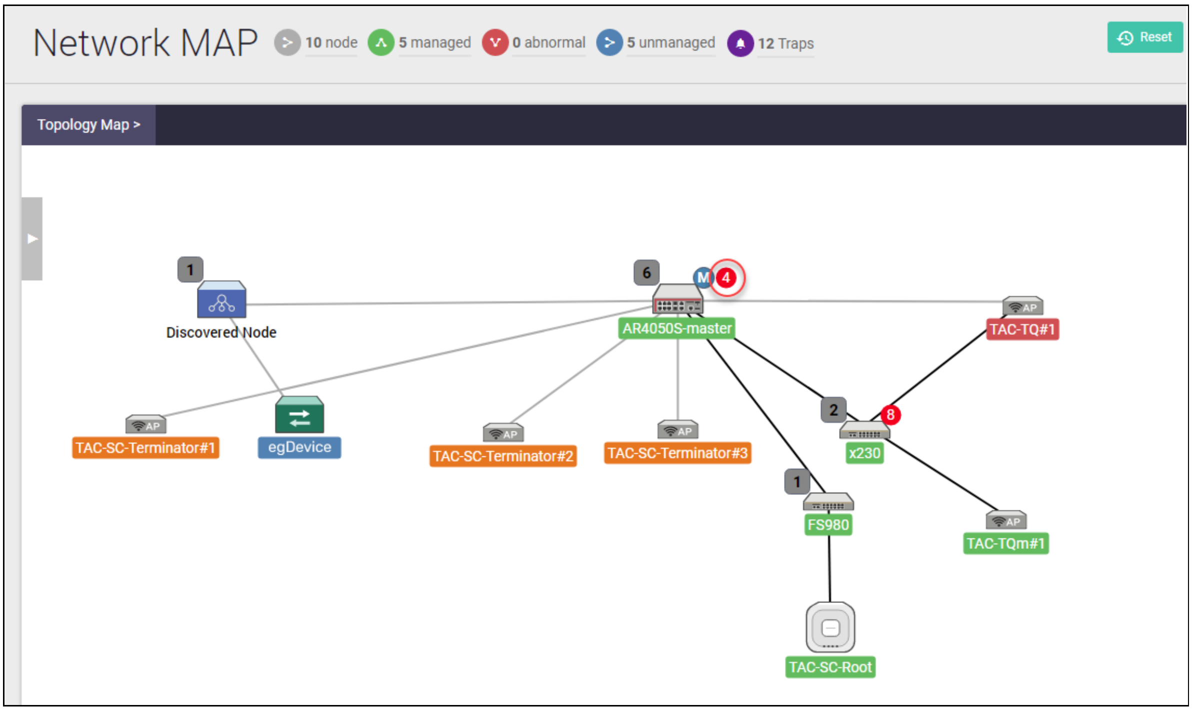


If traps have occurred, the number of traps appears in the menu bar as above showing 10 traps.

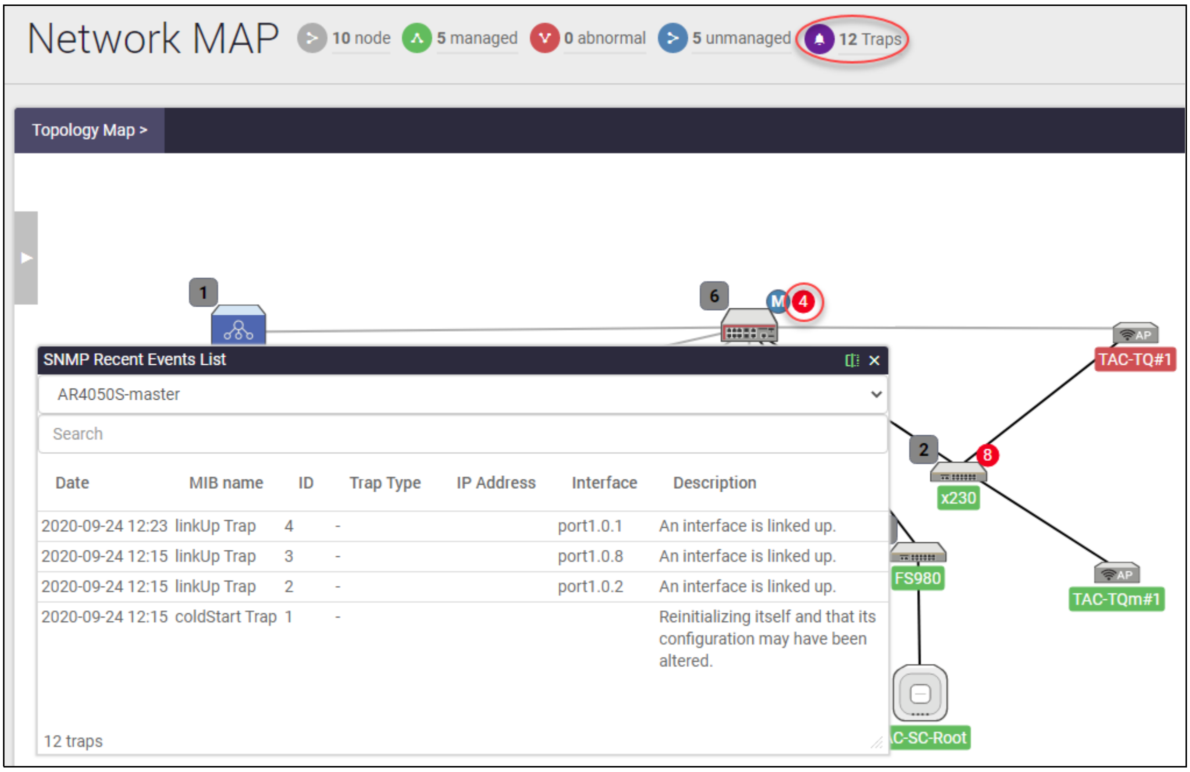
Trap badge

Trap indication also shows on the Network MAP on the node as a **trap badge** with the number of traps that have occurred. In the example below there are 4 traps on the AR4050S-master node and 8 traps on the x230 node. They show illuminated in red.

3. Click on the **traps badge** that appears on a node in the Network MAP shown below:



You can click on either the traps icon in the menu bar or the traps badge that appears on a node. In this example the events list is showing traps for the AR4050-master node. The **SNMP Recent Events List** shows the SNMP traps list:



SNMP Recent Events List

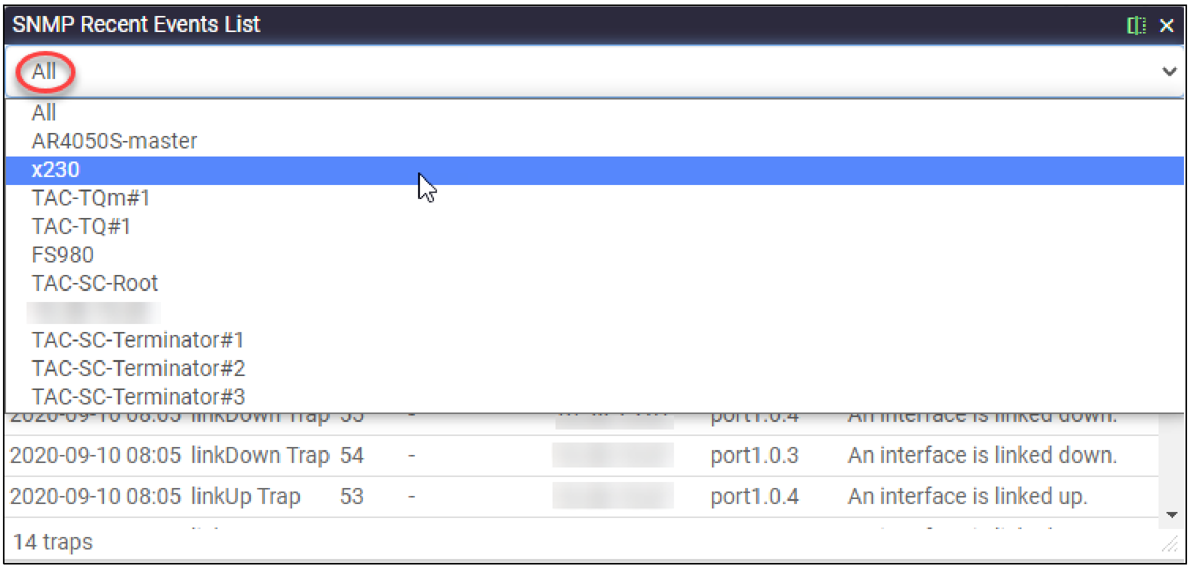
AR4050S-master

Search

Date	MIB name	ID	Trap Type	IP Address	Interface	Description
2020-09-24 12:23	linkUp Trap	4	-		port1.0.1	An interface is linked up.
2020-09-24 12:15	linkUp Trap	3	-		port1.0.8	An interface is linked up.
2020-09-24 12:15	linkUp Trap	2	-		port1.0.2	An interface is linked up.
2020-09-24 12:15	coldStart Trap	1	-			Reinitializing itself and that its configuration may have been altered.

12 traps

4. Click on **all** to display all nodes, then select the node that you want to display the events list for. For example, the x230 node is selected below:



SNMP Recent Events List

All

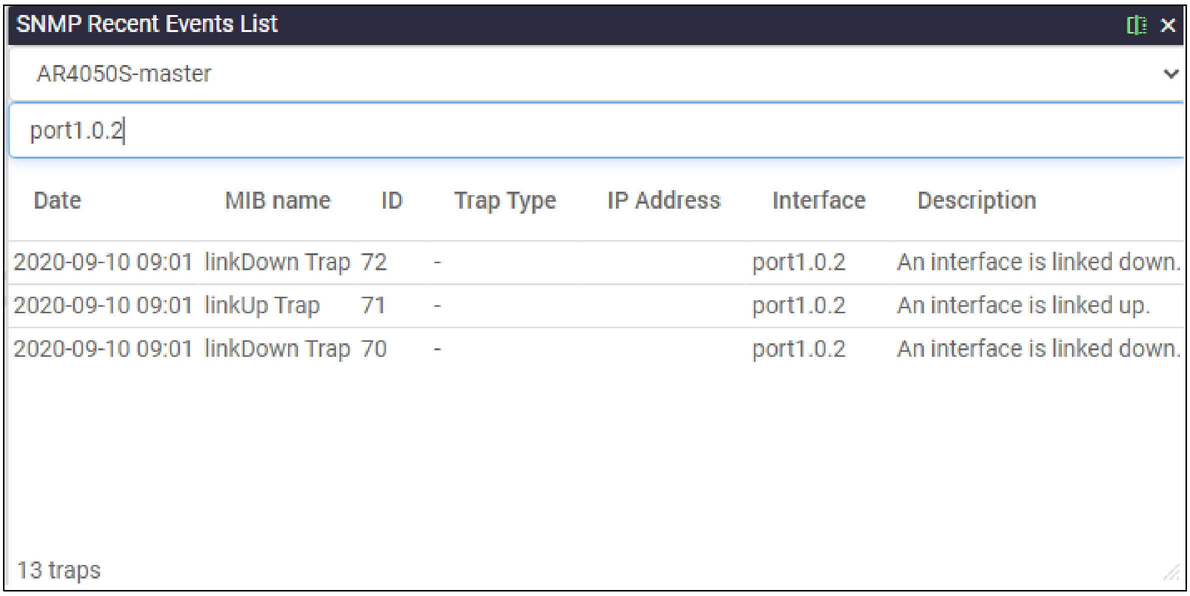
2020-09-10 08:05	linkDown Trap	55	-	[redacted]	port1.0.4	An interface is linked down.
2020-09-10 08:05	linkDown Trap	54	-	[redacted]	port1.0.3	An interface is linked down.
2020-09-10 08:05	linkUp Trap	53	-	[redacted]	port1.0.4	An interface is linked up.

14 traps

After you have seen the list, you can either choose from the node list as above or enter a search term shown below.

5. Enter search criteria if required.

For example, the search below shows traps and notifications for port1.0.2 on the AR4050S-master node:



SNMP Recent Events List

AR4050S-master

port1.0.2

Date	MIB name	ID	Trap Type	IP Address	Interface	Description
2020-09-10 09:01	linkDown Trap	72	-		port1.0.2	An interface is linked down.
2020-09-10 09:01	linkUp Trap	71	-		port1.0.2	An interface is linked up.
2020-09-10 09:01	linkDown Trap	70	-		port1.0.2	An interface is linked down.

13 traps

SNMP Discovery through the AlliedWare Plus CLI

SNMP Device Discovery is also available from the AlliedWare Plus CLI as well as from Vista Manager mini. This feature provides information that allows the CLI to display third party vendor device data in real time. This feature applies to all AlliedWare Plus products that are AMF capable, running version 5.5.0-0.3 or later.

What to configure

The roles that can to be configured for SNMP Discovery are:

- AMF nodes that are directly connected to discoverable devices
- discoverable devices.

Before you start

Before you configure SNMP Discovery, you must first complete the following tasks:

On AMF nodes connected to discoverable devices:

- Run AlliedWare Plus version 5.5.0-0.3 or later.
- Configure your AMF network. For more information about AMF, see the AMF Feature Overview and Configuration Guide.
- Have an IPv4 interface to the discoverable device and be able to ping the device.

And on the discoverable devices

- Set up SNMPv2 or v3
- Make sure that the devices will respond to SNMP ‘get’ requests.

How to configure SNMP Discovery

These commands enable SNMP Discovery to discover devices on an AMF network. The server starts a process which detects IP addresses reachable on a network. An SNMP ‘get’ request is performed on these IP addresses to detect device information. The SNMP Name, SNMP Description, SNMP Location and SNMP Serial Number are obtained if they are available. SNMP Discovery will not run if there are no Layer 3 IP interfaces configured.

To start the discovery service on the AMF node and set the SNMP version, follow these steps:

Step 1: **Enable SNMP Discovery**

To start the discovery service on the AMF node, use the commands:

```
awplus#configure terminal
awplus(config)#service snmp-discovery
```

Step 2: Set the SNMP version

To set the SNMP version to use, use the commands:

```
awplus#configure terminal
awplus(config)#snmp-discovery snmp-version {v1|v2c|v3}
```

This command creates an SNMP community in read only mode.The community allows access to all the MIB objects. The SNMP communities are only valid for SNMPv1 and v2c and provide very limited security. Communities should not be used when operating SNMPv3.

Step 3: If using SNMP v2c, set the community name

To configure the community name (in read only mode) to be 'accounting', use the commands:

```
awplus(config)#configure terminal
awplus(config)#snmp-discovery community accounting
```

Step 4: If using SNMP v3, set the security

You can choose the security level and then the authentication protocol and privacy protocol.

For example, to add SNMP Discovery user 'authuser', with authentication protocol 'sha', authentication password 'Authpass', privacy protocol 'aes' and privacy password 'Privpass', use the commands:

```
awplus(config)#configure terminal
awplus(config)#snmp-discovery user authuser auth sha Authpass priv aes
Privpass
```

The authentication method must match what is used on the devices being discovered and the AMF node they are connected to.

Step 5: Repeat the above steps on other AMF nodes

Repeat the above steps on every AMF node that has a discoverable device connected to it.

How to optionally configure polling intervals

SNMP Discovery first uses ARP to discover subnets that are reachable from the AMF node. This polling happens every 60 seconds by default. To change the ARP request polling interval (in seconds), use the commands:

```
awplus(config)#configure terminal
awplus(config)#snmp-discovery arp-polling-interval <60-3600>
```

This polling happens on each Layer 3 interface with a subnet of 256 members or less. If you need SNMP Discovery on nodes with subnets of greater than 256 members, use the commands:

```
awplus(config)#configure terminal
awplus(config)#snmp-discovery permit ip <ipv4-address>
```

If an IPv4 address responds to an ARP request, the IP address and MAC address are added to a list which is available to SNMP discovery to contact.

ARP polling and SNMP Discovery uses SNMP 'get' requests to poll the devices discovered by the ARP polling. This polling happens every 300 seconds (5 minutes) by default. To change the SNMP request polling interval (in seconds), use the commands:

```
awplus(config)#configure terminal
awplus(config)#snmp-discovery snmp-polling-interval <60-3600>
```

SNMP polling is enabled when **service snmp-discovery** is enabled.

How to optionally deny interfaces and deny or permit IP addresses

In some network situations, you may need to turn SNMP Discovery on or off for specific IP addresses or interfaces.

Deny an IP address

You can use the deny address command to prevent ARP requests from being sent on an IP address.

Due to dynamic learning of IP addresses, it is possible for SNMP Discovery to report duplicate entries. In that case, a message will show multiple connections to the discovered device. You can prevent this by finding out which IP address has reported the unwanted link and denying that IP address. When an IPv4 address is denied, it means an SNMP 'get' request will never be sent to that device when **service snmp-discovery** is enabled.

The example below shows a duplicate address that has been discovered:

```
2020 May 07 00:39:28 daemon.err 04-L3SW1 snmpd[1335]: Received SNMP Packet from
illegal server 172.18.3.1
```

To deny this IPv4 address 172.18.3.1, use the commands:

```
node1#configure terminal
node1(config)#snmp-discovery deny ip 172.18.3.1
```

Permit an IP address

By default all IPv4 interfaces with prefixes of 256 members or less are included in SNMP discovery.

If you want to allow SNMP Discovery to do requests on interfaces with greater than 256 members, you can permit a specific IP address. For example, to permit SNMP Discovery for IPv4 address 10.34.180.100, use the commands:

```
node1#configure terminal
node1(config)#snmp-discovery permit ip 10.34.180.100
```

Deny an interface

By default, all IPv4 interfaces with prefixes of 256 members or less are included in SNMP discovery. AMF and stacking VLANS are denied by default.

You can use the deny interface command to prevent SNMP requests from being sent on an interface. To deny VLAN2, use the commands:

```
node1#configure terminal
node1(config)#snmp-discovery deny interface vlan2
```

Interfaces cannot be specifically permitted, only denied.

How to remove discovered devices

To remove all SNMP discovered devices, use the command:

```
clear snmp-discovery nodes
```

To remove a particular SNMP discovered device, use the command:

```
clear snmp-discovery nodes <ipv4_address>
```

To remove all entries from SNMP Discovery's database of devices discovered by ARP, use the command:

```
clear snmp-discovery ip
```

To remove a particular entry from SNMP Discovery's database of devices discovered by ARP, use the command:

```
clear snmp-discovery ip <ipv4_address>
```

Configuration examples

The following examples show how to configure SNMP v2c, SNMP v3, how to configure a deny/ permit list, and how to deal with duplicate device discovery:

Example 1 Enable SNMP discovery for SNMP version v2c

The simplest case automatically enables SNMP discovery on interfaces and SNMP v2c polling on any discovered IPv4 addresses with the default community name of 'public'. This discovers SNMP devices that are directly connected to the node you enter these commands on.

```
awplus#service snmp-discovery
```

Example 2 Enable SNMP discovery for SNMP version v3

Passwords are stored in encrypted format in the running configuration. The SNMP security level is set according to what authentication and privacy configuration is entered. If no auth or priv are present then noAuthNoPriv is used. If only auth is present then authNoPriv is used and if both are present authPriv is used.

To enable and configure an SNMP v3 user on a node, use the commands:

```
awplus#service snmp-discovery
awplus#snmp-discovery user tim md5 authPassword priv des privPassword
awplus(config)#snmp-discovery snmp-version v3
```

Example 3 Configure deny/permit list

The example below shows two permitted addresses 192.168.4.5 and 192.168.4.55 which are part of the vlan4 interface which is denied. The two permitted addresses override the denied interface configuration, and will take part in ARP discovery and SNMP polling.

```
awplus#service snmp-discovery
awplus(config)#interface vlan4
awplus(config)#ip address 192.168.4.6/24
awplus#snmp-discovery permit ip 192.168.4.5
awplus#snmp-discovery permit ip 192.168.4.55
awplus#snmp-discovery deny interface vlan4
```

Example 4 Duplicate SNMP Device Discovery

Due to dynamic learning of IP addresses, it is possible for SNMP Discovery to report duplicate entries. You can prevent this by finding out which IP address has reported the unwanted link and denying that IP address on all nodes where you do not want them to appear. The deny address 192.168.3.5 in the following example has already been learned on another AMF member node.

```
awplus#service snmp-discovery
awplus(config)#snmp-discovery deny ip 192.168.3.5
```

How to use logging to monitor SNMP Discovery

Logging is available for the SNMP discovery service, to record when it is started and stopped.

An AMF log message is displayed on the AMF master (or controller) when a discovered device joins or leaves the network.

```
10:54:47 AR4050S ATMF[1380]: x530L-28GTX
 port port1.0.7 SNMP Discovered node network test area local parent E1-AR4050S MAC
3863.bb5c.b900 IP 192.168.2.2 has joined. 3 members in total, 1 discovered.
```

How to use show commands to monitor SNMP Discovery

Show commands are used to monitor what is going on with SNMP Discovery:

- **Show snmp-discovery: view settings and information about discovered devices**
- **Displaying information about all nodes**
- **Show atmf: view the number of SNMP discovered devices**
- **Show running-config snmp-discovery: view the configuration**

Show snmp-discovery: view settings and information about discovered devices

To display SNMP discovery configuration or learned device information, use the command **show snmp-discovery [nodeslipldetail]** in User Exec mode.

To display the settings, use the command **show snmp-discovery**:

```
node1#show snmp-discovery
SNMP Discovery information:

SNMP Discovery                : Enabled
SNMP Polling interval         : 300
ARP Polling interval          : 60
SNMP Discovery version        : v2c

SNMPv2 Discovery Community    : accounting
```

To display learned IPv4 addresses, use the command **show snmp-discovery ip**:

```
node1#show snmp-discovery ip
SNMP Discovery Devices:

IP Address       MAC Address     Type     State         Last Seen Time
----------------------------------------------------------------------------
172.18.100.10    -               Permit   -             -
172.18.100.25    0000.cd28.063e  Dynamic  Up            -
172.18.100.15    0001.30fe.c080  Dynamic  Up            -
172.18.100.208   801f.0230.006c  Dynamic  Down          Jul 27, 2020 03:52:01
172.18.100.209   801f.0230.006c  Dynamic  Down          Jul 24, 2020 04:45:30
172.18.100.20    0010.db5c.efe4  Dynamic  Up            -
172.18.100.207   801f.0230.006c  Dynamic  Down          Jul 27, 2020 06:26:20
172.18.100.10    001b.5443.a5b0  Dynamic  Up            -
172.18.100.205   801f.0230.006c  Dynamic  Down          Jul 27, 2020 17:15:15
172.18.100.204   801f.0230.006c  Dynamic  Down          Jul 25, 2020 19:20:35
172.18.100.203   801f.0230.006c  Dynamic  Down          Jul 25, 2020 21:15:04
172.18.100.202   801f.0230.006c  Dynamic  Down          Jul 28, 2020 10:20:10
```

To display the node information learned on an AMF member node, use the command **show snmp-discovery nodes**:

```
node1#show snmp-discovery nodes
SNMP Discovery Node information:

System Name      IP Address       MAC Address     Description
--------------------------------------------------------------------------------
TQ1402           172.18.100.15    0001.30fe.c080  wireless access point ...
NAT-ROUTER-DESK  172.18.100.25    0000.cd28.063e  CentreCOM AR570S version ...

Number of SNMP discovered nodes: 2
```

To display more information, use the command **show snmp-discovery detail**:

```
node1#show snmp-discovery detail
SNMP Discovery Node Details:

Name                      TQ1402
Serial Number             FHK1115F13A
IP Address                172.18.100.10
MAC Address               001b.5443.a5b0
Local Interface           port1.0.1
Description              2-radio 802.11ac Wave 2 Wireless Access Point
State                     Down
Location                  -
Time Last Seen            2020-04-29T03:33:39Z

Name                      NAT-ROUTER-DESK
Serial Number             -
IP Address                172.18.100.20
MAC Address               0010.db5c.efe4
Local Interface           port1.0.1
Description               Router building 2
State                     Up
Location                  -
Time Last Seen            -

Number of SNMP discovered nodes: 2
```

Displaying information about all nodes

AMF enables you to run show commands on all AMF nodes in a single operation.

To do this, use the command **atmf working-set group all** to add all nodes in AMF to the working-set:

```
node1#atmf working-set group all
```

This command displays an output screen similar to the one shown below:

```
=========================================
node1, node2, node3, node4, node5, node6:
=========================================

Working set join

ATMF_NETWORK_Name[6]#
```

Then you can run the command **show snmp-discovery nodes** on that working set of all AMF nodes. This will show you all the discovered nodes in your AMF network.

Show atmf: view the number of SNMP discovered devices

To display the number of discovered nodes found by the AMF network on an AMF master or controller, use the command **show atmf**:

```
node1#show atmf
ATMF Summary Information:

ATMF Status            : Enabled
Network Name           : bob
Node Name              : E1-AR4050S
Role                   : Master
Restricted login       : Disabled
Secure Mode            : Disabled
Current SNMP Nodes     : 1
Current ATMF Guests    : 0
Current ATMF Nodes     : 2
```

Show running-config snmp-discovery: view the configuration

To display the running configuration for SNMP device discovery, use the command **show running-config snmp-discovery**:

```
node1#show running-config snmp-discovery
service snmp-discovery
snmp-discovery community public
snmp-discovery user tim bob encrypted auth md5 U2FsdGVkX1/
LyNttTLDzgjJTG6Eh5g2L4ahgXuHLENA= priv des
U2FsdGVkX1+FJsefN+ZvSzUUviRt9ZdsFwtB6HU12lU=
snmp-discovery permit ip 1.2.3.4
snmp-discovery permit ip 1.2.3.6
snmp-discovery deny ip 1.2.3.5
```

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com