

Vista Manager EX

SNMP Plug-in User Guide

Introduction

The Vista Manager SNMP plug-in can acquire detailed information and statistics from a broad range of networking devices. Different views enable users to manage devices the way they prefer. It supports management of up to 2000 devices, and in large networks it automatically searches for SNMP agents and displays each device found in tree form, for an easy view of the overall network topology. The SNMP plug-in is a powerful addition to Vista Manager EX, adding management flexibility by supporting non-AMF devices.

The SNMP plug-in also offers a MIB compiler, and generates a chart based on MIB values. It offers support for iMG devices and basic SNMP management, like alive monitoring and access to the iMG GUI. You can also backup and restore your settings.

The SNMP plug-in is closely managed by Allied Telesis Vista Manager EX and is available as an optional plug-in to Vista Manager.

Vista Manager EX

Vista Manager EX™ is a graphical network monitoring and management tool for Allied Telesis Autonomous Management Framework™ (AMF) networks. Vista Manager EX automatically creates a complete topology map from an AMF network of switches, firewalls and wireless access points (APs), showing areas and multiple levels of connected nodes and devices. Vista Manager EX facilitates simple management of many, or all, network devices from a dashboard that gives you a central overview of your network. From the dashboard you can monitor up-to-date network status, and take action to resolve any network problems.

Audience for this guide

This guide is intended for computer system administrators and network engineers.

Related documents

For information on how to install and use the Windows-based Vista Manager:

- [Vista Manager EX Windows-based Installation Guide](#)
- [Vista Manager EX Windows-based User Guide](#)

The following documents give more information about Vista Manager EX:

- [Vista Manager EX Datasheet](#)

Planning an AMF network is beyond the scope of this installation guide. The following documents give more information about AMF:

- [AMF Feature Overview and Configuration Guide](#)
- [AMF introduction and videos](#)

For information on how to use the AWC plug-in, see the [AWC Plug-in User Guide](#) on the [Vista Manager User Guide web page](#).

For information on how to use a Vista Manager EX **virtual appliance**, see the [Vista Manager EX Virtual Appliance User Guide](#) on the [Vista Manager User Guide web page](#).

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

Contents

Introduction	1
Vista Manager EX.....	1
Audience for this guide	2
Related documents.....	2
Contents	3
Using the SNMP Plug-in	4
Introduction.....	4
Add an SNMP network	4
Add an SNMP device manually	7
SNMP Dashboard	8
Backup and restore the SNMP plug-in.....	9
Setting up the SNMP Plug-in Server.....	10
SNMP Plug-in System Setting.....	10
MIB Compiler	15
Action Command Settings Utility.....	17
Minimail utility	20
Event Filter Settings Utility.....	21
Device Level Settings Utility	24
Troubleshooting.....	26
Ports and URLs used by Vista Manager EX	26
SNMP plug-in application pool settings	27
Supported Device List.....	29
AlliedWare Plus devices.....	29

Using the SNMP Plug-in

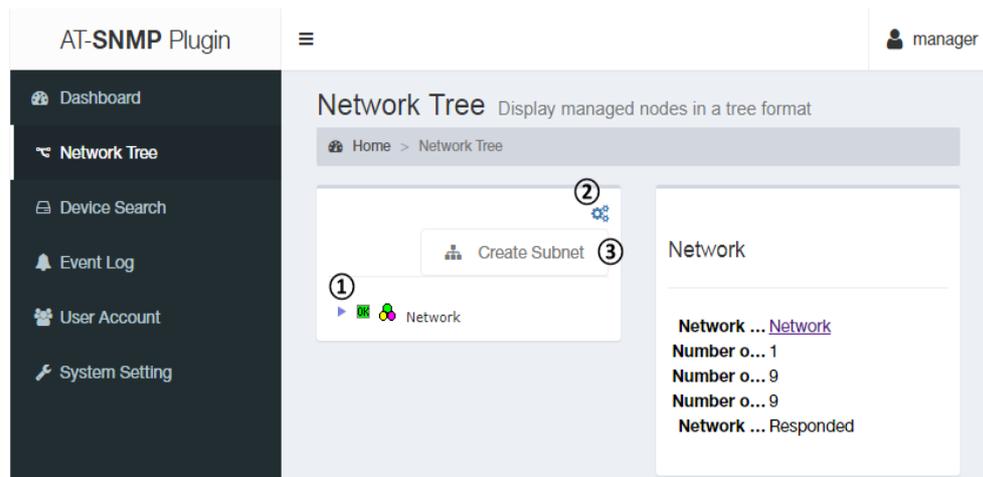
Introduction

The Vista Manager SNMP plug-in can acquire detailed information and statistics from a broad range of networking devices. Different views enable users to manage devices the way they prefer. It supports management of up to 2000 devices, and in large networks it automatically searches for SNMP agents and displays each device found in tree form, for an easy view of the overall network topology. The SNMP plug-in is a powerful addition to Vista Manager EX, adding management flexibility by supporting non-AMF devices.

Add an SNMP network

The following steps are required to set up your SNMP network.

1. Go to **Network Tree** screen, click on the **Network** icon (1), then click on the gear icon (2), then select **Create Subnet** (3).



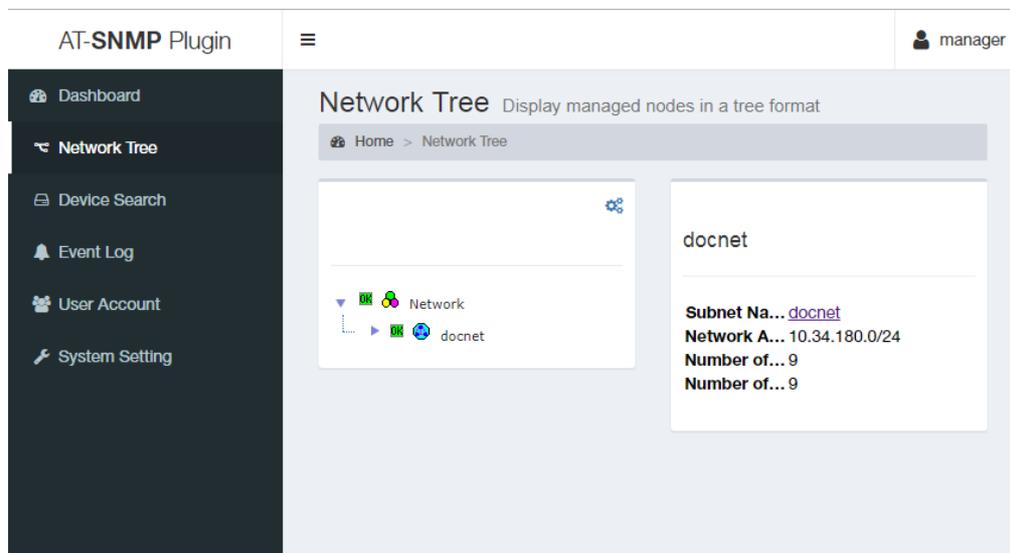
2. Add the subnet parameters.

The screenshot shows the 'AT-SNMP Plugin' interface with a sidebar on the left containing navigation options: Dashboard, Network Tree, Device Search, Event Log, User Account, and System Setting. The main content area is titled 'Subnet Create Subnet' and includes a breadcrumb trail: Home > Network Tree > Create Subnet. The form contains the following fields:

- Subnet Name:** docnet
- Network ID:** 10.34.180.0
- Subnet Mask:** 255.255.255.0 (highlighted in yellow)
- SNMP Parameter Name:** public (selected from a dropdown menu)

There is a 'Create' button at the bottom left and a link for 'SNMP Parameter List' at the bottom right.

3. Once the subnet is added, auto discovery is started for that subnet. This can take up to 30 minutes to discover all monitored devices.
4. To see the progress of the discovery, click on **Network** and select the subnet you created in Step 3, then click on the subnet name in the right-hand pane.



- This opens the detail screen for the subnet. The event log on the screen shows the progress of the auto discovery.

Subnet Subnet Detail

Home > Network Tree > Subnet Detail

docnet

Subnet Name : docnet
 Network Address : 10.34.180.0/24
 Number of discovered nodes : 9
 Number of managed nodes : 9

Edit | Delete

Date	Target Name	Model Name	Event Name	Message
2018-02-22 17:54:51	docnet		Started	A Subnet auto discovery started.
2018-01-23 17:59:49	docnet		Finished	A Subnet auto discovery stopped.

Note the gear icon in the top right of the subnet details pane. Click on it to see an option to start the auto discovery process again.

- After auto discovery is complete you will see a list of devices on the **Network Tree** screen by selecting **Network** and the subnet name.

AT-SNMP Plugin

manager

Network Tree Display managed nodes in a tree format

Home > Network Tree

Network

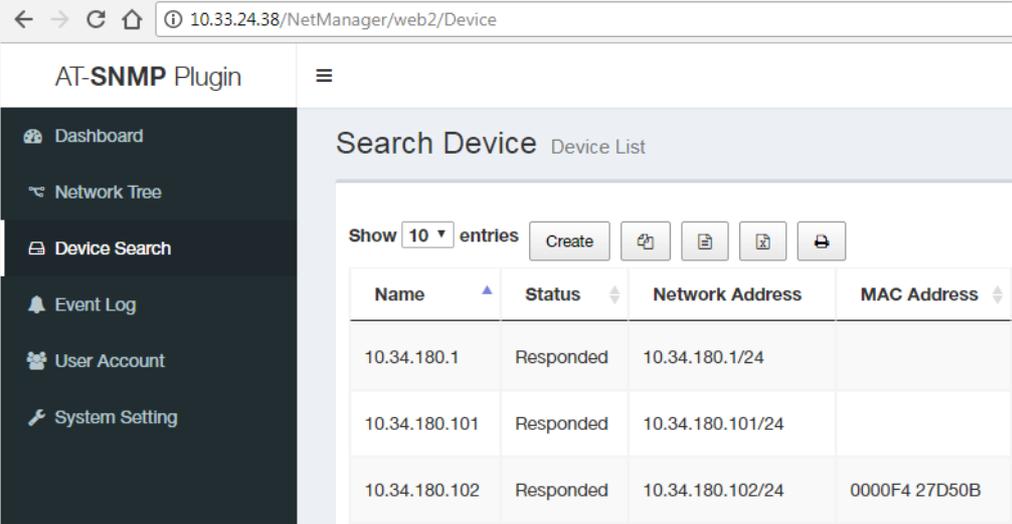
- docnet
 - 10.34.180.1
 - 10.34.180.101
 - 10.34.180.102
 - 10.34.180.103
 - 10.34.180.104
 - 10.34.180.105
 - 10.34.180.106
 - 10.34.180.107
 - 10.34.180.50

docnet

Subnet Name : [docnet](#)
 Network Ad... 10.34.180.0/24
 Number of di... 9
 Number of ... 9

Add an SNMP device manually

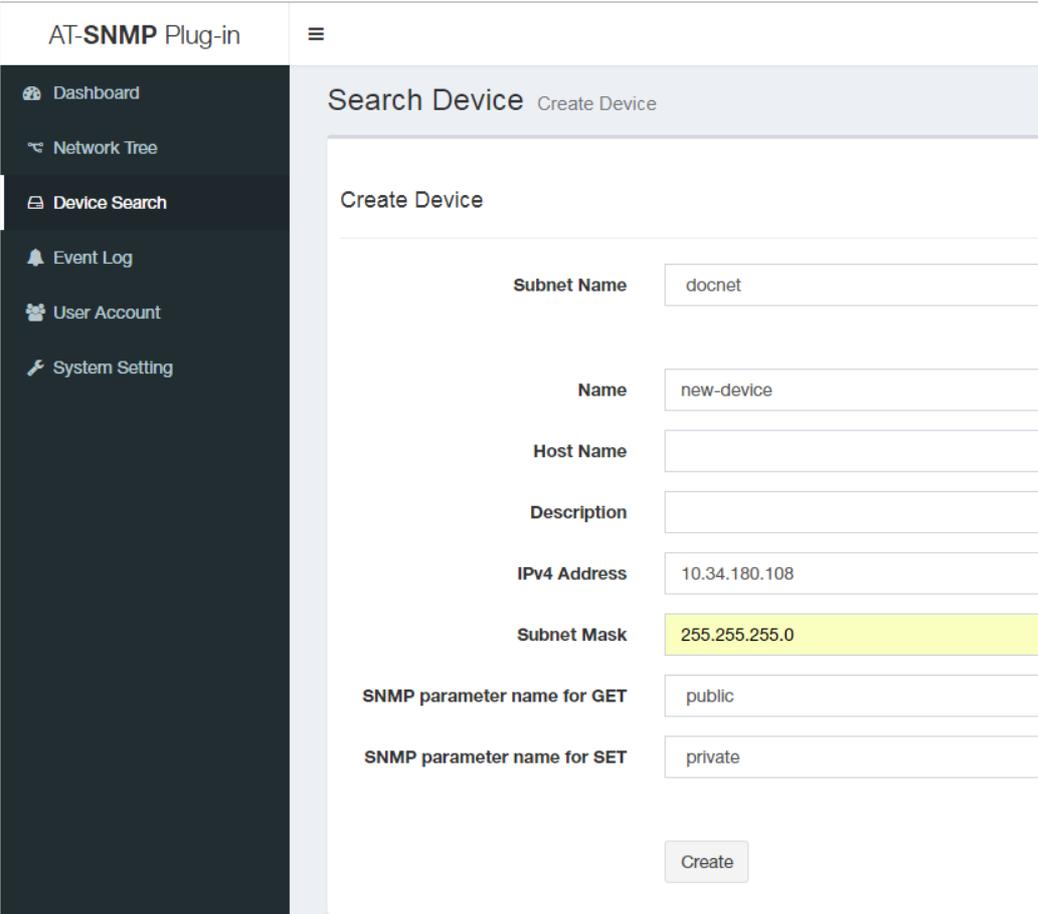
1. Select **Device Search** on the menu bar, then click on **Create**.



The screenshot shows the AT-SNMP Plugin interface. The left sidebar contains a menu with options: Dashboard, Network Tree, Device Search (selected), Event Log, User Account, and System Setting. The main content area is titled 'Search Device' and 'Device List'. It features a 'Show 10 entries' dropdown and a 'Create' button. Below this is a table with the following data:

Name	Status	Network Address	MAC Address
10.34.180.1	Responded	10.34.180.1/24	
10.34.180.101	Responded	10.34.180.101/24	
10.34.180.102	Responded	10.34.180.102/24	0000F4 27D50B

2. Enter the information for the device you wish to monitor, then press the **Create** button.



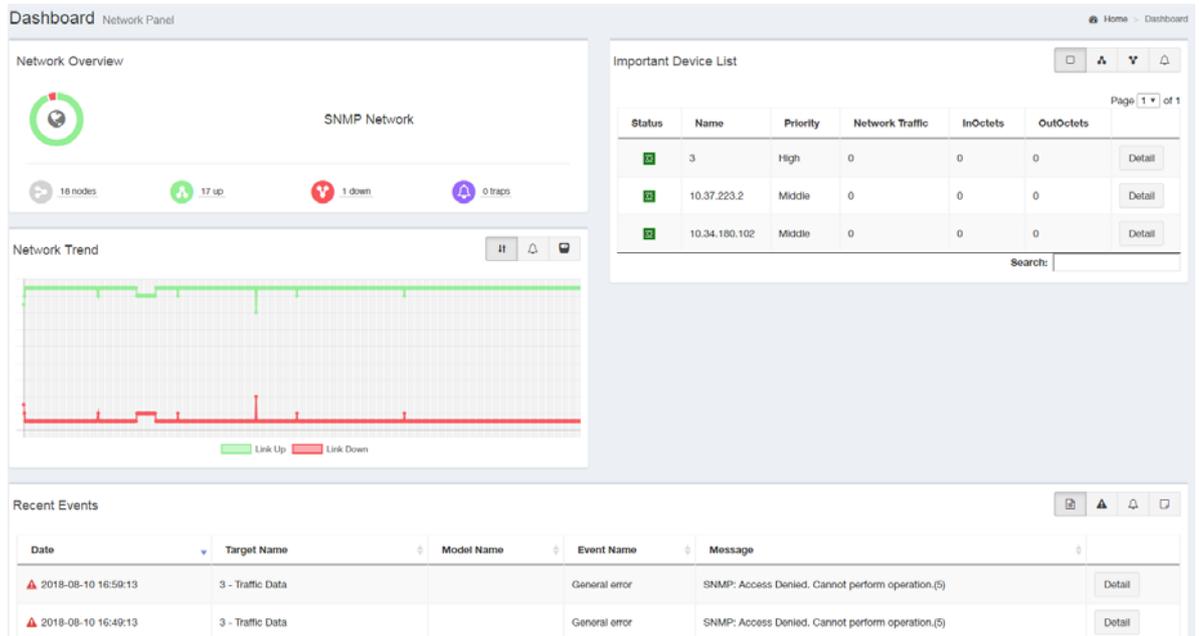
The screenshot shows the AT-SNMP Plugin interface with the 'Create Device' form. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Search Device' and 'Create Device'. The form contains the following fields:

- Subnet Name: docnet
- Name: new-device
- Host Name: (empty)
- Description: (empty)
- IPv4 Address: 10.34.180.108
- Subnet Mask: 255.255.255.0 (highlighted in yellow)
- SNMP parameter name for GET: public
- SNMP parameter name for SET: private

A 'Create' button is located at the bottom of the form.

SNMP Dashboard

Once your SNMP subnet has been added, and your devices discovered, the SNMP dashboard will start to populate. These graphs, however, only update hourly, so it may be some time before you see any results.



Backup and restore the SNMP plug-in

There are 2 utilities, 1 for taking a backup, and 1 for restoring a backup. Run these locally on the SNMP plug-in server.

1. Stop the SNMP server services using the shortcut created during installation or by running the following command line, as an administrator.

```
"<Vista Install Path>\Plugins\AT-SNMP\NetManager\bin\svrcmd.bat" svrstop
```

1. Run the appropriate utility to either backup or restore the SNMP plug-in database. These utilities need to be run as an administrator.

Backup:

```
"<Vista Install Path>\Plugins\AT-SNMP\NetManager\bin\SMBackup.exe"
```

Restore:

```
"<Vista Install Path>\Plugins\AT-SNMP\NetManager\bin\SMRestore.exe"
```

1. Follow the instructions on the screen.
2. Start the SNMP services using the shortcut or by running the following command line, as an administrator.

```
"<Vista Install Path>\Plugins\AT-SNMP\NetManager\bin\svrcmd.bat" svrstart
```

Note: The default location of **<Vista Install Path>** is C:\Program Files (x86)\Allied Telesis\AT-Vista Manager EX

The following information is backed up:

- nodes registered with the plug-in
- MIB files
- log files
- "SNMP Plug-in Setting Utility" configuration.
- "Action Command Setting Utility" configuration
- "Event Filter Setting Utility" configuration
- "Device Level Setting Utility" configuration

Note: The SNMP plug-in backup does not include AMF device information and license information stored in Vista Manager EX, or wireless AP management data stored in the AWC plug-in. This data must be backed up independently in the relevant module.

Note: Restoring Vista Manager backups from a newer version into an older version is not supported. It is not possible, for example, to restore a backup made in Vista Manager 2.4.0 into a Vista Manager 2.3.1 installation.

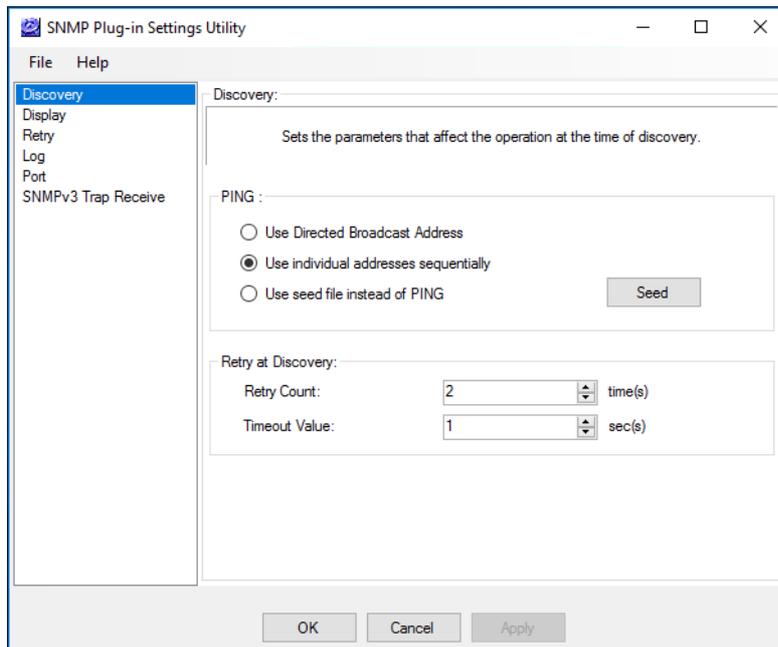
Setting up the SNMP Plug-in Server

SNMP Plug-in System Setting

These are configured using the **SNMP Plug-in Settings Utility**. The utility is located locally on the Vista Manager EX server. Start it by right-clicking on the following executable and choosing to run as an administrator:

<Vista Install Path>\Plugins\AT-SNMP\NetManager\bin32\ANMPluginConfig.exe

Discovery Settings



These settings are used by the SNMP plug-in to discover SNMP devices on the subnet.

Use individual addresses sequentially (default): This is the most reliable, but slowest, detection method. A ping packet is sent to each IP address in the specified subnet.

Use direct broadcast address: Using a broadcast address takes less time and creates less traffic than pinging each address sequentially. Network broadcasts, however, may be filtered out by routers and some devices do not respond to them.

Use seed file instead of ping: A seed file is a text file with one IP address per line. Use this method if the IP addresses of the nodes you want to manage are known in advance.

The path to the seed file is:

<Vista Install Path>\Plugins\AT-SNMP\NetManager\etc\seed.lst

You can create this seed file manually or generate it from an existing hosts file by clicking on the “Seed” button and selecting an appropriate file.

Sample hosts file:

```
# sample hosts file
192.168.10.1 saba
192.168.10.5 tara
192.168.20.1 tai
192.168.20.100
192.168.30.2
```

Notes:

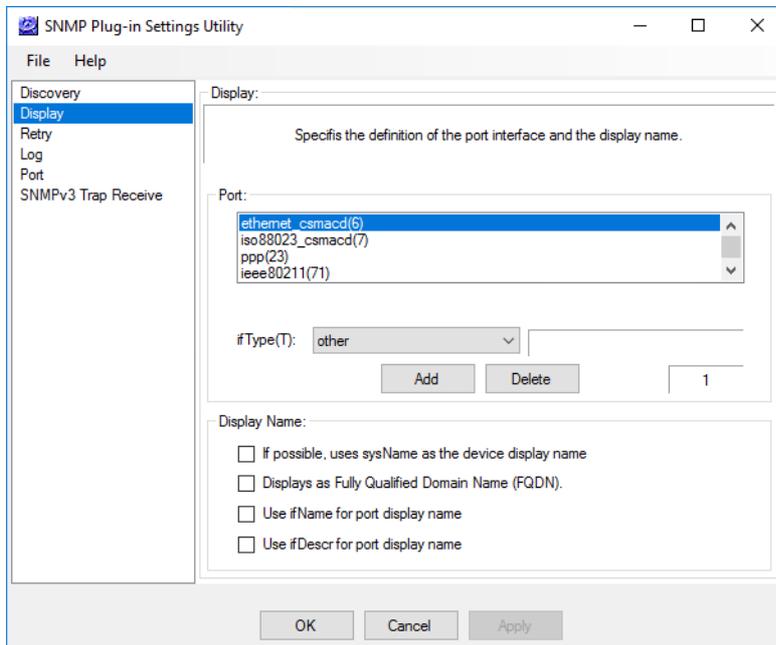
- Any line beginning with an IP address is valid.
- Lines beginning with an # symbol are ignored.
- Host name, or other details, following the IP address are ignored.

Sample seed.lst file:

```
192.168.10.1
192.168.10.5
192.168.20.1
192.168.20.100
192.168.30.2
```

Retry at Discovery: The Retry Count (default 2) and Timeout Value (default 1) specify the number of retries and the wait time before considering a discovery attempt failed.

Display Settings

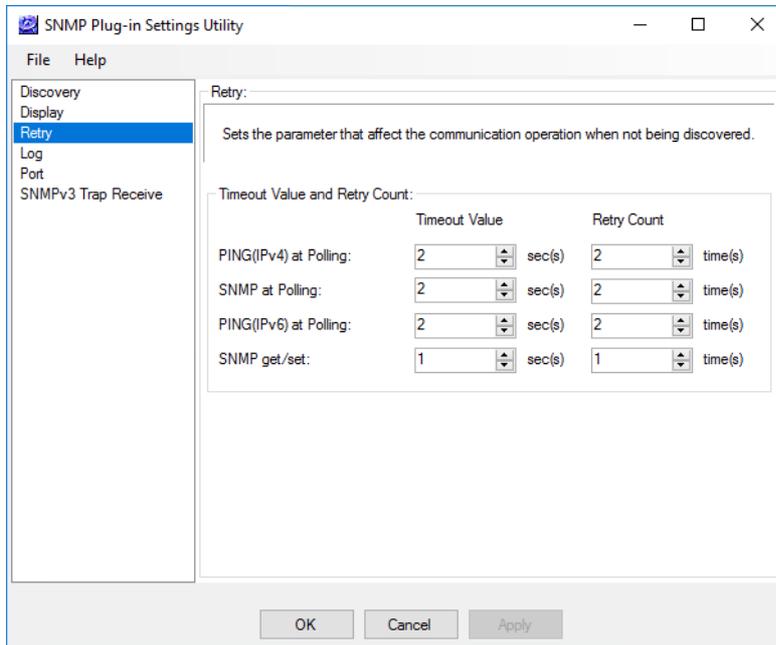


Specify the types of interfaces (ifTypes) displayed as "ports" on the tree or main view. During automatic discovery, only ports with ifTypes specified here are recognized as ports.

If you select "Any" for ifType and click "Add", the "Enter Value" dialog will be displayed and you can add a type that is not included in the list.

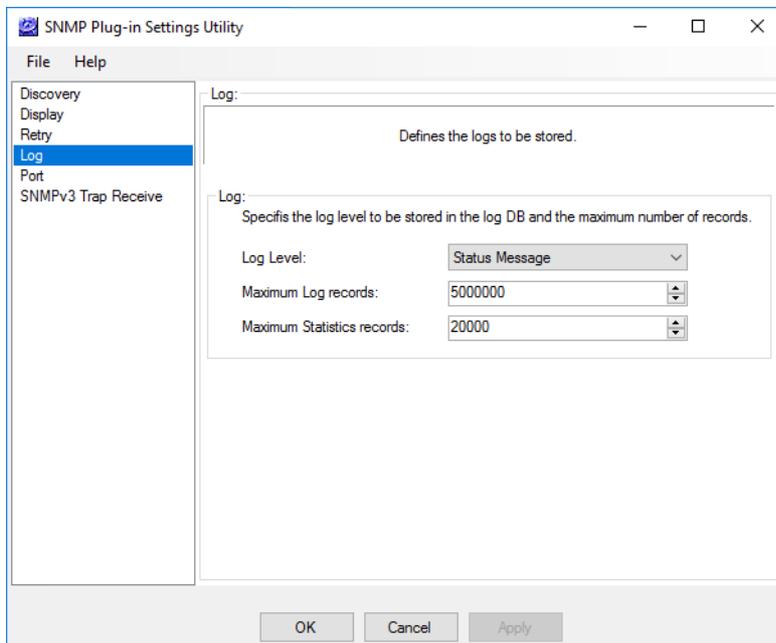
If both ifName and ifDescr are specified as the display name then ifName takes precedence. If ifName cannot be found then ifDescr will be displayed.

Retry Settings



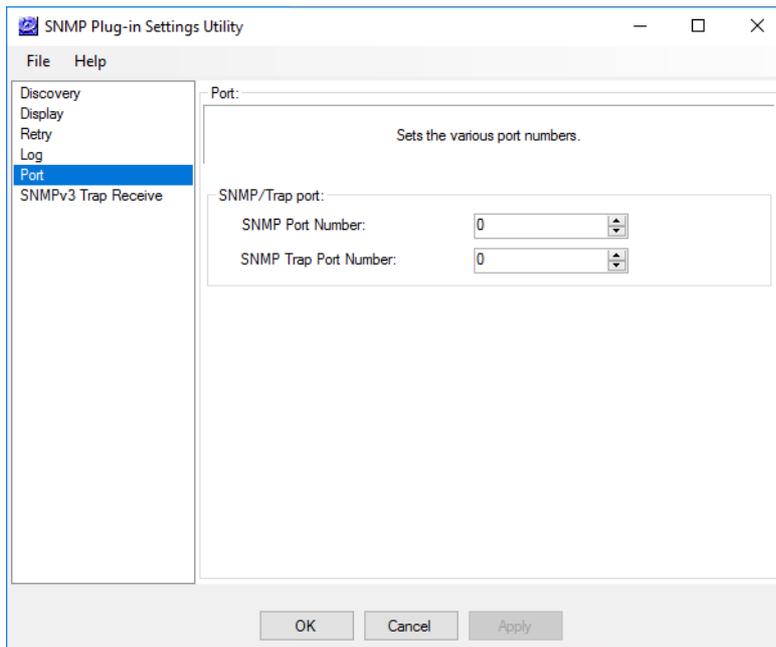
Set the Timeout Value and Retry Count for the polling protocols used by the SNMP plug-in.

Log Settings



Specify the log level for the log history database. There are three types of log levels (default is "Status Message"). This value also determines the log level displayed in the viewer.

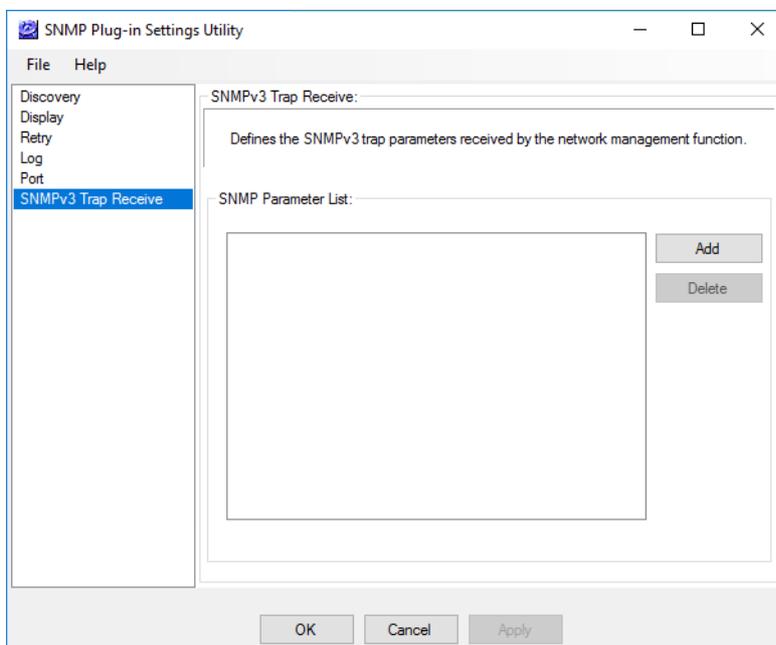
Port Settings



Specify the port numbers used for SNMP. A value of 0 uses the defaults: SNMP port (161) and SNMP trap port (162).

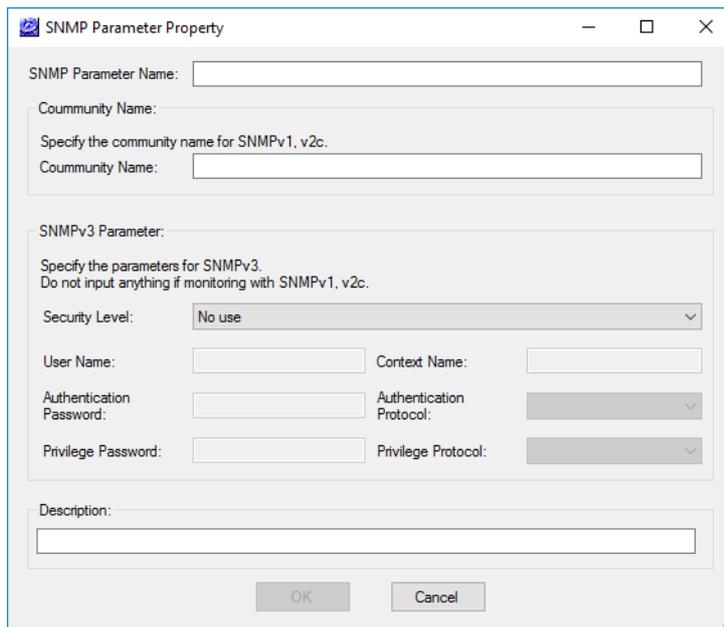
Restart the SNMP plug-in to apply these changes.

SNMPv3 Trap Reception Settings



The parameters in the list will receive SNMPv3 traps. Click on the Add button to see a list of available SNMP parameters. These are the same list of parameters you can use and edit through the web interface.

From the SNMP parameter list screen you have the option to edit or create new SNMP parameters.



The image shows a dialog box titled "SNMP Parameter Property". It contains several input fields and dropdown menus for configuring SNMP parameters. The fields are organized into sections: "SNMP Parameter Name", "Community Name", "SNMPv3 Parameter", and "Description".

SNMP Parameter Name: [Text input field]

Community Name: [Text input field]
Specify the community name for SNMPv1, v2c.

SNMPv3 Parameter:
Specify the parameters for SNMPv3.
Do not input anything if monitoring with SNMPv1, v2c.

Security Level: [Dropdown menu: No use]

User Name: [Text input field] **Context Name:** [Text input field]

Authentication Password: [Text input field] **Authentication Protocol:** [Dropdown menu]

Privilege Password: [Text input field] **Privilege Protocol:** [Dropdown menu]

Description: [Text input field]

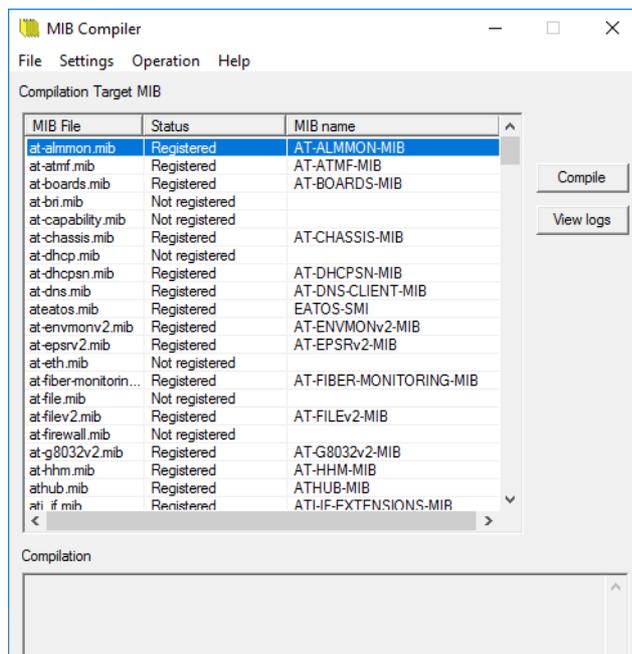
Buttons: [OK] [Cancel]

Restart the SNMP plug-in to apply any changes to the SNMPv3 trap reception settings.

MIB Compiler

The MIB compiler is a utility that converts a MIB file into a format that can be used by the built-in MIB browser. By compiling MIB files with this utility you can browse not only the standard MIBs but also any private MIBs you wish to add. Start the utility by right-clicking on the following executable and choosing to run as an administrator:

<Vista Install Path>\Plugins\AT-SNMP\NetManager\bin\SwimMibc.exe



At startup this displays the contents of the **mibfiles** folder. "Registered" indicates that the MIB has already been compiled and is ready for use by the SNMP plug-in's built-in MIB browser. "Not registered" indicates that it is not compiled and can not be used from the MIB browser.

To compile a MIB file:

1. Select "File" -> "Select a target".
2. Select the MIB file you want to compile (it is possible to select multiple files). Note that ".mib" is the only file extension the dialog recognizes.
3. Click on the "Compile" button.
4. If successful the MIB is compiled and added to the SNMP plug-in's database.

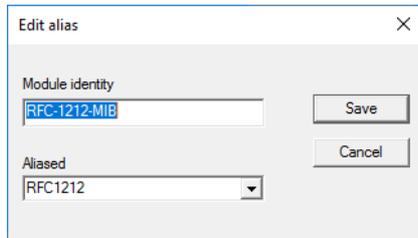
The settings menu has the following 2 advanced utilities:

- MIB file load order
- MIB file aliases

The load order utility is used change the load order of the MIB files. This is useful if a MIB object definition is duplicated. By definition, if a MIB object is duplicated, then the first one loaded becomes valid. In the situation where an object is defined in MIB "A" and then extended and

redefined in MIB “B”, unless MIB “B” is set to be read first then the old definition in MIB “A” will be used.

Define an **alias** for a registered MIB if compilation fails due to a difference in MIB names. In the example below, MIB “RFC1212” is given the fictitious name “RFC-1212-MIB”. At compile time any references to “RFC-1212-MIB” are replaced by the referenced name “RFC1212” and processed.

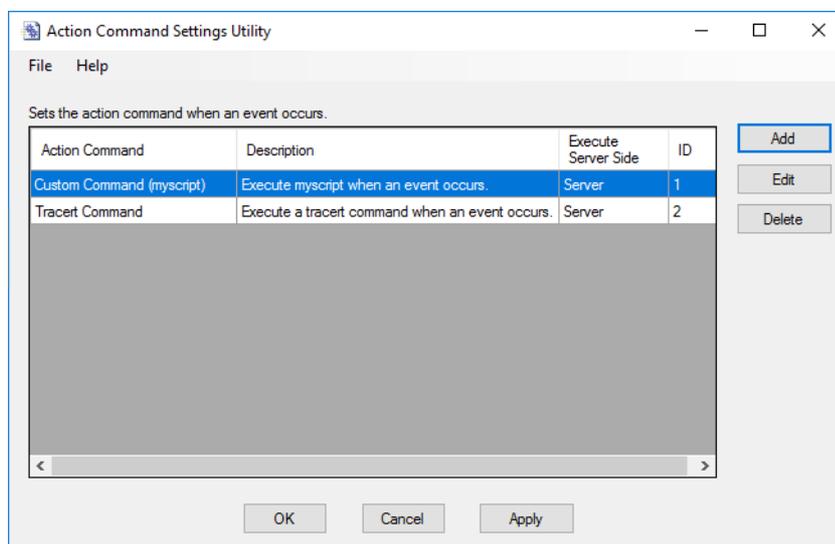


The image shows a dialog box titled "Edit alias" with a close button (X) in the top right corner. It contains two input fields and two buttons. The first field, labeled "Module identity", is a text box containing the text "RFC-1212-MIB". The second field, labeled "Aliased", is a dropdown menu with "RFC1212" selected. To the right of the "Module identity" field is a "Save" button, and below it is a "Cancel" button.

Action Command Settings Utility

You use the action command settings utility to define the action to execute when an event occurs. Start it by right-clicking on the following executable and choosing to run as an administrator:

<Vista Install Path>\Plugins\AT-SNMP\NetManager\bin32\ANMAActionConfig.exe



You can select from a predefined list of action commands or specify your own custom command. You must specify the full path to any custom commands you want to run.

See "[Event Filter Settings Utility](#)" on page 21 for information on attaching these actions to events.

Mail transmission parameters

This uses the mail client "minimail", installed with the SNMP plug-in. Minimail is a simple mail sending client that can send, but not receive, email. It also has limited error checking features so we recommend that you test the parameters on the command line (see "[Minimail utility](#)" on page 20).

format: <server name> <options>

Table 1: Mail transmission parameters

FIELD NAME	DESCRIPTION
server name	Mail server name (required).
-from xxx	Sender's email address.
-to xxx [, yyy]	Destination mail address/es (required). Separate multiple destinations with a comma.
-cc xxx [, yyy]	Carbon copy mail address/es. Separate multiple destinations with a comma.
-bcc xxx	Blind carbon copy mail address/es. Separate multiple destinations with a comma.
-replyto xxx	Reply mail address.

Table 1: Mail transmission parameters

FIELD NAME	DESCRIPTION
-subject xxx	Mail title.
-mailbody xxx \n yyy	Mail body content. ^[1] '\n' is used to indicate a new line.
-mailfile xxx	Mail body obtained from file. ^[1]
-attach xxx	Attachment
encode xxx	Encoding format (Base64 or UUENCODE).

Notes:

^[1] One of either the -mailbody or -mailfile option is required.

Tracert parameters

format: <options> IP address

Table 2: Tracert parameters

FIELD NAME	DESCRIPTION
-Queries	Number of times to execute.
-ImmediateEnd	If specified then terminate immediately if there is no response to a ping on the route.
-TimeOut	Ping timeout (seconds).
-RetryCount	Ping retry count (times).
-TTL	Time to live or hop limit (times).
-Interval	Ping interval (milliseconds).
-MaxHop	Maximum number of hops (times)
-DataSize	ICMP data size (bytes).
-Mask	Subnet mask (not supported).

Special variables

The following special variables can be used as parameters.

Table 3: Special variables

FIELD NAME	DESCRIPTION
%name	Name of log event originator (such as node name).
%adr	Address. If there is both an IP address and a MAC address, the IP address is used.
%ip	IP address. If IPv4 and IPv6 addresses are specified for the target device node, the IPv4 address takes precedence.
%ipv4	IPv4 address.
%ipv6	IPv6 address.
%mac	MAC address. The priority order when IPv4, IPv6, and MAC address are specified for the node is: IPv4 -> IPv6 -> MAC address.

Table 3: Special variables

FIELD NAME	DESCRIPTION
%msg	Message (log event details).
%type	Log type.
%subt	Event.
%level	Log level.
%time	Date and time when the log event occurred.
%aid	Action command ID number.

Minimail utility

Minimail is a simple mail sending client included with the SNMP plug-in. You can use it to send a notification to any mail address when an SNMP trap occurs. If you configure a mail action in the **Action Command Settings Utility** minimail is used. You can also run minimail from the command line. This is useful for testing your mail action parameters.

<Vista Install Path>\Plugins\AT-SNMP\NetManager\bin\minimail.exe

format: <server name> <options>

Table 4: Mail transmission parameters

FIELD NAME	DESCRIPTION
server name	(Required) Specify the name of the SMTP server. Be sure to specify it as the first parameter.
-from addr	Specify the mail address of the mail sender (you).
-to addr [, addr ..]	(Required) Destination mail address/es (required). Separate multiple destinations with a comma.
-cc addr [, addr ..]	Carbon copy mail address/es. Separate multiple destinations with a comma.
-bcc addr [, addr ..]	Blind carbon copy mail address/es. Separate multiple destinations with a comma.
-replyto addr	Reply mail address.
-subject string	(Required) Specify the title of the mail. ^[1]
-mailbody "content"	Mail body content. ^[1] '\n' is used to indicate a new line.
-mailfile filename	Mail body obtained from file. ^[1]
-attach filename	Attachment
-encode {Base64 UUENCODE}	Encoding format (Base64 or UUENCODE).

Notes:

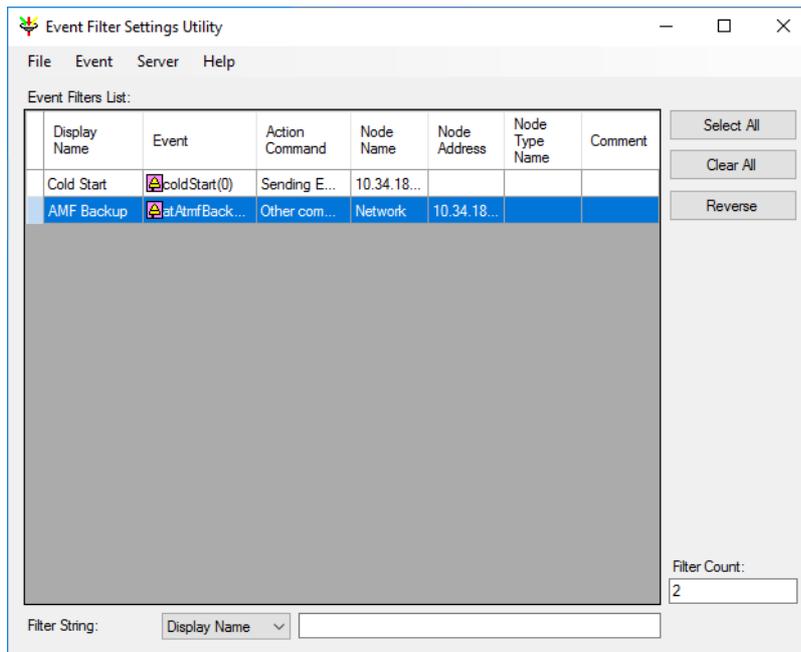
^[1] Use the same the same special variables as those defined in the Action Command Settings Utility.

Event Filter Settings Utility

Use the event filter settings utility to define the events you want to execute actions on. See "[Action Command Settings Utility](#)" on page 17 for information on creating actions to attach to events.

Start the utility by right-clicking on the following executable and choosing to run as an administrator:

<Vista Install Path>\Plugins\AT-SNMP\NetManager\bin32\ANMFilterConfig.exe



The three buttons on the left-hand side of the screen allow you to select all event filters, deselect all event filters, or reverse (flip) your event filter selection. The filter drop-down and field allow you to filter the event filters based on various criteria. The filter count shows the number of filters set on the network.

Events Filter Settings Utility menu options:

■ File Menu

- **Open:** Load an existing event filters file.
- **Save As:** Save the event filters to disk.
- **Exit:** Close the utility.

Load or save event filters to a file on disk.

■ Event Menu

- **New:** Create a new event filter.
- **Edit:** Edit the selected event filter.
- **Delete:** Delete the selected event filter.

Create, edit or delete event filters. See below for an explanation of the create/edit options.

- **Server**

- **Backup filters from the server:** Retrieve filters stored on the SNMP server.
- **Restore filters to the server:** Save event filters to the SNMP server.

These options fetch and save event filters to the SNMP plug-in server. The SNMP plug-in server must be running to use these options. Retrieving from server will overwrite any event filters set in the Event Filter Setting Utility while saving to the server will overwrite any event filters configured on the server.

- **Help**

- **View help:** Not implemented.
- **About Event Filter Settings Utility:** About dialog.

Create/Edit Event Filters dialog

The 'Edit Event Filters' dialog box contains the following fields and controls:

- Display Name:** Text box containing 'AMF Backup'.
- Type of Event:** Radio buttons for 'Trap' (selected), 'Information', 'Error', and 'Alarm'.
- Event:** Text box containing 'atAtmfBackupStatusTrap(0)' and a 'Browse' button.
- Target Node:** Section with three sub-sections:
 - Name:** Table with columns 'Name', 'Device', and 'Subnet'. Below it is a 'Browse(1)' button.
 - Address:** List box containing '10.34.180.104', '10.34.180.107', and '10.34.180.106'. Below it is a 'Browse(2)' button.
 - Model Name:** Text box. Below it is a 'Browse(3)' button.
- ActionCommand:** Table with columns 'ActionCommand', 'Description', 'Execution Side', and 'ID'. Below it is a 'Browse(4)' button.
- Comment:** Text box.

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Filters can be set on trap, information, error, or alarm events. The various browse buttons will present you with a list of valid choices for their respective fields. Use the keyboard delete key to remove items from the field lists.

The **check boxes** on the dialog denote whether a field is editable or not. If you are creating a new event filter, or are editing a single event filter, then all fields are editable. If, however, you are editing multiple event filters then just check the field you would like to edit as this change will be applied to all selected event filters.

For example, in the screenshot below only the comment will be changed on the selected event filters:

Display Name:

Type of Event: Trap: Information: Error: Alarm:

Event:

Target Node:

Name:

Name	Device	Subnet
10.34.180.104	10.34.180.104	docnet

Address:

Address

Model Name:

Model Name

ActionCommand:

ActionCommand	Description	Execution Side	ID
Sending Email(4)	Send an email with th...	Server	4

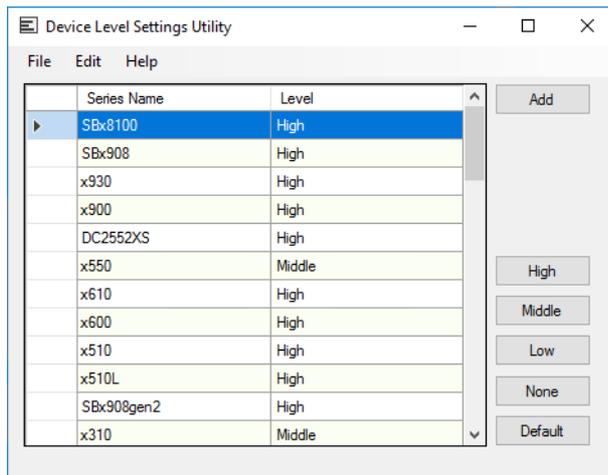
Comment:

Device Level Settings Utility

Use the device level settings utility to define a device level for each device type (series). This level is used by the SNMP plug-in to determine the monitoring cycle, data collection task cycle, and the MIB variables to base network trends on.

Start the utility by right-clicking on the following executable and choosing to run as an administrator:

<Vista Install Path>\Plugins\AT-SNMP\NetManager\bin32\DeviceLevel.exe



Series levels can be set individually, or together using multi-select. In addition, series not on the list can be added by clicking on the **Add** button and selecting a series from the list. After making changes in this utility select **File -> Save** to commit the changes to the server.

It is not possible to set the level for individual devices or for a specific model of a device in a series. Levels can only be set for all models and devices in a series.

Note: Device level changes are applied when a device is added to a subnet. If you want to make changes to existing devices remove them from the subnet and have the SNMP plug-in discover them again.

Table 5: Device level classification and monitoring cycle

Device level	Monitoring cycle	Network trend	
		Task period	MIB variable
High	1 min	10 mins	ifOutErrors
			ifInErrors
			dot1dTpHCPortInFrames (or dot1dTpPortInFrames)
			dot1dTpHCPortOutFrames (or dot1dTpPortOutFrames)
			ifHCInUcastPkts (or ifInUcastPkts)
			ifHCOUcastPkts (or ifOutUcastPkts)
			ifHCInBroadcastPkts (or ifInBroadcastPkts)
			ifHCOBroadcastPkts (or ifOutBroadcastPkts)
			ifHCInOctets (or ifInOctets)
			ifHCOOutOctets (or ifOutOctets)
Middle/ Medium	10 mins	30 mins	ifHCInUcastPkts (or ifInUcastPkts)
			ifHCOUcastPkts (or ifOutUcastPkts)
			ifHCInBroadcastPkts (or ifInBroadcastPkts)
			ifHCOBroadcastPkts (or ifOutBroadcastPkts)
			ifHCInOctets (or ifInOctets)
			ifHCOOutOctets (or ifOutOctets)
Low	20 mins	60 mins	ifHCInOctets (or ifInOctets)
None	30 mins	None	ifHCOOutOctets (or ifOutOctets)

Troubleshooting

Ports and URLs used by Vista Manager EX

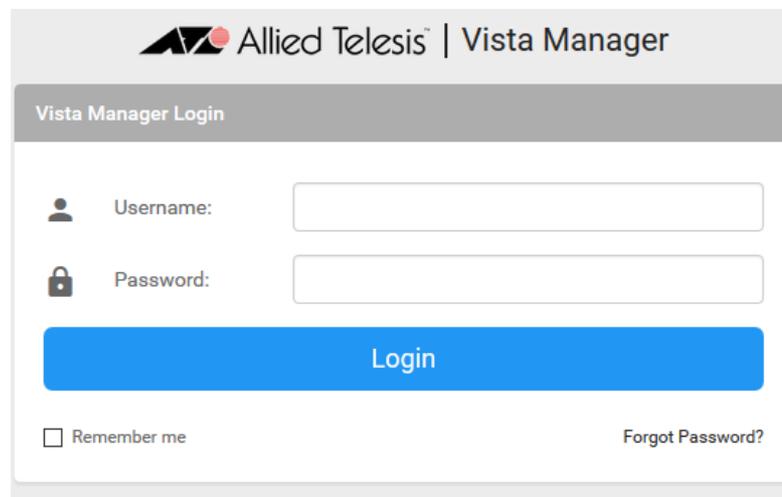
You can use these settings to check that Vista Manager and the plug-ins are installed correctly.

1. After installation, Vista Manager EX, and the plug-ins, will be installed on the following ports.

Vista Manager	Port 5000
AT-AWC	Port 5443
AT-SNMP	Port 6443

2. You can test that Vista Manager is working correctly by using the following URL:

- <http://localhost:5000>



3. You can test whether the plug-in APIs are active using the following URLs:

- https://localhost:5443/wireless_plugin/api/plugin_registration

```
{ "version": "100", "baseUrl": "http://localhost:8080/wireless_plugin/api", "product": { "name": "AT-Vista Man: plugin", "type": "awc", "version": { "major": "1", "minor": "2", "revision": "0", "build": "B06" }, "capabilities": [ "node
```

- https://localhost:6443/netmanager/api/plugin_registration

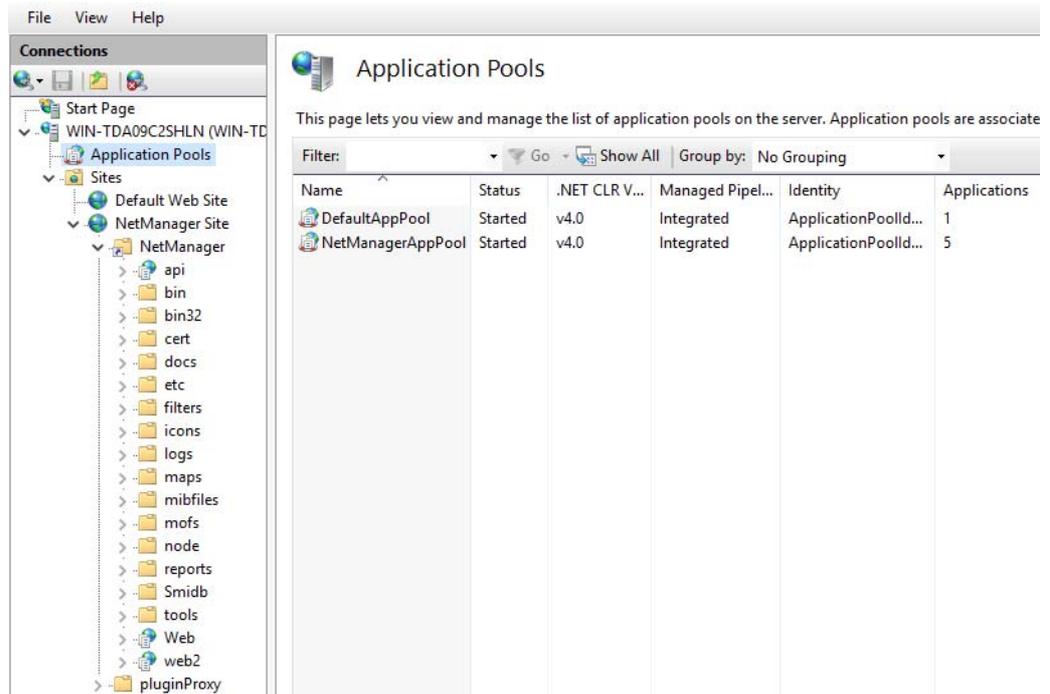
```
{ "version": "1.0.0", "baseUrl": "http://10.33.24.38/NetManager/api", "product": { "name": "SNMP Plugin", "type": "anr", {"major": "1", "minor": "0", "revision": "0", "build": "B04"}, "capabilities": [ "menu", "event" ] }
```

Note: These URLs can only be used locally on the Vista Manager server using “localhost”.

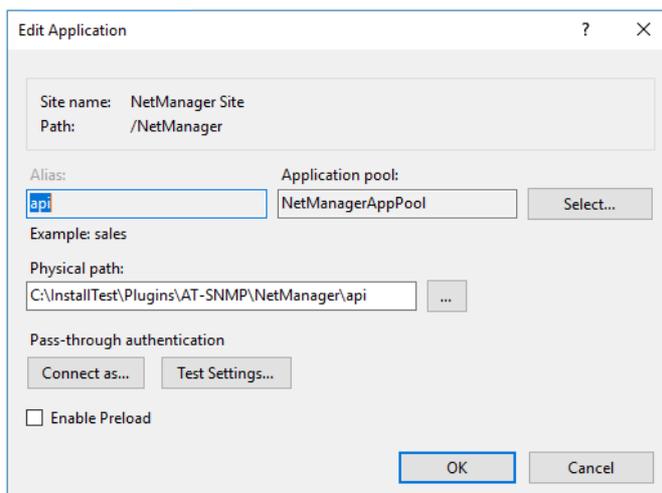
SNMP plug-in application pool settings

If you are having issues with the SNMP plug-in, you can check the IIS settings are correct.

1. Launch **Internet Information Services (IIS) Manager** on the Vista Manager EX server.
2. Expand out the following items in the Connections pane tree on the left-hand side:
Computer name -> Sites -> NetManager Site -> NetManager
3. Make sure that the **api** and **web2** applications are available, and configured, as per the following screenshots.

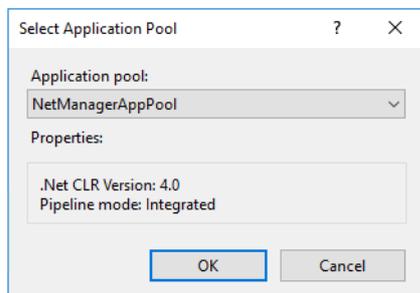


4. Select **api** in the Connections pane and then select Basic Settings in the Actions pane.



5. Click the select button and check that the Select Application Pool settings have the following properties:

- .Net CLR version: 4.0
- Pipeline mode: integration

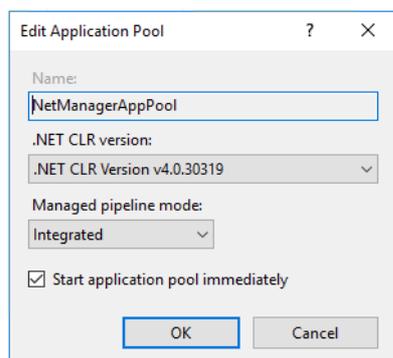


6. Repeat for the **web** application.

7. If the **NetManagerAppPool** does not have the required properties, then select Application Pool in the Connections pane.

8. Select **NetManagerAppPool** from the Application Pools screen and select Basic Settings from the Edit Application Pool pane.

9. The application pool settings should look like the following:



The “xxxxx” portion of the **.Net CLR Version v4.0.xxxxx** version will vary depending on the Windows OS installed.

Supported Device List

AlliedWare Plus devices

The following table lists the AlliedWare Plus devices supported by Vista Manager EX 3.2.0.

We recommend you run the most recent AlliedWare Plus version available for your device. The new features for version 3.2.0 are only available on devices running AlliedWare Plus version 5.4.9-2.3 or later.

Table 6: AlliedWare Plus devices supported by Vista Manager EX 3.2.0

Models	Family
AMF Cloud	
AR2050V AR2010V AR1050V	AR-series VPN routers
AR4050S AR3050S	AR-series UTM firewalls
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28DP FS980M/28PS FS980M/52 FS980M/52PS	FS980M
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX
GS970M/10 GS970M/18 GS970M/28	GS970M
GS980M/52 GS980M/52PS	GS980M
GS980EM/10GH	GS980EM
IE200-6GP IE200-6GT	IE200
IE210L-10GP IE210L-18GP	IE210L
IE340-20GP	IE340
IE340L-18GP	IE340L
IX5-28GPX	IX5
SBx81CFC400 SBx81CFC960	SBx8100
SBx908 GEN2	SBx908 GEN2
x220-28GS x220-52GP x220-52GT	x220

Table 6: AlliedWare Plus devices supported by Vista Manager EX 3.2.0

Models	Family
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230-52GP x230-52GT x230L-17GT x230L-26GT	x230
x310-26FT x310-50FT x310-26FP x310-50FP	x310
x320-10GH	x320
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510
x530-28GPXm x530-28GTXm x530-52GPXm x530-52GTXm x530L-28GPX x530L-28GTX x530L-52GPX x530L-52GTX	x530
x550-18SXQ x550-18XTQ x550-18XSPQm	x550
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930
x950-28XSQ x950-28XTQm	x950
XS916MXS XS916MXT	XS900MX

C613-04084-00 REV A (WIN)



NETWORK SMARTER

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

© 2020 Allied Telesis, Inc. All rights reserved. Information in this document is subject to change without notice. All company names, logos, and product designs that are trademarks or registered trademarks are the property of their respective owners.