Allied Telesis™

Release Note for Vista Manager EX Software Version 3.7.x

Allied Telesis | Vista Manager
building1
box78 | 172.31.0.194 | Backup Status of Master: Good
main-building
box41 | 172.31.0.36 | Backup Status of Master: Good
My Network
10.36.4.238
Network Details
24 Hour Event History
Network Map
Recent Events

VISTA MANAGER™ EX

» 3.7.0

AlliedWare Plus
OPERATING SYSTEM

Acknowledgments

Allied Telesis, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesis, Inc. has been advised of, known, or should have known, the possibility of such damages.

Getting the most from this Release Note

To get the best from this release note, we recommend using Adobe Acrobat Reader version 8 or later. You can download Acrobat free from **www.adobe.com/**

What’s New in Vista Manager EX v3.7.0

Introduction

This release note describes the new features in Vista Manager EX™ v3.7.0. It covers Vista Manager EX plus the optional Autonomous Wave Controller (AWC) and SNMP plug-ins, and Allied Intent-based Orchestrator (AIO).

You can obtain the software files from the Software Download area of the Allied Telesis website. Log in using your assigned email address and password.

Contact your authorized Allied Telesis support center to obtain licenses.

Caution: Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesis, Inc.

While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesis, Inc. can not accept any type of liability for errors in, or omissions arising from, the use of this information.

Vista Manager SNMP plug-in

Applicable to Windows-based Vista Manager installations with the SNMP plug-in.

Prior to version 3.7.0, the Windows-based version of Vista Manager supported a lowercase URL for registering the plug-in. If you are upgrading from an earlier version, or porting to a different platform, please re-register the SNMP plug-in using a mixed-case URL.

Server URL: https://<*ip-address*>:6443/NetManager
where <*ip-address*> is the IP address of the SNMP plug-in.

New Features and Enhancements

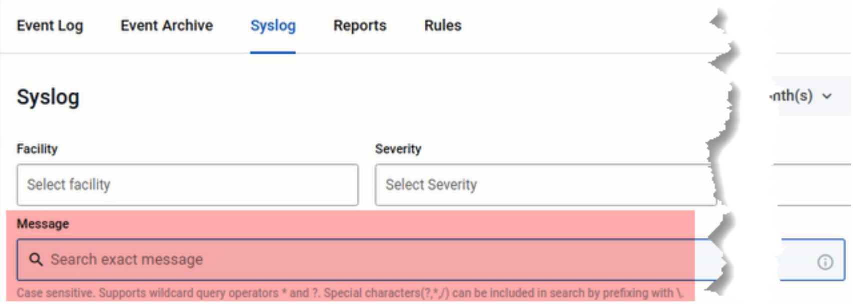
This section summarizes the new features added to Vista Manager EX v3.7.0:

Improved syslog server support

Applicable to all Vista Manager installations.

From version 3.7.0 onwards, the syslog server feature is extended to support syslog message filtering, syslog forwarding, and syslog-based rules that trigger emails or alarms. Admin users will be able to create, edit, disable, and delete rules from the rules table. Syslog rule alarms will appear on the network map and can be dismissed.

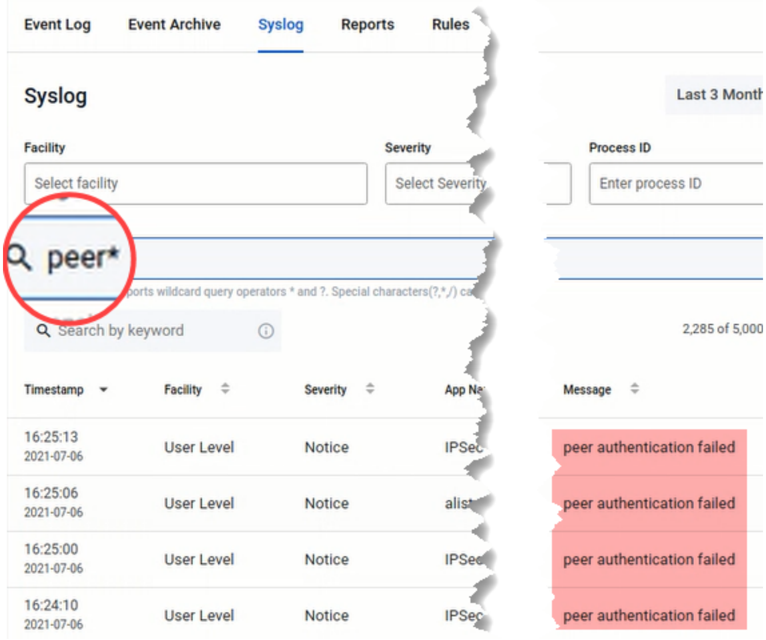
Syslog message filtering



Case sensitive. Supports wildcard query operators * and ?. Special characters(?,*,/) can be included in search by prefixing with \.

You can now filter syslog events by whole message content or partial message content, by using multiple wildcards. Details of supported wildcard query operators and special characters are as follows:

- A question mark (**?**) is used for a single character.
- An asterisk (*****) is used for multiple characters.

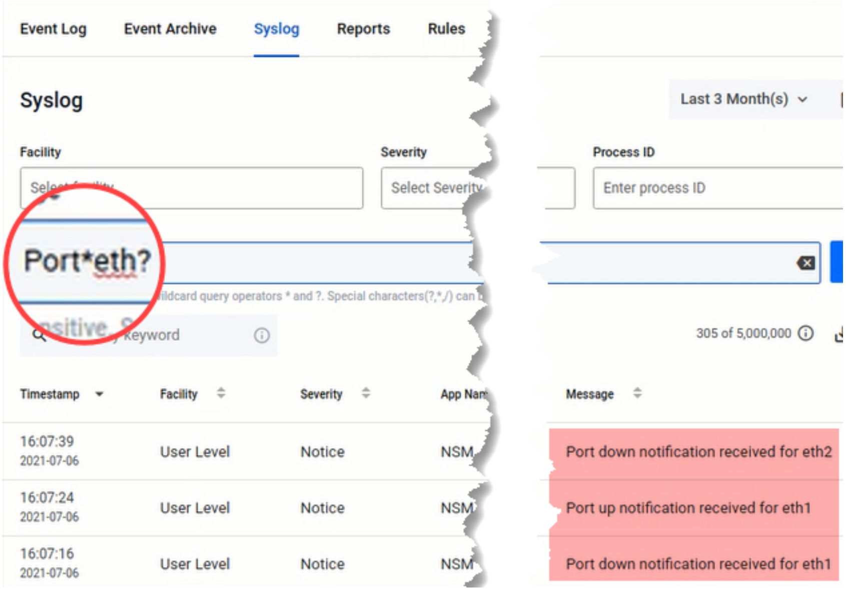


peer*

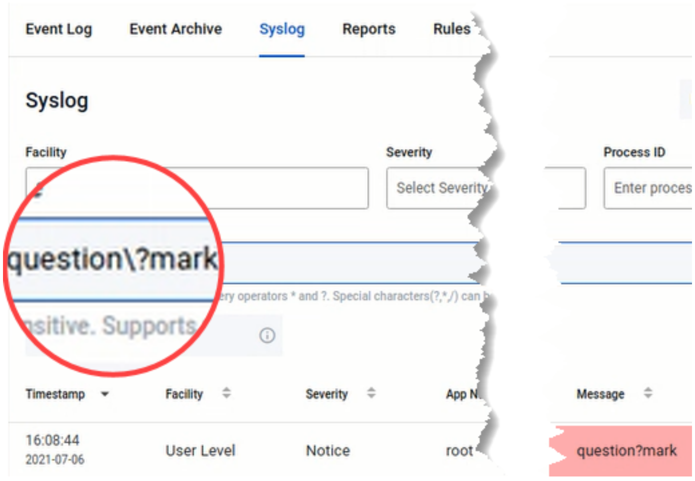
2,285 of 5,000

Timestamp	Facility	Severity	App Na	Message
16:25:13 2021-07-06	User Level	Notice	IPSec	peer authentication failed
16:25:06 2021-07-06	User Level	Notice	alist	peer authentication failed
16:25:00 2021-07-06	User Level	Notice	IPSec	peer authentication failed
16:24:10 2021-07-06	User Level	Notice	IPSec	peer authentication failed

- A backslash (\) is used to escape any special characters (**?**, *, /) after it.
- When a backslash is expected to be part of the message to be matched on, escape it with an additional (preceding) backslash.
- When an asterisk is expected to be part of the message to be matched on, escape it with a preceding backslash.



Timestamp	Facility	Severity	App Nam	Message
16:07:39 2021-07-06	User Level	Notice	NSM	Port down notification received for eth2
16:07:24 2021-07-06	User Level	Notice	NSM	Port up notification received for eth1
16:07:16 2021-07-06	User Level	Notice	NSM	Port down notification received for eth1



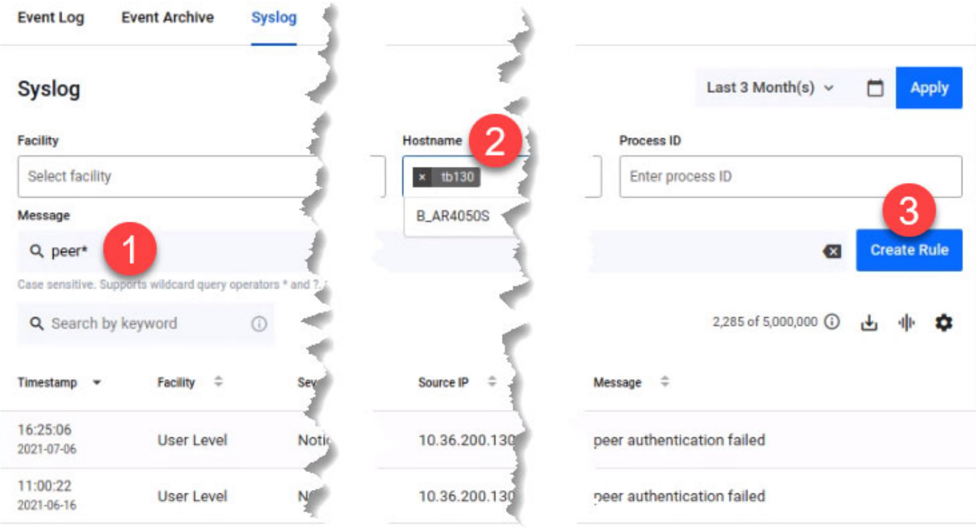
Timestamp	Facility	Severity	App N	Message
16:08:44 2021-07-06	User Level	Notice	root	question?mark

Note: This filtering functionality is case-sensitive.

Syslog rules

Syslog rules work similarly as the existing event rules. Any received syslog that matches a rule will trigger the action associated with the rule. Create a syslog rule based on the syslog message filter from the syslog tab page. When creating a single rule, configure up to two of the following actions:

- email notification
- dismissible alarm
- no action



Hostname: tb130, B_AR4050S

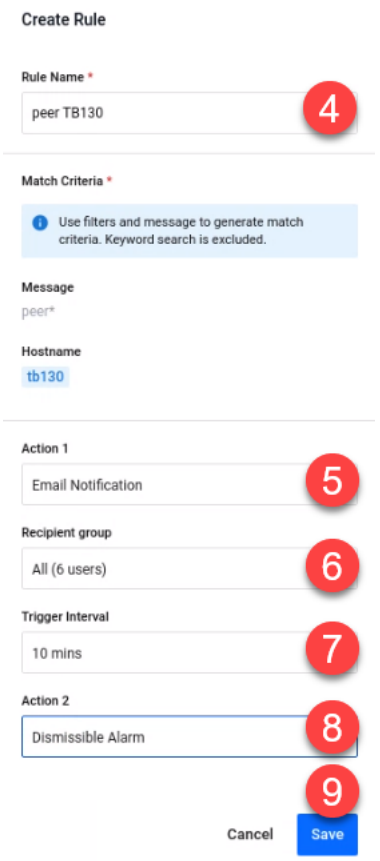
Message: peer*

Case sensitive. Supports wildcard query operators * and ?.

2,285 of 5,000,000

Timestamp	Facility	Sev	Source IP	Message
16:25:06 2021-07-06	User Level	Notic	10.36.200.130	peer authentication failed
11:00:22 2021-06-16	User Level	N	10.36.200.130	peer authentication failed

1. Use the syslog message filtering to search for messages of your choice.
2. Next, select a hostname.
3. Click **Create Rule**. This opens up the side panel.
4. Enter a rule name.
5. Configure a first action for **email notification**.
6. Select a recipient group.
7. Select a trigger interval time.
8. Configure a second action for **dismissible alarm**.
9. Click **Save**.



Create Rule

Rule Name *

peer TB130

Match Criteria *

Use filters and message to generate match criteria. Keyword search is excluded.

Message

peer*

Hostname

tb130

Action 1

Email Notification

Recipient group

All (6 users)

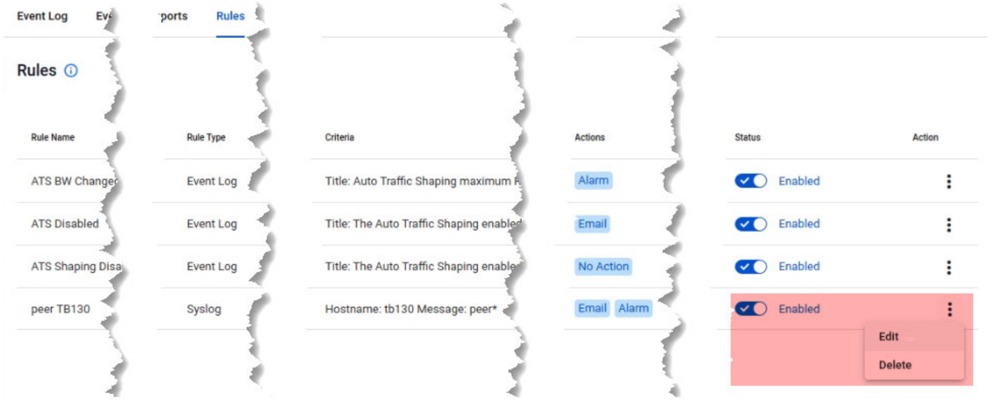
Trigger Interval

10 mins

Action 2

Dismissible Alarm

To view a list of syslog rules, navigate to the Rules tab page. Here, you can also disable a rule, update its settings, or delete it.

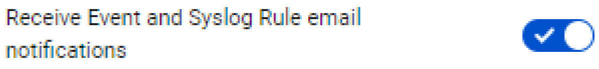


Rules

Rule Name	Rule Type	Criteria	Actions	Status	Action
ATS BW Change	Event Log	Title: Auto Traffic Shaping maximum	Alarm	Enabled	⋮
ATS Disabled	Event Log	Title: The Auto Traffic Shaping enabled	Email	Enabled	⋮
ATS Shaping Disa	Event Log	Title: The Auto Traffic Shaping enable	No Action	Enabled	⋮
peer TB130	Syslog	Hostname: tb130 Message: peer*	Email Alarm	Enabled	⋮ Edit Delete

Syslog rule - email notification

On the **user management** page, a new toggle button enabled by default will be present for all users. This setting determines whether a user will receive an email when a syslog matches a syslog rule configured with email notification.

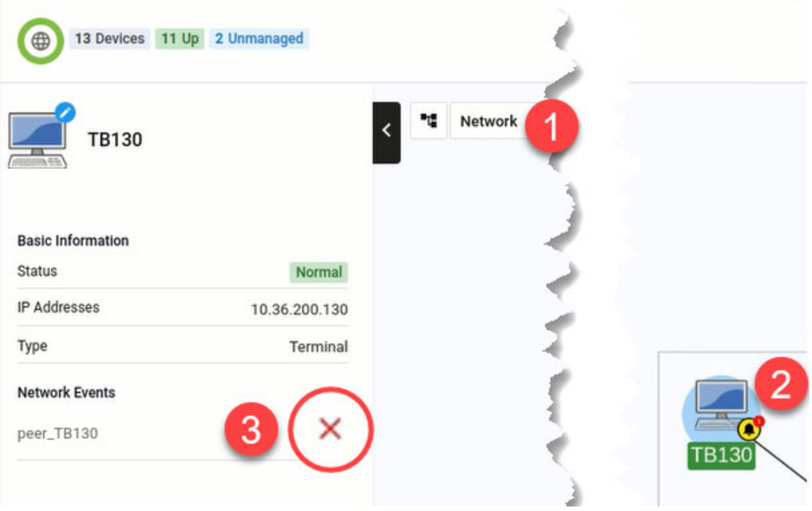


Receive Event and Syslog Rule email notifications

As a non-admin user, you can change this setting only for yourself. Admin users can enable/disable email notification for all users.

Syslog rule - dismissible alarm

A bell icon will appear on the network map for a device that sends a syslog matching a rule. Click on the bell icon to open up the side panel displaying its syslog details. Here, you may also choose to dismiss the alarm.



Basic Information

Status	Normal
IP Addresses	10.36.200.130
Type	Terminal

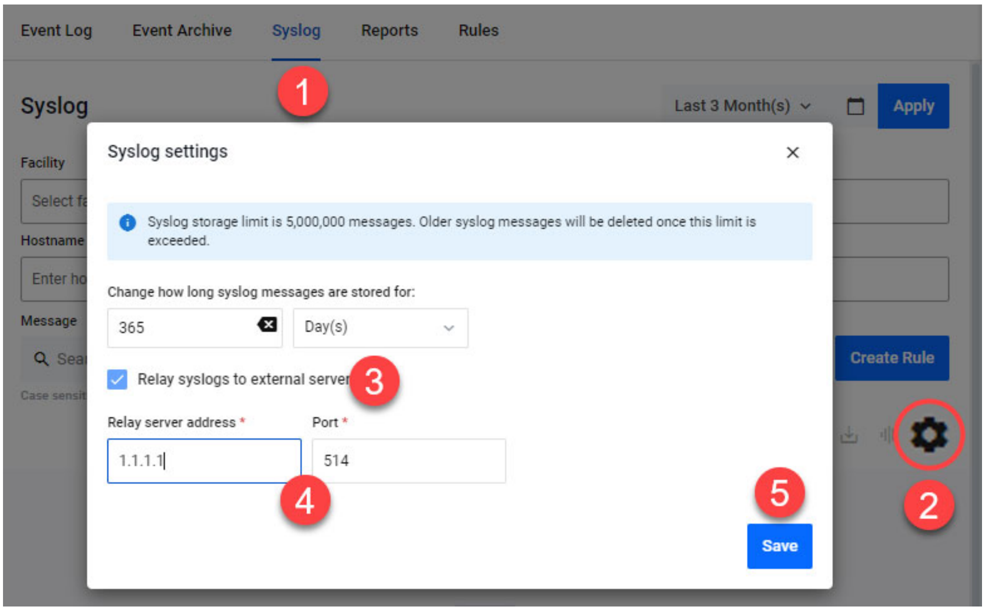
Network Events

peer_TB130

Syslog forwarding

As an admin user, you will have the option to configure syslog forwarding to an external server. This functionality forwards all received syslog messages to a specified syslog server, regardless of any rules configured. Only one external syslog server is supported.

Note: The source address of a syslog cannot be retained to its external server.



Syslog settings

Syslog storage limit is 5,000,000 messages. Older syslog messages will be deleted once this limit is exceeded.

Change how long syslog messages are stored for:

365 Day(s)

☑ Relay syslogs to external server

Relay server address *: 1.1.1.1

Port *: 514

Save

1. From the Events menu, navigate to the **Syslog** tab page.

2. Click on the Syslog settings gear icon.

3. Check the **Relay syslogs to external server** option.

4. Enter the relay server address and port number.

5. Click **Save**.

AMF Security (AMF-Sec) support

Applicable to all Vista Manager installations.

From version 3.7.0 onwards, the existing alarm notification will be extended to support both AlliedWare Plus devices and wireless devices by leveraging on syslog messages from the AMF Security (AMF-Sec) server.

Previously, Vista Manager EX only shows alarms on the integrated map for blacklist security events on AlliedWare Plus devices. This feature now covers both blacklist and whitelist security events.

For the feature to be fully functional, configure all your AMF-Sec servers to send syslog messages to Vista Manager EX. All syslog messages from the AMF-Sec servers will then appear on the **Event > Syslog** page.

Note: In order to process syslog messages from the AMF-Sec server, Vista Manager EX will have some built-in event rules not visible to users. Because of this, if a user creates a rule with the same name in the event log or syslog table, an error message will display: “**Duplicate rule name used. Note may be a duplicate of a hidden system rule name.**”

Alarms on the integrated map

Vista Manager EX will convert only specific actions that match AMF-Sec syslog messages into alarms (high severity event logs) and display them on the map. These specific actions are:

- Blacklist
  - Security Block
  - LinkDown
  - Quarantine VLAN
  - Security Logging (no-action, reporting only)
- Whitelist
  - Auth Failed (deny)

Any other syslog messages from the AMF-Sec server not mentioned above will not be converted. This means the user will not be able to see successful authentication events in the Vista Manager event log table, but those events are present in the Syslog tab page.

The alarms will be associated with devices based on IP addresses and hostnames from the AMF-Sec syslog message. If one AMF-Sec syslog message can be associated with multiple devices, all devices will have their own alarm. If an alarm cannot be associated with any device on the map, it will not be visible on the map.

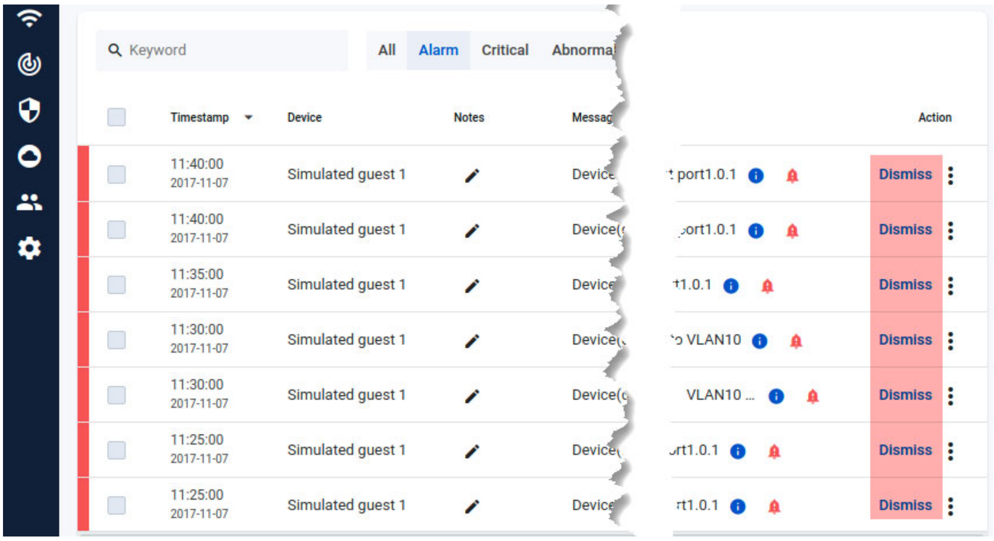
Note: Unmanaged devices are not always visible on the map, such as TQ devices without the AWC plug-in. In this case, alarms will still be associated to the TQ device, but can only be viewed by the zooming into the map. Alternatively, add the AWC plug-in to manage the TQ which then makes it visible by default.

The alarms will keep showing on the map until either

- a user dismisses them proactively, or
- a recovery AMF-Sec syslog message dismisses them automatically.

Users with read/write permissions to the associated device can dismiss the alarms in 2 ways:

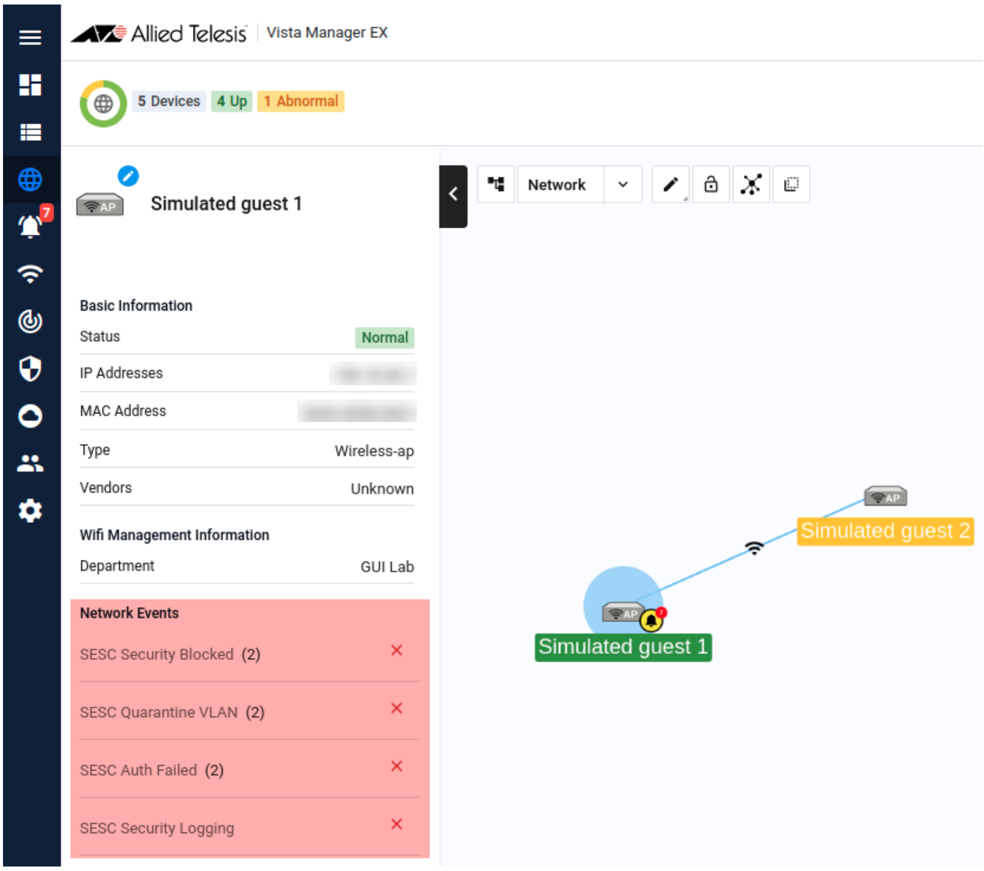
- **from the event log table**, or



Keyword | All | Alarm | Critical | Abnormal

☐	Timestamp	Device	Notes	Message	Action
☐	11:40:00 2017-11-07	Simulated guest 1	✎	Device … t port1.0.1	Dismiss
☐	11:40:00 2017-11-07	Simulated guest 1	✎	Device(… port1.0.1	Dismiss
☐	11:35:00 2017-11-07	Simulated guest 1	✎	Device … t1.0.1	Dismiss
☐	11:30:00 2017-11-07	Simulated guest 1	✎	Device(… o VLAN10	Dismiss
☐	11:30:00 2017-11-07	Simulated guest 1	✎	Device(… VLAN10 ...	Dismiss
☐	11:25:00 2017-11-07	Simulated guest 1	✎	Device(… rt1.0.1	Dismiss
☐	11:25:00 2017-11-07	Simulated guest 1	✎	Device … rt1.0.1	Dismiss

- **from the side panel of the map**.



Allied Telesis | Vista Manager EX

5 Devices 4 Up 1 Abnormal

Simulated guest 1

Basic Information

Status: Normal

IP Addresses: [redacted]

MAC Address: [redacted]

Type: Wireless-ap

Vendors: Unknown

Wifi Management Information

Department: GUI Lab

Network Events

SESC Security Blocked (2) ×

SESC Quarantine VLAN (2) ×

SESC Auth Failed (2) ×

SESC Security Logging ×

Alarm recovery

When a user performs an action in the AMF-Sec server, the AMF-Sec server will send syslog messages to Vista Manager EX to indicate a status change on the alarm.

Vista Manager EX automatically dismisses an alarm and removes it from the map, if they are event recovery types such as:

- DISCONNECT
- ACCEPT

A "recovered" event log will then be generated with detailed information.

Feature limitations

There are some feature limitations to take note of:

- As syslog messages are based on UDP protocol, this functionality can be unreliable at times, meaning messages could sometimes go missing.
- In the event that the Vista Manager EX syslog server goes down, syslog messages lost during the downtime will not be recoverable.
- If the AMF-Sec server changes its syslog format, this feature will fail to work as there is no way to detect such failures.
- AMF-Sec alarms that depend on the DISCONNECT action will not be removed when the parent device reboots or leaves the network. This is because the AMF-Sec server does not send a corresponding disconnect message with a device reboot, therefore causing the alarms to remain on the map.
- AMF-Sec will not send syslog messages for the IP-FILTER action. If sourced from a non-AMF device, Vista Manager EX will not be able to detect this action.
- Some changes have been applied to the event messages from the original blacklist feature. Therefore for any event filtering relying on event messages, the existing event filter may appear broken after upgrading to version 3.7.0.

DPI learning and application sharing support

Applicable to all Vista Manager installations with the AIO license.

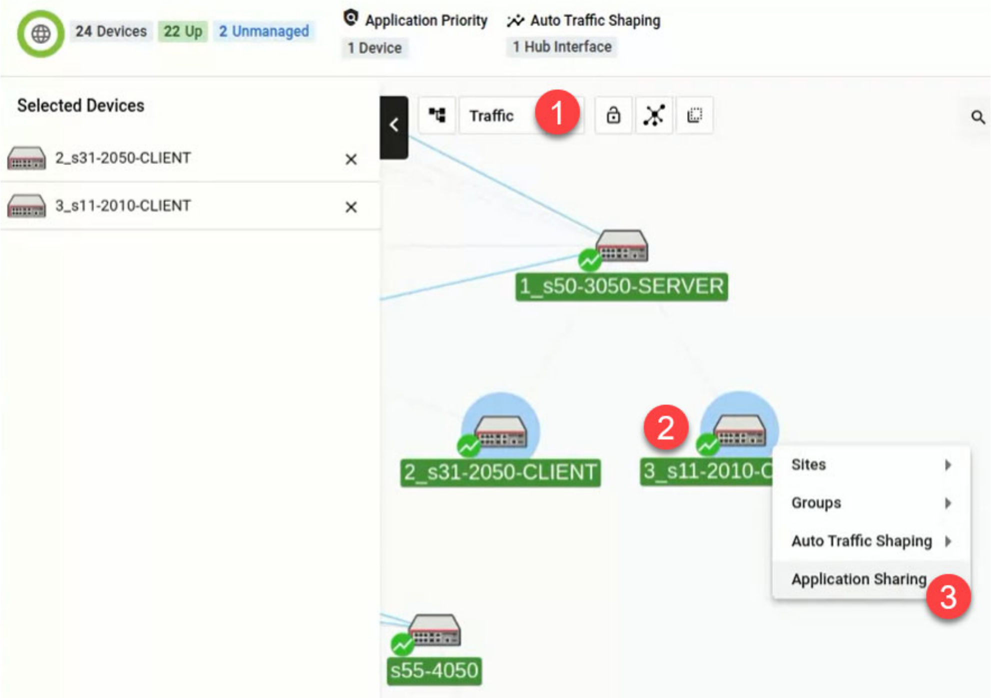
From Vista Manager EX version 3.7.0 onwards, DPI learning and application sharing will allow branch office routers (clients) to gain access to applications on a head office router (server). Applications learned on the servers can be distributed to the clients, thus allowing features like Internet Breakout to be enabled on a client.

- **AR3050S** and **AR4050S** can be used as server devices that have advanced DPI engines available. This means that they can share their applications with other devices.
- **AR2010V** and **AR2050V** can be client devices. They will use a server device to send them the application data.
- This functionality requires AR-series devices to run AlliedWare Plus 5.5.1-1 or later.

Configure application sharing via 3 options:

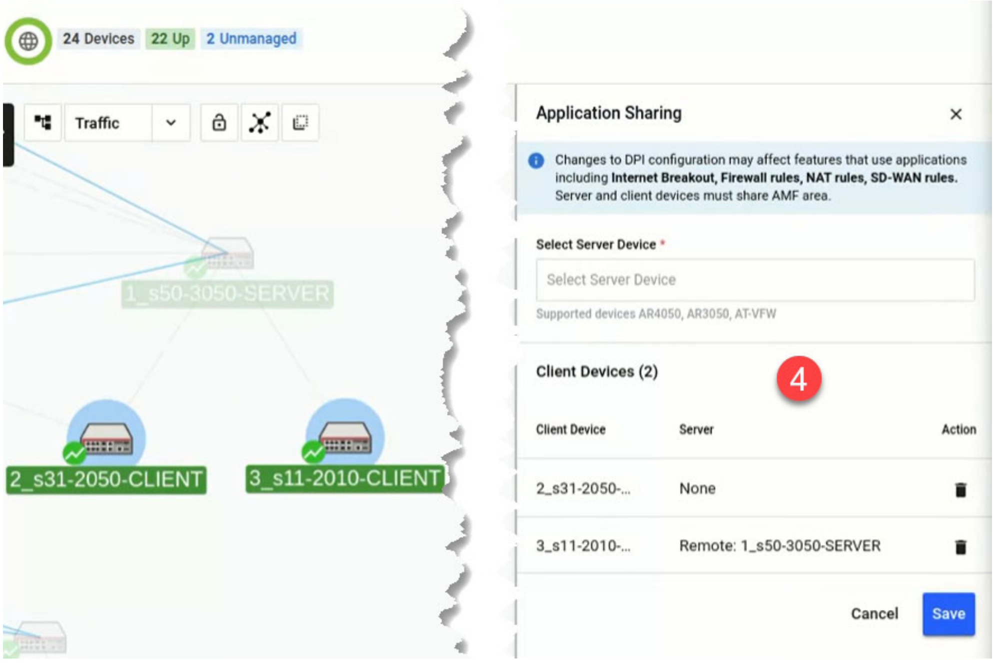
- Traffic map context menu
- Traffic side panel
- Asset Management > Applications tab of individual devices

Option 1: via Traffic map context menu



1. Navigate to the traffic map.
2. Select at least one client router.
3. Right-click on the selected router(s) and select **Application Sharing** from the menu.

4. This opens up the Application Sharing side panel. You may remove or add more client devices here.



Application Sharing

Changes to DPI configuration may affect features that use applications including **Internet Breakout, Firewall rules, NAT rules, SD-WAN rules.** Server and client devices must share AMF area.

Select Server Device *

Select Server Device

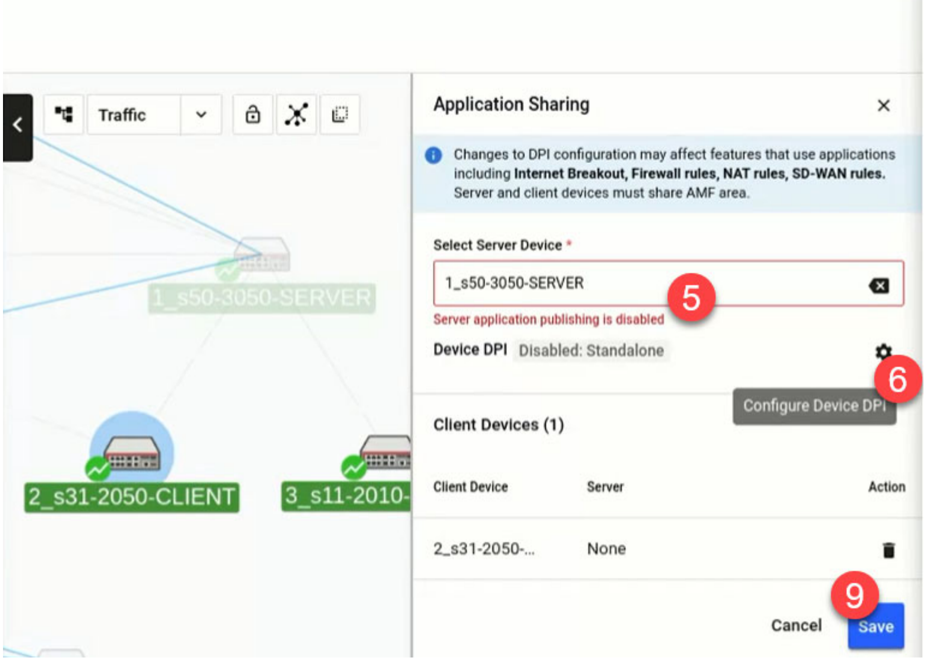
Supported devices AR4050, AR3050, AT-VFW

Client Devices (2)

Client Device	Server	Action
2_s31-2050-...	None	🗑
3_s11-2010-...	Remote: 1_s50-3050-SERVER	🗑

Cancel Save

5. Next, select a server device from the dropdown list. Take note of the current DPI state of the server.



Application Sharing

Changes to DPI configuration may affect features that use applications including **Internet Breakout, Firewall rules, NAT rules, SD-WAN rules.** Server and client devices must share AMF area.

Select Server Device *

1_s50-3050-SERVER

Server application publishing is disabled

Device DPI Disabled: Standalone

Client Devices (1)

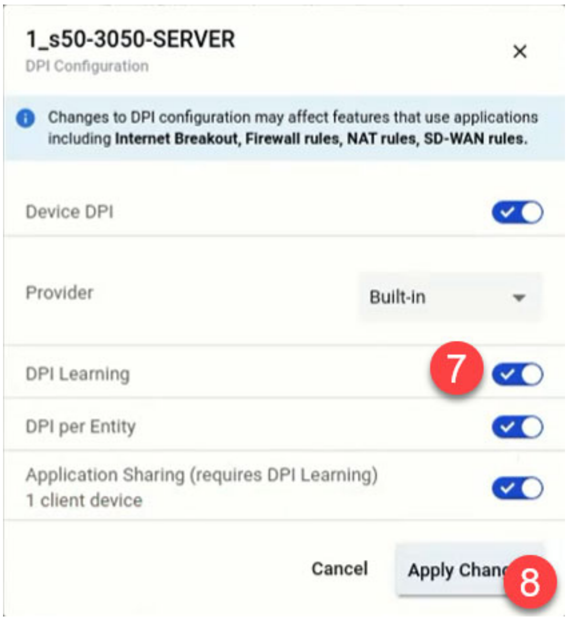
Client Device	Server	Action
2_s31-2050-...	None	🗑

Cancel Save

6. Click on the **Configure Device DPI** gear icon button if device DPI is disabled or to configure its settings.

7. Turn on all settings to ensure a successful application sharing setup.

8. Click **Apply Changes.**



1_s50-3050-SERVER

DPI Configuration

Changes to DPI configuration may affect features that use applications including **Internet Breakout, Firewall rules, NAT rules, SD-WAN rules.**

Device DPI ✓

Provider: Built-in

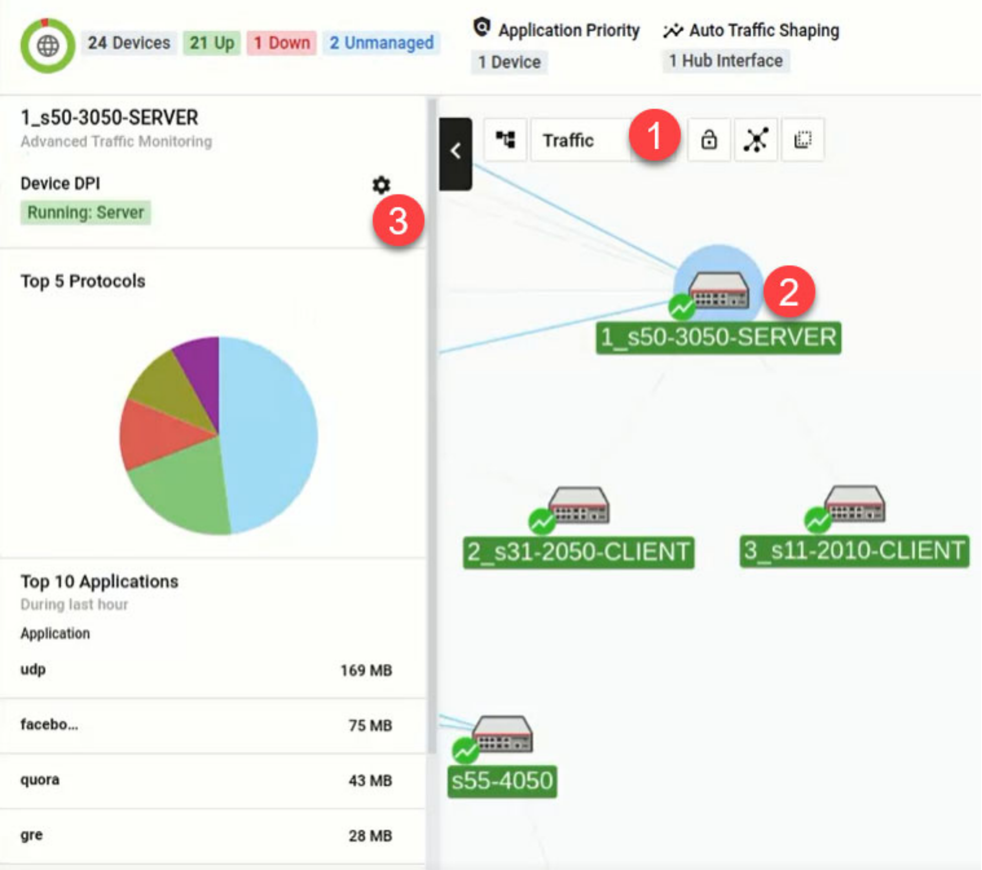
DPI Learning ✓

DPI per Entity ✓

Application Sharing (requires DPI Learning) ✓
1 client device

9. Finally, click **Save** on the side panel.

Option 2: via Traffic side panel



1_s50-3050-SERVER

Advanced Traffic Monitoring

Device DPI

Running: Server

Top 10 Applications

During last hour

Application	
udp	169 MB
facebo...	75 MB
quora	43 MB
gre	28 MB

1. Navigate to the traffic map.

2. Select a supported server/client device. This opens up the Traffic side panel.

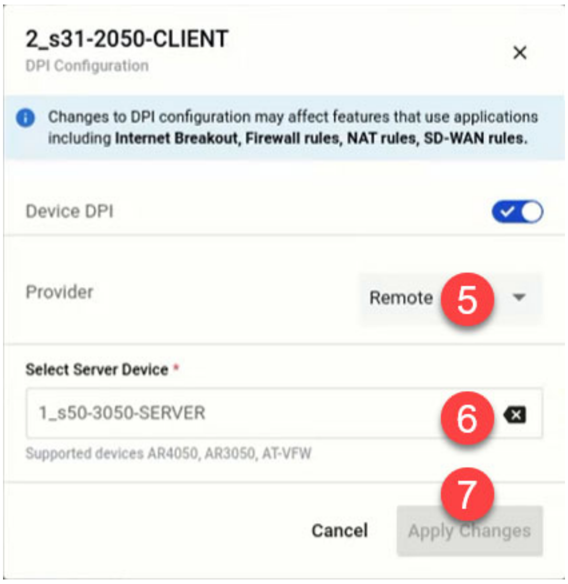
3. Click on the **Device DPI** gear icon button if device DPI is disabled or to configure its settings.

4. If a server device was selected, carry out **Steps 7-8 in Option 1**.

5. If a client device was selected, fewer DPI settings will be displayed. Select a **Remote** provider to choose a server next.

6. Select a server from the dropdown list.

7. Click **Apply Changes**.



2_s31-2050-CLIENT

DPI Configuration

Changes to DPI configuration may affect features that use applications including **Internet Breakout, Firewall rules, NAT rules, SD-WAN rules.**

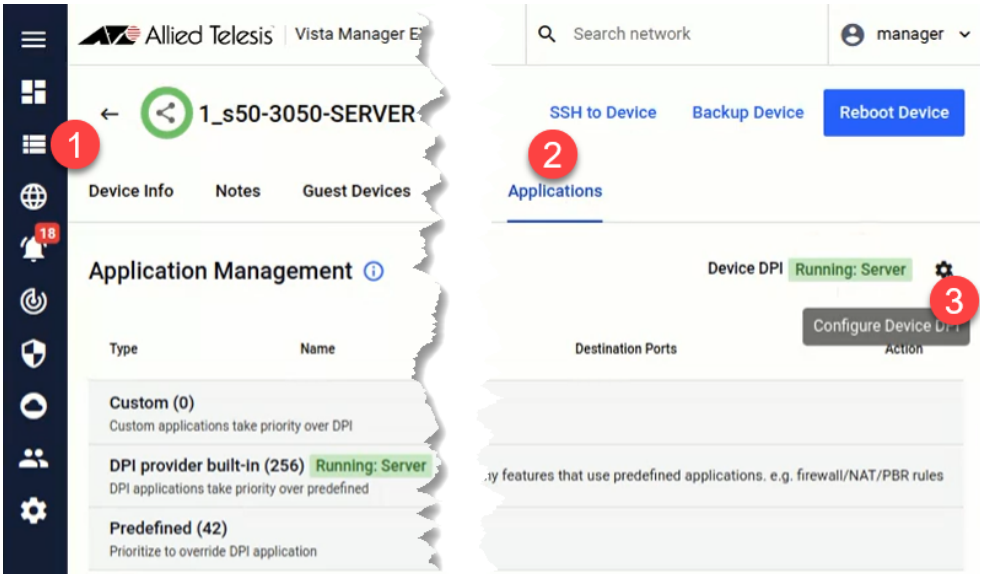
Device DPI: ☑

Provider: Remote

Select Server Device *: 1_s50-3050-SERVER

Supported devices AR4050, AR3050, AT-VFW

Option 3: via Asset Management > Applications tab



Custom (0)
Custom applications take priority over DPI

DPI provider built-in (256) Running: Server
DPI applications take priority over predefined

Predefined (42)
Prioritize to override DPI application

..y features that use predefined applications, e.g. firewall/NAT/PBR rules

1. Navigate to **Asset Management**. Select a supported device from the list.

2. Next, go to the **Applications** tab of that device.

3. Click on the **Configure Device DPI** gear icon button if device DPI is disabled or to configure its settings.

4. If a server device was selected, carry out **Steps 7-8 in Option 1**.

5. If a client device was selected, fewer DPI settings will be displayed. Carry out **Steps 5-7 in Option 2**.

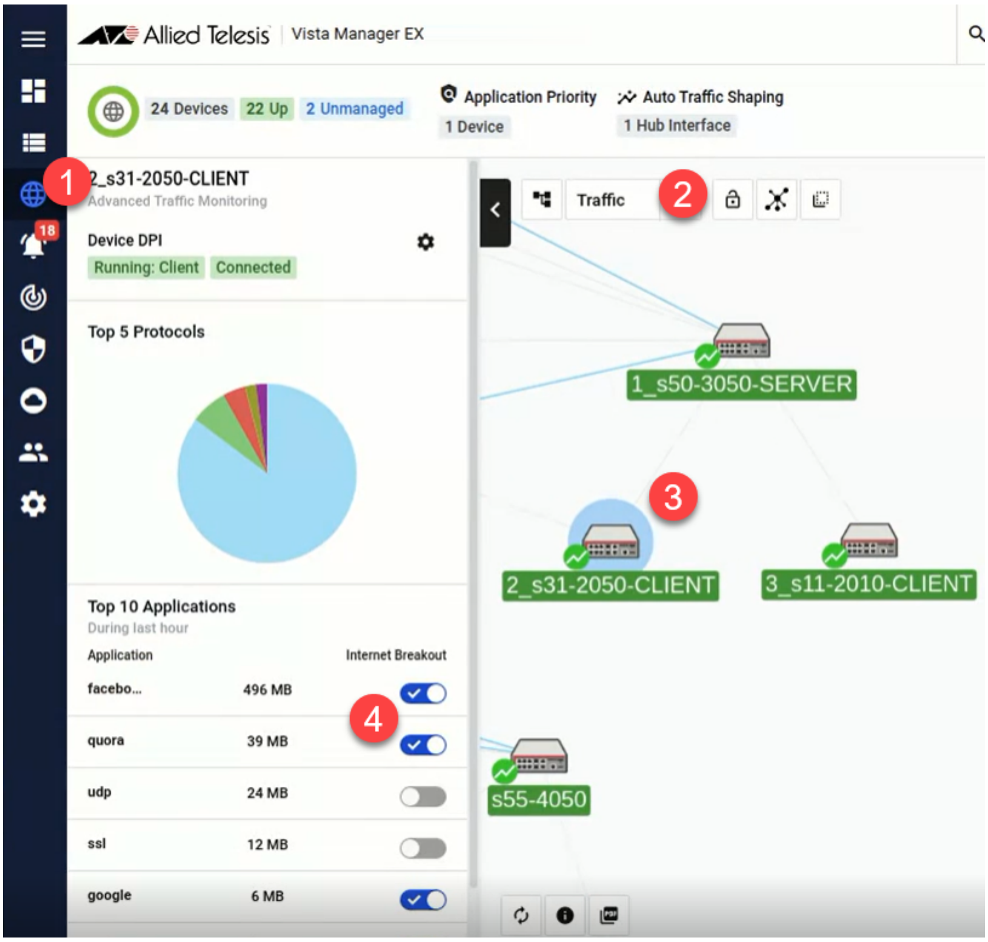
With DPI learning and application sharing configured and running successfully, you can then enable Internet Breakout for specific applications on clients from the Traffic side panel. Here, you can also see what applications have been learned from the server.

1. Navigate to the network map.

2. Select traffic map mode.

3. Select a client device that you wish to enable Internet Breakout for.

4. On the Traffic side panel that launches, enable Internet Breakout accordingly.



2_s31-2050-CLIENT
Advanced Traffic Monitoring

Device DPI
Running: Client | Connected

Top 10 Applications
During last hour

Application		Internet Breakout
facebo...	496 MB	☑
quora	39 MB	☑
udp	24 MB	☐
ssl	12 MB	☐
google	6 MB	☑

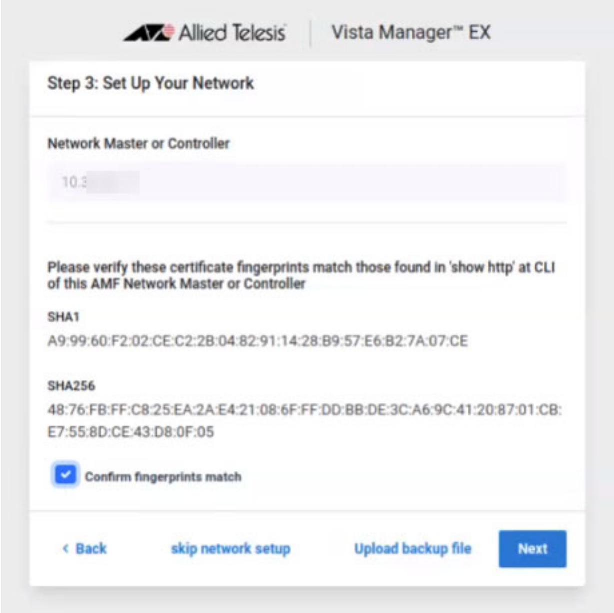
Note: Application sharing (between a server and clients) will only be functional within an AMF area. It is possible to have multiple servers in different areas, but the clients of each server must be located in the same area as the server.

Plug-in certificate fingerprint verification

Applicable to all Vista Manager installations.

From Vista Manager EX version 3.7.0 onwards, when setting up or changing the network master or controller IP address, it is now a mandatory step to verify that the certificate fingerprints match those found in the **show http** command on the CLI.

Note: The master is required to have a version of AlliedWare Plus running to check the fingerprints.



Step 3: Set Up Your Network

Network Master or Controller

10.[redacted]

Please verify these certificate fingerprints match those found in 'show http' at CLI of this AMF Network Master or Controller

SHA1

A9:99:60:F2:02:CE:C2:2B:04:82:91:14:28:B9:57:E6:B2:7A:07:CE

SHA256

48:76:FB:FF:C8:25:EA:2A:E4:21:08:6F:FF:DD:BB:DE:3C:A6:9C:41:20:87:01:CB:E7:55:8D:CE:43:D8:0F:05

☑ Confirm fingerprints match

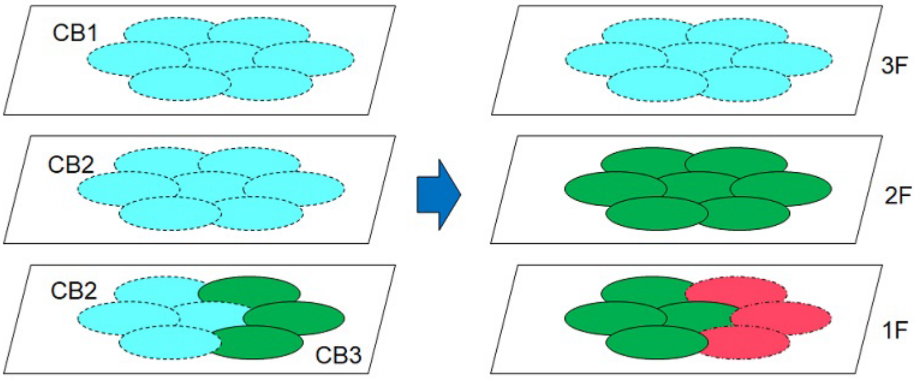
New AWC Plug-in functionalities and settings

Automatic radio optimization

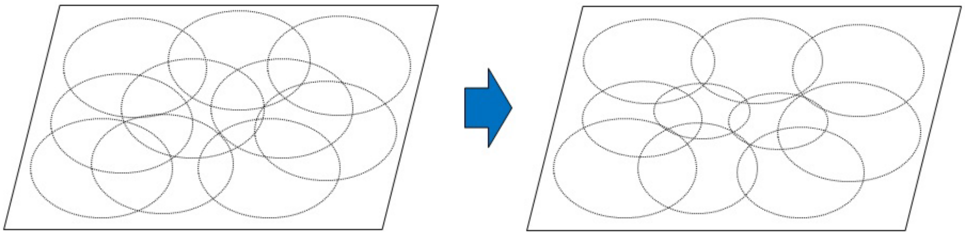
Applicable to all Vista Manager installations with the AWC plug-in

From Vista Manager EX version 3.7.0 onwards, the AWC plug-in will have a new page **Wireless Concierge** added to the wireless configuration submenu. This feature promotes channel blanket (CB) optimization by allowing users to suggest:

- **AP channel** that reduces the interference between CBs. Here, it uses rogue APs' RSSI data for the last 3 hours. You will be able to suggest a CB channel even if the same CB is used on two or more floor maps.



- **AP power level** that minimizes the number of beacons received by clients to retain the coverage area as much as possible.



The Wireless Concierge page also lets you to display multiple floor maps of selected management groups. We recommend that you use browsers other than Internet Explorer for multiple floor maps display mode to be fully functional.

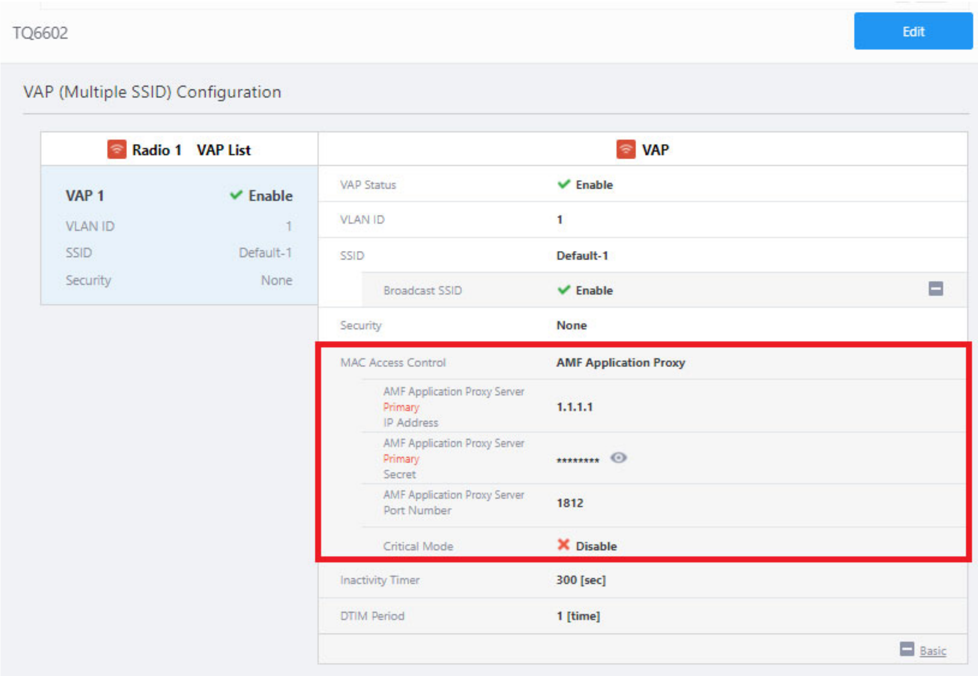
AMF application proxy support

Applicable to the AWC plug-in - Access Point: TQ6602

From Vista Manager EX version 3.7.0 onwards, the AWC plug-in will support AMF Application Proxy on TQ6602 devices. This feature requires the AP to be running firmware version 7.0.1-1.1 or later.

Similar to the TQ5k series, the AMF Application Proxy specifications will be displayed in the MAC Access Control form when selected on the edit page.

Note: The secondary radius server setting is displayed here, but not currently supported.



TQ6602

Edit

VAP (Multiple SSID) Configuration

Radio 1 VAP List

VAP 1 ✓ Enable

VLAN ID	1
SSID	Default-1
Security	None

VAP

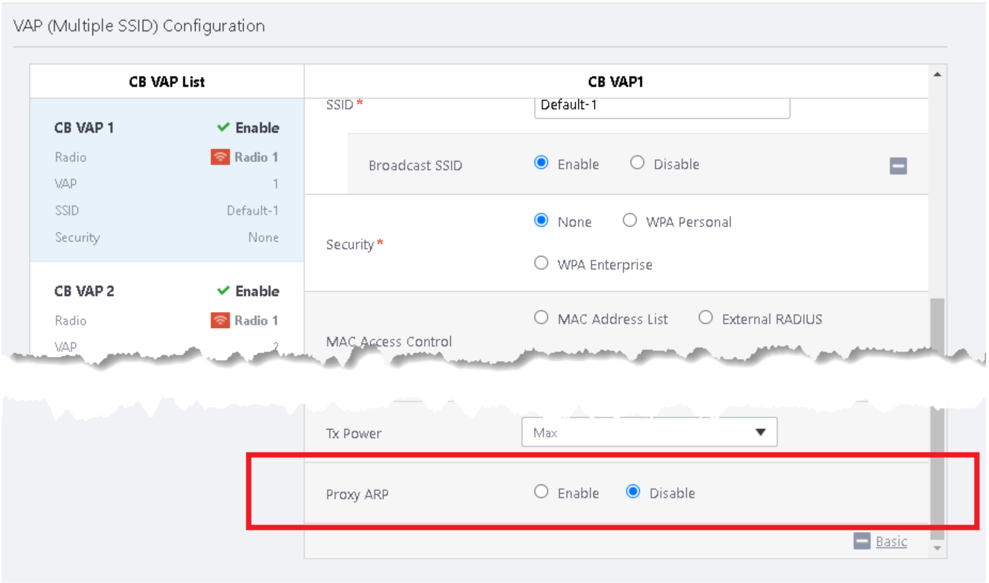
VAP Status	✓ Enable
VLAN ID	1
SSID	Default-1
Broadcast SSID	✓ Enable
Security	None
MAC Access Control	AMF Application Proxy
AMF Application Proxy Server Primary IP Address	1.1.1.1
AMF Application Proxy Server Primary Secret	********
AMF Application Proxy Server Port Number	1812
Critical Mode	✗ Disable
Inactivity Timer	300 [sec]
DTIM Period	1 [time]

Basic

Proxy ARP support

Applicable to the AWC plug-in - Access Point: TQ6602

From Vista Manager EX version 3.7.0 onwards, the AWC plug-in will support proxy ARP on TQ6602 devices. This feature requires the AP to be running firmware version 7.0.1-1.1 or later.



VAP (Multiple SSID) Configuration

CB VAP List

CB VAP 1 ✓ Enable

Radio	Radio 1
VAP	1
SSID	Default-1
Security	None

CB VAP 2 ✓ Enable

Radio	Radio 1
VAP	2

CB VAP1

SSID *	Default-1
Broadcast SSID	● Enable ○ Disable
Security *	● None ○ WPA Personal ○ WPA Enterprise
MAC Access Control	○ MAC Address List ○ External RADIUS
Tx Power	Max
Proxy ARP	○ Enable ● Disable

Basic

Proxy ARP will be displayed (disabled by default) when you select:

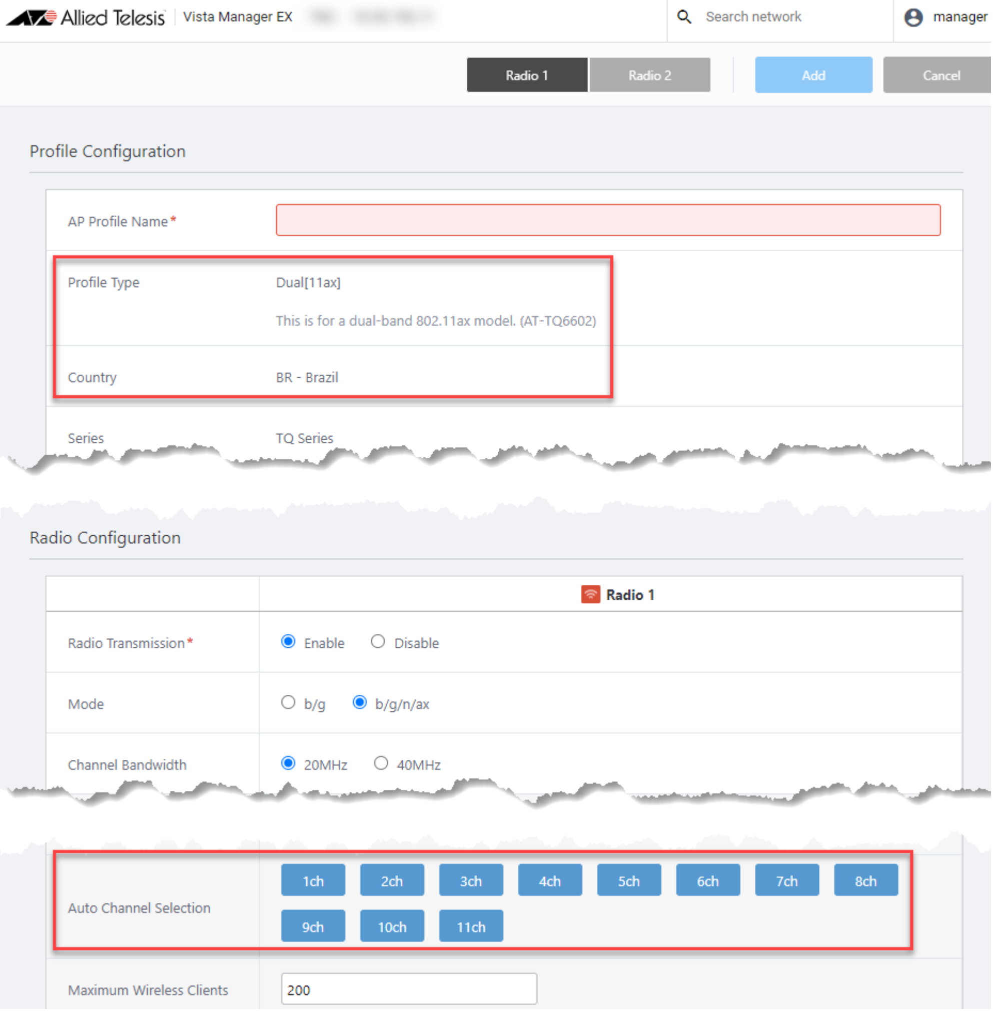
- Dual[11ax] in the AP profile type
- TQ6602 model in the CB profile

DFS channel support

Applicable to the AWC plug-in - Access Point: TQ6602

FCC country codes have been added for Dual[11ax] AP profile types from version 3.7.0 onwards. As DFS channels vary from country to country, DFS channels corresponding to the selected country will then become available in the Auto Channel Selection setting. The following country codes are:

- BR - Brazil
- ID - Indonesian
- MX - Mexico
- US - United States



Profile Configuration

AP Profile Name*	
Profile Type	Dual[11ax] This is for a dual-band 802.11ax model. (AT-TQ6602)
Country	BR - Brazil
Series	TQ Series

Radio Configuration

	Radio 1
Radio Transmission*	● Enable ○ Disable
Mode	○ b/g ● b/g/n/ax
Channel Bandwidth	● 20MHz ○ 40MHz
Auto Channel Selection	1ch 2ch 3ch 4ch 5ch 6ch 7ch 8ch 9ch 10ch 11ch
Maximum Wireless Clients	200

Increased VAPs for channel blanket

Applicable to the AWC plug-in - Access Point: TQ6602

The AWC plug-in now lets you create up to sixteen channel blanket virtual access points (VAPs) for each radio, for a total of two.

AWC Client Filter - Extended MAC address registration

Applicable to the Windows-based Vista Manager installations with the AWC plug-in.

From version 3.7.0 onwards, Vista Manager EX will be able to detect MAC addresses of all Bring Your Own Device users in the GIGA school networks. The AWC Client Filter utility has been developed for this purpose. With permission granted by the AWC administrators, teachers can login to the AWC Client Filter with a user ID and password. They can easily collect MAC addresses of their students' devices and monitor their connection status. Allow/deny connection to the AP can then be set for the collected MAC addresses.

MIB browser support

Applicable to the Windows-based Vista Manager installations with the SNMP plug-in.

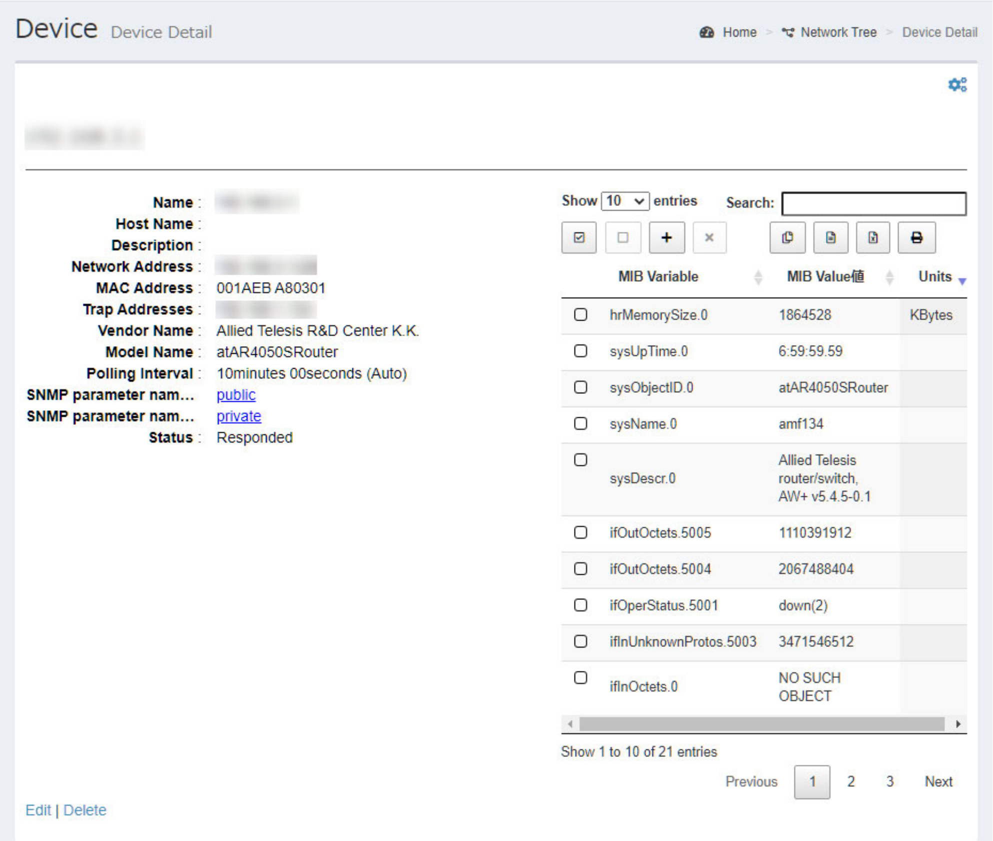
From version 3.7.0 onwards, the SNMP plug-in will support MIB browser functions to see values of the registered MIB variables. Supported functionalities are **device details page, MIB monitor**, **MIB browser**, and **select index**. MIB walk is currently not supported. The basic user interface of the MIB browser page will look similar to the network tree page.

As a user, this feature offers you a range of functionalities:

- access the MIB browser page
- see the compiled and available MIB variables in a tree format
- select MIB variables that you want to monitor
- check MIB variables in the MIB browser page
- check MIB variable contents on the device details page

Device detail page

Click on the gear icon and select the **MIB monitor** menu to open the MIB monitor. This page displays the monitored MIB variables and their current values. Click on the **MIB variable** button to display the MIB variable page. Here, you can configure the MIB variables that you wish to monitor.



[redacted]

Name : [redacted]
Host Name :
Description :
Network Address : [redacted]
MAC Address : 001AEB A80301
Trap Addresses : [redacted]
Vendor Name : Allied Telesis R&D Center K.K.
Model Name : atAR4050SRouter
Polling Interval : 10minutes 00seconds (Auto)
SNMP parameter nam… public
SNMP parameter nam… private
Status : Responded

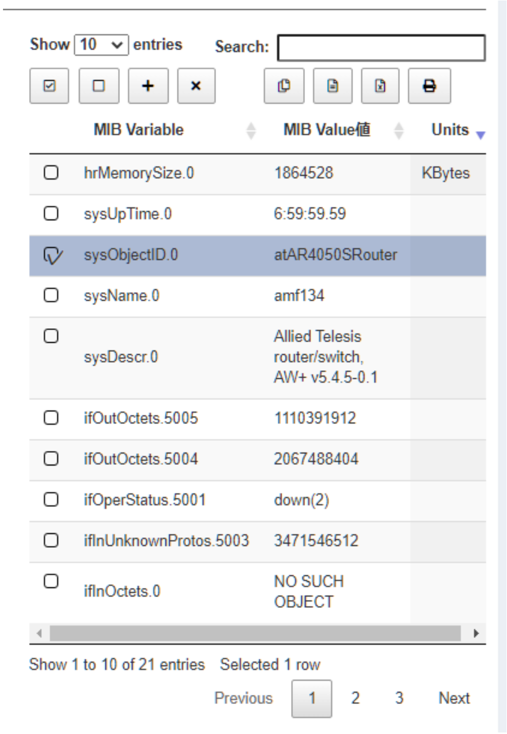
Show 10 entries Search:

	MIB Variable	MIB Value値	Units
□	hrMemorySize.0	1864528	KBytes
□	sysUpTime.0	6:59:59.59	
□	sysObjectID.0	atAR4050SRouter	
□	sysName.0	amf134	
□	sysDescr.0	Allied Telesis router/switch, AW+ v5.4.5-0.1	
□	ifOutOctets.5005	1110391912	
□	ifOutOctets.5004	2067488404	
□	ifOperStatus.5001	down(2)	
□	ifInUnknownProtos.5003	3471546512	
□	ifInOctets.0	NO SUCH OBJECT	

Show 1 to 10 of 21 entries

MIB monitor

Add or delete any MIB variables that you wish to monitor. There is no editing functionality. Only leaf nodes can be monitored, up to a maximum of 25 MIB variables. Leaf nodes are MIB variables without children.



Show 10 entries Search:

	MIB Variable	MIB Value値	Units
□	hrMemorySize.0	1864528	KBytes
□	sysUpTime.0	6:59:59.59	
☑	sysObjectID.0	atAR4050SRouter	
□	sysName.0	amf134	
□	sysDescr.0	Allied Telesis router/switch, AW+ v5.4.5-0.1	
□	ifOutOctets.5005	1110391912	
□	ifOutOctets.5004	2067488404	
□	ifOperStatus.5001	down(2)	
□	ifInUnknownProtos.5003	3471546512	
□	ifInOctets.0	NO SUCH OBJECT	

Show 1 to 10 of 21 entries Selected 1 row

Previous 1 2 3 Next

MIB variables are selected in the MIB browser and displayed as they are. If the MIB variable does not exist on the actual device, it is not supported. However, it is possible to set them even if they are not supported.

Table display is not supported. Please individually number the MIB variables that you wish to display.

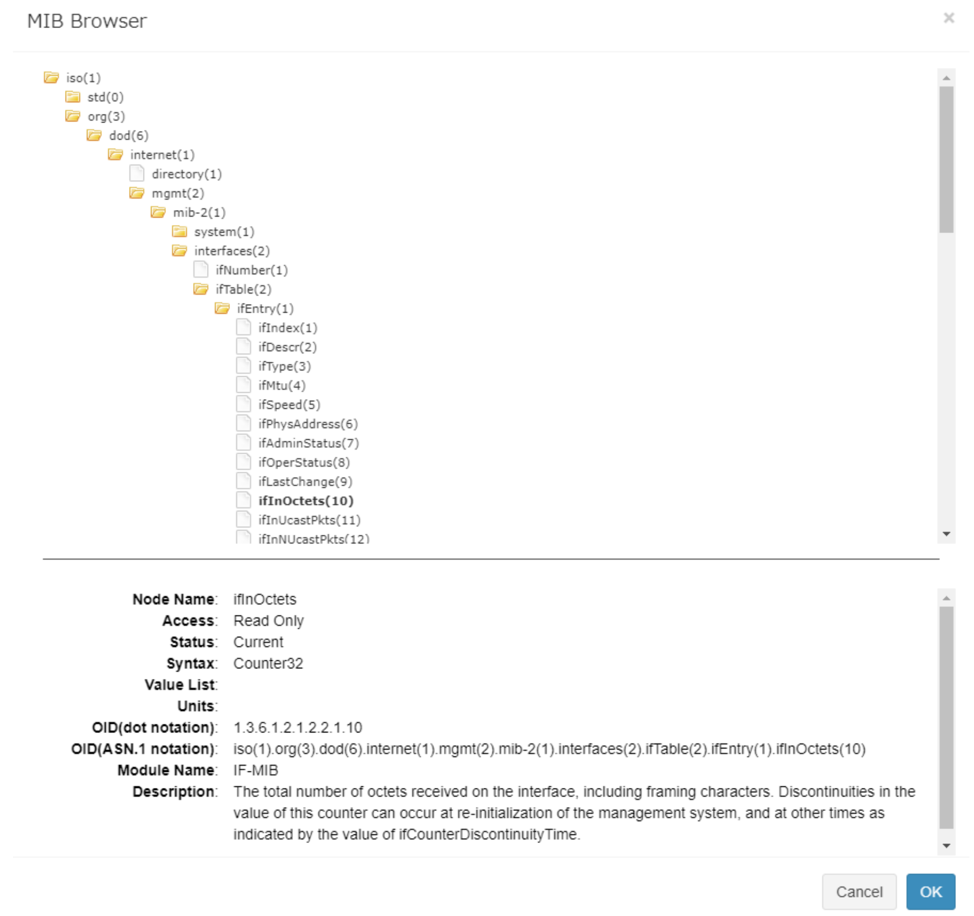
The monitor has four buttons:

☑ □ + ×

- **Select All** - selects all MIB variables that are being monitored.
- **Clear All** - deselects all selected MIB variables.
- **Add** - adds selected MIB variable(s) you want to monitor in the MIB browser.
- **Delete** - deletes selected MIB variable(s). Please note that there is no confirmation of deletion.

MIB browser

On the MIB browser, the MIB node tree displays compiled and available MIB variables hierarchically by its object ID. Each node is represented by a single icon and a node name. The node icon is a smaller icon appearing on the left side of the node row and indicates the type of node. The node name, also known as the MIB variable name, is the administrative name of the node.



```
iso(1)
  std(0)
  org(3)
    dod(6)
      internet(1)
        directory(1)
        mgmt(2)
          mib-2(1)
            system(1)
            interfaces(2)
              ifNumber(1)
              ifTable(2)
                ifEntry(1)
                  ifIndex(1)
                  ifDescr(2)
                  ifType(3)
                  ifMtu(4)
                  ifSpeed(5)
                  ifPhysAddress(6)
                  ifAdminStatus(7)
                  ifOperStatus(8)
                  ifLastChange(9)
                  ifInOctets(10)
                  ifInUcastPkts(11)
                  ifInNUcastPkts(12)
```

Node Name: ifInOctets
Access: Read Only
Status: Current
Syntax: Counter32
Value List:
Units:
OID(dot notation): 1.3.6.1.2.1.2.2.1.10
OID(ASN.1 notation): iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).interfaces(2).ifTable(2).ifEntry(1).ifInOctets(10)
Module Name: IF-MIB
Description: The total number of octets received on the interface, including framing characters. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.

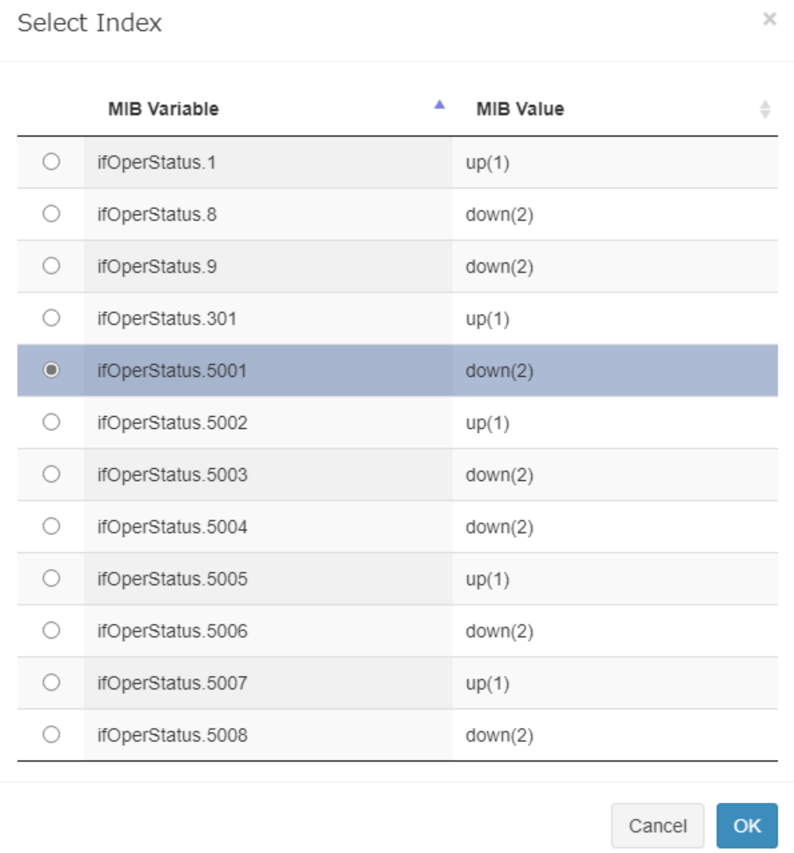
MIB node attributes display basic information about the selected MIB node in the tree view. They are detailed as follows:

- **Node name** - displays the MIB variable name.
- **Access** - displays the access rights of the MIB object. Currently, ACCESS of OBJECT-TYPE for SMIv1 and MAX-ACCESS of OBJECT-TYPE for SMIv2 are applicable.
- **Status** - displays the implementation support status of MIB objects, ie. mandatory, optional, etc.
- **Syntax** - displays the data type of the MIB object.
- **Value list** - lists the names described when numeric name values are used. For example, “syntax” is used for integer, bits, etc.
- **Units** - displays the unit of the MIB value when the units clause is present.
- **OID(dot notation)** - displays the object ID that uniquely identifies the MIB object.
- **OID(ASN.1 notation)** - displays the full path of the MIB object.
- **Module name** - indicates the name of the MIB module that contains the MIB object.
- **Description** - displays descriptions and comments about the MIB object.

The information of a MIB node is described in the MIB file before compilation. Please refer to SMIv1 and SMIv2 for the description of the MIB file.

Select index page

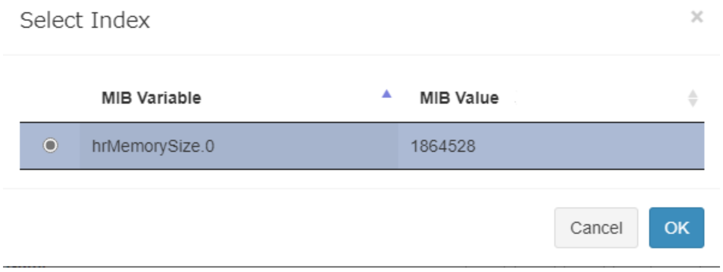
Acquire the value of the MIB variable selected in the MIB browser from the actual device and list it. Select the MIB variable of the index that you wish to monitor with reference to the displayed MIB value.



Select Index

	MIB Variable	MIB Value
○	ifOperStatus.1	up(1)
○	ifOperStatus.8	down(2)
○	ifOperStatus.9	down(2)
○	ifOperStatus.301	up(1)
●	ifOperStatus.5001	down(2)
○	ifOperStatus.5002	up(1)
○	ifOperStatus.5003	down(2)
○	ifOperStatus.5004	down(2)
○	ifOperStatus.5005	up(1)
○	ifOperStatus.5006	down(2)
○	ifOperStatus.5007	up(1)
○	ifOperStatus.5008	down(2)

In scalar type variables, the index is always ".0". Just click **OK** as it is.



Select Index

	MIB Variable	MIB Value
●	hrMemorySize.0	1864528

Important Considerations Before Upgrading

This section describes changes that may affect Vista Manager EX or your network's behavior if you upgrade. Please read it carefully before upgrading.

AMF software version compatibility

- All AMF nodes must run version 5.4.9-0.1 or later.
- Some of the latest functionality is only available on AMF nodes running version 5.5.1-1.1 or later.

Wireless AP software version compatibility

- TQ6602 APs with firmware version 7.0.0-1.3 or later. Some of the latest functionality is only available on APs running version 7.0.1-0.1 or later.
- TQ5403 series APs with firmware version 5.0.x or later. Some of the latest functionality is only available on APs running version 6.0.1-6.1 or later.
- TQ4x00/3x00/2450 APs with firmware version 4.2.x

Internet Explorer 11 compatibility

When using the Vista Manager EX 3.7.0 integrated map with Internet Explorer 11, you may find performance to be slower, particularly with large maps. Therefore, we recommend using a different browser, especially if you have a large network.

Virtualization Support

The Vista Manager EX virtual appliance is not supported on VMware vSphere Hypervisor (ESXi) 5.5. Please upgrade to VMware vSphere Hypervisor (ESXi) 6.0/6.5/6.7 if you wish to use this version of Vista Manager EX.

Vista Manager plug-ins

Vista Manager plug-ins are not available on the standalone Vista Manager appliance. They are available on all other Vista Manager implementations.

Disabling Internet Breakout disables all PBR rules

Internet Breakout uses policy-based routing (PBR) rules. When you use Vista Manager EX to disable Internet Breakout, it disables all PBR rules, including:

- rules created by SDWAN, and
- rules created by Internet Breakout, and
- rules created manually through the CLI.

Integrated map won’t display some links from earlier versions

If you are running some older versions of AlliedWare Plus, the links will not be displayed on the integrated map. Any device running AlliedWare Plus version 5.4.5 or earlier will not have its links shown on the map.

In addition, links from SBx908 GEN1 and x200 devices will not be shown on the integrated map.

Traffic map data not restored

When you are upgrading to Vista Manager EX 3.7.0, traffic map data from earlier versions will not be imported.

Obtaining User Documentation

Vista Manager documentation

Installation Guides, User Guides and Release Notes for Vista Manager EX are available on our website, alliedtelesis.com.

AMF documentation

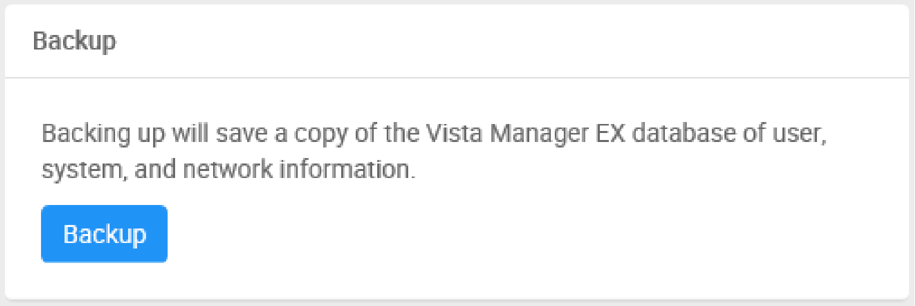
For full AlliedWare Plus documentation, see our online documentation library. For AMF, the library includes the following documents:

- the AMF Feature Overview and Configuration Guide
- the AMF Datasheet
- the AMF Cloud (VAA) Installation Guide.

Upgrading Vista Manager as a virtual appliance

To upgrade Vista Manager as a virtual appliance, use the following steps:

1. Log on to your current Vista Manager. From the System Management page, backup the database to a safe location.



Backup

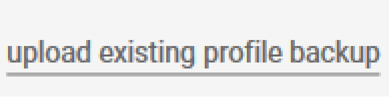
Backing up will save a copy of the Vista Manager EX database of user, system, and network information.

2. Download the software files for Vista Manager EX from the Software Download area of the Allied Telesis website.

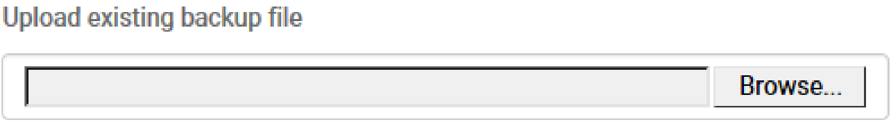
3. Import and start the new version of Vista Manager on your virtual machine host, following the instructions from the Vista Manager EX Installation on the Allied Telesis website.

4. In the new Vista Manager, log in using the default credentials.

5. A dialog displays once you have logged in. On the displayed dialog, click the "Upload existing profile backup" link.



6. Browse to and upload the backup you created in Step 1.



Upload existing backup file

7. In the new Vista Manager, log in again using the credentials from your current Vista Manager. Check that everything is functioning correctly, and that your settings have been correctly imported.

8. If you use a TLS proxy to provide HTTPS access to Vista Manager, then when you are satisfied that the new Vista Manager is working correctly, reconfigure your TLS terminating proxy to point to the new Vista Manager and stop the current one.

Upgrading Vista Manager as a Windows-based installation

Windows-based Vista Manager has two optional plug-ins. These can be upgraded at the same time as Vista Manager EX.

Obtain the executable files

1. Download Vista Manager EX from the Allied Telesis download center. If you are going to install the AWC and/or SNMP plug-ins then download these files from the same location.

    - The Vista Manager EX installation executable is named 'atvmex*XXX*b*XX*w.exe', with the *Xs* denoting the version and build numbers.
    - The AWC plug-in is called 'atawc*XXX*b*XX*w.exe'.
    - The SNMP plug-in is called 'atsnmp*XXX*b*XX*w.exe'.

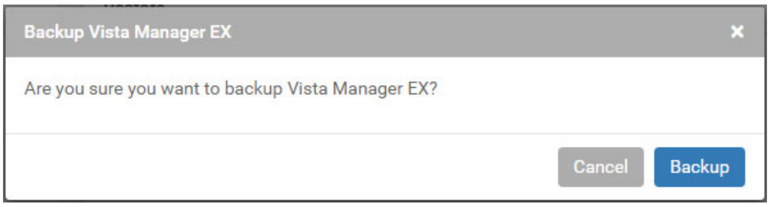
    Do not rename these files. The installation requires them to be in this format.

2. Put the executables for Vista Manager and any plug-ins you wish to install in a single folder. This folder must be accessible from the machine you wish to install Vista Manager on.

Backup Vista Manager EX and the plugins

Backup Vista Manager EX

3. Log on to your Vista Manager EX and select the System Management page.
4. Click on the Backup button in the Database Management Pane.
5. Click Backup again to confirm you wish to make a backup.



Backup Vista Manager EX

Are you sure you want to backup Vista Manager EX?

This automatically downloads a ***tar*** file backup to your default download location.

Backup the SNMP plug-in

6. If you have the SNMP plug-in installed then log on locally to the Vista Manager EX server.
7. Stop the SNMP server services using the shortcut or by running the following command line.

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

8. Run the backup utility by using the shortcut or by running the following command line.

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

    Follow the instructions on the screen.

Backup the AWC plug-in

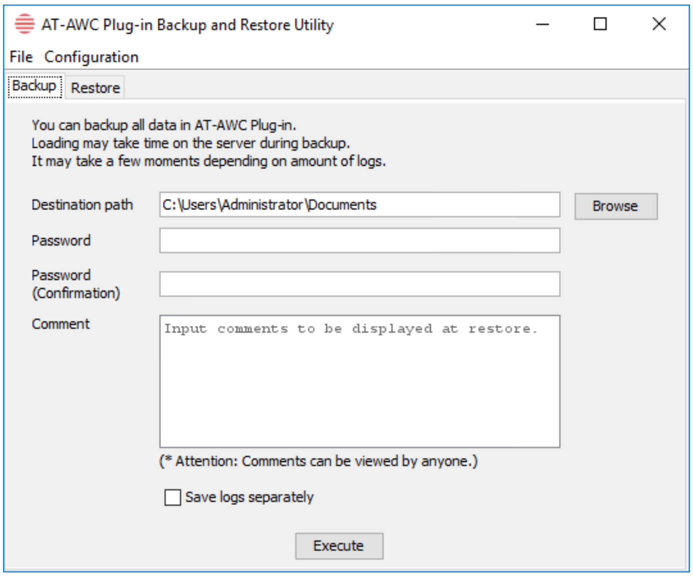
9. If you have the AWC plug-in installed then log on locally to the Vista Manager EX server.

10. Stop the AWC server services using the shortcut or by running the following command line.

    ***"<Vista Install Path>*\Plugins\AT-AWC\root\stopserver.bat"**

11. Run the backup/restore utility by using the shortcut or running the following command line.

    ***"<Vista Install Path>*\Plugins\AT-AWC\tools\maintenance\maintenance.bat"**



You can backup all data in AT-AWC Plug-in.
Loading may take time on the server during backup.
It may take a few moments depending on amount of logs.

Destination path: C:\Users\Administrator\Documents

Password:

Password (Confirmation):

Comment: Input comments to be displayed at restore.

(* Attention: Comments can be viewed by anyone.)

□ Save logs separately

12. Select the backup tab and follow the instructions on the screen.

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

Uninstall the existing version

13. Log on as the same user as when installing.

14. Stop the server. Select **AT-Vista Manager EX** and then **AT-Vista Manager EX - Stop Server** from the Windows menu.

15. From the Windows menu, select **AT-Vista Manager EX** then **AT-Vista Manager EX - Uninstall**.

16. The AT-Vista Manager EX uninstaller starts.

17. Click the **Uninstall** button to uninstall.

18. If a dialogue box prompting you to restart the system is displayed, select **Restart the system** or **Restart later** and click the **Finish** button.

19. Delete the installation folder. The default installation folder is:
    C: \ Program Files (x86) \ Allied Telesis \ AT-Vista Manager EX

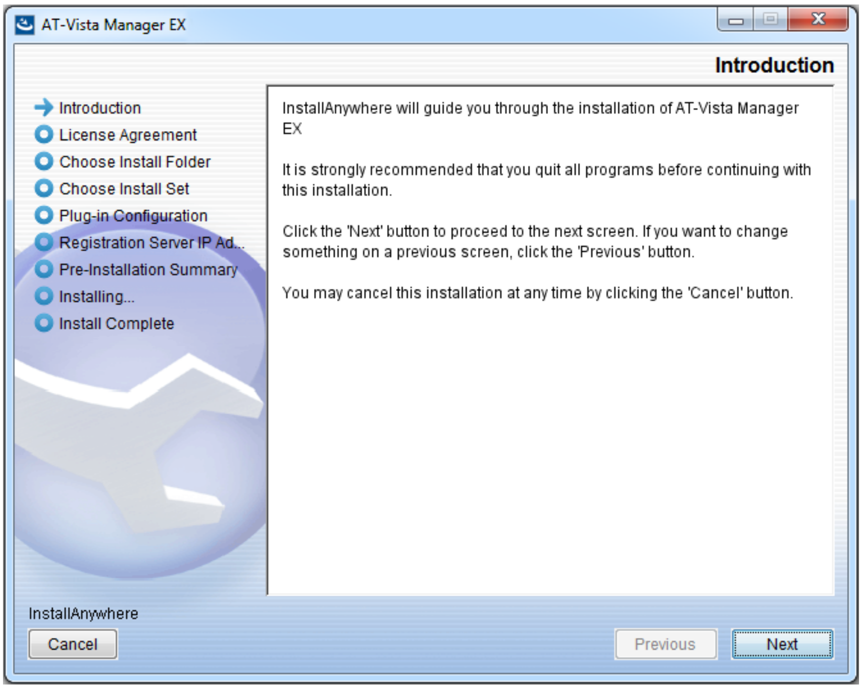
20. Reboot the system.

Install the new version

21. Execute the Vista Manager EX installation program ‘atvmex*XXX*b*XX*w.exe’.

Note: You must have administrator privileges to run the installer.

22. The **Introduction** dialog displays:



InstallAnywhere will guide you through the installation of AT-Vista Manager EX

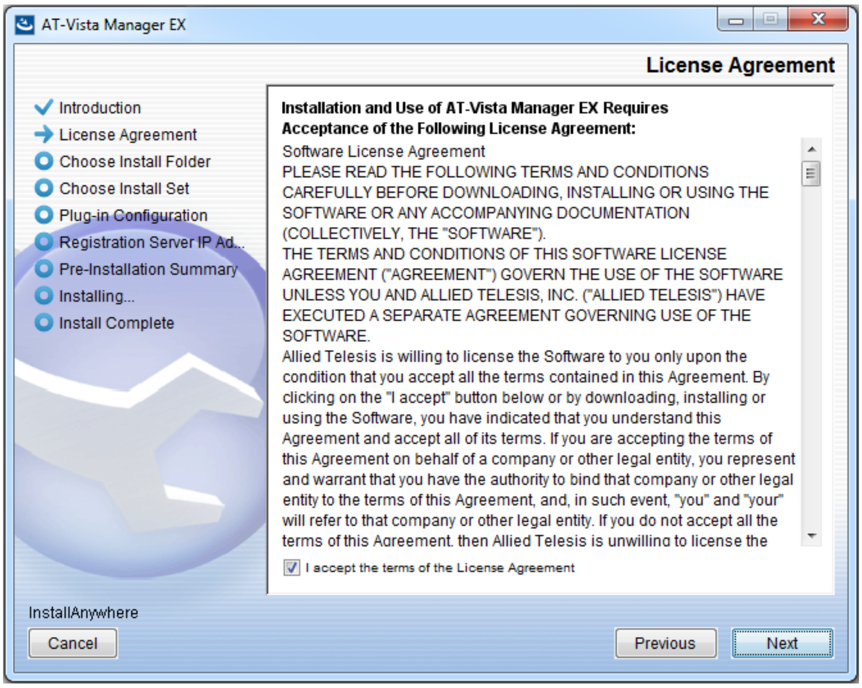
It is strongly recommended that you quit all programs before continuing with this installation.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

You may cancel this installation at any time by clicking the 'Cancel' button.

This wizard will guide you through the installation of the latest version of Vista Manager EX. Click **Next**.

23. The **License Agreement** dialog displays:



Installation and Use of AT-Vista Manager EX Requires Acceptance of the Following License Agreement:

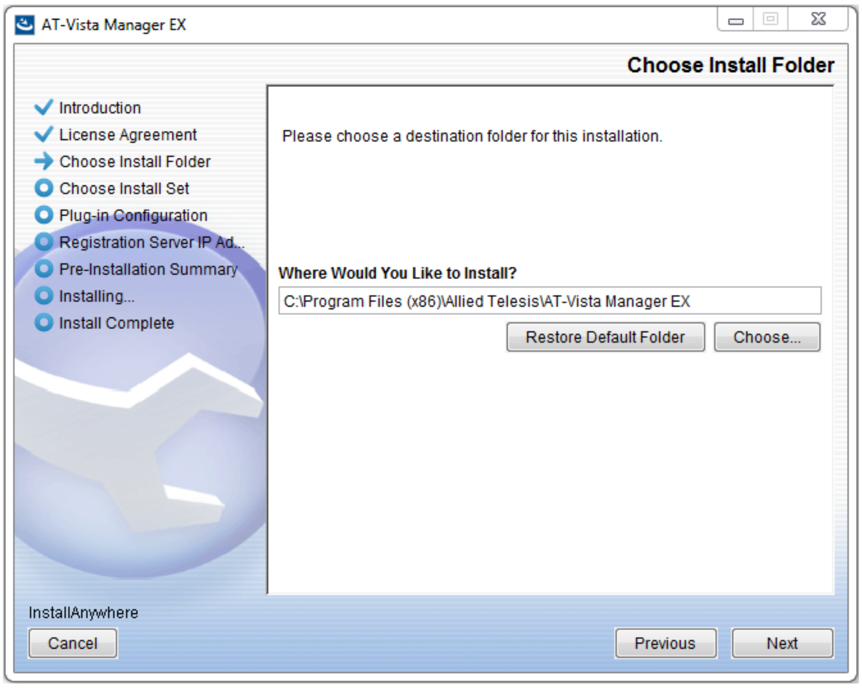
Software License Agreement
PLEASE READ THE FOLLOWING TERMS AND CONDITIONS CAREFULLY BEFORE DOWNLOADING, INSTALLING OR USING THE SOFTWARE OR ANY ACCOMPANYING DOCUMENTATION (COLLECTIVELY, THE "SOFTWARE").
THE TERMS AND CONDITIONS OF THIS SOFTWARE LICENSE AGREEMENT ("AGREEMENT") GOVERN THE USE OF THE SOFTWARE UNLESS YOU AND ALLIED TELESIS, INC. ("ALLIED TELESIS") HAVE EXECUTED A SEPARATE AGREEMENT GOVERNING USE OF THE SOFTWARE.
Allied Telesis is willing to license the Software to you only upon the condition that you accept all the terms contained in this Agreement. By clicking on the "I accept" button below or by downloading, installing or using the Software, you have indicated that you understand this Agreement and accept all of its terms. If you are accepting the terms of this Agreement on behalf of a company or other legal entity, you represent and warrant that you have the authority to bind that company or other legal entity to the terms of this Agreement, and, in such event, "you" and "your" will refer to that company or other legal entity. If you do not accept all the terms of this Agreement, then Allied Telesis is unwilling to license the

☑ I accept the terms of the License Agreement

Read the software license agreement terms and conditions. If you agree to accept the terms of the license agreement:

- Click **I accept the terms of the License Agreement**
- Click **Next**

24. The **Choose Install Folder** dialog displays:



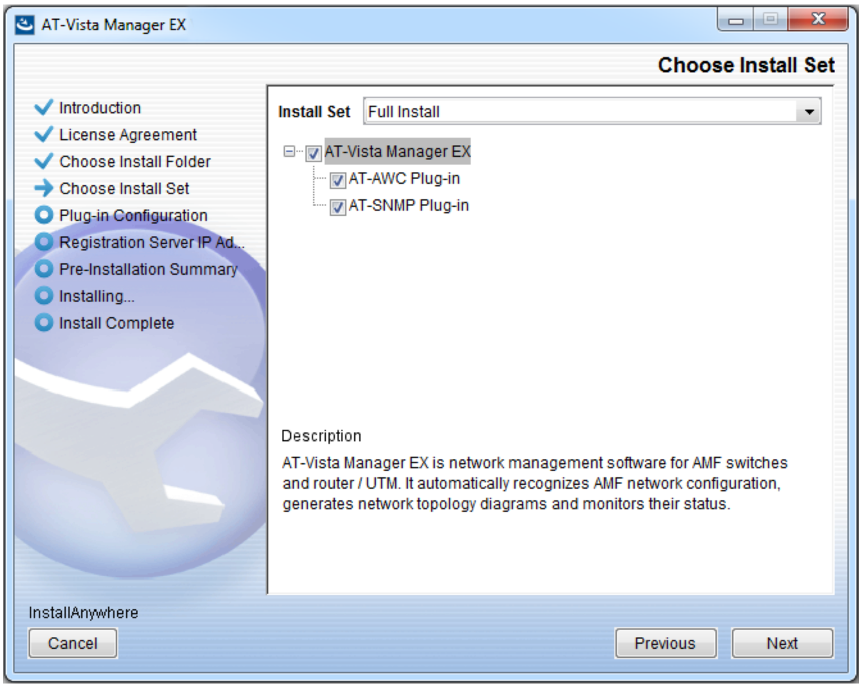
Please choose a destination folder for this installation.

Where Would You Like to Install?

C:\Program Files (x86)\Allied Telesis\AT-Vista Manager EX

Select a destination location and click **Next**.

25. The **Choose Install Set** dialog displays:



AT-Vista Manager EX

Choose Install Set

- ✓ Introduction
- ✓ License Agreement
- ✓ Choose Install Folder
- → Choose Install Set
- ○ Plug-in Configuration
- ○ Registration Server IP Ad...
- ○ Pre-Installation Summary
- ○ Installing...
- ○ Install Complete

Install Set: Full Install

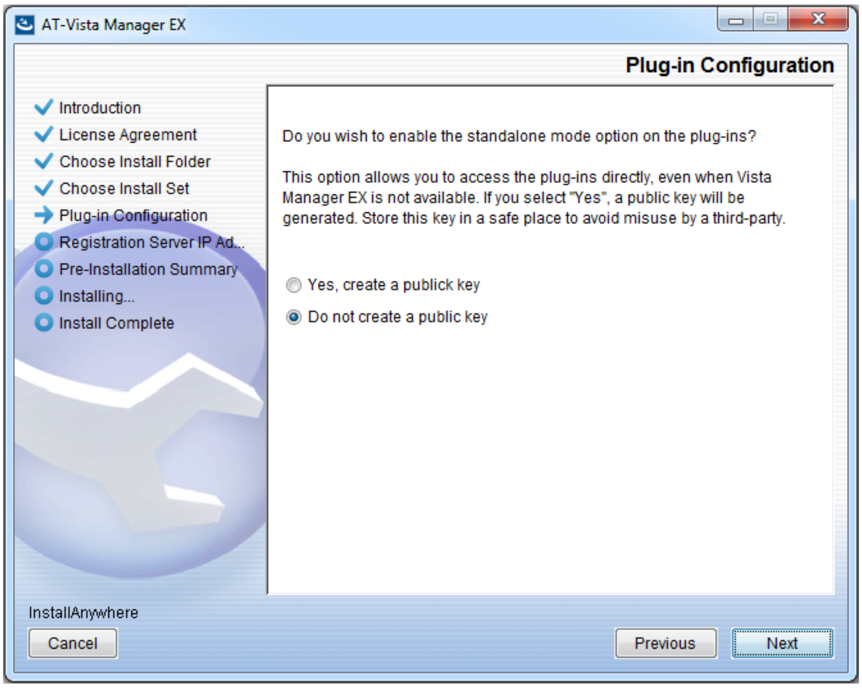
- ☑ AT-Vista Manager EX
  - ☑ AT-AWC Plug-in
  - ☑ AT-SNMP Plug-in

Description

AT-Vista Manager EX is network management software for AMF switches and router / UTM. It automatically recognizes AMF network configuration, generates network topology diagrams and monitors their status.

Select **Full Install** from the drop down list. By default all plug-ins will be selected. Clear the check box for any plug-ins you do not wish to install. Click **Next**.

26. The **Plug-In Configuration** dialog displays:



AT-Vista Manager EX

Plug-in Configuration

- ✓ Introduction
- ✓ License Agreement
- ✓ Choose Install Folder
- ✓ Choose Install Set
- → Plug-in Configuration
- ○ Registration Server IP Ad...
- ○ Pre-Installation Summary
- ○ Installing...
- ○ Install Complete

Do you wish to enable the standalone mode option on the plug-ins?

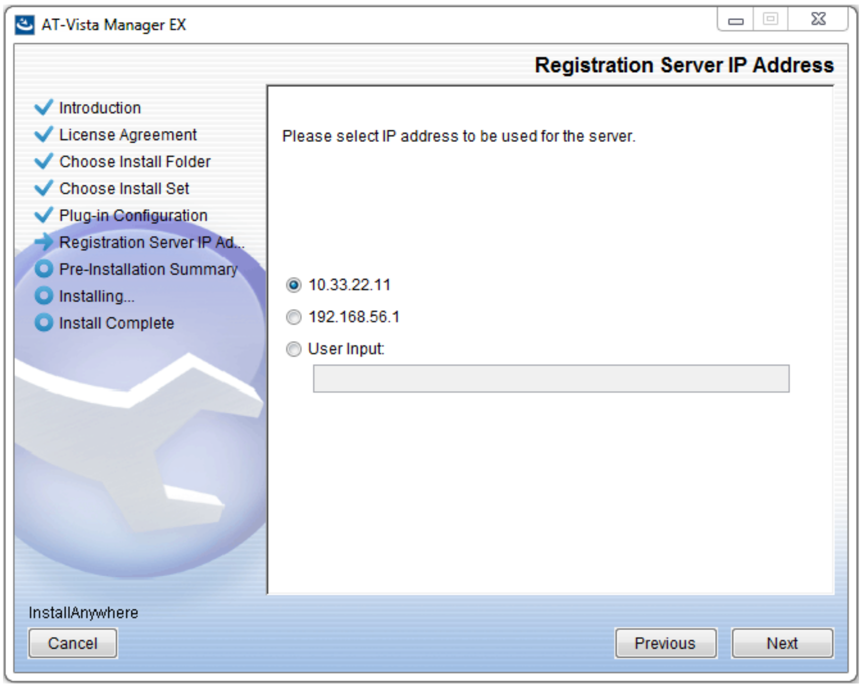
This option allows you to access the plug-ins directly, even when Vista Manager EX is not available. If you select "Yes", a public key will be generated. Store this key in a safe place to avoid misuse by a third-party.

○ Yes, create a publick key

● Do not create a public key

Select **Do not create a public key** unless you are intending to use the plug-ins in standalone mode. For more information on standalone mode, refer to the Installation Guide. Click **Next**.

27. The **Registration Server IP Address** dialog displays:



Registration Server IP Address

Please select IP address to be used for the server.

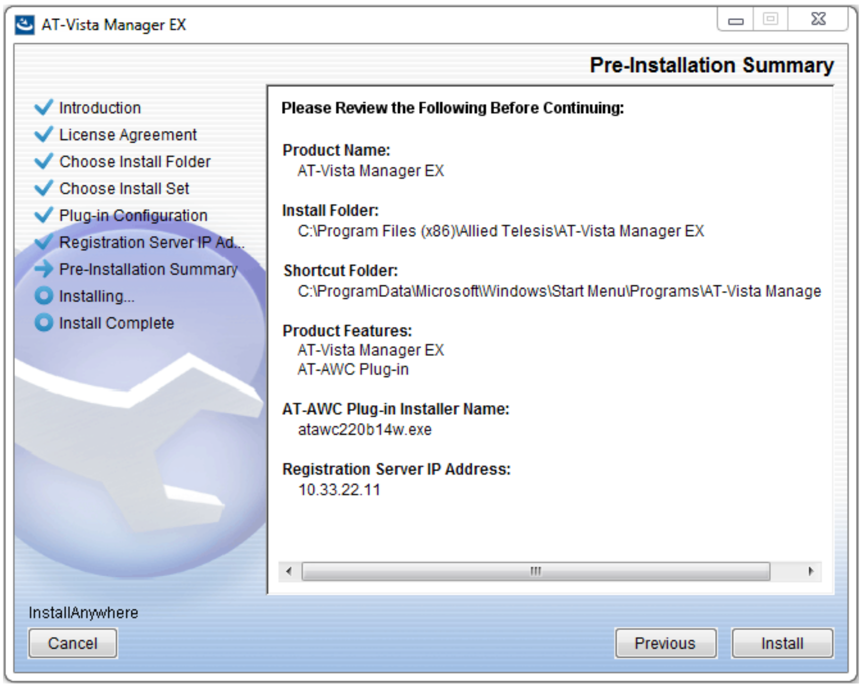
● 10.33.22.11

○ 192.168.56.1

○ User Input:

Either select from the list of IP addresses already configured on the Windows machine, or input a valid IP address. Click **Next**.

28. The **Pre-Installation Summary** dialog displays:



Pre-Installation Summary

Please Review the Following Before Continuing:

Product Name:
AT-Vista Manager EX

Install Folder:
C:\Program Files (x86)\Allied Telesis\AT-Vista Manager EX

Shortcut Folder:
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\AT-Vista Manage

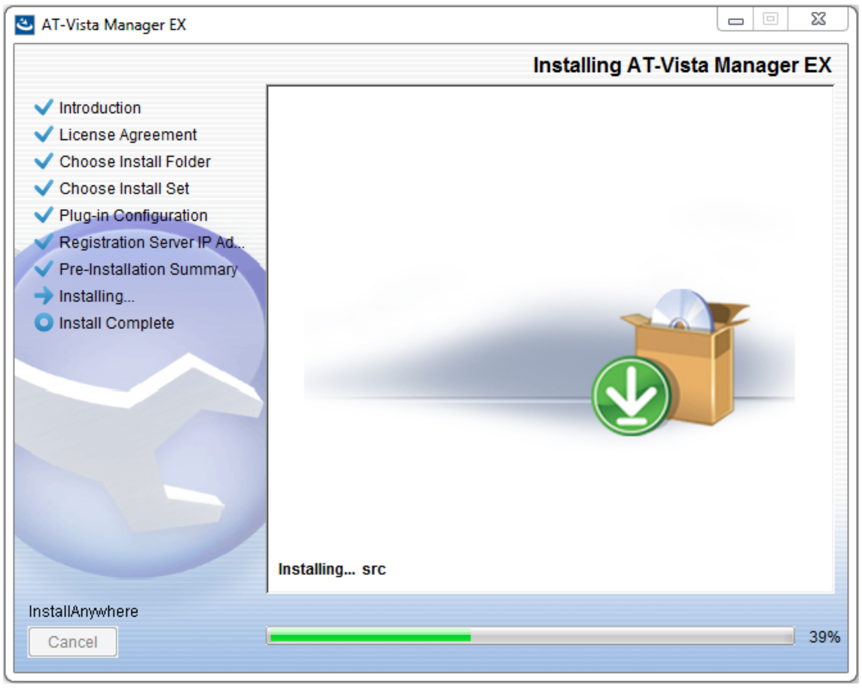
Product Features:
AT-Vista Manager EX
AT-AWC Plug-in

AT-AWC Plug-in Installer Name:
atawc220b14w.exe

Registration Server IP Address:
10.33.22.11

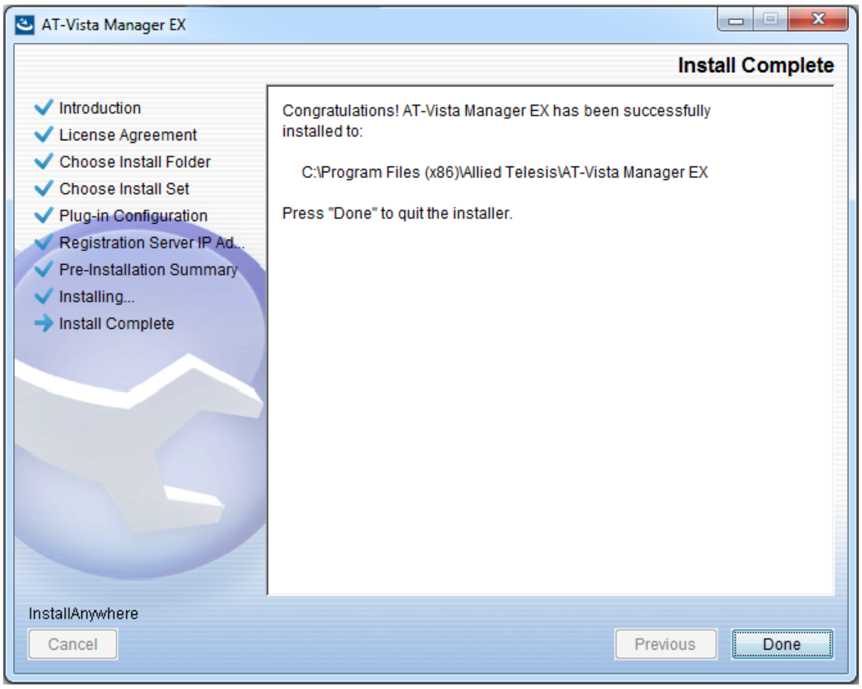
Check that your Product Name, Install Folder, Shortcut Folder, Product Features, Plugin Installer Name and Registration IP Address are correct, and then click **Install**.

29. The **Installing...** dialog displays:



Installing... src

30. Once the installation is complete you will see the **Install Complete** dialog:



Congratulations! AT-Vista Manager EX has been successfully installed to:

C:\Program Files (x86)\Allied Telesis\AT-Vista Manager EX

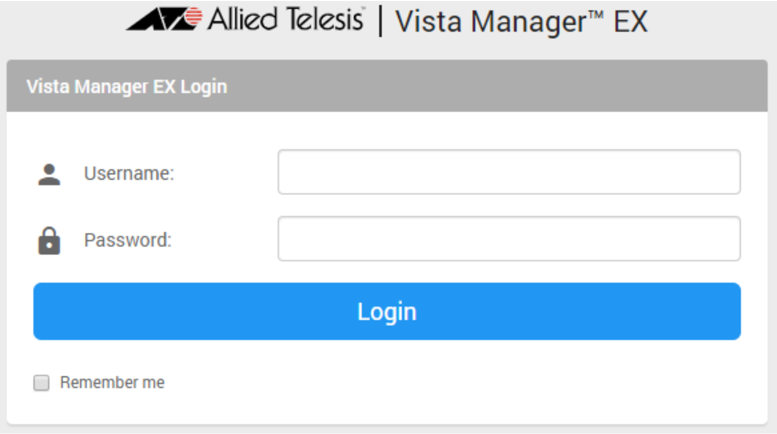
Press "Done" to quit the installer.

Check that the installation has completed successfully and click **Done**.

Restore the Vista Manager database

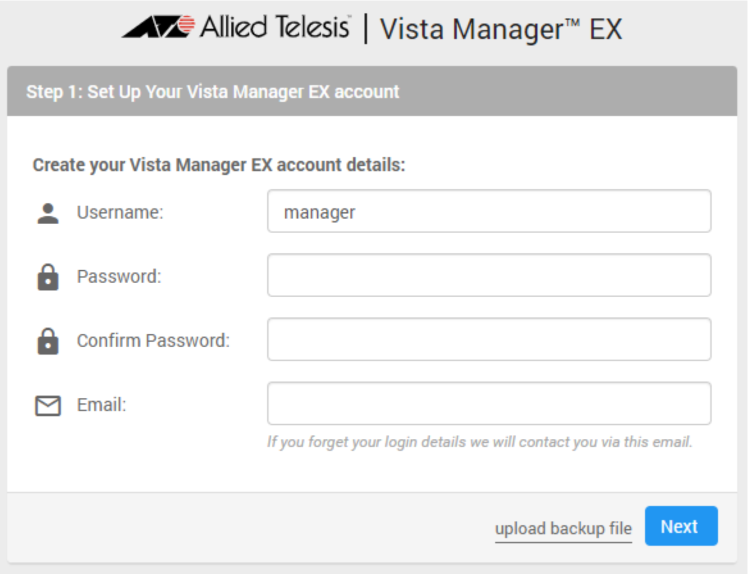
After the upgrade is complete, you need to restore the Vista Manager database. To do this, use the following procedure.

31. Login to Vista Manager.



Enter the **Username** manager and the **Password** friend. Click Login.

32. Click on upload backup file.


Allied Telesis | Vista Manager™ EX
Step 1: Set Up Your Vista Manager EX account

Create your Vista Manager EX account details:

Username: manager

Password:
Confirm Password:
Email:
If you forget your login details we will contact you via this email.
upload backup file
Next

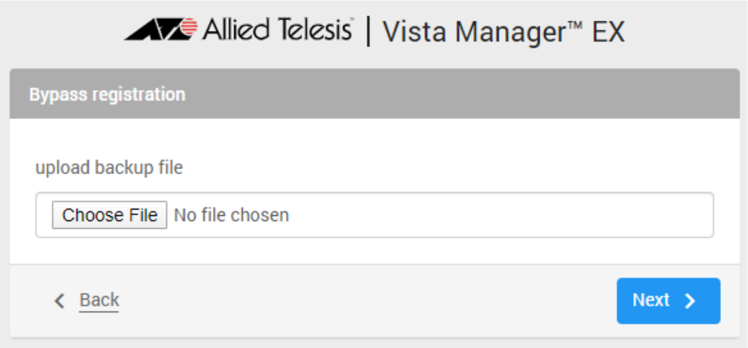
Caution

Your serial number and license information are part of your database backup. If you upload the backup file when upgrading, you will keep the same serial number, and your licensing will continue to work without interruption.

However, if you configure a new instance of Vista Manager EX, without uploading your backup, a new serial number will be generated, and your existing licensing will no longer work. You will need to contact Allied Telesis support to generate a new license.

Therefore, it is STRONGLY recommended that you upload your database backup to ensure your licensing keeps working.

33. Select the database backup to upload. Click on Choose File, and browse to your Vista Manager database backup. Click Next. The Vista Manager database will be restored.



Restore the SNMP plug-in

34. If you have the SNMP plug-in installed then log on locally to the Vista Manager EX server.

35. Stop the SNMP server services using the shortcut or by running the following command line.

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

36. Run the restore utility by using the shortcut or by running the following command line.

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

Follow the instructions on the screen.

Restore the AWC plug-in

37. If you have the AWC plug-in installed then log on locally to the Vista Manager EX server.

38. Stop the AWC server services using the shortcut or by running the following command line.

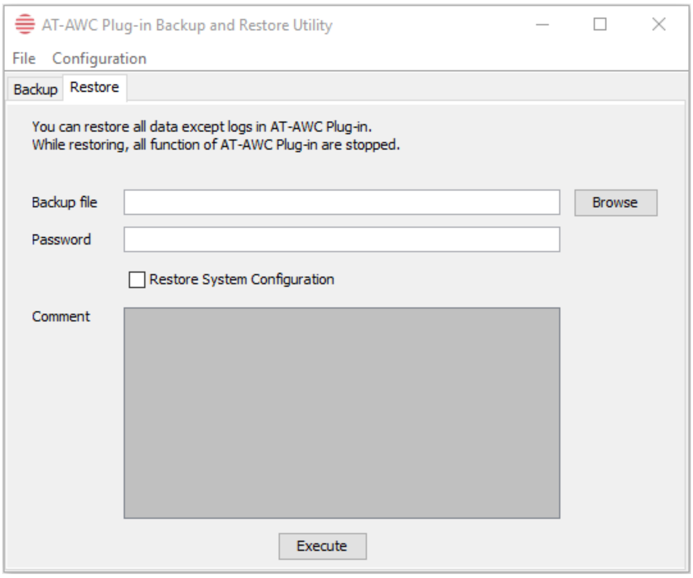
“<*Vista Install Path*>\Plugins\AT-AWC\root\stopserver.bat"

39. Run the backup/restore utility by using the shortcut or running the following command line.

“<*Vista Install Path*>\Plugins\AT-AWC\tools\maintenance\maintenance.bat"

40. Select the restore tab on the dialog and follow the instructions on the screen.

Note: By default, restoring the AWC database will not restore the system configuration. You can restore the system configuration by checking the Restore System Configuration checkbox in the backup/restore utility.



You can restore all data except logs in AT-AWC Plug-in.
While restoring, all function of AT-AWC Plug-in are stopped.

□ Restore System Configuration

We recommend that you check the Restore System Configuration checkbox, as it will allow you to restore the following system configuration settings:

- Database Settings
  - Maximum Memory Usage
- Data Retention Period Settings
  - Associated Client History
  - Client Location Estimation History
  - IDS Report History
- Network Map Settings
  - Wireless Client Update-Interval
- Client Location Estimation History data

The system configuration contains settings that are tailored to the machine that created the backup. If you are restoring the backup on a different machine, particularly if that machine has a lower specification, it is recommended not to restore the system configuration.

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

Upgrading Vista Manager on VST-APL

See the Vista Manager Network Appliance (VST-APL) User Guide.

Troubleshooting

See the Troubleshooting chapter in the Vista Manager EX User Guide.

Allied Telesis™

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