

Release Note for Vista Manager EX v3.0



v. 3.0.0

v. 3.0.1

v. 3.0.2

Acknowledgments

©2019 Allied Telesis Inc. All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesis, Inc.

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.

Allied Telesis, AlliedWare Plus, Allied Telesis Management Framework, EPSRing, SwitchBlade, VCStack and VCStack Plus are trademarks or registered trademarks in the United States and elsewhere of Allied Telesis, Inc. Adobe, Acrobat, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Additional brands, names and products mentioned herein may be trademarks of their respective companies.

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/

Content

What's New in Vista Manager EX v3.0.2	4
Introduction.....	4
Issues Resolved in v3.0.2	4
What's New in Vista Manager EX v3.0.1	5
Introduction.....	5
Issues Resolved in v3.0.1	5
What's New in Vista Manager EX v3.0.0	6
Introduction.....	6
New Features and Enhancements.....	6
Important Considerations Before Upgrading	27
Information After Upgrading	28
Obtaining User Documentation	30
Upgrading Vista Manager as a virtual appliance.....	31
Upgrading Vista Manager as a Windows-based installation	32
Restoring Vista Manager EX	39

What's New in Vista Manager EX v3.0.2

Introduction

This release note describes the new features in Vista Manager EX™ v3.0.2. It covers Vista Manager EX plus the optional Autonomous Wave Controller (AWC) and SNMP plug-ins.

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 a license.



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.

Issues Resolved in v3.0.2

This Vista Manager EX release version resolves the issues in the following table:

CR	Module	Description
CR-63740	Base	Previously, if you moved a guest node from one switch to another switch, Vista Manager EX still displayed the guest's old link (as a dotted line), as well as displaying the new link. This issue has been resolved. Once the new link has been established, the old link will now disappear. Also, if a node was offline/critical, when it changes back to online/normal, all the missing links (dotted lines) related to that node will be removed. You will now only see the current active links.
CR-63868	Base	Previously, if you used AWC auto-recovery to replace a guest node AP, the old AP was not removed from device search or the node count. This issue has been resolved.

What's New in Vista Manager EX v3.0.1

Introduction

This release note describes the new features in Vista Manager EX™ v3.0.1. It covers Vista Manager EX plus the optional Autonomous Wave Controller (AWC) and SNMP plug-ins.

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 a license.



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.

Issues Resolved in v3.0.1

This Vista Manager EX release version resolves the issues in the following table:

CR	Module	Description
CR-62993	Base	After replacing one node with another, and then renaming the original node, upgrading Vista from 2.5.0 to 3.0.0 sometimes merged the two nodes into one. This issue has been resolved.

What's New in Vista Manager EX v3.0.0

Introduction

This release note describes the new features in Vista Manager EX™ v3.0.0. It covers Vista Manager EX plus the optional Autonomous Wave Controller (AWC) and SNMP plug-ins.

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 a license.



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.

New Features and Enhancements

This section summarizes the new features added to Vista Manager EX v3.0.0.

Disable automatic logout

Applicable to all Vista Manager installations.

From Vista Manager EX version 3.0.0, you will be able to disable the automatic logout of a user. When the idle timeout for a user is set, if the amount of time with no user input is exceeded, the browser session is logged out. An additional setting has been added which allows you to disable this functionality on a per user basis.

To disable the automatic logout, open the User Management screen, and select the user you wish to change. Click on Edit, and then from the Timeout (in mins) drop-down, select Never. Click Save to make the change.

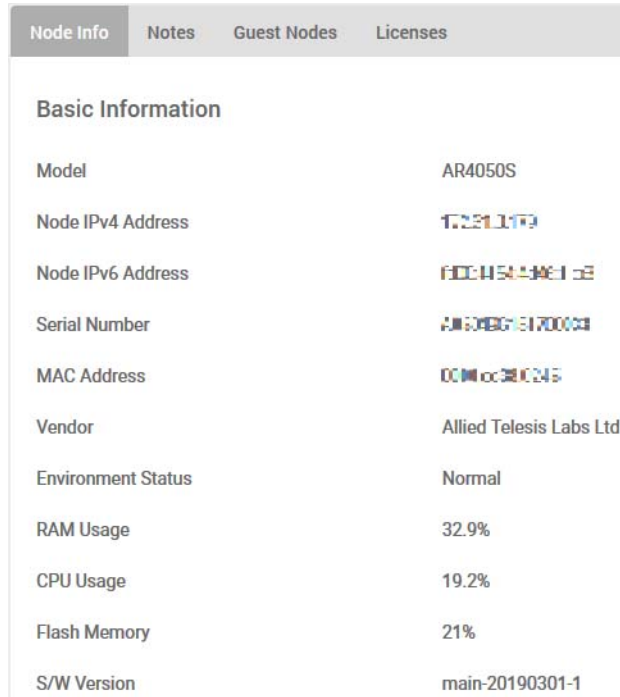
The screenshot shows a form with three fields: 'Country Code', 'Language:', and 'Timeout (in mins):'. The 'Timeout (in mins):' field has a dropdown menu open, showing options: 5 minutes, 10 minutes, 20 minutes, 30 minutes, 1 hour, and Never. The 'Never' option is highlighted in blue. Below the form are two buttons: 'Save' and 'Cancel'.

Vendor information for devices

Applicable to all Vista Manager installations.


From Vista Manager EX version 3.0.0, you will be able to view the vendor for each device in the network. You will also be able to search for a device by vendor, and export a report of devices and their vendors.

The vendor is viewable in the Node Info screen.



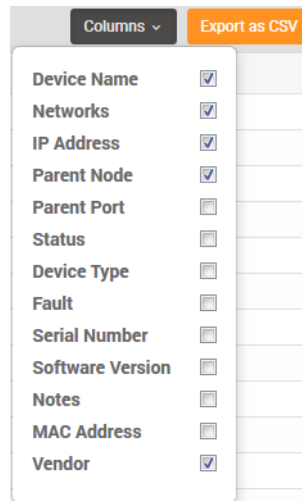
Node Info	Notes	Guest Nodes	Licenses
Basic Information			
Model			AR4050S
Node IPv4 Address			172.31.1.179
Node IPv6 Address			fd00:454:4461::3
Serial Number			AJ6386E170000
MAC Address			0000cc300245
Vendor			Allied Telesis Labs Ltd
Environment Status			Normal
RAM Usage			32.9%
CPU Usage			19.2%
Flash Memory			21%
S/W Version			main-20190301-1

The vendor is also viewable in the Network Map when selecting a node.

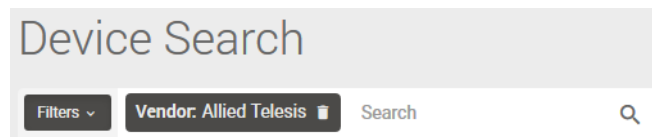


area1 Map	VLAN Map	Traffic M
 02-AR4050		
Basic Information		
Status		Normal
IP Addresses		172.31.1.179
Type		router
Model		AR4050S
Serial		AJ6386E170000
Version		main-20190301-1
Last Backup		Mar 6, 2019
Vendors		Allied Telesis Labs ...

In the Device Search screen, the vendor details can be viewed by selecting the check box next to Vendor in the Columns dropdown. This information can also be exported using the Export as CSV button.



You can also enter a vendor in the Search field of the Device Search screen to search by vendor, or from the Filters dropdown to filter on a vendor.



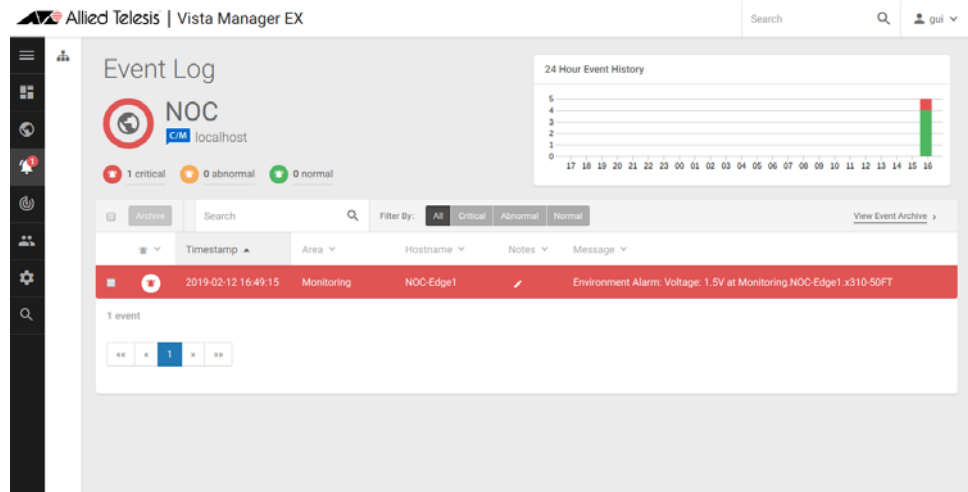
New entries have also been added to the Device Search dropdown for MAC Address and Location. MAC Address allows you to search and filter on the MAC address of the device. Location shows the port of the parent node that a guest device is connected to. Location is only shown for AMF guest nodes. Both MAC Address and Location can also be exported to CSV.

Alerts for environmental alarms

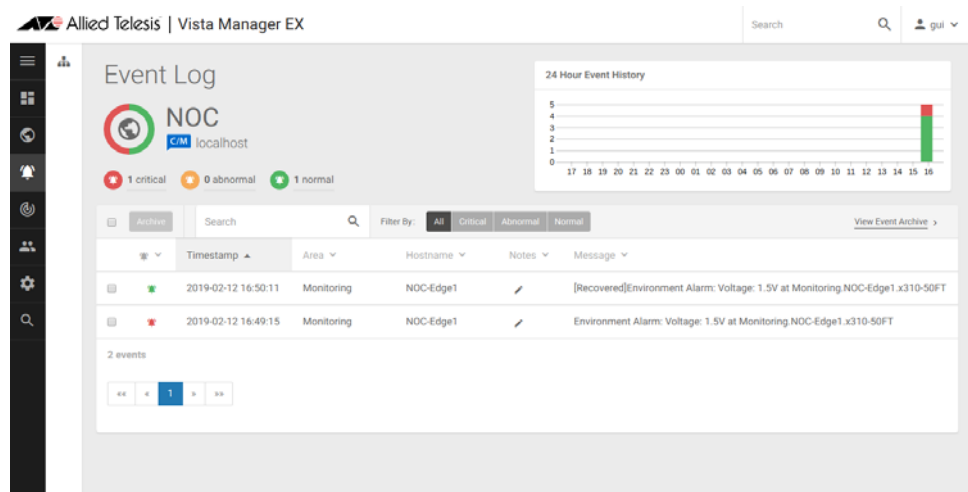
Applicable to all Vista Manager installations.

From Vista Manager EX version 3.0.0, environmental alarms will be displayed in Vista Manager. They are shown as an event in the Event Log and a notification on the Network Map.

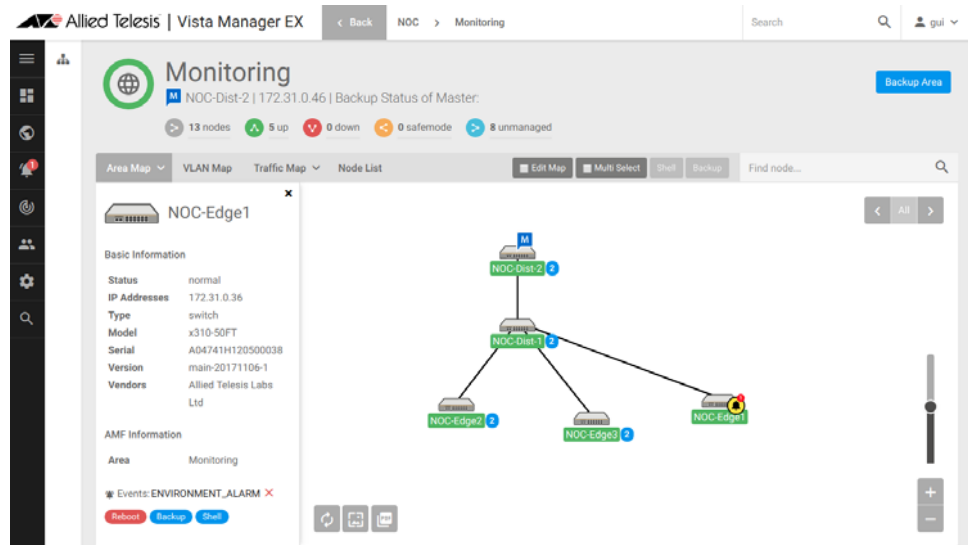
Alarms are checked for every 5 seconds. If an alarm occurs, it will show as a new row in the event log.



If an alarm auto-recovers, a new row in the event log will show it as "Recovered", and the previous row will be dismissed.



Active alarms appear on the network map as a notification bell. The number of active alarms for a node is displayed on the side panel of the network map.



Improved device alignment on map

Applicable to all Vista Manager installations.

From Vista Manager EX version 3.0.0, Vista Manager will improve the automatic positioning of the nodes on the map to allow users to better understand the topology.

The new node layout function only works on new installations and registrations from Vista Manager EX 3.0.0 onwards. Existing topologies will remain unchanged.

The new algorithm only applies to maps with 30 or more nodes. Maps with fewer nodes will continue to use the old algorithm.

Static icon map support

Applicable to all Vista Manager installations.

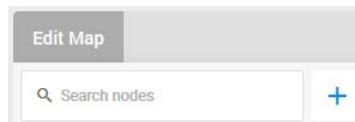
From Vista Manager EX version 3.0.0, the integrated map will support the manual addition and deletion of static devices and links. These allow administrators to configure devices and links that have not been automatically learned.

Non-administrative users are restricted to being able to change the position of nodes on the integrated map. Editing the map requires administrative permissions.

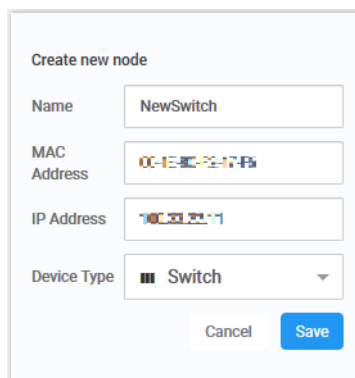
Administrative users are able to see the Edit Map option. Selecting Edit Map puts the integrated map in edit mode.



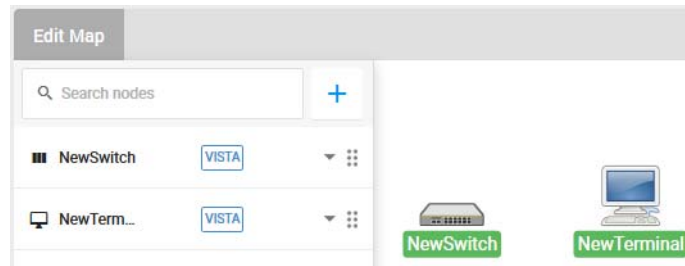
While in edit mode, a list of all static devices will appear as a side panel. You can add new devices by clicking on the + button.



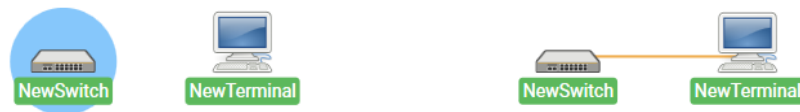
Each new device must be given a name, MAC address, IP address, and device type. Click Save to add the device.

A dialog box titled "Create new node" with a light grey background. It contains four input fields: "Name" with the text "NewSwitch", "MAC Address" with the text "00-1E-3C-2E-47-F8", "IP Address" with the text "10.0.0.1", and "Device Type" with a dropdown menu showing "Switch". At the bottom right, there are two buttons: "Cancel" and "Save".

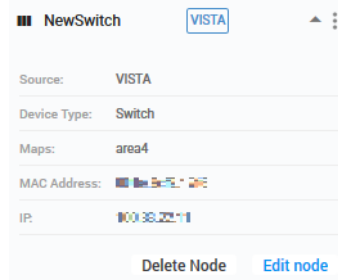
New static devices that have been created can be added to the map by dragging and dropping them from the side panel.



Static links can be made between devices by selecting one of them, and then clicking on the device you want to link it to.



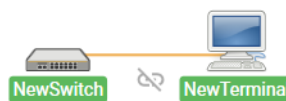
Static devices can be deleted from the side panel by selecting Delete Node,



or from the map by hovering over them and clicking the icon.



Static links can be deleted from the map by hovering over them and clicking the icon.



Service monitoring map

Applicable to all Vista Manager installations.

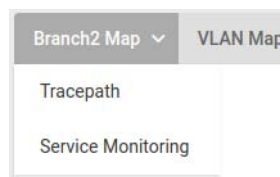
From Vista Manager EX version 3.0.0, the Service Monitoring map has been added. In this map, you can click on a node in the map, and configure services to be monitored. Service monitoring events (like a service going into a critical state) will be displayed on nodes in the map in the form of an alarm bell.

This allows convenient adding, editing, and deleting of monitored services on a node within the topology map. The monitoring provides visual notification when a service goes down on the map.

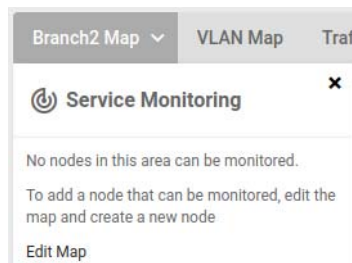
Note: This is a parallel feature to the service monitoring added to Vista Manager in 2.5.1. The service monitoring map does not replace the existing card-based service monitoring functionality.

Note: The service monitoring map only monitors user-created nodes that have been added through the Edit Map screen. It does not allow the monitoring of AMF nodes. These can still be monitored using the card-based service monitoring.

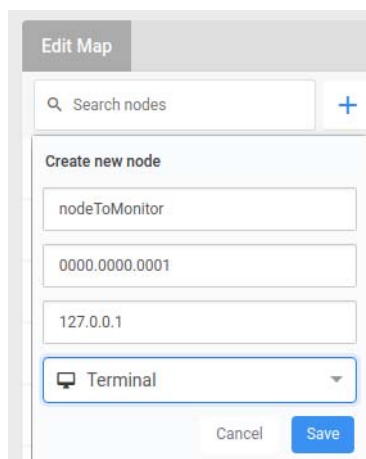
From the drop-down menu of the map, select Service Monitoring.



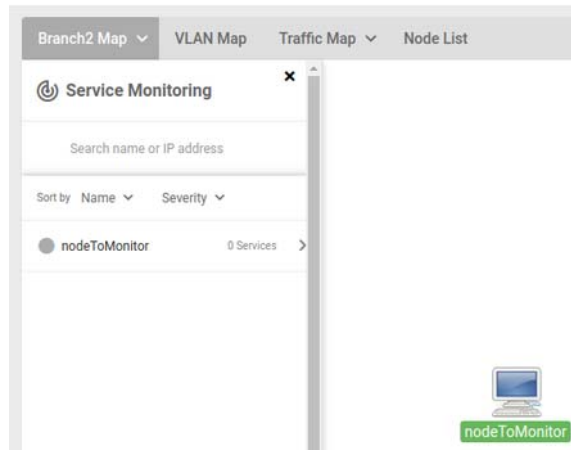
Service monitoring monitors user-created nodes. If there are no user-created nodes, you will see the following message.



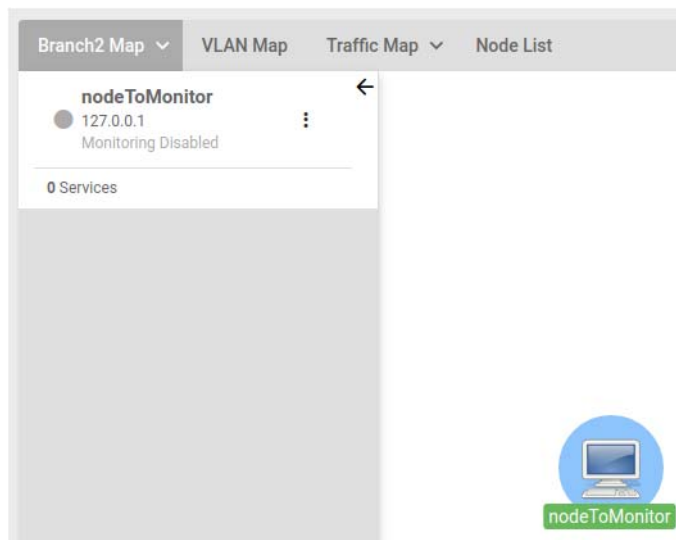
You can create a new node from the Edit Map screen.



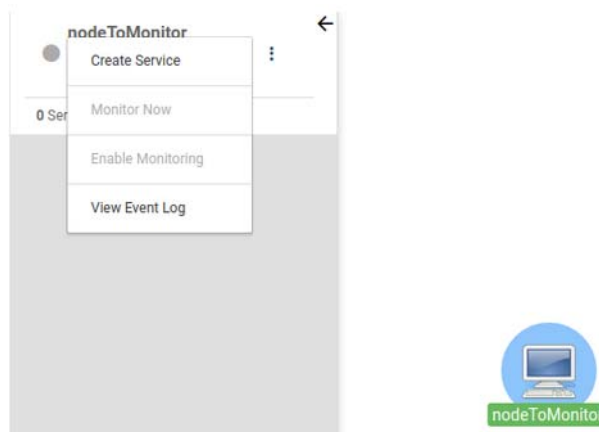
Created nodes will appear in the service monitoring node list.



To add a monitoring service to the node, click on it from the list or from the map. Initially, there will be no monitoring services on the node.

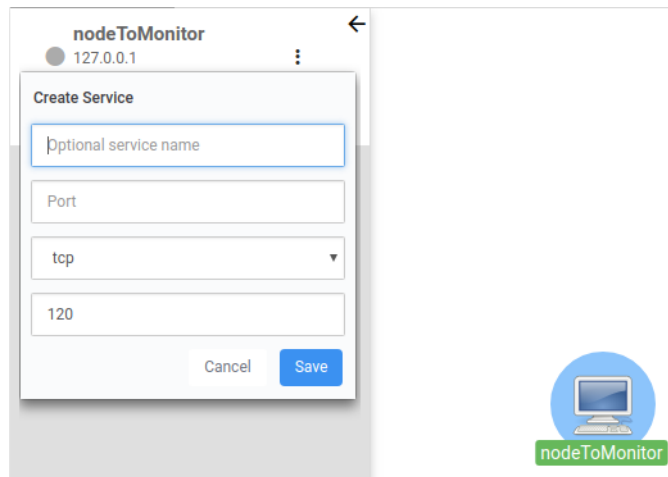


From the drop-down menu for the node, select Create Service.

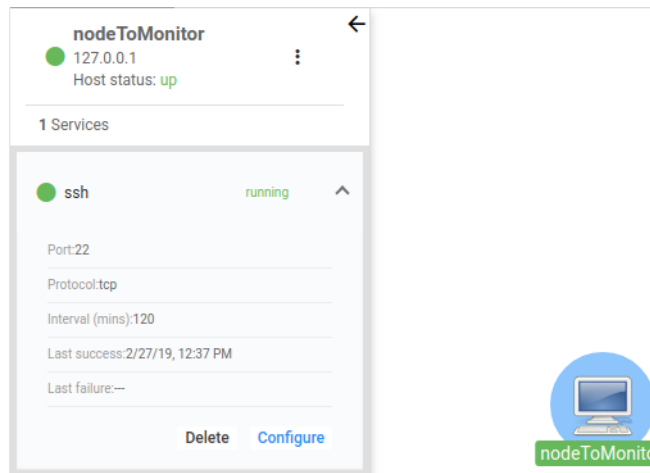


When creating the service, you need to provide the following fields:

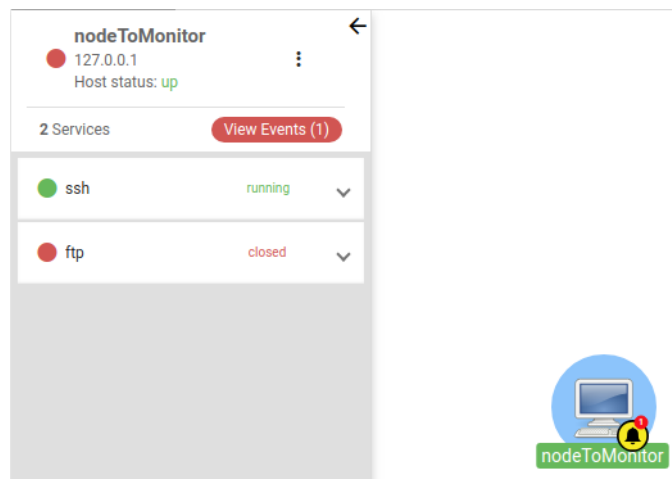
- A service name to identify the service (this is optional).
- The port that the service will monitor.
- The protocol that the service will monitor (either TCP or UDP).
- The time interval that determines how frequently monitoring will be performed.



Once the service has been configured, selecting the node will show the details of any monitoring services for that node.



Services in a critical state will show alarm bells on the map.



The service statuses may be one of the following:

- Pending: The service has not been monitored yet.
- Running: The service has responded to the latest monitoring probe.
- Filtered: Unable to determine the status of the service, because it is blocked by a network obstacle such as a firewall.
- Indeterminate: Unable to determine the status of the service. It may be blocked by a network obstacle, up, or down.
- Closed: No application is listening on the specified port.
- Unresponsive: A service exists on the port, but is not responding to probes.
- Unreachable: Unable to monitor the service, because the target IP address is unreachable.
- Error: Unable to monitor this service, because an error occurred while attempting to do so.

The status categories and the statuses that fall into each category are as follows:

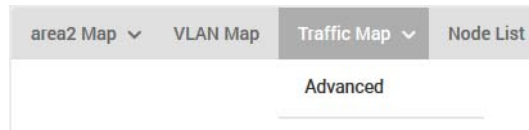
- Category Pending - Pending status
- Category Normal - Running status
- Category Unknown - Filtered and Indeterminate statuses
- Category Critical - Closed, Unresponsive, Unreachable, and Error statuses

Advanced traffic monitoring with sFlow

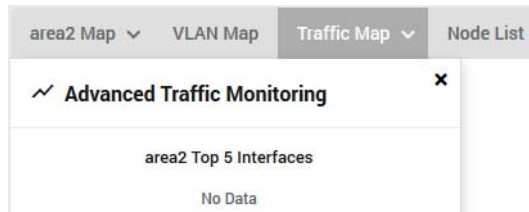
Applicable to all Vista Manager installations.

From Vista Manager EX version 3.0.0, you will be able to monitor traffic in your network using sFlow (sampled flow). After configuring sFlow on your network devices, you can use advanced traffic monitoring to view information about network traffic, protocols, and applications.

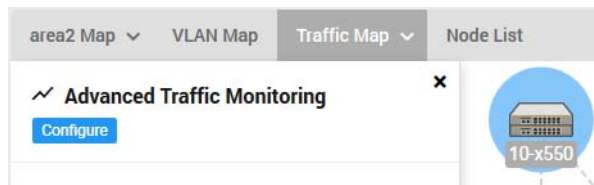
Advanced traffic monitoring can be accessed from the network map menu. Click on Traffic Map, then select Advanced.



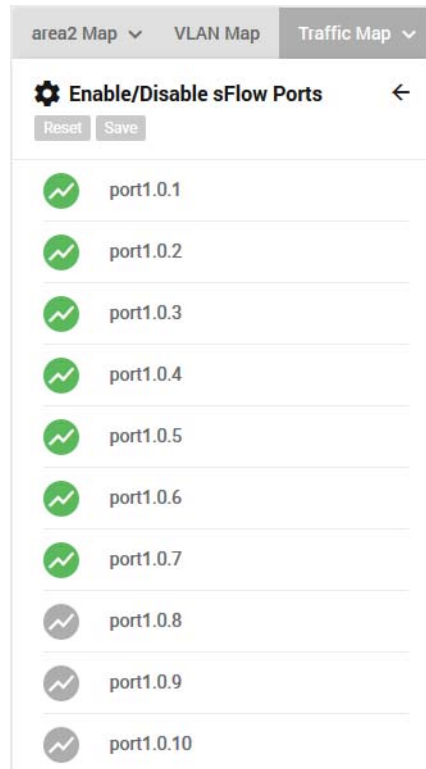
This will open the Advanced Traffic Monitoring sidebar. When you first open it, there will be no data, since you will not have configured any nodes for sFlow.



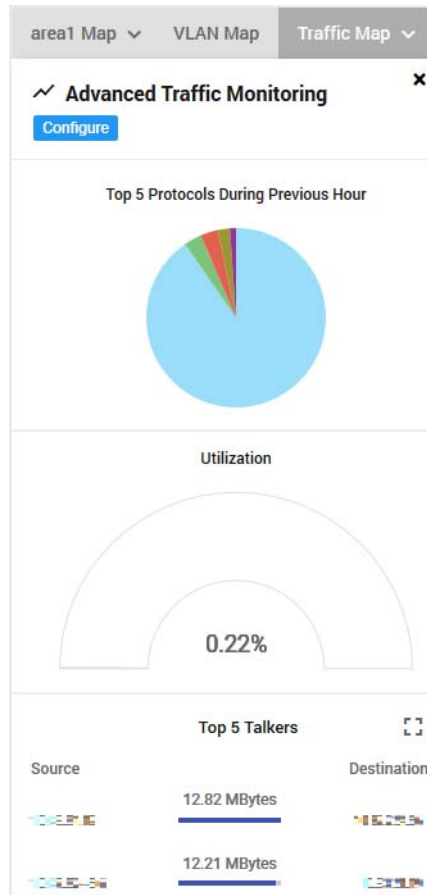
Select a node from your network map, and click on Configure to configure it.



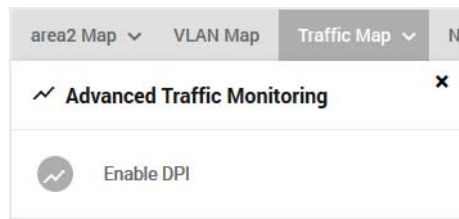
The side bar will show a list of the ports on the node. Click on a port to enable (green) or disable (gray) sFlow on the port. Click Save to make the changes.



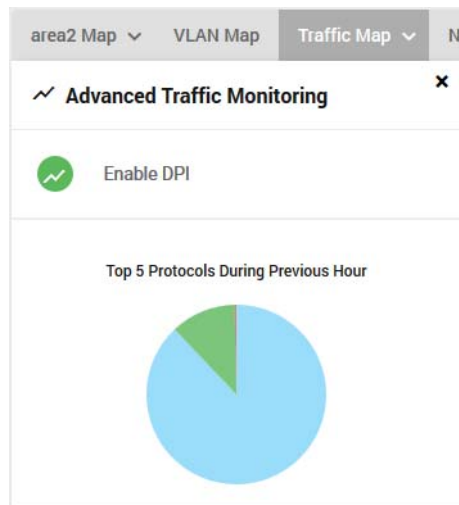
The side panel will then show monitoring output from the selected switch, including the protocols, utilizations, and talkers.



Routers do not support sFlow. However, by enabling DPI on a router, some traffic monitoring can be carried out. Click to enable DPI.

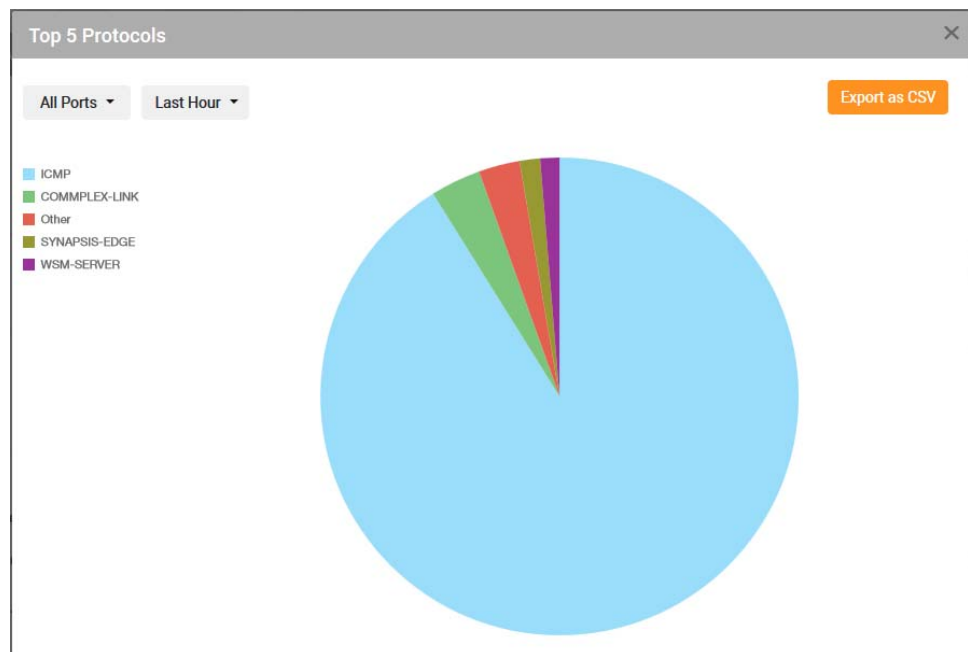


The side panel will show the protocols being used by the router.

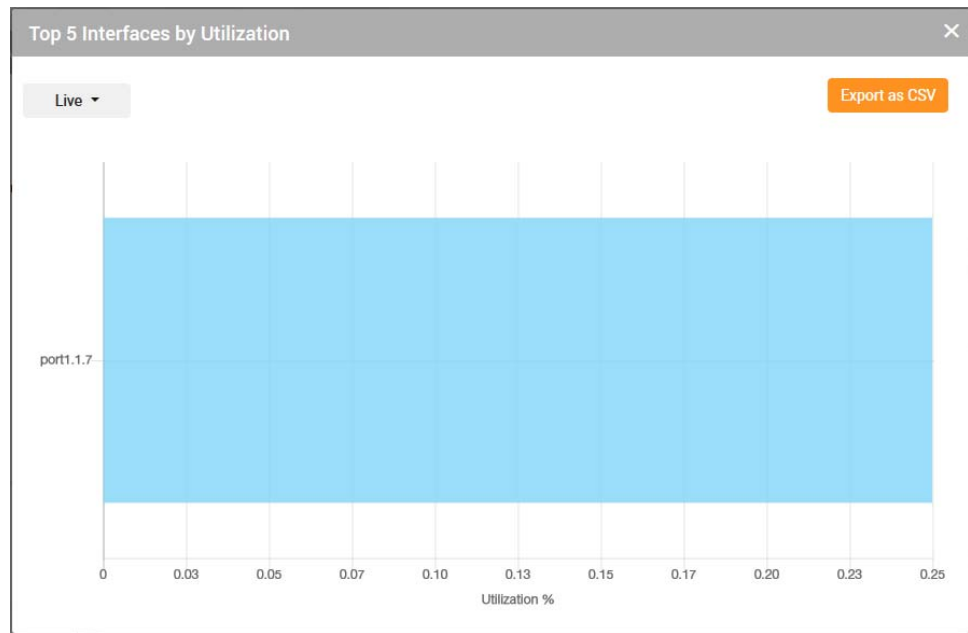


You can click on the items in the side panel to open the associated widget.

Top 5 Protocols:



Top 5 Interfaces by Utilization:



Top 5 Talkers:



Information from the widgets can also be exported to a CSV file. To do so, click on the Export as CSV button in the top right corner.

Note: Configuring devices for sFlow using Vista Manager requires the device to be running AlliedWare Plus version 5.4.8-2 or later. Devices running older releases are still compatible with this feature; however, the sFlow configuration will have to be done manually through the CLI.

Sample sFlow CLI configuration:

```
sflow agent ip 172.31.1.245
sflow collector ip 192.168.1.1
sflow enable
!
interface port1.1.1
sflow sampling-rate 8192
sflow polling-interval 60
```

Vista Manager uses the sFlow agent IP address to match the data received with the correct AMF device. The agent IP address must be the same as the AMF Management IP address. The IP address can be found using the **show atm detail** command.

Integrated topology map

Applicable to Windows-based Vista Manager installations with the AWC or SNMP plug-ins.

From Vista Manager EX version 3.0.0, the network map will include nodes from the AWC and SNMP plug-ins. This lets you visualize your networks in one integrated map.

This also means that:

- the Device Search allows you to search across all networks
- the Network Tree shows all networks and the devices associated with them
- User Management lets you set permissions for each network's map
- the network name displayed on the dashboard and network map can be edited in the System Management page
- the side panel will display node details when a node from any network is selected on the map

Note: The current implementation of the integrated topology map does not show links between AMF and plug-in networks.

Client locus on AWC floor map

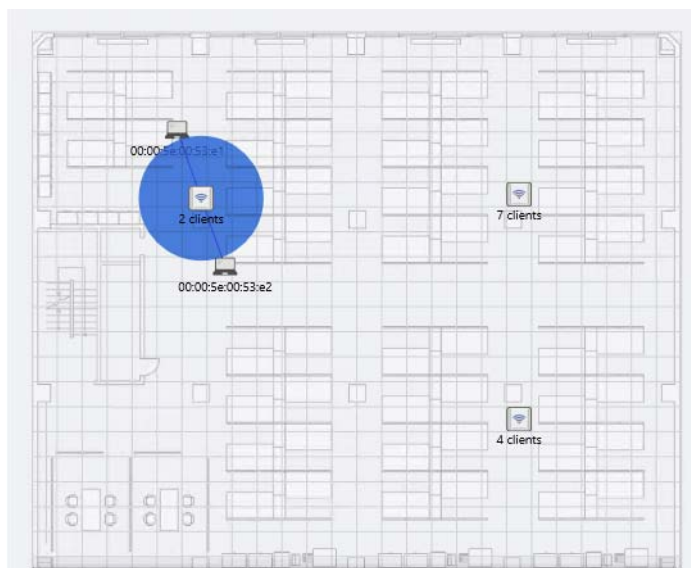
Applicable to Windows-based Vista Manager installations with the AWC plug-in.

From Vista Manager EX version 3.0.0, the AWC plug-in lets you visualize the movement of a wireless client between APs on your floor map. You can filter by device and time period, and see the connections the client has made on your map.

From the AWC Plug-in menu, select Wireless Monitoring, then Floor Map. Select the floor map, click on View Details, then click on Associated Client view. This displays the associated clients.

Select the Associated Client History view checkbox to display the filters. This allows you to specify a date range, as well as the maximum trace count. Click on Search to filter the list of clients by these criteria.

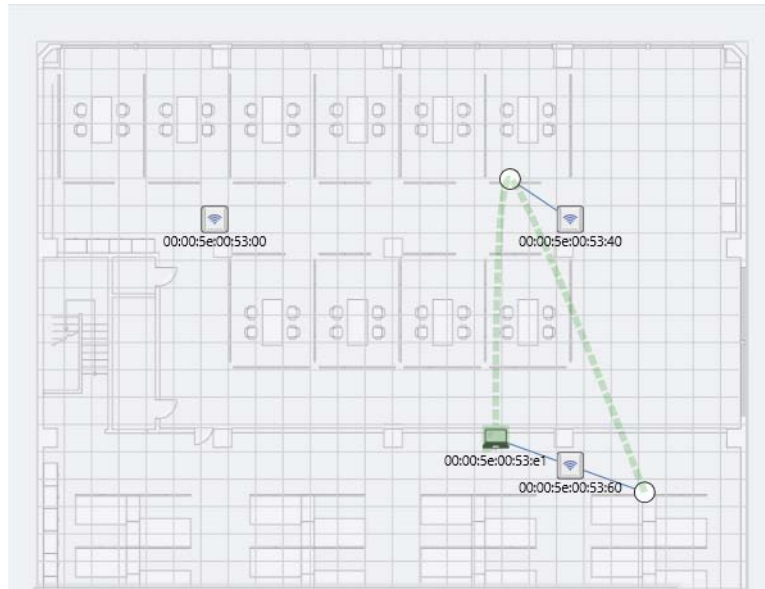
While the filter is on, the floor map displays the MAC address of the AP and clients.



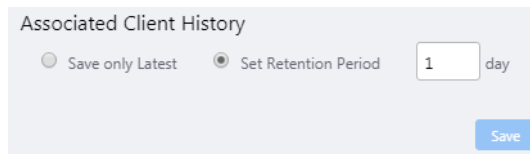
You can select a particular client from the filtered list to focus on its history.

<input type="checkbox"/>	MAC Address	Hops
<input checked="" type="checkbox"/>	00:00:00:00:00:02	2
<input type="checkbox"/>	88:88:88:88:88:88	0
<input type="checkbox"/>	99:99:99:99:99:99	55

You can then visualize the movement history of that client on your floor map.



The retention period can be set in the AWC plug-in System Settings. You can choose to save only the latest, or set a specific number of days to retain the data.



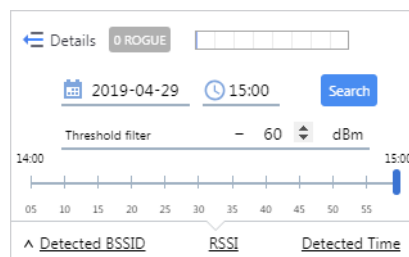
Rogue AP history

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

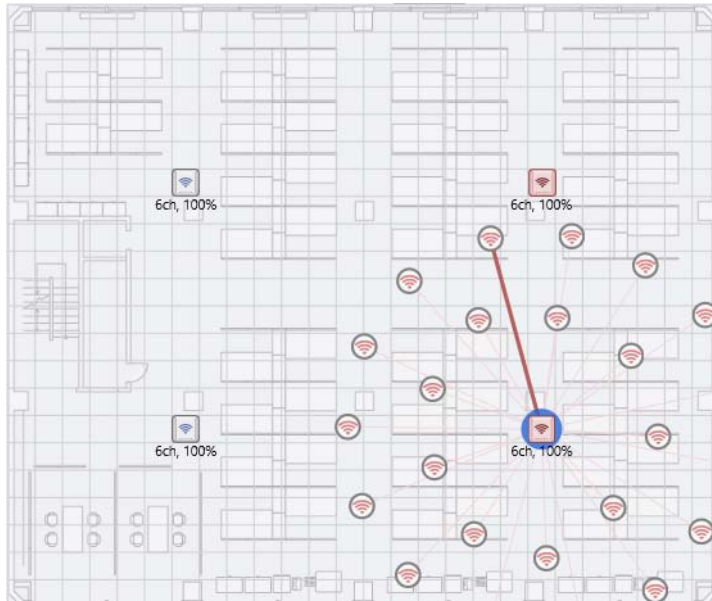
From Vista Manager EX version 3.0.0, you can view the history of any rogue APs from the floor map.

From the AWC Plug-in menu, select Wireless Monitoring, then Floor Map. Select the floor map, click on View Details, then click on Rogue view. This displays the details of any rogue APs, including the detected BSSID, the RSSI, and the Detected Time. You can also click on Details to get an expanded view of the rogue AP details. This includes the SSID, Channel, Detecting AP, and Rogue Reason.

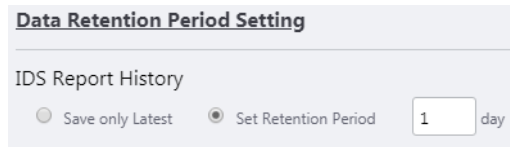
You can filter the results that are shown by date, time, and threshold signal reception strength.



The floor map will show the locations and details of any rogue APs that match the filters you have selected. Clicking on the rogue AP on the map will highlight the corresponding BSSID line in the list.



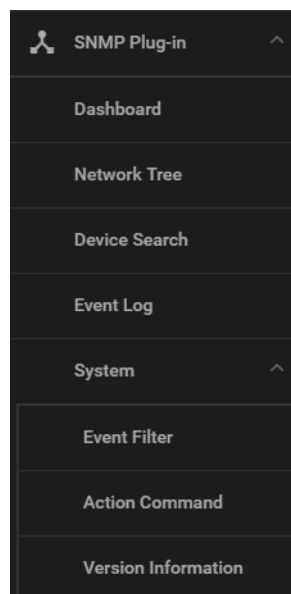
The retention period can be set in the AWC plug-in System Settings. You can choose to save only the latest, or set a specific number of days to retain the data.



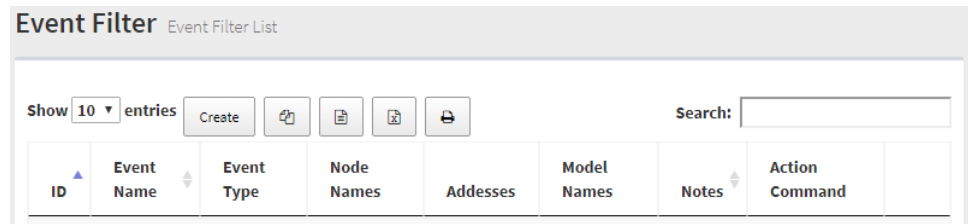
Action commands and event filters in GUI

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

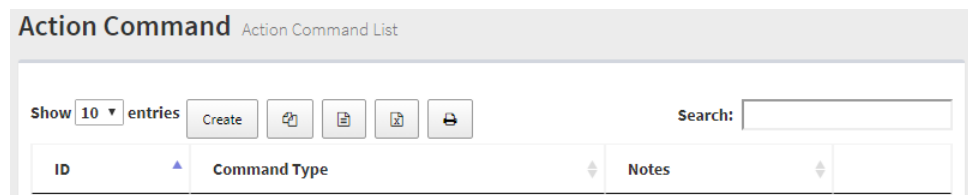
From Vista Manager EX version 3.0.0, you can view event filters and action commands in the GUI. Menu items for these have been added to the SNMP plug-in menu.



The GUI replicates the functionality of the applications. The event filter screen lets you view and search the event filters. You can also create new event filters, export them to the clipboard, CSV, or Excel, or print them.



Similarly, the action command screen allows the same functionality for action commands.



Third party polling interval

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

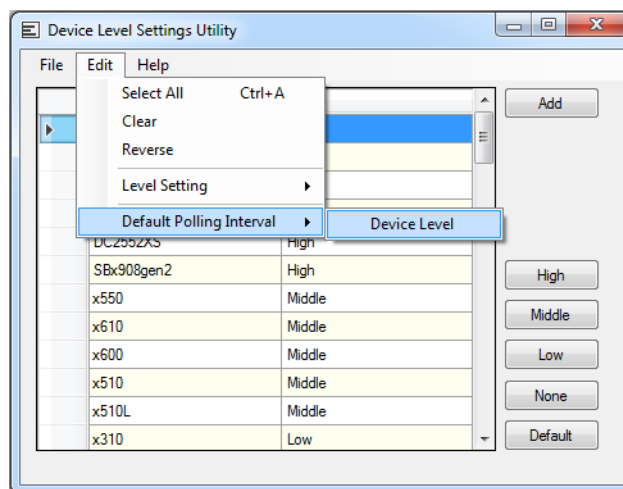
From Vista Manager EX version 3.0.0, you can configure the polling interval for managed devices. The polling interval can be set for a new device on the Create Device page, or for an existing device on the Update Device page.

The polling interval can be set to auto-detect, or manually set to a specific number.

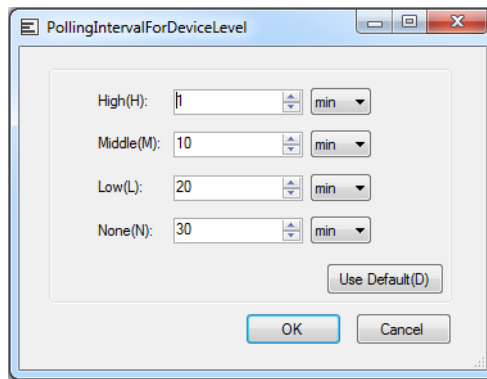


The polling interval can be seen on the Device Detail page for the device.

You can also use the Device Level Settings Utility to set the polling interval by device level. To access the settings, select Edit/Default Polling Interval/Device Level.



From there, you can set the polling interval for each of the different device levels.



Manual fiber monitoring alarm dismissal

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

From Vista Manager EX version 3.0.0, when SNMP reports a critical fiber monitoring alarm, the administrator must manually dismiss the alarm, even if it has automatically recovered.

New platform support

Support has been added for the following devices:

- x950-28XTQm
- x530-52GPXm
- x530-52GTXm
- x530L-28GPX
- x530L-52GPX
- x530L-28GTX
- x530L-52GTX
- GS980M/52
- GS980M/52PS
- GS980MX/28
- GS980MX/28PSm
- GS980MX/52
- GS980MX/52PSm
- TQm1402
- TQ1402
- TQ5403e
- IE340-20GP
- AR1050V
- IS230-10GP (SNMP only)

Support has been added for the following operating systems:

- Windows Server 2019
 - ◀ Standard
 - ◀ Datacenter
 - ◀ Essentials

Important Considerations Before Upgrading

This section describes changes since Vista Manager EX v3.0.0 that may affect your network behavior if you upgrade. Please read it carefully before upgrading.

AMF software version compatibility

- All AMF nodes must run version 5.4.7-0.1 or later.
- If your AMF Master node is running 5.4.7-0.x, then all other nodes must also run 5.4.7-0.x (not a later release).
- If **any** of your Controller or Area Master nodes are running 5.4.7-1.1 or later, then they **all** must run 5.4.7-1.1 or later.
- If your AMF Master node is running 5.4.7-2.x or later, then member nodes can run 5.4.7-0.x or 5.4.7-1.x, although we recommend that all nodes in an AMF network run the same software version.

Wireless AP software version compatibility

- TQ5403 APs with firmware version 5.0.x
- TQ4x00/3x00/2450 APs with firmware version 4.2.x
- MWS series AP with firmware version 2.2.5

Virtualization Support

The Vista Manager 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 only available on Windows-based Vista Manager installations. Plug-ins are not available on Vista Manager virtual appliances.

Vista Manager backup compatibility

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 3.0.0 into a Vista Manager 2.5.0 installation.

Vista Manager and RMON

When Vista Manager connects to an AlliedWare Plus network, it automatically enables the RMON (Remote Network Monitoring) commands on each ATMf interface port that it finds. This is done for the purpose of collecting traffic statistics. It does this by modifying the running config on all switchports that interconnect AMF devices (including LAGs). No notification is shown that these changes are being made.

Caution If the **copy run start** or **wr** commands are run on one of these devices, these config changes will be made permanent.

Information After Upgrading

This section lists the steps to take after upgrading Vista Manager EX. It also includes troubleshooting tips should you experience any problems with the upgrade process.

Clear browser cache

Applicable to all Vista Manager installations.

Clear your browser's cache after upgrading your Vista Manager EX installation. Incomplete dialog boxes, incorrectly populated drop-down lists, and truncated forms are all symptoms of a caching problem.

Remove and reinstall Vista Manager

Applicable to Windows-based Vista Manager installations with or without the SNMP and AWC plug-ins.

If you see an error message during the upgrade process, or experience database errors after installation, try a fresh install of Vista Manager EX.

- First, ensure your Vista Manager EX and plug-in's backups are in a secure location.
- Remove Vista Manager EX, and any installed plug-ins, using the Windows "Programs and Features" utility.
- Re-install Vista Manager EX.
- Restore your backups.

See upgrading "[Upgrading Vista Manager as a Windows-based installation](#)" on page 32 for information on making backups, installing, and restoring Vista Manager EX.

De-register the AWC plug-in on large wireless networks

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

Individual APs may disappear from the AWC plug-in if the plug-in is managing a large wireless network (approximately 600 APs or more). If this occurs, de-register the AWC plug-in from the Vista Manager's **System Management** -> **Plug-in Management** page. Features such as licensing, auto-recovery, and importing an AP from a guest node will still work, even if the plug-in is not registered.

Secure client access and disabling HTTPS

Applicable to all Vista Manager installations.

When HTTPS is enabled in Vista, the user's browser receives a Strict-Transport-Security header as is recommended for a secure client to server environment. If the user elects to disable HTTPS in Vista, their browser is likely to continue to use HTTPS to access that site, despite the user specifying an HTTP URL in the address bar.

This setting is local to the browser, and users are advised to consult their browser documentation on how to reset the HSTS security settings for a target site. Other quick workarounds are to use an incognito or private browser tab, or to use a different browser.

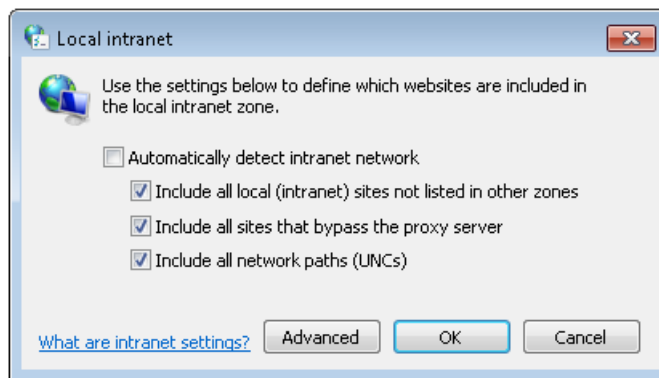
Microsoft Edge support

Applicable to all Vista Manager installations.

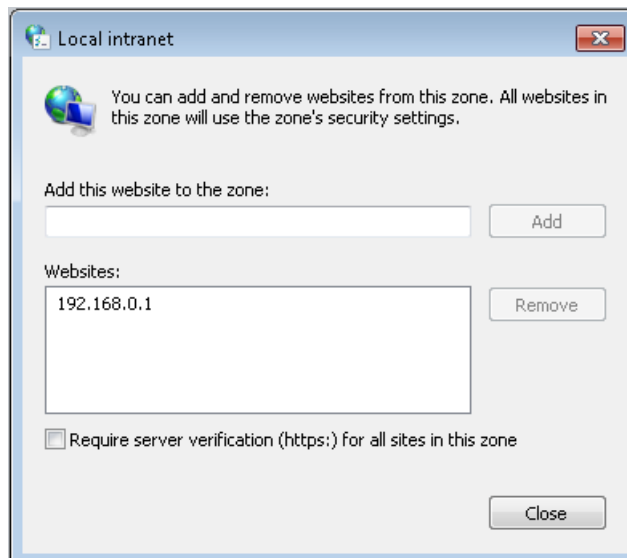
Security in Microsoft Edge may prevent you from navigating to Vista Manager using an IP address. We recommend that rather than using the IP address, you use DNS and a FQDN for Vista Manager.

If this is not possible, you can configure Microsoft Edge to allow communication with Vista Manager by doing the following:

1. In the Control Panel, open Internet Options. Click on the Security tab. Select Local Intranet, then click on Sites.
2. Set the following checkboxes:



3. Click on Advanced. In the Add this website to the zone text field, enter the IP address of Vista Manager, then click on Add. Once it has been added, click on Close.



Note: Adding sites to your local intranet settings is a potential security risk. Before making these changes, ensure that the site is secure, and that you are aware of the security issues. If these risks are unacceptable, we recommend using a different browser.

Obtaining User Documentation

Vista Manager documentation An Installation and User Guide for Vista Manager EX is available from the Allied Telesis website, [Vista Manager EX Installation and User Guide](#).

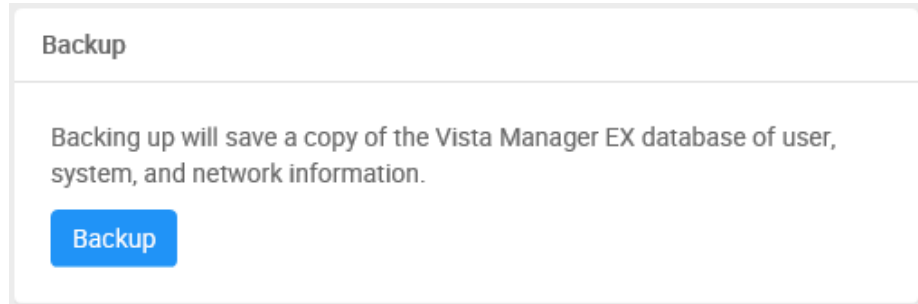
AMF documentation For full AlliedWare Plus documentation, see our online documentation library. For Vista Manager, the library includes the following documents:

- the [AMF Feature Overview and Configuration Guide](#).
- the [AMF Datasheet](#).
- the [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.



2. Download the software files for Vista Manager EX v3.0.2 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 and User Guide 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.

[upload existing profile backup](#)

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 'atvmexXXXbXXw.exe', with the Xs denoting the version and build numbers.
 - The AWC plug-in is called 'atawcXXXbXXw.exe'.
 - The SNMP plug-in is called 'atsnmpXXXbXXw.exe'.

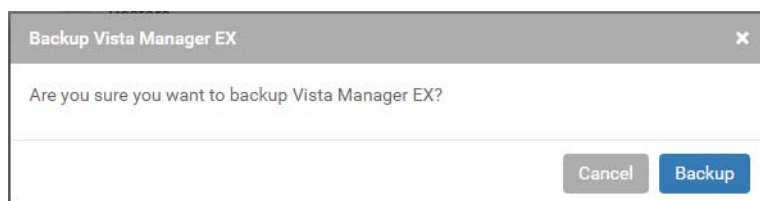
Do not rename these files. The installation requires them to be in this format.

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 Backup Pane.
5. Click Backup again to confirm you wish to make a backup.



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\svr cmd.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.

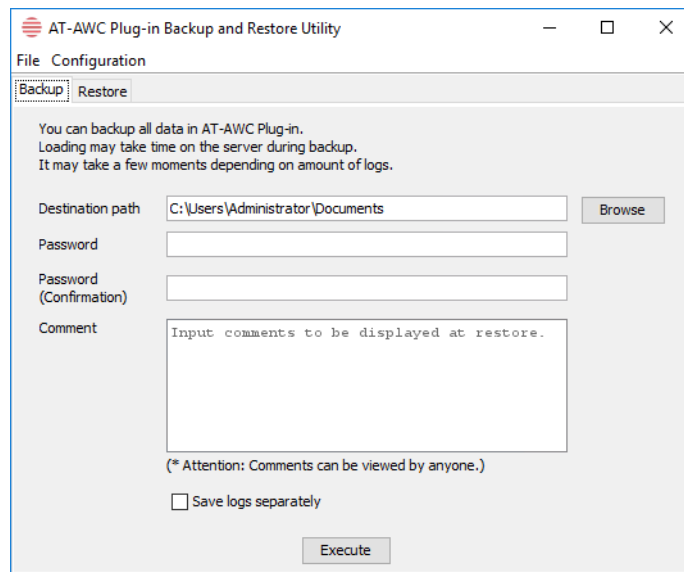
Backup the AWC plug-in

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"



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

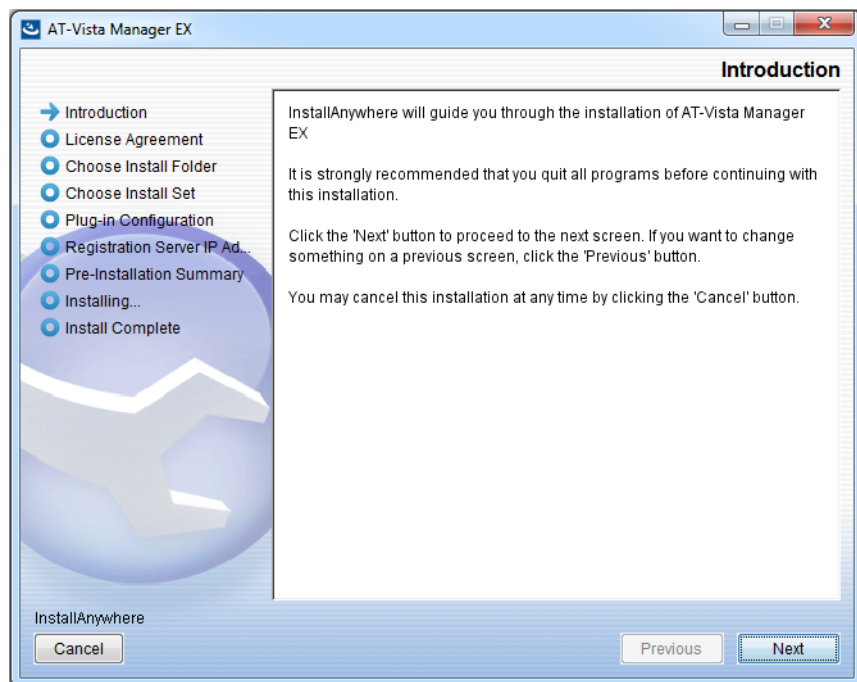
21. Execute the Vista Manager EX installation program 'atvmexXXXbXXw.exe'. This opens the following **AT-Vista Manager EX** dialog:



- Select the language from the drop down list
- Click **OK**

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

22. The **Introduction** dialog displays:



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

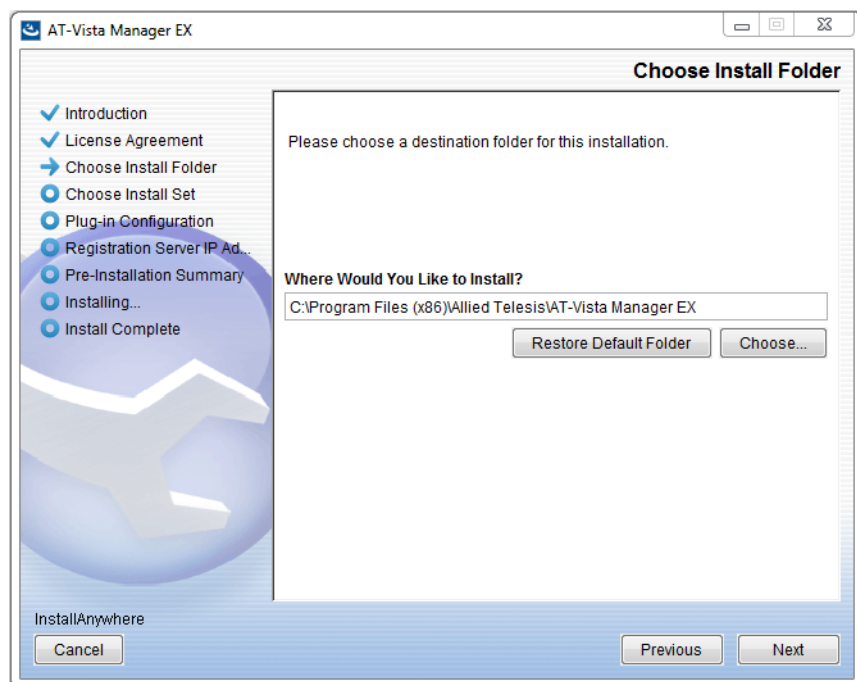
23. The **License Agreement** dialog displays:



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

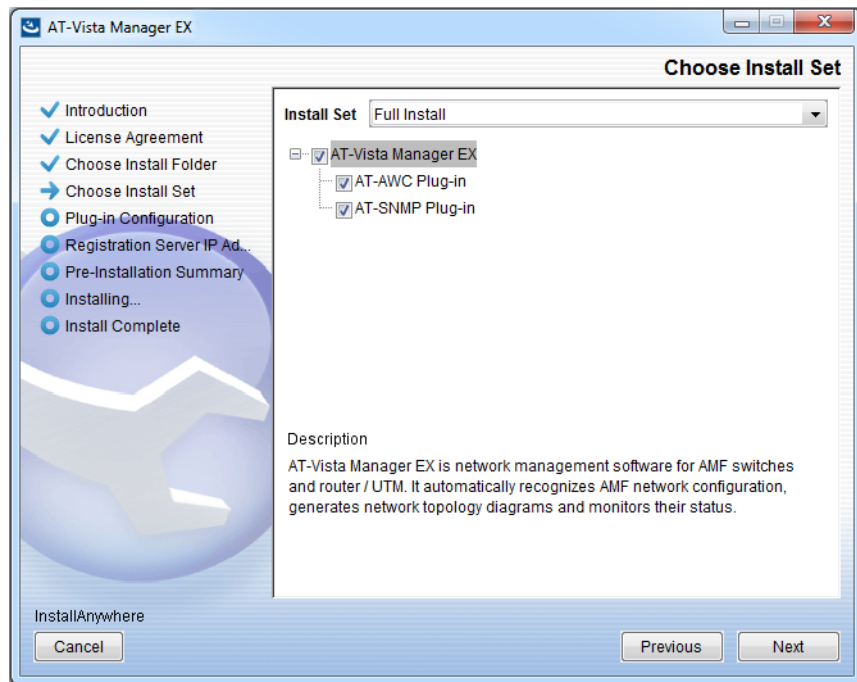
- Click **I accept the terms of the License Agreement**
- Click **Next**

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



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

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



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:



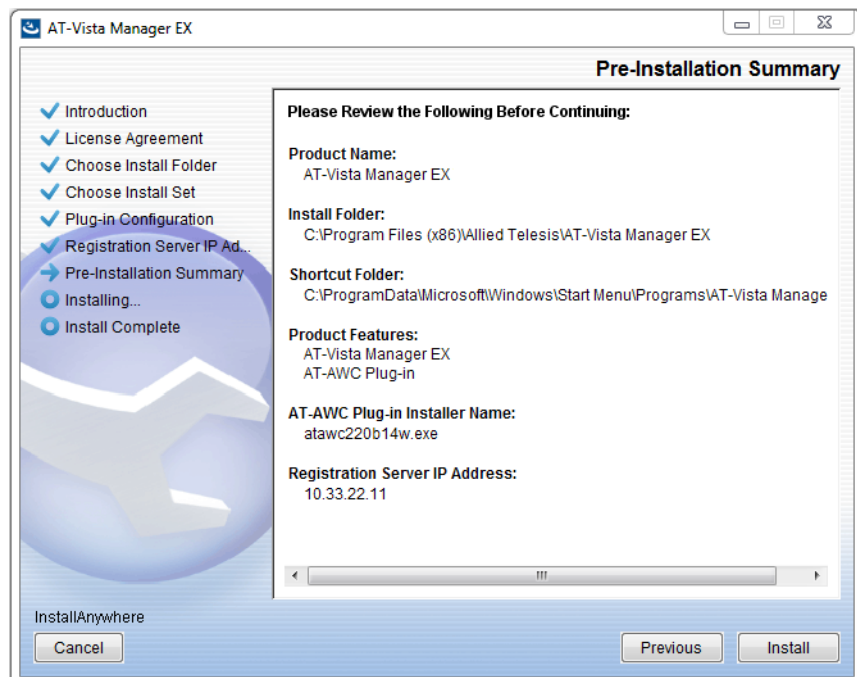
Select **Do not create a public key** unless you are intending to use the plug-ins in standalone mode. For more information on standalone mode, refer to the Installation Guide. Click **Next**.

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



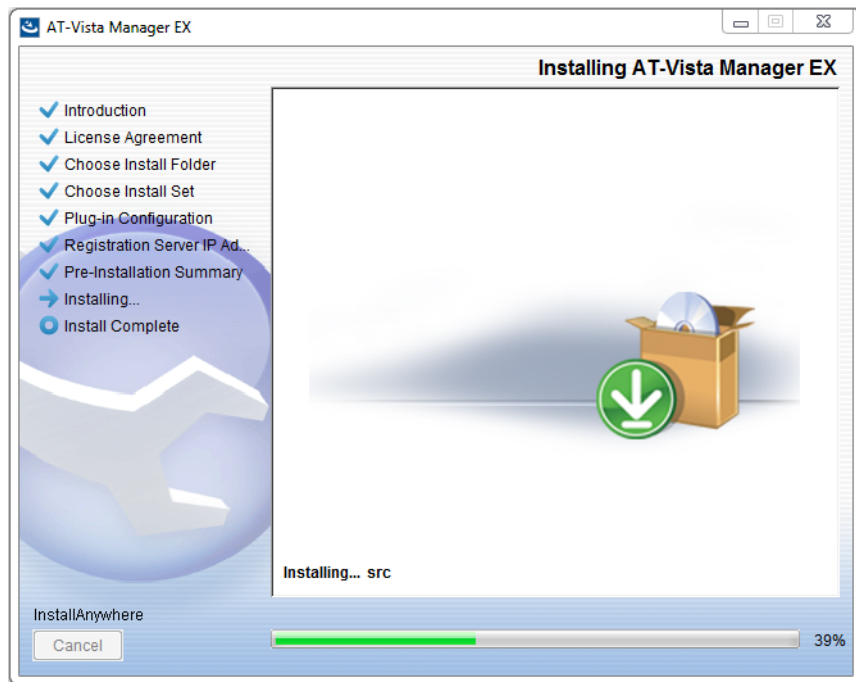
Either select from the list of IP addresses already configured on the Windows machine, or input a valid IP address. Click **Next**.

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

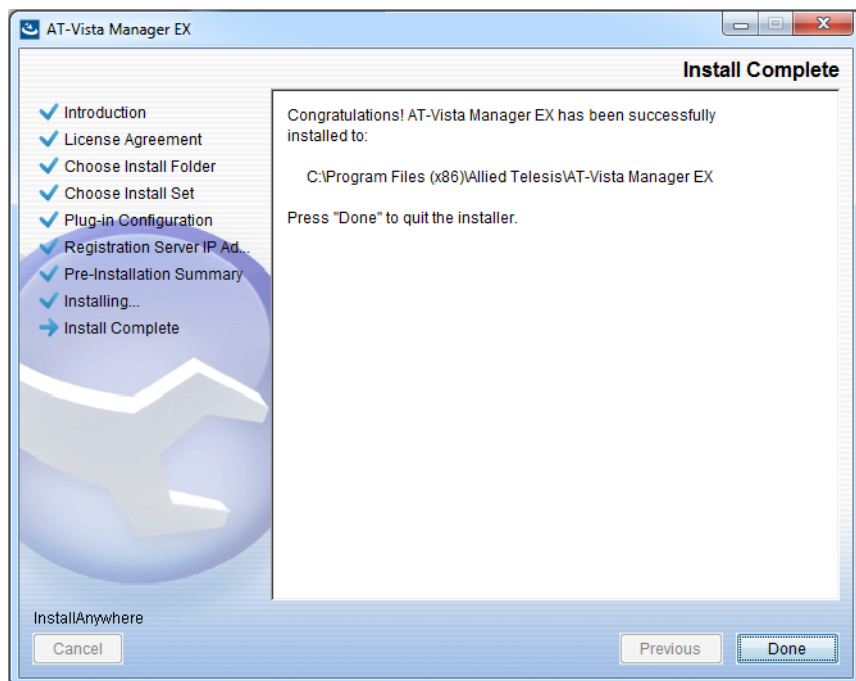


Check that your Product Name, Install Folder, Shortcut Folder, Product Features, Plugin Installer Name and Registration IP Address are correct, and then click **Install**.

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



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



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

Register the plug-ins

After the upgrade is complete, if you are using the AWC or SNMP plug-ins, you need to register them with Vista Manager. To do this, use the following procedure.

31. Log on to Vista Manager. From the menu, select System Management, then click on the Manage Plug-ins button.
32. Under the list of plug-ins on the left, select the plug-in. Click on the Edit button.

Plug-ins
SNMP Plug-in
AWC Plug-in

33. In the Server URL field, enter the URL. For the AWC plug-in, use the following URL:
https://localhost:5443/wireless_plugin
For SNMP plug-in, use the following URL:
https://localhost:6443/netmanager
34. Click on the Verify Connection button. Once you have verified that the certificate fingerprint is correct, click on the Save button.
35. If you have both plug-ins installed, repeat this process for the other plug-in.

Restoring Vista Manager EX

If you need to restore Vista Manager EX or any of plug-ins' data, use the appropriate procedure.

Restore Vista Manager EX

1. Log on to your Vista Manager EX and select the System Management page.
2. Click on the Restore button in the Restore Pane.
3. Select the appropriate tar file and restore.

Restore the SNMP plug-in

4. If you have the SNMP plug-in installed then log on locally to the Vista Manager EX server.
5. Stop the SNMP server services using the shortcut or by running the following command line.
"<Vista Install Path>\Plugins\AT-SNMP\NetManager\bin\svr cmd.bat" svrstop
6. 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

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

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

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

9. 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"
```

10. Select the restore tab on the dialog 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**