

Release Note for Vista Manager EX v3.1



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 v3.1.0	4
Introduction.....	4
New Features and Enhancements.....	4
Important Considerations Before Upgrading	20
Information After Upgrading	21
Obtaining User Documentation	23
Upgrading Vista Manager as a virtual appliance.....	24
Upgrading Vista Manager as a Windows-based installation	25
Restoring Vista Manager EX	32

What's New in Vista Manager EX v3.1.0

Introduction

This release note describes the new features in Vista Manager EX™ v3.1.0. 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 v3.1.0.

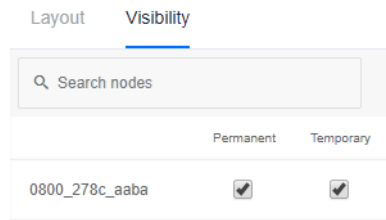
SD-WAN

Applicable to all Vista Manager installations.

From Vista Manager EX version 3.1.0, you will be able to manage your SD-WAN network from the Vista Manager GUI. This allows you to visualize the configuration of your WAN with a topology map. This also lets you carry out link monitoring, health monitoring, and probe configuration.

For more information about configuring and using the SD-WAN plug-in, refer to the “Using the SD-WAN Feature” chapter in the [Vista Manager Installation and User Guide](#).

Static icon map support



Applicable to all Vista Manager installations.

From Vista Manager EX version 3.1.0, you will be able to change which nodes are visible on the network map. For example, you may only be interested in seeing servers on the network map, and can therefore hide the other nodes.

As an administrative user, you will be able to modify the default view of the map. You can temporarily or permanently hide nodes. Temporarily hidden nodes will be hidden for your session, but will return when you log back in. Permanently hidden nodes will be hidden for all users until you choose to show them again.

As a user, you will only be able to temporarily hide nodes that you are not interested in seeing. They will remain hidden while you are logged in, but if you log back in, the map will return to the default view set by the administrator.

To change the visibility of nodes, click on Edit Map on the network map screen. Click on the Visibility tab to show a list of nodes.

- Nodes with the Permanent checkbox checked will be visible to all users when they log in.
- Nodes with the Permanent checkbox unchecked will be hidden.

Note: Only administrative users can change the Permanent status of a node.

- A user can check the Temporary checkbox, making that node visible during their session.
- A user can uncheck the Temporary checkbox, making that node hidden during their session.

Note: Any user can change the Temporary status of a node during their session.

Changes to the Permanent status of a node are persistent. Changes to the Temporary status only persist for the session.

Note: The visibility of base nodes cannot be changed. Therefore, on an AMF network, AMF nodes will always be visible and cannot be hidden. Likewise, if the network is a plug-in view, then the plug-in nodes will always be visible.

Inventory

Applicable to all Vista Manager installations.

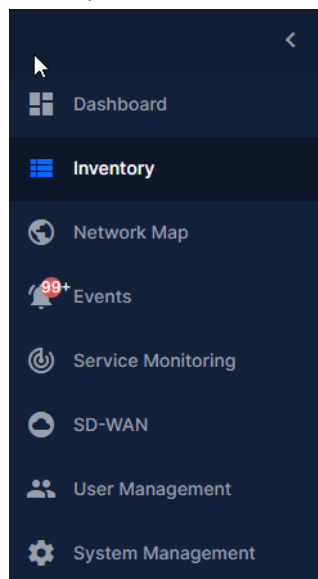
From Vista Manager EX version 3.1.0, you will be able to more easily manage the assets in your network. The inventory is made up of several components.

- Device discovery - devices on the network are discovered via AMF and plug-ins.
- Device classification - during discovery, a best effort is made to categorize what type of device has been discovered. However, this may be incorrect, so it allows you to specify what type of device has actually been discovered.
- Device management - once discovery is complete, the asset information should be available to you.

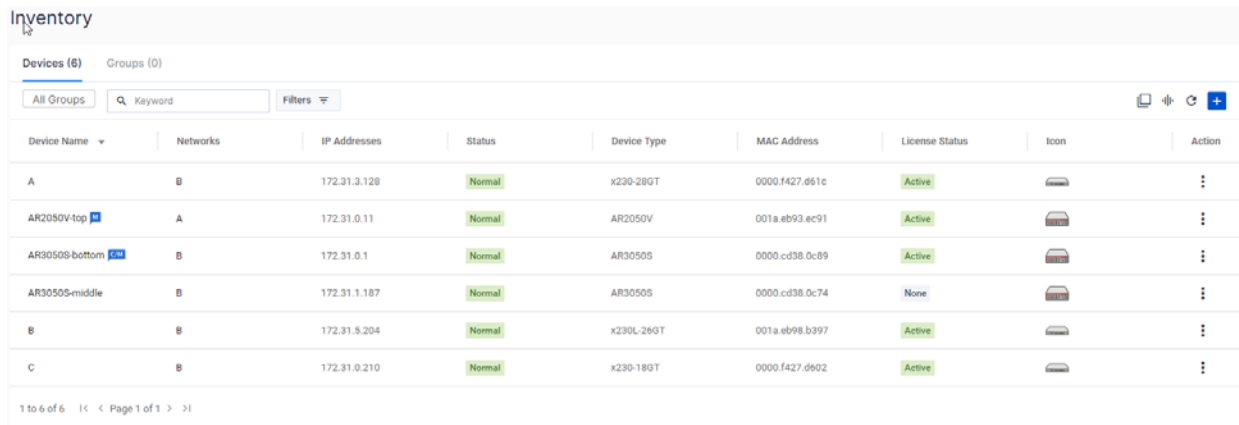
You can use the inventory to:

- get a complete list of all assets on your network.
- display the assets on the integrated map, and select the most relevant icon for each device.
- view the license information for all Allied Ware Plus devices.
- be notified when a license is about to expire or has recently expired.
- create a group defined by either IP/MAC address range or Vendor, and assign an icon to this group.
- filter the list of assets, and print/export this list.

Inventory is accessed from the sidebar menu by selecting the Inventory menu item.



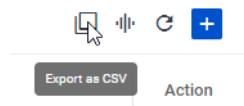
The Inventory screen shows you the details of the items in your network. It also allows you to search for particular devices.



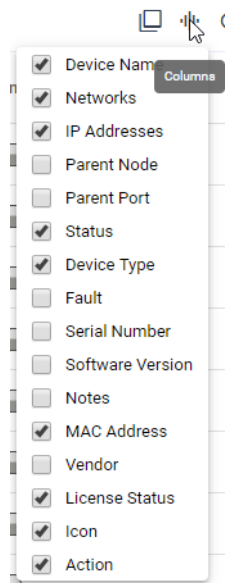
The screenshot shows the 'Inventory' screen with a table of 6 devices. The table has columns for Device Name, Networks, IP Addresses, Status, Device Type, MAC Address, License Status, Icon, and Action. The devices listed are A, AR2050V-top, AR3050S-bottom, AR3050S-middle, B, and C.

Device Name	Networks	IP Addresses	Status	Device Type	MAC Address	License Status	Icon	Action
A	B	172.31.3.128	Normal	x230-28GT	0000.f427.d61c	Active		
AR2050V-top	A	172.31.0.11	Normal	AR2050V	001a.eb93.ec91	Active		
AR3050S-bottom	B	172.31.0.1	Normal	AR3050S	0000.cd38.0c89	Active		
AR3050S-middle	B	172.31.1.187	Normal	AR3050S	0000.cd38.0c74	None		
B	B	172.31.5.204	Normal	x230L-28GT	001a.eb98.b397	Active		
C	B	172.31.0.210	Normal	x230-18GT	0000.f427.d602	Active		

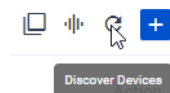
The list of assets can be downloaded as a CSV file by clicking on the Export as CSV button.



The columns that are shown can be changed by clicking on the Columns button.

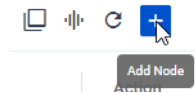


You can discover devices from the Inventory screen. By clicking on Discover Devices, Vista Manager will use ARP to discover any new devices, and return a list to you. A message will appear indicating the number of new devices found.



Discover device will only discover IPv4 neighbors. Any detected devices will not automatically appear on the map, but will require you to add them manually once they have been discovered. The detected devices will not provide link information, but you can manually add the links. Detected devices that fall into a user defined inventory group will inherit the assigned custom icon.

You can add a new node by clicking on the Add Node button.



You will be prompted to name the node, as well as specify the MAC address and IP address. You can also select an icon to represent the node.

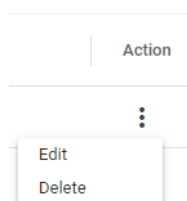
A screenshot of a 'Create Node' dialog box. It has a title bar 'Create Node'. Below the title bar are three input fields: 'Name' with a placeholder 'Node Name' and a lock icon, 'MAC Address' with a placeholder 'MAC Address', and 'IP Address' with a placeholder 'IP Address'. Below these fields is a section titled 'Select Custom Icons' with four icons representing different device types (server, storage, laptop, server rack) and a plus sign. At the bottom of the dialog are two buttons: 'Cancel' and 'Save'.

If you click on the Plus button, you can choose to upload a custom icon for the node. The custom icon dialog supports SVG, JPG, and PNG image files. Only administrators have the permission to upload and change custom icons.

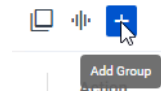
A screenshot of an 'Add Custom Icon' dialog box. The title bar contains 'Add Custom Icon' and 'Upload Image'. The main area is a large, empty light gray rectangle. At the bottom right of the dialog is a 'Cancel' button.

Note: AMF nodes cannot have their default icon changed.

You can also edit existing nodes, changing their properties and assigning them a different icon. Nodes can also be deleted from the inventory. To edit or delete a node, click on the appropriate menu item in the Action column.



The inventory also allows you to create groups to organize your inventory. To create a group, click on the Groups tab, and then click on the Add Group button.



You will be prompted to name the group. You can also specify which nodes will be added to the group. You can specify a MAC address range, an IP address range, a vendor, or a combination of these. You can also select an icon to represent the group.

Add Group

Name

MAC Address

IP Range Start:

IP Range End:

Vendor

Select Custom Icons

Once the group has been created, you can use it to view the details of the members of that group, as well as export that information to CSV. New devices that are discovered and meet the group's criteria will automatically be added to the group.

Inventory

Devices (41) **Groups (1)**

Group Name	Members	MAC Address	IP Range	Vendor	Icon	Action
Group 1	8 Nodes		172.31.0.0 - 172.31.0.255			

1 to 1 of 1 |< < Page 1 of 1 > >|

Increased VAPs for channel blanket

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

From Vista Manager EX version 3.1.0, the AWC plug-in lets you create up to three channel blanket virtual access points (VAP) for each radio, for a total of six. Previously, each radio supported two VAPs, for a total of four.

Improvements to the AWC floor map

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

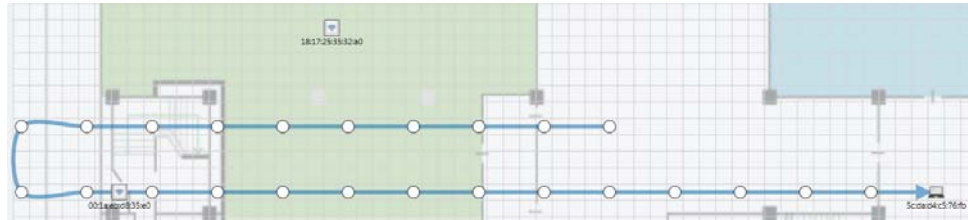
From Vista Manager EX version 3.1.0, the AWC plug-in now adds new functionality to the floor maps. You can now see the calculated location for clients on the floor map, you can draw custom areas on the floor map, and you can add a client definition to clients on the map.

Client location

The AWC plug-in now displays the associated icon of a client on the floor map based on the calculated location. Previously, the location was generated randomly on the map, but with this version, the Wireless Status View will now show the calculated location.

The location calculation runs as a background process, and the location is polled once every minute.

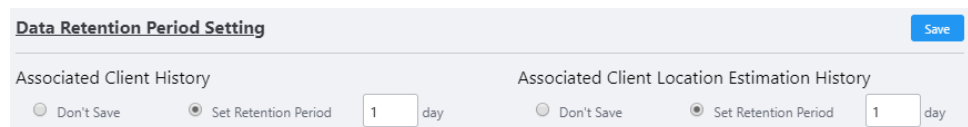
Displaying the client icon based on the calculated location is also available when Associated Client History View is enabled. When it is enabled, all locations for the client are also calculated, and an arrow is drawn showing client history.



If the location cannot be determined, either because the location calculation fails, there is no location data in the database, or the calculation engine has stopped, then the client will be displayed randomly as before.

Note: In order to enable this functionality, the following settings must be enabled:

- In System setting on the AWC Plug-in menu, in the Data Retention Period Setting section, Associated Client History and Associated Client Location Estimation History must both be enabled and set.



- AWC-CB and SyncScan must be enabled on APs.

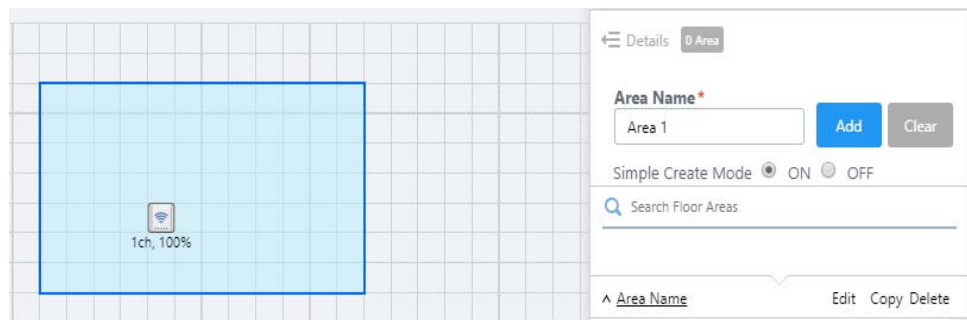
Drawing an area

You can also draw an area and name it on the floor map. Combined with the client location, this allows you to identify if a client is located in the specific area.

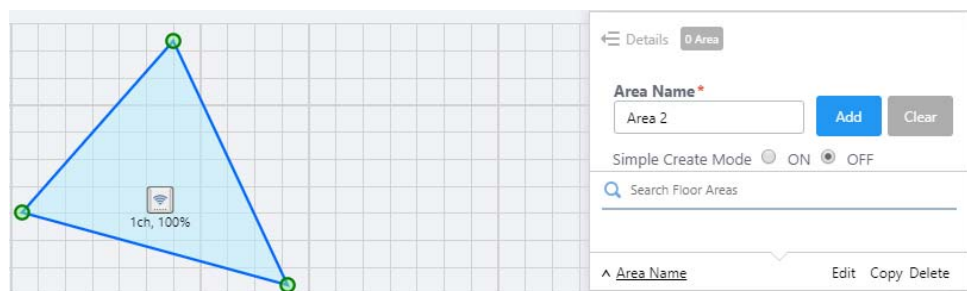
To draw an area, select Edit Area mode from the Floor Map menu.



To create a new area, define the area on the map, and give the area a name. Click Add to save the area.

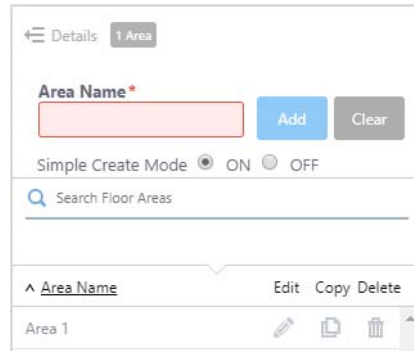


With the Simple Create Mode radio button turned On, you will be constrained to a rectangular area. To add a new area with an irregular shape, turn the radio button Off.

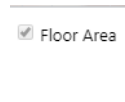


The area list can be filtered by typing text next to the Search icon. Note that this filter is case sensitive.

To edit an area, click on the Edit button for that area, which will allow you to change the name or shape of the area. To copy an area, click on the Copy button for that area. This will create a new area with the same shape, and the same name appended by “_copy”. To delete an area, click on the Delete button for that area. You will be prompted whether you want to delete the area.



You can choose whether to show or hide areas by checking or unchecking the Floor Area checkbox in the footer menu.



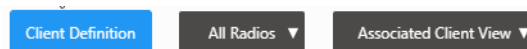
There are some limitations to the functionality:

- Creating overlapping areas is not supported.
- Only simple polygons are supported.
- When editing an existing area, changing the number of polygon vertices is not supported.

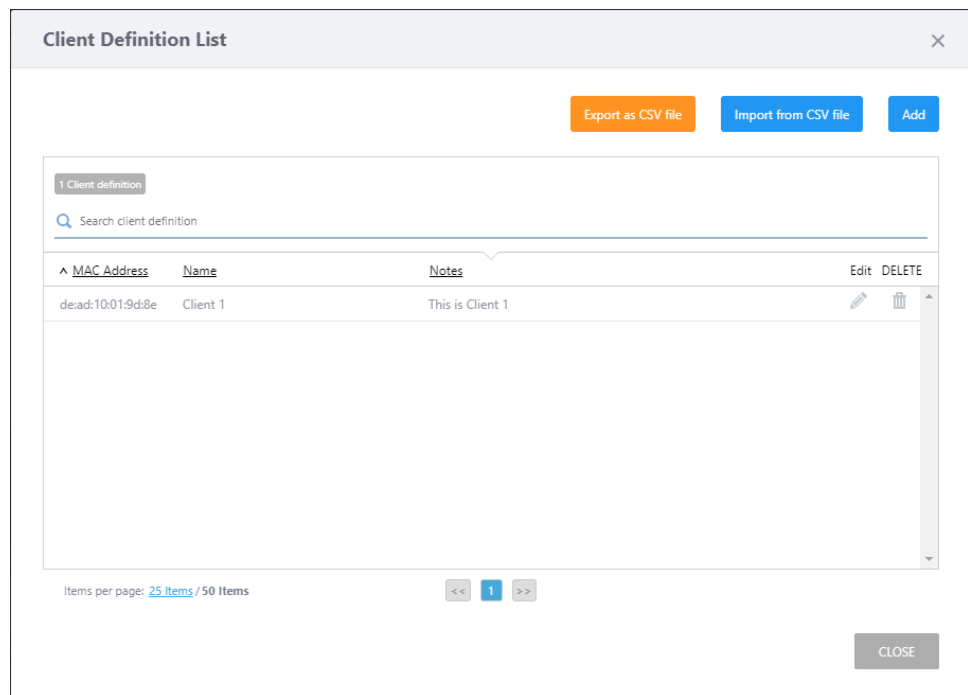
Client definition

Client definition allows you to specify a name that will be displayed for the client, rather than using the MAC address. In addition, you can add notes about the client.

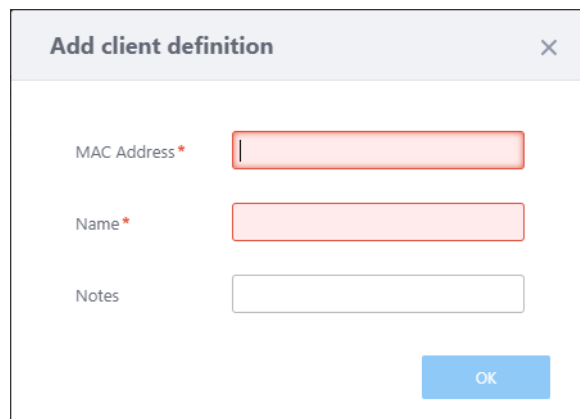
In Associated Client view on the floor map, click the Client Definition button.



The Client Definition List screen will be shown.



Click on Add to add a new client definition.



You must enter the MAC address for a client, and provide a name for them. The name may be up to 255 characters in length. You can also add notes about the client, up to 1000 characters in length.

To edit a client definition, click on the Edit icon. This will allow you to change the name or notes. To delete a client definition, click on the Delete icon. You will be prompted whether or not to delete the definition.

The client definition list can be filtered by typing text next to the Search icon. Note that this filter is case sensitive.

You can export your client definitions to a CSV by clicking on the Export as CSV file button. You can also import definitions by clicking on the Import as CSV file button. You can import CSV files you have previously exported, or other CSV files in the correct format as shown below.

Import from CSV

File Selection

Select a CSV file for import. The CSV format is as follows.
If the 1st column starts with "#", the row will be skipped.

Select File

1st Column: MAC Address
2nd Column: Name
3rd Column: Note

CSV Format

12:34:56:78:90:ab	Client Name	Comment about entry.
-------------------	-------------	----------------------

Add Cancel

WPA3 support

Security * None WPA Personal WPA Enterprise

Security Key (WPA-PSK) *

WPA Versions WPA3 WPA2 WPA

Encryption Protocol CCMP

Management Frame Protection Enable

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

From Vista Manager EX version 3.1.0, the AWC plug-in now supports WPA3 for TQ1402 and TQ5403 devices. You can select WPA3 when configuring AP and channel blanket profiles. If WPA3 is selected, TKIP will be removed as an encryption protocol option, and Management Frame Protection will be enabled by default.

Increased AP profiles

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

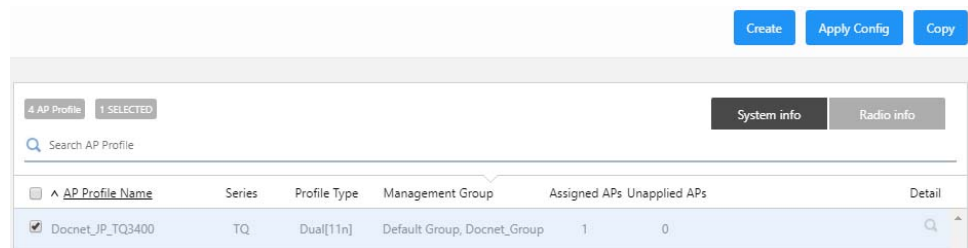
From Vista Manager EX version 3.1.0, the AWC plug-in now supports more AP profiles. You can now have up to 300 AP profiles.

Increased wireless management groups

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

From Vista Manager EX version 3.1.0, the AWC plug-in now supports more management groups. You can now have up to 100 wireless management groups.

AP profile copy



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

From Vista Manager EX version 3.1.0, the AWC plug-in lets you create a copy of an AP profile. This lets you quickly create multiple similar profiles.

To copy one or more profiles, select their checkbox in the AP Profile screen. Click on Copy in the top right corner. This will create a copy of each selected profile. The copy will have the same name, with “_copy” added at the end. The copy is identical, apart from the assigned APs of the source profile.

Improved client power consumption

DTIM Period	<input type="text" value="1"/>	[time]
RSSI Threshold	<input type="text" value="0"/>	
Tx Power	<input type="text" value="Max"/>	

Basic

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

From Vista Manager EX version 3.1.0, the AWC plug-in lets you configure the power consumption settings of your TQ5403 devices. The DTIM period, RSSI threshold, and TX power can be configured for each channel blanket. In addition, the DTIM period can be configured for individual APs.

- The default DTIM period is 1, and can be set to a value from 1 to 5. The DTIM period setting is independent for each virtual AP.
- The default RSSI threshold is 0, and can be set to a value from 0 to 91. The RSSI threshold setting is the same for each virtual AP and radio.
- The default TX power is Max, and can be set to Min, Low, Middle, High, or Max. The TX power setting is independent for each radio.

New AWC settings

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

From Vista Manager EX version 3.1.0, the AWC plug-in has a number of new settings.

In the AP Profile, the following new settings have been added for TQ1402 and TQ5403 devices.

Band Steering	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Wi-Fi Multimedia (WMM)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
APSD	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Neighbor AP Detection	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

In the Radio configuration section, you can now enable or disable Neighbour AP Detection. This is enabled by default. If you disable this setting, the wireless IDS/IPS feature and AWC calculation will not be performed correctly.

VAP (Multiple SSID) Configuration

Radio 1 VAP List	VAP1
VAP 1 ✔ Enable	VAP Status * <input checked="" type="radio"/> Enable
VLAN ID 1	VLAN ID * <input type="text" value="1"/>
SSID Default-1	SSID * <input type="text" value="Default-1"/>
Security None	Broadcast SSID <input checked="" type="radio"/> Enable <input type="radio"/> Disable
+ Add VAP	Security * <input checked="" type="radio"/> None <input type="radio"/> WPA Personal <input type="radio"/> WPA Enterprise
	Captive Portal <input type="radio"/> External RADIUS <input type="radio"/> Click-through <input checked="" type="radio"/> Disable
	MAC Address Authentication <input type="radio"/> External RADIUS <input type="radio"/> MAC Filtering <input checked="" type="radio"/> Disable
	Inactivity Timer <input type="text" value="300"/> [sec]
	Duplicate AUTH received <input checked="" type="radio"/> Disconnect <input type="radio"/> Ignore
	Association Advertisement <input type="radio"/> Enable <input checked="" type="radio"/> Disable

In the VAP configuration section, you can configure the Inactivity Timer. You can specify a number of seconds between 5 and 65535, with a default of 300.

By setting the Duplicate AUTH received radio button, you can choose whether to disconnect or ignore when a duplicate is received. This is set to disconnect by default.

You can enable or disable Association Advertisement. This is set to disabled by default. This must be disabled for Channel Blanket. If this AP is assigned to a CB profile, Association Advertisement is disabled and applied to the AP.

In the CB Profile, the following new settings have been added.

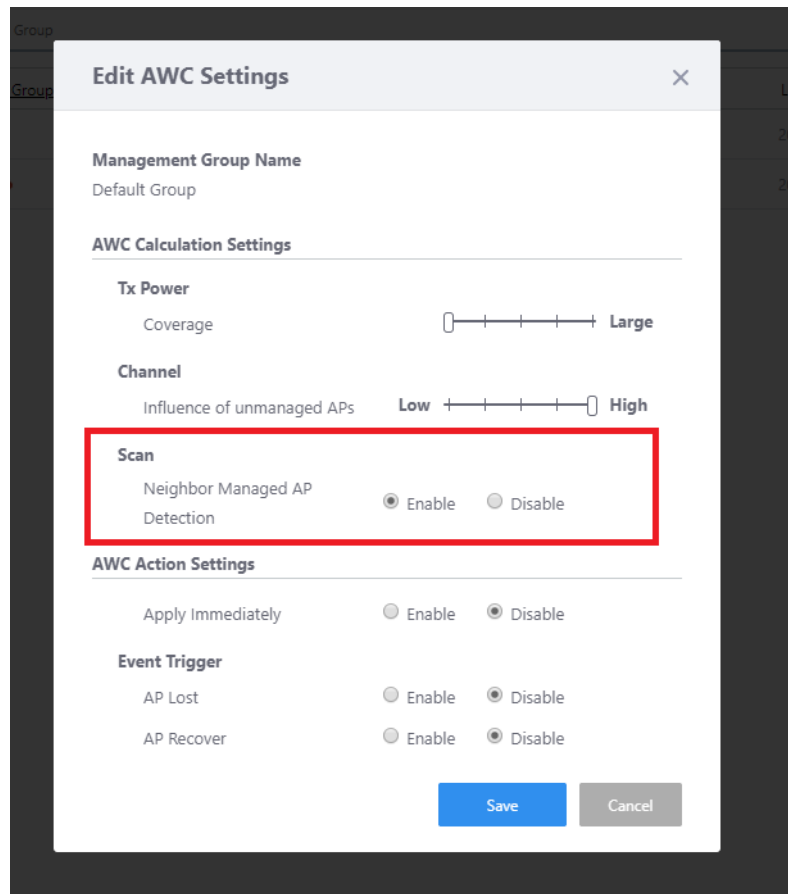
The screenshot displays the 'VAP (Multiple SSID) Configuration' interface. On the left, the 'CB VAP List' shows 'CB VAP 1' with a status of 'Enable' and a radio icon. The main configuration area for 'CB VAP1' includes the following settings:

- Radio: Radio 1 (selected), Radio 2
- VAP: (empty field)
- Channel: (dropdown menu)
- VAP Status: Enable (selected), Disable
- VLAN ID: 1
- SSID: Default-1
- Broadcast SSID: Enable (selected), Disable
- Security: None (selected), WPA Personal, WPA Enterprise
- MAC Address Authentication: External RADIUS, MAC Filtering, Disable (selected)
- Wireless Client Isolation: Enable, Disable (selected)
- Inactivity Timer: 300 [sec] (highlighted in red)
- Duplicate AUTH received: Disconnect (selected), Ignore (highlighted in red)

In the VAP configuration section, you can configure the Inactivity Timer. You can specify a number of seconds between 5 and 65535, with a default of 300.

By setting the Duplicate AUTH received radio button, you can choose whether to disconnect or ignore when a duplicate is received. This is set to disconnect by default.

In the AWC Settings, the following new settings have been added.



You can enable or disable Neighbour Managed AP Detection. This is enabled by default. If you disable this setting, AWC calculation will not be performed correctly.

Autonomous Wave Control – Smart Connect

AWC-SC is a new feature of AWC, that saves installation time and expense when adding new APs to a wireless network. Instead of cabling new APs into the network, AWC-SC uses one of the AP's channels to join it to the network.

AWC-SC will be available from late 2019 on TQ5403 and TQ5403e APs. It will require software version 6.0.1 or later on the APs.

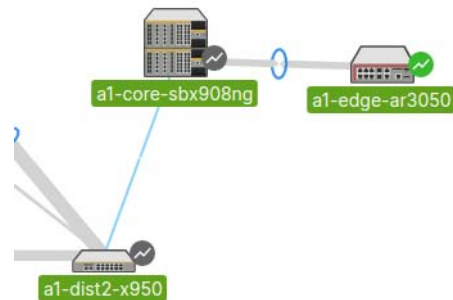
New platform support

Support has been added for the following devices:

- FS980M/28DP
- XEM2-8XSTm
- XEM2-12XS (LC)
- x320-10GH
- x320-11GPT
- IE340L-18GP
- GS980EM/10H
- GS980EM/11PT

Known Issues

- On the Traffic Map, 100G links are instead shown as 10/100M links.



Important Considerations Before Upgrading

This section describes changes since Vista Manager EX v3.1.0 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 25 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.

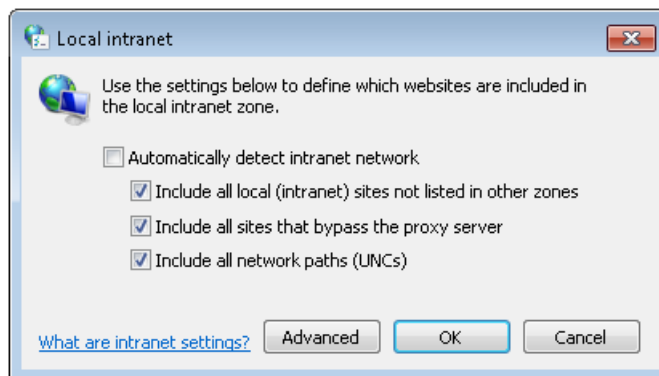
Microsoft Edge support

Applicable to all Vista Manager installations.

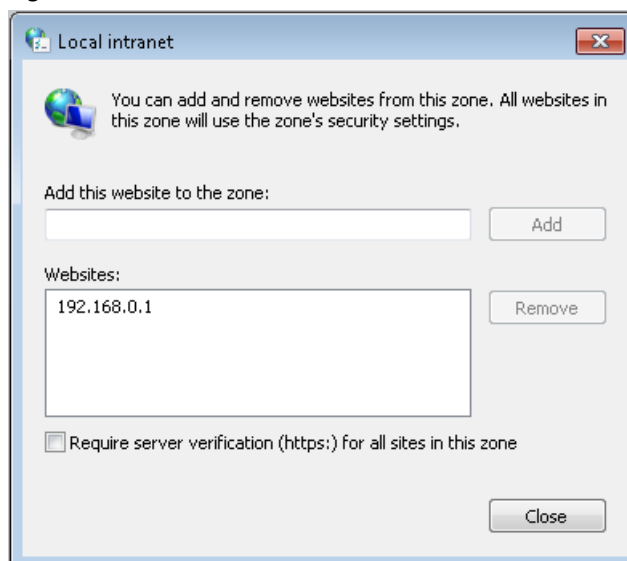
Security in Microsoft Edge may prevent you from navigating to Vista Manager using an IP address. We recommend that rather than using the IP address, you use DNS and a FQDN for Vista Manager.

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](#).

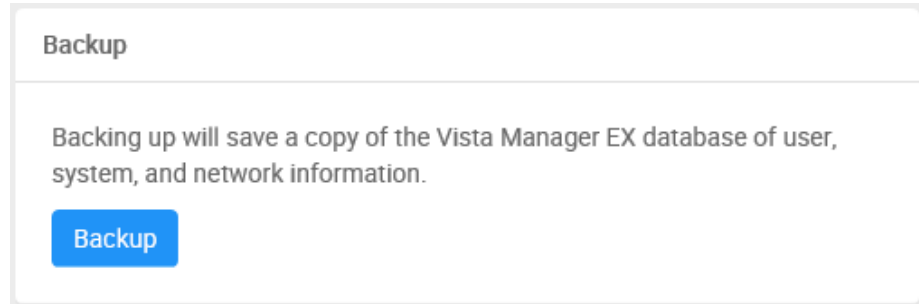
AMF documentation For full AlliedWare Plus documentation, see our online documentation library. For Vista Manager, the library includes the following documents:

- 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 v3.1.0 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'.

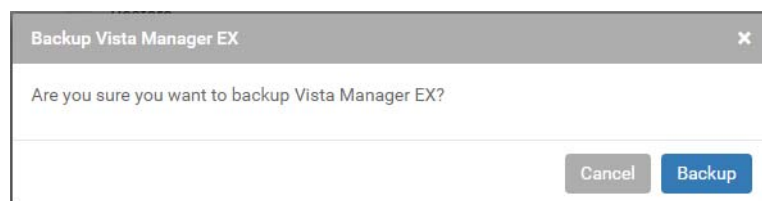
Do not rename these files. The installation requires them to be in this format.

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.

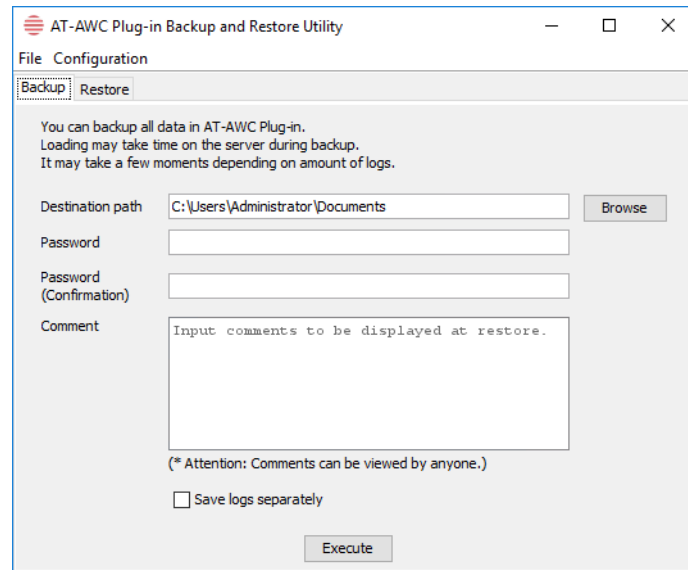
Backup the AWC plug-in

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.

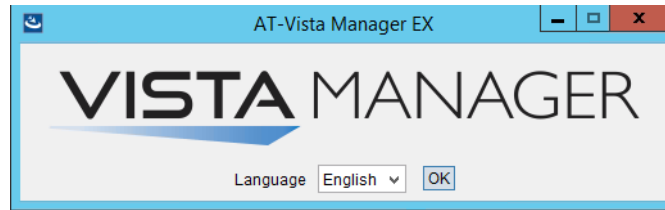
Note: The default location of <Vista Install Path> is **C:\Program Files (x86)\Allied Telesis\AT-Vista Manager EX**

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

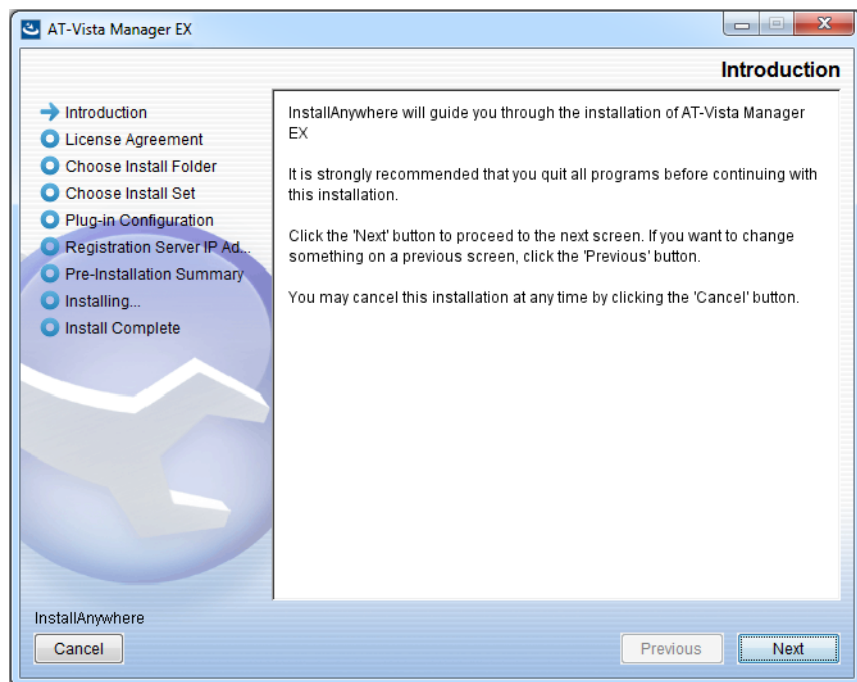
21. Execute the Vista Manager EX installation program 'atvmexXXXbXXw.exe'. This opens the following **AT-Vista Manager EX** dialog:



- 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**.

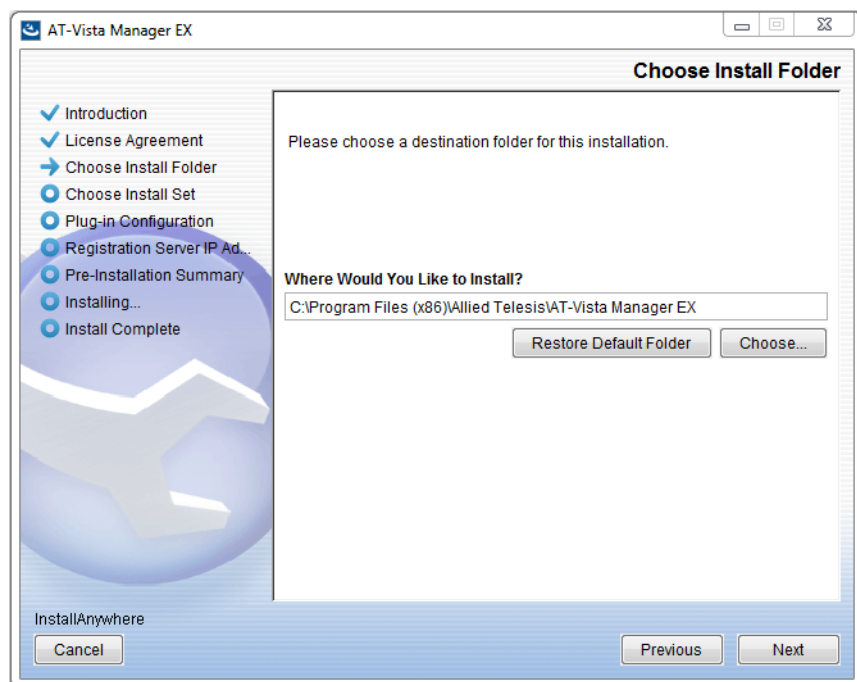
23. The **License Agreement** dialog displays:



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

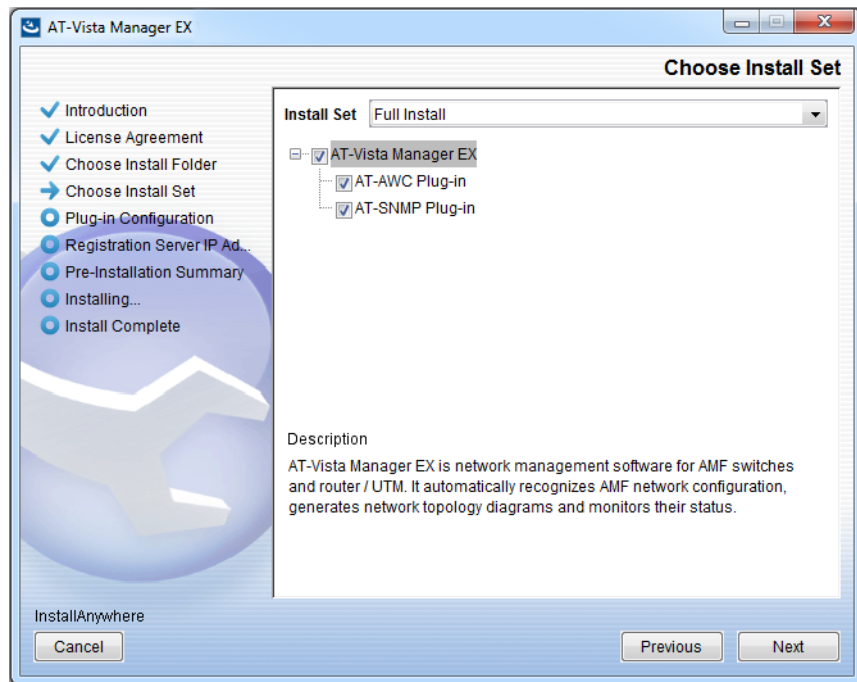
- Click **I accept the terms of the License Agreement**
- Click **Next**

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



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

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



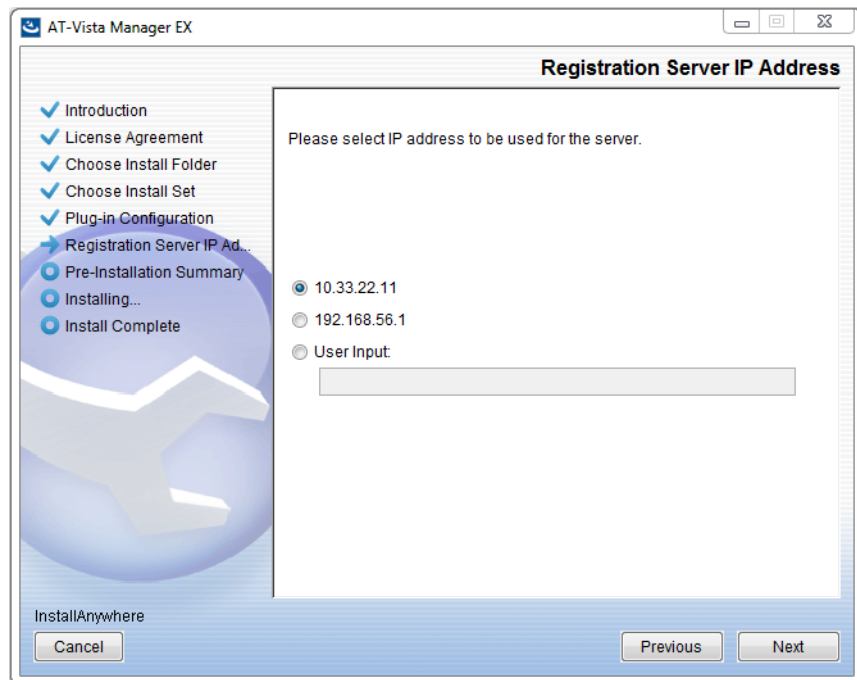
Select **Full Install** from the drop down list. By default all plug-ins will be selected. Clear the check box for any plug-ins you do not wish to install. Click **Next**.

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



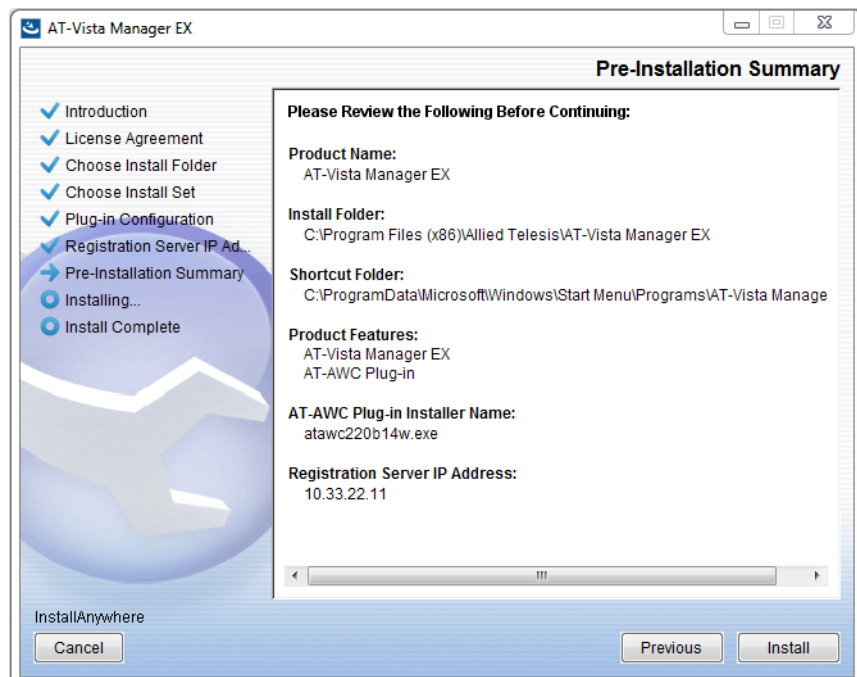
Select **Do not create a public key** unless you are intending to use the plug-ins in standalone mode. For more information on standalone mode, refer to the Installation Guide. Click **Next**.

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



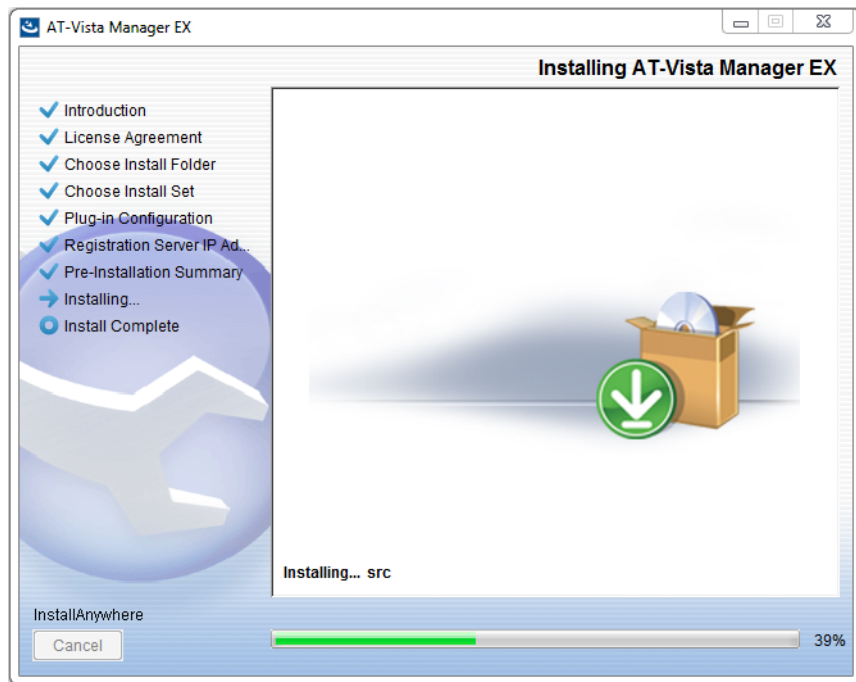
Either select from the list of IP addresses already configured on the Windows machine, or input a valid IP address. Click **Next**.

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

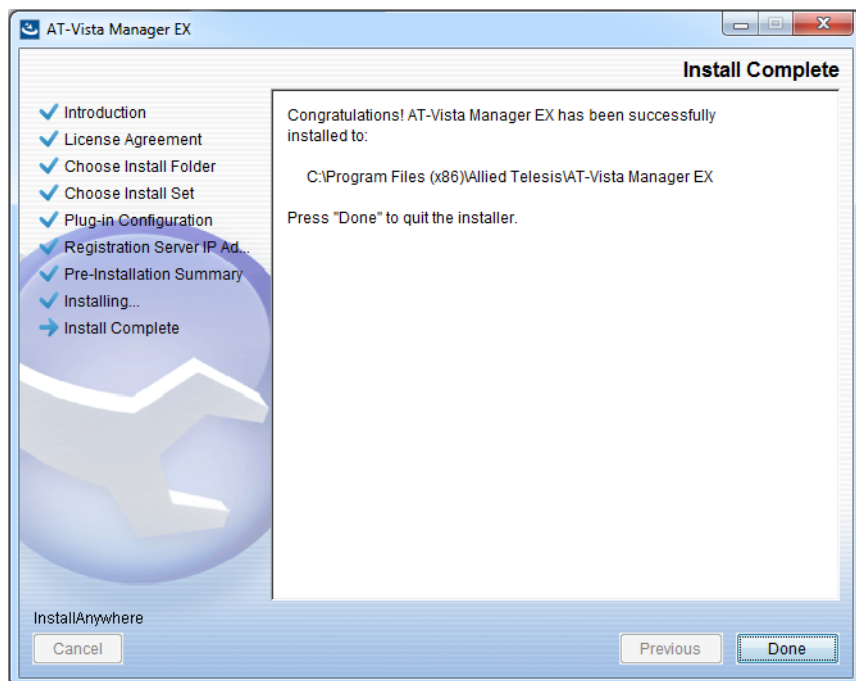


Check that your Product Name, Install Folder, Shortcut Folder, Product Features, Plugin Installer Name and Registration IP Address are correct, and then click **Install**.

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**