

# Release Note for Vista Manager EX Software Version 3.8.x



## VISTA MANAGER™ EX

» 3.8.0

» 3.8.1

---

## Acknowledgments

©2022 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/](http://www.adobe.com/)

---

<b>What's New in Vista Manager EX v3.8.1 .....</b>	<b>2</b>
<b>What's New in Vista Manager EX v3.8.0 .....</b>	<b>3</b>
<b>Important Considerations Before Upgrading.....</b>	<b>30</b>
<b>Obtaining User Documentation.....</b>	<b>31</b>
<b>Upgrading Vista Manager as a virtual appliance .....</b>	<b>32</b>
<b>Upgrading Vista Manager as a Windows-based installation.....</b>	<b>33</b>
<b>Upgrading Vista Manager on VST-APL.....</b>	<b>43</b>
<b>Upgrading Vista Manager on VST-VRT.....</b>	<b>43</b>
<b>Troubleshooting .....</b>	<b>43</b>

# What's New in Vista Manager EX v3.8.1

## Introduction

This release note describes the issues resolved in Vista Manager EX™ v3.8.1. 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.

---

## Issues resolved

This section summarizes the issues resolved in Vista Manager EX v3.8.1:

- [“Preventing vulnerability scanning tools from incorrectly reporting Vista Manager EX as vulnerable to Log4j” on page 2](#)

### Preventing vulnerability scanning tools from incorrectly reporting Vista Manager EX as vulnerable to Log4j

*Applies to all Vista Manager installations.*

A high severity vulnerability, CVE-2021-44228, has been reported in Apache Log4j, a popular Java logging package. The Allied Telesis Cybersecurity Team has reviewed the vulnerability and assessed that currently-used versions of Vista Manager EX are not affected, including v3.8.0.

However, some vulnerability scanning tools indicated that Vista Manager EX uses vulnerable versions of the library. This is because Vista Manager EX uses Elasticsearch and Logstash, and these did contain vulnerable versions of the library. However, the vulnerability can only be exploited if the library is used with certain older versions of Java, which Vista Manager EX does not use in versions 3.0.3 and newer.

In version 3.8.1, Vista Manager EX has been upgraded to use the latest versions of Elasticsearch and Logstash, which do not contain vulnerable versions of the library.

**Recommended Action:** If you wish to prevent your vulnerability scanning tool from incorrectly indicating that Vista Manager EX uses vulnerable versions of the library, upgrade to version 3.8.1.

# What's New in Vista Manager EX v3.8.0

## Introduction

This release note describes the new features in Vista Manager EX™ v3.8.0. 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.

---

## New Features and Enhancements

This section summarizes the new features added to Vista Manager EX v3.8.0:

- “Topology map layout management” on page 4
- “Improved WAN visibility on integrated map” on page 7
- “Improved application priority” on page 11
- “Distributed tunnel routing support” on page 13
- “New IP map layer for walk path” on page 16
- “MIB browser support”
- “New AWC Plug-in functionalities and settings” on page 18
  - ◀ “Smart activation (AWC-SAC)” on page 18
  - ◀ “Enhanced floor map support” on page 22
  - ◀ “Captive Portal support for TQ6602” on page 26
  - ◀ “Reauthentication timer settings” on page 27
  - ◀ “Sky Defender (AWC-SDF)” on page 29

---

## Topology map layout management

*Applicable to all Vista Manager installations.*

From version 3.8.0, topology map layout management gives you the ability to design map layouts so that you can predefine the default layouts for different users. You can design different network map layouts, and switch the network map layouts easily. You can also set a designed network map layout as the default map layout for everyone, or for a specific user. This means each user will see a well-organized network map when they log in for the first time.

You can design integrated map layouts in all the map modes. The Topology Map layout contains the following:

- Node positions
- Background image
- Expand/collapse status of sites and stacking devices
- Zoom and panning position
- Manually add static/discovered devices

### Creating a new layout

To create a new layout:

1. Click on the layout drop-down. If this is your first layout, the name will be **No layout**. Otherwise, it will be the name of the currently selected layout.
2. Enter a name for your new layout, and click on the check mark to save the layout.
3. The new layout will become the selected layout.

You can create a new layout based on an existing layout by saving the current layout with a new name. Different users can have different map layouts with the same name.

If you save your current layout with the name of an existing layout, it will overwrite it. You can only overwrite map layouts you create.

### Selecting a layout

The integrated map has a drop-down list to show the current layout, and all available layouts. All the layouts created by the current user are visible in the drop-down list. Additionally, if the current user is an administrator user, the layouts created by other administrators will also be visible in the drop-down list. If a network layout has been set as the default layout for this user or everyone, the default layout is also visible in the drop-down list. For map layouts created by other users, the author's name is displayed as part of the map name to help identify it.

To select a layout:

1. Click on the layout drop-down.
2. Select a layout from the displayed list.

---

## Setting the default layout

Administrators can select a map layout and set it as the global default map layout for all users.

To set the global default layout:

1. Select **User Management** from the menu.
2. Select your user, and click on the **Edit** button.
3. In the **Global Default Network Topology** section, click on the drop-down, and select the layout to be the default.
4. Click on the **Save** button.

Administrators can also select a map layout and set it as the default map layout for a specific user.

To set the default layout for a specific user:

1. Select **User Management** from the menu.
2. Select the user whose default you want to set, and click on the **Edit** button.
3. In the **Global Default Network Topology** section, click on the drop-down, and select the layout to be the default.
4. Click on the **Save** button.

When a user logs in for the first time, the default map layout is used. The default map layout will also be included in the map layout drop-down list.

## Deleting a saved layout

Administrators can delete any map layout. Users can only delete map layouts that they created.

If an administrator deletes a map layout that is being used as the default map layout by some Vista users, those users' default map layout will change to the global default map layout. If an administrator deletes the global default layout, there will be no default map layout.

If the currently selected layout is deleted, including the default layout, the selected layout will be changed to **No layout**, while the map will remain unchanged.

To delete a layout:

1. Click on the layout drop-down.
2. Select the layout you want to delete, and click on the **X** icon.
3. On the confirmation dialog, click **Continue** to delete the layout.

---

## Hiding devices in the layout

You can change which devices 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 devices.

To change the visibility of a device:

1. Click **Edit** in the drop-down on the network map screen.
2. Right click on the device you want to hide.
3. Click on **Hide**.

The hidden device is added to the **Devices** list. Click the down arrow to see the details of a device in the list.

Hidden devices are specific to the layout. Users can hide devices on a per-layout basis, and they are hidden for any user using that layout.

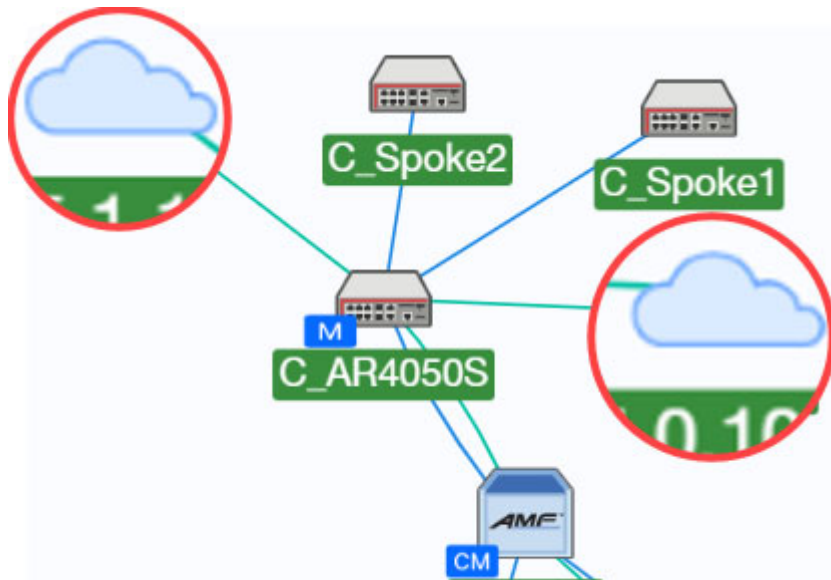
**Note:** The visibility of base devices cannot be changed. Therefore, on an AMF network, AMF devices will always be visible and cannot be hidden. Likewise, if the network is a plug-in view, then the plug-in device(s) will always be visible.



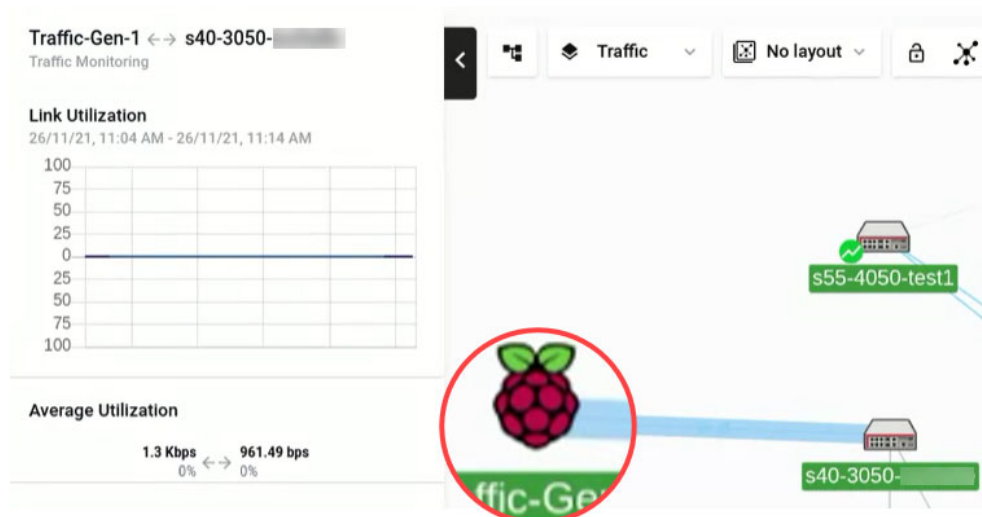
## Improved WAN visibility on integrated map

*Applicable to all Vista Manager installations.*

From version 3.8.0 onwards, the integrated map is improved to display more links and their utilization information. Previously, the only links shown are AMF links between AlliedWare Plus devices, devices added through the Asset Management page or AMF guest devices. The integrated map now detects non-AMF devices that have an AlliedWare Plus device connected to them by a tunnel. The new non-AMF device is represented as a cloud icon. The hostname is the IP address of the tunnel destination.

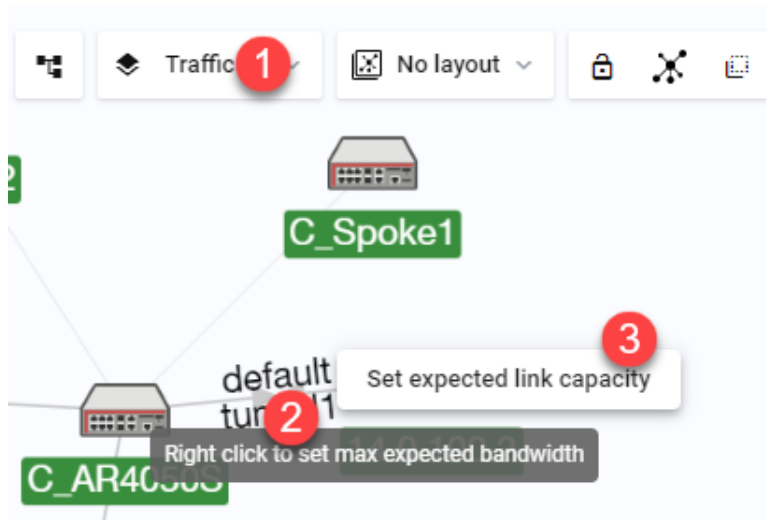


Prior to version 3.8.0, devices through Vista Manager can be added from the Asset Management page. Now there is also the ability to monitor link utilization on devices that are manually added.



This feature greatly enhances overall user experience. Allowing users to manually configure custom links when they are not automatically picked up then provides a complete solution. Because of this improvement, users can also monitor internet breakout links that are directly connected to the Internet via a WAN interface.

In Traffic map mode, right-click on a tunnel to set the expected link capacity. The link traffic utilization then becomes available for monitoring.



Set expected link capacity

default ↔ tunnel1

**i** The Mbits/sec value entered will affect the visual appearance of a link in the map  
Link width represents bandwidth capacity

Expected Capacity (Mbits/sec)

14.0.100.2 → C\_AR4050S

C\_AR4050S → 14.0.100.2

1000

1000

4

Cancel

Save

5

14.0.100.2 ↔ C\_AR4050S

Traffic Monitoring

Link Utilization

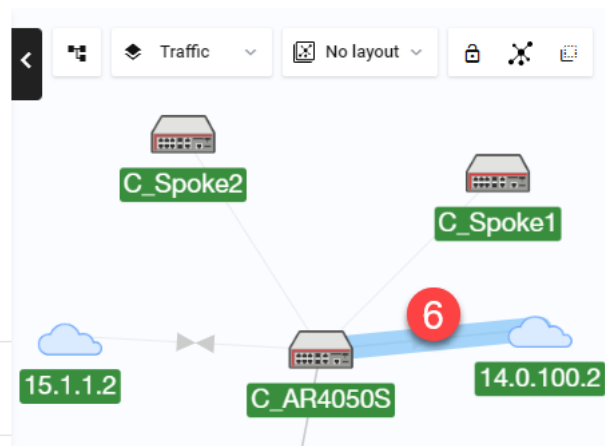
30/11/21, 1:22 PM - 30/11/21, 1:32 PM



7

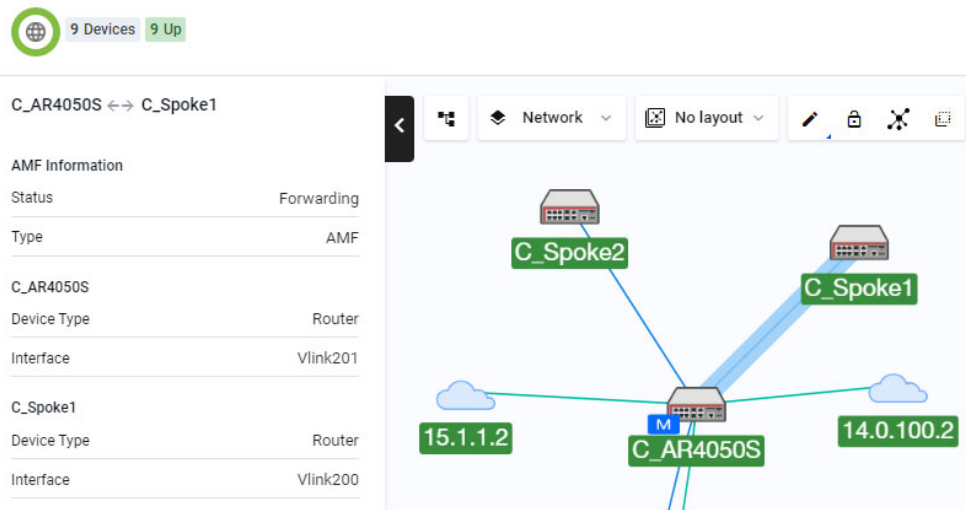
Average Utilization

4.41 Kbps ↔ 42.29 Kbps  
0% ↔ 0%



There are multiple functionalities to this feature:

- automatically detect supported tunnels between an AlliedWare Plus device and a remote device that is not part of the network
- automatically create custom devices represented by cloud icons on the remote end of the tunnel and add them to the map
- automatically update map if there are any changes to an existing tunnel or when a new tunnel is configured
- detect IPv4 PPPoE configuration and display these links and devices on the map similar to the tunnels
- display read-only information about the tunnel on the map side panel



- configure interfaces and bandwidth on a custom link so that the link utilization data is available

Set the interfaces for each end of the link

Specifying the interfaces for the link will add support for link utilization

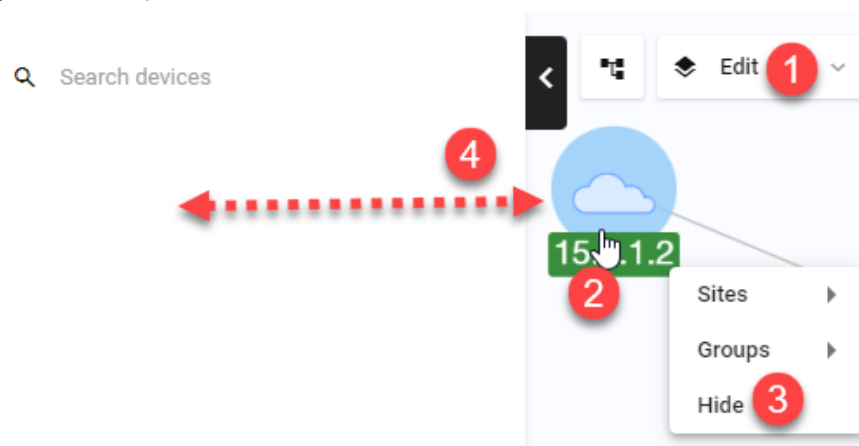
Traffic-Gen-1      s40-3050

custom      port1.0.3

Cancel      Save

- display link utilization statistics for tunnels on the traffic map

- hide/display non-AMF (remote) devices and their associated WAN tunnels via the edit layer of the map



- enhance custom links to allow you to specify the associated interfaces of the link

There are some limitations to take note of:

- This feature is unable to detect the up/down status of a remote device.
- If two WAN tunnels are connecting to the same device, two cloud icons will show instead of one. Vista Manager EX is unable to discover if two IPs are on the same device.
- Removing or configuring interfaces on automatically discovered tunnels are not possible. You can only hide a remote device and its associated links.
- Link utilization data of a port connected to a server is not supported unless the connection is via a tunnel. Manually adding a remote device and a custom link, and specifying the associated interface will display its link utilization data.

# Improved application priority

Applicable to Vista Manager installations with the AIO license.

From version 3.8.0 onwards, the **Add Policy** and **Edit Policy** pages under the Application Priority feature are visually enhanced to improve overall user experience. The design enhancements will make it easier for you to understand what the feature will do, how you can use it, allow you to visualize how much guaranteed bandwidth each class has and how much shared bandwidth remains. A minimum guaranteed bandwidth percentage for system traffic, which is a reserved amount on all new policies, is also displayed.

Policy Name \*

ZoomCalls\_Guaranteed5Mbps

Give your policy a descriptive title E.g. AppCategory\_RequiredMbps

Application Provider

Built-in Procera (license required)

### Application Priority

Assign applications to give priority over lower classes and default traffic

**1 Critical Services**  
Applications critical to business operations.  
Include services whose disruption would result in a high cost. E.g. Database & Backup.

Applications

dataserver x mysql x drda x Clear All

**2 Daily Operations**  
Applications used in day-to-day business operations.  
E.g. File sharing.

Applications

zoom x pastebin x git x googledoc x Clear All

**3 Non-Essential**  
Applications that are commonly used but not essential to business operations.  
E.g. Social media.

Applications

facebook x Clear All

### Guaranteed Bandwidth

Control minimum bandwidth requirements to ensure application traffic when network is congested.  
Percentages will be converted to Mbps values when deployed to device.

60%

Low amount of shared bandwidth remains for default traffic. This could affect your overall network performance. At least 45% of Shared Bandwidth is recommended.

System 5 %

Critical Services	10 %
Daily Operations	25 %
Non-Essential	20 %
Shared Bandwidth	40 %

---

The list of improvements will allow you to do the following, but are not limited to:

- a.** Set the policy name
- b.** Select the application provider
- c.** See what applications are in which class
  - « Critical Services (formerly Essential)
  - « Daily Operations (formerly Business Relevant)
  - « Non-Essential
- d.** Remove applications from classes
- e.** Set guaranteed bandwidth percentage to preset values using a slider
  - « Individual guaranteed bandwidth percentage sliders have been removed from the classes and replaced with a one combined slider. The new slider can be set between 10% and 55% of the device bandwidth. Based on that figure, the value then gets divided up into guaranteed bandwidth percentage for each class.
- f.** Edit guaranteed bandwidth percentage values manually via an advanced option
  - « If the advanced option is used followed by the slider, any manually-set values are automatically replaced by the presets generated by the slider.
- g.** See a **warning** if total combined guaranteed bandwidth percentage **exceeds 55%**  
See an **error** if total combined guaranteed bandwidth percentage **hits 100%**
  - « The warning does not prevent you from submitting any values.
  - « The error will block you from submitting the form.
- h.** See the reserved percentage of guaranteed bandwidth for system traffic
  - « This 5% value is based on the default value that traffic control sets on a device. The actual value reserved for system traffic may vary depending on what device(s) the user deploys the policy on to. Vista Manager will just show 5% as the system-reserved bandwidth.
- i.** See the remaining percentage for shared bandwidth
  - « This is the remaining amount automatically calculated and shown after the bandwidths for system traffic and three classes are taken out.

---

## Distributed tunnel routing support

*Applicable to Vista Manager installations with the AIO license.*

In Vista Manager version 3.8.0, the existing functionality of creating VPN connections (tunnels) is enhanced to enable altering the tunnel routing option from the Dynamic Connection page. When a tunnel is created, users will have the option to distribute routes to further devices to create a return routing path. Side panel menus are improved to include potential networks and hosts to add as routes. Users are given a list of subnets to choose from, with these subnets being accessible from the device. However, not all networks and devices at the tunnel destination are used to form new primary routes. The list of destinations are pre-filtered.

These types of networks and hosts are allowed:

- connected by static routes
- directly connected to the end router (direct routes)
- routed through a dynamic routing protocol

**Example:** When a tunnel is created from (A) to (B), (A) will distribute networks and hosts (X) to (B). However, that does not necessarily mean (X) can reach (B), so networks on (B) are allowed to be distributed to add as routes on (X).

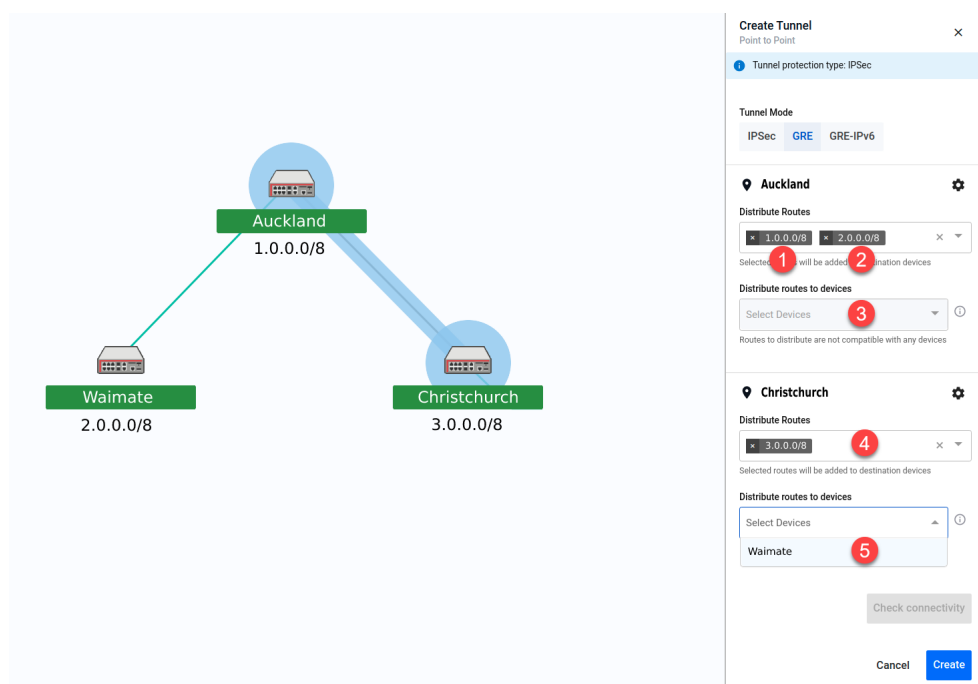
When adding a new router (B) with a point-to-point tunnel connection to an existing router (A), the side panel on B will have a list of networks and hosts that are local and attached to it. The networks and hosts on B can then be distributed to A with the tunnel as the gateway.

If the user deletes a tunnel, all static routes associated with the nexthops of that tunnel will also be deleted. However, manual routes can still be added from the pull-down menus.

Administrative distances are added to static routes; static routes with the same default administrative distance (zero) to the same destination is not supported. When a route is shared, Vista Manager adds a 1 to its distance. Therefore, a direct connection route with a default distance of 0 will have a distance of 1 when added to a destination device's route table.

Existing AlliedWare Plus configuration can be imported into Vista Manager for this feature.

For this feature to be fully supported, AlliedWare Plus version 5.5.1-2.1 or later is required.



## Settings for the source end of tunnel (Auckland)

1. The route to **Auckland (1.0.0.0/8)**, is selected in the "Distribute Routes" input. This route is added to the route table of the Christchurch device, allowing traffic to go from Auckland to Christchurch.
2. A tunnel between Auckland and Waimate already exists, so the route to **Waimate (2.0.0.0/8)**, is an option in the "Distribute Routes" input. This route is added to the route table of the Christchurch device, allowing traffic to go from Waimate to Christchurch.
3. Nothing is needed in the "Distribute routes to devices" input because the selected routes are automatically distributed to the destination end of the tunnel (Christchurch).

## Settings for the destination end of tunnel (Christchurch)

4. The route to **Christchurch (3.0.0.0/8)**, is selected in the "Distribute Routes" input. This route is added to the route table of the Auckland device, allowing traffic to go from Christchurch to Auckland.
5. Because the route to Waimate is added to the route table of the Christchurch device, there is now an option to distribute a route to Christchurch on the Waimate device. This route is added to Waimate, allowing traffic to go from Christchurch to Waimate.

**Note:** It is mandatory for users to choose a route. Vista Manager is unable to prevent loops from being created as all forwarding paths in the network are not known. Some WAN-facing interfaces will not be included in the list of routing destinations, as this could form routing loops caused by networks beyond the immediate control of the user.



---

## Feature limitations

There are some feature limitations to take note of:

- Because this is adding static routing, there may be potential for routing loops. The risk of causing such loops cannot be eliminated.
- Entity subnets will not be filtered out if they overlap or are duplicated with other subnets. It is up to the user to create valid entities.
- Changes made to subnets and entities after the tunnel has been created will not be automatically detected; routes on the devices will not be updated. Users will have to make these changes on the tunnels and devices if they make changes to subnet and entities.
- IPv6 routes are supported as static routes, but are not supported as distributed subnets. The IP version of static routes must match the IP version of the tunnel IP address.
- mGRE tunnels use GRE-based protocols and are therefore stateless. Static routes on mGRE will not be re-routed automatically if a hub-to-spoke tunnel link goes down.

---

## New IP map layer for walk path

*Applicable to Vista Manager installations with the AIO license.*

From version 3.8.0, a new IP map layer is added to the integrated map, merging the current tracepath layer into it. Within this new map layer, the side panel provides selection between either tracepath or walk path. The walk path feature will allow users to determine if there are any configured routing paths from one node to a destination IP within the network known to Vista Manager. This is usually performed for installation or diagnostic purposes.

**Note:** The AIO license is not required for IP map layer (view) and tracepath as these were existing functionalities prior to version 3.8.0.

Similar to the tracepath functionality, select a source node and destination node with IP address, and request routing paths to be drawn between these two nodes. The paths are determined by Vista Manager querying the routing tables on the nodes. No probing will occur between nodes. Users are notified of any route paths that reach a dead end.

### Source and destination nodes

- **Source node** must be a routing API-capable device. A routing API-capable device is any AlliedWare Plus device running on software version 5.5.1-2.1 and above. There is no starting IP address, as only destination is used in the routing calculation.
- **Destination node** is not restricted to AMF devices and can be any node in the network that is known to Vista Manager that has an IP address. It may also have secondary IP addresses, connecting L3 paths are supported.

### Path calculation

The path is calculated from the source to the destination; the reverse is not calculated. However, users can request the reverse path, by swapping the destination node for source node and selecting an IP address on what was previously the source but is now destination. Calculation happens in two parts:

1. First, beginning on the source node, it finds the longest prefix match on the routes.
2. Next, it uses that route to identify the nexthop node via IP or interface (if topology is known).
3. Then it repeats until it reaches the destination node or an obstacle.

**Note:** Recursive routes are supported.

### Path names

- When there is **only one path** from the source to the destination, the path is **unnamed**.
- When there is **more than one path**, each path is named "**via node name**", where node name is the nexthop where the path diverted. Any subsequent branching of that path resulting in new paths will follow the same naming process.
- If the **nexthop is already the destination**, the path is **unnamed**.

---

## Topology usage and map lines

When routes along the path have an interface as nexthop (no IP address), Vista Manager will then use the topology to determine the next node in the path, if topology is known. For custom links to static nodes, we recommend specifying the interface.

Lines are drawn on the map in segments of the journey from L3 node to L3 node, regardless of the underlying topology. This is because:

- Consistency with tracepath can be maintained
- Without knowledge of the neighbour API call, the links used will not be known
- Vista Manager often does not have knowledge of the topology, so topology lines may not be present to indicate the links

## MIB browser support

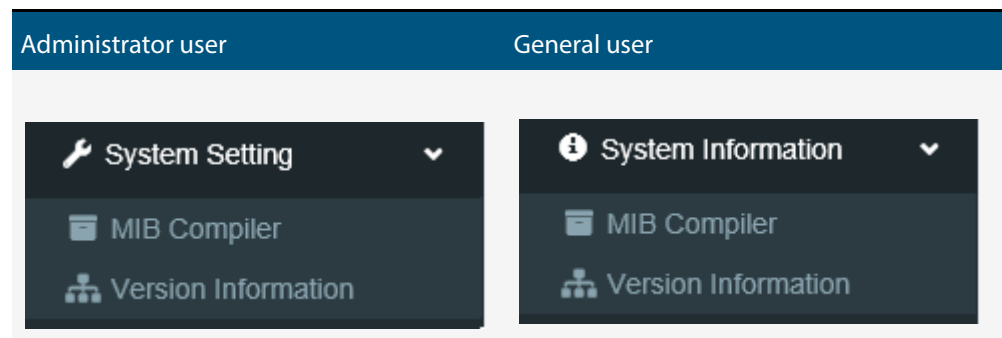
*Applicable to Vista Manager installations with the SNMP plug-in.*

The MIB browser feature was previously implemented for the Windows platform.

From version 3.8.0 onwards, these platforms will also be supported:

- **VST-APL**
- **VST-VRT**

These platforms also have a new MIB compiler introduced to the system menu structure. Administrator users and general users will see slightly different views:



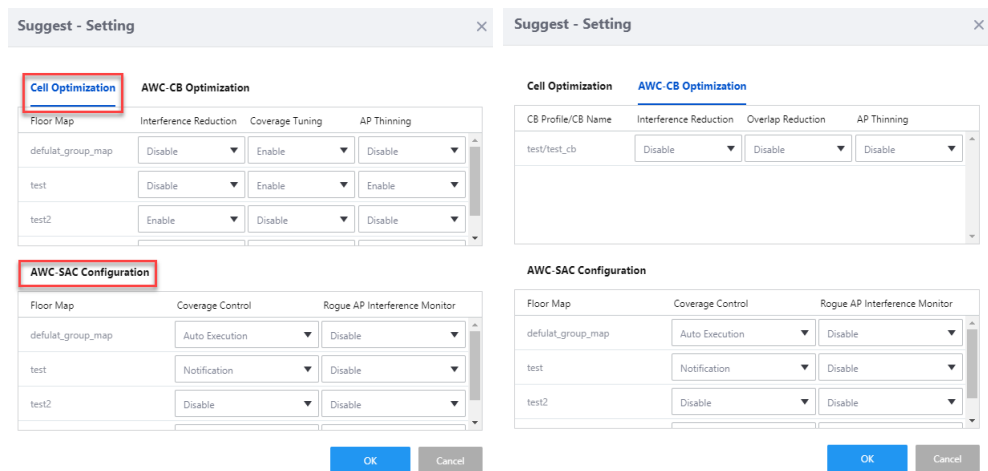
# New AWC Plug-in functionalities and settings

For more detailed information on the following AWC features, refer to the [User Guide: Autonomous Wave Control \(AWC\) Plug-in](#).

## Smart activation (AWC-SAC)

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

From version 3.8.0 onwards, the AWC plug-in will have a new feature **Smart Activation (AWC-SAC)** added to the Wireless Concierge page. The user interface will have some enhancements.

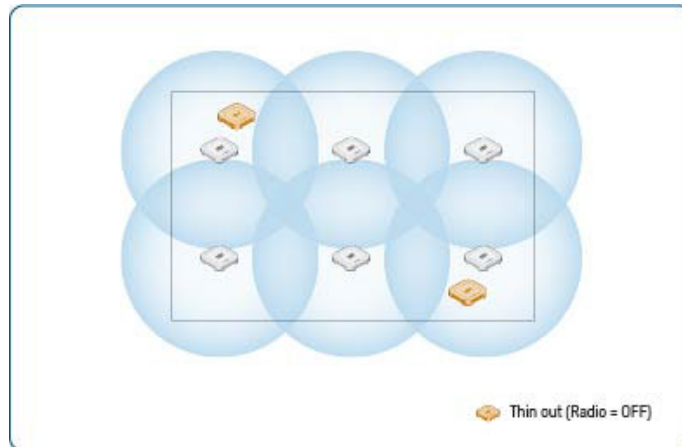


Smart Activation covers three main components:

- **AP Thinning**
- **Coverage Control**
- **Rogue AP Interference Monitor**

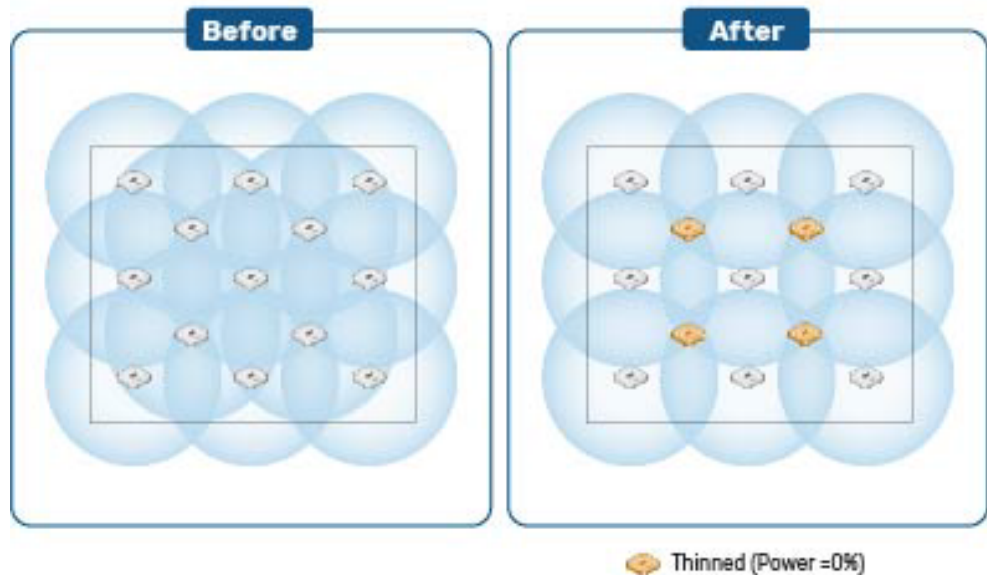
■ **AP Thinning**

- « The system detects APs in standby mode and turns off their transmit power.



- « By reusing those APs when a lost AP or location situation change occurs, an automatic complementary system for wireless coverage is achieved.
- « Initial installation cost for both coverage and interference management can be reduced.
- « Periodic monitoring of the coverage status is carried out for each floor.
- « An event message is sent when there are changes to the AP management status and coverage status.

**Before and after AP thinning**



---

- **Coverage Control**

- « Coverage control is a trigger that controls coverage state change detection and execution.
- « It starts to monitor the coverage status after a sufficient amount of neighbor managed AP data is scanned.
- « When the AP location changes or during the execution of an operation (AP reboot/config applying/firmware upgrade), this functionality pauses to monitor the management or coverage.
- « Enabling event trigger and coverage control simultaneously is not supported.

- **Rogue AP Interference Monitor**

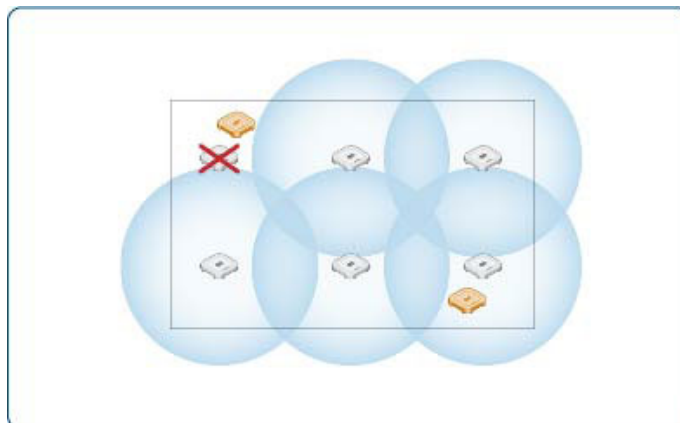
- « Periodic monitoring of the interference level for each floor happens every hour.
- « When the number of changed APs does not exceed 30% of the total, no detection happens for the interference status change.
- « Users can select the sensitivity; the threshold values are 25% for low, 50% for middle, 75% for high.
- « An event message is sent when the configured percentage exceeds the threshold.

## Operating conditions of Smart Activation (AWC-SAC)

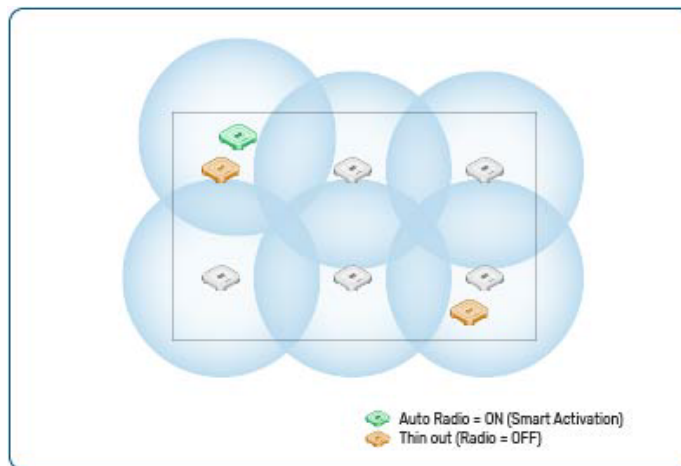
The plug-in operates AWC-SAC when detecting the following conditions:

- **AP disconnection** - loss of communication with AP due to failed wired interface, etc.
- **AP recovery** - resolution of wired interface problems due to replacing a failed AP, etc.
- **Change of environment** - change in visibility between managed APs due to relocation of partitions, etc.

Detecting a failed AP:



AWC-SAC in operation:



## Installation to operation

The flow from installation to operation is as follows:

1. Place APs to be managed via the wired LAN in a dense area. This reduces the probability of a coverage hole. There is no need for a site survey.
2. With the AWC plug-in, the administrator determines unnecessary APs and sets their transmission output to 0%.
3. The administrator uses the AWC plug-in to optimize the channel and transmission output of the AP, and then applies it to the AP.
4. If the system detects an AP failure, it automatically determines the recovery solution using the “unnecessary AP” and applies it to the AP.
5. When a failed AP becomes “Managed” again, the system automatically reduces the number of APs, determines the optimal environment, and applies it to the AP.

## Cell optimization

To optimize cell type AP channel and power levels for each radio interface:

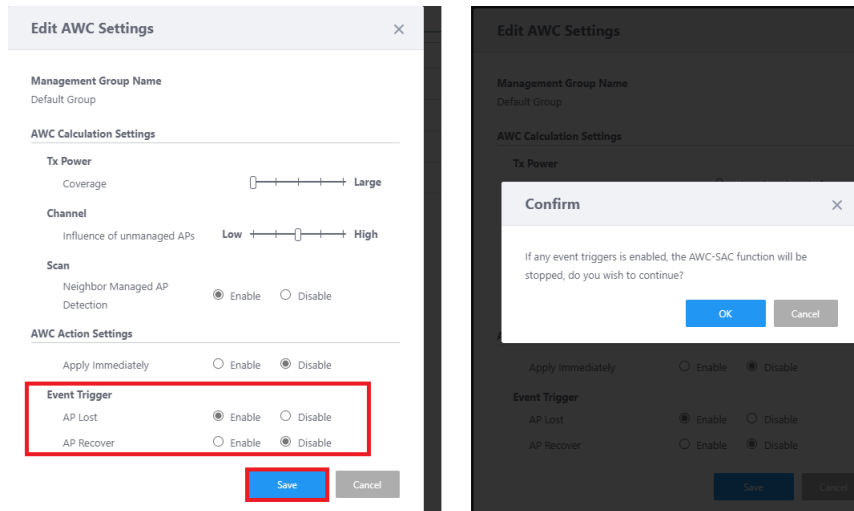
1. Suggest a cell AP channel that minimizes the interference level as much as possible.
2. Use Rogue APs’ RSSI data for the last 3 hours.
3. Suggest a cell AP power level that minimizes the radio overlap area as much as possible.

AWC-SAC only uses APs with power level set to 0%. This means that you must configure the AP radio interface to OFF. To set AP power level to 0%:

- Do not change coverage area when AP power level is set to 0%
- Distance between AP and AP is must be less than or equal to 7 metres on the floor map
- If the radio configuration of the nearest AP is different from the target AP, the AP power level is **not set to 0%**
- If the AP has AWC-SC root configuration, the AP is less likely to be thinned out

## Event trigger

Enabling event trigger will stop AWC-SAC from operating. However, any AWC-SAC settings that are already configured will remain.



**Note:** AWC-SAC will not operate if there is a loss of SSID due to a wireless interface failure causing the loss of AP signal.

AWC-SAC is supported on the following AP models and firmware versions:

- TQ6602: version 7.0.1-1.1 or later
- TQ5403/TQ5403e: version 6.0.1-6.2 or later
- TQ1402: version 6.0.1-7.1 or later

## Enhanced floor map support

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

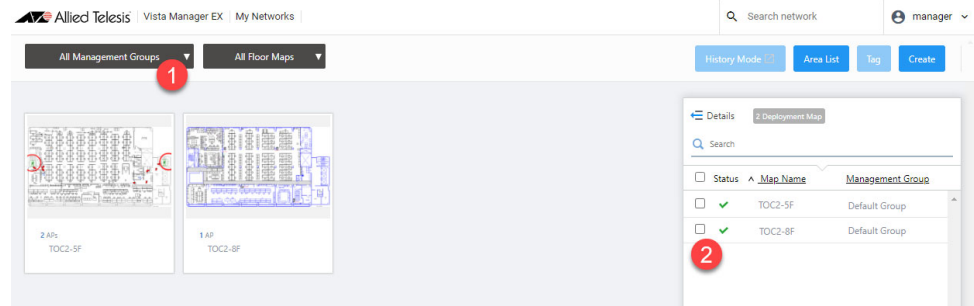
From version 3.8.0 onwards, the AWC plug-in floor map functionality is enhanced to display multiple floor maps simultaneously. There is a three-dimensional (3D) view available, enabling switching between the usual (panel) view and the new 3D view. Most of the functionalities are essentially similar to the Wireless Concierge feature implemented in version 3.7.0. This enhancement will also display the movement trajectory of wireless clients and Smart Connect topology links across floors.

This feature will allow users to:

- monitor multiple floors at one time
- track wireless clients moving across floors
- monitor radio wave power between APs and the connection status Smart Connect across floors.



## How to switch views



### How to switch to 3D floor map view:

1. Select a management group from the pull-down menu in the page heading.
2. Check one or more items in the list of floor maps on the right-hand panel.

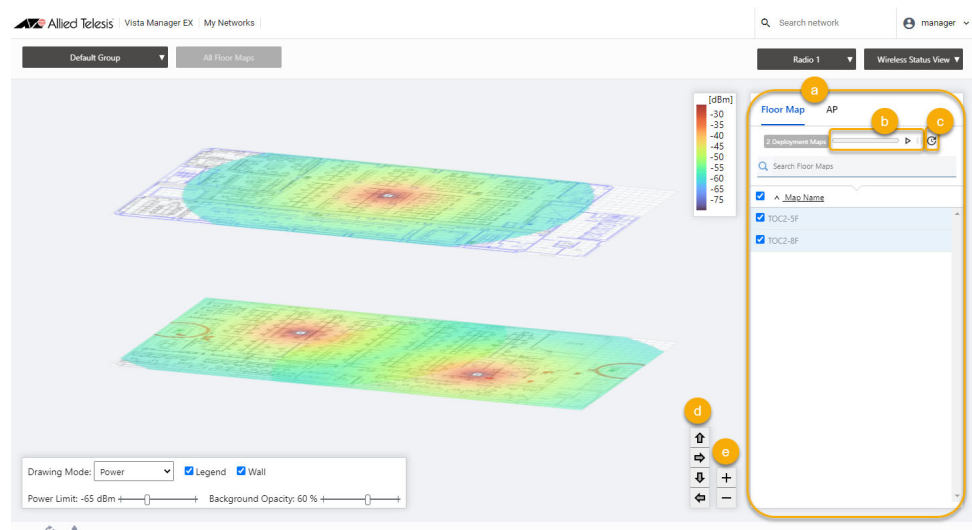
**Note:** When All Management Groups are selected from the pull-down menu, the 3D floor map view cannot be switched.

### How to switch to floor map panel view:

1. Select All Management Groups from the pull-down menu in the page heading.
2. Uncheck all items in the list of floor maps.
3. Refresh the page.

This 3D floor map enhancement is supported for **Wireless Status**, **Associated Client** and **Smart Connect** views. Enhanced floormaps will have these basic functionalities:

## 3D floor map in Wireless Status View



- a. On the right-hand panel, you can **switch (tabs)** between the list of floor maps and APs.

b. The **timer** for automatic updates is stopped by default. The timer also stops when you perform any of the following actions:

- « switch radios
- « select a 3D map from the list
- « change drawing mode
- « change power limit
- « switch tabs
- « switch views (timer initializes)

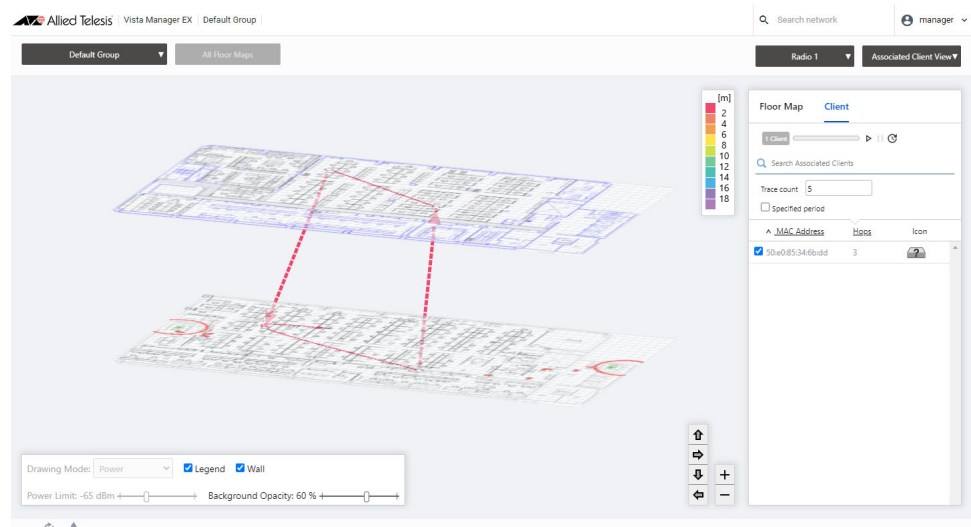
**Note:** You can change the setting of the refresh rates from **User Management > Refresh Rates** section.

c. You can update the page information manually using the **manual update** button.

d. The **top, right, bottom, left arrows** rotate 5 degrees in the direction clicked.

e. The **plus, minus buttons** zoom in and out about 1.1486 times.

## 3D floor map in Associated Client View

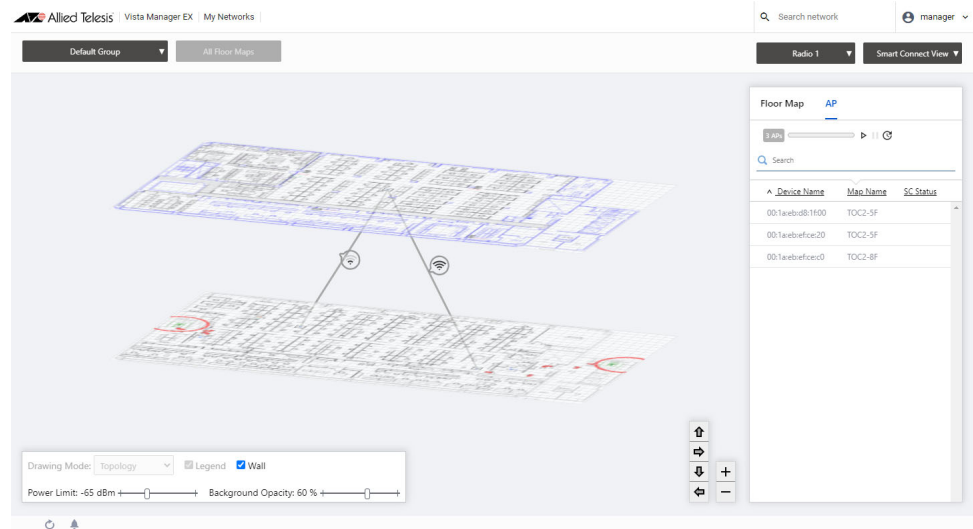


On the right-hand panel, you can switch (tabs) between the list of floor maps and clients. The timer for automatic updates is stopped by default. The timer also stops when you perform any of the following actions:

- « switch radios
- « select a client from the list
- « switch tabs
- « switch views (timer initializes)

**Note:** The update interval is **(Number of Associated Clients x 3) seconds**.

## 3D floor map in Smart Connect View

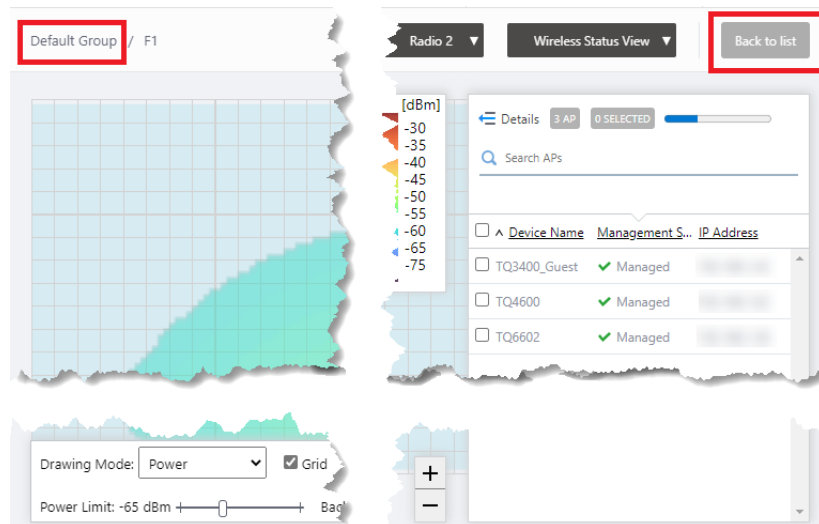


On the right-hand panel, you can switch (tabs) between the list of floor maps and APs. The timer for automatic updates is stopped by default. The timer also stops when you perform any of the following actions:

- « switch radios
- « switch tabs
- « switch views (timer initializes)

**Note:** The update interval is **(Number of Smart Connect floor maps x 3) seconds**.

## 2D floor map enhancements



On the 2D floor map page, these minor enhancements have been added:

- The header now displays the **management group name** and floor map name.
- Clicking the **Back to list** button brings you back to the floor map list page.

## Captive Portal support for TQ6602

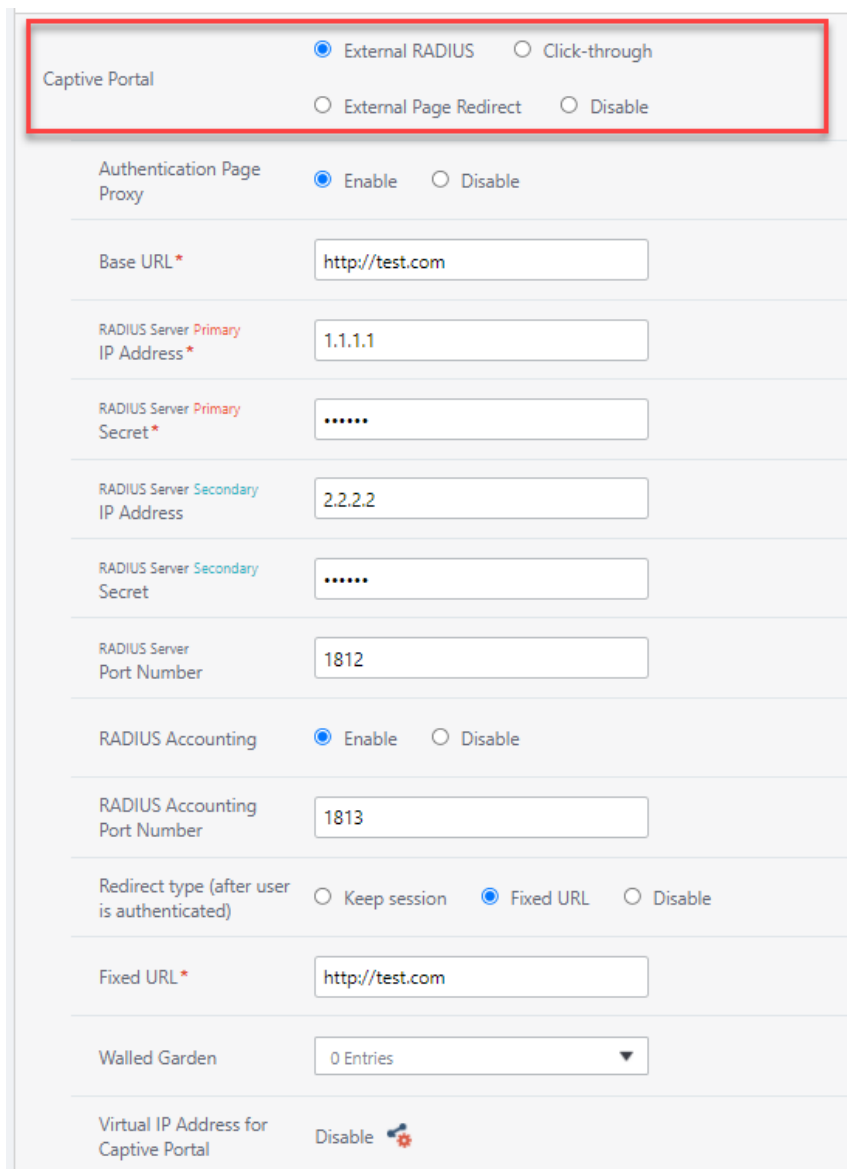
Applicable to Vista Manager installations with the AWC plug-in.

From version 3.8.0 onwards, the AWC plug-in will support Captive Portal for **Dual[11ax]** AP profiles. You can now apply this configuration to TQ6602 devices. Most of these settings are essentially similar to the Tri[11ac Wave2] profile. Applying an AP profile with Captive Portal enabled and SC profile to the same device is also supported.

Captive Portal is disabled by default and will have 4 initial options.

- External RADIUS
- Click-through
- External Page Redirect
- Disable

Selecting External RADIUS enables the full range of settings available.



Captive Portal

External RADIUS  Click-through

External Page Redirect  Disable

Authentication Page Proxy  Enable  Disable

Base URL \*

RADIUS Server Primary IP Address \*

RADIUS Server Primary Secret \*

RADIUS Server Secondary IP Address

RADIUS Server Secondary Secret

RADIUS Server Port Number

RADIUS Accounting  Enable  Disable

RADIUS Accounting Port Number

Redirect type (after user is authenticated)  Keep session  Fixed URL  Disable

Fixed URL \*

Walled Garden

Virtual IP Address for Captive Portal

Examples of a complete AP profile configuration on 3 different Captive Portal settings:

Captive Portal	External RADIUS
Authentication Page Proxy	✓ Enable
Base URL	http://test.com
RADIUS Server <b>Primary</b> IP Address	1.1.1.1
RADIUS Server <b>Primary</b> Secret	*****
RADIUS Server <b>Secondary</b> IP Address	2.2.2.2
RADIUS Server <b>Secondary</b> Secret	*****
RADIUS Server Port Number	1812
RADIUS Accounting	✓ Enable
RADIUS Accounting Port Number	1813
Redirect type (after user is authenticated)	Fixed URL
Fixed URL	http://test.com
Walled Garden	<a href="#">1 Entries</a>
Virtual IP Address for Captive Portal	1.1.1.1

Captive Portal	Click-through
Authentication Page Proxy	✓ Enable
Base URL	http://test.com
Redirect type (after user is authenticated)	Fixed URL
Fixed URL	http://test.com
Walled Garden	<a href="#">1 Entries</a>
Virtual IP Address for Captive Portal	1.1.1.1

Captive Portal	External Page Redirect
External Page URL	http://test.com
RADIUS Server <b>Primary</b> IP Address	1.1.1.1
RADIUS Server <b>Primary</b> Secret	*****
RADIUS Server <b>Secondary</b> IP Address	2.2.2.2
RADIUS Server <b>Secondary</b> Secret	*****
RADIUS Server Port Number	1812
RADIUS Accounting	✓ Enable
RADIUS Accounting Port Number	1813
Redirect type (after user is authenticated)	Fixed URL
Fixed URL	http://test.com
Walled Garden	<a href="#">1 Entries</a>
Virtual IP Address for Captive Portal	1.1.1.1

Captive Portal for AP profiles are also implemented in CB profiles for TQ6602 devices.

When a CB profile is applied to a device, the Captive Portal settings of the CB profile will take precedence over the AP profile settings.

However, CB profiles will not support settings particularly for **RADIUS Accounting**, **RADIUS Accounting Port Number** and **Virtual IP Address for Captive Portal**.

## Reauthentication timer settings

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

From version 3.8.0 onwards, the AWC plug-in will have reauthentication timer settings added to each VAP for the following AP profiles:

- Dual[11ax]
- Tri[11ac Wave2]
- Tri[11ac Wave2] with External Antenna
- Dual[11ac Wave2]

When configuring for Captive Portal, session timeout can be set. The allowed range is from 0 to 86400 seconds (0 seconds means timer is disabled). You can opt to re-authenticate or disconnect when the set time expires.

The screenshot shows the configuration page for Captive Portal. At the top, there are radio buttons for 'External RADIUS' (selected), 'Click-through', 'External Page Redirect', and 'Disable'. Below this is the 'Authentication Page' section with 'Enable' and 'Disable' (selected) radio buttons. The 'RADIUS Server Port Number' is set to 1812. A red box highlights the 'Session Timeout' field, which is set to 0 [sec], and the 'Session Timeout Action' section, which has 'Reauthentication' (selected) and 'Disconnection' radio buttons. Below this, 'RADIUS Accounting' is set to 'Disable' (selected).

When configuring WPA Enterprise for VAP security, the session key update interval can be set. The allowed range is from 0 to 86400 seconds (0 seconds means timer is disabled). You can opt to re-authenticate or disconnect after a set update interval.

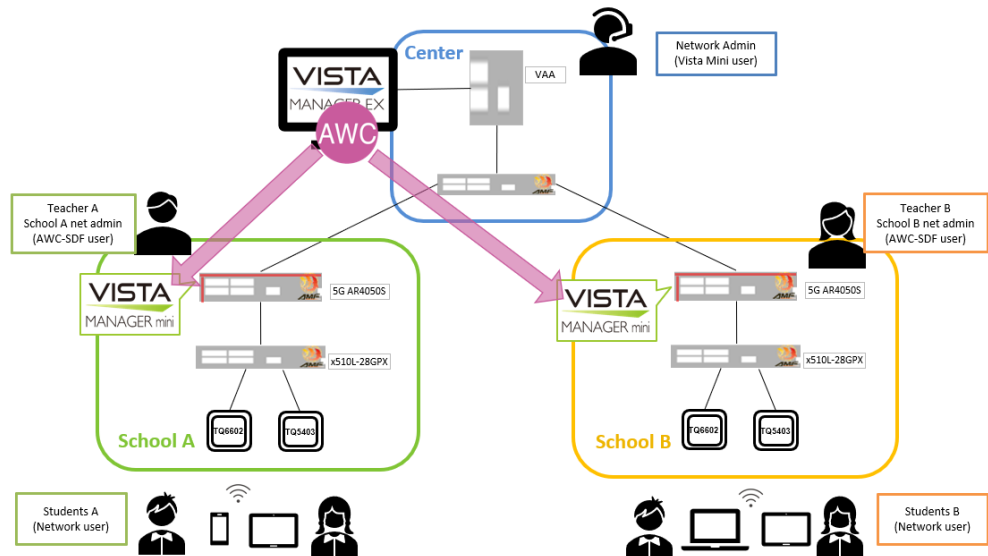
The screenshot shows the configuration page for WPA Enterprise security. At the top, there are radio buttons for 'None', 'WPA Personal', 'WPA Enterprise' (selected), and 'OSEN'. Below this is the 'Encryption Protocol' section with 'CCMP' (selected) and 'TKIP' radio buttons. The 'Management Frame Protection' section has 'Required', 'Capable' (selected), and 'Disable' radio buttons. The 'Broadcast Key Refresh Rate' is set to 0 [sec]. A red box highlights the 'Session Key Refresh Rate' field, which is empty [sec], and the 'Session Key Refresh Action' section, which has 'Reauthentication' (selected) and 'Disconnection' radio buttons. Below this, 'RADIUS Accounting' is set to 'Disable' (selected).

## Sky Defender (AWC-SDF)

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

This feature was described in the previous release note (version 3.7.0) as the Client Filter. It is now officially known as **Sky Defender (AWC-SDF)**.

Functionalities remain the same. By installing the AWC-SDF utility, Vista Manager EX is able to detect MAC addresses of all Bring Your Own Device users in a school network. After permission is granted by an administrator user, teachers can easily collect MAC addresses of their students' devices and monitor their connection status. Allow/deny connections to the AP device can then be set for the collected MAC addresses.



For this feature to be fully supported, a working configuration is required across Vista Manager EX, Vista Manager Mini, AWC-SDF and the necessary AP devices. Refer to the [User Guide: Autonomous Wave Control \(AWC\) Plug-in](#) for the complete configuration.

---

# 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 5.5.1-2.1 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 7.0.1-1.1 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 or later. Some of the latest functionality is not supported.

## Internet Explorer 11 compatibility

When using the Vista Manager EX 3.8.0 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.

Do **not** delete a plug-in from Vista Manager during a version upgrade. No de-registering or re-registering of plug-ins is required during this time. If for any reason connections to plug-ins need to be restored, you can update a plug-in without deleting it. Refer to the Troubleshooting chapter.

## 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 3.8.0, 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](http://our website, alliedtelesis.com).

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

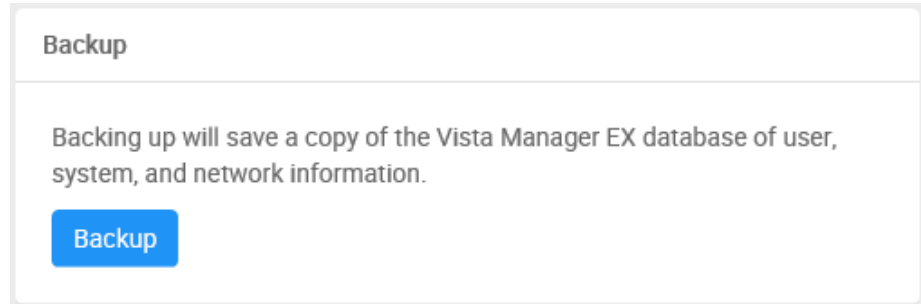
- the [AMF Feature Overview and Configuration Guide](#)
- the [AMF Datasheet](#)
- the [AMF Cloud \(VAA\) Installation Guide](#).

---

# 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.



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.

[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'.

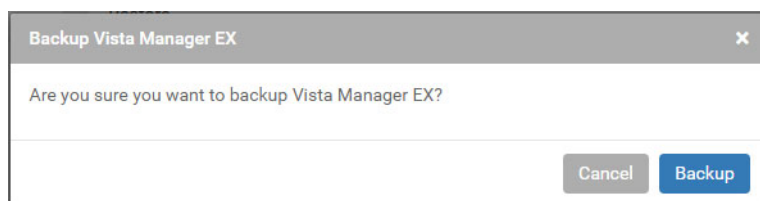
*Do not rename these files. The installation requires them to be in this format.*

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 Database Management 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.

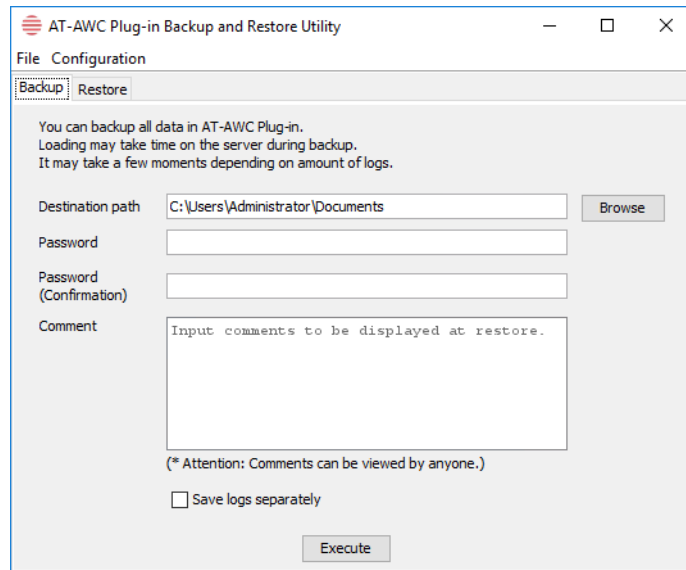
## Backup the AWC plug-in

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.

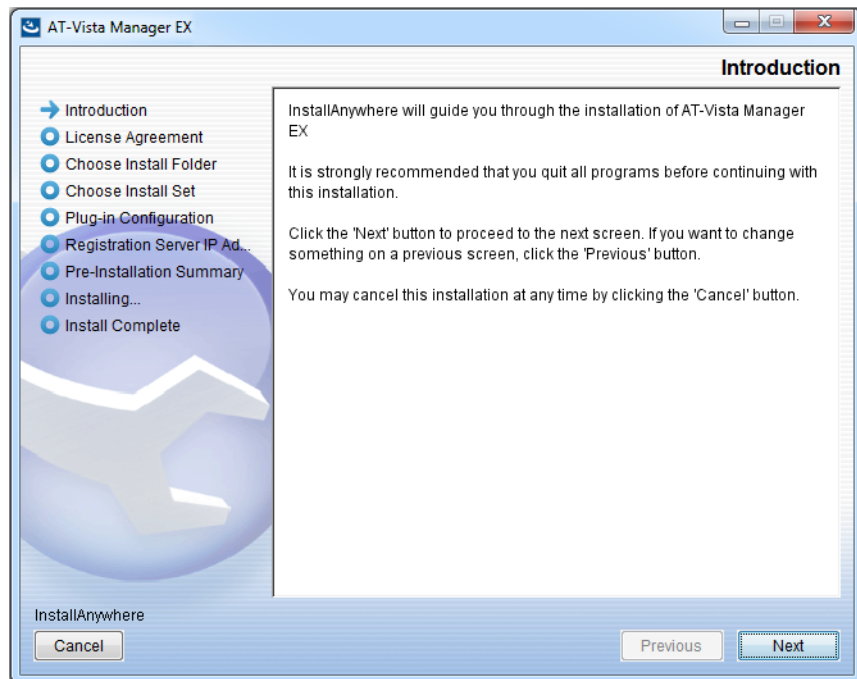
---

## Install the new version

21. Execute the Vista Manager EX installation program 'atvmexXXXbXXw.exe'.

**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**.

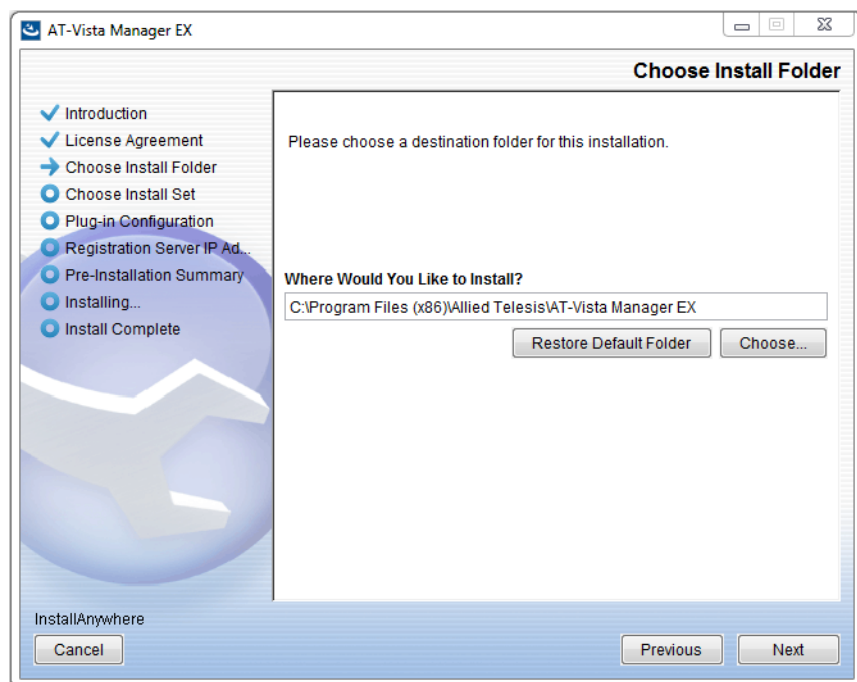
23. The **License Agreement** dialog displays:



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

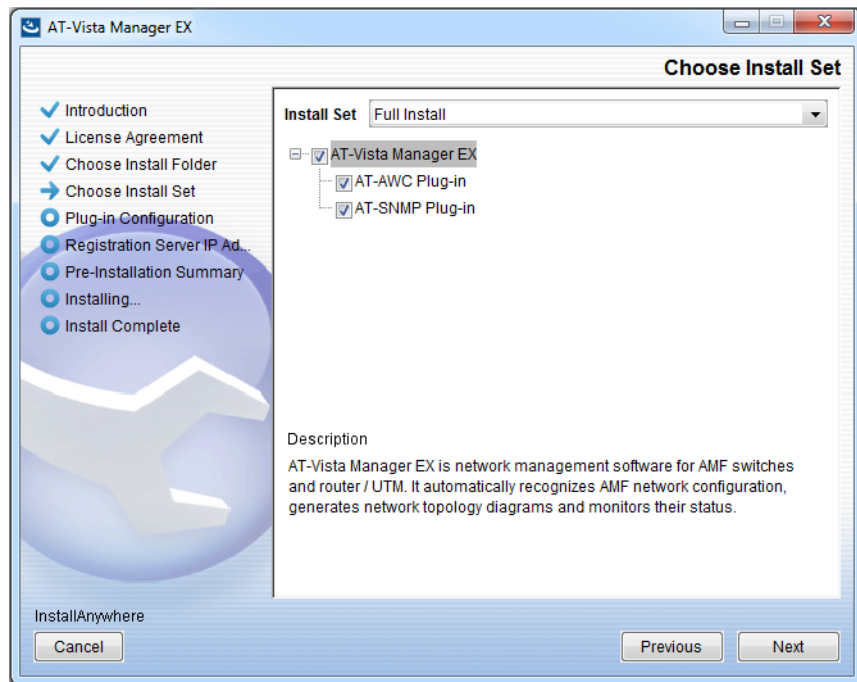
- Click **I accept the terms of the License Agreement**
- Click **Next**

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



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

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



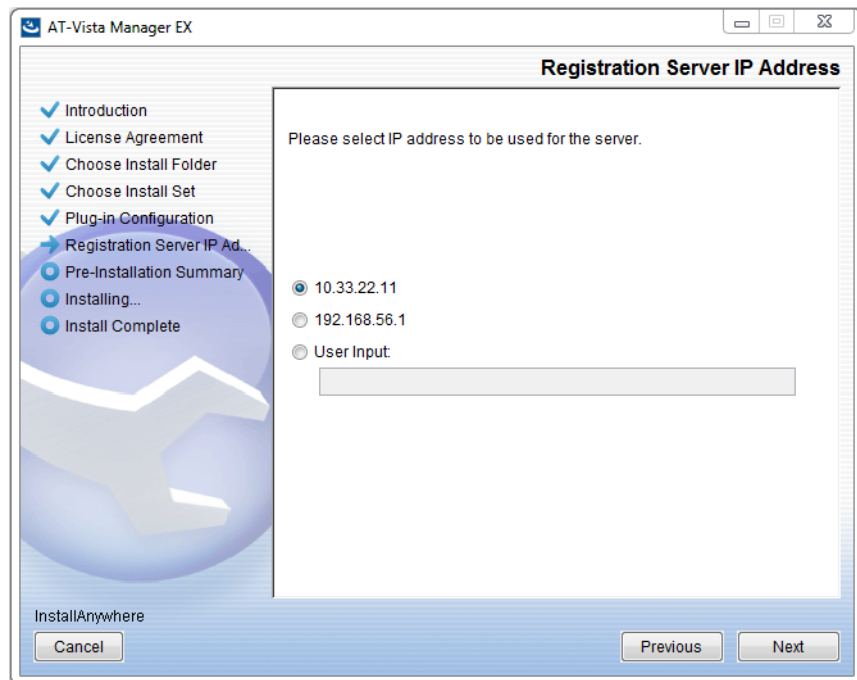
Select **Full Install** from the drop down list. By default all plug-ins are selected. Clear the check box for any plug-ins you do not wish to install. Click **Next**.

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



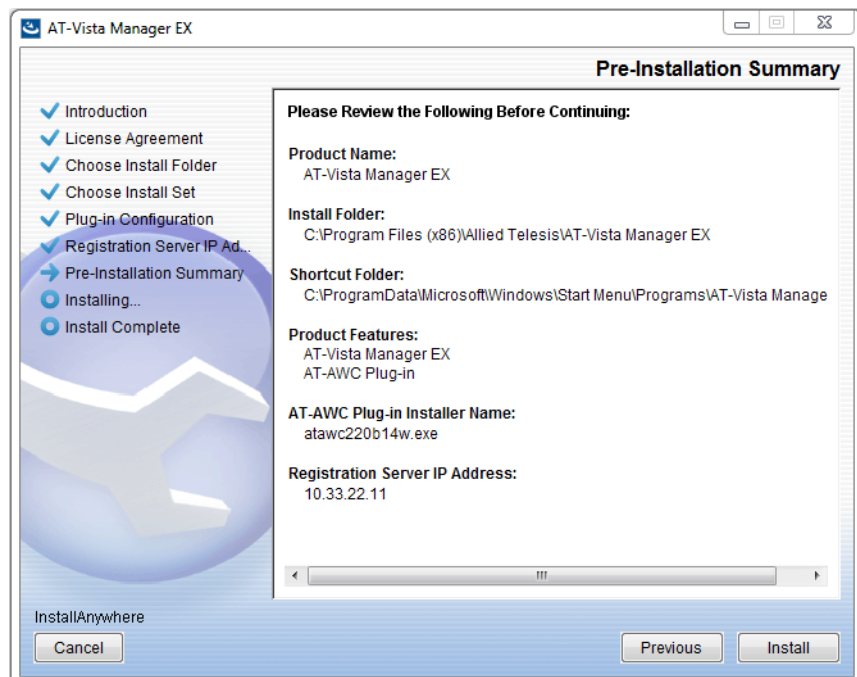
Select **Do not create a public key** unless you are intending to use the plug-ins in standalone mode. For more information on standalone mode, refer to the Installation Guide. Click **Next**.

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**.

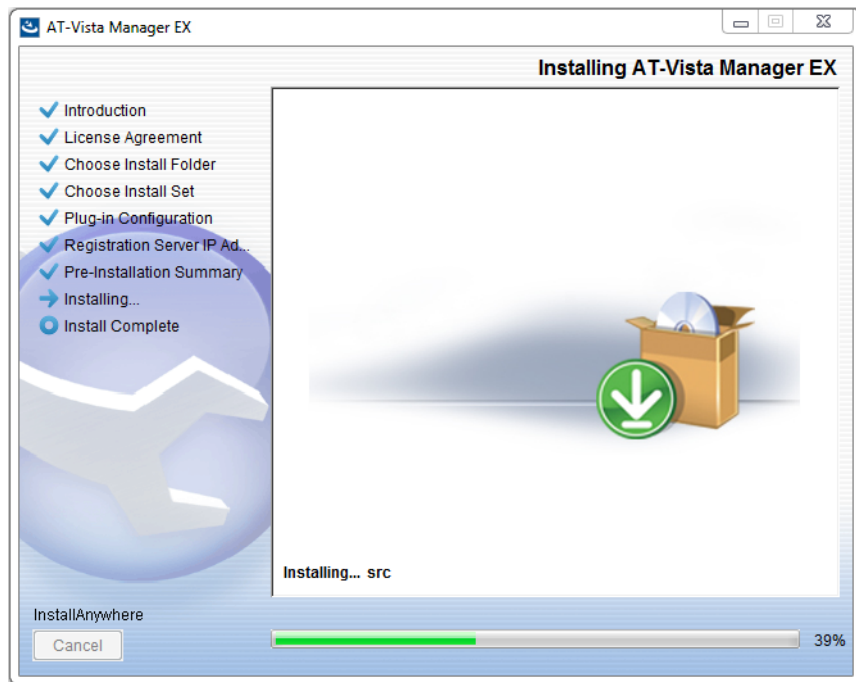
28. The **Pre-Installation Summary** dialog displays:



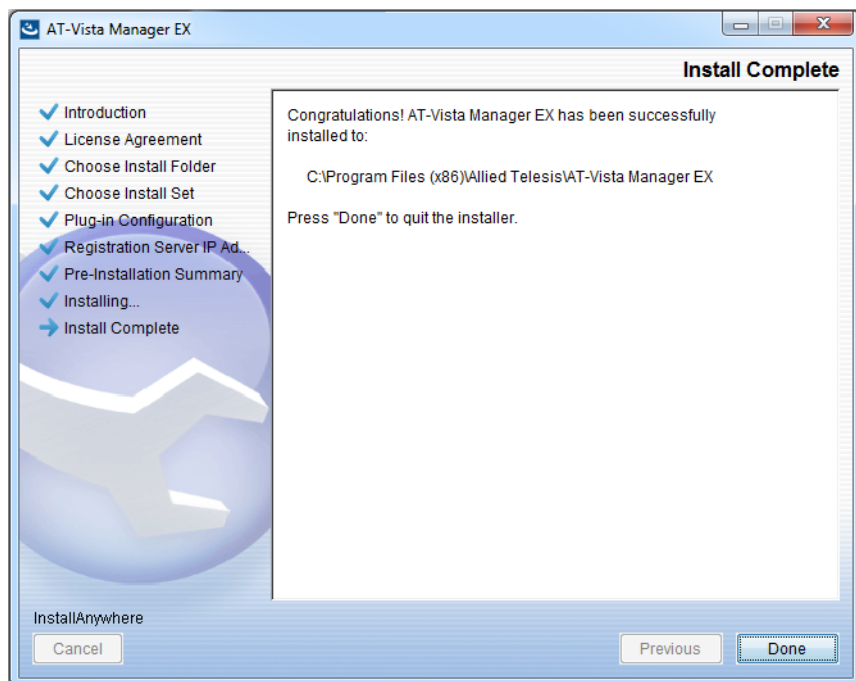
Check that your Product Name, Install Folder, Shortcut Folder, Product Features, Plugin Installer Name and Registration IP Address are correct, and then click **Install**.



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



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

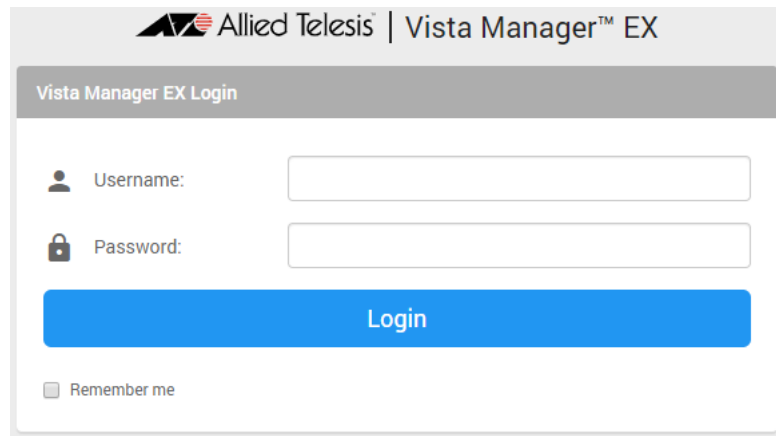


Check that the installation has completed successfully and click **Done**.

## Restore the Vista Manager database

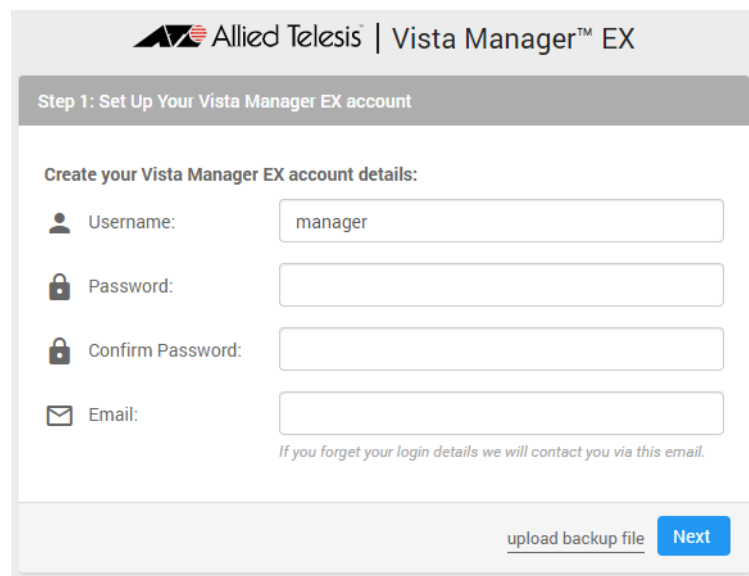
After the upgrade is complete, you need to restore the Vista Manager database. To do this, use the following procedure.

31. Login to Vista Manager.



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

32. Click on upload backup file.

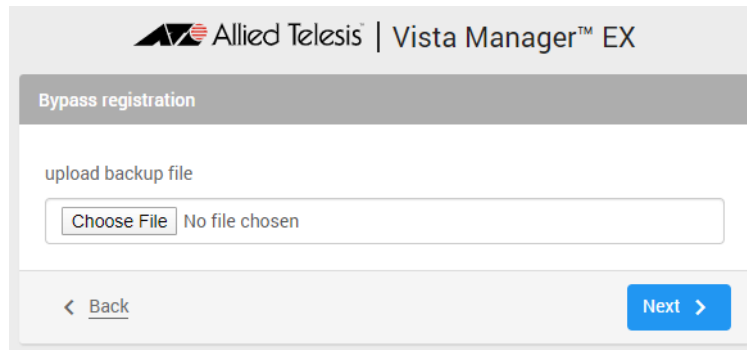


**Caution** Your serial number and license information are part of your database backup. If you upload the backup file when upgrading, you will keep the same serial number, and your licensing will continue to work without interruption.

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

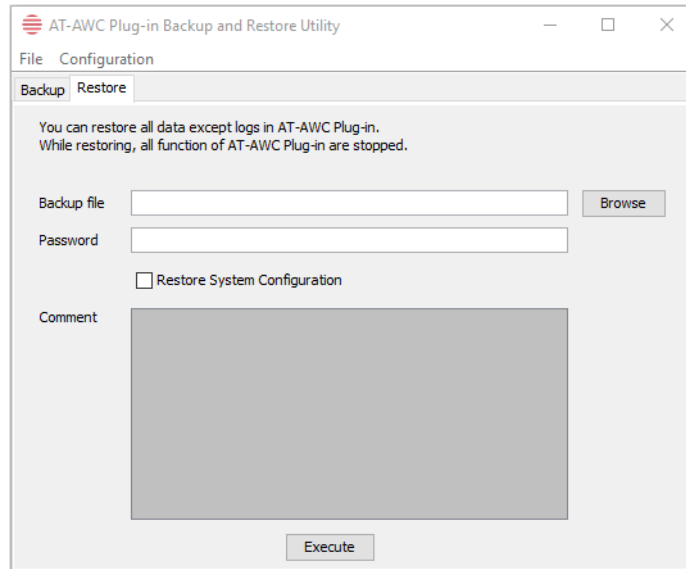
34. If you have the SNMP plug-in installed then log on locally to the Vista Manager EX server.
35. Stop the SNMP server services using the shortcut or by running the following command line.  
**"<Vista Install Path>\Plugins\AT-SNMP\NetManager\bin\svrcmd.bat" svrstop**
36. Run the restore utility by using 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.



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](#).

## Upgrading Vista Manager on VST-VRT

See the [Vista Manager Virtual \(VST-VRT\) User Guide](#).

## Troubleshooting

See the Troubleshooting chapter in the [Vista Manager EX User Guide](#).