

Release Note for Vista Manager EX Software Version 3.5.x



VISTA MANAGER™ EX

» 3.5.0

Acknowledgments

©2020 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/

What's New in Vista Manager EX v3.5.0	2
Important Considerations Before Upgrading.....	34
Obtaining User Documentation.....	36
Upgrading Vista Manager as a virtual appliance	37
Upgrading Vista Manager as a Windows-based installation.....	38
Information After Upgrading	48

What's New in Vista Manager EX v3.5.0

Introduction

This release note describes the new features in Vista Manager EX™ v3.5.0. 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 v3.5.0:

- “AIO - Dynamic Connection” on page 3
- “AIO - Internet Breakout” on page 6
- “AIO - Auto Traffic Shaping” on page 8
- “AIO - Application Priority” on page 9
- “AIO - Security” on page 13
- “Enhanced traffic legend with multi-gigabit speed links” on page 16
- “Event filter support” on page 17
- “Enhancements to Captive Portal” on page 18
- “Wi-Fi Alliance certified Passpoint® (Hotspot 2.0) support and WiFi4EU” on page 22
- “Multi select deletion from MAC address list” on page 28
- “Enable MAC address list and external RADIUS” on page 29
- “AMF Application Proxy and Critical Mode” on page 31
- “SNMPv3 now supported on Access Points via Vista Manager EX” on page 32
- “Creating static links on the network map” on page 32
- “Background image shows on dashboard map” on page 32
- “Improvements to firmware distribution” on page 33

Allied Intent-based Orchestrator (AIO)

Applicable to all Vista Manager installations.

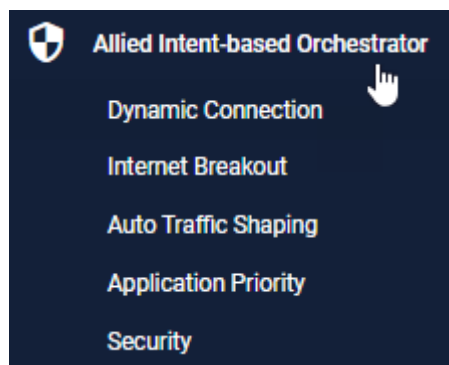
From Vista Manager EX version 3.5.0 onwards, the Allied Intent-based Orchestrator (AIO) provides network optimization, automation, management, and visualization. The uniquely designed intent-based configuration, reporting and map facilities of Vista Manager EX make these powerful tools simple to configure, initiate, and manage. AIO offers automation of branch security and WAN bandwidth management.

For this feature to become fully available to you and all menu items activated, install the feature license. This license is separate from the rest of Vista Manager EX and is included in the existing 90 day trial license, which includes Vista Manager EX running on the appliance box.

The AIO feature is made up of several components.

- Dynamic Connection
- Internet Breakout
- Auto Traffic Shaping
- Application Priority
- Security

Access the Allied Intent-based Orchestrator from the sidebar menu.



For more information about configuring and using the AIO, refer to the “Using the Allied Intent-based Orchestrator feature” chapter in the [Vista Manager User Guide](#).

AIO - Dynamic Connection

Applicable to all Vista Manager installations with the AIO feature.

This feature lets you use the simplicity of drag-and-drop on the network map, to create new VPN tunnels between the AR-Series devices (firewalls or routers) at different locations across your WAN.

- Point-to-point tunnels require a source device and destination device.
- Point-to-multipoint tunnels require a source device and multiple destination devices.

To create a tunnel, both devices must be part of the AMF network, and be running firmware version AlliedWare Plus 5.5.0-2.x or later.

You cannot create multiple tunnels with the same source and destination interface pair (e.g. eth1). Split up the interface if you wish to create more than one tunnel, for example, split eth ports into sub interfaces. You may create another tunnel with the same source interface as long as the destinations are on different devices.

All tunnels are encrypted with IPSec to secure your WAN traffic. Each tunnel will have a different crypto key with a unique name.

Option 1: Create a Point-to-Point Tunnel

The screenshot shows the 'Create Point to Point Tunnel' dialog box. On the left, a vertical toolbar contains a pencil icon (1) and two device icons connected by a line. The dialog is titled 'Create Point to Point Tunnel' and shows configuration options for two devices: AR4050S and AR2010V. The configuration fields are: Tunnel Mode (GRE, 2), Tunnel Interface (eth1, 3), Tunnel IP Address (172.28.0.1, 4) with Subnet (/30), Tunnel Description (AKL-source, 5), Tunnel Routing (No Routing, 6), Tunnel Interface (eth2, 7), Tunnel IP Address (172.28.0.2, 8) with Subnet (/30), and Tunnel Description (NSN-destination). At the bottom are 'Check connectivity' (8), 'Cancel', and 'Create' (9) buttons.

1. Use the pencil icon to draw a line between devices (firewalls/routers) at the two locations you wish to connect with a new VPN tunnel.

2. Next, set up tunnel options. Select tunnel mode.

3. Select an interface for the tunnel to be on.

4. Vista Manager EX generates the tunnel interface IP addresses. The subnet prefix is /30.

Note: If you choose your own IP address, it must be in the same subnet and must not be used on another interface on those devices.

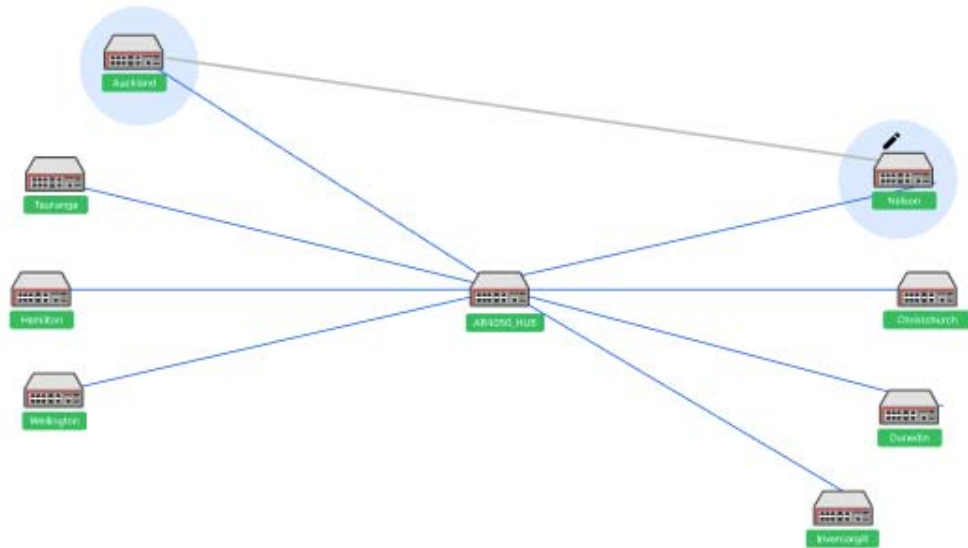
5. Enter a description name for the tunnel.

6. Configure tunnel routing.

Note: The options here are default or static. You may enter IP addresses for each end of the tunnel by selecting static routing.

7. Repeat steps 3-6 to set up tunnel options for the destination device.
8. Click **Check connectivity**. There should be a ping from the source interface to destination interface if there is a connection.
9. Click **Create** when complete.

Option 2: Create a Point-to-Multipoint Tunnel



1. Click on the pencil icon and select point-to-multipoint tunnel.
2. Use the pencil icon to first select a tunnel hub. This is usually a head office router.
3. Next, select spokes one by one. These should be your branch offices.
4. Perform Option 1 steps 2-6 to set up tunnel options.

Note: In version 3.5.0, adding a static route to the hub of a multipoint tunnel is not supported.

5. Repeat for all your spokes (branch offices).
6. Click **Check connectivity**.
7. Click **Create** when complete.

Note: For multipoint tunnels, a hub of a multipoint tunnel cannot share the same interface (with the same IP address) as a GRE point-to-point tunnel.

Note: Connectivity is not needed for the new tunnel configuration to be created, although the tunnel will not be fully formed until there is a connection.

AIO - Internet Breakout

Applicable to all Vista Manager installations with the AIO feature.

Internet Breakout lets specific applications being used at branch office locations access the Internet directly, rather than going via the head office. This improves the performance of cloud-based applications (e.g. Office 365) and reduces traffic volumes on VPN connections between branch offices and the head office.

- This feature requires AR-series devices to run AlliedWare Plus 5.5.0-2.1 or later.
- Before configuring, start by identifying the types of applications you may want to allow direct Internet access.
- Enabling this feature reduces router throughput.
- Any traffic that bypasses security processing may reduce security and threat protection at the local branch office. Carefully consider the potential consequences of giving direct Internet access to a type of traffic, and whether additional local or cloud-based security needs to be implemented to protect Internet Breakout traffic and the branch office.
- Internet Breakout needs to classify applications for sending direct to the Internet. It does this most effectively when it can read both incoming and outgoing traffic on the interface that was/is sending those applications to the head office. For IPSec protected tunnels, this requires a feature called tunnel security reprocessing. Vista Manager does not enable tunnel security reprocessing because it reduces router performance. To enable it, enter the following commands on the router's CLI:

```
enable  
conf t  
tunnel security-reprocessing
```

Step 1: Enable Internet Breakout and specify the traffic path.

Use the Internet Breakout > General tab

1. Enable Breakout on the AR-series firewall at each desired location.
2. Select the interfaces to break from and break to.
3. Enter the next hop address.
4. Click **Apply Changes**.

BranchOffice-Firewall Cancel Apply Changes

General Breakout Monitoring

Breakout 1

Break From 2
tunnel1 x ▾

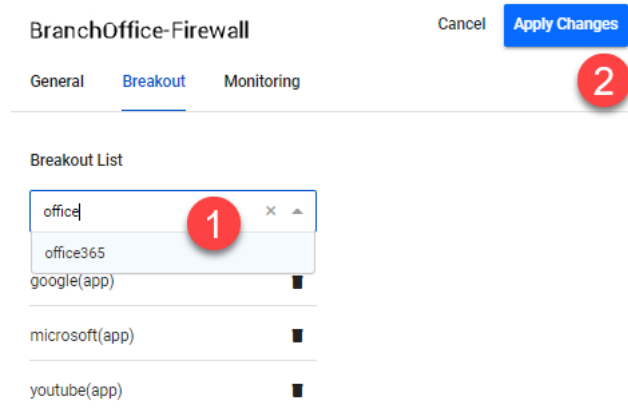
Break To 2
eth1 x ▾

Next Hop 3
1.1.1.1

Step 2: Add applications to break out.

Use the Internet Breakout > Breakout tab

1. Add applications to the Breakout List, for example, Office365, Google, Youtube, etc.
2. Click **Apply Changes**.

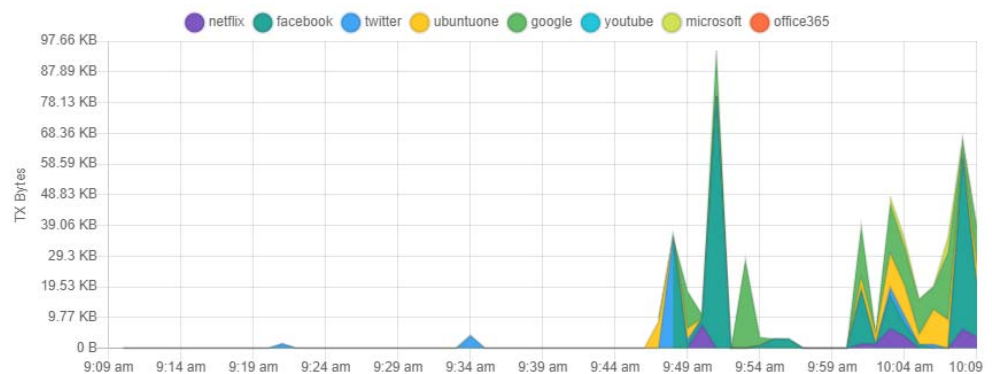


Step 3: Monitor the breakout.

Use the Internet Breakout > Monitoring tab

Two charts are available here:

- The pie chart shows top 5 breakout applications. Clicking applications on the vertical legend adds/removes them to/from the chart.
- The line graph shows breakout traffic over a set period of time. Clicking applications on the horizontal legend or using the dropdown list adds/removes them to/from the graph.



AIO - Auto Traffic Shaping

Applicable to all Vista Manager installations with the AIO feature.

This feature dynamically adjusts the maximum transmit capacity of remote locations (spoke tunnels) to not exceed the receive capacity of the central site (hub). This is termed the **maximum Rx bandwidth** of the hub.

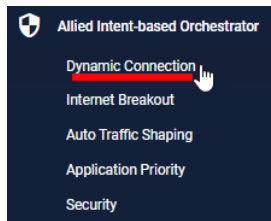
To allocate this bandwidth optimally, we recommend you also deploy Application Priority profiles on each spoke tunnel.

To manage traffic, an algorithm uses current spoke tunnel traffic rates, and any configured application priority settings, across all spoke tunnels to fairly allocate bandwidth. Spoke tunnels have a guaranteed transmit bandwidth. This equals the sum of the CIRs (committed information rate) plus system bandwidth defaulted to 5%.

Prerequisite Step: Configure tunnels between spokes and hubs.

Use the Allied Intent-based Orchestrator > Dynamic Connection feature

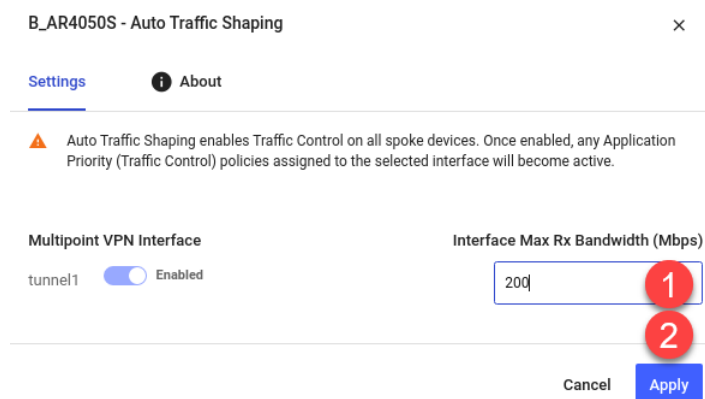
This step requires you to navigate away from Auto Traffic Shaping.



Step 1: Configure the Interface Max Rx Bandwidth value.

Use the Auto Traffic Shaping > Settings tab or button

1. Enter the maximum bandwidth a hub can handle. The algorithm calculates and applies optimal traffic shaping based on this number.
2. Click **Apply**.



Step 2: Monitor hub utilization and traffic loss.

Use the Auto Traffic Shaping > Monitoring tab

View charts in the Monitoring page, where you can use filters to specify what traffic is shown.



AIO - Application Priority

Applicable to all Vista Manager installations with the AIO feature.

Application Priority enables you to choose specific applications and prioritize or deprioritize them. This ensures your most important business traffic is prioritized for transmission between locations across your WAN. Vista Manager EX provides 3 priority classes:

- **Essential**
- **Business Relevant**
- **Non-essential**

You can assign different applications to each priority class, save the assignment in a policy, and deploy the policy on the AR-Series device (firewall or router) at each location in your WAN.

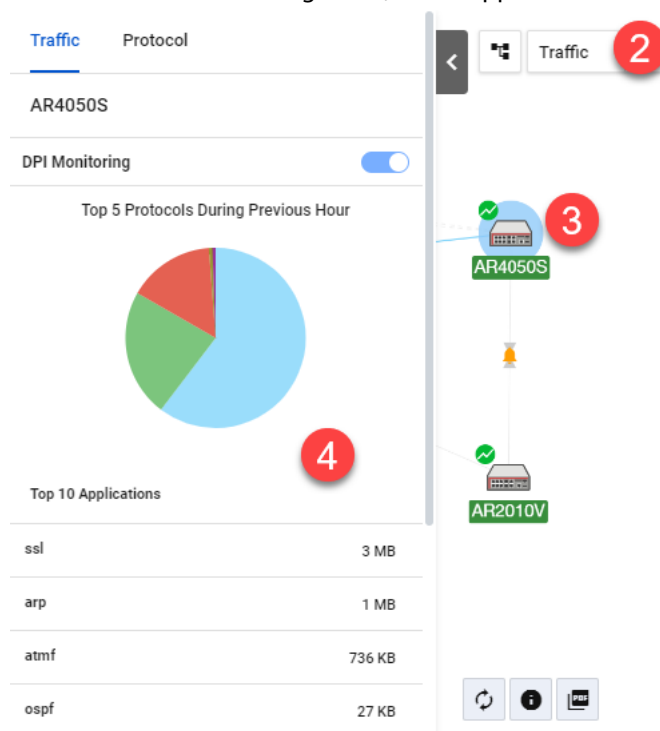
A policy is the overall title for a set of rules and priorities. It also defines the type of algorithm for how it calculates the priority of traffic. Traffic for any unassigned applications set in the rules will fall into the **Default** policy class. The default class is not directly visible when creating a policy, but the traffic matching the default class (either in throughput or packet loss) can be seen in the Monitoring graphs.

This feature lets you view any existing Application Priority policies, and shows throughput and packet loss graphs for devices that have a policy deployed on them.

Vista Manager EX application usage data lets you better prioritize applications. When creating or deploying policies, you can analyze current traffic present on a device, which helps you assign applications into the most appropriate priority classes for a policy.

Step 1: Check application usage on a device.

1. Navigate to the Network Map.
2. Select **Traffic** mode from the dropdown list.
3. Select the device you want to check. A blue circle appears around it.
4. Examine the traffic usage data, which appears in the left-hand panel.



Step 2: Create an Application Priority policy.

1. To create a policy, you may:
 - Right-click on the device in Traffic mode of the Network Map and select Application Priority > Add Policy, or
 - Navigate to the Application Priority menu item and click **+Add Policy**, or
 - Navigate to the Application Priority menu item, and **clone** an existing policy by clicking the 3 dots for that policy, in the Action column.

All of the above approaches open the Add Policy page.

2. Next, type in a policy name. For example, **"Branch-Office"**.
3. Select an Application Provider. By default, Built-in is selected. If you have bought an Advanced Firewall licence for your AR-Series UTM firewall, select Procera instead,

which enables a much larger application list to work with. On the righthand panel, choose a Category of applications. For example, **Remote Access**.

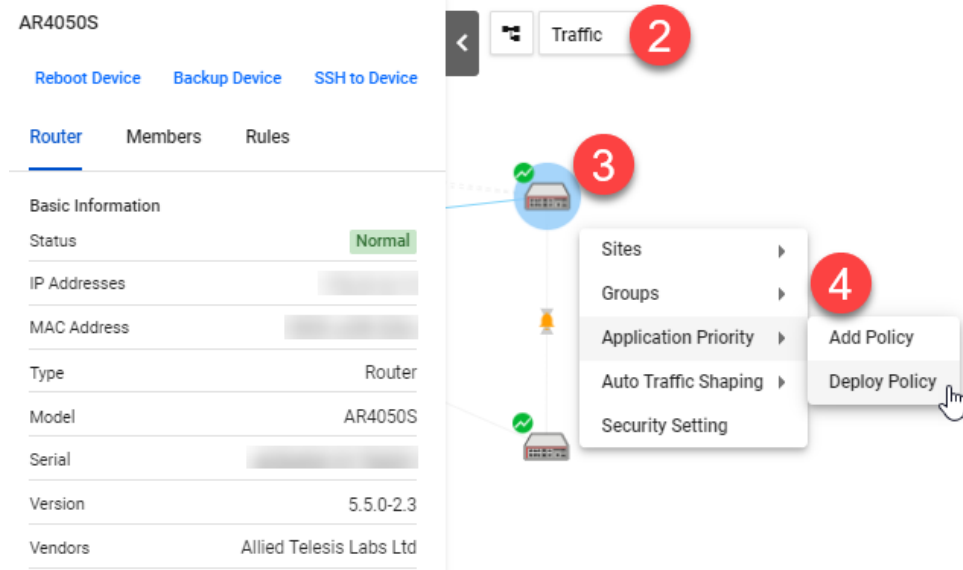
4. A list of applications will appear. Assign appropriate classes to the relevant applications. You can use the Assigned Class filter at any point to see what applications you have assigned to a class.
5. When you assign a class, it appears on the color-coded policy classes on the left. Here, you may adjust the bandwidth for each class. To do this, either type in a percentage or move the slider.
6. If you have accessed the page via the Network Map, click **Save and Deploy**. Otherwise, click **Save**.

The screenshot shows the 'Add Policy' configuration interface. At the top left, there is a back arrow and the title 'Add Policy'. Below this, there are two input fields: 'Policy Name*' with the value 'Branch-Office' (callout 2) and 'Application Provider' with a dropdown menu set to 'Built-in' (callout 3). On the right side, there are 'Cancel' and 'Save' buttons (callout 7). The main area is divided into two sections for policy classes. The first section is 'Class: Essential' (highlighted in red), showing a 'Percentage of bandwidth allocated' slider set to 34 (callout 4) and a list of 'Applications (3)' including 'Citrix', 'Rdp', and 'ssh' (callout 6). The second section is 'Class: Business Relevant' (highlighted in orange), showing a 'Percentage of bandwidth allocated' slider set to 33 and a list of 'Applications (2)' including 'teamviewer' and 'telnet'. On the right side, there is a search bar 'Search applications' and a table with columns 'CATEGORY' and 'Assigned class'. The table lists applications like 'Citrix', 'Pcanywhere', 'Rdp', 'Ssh', 'Teamviewer', 'Telnet', and 'Vnc' with their assigned classes (callout 5). At the bottom right, there is a pagination indicator '1 to 7 of 7' and navigation arrows.

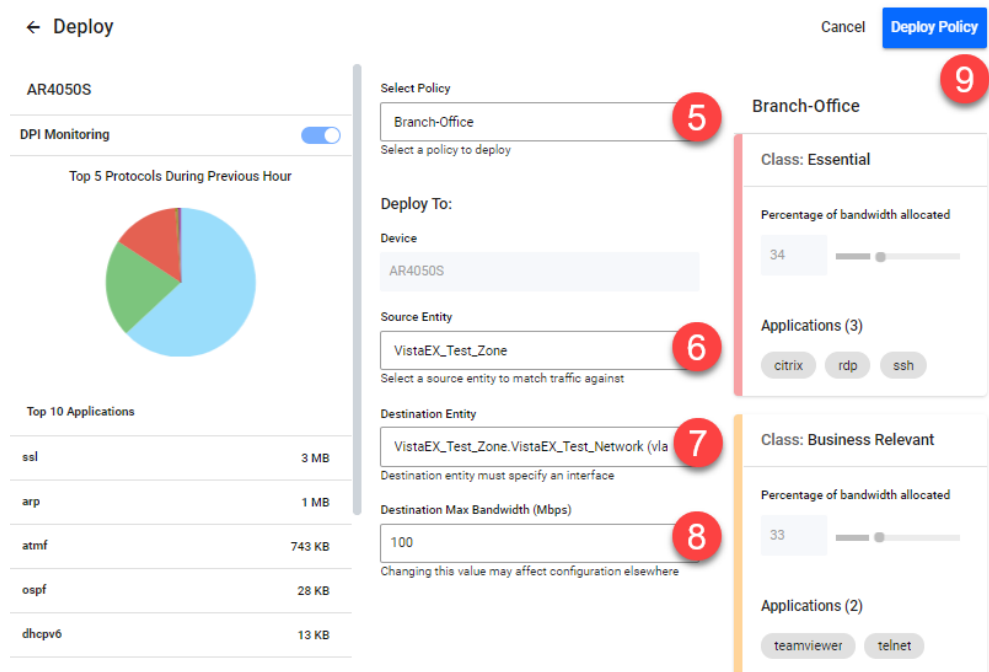
Step 3: Deploy a policy.

1. Navigate to the Network Map.
2. Select **Traffic** mode from the dropdown list.
3. Select the device you want to deploy a policy to. A blue circle appears around it.

- Right-click on the device, select Application Priority > **Deploy Policy**.



- Select a policy to deploy.
- Specify a **Source Entity** to match traffic against.
- Specify an interface for **Destination Entity**.
- Define a **maximum bandwidth**. This places a cap on the virtual bandwidth.
- Click **Deploy Policy** when complete.



AIO - Security

Applicable to all Vista Manager installations with the AIO feature.

The security feature lets you configure the web control and IP reputation features on the UTM firewalls at a number of locations simultaneously, for centralized and simplified management.

- **Web control** offers an easy way to monitor and control the types of websites viewed by employees.
- **IP reputation** blocks employee access to websites that are known source of spam, viruses and other malicious activity, to protect your network against security threats.

The overall security feature allows you to enable recommended security settings for a group of UTM firewall devices based on an industry type and security strength. This simplifies the process as there is no need to manually choose website or reputation categories for each device.

Note: For this feature to be fully functional, you may need to do additional configuration in the device GUI. Internet access and domain name lookup are required. Enable the ATL Live update server in order to download and check for IP reputation or web control updates.

Step 1: Enable security features and select industry settings.

Use the Security > General tab

1. Enable **IP Reputation** and **Web Control** for the desired device group(s).
2. Select the industry type (e.g. school).
3. Set a time to check for updates.
4. Select the desired security strength for the industry (e.g. medium).
5. Click **Apply Changes**.

CanterburyHigh 5 [Apply Changes](#)

[General](#) [Advanced IP Reputation](#) [Advanced Web Control](#) [Monitoring](#)

Security Features

IP Reputation Enabled 1

Web Control Enabled

Industry 2

High School x ▾

Check for updates every 3

24 hours ▾

Industry Strength 4

Low **Medium** High

Step 2: Edit advanced IP reputation settings if required.

Use the Security > Advanced IP reputation tab

1. Click **Edit Industry Settings**.

CanterburyHigh 3 [Apply Changes](#)

General [Advanced IP Reputation](#) Advanced Web Control Monitoring

Industry Strength Check for updates every

Low **Medium** High 24 hours

Industries 1

Custom [Edit Industry Settings](#)

Infant School [View Details](#)

Elementary School [View Details](#)

Junior High School [View Details](#)

High School [View Details](#)

2. **Permit, alert, or deny** a reputation category action as needed.
A warning appears if one or more devices in the group have had different IP reputation or Web Control settings already applied via another group.

IP Reputation	Permit	Alert	Deny
Abused TLD	Permit	Alert	Deny
Bitcoin Related	Permit	Alert	Deny
Blackhole	Permit	Alert	Deny
Bot	Permit	Alert	Deny

3. Click **Apply Changes**. This changes the industry type to Custom.

Step 3: Edit advanced Web Control settings if required.

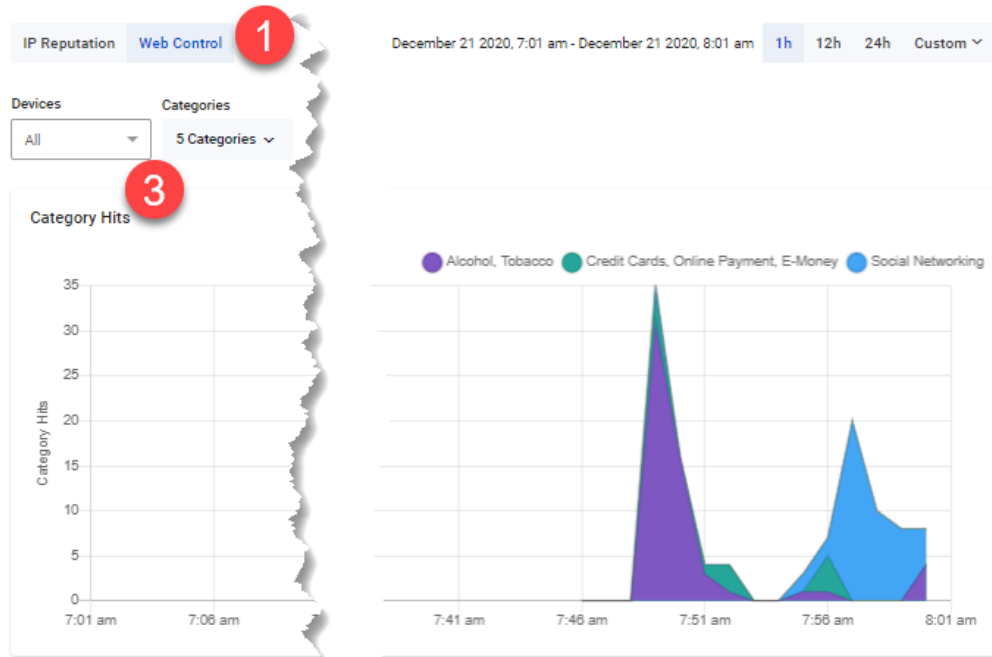
Use the Security > Web Control tab

1. Click **Edit Industry Settings**.
2. **Permit or deny** website categories as needed.
A warning appears if one or more devices in the group have had different IP reputation or Web Control settings already applied via another group.
3. Click **Apply Changes**. This changes the industry type to Custom.

Step 4: Monitor Web Control and IP Reputation performance.

Use the Security > Monitoring tab

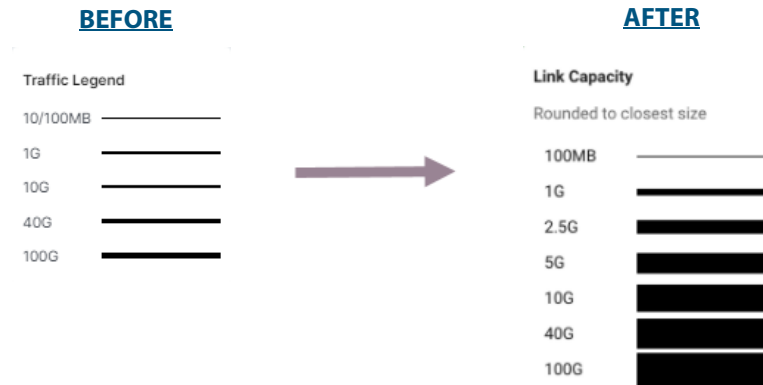
1. Click on the IP Reputation and Web Control buttons to view respective graphs.
2. For IP Reputation, click the dropdown list to select the UTM firewall device from a specific location to view.
3. For Web Control, click the dropdown list to select the UTM firewall device from a specific location to view. Clicking Categories on the legend or dropdown list lets you add/remove categories to view on the graph.



Enhanced traffic legend with multi-gigabit speed links

Applicable to all Vista Manager installations.

From version 3.5.0, the traffic-link capacity legend on the integrated maps has been updated to clearly represent the interface speeds. The thickness of a link is rounded to the closest speed appearing in the legend. This was unclear, although Vista Manager EX already supports any link speed on AlliedWare Plus devices prior to version 3.5.0. Users may have previously thought that only speeds listed in the legend were supported.



Event filter support

Applicable to all Vista Manager installations - (For Admin users)

From Vista Manager EX version 3.5.0, you can create event rules to notify you whenever certain events occur, such as a port goes up/down, configuration on a device is changed or a fan or power supply failure occurs.

Previously, you had to be actively looking at Vista Manager to notice these things. Now you can simply check your emails.

You can also place an alarm on an event rule to identify it as a critical event. Critical events have a dismissible red alarm icon showing next to them in the **Event Log** window. You can decide if the alarmed event requires immediate action or dismiss it as a normal alert.

To create an event rule:

1. From the left-hand menu, select **Events**
2. From the **Event Log** tab, select an existing event.
3. In the **Action** column, click on the three vertical dots for more options.
4. Select **Create Event Rule**.
5. The Create Event Rule side-panel opens.
The criteria will be pre-filled based on the event that has been selected.
6. Configure as required:
 - « select **any** to match on anything.
 - « select an **Action**: Email, Alarm, or No Action.
7. Click **Save**.

Note: An SMTP server is required for email notifications to be sent. You can configure users' email addresses in the **User Management** window.

Tip: Use the **Event Rules** tab to view, edit, or delete configured rules.

Enhancements to Captive Portal

Applicable to AWC Plug-in - Access Points: TQ1K and TQ5k

Wireless Configuration > AP Profile

From Vista Manager EX version 3.5.0, you can configure additional Captive Portal settings for an AP profile.

The additional settings are:

- RADIUS Accounting
- Virtual IP Address
- Walled Garden
- Authentication Page Redirection

RADIUS Accounting

Enable this option to enable accounting on the Captive Portal with an external RADIUS server. RADIUS Accounting collects a variety of information that can be used for accounting and for reporting on network activity. RADIUS accounting uses the same RADIUS server as Captive Portal RADIUS authentication.

In the **Captive Portal** section:

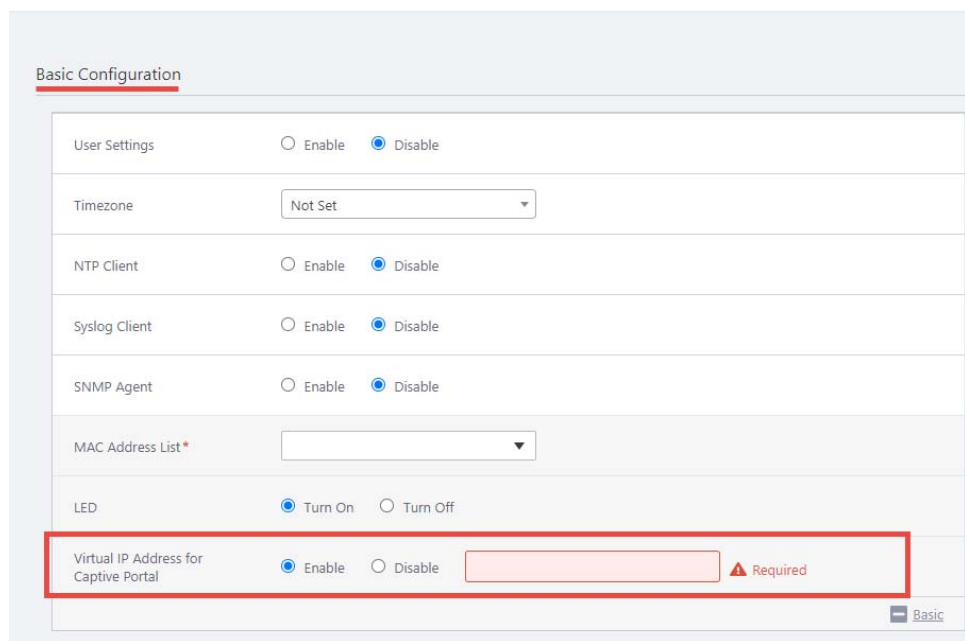
- Select **External RADIUS**.
- **Enable** RADIUS Accounting.
- Enter the RADIUS Accounting **Port Number**, 1-65535, (default: 1813).

The screenshot shows the 'Captive Portal' configuration page. At the top, there are radio buttons for 'External RADIUS' (selected) and 'Click-through'. Below that are radio buttons for 'External Page Redirect' and 'Disable'. The 'Authentication Page Proxy' section has radio buttons for 'Enable' and 'Disable' (selected). The 'RADIUS Server Primary' section has input fields for 'IP Address *' and 'Secret *'. The 'RADIUS Server Secondary' section has input fields for 'IP Address' and 'Secret'. The 'RADIUS Server Port Number' field contains the value '1812'. The 'RADIUS Accounting' section has radio buttons for 'Enable' (selected) and 'Disable'. Below it, the 'RADIUS Accounting Port Number' field is highlighted with a red box and contains a dropdown menu with a red warning icon and the text 'Required'. The 'Redirect type (after user is authenticated)' section has radio buttons for 'Keep session', 'Fixed URL', and 'Disable' (selected). The 'Walled Garden' section has a dropdown menu with the value '0 Entries'.

Virtual IP Address Captive Portal uses the AP's management IP address to show an authentication page. This might be a security risk because it lets other wireless users discover the AP's IP address. Use a virtual IP address to hide the AP management IP address for Captive Portal users.

From the **Basic Configuration** section, use the following steps to configure a virtual IP address for Captive Portal:

- **Enable** the Virtual IP Address for Captive Portal.
- Enter the IP address:
 - ◀ Captive Portal translates this address to become the AP's management address, so this address does not have to be reachable on your network. You can use any address that isn't already used in your network, except ones in the range 127.x.x.x or between 224.x.x.x and 255.x.x.x.

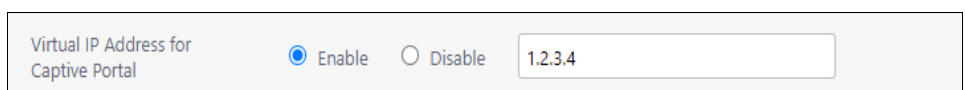


- The Virtual IP Address for Captive Portal is also visible in the VAP Configuration section.
- Click on the red settings icon to jump back to the Basic Configuration section.

VAP Configuration



Basic Configuration



Walled Garden A Walled Garden limits users to accessing only a selection of web pages before Captive Portal authentication. The Captive Portal page is presented if a user tries to access a web page that is not listed in the Walled Garden.

A common example could be a hotel environment where unauthenticated users are allowed to navigate to a designated login page (for example, the hotel website) and all its contents.

From the **Captive Portal** section, use the following steps to configure a Walled Garden for Captive Portal:

- Select one of the Captive Portal type options: External RADIUS, Click-through, or External Page Redirect.
- The window displays the **Walled Garden** field.
- Click the drop-down arrow.

The screenshot shows the 'Captive Portal' configuration interface. At the top, there are radio buttons for 'External RADIUS', 'Click-through' (selected), and 'External Page Redirect'. Below that, there are radio buttons for 'External Page Redirect' and 'Disable'. The 'Authentication Page Proxy' section has 'Enable' selected. The 'Base URL' field is empty. The 'Redirect type (after user is authenticated)' section has 'Keep session', 'Fixed URL', and 'Disable' (selected) options. The 'Walled Garden' field shows '0 Entries' and a red circle highlights the drop-down arrow. The 'Virtual IP Address for Captive Portal' section has a 'Disable' button.

The **Walled Garden List** window opens.

From here you can:

1. manually add IP addresses.
2. import a list of addresses from a CSV file.
3. use the search tool to locate an existing IP address.

The screenshot shows the 'Walled Garden List' window. At the top, there is a search bar labeled 'Address' with a red circle and '1' next to it. Below the search bar, there are two buttons: 'Add' and 'Clear'. The 'Add' button is circled in red with a '2' next to it. To the right of the 'Add' button, there is a button labeled 'Import from CSV file' which is circled in red with a '3' next to it. Below the buttons, there is a search bar labeled 'Search Walled Garden Address' with a red circle and '3' next to it. Below the search bar, there is a table with columns for 'Address' and 'Delete'. The table contains two rows of IP addresses: '192.168.1.2' and '192.168.1.1'. Each row has a 'Delete' button next to it.

Authentication Page Redirect

This option redirects the authentication page to a user-configured URL such as a third-party Captive Portal vendor page. Use this if you want guests to login via the third-party vendor.

From the **Captive Portal** section, use the following steps to configure Authentication Page Redirect for Captive Portal:

- Select the Captive Portal type: **External Page Redirect**.
- Specify the web page a user will see after passing web authentication.
- Complete the authenticating RADIUS Server details.
- Select the **Redirect type**:
 - ⏪ **Session Keep**: Shows the original URL page that was entered in the client's browser before web authentication. For example, if the user is trying to access the airport's webpage from the airport wi-fi network, the browser will be redirected to the RADIUS user URL and after it is authenticated, it will be redirected back to the airport's webpage.
 - ⏪ **Fixed URL**: Always shows a fixed URL that you specify.
 - ⏪ **Disable**: Does not redirect the browser after successful web authentication.

The screenshot displays the configuration page for a Captive Portal. At the top, there are three radio button options: 'External RADIUS', 'Click-through', and 'External Page Redirect' (which is selected and underlined in red). Below this, there are several input fields: 'External Page URL *' with the value '192.168.4.1', 'RADIUS Server Primary IP Address *' with '1.1.1.1', 'RADIUS Server Primary Secret *' with masked characters, 'RADIUS Server Secondary IP Address', 'RADIUS Server Secondary Secret', and 'RADIUS Server Port Number' with '1812'. At the bottom, there are two radio button options for 'RADIUS Accounting' (Enable and Disable) and three for 'Redirect type (after user is authenticated)' (Keep session, Fixed URL, and Disable), with 'Keep session' being selected.

Wi-Fi Alliance certified Passpoint® (Hotspot 2.0) support and WiFi4EU

Applicable to the AWC Plug-in - Access Points: TQ5403, TQm5403, TQ5403e

Wireless Configuration > AP Profile

From Vista Manager EX version 3.5.0, you can enable Hotspot 2.0 on your AP profiles.

Hotspot 2.0, also known as Passpoint™ is the open standard for public Wi-Fi, introduced by the [Wi-Fi Alliance™](#). Passpoint brings seamless, secure Wi-Fi connectivity to any network employing Passpoint enabled Wi-Fi hotspots. It also provides user connections with WPA3™ security protection, enabling users to feel confident that their data is safe.

How does Passpoint work?

Passpoint lets users sign in to a Wi-Fi hotspot once, then uses their credentials as their devices hop from one access point to the next. Users' authentication occurs every time they connect. Of course, the hotspot (i.e., router) must support Passpoint for this connectivity transfer to happen.

Once a user accesses the Wi-Fi network offered at a location, the Passpoint-enabled client device will automatically connect upon subsequent visits. This eliminates the need for users to search for and choose a network, request Wi-Fi access, and re-enter authentication credentials each time they visit.

Passpoint improves the mobile user experience by offering:

- Automatic network discovery and selection
- Simplified online sign-up and instant account provisioning
- Seamless network access and cellular-like roaming between hotspots
- Enhanced security

The WiFi4EU Program

The WiFi4EU program provides funding to municipalities that want to participate in the development of a European free Wi-Fi network, so everyone has access. The program described on the WiFi4EU portal is open to any municipality that wants to provide this service.

To participate in this project, the Wi-Fi Access Points deployed within the municipality must be Passpoint certified so that interoperability with the whole system is guaranteed.

The Allied Telesis No Compromise Wi-Fi solution has been developed to support Passpoint 2.0 and is ready for WiFi4EU projects.

Enabling Hotspot 2.0

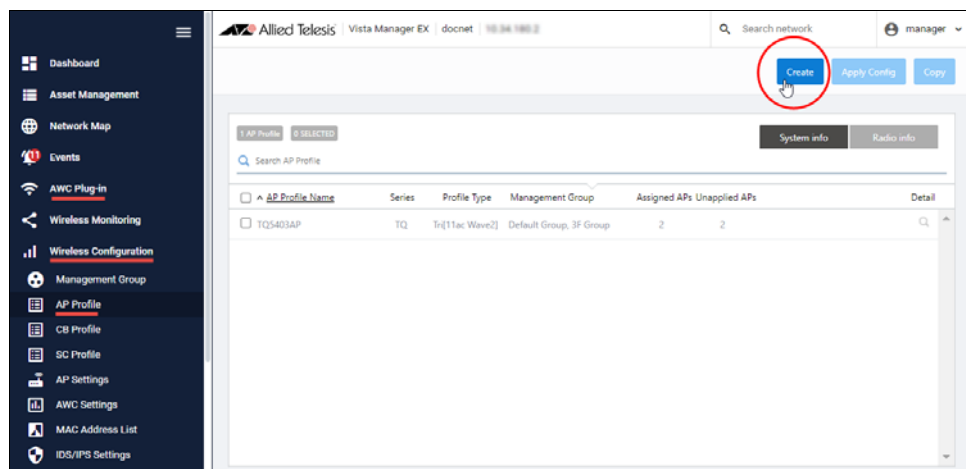
You enable Hotspot 2.0 in the AP Profile settings. There are two ways you can access the AP Profile settings:

- create an AP Profile
- edit an existing AP Profile

Create an AP Profile

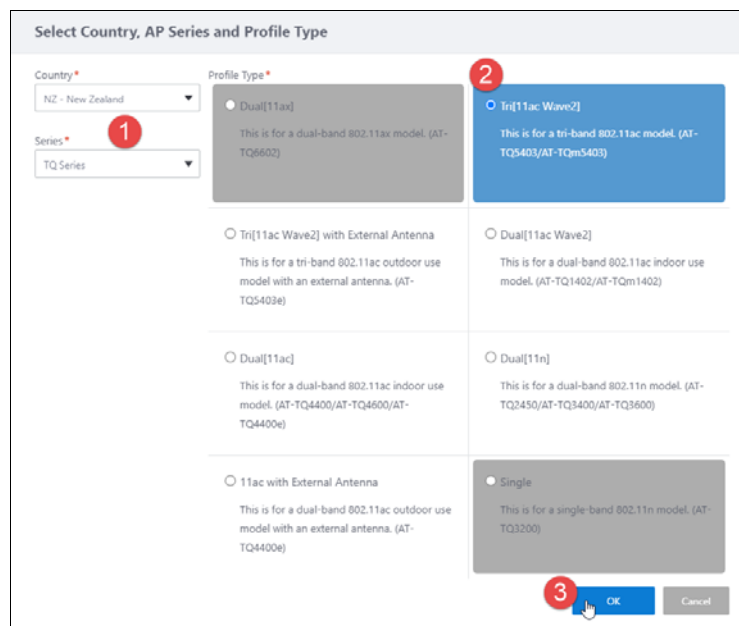
To create an AP Profile and access the Hotspot settings:

- Select **AWC Plug In > Wireless Configuration > AP Profile**
- Click **Create**.

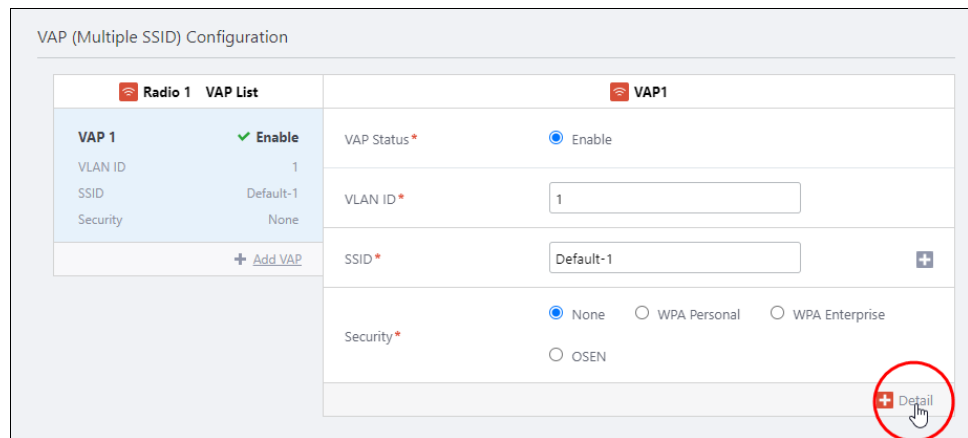


- The AP Profile window opens. From here you can:

1. Select the **Country**
2. Select the **Profile Type** (AP model).
3. Click **OK**.

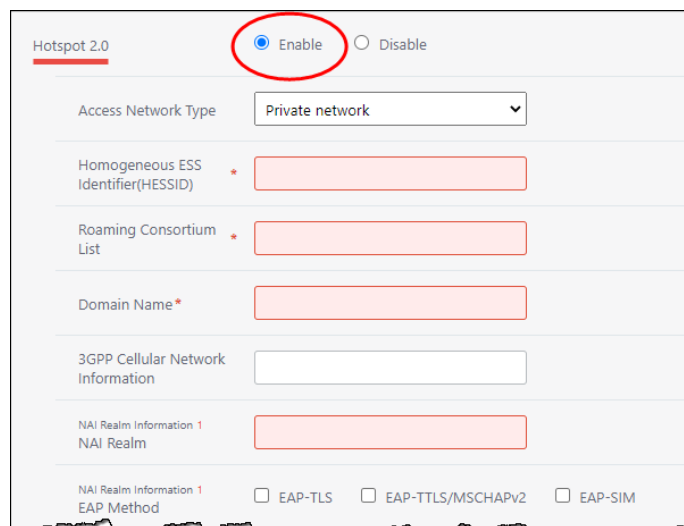


- Scroll down to the **VAP (Multiple SSID) Configuration** section.
- Click **Detail** to see more configuration fields.

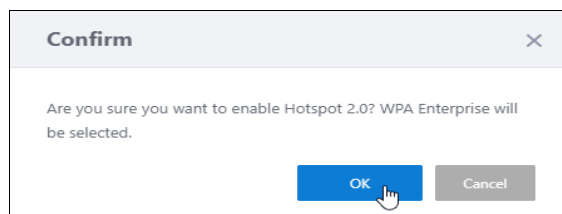


Configuring Hotspot 2.0

- **Enable** Hotspot 2.0.



- Click **OK** to accept the WPA Enterprise security type required for Hotspot 2.0.



- Go back up to the AP Profile **Security** section.
- **WPA Enterprise** security type is selected.

The screenshot shows the Security configuration interface. At the top, there are radio buttons for 'None', 'WPA Personal', 'WPA Enterprise' (which is selected), and 'OSEN'. Below this, there are several input fields: 'RADIUS Server Primary IP Address*', 'RADIUS Server Primary Secret*', 'RADIUS Server Secondary IP Address', 'RADIUS Server Secondary Secret', and 'RADIUS Server Port Number' (with the value '1812' entered).

- Enter the **RADIUS Server** details.
 - ⏪ Primary IP Address: IPv4 address format("X.X.X.X", X=1-255).
 - ⏪ Primary Secret: ASCII Printable characters(*4)

Note: You need to use an external RADIUS server, rather than the local RADIUS server on your AlliedWare Plus device.

- Go back down to the **Hotspot 2.0** section.
- From the **Access Network Type** drop-down list, choose to the network type that best describes the AP environment you want to configure.

The screenshot shows the Hotspot 2.0 configuration interface. At the top, there are radio buttons for 'Enable' (selected) and 'Disable'. Below this, there is a dropdown menu for 'Access Network Type' which is open, showing options: 'Private network', 'Private network with guest access', 'Chargeable public network', 'Free public network', 'Personal device network', 'Emergency service only network', 'Test or experimental', and 'Wildcard'. Other fields include 'Homogeneous ESS Identifier(HESSID)*', 'Roaming Consortium List*', 'Domain Name*', '3GPP Cellular Network Information', 'NAI Realm Information 1 NAI Realm', and 'NAI Realm Information 1 EAP Method' with radio buttons for 'EAP-TLS', 'EAP-TTLS/MSCHAPv2', and 'EAP-SIM'.

- Complete the remaining Hotspot 2.0 configuration fields:
 - ⏪ Fields vary depending on the options you configure.
 - ⏪ The table below describes these fields.

Table-1: Hotspot 2.0 configuration fields

Field	Description
Access Network Type	<p>Specify any of the following 802.11u network types.</p> <ul style="list-style-type: none">■ private network — This network is accessible for authorized users only. For example, home networks or enterprise networks that require user authentication.■ private network with guest access— This network is accessible to guest users based on guest authentication methods. For example, enterprise networks that allow guest users with captive portal authentication.■ chargeable public network — This network provides access to the Internet based on payment. For example, a subscription-based Internet access in a coffee shop or a hotel offering chargeable in-room Internet access service.■ free public network —This network is accessible to all without any charges applied. For example, a hotspot in airport or other public places that provide Internet access with no additional cost.■ personal device network — This network is accessible for personal devices. For example, a laptop or camera configured with a printer for the purpose of printing.■ emergency service only network —This network is limited to accessing emergency services only.■ test or experimental — This network is used for test purposes only.■ wildcard —This network indicates a wildcard network.
Homogeneous ESS Identifier HEISS	<p>Homogeneous Extended Service Set Identifier. The device MAC address in a hexadecimal format separated by colons. For example, 10:22:33:44:55:66</p>
Roaming Consortium List	<p>A group of subscription service providers (SSPs) having inter-SSP roaming agreements.</p> <ul style="list-style-type: none">■ The Roaming Consortium list tells a mobile device which roaming consortiums or service providers are available through an AP.■ The list must be in Hexadecimal format. For example, "506f9a, 001aeb"
Domain Name	<p>Domain name of the access network operator, which is the identifier of the operated Hotspot2.0 network. For example, "example.com, example.net"</p>

Table-1: Hotspot 2.0 configuration fields(cont.)

Field	Description
3GPP Cellular Network Information	<p>The cellular network identifier.</p> <ul style="list-style-type: none">■ This is a string concatenated Mobile Country Code (MCC) and comma(,) and Mobile Network Code (MNC). The MCC code is three digits, and the MNC is two or three digits. For example: "440,10" means "NTT DoCoMo, Inc" which is a mobile network in Japan.■ Each "MCC, MNC" pair is separated by a semi-colon(;). For example: "440,10;440,50"■ For more information on mobile network codes, see: Mobile Network Codes
NAI Realm Information	<p>The Network Access Identifier (NAI) Realm information.</p> <ul style="list-style-type: none">■ The realm in the NAI format is represented after the @ symbol, which is specified as domain.com For example: user@realm.example.com
EAP Method	<p>The method that this NAI realm uses for authentication:</p> <ul style="list-style-type: none">■ EAP-TLS■ EAP-TTLS/MSCHAPv2■ EAP-SIM
Operator Friendly Name	<p>The name of the operator you are providing. Use the language code, for example: 'jpn','eng' And the operator name string. <language code>:<name> For example: eng : Allied Telesis Holdings K.K. jpn : アライドテレシス株式</p>
Disable Downstream Group-Address Forwarding (DGAF)	<p>Select 'Enable' to disable Downstream Group-Addressed Forwarding, change Disable Downtown Group-Addressed Forwarding (DGAF).</p>
L2 Traffic Inspection and Filtering	<p>If you want to discard L2 traffic between VAPs, enable L2 Traffic Injection and Filtering. The packets that TQ restricts are: Arp, ICMP, and TDLS.</p>

Multi select deletion from MAC address list

Applicable to the AWC Plug-in.

From version 3.5.0 onwards, when you are editing a MAC address list in the AWC plug-in, you can select and delete multiple list entries at the same time. This means you can more easily manage large lists of MAC addresses.

To edit a MAC address list:

- From the Vista Manager EX menu, select AWC Plug-in -> Wireless Configuration -> MAC Address List.
- Click on the list to edit, and then click on the Edit button.
- Click on the check-boxes to select the MAC addresses you want to delete. To select all MAC addresses, click on the check-box at the top of the list.
- Once you have selected the MAC addresses to be deleted, click on the Delete button.

The screenshot shows the 'MAC Address List' interface. At the top right, there is an 'Import from CSV' button. Below this, there are two input fields: 'MAC Address*' and 'Notes', with 'Add' and 'Clear' buttons to their right. A status bar indicates '5 Entry' and '3 Selected'. Below the status bar is a search field labeled 'Search Entries'. The main area contains a table with columns for 'MAC Address', 'Notes', and 'Edit'. The table has 5 rows, each with a checkbox, a MAC address, a notes field, and an edit icon. The first, third, and fifth rows have their checkboxes checked. At the bottom left of the table area, there is a 'Delete' button.

<input type="checkbox"/>	MAC Address	Notes	Edit
<input checked="" type="checkbox"/>	00:00:00:00:00:01		
<input type="checkbox"/>	00:00:00:00:00:02		
<input checked="" type="checkbox"/>	00:00:00:00:00:03		
<input type="checkbox"/>	00:00:00:00:00:04		
<input checked="" type="checkbox"/>	00:00:00:00:00:05		

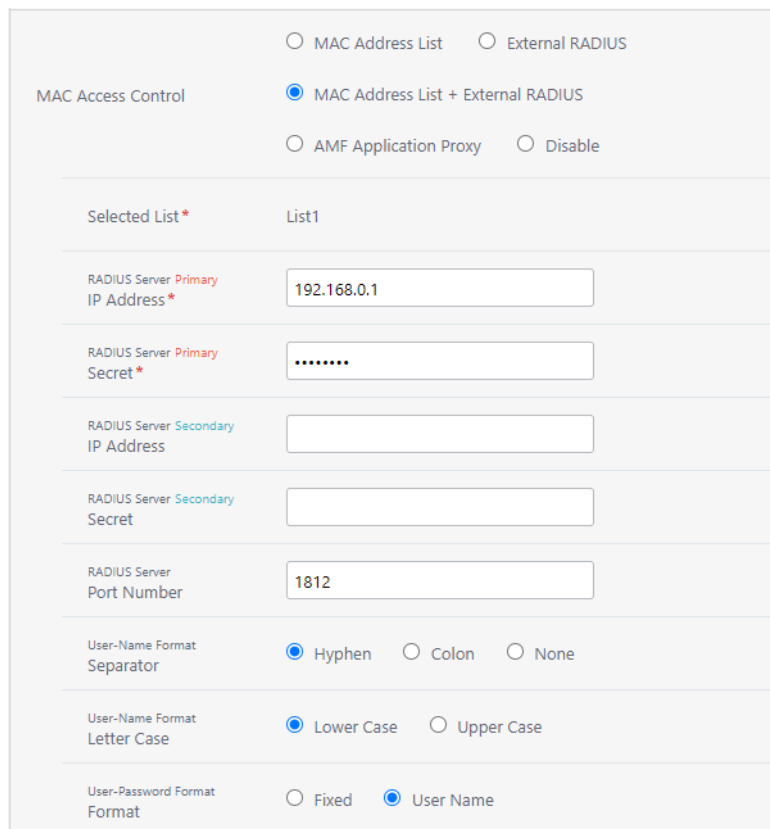
Enable MAC address list and external RADIUS

Applicable to the AWC Plug-in.

From version 3.5.0 onwards, you can enable both a MAC address list and an external RADIUS server at the same time. Previously, only one or the other could be used for security.

There are two ways you can enable the functionality:

1. You can configure the setting in the AP Profile.
 - From the Vista Manager EX menu, select AWC Plug-in -> Wireless Configuration -> AP Profile.
 - Select the AP profile you want to change, then click Edit, or create a new profile.
 - Under the VAP Configuration section, click on +Detail.
 - In the MAC Access Control section, select the MAC Address List + External RADIUS radio button.
 - Make sure you have a MAC address list specified in the Basic Configuration MAC Address List dropdown.
 - Specify the IP Address and Secret of your RADIUS server, as well as the Secondary server if you are using one, and the Port Number if it is different than the default.
 - Click Save to apply the settings to the AP profile.



MAC Access Control

MAC Address List External RADIUS

MAC Address List + External RADIUS

AMF Application Proxy Disable

Selected List * List1

RADIUS Server *Primary* IP Address * 192.168.0.1

RADIUS Server *Primary* Secret *

RADIUS Server *Secondary* IP Address

RADIUS Server *Secondary* Secret

RADIUS Server Port Number 1812

User-Name Format Separator Hyphen Colon None

User-Name Format Letter Case Lower Case Upper Case

User-Password Format Format Fixed User Name

2. If you are using Channel Blanket on TQ5403/TQ5403e devices, you can configure the setting in the Channel Blanket Profile.
 - From the Vista Manager EX menu, select AWC Plug-in -> Wireless Configuration -> CB Profile.
 - Select the CB profile you want to change, then click Edit, or create a new profile.
 - Under the VAP Configuration section, click on +Detail.
 - In the MAC Access Control section, select the MAC Address List + External RADIUS radio button.
 - Specify the IP Address and Secret of your RADIUS server, as well as the Secondary server if you are using one, and the Port Number if it is different than the default.
 - Click Save to apply the settings to the AP profile.

MAC Address List External RADIUS

MAC Access Control

MAC Address List + External RADIUS Disable

RADIUS Server *Primary*
IP Address *

RADIUS Server *Primary*
Secret *

RADIUS Server *Secondary*
IP Address

RADIUS Server *Secondary*
Secret

RADIUS Server
Port Number

User-Name Format
Separator Hyphen Colon None

User-Name Format
Letter Case Lower Case Upper Case

User-Password Format
Format Fixed User Name

AMF Application Proxy and Critical Mode

Applicable to the AWC Plug-in.

From version 3.5.0 onwards, you can use AMF Application Proxy for your MAC access control in Vista Manager EX. In addition, you can enable Critical Mode. When Critical Mode is enabled, if the connection to the AMF Application Proxy is lost, connections are still permitted.

You can configure the setting in the AP Profile.

- From the Vista Manager EX menu, select AWC Plug-in -> Wireless Configuration -> AP Profile.
- Select the AP profile you want to change, then click Edit, or create a new profile.
- Under the VAP Configuration section, click on +Detail.
- In the MAC Access Control section, select the AMF Application Proxy radio button.
- Specify the IP Address and Secret of your AMF Application Proxy Server, as well as the Secondary server if you are using one, and the Port Number if it is different than the default.
- To enable critical mode, select the Critical Mode radio button.
- Click Save to apply the settings to the AP profile.

MAC Access Control

MAC Address List External RADIUS

MAC Address List + External RADIUS

AMF Application Proxy Disable

AMF Application Proxy Server
Primary
IP Address * 192.168.0.1

AMF Application Proxy Server
Primary
Secret *

AMF Application Proxy Server
Secondary
IP Address

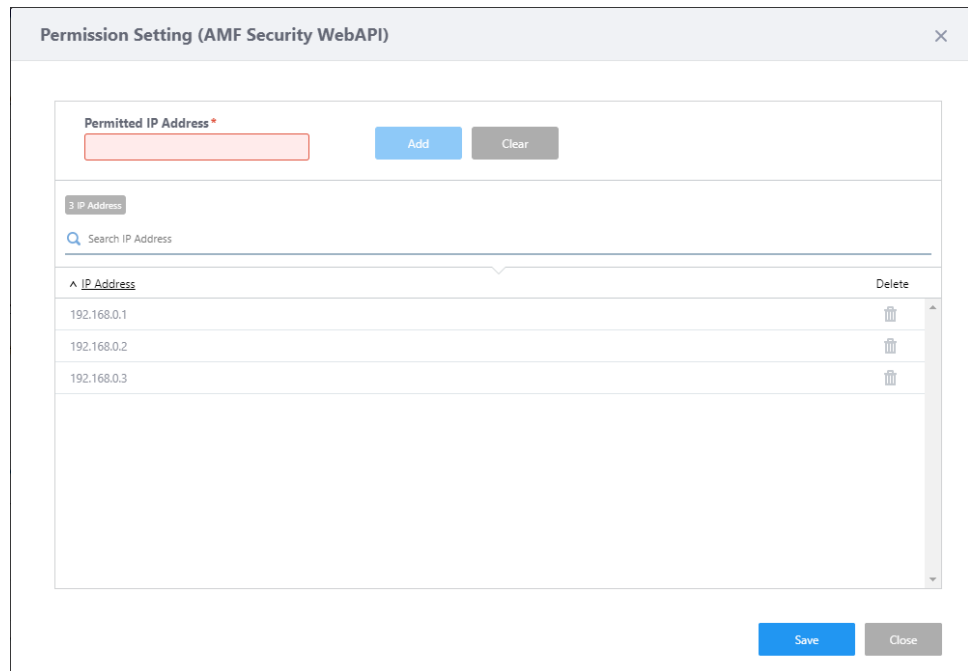
AMF Application Proxy Server
Secondary
Secret

AMF Application Proxy Server
Port Number 1812

Critical Mode Enable Disable

Once you have configured the AMF Application Proxy, you can create the IP address white list.

- From the Vista Manager EX menu, select AWC Plug-in -> Wireless Maintenance -> System Setting.
- Under AMF Security WebAPI, click on Edit.
- Add the permitted IP addresses to your white list, then click Save.



SNMPv3 now supported on Access Points via Vista Manager EX

Applicable to the AWC Plug-in - TQ5403, TQm5403, TQ5403e FW version v6.0.1-x.x

From version 3.5.0 onwards, you can configure SNMPv3 settings on Access Points from the Vista Manager AWC plug-in. This is in addition to SNMPv1 and v2c.

This feature supports Tri-band access points AT-TQ5403, AT-TQm5403 and AT-TQ5403e, running version 6.0.1-x.x. When you create an AP profile, you will find a new option called 'SNMP Agent' under the Basic Configuration section. Click Enable to enable the SNMP Agent. Choose the SNMP version and complete the required fields.

For more information about how to configure SNMPv3 settings, see the [User Guide: Vista Manager AWC Plug-in](#).

Creating static links on the network map

Applicable to all Vista Manager installations.

From version 3.5.0 onwards, you can draw static links on the network map to wired or wireless devices that are connected to each AP.

Note that if the device moves to another AP, you have to update the link manually. We recommend using this feature only for devices that seldom or never move.

Background image shows on dashboard map

Applicable to all Vista Manager installations.

From version 3.5.0 onward, if you add a background image, it now displays on all maps (except for the WAN map). Previously, it did not display on the dashboard map.

Improvements to firmware distribution

Applicable to all Vista Manager installations.

From version 3.5.0 onwards, the mechanism that Vista Manager EX uses for distributing firmware has been improved.

Note that firmware distribution can only update devices that are currently running AlliedWare Plus version 5.4.9-0.1 or later. Devices running software earlier than 5.4.9-0.1 are not displayed on the firmware page.

Also from version 3.5.0 onward, if you use firmware distribution to copy a firmware file to devices, and that file already exists on a device, then firmware distribution will overwrite the existing file. This makes it possible to use firmware distribution to repair a corrupted firmware file on a device.

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 5.5.0-2.1 or later.

Wireless AP software version compatibility

- TQ5403 series APs with firmware version 5.0.x or later. Some of the latest functionality is only available on APs running version 6.0.1-1.1 or later.
- TQ4x00/3x00/2450 APs with firmware version 4.2.x

Internet Explorer 11 compatibility

When using the Vista Manager EX 3.5.0 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 only available on Windows-based Vista Manager installations. Plug-ins are not available on Vista Manager virtual appliances.

.Net Framework 4.8 required for SNMP plug-in

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

For Vista Manager EX version 3.5.0, .NET Framework 4.8 or later is required if you are using the SNMP plug-in.

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 3.5.0 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.

Vista Manager and Npcap

For Vista Manager EX version 3.5.0, Vista Manager cannot be installed on the same computer as Npcap. This restriction also applies to applications that include Npcap.

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.

Change to link color when editing network map

From version 3.5.0 onwards, non-wireless custom links are represented in black when you edit the network map. This matches the color used when viewing the map.

Change to reboot scheduling

From version 3.5.0 onwards, you can no longer schedule Vista Manager EX to reboot individual devices at the same time. However, you can use "Reboot Updated Devices" to schedule a reboot for every updated node in the network. These reboots can be scheduled for the same time with this method.

VLAN and EPSR interaction

Previously, it was possible to use Vista Manager EX to create and edit VLANs on ports that had EPSR configured. From version 3.5.0 onwards, EPSR ports are disabled on the VLAN editing page. Users can easily identify EPSR ports when editing VLANs and avoid misconfigurations.

Integrated map won't display some links from earlier versions

Applicable to all Vista Manager installations.

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 x908 GEN1 and x200 devices will not be shown on the integrated map.

Traffic map data not restored

Applicable to all Vista Manager installations.

When you are upgrading to Vista Manager EX 3.5.0, traffic map data from earlier versions will not be imported.

Station location and channel blanket

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

If Station Location is enabled, the maximum number of APs that can have a channel blanket profile applied is 500.

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://www.alliedtelesis.com).

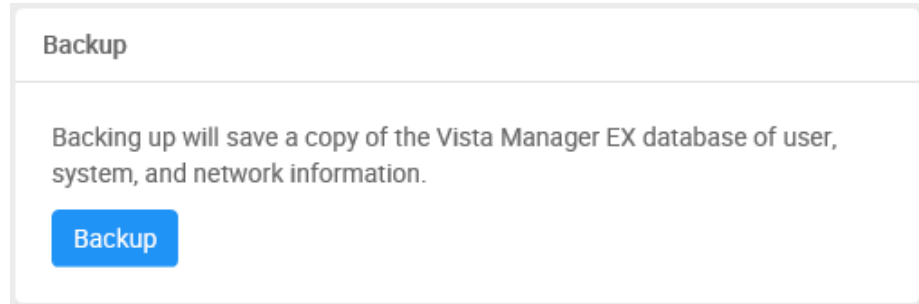
AMF documentation For full AlliedWare Plus documentation, see our online documentation library. For AMF, the library includes the following documents:

- 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'.

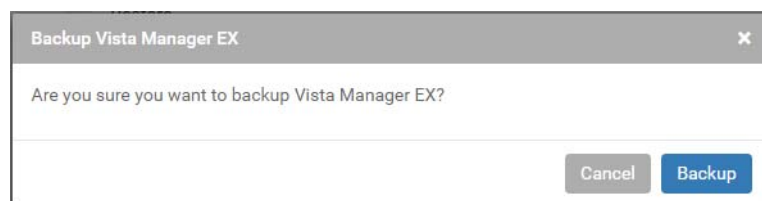
Do not rename these files. The installation requires them to be in this format.

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.

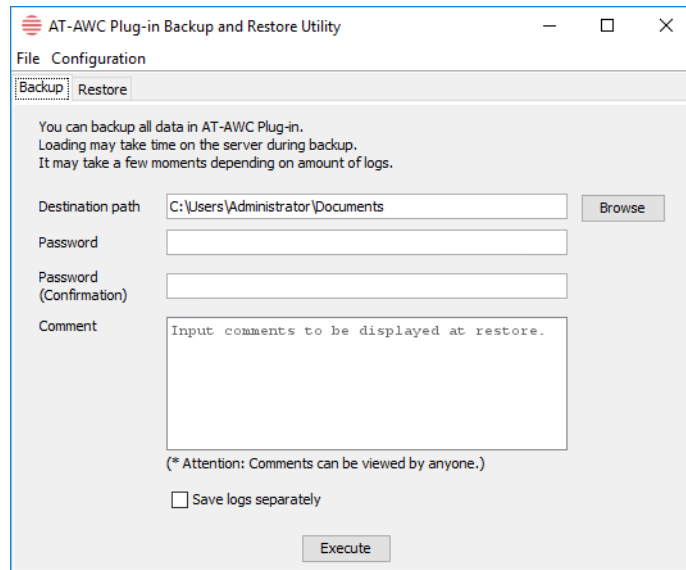
Backup the AWC plug-in

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

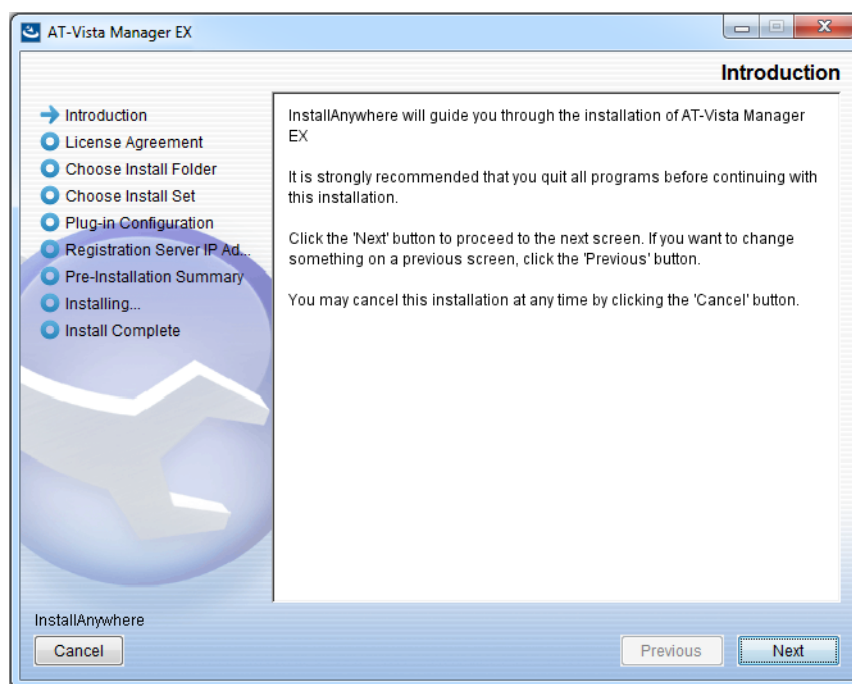
13. Log on as the same user as when installing.
14. Stop the server. Select **AT-Vista Manager EX** and then **AT-Vista Manager EX - Stop Server** from the Windows menu.
15. From the Windows menu, select **AT-Vista Manager EX** then **AT-Vista Manager EX - Uninstall**.
16. The AT-Vista Manager EX uninstaller 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**.

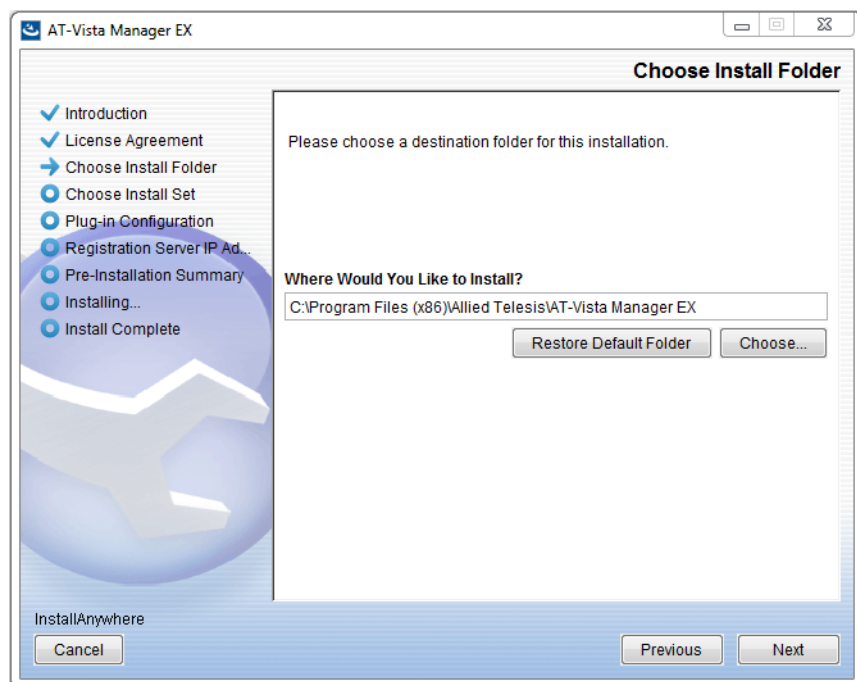
23. The **License Agreement** dialog displays:



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

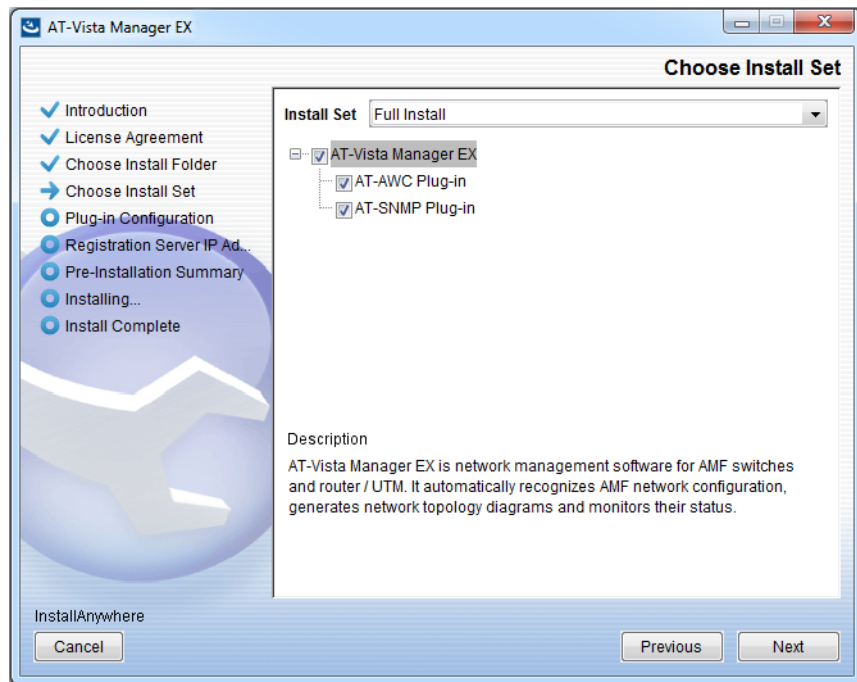
- Click **I accept the terms of the License Agreement**
- Click **Next**

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 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:



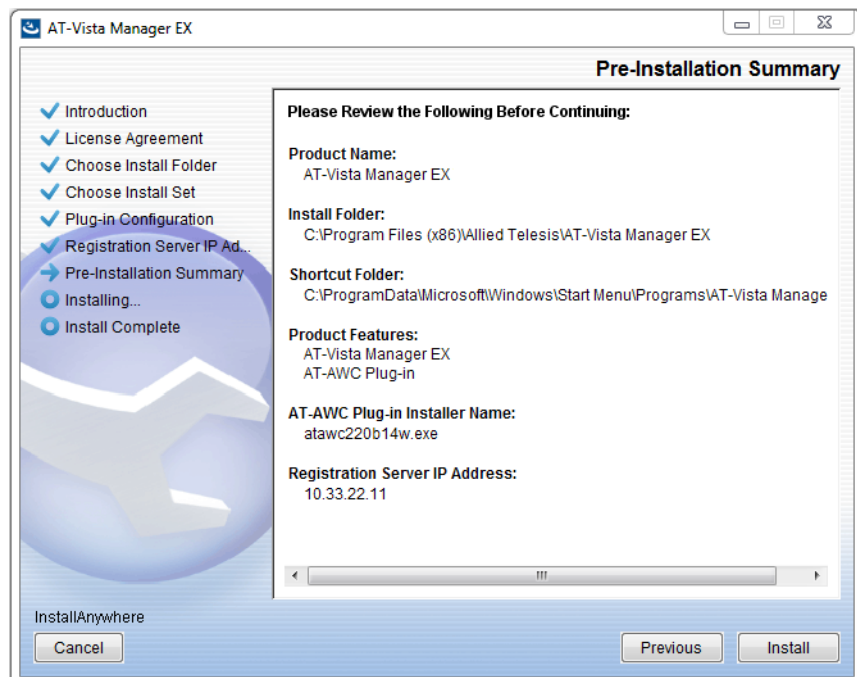
Select **Do not create a public key** unless you are intending to use the plug-ins in standalone mode. For more information on standalone mode, refer to the Installation Guide. Click **Next**.

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



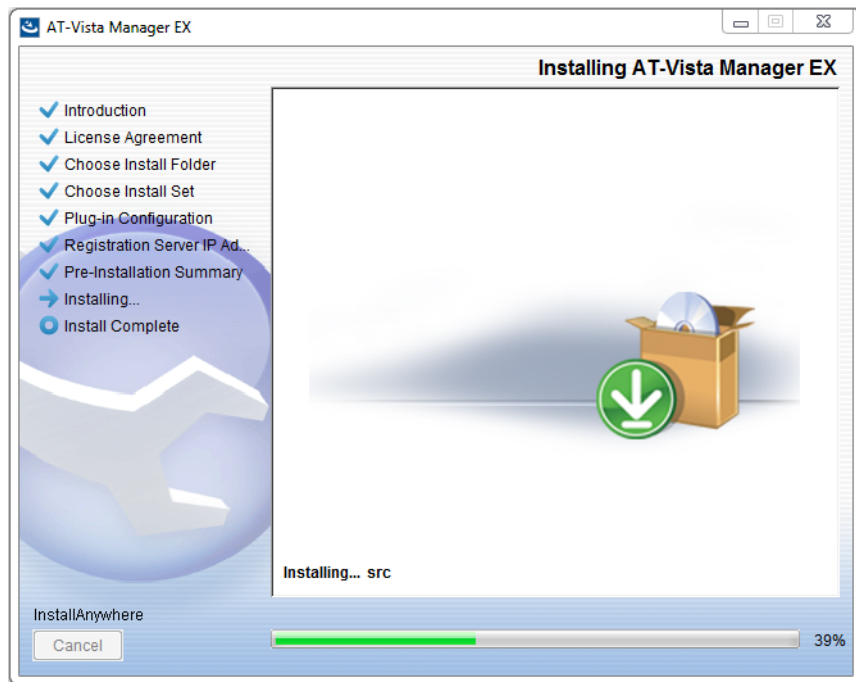
Either select from the list of IP addresses already configured on the Windows machine, or input a valid IP address. Click **Next**.

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

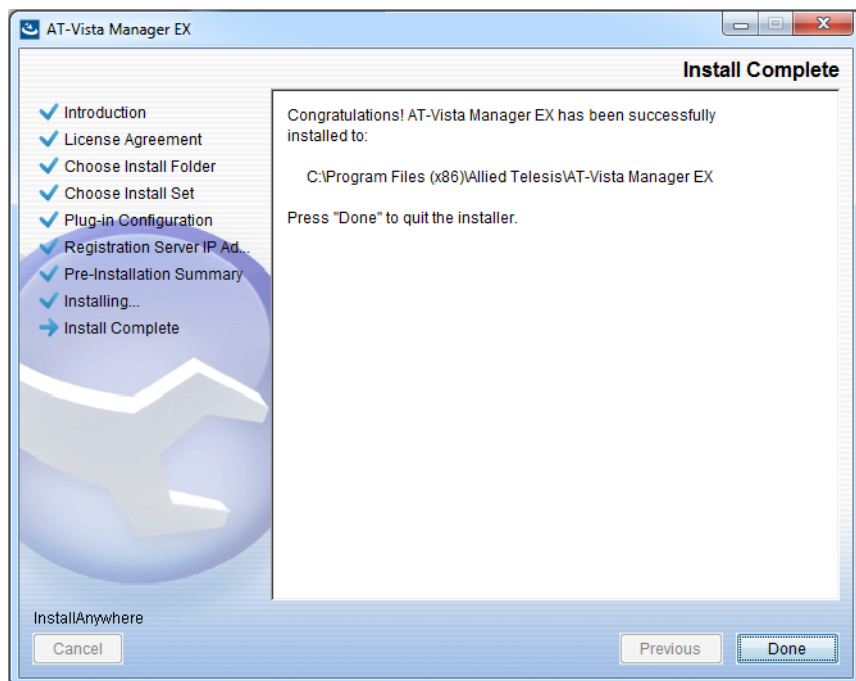


Check that your Product Name, Install Folder, Shortcut Folder, Product Features, Plugin Installer Name and Registration IP Address are correct, and then click **Install**.

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



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

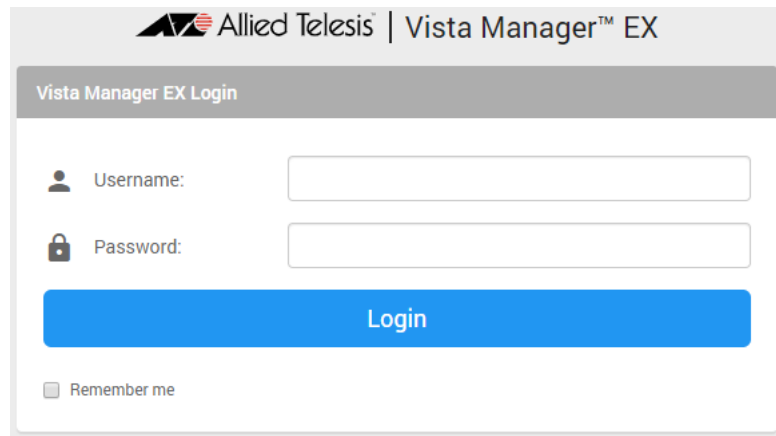


Check that the installation has completed successfully and click **Done**.

Restore the Vista Manager database

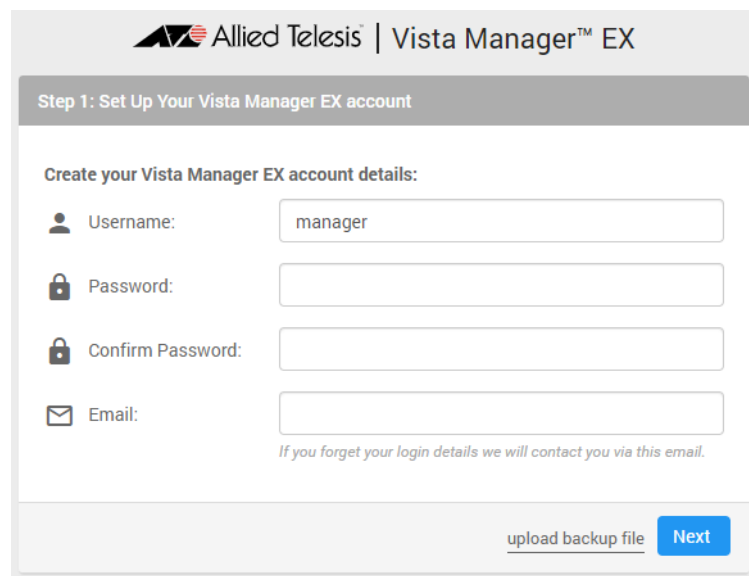
After the upgrade is complete, you need to restore the Vista Manager database. To do this, use the following procedure.

31. Login to Vista Manager.



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

32. Click on upload backup file.

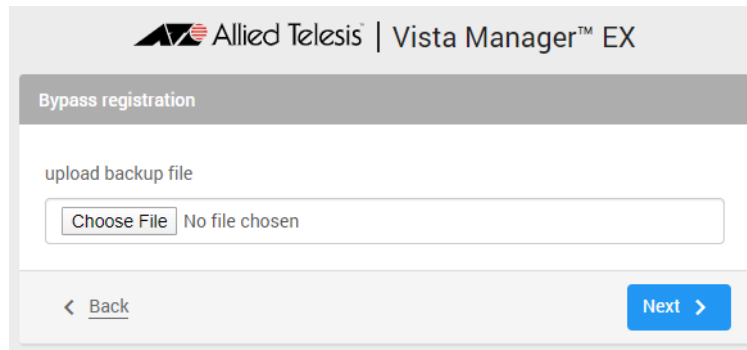


Caution Your serial number and license information are part of your database backup. If you upload the backup file when upgrading, you will keep the same serial number, and your licensing will continue to work without interruption.

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

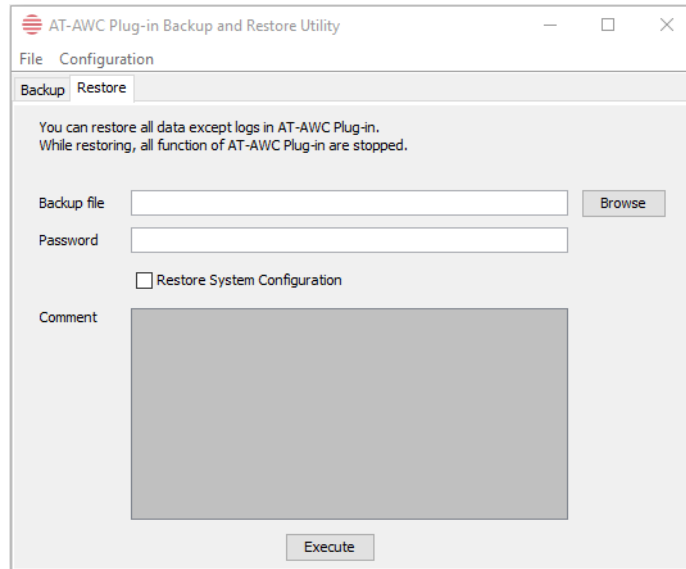
34. If you have the SNMP plug-in installed then log on locally to the Vista Manager EX server.
35. Stop the SNMP server services using the shortcut or by running the following command line.
"<Vista Install Path>\Plugins\AT-SNMP\NetManager\bin\svrcmd.bat" svrstop
36. Run the restore utility by using the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

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.

Google Chrome (Method A)

1. Press **F12** or **Ctrl+Shift+I** to open Chrome Developer Tools.
2. Right-click on the **Reload** button.
3. Select **Empty Cache and Hard Reload**.

Google Chrome (Method B)

1. Click on the three dots at the top right corner of the browser.
2. Select More tools > **Clear browsing data**.
3. Check **Cookies and other site data** and **Cached images and files**.
4. In the Time range dropdown list, select **All time**.
5. Click on the **Clear data** button.
6. Press **Ctrl+F5**.

Internet Explorer

1. Click on **Tools** (wheel icon) at the top right corner of the browser.
2. Select Safety > **Delete browsing history**.
3. Check **Temporary Internet files and website files**.
4. Click the **Delete** button.
5. Press **Ctrl+F5**.

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 38](#) for steps for 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.

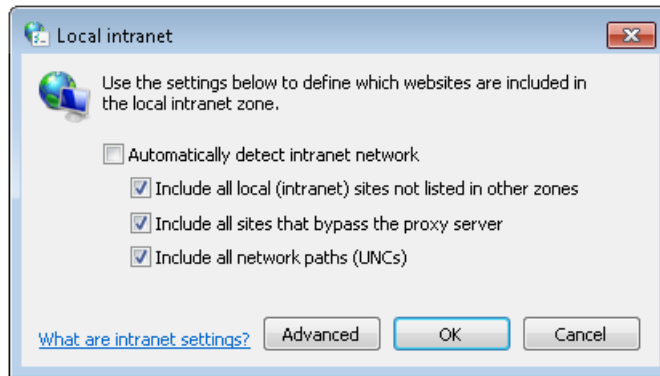
Microsoft Edge support

Applicable to all Vista Manager installations.

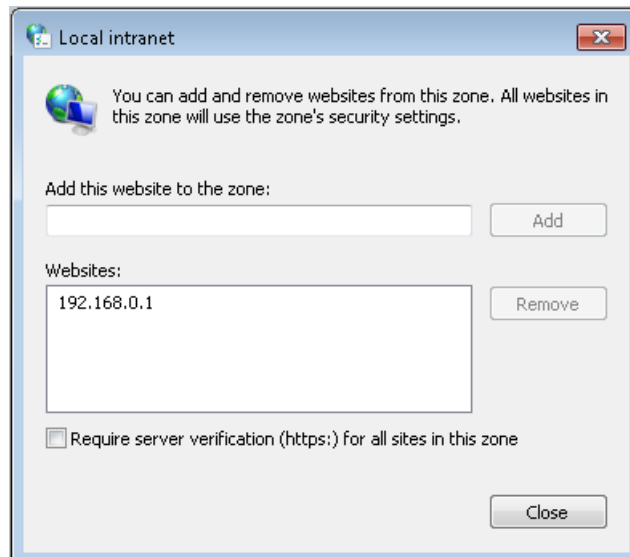
Security in Microsoft Edge may prevent you from navigating to Vista Manager using an IP address. We recommend that rather than using the IP address, you use DNS and a FQDN for Vista Manager.

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.

Down nodes in backups

Applicable to all Vista Manager installations.

If you are importing a backup from Vista Manager EX 2.5.0 or earlier, nodes that are down when the backup was taken will not appear on the network map. Once the nodes are brought back up again, they will appear on the network map.