Release Note for Vista Manager EX Software Version 3.13.x

» 3.13.1

Acknowledgments

Getting the most from this Release Note

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

Content

What's New in Vista Manager EX v3.13.1

Introduction

This release note describes the new features in Vista Manager EX™ v3.13.1. It covers Vista Manager EX plus the optional Autonomous Wave Controller (AWC) and SNMP plug-ins, and AMF Plus Menu (formerly 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 and enhancements added to Vista Manager EX version 3.13.1.

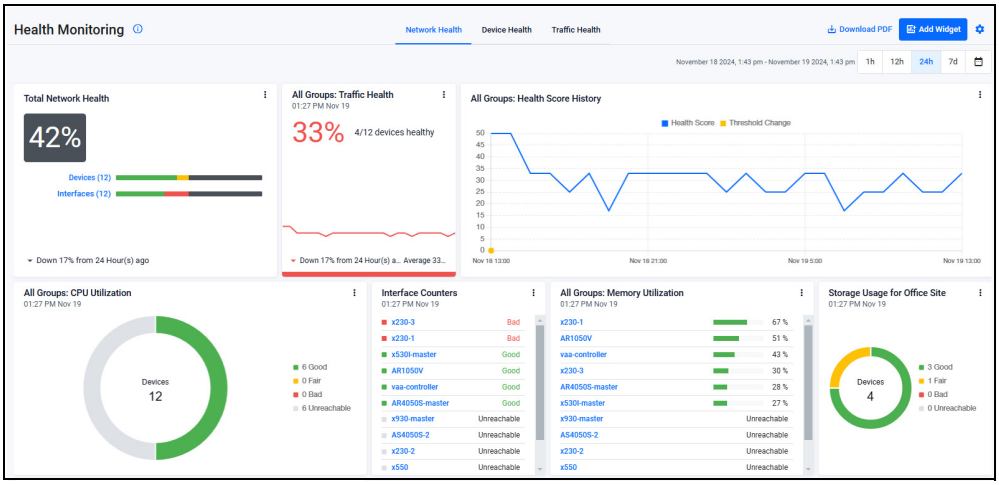
It includes:

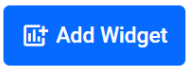
Customizable Network Health Dashboard

Applies to all Vista Manager EX installations with an AMF Plus License

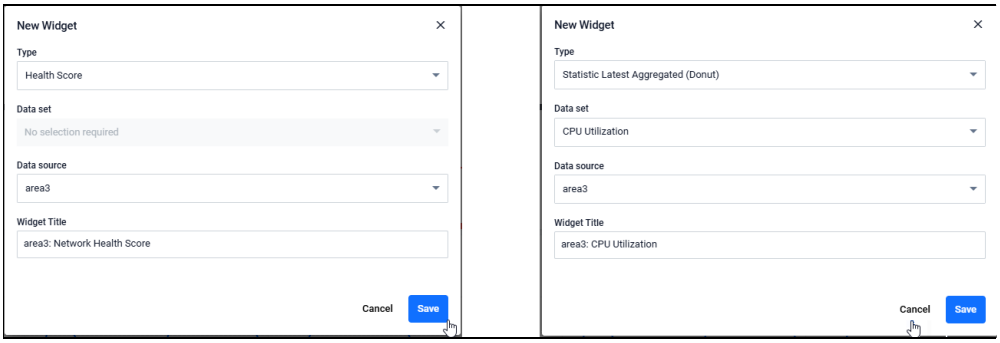
From version 3.13.1 onwards, you can customize the Health Monitoring page's Network Health Dashboard.

You can click and drag the widgets on the Network Health Dashboard to create a custom dashboard layout. Widgets are stackable and display in a grid format, meaning you can sort them into columns.

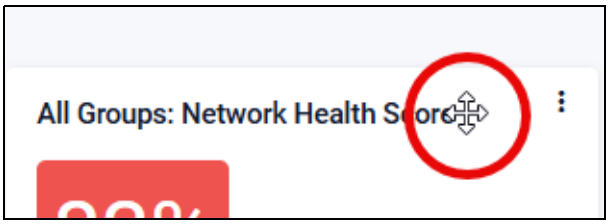




You can add widgets by clicking the **+ Add Widget** button in the top right of the Health Monitoring page. You can also add a custom name to display as the title of the widget.



To move a widget, hover over the widget heading and click and drag the widget to the desired location.



You can also resize widgets, such as the Health Score History graph, for a bigger or smaller view.

To delete a widget, click the Action button (the 3 dots) in the corner of the widget.

View Windows Server charts from Health Monitoring

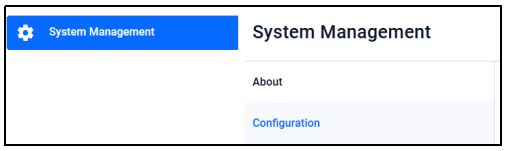
Applies to all Vista Manager EX installations with an AMF Plus License

From version 3.13.1 onwards, you can now view Windows Server Monitoring charts and metric data from the Health Monitoring page. This means you can monitor Windows Server information in Vista Manager.

How to add a Windows Server to Vista Manager

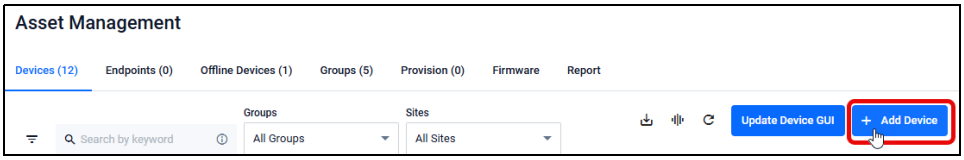
Step 1. Enable Advanced Monitoring from System Management.

Go to **System Management** > **Configuration** and enable the Advanced Monitoring feature.

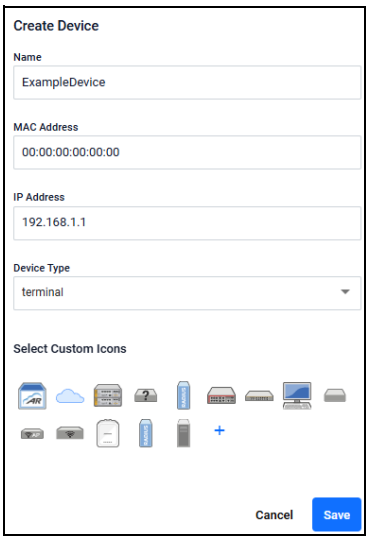


Next add the windows server as a device in the Asset Management menu. Note that you do not have to perform this if it has already been discovered from another source.

Step 2. Go to the **Asset Management** page and click **+ Add Device**



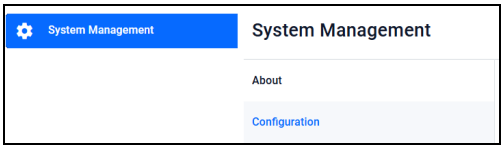
Enter the Name, MAC Address, IP Address, Device Type, and optionally a custom icon.



Click **Save**.

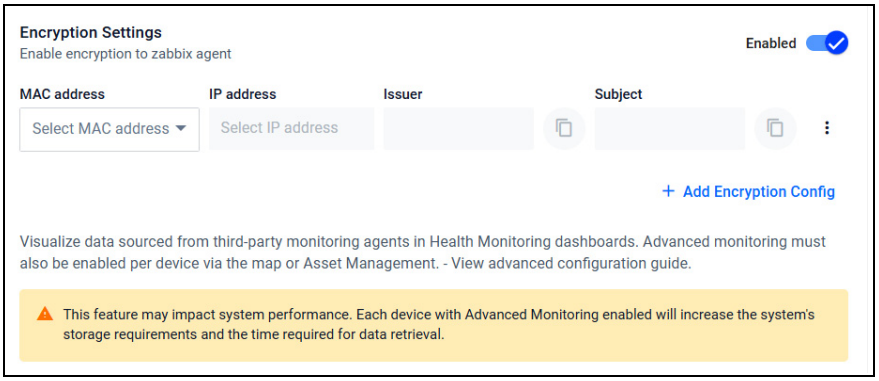
Step 3. **(Optional)** Enable Encryption settings and enter the zabbix agent information.

Go back to the **System Management** > **Configuration** page.

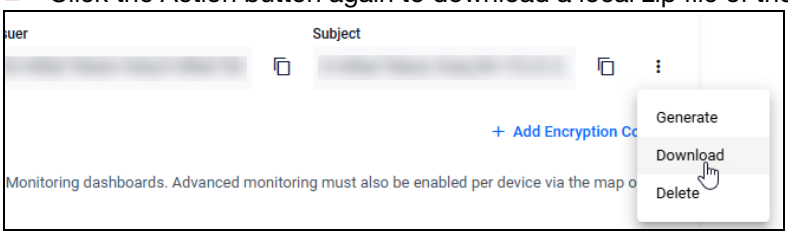


Scroll down to **Optional Features**, and toggle the Advanced Monitoring Encryption Settings toggle. Using the information from the previous step, select this device from the dropdown for encryption.

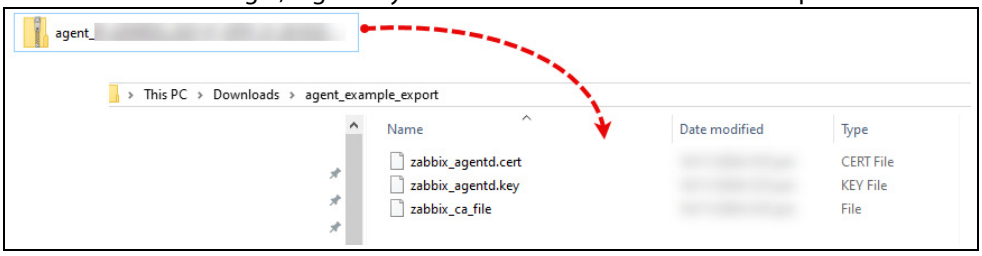
Add the Windows device's information from the dropdown into the Encryption Settings fields.



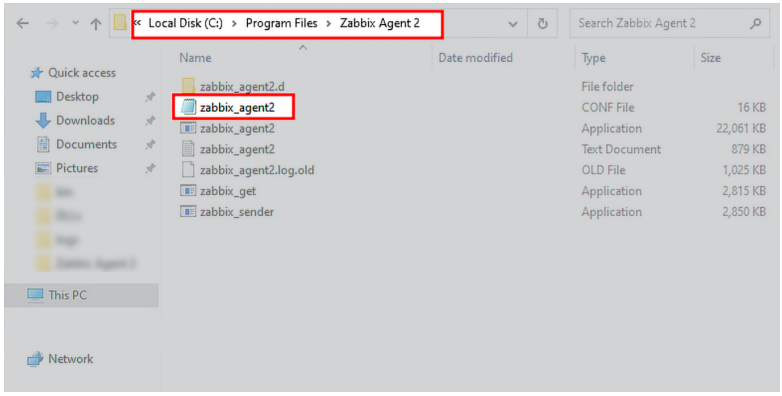
- You can optionally click the Action button and select Generate to get the Issuer and Subject information.
- Click the Action button again to download a local zip file of the configuration.



Outside of Vista Manager, log onto your remote server and extract the zip file.



Navigate to your Zabbix Agent 2 installation folder and open the Zabbix_Agent2.CONF file in a text editor of your choice.



The default path for the installation folder is ***C:\Program Files\Zabbix Agent 2***

Follow the documentation from the Official Zabbix Agent 2 Documentation to see how to edit the configuration file.

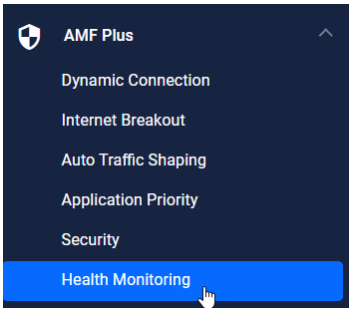
Step 4. **Restart the Zabbix_agent2 service** from Task Manager on your remote server to apply the updated configuration.

Step 5. In Vista Manager, refresh the Network Map topology by clicking the **Refresh button**.

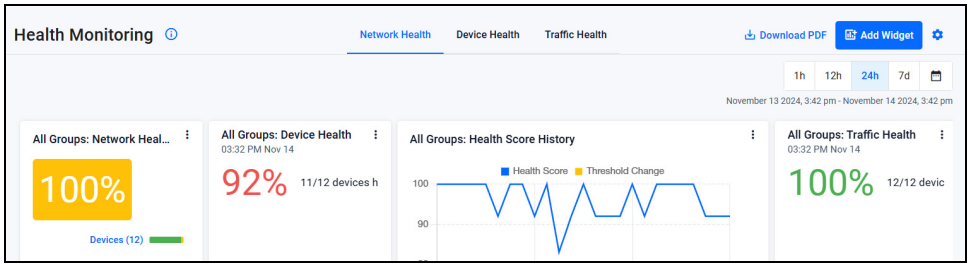
The Windows Server will appear as a device on the Network Map.

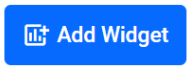
How to add a Widget to the Health Monitoring Page

Step 1. Click on **Health Monitoring** from the **AMF Plus** menu.

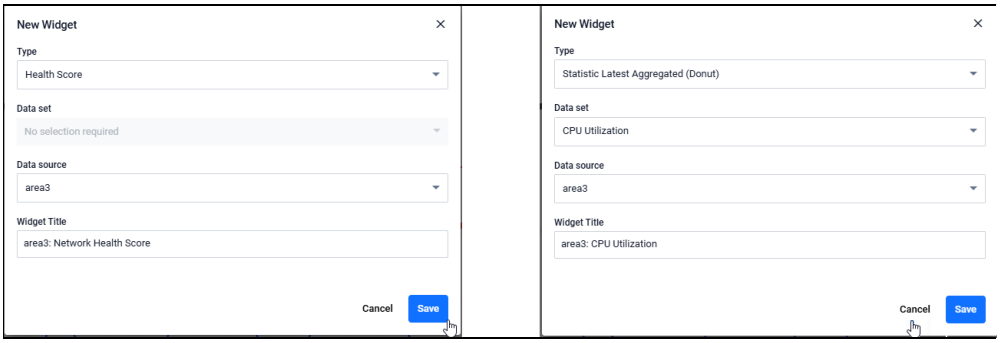


This opens the Health Monitoring page:





Step 2. Click **Add Widget** to add a widget, and click on the **Type**.



For the windows server specifically, you can select from:

- Advanced Monitoring - Individual Value (CPU, RAM)
- or Advanced Monitoring - Process List (CPU, RAM)

Step 3. Select the **Windows Server** as the **Data Source.**

Step 4. **Wait a moment** for polling and the data will appear on the **Network Health dashboard**.

New RADgate (external RADIUS Server) support

Applies to all Vista Manager EX installations

From version 3.13.1 onwards, Allied Telesis' new RADIUS application (**AT-RADgate**) is supported as a plugin in Vista Manager. This means you can add RADgate as an external RADIUS server and manage it from Vista Manager.

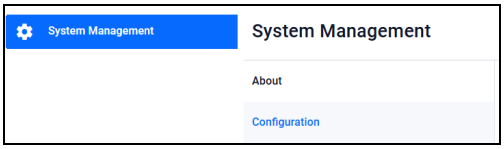
RADgate runs as a separate application, and can be accessed directly from Vista Manager for any advanced configuration. For more information about RADIUS, see the RADIUS Feature Overview and Configuration Guide.

As a Vista Manager plugin, the RADgate user database and information are synced to Vista Manager for an integrated view and simplified user access management.

Note: To use RADgate as part of Vista Manager's Intelligent Edge Security (IES) solution an AMF Plus license is required.

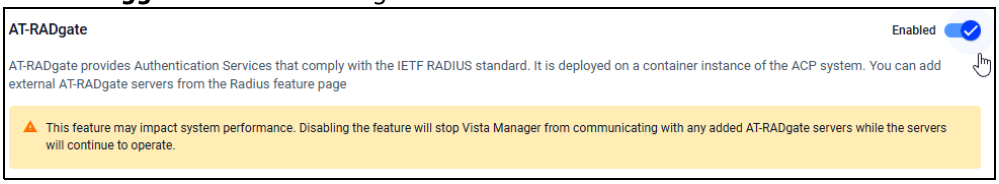
The following steps describe enabling RADgate as a Vista Manager plugin, and adding it as an external RADIUS server.

Go to **System Management** > **Configuration**



Scroll down to **Optional Features**.

Use the **Toggle** to enable AT-RADgate:

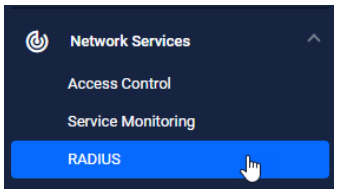


The RADgate feature is now enabled.

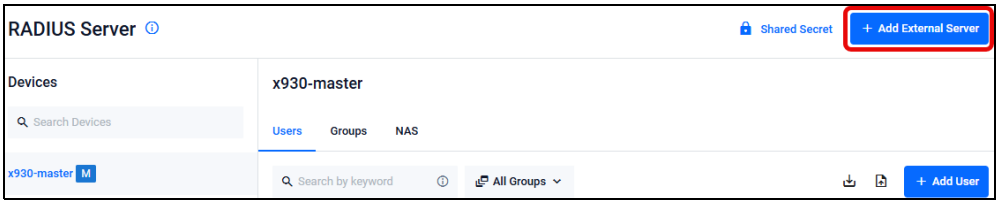
Note: The AT-RADgate RADIUS server is not yet available in all regions. See your Allied Telesis representative for more information.

To add an External RADIUS Server for RADgate:

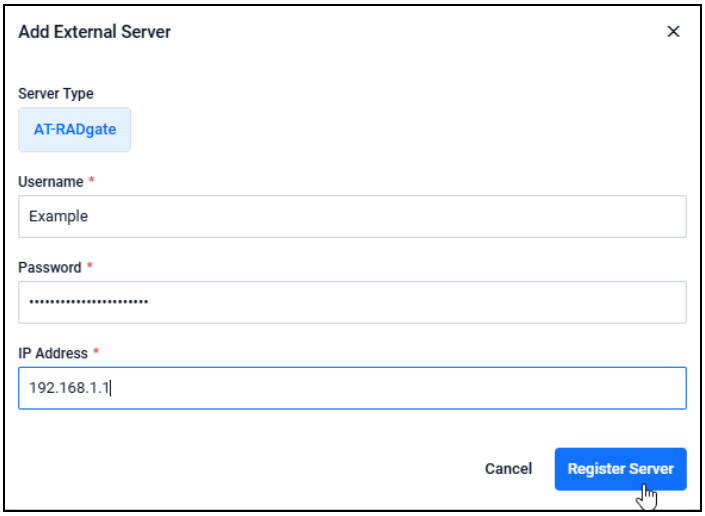
Go to the **Network Services** > **RADIUS** page



Click the + **Add External Server** button



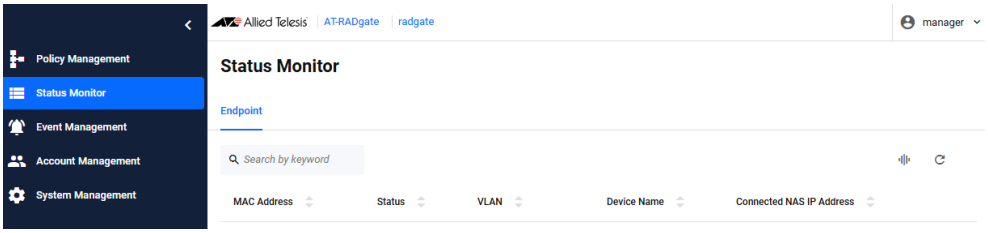
Enter the server credentials and IP address



Click **Register Server** to add it to Vista Manager.

- The server will appear in the side panel. You can freely add users from the RADIUS page, and they will display in Vista Manager as well as in the RADgate application.
- The newly added server also appears as a device on the Network Map.
- You can delete the RADgate server by clicking the Delete button on the RADIUS page, but you cannot delete local RADIUS servers.

To check information about the RADIUS Server, please check the RADgate application. To do this, **right-click** on the RADGate server device icon on the map.



Note: If you disable the AT-RADgate feature from **Optional Features**, it will disconnect from Vista Manager. However, if you re-enable the feature from Vista Manager, then the connection to AT-RADgate servers will be resumed.

Support for viewing DPI traffic of multiple devices

Applies to all Vista Manager EX installations

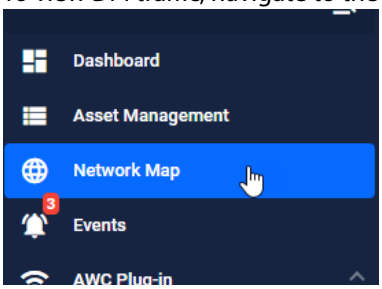
From version 3.13.1 onwards, you can select multiple devices when viewing DPI traffic.

This means that you can click on multiple DPI-enabled devices to display an aggregated view of traffic statistics across the selected devices.

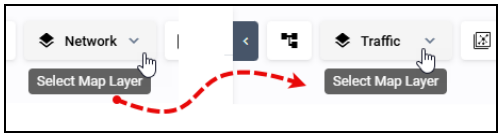
This means that as an admin user, you can analyze traffic across multiple zones or locations. Statistics and visuals of applications from the selected devices are shown on the left side-panel.

How to enable DPI:

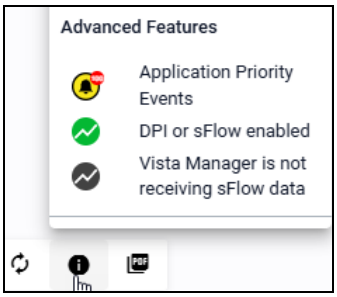
To view DPI traffic, navigate to the **Network Map**.



Click the dropdown to turn the Network Map into the Traffic Map.

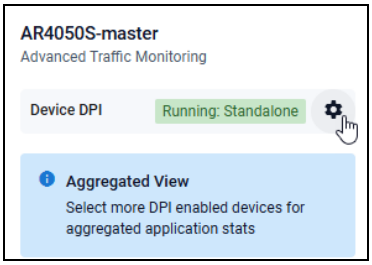


DPI Enabled devices have a green icon next to them.

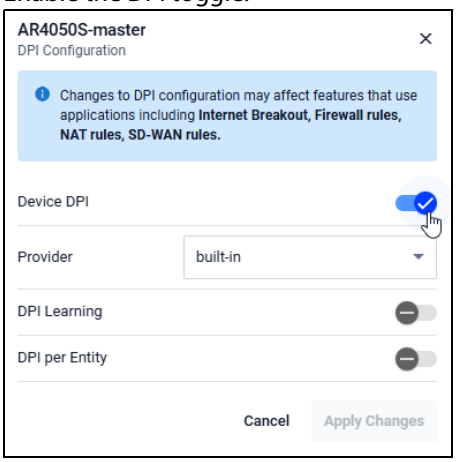


To enable DPI on a device, click on the device to bring up its information on the side panel.

Click the **Cog** icon to open the DPI settings.



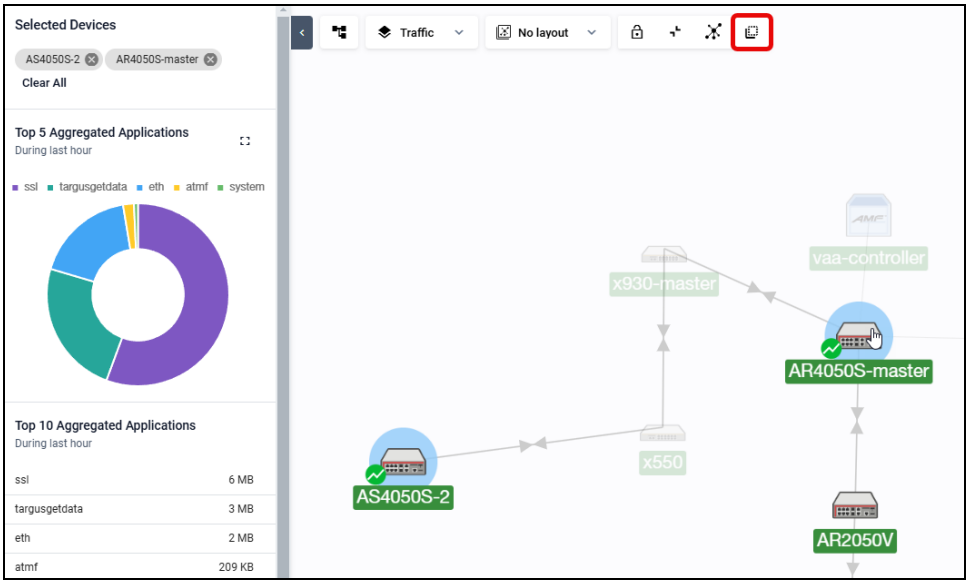
Enable the DPI toggle.



Click **Apply Changes**.

Once enabled, the DPI application information and DPI icon will display on the Network map.

To select multiple devices, **Ctrl + Click** or use the **Multi Select Devices button** to select multiple devices to include in them in the chart on the left panel.

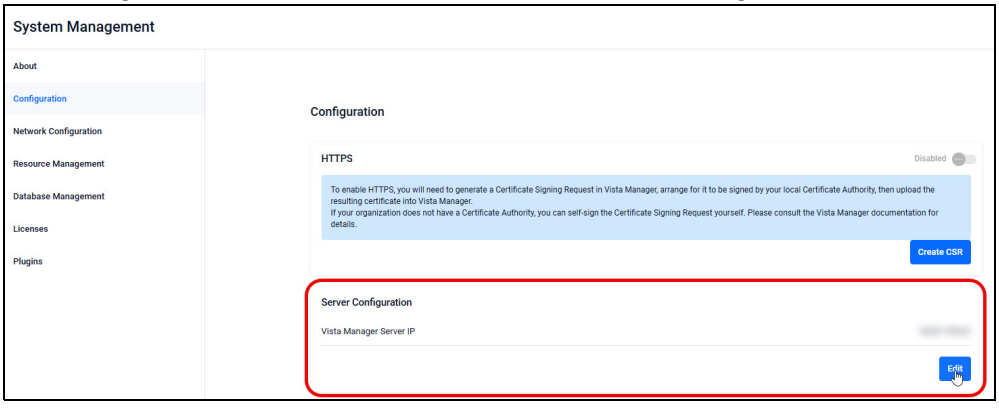


Support for changing server IP address for sFlow and SMTP

Applies to all Vista Manager EX installations

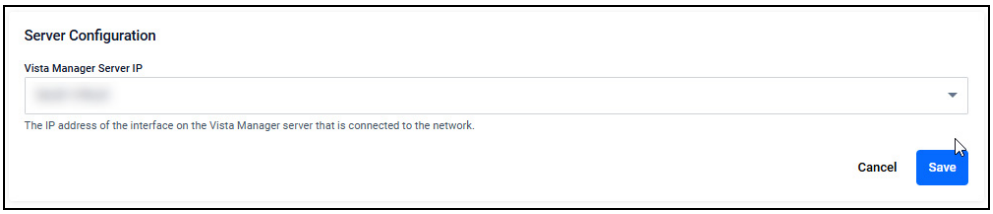
From version 3.13.1 onwards, support has been added to change the IP Address of the sFlow server.

This IP is used by devices with sFlow enabled for its Collector IP, and for SMTP when sending license expiration email alerts. Note that If this Server IP is changed, you will need to re-configure sFlow on the AlliedWare Plus devices that are configured to use it.



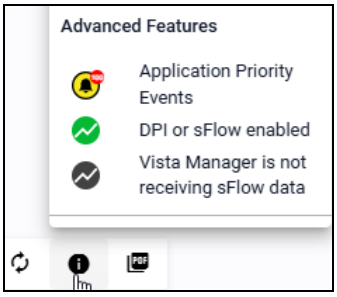
To change the IP Address for sFlow, go to **System Management** > **Configuration**.

Under **Server Configuration**, click **Edit** to change the Vista Manager IP address. Vista Manager will display a list of IPv4 addresses that you can select from.



The default is set to the first public IPv4 address in the list.

On the Network map, sFlow enabled devices with an IP address that matches the Vista Server IP address have a green icon next to them.

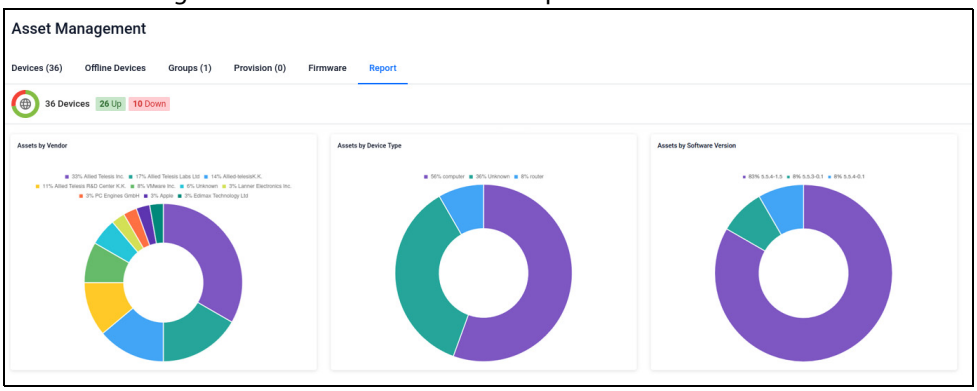


Updates to the Asset Management Reports tab

Applies to all Vista Manager EX installations

From version 3.13.1 onwards, you can view statistics on vendors, device types, and software versions of the devices discovered by Vista Manager and its plugins on the **Reports** tab of the Asset Management page.

The **Asset Management** > **Reports** tab shows you pie graphs of vendors for devices learned from all sources, device types, and software versions. Any device Vista displays in the Asset Management table is included in the report charts.



Minor changes for other pages include:

- If either Vista Manager or a plugin cannot identify a device's vendor, it will not display the vendor on the Network map side-panel.
- On the Devices tab of the Asset Management page, the Device Type column header has changed to Model. This change is to accurately distinguish it from the device type.

Improvement of the CPU Usage widgets in Health Monitoring

Applies to all Vista Manager EX installations with an AMF Plus License

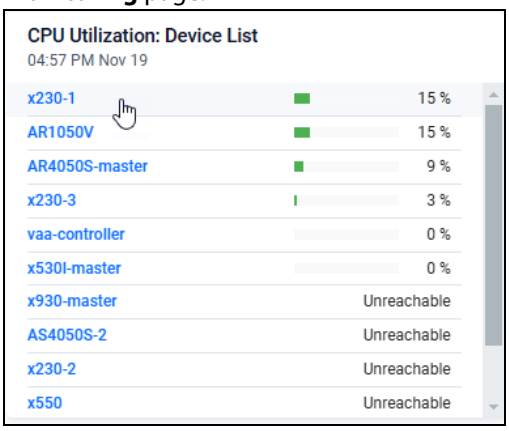
From version 3.13.1 onwards, the Health Monitoring dashboard has improved CPU usage statistics.

- Historical CPU usage data has been improved to show accurate historical data.
- CPU usage data now correctly matches the CLI command equivalent (**show cpu**).
- CPU charts in Vista Manager update in real-time.

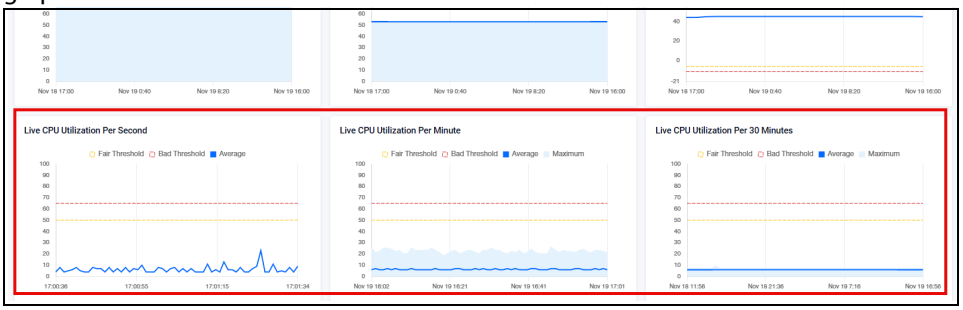
New CPU charts include:

- CPU load history per second (over the last 60 seconds)
- CPU load history per minute (over the last 60 minutes)
- CPU load per 30 minutes (the last 60 load values over 30 hours)

To see a device's live CPU statistics, click on a device from the **Device list** on the **Health Monitoring** page.



Scroll to the bottom of the Device's Health Monitoring page and you will see the Live CPU graphs.



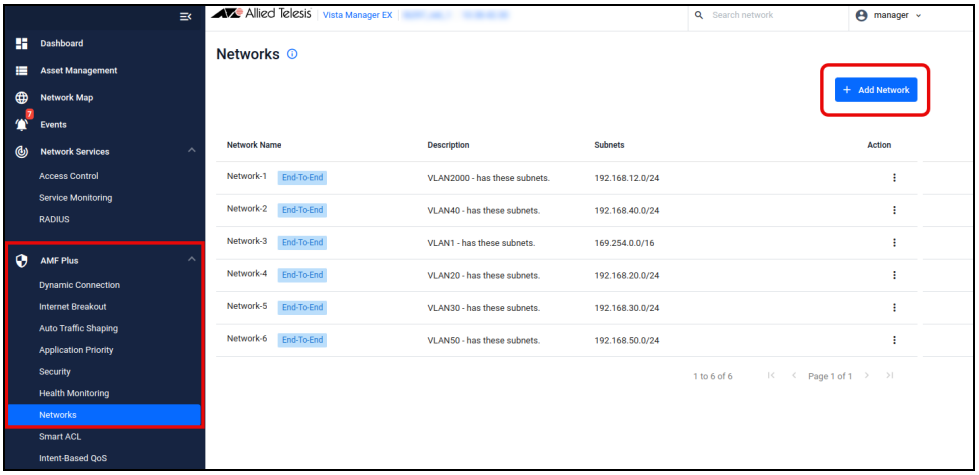
Enhancement to Smart ACLs

Applies to all Vista Manager EX installations with an AMF Plus License

From version 3.13.1 onwards, four new enhancements have been added to the Intent-based Access Control List feature.

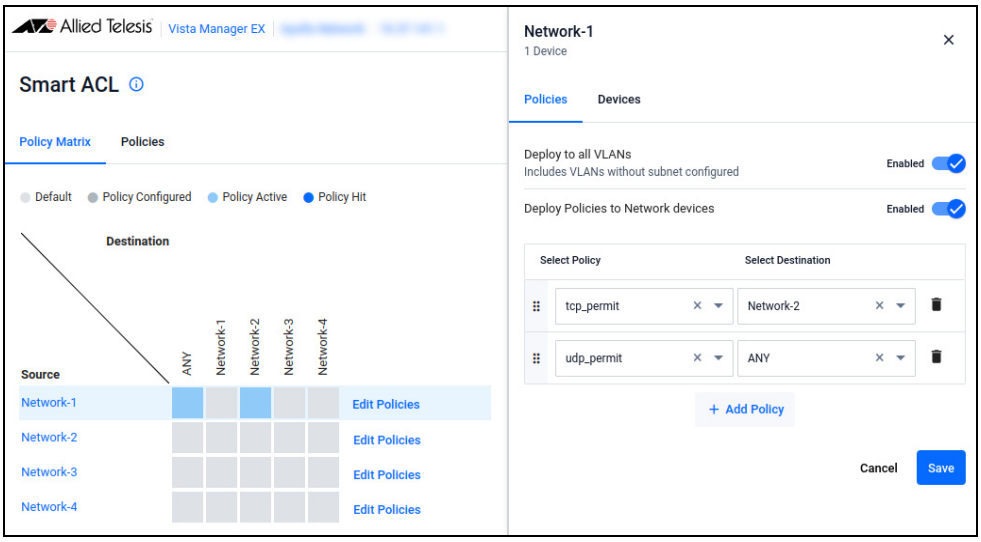
1. Use **destination networks** when creating ACLs to permit or deny traffic to these destinations. These destination networks can include networks outside of ones Vista Manager knows about.

You can add a new network by clicking the **+ Add Network** button from the **AMF Plus** > **Networks** menu.



2. A new **ANY** destination has been added, which allows you to to block or permit user access to all external networks. You can filter traffic through a list of rules, with ANY as a catch-all final rule.

3. When using **IP filtering** for managing which traffic types (protocols) an ACL will block or permit, a new ANY option will select all IP protocols (e.g. TCP, UDP, ICMP, etc). This makes configuration simpler, and saves needing a separate IP filter for each individual IP protocol.



4. You can apply **Smart ACL policies** to all network devices if desired (although this is not often necessary for ACL operation in the network). When choosing to

deploy to all switches, a toggle has been added to allow you to exclude edge switches with a low ACL limit to avoid oversubscribing capacity if you expect to need a large number of ACLs (see below).

Switches with a low ACL limit

A low limit of ACLs refers to devices with less than 512 ACL entries.

You can confirm the number of ACL entries on a device with the **show platform classifier statistics utilization brief** CLI command.

Edge devices with a low limit of ACLs include the following devices:

Device Series	ACL Entries
FS980M	496/408
GS900MX	119
IE200	496
IE210L	119
IE220	247
IE300	247
IE340, IE340L	119
IE510	247
x230, GS970M, x230L	119
x310	119
GS970EMX, x330	247
x510, x510L, x510DP, IX5	247
XS900MX	248

New Plugin support for Microsoft InTune

Applies to all Vista Manager EX installations with an AMF Plus License

From version 3.13.1 onwards, you can view alert information that is gathered by Microsoft InTune in Vista Manager. Vista Manager integrates information from Microsoft InTune for its InTune plugin to obtain a full picture of the monitored devices and security alerts.

Devices enrolled in InTune are shown on the Network Map and Asset Management pages in Vista Manager.

Note that you must have Microsoft InTune and associated applications, such as Microsoft Defender and Azure Event Hubs already configured. This includes endpoint devices synced with InTune. To see how to configure Microsoft InTune, see Microsoft InTune's Official Documentation.

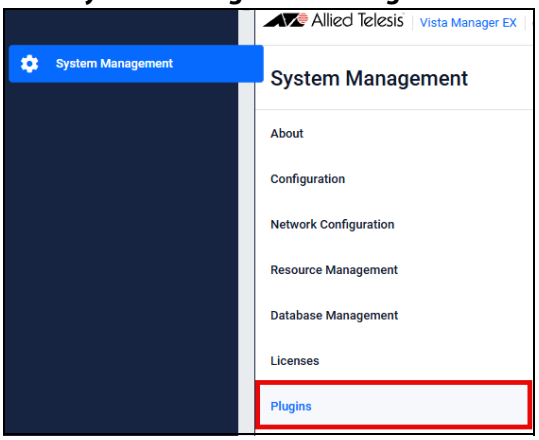
Security alerts are shown in the Event log. These are linked to the device that the alert occurred on. If the device has been removed from InTune, then no device information will be included in the Event.

On the Network Map, an alarm badge will be shown on devices that have security alerts.

Do not enable the Automatic Blocking feature from the Endpoints table while using the InTune plugin. If you have previously enabled Automatic Blocking, disable it.

How to install the InTune plugin:

Go to **System Management** > **Plugins**



Click **+ Add Plugin** on the Plugin table.

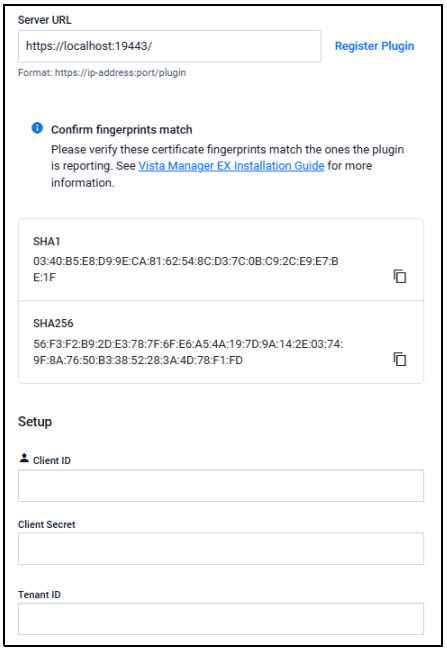
Register the plugin in the textbox with the server URL of **https://localhost:19443/**

Click outside of the textbox and Vista Manager will generate the certificate's fingerprints.

Confirm that the fingerprints match the InTune program.

Click **Confirm Fingerprints**.

Enter the Client ID, Client Secret, and Tenant ID



Click **Save.**

The Plugin will be added to your plugin list.

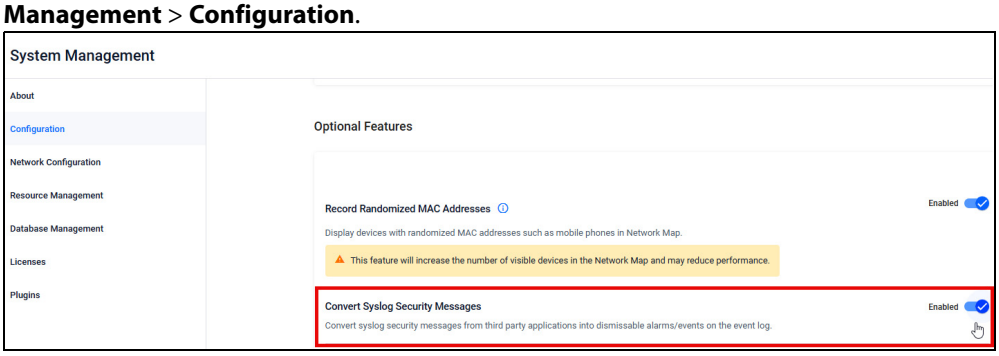
Support for Nozomi: Syslog Events and Endpoint blocking

Applies to all Vista Manager EX installations with an AMF Plus License

From version 3.13.1 onwards, support for third party security features from the Nozomi plugin have been implemented into Vista Manager. These changes include converting syslog security messages to dismissable alarms, and the ability to set up automatic endpoint blocking.

You can toggle Convert Syslog Security Messages to allow Vista Manager to create alarm events from the Nozomi plugin. These events are created with a severity level of ALERT.

To generate syslog event messages in Vista Manager when it receives a security related syslog from Nozomi, enable the **Convert Syslog Security Messages** feature in **System Management** > **Configuration**.



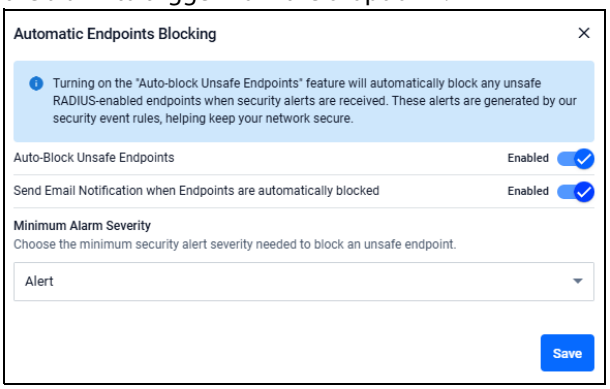
When you enable this feature:

- When Vista Manager receives a Syslog security message from Nozomi matching a security rule, it will create a event in the event log with a severity level of ALERT.
- This creates an alarm visible on the Network map and the Event log.
- An alarm count of endpoint device alarms with a severity of ALERT or higher is shown in the **Asset Management** > **Endpoints** Table. These can be dismissed to remove the alarm.

You can also automatically block devices discovered by Nozomi, based on security severity levels. When you enable **Automatic Blocking** from the **Asset Management** page, you can choose the severity level that triggers the automatic blocking from **Alert**, or **Emergency** levels.

To enable Automatic Blocking, click the **Cog icon** on the **Endpoints** tab of the **Asset Management** page.

Toggle to enable Automatic Blocking, and select the minimum security severity level for the alarm to trigger from the dropdown.



- When you enable **Automatic Blocking**, endpoints will be automatically blocked if a security alarm above the chosen severity occurs.
- You can enable email notifications for security related alarms.
- If an Endpoint has been automatically blocked you can manually unblock the device from the Asset Management table.

Endpoint history and statistical data from RADIUS is supported

Applies to all Vista Manager EX installations

From version 3.13.1 onwards, statistical data from RADIUS server connections are added to the Endpoints table on the Asset Management page, and the RADIUS User page.

The following columns have been added to the Endpoints page:

- The **Last Interaction Time** column displays the local timestamp for the most recent connection between an endpoint device and its associated RADIUS server
- The **Failed Connection Attempts** column displays the count of unsuccessful attempts from an endpoint device to connect to the specific RADIUS server since the server's last reboot.
- The **Successful Connections** displays the count of successful connections made by an endpoint device to the specific RADIUS server since the server's last reboot.

The value of these columns is updated every 5 minutes.

Similar columns are added to the RADIUS User table. You can track the timestamp of the most recent interactions between a RADIUS user and the RADIUS server.

These **RADIUS User** columns include:

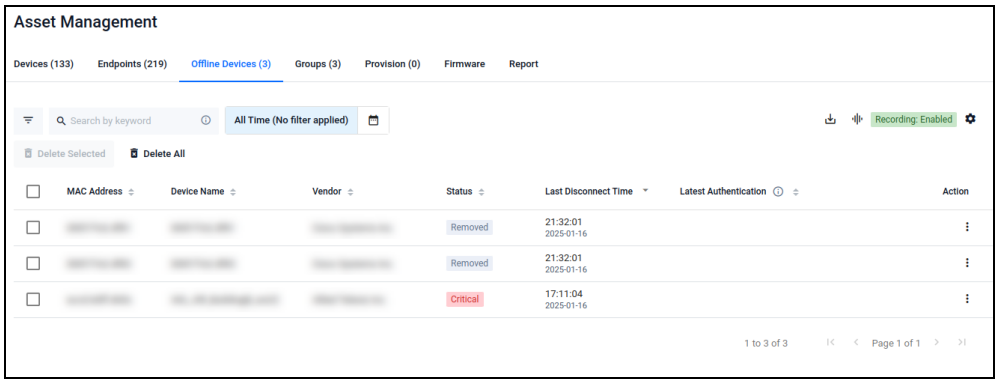
- The **Last Interaction Time** column displays the local timestamp for the most recent interaction between a RADIUS user and its associated RADIUS server. If the RADIUS user has no connected physical device, the value in this column may be empty.
- The **Failed Login Attempts** column displays the count of unsuccessful login attempts made by the RADIUS user since the server's last reboot.
- The **Successful Logins** column displays the count of successful logins of the RADIUS user since the server's last reboot.

You can sort the table data by the column types. The RADIUS users table will refresh when there are user changes on the RADIUS server, for example, user creation or user deletion.

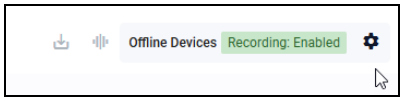
Offline Device Table (Device History) added to Asset Management

Applies to all Vista Manager EX installations

From version 3.13.1 onwards, the Offline Devices tab has been added to the Asset Management page. You can see all devices that have connected to your network and then left the network in the last 1.5 years by default from the **Asset Management** > **Offline Devices** tab. It is sorted with the most recently left device at the top.



- Filter the Offline Devices tab by the last disconnect time by using the new **Asset Management** > **Offline Devices** > **Time Range Picker**.
- Configure the Maximum offline device storage time within the range of 1 day to 2 years (731 days) by clicking the **Settings Cog**.

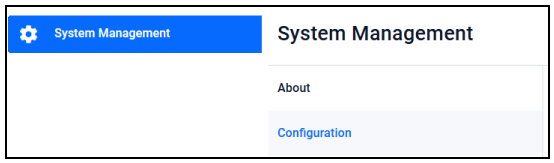


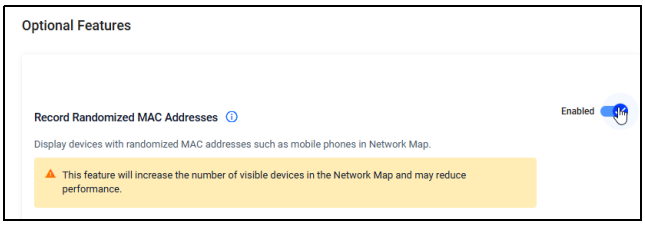
- Download a CSV file with all devices listed within the specified maximum storage time range. Click on the **Download CSV** button on the Offline Devices table.
- To see all devices that are currently part of my network, use the existing **Asset Management** > **Devices** table.
- You can export a PDF of the list by clicking the Download button.

Recording Randomized MAC Addresses feature

You can choose whether or not to record devices with randomized MAC addresses.

You can enable or disable the Record Randomized MAC Addresses feature from the **System Management** > **Configuration** page.





This feature is set to disabled by default.

When you initially toggle the Record Randomized MAC Addresses feature, and later if you decide there are now too many endpoints on the Network Map and Asset Management pages, you can remove the endpoints by disabling the Record Randomized MAC Addresses feature.

It may take several minutes for this change to appear. When you disable the Record Randomized MAC Addresses feature, the previously collected information will be removed from the Offline Device table.

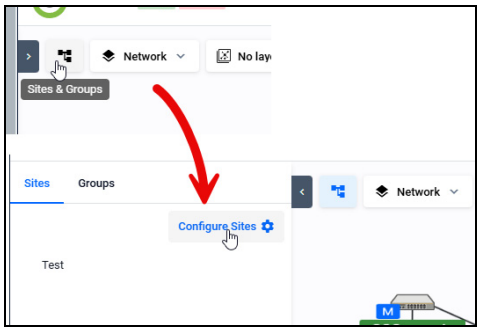
Further support for Sites, Layouts, and Auto-generated sites on the Network Map

Applies to all Vista Manager EX installations

From version 3.13.1 onwards, the network maps are made simpler. Vista Manager now offers the ability to focus on one site at a time, with improved flexibility to the Auto Sites Generator.

The existing **Auto Generate Sites** feature has been redesigned:

- The Network Hierarchy side panel has been changed to the **Sites & Groups** side panel, with two tabs of Sites and Groups.
- The menu on the Sites tab has been changed to **Configure Sites**, which is only available for Admin users. This menu includes three menu items, the existing **Add Site** and **Auto Generate Sites**, and a new menu item **Remove Auto Generated Sites** has been added.



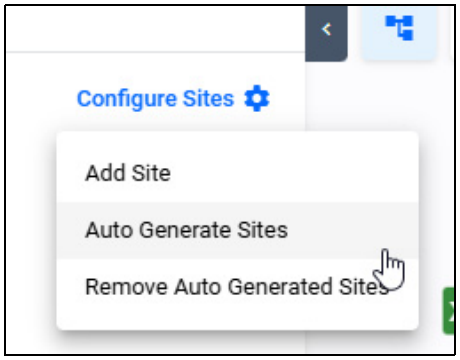
See the following sections for more information:

- "Auto-Generated Sites" on page 25.
- "Manually Created Sites" on page 27.
- "Regex format separator support for auto-site generation" on page 28.
- "Regex Hostname matcher support for auto site generation" on page 29.

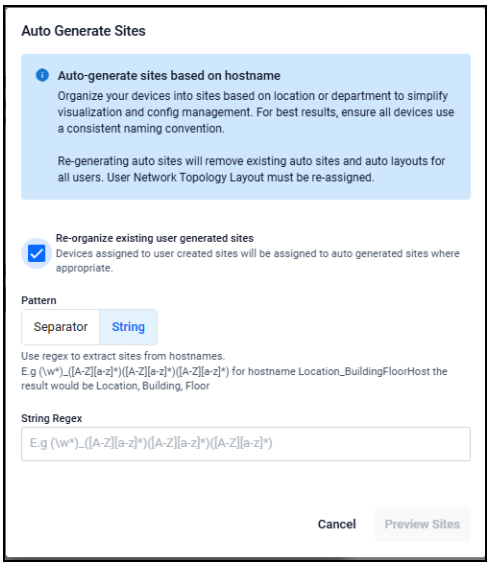
Auto-Generated Sites

Vista Manager can create auto-generated sites. Note that auto-generated sites are read-only, and cannot be edited after they are generated.

To auto-generate a site setup, click Auto Generate Sites from the Sites & Groups tab on the Network Map.



The Auto Generate Sites window will appear, where you can customize the regex pattern.



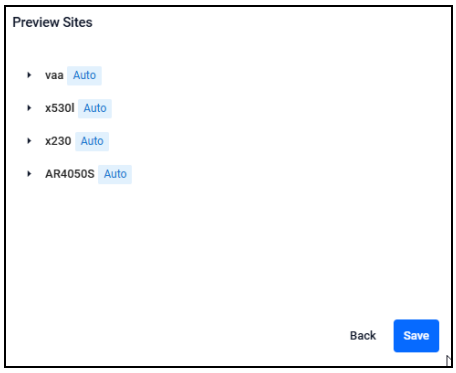
You can either enter a regex string, or choose to use an individual separator.

For more information about regex strings, see "Regex format separator support for auto-site generation" on page 28.

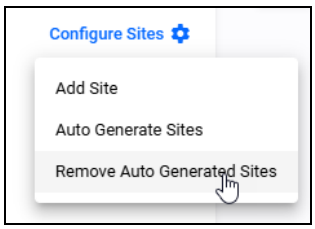
- If a device fails to be auto-assigned, it will remain in its original manually created site if it existed prior.
- When a new device joins the network after you auto-generate a site, Vista Manager will try to classify the hostname with the existing sites hierarchy automatically. If no existing sites exist. Vista Manager will create new sites for it.

If the hostname matches the parent site but not child sites, Vista Manger will create sites under the same parent site.

Click **Preview Sites** to get an example to confirm the generated setup.



When you click the **Remove Auto Generated Sites** button, all Auto-generated sites and their corresponding layouts will be deleted. All devices assigned to Auto-generated sites will be reset.

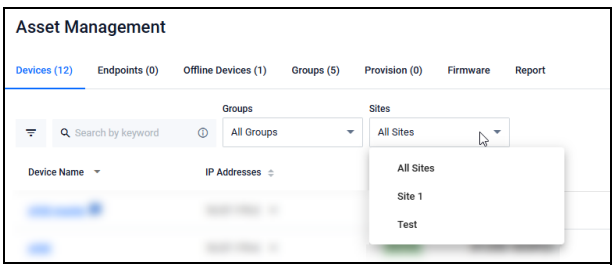


Auto-generated sites also generate **Layouts** with the same names as the sites. This allows you to easily switch between site layouts. See "Network Map Layouts" on page 27.

You can decide whether the existing manually created sites should be re-organized after the new auto-generated sites are confirmed.

- If you choose to re-organize the existing manually created sites, Vista Manager will try again to auto-assign a new generated site for all the managed devices. This includes the previously assigned devices.
- If you choose not to re-organize the existing manually created sites, the managed devices that do not belong to any manually created sites will attempt to auto-assign to the new auto-generated sites. The manually assigned devices will remain in the manually created sites.

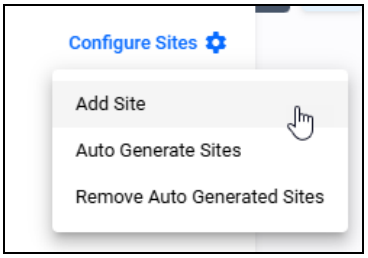
You can filter by Sites in the **Asset Management** > **Devices** tab. This filter can be used in combination with the pre-existing Groups filter on the Devices tab.



Note: Guest and 802.1x nodes won't appear when filtering devices by a specific site even if they are connected to a device located in that site, because those devices do not explicitly belong to that site.

Manually Created Sites

You can manually create sites via the Sites & Groups side panel by clicking the **Configure Sites** button and selecting the **Add Site** button.



Similarly to Auto-Generated sites, once a site is created, an automatically generated layout with the same name will be created for each user who has access to this site.

- You can also create a site from the Network Map by **right-clicking on device(s)** and selecting **Add Device(s) to New Site**.
- Admin users can edit user-created sites.

Network Map Layouts

On the Network Map, double click on a site to switch to the corresponding Layout.

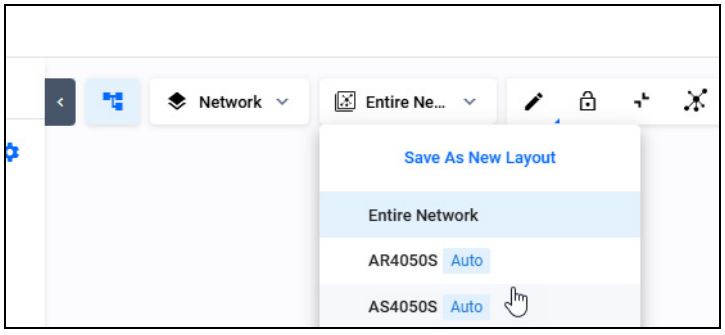
Click the top left button group of the integrated map to collapse all visible parent sites. Note that child sites will not be collapsed.

When viewing layouts for auto-generated sites, sites (including child sites) are expanded by default.

When expanding or collapsing sites, they will be saved like this automatically.

Note: The default layout for all users is the Entire Network. The Entire Network layout cannot be deleted. The Entire Network layout is read-only; it is not possible for the user to delete this layout.

Layouts of auto-generated sites and manually created sites have an **Auto** badge displayed next to its name in the layouts dropdown menu. Layouts are displayed in alphabetical order.



When you make changes to the Network Map, they will be automatically saved, including:

- Changing the position of devices/sites,
- Expanding/collapsing sites on the map,
- Changing the background image,
- and changing the zoom level of the map.

This change applies to all layouts, including Auto-sites layouts, user-created layouts, and the entire network.

- For non-admin users, the layouts they are given will depend on which auto-generated sites they are given permission for. Any auto-generated site that the user has permission for will have a corresponding layout for that user.
- Each user has their own layouts based on the auto-generated sites. Layouts are not shared between users, so each user can make their own changes to a layout and it will not affect the layouts for other users.
- Likewise, if permission was removed from some auto-generated sites, the layouts for those sites will be removed. If a user saved their own copy of an auto-generated layout, that copy will not be affected.
- Layouts that were originally created from auto-generated sites will appear in a nested format.
- After running the Auto Site Generator again, the selected or default layout of all users may change.

A blue dot displays on the top right corner of the layout list if you make any changes to a manually created layout that require saving. An undo icon and save icon will appear next to the selected layout in the layouts list.

Examples of actions that can be saved include adding or removing a node.

- A non-admin user will only be able to see dot1x supplicants if the user has permission for a group and the group contains the dot1x supplicant.
- When sites are collapsed, a blue circle icon next to the site shows how many devices are in this collapsed site.

When migrating from an older release of Vista Manager any device that is a 802.1x supplicant and belongs to a site will be removed from the site during the database migration. It is very unlikely that a dot1x supplicant will have been explicitly added to a site. The device will now implicitly belong to whatever site the device is attached to.

In the **User Management** menu, you can set default layouts to your admin user account, as well as other users.

- When an Admin user edits their details, the user can see all accessible layouts in the Network Topology Layout drop-down list. This includes the entire network, all Auto-Generated Layouts, all manually-created site layouts, and all user-created layouts.
- When an Admin user is editing another user's details or creating a new user, the Network Topology Layout drop-down list only includes layouts that are allowed to be shared between users.

Regex format separator support for auto-site generation

You can select Regex as a **sites separator** for auto site generation. This feature allows you to define a custom separator pattern inside square brackets, where it will be read, and split into sites, child sites, and devices based on hostnames.

Vista Manager reads this data in a *Site* > *Child Site* > *Device* order.

For example, you can use an underscore inside square brackets as a Regex pattern for the following output:

Hostname format: CHCH_IT01SW01
Regex pattern: [_]

Results:

- One site named: CHCH
- One Device named: IT01SW01

Another example is:

Hostname format: CHCH_IT01-SW.01
Regex pattern: [_-.]

Results:

- One site named: CHCH,
- One child site named: IT01
- One child site nested in the IT01 site named: SW
- One device named: 01

Click Save after importing the regex string to store it.

If a site called Office has a child site named Building1, and a new device classified as "Office, Building2" joins, then Vista Manager will create a new child site for Building2 with the parent as Office.

Note: If the hostname fits any of the following examples it will be seen as an invalid hostname. Automatic site generation will not be performed on the below hostnames.

- starts with a separator (such as '_CHCH_Building'),
- ends with a separator (such as 'CHCH_Building_'),
- or has consecutive separator (such as 'CHCH__Building')

Regex Hostname matcher support for auto site generation

You can select Regex as a **site hostname matcher** for auto site generation as well. This feature allows you to define a custom regex string pattern to extract and create sites based on hostnames.

The following examples show example patterns:

Hostname format: CHCH_IT01SW01
Regex pattern: ([A-Za-z]+)_(\w{2})(\d{2})

Results:

- One site named: CHCH,
- One child site named: IT01

Hostname format: aklvaa01, aklswi02
Regex pattern: (\w{3})(\w{3})(\d{2})

Results:

- One site named: akl
- One child site named: vaa
- One device named: 01
- A second child site named: swi
- A second device in that site named: 02

The input regex string will be stored after clicking **Save**.

Live Migration support

Applies to all Vista Manager EX installations

From version 3.13.1 onwards, a banner system has been implemented for live migration of collections that may take a long time. During a live migration, these collections may not display correctly and may be inaccurate during migration.

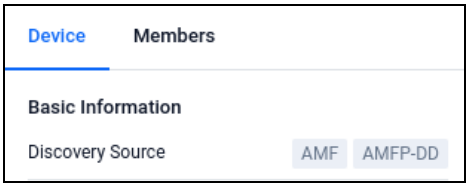
Live Migration is triggered when a database restore is performed. This is either enacted by you as a user from the **System** > **Database** screen, or automatically when AWC is upgrading the Vista Manager version.

Large collections include Health Monitoring information and history metrics, SDWAN history metrics, and pages with events, such as the Event page and Network Map.

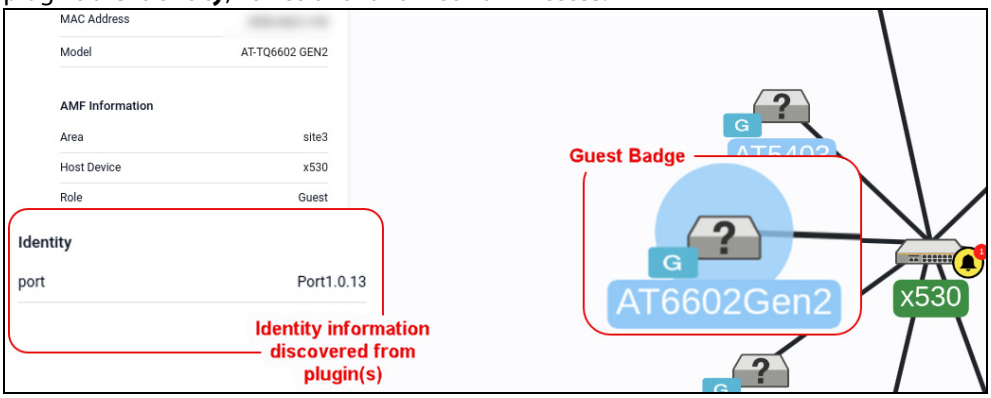
Discovery Source badges and Guest badge additions

Applies to all Vista Manager EX installations

From version 3.13.1 onwards, Vista Manager displays a **Discovery Source badge** under a device's Basic Information, about how the device was discovered.



In the Device information side-panel, new tabs including information gathered from plugins are **Identity**, **Functional** and **Network Access**.



An Guest badge has been added next to AMF Guest devices on the Network Map.

The badges M, C, C/M and G appear on Network layer of the Map and the Asset Management pages. These stand for:

- M - Master
- C - Client
- C/M - Client/Master
- G - Guest

Device management updates and Map Type column added to Asset Management

Applies to all Vista Manager EX installations

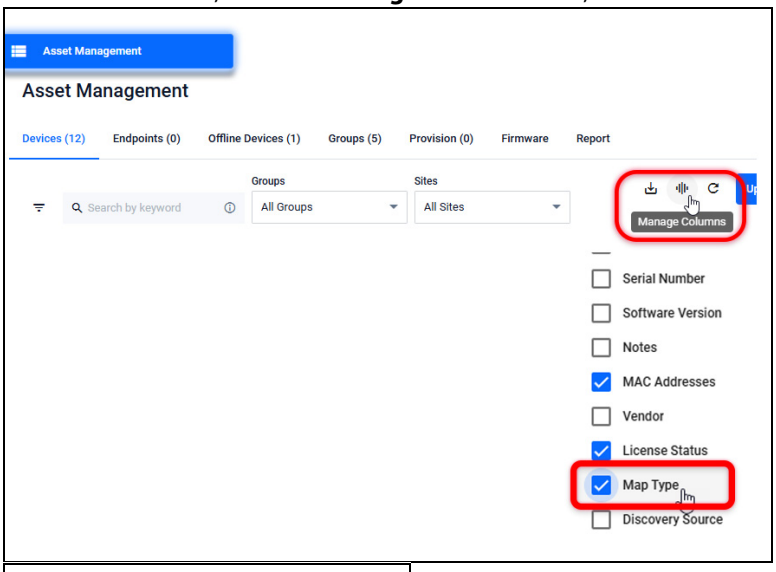
From version 3.13.1 onwards, changes to device management labels on the Asset Management page, such as devices statuses and node types have been made.

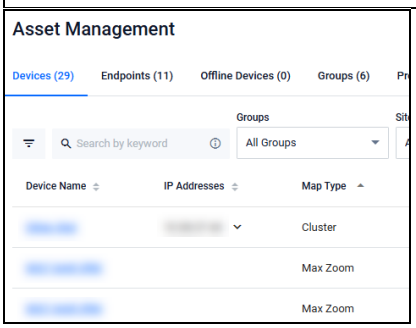
- Devices will not display a Status if the device does not provide one.
- The 'Unmanaged' status for devices has been removed.

This change has also been made on other pages where you see status information about your network (such as the Dashboard, Network Map etc.)

On the **Asset Management** page, a new column titled **Map Type** has been added.

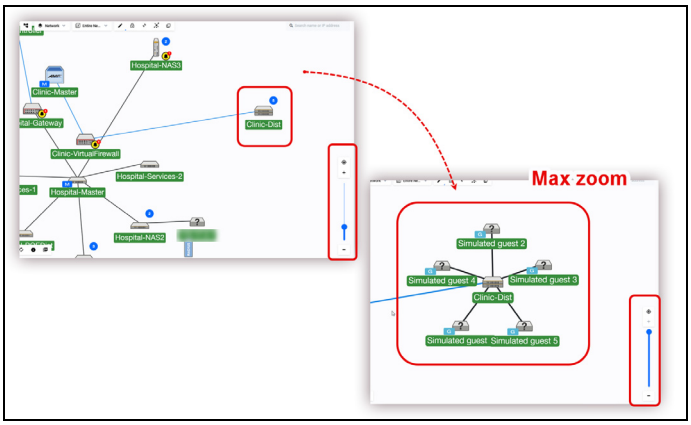
To add this column, click the **Manage Columns icon**, and check the **Map Type** column.





The Map Type column aims to differentiate nodes that are:

- Cluster nodes (Stacked devices),
- Device nodes (Devices seen on the map at all zoom levels),
- or Max-Zoom (Devices that are only seen on maximum zoom).



Support for more characters on the AMF Plus Networks page

Applies to all Vista Manager EX installations with an AMF Plus License

From version 3.13.1 onwards, restrictions on network names on the AMF Plus > Networks page have been reduced. Previously, users were only allowed to use English characters. This restriction has been updated to allow any characters except a single '-' or '_'.

AWC enhancements

TQ6403 GEN2 supports Channel Blanket

Applies to the TQ6403 GEN2 on all Vista Manager EX installations.

From version 3.13.1 onwards, the TQ6403 GEN2 access point now supports Channel Blanket (AWC-CB). This means that you can select the TQ6403 GEN2 as an AP model, and configure Channel Blanket from the AWC Plugin side menu in Vista Manager.

This feature requires firmware version 9.0.4-0.1 or later.

TQ6702 GEN2-R is supported with the AWC Plugin

Applies to the TQ6702 GEN2-R on all Vista Manager EX installations.

From version 3.13.1 onwards, the TQ6702 GEN2-R wireless router is supported with the AWC Plugin. This means that you can manage the TQ6702 GEN2-R from the AWC plugin sub-menu in Vista Manager, and can create AP profiles with the "Dual[11ax] GEN2-R" profile type.

New features include:

- If you change the configuration applied to the AP, it will display as Modified as its status.
- Rogue APs are displayed as detected by the TQ6702 GEN2-R
- AWC History calculation is supported.
- Logs related to AlliedWare Plus usage can be output.

Alongside this, you can perform reboots, upgrade firmware, and create tech support files for the TQ6702 GEN2-R from the AWC plugin menu. Note that other functions, such as router functions for the TQ6702 GEN2-R, cannot be configured via the AWC plugin.

This feature requires firmware version 5.5.4-2.x or later.

TQ6702 GEN2-R supports Airtime Fairness

Applies to the TQ6702 GEN2-R on all Vista Manager Installations.

From version 3.13.1 onwards, the TQ6702 GEN2-R supports Airtime Fairness. This means you can configure Airtime Fairness from the Radio Configuration page of an AP profile.

This feature requires AlliedWare Plus 5.5.4-2.x or later.

TQ6702 GEN2-R supports Passpoint

Applies to the TQ6702 GEN2-R on all Vista Manager Installations.

From version 3.13.1 onwards, the TQ6702 GEN2-R devices support the Passpoint feature. This means you can configure Passpoint for the TQ6702 GEN2-R device, and AP Profiles.

Passpoint™, also known as Hotspot 2.0, 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.

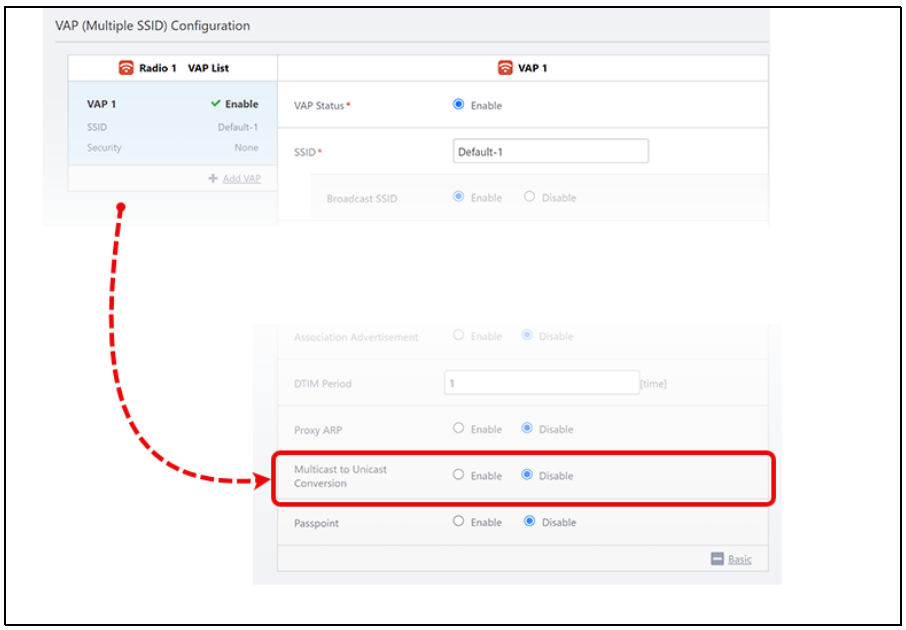
This feature requires firmware version 5.5.4-2.x or later.

TQ6702 GEN2-R supports multicast to unicast conversion

Applies to TQ6702 GEN2-R on all Vista Manager Installations.

From version 3.13.1 onwards, Multicast to Unicast conversion is supported on the TQ6702 GEN2-R.

You can enable the Multicast to Unicast feature in AP Profile > VAP (Multiple SSID) Configuration. It is disabled as default.



This feature requires firmware version 5.5.4-2.x or later.

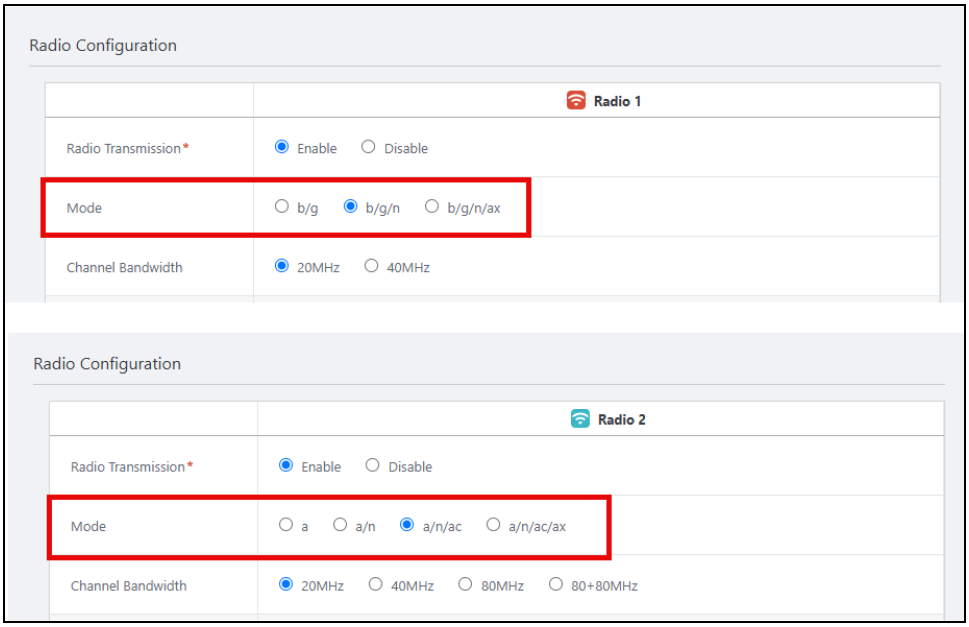
2.4GHz and 5GHz Wireless LAN modes supported for the TQ6702 GEN2-R

Applies to TQ6702 GEN2-R on all Vista Manager Installations.

From version 3.13.1 onwards, 2.4GHz and 5GHz band radio settings are selectable from the Wireless LAN settings on TQ6702 GEN2-R devices.

This includes:

- 2.4GHz band:
  - b/g/n
- 5GHz band:
  - a/n
  - a/n/ac



This feature requires AlliedWare Plus version 5.5.4-2.x or later.

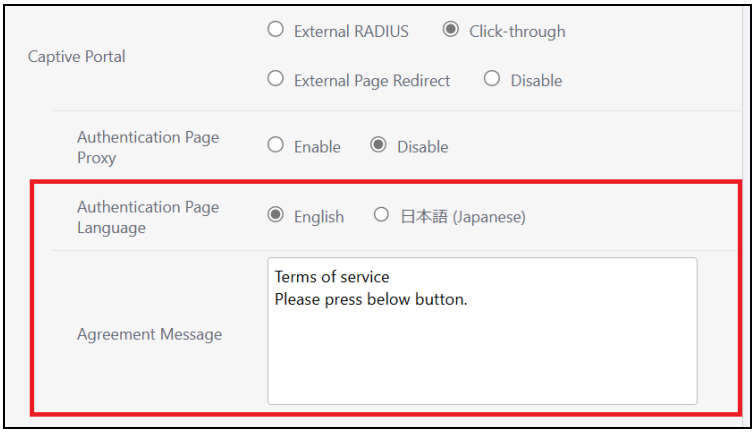
Agreement Message feature added to AP and CB Profiles

Applies to various access points on all Vista Manager EX installations (see below).

From version 3.13.1 onwards, you can create a custom Agreement Message as part of a client's authentication process. This will display when a client connects to your AP.

You can also select the language the text you input is written in, by switching the language from Authentication Page Language field between either English or Japanese.

The Agreement Message and Authentication Page Language fields are only displayed when you set Captive Portal to External RADIUS or Click-Through, and Authentication Page Proxy to Disable.



The Agreement Message field is displayed on the following AP Profile types:

- Dual[11ax] GEN2/Dual[11ax] GEN2 with External Antenna
- Tri[11ax]/Tri[11ax]

The Agreement Message field is displayed on the following CB Profile types:

- TQ6702 GEN2
- TQ6602 GEN2
- TQ6702e GEN2
- TQ6403 GEN2
- TQ7403

Note that this feature applies to the following devices and firmware:

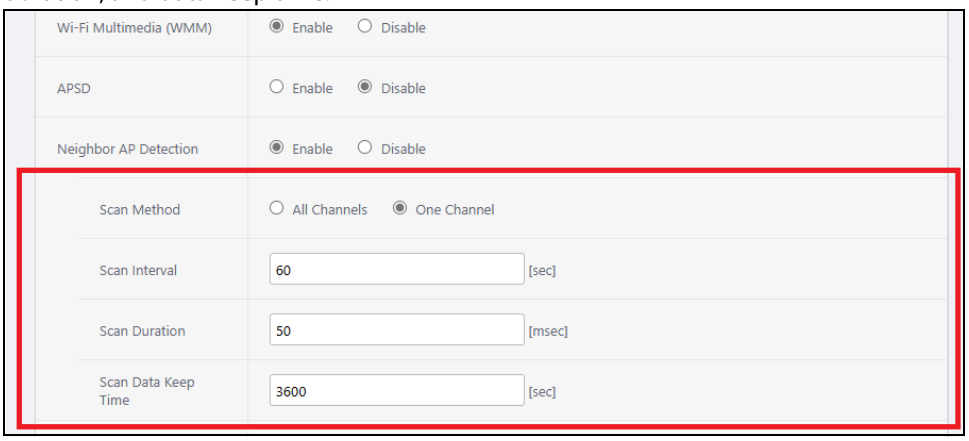
- TQ6602 GEN2 / TQm6602 GEN2 / TQ6702 GEN2 / TQm6702 GEN2: v8.0.4-0.1
- TQ6702e GEN2 / TQ6403 GEN2 / TQ7403: v9.0.4-1.1
- TQ7403: v10.0.4-1.1

Neighbor AP Detection Enhancements

Applies to various access points on all Vista Manager EX installations (see below).

From version 3.13.1 onwards, you can select a Scan Method for each radio when you enable Neighbor AP Detection in an AP Profile.

When you select One Channel as the Scan Method, you can also configure the scan interval, duration, and data keep time.



The Scan Method feature applies to the following AP Profile types:

- Dual[11ax] GEN2 with External Antenna
- Dual[11ax] GEN2
- Tri[11ax] GEN2
- Tri[11ax]

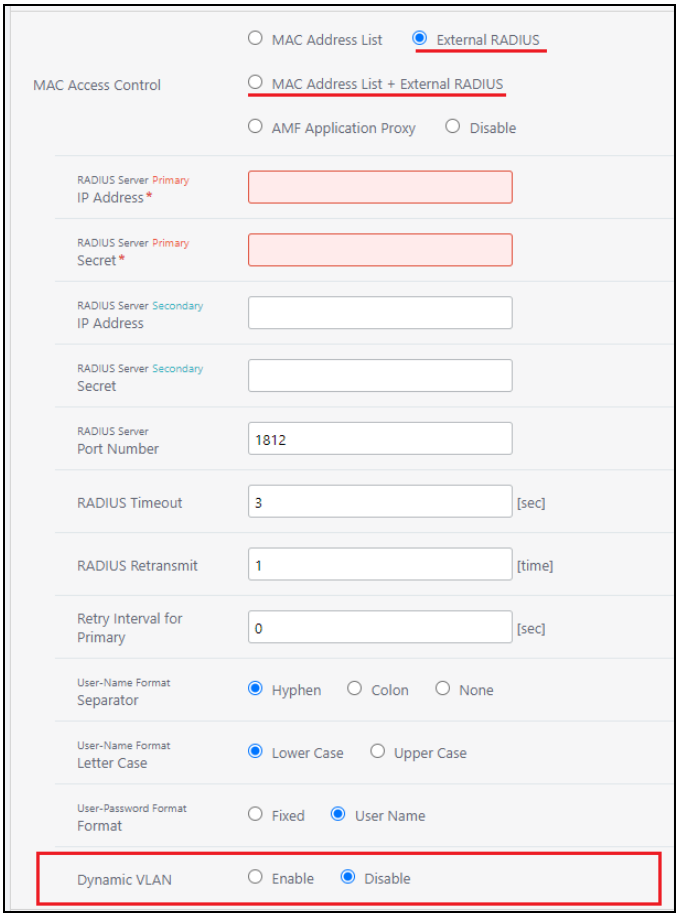
This feature requires the following firmware:

- TQ6602 GEN2 / TQm6602 GEN2 / TQ6702 GEN2 / TQm6702 GEN2: v8.0.4-0.1
- TQ6702e GEN2 / TQ6403 GEN2: v9.0.4-3.1
- TQ7403: v10.0.4-1.1

Support for Dynamic VLAN with WPA Personal and MAC Address List combinations

Applies to various access points on all Vista Manager EX installations (see below).

From version 3.13.1 onwards, you can enable or disable Dynamic VLAN from the MAC Access Control page in the AWC Plugin. This feature is available if you enable External RADIUS, or MAC Address List + External RADIUS.



The following AP Profile types are supported:

- Dual[11ax] GEN2-R
- Dual[11ax] GEN2 with External Antenna
- Dual[11ax] GEN2
- Tri[11ax] GEN2
- Tri[11ax]-R
- Tri[11ax]

The following CB Profile types are supported:

- AT-TQ6702 GEN2/AT-TQ6602 GEN2/AT-TQ6702e GEN2
- AT-TQ6403 GEN2
- AT-TQ7403

This feature requires the following firmware:

- TQ6602 GEN2 / TQm6602 GEN2 / TQ6702 GEN2 / TQm6702 GEN2: v8.0.4-1.1
- TQ6702e GEN2 / TQ6403 GEN2: v9.0.4-3.1
- TQ6702 GEN2-R: AlliedWare Plus v5.5.4-2.3
- TQ7403: v10.0.4-3.1

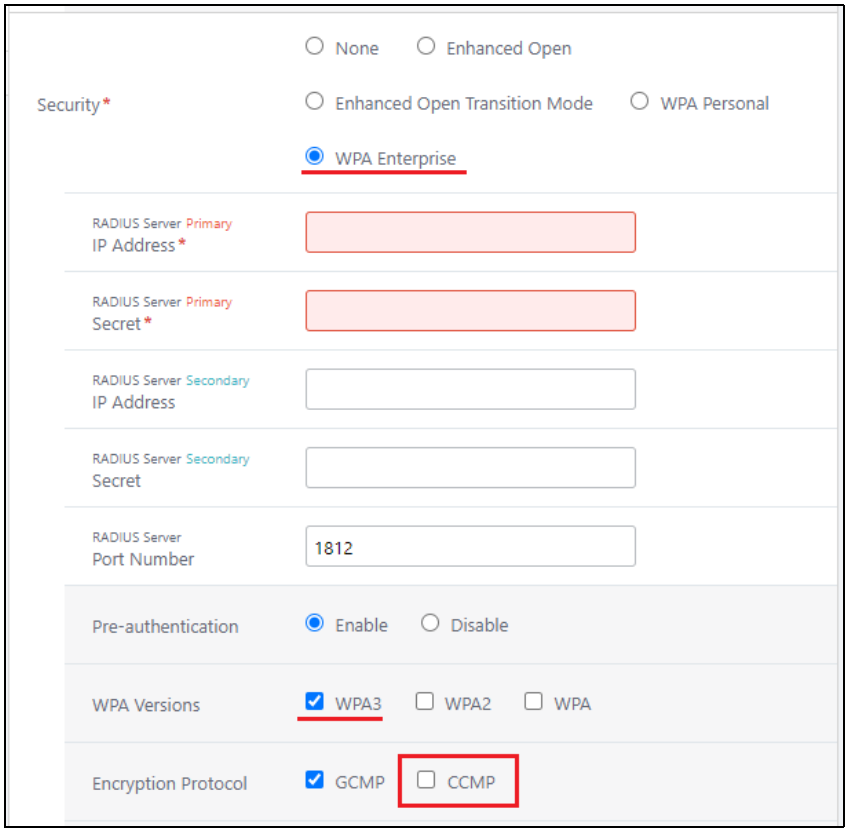
CCMP Protocol added to list of Selectable Encryption Protocols

Applies to various access points on all Vista Manager EX installations (see below).

From version 3.13.1 onwards, You can select the CCMP Protocol as an Encryption Protocol when you select the Security option WPA Enterprise and WPA version WPA3.

These settings are for AP Profiles, CB Profiles, and DCN Profiles.

Note that you can only select one Encryption Protocol.



This applies to the following AP Profile types:

- Dual[11ax] GEN2-R
- Dual[11ax] GEN2 with External Antenna
- Dual[11ax] GEN2
- Tri[11ax] GEN2
- Tri[11ax]-R
- Tri[11ax]

This also applies to the following CB Profiles:

- TQ6702 GEN2 / TQ6602 GEN2 / TQ6702e GEN2
- TQ6403 GEN2

This feature requires the following firmware:

- TQ6602 GEN2 / TQm6602 GEN2 / TQ6702 GEN2 / TQm6702 GEN2: v8.0.4-1.1
- TQ6702e GEN2/ TQ6403 GEN2: v9.0.4-3.1
- TQ6702 GEN2-R: AlliedWare Plus v5.5.4-2.3

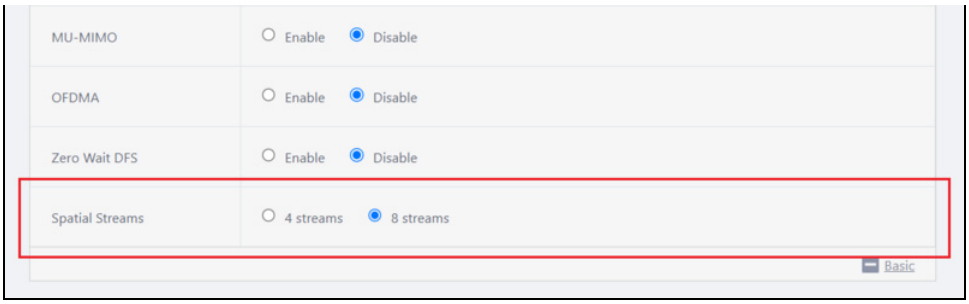
4 or 8 Spatial Streams selectable for Radio 2 on TQ6702 GEN2 and TQm6702 GEN2

Applies to TQ6702 GEN2 and TQm6702 GEN2 with firmware version v8.0.4-1.1 on all Vista Manager Installations.

From version 3.13.1, you can set the value of Spatial Streams for Radio 2 on TQ6702 GEN2 and TQm6702 GEN2 AP Profile pages.

You can select either 4 streams, or 8 streams. The default is 8 streams.

This feature is available on the Radio 2 section of the Radio Configuration section of the Dual[11ax] GEN2 AP Profile.



This feature requires firmware version v8.0.4-1.1 or later.

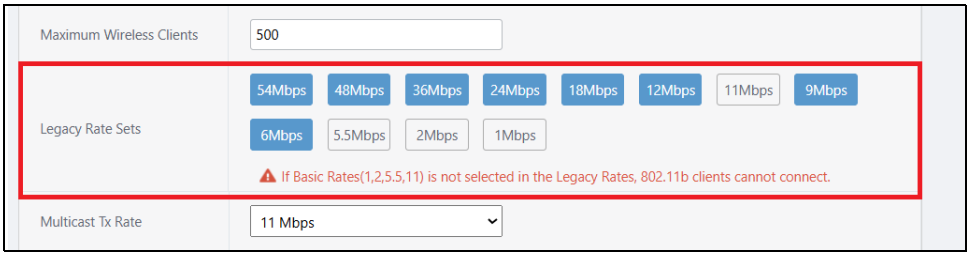
Change to Legacy Rate Sets Restriction

Applies to various access points on all Vista Manager EX installations (see below).

From version 3.13.1, the restriction of at least one Legacy Rate is no longer enabled, so you can manually disable all of them if required. By default, all the Legacy Rate Sets are selected.

Note that if Basic Rates(1,2,5.5,11) is not selected in the Legacy Rates, 802.11b clients cannot connect.

You can also select a Multicast Tx Rate from the assorted selected Legacy Rate sets you have already set above the dropdown.



This feature requires the following firmware:

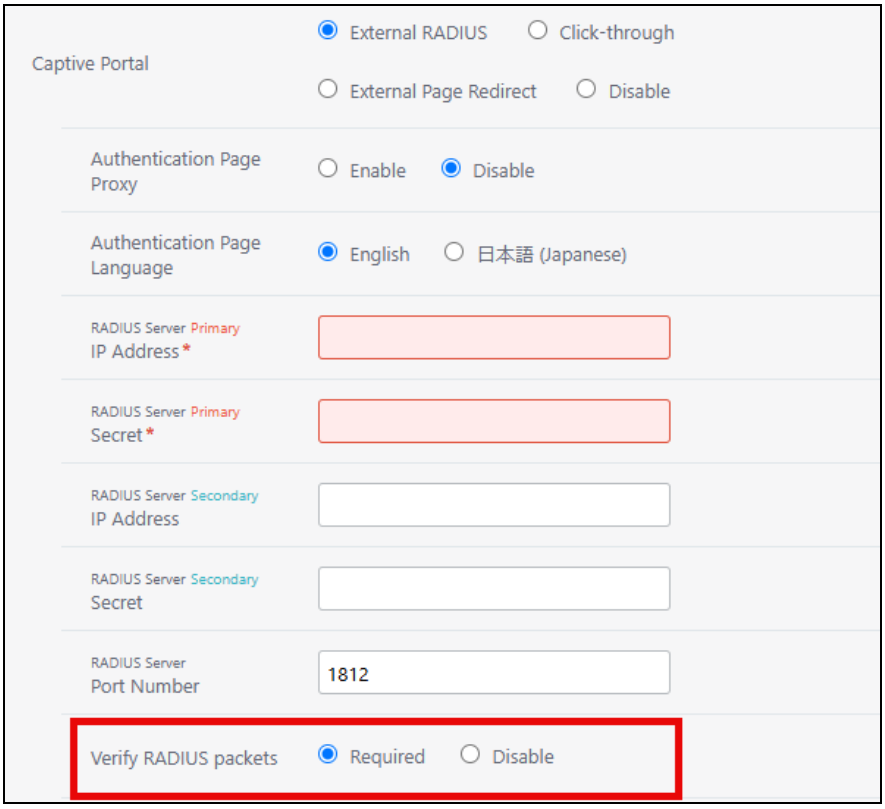
- TQ6602 GEN2 / TQm6602 GEN2 / TQ6702 GEN2 / TQm6702 GEN2: v8.0.4-1.1
- TQ6702e GEN2 / TQ6403: v9.0.4-3.1

Verify RADIUS Packets for RADIUS Authentication

Applies to various access points on all Vista Manager EX installations (see below).

From version 3.13.1, you can select Verify RADIUS Packets for WPA Enterprise, MAC Access Control, and Captive Portal. This feature uses RADIUS authentication to ensure responses are legitimate.

Note that it is Disabled by default.

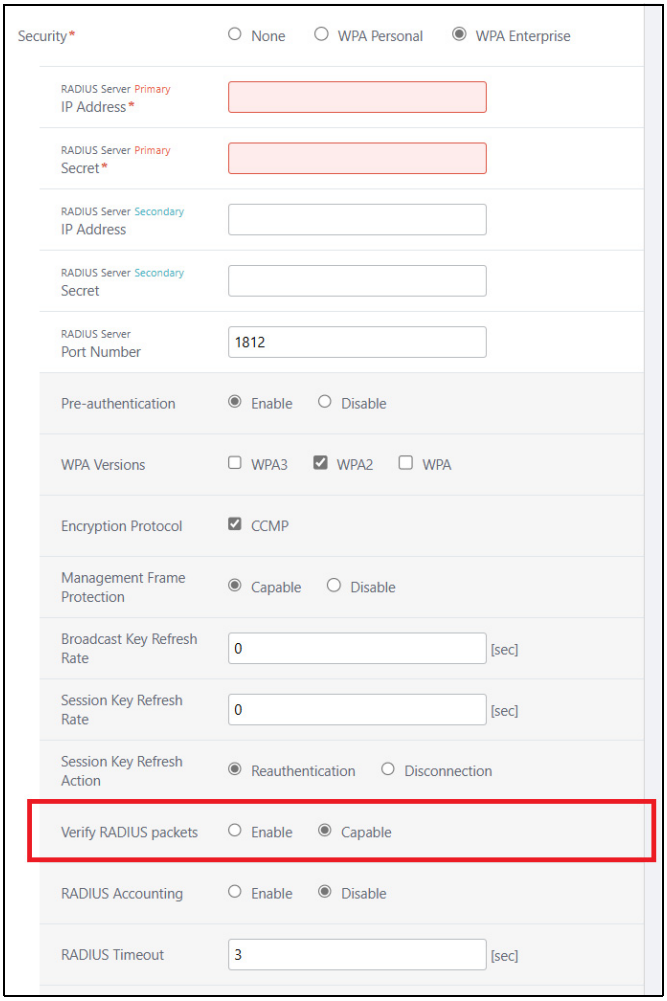


The Verify RADIUS Packets feature is available in the following AP Profiles:

- Dual[11ax] GEN2 with External Antenna
- Dual[11ax] GEN2
- Tri[11ax] GEN2
- Tri[11ax]

and the following CB Profiles:

- TQ6702 GEN2 / TQ6602 GEN2 / TQ6702e GEN2
- TQ6403 GEN2



This feature requires the following firmware:

- TQ6602 GEN2 / TQm6602 GEN2 / TQ6702 GEN2 / TQm6702 GEN2: v8.0.4-1.1
- TQ6403 GEN2 / TQ6702e GEN2: v9.0.4-3.1

Added new RADIUS Timeout and Retransmit fields for RADIUS client timeout

Applies to various access points on all Vista Manager EX installations (see below).

From version 3.13.1 onwards, you can edit the AP profile page to change the length of time to wait for a response from the RADIUS server before a client timeouts. You can find these settings on the AP Profile and CB Profile pages under MAC Access Control with either External RADIUS, or MAC Address List + External RADIUS selected.

In network environments with an external LDAP server, the RADIUS server may be slow to perform authentication, this feature enables you to customize the timeout and retransmit times.

The following fields including defaults are:

- RADIUS Timeout: (1-29 seconds max): Default 3s
- RADIUS Retransmit: (0-8 times max): Default 1
- Retry Interval for Primary: (0-600 seconds max): Default 0

This feature requires the following firmware versions:

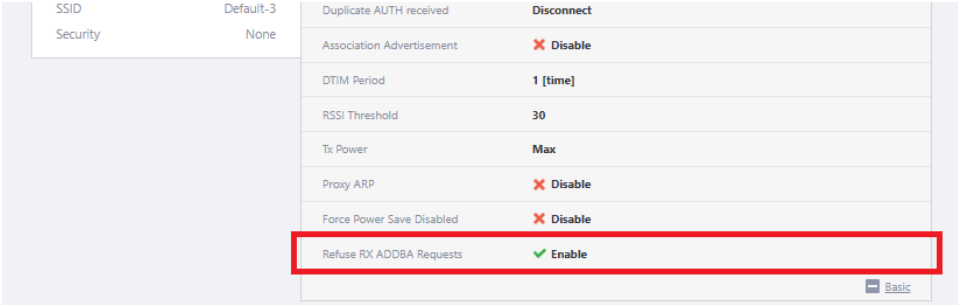
- TQ6702 GEN2 / AT-TQ6602 GEN2 / AT-TQ6702e GEN2: v8.0.4-0.1
- TQ6403 GEN2: v9.0.4-1.1
- TQ7403: v10.0.4-1.1

Support for TQ5403 and TQ5403e APs to refuse RX ADDBA requests for CB Profiles

Applies to TQ5403 and TQ5403e access points with firmware version 6.0.3-0.2

From version 3.13.1 onwards, you can choose to refuse RX ADDBA requests on the CB Profile page. It is disabled as default.

When you Enable the setting to refuse RX ADDBA requests, it will display as shown on the CB Profile:



This feature requires the following firmware versions:

AT-TQ5403 / AT-TQ5403e : v6.0.3-0.2

TQ6702 GEN2-R autonomous optimization has been enhanced

Applies to the TQ6702 GEN2-R on all Vista Manager installations with the AWC plug-in.

From version 3.13.1 onwards, AWC autonomous optimization of TQ6702 GEN2-R APs has been enhanced.

This requires firmware version 5.5.4-2x or later.

Enhancements to Dual[11ax] GEN2 with External Antenna AP Profile for TQ6702e GEN2

Applies to the TQ6702e GEN2 on all Vista Manager EX installations.

From version 3.13.1 onwards, the following configuration items are added to the TQ6702e GEN2 AP Profile.

Radio Configuration:

- Radio mode "b/g/n" for 2.4GHz and "a/n", "a/n/ac" for 5GHz are supported and added to the "Mode" section.

Table 1: Channel Bandwidth, MU-MIMO and OFDMA settings per Radio (TQ6702e GEN2)

	Radio 1			Radio 2			
	b/g	b/g/n	b/g/n/ax	a	a/n	a/n/ac	a/n/ac/ax
Channel Bandwidth	20MHz	20MHz 40MHz	20MHz 40MHz	20MHz	20MHz 40MHz 80MHz	20MHz 40MHz 80MHz 80MHz+80MHz	20MHz 40MHz 80MHz 80MHz+80MHz
MU-MIMO	-	-	Yes	-	-	Yes	Yes
ODFMA	-	-	Yes	-	-	-	Yes

- Wireless Client Isolation (within APs and VAPs) is supported.
- Airtime Fairness is supported.
  This item is displayed when Captive Portal and MAC Access Control are enabled.

VAP (Multiple SSID) Configuration:

- You can use a wildcard (*) in Walled Garden domain entries.
- DNS Proxy for a Walled Garden is supported in the Captive Portal section.
- MAC Address List + External RADIUS is supported in the MAC Access Control section. It is disabled by default.
- AMF Application Proxy is supported in the MAC Access Control section.
- Two-step authentication with Captive Portal is supported in the MAC Access Control section. This item is displayed when "Captive Portal" and "MAC Access Control" are set to enabled.
- Wireless Client Isolation (within APs and VAPs) is supported. It is disabled by default.
- Multicast to Unicast Conversion is supported. It is disabled by default.
- Pre-allocated Airtime Percentage is supported.
  This item is displayed as Airtime Fairness on Radio settings when set to Manual. The range limit is 0-100. 0 is the default.
- Passpoint is supported. It is disabled by default.

To access all of the above features, TQ6702e GEN2 APs require firmware version v9.0.4-3.1 .

Enhancements to the Tri[11ax] GEN2 AP Profile for TQ6403 GEN2

Applies to the TQ6403 GEN2 on all Vista Manager EX installations.

From version 3.13.1 onwards, the following configuration items are added to the TQ6403 GEN2 AP Profile.

Radio Configuration:

- Radio Modes "b/g/n" for 2.4GHz and "a/n", "a/n/ac" for 5GHz have been added.

Table 2: Channel Bandwidth, MU-MIMO and OFDMA settings per Radio (TQ6403)

	Radio 1			Radio 2				Radio 3			
	b/g	b/g/n	b/g/n/ax	a	a/n	a/n/ac	a/n/ac/ax	a	a/n	a/n/ac	a/n/ac/ax
Channel Bandwidth	20MHz	20MHz 40MHz	20MHz 40MHz	20MHz	20MHz 40MHz	20MHz 40MHz 80MHz	20MHz 40MHz 80MHz	20MHz	20MHz 40MHz	20MHz 40MHz 80MHz 160MHz	20MHz 40MHz 80MHz 160MHz
MU-MIMO	-	-	Yes	-	-	Yes	Yes	-	-	Yes	Yes
ODFMA	-	-	Yes	-	-	-	Yes	-	-	-	Yes

- Wireless Client Isolation (Within APs and VAPs) is supported.

VAP (Multiple SSID) Configuration:

- You can use a wildcard (*) in Walled Garden domain entries.
- DNS Proxy for a Walled Garden is supported in the Captive Portal section.
- Two-step authentication with Captive Portal is supported in the MAC Access Control section.

To access all of the above features, TQ6403 GEN2 APs require firmware version v9.0.4-3.1.

Enhancements to the Tri[11ax] AP Profile for TQ7403

Applies to the TQ7403 on all Vista Manager EX installations.

From version 3.13.1 onwards, the following configuration items are added to the TQ7403 AP Profile.

Radio Configuration:

- Radio Modes "b/g/n" for 2.4GHz and "a/n", "a/n/ac" for 5GHz have been added.

Table 3: Channel Bandwidth, MU-MIMO and OFDMA settings per Radio (TQ7403)

	Radio 1			Radio 2				Radio 3
	b/g	b/g/n	b/g/n/ax	a	a/n	a/n/ac	a/n/ac/ax	a/n/ac/ax
Channel Bandwidth	20MHz	20MHz 40MHz	20MHz 40MHz	20MHz	20MHz 40MHz	20MHz 40MHz 80MHz	20MHz 40MHz 80MHz	20MHz 40MHz 80MHz 160MHz
MU-MIMO	-	-	Yes	-	-	Yes	Yes	Yes
ODFMA	-	-	Yes	-	-	-	Yes	Yes

- Wireless Client Isolation (Within APs and VAPs) is supported.

VAP (Multiple SSID) Configuration:

- You can use a wildcard (*) in Walled Garden domain entries.
- DNS Proxy for a Walled Garden is supported in the Captive Portal section. It is disabled by default. This is also in the CB Profile.
- Two-step authentication with Captive Portal is supported in the MAC Access Control section. It is enabled by default. This is also in the CB Profile.

To access all of the above features, TQ7403 APs require firmware version v10.0.4-3.1.

Wireless Client Update-Interval has been renamed to Topology Data Update-Interval

Applies to Vista Manager EX v3.13.1 installations onwards.

From version 3.13.1 onwards, the label for the Wireless Client Update-Interval section in the AWC Settings page has changed to Topology Data Update-Interval. This title change was made to clarify that the AWC Network Map repopulates with APs, not just client devices.

Channel Blanket supports TQ7403

Applies to Vista Manager EX v3.13.1 installations onwards.

From version 3.13.1 onwards, Channel Blanket (AWC-CB) supports TQ7403 access points.

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.

Manual polling recommended if upgrading

Applies to all Vista Manager EX installations

From version 3.11.0 onwards, we recommend that you poll the network manually after upgrading Vista Manager EX.

This makes sure that Vista Manager EX acquires functionality that has been added in the new release, including functionality that depends on information from devices. Otherwise, features may fail to detect devices and will not work as intended.

To poll manually, use the **Refresh Topology** button on the Network Map:

Internet Explorer 11 compatibility

When using the Vista Manager EX 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, 7, or 8 if you wish to use this version of Vista Manager EX.

Vista Manager plugins

Do **not** delete a plugin from Vista Manager during a version upgrade. No de-registering or re-registering of plugins is required during this stage.

Fibre monitoring feature permissions

Note that on a **new** installation of Vista Manager EX, you will need to enable ***Active Fibre Monitoring*** permissions for users. This can be done on the ***User Management*** page.

Change to default value of RSSI Threshold for AWC Channel Blanket

Applies to TQ5403, TQ5403e, TQm5403, and TQ6602 APs

From version 3.9.0 onwards, when you create a new Channel Blanket profile, the default value for RSSI threshold is 30. Previously it was 0.

Note that if you restore a profile from backup and it uses the old default value of 0, the restored profile will continue to have a value of 0.

To configure a Channel Blanket profile, select **AWC Plug-in** > **Wireless Configuration** > **CB Profile** in the left-hand menu.

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.

Traffic map data not restored

When you upgrade Vista Manager EX, traffic map data from earlier versions will not be imported.

Obtaining User Documentation

Vista Manager documentation

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

AMF Plus documentation

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

- the AMF Plus Feature Overview and Configuration Guide
- the AMF Plus Datasheet
- the AMF Plus Cloud Installation Guide.

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 Support Portal. If you are going to install the AWC and/or SNMP plug-ins then download these files from the same location.

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

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

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

Backup Vista Manager EX and the plug-ins

Backup Vista Manager EX

1. Log in to Vista Manager and select the **System Management** page.
2. In the **Database Management** page, click on the **Backup** button next to the Backup tab.
3. 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

4. If you have the SNMP plug-in installed, log on locally to the **Vista Manager EX Server** on your Windows device.
5. **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**

6. 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.

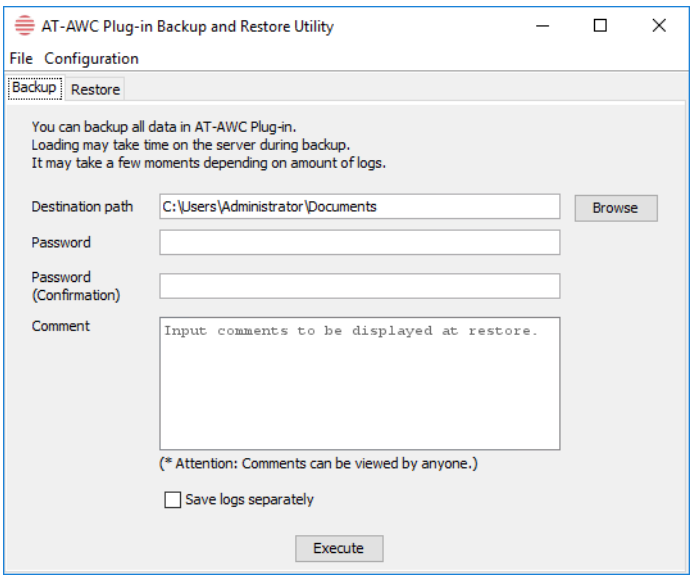
Backup the AWC plug-in

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

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

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

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



10. Select the 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

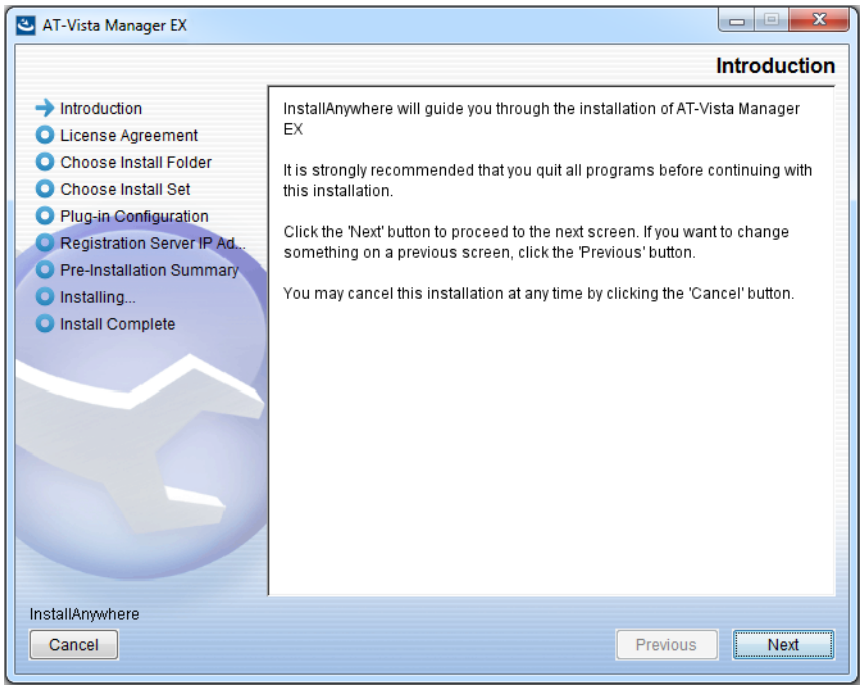
1. Log on to your Windows device as the same user as when installing.
2. Stop the server. Select ***AT-Vista Manager EX*** and then ***AT-Vista Manager EX - Stop Server*** from the Windows menu.
3. From the Windows menu, select ***AT-Vista Manager EX*** then ***AT-Vista Manager EX - Uninstall***.
4. The AT-Vista Manager EX uninstaller starts.
5. Click the ***Uninstall*** button to uninstall.
6. If a dialogue box prompting you to restart the system is displayed, select ***Restart the system*** or ***Restart later*** and click the ***Finish*** button.
7. Delete the installation folder. The default installation folder is:
   C: \ Program Files (x86) \ Allied Telesis \ AT-Vista Manager EX
8. Reboot the system.

Install the new version

1. From your Windows device, execute the Vista Manager EX installation program ‘atvmex***XXX***b***XX***w.exe’.

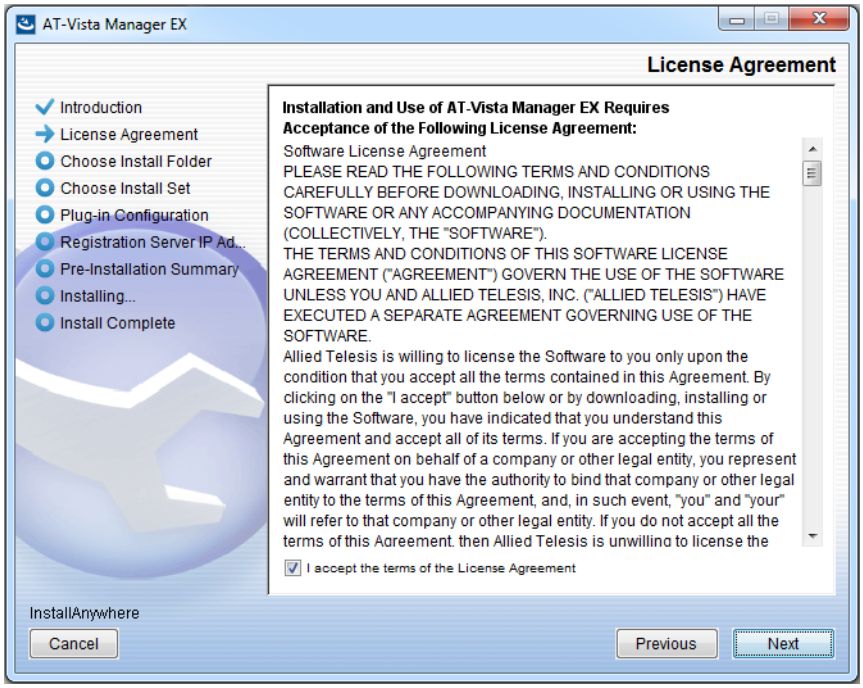
Note: You must have administrator privileges to run the installer.

2. The ***Introduction*** dialog displays:



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

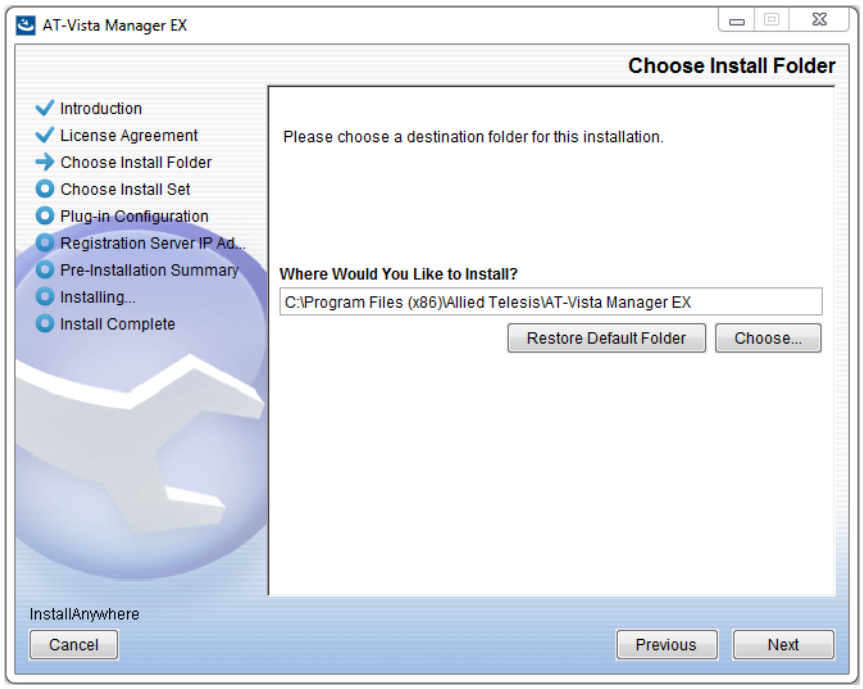
3. The ***License Agreement*** dialog displays:



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

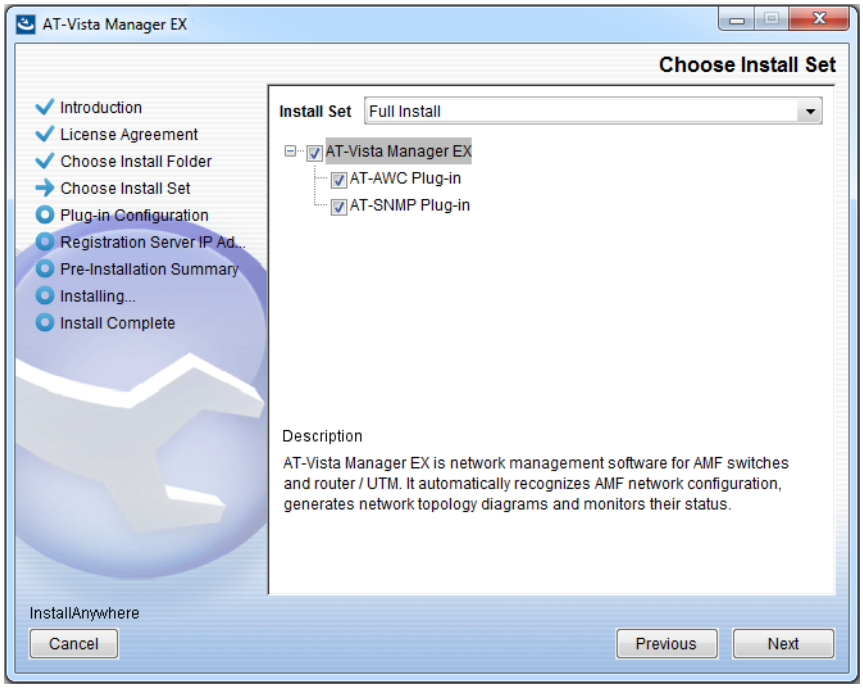
- Click **I accept the terms of the License Agreement**
- Click **Next**

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



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

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

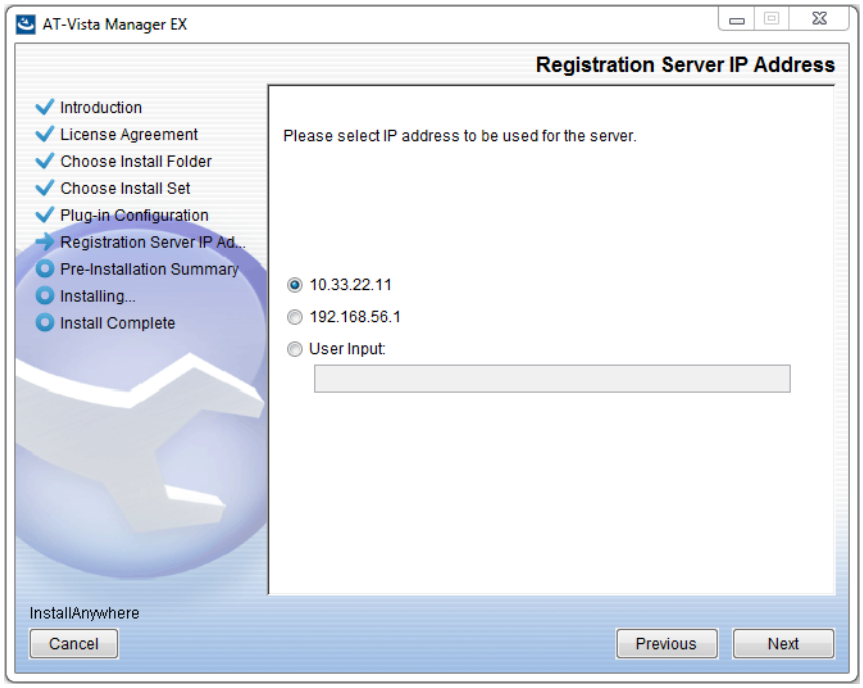


Select ***Full Install*** from the drop down list. By default all plug-ins are selected. Clear the check box for any plug-ins you do not wish to install. Click **Next**.

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

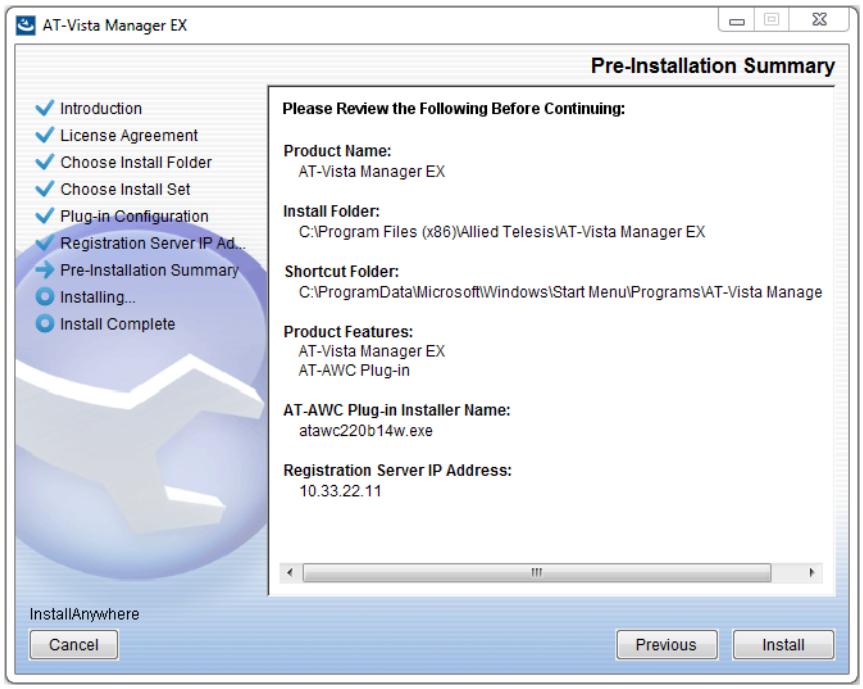
Select ***Do not create a public key*** unless you are intending to use the plug-ins in standalone mode. For more information on standalone mode, refer to the Installation Guide. Click **Next**.

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



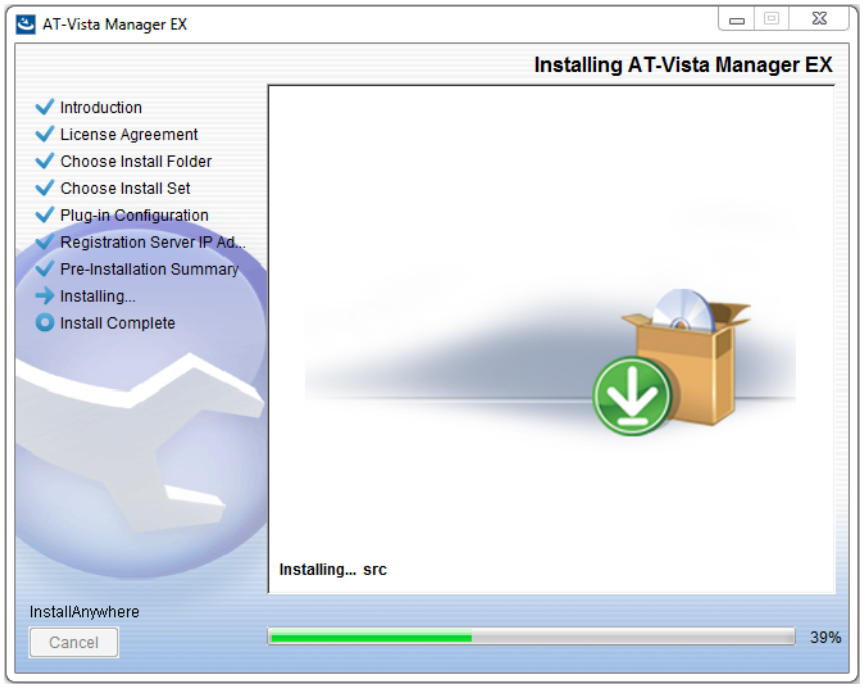
Either select from the list of IP addresses already configured on the Windows machine, or input a valid IP address. Click **Next**.

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

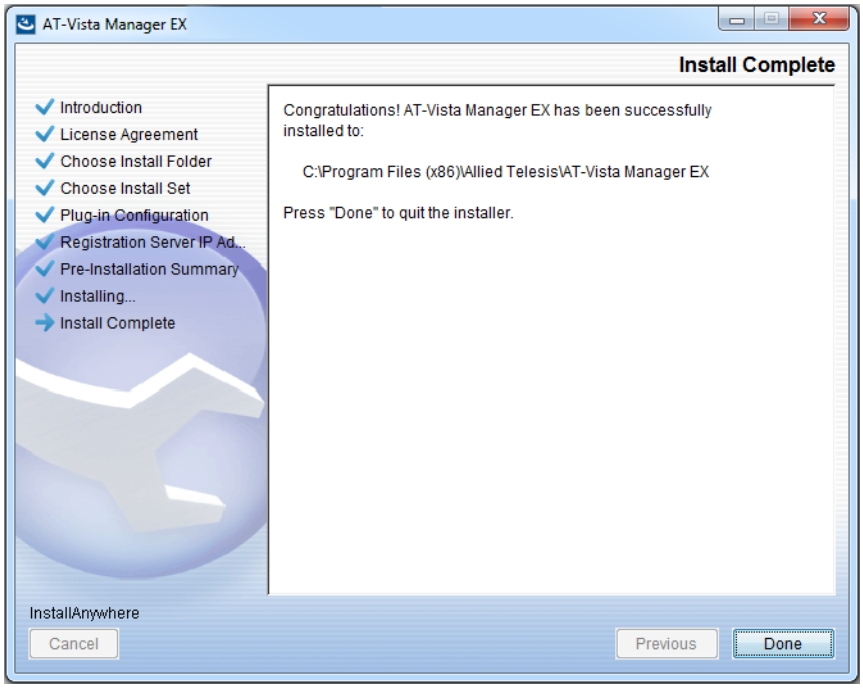


Check that your Product Name, Install Folder, Shortcut Folder, Product Features, Plug-in Installer Name and Registration IP Address are correct, and then click **Install**.

9. The ***Installing...*** dialog displays:



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

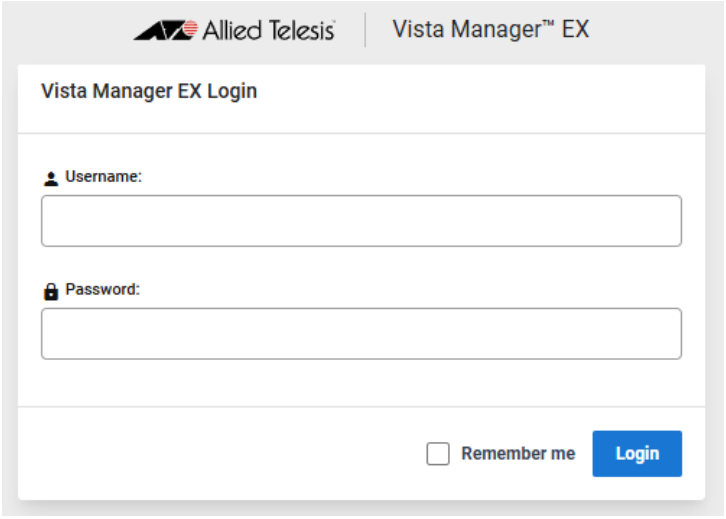


Check that the installation has completed successfully and click **Done**.

Restore the Vista Manager database

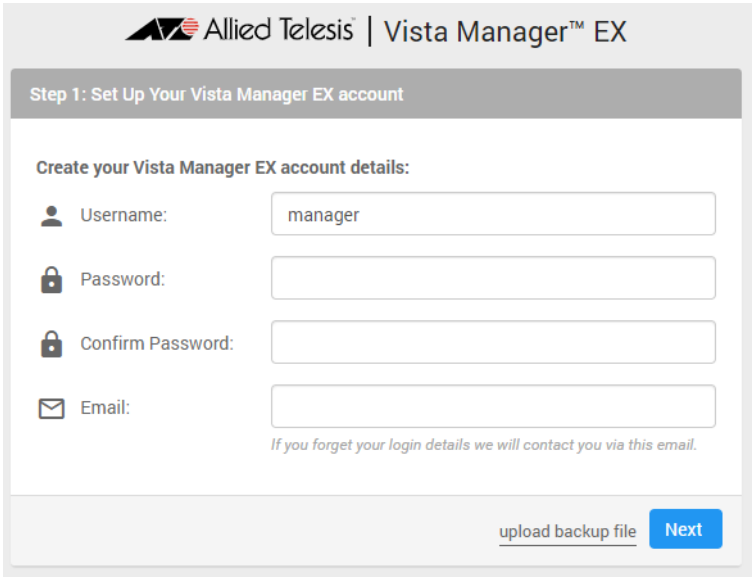
After the upgrade is complete, you need to restore the Vista Manager database. To do this, use the following procedure.

1. Login to Vista Manager.



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

2. Click on upload backup file.

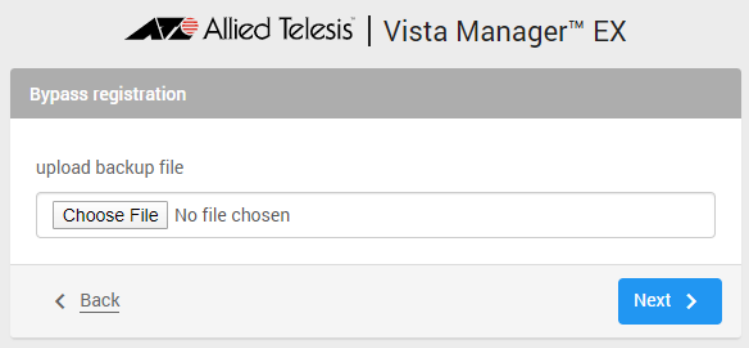


Caution Your serial number and license information are part of your database backup. If you upload the backup file when upgrading, you will keep the same serial number, and your licensing will continue to work without interruption.

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.

3. 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

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

   ***"<Vista Install Path>*\Plugins\AT-SNMP\NetManager\bin\svrcmd.bat" svrstop**
6. Run the restore utility by using the shortcut or by running the following command line.

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

   Follow the instructions on the screen.

Restore the AWC plug-in

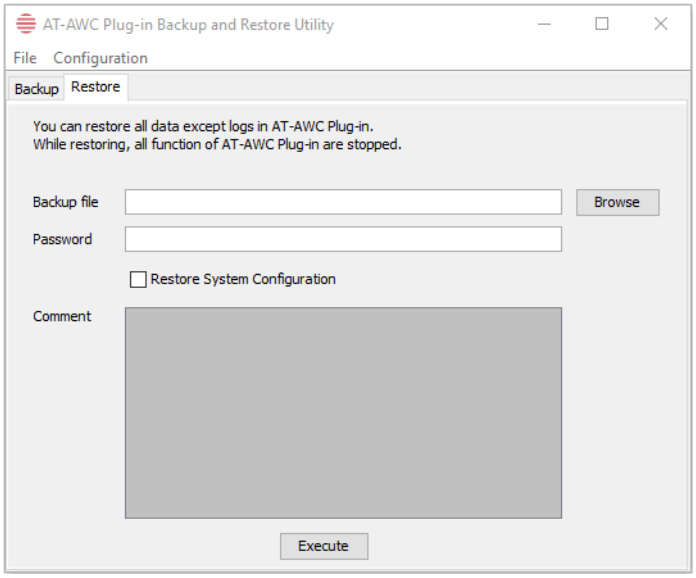
7. If you have the AWC plug-in installed then log on locally to the Vista Manager EX server.
8. Stop the AWC server services using the shortcut or by running the following command line.

   ***"<Vista Install Path>*\Plugins\AT-AWC\root\stopserver.bat"**
9. Run the backup/restore utility by using the shortcut or running the following command line.

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

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

Note: 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) Release Note.

Upgrading Vista Manager on VST-VRT

See the Vista Manager Virtual (VST-VRT) Release Note.

Troubleshooting

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

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com