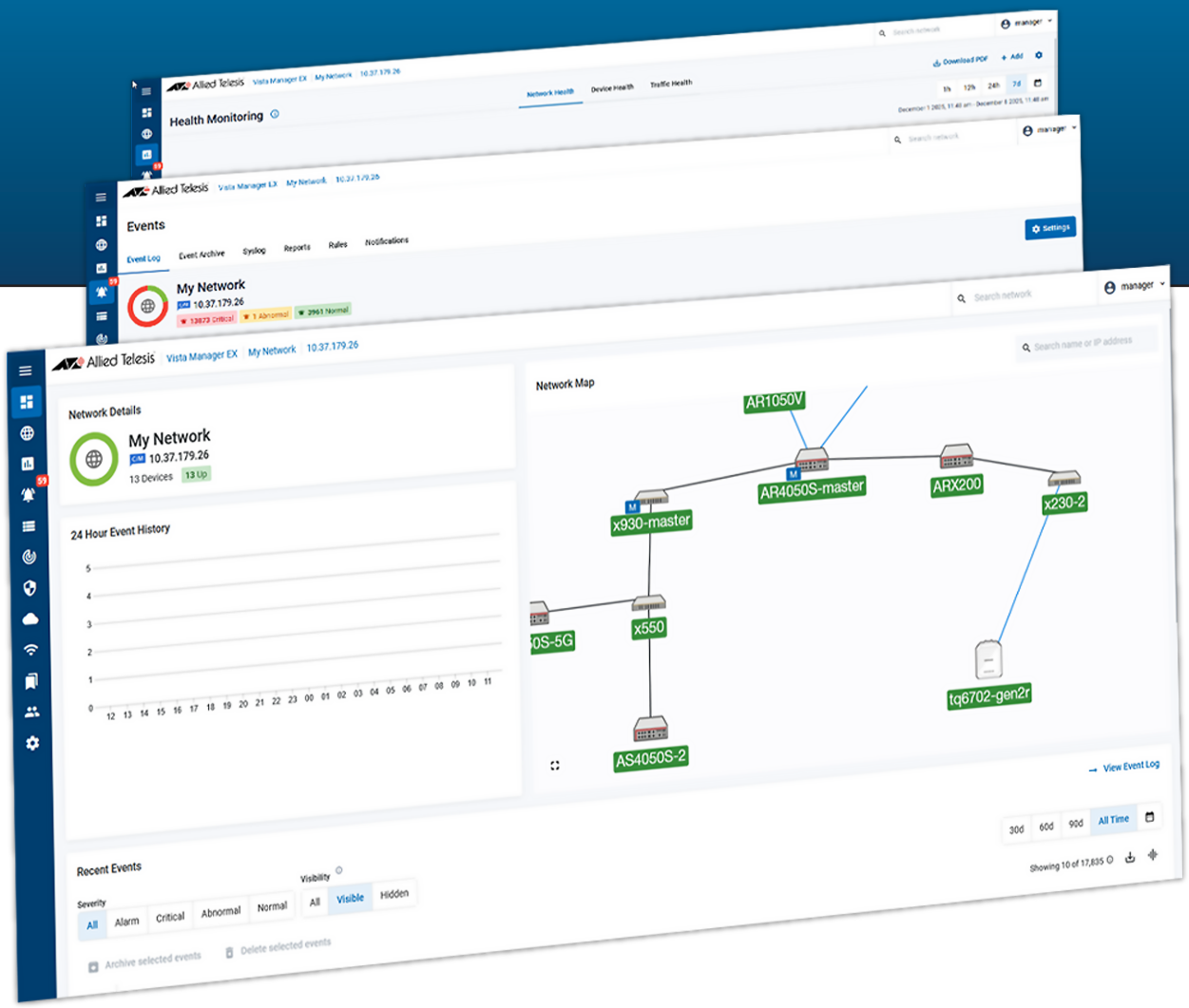
Release Notes



Vista Manager EX Version 3.17.x

3.17.1

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 v3.17.1

Introduction

This release note describes the new features in Vista Manager EX™ v3.17.1. It covers changes to Vista Manager EX plus the optional Autonomous Wave Controller (AWC) plugin.

Further information is included for other supported plugins, and AMF Plus supported menu items, highlighted with a badge in the Vista Manager EX UI.

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 3.17.1.

It includes:

AI Network Assistant

From version 3.17.1 onwards, you can obtain a license for the AI Network Assistant to enhance your Vista Manager experience.

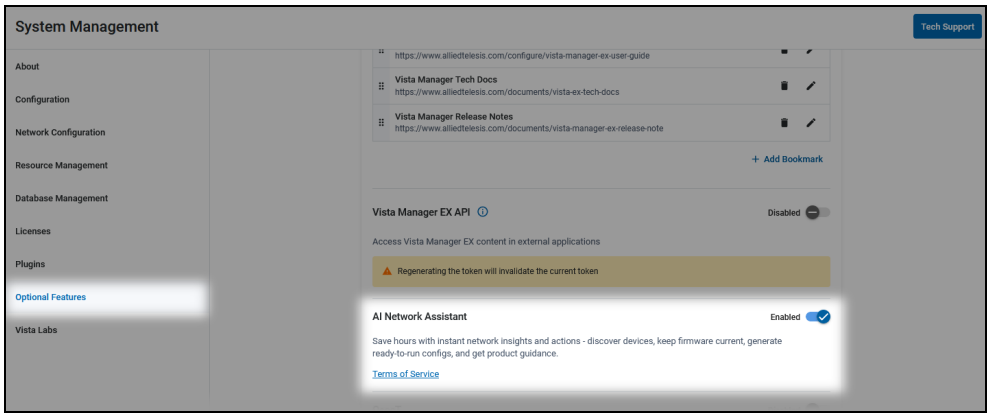
You can trial the Advanced AI license-exclusive features as part of the Vista Manager 90 day trial. Enable the AI Network Assistant feature from the **Optional Features** page, toggling to **Enable**, and agreeing to the terms of service.

The AI Network Assistant is a conversational interface within Vista Manager that helps users manage their network more easily. It can assist with checking network information, providing guidance on configuration and features, answering questions about Allied Telesis products, summarizing recent network events, and supporting selected AI-assisted workflows.

Available Features

- **Network Visibility** - Check firmware-manageable devices and network information using natural language.
- **Event Summarzation** - Summarize recent network events to help identify issues more quickly. (Advanced AI License required).
- **Firmware Upgrades** - Assist with checking firmware files and upgrading devices.
  (Advanced AI License required).
- **Configuration Guidance** - Get step-by-step configuration guidance and ready-to-run commands for your devices.
- **Product Information** - Ask questions about Allied Telesis products and features.
- **Networking Knowledge** - Get explanations of networking concepts in natural language.

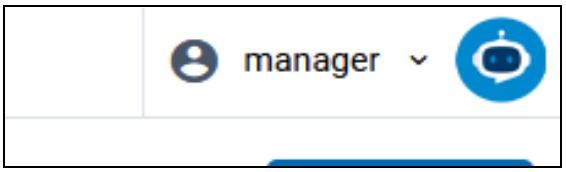
Note: Some responses may include source links to relevant documents. Use these links to review the referenced material or confirm the answer in more detail.



How to enable the AI Network Assistant

You can enable the AI Network Assistant from **System Management** > **Optional Features**.

- When you first see the widget, the Enable/Disable toggle will be greyed out.
- To enable the AI assistant, you must first read the Terms of Service under the widget before you can Enable the feature. Once accepted, you can enable the feature.
- After you enable the AI assistant, click the new icon in the top right corner to start a chat.



When upgrading from a version prior to 3.17.1, you need to agree to the updated terms of service.

License Details

You can chat with the AI Network Assistant without a license. However, some advanced features require an Advanced AI License. These include:

- Event Summarization
- Firmware Upgrades

These licensed features extend the AI Network Assistant with additional workflow support for reviewing recent event activity and performing firmware upgrade tasks.

To obtain an Advanced AI License, contact your Allied Telesis support representative.

Event Summarisation

From version 3.17.1 onwards, with an Advanced AI License, you can use the AI Network Assistant to help you review and summarize network events.

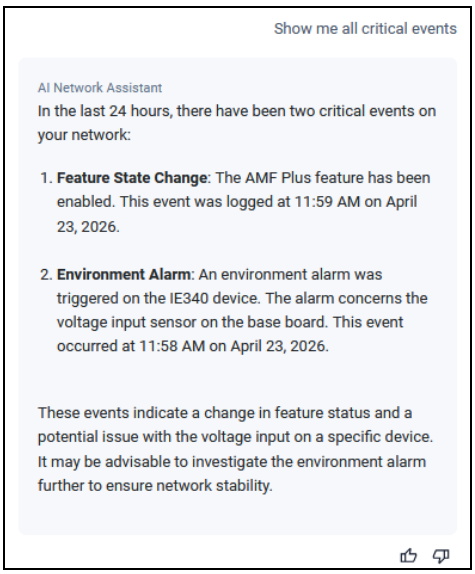
Enter natural language prompts to quickly retrieve event data based on time, severity, location, or specific criteria.

The AI Network Assistant analyzes event logs and returns concise results, allowing you to identify issues quickly without manually reviewing logs.

The AI Network Assistant supports filtering by node name, AMF area, severity, and free-text terms, allowing you to refine results directly in the chat.

It also recognizes both grouped severity terms (such as alarm, critical, abnormal, and normal) and explicit severity levels (such as warning, error, and notice) when applying filters.

For example, you can use the assistant to check information about critical events over a 24 hour period. It provides a summary list of detected events along with their time of occurrence, helping you quickly identify recent issues.



- The AI Network Assistant converts timestamps into a readable format using your local time zone.
- The AI Network Assistant will not rewrite any events, and event retrieval is read-only. The assistant reports event information without modifying or otherwise changing events.
- The AI Network Assistant filters archived events based on your request. The Assistant excludes them by default, includes them when specified, or returns only archived events when requested.
- The AI Network Assistant filters archived and hidden events by default. It includes them when specified, or can be used to only include archived or hidden events.
- The AI Network Assistant limits each query to a maximum of 100 returned events and notifies you when additional matching events are available beyond this limit.
- Results are restricted by the permissions of the user account.

Example prompts

Use these example prompts as a guide to create your own queries and generate summaries that match your operational needs.

Example prompts include:

- "What should I know about my network activity from the last 24 hours?"
- "Show me all critical events from the last 2 hours."
- "What events happened in AMF area "Tokyo-South" between midnight March 23rd 2026 and midnight March 24th 2026?"
- "Find warning or error events for node x930-core-1 in the last 24 hours."
- "Search event logs from 8am March 23rd 2026 to midday March 23rd 2026 for the text 'authentication failed'."

Upgrading Firmware

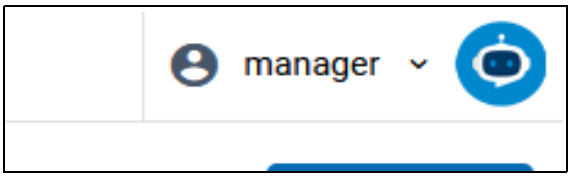
From version 3.17.1 onwards, you can ask the assistant to check current firmware files and distribute firmware files to devices on your network from the AMF Master device. This helps simplify firmware upgrade workflows while keeping you in control of the process. The assistant helps reduce the effort involved in planning and initiating upgrades, while confirmation steps allow you to verify the changes before being applied.

Sample prompts include:

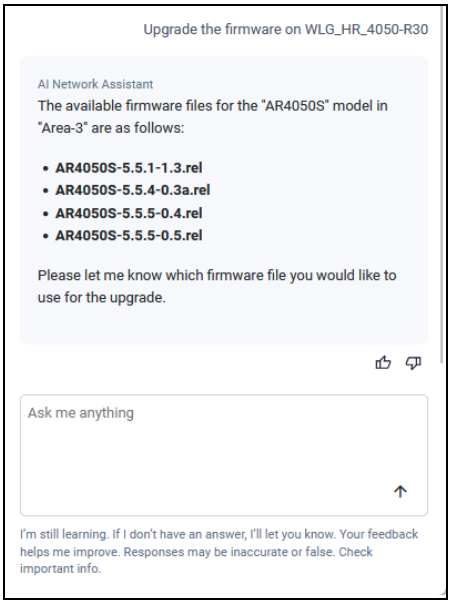
- "Upgrade the firmware on <device>"
- "Upgrade the firmware on <device> to <firmware_version>"

To upgrade firmware:

1. Upload firmware files to your AMF master device.
   This feature requires the firmware files are on the AMF Master device for the area you're looking to upgrade devices in.
2. Click on the AI Network Assistant icon from the top right of the screen.



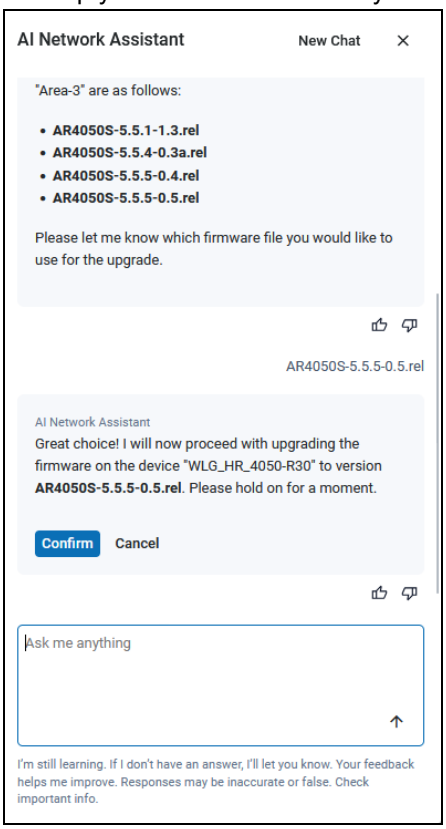
3. Ask the assistant to upgrade firmware on the network from the AMF master device.



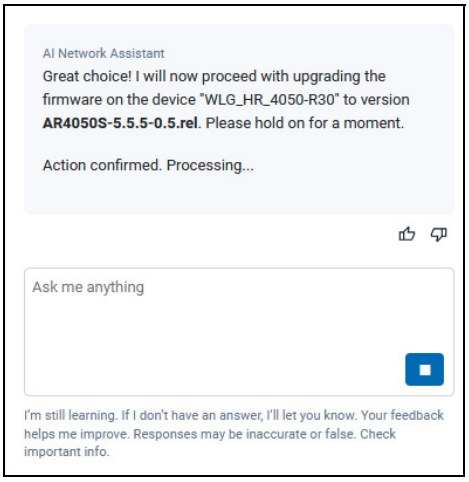
4. Review the files identified by the assistant and confirm that they are correct before proceeding.

5. If there are multiple files detected, select the file you would like to use.

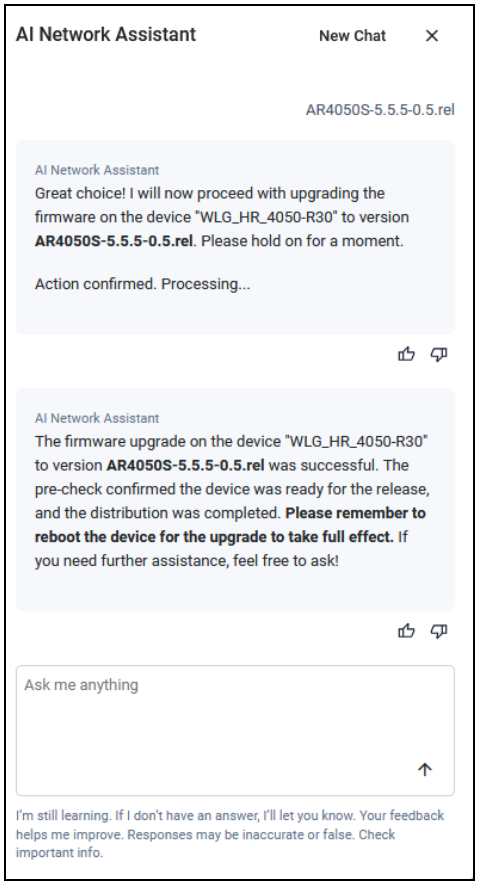
6. Reply with the firmware file you'd like to upgrade to.



7. Click **Confirm** to proceed with the upgrade.



8. The assistant confirms when the task has been completed.



9. **Reboot** the device outside of the AI Network Assistant from the CLI or Device GUI.

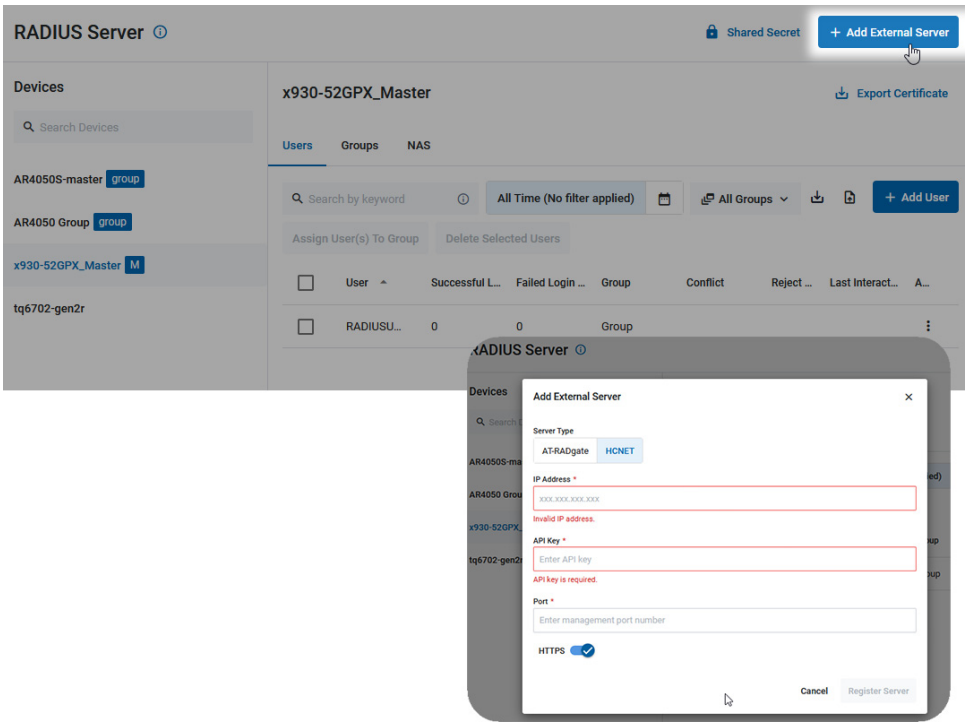
HCNET Account@Adapter integration support

From version 3.17.1 onwards, Vista Manager EX can integrate with HCNET servers to manage RADIUS authentication for network devices.

To enable HCNET external RADIUS support:

1. Go to **Optional Features** and toggle to enable HCNET.
    - Once enabled, the selectable Server Type 'HCNET' will appear in the Server List on the **RADIUS** page, and the Network Map page when you add it as an External Server.
2. Go to the **Network Services** > **RADIUS** page and click **+ Add External Server**.
3. Add a custom server entry for HCNET by clicking the HCNET tab and entering the credentials from your HCNET Account@Adapter instance.

Note that you cannot enable or disable the external RADIUS server from the Network map.



Using HCNET

- As an Admin user, you can enter the HCNET IP address, API key, and management port number.
- You can view, add, edit, or delete RADIUS users from HCNET from the RADIUS feature page.
- You can block or allow endpoints from the Endpoints table.
- If you delete the RADIUS server from Vista Manager, the external server will still function, but it will no longer communicate with Vista Manager unless re-added.
- Vista Manager synchronizes with the HCNET server every 5 minutes.
- You can include HCNET as a member in a Vista Manager RADIUS Server group. Note that Vista Manager's RADIUS NAS or Group functions are not supported by HCNET.

New events added for this integration are as follows:

Severity	Title	Message
NOTICE	Optional Feature Enabled	Successfully Enabled HCNET
NOTICE	Optional Feature Disabled	Successfully Disabled HCNET
INFORMATION	HCNET Server Deleted	Successfully deleted the HCNET server: {ip}
INFORMATION	HCNET Server Added	Successfully added the HCNET server: {ip}

Requirements

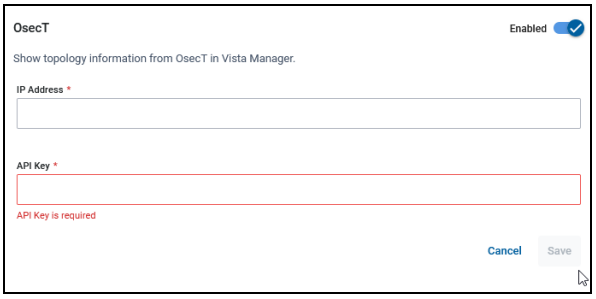
- Vista Manager is compatible with HCNET servers running Account@Adapter ver. 7.02.00 or later. This feature requires a NAS device and a RADIUS server.
- A shared secret must be configured on the NAS device. This secret is used to authenticate communication between the NAS and the RADIUS server.
- The NAS should be provisioned and managed by the HCNET server to ensure consistent RADIUS and MAC authentication behavior.
- When PAP or CHAP is enabled for MAC authentication, the HCNET server RADIUS settings must be configured to ignore the MAC address delimiter.
    - This is because Alliedware Plus NAS devices use the delimited MAC address format (e.g. xx-xx-xx-xx-xx-xx) as both the username and the password during authentication, while HCNET stores MAC-auth terminal accounts without delimiters. Without ignoring the delimiter, the RADIUS server would not be able to match incoming authentication requests to existing users.
- To ensure successful authentication with NAS devices that send the MAC address with delimiters as the password, Vista Manager explicitly configures the optional password of MAC-auth terminal accounts to the delimited MAC address using the optional API parameters.

OsecT plugin support for Vista Manager

From version 3.17.1 onwards, OsecT is supported with Vista Manager as a plugin.

OsecT is an Operational Technology (OT) intrusion detection system that monitors and protects industrial control systems and OT networks, helping identify potential threats while ensuring normal operations are not disrupted.

Vista Manager supports connecting to OsecT through an IPv4 address or a hostname. As an admin user, you can enable OsecT from the **Optional Features** page.

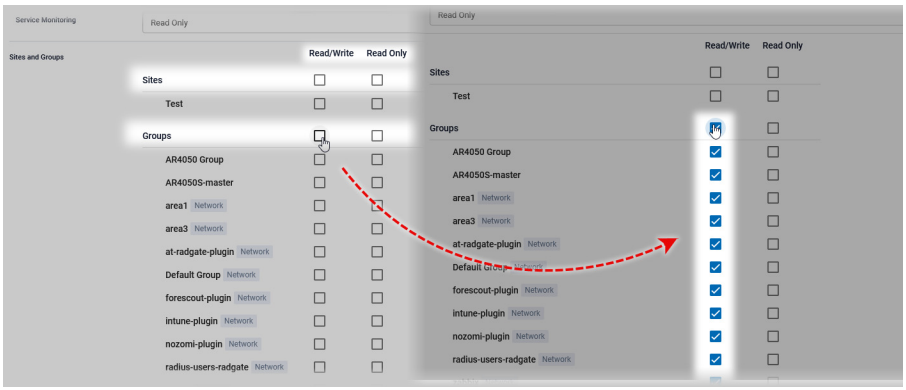


- Vista Manager 3.17.1 is compatible with OsecT version 4.2.0 or later.
- When OsecT is enabled, devices will start appearing in Vista Manager shortly after. Vista Manager requests updates from OsecT every hour.
- OsecT-discovered devices do not report whether they are online or offline, so these devices will always have a "Normal" status in Vista Manager.
- If OsecT is disabled, devices will be removed from Vista Manager.
- However, if you enable offline device recording, a record of these removed devices will still remain in the Offline Devices tab of the Asset Management page

Ability to select all Sites and Groups

From version 3.17.1 onwards, you can select all permissions for sites and groups when managing user accounts from the **User Management** page.

To add read/write or read-only permissions for a user, click the **Select All** checkbox above the permission type from the specified user's predefined settings from the **User Management** page.



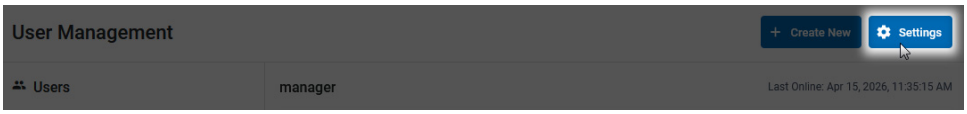
This enables you to immediately assign permissions for all sites and groups on your network, regardless of size.

RADIUS Login for Vista Manager

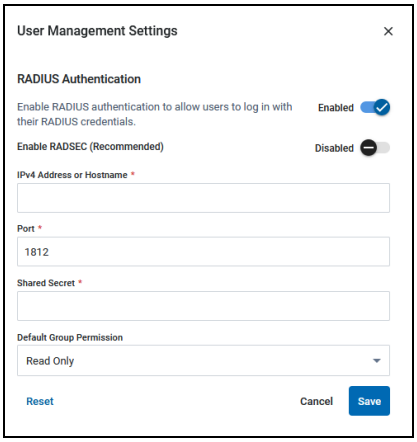
From version 3.17.1 onwards, as an admin user, Vista Manager supports external user authentication through a RADIUS server. This allows users to log in without local Vista Manager accounts.

To enable RADIUS login:

1. Go to **User Management**.
2. Click on the **Settings** button to open the User Management Settings.



3. Toggle RADIUS Authentication to enable RADIUS login.



Requirements

- At least one local admin account in Vista Manager is required.
- You cannot remove the last local admin account.
- RADIUS authentication is only available after initial configuration is complete.
- After a RADIUS user logs in to Vista Manager for the first time, that user account appears in User Management.

Email address behavior

- If a RADIUS user has no email address, they are redirected to User Management after login and prompted to enter one.
- If an email notification rule includes a user with no email address, Vista Manager shows a warning.

Permission assignment

When enabling RADIUS users to login, you can also set a default permission level for users that do not have Filter-Id values assigned to their account. Vista Manager reads the Filter-Id value returned by the RADIUS server and applies permissions automatically.

Vista Manager recognizes the following filter-id values:

```
vista-admin
vista-readonly
vista-readwrite
vista-none
```

If no filter-id is provided, Vista Manager applies the configured default permission.

In Vista Manager, you can specify a default permission from the following:

- Read-only
- Read-write
- None

If you select none, an admin will need to manually set their permission through the User Management page.

Important limitations

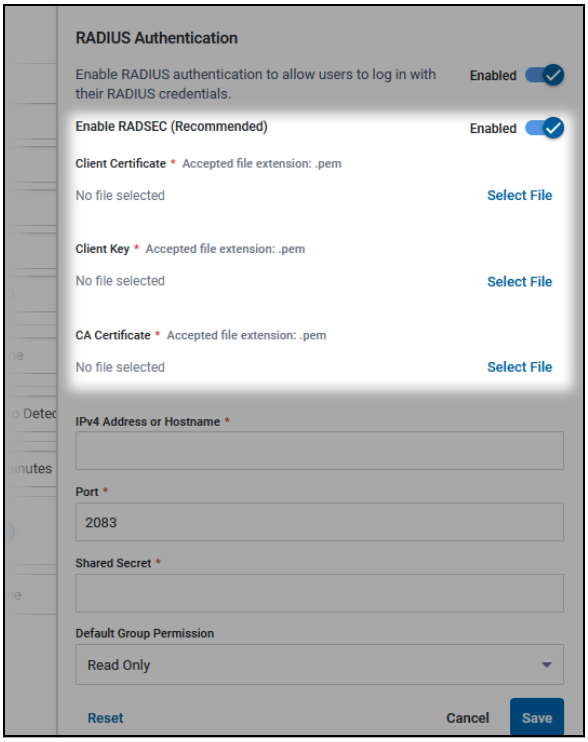
- If a RADIUS username matches an existing local Vista Manager username, the RADIUS user cannot log in.
- RADIUS user permissions are evaluated at each login. Permission changes should be made on the RADIUS server, not locally in Vista Manager.
- Password changes and resets for RADIUS users must be done on the RADIUS server.
- If Vista Manager cannot reach the RADIUS server, RADIUS users cannot log in until connectivity is restored.
    - RADIUS users who are already logged in are not affected until they log out.

RADSEC

Enabling RADSEC (RADIUS over TLS) is strongly recommended.

For RADSEC, you need to provide three certificates:

- Client certificate (.pem)
- Client private key (.pem)
- CA certificate (.pem)



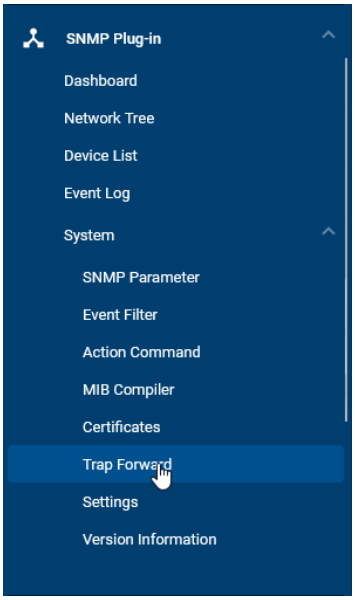
Certificate Usage

- The **Client Certificate** identifies Vista Manager to the RADIUS server.
- The **Client Private Key** proves ownership of the client certificate.
- The **CA Certificate** validates the RADIUS server certificate during TLS setup.

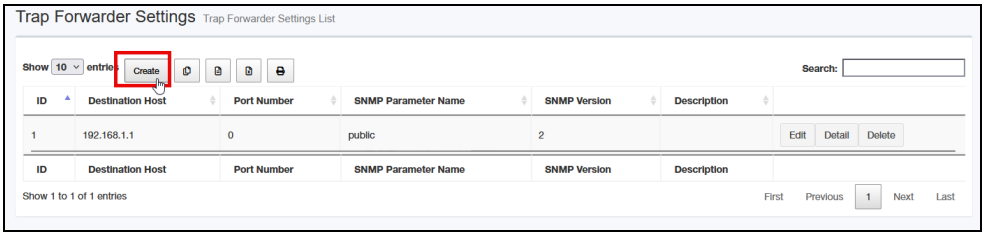
SNMP Trap Relay

From version 3.17.1 onwards, you can use the Trap Forwarding feature in SNMP Plugin version 2.15.0. This means you can send SNMP traps from 3rd-party devices, and forward them through to other hosts with the SNMP Plugin.

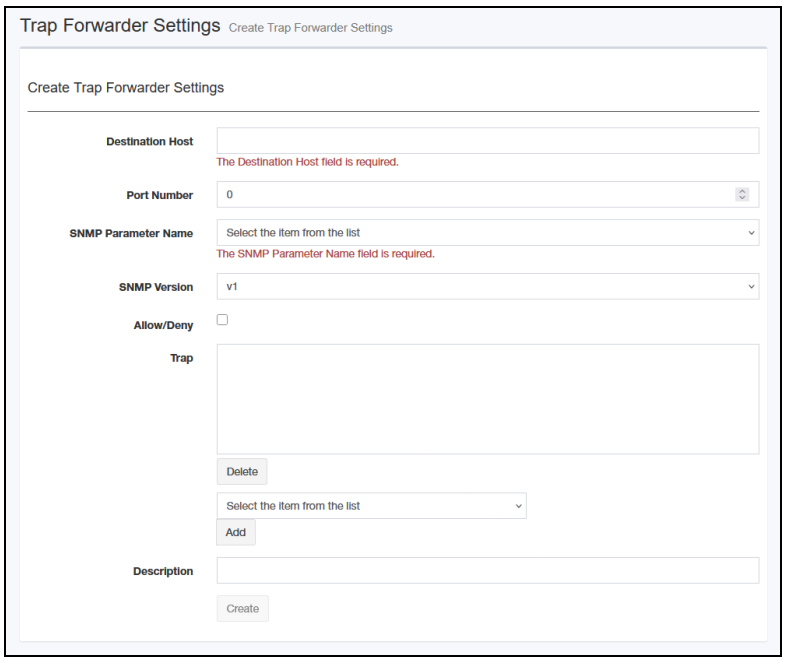
Navigate to **SNMP Plug-in > System > Trap Forward** to use this feature.



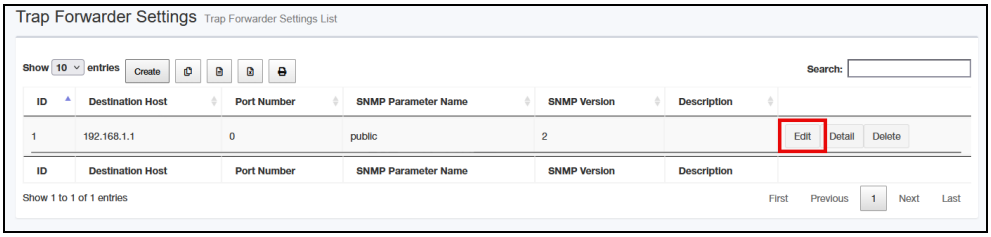
Click **Create** to create a new entry in the trap forwarding table.



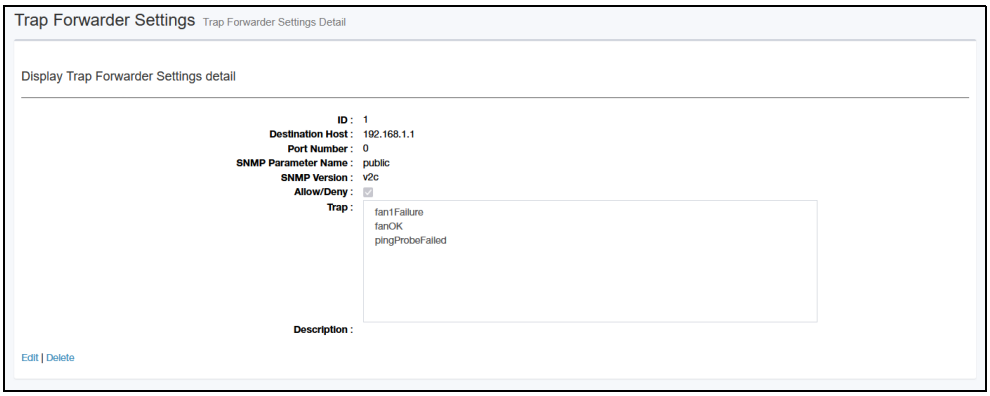
- The destination port is optional. If the port value is set to 0 or left unspecified, the trap forwarder uses UDP port 162. It is 0 by default.
- Parameter Name specifies the SNMP parameter name (public, private, or netman).
  - Additionally, users can add or delete SNMP parameters on the SNMP Parameter page.
- The trap list is optional, and you can select from a list of specific traps. When the list is empty, the trap forwarder forwards all traps.
- The **allow/deny** checkbox relates to the SNMP Trap Receive List on the System Settings page.
  - Allow mode forwards only the traps explicitly listed (whitelist behavior).
  - Deny mode forwards all traps except those listed (blacklist behavior).



Click **Edit** to edit any existing trap forwarder entry you wish to update.



Click **Detail** to see information about a specific trap forwarder entry.



Ability to check speed of AMF guest links

From version 3.17.1 onwards, when selecting an AMF Guest Link on the Network map's Traffic map, you can see the link speed on the left side panel from the **amf-guest-link** tab.

When selecting an AMF Guest Link on the Network >Traffic map, the link thickness indicates the speed. You can find the link capacity scale by clicking the info icon near the bottom left of the Network map.

Device details update when details page is loaded

From version 3.17.1 onwards, node system details, including CPU, RAM, and flash storage are updated from the device when its detail page is loaded.

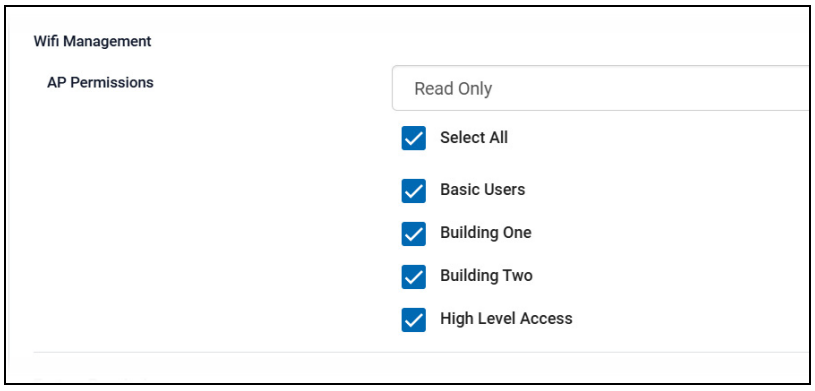
Any changed information is refreshed from the device when the page is loaded, and if the device cannot be reached a warning icon is shown.

To get the latest information, reload the device's detail page.

AWC enhancements

Select all settings for AP Permissions for Wifi Management

From version 3.17.1 onwards, you can quickly select all settings under the Wifi Management > AP Permissions section of the System Settings page



Apply configuration to Wireless APs Manually or Automatically

From version 3.17.1 onwards, you have control over when AWC plugin settings get applied after restoring a backup file.

By default, when a backup file is restored, the AWC plugin immediately applies settings to the wireless APs managed by the plugin. Applying these settings disrupts wireless communication on the APs for a few minutes.

Instead of this immediate Auto application, you can now schedule the application.

To change from Auto to Manual prior to updating, go to AWC Plugin > **System Setting** section. Scroll down to Options for Applying Configuration to Wireless AP > Apply Configurations on Wireless AP Join.

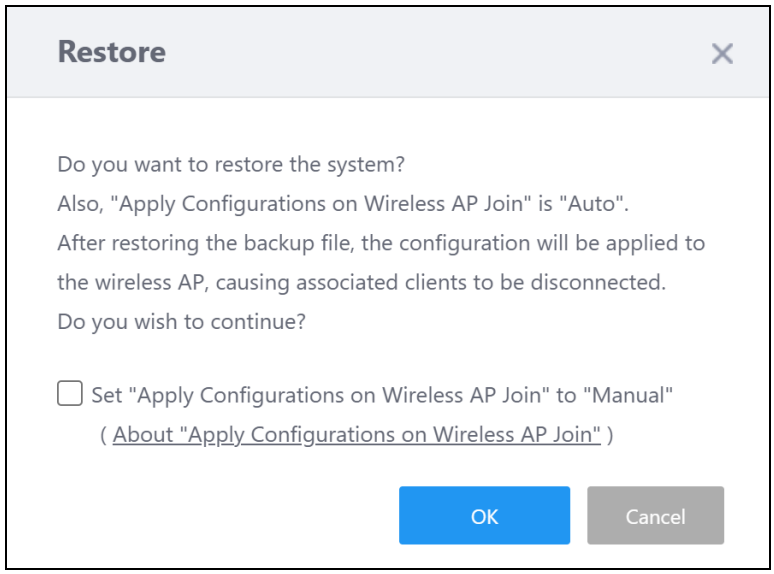
When you restore a configuration file, you can also choose to **not** automatically apply the settings to wireless APs after restoring.

By default, when you click Restore the pop-up will ask if you wish to set it to manual.

Apply Configurations on Wireless AP Join set to Auto

When you click Restore, the dialog will give you the option to switch to Manual.

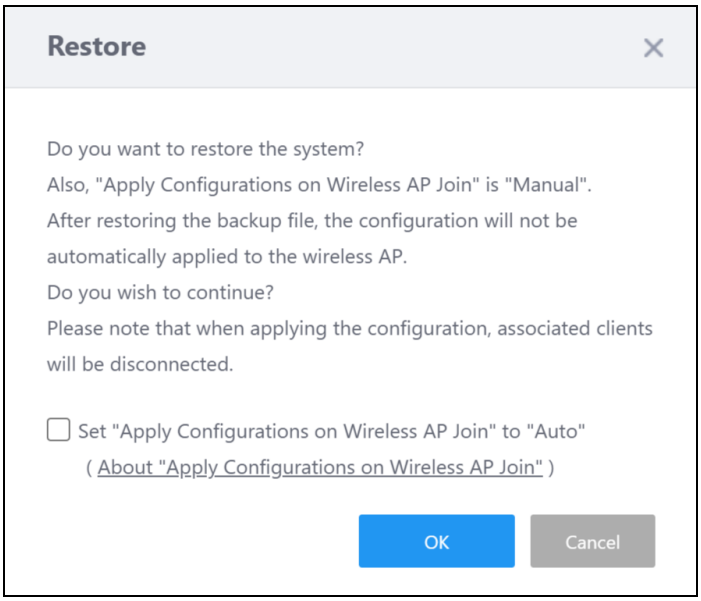
- Click the checkbox to set the configuration application to manual if you wish to not automatically apply these settings.
- Otherwise click OK without checking the checkbox and resume the restoration resume the restoration, which will stop wireless communication.



Apply Configurations on Wireless AP Join set to Manual

If you have already set the Apply Configurations on Wireless AP Join to Manual, then the checkbox will let you enable the Auto Wireless communication feature as per default.

- This will disrupt AP communication, so if you do not want to re-enable this then ignore the checkbox.



After the restore, the AP's management status will become 'Monitoring' and the settings will not be applied to the APs.

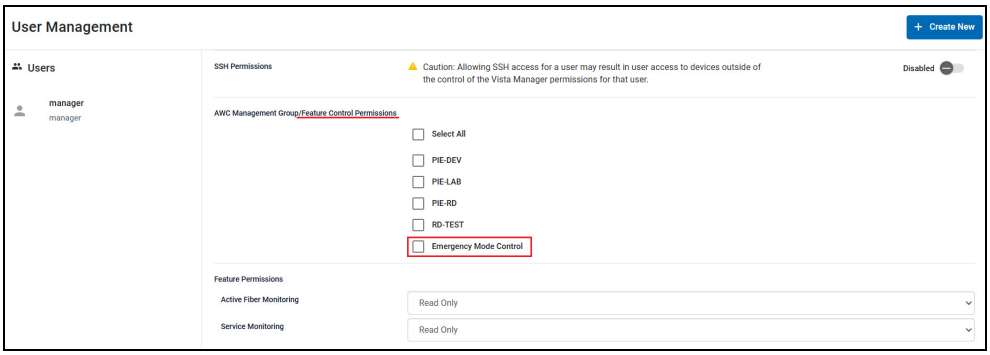
Please apply these settings manually, or schedule them using the AWC plugin's Schedule function from the **Wireless Maintenance > Task Scheduling** section of the AWC Plugin.

Emergency Mode Control added to AWC Management Group/Feature Control Permissions

From version 3.17.1 onwards, you can enable Emergency Mode Control permissions for Management Groups on a per-user basis. It is disabled by default.

To enable Emergency Mode Control for a user:

1. From the **User Management** page, select the user you wish to modify.
2. Scroll down to the **AWC Permissions Setting** and click the checkbox of **Emergency Mode Control**.

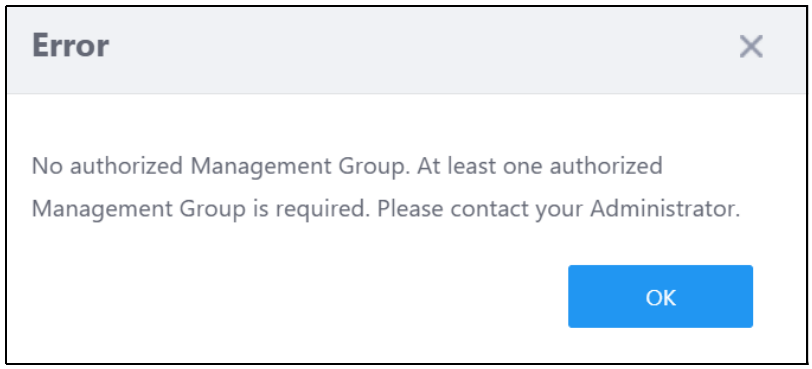


With the Emergency Mode Control permission enabled, you can turn Emergency Mode On or Off for each Management Group from the Emergency Mode page.

Emergency Mode

If you try to click Apply with no Management Group permissions assigned, an error screen will appear. You need to have at least one authorized Management Group permission assigned to use this feature.

To create a management group, go to **Wireless Configuration** > **Management Group** from the AWC Plug-in menu, and click **Create** on the top right of the Management Group page.

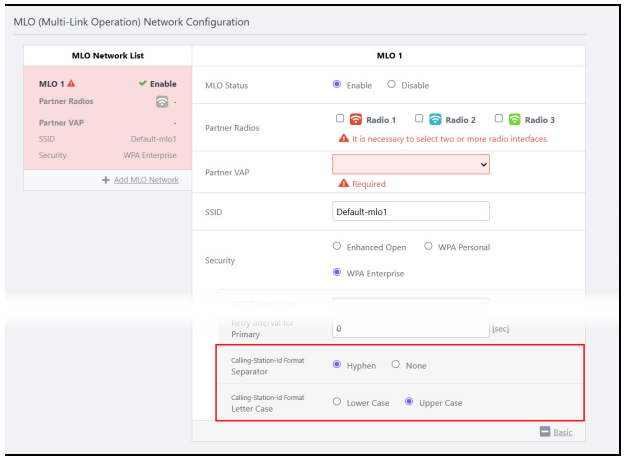


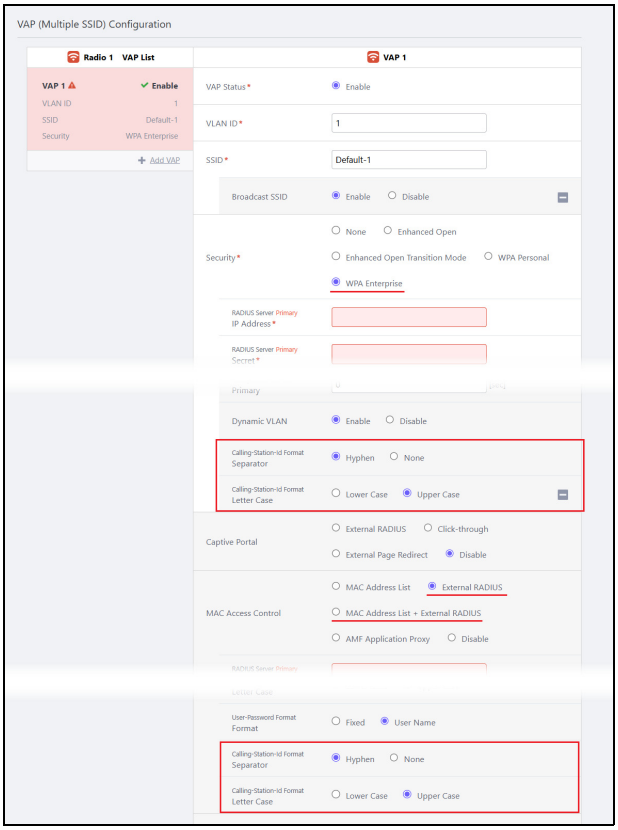
Ability to customize the Calling Station ID

From version 3.17.1 onwards, you have the ability to customize the Calling Station ID sent by an AP during RADIUS authentication.

To enable this:

1. Go to the AWC Plug-in > AP Profile Page.
2. Create an AP Profile.
3. Select one of the following combinations and change the Calling-Station-Id Format value:
   - MLO Network Configuration > Security > WPA Enterprise
   - VAP Configuration > Security > WPA Enterprise
   - VAP Configuration > MAC Access Control > (MAC Address +) External RADIUS





Edit AP Mode and Monitoring Mode

From version 3.17.1 onwards, you can use Edit AP Mode to enable or disable AP Monitoring mode from the floor map. This may be useful if you would like to collect client location estimation results.

This feature enables RSSI information to be collected when you enable Monitoring Mode.

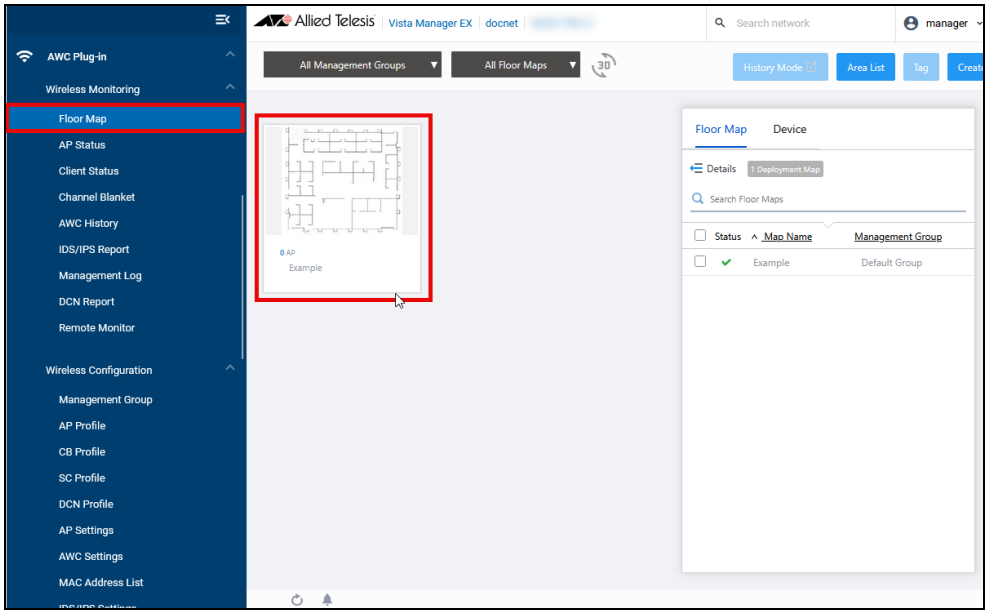
Monitoring Mode is only supported for TQ6702 GEN2-R Wireless AP Routers. Other TQR Series devices will be supported in future updates.

When APs operate in Monitoring Mode, they do not transmit beacons and only detect wireless clients.

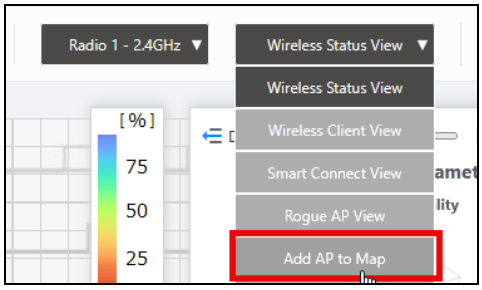
AWC receives this RSSI information and uses it to estimate wireless client locations.

To enable Monitoring Mode:

1. Add APs to the floormap by going to **Floor Map**, clicking on a floormap.

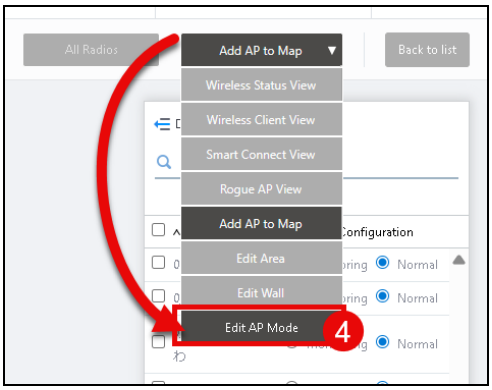


2. Switch to the **Add AP to Map** mode.



3. Click and drag the APs on the side menu and arrange them on the floormap.

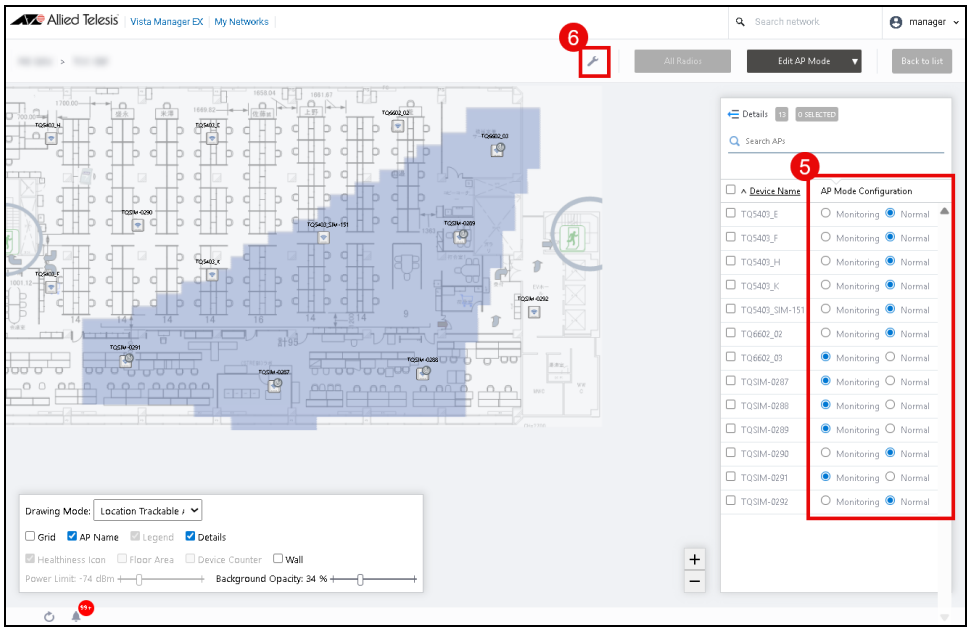
4. Switch the Floormap mode to **Edit AP Mode**.



5. Enable Monitoring on an AP by **clicking the radio button** in the side menu.

6. Click the Spanner icon and click **Apply Configuration**.

7. Click **Apply** to confirm the APs this will apply to.



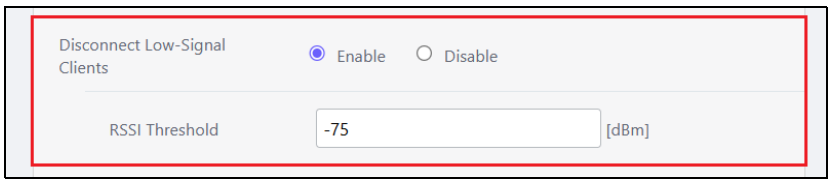
Disconnect Low Signal Clients and set RSSI threshold

From version 3.17.1 onwards, you can enable the ability to disconnect low signal clients from the **AP Profile** > **VAP Configuration** section of an AP Profile.

Disconnect Low Signal Clients is disabled by default.

Enabling Disconnect Low Signal Clients enables the RSSI Threshold where you can select the range in which a client is detected as having a low signal.

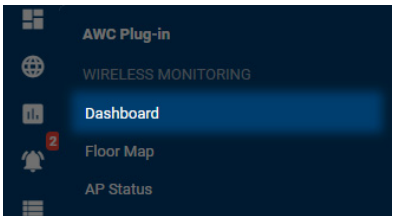
- The default for RSSI Threshold is -75dBm.
- You can select a range between -90dBm to 0dBm.
- Note that you cannot enable Band Steering at the same time as you have Disconnect Low Signal Clients enabled.



Wireless Monitoring Dashboard

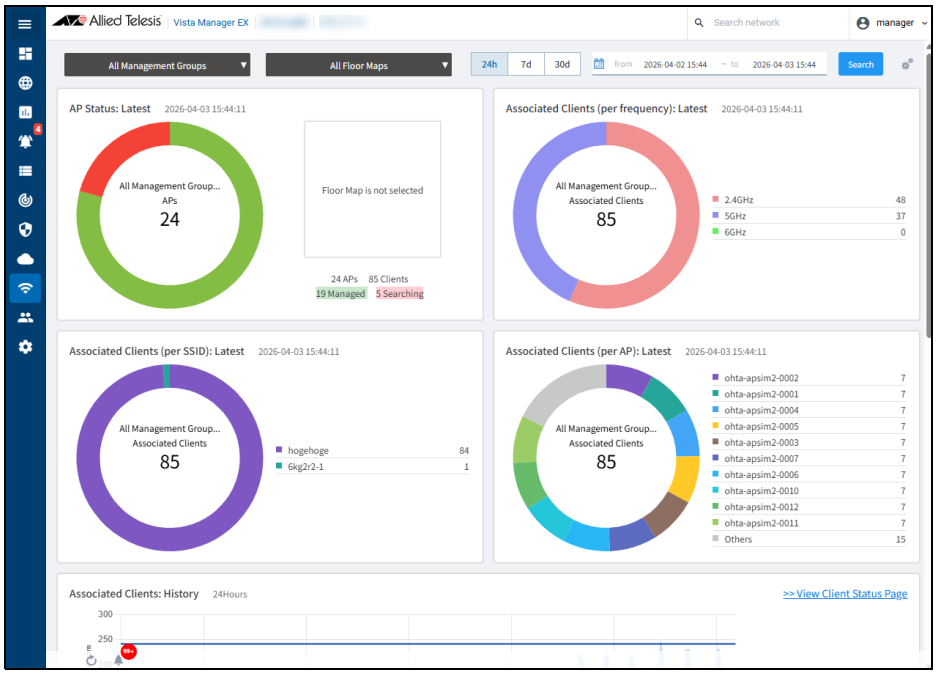
From version 3.17.1 onwards, you can access the Wireless Monitoring Dashboard to see summarized information of the Wireless APs and client devices in your network.

Click on the **Dashboard** menu item from the AWC Plug-in menu to access the Dashboard.

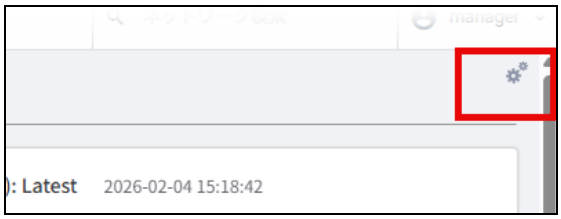


The AWC Wireless Monitoring Dashboard has customizable widgets including:

- AP Status donut charts
- Floor Map status charts
- Associated Client History charts
- Recent AP alert log history



By clicking the **cog icon** in the top right, you will be redirected to the **Dashboard Settings** section of the AWC Plugin's System Settings page.



You can manually choose to change charts displayed on the dashboard to monitor your network organized per SSID, per frequency, or per AP.

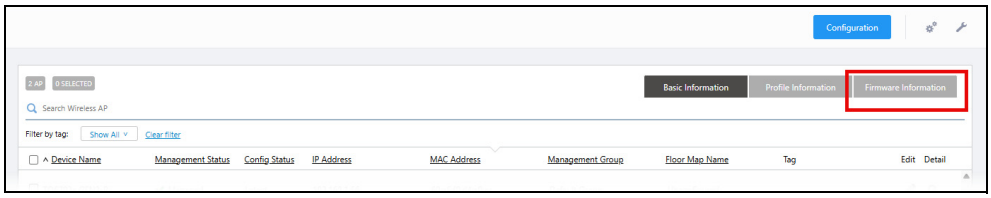
Vista Manager automatically updates the charts based on the AWC Dashboard refresh rates. You can change this from the User Management page.

- Note that the charts on the Client Status page have moved to the Dashboard page as part of this change.
- Loading times of widgets will vary with your network environment's hardware specifications.

AWC Usability Improvements for 3.17.1

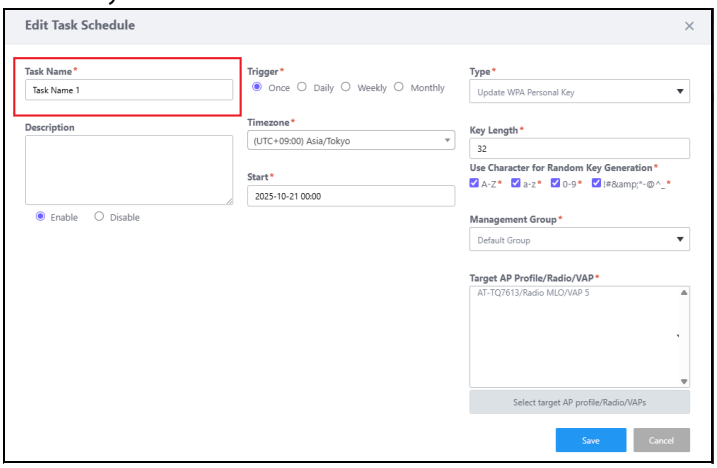
From version 3.17.1 onwards, the following improvements have been added:

- You can check an AP's firmware version from **AP Settings** > **Firmware information** tab.



  - The tab structure has changed and Additional Information has been removed.
  - Tab structure is now:
    Basic Information > Profile Information > Firmware Information.

- Ability to edit a scheduled task's name from the **Task Scheduling** page.



- Ability to switch the floor heatmap gradient colors from the **System** > **Floor Map Setting** section.

- On the **Wireless AP Status Detail** page, the bytes per second unit of the Statistics graph has changed from "byte/s" to "bps".

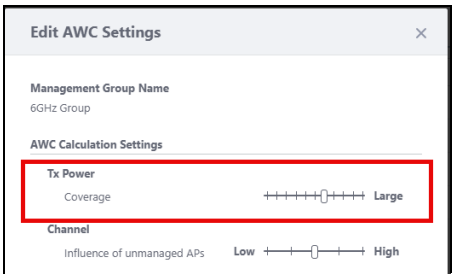
- Ability to click/tap and drag to select and copy logs on the **Log page**.
- **Details column** added to the Log Management page that redirects to the **Wireless AP Status Detail** page.
- Option to display 100 items per page on pages with table lists by clicking on the **100 maximum** on the bottom left of the screen.

Transmit Power Output Slider Adjustments

From version 3.17.1 onwards, by moving the slider from the center toward the right, you can obtain calculation results that provide wider coverage.

Use the slider on the **AWC System Settings > AWC Coverage Settings** page to change the Power Coverage value.

In versions earlier than 3.16.0 of the AWC Plugin, the coverage achieved when the slider was set to the rightmost position is equivalent to the center position of the slider in the current version.



Updating passwords for AMF Plus devices

This section applies to customers using passwords across their AMF Plus and Vista Manager network.

If you update your AMF device passwords, you must follow this procedure to ensure Vista Manager can still access the AMF devices after the update.

In summary, this procedure has five steps:

1. Create a temporary account, e.g. 'vista-temp'
2. Switch Vista Manager's credentials to use the new account
3. Change the password on the 'main' account
4. Switch Vista Manager back to the 'main' account.
5. Delete the temporary account.

The rest of this section describes this procedure in detail.

Step 1: Create the temporary account

First you must create a new user on the AMF Master and Member nodes. To do this:

1. Open a terminal session on the AMF Master node.
2. Enter the global configuration mode on the AMF Master:

```
awplus# configure terminal
```

3. Use the **atmf working-set group all** command to target all nodes in the group:

```
awplus(config)# atmf working-set group all
```

4. Enter the configuration mode for the working set:

```
AMF[all]# configure terminal
```

5. Create a new user named **'vista-temp'** with a specified password:

```
AMF[all](config)# username vista-temp password
your_password
```

6. Exit the configuration mode:

```
AMF[all](config)# exit
```

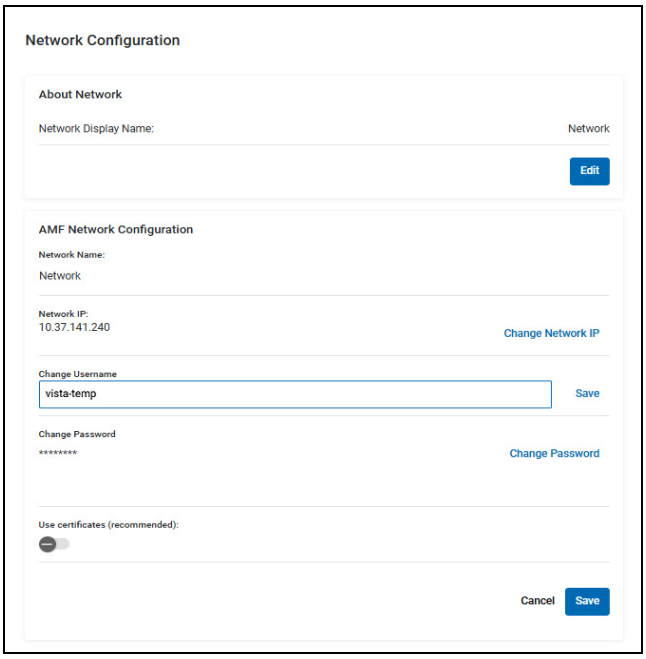
7. Save the configuration

```
AMF[all]# write
```

The above process creates the user 'vista-temp' on all nodes within the specified working set group. Make sure to replace your_password with a secure password of your choice.

Step 2: Switch Vista Manager's credentials to use the new account

1. Go to **System Management** > **Network Configuration** from the side menu in Vista Manager.
2. Add the previously created 'vista-temp' username and password:



3. Click **Save**.

Step 3: Change the password on the 'main' account

1. Open a terminal session on the AMF Master node.
2. Enter the global configuration mode on the AMF Master:

```
awplus# configure terminal
```

3. Use the **atmf working-set group all** command to target all nodes in the group:

```
awplus(config)# atmf working-set group all
```

4. Enter the configuration mode for the working set:

```
AMF[all]# configure terminal
```

5. Update the password for **'manager'**:

```
AMF[all](config)# username manager password new_password
```

6. Exit the configuration mode:

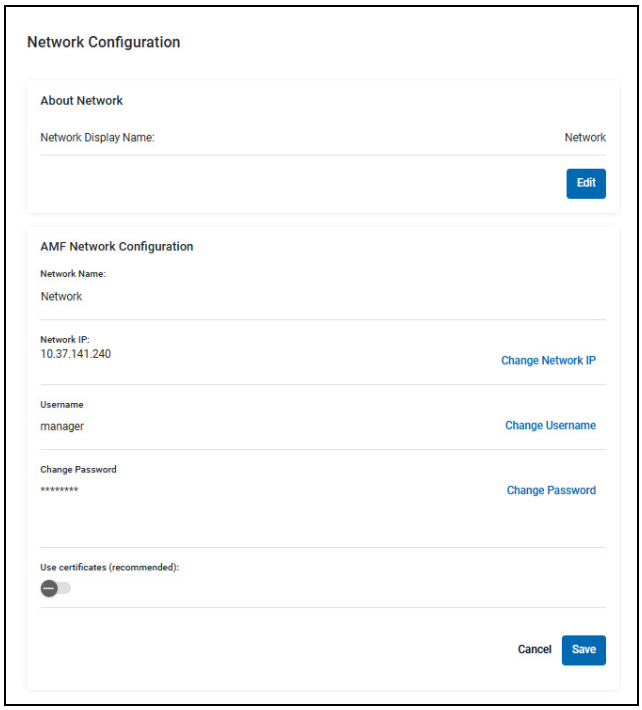
```
AMF[all](config)# exit
```

7. Save the configuration

```
AMF[all]# write
```

Step 4: Change Vista Manager back to the 'main' account.

1. Add the manager user details back to Vista Manager:



2. Click **Save**.

Step 5: Delete the temporary account.

1. Open a terminal session on the AMF Master node.
2. Enter the global configuration mode on the AMF Master:

```
awplus# configure terminal
```

3. Use the **atmf working-set group all** command to target all nodes in the group:

```
awplus(config)# atmf working-set group all
```

4. Enter the configuration mode for the working set:

```
AMF[all]# configure terminal
```

5. Delete the **'vista-temp'** user

```
AMF[all](config)# no username vista-temp
```

6. Exit the configuration mode:

```
AMF[all](config)# exit
```

7. Save the configuration

```
AMF[all]# write
```

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.

Disable http check-api-content-type-header before using Vista Manager

The **http check-api-content-type-header** command cannot be used on devices together with Vista Manager as this command will cause the device to drop some Vista Manager requests. It is disabled by default.

If you have enabled it, disable it using the **no http check-api-content-type-header** command. See your device's command reference for more information.

Manual polling recommended if upgrading

Applies to all Vista Manager EX installations

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:

Traffic map data not restored

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

Upgrading versions earlier than 3.9.0

If you create a backup on a version earlier than 3.9.0, and you want to upgrade to a new version, you must first install your backup on version 3.9.0 and export the backup again. Then you can upload the new backup to a later version of Vista Manager (such as v3.17.1).

If you upgrade directly to 3.17.1 instead (for example, from 3.7.0 to 3.17.1 without upgrading to 3.9.0 first), you may encounter data corruption or incompatibility issues.

Alternatively, you can choose to perform a fresh install of the newer version and configure it from new.

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.

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.

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 VST-VRT installation

This section describes how to upgrade the VST-VRT software and applications. It describes how to:

- "Back up application data" below
- "Upgrade the VST-VRT operating system and GUI on Hyper-V Server" below
- "Upgrade the VST-VRT operating system and GUI on VMware VSphere ESXi" on page 41
- "Upgrade Vista Manager, AMF Cloud, AMF Security, and RADgate applications" on page 43
- "Upgrade Wireless Controller (AWC) and SNMP (Full) plugin applications" on page 46

For information about migrating existing network data from the Windows installation to a new VST-VRT installation, see the Windows to VST-VRT Vista Manager Migration User Guide.

Back up application data

We recommend backing up application data for all applications regularly. You should also back up all the application data before following this upgrade procedure. See the relevant application's user manual for information on how to backup an application.

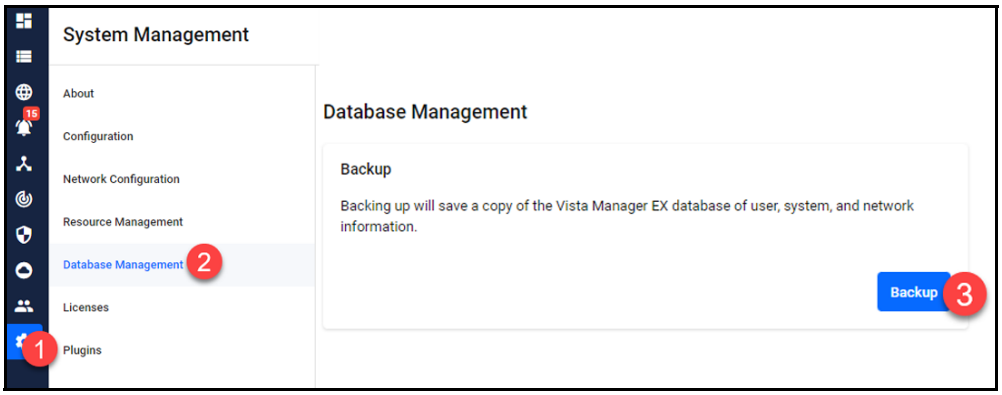
If you are using the ***Wireless Controller (AWC)*** or the ***SNMP (full)*** plugin applications, you must back up these applications before proceeding. This is because the process destroys and recreates the application instance. See "Upgrade Wireless Controller (AWC) and SNMP (Full) plugin applications" on page 46 for information on backing up these applications before you continue with the following section.

Backup system data for Vista Manager EX

1. Log into the Vista Manager EX app using an Admin account. You can open it either by clicking **Open** next to it on the VST-VRT Dashboard or by pointing your browser to its IP address.

2. In the Vista Manager EX GUI, navigate to the **System Management** menu item and then to the **Database Management** tab.

3. Click on the **Backup** button in the **Backup** pane.



4. Click **Backup** again to confirm you wish to make a backup.
   This automatically downloads a ***tar*** file backup to your default download location.
   Keep this ***tar*** file in a safe location.

Note: 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 3.17.1 into a Vista Manager 3.13.0 installation.

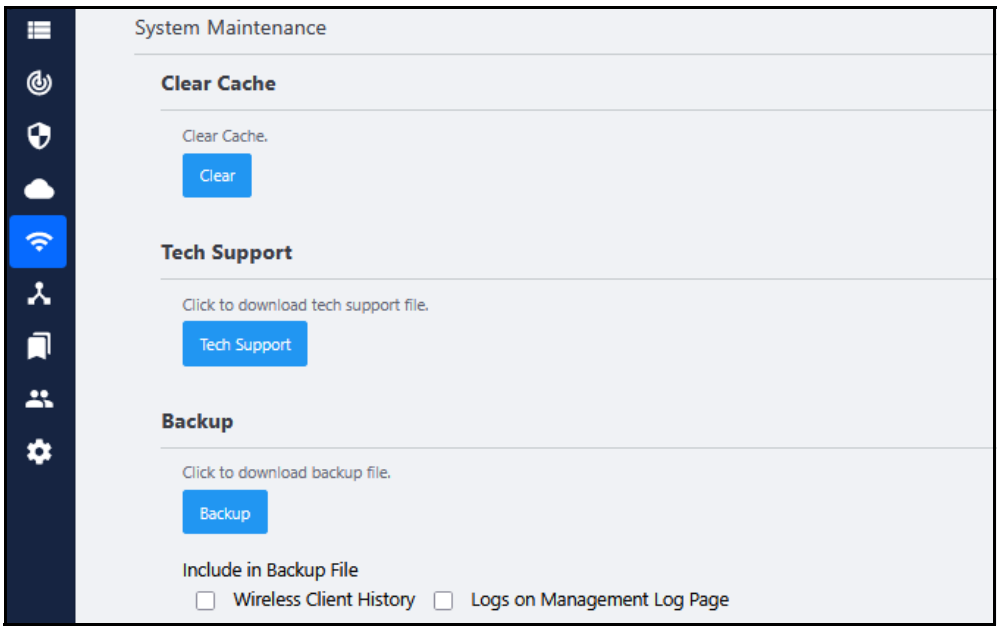
Back up system data for the Wireless Controller (AWC) plug-in application

Before upgrading the Wireless Controller application, you must back up its system data. This is because you have to destroy the application instance to upgrade it.

Note: Make sure that directories and filenames used for backup and restoration do not contain any multibyte characters.

1. Log into the Vista Manager EX app using an Admin account.

2. From the AWC plugin menu, select ***System Setting***. In the **System Information** page, scroll down to the **System Maintenance** section, and in that to the **Backup** section.



3. Optionally, check the **Wireless Client History** and **Logs on Management Log Page** boxes to back up these in addition to other data backup.

4. To start downloading the backup, click the **Backup** button.

5. From your web browser's dialog box, save the backup file to a safe location.

   The backup filename will be in the format:
   "config_atawc-X.X.X_-YYYYMMDDhhmmss.zip".

Back up system data for the SNMP plugin application

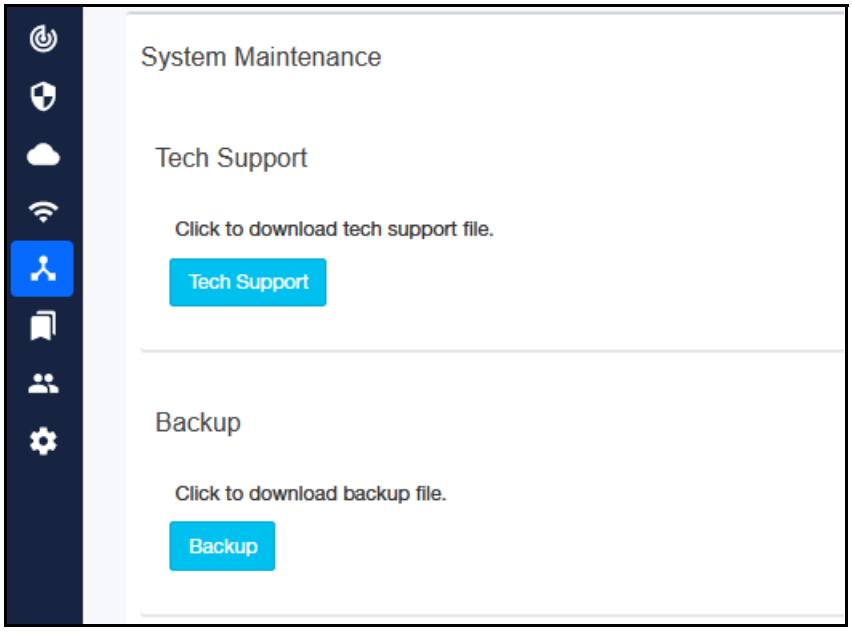
Before upgrading the SNMP Full application, you must back up its system data. This is because you have to destroy the application instance to upgrade it.

Note: Make sure that directories and filenames used for backup and restoration do not contain any multibyte characters.

1. Log in to Vista Manager EX using an Admin account.

2. Click the **SNMP plugin** icon in the left menu of the Vista Manager application, then click the **Version Information** in the menu.

3. In the System Settings panel, scroll down to the ***System Maintenance*** panel, and in that to the **Backup** section. Click the ***Backup*** button. This creates a backup of application data.



4. Save the backup file to a safe location.

Upgrade the VST-VRT operating system and GUI on Hyper-V Server

There are two different upgrade methods, depending on how you installed VST-VRT. Follow the appropriate instructions below.

When installing using the .iso image method

If the product was installed using the .iso image method, the .iso image file is used when updating the VST-VRT operating system. To upgrade the VST-VRT operating system, follow these steps.

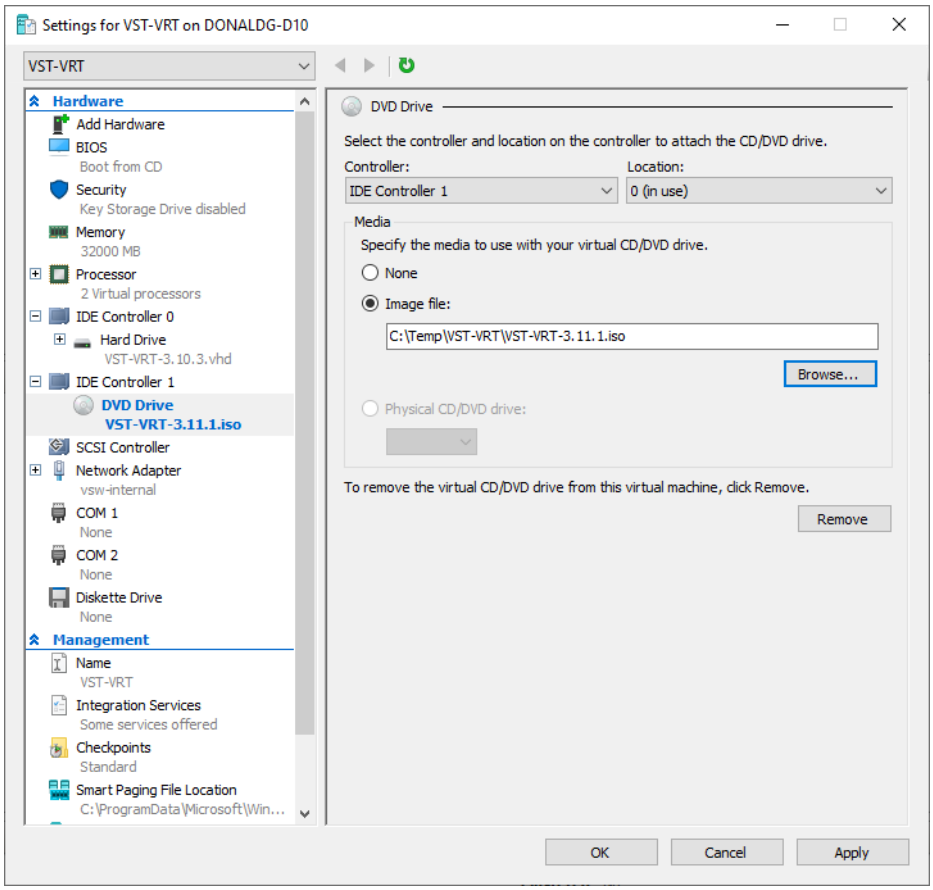
1. Get the latest version of the VST-VRT software from the Allied Telesis Support Portal. This will have a filename like VST_VRT-x.x.x.iso, where x.x.x is the version. Download it to a directory that is visible to your VST-VRT virtual machine.

2. If you want to retain the current unsaved configuration of VST-VRT, login to the VST-VRT GUI and click the ***Save*** button on the top right of the page. This stores the current state of the applications. The upgrade process will reboot the VST-VRT.

3. If the virtual machine is running, stop the machine. To stop the machine, right-click the virtual machine in the Virtual Machines pane of Hyper-V Manager, and select Shut Down from the context menu.

4. Right-click the virtual machine in the Virtual Machines pane of Hyper-V Manager, and select Settings from the context menu.

5. Select Hardware > IDE Controller 1 > DVD Drive on the left pane, then specify the new .iso image file in the Image file field. Click OK.



6. Right-click the virtual machine in the Virtual Machines pane of Hyper-V Manager, and select Start from the context menu.

7. The product will start with the new version. This completes updating the firmware of this product using the ISO image method.

When installing using the .vhd image method

If the product was installed using the .vhd image method, the .vhd image file is used when updating the firmware. To upgrade the VST-VRT operating system, follow these steps.

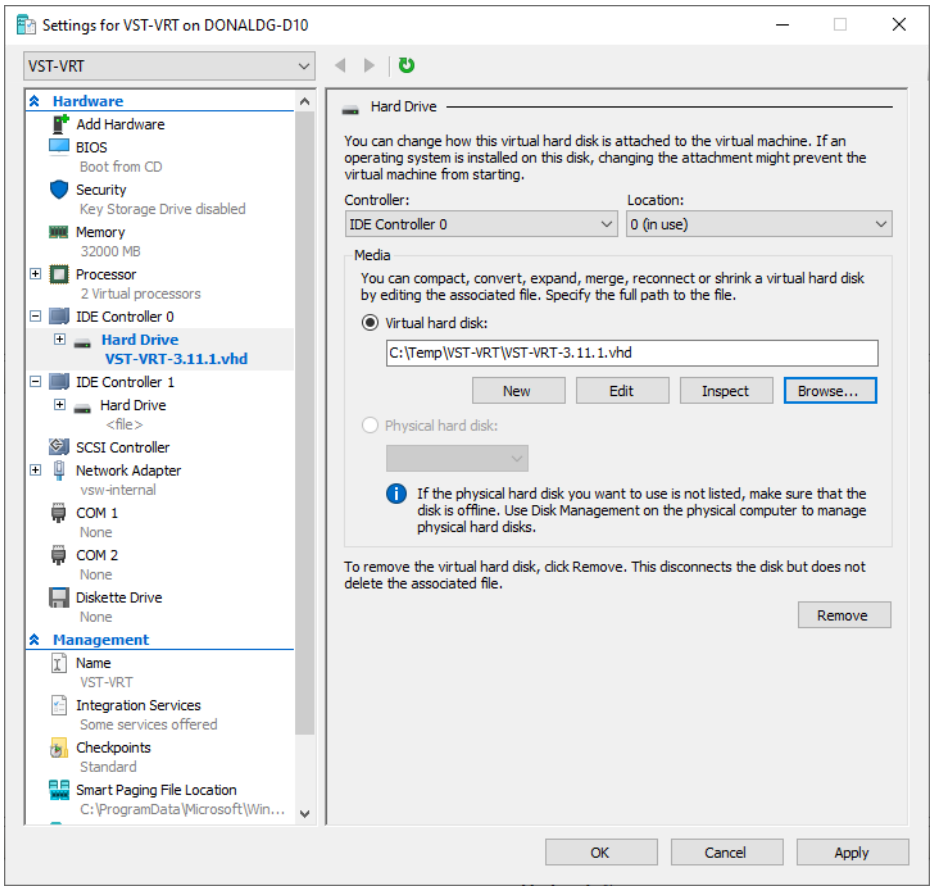
1. Get the latest version of the VST-VRT software from the Allied Telesis Support Portal. This will have a filename like VST_VRT-x.x.x.vhd, where x.x.x is the version. Download it to a directory that is visible to your VST-VRT virtual machine.

2. If you want to retain the current unsaved configuration of VST-VRT, login to the VST-VRT GUI and click the ***Save*** button on the top right of the page. This stores the current state of the applications. The upgrade process will reboot the VST-VRT.

3. If the virtual machine is running, stop the machine. To stop the machine, right-click the virtual machine in the Virtual Machines pane of Hyper-V Manager, and select Shut Down from the context menu.

4. Right-click the virtual machine in the Virtual Machines pane of Hyper-V Manager, and select Settings from the context menu.

5. Select Hardware > IDE Controller 0 > Hard Drive on the left pane, then specify the new .vhd file in the Virtual hard disk field. Click OK.



6. Right-click the virtual machine in the Virtual Machines pane of Hyper-V Manager, and select Start from the context menu.

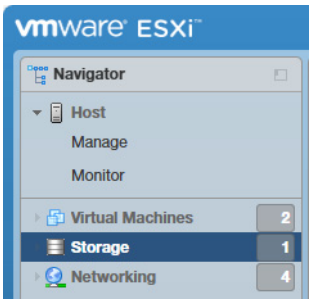
7. The product will start with the new version. This completes updating the firmware of this product using the .vhd image method.

Upgrade the VST-VRT operating system and GUI on VMware VSphere ESXi

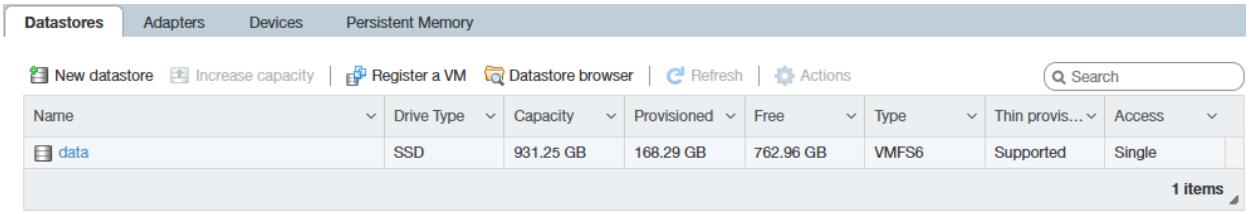
To upgrade or downgrade the VST-VRT operating system of the virtual machine, use the following steps:

1. Enter the IP address of the VMware ESXi server in the web browser, and enter the user name and password on the login screen to log in.

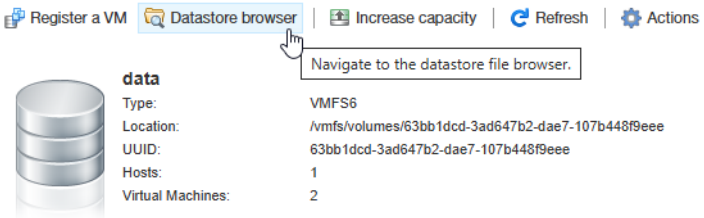
2. Select ***Storage*** from the menu on the left side of the management screen.



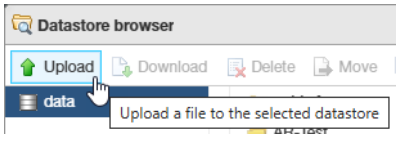
3. Select the datastore you want to upload the VST-VRT .iso image file to from the displayed datastores.



4. Select ***Datastore Browser***.



5. Click the ***Upload*** button.



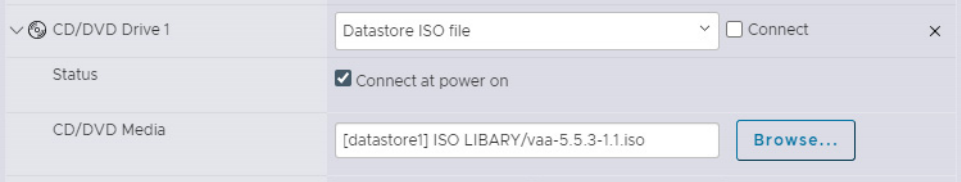
6. Select the .iso image file of VST-VRT to be uploaded on the local side, and save the .iso image in the datastore.

7. If the virtual machine is running, stop the virtual machine.

8. From the VM menu, click on your virtual machine.

9. Click on Edit from the top menu.

10. Click the arrow to the left of CD/DVD Drive 1 to expand it. Click Browse to select the new .iso file, then click Select.



11. Click Save when you return to the settings screen.

12. Start the virtual machine.

13. The virtual machine will start from the updated .iso.

Upgrade Vista Manager, AMF Cloud, AMF Security, and RADgate applications

Upgrade these applications as a bundle. This ensures they are compatible with each other and with the operating system version.

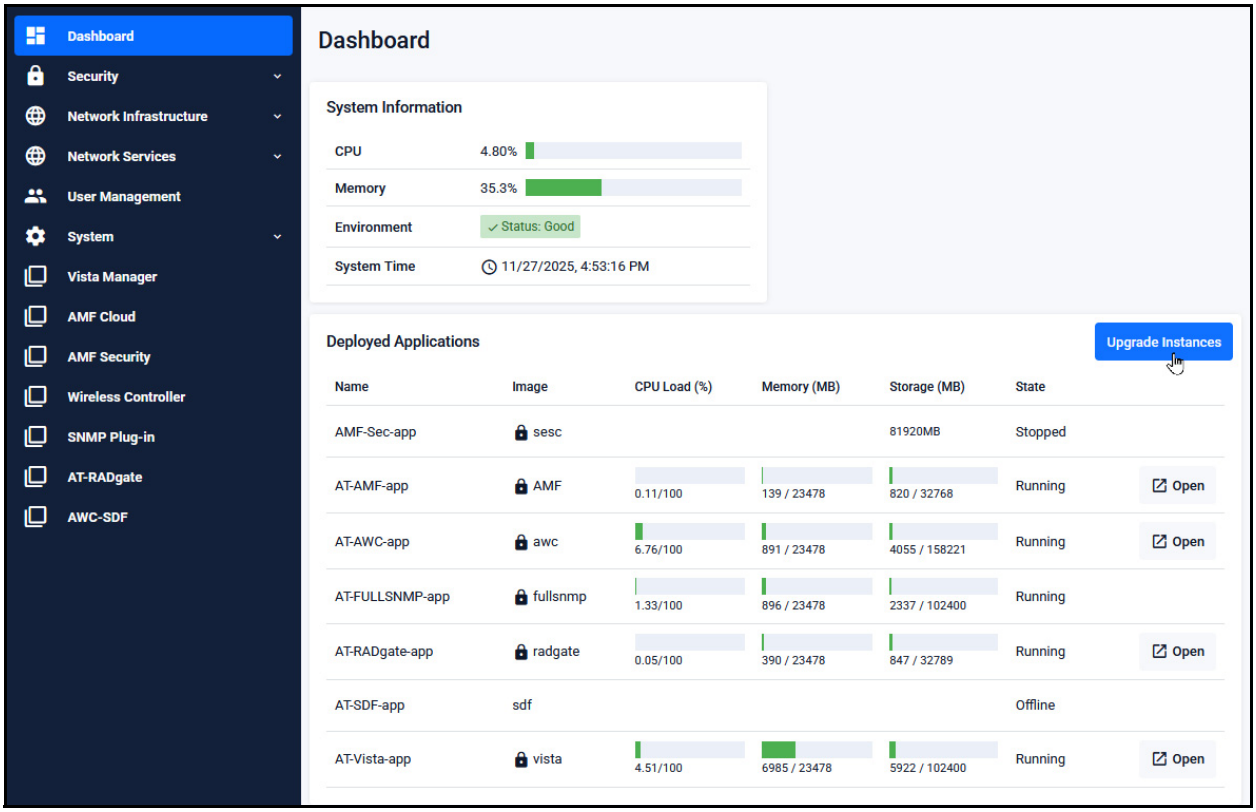
Before upgrading these applications:

- We recommend backing up application data for all applications regularly, and before upgrading the applications.
- "Upgrade the VST-VRT operating system and GUI on Hyper-V Server" on page 38.

Use the procedure in this section to upgrade these applications:

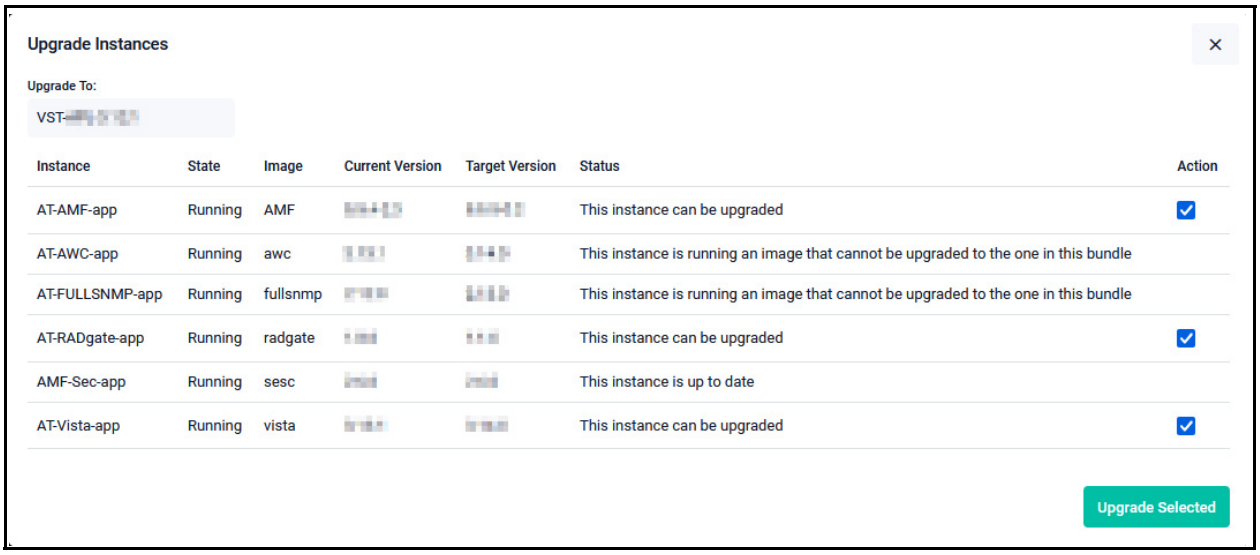
- Vista Manager
- AMF Cloud
- AMF Security
- AT-RADgate

1. In the VST-VRT ***Dashboard*** page, click the ***Upgrade Instances*** button.



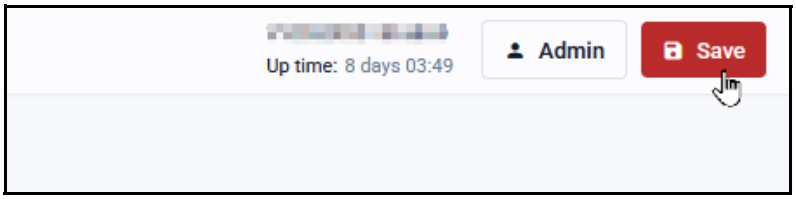
2. Make sure the correct version of the bundle file is displayed in the ***Upgrade to*** field at the top left of the upgrade instances panel. If not, use the drop down list to select the correct version.

   Applications that can be upgraded are shown as selected. We recommend upgrading them all.



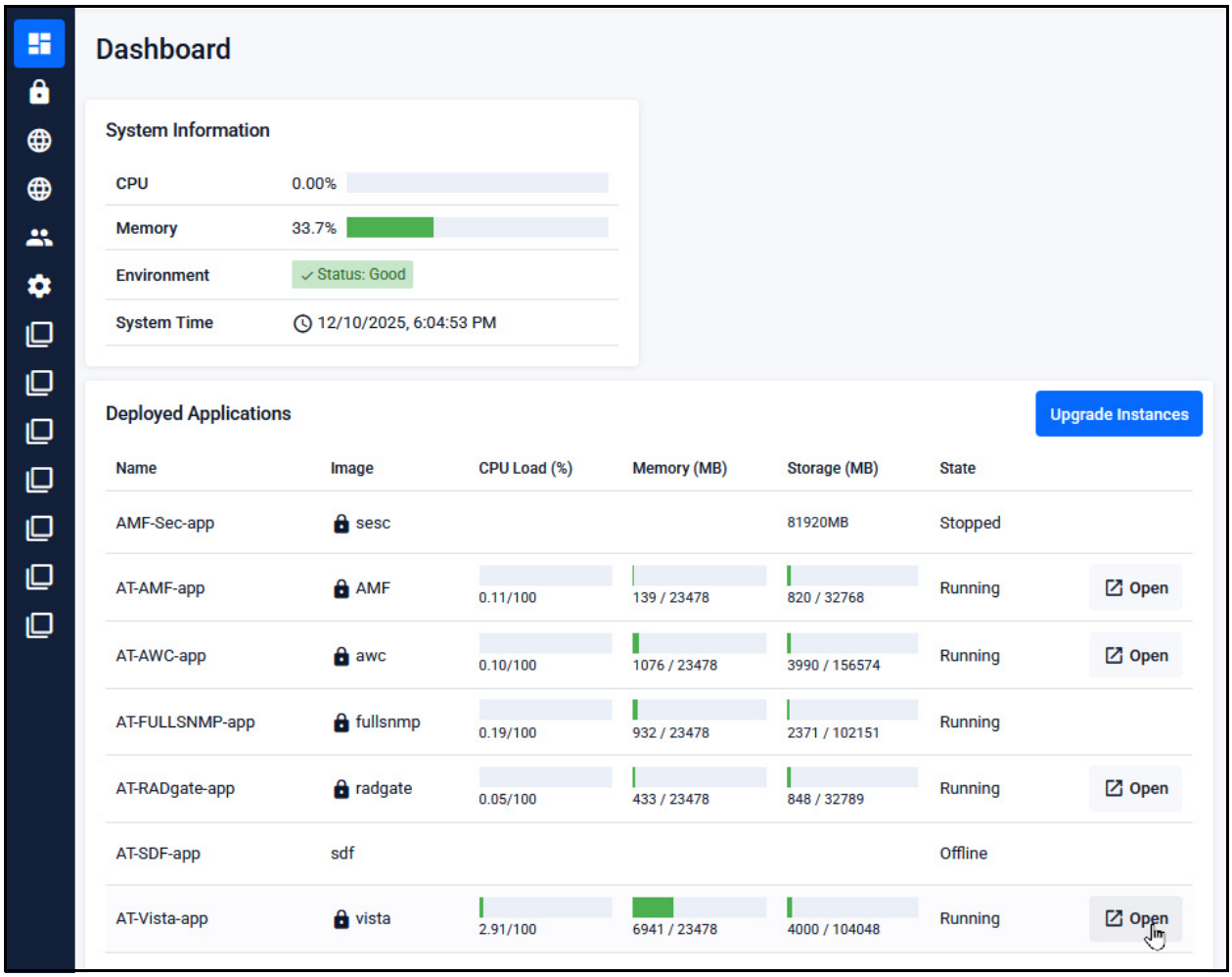
3. Click the ***Upgrade Selected*** button and wait until the upgrade is complete. The ***Status*** column shows progress. The applications first stop, then change to the new version, then start.

4. It is important to save the state of the VST-VRT operating system after the upgrade. The ***Save*** button in the top right corner of the screen is orange when there are unsaved changes. Click on the button to save the changes.

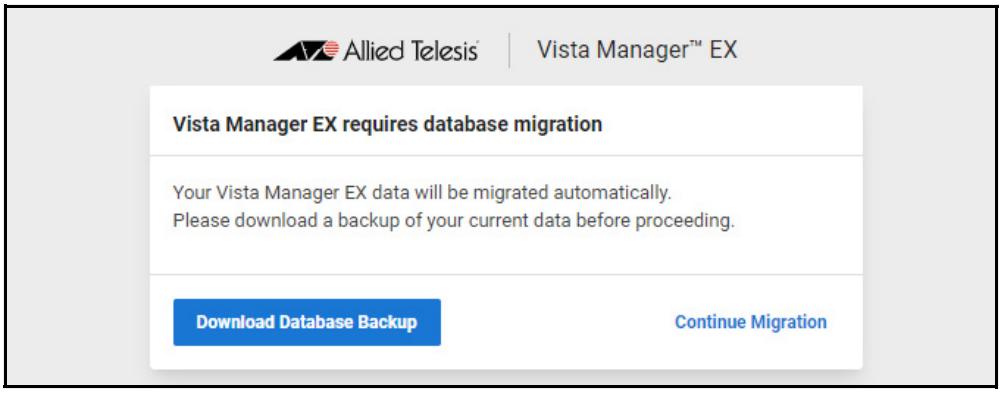


If you do not save the changes and VST-VRT is rebooted, the upgraded applications will revert to the old app images and fail to start. You will see 'configured image "<image-name>" doesn't exist' messages if this happens.

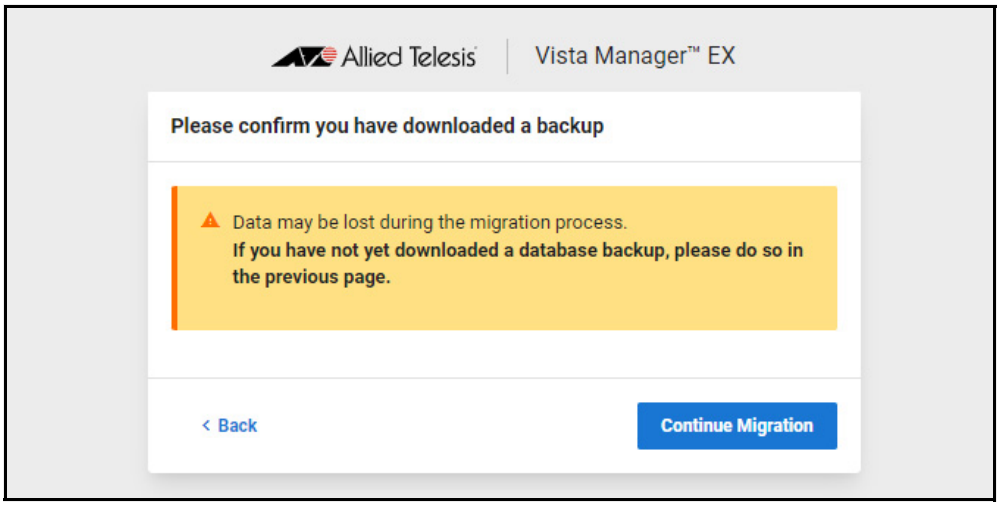
5. In the VST-VRT GUI ***Dashboard*** page, open Vista Manager by clicking the **Open** button next to AT-Vista-app.

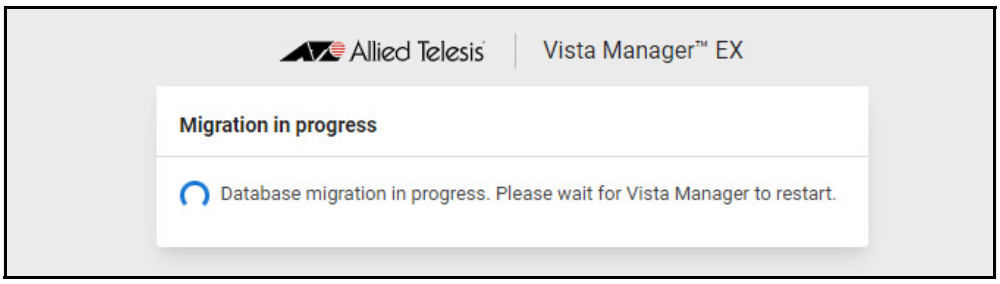


6. Vista Manager EX may prompt you to migrate the database. Select ***Download Database Backup*** to make a backup.



7. Confirm you have successfully downloaded a backup file, then select ***Continue Migration***. If you get a browser error about the page becoming unreachable, then refresh your browser.





8. Once the migration has completed, your connection may be lost. If this happens, close your browser and reopen the application from the VST-VRT dashboard.

Upgrade Wireless Controller (AWC) and SNMP (Full) plugin applications

Use this manual procedure to upgrade the following applications by destroying the old instances and creating new instances.

- Wireless Controller (AWC)
- SNMP (Full)

Before upgrading these applications, complete the following steps:

- "Back up application data" on page 35.
- "Upgrade the VST-VRT operating system and GUI on Hyper-V Server" on page 38..

For AWC and SNMP (full) applications, you ***cannot***:

- upgrade these as part of a set
- use the upgrade procedure from versions earlier than VST-VRT 3.4.1 to perform the upgrade.
- use the Upgrade button in the VST-VRT GUI to upgrade.

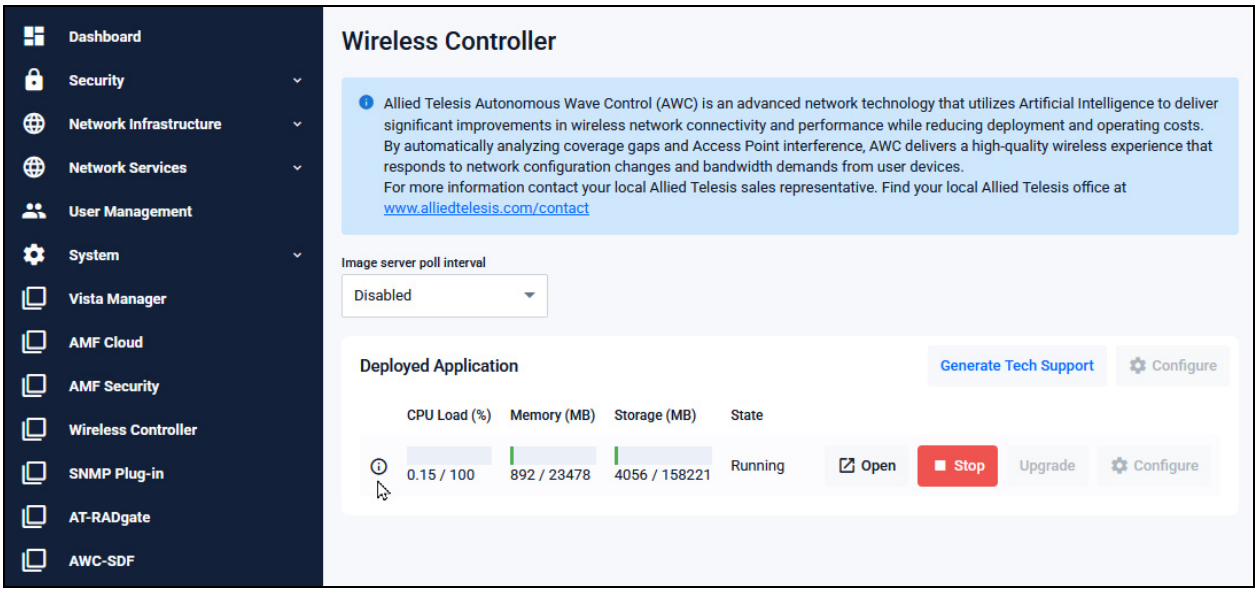
Instead, use these procedures:

- "Destroy and recreate the application instances" on page 47.
- "Re-register plugins in Vista Manager" on page 50.
- "Restore application data from back-up" on page 52..

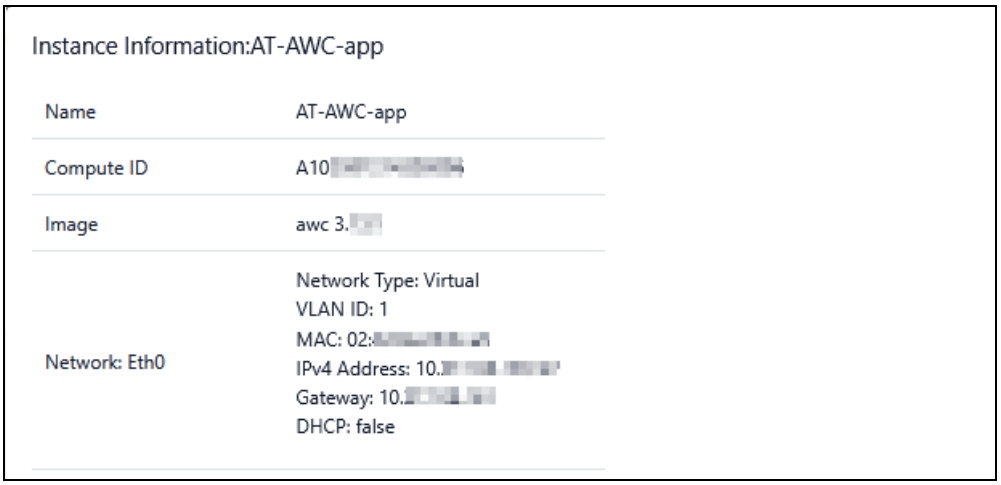
Destroy and recreate the application instances

In the VST-VRT GUI, follow these steps.

1. Navigate to the application page for the application.

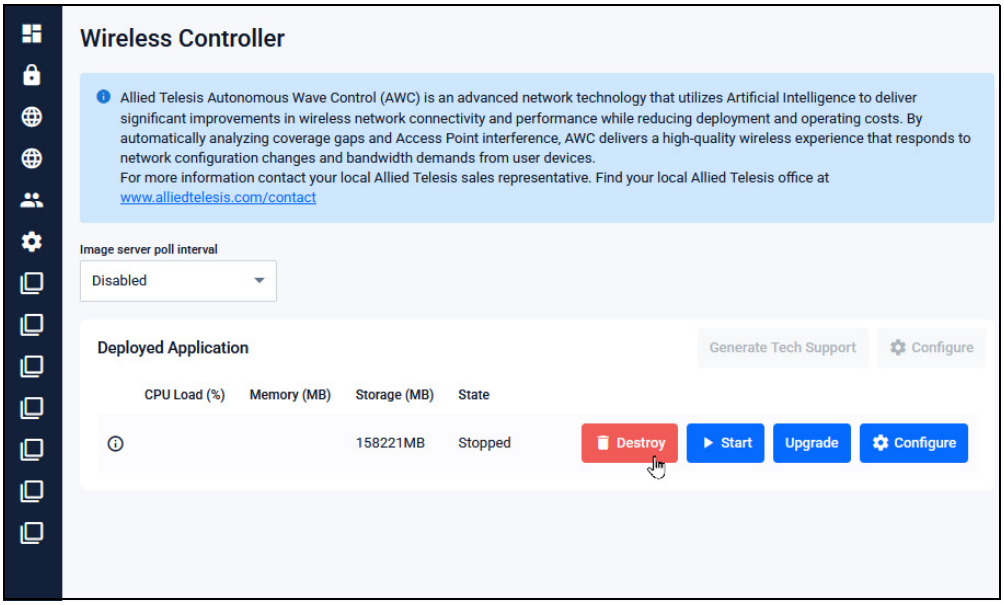


2. Hover over the Instance Information icon (i) and record information about the application from the ***Instance Information*** panel. Record all the network settings (Network Type, etc). You will need this information in a later step.



3. In the application page, stop the application by clicking the ***Stop*** button.

4. Destroy the application by clicking the ***Destroy*** button.

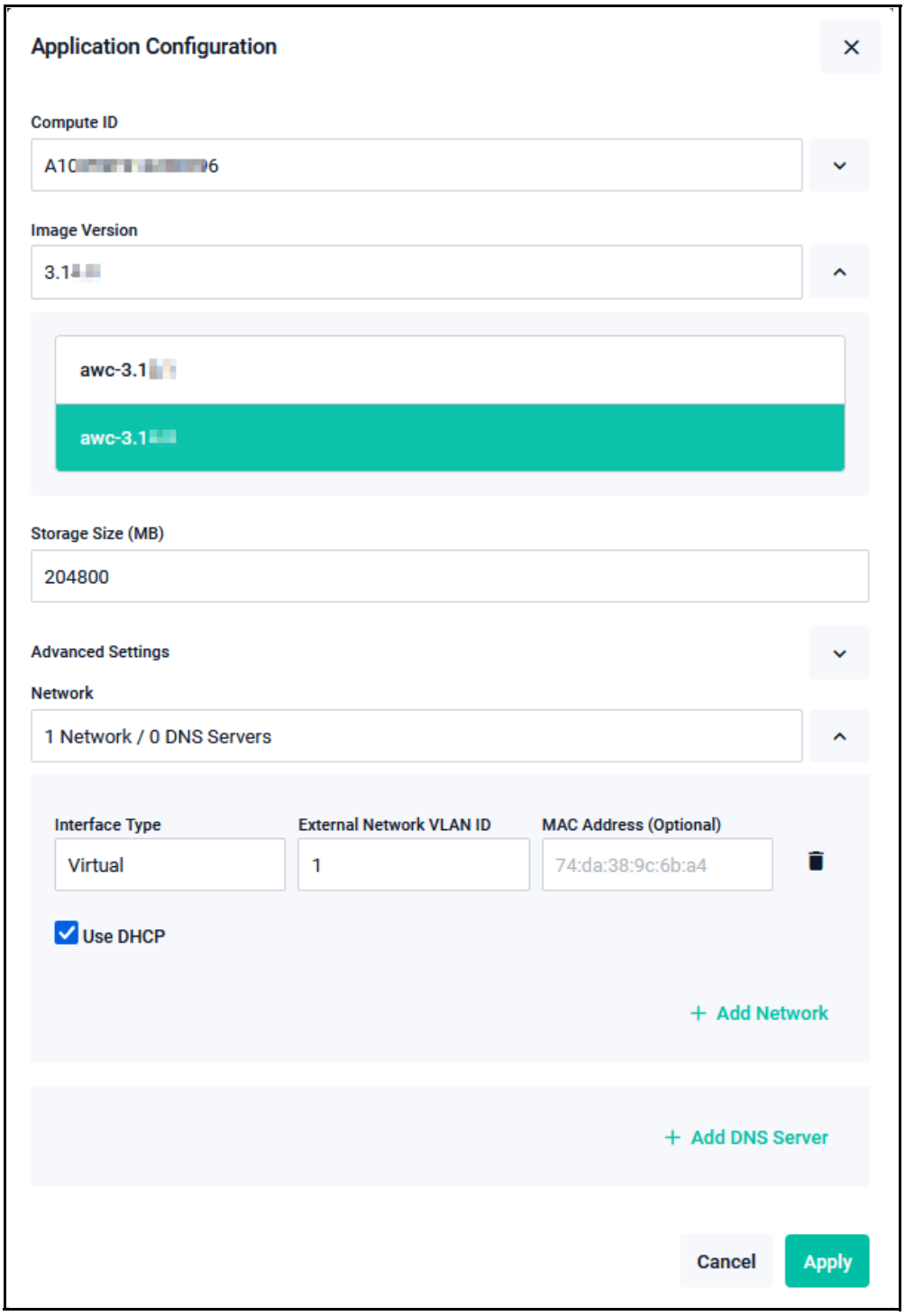


5. Create a new instance. First, in the application page, click the ***Configure*** button.

6. Add an interface to connect the application to your network. Expand the Network section. Either select DHCP or add a static IP address and gateway address, and add a DNS server if needed.

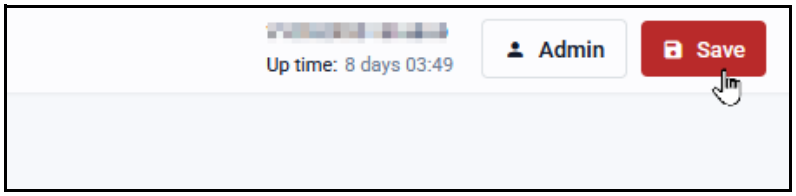
7. In the ***Application Configuration*** dialog box, fill in the storage and recorded network data. The recommended storage values are:

   AWC: 204 800 MB
   SNMP Full: 102 400 MB



8. Click the ***Apply*** button. This creates a new version of the application instance. Wait a few minutes for this to start and for the ***Open*** button to appear.

9. It is important to save the state of the VST-VRT operating system after the upgrade. The ***Save*** button in the top right corner of the screen is orange when there are unsaved changes. Click on the button to save the changes.



10. From the VST-VRT menu, navigate to the ***Vista Manager*** page and click the ***Open*** button. If necessary, wait for Vista Manager EX to perform its initial set up.

11. Log in to Vista Manager EX.

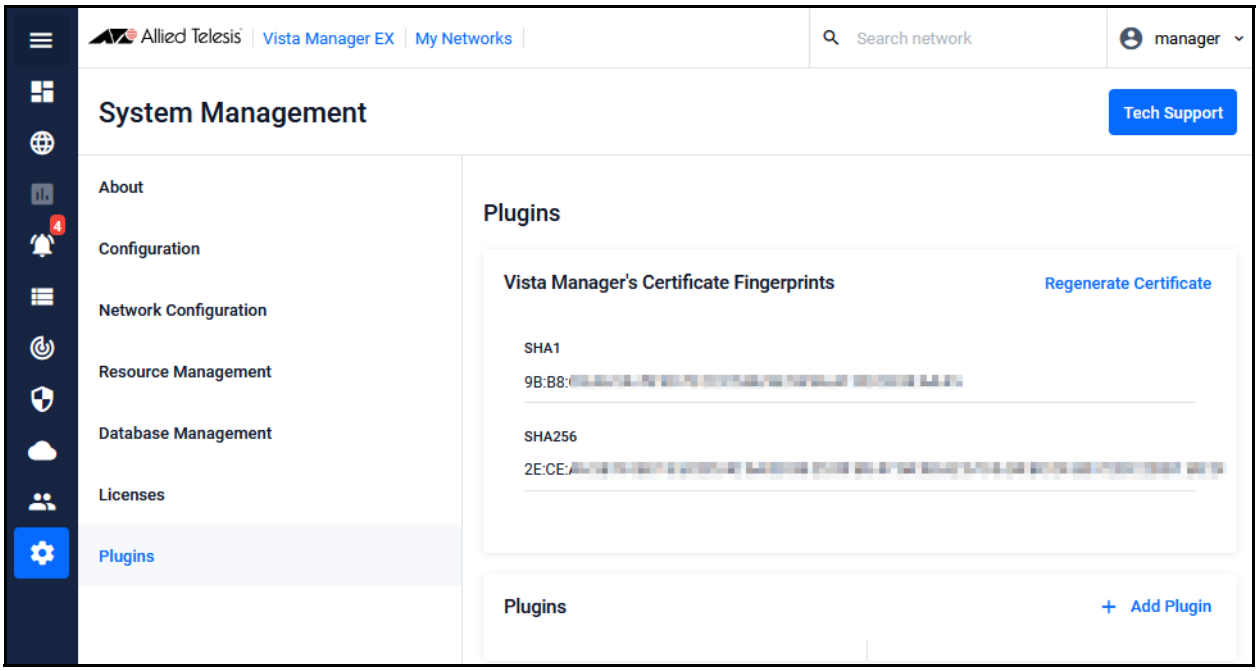
Re-register plugins in Vista Manager

If you are using these plugins in Vista Manager EX, you will need to re-register them:

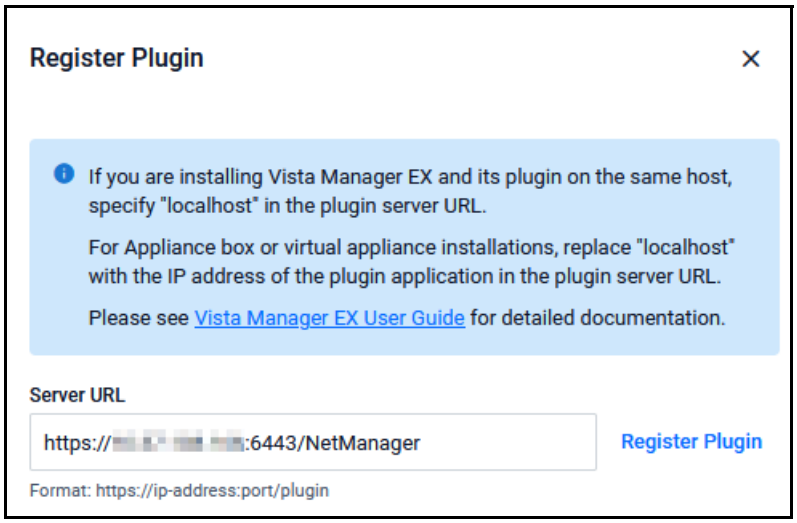
- Wireless Controller (AWC)
- SNMP (Full)

Follow these steps for each of the plugins.

1. On the Vista Manager EX page, navigate to ***System Management*** > ***Plugins***.



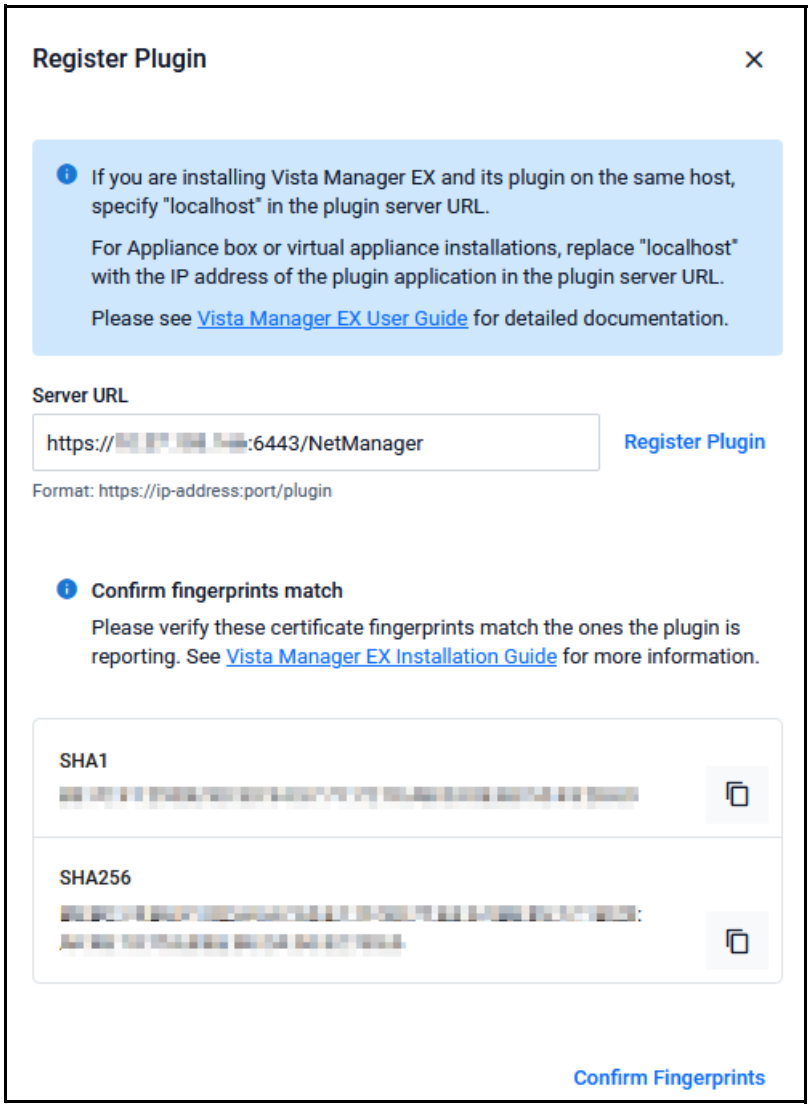
2. Click **+Add Plugin**.



3. Enter the server URL. This includes the IP address of the plugin application.

- For the SNMP (Full) plugin, this is `<ip-address>:6443/NetManager`
- For the Wireless Controller (AWC) plugin, this is `<ip-address>:5443/wireless_plugin`

Click **Register Plugin**.



4. Check that the certificate fingerprints match the ones reported in the plugin. Click **Confirm Fingerprints**. A 'plugin updated' pop-up message confirms that the plugin has been updated.

Next, restore system data for the plugin application from the back-up file, as required.

Restore application data from back-up

For the Wireless Controller and SNMP (Full) applications, use the following procedures to restore the system data from backup files:

- "Restore system data for the Wireless Controller plugin" below
- "Restore system data for the SNMP plugin" on page 54.

Note that:

- Restoring a backup file made on another platform is not supported.
- For the applications upgraded as a set in this procedure "Upgrade Vista Manager, AMF Cloud, AMF Security, and RADgate applications" on page 43., the data is restored automatically.

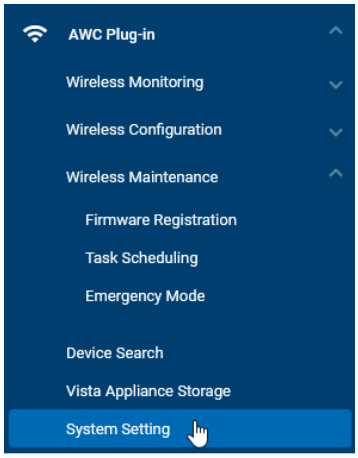
Restore system data for the Wireless Controller plugin

Note that restoring a backup file made on another platform is not supported.

To restore data from the back-up file for the Wireless Controller (AWC) plugin application, follow these steps:

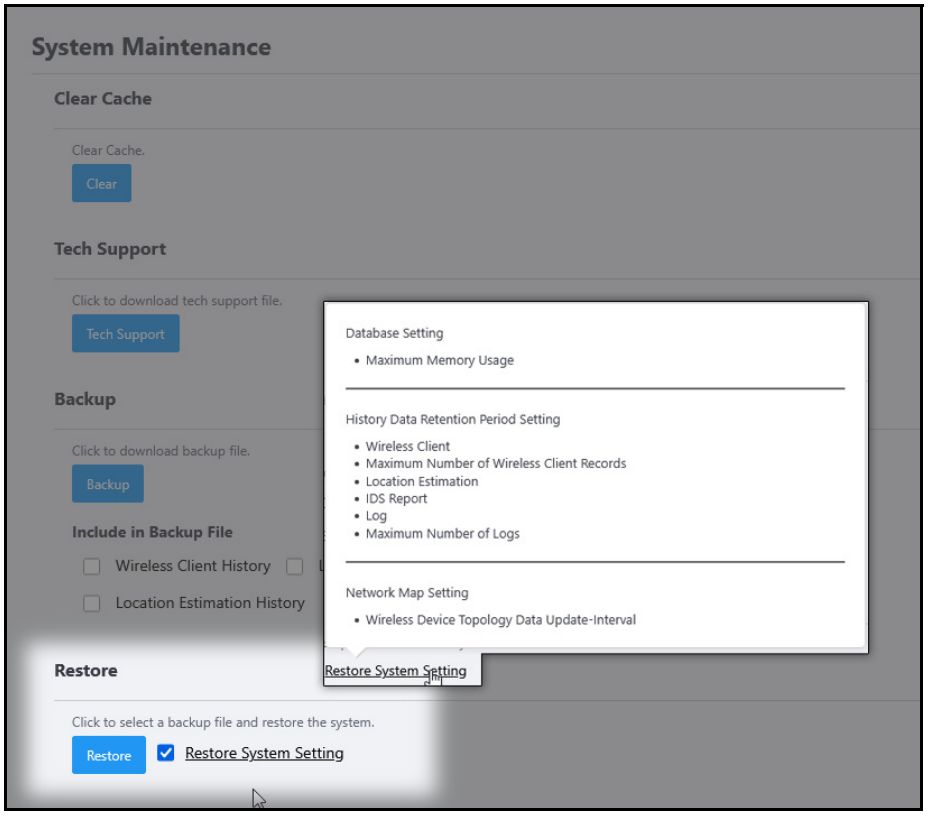
1. Log in to Vista Manager EX using an Admin account.

2. In the Vista Manager EX menu, navigate to ***AWC plugin*** > ***System Setting***.



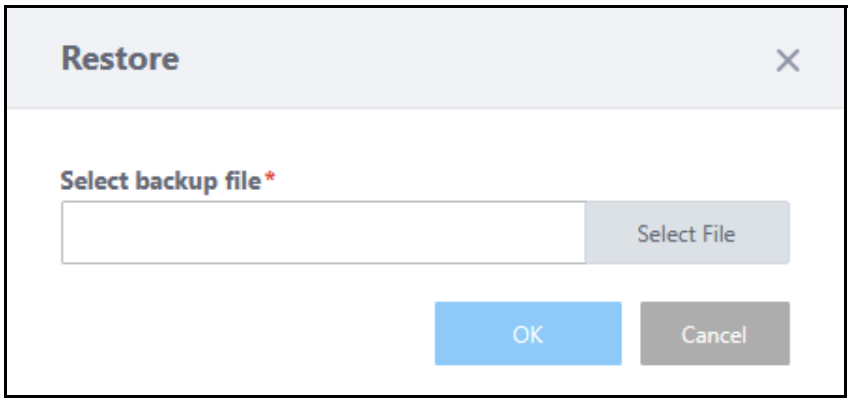
3. On the **System Information** page, scroll down to the **System Maintenance** section.

4. Scroll down to the **Restore** section.



Hover over **Restore System Setting** to see the system settings that will be restored. Check the box and click the **Restore** button.

5. In the Restore dialog box, click ***Select File*** and select the backup file.



6. Click ***OK***. Confirm.

7. After it has finished restoring, a dialog box shows that restoration is complete. Click ***OK***.

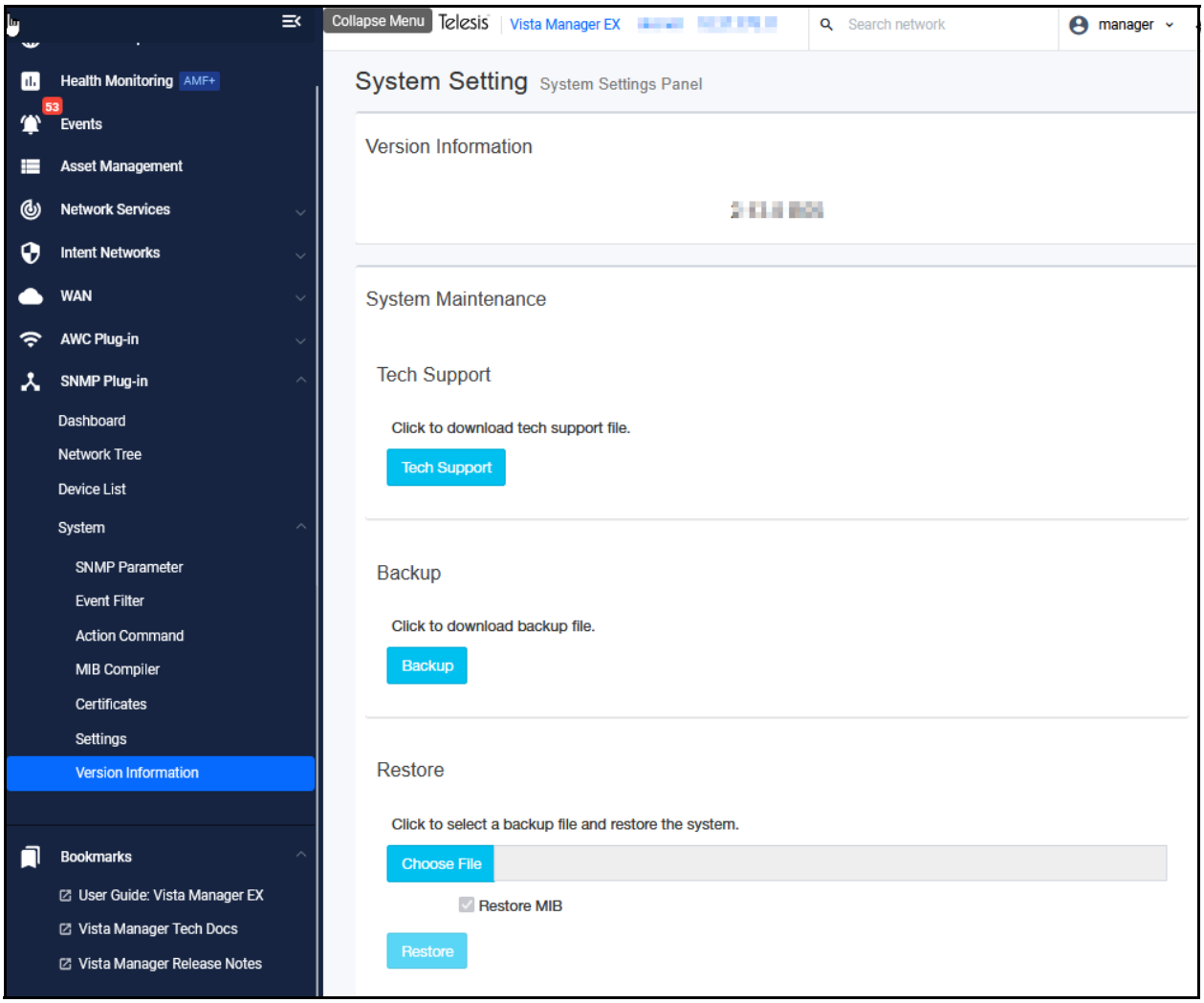
Restore system data for the SNMP plugin

To restore data from the backup of application data for the SNMP plugin application, follow these steps.

1. Log in to Vista Manager EX using an Admin account.

2. In the left menu of Vista Manager EX, click the ***SNMP plugin*** icon, then click ***Version Information***.

3. In the ***System Setting*** panel, scroll down to the ***System Maintenance*** panel and in that, to the **Restore** panel.



4. Select the file to restore from and click the ***Restore*** button. This restores the data from the back-up for the SNMP plugin application.

Remove obsolete files from memory

You can make more space available by removing obsolete files. Keep the current versions of all the files.

1. From the VST-VRT dashboard, navigate to the ***System*** > ***File Management*** page.

2. Click the ***Delete*** button to the right of the obsolete files you want to remove.

Migrating from Windows to VST-VRT

See the Windows to VST-VRT Vista Manager Migration User Guide.

Upgrading Vista Manager on VST-APL

See the Vista Manager Network Appliance (VST-APL) 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