

Release Note for Vista Manager EX Software Version 3.11.x



VISTA MANAGER™ EX

» 3.11.0

» 3.11.1

Acknowledgments

©2023 Allied Telesis Inc. All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesis, Inc.

Allied Telesis, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesis, Inc. has been advised of, known, or should have known, the possibility of such damages.

Allied Telesis, AlliedWare Plus, Allied Telesis Management Framework, EPSRing, SwitchBlade, VCStack and VCStack Plus are trademarks or registered trademarks in the United States and elsewhere of Allied Telesis, Inc. Adobe, Acrobat, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Additional brands, names and products mentioned herein may be trademarks of their respective companies.

Getting the most from this Release Note

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

Contents

What's New in Vista Manager EX v3.11.1	4
What's New in Vista Manager EX v3.11.0	6
Important Considerations Before Upgrading	39
Obtaining User Documentation	40
Upgrading Vista Manager as a Windows-based installation	41
Upgrading Vista Manager on VST-APL	51
Upgrading Vista Manager on VST-VRT	51
Troubleshooting	51

What's New in Vista Manager EX v3.11.1

Introduction

This release note describes the new features in Vista Manager EX™ v3.11.1. It covers Vista Manager EX plus the optional Autonomous Wave Controller (AWC) and SNMP plug-ins, and Allied Intent-based Orchestrator (AIO).

You can obtain the software files from the [Software Download area of the Allied Telesis website](#). Log in using your assigned email address and password.

Contact your authorized Allied Telesis support center to obtain licenses.



Caution: Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesis, Inc.

While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesis, Inc. can not accept any type of liability for errors in, or omissions arising from, the use of this information.

Additional virtualization platforms for deployment

Applies to the Vista Manager EX virtual machine installation

From version 3.11.1 onwards, Vista Manager EX can be deployed on the following additional virtualization platforms:

- Hyper-V on Windows Server version 2012 R2 onwards
- VMware vSphere Hypervisor (ESXi) versions 6.0/6.5/6.7/7.0/8.0

Note that the Vista Manager EX plug-ins are not available with this deployment.

New Features and Enhancements

This section summarizes the new features and enhancements added to Vista Manager EX version 3.11.1.

It includes:

- “Limiting the number of stored events” on page 5.
- “Support for receiving syslog messages in CEF format” on page 5.
- “Additional wireless modes for TQ6000 GEN2 Series Access Points” on page 5.
- “Multicast to unicast conversion for Wi-Fi” on page 5.

Limiting the number of stored events

Applies to all Vista Manager EX installations

From version 3.11.1 onwards, Vista Manager EX automatically limits the number of events it stores, to 5 million events by default. You can change this default number.

This means that when you update your Vista Manager EX installation to version 3.11.1 or later, Vista Manager EX will only keep the 5 million most recent event messages. If Vista Manager EX has more than 5 million events, older events will be deleted, to reduce the number of events to 5 million.

If you do not wish to lose the older events, archive them before you upgrade.

Support for receiving syslog messages in CEF format

Applies to all Vista Manager EX installations

From version 3.11.1 onwards, Vista Manager EX can interpret and act on syslog messages in CEF format. Previously, Vista Manager EX could only interpret syslog messages if they were in ISO format.

This enhancement improves Vista Manager EX's support for third-party security appliances that only send messages in CEF format.

Additional wireless modes for TQ6000 GEN2 Series Access Points

Applies to the AWC wireless manager plug-in, when managing TQ6702 GEN2, TQm6702 GEN2, TQ6602 GEN2 and TQm6602 GEN2 APs

From version 3.11.1 onwards, you can set the radio on these APs to the following additional modes, in the AP Profile:

- Radio 1: b/g/n
- Radio 2: a/n and a/n/ac

This is in addition to the following modes that were already supported: b/g, b/g/n/ax, a, a/n/ac/ax.

Multicast to unicast conversion for Wi-Fi

Applies to the AWC wireless manager plug-in, when managing TQ6702 GEN2, TQm6702 GEN2, TQ6602 GEN2 and TQm6602 GEN2 APs that are running firmware version v8.0.3-1.1 or later

From version 3.11.1 onwards, you can turn on multicast to unicast packet conversion on these APs, in the AP Profile settings. Multicast packets are not always the most efficient or reliable way to send traffic over Wi-Fi, so in many networks it is better to convert multicast packets to unicast before sending them over Wi-Fi.

What's New in Vista Manager EX v3.11.0

Introduction

This release note describes the new features in Vista Manager EX™ v3.11.0. It covers Vista Manager EX plus the optional Autonomous Wave Controller (AWC) and SNMP plug-ins, and Allied Intent-based Orchestrator (AIO).

You can obtain the software files from the [Software Download area of the Allied Telesis website](#). Log in using your assigned email address and password.

Contact your authorized Allied Telesis support center to obtain licenses.



Caution: Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesis, Inc.

While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesis, Inc. can not accept any type of liability for errors in, or omissions arising from, the use of this information.

New Features and Enhancements

This section summarizes the new features and enhancements added to Vista Manager EX version 3.11.0.

It includes:

- “Importing network-associated RADIUS groups” on page 8.
- “Health monitoring enhancements” on page 10.
- “Local RADIUS batch support” on page 17.
- “Improved AMF Plus device discovery” on page 19.
- “Duplicate node manual merge tool” on page 20.
- “Autonomous queue threshold configuration and queue priority reassignment” on page 22.
- “Left-hand menu navigation improvement” on page 24.
- “SD-WAN map displays custom icons” on page 25.
- “Error notifications for exceeding user limits in RADIUS groups” on page 25.
- “Vista Manager EX supports Windows Server 2022” on page 25.
- “Vista Manager EX supported on VMware ESXi 7” on page 25.
- “Vista Manager EX supported on VMware ESXi 8” on page 25.
- “Vista Manager EX supports Nutanix AHV” on page 25.
- “Asset Management grouping enhancement” on page 26.
- “Backup running config available on AMF devices” on page 27.
- “Tech Support log export customization” on page 28.
- “SNMP plug-in is enabled by default in AMF Plus networks” on page 28.
- “Feature permissions changes (including Sites and Groups permissions)” on page 29.
- “AWC enhancements” on page 29.

Importing network-associated RADIUS groups

Applies to all Vista Manager EX installations

From version 3.11.0 onwards, you can import Network-associated RADIUS groups for end-to-end (e2e) networks. An end-to-end network is a network that uses the same VLAN subnet on all devices.

A Network-associated RADIUS group is a RADIUS group created from an e2e network. The RADIUS group contains a VLAN attribute set to the VLAN ID in use by the corresponding source network.

These Network-associated RADIUS groups are what links the RADIUS users to the networks (via VLAN ID) and thus Access Control.

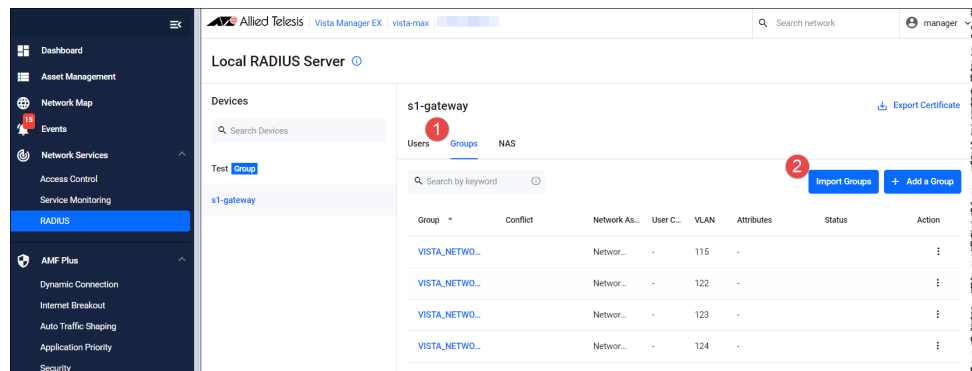
This means that when RADIUS users in these Network-associated RADIUS groups authenticate, the port they authenticate on will be automatically assigned to the VLAN ID associated with the network, and they will be connected to the correct AMF Plus Network, rather than statically adding the VLAN to the expected port.

Moving RADIUS users from one Network-associated RADIUS group to another will also update their access control.

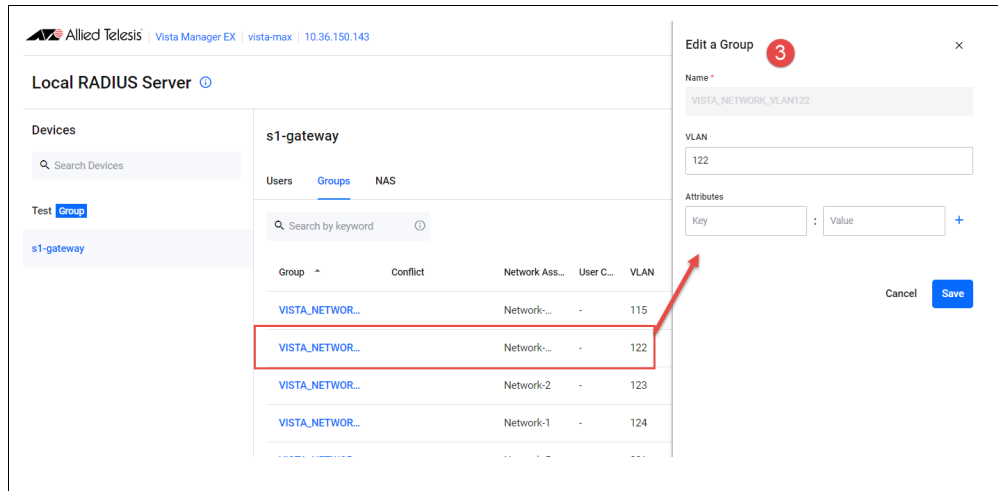
To use this feature:

First create a VLAN on the device(s) that you want to use in the Network-associated RADIUS Group. Assign an IP address to the VLAN, then:

1. Go to **RADIUS > Groups**
2. Click **Import Groups**.
« This action imports RADIUS groups based on AMF plus e2e networks.



3. Select a Group and click **Edit** to see its detail:



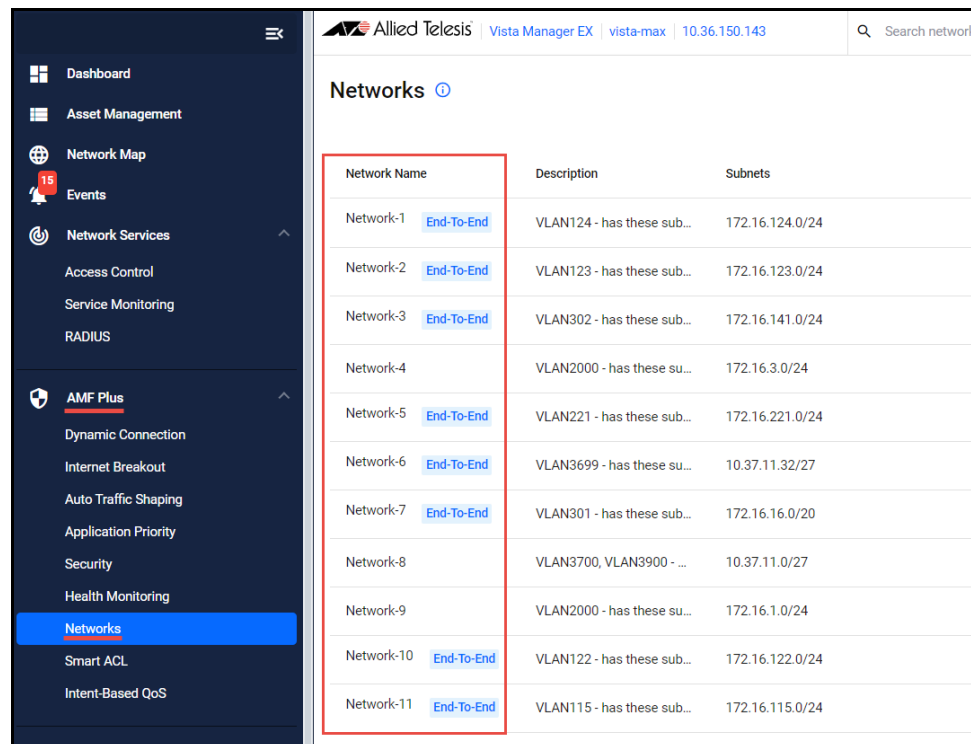
You will see that the newly created RADIUS group has:

- a **Name** - VISTA_network_VLANX. X is the VLAN ID
- a **VLAN** attribute with the same VLAN ID as the e2e network

To view e2e networks go to:

- **AMF Plus > Networks**

In the **Network Name** column, End-to-End networks are easy to identify:



For more information, see the [Vista Manager EX User Guide](#).

Health monitoring enhancements

Network health and passive monitoring by error counters

Applies to all Vista Manager EX installations

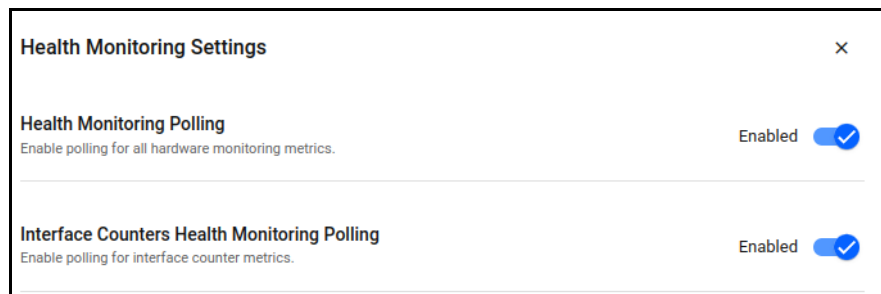
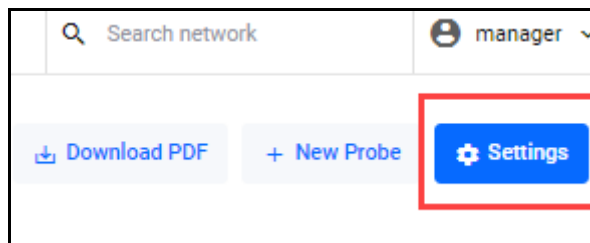
From version 3.11.0 onwards, the Health Monitoring dashboard is split into two tabs. Device Health and Network Health.

- **Device Health:** hardware state (CPU, memory, storage, temperature)
- **Network Health:** traffic and related errors (traffic health, interface counters)

The Network Health tab supports the Interface Counters dashboard. This dashboard provides a detailed view of interface errors on a specific device. It helps you monitor and troubleshoot interface issues for optimal device performance.

To view updated information on Interface Counters in the Network Health tab, you must first enable both **Health Monitoring Polling** and **Interface Counters Health Monitoring Polling** in the settings. This is because Interface Counters Health Monitoring Polling only affects the interface counters (not the entire network health tab, just the right column).

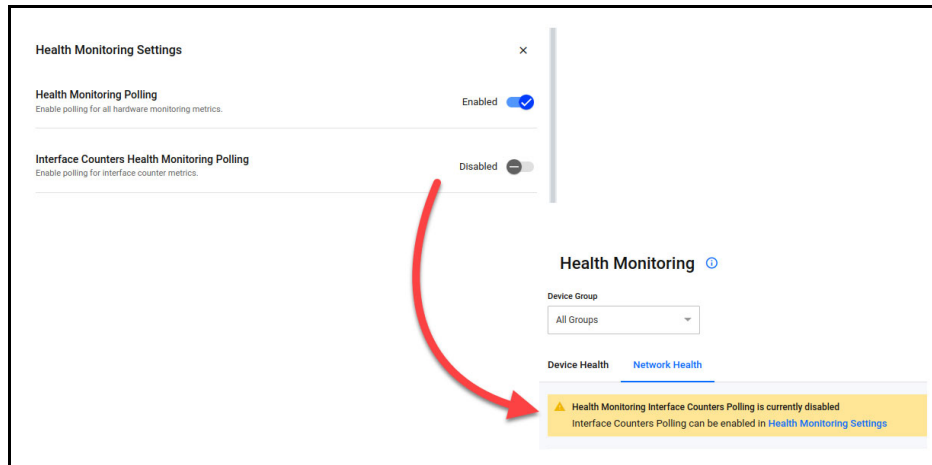
To access the Health Monitoring settings, click the **Settings** button on the top right corner of the Health Monitoring page:



Note: You must first enable Health Monitoring Polling before you can enable Interface Counters Health Monitoring Polling.

Interface Counter Polling is a subset of Health Monitoring Polling and cannot be enabled otherwise.

A warning will appear on the Network Health tab of Health Monitoring if **Interface Counters Health Monitoring Polling** is disabled, but Health Monitor polling is enabled:



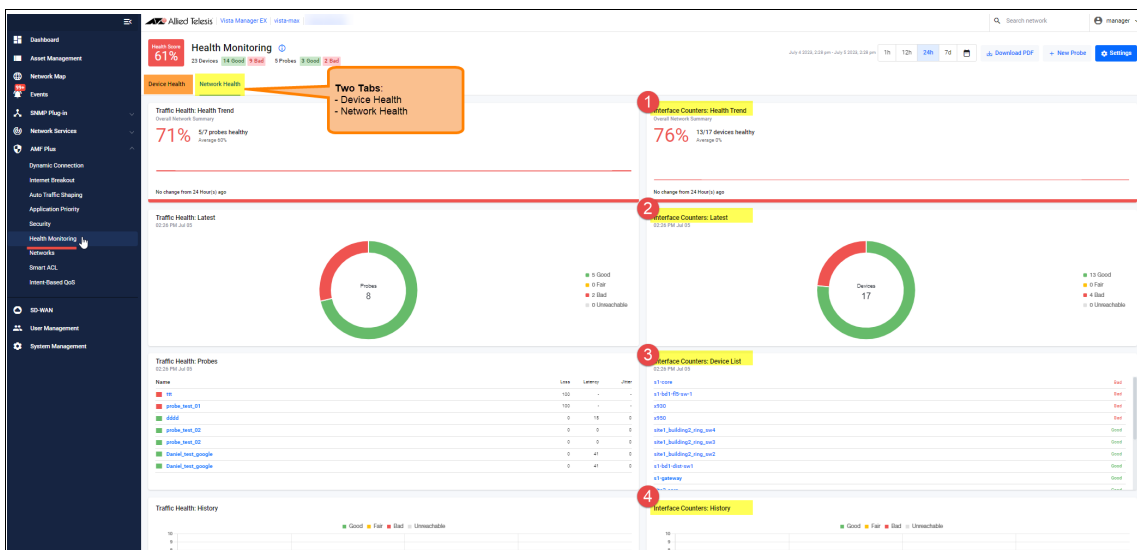
The interface counters dashboard includes the following widgets:

1. Health Trend
2. Latest
3. Device List
4. History

Use the dashboard to easily monitor:

- Interface errors occurring across the entire network or on a particular device.
- Overall health status and specific health metrics of interfaces.
- Detailed explanations of the errors, enabling you to effectively diagnose and resolve any issues that arise.

You can configure the threshold values for each interface error type in the main settings panel of the dashboard. These thresholds apply to the entire network and are used to determine the health status of devices and interfaces.



For more information, see the Health Monitoring section of the [Vista Manager EX User Guide](#).

Filtering feature for hardware health monitoring

Applies to all Vista Manager EX installations

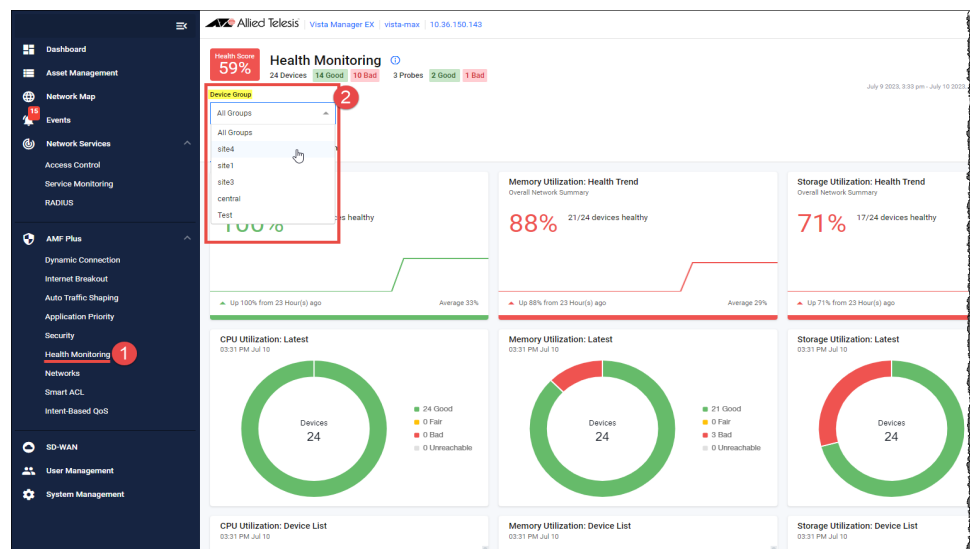
Currently the Health Monitoring dashboard shows all devices in the network that are known.

From version 3.11.0 onwards, Health Monitoring supports filtering of devices in the main dashboard. Devices can be filtered by device group. Only devices from the selected device group will be displayed in the dashboard. The selected filter is applied to both Device health and Network health tabs. Probes listed in the Network health tab are filtered based on the configured source device.

This lets you focus attention on particular devices you are interested in viewing rather than being overloaded with a large amount of information which is possible in a much larger network.

To use this feature:

1. Go to **AMF Plus > Health Monitoring**
2. Click **Device Group** and select a group from the selector:
 - « The default is *All Groups* (i.e. all known devices). You can select all auto-generated devices pulled in through SNMP or you can select a group for a specific area in the topology via the auto-generated AMF groups. Auto-generated and user generated groups are located under the **Asset Management** menu.
 - « You can also type in the search box of the selector to show only groups that match that string.



Active Health Monitoring of traffic links

Applies to all Vista Manager EX installations

From version 3.11.0 onwards, AMF Plus Health Monitoring supports active monitoring of traffic health.

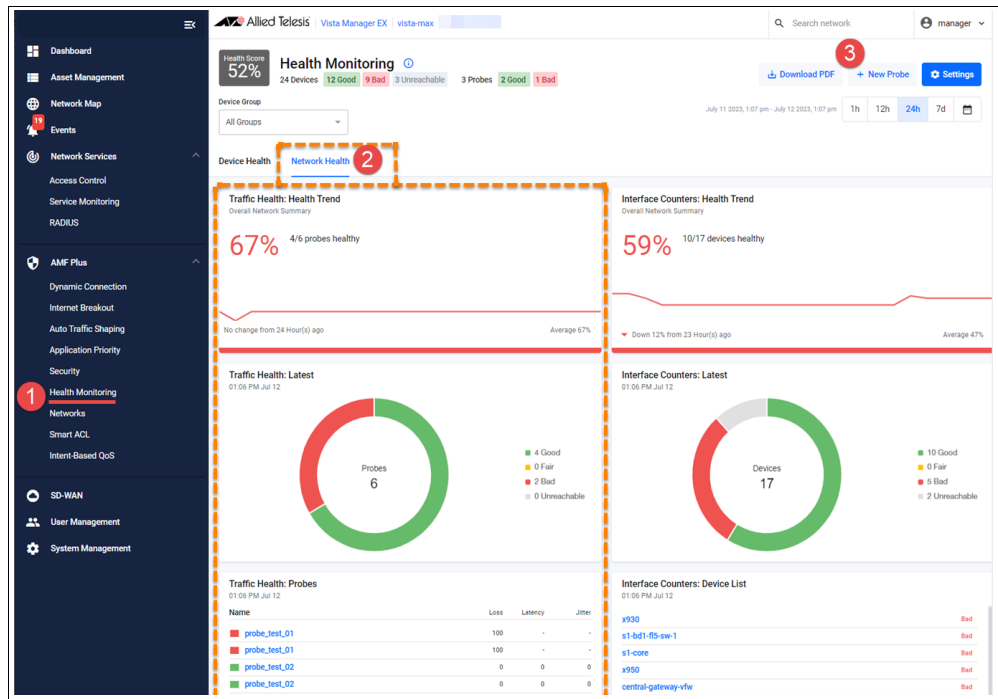
The Health Monitoring feature allows you to create Linkmon Probes and will report statistics (latency, jitter, and packet loss) on these probes, representing the health of the traffic.

For example, you could use the probes to monitor links:

- from a company's router to the Internet, to ensure it is operating and at an acceptable level.
- inside a company's LAN from the core switch to a highly used backup server to check latency.
- to a remote office used for video broadcast to check the jitter.
- between the core switches of two remote offices.

To locate this feature:

1. Go to **AMF Plus > Health Monitoring**
2. Click **Network Health**.
« The following widgets are visible: Health Trend, Latest, Probes, and History.
3. To add a probe, click **+ New Probe**



4. The **New Traffic Health Probe** window opens.
 - « Select the **Probe Type** - ICMP Echo or HTTP GET.
 - « Select a **Source** device - the drop down box lists all linkmon capable devices in the network.
 - « Type in a **Destination** - for ICMP echo probes, this is either an IP address or FQDN. For HTTP GET probes, this can only be an FQDN.
 - « Enter an **Interval** in seconds. For ICMP probes the default is 1 and for HTTP GET probes the default is 30.
 - « Set the **Thresholds** for packet loss, jitter, and latency.

The screenshot shows the 'New Traffic Health Probe' configuration window. It includes a 'Name' field, a 'Probe Type' selector (ICMP Echo(ping) is selected), a 'Source Device' dropdown, a 'Destination' field, an 'Interval(s)' field set to 1, and 'Link Health Thresholds' for Loss (1-2%), Jitter (15-30ms), and Latency (150-300ms). 'Cancel' and 'Save' buttons are at the bottom right.

For more information, see the [Vista Manager EX User Guide](#).

Health monitoring with third-party devices

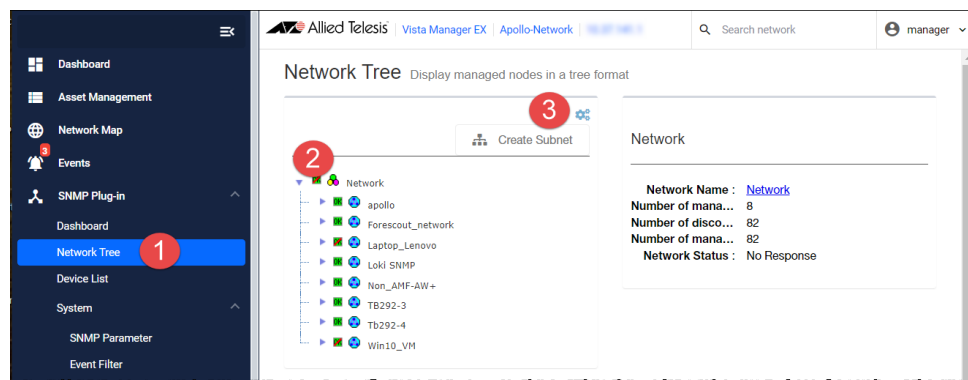
Applies to all Vista Manager EX installations

From version 3.11.0 onwards, you can use the existing Health Monitoring feature to monitor non-AMF third-party devices.

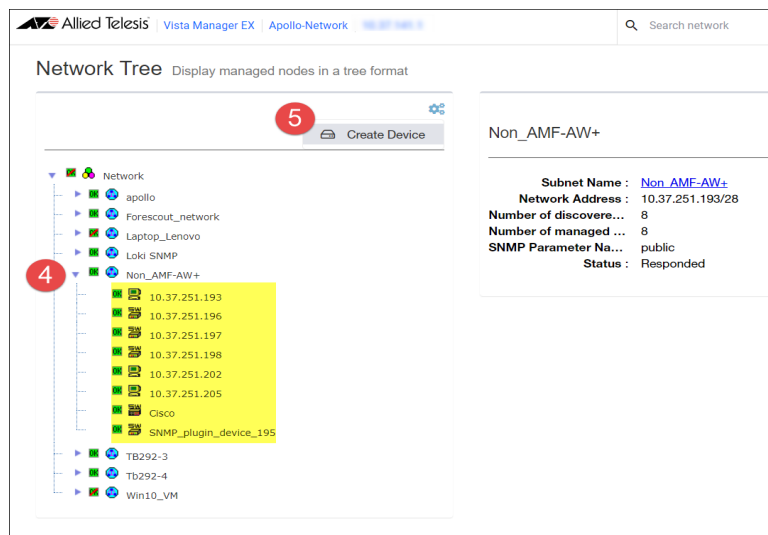
Previously only AMF devices were visible in **Health Monitoring**; now third-party devices can be seen as long as they are discovered via the SNMP plug-in and have the correct MIB.

To use this feature, make sure you have the SNMP Plug-in installed, then:

1. Go to **SNMP Plug-in > Network Tree**
2. Expand the network tree, to see existing subnets.
3. Create a subnet (if required).



4. Click on a subnet to see its devices.
5. To add more devices, click **Create Device**.



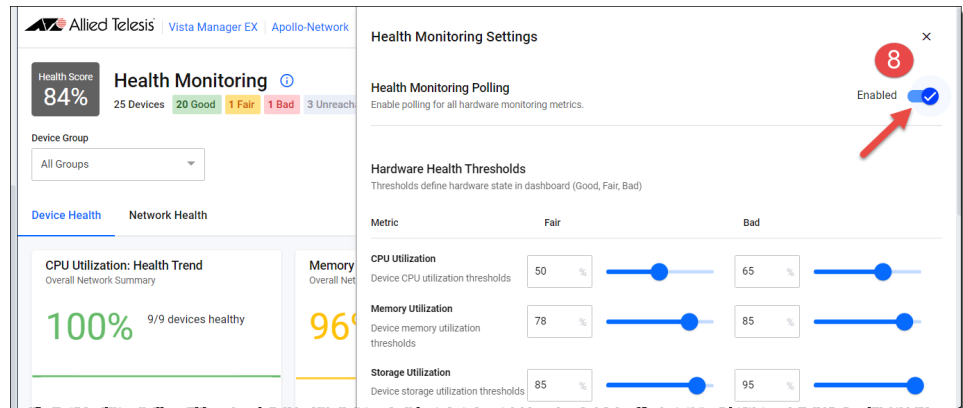
To see the third-party devices discovered by the SNMP plug-in on the network map:

6. Go to the **Network Map**.

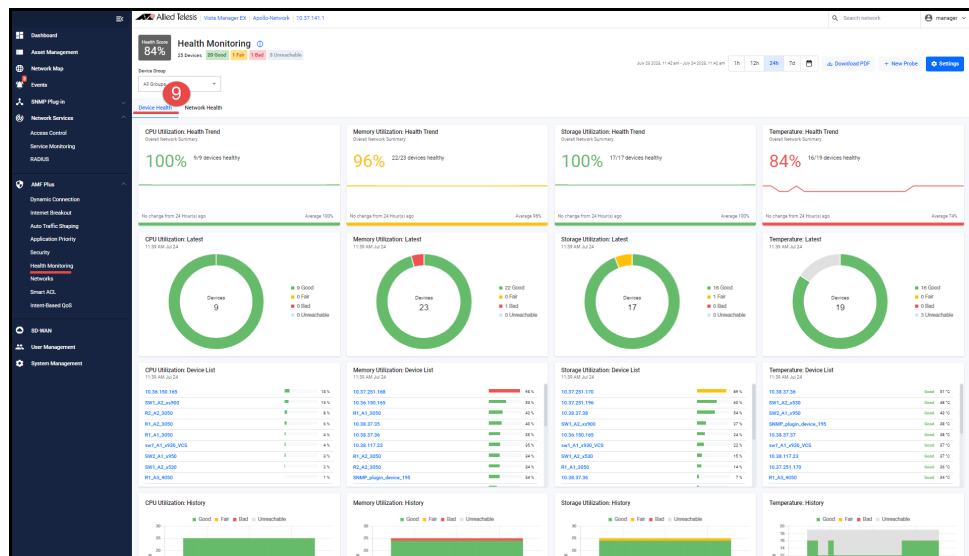
To monitor device health:

7. Go to **Health Monitoring > Settings**

8. **Enable** Health Monitor Polling (if it is disabled).



9. Use the **Device Health** tab to monitor your network devices.



Please note that you can only find third-party devices on the Health Monitoring dashboard if the correct MIB is supported on the third party device.

For more information, see the [Vista Manager EX User Guide](#).

Local RADIUS batch support

Applies to all Vista Manager EX installations

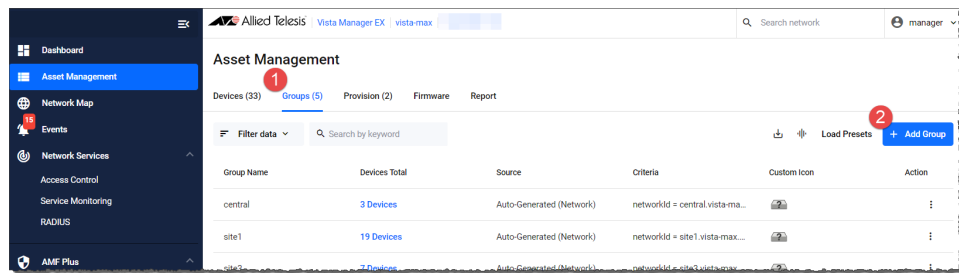
From version 3.11.0 onwards, you can manage common RADIUS Users/Groups/NAS on multiple devices easily.

Previously, you could manage individual devices, but each device needed to be configured one by one.

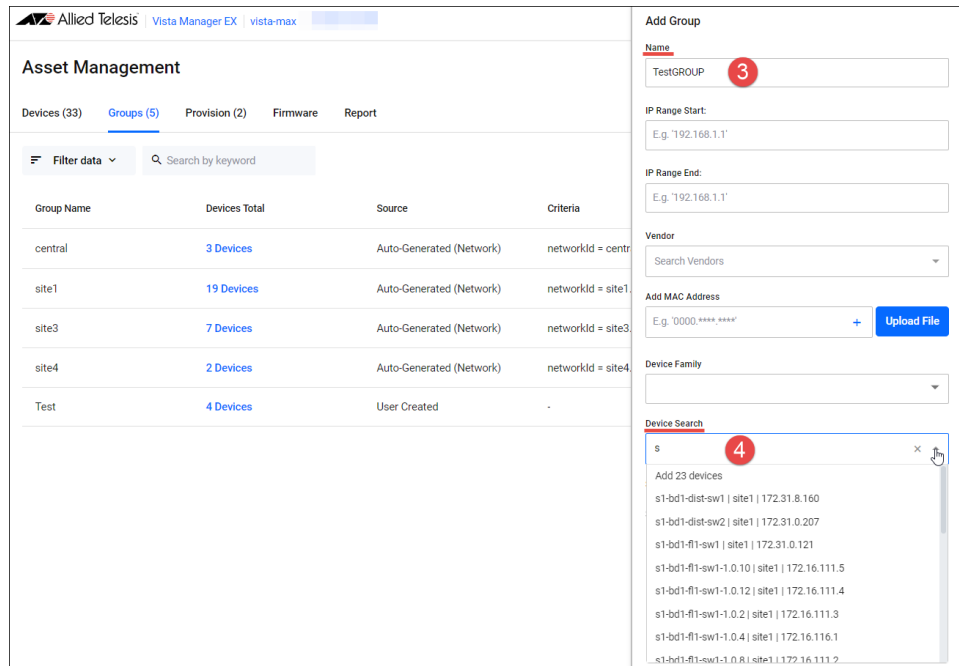
With this update, you can manage Vista grouped devices in the same way as is currently possible for a single device.

To use this feature:

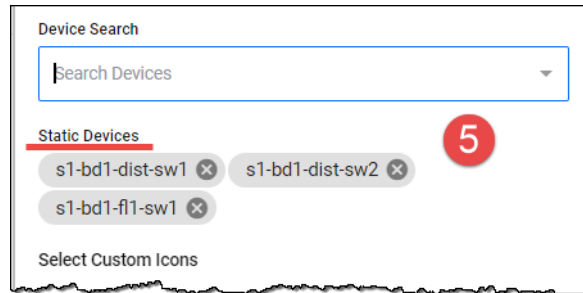
1. Go to **Asset Management > Groups**
2. Click **+Add Group**



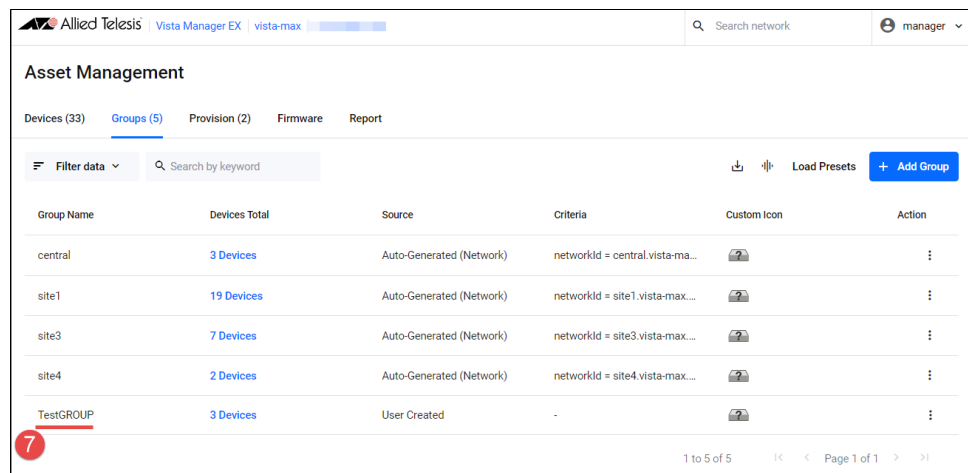
3. Enter a group **Name**.
4. In the **Device Search** field, start typing a device name. A drop-down list appears.



5. Select the devices you want for the group. Each device is added one-by-one to **Static Devices**



6. Click **Save**.
7. The Vista **Group** is now visible in the Asset Management window.



For detailed instructions on configuring Local RADIUS on devices and establishing Users and Groups, refer to the [Vista Manager EX User Guide](#).

Improved AMF Plus device discovery

Applies to all Vista Manager EX installations

Vista Manager's AMF Plus Device Discovery provides a more complete view of the network.

Together, Vista Manager EX 3.11.0 onward and AlliedWare Plus software version 5.5.3-1 support AMF Plus Device Discovery using the STOAT (Standardized Topology Organizer and Transport) discovery protocol. STOAT learns about network devices and their links, and Vista Manager EX, using its AMF Plus Device Discovery feature, can then access this information so they can be displayed on the network map.

Currently, the Vista Manager EX map provides a visual view of the network topology, however this view only includes AMF nodes, links, guest-nodes, guest links, stacked devices (those using Virtual Chassis Stacking), and WAN topologies.

Now, Vista Manager EX merges the data from existing discovery methods such as AMF, and AMF Plus Device Discovery, to provide a single, accurate, and more complete view of the network.

How does STOAT work?

STOAT is a protocol designed to gather topology information about networks. It standardizes the output of various discovery protocols into a common format and transports the resulting topology data to a central point for use by Vista Manager EX.

Using LLDP and DHCP Snooping, STOAT discovers and gathers information about devices in the local network. These devices may include IP cameras, IP phones, PCs, laptops, Wi-fi access points, printers, and so on. LLDP is limited to discovering devices directly connected to the STOAT device, however DHCP Snooping can discover devices one or more hops away.

Configuring a STOAT network

You need an AMF Plus license and AlliedWare Plus software version 5.5.3-1 to be able to use STOAT to discover devices and links on a network.

Then use the CLI to:

- Enable the STOAT service and STOAT discovery protocols
- Configure STOAT Collectors
- Configure STOAT Sources
- Enable LLDP on non-STOAT devices

Once this initial configuration is completed, VISTA Manager EX will check if STOAT is configured on the AMF network using the network IP address, then locate the root STOAT Collector to retrieve the STOAT topology from that device. Then you will see discovered devices and links displayed in the network map.

Licensing

An active AMF Plus license is required.

For more information, see the [Device Discovery using STOAT Feature Overview Guide](#).

Duplicate node manual merge tool

Applies to all Vista Manager EX installations

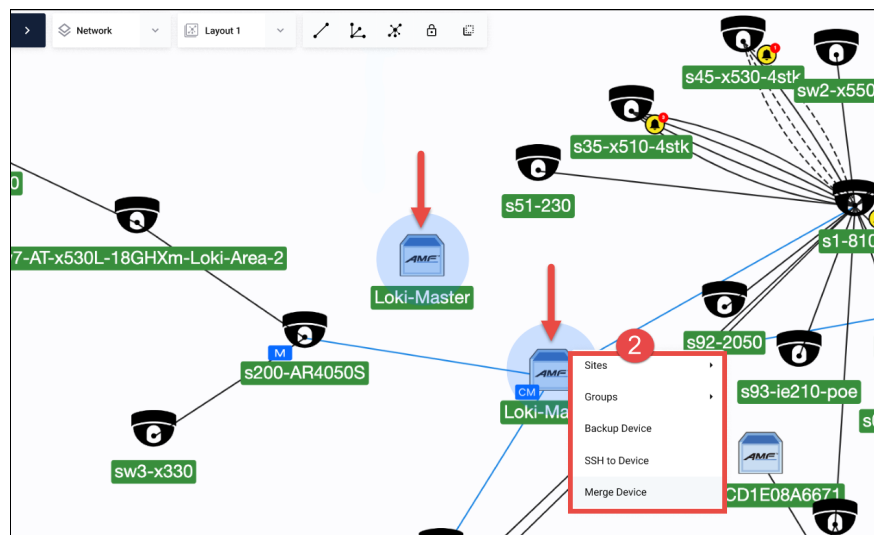
This enhancement is an extension to the STOAT (Standardized Topology Organizer and Transport) protocol.

In most cases Vista Manager EX with STOAT support is able to merge topology information including duplicate nodes. However, when Vista Manager EX can't automatically merge nodes together, this enhancement allows you to:

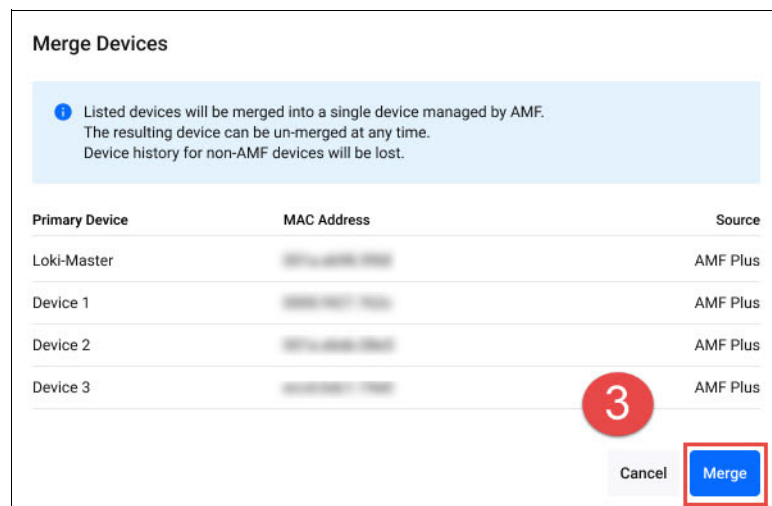
- manually merge duplicated nodes and have them appear as a single node
- un-merge nodes that have been manually merged
- see what nodes have been merged and where their information was obtained (source).

To merge devices:

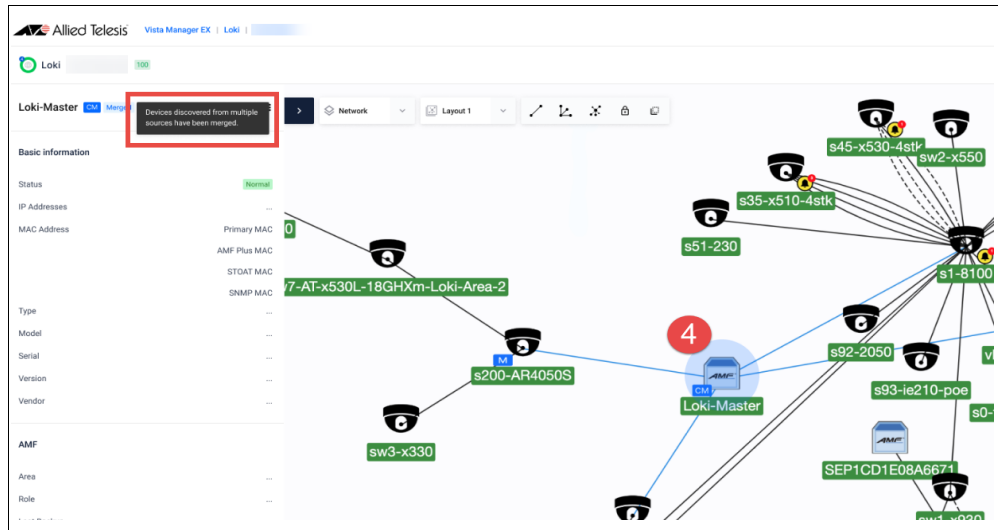
1. Go to the **Network Map**, and select the devices you want to merge.
2. Right click to see the context menu.



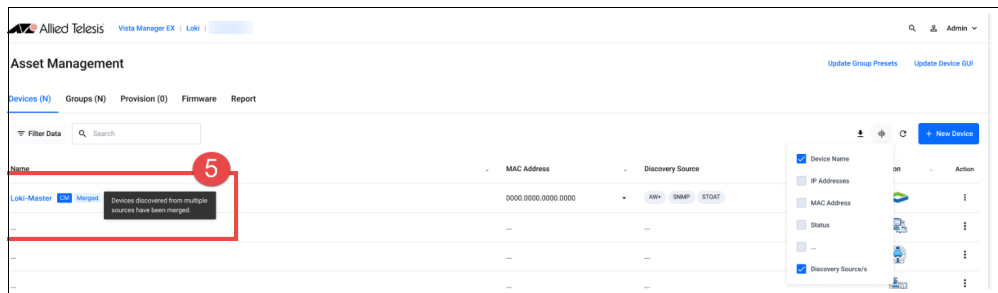
3. In the Merge Devices dialog, click **Merge**.



- The nodes are merged into one. You will see more details in the left side panel.

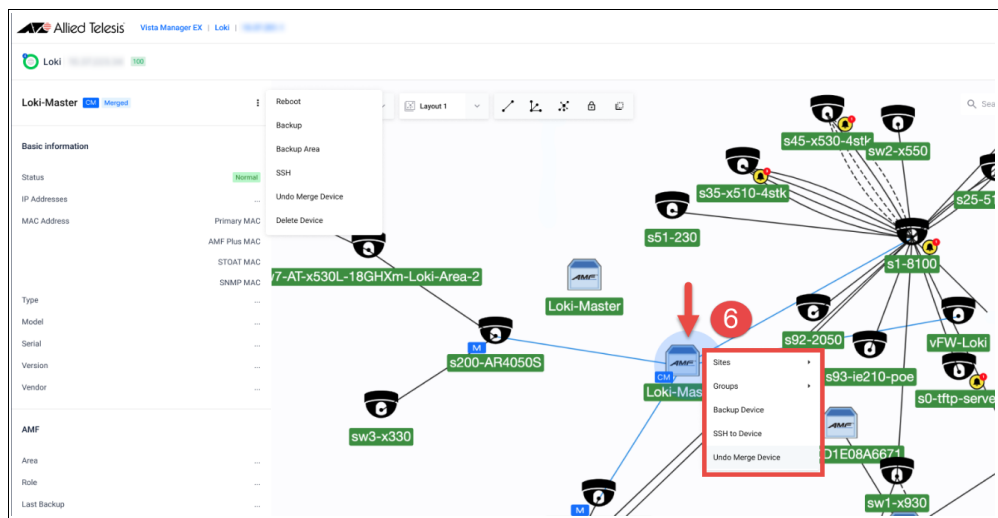


- In **Asset Management** you can see which nodes are merged at a glance with the 'Merged' badge.

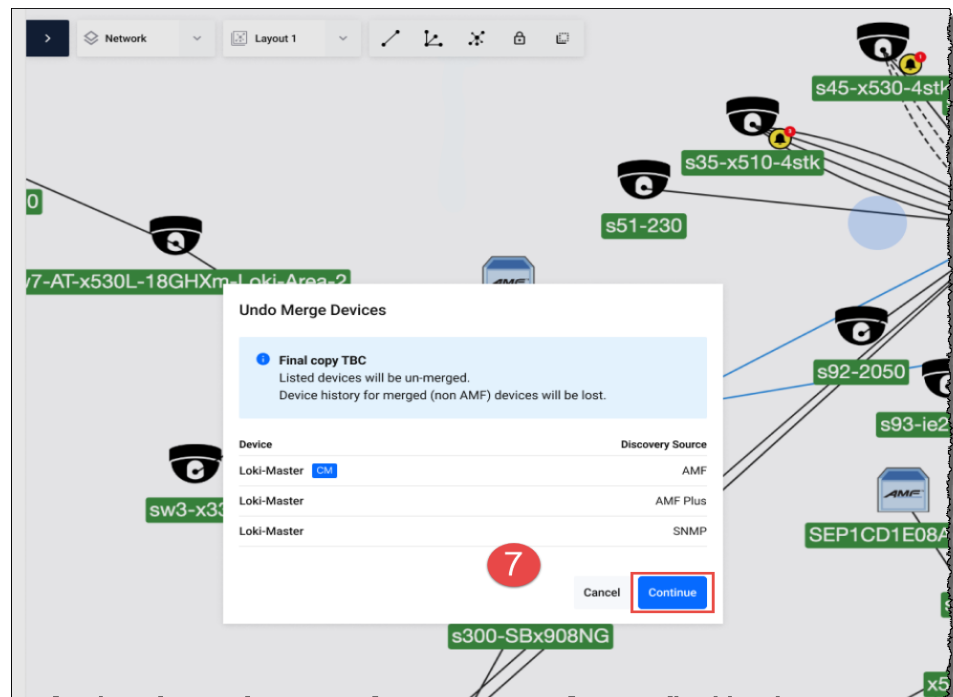


To un-merge devices:

- Go to the **Network Map**, select the merged device and right click to see the context menu. A similar merge dialog will appear showing the duplicates.



7. If you click **Continue**, then the nodes will be un-merged into their previous state.



For more information, see the [Device Discovery using STOAT Feature Overview Guide](#).

Autonomous queue threshold configuration and queue priority reassignment

Applies to all Vista Manager EX installations

From version 3.11.0 onwards, you can use the Autonomous Queue Configuration feature to dynamically adjust bandwidth allocation to prevent queue drops. This feature empowers you to automate QoS configuration changes across the network in response to changing traffic flows.

If any queue's number of egress drops exceeds the 'bad' monitoring thresholds, the Auto Queues Configuration feature will adjust the resource allocated to that queue.

To access this feature, go to:

AMF Plus > Intent-Based QoS > Settings > Auto Queue Configuration

You can choose how frequently you want the autonomous configuration to run. You can also provide upper and lower bounds for resources automatically allocated to each queue.

Each time the Auto Queue Configuration feature changes the QoS configuration, you will receive a message in the event log specifying which queues changed, their previous values, and their new values.

The screenshot displays the 'Intent-Based QoS Settings' window in the Vista Manager EX application. The 'Auto Queue Configuration' tab is highlighted with a red box. The interface is divided into several sections:

- Monitoring Thresholds:** Includes 'Auto Queue Configuration' (Enabled), 'Frequency' (5 minutes), and 'Reset Defaults'.
- Queue Configuration:**
 - 7 Voice:** Traffic requiring minimum loss, latency and jitter, such as VoIP Telephony. Current egress rate limit: 10%, Max egress rate limit: 13%.
 - 6 Video:** Traffic requiring low loss, latency and jitter, such as Videoconferencing. Current egress rate limit: 33%, Max egress rate limit: 33%.
 - WRR Queue:**
 - 5 Network Management:** Traffic protected with a minimum bandwidth guarantee such as SNMP, NTP and Syslog. Min weight 1-15: 4, Current weight (auto): 4, Max weight 1-15: 5.
 - 4 Streaming:** Highly interactive traffic, such as. Min weight 1-15: 6, Current weight (auto): 6, Max weight 1-15: 7.

Buttons for 'Cancel' and 'Save' are located at the bottom right of the settings window.

For more information, see the [Vista Manager EX User Guide](#).

Left-hand menu navigation improvement

Applies to all Vista Manager EX installations

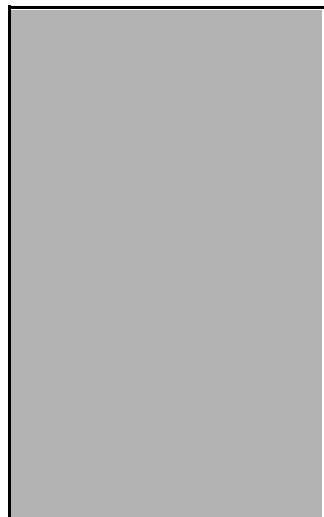
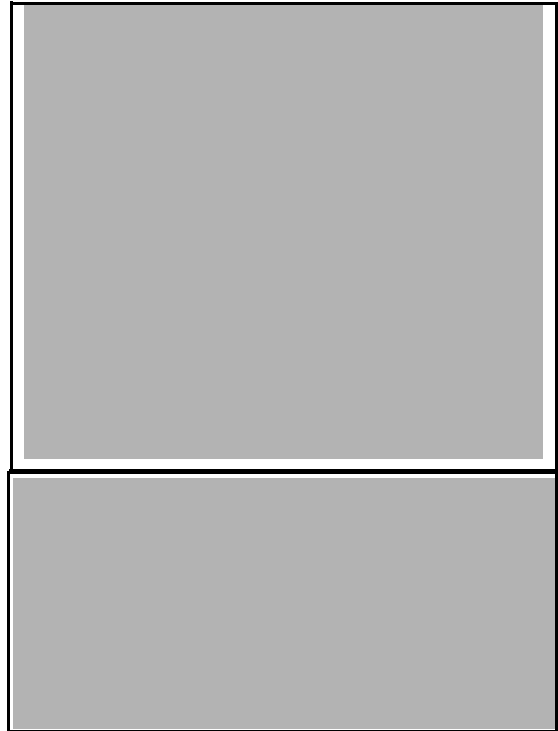
From version 3.11.0 onwards, the menu navigation has been improved.

When you log into your dashboard in Vista Manager EX, the left-hand menu will be opened automatically to display all of the menu items, provided your screen is larger than 1200px wide. The menu item that you have selected will appear in a light blue color.

The active page item's text and color formatting has also been updated to improve visibility.

Icons are provided for top level menu items.

When you mouse over an icon, a tooltip header is shown to show you what the menu item corresponds to. When you mouse over menu items with sub items, they are displayed and can be selected.



For smaller screens such as tablets or other touch devices, the menu will collapse to save screen space. You can reopen it by tapping on the hamburger menu icon.

For more information, see the [Vista Manager EX User Guide](#).

SD-WAN map displays custom icons

Applies to all Vista Manager EX installations

From version 3.11.0 onwards, you can see custom icons on the SD-WAN topology map.

In Vista Manager EX 3.10.3, custom icons would not display on the map. This has been restored in release 3.11.0.

Error notifications for exceeding user limits in RADIUS groups

Applies to all Vista Manager EX installations

From version 3.11.0 onwards, error messages will display when you exceed the limit of users in a RADIUS group. When you have multiple devices in a RADIUS group and try to add or import a user when the user limit has been met, an error message will display in the bottom right.

Depending on if the limited amount of users has been met, the notification will display as a success or a failure.

Vista Manager EX supports Windows Server 2022

Applies to the Windows installation of Vista Manager EX

From version 3.11.0 onwards, Vista EX now supports Microsoft's Windows Server 2022 operating system.

Vista Manager EX supported on VMware ESXi 7

Applies to the Windows installation of Vista Manager EX, not to VST-VRT

From version 3.11.0 onwards, Vista Manager EX is supported on vSphere's hypervisor VMware ESXi 7.

Vista Manager EX supported on VMware ESXi 8

Applies to the Windows installation of Vista Manager EX, not to VST-VRT

From version 3.11.0 onwards, Vista Manager EX is supported on vSphere's hypervisor VMware ESXi 8.

Vista Manager EX supports Nutanix AHV

Applies to the Windows installation of Vista Manager EX, not to VST-VRT

From version 3.11.0 onwards, Vista Manager EX supports Nutanix AHV.

Asset Management grouping enhancement

Applies to all Vista Manager EX installations.

From version 3.11.0 onwards, the Groups list on the **Asset Management** menu has been updated.

A **Load Presets** button has been added. You can click on this button to upload a preset file (ZIP or GZ file) with groups inside to import groups into Vista Manager EX. For more information about preset files and to see if one is available or required, contact your Allied Telesis sales representative.

Alongside this, a **Criteria** column has been added to the Groups list, so you can see the criteria for your named groups without needing to click each individual group to expand the information.



Both the Load Presets button and Criteria column are visible on the Asset Management page of Vista Manager EX.

For more information, see the Asset Management section of the [Vista Manager EX User Guide](#).

Backup running config available on AMF devices

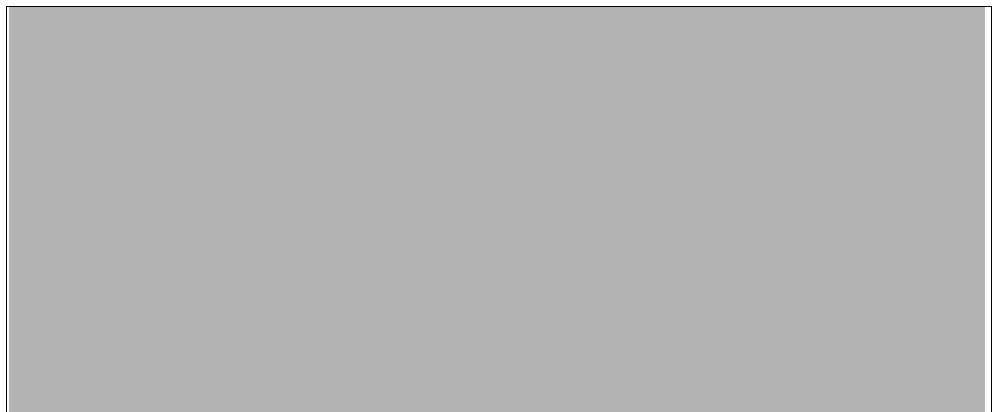
Applies to all Vista Manager EX installations

From version 3.11.0 onwards, you can back up the running configuration file from the **Asset Management** menu in the Vista Manager EX GUI.

You can:

- select the device name that you would like to backup
- click **Configs**.
- click **Backup Running** to backup the running configuration on your device.

A notification on the bottom left will confirm the backup was successful.



When you reload the page, the running backup will be displayed in the configuration backups list.

You can download it by clicking the **Action** menu (three dots icon).



For more information, see the Asset Management section of the [Vista Manager EX User Guide](#).

Tech Support log export customization

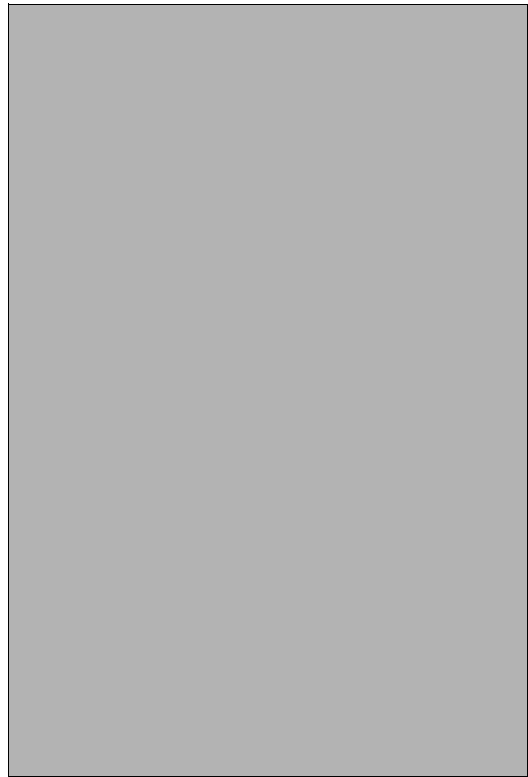
Applies to all Vista Manager EX installations

From version 3.11.0 onwards, Vista Manager EX admin users have more customization abilities for Tech Support log exports. Specifics can be enabled or disabled depending on the logs required.

You can include the following options when a Tech Support log is exported:

- diagnostic collection of all responses and requests from Vista Manager EX networking devices.
- nodeJS version json file
- mongo build info json file
- configuration json file

For more information, see the **System Management** sections of the [Vista Manager EX User Guide](#).



SNMP plug-in is enabled by default in AMF Plus networks

Applies to all Vista Manager EX installations

From version 3.11.0 onwards, the SNMP plug-in is enabled by default in an AMF Plus environment. You can now view information about devices that are discovered through the SNMP plug-in, without the requirement of an SNMP license.

These include:

- Memory usage
- CPU Usage
- Device Temperature
- Storage

To see this information, go to **AMF Plus > Health Monitoring**

Providing that all AMF Plus master and AMF Plus controller devices have an AMF Plus license, the features for the SNMP plug-in are made available in Vista Manager EX. This is disabled on AMF/AMF Plus mixed environments.

For more information, see the **Plugins** section of the [Vista Manager EX User Guide](#).

Feature permissions changes (including Sites and Groups permissions)

Applies to all Vista Manager EX installations

From version 3.11.0 onwards, the **User Management** page in Vista Manager EX has been updated to clarify user permissions.

When creating or editing a user profile, two new sections have been added:

- Feature Permissions
- Sites and Groups

The **Feature Permissions** section lets you choose the user's permission level for the **Service Monitoring** page of Vista Manager EX. You can choose to give the user read only or read/write access.

The **Sites and Groups** section has been updated to include auto-generated groups for topology networks discovered during initialization. This replaces the previous **Management Group** permissions, which listed all topology networks for permission purposes.

Vista Manager EX adds labels to groups that are auto-generated, to distinguish them from user-created groups. These features can be found on the **User Management** menu:



For more information, see the **Creating Groups and Sites** sections of the [Vista Manager EX User Guide](#).

AWC enhancements

Two-step Authentication with Captive Portal and MAC Access Control now supported on TQ6000 GEN2 series APs

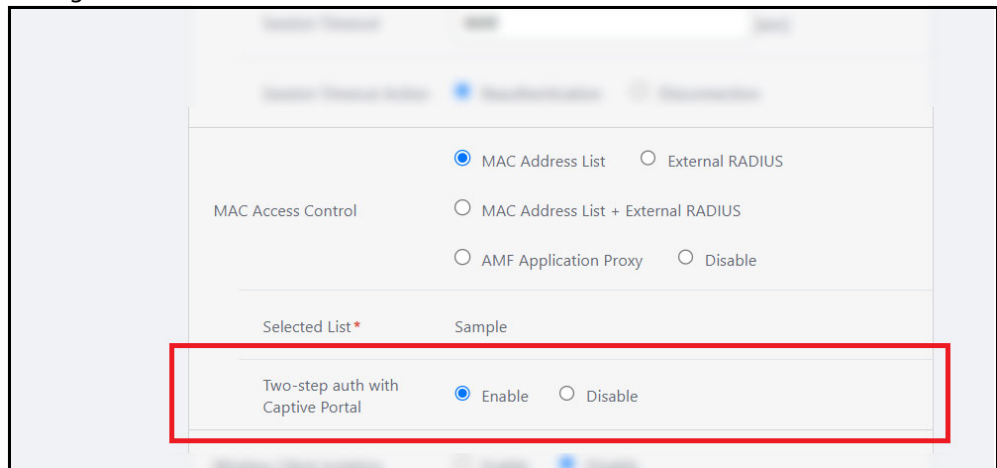
Applies to TQ6602 GEN2, TQ6702 GEN2, TQm6602 GEN2, and TQm6702 GEN2 on all Vista Manager EX installations that have the AWC plug-in

From version 3.11.0 onwards, Two-step authentication with Captive Portal is now supported on the TQ6602 GEN2, TQ6702 GEN2, TQm6602 GEN2, and TQm6702 GEN2 APs. Two-step Authentication with Captive Portal allows you to combine both Captive Portal and MAC Access Control.

The **Two-step auth with Captive Portal** option appears on AP and CB profile pages when you select any one of the following options in the MAC Access Control section on those pages:

- MAC Address List
- External RADIUS, or
- MAC Address List + External RADIUS
- AMF Application Proxy

You can find these settings in the VAP (Multiple SSID) Configuration section in Vista Manager EX:



This feature requires AP firmware version: 8.0.3-0.1 and later.

Wireless client isolation functionality has been extended

Applies to TQ6602 GEN2 and TQ6702 GEN2 on all Vista Manager EX installations that have the AWC plug-in.

From version 3.11.0 onwards, the Dual[11ax] GEN2 AP profile type supports Wireless Client Isolation.

You can configure wireless client isolation from the **Radio Configuration** settings page.

You can set Wireless Client Isolation to:

- Within AP
- Within VAP, or
- disabled (which is the default).

When enabled, it blocks all terminal-to-terminal communication between different APs, including between radios, without depending on the VLAN network settings.

The setting choice on the **VAP (Multiple SSID)** Configuration page depends on the Radio Configuration page:

If **Within AP** or **Within VAP** is set on the Radio Configuration page, then the settings will be shared with all VAPs in the same radio. The other options for Wireless Isolation on the VAP (Multiple SSID) page cannot be selected and are hidden.

If **Disabled** is set on the Radio Configuration page, the VAP (Multiple SSID) Configuration page will show this. Note that if you select Disabled, the Within AP and Within VAP settings on this page will still be visible and can be selected.

LED Color Support for APs

Applies to TQ6602 GEN2 and TQ6702 GEN2 on all Vista Manager EX installations that have the AWC plug-in.

From version 3.11.0 onwards, TQ6602 GEN2, and TQ6702 GEN2 APs with the Dual[11ax]GEN2 profile can now be configured to change LED color when powered over ethernet (PoE).

The LED setting is displayed on the edit page of the Dual[11ax]GEN2 profile under the Basic Configuration heading.

To change this, open the edit page of the Dual[11ax]GEN2 profile and:

- in the **Basic Configuration** section, select either 'turn on' or 'turn off'. The LED is set to on by default.
- in the PoE LED section, set the color to either amber or green.

This feature requires AP firmware version: 8.0.2-0.1 and later.

Secret Key byte number changed

Applies to TQ6602 GEN2 and TQ6702 GEN2 on all Vista Manager EX installations that have the AWC plug-in.

From version 3.11.0 onwards, the secret keys created in the CB Profile have been changed from 16 bytes to 32 bytes.

Note that if a previous version of the AWC Plug-in backup file is restored, the 16 bytes secret key is used.

This feature requires AP firmware version: 8.0.2-1.1 and later.

Wildcard character entry is now supported in the Walled Garden List

Applies to TQ6602 GEN2, TQ6702 GEN2, TQm6602 GEN2, and TQm6702 on all Vista Manager EX installations that have the AWC plug-in.

From version 3.11.0 onwards, you can now input a wildcard character per entry into the address field on the Walled Garden list on AP and Channel Blanket (CB) Profiles, which can be applied to APs with the respective profiles.

In the VAP (Multiple SSID) Configuration page, DNS Proxy for Walled Garden can be toggled on the AP and CB profile pages. It is displayed when Captive Portal is enabled. Wildcard characters are not supported in IP Addresses.

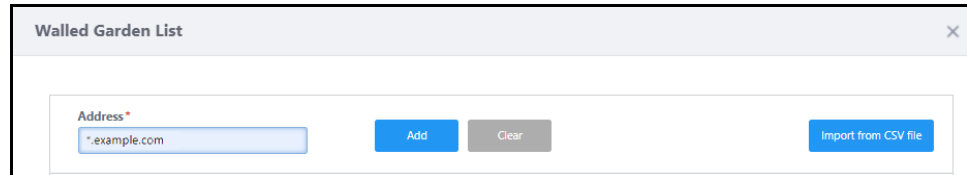
The DNS Proxy for Walled Garden is set to disabled as default, but it is automatically enabled when a wildcard character is entered in an address on the **Walled Garden List**. It is still enabled after all wildcard character entries in the list are deleted.

Target AP Profile types:

- Dual[11ax] GEN2 (for TQ6702 GEN2, TQm6702 GEN2, TQ6602 GEN2, TQm6602 GEN2)

Target CB Profile types:

- TQ6702 GEN2, TQ6602 GEN2 (for TQ6702 GEN2, TQ6602 GEN2)



WPA3, GCMP, and Management Frame Protection has been added to AWC-CB Settings

Applies to TQ6602 GEN2 and TQ6702 GEN2 on all Vista Manager EX installations that have the AWC plug-in.

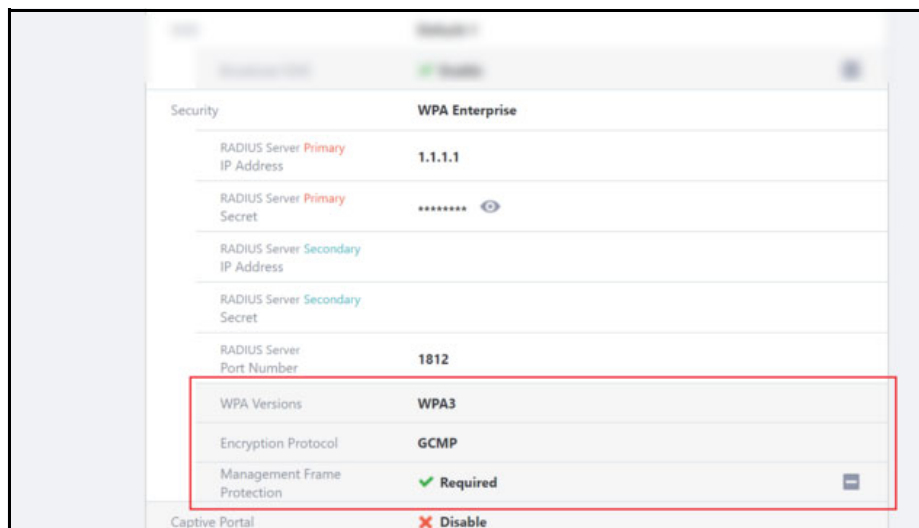
From version 3.11.0 onwards, the following can be added to the security section of the VAP (Multiple SSID) Configuration of Channel Blanket (CB) Profiles. AWC Channel blanket now supports the following functions for TQ6702 GEN2 and TQ6602 GEN2 in the CB Profile and edit page:

- WPA3 has been added to the list of WPA Versions selectable in the security section.
- GCMP has been added to the **Encryption Protocol** section in the security section. Note that it can only be selected with WPA Enterprise version WPA3.
- Management Frame Protection has been added in the security section. The displayed setting depends on the WPA version(s) that are selected.

Depending on the security settings selected, they will appear on the CB profile page.

The following settings can be applied in the AP profile alongside CB profile settings:

- MU-MIMO
- OFDMA

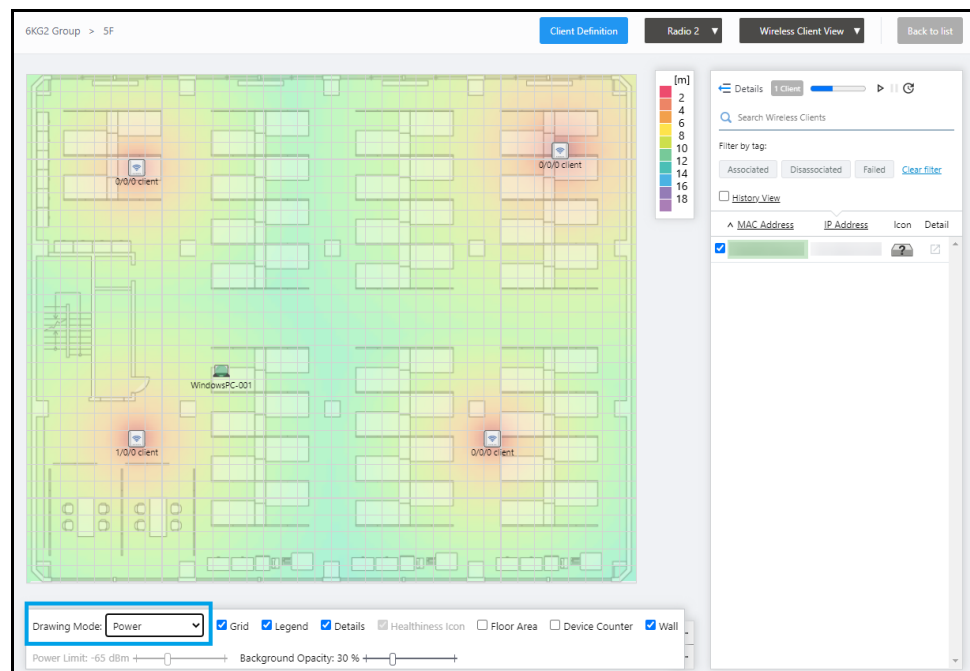


This feature requires AP firmware version: v8.0.3-0.1 and later.

Radio Clip has been added to floormaps

Applies to all Vista Manager EX installations that have the AWC plug-in.

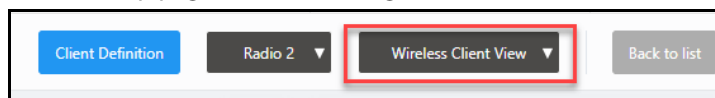
From version 3.11.0 onwards, a Radio Clip feature has been added to the AWC Plug-in. Radio Clip shows you the radio status of Wireless clients that are connected to APs as icons on the floormap's heatmap backgrounds when you are in **Wireless Client View**.



If you select a specific AP, only the wireless clients connected to that AP are displayed. In the list displaying connected clients, you can sort by MAC addresses and IP addresses.

If you don't select any APs, all wireless clients connected to all APs on the floor map are displayed and their radio status is shown.

To select **Wireless Client View**, select it from the **Wireless Status View** dropdown in the top right of the Floormap page in the AWC Plug-in menu.



This change helps to show client information about the radio status, for problem-solving purposes.

To change the drawing mode, select from the dropdown next to **Drawing Mode** on the bottom left of the Floormap page.

You can view client icons on the following floormap drawing modes when selecting Wireless Client View:

- Comfort Level
- Power
- Channel

Note that the heatmap background is not shown when "All Radios" is selected, or when "History View" is checked.

The RSSI level of client devices can be shown by hovering your mouse over a client icon on Wireless Client View while client location is estimated.

This feature requires the following firmware versions:

- TQ6702 GEN2 and TQ6602 GEN2 version 8.0.3-1.1 and later.
- TQ5403 and TQ5403e version 6.0.2-0.2
- TQ6602 version 7.0.1-3.1 and later.

TQ6000 GEN2 series support Smart Connect

Applies to TQ6602 GEN2 and TQ6702 GEN2 on all Vista Manager EX installations that have the AWC plug-in.

From version 3.11.0 onwards, the AWC Plug-in supports Smart Connect (AWC-SC) profile settings for the TQ6602 GEN2, and TQ6702 GEN2 (TQ6000 GEN2 series) models of APs.

See the [AWC Plug-in User Guide](#) for more information about Smart Connect.

This feature requires AP firmware version: v8.0.3-0.1 and later.

Passpoint is supported for TQ6000 GEN2 series, TQm6000 GEN2 series

Applies to TQ6602 GEN2, TQ6702 GEN2, TQm6602 GEN2, and TQm6702 GEN2 on all Vista Manager EX installations that have the AWC plug-in.

Version 3.11.0 onward now supports Passpoint for the TQ6000 GEN2 series and TQm6000 GEN2 series APs. Passpoint has also been updated for the TQ5000 and TQm5000 series.

Passpoint features have been updated on the following AP profiles:

- Dual[11ax] GEN2
- Tri[11ac Wave2]
- Tri[11ac Wave2] with External Antenna

Support for Passpoint was added to the TQ6702 GEN2, TQm6702 GEN2, TQ6602 GEN2, and TQm6602 GEN2.

On TQ5403, TQm5403, and TQ5403e, the following changes were made to the Passpoint implementation:

- **Internet Access** - You can enable or disable Internet Access. It is enabled by default.
- **HESSID** - It is set to 00:00:00:00:00:00 by default.
- **Roaming Consortium List** - optional for Dual[11ax] GEN2, required for both Tri[11ac Wave2] and Tri[11ac Wave2] with External Antenna.
- **EAP-AKA** - Added to the NAI Realm Information settings. You can select it from the EAP Method sub-sections.

This also applies to Passpoint on TQ6702 GEN2, TQm6702 GEN2, TQ6602 GEN2, and TQm6602 GEN2.

This feature requires the following firmware versions:

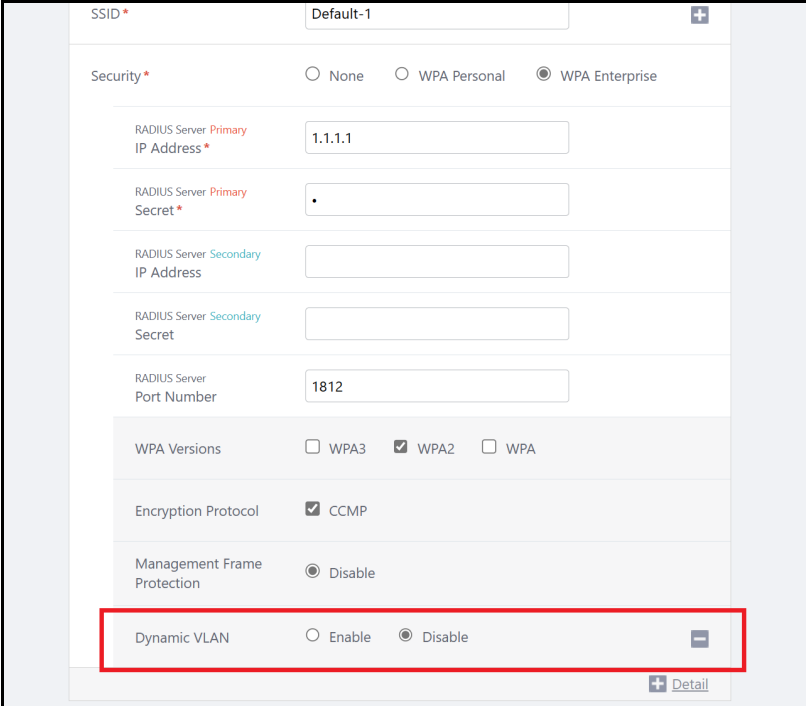
- TQ6702 GEN2 and TQ6602 GEN2 version 8.0.3-0.1 and later.

Dynamic VLAN is supported for TQ6000 GEN2 series Channel Blankets

Applies to TQ6602 GEN2 and TQ6702 GEN2 on all Vista Manager EX installations that have the AWC plug-in.

From version 3.11.0 onwards, you can now create Channel Blanket profiles with Dynamic VLAN, and apply these settings to TQ6602 GEN2 and TQ6702 GEN2 APs.

The Dynamic VLAN setting is displayed when WPA-Enterprise is selected in the **Security** section. It is located in the Security setting area in the VAP (Multiple SSID) Configuration section of the CB Profile settings page. It is set to disabled as default.



The screenshot shows the configuration page for a Channel Blanket profile. The SSID is set to 'Default-1'. Under the 'Security' section, 'WPA Enterprise' is selected. The RADIUS Server Primary IP Address is '1.1.1.1', and the RADIUS Server Primary Secret is masked with a dot. The RADIUS Server Secondary IP Address and Secret are empty. The RADIUS Server Port Number is '1812'. Under 'WPA Versions', 'WPA2' is checked. Under 'Encryption Protocol', 'CCMP' is checked. Under 'Management Frame Protection', 'Disable' is selected. At the bottom, the 'Dynamic VLAN' setting is highlighted with a red box and is set to 'Disable'.

This feature requires AP firmware version 8.0.3-0.1 and later.

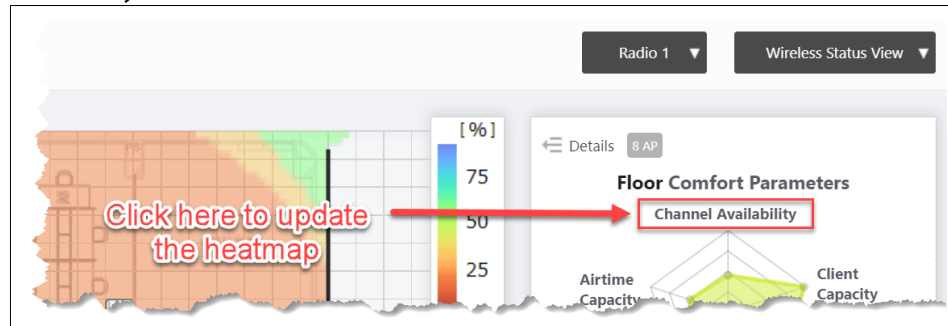
Storing functionality for Wireless Comfort Level Heatmap data on AWC-VAS

Applies to installations that include AWC-VAS

From version 3.11.0 onwards, comfort level heatmap history and data can be saved and displayed using AWC-VAS (Virtual Application Storage). AWC-VAS can display floor map, heatmap, and associated client history. AWC can download data from a range that you can select from an external VAS (a Vista Manager EX Network Appliance (VST-APL) configured as VAS).

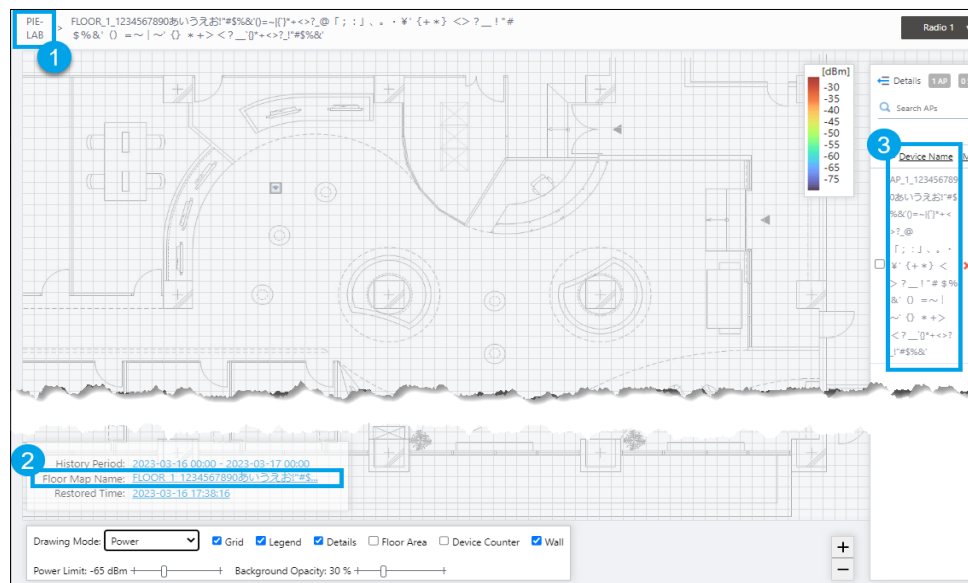
In Wireless Status View, **Comfort Level** is automatically displayed, and displays the comfort level heatmap. Comfort level is displayed as default.

If you click the **Channel Availability** text on the Floor Comfort Parameters section of the details panel, the label will change to a disabled color and the heatmap will update automatically.



The floormap display includes the following changes:

1. **The management group name** - in the top left next to the full floormap name.
2. **The floormap name** - appears in the VAS history box. If it is over 33 characters it will be cut off.
3. **The configured AP name** - appears in the display menu



Updates to AWC Channel Blanket

Applies to all Vista Manager EX installations that have the AWC plug-in.

From version 3.11.0 onwards, changes have been made to various Channel Blanket window titles, and a **Suggestion of Interference Reduction** check-box has been added in the Divide Channel Blanket popup window. Suggestion of Interference Reduction is checked by default.

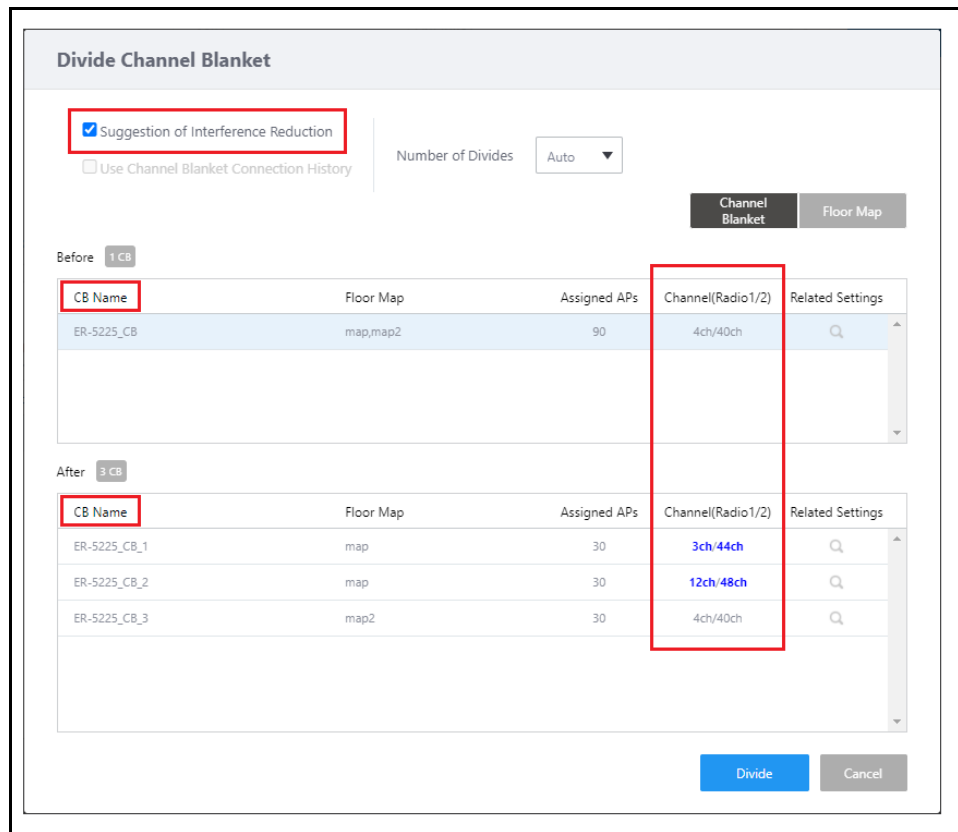
The following changes have been made to the following Channel Blanket headings:

- Divide Channel Blanket window: CB Name
- Create Channel Blanket and Edit Channel Blanket popup: CB Name
- Channel Blanket List: CB Name

Channel(Radio1/2) is now viewable on the Channel Blanket list and Divide Channel Blanket popup window.

If you add or delete a radio interface before saving the Channel Blanket, you will not be able to Divide the Channel Blanket before you save the profile. Hovering over the Divide button will show you a tooltip message.

When **Suggestion of Interference Reduction** is checked, Vista Manager EX suggests the optimal channels for each divided channel blanket. These suggested channels are highlighted in blue.



This function is supported on the following devices:

- TQ5403 and TQ5403e version 6.0.2-0.2 and later
- TQ6602 version 7.0.1-2.3 and later
- TQ6602 GEN2 and TQ6702 GEN2 version 8.0.2-1.1 and later

Floormap loading screen has been updated

Applies to all Vista Manager EX installations that have the AWC plug-in.

From version 3.11.0 onwards, the loading screen has been updated for multiple pages where Vista Manager EX draws floormaps or heatmaps. These changes are reflected on the following pages:

- Wireless Monitoring: Floormap and Floormap History
- Remote Monitor: Remote Vista Manager mini list
- Wireless Concierge: Floormap

When you click on a floor map, the loading screen has been darkened to show that the floormap is loading, and/or the heatmap is being generated.

WPA enterprise supports WPA2/WPA3 transition mode for TQ6000 GEN2 series

Applies to TQ6602 GEN2 and TQ6702 GEN2 on all Vista Manager EX installations that have the AWC plug-in.

From version 3.11.0 onwards, WPA enterprise supports WPA2/WPA3 Transition mode for TQ6602 GEN2, and TQ6702 GEN2 (TQ6000 GEN2 series) APs.

This allows clients with older devices with WPA2 to connect to the network while it runs WPA3.

This feature requires TQ6702 GEN2/TQ6602 GEN2: v8.0.3-0.1 and later.

AWC-SDF supports TQ6000 GEN2 and TQm6000 series

Applies to TQ6602 GEN2, TQ6702 GEN2, TQm6602 GEN2, and TQm6702 GEN2 on all Vista Manager EX installations that include AWC-SDF.

From version 3.11.0 onwards, Sky Defender (AWC-SDF) now supports TQ6000 GEN2 and TQm6000 GEN2 Series of APs.

This feature requires firmware version 8.0.3-0.1 or later.

AWC Plug-in supports TQ6702e GEN2

Applies to TQ6702e GEN2 on all Vista Manager EX installations that have the AWC plug-in.

From version 3.11.0 onwards, AWC supports the TQ6702e GEN2.

This feature requires firmware version 9.0.3-0.1.

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.

Older events may be automatically deleted when upgrading to 3.11.1 or later

When you update your Vista Manager EX installation to version 3.11.1 or later, Vista Manager EX will only keep the 5 million most recent event messages. If Vista Manager EX has more than 5 million events, older events will be deleted, to reduce the number of events to 5 million.

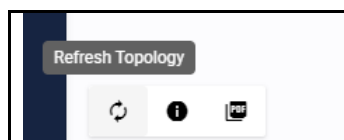
If you do not wish to lose the older events, archive them before you upgrade.

Manual polling recommended if upgrading to 3.11.0 or later

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 plug-ins

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

Fiber monitoring feature permissions

Note that on a **new** installation of Vista Manager EX 3.11.0 onwards, you will need to enable Fiber monitoring permissions for users. This can be done on the User Management page.

Disabling Internet Breakout disables all PBR rules

Internet Breakout uses policy-based routing (PBR) rules. When you use Vista Manager EX to disable Internet Breakout, it disables all PBR rules, including:

- rules created by SDWAN, and
- rules created by Internet Breakout, and
- rules created manually through the CLI.

Integrated map won't display some links from early firmware versions

If you are running some older versions of AlliedWare Plus, the links will not be displayed on the integrated map. Any device running AlliedWare Plus version 5.4.5 or earlier will not have its links shown on the map.

In addition, links from first-generation SBx908 and x200 devices will not be shown on the integrated map.

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](http://www.alliedtelesis.com).

AMF documentation

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

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

Upgrading Vista Manager as a Windows-based installation

Windows-based Vista Manager has optional plug-ins. These can be upgraded at the same time as Vista Manager EX.

Obtain the executable files

1. Download Vista Manager EX from the [Allied Telesis download center](#). If you are going to install the AWC and/or SNMP plug-ins then download these files from the same location.
 - The Vista Manager EX installation executable is named 'atvmexXXXbXXw.exe', with the Xs denoting the version and build numbers.
 - The AWC plug-in is called 'atawcXXXbXXw.exe'.
 - The SNMP plug-in is called 'atsnmpXXXbXXw.exe'.

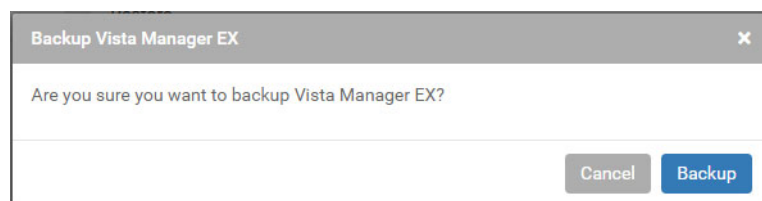
Do not rename these files. The installation requires them to be in this format.

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

Backup Vista Manager EX and the plug-ins

Backup Vista Manager EX

3. Log on to your Vista Manager EX and select the System Management page.
4. Click on the Backup button in the Database Management Pane.
5. Click Backup again to confirm you wish to make a backup.



This automatically downloads a **tar** file backup to your default download location.

Backup the SNMP plug-in

6. If you have the SNMP plug-in installed then log on locally to the Vista Manager EX server.
7. Stop the SNMP server services using the shortcut or by running the following command line.
"<Vista Install Path>\Plugins\AT-SNMP\NetManager\bin\svr cmd.bat" svrstop
8. Run the backup utility by using the shortcut or by running the following command line.

"<Vista Install Path>\Plugins\AT-SNMP\NetManager\bin\SMBackup.exe"

Follow the instructions on the screen.

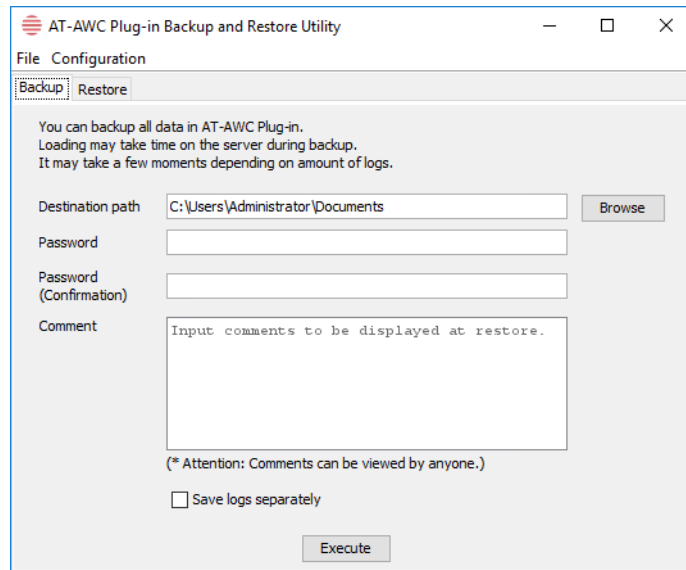
Backup the AWC plug-in

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

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

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

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



12. Select the backup tab and follow the instructions on the screen.

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

Uninstall the existing version

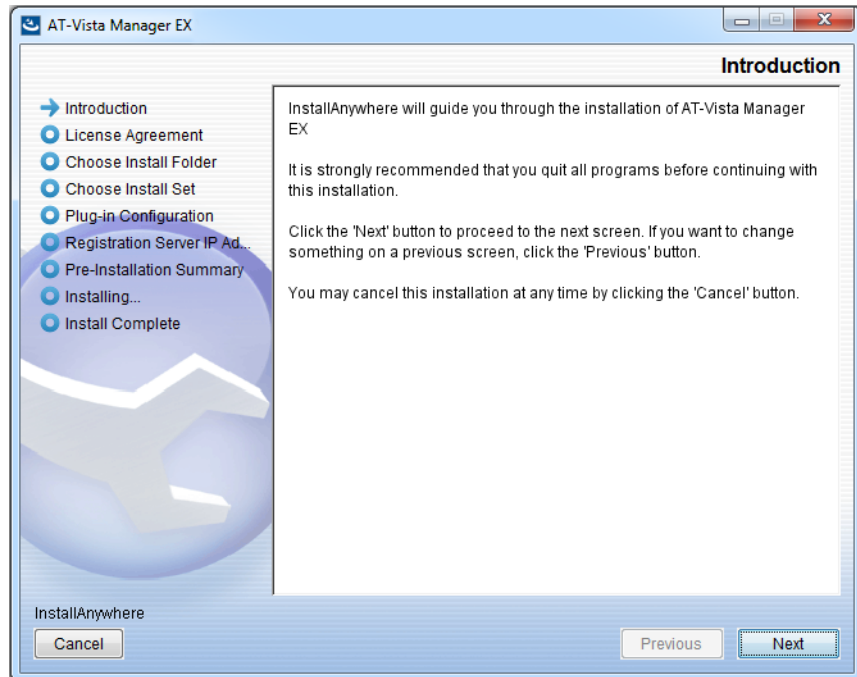
13. Log on as the same user as when installing.
14. Stop the server. Select **AT-Vista Manager EX** and then **AT-Vista Manager EX - Stop Server** from the Windows menu.
15. From the Windows menu, select **AT-Vista Manager EX** then **AT-Vista Manager EX - Uninstall**.
16. The AT-Vista Manager EX uninstaller starts.
17. Click the **Uninstall** button to uninstall.
18. If a dialogue box prompting you to restart the system is displayed, select **Restart the system** or **Restart later** and click the **Finish** button.
19. Delete the installation folder. The default installation folder is:
C:\Program Files (x86)\Allied Telesis\AT-Vista Manager EX
20. Reboot the system.

Install the new version

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

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

22. The **Introduction** dialog displays:



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

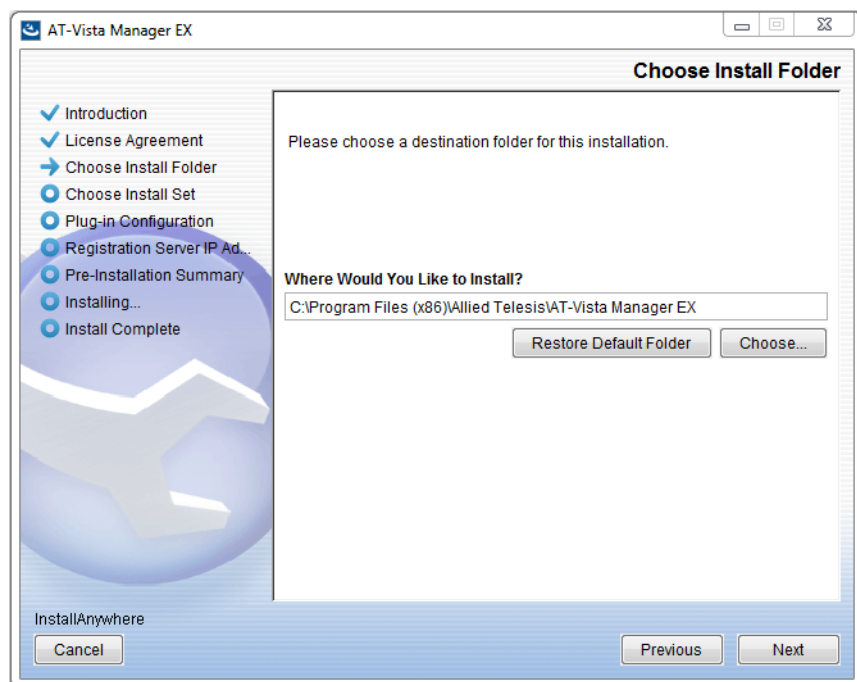
23. The **License Agreement** dialog displays:



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

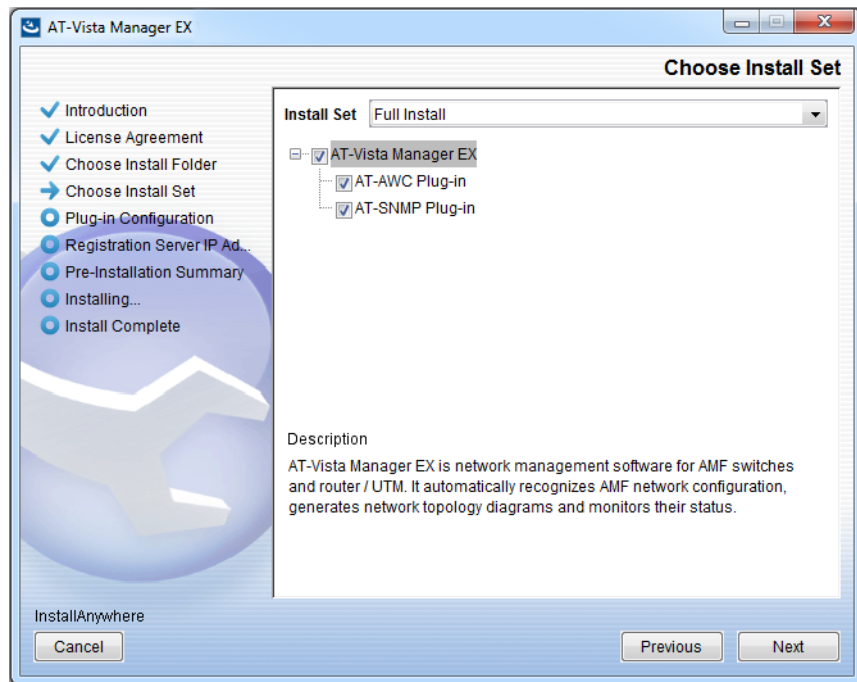
- Click **I accept the terms of the License Agreement**
- Click **Next**

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



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

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



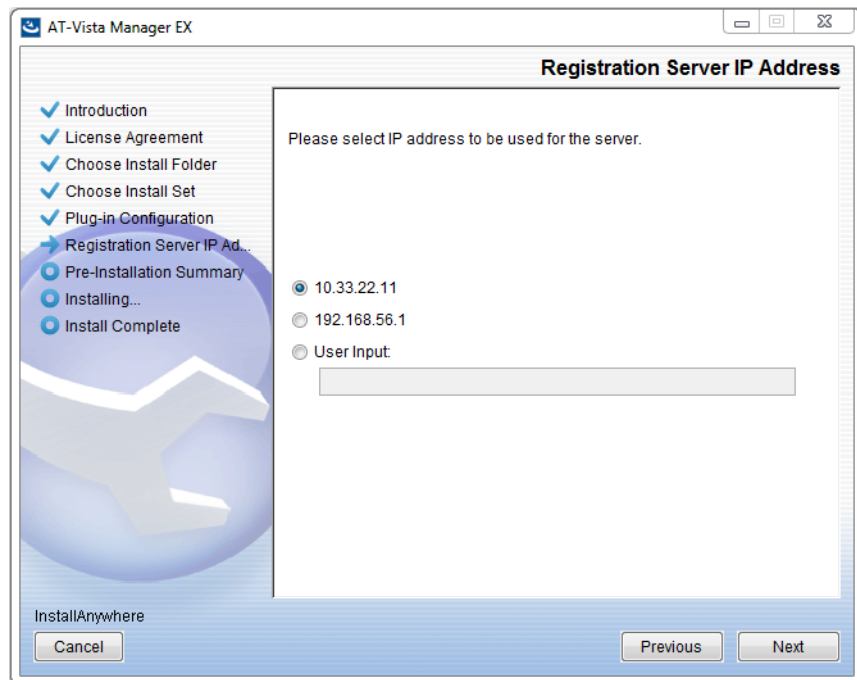
Select **Full Install** from the drop down list. By default all plug-ins are selected. Clear the check box for any plug-ins you do not wish to install. Click **Next**.

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



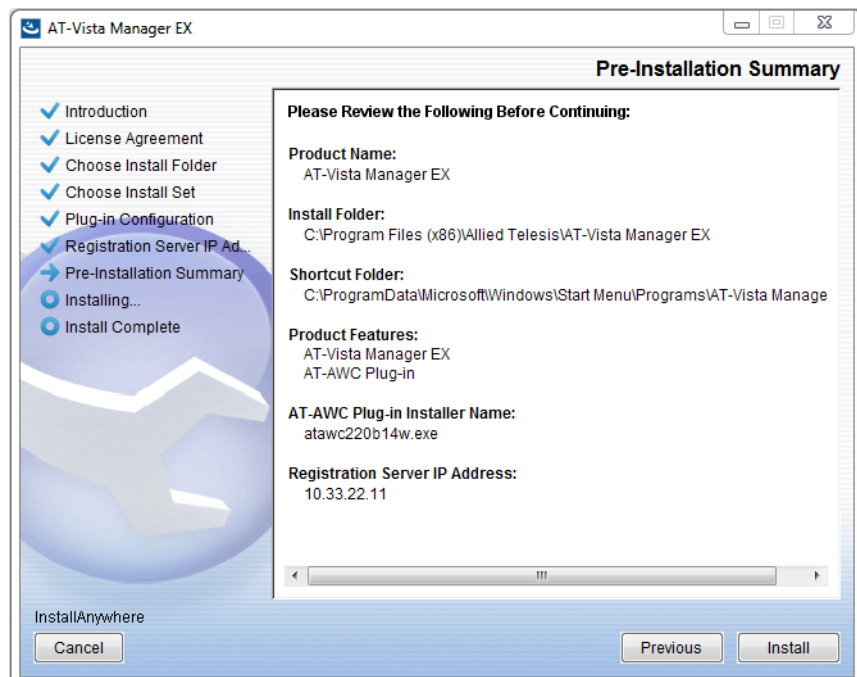
Select **Do not create a public key** unless you are intending to use the plug-ins in standalone mode. For more information on standalone mode, refer to the Installation Guide. Click **Next**.

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



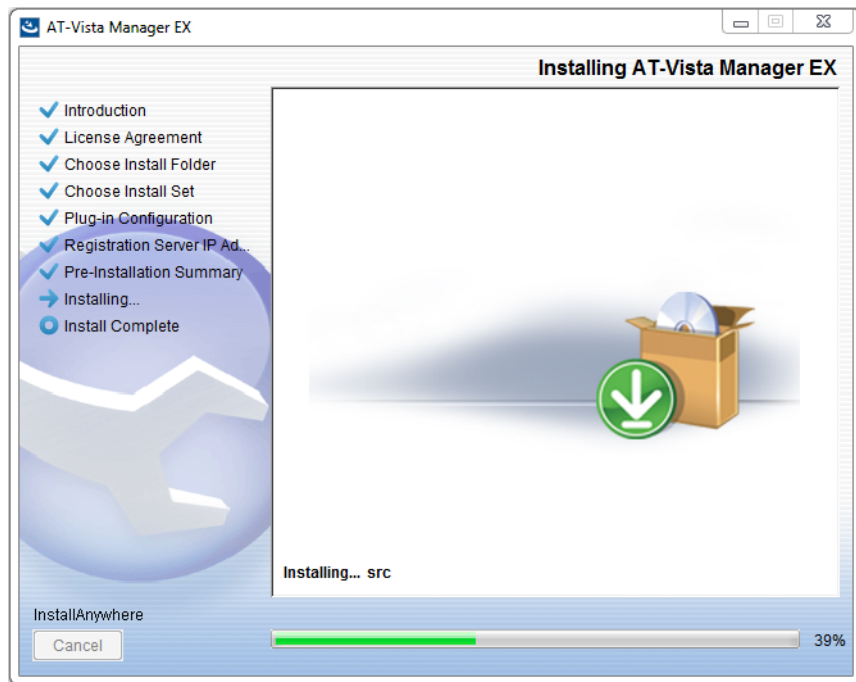
Either select from the list of IP addresses already configured on the Windows machine, or input a valid IP address. Click **Next**.

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

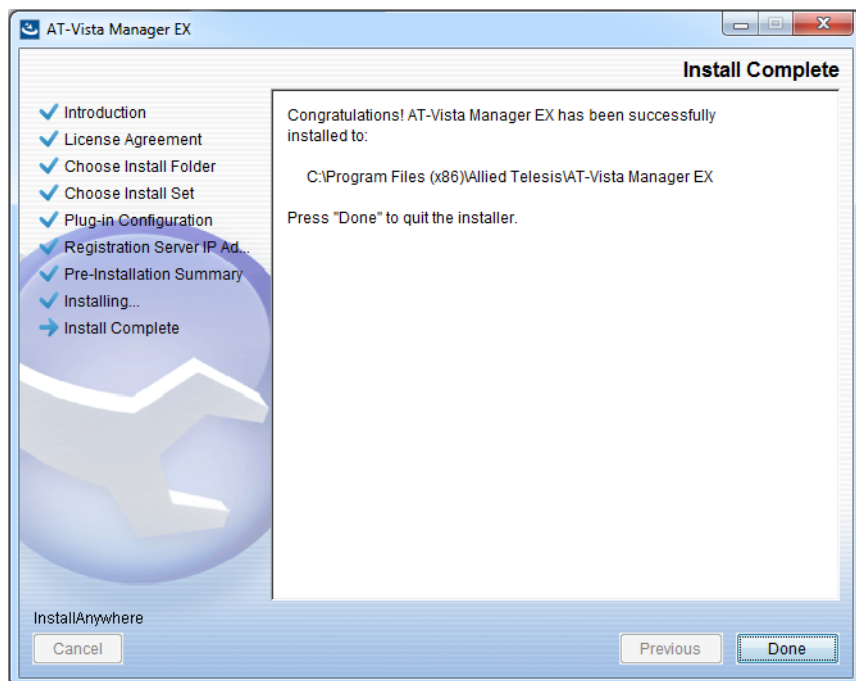


Check that your Product Name, Install Folder, Shortcut Folder, Product Features, Plug-in Installer Name and Registration IP Address are correct, and then click **Install**.

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



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

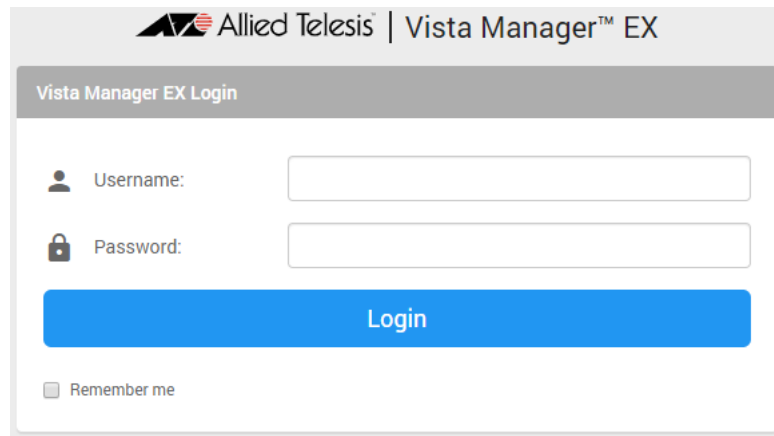


Check that the installation has completed successfully and click **Done**.

Restore the Vista Manager database

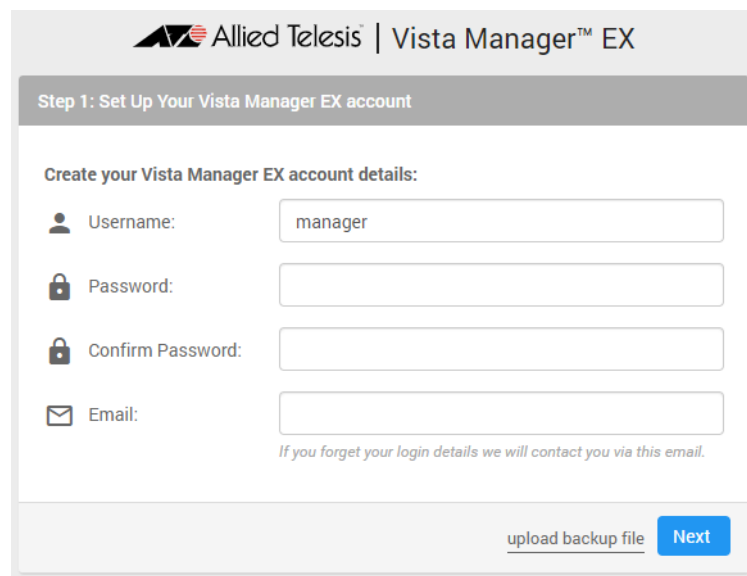
After the upgrade is complete, you need to restore the Vista Manager database. To do this, use the following procedure.

31. Login to Vista Manager.



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

32. Click on upload backup file.

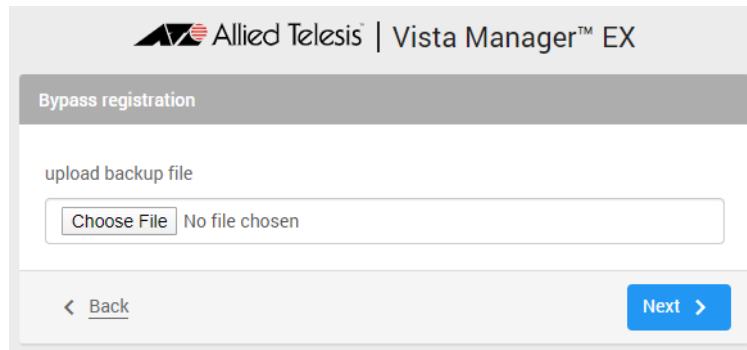


Caution Your serial number and license information are part of your database backup. If you upload the backup file when upgrading, you will keep the same serial number, and your licensing will continue to work without interruption.

However, if you configure a new instance of Vista Manager EX, without uploading your backup, a new serial number will be generated, and your existing licensing will no longer work. You will need to contact Allied Telesis support to generate a new license.

Therefore, it is **STRONGLY** recommended that you upload your database backup to ensure your licensing keeps working.

33. Select the database backup to upload. Click on Choose File, and browse to your Vista Manager database backup. Click Next. The Vista Manager database will be restored.



Restore the SNMP plug-in

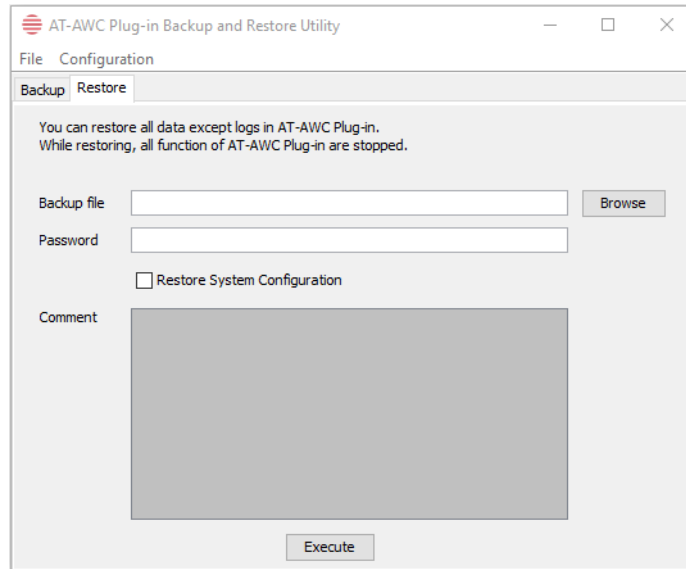
34. If you have the SNMP plug-in installed then log on locally to the Vista Manager EX server.
35. Stop the SNMP server services using the shortcut or by running the following command line.
"<Vista Install Path>\Plugins\AT-SNMP\NetManager\bin\svrcmd.bat" svrstop
36. Run the restore utility by using the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

Restore the AWC plug-in

37. If you have the AWC plug-in installed then log on locally to the Vista Manager EX server.
38. Stop the AWC server services using the shortcut or by running the following command line.
"<Vista Install Path>\Plugins\AT-AWC\root\stopserver.bat"
39. Run the backup/restore utility by using the shortcut or running the following command line.
"<Vista Install Path>\Plugins\AT-AWC\tools\maintenance\maintenance.bat"

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

Note: By default, restoring the AWC database will not restore the system configuration. You can restore the system configuration by checking the Restore System Configuration checkbox in the backup/restore utility.



We recommend that you check the Restore System Configuration checkbox, as it will allow you to restore the following system configuration settings:

- Database Settings
 - « Maximum Memory Usage
- Data Retention Period Settings
 - « Associated Client History
 - « Client Location Estimation History
 - « IDS Report History
- Network Map Settings
 - « Wireless Client Update-Interval
- Client Location Estimation History data

The system configuration contains settings that are tailored to the machine that created the backup. If you are restoring the backup on a different machine, particularly if that machine has a lower specification, it is recommended not to restore the system configuration.

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

Upgrading Vista Manager on VST-APL

See the [Vista Manager Network Appliance \(VST-APL\) 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](#).