Allied Telesis™

Release Note for Vista Manager EX Software Version 3.10.x

VISTA MANAGER™ EX

» 3.10.1 » 3.10.3

Acknowledgments

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.

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 v3.10.3

Introduction

This release note describes the new features in Vista Manager EX™ v3.10.3. 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 3.10.3, it includes:

- "New AWC Plug-in functionalities and settings" on page 5.

New AWC Plug-in functionalities and settings

Client isolation per VAP support

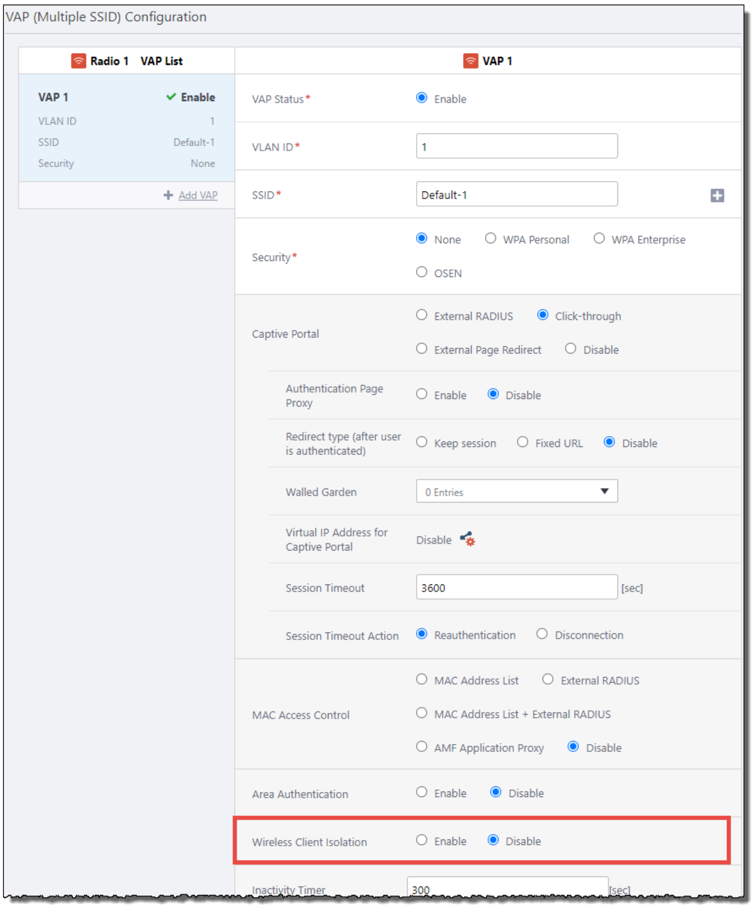
Applicable to all Vista Manager EX installations with the AWC plug-in: Access Points TQ5403, TQm5403, TQ5403e

From Vista Manager EX version 3.10.3 onwards, you can configure wireless client isolation for each VAP on TQ5403 devices.

Enabling this feature prevents devices connected to the same VAP from communicating with each other, thus effectively isolating them. This feature is often utilized in public or guest Wi-Fi networks to safeguard the privacy and security of individual users. Client isolation per VAP serves to block unauthorized access to other devices on the same network and also assists in preventing the spread of malware or other malicious activities among devices.

To configure the **Wireless Client Isolation** feature, go to:

- **Wireless Configuration** > **AP Profile** > **VAP** Configuration on Profile Edit and Profile Detail pages:



VAP (Multiple SSID) Configuration

Radio 1 VAP List

VAP 1 ✓ Enable

VLAN ID	1
SSID	Default-1
Security	None

+ Add VAP

VAP 1

VAP Status*	● Enable
VLAN ID*	1
SSID*	Default-1
Security*	● None ○ WPA Personal ○ WPA Enterprise ○ OSEN
Captive Portal	○ External RADIUS ● Click-through ○ External Page Redirect ○ Disable
Authentication Page Proxy	○ Enable ● Disable
Redirect type (after user is authenticated)	○ Keep session ○ Fixed URL ● Disable
Walled Garden	0 Entries
Virtual IP Address for Captive Portal	Disable
Session Timeout	3600 [sec]
Session Timeout Action	● Reauthentication ○ Disconnection
MAC Access Control	○ MAC Address List ○ External RADIUS ○ MAC Address List + External RADIUS ○ AMF Application Proxy ● Disable
Area Authentication	○ Enable ● Disable
Wireless Client Isolation	○ Enable ● Disable
Inactivity Timer	300 [sec]

This feature requires AP firmware versions:

- TQ5403: v6.0.3-0.1or later

Support for Redirect-URL in AMF Security

Applicable to all Vista Manager EX installations with the AWC plug-in: Access Points TQ5403, TQm5403, TQ5403e

From Vista Manager EX version 3.10.3 onwards, you can configure the Redirect URL feature on TQ5403 devices.

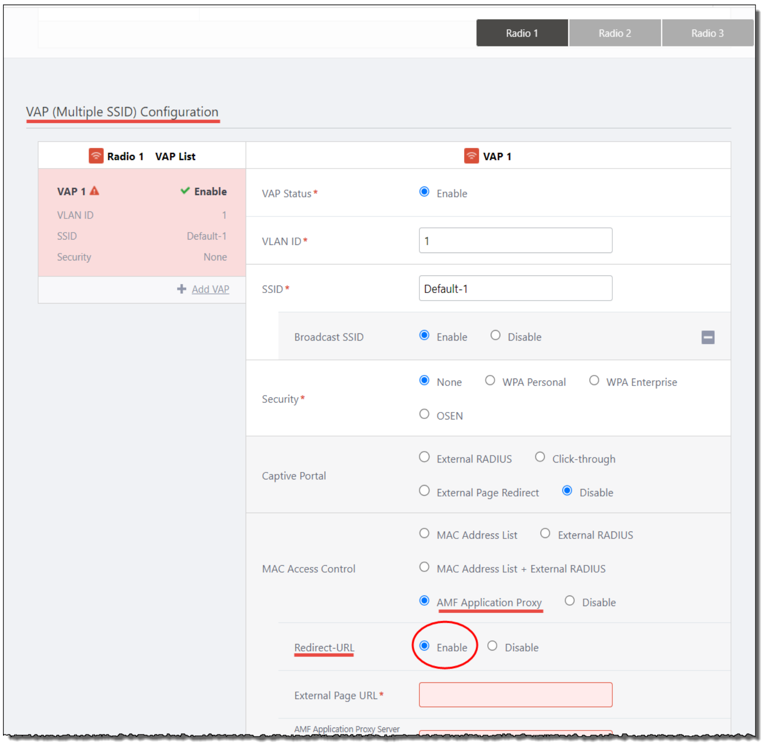
Redirect URL refers to a configuration setting that determines the website or application that users will be redirected to when they attempt to access a resource through the AMF Application Proxy.

The AMF Application Proxy acts as a gateway between the client and the application server, and allows users to access web applications without requiring them to connect to the internal network directly.

After successful authentication by the proxy, the system will direct users to the web address specified as the Redirect URL. This can be a landing page or the main dashboard of the application that the user is accessing.

To configure the **Redirect URL** feature, go to:

- **Wireless Configuration** > **AP Profile** > **VAP** Configuration on Profile Edit and Profile Detail pages.



VAP (Multiple SSID) Configuration

Radio 1 VAP List

VAP 1	✓ Enable
VLAN ID	1
SSID	Default-1
Security	None

+ Add VAP

VAP 1

VAP Status*	● Enable
VLAN ID*	1
SSID*	Default-1
Broadcast SSID	● Enable ○ Disable
Security*	● None ○ WPA Personal ○ WPA Enterprise ○ OSEN
Captive Portal	○ External RADIUS ○ Click-through ○ External Page Redirect ● Disable
MAC Access Control	○ MAC Address List ○ External RADIUS ○ MAC Address List + External RADIUS ● AMF Application Proxy ○ Disable
Redirect-URL	● Enable ○ Disable
External Page URL*	
AMF Application Proxy Server	

This feature requires AP firmware versions:

- TQ6702 GEN2/TQm6702 GEN2: v8.0.2-1.1or later

Two-step authentication with Captive Portal

Applicable to all Vista Manager EX installations with the AWC plug-in: Access Points TQ5403, TQm5403, TQ5403e

From Vista Manager EX version 3.10.3 onwards, you can configure two-step authentication on TQ5403 devices.

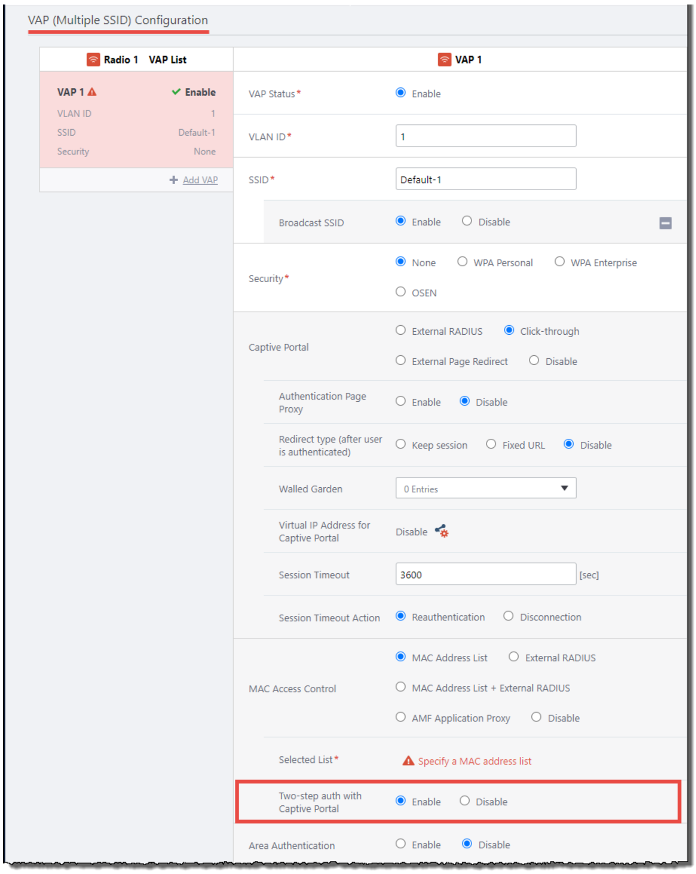
This feature allows MAC authentication and Web authentication to be used together under OR conditions. This means that clients can connect to the AP if they pass either authentication. Both MAC and Web authentication must be enabled.

Two-step authentication with Captive Portal is a security measure often used in wireless networks to ensure that only authorized users are able to connect to the network. It involves a two-step authentication process, where users must first connect to a captive portal before being granted access to the network.

This approach provides an additional layer of security for wireless networks, as it helps to ensure that only authorized users are able to connect to the network. It can also help to prevent unauthorized access and protect sensitive data from being compromised.

To configure the **Two-step authentication** feature, go to:

- **Wireless Configuration** > **AP Profile** > **VAP** Configuration on Profile Edit and Profile Detail pages:



VAP (Multiple SSID) Configuration

Radio 1 VAP List

VAP 1 ✓ Enable
VLAN ID 1
SSID Default-1
Security None

+ Add VAP

VAP 1

VAP Status* ● Enable

VLAN ID* 1

SSID* Default-1

Broadcast SSID ● Enable ○ Disable

Security* ● None ○ WPA Personal ○ WPA Enterprise ○ OSEN

Captive Portal ○ External RADIUS ● Click-through ○ External Page Redirect ○ Disable

Authentication Page Proxy ○ Enable ● Disable

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

Walled Garden 0 Entries

Virtual IP Address for Captive Portal Disable

Session Timeout 3600 [sec]

Session Timeout Action ● Reauthentication ○ Disconnection

MAC Access Control ● MAC Address List ○ External RADIUS ○ MAC Address List + External RADIUS ○ AMF Application Proxy ○ Disable

Selected List* Specify a MAC address list

Two-step auth with Captive Portal ● Enable ○ Disable

Area Authentication ○ Enable ● Disable

This feature requires AP firmware versions:

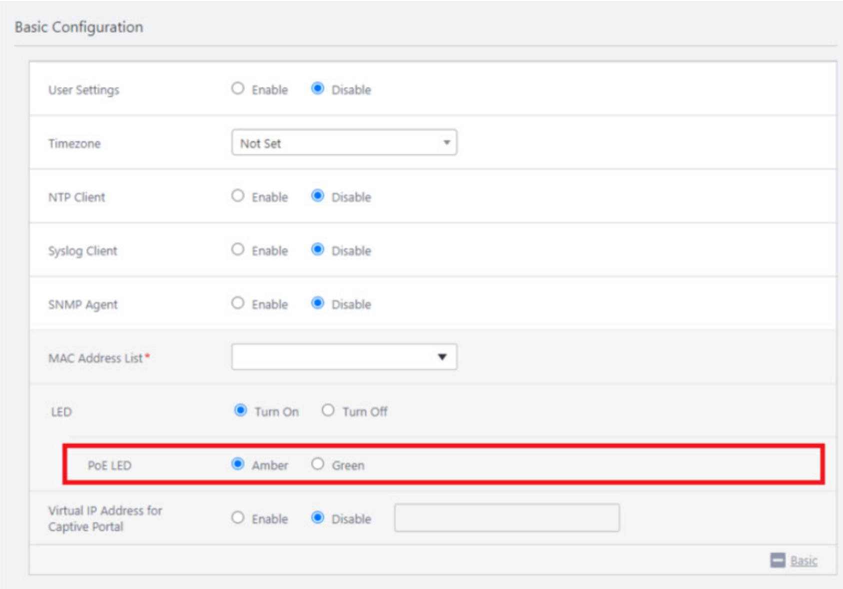
- TQ5403/TQm5403/TQ5403e : v6.0.3-0.1 or later

PoE LED color can be amber or green

Applicable to all Vista Manager EX installations with the AWC plug-in: Access Point TQ6602

From Vista Manager EX version 3.10.3 onwards, you can select either Amber or Green as the PoE LED color. Previously, when PoE was enabled, the LAN port power LED was colored only amber.

Amber is the default.



Basic Configuration

User Settings	○ Enable ● Disable
Timezone	Not Set
NTP Client	○ Enable ● Disable
Syslog Client	○ Enable ● Disable
SNMP Agent	○ Enable ● Disable
MAC Address List*	
LED	● Turn On ○ Turn Off
PoE LED	● Amber ○ Green
Virtual IP Address for Captive Portal	○ Enable ● Disable

This feature requires AP firmware versions:

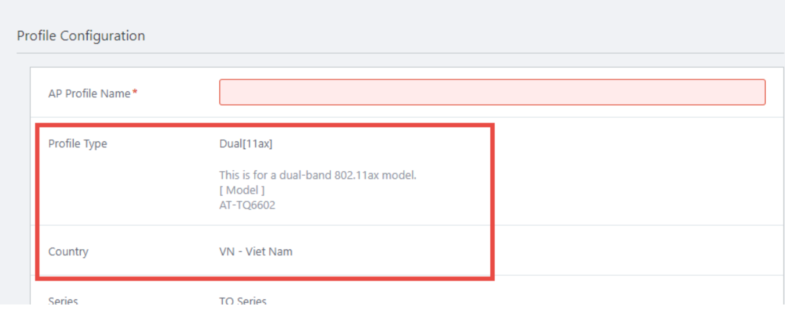
- TQ6602: v7.0.1-3.1or later

DFS channel support

Applicable to the AWC plug-in - Access Point: TQ6602

A new FCC country code has been added for Dual[11ax] AP profile types from version 3.10.3 onwards. As DFS channels vary from country to country, DFS channels corresponding to the selected country will then become available in the Auto Channel Selection setting. The following new country code is available:

- VN - Viet Nam



Profile Configuration

AP Profile Name*	
Profile Type	Dual[11ax] This is for a dual-band 802.11ax model. [Model] AT-TQ6602
Country	VN - Viet Nam
Series	TQ Series

This feature requires AP firmware versions:

- TQ6602: v7.0.1-3.1or later

Enable or Disable individual floor maps

Applicable to all Vista Manager EX installations with the AWC plug-in:

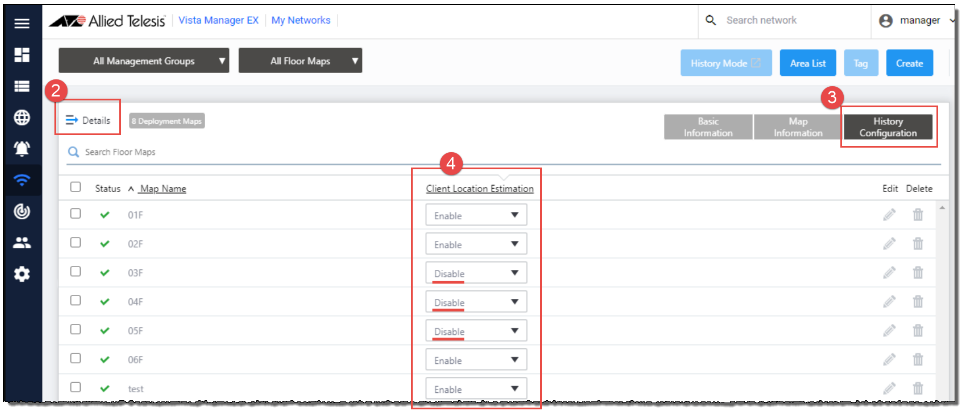
From Vista Manager EX version 3.10.3 onwards, you can enable or disable location estimation on individual floor maps using the **Floor Map** page. Location estimation refers to the process of determining the geographical coordinates or position of a mobile device or wireless access point. It involves using various techniques and measurements to calculate or estimate the location accurately.

Previously, it was only possible to enable or disable all floor maps at once using the **System Setting** page.

By enabling location estimation on only the necessary floor maps, the network can reduce the amount of storage used by log data. This means that instead of storing and processing location data for the entire building or multiple floors, the system focuses only on the relevant floor maps, optimizing storage resources and improving efficiency.

To enable or disable location estimation for floor maps:

1. Go to **Wireless Monitoring**> **Floor Map**:



☐	Status	Map Name	Client Location Estimation	Edit	Delete
☐	✓	01F	Enable		
☐	✓	02F	Enable		
☐	✓	03F	Disable		
☐	✓	04F	Disable		
☐	✓	05F	Disable		
☐	✓	06F	Enable		
☐	✓	test	Enable		

2. Open **Details** and select the **History Configuration** tab.

3. Select the floor map(s).

4. Enable or disable **Client Location Estimation** for the corresponding floor map.

5. Open the **AP Settings** page

6. Select the target APs and apply the relevant settings.

Enhanced log settings

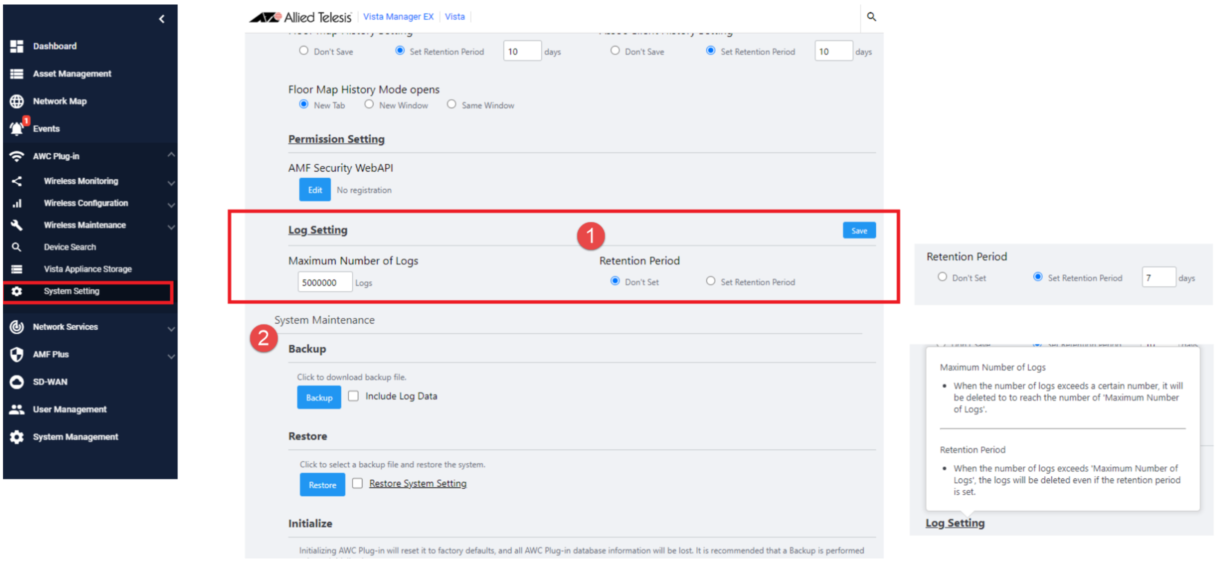
Applicable to all Vista Manager EX installations with the AWC plug-in:

From Vista Manager EX version 3.10.3 onwards, you have more control over log retention and storage. Specifically, while the **Log Settings** currently retains a fixed number of logs (5 million), you can now adjust the retention number within a range of 10,000 to 5 million.

Additionally, you can:

1. configure the log retention period (1-31days),
2. backup and restore logs
3. monitor and manage AWC notification logs.

Overall, these enhancements result in reduced storage usage for log data.



○ Don't Save ● Set Retention Period 10 days ○ Don't Save ● Set Retention Period 10 days

Floor Map History Mode opens
● New Tab ○ New Window ○ Same Window

Permission Setting

AMF Security WebAPI
Edit No registration

Log Setting Save

Maximum Number of Logs
5000000 Logs

Retention Period
● Don't Set ○ Set Retention Period

System Maintenance

Backup

Click to download backup file.
Backup □ Include Log Data

Restore

Click to select a backup file and restore the system.
Restore □ Restore System Setting

Initialize

Initializing AWC Plug-in will reset it to factory defaults, and all AWC Plug-in database information will be lost. It is recommended that a Backup is performed

Retention Period
○ Don't Set ● Set Retention Period 7 days

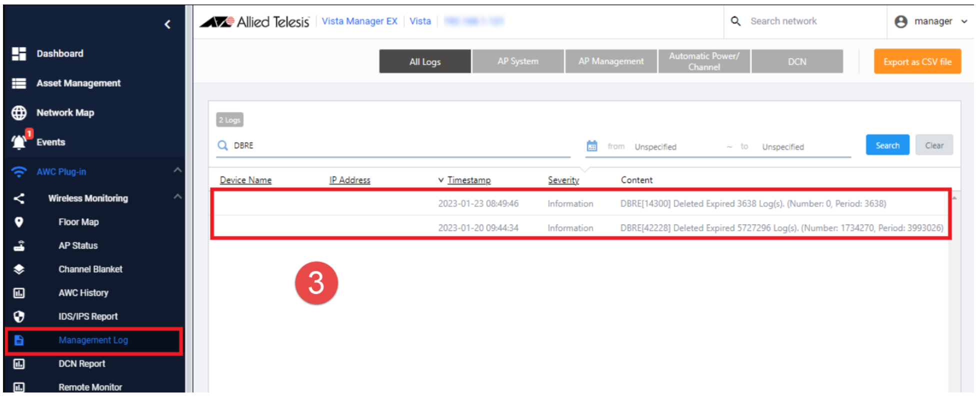
Maximum Number of Logs

- When the number of logs exceeds a certain number, it will be deleted to to reach the number of 'Maximum Number of Logs'.

Retention Period

- When the number of logs exceeds 'Maximum Number of Logs', the logs will be deleted even if the retention period is set.

Log Setting



[redacted]

2 Logs

DBRE from Unspecified ~ to Unspecified

Device Name	IP Address	Timestamp	Severity	Content
		2023-01-23 08:49:46	Information	DBRE[14300] Deleted Expired 3638 Log(s). (Number: 0, Period: 3638)
		2023-01-20 09:44:34	Information	DBRE[42228] Deleted Expired 5727296 Log(s). (Number: 1734270, Period: 3993026)

What's New in Vista Manager EX v3.10.1

Introduction

This release note describes the new features in Vista Manager EX™ v3.10.1. 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.

New Features and Enhancements

This section summarizes the new features and enhancements added to Vista Manager EX version 3.10.1, it includes:

- "Introducing AMF Plus" on page 12.
- "Health Monitoring" on page 16.
- "Intent-Based QoS" on page 21.
- "Alternative and additional security options" on page 22.
- "AWC enhancements" on page 23.

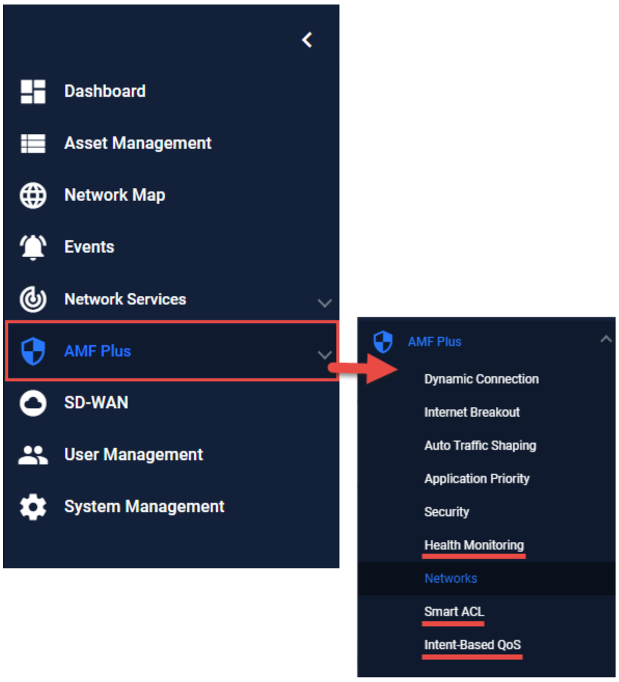
Introducing AMF Plus

Applicable to all Vista Manager installations with the AMF Plus license.

AMF Plus is the new name for the intent-based networking feature menu in Vista Manager EX. From version 3.10.1, it replaces the current Allied Intent-based Orchestrator (AIO) menu on systems that have an AMF Plus license.

With intent-based networking, instead of you having to manually configure and monitor each device on the network, the system uses algorithms to automatically set up, optimize, and maintain the network according to predetermined goals and policies. This allows for more efficient and agile network management, and can improve network performance and visibility.

As well as the existing AIO features for WAN management, the AMF Plus menu adds LAN-based features such as Health Monitoring, Smart ACLs, and Intent-Based QoS. These are described further later in this release note.



AMF Plus licensing

From AlliedWare Plus version 5.5.2-2.3 onwards, AMF licenses are no longer available to purchase. Instead, AMF Plus licenses are available. Existing AMF licenses are still valid, so you only need to change to AMF Plus licenses if you:

- need to manage more nodes, or
- want to use the new AMF Plus menu in Vista Manager EX.

If you would like to change to AMF Plus licenses, contact your Allied Telesis salesperson.

Upgrading an AMF area to use AMF Plus in Vista Manager EX

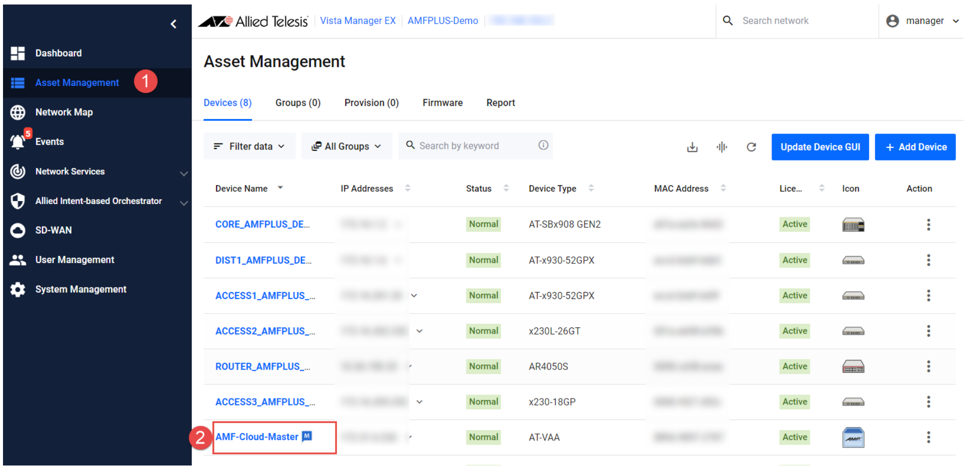
For existing AMF license holders wanting to upgrade an AMF area Master to AMF Plus, use the following steps:

1. Upgrade the following devices to AlliedWare Plus software version 5.5.2-2.3: the AMF masters, and any other nodes that have downstream nodes attached to them.

2. Obtain enough AMF Plus licenses for all the nodes.

3. Go to **Asset Management**.

4. Select the **Master** device.

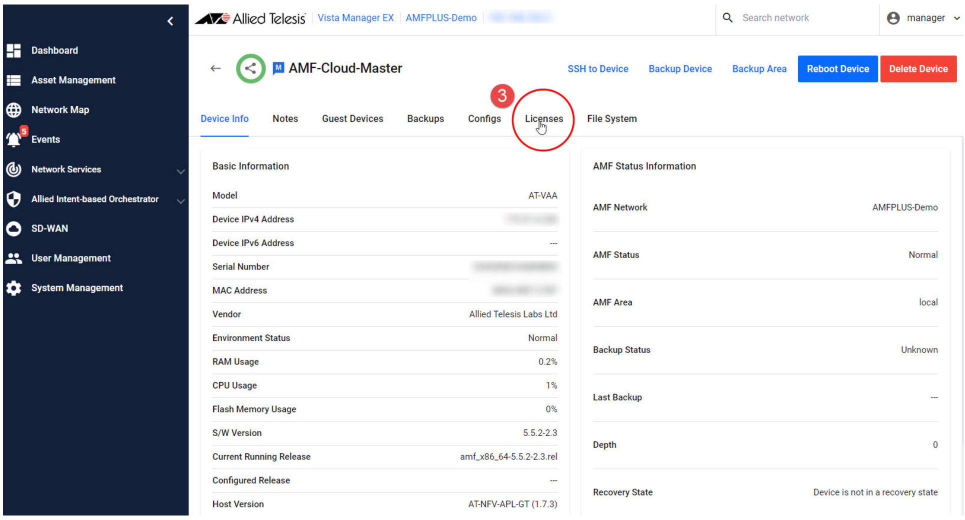


Asset Management

Devices (8) | Groups (0) | Provision (0) | Firmware | Report

Device Name	IP Addresses	Status	Device Type	MAC Address	Lice...	Icon	Action
CORE_AMFPLUS_DE...	[redacted]	Normal	AT-SBx908 GEN2	[redacted]	Active		⋮
DIST1_AMFPLUS_DE...	[redacted]	Normal	AT-x930-52GPX	[redacted]	Active		⋮
ACCESS1_AMFPLUS_...	[redacted]	Normal	AT-x930-52GPX	[redacted]	Active		⋮
ACCESS2_AMFPLUS_...	[redacted]	Normal	x230L-26GT	[redacted]	Active		⋮
ROUTER_AMFPLUS_...	[redacted]	Normal	AR4050S	[redacted]	Active		⋮
ACCESS3_AMFPLUS_...	[redacted]	Normal	x230-18GP	[redacted]	Active		⋮
AMF-Cloud-Master M	[redacted]	Normal	AT-VAA	[redacted]	Active	AMF	⋮

5. Select the **Licenses** tab.



M AMF-Cloud-Master

Device Info | Notes | Guest Devices | Backups | Configs | Licenses | File System

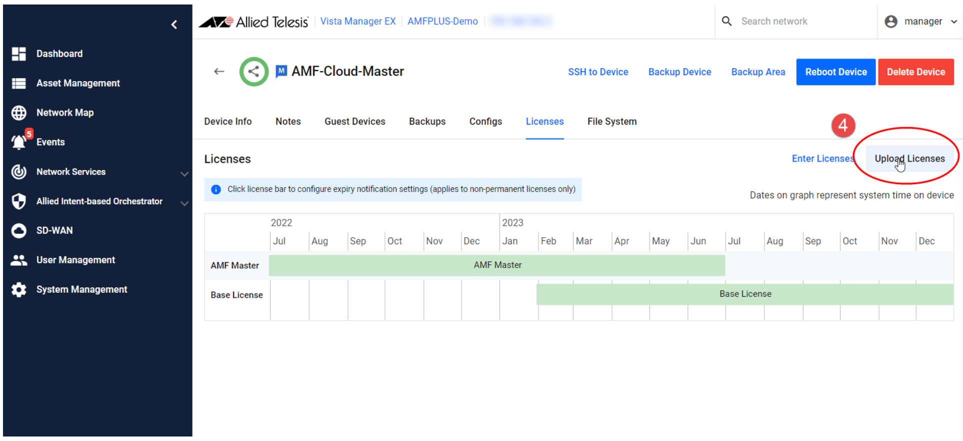
Basic Information

Model	AT-VAA
Device IPv4 Address	[redacted]
Device IPv6 Address	---
Serial Number	[redacted]
MAC Address	[redacted]
Vendor	Allied Telesis Labs Ltd
Environment Status	Normal
RAM Usage	0.2%
CPU Usage	1%
Flash Memory Usage	0%
S/W Version	5.5.2-2.3
Current Running Release	amf_x86_64-5.5.2-2.3.rel
Configured Release	---
Host Version	AT-NFV-APL-GT (1.7.3)

AMF Status Information

AMF Network	AMFPLUS-Demo
AMF Status	Normal
AMF Area	local
Backup Status	Unknown
Last Backup	---
Depth	0
Recovery State	Device is not in a recovery state

6. Click **Upload Licenses**

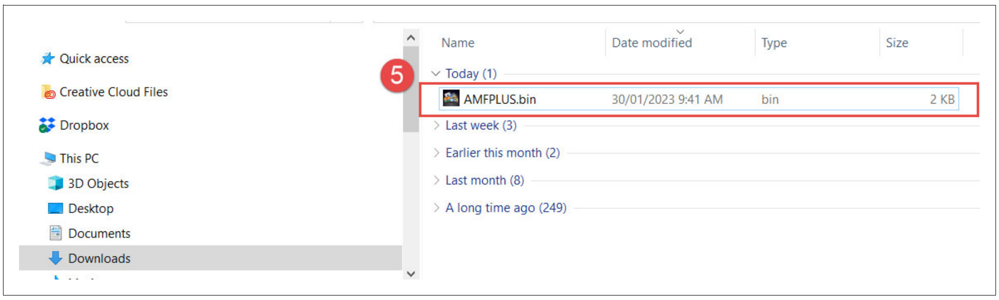


Licenses

Click license bar to configure expiry notification settings (applies to non-permanent licenses only)

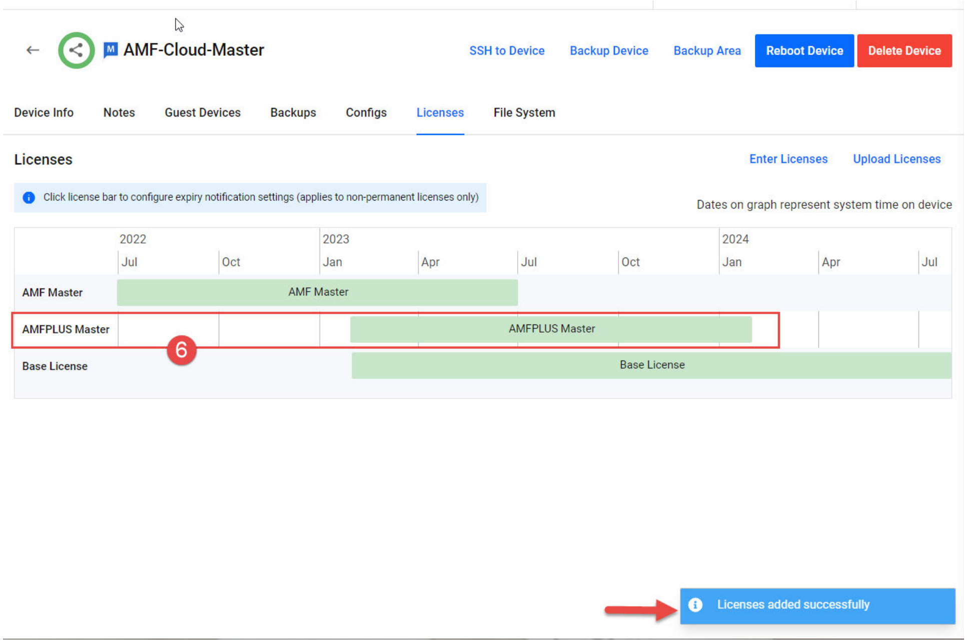
Dates on graph represent system time on device

7. Browse to locate and select your AMF Plus license *.bin file.



Name	Date modified	Type	Size
Today (1)			
AMFPLUS.bin	30/01/2023 9:41 AM	bin	2 KB
Last week (3)			
Earlier this month (2)			
Last month (8)			
A long time ago (249)			

8. The AMF Plus Master license is added to the Licenses list.



Licenses

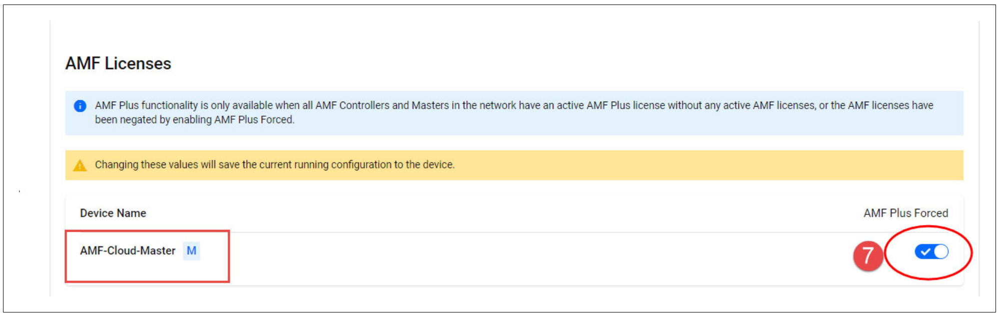
Click license bar to configure expiry notification settings (applies to non-permanent licenses only)

Dates on graph represent system time on device

Licenses added successfully

9. Go to **System Management** > **Licenses** and enable the **AMF Plus Forced** button.

Note: It is essential to have enough AMF Plus node licenses - as the existing AMF node licenses will no longer be counted.



AMF Licenses

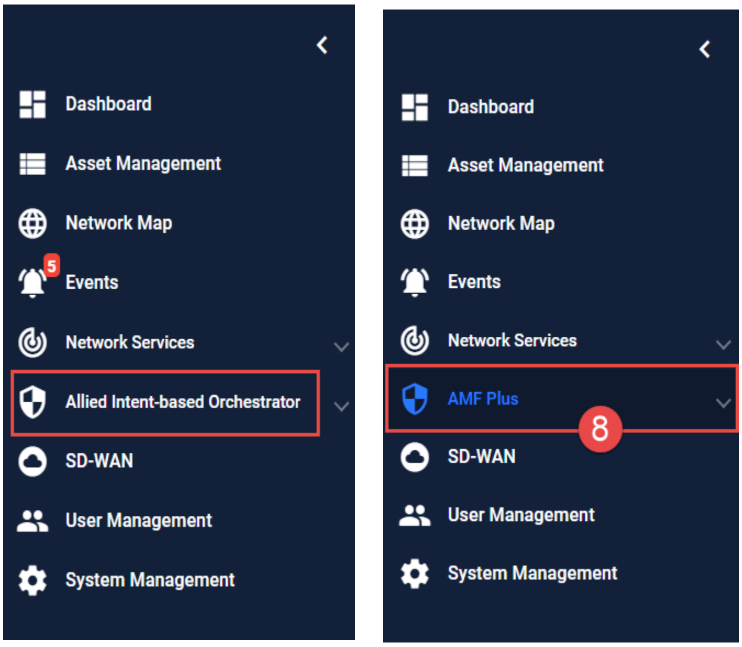
AMF Plus functionality is only available when all AMF Controllers and Masters in the network have an active AMF Plus license without any active AMF licenses, or the AMF licenses have been negated by enabling AMF Plus Forced.

Changing these values will save the current running configuration to the device.

Device Name	AMF Plus Forced
AMF-Cloud-Master M	☑

10. Go to the Dashboard. The **Allied Intent-based Orchestrator** menu will have changed to the **AMF Plus** menu.

Note: If you did not have an existing AIO license, then the AMF Plus menu will have been added to the main menu.



This completes the AMF Plus license upgrade process for a **single-area network**.

Upgrading a multi-area network to AMF Plus

If you have a multi-area network, you must ensure that you have enough AMF Plus licenses to cover all the nodes in the network, and that each **Master** and **Controller** node is running AlliedWare Plus software version **5.5.2-2.3** or later.

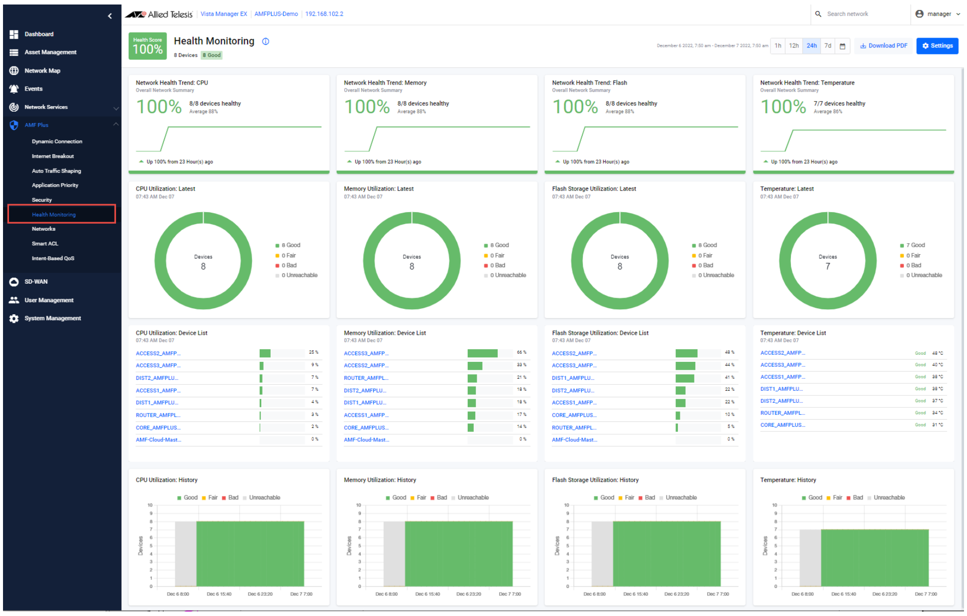
For more information about putting AMF Plus on AMF networks, contact your Allied Telesis technical service representative.

Health Monitoring

Applicable to all Vista Manager installations with the AMF Plus license.

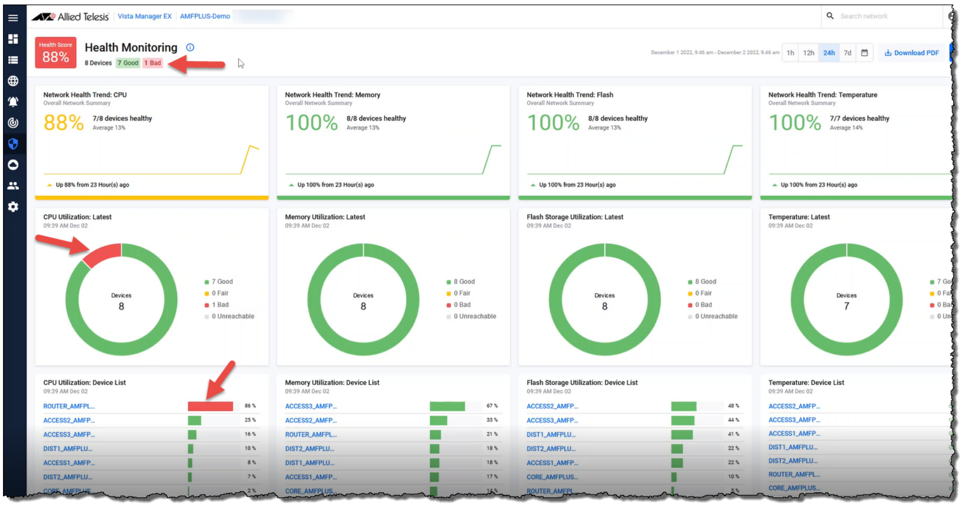
From version 3.10.1 onwards, you can view a summary of the state of your network's health as part of AMF Plus.

Understanding network health indicators enables you to investigate, analyze, and improve the overall health of your network quickly. Such indicators include CPU utilization, storage, temperature, and memory usage.

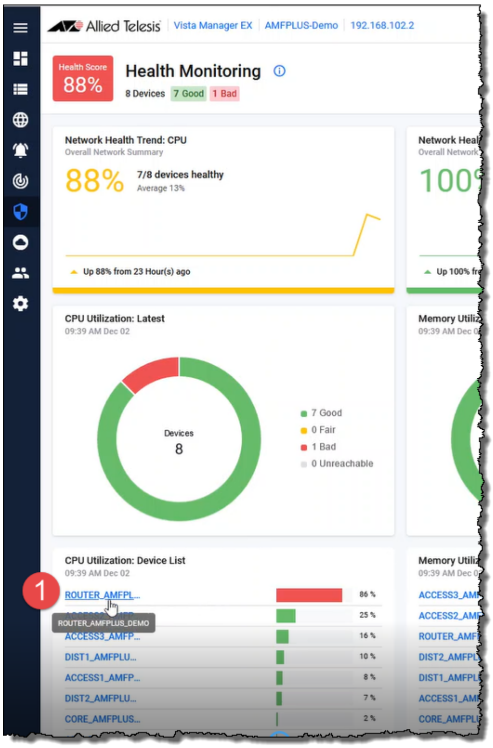


The **Health Score** is a percentage based on how many devices are healthy in the network. The state of each device is selected based on the worst state of any of the gathered statistics. Result charts are color coded for easy understanding of device status: Green = Good, Yellow=Fair, Red=Bad, and Grey= Unreachable.

Example In the example below, you can see a Health Score of 88%. There are 8 devices in this network, but there's a CPU issue with one of them. The bad device is highlighted in red.

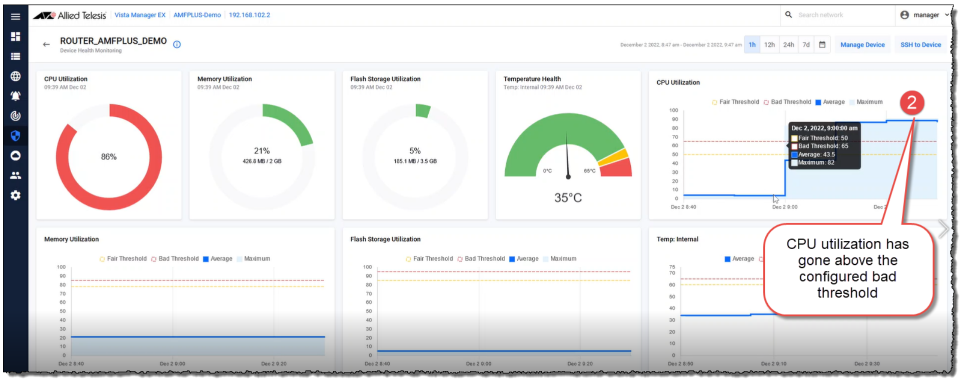

Allied Telesis | Vista Manager EX | AMFPLUS-Demo
Health Score 88%
Health Monitoring
8 Devices 7 Good 1 Bad
Download PDF
Network Health Trend: CPU
88%
7/8 devices healthy
Network Health Trend: Memory
Network Health Trend: Flash
100%
8/8 devices healthy
Network Health Trend: Temperature
7/7 devices healthy
CPU Utilization: Latest
Devices 8
7 Good
0 Fair
1 Bad
0 Unreachable
Memory Utilization: Latest
Flash Storage Utilization: Latest
8 Good
0 Bad
Temperature: Latest
Devices 7
CPU Utilization: Device List
ROUTER_AMFPL...
86 %
Memory Utilization: Device List
Flash Storage Utilization: Device List
Temperature: Device List

1. Click on the ‘bad’ device name to investigate further.



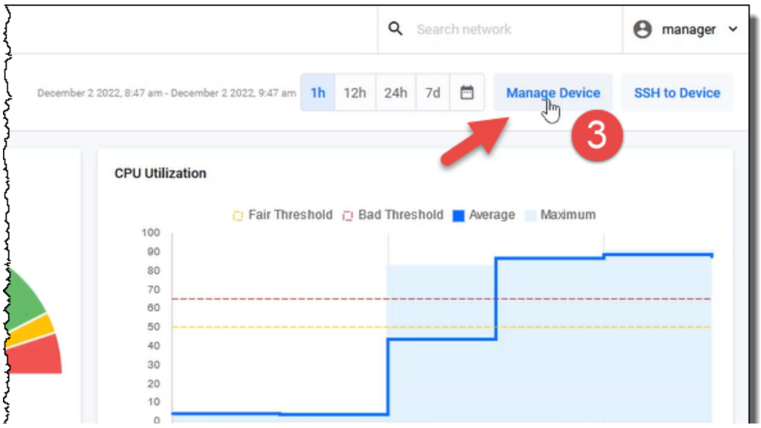
ROUTER_AMFPL...	86 %
	25 %
ACCESS3_AMFP...	16 %
DIST1_AMFPLU...	10 %
ACCESS1_AMFP...	8 %
DIST2_AMFPLU...	7 %
CORE_AMFPLUS...	2 %

2. Drilling down confirms that around 9am CPU utilization rose above the configured band threshold.

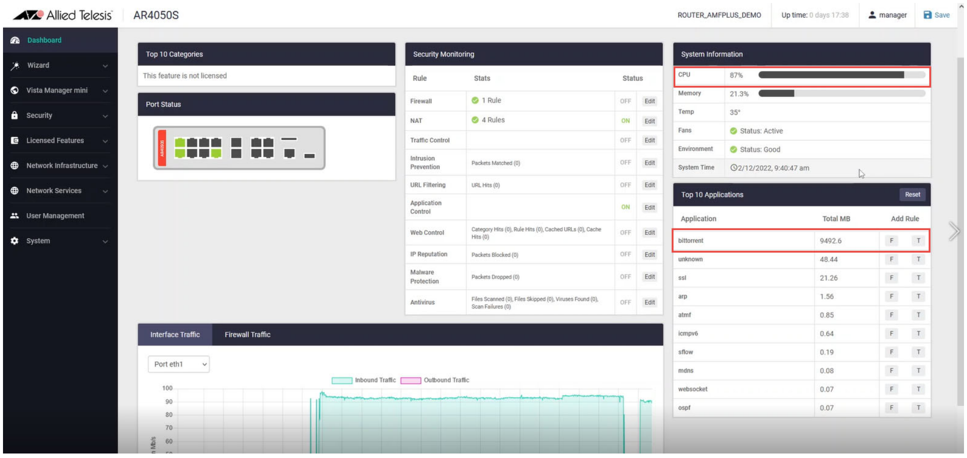


CPU utilization has gone above the configured bad threshold

3. To further diagnose the issue, click on **Manage Device** to open the device's GUI.



For this example device (AR4050S), the system information indicates a very high CPU usage and the applications show the bittorrent traffic increasing quite rapidly...which is likely to be the cause of the high CPU utilization.



Top 10 Categories

This feature is not licensed

Security Monitoring

Rule	Stats	Status	
Firewall	1 Rule	OFF	Edit
NAT	4 Rules	ON	Edit
Traffic Control		OFF	Edit
Intrusion Prevention	Packets Matched (0)	OFF	Edit
URL Filtering	URL Hits (0)	OFF	Edit
Application Control		ON	Edit
Web Control	Category Hits (0), Rule Hits (0), Cached URLs (0), Cache Hits (0)	OFF	Edit
IP Reputation	Packets Blocked (0)	OFF	Edit
Malware Protection	Packets Dropped (0)	OFF	Edit
Antivirus	Files Scanned (0), Files Skipped (0), Viruses Found (0), Scan Failures (0)	OFF	Edit

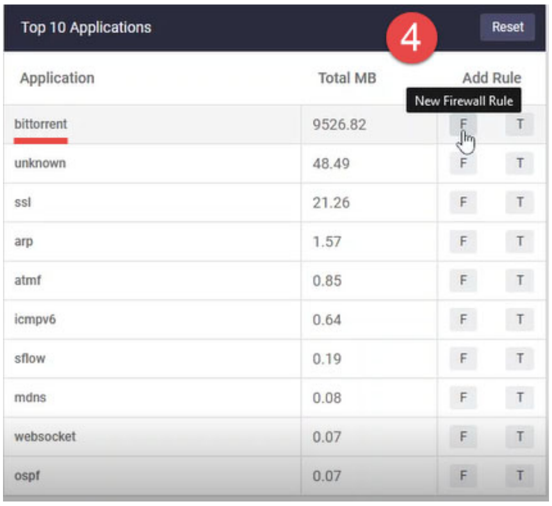
System Information

CPU	87%
Memory	21.3%
Temp	35°
Fans	Status: Active
Environment	Status: Good
System Time	2/12/2022, 9:40:47 am

Top 10 Applications Reset

Application	Total MB	Add Rule	
bittorrent	9492.6	F	T
unknown	48.44	F	T
ssl	21.26	F	T
arp	1.56	F	T
atmf	0.85	F	T
icmpv6	0.64	F	T
sflow	0.19	F	T
mdns	0.08	F	T
websocket	0.07	F	T
ospf	0.07	F	T

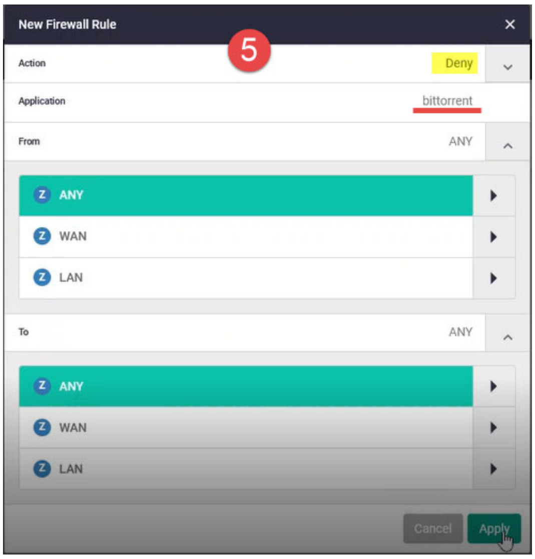
4. At this point you may decide to disallow the bittorrent traffic by adding a firewall rule.



Top 10 Applications Reset

Application	Total MB	Add Rule	
bittorrent	9526.82	F	T
unknown	48.49	F	T
ssl	21.26	F	T
arp	1.57	F	T
atmf	0.85	F	T
icmpv6	0.64	F	T
sflow	0.19	F	T
mdns	0.08	F	T
websocket	0.07	F	T
ospf	0.07	F	T

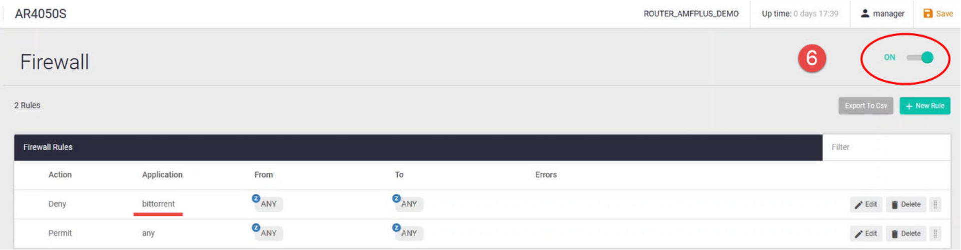
5. Configure the firewall rules.



New Firewall Rule

Action	Deny
Application	bittorrent
From	ANY
To	ANY

6. Turn on the firewall.



AR4050S

ROUTER_AMFPLUS_DEMO Up time: 0 days 17:39 manager Save

Firewall

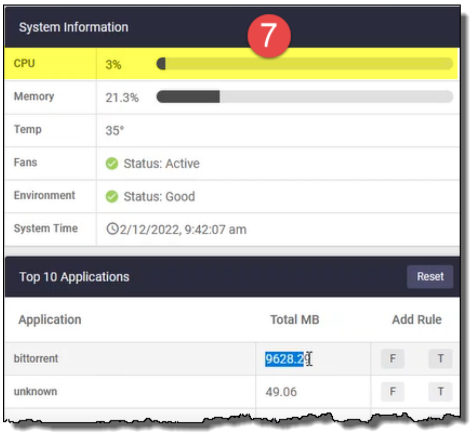
ON

2 Rules

Firewall Rules

Action	Application	From	To	Errors
Deny	bittorrent	ANY	ANY	
Permit	any	ANY	ANY	

7. Go back to the Dashboard and check the CPU percentage.



System Information

CPU	3%
Memory	21.3%
Temp	35°
Fans	Status: Active
Environment	Status: Good
System Time	2/12/2022, 9:42:07 am

Top 10 Applications

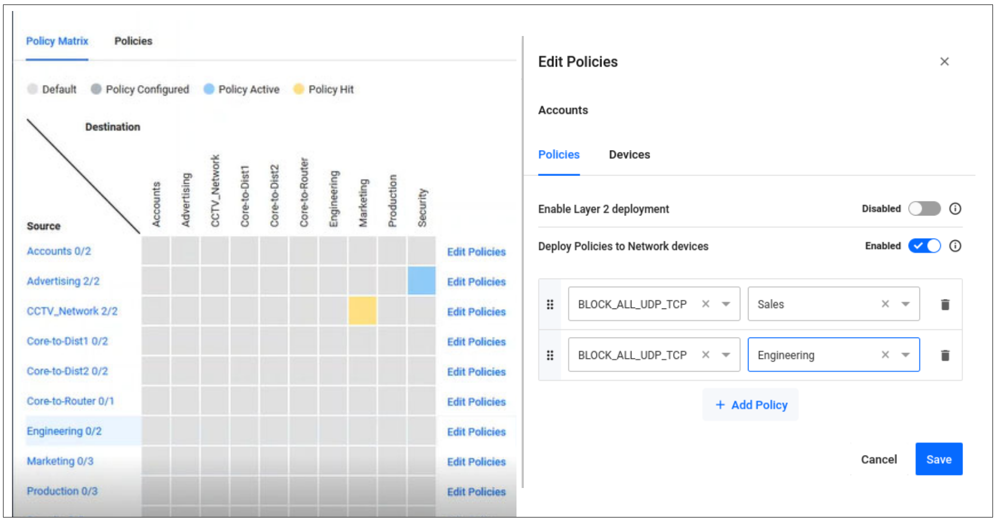
Application	Total MB	Add Rule
bittorrent	9628.2	F T
unknown	49.06	F T

Smart ACL

From version 3.10.1 onwards, Smart ACL makes management of ACLs easier, as part of AMF Plus. You can use **Smart ACL** to control the resources that clients access in the network. For example, you might want to stop marketing clients from being able to see a security client’s CCTV video stream and also stop the security clients from accessing marketing videos.

Smart ACL uses intent-style network management.

To locate this feature, go to **AMF Plus** > **Smart ACL**



Policy Matrix | Policies

● Default ● Policy Configured ● Policy Active ● Policy Hit

Destination / Source	Accounts	Advertising	CCTV_Network	Core-to-Dist1	Core-to-Dist2	Core-to-Router	Engineering	Marketing	Production	Security	
Accounts 0/2											Edit Policies
Advertising 2/2										🟦	Edit Policies
CCTV_Network 2/2								🟨			Edit Policies
Core-to-Dist1 0/2											Edit Policies
Core-to-Dist2 0/2											Edit Policies
Core-to-Router 0/1											Edit Policies
Engineering 0/2											Edit Policies
Marketing 0/3											Edit Policies
Production 0/3											Edit Policies

Edit Policies

Accounts

Policies | Devices

Enable Layer 2 deployment — Disabled

Deploy Policies to Network devices — Enabled

BLOCK_ALL_UDP_TCP	Sales
BLOCK_ALL_UDP_TCP	Engineering

There are three parts to the Smart ACL feature:

- Network elements such as VLAN subnets, and ACL source host groups, are wrapped into one concept known as a **Network**.
- The Network Access **Matrix** represents all source and destination networks currently configured on connected network devices.
- The access relationships between Networks is simplified by the use of **Policies**. Policies stipulate the Access List filters that go to define the traffic control that the network requires.

Intent-Based QoS

Applicable to all Vista Manager installations with the AMF Plus license.

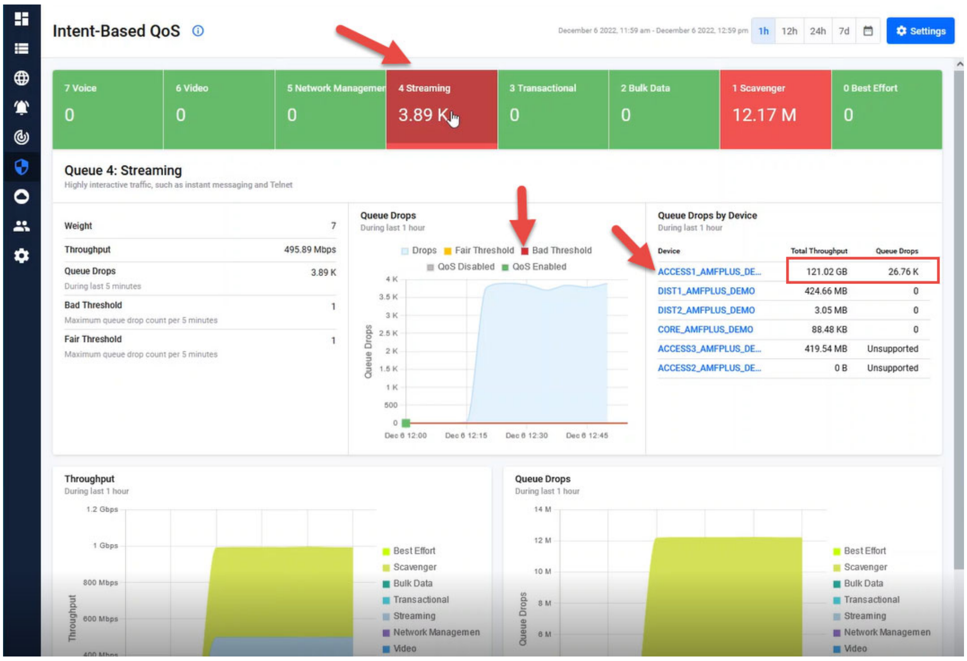
From version 3.10.1 onwards, you can easily manage and troubleshoot a basic QoS configuration on your network as part of AMF Plus.

For example, you may have issues with a poor quality video stream. Understanding where the queue drops are occurring allows you to perhaps adjust the QoS queue weighting and improve the video quality.

Getting started

First you need to manually apply a default QoS configuration to all switches in your network. This configuration sets up 2 priority queues and 6 weighted-round-robin queues. The priority queues have an egress rate limit applied, and the weighted-round-robin queues each have a weighting applied. The configuration also defines a mapping of DSCP fields to QoS queue based on industry standards. This mapping cannot be changed via Vista Manager.

Once this default configuration has been applied on the network, the new **Intent-Based QoS** page will show the state of the network in regards to the QoS queues.



Intent-Based QoS

December 6 2022, 11:59 am - December 6 2022, 12:59 pm

7 Voice	6 Video	5 Network Managemer	4 Streaming	3 Transactional	2 Bulk Data	1 Scavenger	0 Best Effort
0	0	0	3.89 K	0	0	12.17 M	0

Queue 4: Streaming

Highly interactive traffic, such as instant messaging and Telnet

Weight	7
Throughput	495.89 Mbps
Queue Drops During last 5 minutes	3.89 K
Bad Threshold Maximum queue drop count per 5 minutes	1
Fair Threshold Maximum queue drop count per 5 minutes	1

Queue Drops by Device

During last 1 hour

Device	Total Throughput	Queue Drops
ACCESS1_AMFPLUS_DE...	121.02 GB	26.76 K
DIST1_AMFPLUS_DEMO	424.66 MB	0
DIST2_AMFPLUS_DEMO	3.05 MB	0
CORE_AMFPLUS_DEMO	88.48 KB	0
ACCESS3_AMFPLUS_DE...	419.54 MB	Unsupported
ACCESS2_AMFPLUS_DE...	0 B	Unsupported

Each of the eight QoS queues has a label based loosely on what sort of traffic is expected on the queue. For example, the highest priority queue, QoS queue 7 has the label ‘Voice’ as this queue will be used for VoIP traffic. Queue 6 has the label ‘Video’ as this queue will be used for a variety of video services, and so on.

You can see in the diagram above that the **Streaming** queue is experiencing queue drops. On further investigation you can see when and on which device the drops are occurring.

Now you can adjust the rate limit or weighting of the problematic queue on the entire network by using a simple graphical tool - the Intent-Based QoS dashboard.

Alternative and additional security options

Applicable to all Vista Manager installations with the AMF Plus license.

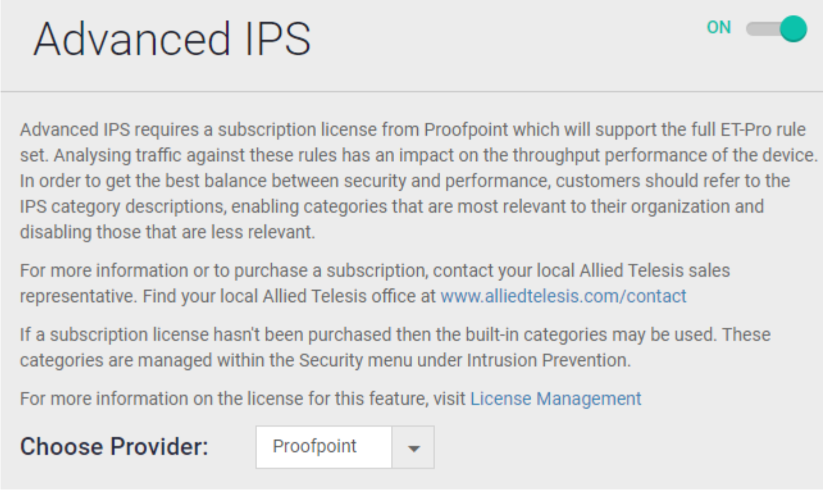
From version 3.10.1 onwards, AlliedWare Plus provides Advanced IPS (Intrusion Prevention System) functionality.

This is made possible by the addition of the third-party vendor Proofpoint's ET Pro Ruleset.

The Proofpoint ET Pro Ruleset detects and blocks advanced threats. Updated daily, it covers Malware delivery, command and control, attack spread, in-the-wild exploits and vulnerabilities, and credential phishing. It also detects and blocks distributed denial-of-service attacks (DDoS), protocol and application anomalies, exploit kits and supervisory control and data acquisition (SCADA) attacks.

This feature requires a license, which is available in the bundle pack: AT-AR4-UTM-02-1/3/5YR. Contact your authorized Allied Telesis support center to obtain a license.

You can choose Proofpoint as your provider on the **AMF Plus** > **Security** > **Advanced IP Reputation** screen.



Advanced IPS

Advanced IPS requires a subscription license from Proofpoint which will support the full ET-Pro rule set. Analysing traffic against these rules has an impact on the throughput performance of the device. In order to get the best balance between security and performance, customers should refer to the IPS category descriptions, enabling categories that are most relevant to their organization and disabling those that are less relevant.

For more information or to purchase a subscription, contact your local Allied Telesis sales representative. Find your local Allied Telesis office at www.alliedtelesis.com/contact

If a subscription license hasn't been purchased then the built-in categories may be used. These categories are managed within the Security menu under Intrusion Prevention.

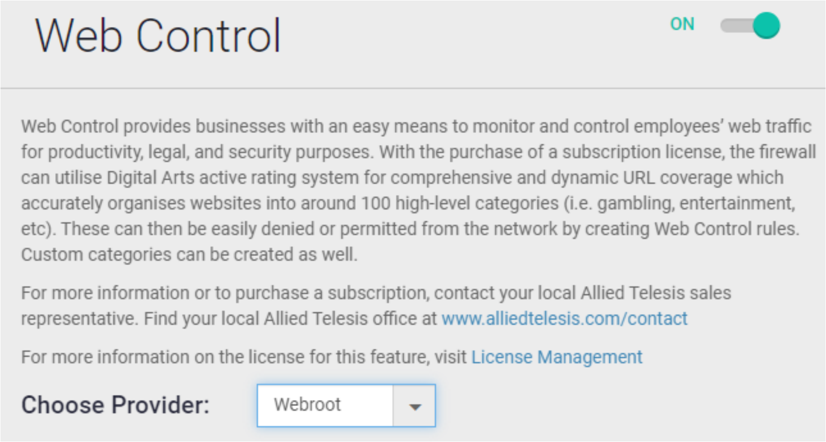
For more information on the license for this feature, visit License Management

Choose Provider: Proofpoint

Also available from AlliedWare Plus version 5.5.2-2.1, support for provider Webroot has be added to **Web Categorization** and **Web Control**. Webroot delivers multi-vector protection for endpoints and networks and threat intelligence.

Additionally, an alternative solution for Kaspersky URL Filtering based on a combination of DPI Web Categorization (provider Webroot) and firewall rules has been added.

You can choose Webroot as your provider on the **Licensed Features** > **Web Control** screen.



Web Control

Web Control provides businesses with an easy means to monitor and control employees' web traffic for productivity, legal, and security purposes. With the purchase of a subscription license, the firewall can utilise Digital Arts active rating system for comprehensive and dynamic URL coverage which accurately organises websites into around 100 high-level categories (i.e. gambling, entertainment, etc). These can then be easily denied or permitted from the network by creating Web Control rules. Custom categories can be created as well.

For more information or to purchase a subscription, contact your local Allied Telesis sales representative. Find your local Allied Telesis office at www.alliedtelesis.com/contact

For more information on the license for this feature, visit License Management

Choose Provider: Webroot

Note: Support for existing features/capabilities via Digital Arts and Kaspersky remain.

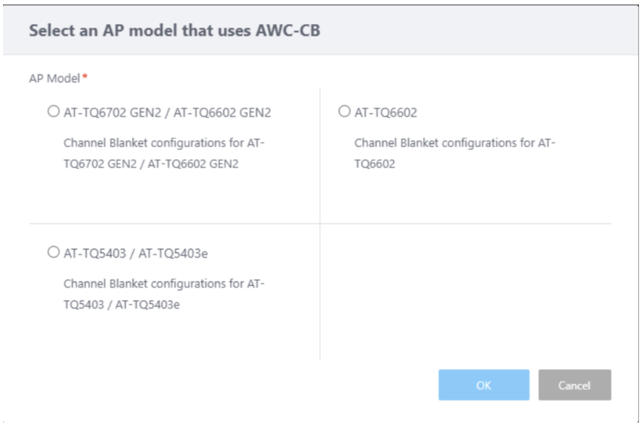
AWC enhancements

TQ6702 GEN2, TQ6602 GEN2 support AWC-CB

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

From version 3.10.1 onwards, the AWC plug-in supports AWC-CB on the TQ6702 GEN2 and TQ6602 GEN2 APs. You can configure up to 7 channel blanket VAPs per radio.

To add these APs to a Channel Blanket profile, select:
AWC plugin > **Wireless Configuration** > **CB Profile** in the left-hand menu.



Select an AP model that uses AWC-CB

AP Model*

○ AT-TQ6702 GEN2 / AT-TQ6602 GEN2

Channel Blanket configurations for AT-TQ6702 GEN2 / AT-TQ6602 GEN2

○ AT-TQ6602

Channel Blanket configurations for AT-TQ6602

○ AT-TQ5403 / AT-TQ5403e

Channel Blanket configurations for AT-TQ5403 / AT-TQ5403e

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

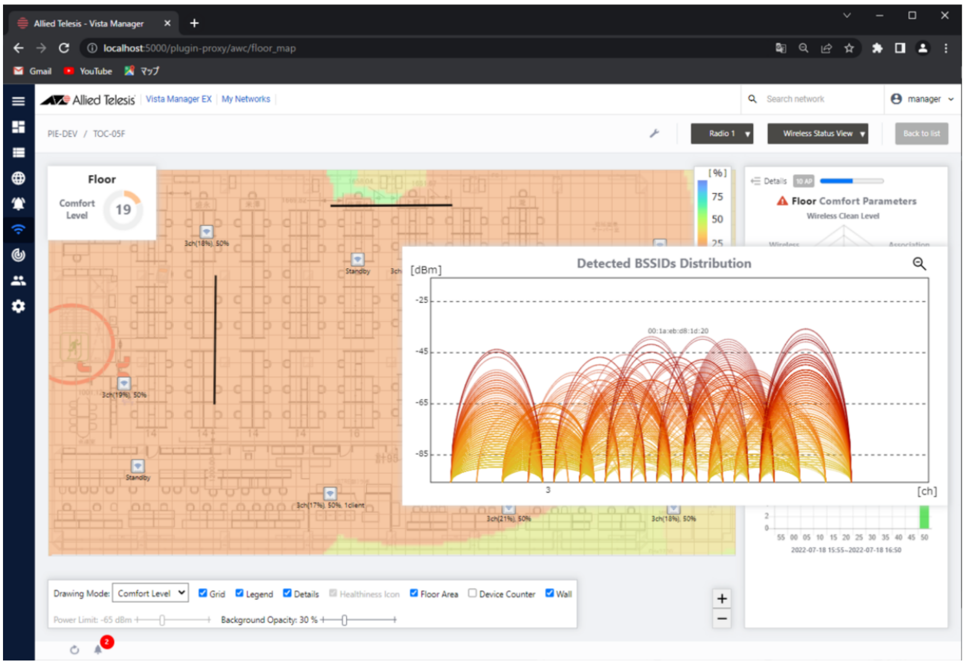
Heatmap showing Wi-Fi quality level

Applicable to all Vista Manager installations with the AWC plug-in:

From version 3.10.1 onwards, the AWC plug-in supports the wireless Comfort level heatmap feature. The Comfort level heatmap is located on the AWC Floor map details page. This is now the default view of the floor map.

Use the Comfort level map to:

- monitor the wireless environment
  - airtime capacity
  - connection stability
  - client capacity
  - wi-fi signal stability
  - channel availability
- detect rogue BSSIDs
  - A rogue access point is a wireless access point that has been set up on a network without the network administrator's permission. This unauthorized access point can be used to gain access to the network and potentially cause harm.



This feature requires AP firmware versions:

- *TQ1402, TQm1402: 6.0.2-0.1 or later*
- *TQ5403, TQm5403, TQ5403e: 6.0.2-0.2 or later*
- *TQ6602 GEN2, TQm6602 GEN2, TQ6702 GEN2: 8.0.2-1.1 or later.*

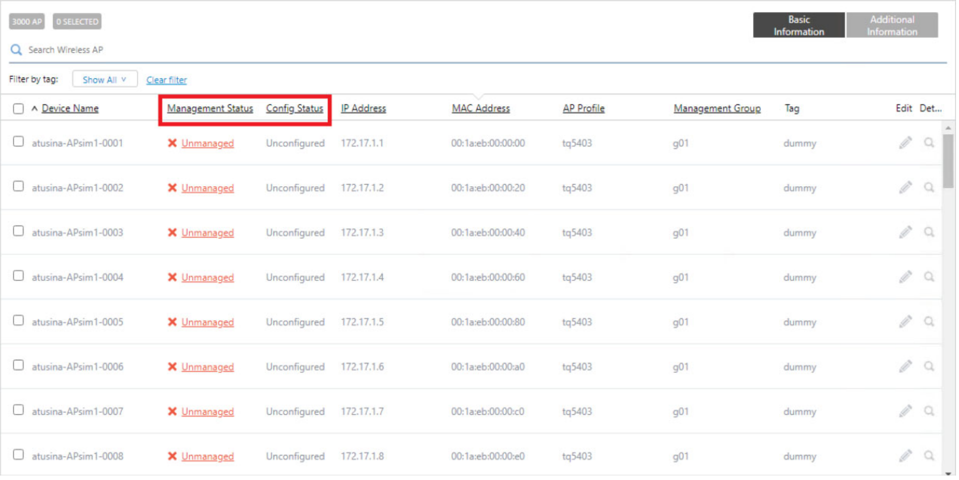
Sort by Management and Configuration status

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

From version 3.10.1 onwards, the AWC plug-in supports AP management and configuration status.

Using the **AP Settings** and **AP Status** pages, you can use sorting and search functions for easy confirmation of AP management and configuration status.

This is especially useful if you have a large number of APs, as it will be easier to find which APs are **unmanaged**. Similarly, it will be easier to find APs that have changed their settings but have not applied the settings, i.e. are in an **unconfigured** state.



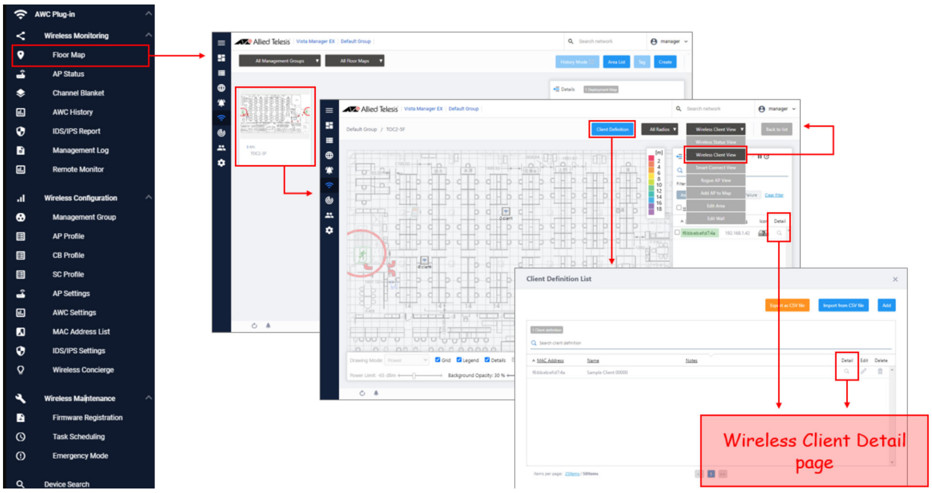
□ Device Name	Management Status	Config Status	IP Address	MAC Address	AP Profile	Management Group	Tag	Edit	Det...
□ atusina-APsim1-0001	✗ Unmanaged	Unconfigured	172.17.1.1	00:1a:eb:00:00:00	tq5403	g01	dummy		
□ atusina-APsim1-0002	✗ Unmanaged	Unconfigured	172.17.1.2	00:1a:eb:00:00:20	tq5403	g01	dummy		
□ atusina-APsim1-0003	✗ Unmanaged	Unconfigured	172.17.1.3	00:1a:eb:00:00:40	tq5403	g01	dummy		
□ atusina-APsim1-0004	✗ Unmanaged	Unconfigured	172.17.1.4	00:1a:eb:00:00:60	tq5403	g01	dummy		
□ atusina-APsim1-0005	✗ Unmanaged	Unconfigured	172.17.1.5	00:1a:eb:00:00:80	tq5403	g01	dummy		
□ atusina-APsim1-0006	✗ Unmanaged	Unconfigured	172.17.1.6	00:1a:eb:00:00:a0	tq5403	g01	dummy		
□ atusina-APsim1-0007	✗ Unmanaged	Unconfigured	172.17.1.7	00:1a:eb:00:00:c0	tq5403	g01	dummy		
□ atusina-APsim1-0008	✗ Unmanaged	Unconfigured	172.17.1.8	00:1a:eb:00:00:e0	tq5403	g01	dummy		

Troubleshooting wireless client connections

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

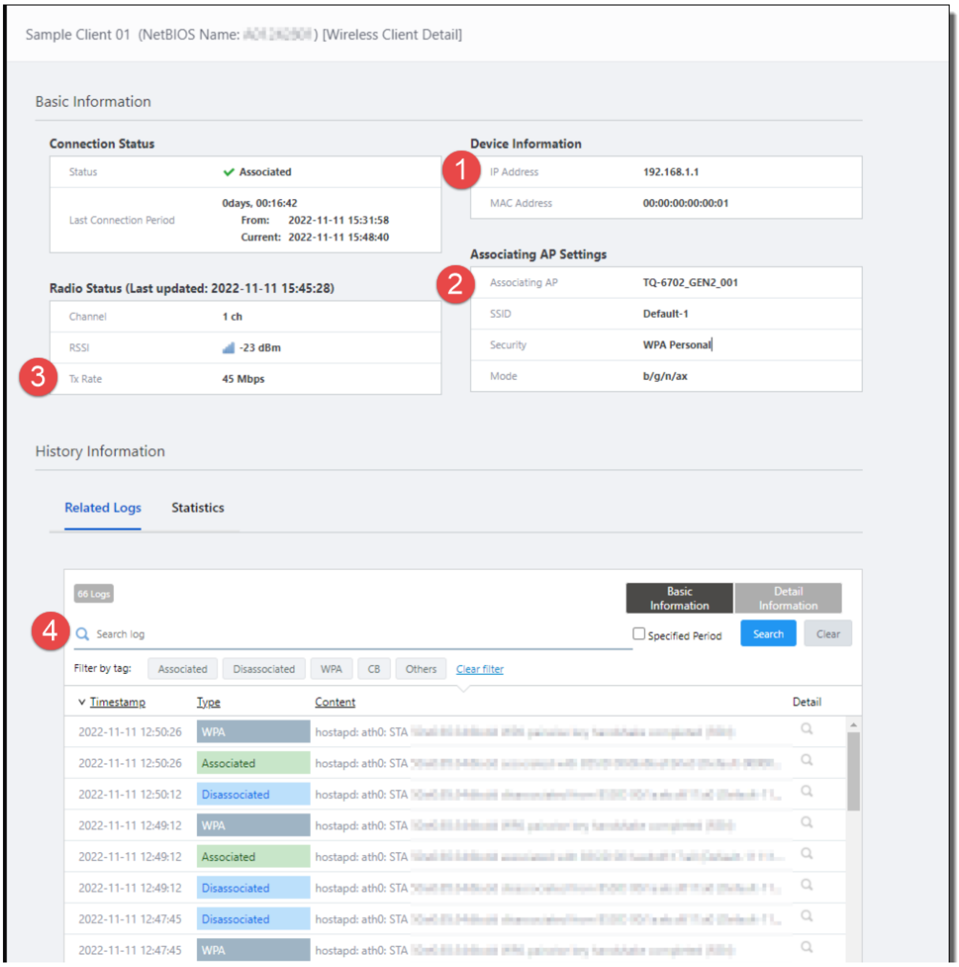
From version 3.10.1 onwards, the AWC plug-in supports the **Wireless Client Detail** page.

If a wireless client cannot connect to a wireless AP or the wireless client is connected to the wireless AP but cannot communicate, you can investigate the cause using the Wireless Client Detail page located from the **Client Definition List**.



From here you can check if the connection information is correct, for example:

1. Is the client IP address correct?
2. Is the client using the correct AP/SSID/channel?
3. Are there any abnormalities in the Tx/Rx rate?
4. Does the log information provide any reasons for the problems? Is the password correct?



Sample Client 01 (NetBIOS Name: [redacted]) [Wireless Client Detail]

Basic Information

Connection Status

Status	✓ Associated
Last Connection Period	0days, 00:16:42 From: 2022-11-11 15:31:58 Current: 2022-11-11 15:48:40

Radio Status (Last updated: 2022-11-11 15:45:28)

Channel	1 ch
RSSI	-23 dBm
Tx Rate	45 Mbps

Device Information

IP Address	192.168.1.1
MAC Address	00:00:00:00:00:01

Associating AP Settings

Associating AP	TQ-6702_GEN2_001
SSID	Default-1
Security	WPA Personal
Mode	b/g/n/ax

History Information

Timestamp	Type	Content	Detail
2022-11-11 12:50:26	WPA	hostapd: ath0: STA [redacted]	
2022-11-11 12:50:26	Associated	hostapd: ath0: STA [redacted]	
2022-11-11 12:50:12	Disassociated	hostapd: ath0: STA [redacted]	
2022-11-11 12:49:12	WPA	hostapd: ath0: STA [redacted]	
2022-11-11 12:49:12	Associated	hostapd: ath0: STA [redacted]	
2022-11-11 12:49:12	Disassociated	hostapd: ath0: STA [redacted]	
2022-11-11 12:47:45	Disassociated	hostapd: ath0: STA [redacted]	
2022-11-11 12:47:45	WPA	hostapd: ath0: STA [redacted]	

This feature requires AP firmware versions:

- *TQ1402, TQm1402: v6.0.2-0.1 or later*
- *TQ5403, TQ5403e, TQm5403: v6.0.2-0.2 or later*
- *TQ6602: v7.0.1-3.1 or later*
- *TQ6602 GEN2, TQm6602 GEN2: v8.0.2-1.1 or later*
- *TQ6702 GEN2, TQm6702 GEN2: v8.0.2-1.1 or later*

Support added for client isolation per VAP

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

From version 3.10.1 onwards, the AWC plug-in supports client isolation per VAP.

Previously, client isolation worked by not allowing a client connected to a VAP to communicate with other clients connected to the same VAP for all VAPs on a radio. This new feature will allow for VAPs to individually be configured for client isolation.

This feature requires AP firmware versions:

- *TQ6702 GEN2/TQm6702 GEN2: v8.0.2-1.1or later*
- *TQ6602 GEN2/TQm6602 GEN2: v8.0.2-1.1or later*

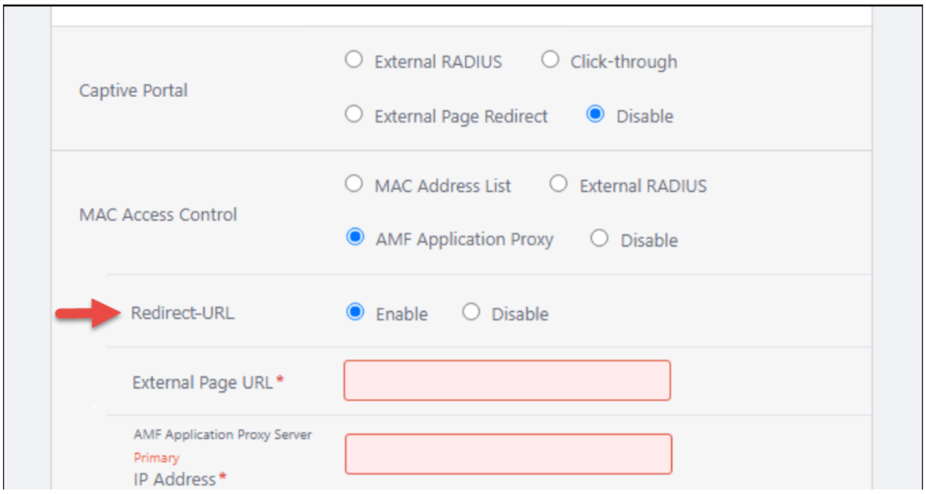
Redirect-URL function for AMF-Security

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

From version 3.10.1 onwards, the AWC plug-in supports **Redirect-URL**.

This feature redirects a user to a helpful URL when they are blocked because of an application-proxy ip-filter.

Note: Captive Portal and Application Proxy Redirect URL cannot be used together.



Captive Portal	○ External RADIUS ○ Click-through ○ External Page Redirect ● Disable
MAC Access Control	○ MAC Address List ○ External RADIUS ● AMF Application Proxy ○ Disable
Redirect-URL	● Enable ○ Disable
External Page URL *	
AMF Application Proxy Server Primary IP Address *	

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

Support for 3K MAC filters on TQ6000 GEN2 series

From version 3.10.1 onwards, the AWC plug-in supports filtering up to 3072 MAC addresses on TQ6702 GEN2, TQ6602 GEN2, TQm6702 GEN2, and TQm6602 GEN2 Access Points.

Channel Blanket auto-grouping

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

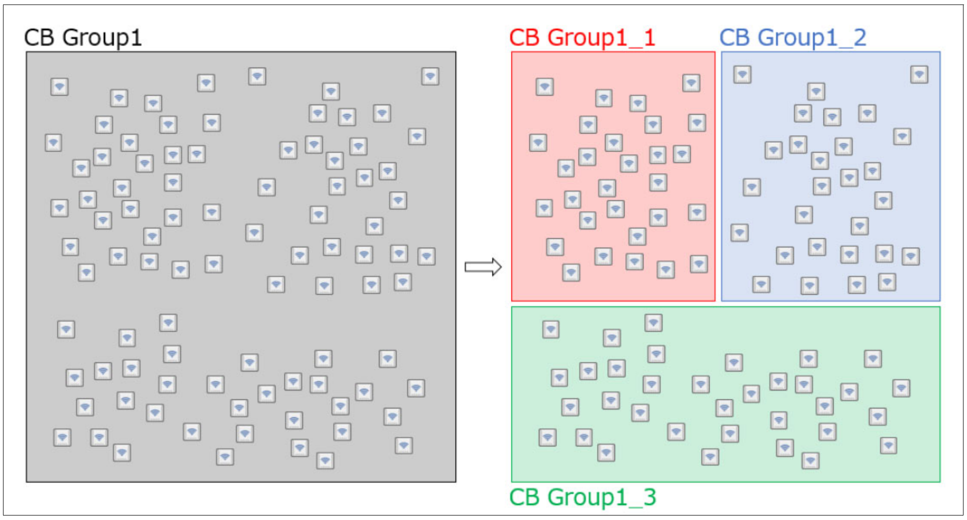
From version 3.10.1 onwards, the AWC plug-in supports AWC-CB auto-grouping. Auto-grouping is based on an AP's location on the floor MAP. This means you must place APs on the floor MAP to use auto-grouping.

AWC-CB auto-grouping allows you to automatically:

- divide single or multiple channel blankets into optimal groups
- combine multiple channel blankets into one

You can use this feature if you are creating a large scale channel blanket environment. For example, to save configuration time, you could:

- register all the APs
- create the floor map and place all the registered APs
- create only one CB profile
- create only one channel blanket in the CB profile A
- assign all registered APs to the channel blanket
- divide the channel blanket into optimal groups
- optimize and apply channel/transmit power to each group



This feature requires AP firmware versions:

- *TQ5403/TQ5403e: 6.0.2-0.2 or later*
- *TQ6602: 7.0.1-2.3 or later*
- *TQ6602 GEN2/TQ6702 GEN2: 8.0.2-1.1 or later*

Displaying the number of transmit/receive packets for Channel Blanket

From version 3.10.1 onwards, when using Channel Blanket, AWC now displays the number of packets received and transmitted by wireless clients.

New AP and CB profile settings

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

From version 3.10.1 onwards, the AWC plug-in supports some additional AP and CB profile settings.

The additional settings are:

- AP Profile: Dual[11ax] GEN2
  - Inactivity Timer
  - Security - WPA3 + Fast Roaming - 802.11k RRM
  - Security - WPA3 + Fast Roaming - 802.11v WNM
- CB Profile: AT-TQ6602, AT-TQ5403/AT-TQ5403e
  - Force Power Save Disabled

New supported countries and channels

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

From version 3.10.1 onwards, the AWC plug-in supports some additional countries and channels on the TQ6000 GEN2 series APs, with firmware v8.0.2-0.1 or later.

The new countries are:

- China
- Malaysia
- India
- Singapore
- Taiwan

DFS channel support:

- Canada
- United States

AWC-DCN (Dynamic Client Navigation)

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

From version 3.10.1 onwards, the AWC plug-in supports AWC-DCN. AWC-DCN resolves sticky client problems and improves load balancing among APs.

Sticky client

A sticky client remains connected to an AP even as the device roams further and further away from the AP. This can be frustrating because the device shows a low signal, even when standing directly underneath an AP.

In simple terms, AWC-DCN will perform the following steps:

- detect a sticky client by its Tx rates, Tx MCS indexes, Tx failure packet ratio, retransmitted packet ratio, RSSI and Signal-to-Noise ratio.
- find the best AP
- guide the sticky client to the AP

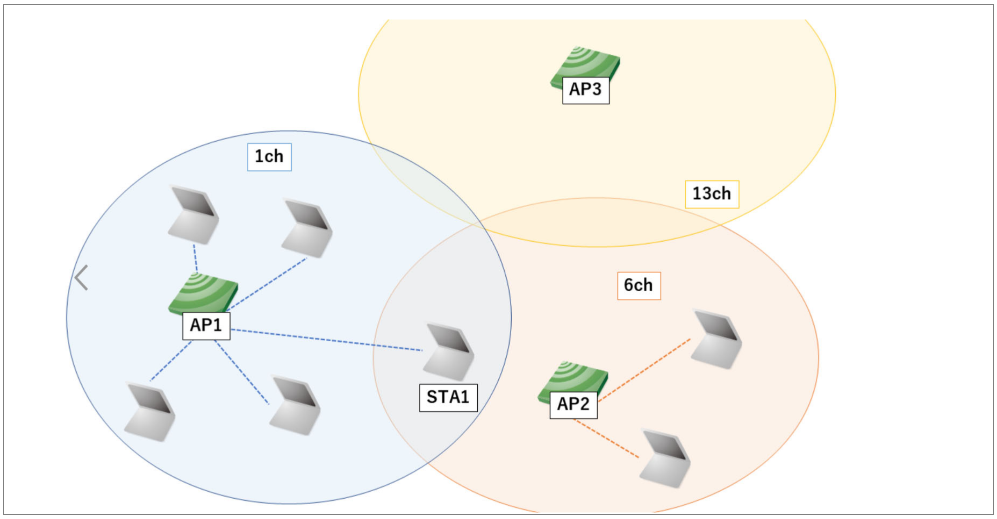
This feature uses 11k (RRM) and 11v (WNM) to achieve core operations. 11k and 11v are IEEE 802.11 standard features and currently supported by most smart phones and some laptops. Specifically, this feature uses the following 11k/11v functions:

- (11k) Beacon Request - to determine a suitable AP around the STA
- (11v) BSS Transition Management Request - to transit the STA to the AP

Load balancing

AP load can be a bad influence on the wireless communication. Load Balancing shares the load among APs when a certain threshold has been exceeded.

For example, if many clients connect to an AP and the traffic is high, AWC-DCN will change some of the clients to connect to the other low load AP.



The above figure shows that AP1 (1ch) is busy, AP2 (6ch) is not busy and AP3 (13ch) is vacant but no one can connect to it.

In the figure, the client called STA1 is connecting to AP1. If STA1 moves to AP2, the overall wireless performance will improve. AWC-DCN will detect that AP1's load is high and will lead clients to a better-suited AP.

Note: AWC-DCN can't be used together with AWC-Channel Blanket or AWC-Smart Connect

This feature requires AP firmware versions:

- *TQ6602 GEN2 v8.0.2-1.1*
- TQ6702 GEN2 v8.0.2-1.1
- Not supported on VST-APL/VRT

Resolving a rare database issue

Applicable only on VST-APL and VST-VRT.

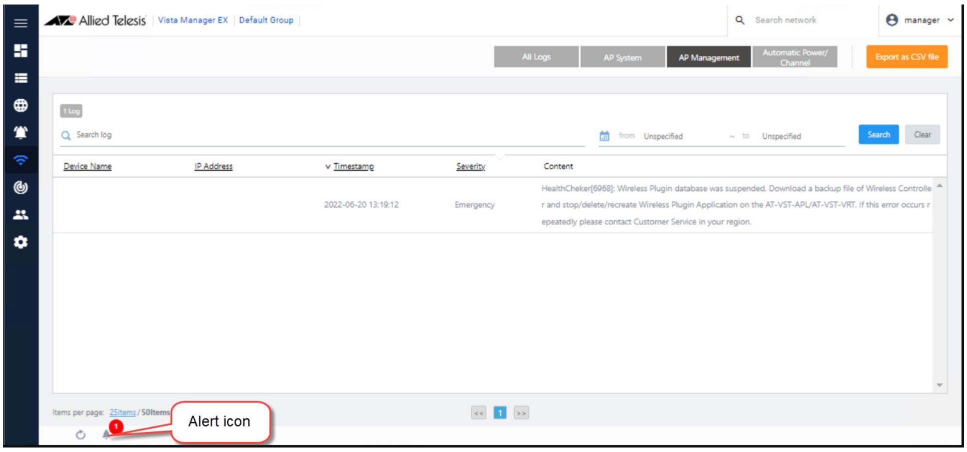
Previously, in rare cases, the AWC GUI sometimes could not be accessed. This was due to an overload of the database cache.

This issue has been resolved.

From version 3.10.1 onwards, if there is an issue with the AWC database, the database is suspended and a log produced which advises:

- the AWC Plugin database was suspended
- download a backup file of the wireless controller
- stop/delete/recreate AWC Plugin Application on the VST-APL or VST-VRT
- if this error occurs repeatedly, contact Customer Service in your region

The log page also displays an alert icon in the lower left corner. When you click on the alert icon, you are re-directed to the System settings page. You can download a backup file from the System setting page.



Device Name	IP Address	Timestamp	Severity	Content
		2022-06-20 13:19:12	Emergency	HealthCheker[6968]: Wireless Plugin database was suspended. Download a backup file of Wireless Controller and stop/delete/recreate Wireless Plugin Application on the AT-VST-APL/AT-VST-VRT. If this error occurs repeatedly please contact Customer Service in your region.

AWC plugin’s external IP address is set automatically

Applicable only on VST-APL and VST-VRT.

Previously, to install/upgrade/restore the AWC plug-in, you entered the External IP address for the AWC plugin each time via: **AWC plugin** > **System settings**

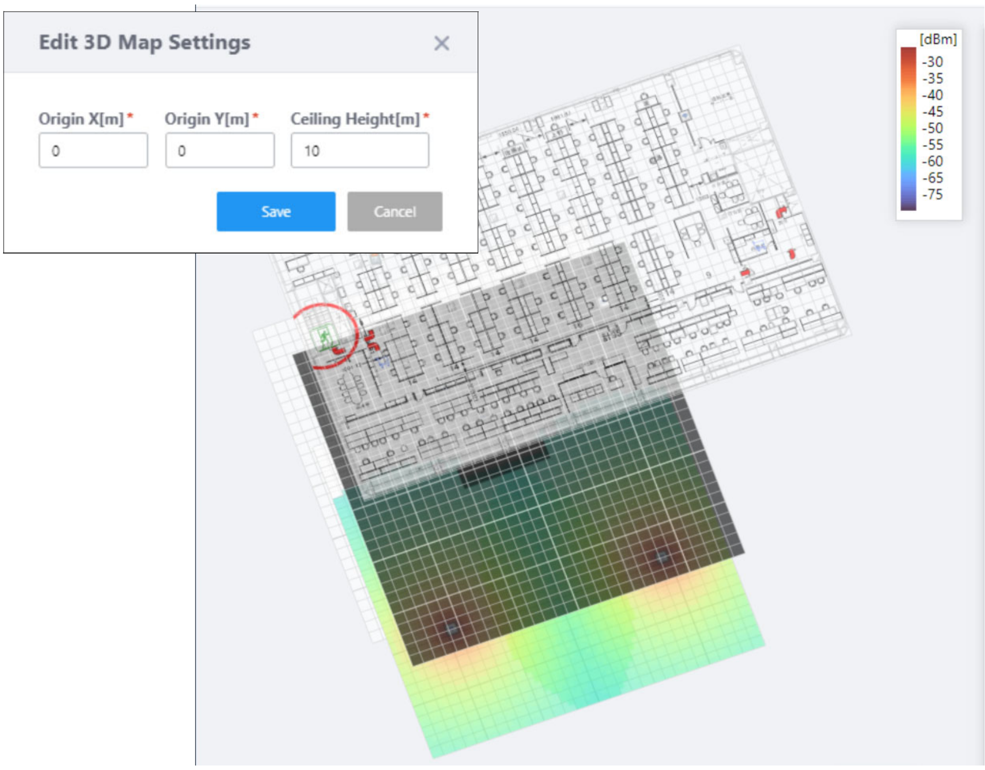
From version 3.10.1 onwards, the AWC plugin’s external IP address is set automatically.

Set a floor map origin point and ceiling height

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

From version 3.10.1 onwards, in the floor map 3D display, xy-coordinates and ceiling height can be set and reflected in the display.

Additionally, the order of overlapping floor maps can be changed by rearranging the order of the listings. All floor maps in the 3D display rotate in their entirety.



Edit 3D Map Settings

Origin X[m]*: 0

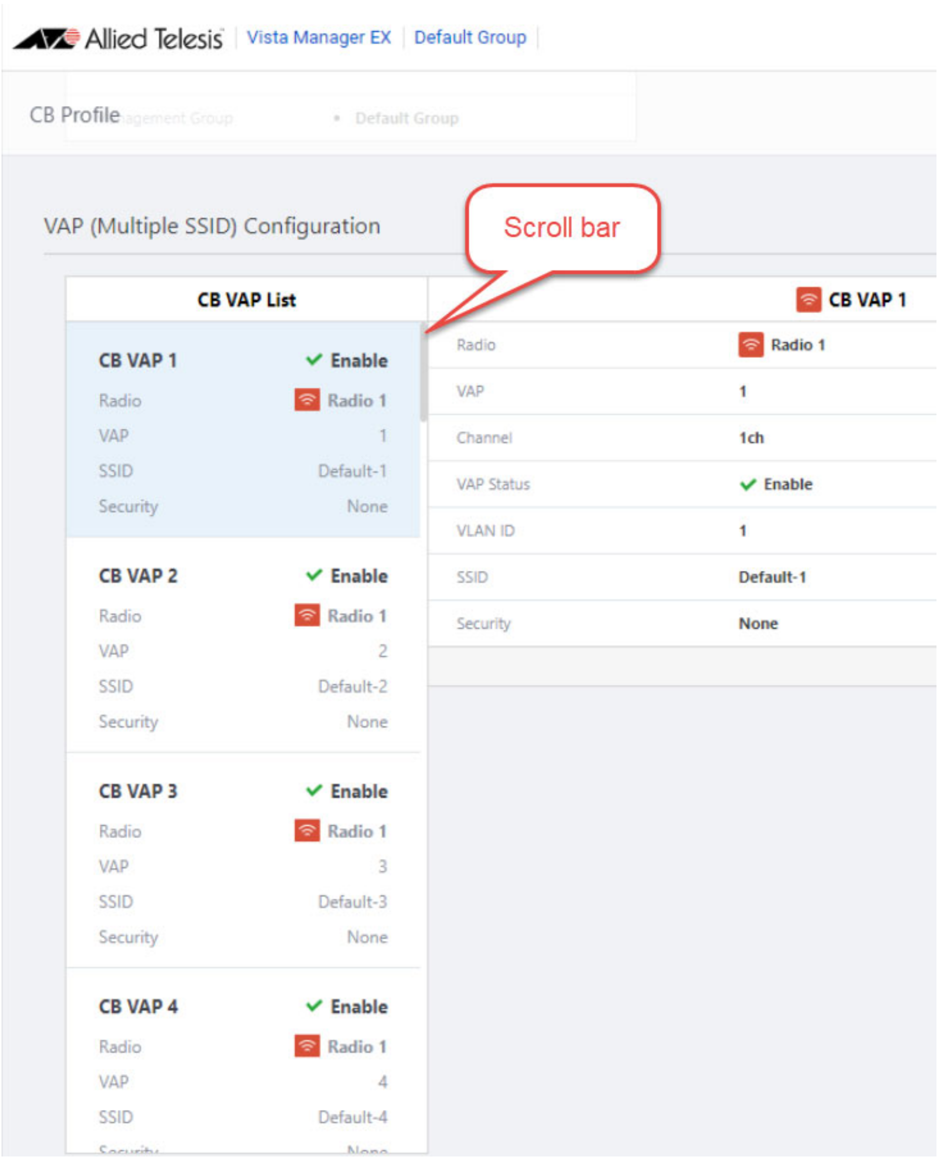
Origin Y[m]*: 0

Ceiling Height[m]*: 10

Scrolling of VAP list

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

From version 3.10.1 onwards, VAP items in the list can be scrolled on AP and CB profiles. This means you can easily set or check individual VAP details especially if there are a large number of VAPs.



Allied Telesis | Vista Manager EX | Default Group

CB Profile

VAP (Multiple SSID) Configuration

CB VAP List

CB VAP 1	✓ Enable
Radio	Radio 1
VAP	1
SSID	Default-1
Security	None

CB VAP 2	✓ Enable
Radio	Radio 1
VAP	2
SSID	Default-2
Security	None

CB VAP 3	✓ Enable
Radio	Radio 1
VAP	3
SSID	Default-3
Security	None

CB VAP 4	✓ Enable
Radio	Radio 1
VAP	4
SSID	Default-4
Security	None

CB VAP 1

Radio	Radio 1
VAP	1
Channel	1ch
VAP Status	✓ Enable
VLAN ID	1
SSID	Default-1
Security	None

Important Considerations Before Upgrading

This section describes changes that may affect Vista Manager EX or your network's behavior if you upgrade. Please read it carefully before upgrading.

AMF software version compatibility

- All AMF nodes must run version 5.4.9-0.1 or later.
- Some of the latest functionality is only available on AMF nodes running version 5.5.2-0.1 or later.

Wireless AP software version compatibility

Series	Model	Supported Versions The latest features are only available in bolded versions
Legacy	TQ4400e	4.3.2-B01
	TQ4600	4.3.2-B01
TQ1K	TQ1402 TQm1402	**6.0.2-0.1 and later versions of 6.0.2-0.x** 6.0.1-2.1 and later versions of 6.0.1-x.x 6.0.0-0.2 and later versions of 6.0.0-x.x
TQ5K	TQ5403 TQm5403 TQ5403e	**6.0.2-0.1 and later versions of 6.0.2-0.x** 6.0.1-1.1 and later versions of 6.0.1-x.x 5.4.x
TQ6K	TQ6602 TQm6602	**7.0.2-0.1**[1] **and later versions of 7.0.2-0.x** 7.0.1-0.1 and later versions of 7.0.1-x.x 7.0.0-1.1 and later versions of 7.0.0-1.x
TQ6K GEN2	TQ6602 GEN2 TQm6602 GEN2	**8.0.1-1.1 and later versions of 8.0.1-1.x**
	TQ6702 GEN2	**8.0.1-1.1 and later versions of 8.0.1-1.x** 8.0.0-0.1

[1] Coming soon

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 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.

Time taken to restore from a backup

Restoring a backup in Vista Manager EX 3.9.0 takes longer than it did in earlier versions.

Change to default value of RSSI Threshold for AWC Channel Blanket

Applicable to TQ5403, TQ5403e, TQm5403, and TQ6602 APs

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

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

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

Disabling Internet Breakout disables all PBR rules

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

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

Integrated map won’t display some links from earlier versions

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

In addition, links from SBx908 GEN1 and x200 devices will not be shown on the integrated map.

Traffic map data not restored

When you are upgrading to Vista Manager EX 3.8.0, traffic map data from earlier versions will not be imported.

Obtaining User Documentation

Vista Manager documentation

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

AMF documentation

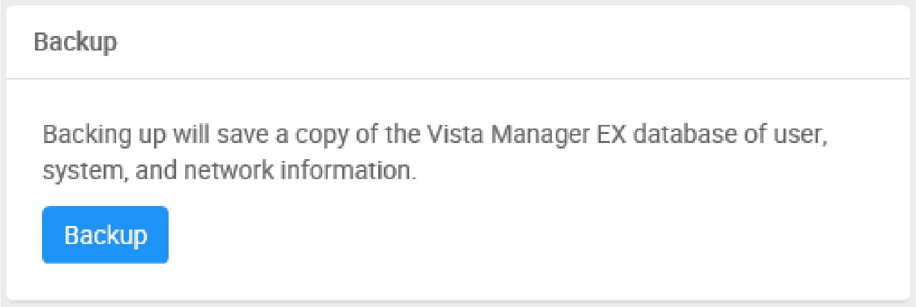
For full AlliedWare Plus documentation, see our online documentation library. For AMF, the library includes the following documents:

- the AMF Feature Overview and Configuration Guide
- the AMF Datasheet
- the AMF Cloud (VAA) Installation Guide.

Upgrading Vista Manager as a virtual appliance

To upgrade Vista Manager as a virtual appliance, use the following steps:

1. Log on to your current Vista Manager. From the System Management page, backup the database to a safe location.



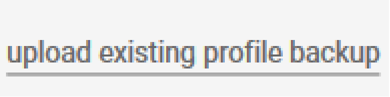
Backing up will save a copy of the Vista Manager EX database of user, system, and network information.

2. Download the software files for Vista Manager EX from the Software Download area of the Allied Telesis website.

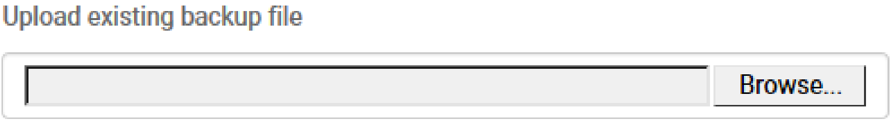
3. Import and start the new version of Vista Manager on your virtual machine host, following the instructions from the Vista Manager EX Installation on the Allied Telesis website.

4. In the new Vista Manager, log in using the default credentials.

5. A dialog displays once you have logged in. On the displayed dialog, click the “Upload existing profile backup” link.



6. Browse to and upload the backup you created in Step 1.



7. In the new Vista Manager, log in again using the credentials from your current Vista Manager. Check that everything is functioning correctly, and that your settings have been correctly imported.

8. If you use a TLS proxy to provide HTTPS access to Vista Manager, then when you are satisfied that the new Vista Manager is working correctly, reconfigure your TLS terminating proxy to point to the new Vista Manager and stop the current one.

Upgrading Vista Manager as a Windows-based installation

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

Obtain the executable files

1. Download Vista Manager EX from the Allied Telesis download center. If you are going to install the AWC and/or SNMP plug-ins then download these files from the same location.

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

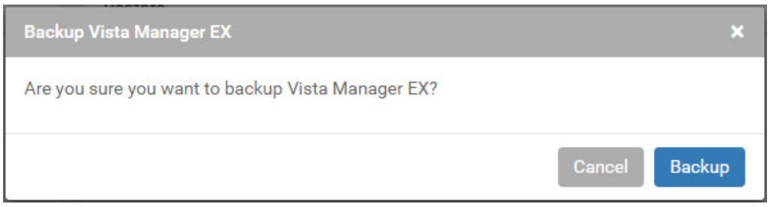
   Do not rename these files. The installation requires them to be in this format.

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

Backup Vista Manager EX and the plug-ins

Backup Vista Manager EX

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.



Backup Vista Manager EX

Are you sure you want to backup Vista Manager EX?

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\svrcmd.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

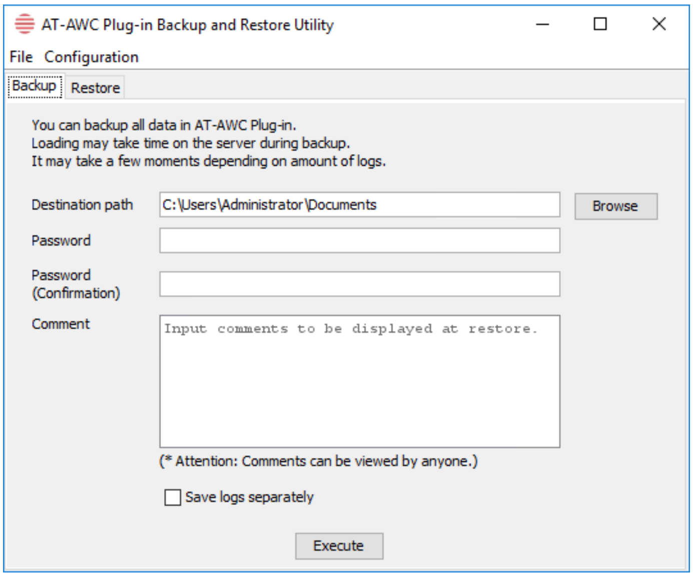
9. If you have the AWC plug-in installed then log on locally to the Vista Manager EX server.

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"**



You can backup all data in AT-AWC Plug-in.
Loading may take time on the server during backup.
It may take a few moments depending on amount of logs.

Destination path: C:\Users\Administrator\Documents

Password:

Password (Confirmation):

Comment: Input comments to be displayed at restore.

(* Attention: Comments can be viewed by anyone.)

□ Save logs separately

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

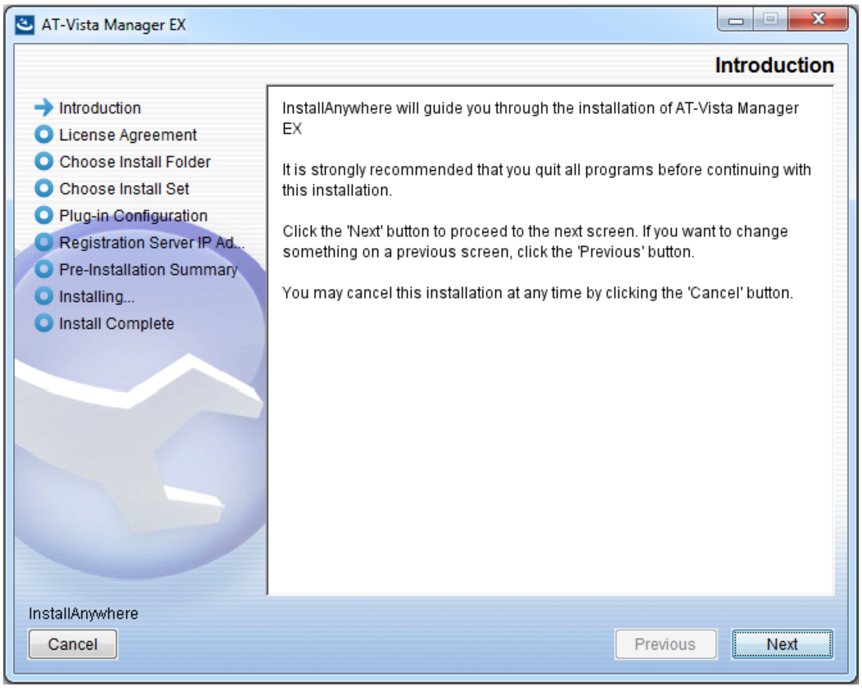
20. Reboot the system.

Install the new version

21. Execute the Vista Manager EX installation program 'atvmex*XXX*b*XX*w.exe'.

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

22. The **Introduction** dialog displays:



InstallAnywhere will guide you through the installation of AT-Vista Manager EX

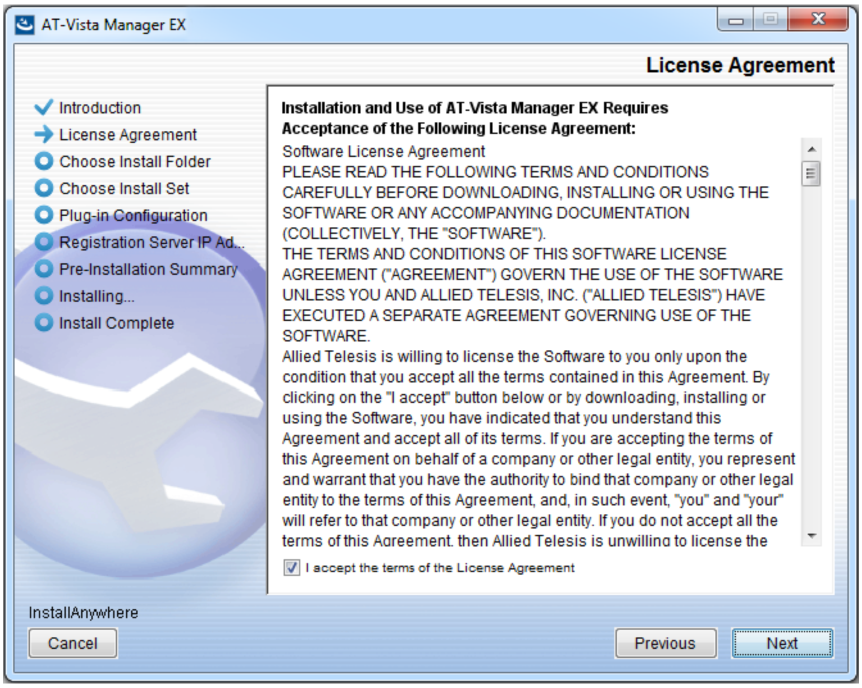
It is strongly recommended that you quit all programs before continuing with this installation.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

You may cancel this installation at any time by clicking the 'Cancel' button.

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

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



Installation and Use of AT-Vista Manager EX Requires Acceptance of the Following License Agreement:

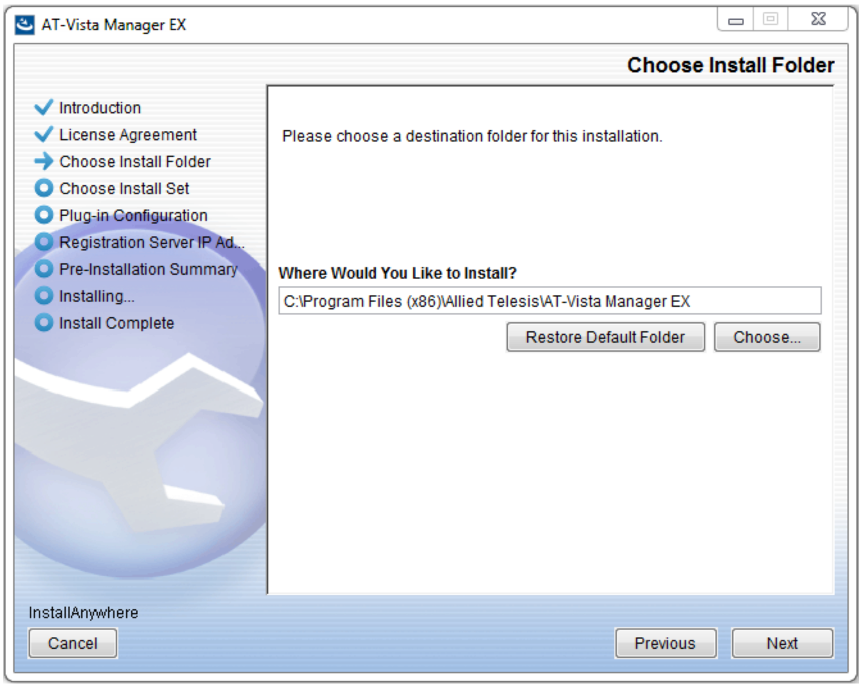
Software License Agreement
PLEASE READ THE FOLLOWING TERMS AND CONDITIONS CAREFULLY BEFORE DOWNLOADING, INSTALLING OR USING THE SOFTWARE OR ANY ACCOMPANYING DOCUMENTATION (COLLECTIVELY, THE "SOFTWARE").
THE TERMS AND CONDITIONS OF THIS SOFTWARE LICENSE AGREEMENT ("AGREEMENT") GOVERN THE USE OF THE SOFTWARE UNLESS YOU AND ALLIED TELESIS, INC. ("ALLIED TELESIS") HAVE EXECUTED A SEPARATE AGREEMENT GOVERNING USE OF THE SOFTWARE.
Allied Telesis is willing to license the Software to you only upon the condition that you accept all the terms contained in this Agreement. By clicking on the "I accept" button below or by downloading, installing or using the Software, you have indicated that you understand this Agreement and accept all of its terms. If you are accepting the terms of this Agreement on behalf of a company or other legal entity, you represent and warrant that you have the authority to bind that company or other legal entity to the terms of this Agreement, and, in such event, "you" and "your" will refer to that company or other legal entity. If you do not accept all the terms of this Agreement, then Allied Telesis is unwilling to license the

☑ I accept the terms of the License Agreement

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:



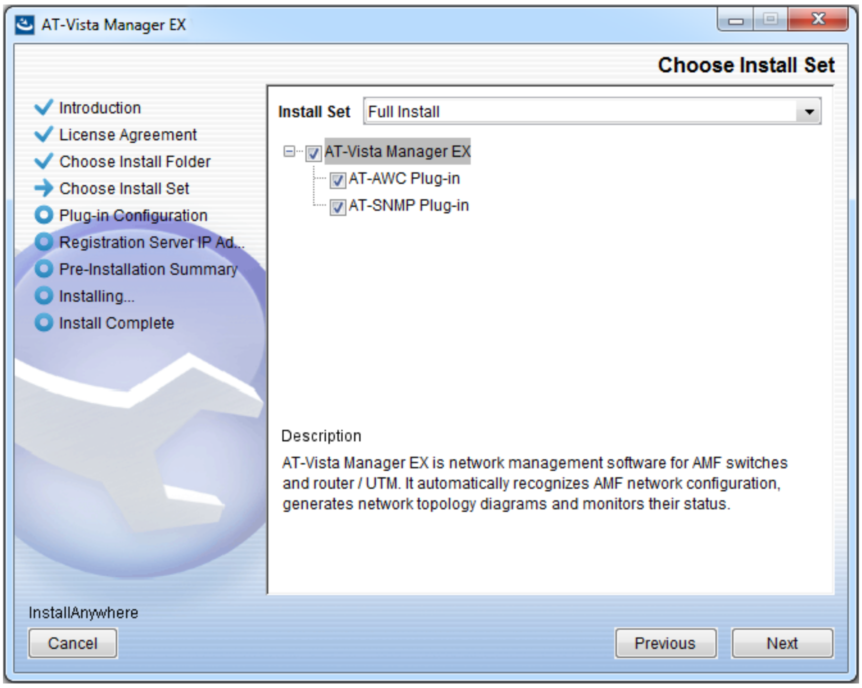
Please choose a destination folder for this installation.

Where Would You Like to Install?

C:\Program Files (x86)\Allied Telesis\AT-Vista Manager EX

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

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



Install Set: Full Install

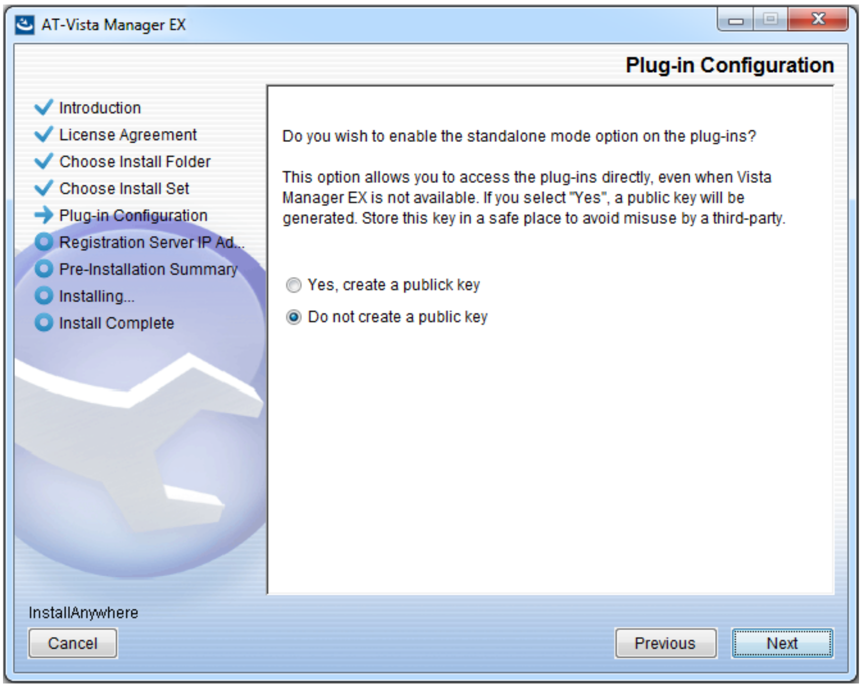
- ☑ AT-Vista Manager EX
  - ☑ AT-AWC Plug-in
  - ☑ AT-SNMP Plug-in

Description

AT-Vista Manager EX is network management software for AMF switches and router / UTM. It automatically recognizes AMF network configuration, generates network topology diagrams and monitors their status.

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:



Do you wish to enable the standalone mode option on the plug-ins?

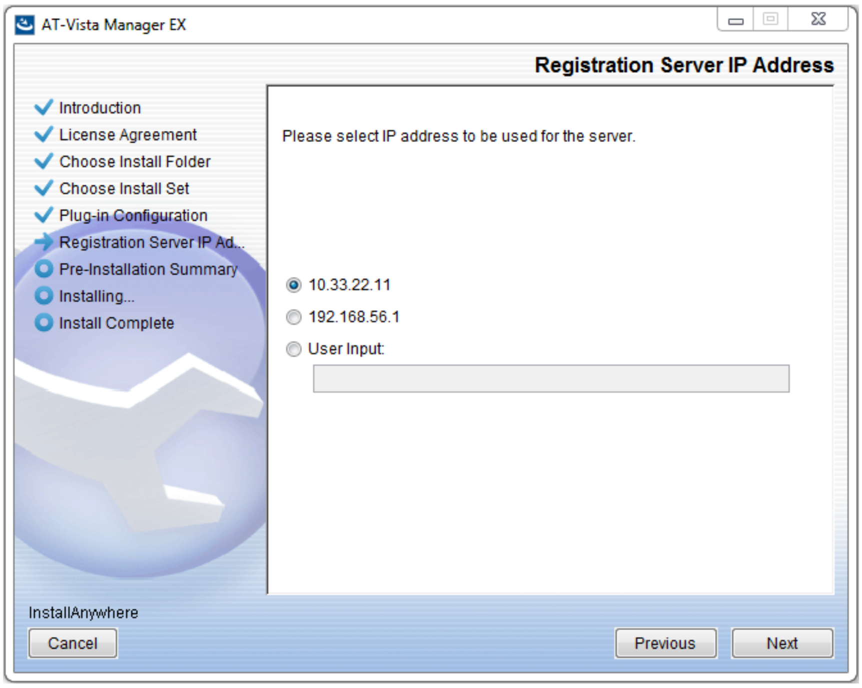
This option allows you to access the plug-ins directly, even when Vista Manager EX is not available. If you select "Yes", a public key will be generated. Store this key in a safe place to avoid misuse by a third-party.

○ Yes, create a publick key

● Do not create a public key

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:



Please select IP address to be used for the server.

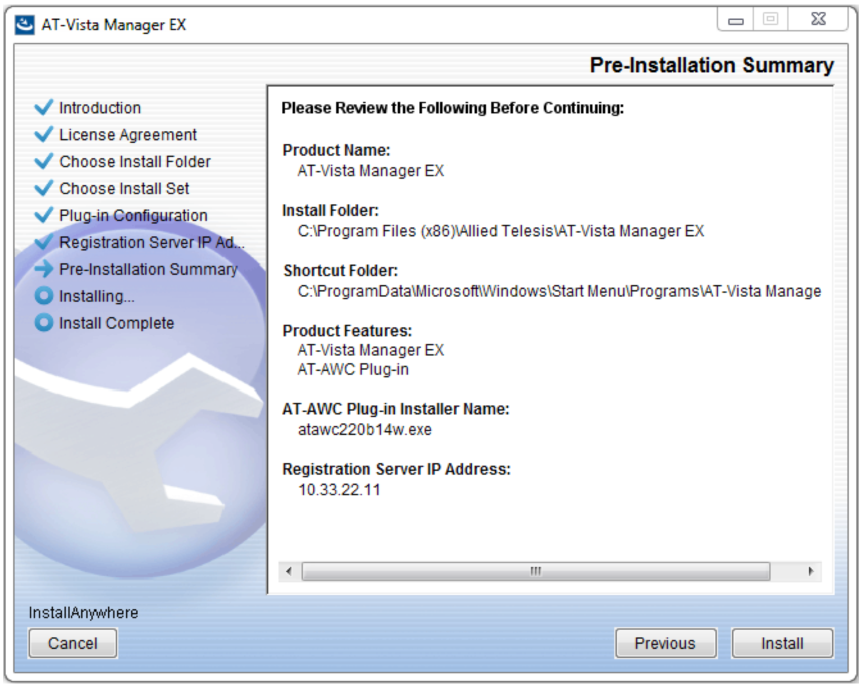
● 10.33.22.11

○ 192.168.56.1

○ User Input:

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:



Please Review the Following Before Continuing:

Product Name:
AT-Vista Manager EX

Install Folder:
C:\Program Files (x86)\Allied Telesis\AT-Vista Manager EX

Shortcut Folder:
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\AT-Vista Manage

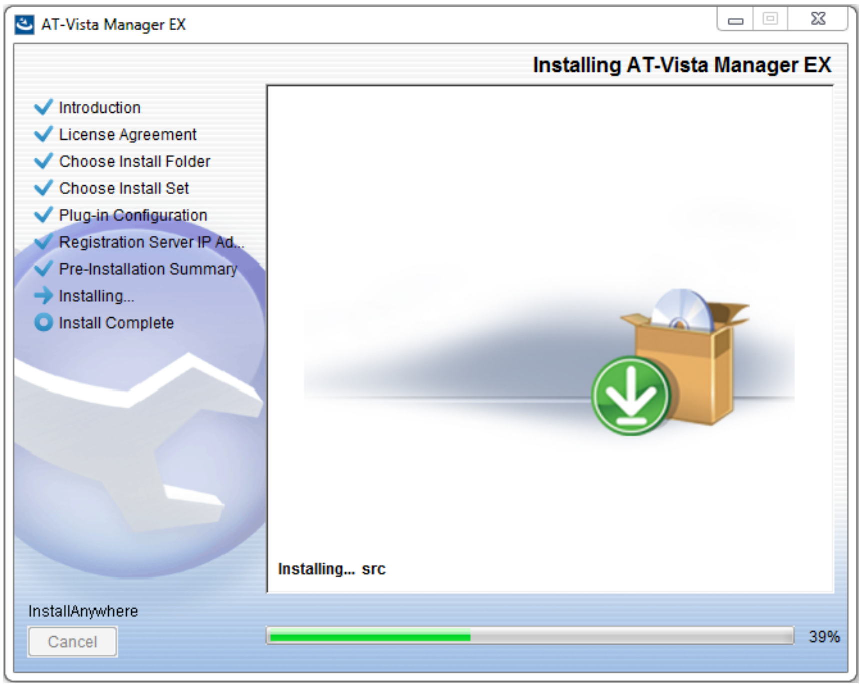
Product Features:
AT-Vista Manager EX
AT-AWC Plug-in

AT-AWC Plug-in Installer Name:
atawc220b14w.exe

Registration Server IP Address:
10.33.22.11

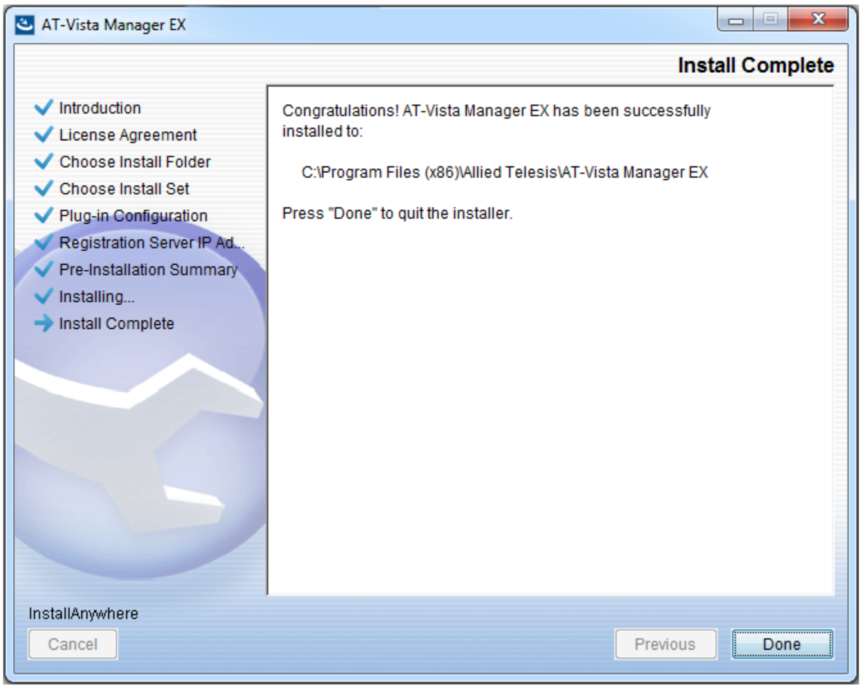
Check that your Product Name, Install Folder, Shortcut Folder, Product Features, Plug-in Installer Name and Registration IP Address are correct, and then click **Install**.

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



Installing... src

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



Congratulations! AT-Vista Manager EX has been successfully installed to:

C:\Program Files (x86)\Allied Telesis\AT-Vista Manager EX

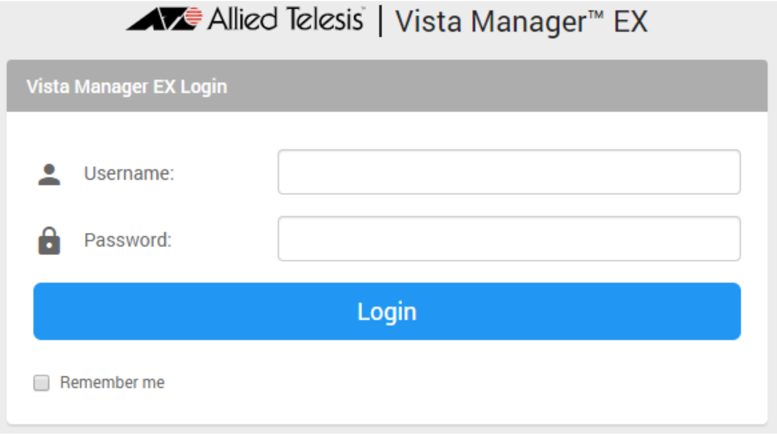
Press "Done" to quit the installer.

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.



Allied Telesis | Vista Manager™ EX

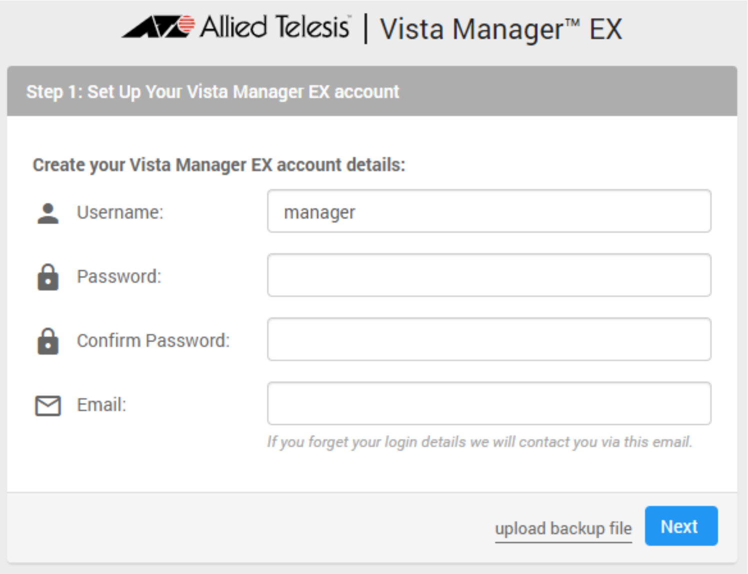
Vista Manager EX Login

Username:

Password:

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

32. Click on upload backup file.



Allied Telesis | Vista Manager™ EX

Step 1: Set Up Your Vista Manager EX account

Create your Vista Manager EX account details:

Username: manager

Password:

Confirm Password:

Email:

If you forget your login details we will contact you via this email.

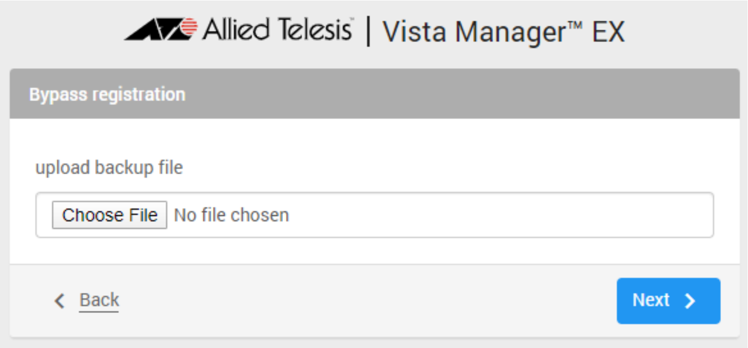
Caution

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.

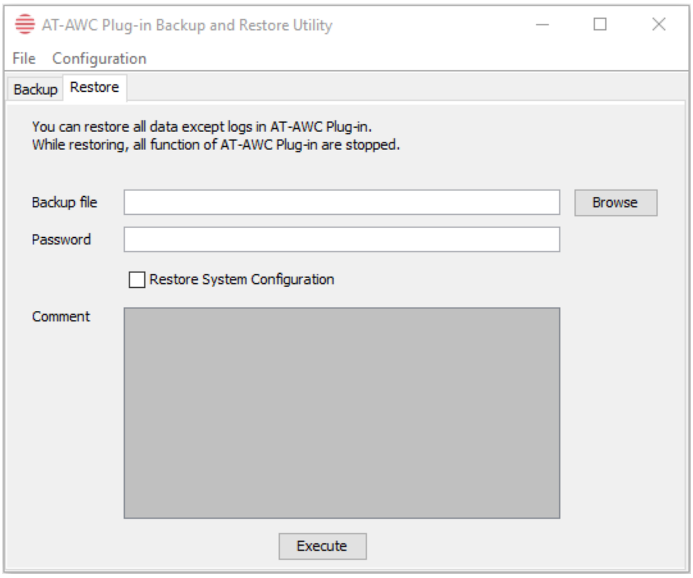
"<*Vista Install Path*>\Plugins\AT-AWC\root\stopserver.bat"

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.



You can restore all data except logs in AT-AWC Plug-in.
While restoring, all function of AT-AWC Plug-in are stopped.

Backup file

Password

□ Restore System Configuration

Comment

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

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

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

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

Upgrading Vista Manager on VST-APL

See the Vista Manager Network Appliance (VST-APL) User Guide.

Upgrading Vista Manager on VST-VRT

See the Vista Manager Virtual (VST-VRT) User Guide.

Troubleshooting

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

Allied Telesis NETWORK SMARTER

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