Allied Telesis™

Release Note for Vista Manager EX Software Version 3.9.x

VISTA MANAGER™ EX

» 3.9.0 » 3.9.1

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 v3.9.1

Introduction

This release note describes the new features in Vista Manager EX™ v3.9.1. It covers Vista Manager EX plus the optional Autonomous Wave Controller (AWC) and SNMP plugins, 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 enhancements added to Vista Manager EX v3.9.1:

- “Integration with Forescout Continuum” on page 3.
- “Issues resolved” on page 5.

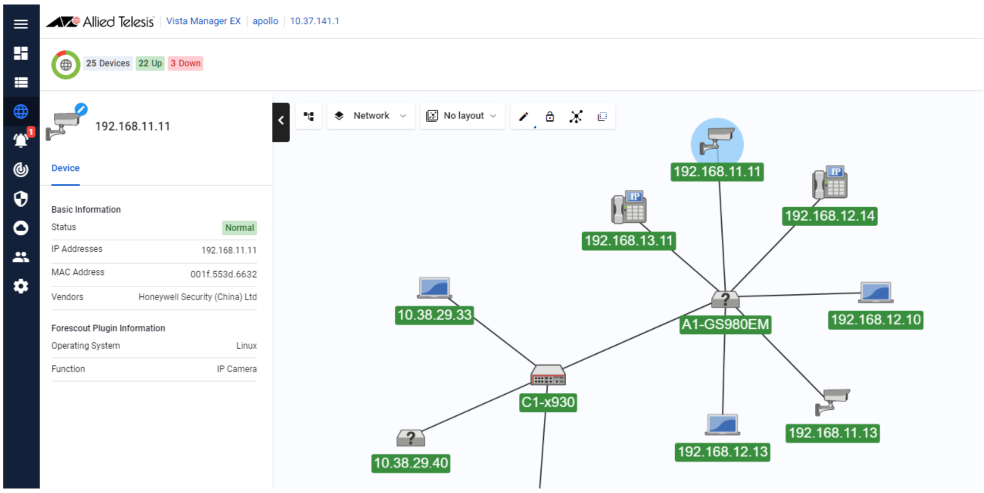
Integration with Forescout Continuum

Organizations with a large number of connected IoT devices need an easy way to manage those devices. The Forescout Continuum Platform is the most widely deployed scalable, enterprise-class solution for this. Allied Telesis has partnered with Forescout to integrate Forescout Continuum Platform with Vista Manager EX version 3.9.1 onwards.

The Forescout plugin automatically discovers non–Allied Telesis devices and displays them as dynamic icons on the integrated map. It also displays information about those devices in the side panel summary. Vista Manager polls Forescout every 5 minutes to retrieve the latest information.

Additionally, Forescout classifies each device by device type. Vista Manager then uses this information to automatically select an appropriate icon specific to each discovered device. Examples of such devices could be printers, phones, cameras or personal computers connected to your network. As a result, you see a more complete view of your network.

For example, the following figure shows a Honeywell IP camera that has been discovered through the Forescout plugin.



192.168.11.11

Device

Basic Information

Status	Normal
IP Addresses	192.168.11.11
MAC Address	001f.553d.6632
Vendors	Honeywell Security (China) Ltd

Forescout Plugin Information

Operating System	Linux
Function	IP Camera

You can also:

- create a group of Forescout-discovered devices from the map or Asset Management page. For example, you can make a group of all your printers
- change the default icon for different discovered devices
- hide and unhide discovered devices via the Edit layer of the map
- manually add custom links between a discovered device and an Allied Telesis device via the Edit layer of the map.

Note that Vista Manager EX only displays the information that Forescout has discovered. Forescout only finds links to edge devices, so the complete topology with links may not display. To resolve this, you can manually add custom links to the Vista Manager EX map.

Also, when Vista Manager EX polls Forescout, it receives the information that Forescout has at that time. If device changes do not display in Vista Manager after polling, check the update interval in Forescout.

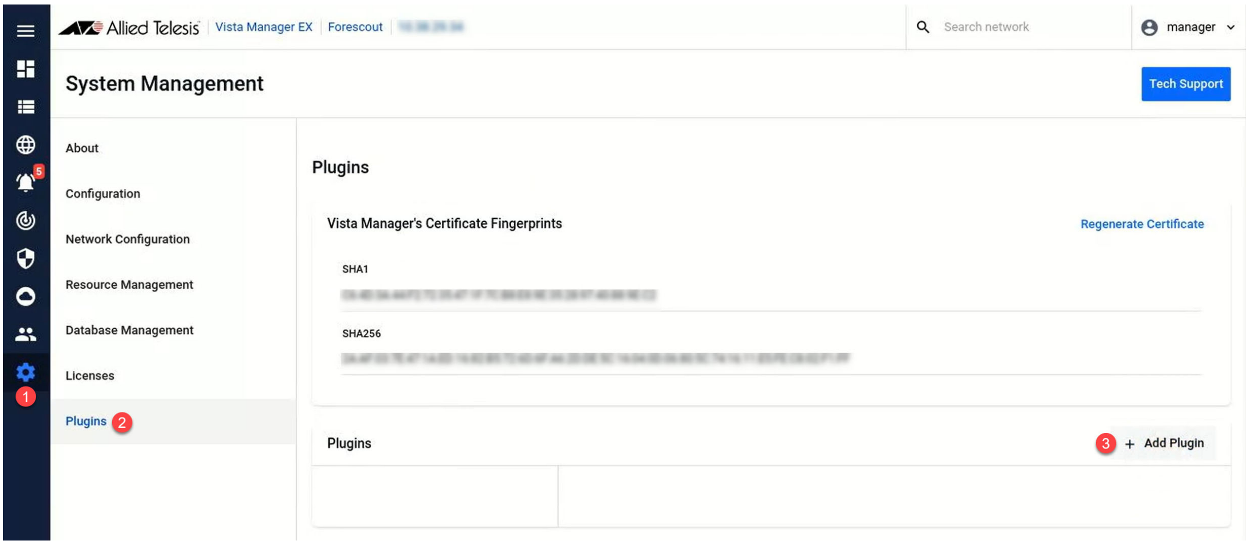
To see a demo of the plugin, watch our video on Vimeo.

Registering the plugin

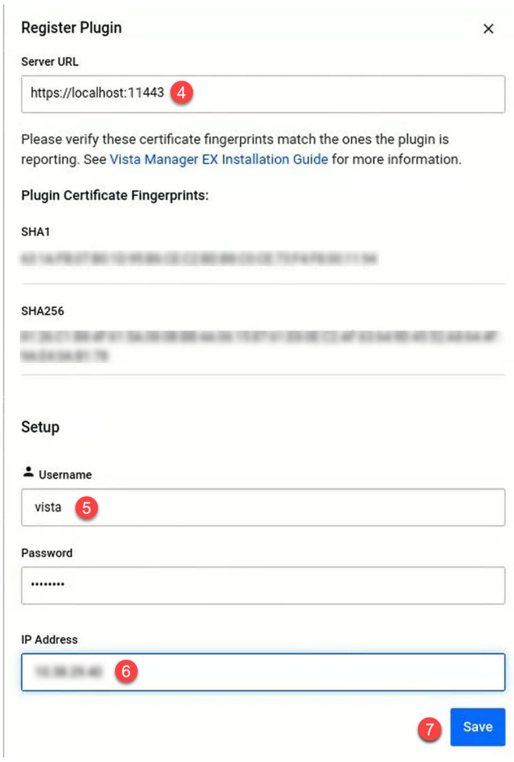
The Forescout plugin is included as part of the Vista Manager EX software package. You do not need to download it separately; just download Vista Manager EX 3.9.1 from our Software Download site.

After upgrading to version 3.9.1, you need to register the plugin. To do this:

1. Select Settings in the left-hand menu.
2. Select Plugins in the System Management sub-menu.
3. Click on the Add Plugin button.



4. The Register Plugin dialog opens. Enter the server URL, which is https://localhost:11443
5. In the Setup section, enter the username and password. You must have already created this user in the Forescout Continuum Platform.
6. Enter the IP address of the Forescout server.
7. Click Save.



Register Plugin

Server URL: https://localhost:11443

Please verify these certificate fingerprints match the ones the plugin is reporting. See Vista Manager EX Installation Guide for more information.

Plugin Certificate Fingerprints:

SHA1: [redacted]

SHA256: [redacted]

Setup

Username: vista

Password: ••••••••

IP Address: [redacted]

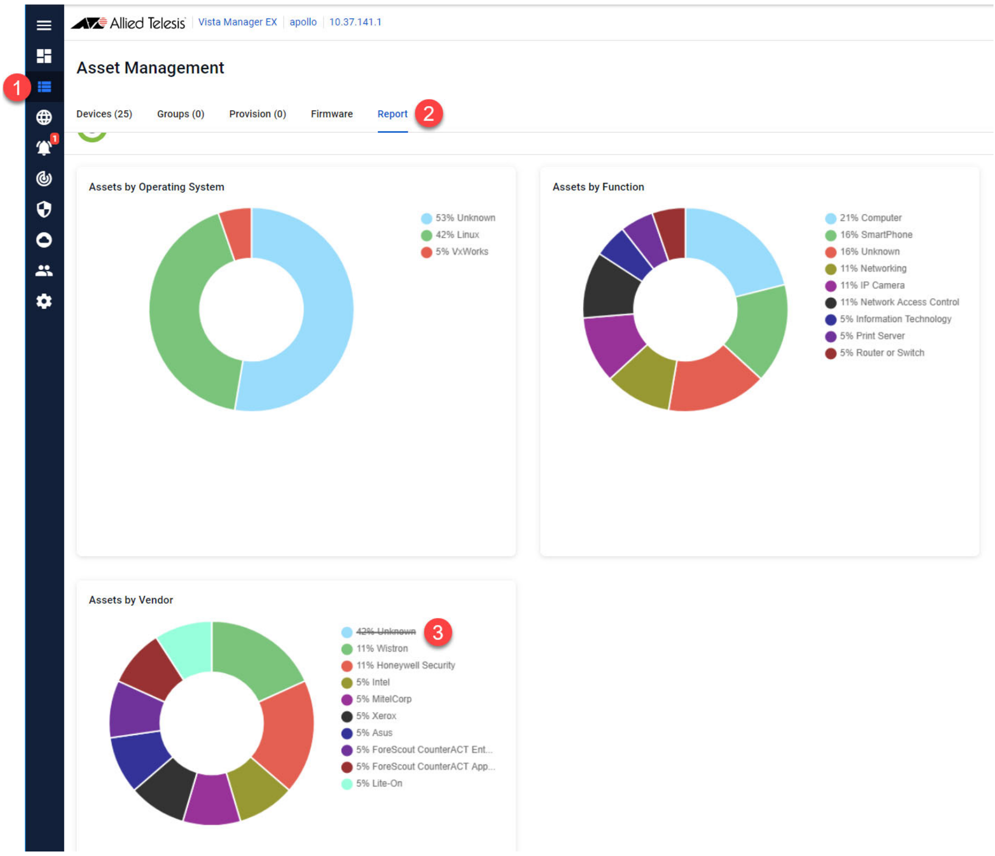
Viewing discovered devices

As well as seeing the discovered devices on the map, you can view them as assets in the Asset Management section of Vista Manager EX. To do this:

1. Select Asset Management in the left-hand menu. This displays a list of devices, including the Forescout-discovered devices. Click on the 3 dots in the Action column to rename the device or change its icon.

2. Select Report in the tabbed sub-menu. This displays graphs of the devices according to their operating system, function, and vendor.

3. If desired, you can filter the graphs to show only devices you want to see. To do this, click on an item in the graph's key to remove that item from the graph.



Issues resolved

CR-76945; CR-76835; CR-76876

The traffic map uses sflow to calculate some traffic flow statistics. If you do not configure sflow, then the traffic map will not be able to show that data but will show other statistics. Previously, in rare situations, the traffic map would fail to update any data correctly if sflow was unconfigured. This has been resolved. Vista Manager EX now displays the non-sflow statistics correctly and displays a "No data" error message for the sflow-dependent statistics.

What’s New in Vista Manager EX v3.9.0

Introduction

This release note describes the new features in Vista Manager EX™ v3.9.0. It covers Vista Manager EX plus the optional Autonomous Wave Controller (AWC) and SNMP plugins, and Allied Intent-based Orchestrator (AIO).

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

Contact your authorized Allied Telesis support center to obtain licenses.

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

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

New Features and Enhancements

This section summarizes the new features added to Vista Manager EX v3.9.0:

- “Access Control List matrix” on page 7.
- “Support for Native VLANs” on page 14.
- “RADIUS server support” on page 16.
- “Selective firmware upgrade” on page 18.
- “Enhanced event log management” on page 19.
- “Resource management” on page 20.
- “Intelligent networking and data analysis” on page 21.
- “Internet Breakout: Multiple destination interface support” on page 22.
- “Internet Breakout: Ethernet interface support” on page 23.
- “Windows 11 Pro support” on page 23.
- “Additional country support for TQ6602” on page 23.
- “TQ6602 GEN2 support” on page 24.
- “TQ6702 GEN2 support” on page 24.
- “TKIP support for TQ5403/TQ5403e/TQ6602” on page 25.
- “Technical Support Information download” on page 26.
- “Smart Connect support for TQ6602” on page 27.
- “AWC SkyDefender IP address change tool” on page 27.
- “MongoDB repair support” on page 28.

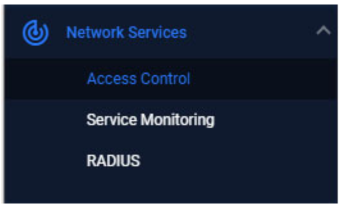
Access Control List matrix

Applicable to all Vista Manager installations.

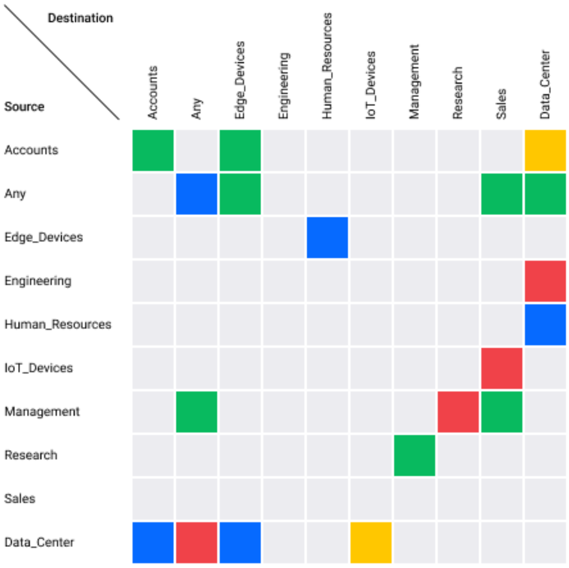
From version 3.9.0, the Access Control List Matrix provides you with a visual representation of the Access Control Lists (ACLs) applied to your network.

Using the Access Control List matrix

To view the Access Control List Matrix, from the menu select **Network Services** > **Access Control**.



This displays the Access Control List Matrix.



Source \ Destination	Accounts	Any	Edge_Devices	Engineering	Human_Resources	IoT_Devices	Management	Research	Sales	Data_Center
Accounts	🟩	⬜	🟩	⬜	⬜	⬜	⬜	⬜	⬜	🟨
Any	⬜	🟦	🟩	⬜	⬜	⬜	⬜	⬜	🟩	🟩
Edge_Devices	⬜	⬜	⬜	⬜	🟦	⬜	⬜	⬜	⬜	⬜
Engineering	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟥
Human_Resources	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟦
IoT_Devices	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟥	⬜
Management	⬜	🟩	⬜	⬜	⬜	⬜	⬜	🟥	🟩	⬜
Research	⬜	⬜	⬜	⬜	⬜	⬜	🟩	⬜	⬜	⬜
Sales	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜
Data_Center	🟦	🟥	🟦	⬜	⬜	🟨	⬜	⬜	⬜	⬜

The axes of the Access Control List Matrix show the IP host groups discovered across the network. Each host group contains one or more hosts or subnets. A host group can be used as a source or destination match in a named hardware ACL. This means only named hardware ACLs are displayed within the matrix. Using host groups is recommended, as it greatly simplifies any ACL config containing many hosts, subnets, or ports.

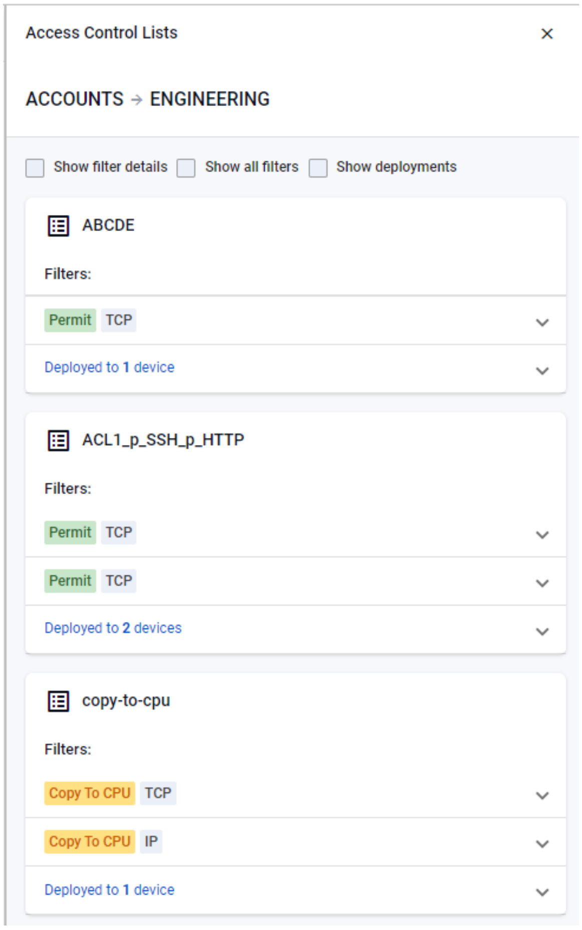
The advantage of using the Access Control List Matrix is that it provides a visual representation of the ACLs on the network. The rows and columns show which host groups are being used, and the cell color shows how they are being used. For example, it is easy to see if no ACLs exist matching network traffic from host group SALES to host group ENGINEERING. And it is simple to view an ACL's configuration by clicking on a cell.

⚪ No Action 🔴 Deny 🟢 Permit 🔵 Deny/Permit 🟡 Other

The color of each cell indicates if a matching Hardware ACL has been found for that combination of Source and Destination host groups. The cell colors show the following conditions:

Cell Color	Condition
Red	At least one deny filter is deployed in a hardware ACL for the source/destination cell combination. There are no permit filters configured for the source/destination combination.
Green	At least one permit filter is deployed in a hardware ACL for the source/destination cell combination. There are no deny filters configured for the source/destination combination.
Blue	At least one filter for both permit and deny is deployed in a hardware ACL for the source/destination cell combination.
Yellow	Filters are deployed for the source/destination cell combination, but none have a permit or deny action (for example, the **Send to CPU** action).
Grey	No filters are deployed for the source/destination cell combination.

You can click on a cell to learn more detail about the ACLs with the cell's matching source and destination host groups. The complete ACL configuration is displayed. This includes the filter type and action, and any source and destination host group or port group configuration. The network devices and switchports where a given ACL is deployed can also be seen.



Access Control Lists ×

ACCOUNTS → ENGINEERING

□ Show filter details □ Show all filters □ Show deployments

ABCDE

Filters:

Permit TCP

Deployed to 1 device

ACL1_p_SSH_p_HTTP

Filters:

Permit TCP

Permit TCP

Deployed to 2 devices

copy-to-cpu

Filters:

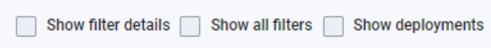
Copy To CPU TCP

Copy To CPU IP

Deployed to 1 device

There are several check boxes that provide additional information.

Filter details and deployments



□ Show filter details □ Show all filters □ Show deployments

Checking the “Show filter details” check box provides additional information about the filters.

By default, only the filters that exactly match the source/destination cells are displayed. You can check the “Show all filters” checkbox to display all filters contained in the ACL.

Checking the “Show deployments” checkbox will show which devices the filters are deployed to.

Any ACLs with identical name and configuration are aggregated in the side panel. For example, if ten switches have the same ACL, it will appear only once in the side panel. Expanding the section immediately below the ACL name will reveal where the ACL is deployed. If interfaces are not listed, then the ACL exists, but is not deployed to any switchports.

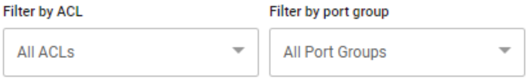
An ACL can contain multiple filter lines. Each line starts with a single action (Permit, Deny, etc), then the filter type, followed by the source and destination matching criteria. Rather than using a host group, you can use 'any' for a wildcard match for source and/or destination.

The Hardware ACLs configured on the network must use one of the following filter types to appear in the Access Control List Matrix:

- icmp
- ip
- proto
- tcp
- udp

Note: ACLs using MAC filters are not supported by the Access Control List Matrix, and are not displayed. Numbered ACLs and Software ACLs are also not supported.

Filter by ACL and port group



Filter by ACL: All ACLs

Filter by port group: All Port Groups

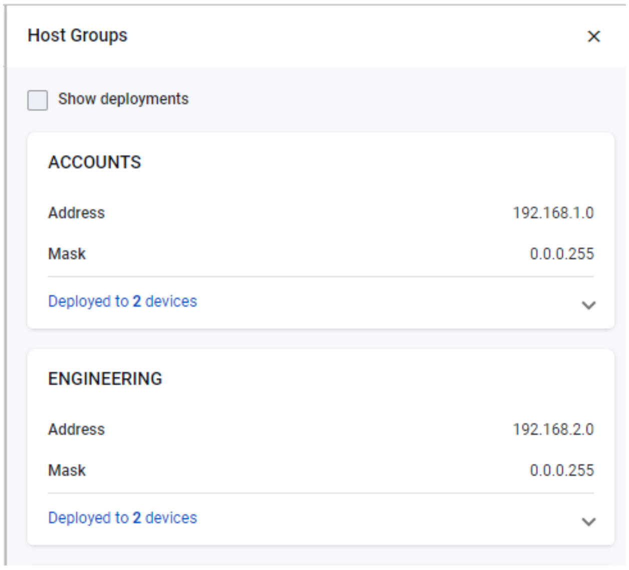
Two selection filters are available above the Access Control List Matrix. The first filter is 'Filter by ACL'. This allows you to quickly see where a single ACL exists on the matrix. The second filter is 'Filter by port group'. This lets you filter out all cells containing an ACL that does not use the specified ACL port group. Named ACL port groups contain port matching rules. For example, a port group called 'HTTP' could contain a rule to match port 80. The name given to host groups and port groups is user-defined, but should describe the group's content.

Any named hardware ACL using host groups will be displayed on the Access Control List Matrix, it does not need to be deployed. Any ACL that is deployed will show the device's name and deployed switchports under the ACL Name.

Host and port groups

Host Groups   Port Groups

The Host Groups and Port Groups buttons allow you to see all the groups that are configured on the network.



Host Groups ×

□ Show deployments

ACCOUNTS

Address	192.168.1.0
Mask	0.0.0.255

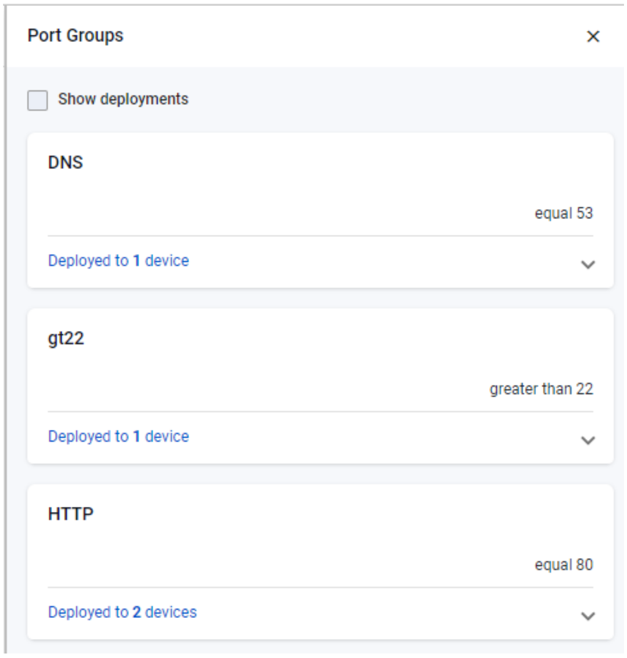
Deployed to **2** devices

ENGINEERING

Address	192.168.2.0
Mask	0.0.0.255

Deployed to **2** devices

Host groups define one or more lists of hosts using the **acl-group** command. These hosts can have masks in the same way hosts specified in existing ACLs do. The Host groups button shows details of the host groups, and where they are deployed.



Port Groups ×

□ Show deployments

DNS

equal 53

Deployed to **1** device

gt22

greater than 22

Deployed to **1** device

HTTP

equal 80

Deployed to **2** devices

Port groups define one or more lists of ports, along with their operation (equal, not equal, greater than, less than). The Port groups button shows details of the port groups, and where they are configured in the network.

Creating new hardware ACLs

Hardware ACLs and associated host/port groups can be created on a switch using the Alliedware Plus CLI. Follow these steps (in configuration mode) to create and deploy an ACL.

1. Create the source and destination IP Host Groups. These contain the hosts or subnets the ACL is to match on.

```
awplus# configure terminal
awplus(config)# acl-group ip address GUESTS
awplus(config-ip-host-group)# ip 192.168.10.0/24
awplus(config-ip-host-group)# exit
awplus(config)# acl-group ip address HEADOFFICE
awplus(config-ip-host-group)# ip 10.1.1.0/24
awplus(config-ip-host-group)# exit
```

2. Create the ACL port group containing the ports the ACL is to match on. In this example, we are going to match against SSH port 22.

```
awplus(config)# acl-group ip port SSH
awplus(config-ip-port-group)# eq 22
awplus(config-ip-port-group)# exit
```

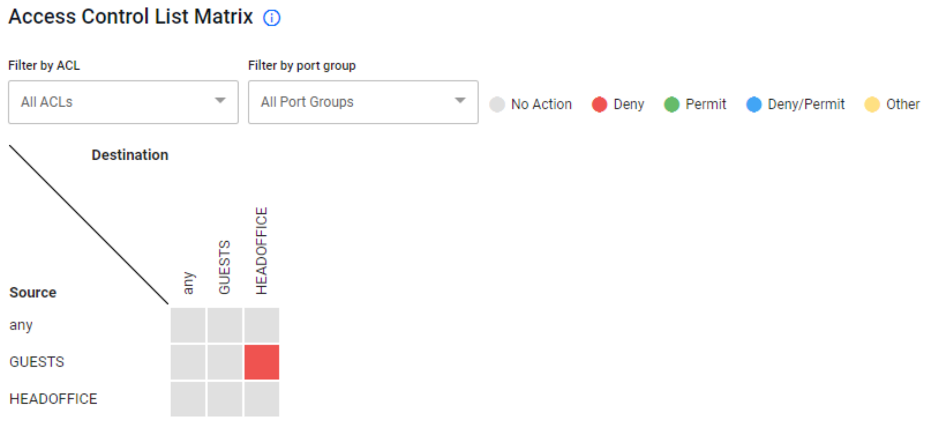
3. Create the hardware ACL to deny TCP packets matching port group SSH from source host group GUESTS to destination host group HEADOFFICE.

```
awplus(config)# access-list hardware
Deny_SSH_GUESTS_to_HEADOFFICE
awplus(config-ip-hw-acl)# deny tcp host-group GUESTS
host-group HEADOFFICE port-group SSH
awplus(config-ip-hw-acl)# exit
```

4. Deploy the ACL to a switchport.

```
awplus(config)# interface port1.0.1
awplus(config-if)# access-group Deny_SSH_GUESTS_to_HEADOFFICE
```

This ACL would display like this on the ACL Matrix:



Access Control List Matrix ⓘ

Filter by ACL: All ACLs

Filter by port group: All Port Groups

● No Action ● Deny ● Permit ● Deny/Permit ● Other

Source \ Destination	any	GUESTS	HEADOFFICE
any	⬜	⬜	⬜
GUESTS	⬜	⬜	🟥
HEADOFFICE	⬜	⬜	⬜

Converting existing hardware ACLs

ACLs that do not use ACL Host Groups can take up many lines of configuration. In the example below, a numbered hardware ACL is used to block 8 ports on two hosts:

```
awplus(config)# access-list hardware 3005_My_ACL
awplus(config-ip-hw-acl)# deny tcp 1.1.1.1/32 any eq 10
awplus(config-ip-hw-acl)# deny tcp 1.1.1.1/32 any eq 20
awplus(config-ip-hw-acl)# deny tcp 1.1.1.1/32 any eq 30
awplus(config-ip-hw-acl)# deny tcp 1.1.1.1/32 any eq 40
awplus(config-ip-hw-acl)# deny tcp 1.1.1.1/32 any eq 50
awplus(config-ip-hw-acl)# deny tcp 1.1.1.1/32 any eq 60
awplus(config-ip-hw-acl)# deny tcp 1.1.1.1/32 any eq 70
awplus(config-ip-hw-acl)# deny tcp 1.1.1.1/32 any eq 80
awplus(config-ip-hw-acl)# deny tcp 2.2.2.2/32 any eq 10
awplus(config-ip-hw-acl)# deny tcp 2.2.2.2/32 any eq 20
awplus(config-ip-hw-acl)# deny tcp 2.2.2.2/32 any eq 30
awplus(config-ip-hw-acl)# deny tcp 2.2.2.2/32 any eq 40
awplus(config-ip-hw-acl)# deny tcp 2.2.2.2/32 any eq 50
awplus(config-ip-hw-acl)# deny tcp 2.2.2.2/32 any eq 60
awplus(config-ip-hw-acl)# deny tcp 2.2.2.2/32 any eq 70
awplus(config-ip-hw-acl)# deny tcp 2.2.2.2/32 any eq 80
```

Blocking the same ports on a third host would take another 8 lines of configuration.

With ACL Host and Port Groups, the equivalent configuration would be:

```
awplus(config)# acl-group ip address My_Host_ACL_Group
awplus(config-ip-host-group)# ip 1.1.1.1/32
awplus(config-ip-host-group)# ip 2.2.2.2/32
awplus(config)# acl-group ip port My_Port_ACL_Group
awplus(config-ip-port-group)# eq 10
awplus(config-ip-port-group)# eq 20
awplus(config-ip-port-group)# eq 30
awplus(config-ip-port-group)# eq 40
awplus(config-ip-port-group)# eq 50
awplus(config-ip-port-group)# eq 60
awplus(config-ip-port-group)# eq 70
awplus(config-ip-port-group)# eq 80
awplus(config)# access-list hardware 3005_My_ACL
awplus(config-ip-hw-acl)# deny tcp host-group
My_Host_ACL_Group any port-group My_Port_ACL_Group
```

This is already a smaller configuration. But blocking the same ports on a third host would be just one extra line of configuration:

```
awplus(config)# acl-group ip address My_Host_ACL_Group
awplus(config-ip-host-group)# ip 3.3.3.3/32
```

Support for Native VLANs

Applicable to all Vista Manager installations.

From version 3.9.0 onwards, you can use the VLAN map to assign native VLANs to switchports on devices.

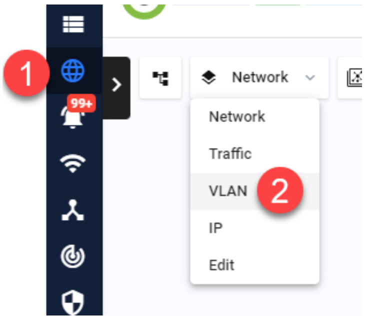
Once a port has a native VLAN, any packets received on the switchport without a VLAN tag are placed into the native VLAN. Packets leaving a switchport on the native VLAN will not be tagged.

Different native VLANs can be assigned to different switchports on a device. Only one native VLAN can exist per switchport.

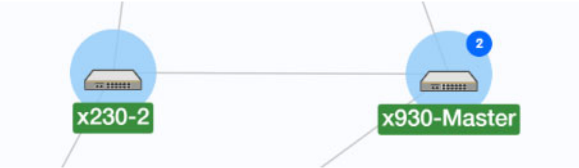
Native VLANs only apply to switchports in trunk mode, so the following procedure first uses the VLAN map to put the switchport into trunk mode, then sets the correct native VLAN:

1. In the lefthand menu, select **Network Map**.

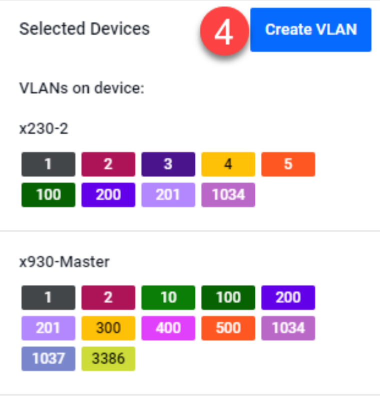
2. Select **VLAN** from the Network dropdown list.



3. Select the device or devices you want to add the VLAN to. Click to select one device, and Shift-click to select more devices.



4. Click **Create VLAN** to create a new VLAN.



Selected Devices

VLANs on device:

x230-2

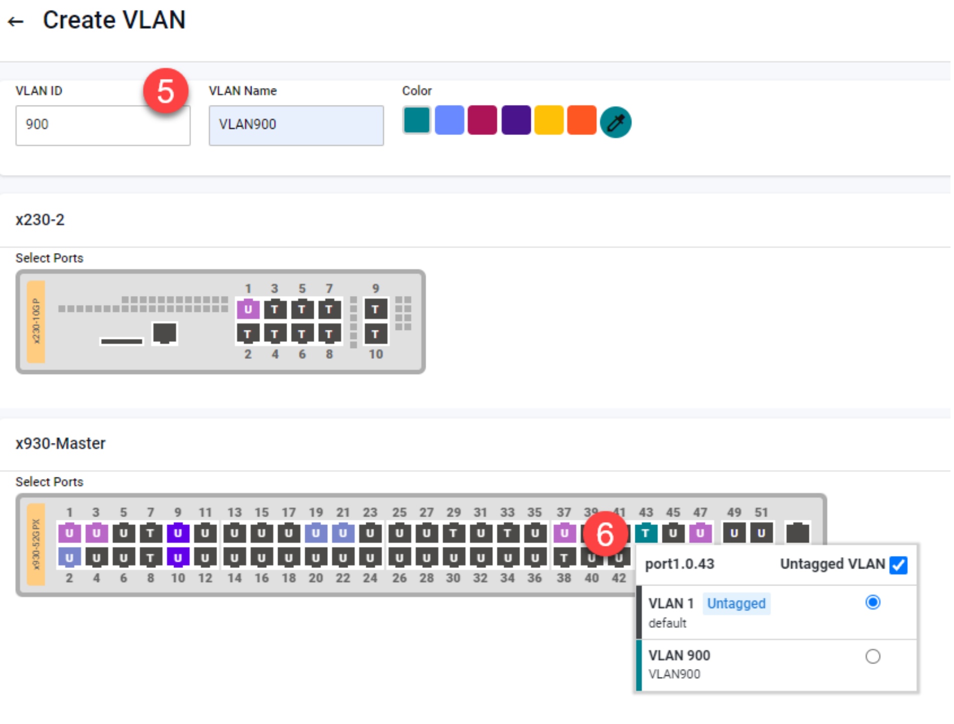
1 2 3 4 5
100 200 201 1034

x930-Master

1 2 10 100 200
201 300 400 500 1034
1037 3386

5. Enter the VLAN ID and name, and select a display color for it.

6. Click on the switchport you want to add the VLAN to, until it changes to the VLAN’s color and shows a **T** (for “trunk”).



← Create VLAN

VLAN ID: 900

VLAN Name: VLAN900

Color

x230-2

Select Ports

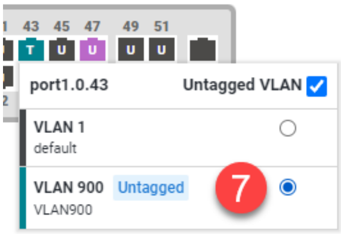
x930-Master

Select Ports

port1.0.43 — Untagged VLAN ☑

- VLAN 1 Untagged — default ●
- VLAN 900 — VLAN900 ○

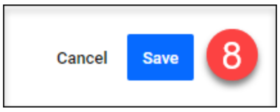
7. A pop-up will appear, showing the current native VLAN (probably VLAN 1) and the port’s other VLANs, including the new VLAN. In the pop-up, select the VLAN that you want to make the native VLAN.



port1.0.43 — Untagged VLAN ☑

- VLAN 1 — default ○
- VLAN 900 Untagged — VLAN900 ●

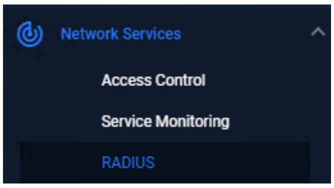
8. Click **Save** to save the configuration.



RADIUS server support

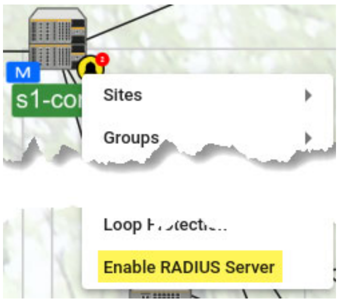
Applicable to all Vista Manager installations.

From version 3.9.0 onwards, the RADIUS server support feature lets users view and edit local RADIUS server configurations on AlliedWare Plus devices. To access this, select **Network Services** > **RADIUS** in the left-hand menu.



The RADIUS page displays a list of all AlliedWare Plus devices with local RADIUS enabled. Users with read/write permissions can perform the following RADIUS configurations:

- enable/disable RADIUS server on a device. To do this, use the context menu for the device on the Network Map:



- view a list of devices with RADIUS server enabled
- view the RADIUS server configuration of a RADIUS server–enabled device
- edit the RADIUS server user/group configuration of a device
- import/export RADIUS user settings to/from a device
- share multiple RADIUS entities from one device to another by first exporting CSV files, editing them offline and importing them onto the new device
- export RADIUS user keys to local PC in pk12 format
- export the local CA certificate to a local PC.

For selected devices, the **Users**, **Groups**, and Network Access Server (**NAS)** tabs are available on the RADIUS page.

The **Users** tab allows you to:

- add/edit/delete users to the local RADIUS server of a selected device
- import/export multiple user entries to/from a device
- manage the RADIUS group of a user
- export a pk12 file when performing 802.1x certificate–based authentication.

The **Group** tab allows you to:

- add/edit/delete groups to the local RADIUS server of a selected device
- optionally specify the Dynamic VLAN of a group
- manage the Dynamic VLAN of a group
- optionally specify the RADIUS attributes of a group
- manage/change the RADIUS attributes of a group
- see an error if attempting to delete a group that has users assigned on the device.

The RADIUS group attributes allow you to:

  - see all attributes for a group
  - add/delete one or multiple attributes to a group.

The **NAS** tab allows you to:

- add/delete a NAS to the local RADIUS server of a selected device
- manage up to 1000 network access servers.

Selective firmware upgrade

Applicable to all Vista Manager installations.

Prior to version 3.9.0, all devices in a given family are selected together when performing a firmware upgrade. With this enhancement, Vista Manager now provides the ability to exclude selected devices.

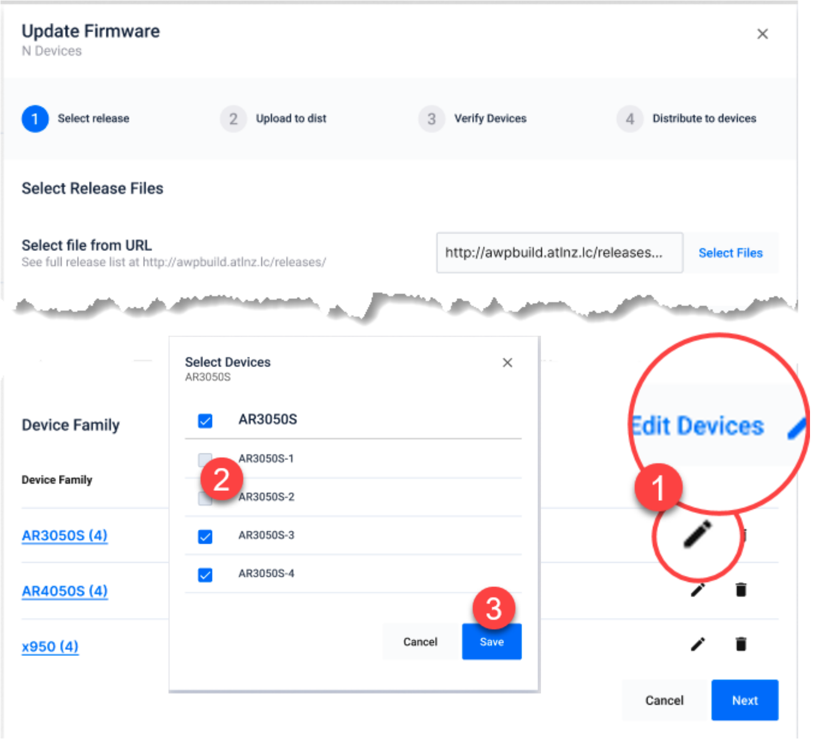
To do this, navigate to the Firmware Update wizard by selecting **Asset Management** in the left-hand menu, then select the **Firmware** tab, then click the **Update Firmware** button.

1. Select the release files from your desired location. Then click on the **Edit Devices** button or the pencil **Edit** icon in the **Action** column.

- Edit Devices - to select devices per family
- Edit action - to select devices for specific families in the same area

2. A pop-up then appears listing all devices under the device family. This allows you to deselect specific devices before upgrading the firmware.

3. Click **Save** when you have finished. The number of target devices are updated after you save the changes.



This feature is especially helpful if you need to upgrade only specific devices in a critical network, such as a hospital ICU network.

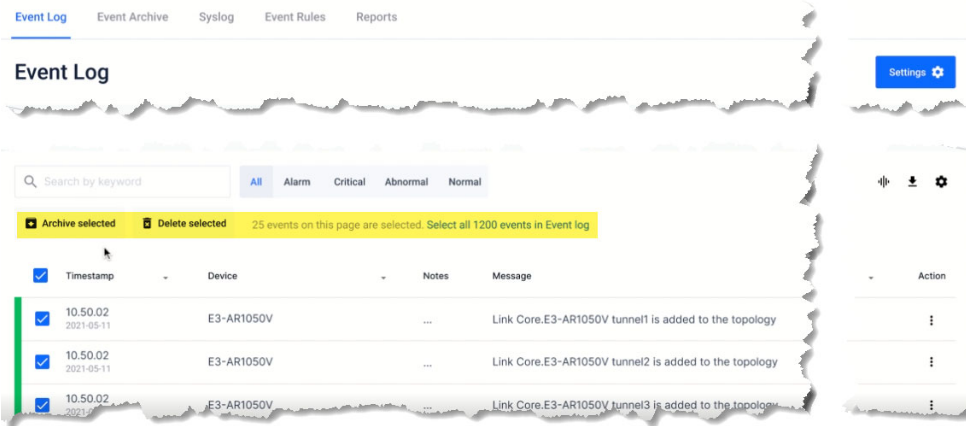
Enhanced event log management

Applicable to all Vista Manager installations.

From version 3.9.0 onwards, enhanced event log management gives you the ability to:

- export a selection of event logs (with applied filters) as a CSV file
- delete a selection or all event logs from the Event Log
- filter event logs and delete selected or matching logs from the Event Log.

To access event log management, click **Events** in the left-hand panel. The Event Log displays:

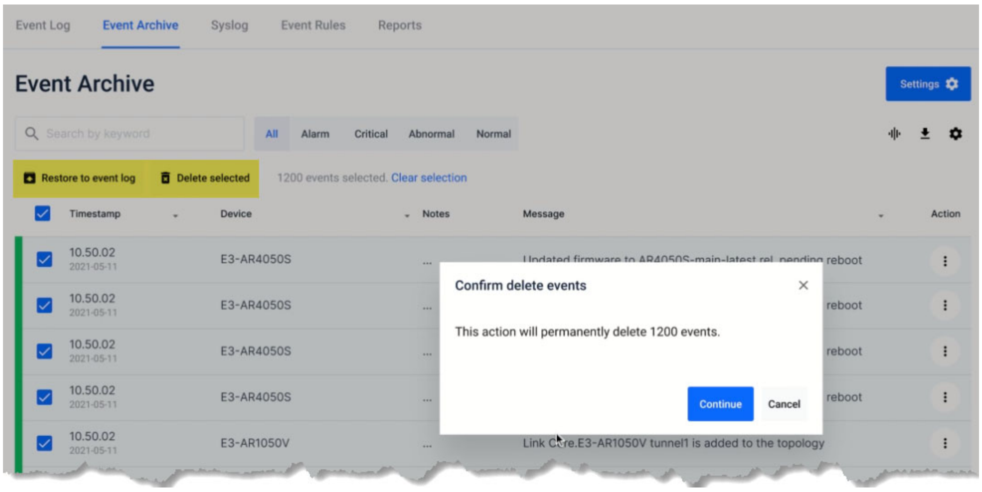


25 events on this page are selected. Select all 1200 events in Event log

☑	Timestamp	Device	Notes	Message	Action
☑	10.50.02 2021-05-11	E3-AR1050V	...	Link Core.E3-AR1050V tunnel1 is added to the topology	⋮
☑	10.50.02 2021-05-11	E3-AR1050V	...	Link Core.E3-AR1050V tunnel2 is added to the topology	⋮
☑	10.50.02 2021-0	E3-AR1050V	...	Link Core.E3-AR1050V tunnel3 is added to the topolog	⋮

From version 3.9.0 onwards, you can also:

- restore individual or all logs from the Event Archive back to the Event Log
- permanently delete logs from the Event Archive



1200 events selected. Clear selection

☑	Timestamp	Device	Notes	Message	Action
☑	10.50.02 2021-05-11	E3-AR4050S	...	Updated firmware to AR4050S-main-latest rel, pending reboot	⋮
☑	10.50.02 2021-05-11	E3-AR4050S	...	reboot	⋮
☑	10.50.02 2021-05-11	E3-AR4050S	...	reboot	⋮
☑	10.50.02 2021-05-11	E3-AR4050S	...	reboot	⋮
☑	10.50.02 2021-05-11	E3-AR1050V	...	Link Core.E3-AR1050V tunnel1 is added to the topology	⋮

Confirm delete events

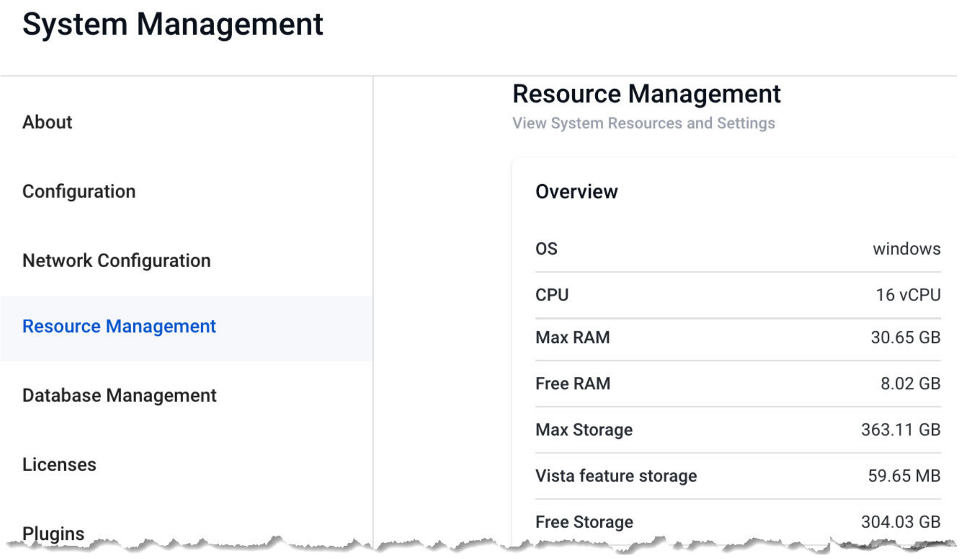
This action will permanently delete 1200 events.

A server log message is displayed after a successful restore or delete operation.

Resource management

Applicable to all Vista Manager installations.

In small and large network environments, Vista Manager needs to scale accordingly. To cater to this scenario, in version 3.9.0 a new **Resource Management** page has been added under the **System Management** menu.



OS	windows
CPU	16 vCPU
Max RAM	30.65 GB
Free RAM	8.02 GB
Max Storage	363.11 GB
Vista feature storage	59.65 MB
Free Storage	304.03 GB

From this page, you can manage what features are running and the amount of resources to use from the environment given (RAM/disk space/CPU). You can also match the resources to feature requirements and vice versa. This allows you to maximize the functionality that you need. You can also view:

- the resource consumption of Vista Manager on your machine and how much is available
- the resource consumption of Vista Manager inside a container and how much is available
- the resource consumption of each running feature
- how many event logs/syslogs are stored and how much storage they take up (total counts are only available for event logs)

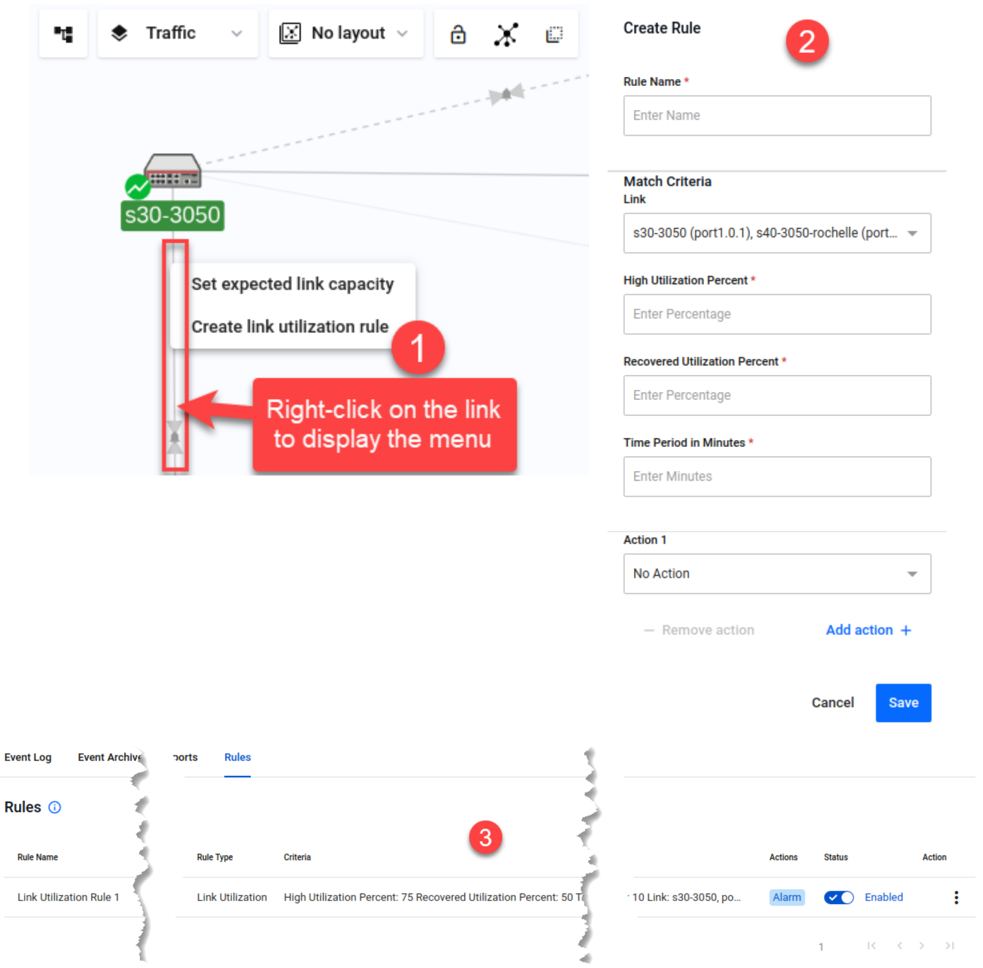
Intelligent networking and data analysis

Applicable to all Vista Manager installations.

Vista Manager version 3.9.0 is enhanced with an intelligent networking and data analysis functionality that suggests actions to improve your network or solve network issues. As a user, you are:

- able to create a rule which generates an action on any link having high utilization over a period of time (consistently oversubscribed)
- notified when any links have a high utilization (consistently oversubscribed)
- able to create a rule which generates an action on a link that no longer has high utilization
- notified when a link that previously had high utilization no longer has high utilization (recovered)
- able to configure the percentage/time period for defining high/recovered link utilization

To access this, select Network Map in the left-hand menu, then select **Traffic** from the Network dropdown list. Then right-click on a link you want to monitor.


Traffic
No layout
s30-3050
Set expected link capacity
Create link utilization rule
1
Right-click on the link to display the menu
2
3

Create Rule

Rule Name *

Enter Name

Match Criteria

Link

s30-3050 (port1.0.1), s40-3050-rochelle (port...

High Utilization Percent *

Enter Percentage

Recovered Utilization Percent *

Enter Percentage

Time Period in Minutes *

Enter Minutes

Action 1

No Action

— Remove action   Add action +

Cancel   Save

Event Log   Event Archive   ports   Rules

Rules ⓘ

Rule Name	Rule Type	Criteria		Actions	Status	Action
Link Utilization Rule 1	Link Utilization	High Utilization Percent: 75 Recovered Utilization Percent: 50 T	10 Link: s30-3050, po...	Alarm	Enabled	⋮

1

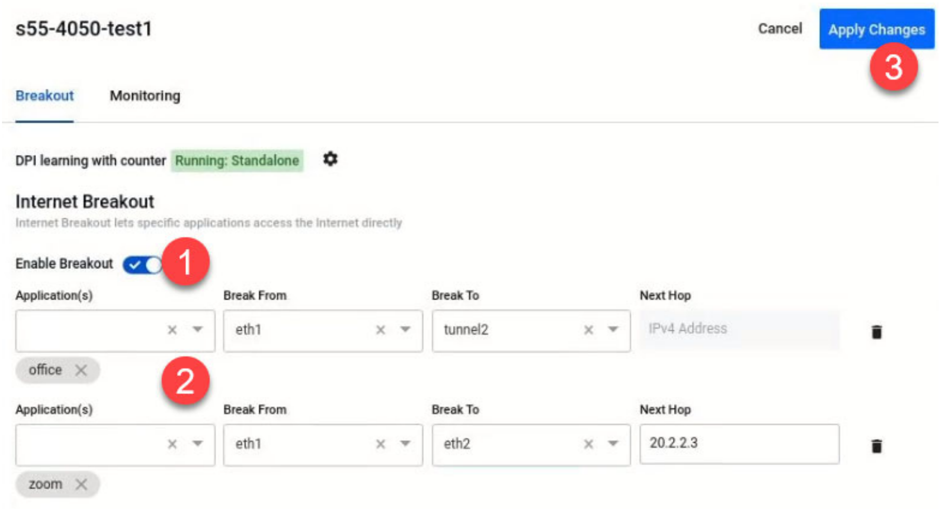
Internet Breakout: Multiple destination interface support

Applicable to all Vista Manager installations with the AIO license.

Previously, Internet Breakout only had one break-from and one break-to interface available. From version 3.9.0 onwards, you can choose multiple breakout configurations.

To access Internet Breakout, select **Allied Intent-based Orchestrator** > **Internet Breakout** in the left-hand menu.

Example: *Office365* to go directly to the internet via *tunnel2*; *Zoom* to go directly to the internet via *eth2*. After applying the changes, you will see the network zones and policies have been applied to the device.



s55-4050-test1

DPI learning with counter: Running: Standalone

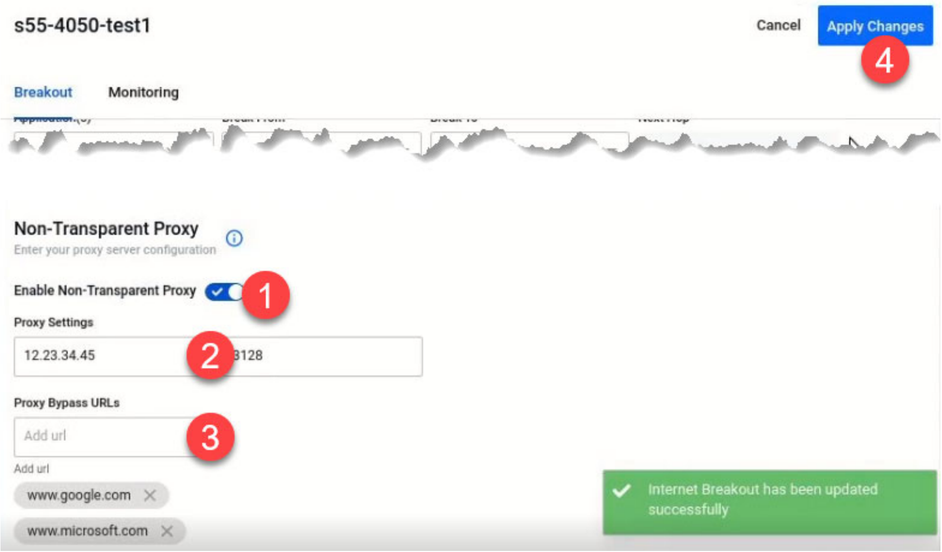
Internet Breakout

Internet Breakout lets specific applications access the Internet directly

Enable Breakout: ✓

Application(s)	Break From	Break To	Next Hop
office	eth1	tunnel2	IPv4 Address
zoom	eth1	eth2	20.2.2.3

In the Non-Transparent Proxy settings, you can also set multiple Proxy Bypass URLs.



s55-4050-test1

Non-Transparent Proxy

Enter your proxy server configuration

Enable Non-Transparent Proxy: ✓

Proxy Settings: 12.23.34.45 3128

Proxy Bypass URLs: Add url

Add url

www.google.com

www.microsoft.com

Internet Breakout has been updated successfully

After applying these changes, you will see selected Proxy Bypass URLs saved as web redirect exclusions on the device.

Internet Breakout: Ethernet interface support

Applicable to all Vista Manager installations with the AIO license.

Prior to version 3.9.0, it was only possible to choose a point-to-point interface (tunnel) in the break-from configuration of Internet Breakout. With this feature enhancement, Ethernet interface is also now supported.

To access Internet Breakout, select **Allied Intent-based Orchestrator** > **Internet Breakout** in the left-hand menu.

Note: By default, Internet Breakout inputs are disabled until Breakout or Non-Transparent Proxy is enabled. If invalid options are selected followed by disabling Internet Breakout, these options will be removed. This prevents the user from trying to save a disabled but invalid configuration.

Windows 11 Pro support

Applicable to all Vista Manager installations.

From version 3.9.0 onwards, support has been added for the Windows 11 Pro operating system.

Additional country support for TQ6602

Applicable to the AWC plugin with Access Point: TQ6602 (not TQ6602 GEN2)

From version 3.9.0 onwards, the Dual[11ax] profile supports the following countries:

- India
- Canada
- Taiwan

You can now apply these countries to TQ6602 when creating an AP profile.

To create an AP Profile, select **AWC plugin** > **Wireless Configuration** > **AP Profile** in the left-hand menu. Then click the **Create** button.

TQ6602 GEN2 support

Applicable to the AWC plugin with Access Point: TQ6602 GEN2

From version 3.9.0 onwards, the AWC plugin will support TQ6602 GEN2 APs. You can now configure, apply settings and execute operation to the TQ6602 GEN2 APs from the plugin. They use the same profile type as the TQ6702 or TQm6702 GEN2 APs.

However, the following features are **not** currently supported:

- Channel Blanket
- Smart Connect
- Openflow (SDN)
- OSEN
- Passpoint
- Second Channel
- Wireless Concierge
- Rogue Client Detection
- IPS-related features (AP De-auth Attack, etc.)

TQ6702 GEN2 support

Applicable to the AWC plugin with Access Point: TQ6702 GEN2

From version 3.9.0 onwards, the AWC plugin will also support TQ6702 GEN2 APs. You can now configure these additional features:

- Duplicate AUTH Received
- AMF application proxy
- Captive Portal
- SNMP agent
- Airtime fairness
- MU-MIMO
- OFDMA
- Inactivity timer
- Association advertisement
- Reauthentication timer
- Zero Wait DFS

Note: **Zero Wait DFS** is the only feature supported on TQ6702 GEN2 but not on the original TQ6602.

Note: Channel Blanket is not supported on TQ6702 GEN2 models.

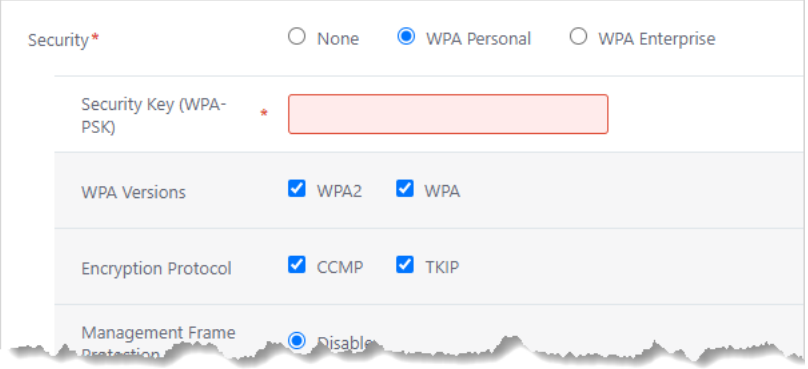
TKIP support for TQ5403/TQ5403e/TQ6602

Applicable to all Vista Manager installations with the AWC plugin.

From version 3.9.0 onwards, the AWC plugin supports the TKIP encryption protocol for these APs.

To access this, select **AWC plugin** > **Wireless Configuration** > **AP Profile** in the left-hand menu. Edit a profile or click Create to create a new profile. Select the AP type. In the VAP (Multiple SSID) Configuration section, click Detail. In the Security section, select WPA Personal or WPA Enterprise.

The Encryption Protocol setting becomes available. You can select CCMP only, or both CCMP and TKIP. Selecting only TKIP is not supported.



Security* ○ None ● WPA Personal ○ WPA Enterprise

Security Key (WPA-PSK) *

WPA Versions ☑ WPA2 ☑ WPA

Encryption Protocol ☑ CCMP ☑ TKIP

Management Frame Protection ● Disable

Similarly, you can select TKIP in a CB Profile for Channel Blanket. Follow the instructions above, but from **AWC plugin** > **Wireless Configuration** > **CB Profile** in the left-hand menu.

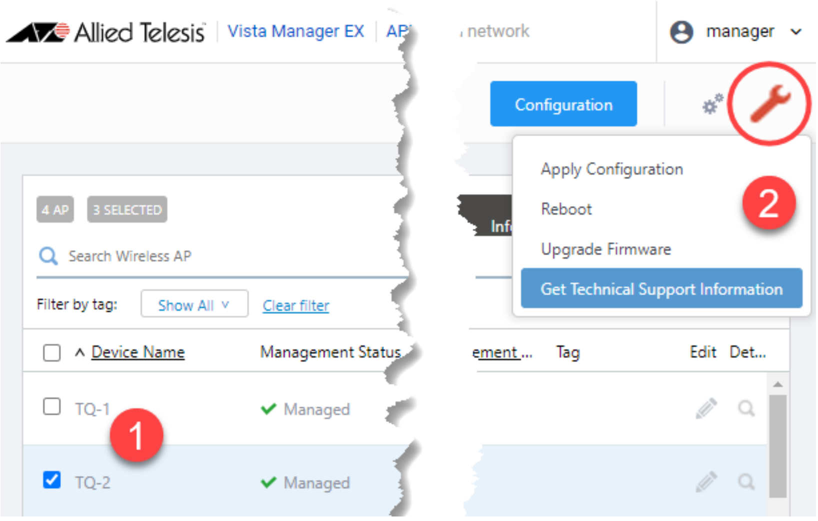
In 3.9.0, this enhancement is available on the original TQ6602, not TQ6602 GEN2.

Technical Support Information download

Applicable to all Vista Manager installations with the AWC plugin.

From version 3.9.0, you can get tech-support files via Vista Manager from a single managed AP or all of the APs that belong to an AWC-CB or AWC-SC group.

To access this feature, go to **AWC plugin** > **Wireless Configuration** > **AP Settings** and:

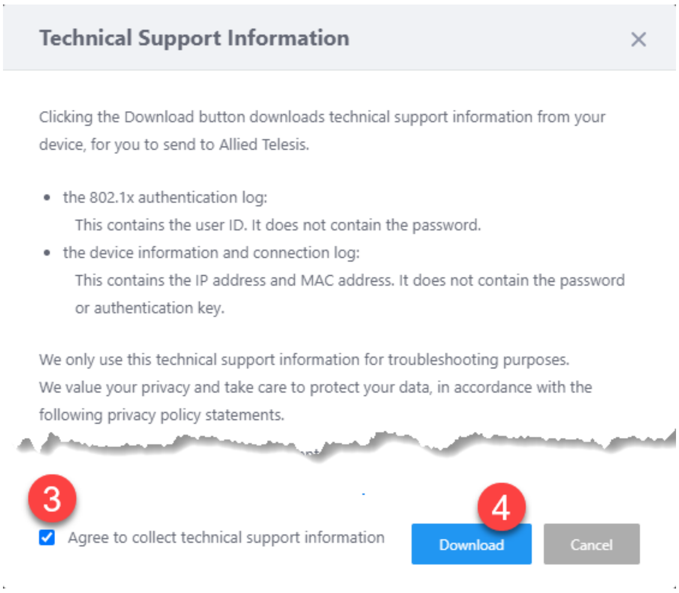


1. Use the **checkboxes** to select the AP or APs.

2. Click on the **spanner icon** and select **Get Technical Support Information**.

3. Check the **"Agree to collect technical support information".**

4. Click on **Download**.



Technical Support Information ×

Clicking the Download button downloads technical support information from your device, for you to send to Allied Telesis.

- the 802.1x authentication log:
  This contains the user ID. It does not contain the password.
- the device information and connection log:
  This contains the IP address and MAC address. It does not contain the password or authentication key.

We only use this technical support information for troubleshooting purposes.
We value your privacy and take care to protect your data, in accordance with the following privacy policy statements.

☑ Agree to collect technical support information

Download Cancel

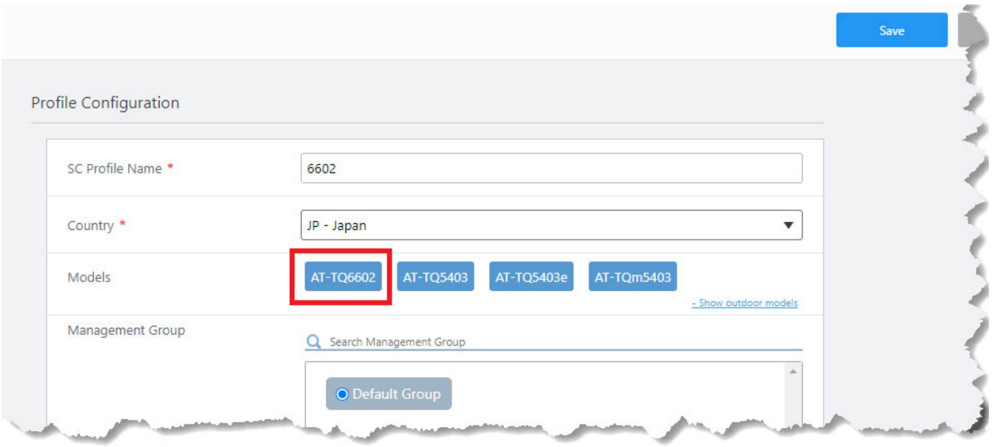
Smart Connect support for TQ6602

Applicable to the AWC plugin with Access Point: TQ6602 (not TQ6602 GEN2)

From version 3.9.0 onwards, the AWC plugin will support Smart Connect for TQ6602 models. TQ6602 is now an option when configuring a Smart Connect profile.

To create a Smart Connect profile, select **AWC plugin** > **Wireless Configuration** > **SC Profile** in the left-hand menu. Then click the **Create** button.

Unselect all models except the TQ6602.


Profile Configuration

SC Profile Name * 6602

Country * JP - Japan

Models AT-TQ6602 AT-TQ5403 AT-TQ5403e AT-TQm5403

Management Group

Default Group

Note: We recommend that you do not combine TQ5403 and TQ6602 configurations. Although this is allowed, it is not currently supported.

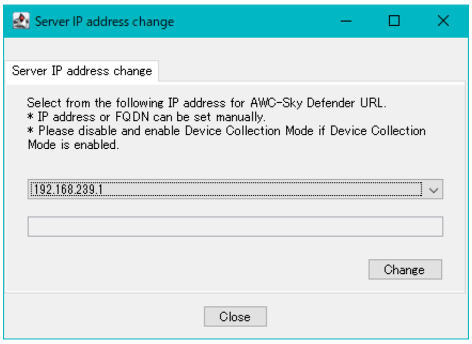
AWC SkyDefender IP address change tool

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

Some organizations may want to separate their management network from their guest network for security purposes. For this reason, the SkyDefender (AWC-SDF) IP address change tool can allow one party to connect to the guest network only, while other parties connect to the management network.

The IP address change tool sets the IP address or fully qualified domain name (FQDN) of the guest network, where AWC-SDF runs on. In this scenario, guest users and AWC-SDF users no longer need to connect to the management network. In a school environment, for example, students and teachers do not have to connect to the management network.

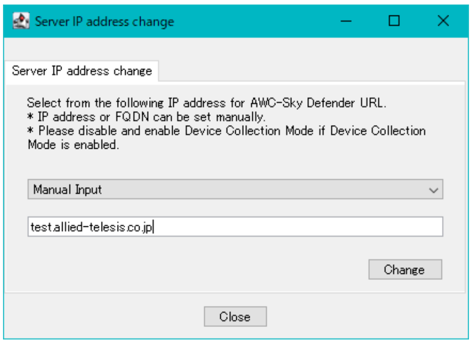
As an admin user, you can either select an IP address from the list or manually input one.


Server IP address change

Server IP address change

Select from the following IP address for AWC-Sky Defender URL.
* IP address or FQDN can be set manually.
* Please disable and enable Device Collection Mode if Device Collection Mode is enabled.

192.168.239.1


Server IP address change

Server IP address change

Select from the following IP address for AWC-Sky Defender URL.
* IP address or FQDN can be set manually.
* Please disable and enable Device Collection Mode if Device Collection Mode is enabled.

Manual Input

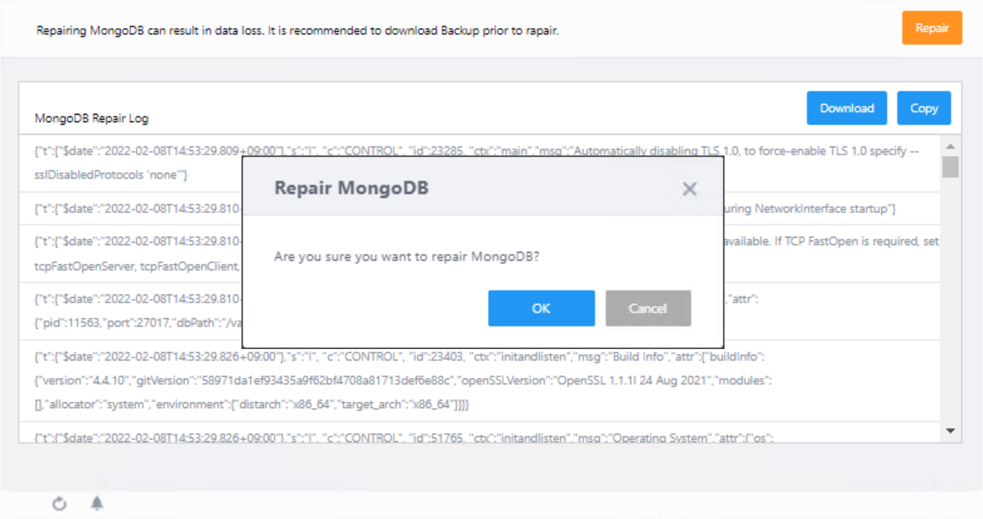
test.allied-telesis.co.jp

For more information on the tool configuration, see the AWC User Guide.

MongoDB repair support

Applicable to all Vista Manager installations with the AWC plugin.

There are a small number of situations when the AWC's MongoDB can suddenly fail with corrupted data files. From version 3.9.0 onwards, administrator users can access a GUI page to execute a MongoDB repair command. The command rebuilds corrupted data and removes the dirty cache in MongoDB. Non-authorized users are redirected to an error page.



Repairing MongoDB can result in data loss. It is recommended to download Backup prior to rapair.

```
{"t":{"$date":"2022-02-08T14:53:29.809+09:00"},"s":"I", "c":"CONTROL", "id":23285, "ctx":"main","msg":"Automatically disabling TLS 1.0, to force-enable TLS 1.0 specify --
sslDisabledProtocols 'none'"}
{"t":{"$date":"2022-02-08T14:53:29.810-                                                      uring NetworkInterface startup"}
{"t":{"$date":"2022-02-08T14:53:29.810-                                                      available. If TCP FastOpen is required, set
tcpFastOpenServer, tcpFastOpenClient,
{"t":{"$date":"2022-02-08T14:53:29.810-                                                      ,"attr":
{"pid":11563,"port":27017,"dbPath":"/va
{"t":{"$date":"2022-02-08T14:53:29.826+09:00"},"s":"I", "c":"CONTROL", "id":23403, "ctx":"initandlisten","msg":"Build Info","attr":{"buildInfo":
{"version":"4.4.10","gitVersion":"58971da1ef93435a9f62bf4708a81713def6e88c","openSSLVersion":"OpenSSL 1.1.1l 24 Aug 2021","modules":
[],"allocator":"system","environment":{"distarch":"x86_64","target_arch":"x86_64"}}}}
{"t":{"$date":"2022-02-08T14:53:29.826+09:00"},"s":"I", "c":"CONTROL", "id":51765, "ctx":"initandlisten","msg":"Operating System","attr":{"os":
```

Repair MongoDB

Are you sure you want to repair MongoDB?

To access this feature, browse to:
http://<*vista-manager-ex_ip_address*>**/plugin-proxy/awc/system/repair_mongodb**.

You can:

- execute the repair command
- download the command log
- copy the command log to the clipboard
- view the command results.

Running MongoDB repair is required when an AWC container consumes most of the disk space, due to MongoDB's downtime prompting restarts with corrupted data.

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 plugin** > **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

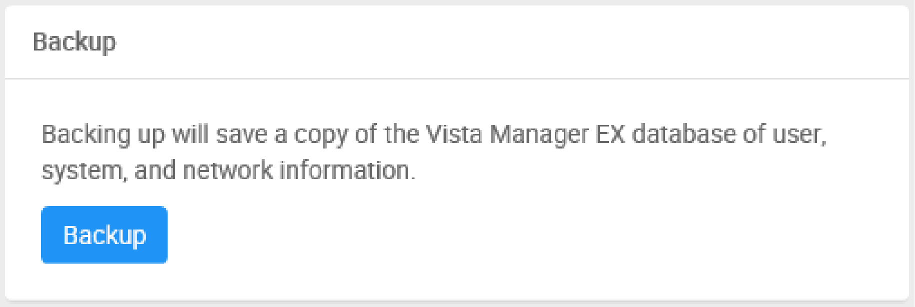
For full AlliedWare Plus documentation, see our online documentation library. For AMF, the library includes the following documents:

- 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.



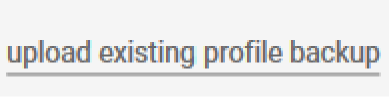
Backing up will save a copy of the Vista Manager EX database of user, system, and network information.

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

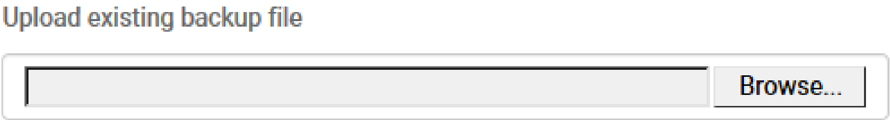
3. Import and start the new version of Vista Manager on your virtual machine host, following the instructions from the Vista Manager EX Installation on the Allied Telesis website.

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'.

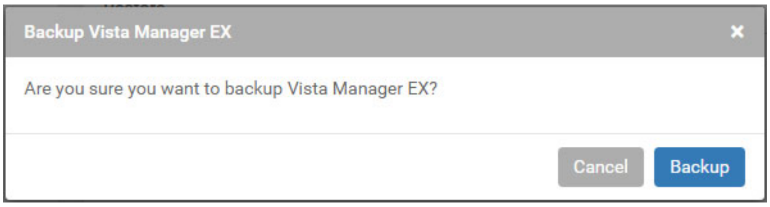
   Do not rename these files. The installation requires them to be in this format.

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 plugins

Backup Vista Manager EX

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



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

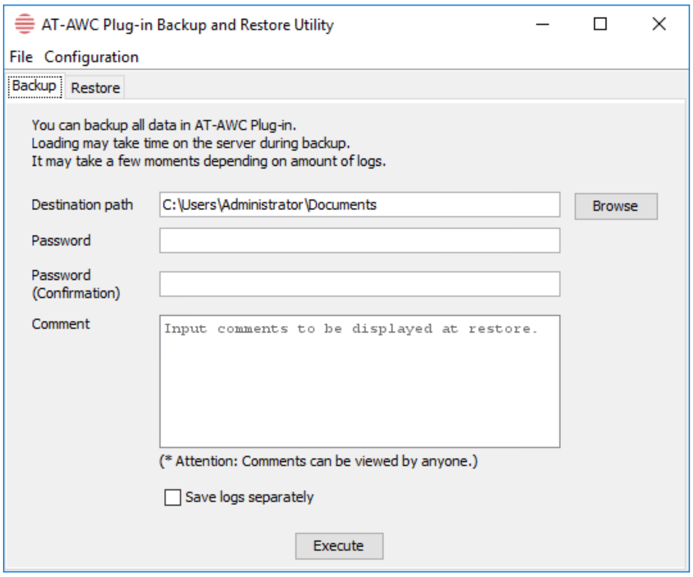
9. If you have the AWC plug-in installed then log on locally to the Vista Manager EX server.

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

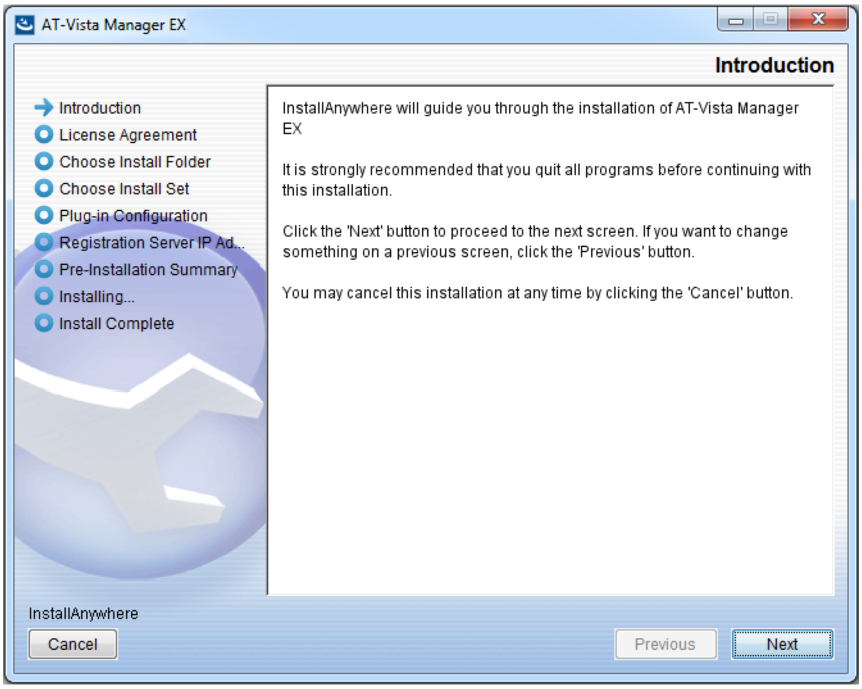
20. Reboot the system.

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

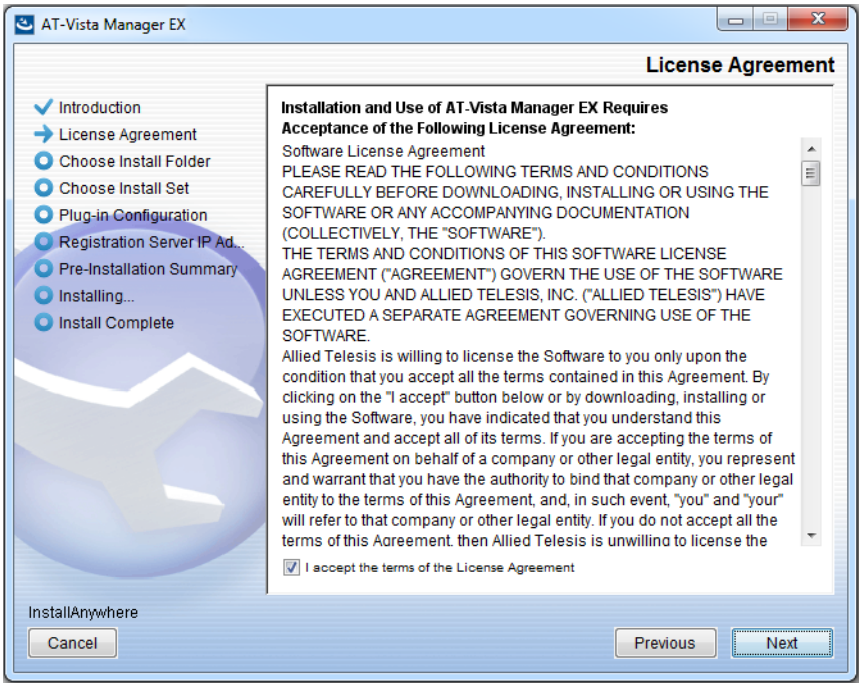
It is strongly recommended that you quit all programs before continuing with this installation.

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:



License Agreement

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

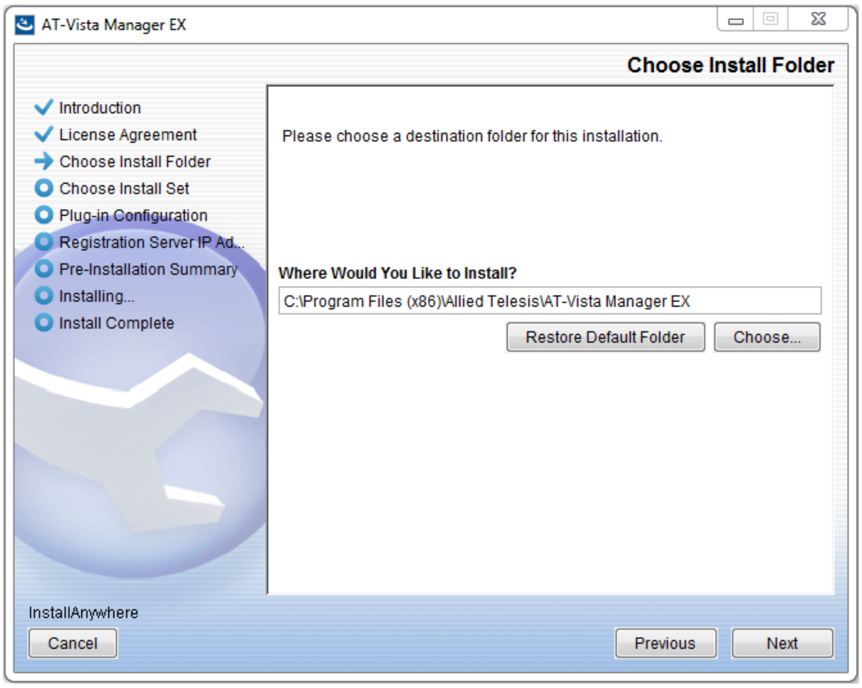
Software License Agreement
PLEASE READ THE FOLLOWING TERMS AND CONDITIONS CAREFULLY BEFORE DOWNLOADING, INSTALLING OR USING THE SOFTWARE OR ANY ACCOMPANYING DOCUMENTATION (COLLECTIVELY, THE "SOFTWARE").
THE TERMS AND CONDITIONS OF THIS SOFTWARE LICENSE AGREEMENT ("AGREEMENT") GOVERN THE USE OF THE SOFTWARE 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:



Choose Install Folder

Please choose a destination folder for this installation.

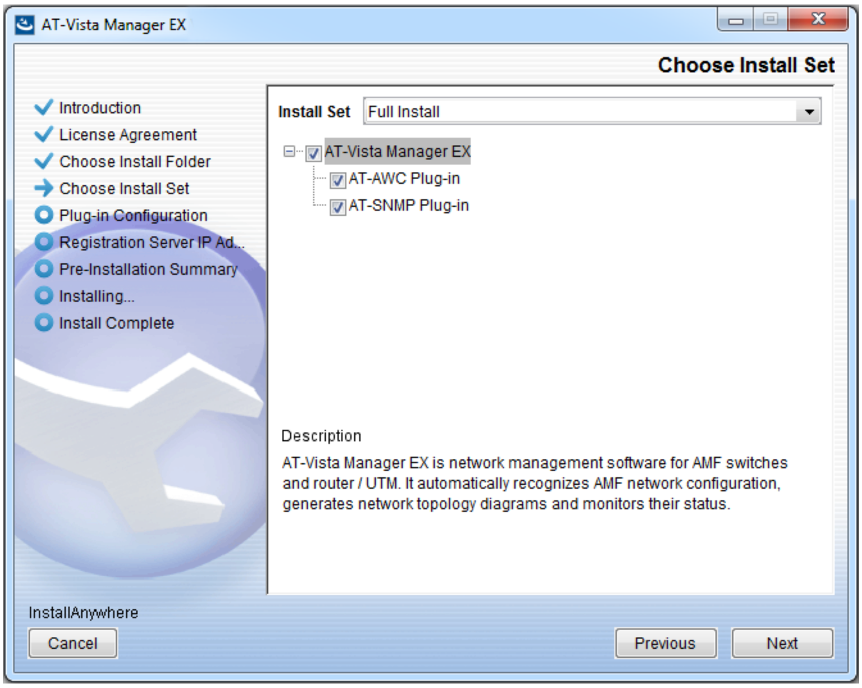
Where Would You Like to Install?

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

Restore Default Folder | Choose...

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

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



Install Set: Full Install

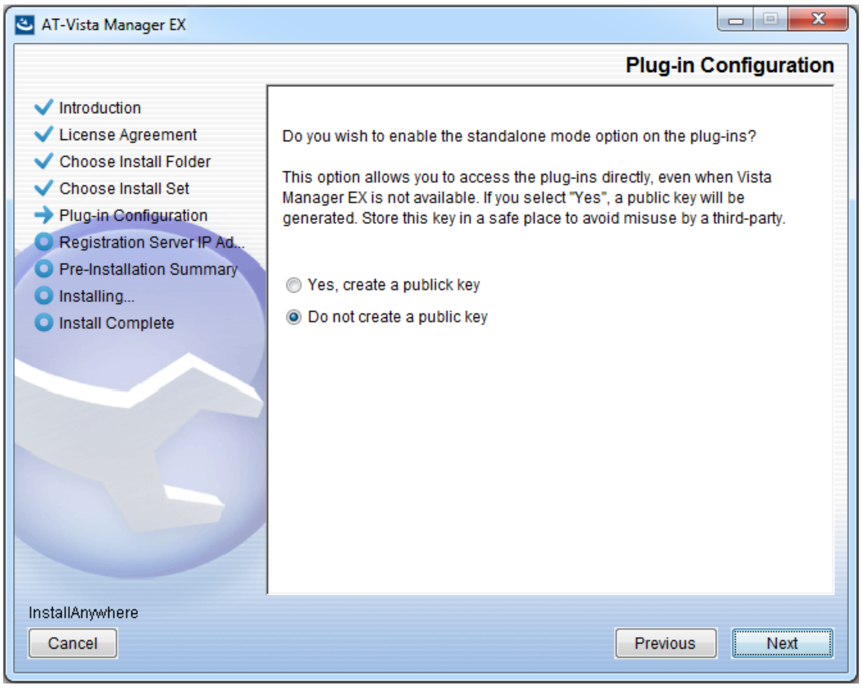
☑ AT-Vista Manager EX
☑ AT-AWC Plug-in
☑ AT-SNMP Plug-in

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?

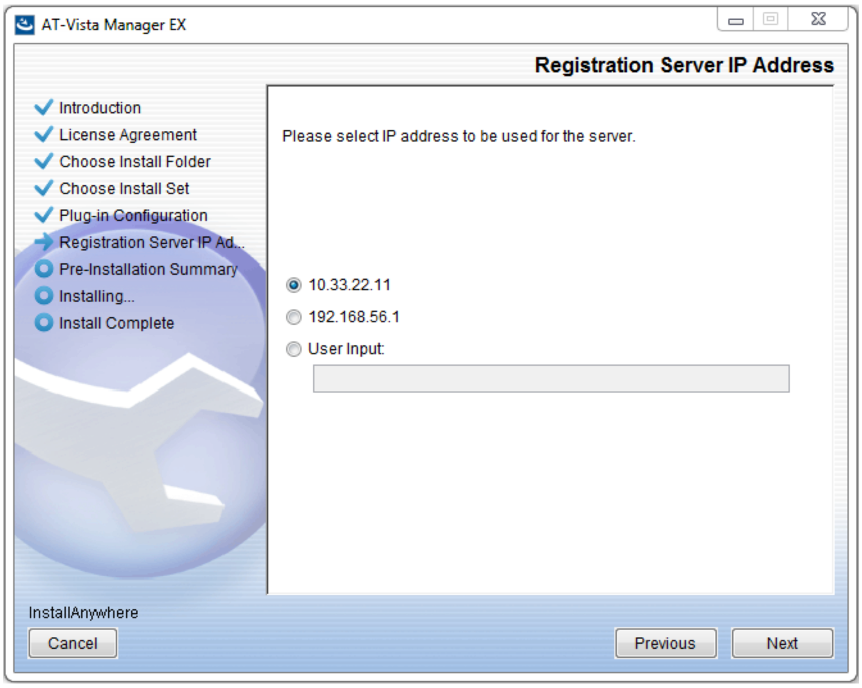
This option allows you to access the plug-ins directly, even when Vista Manager EX is not available. If you select "Yes", a public key will be generated. Store this key in a safe place to avoid misuse by a third-party.

○ 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:

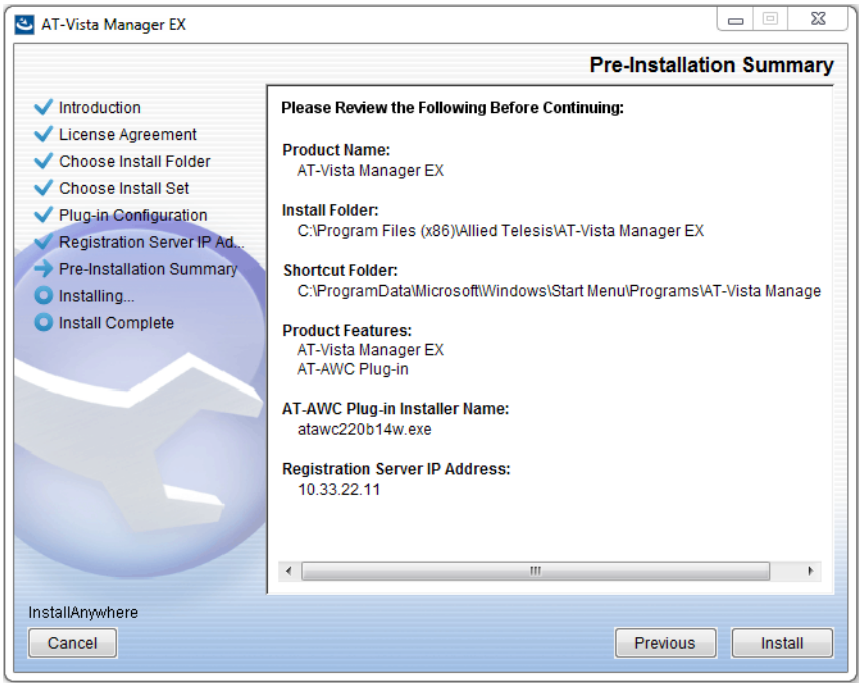


Please select IP address to be used for the server.

● 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

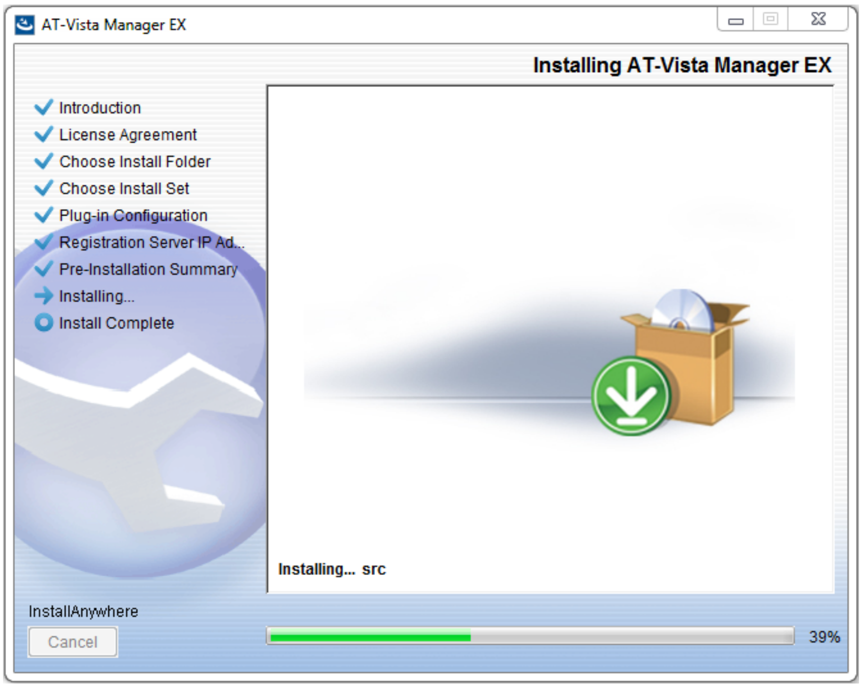
Product Features:
AT-Vista Manager EX
AT-AWC Plug-in

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, Plugin Installer Name and Registration IP Address are correct, and then click **Install**.

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

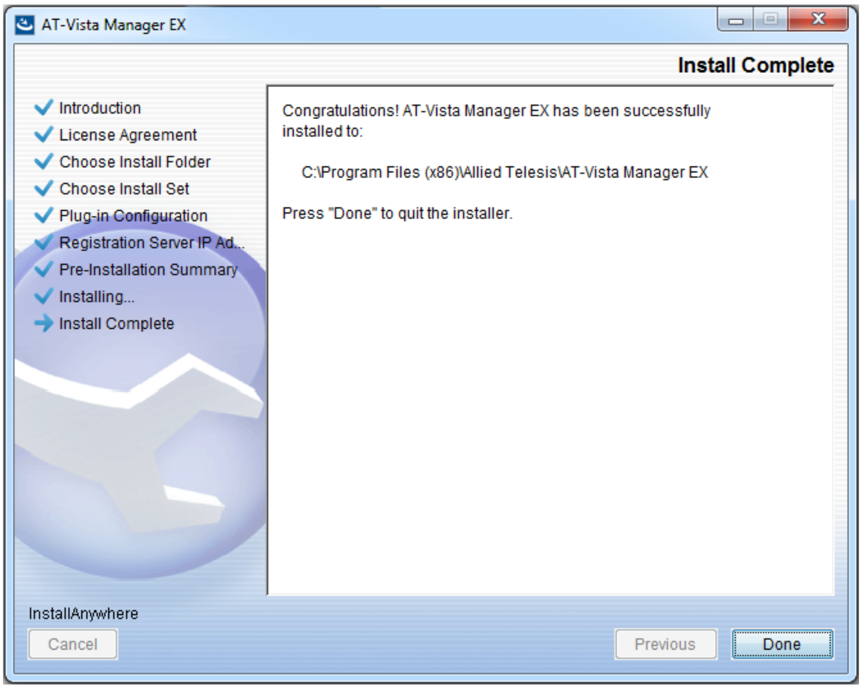


AT-Vista Manager EX

Installing AT-Vista Manager EX

Installing... src

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



AT-Vista Manager EX

Install Complete

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

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

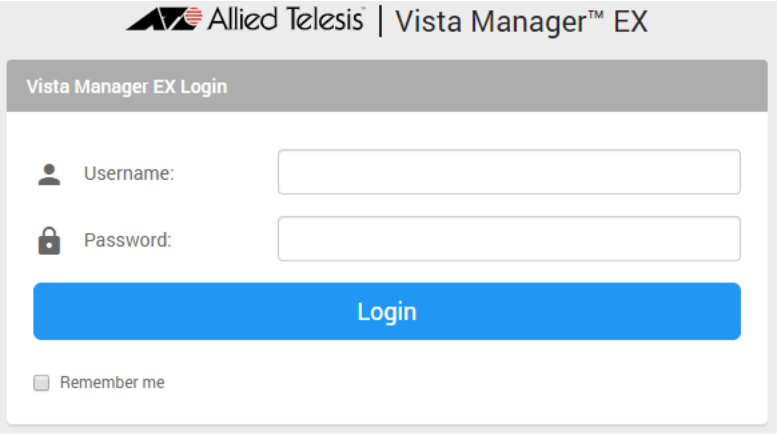
Press "Done" to quit the installer.

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

Restore the Vista Manager database

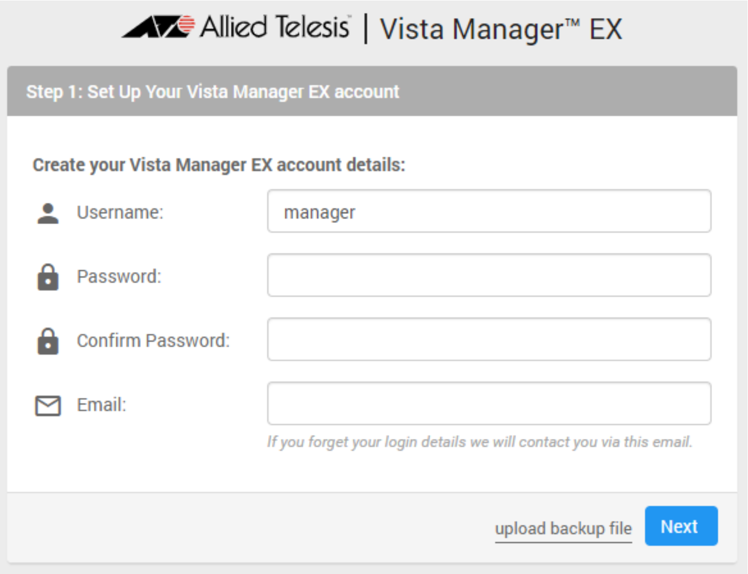
After the upgrade is complete, you need to restore the Vista Manager database. To do this, use the following procedure.

31. Login to Vista Manager.



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:
Password:
Confirm Password:
Email:
If you forget your login details we will contact you via this email.
upload backup file
Next

Username: manager

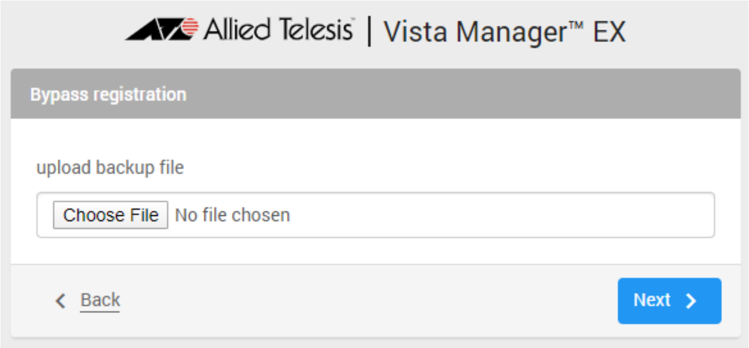
Caution

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.

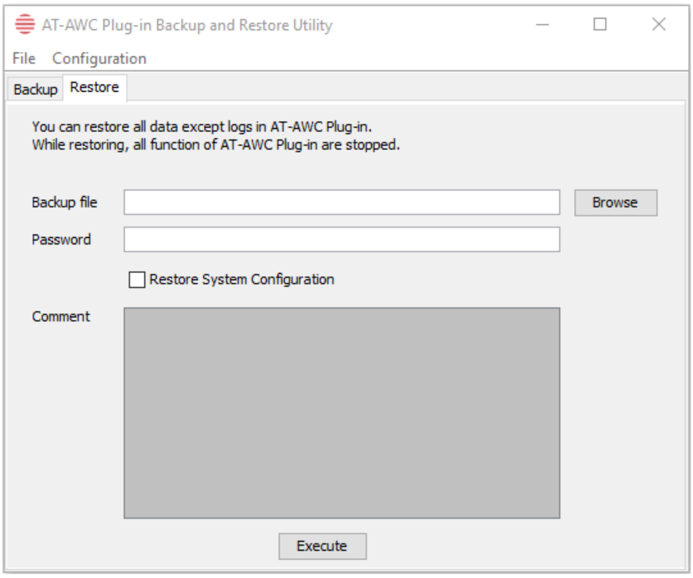
“<*Vista Install Path*>\Plugins\AT-AWC\root\stopserver.bat"

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.


AT-AWC Plug-in Backup and Restore Utility
File
Configuration
Backup
Restore
Backup file
Browse
Password
□ Restore System Configuration
Comment
Execute

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

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 release note for the applicable version of VST-APL at Vista Manager Network Appliance (VST-APL) Release Notes.

Upgrading Vista Manager on VST-VRT

See the release note for the applicable version of VST-VRT at Vista Manager Virtual (VST-VRT) Release Notes.

Troubleshooting

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