Technical Guide

Vista Manager EX

Windows-based User Guide

Introduction

Vista Manager EX

Vista Manager EX™ is a graphical network monitoring and management tool for Allied Telesis Autonomous Management Framework™ (AMF) networks. Vista Manager EX automatically creates a complete topology map from an AMF network of switches, firewalls and wireless access points (APs). Vista Manager EX facilitates simple management of many, or all, network devices from a dashboard that gives you a central overview of your network. From the dashboard you can monitor up-to-date network status, and take action to resolve any network problems.

AMF operations can be performed directly by navigating from the following tools available from the central dashboard:

- Dashboard
  Displays all areas in your network including a drop down list that shows all devices connected to each Area.
- Network Map
  Displays a graphical topology map of your AMF network. From here you can view pop up details of an area that displays the number of AMF nodes, guest nodes, device name and IP address. Actions such as backup master, SSH to master, and backup area can be carried out directly from the network map.
- Event Log
  Displays a list of events that are color coded red for critical, orange for abnormal and green for normal. Events can be filtered by status.
- User Management
  Administrator access allows you to add, change or delete Vista Manager EX users.
- System Management
  Displays various system details such as the current version, serial

number, and license information. It also allows you to manage the system configuration, such as SMTP settings.

- Device Search
  Displays a list of all devices on the network and allows you to search for specific devices or sort by device name, serial number, device type, AMF area, or IP address.

Vista Manager AWC plug-in

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

Allied Telesis Autonomous Wave Control (AWC) is an advanced network technology that utilizes game theory to deliver significant improvements in wireless network connectivity and performance. AWC can automatically minimize coverage gaps and reduce Access Point (AP) interference and respond to network configuration changes and bandwidth demands from user devices.

AWC is closely integrated with Allied Telesis Autonomous Management Framework (AMF) and is managed by Allied Telesis Vista Manager EX. AWC is available as an optional plug-in to Vista Manager.

For documentation on how to use the AWC plug-in, see the AWC Plug-in User Guide on the Vista Manager User Guide web page.

Vista Manager SNMP plug-in

Applicable to Windows-based Vista Manager installations with the SNMP plug-in.

The Vista Manager SNMP plug-in can acquire detailed information and statistics from a broad range of networking devices. Different views enable users to manage devices the way they prefer. It supports management of up to 2000 devices, and in large networks it automatically searches for SNMP agents and displays each device found in tree form, for an easy view of the overall network topology. The SNMP plug-in is a powerful addition to Vista Manager EX, adding management flexibility by supporting non-AMF devices.

The SNMP plug-in also offers a MIB compiler, and generates a chart based on MIB values. It offers support for iMG devices and basic SNMP management, like alive monitoring and access to the iMG GUI. You can also backup and restore your settings.

The SNMP plug-in is closely managed by Allied Telesis Vista Manager EX and is available as an optional plug-in to Vista Manager.

For documentation on how to use the SNMP plug-in, see the SNMP Plug-in User Guide on the Vista Manager User Guide web page.

Audience for this guide

This guide is intended for computer system administrators and network engineers. It describes how to use **Windows-based** Vista Manager EX, with optional plug-ins. For information on how to use a Vista Manager EX **virtual appliance**, see the Vista Manager EX Virtual Appliance User Guide.

Related documents

For information on how to install Vista Manager, see the Vista Manager EX Windows-based Installation Guide.

The following documents give more information about Vista Manager EX:

- Vista Manager EX Datasheet

Planning an AMF network is beyond the scope of this installation guide. The following documents give more information about AMF:

- AMF Feature Overview and Configuration Guide
- AMF Introduction and videos

These documents are available from the links above or on our website at alliedtelesis.com

Contents

Introduction 1

- Vista Manager EX 1
- Vista Manager AWC plug-in 2
- Vista Manager SNMP plug-in 2
- Audience for this guide 3
- Related documents 3

Contents 4

Using Vista Manager EX 6

- Logging into Vista Manager EX 6
- Displaying an overview of your AMF network: the dashboard 7
- Navigating around Vista Manager: the left-hand menu 8
- Displaying sites and devices: the integrated map 9
- Asset Management 18
- Managing sites and devices 27
- Intelligent device grouping 30
- AMF node licenses 32
- Traffic monitoring 33
- Advanced traffic monitoring with sFlow 34
- Tracepath 38
- VLAN management 39
- Firmware management 40
- Configuration management 42
- Using the event log 44
- High priority events 45
- Using the syslog server 46
- Service monitoring 47
- HTTPS access to Vista Manager EX 49
- Managing user accounts 52
- Managing the Vista Manager EX system 55
- Changing the Vista Manager EX controller IP address 55
- Backup Vista Manager EX 56

Using the SD-WAN Feature 57

- Introduction 57
- Limitations 57
- Configuring devices for SD-WAN 58
- Dashboard 62
- Topology map 65

Linkmon probes 69
SD-WAN rules 70
Health 75
Monitoring 76
Troubleshooting 80
Ports and URLs used by Vista Manager EX 80
SNMP plug-in application pool settings 81
Supported Device List 83
AlliedWare Plus devices 83
Allied Telesis Wireless APs 85

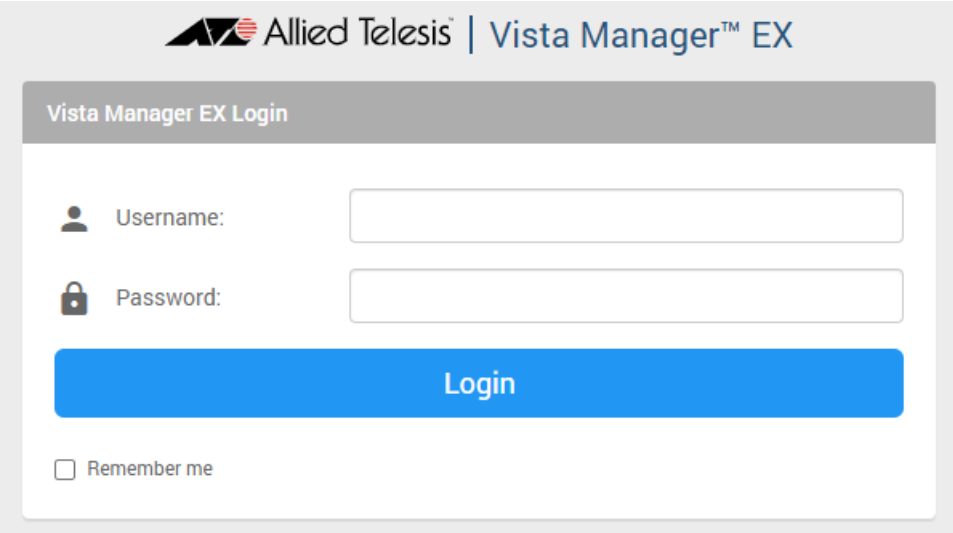
Using Vista Manager EX

Logging into Vista Manager EX

To connect locally you can use the URL: http://localhost:5000

To connect remotely use the URL: http://<ip address>:5000, where ***<ip address>*** is the address you picked on the **Registration Server IP Address** dialog.

The **Vista Manager Login** dialog displays:



- Enter your **Username**.
- Enter your **Password**.
- Click **Login**.

Change password

1. Click on **User Management** from the menu and select your user name
2. Click the **Edit** button
3. Click the **Change Password** button
4. Enter your new password and then re-enter your new password to confirm
5. Click the **Save button**

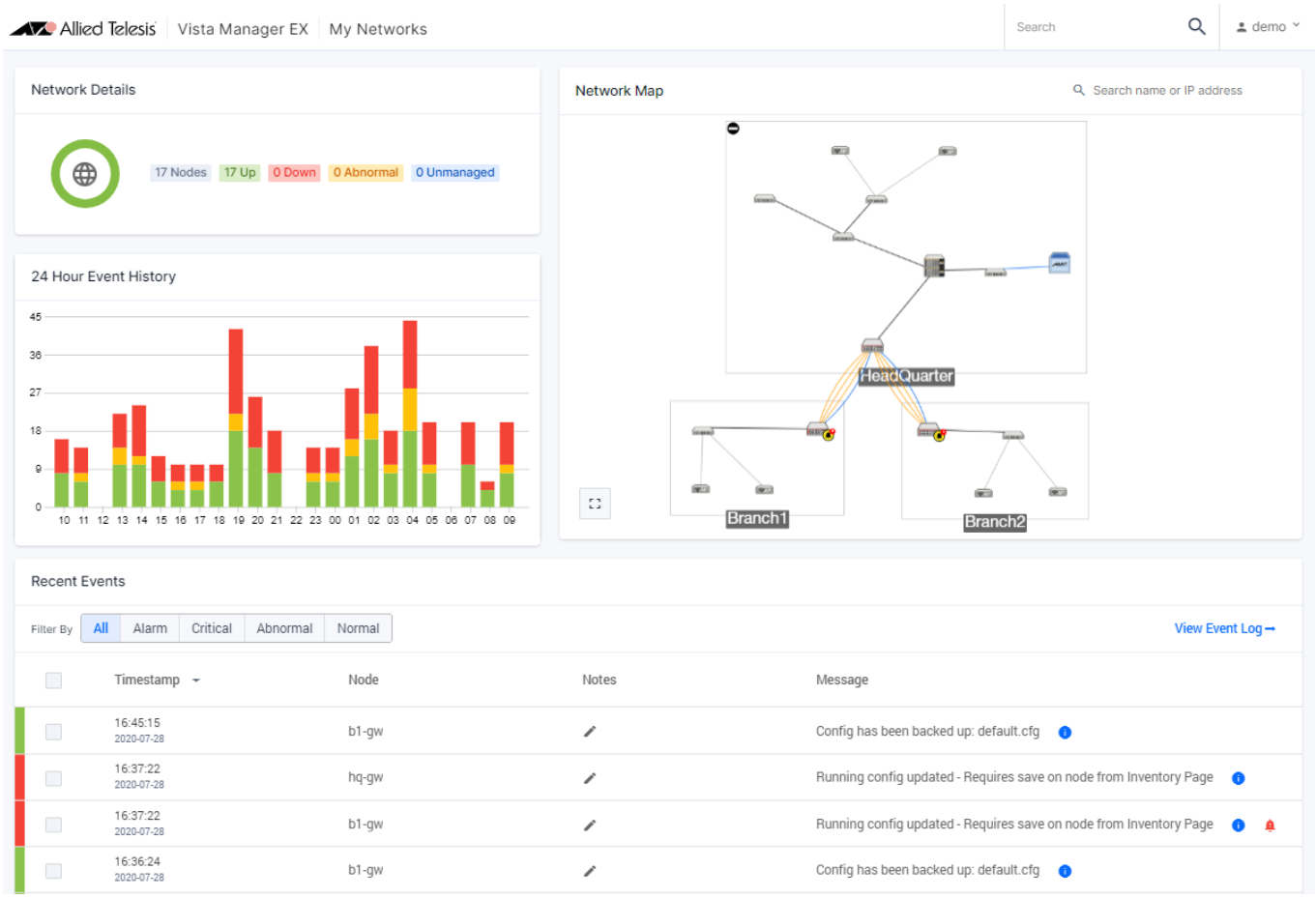
Logout

On any Vista Manager screen, click on your username in the top right-hand corner and select **Logout**.

After logging out the login window will appear.

Displaying an overview of your AMF network: the dashboard

The **Dashboard** is the default screen displayed after you have logged in to Vista Manager EX:



The dashboard displays the following information about your network:

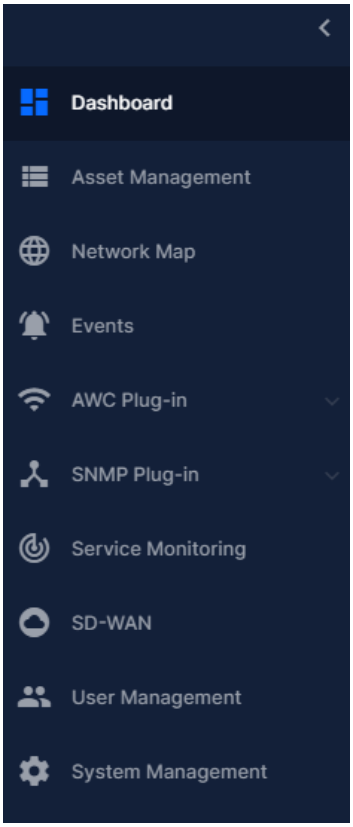
Field	Description
Network Details	Shows the number of nodes and status (up, down, abnormal or unmanaged).
24 Hour Event History	Shows a graph of the last 24 hours of log events history.
Recent Events	Displays time, node (device name) and any notes or messages relating to each event.
Network Map	Displays the network topology in graphical form.
Critical Message Bar	The last critical log message is highlighted in a message bar, if critical problems exist.

Navigating around Vista Manager: the left-hand menu

On the left-hand side of every Vista Manager Screen is an expandable **Menu**. The menu enables you to navigate to and from the Dashboard, Asset Management, Network Map, Events, Service Monitoring, SD-WAN, User Management, and System Management. Any optional plug-ins will also appear in the menu.

You can expand or collapse the menu. The expanded menu displays the name of each menu option.

For easy navigation from any window in Vista Manager EX you can access the show/hide **Menu** as follows:



Displaying sites and devices: the integrated map

The dashboard includes an integrated map showing all devices known to Vista Manager on the network. This makes it easier for users to see and visualize what is happening on their network.

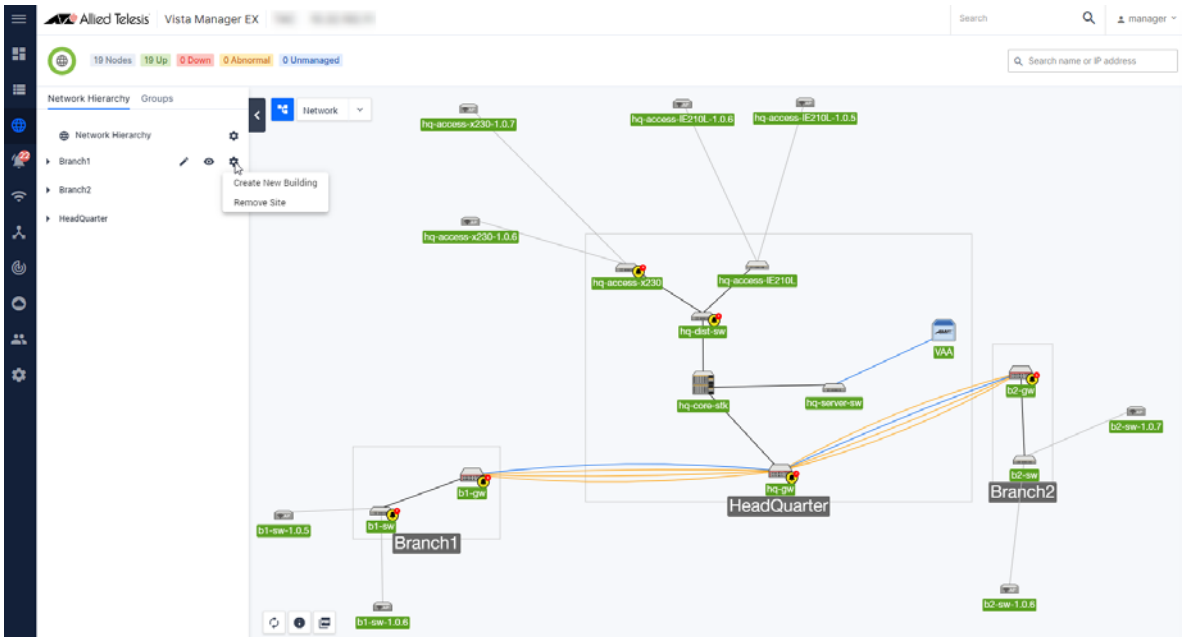
Access the integrated map in its own screen by using the Network Map option in the left-hand menu. From the Network Map you can display details about sites in the network hierarchy and identify the devices in each site.

Click the **Network Hierarchy** icon at the top left of the map screen to display the list of sites. This can be a:

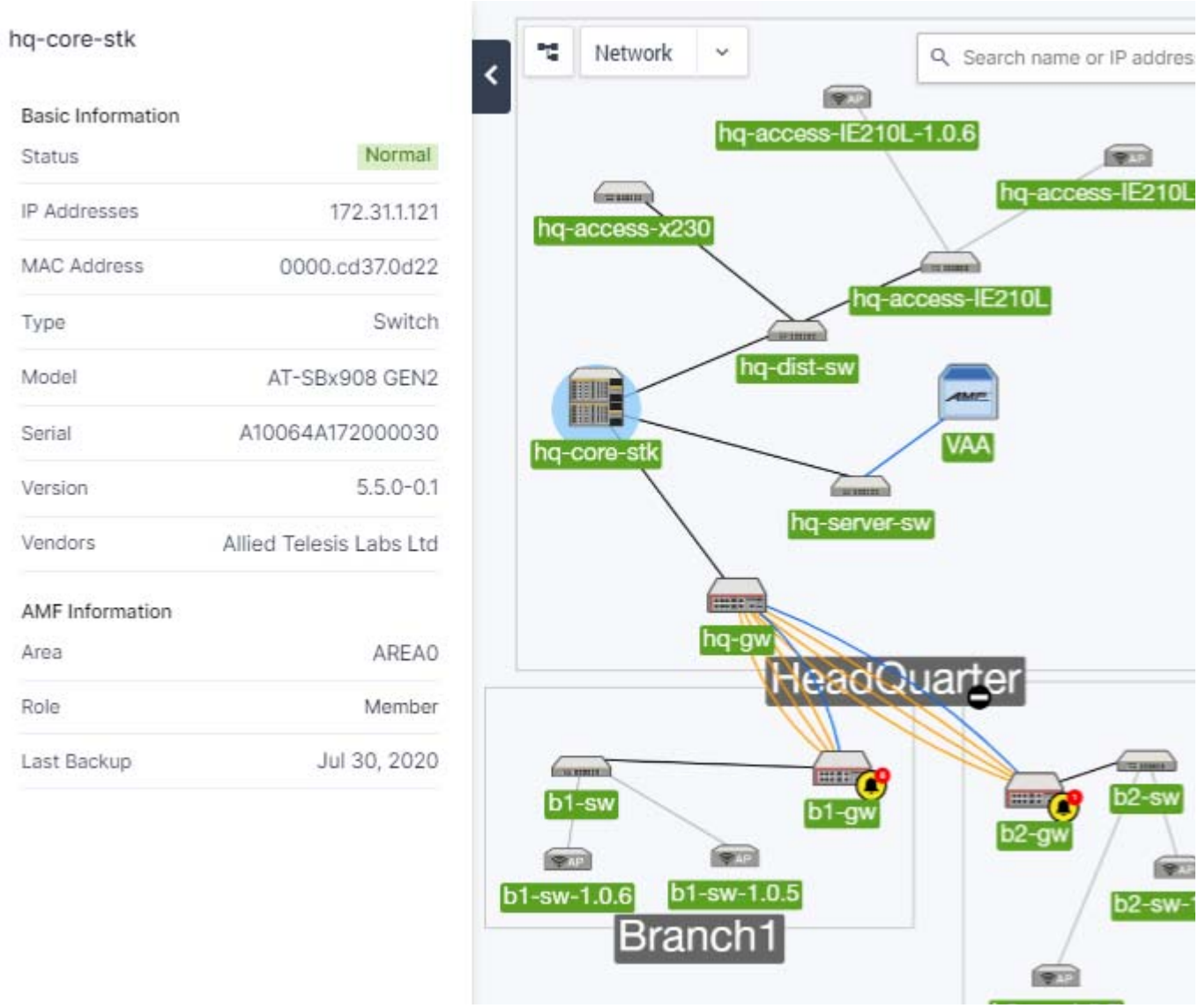
- Location - buildings and devices can be assigned to a location.
- Building - floors and devices can be assigned to a building.
- Floor - devices can be assigned to a floor.

Devices can be assigned to any one of these sites.

From the site side panel, you can also perform functions like **Create**, **Remove**, **Edit**, and **Hide** for each site, as well as create child sites.

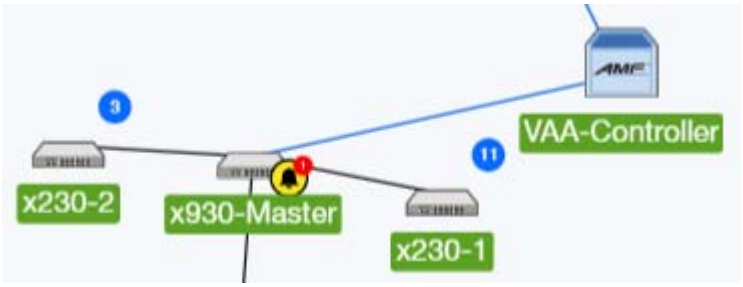


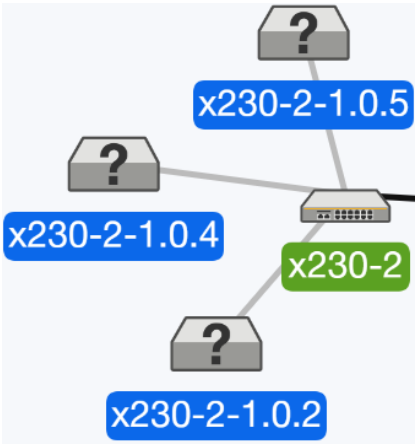
Clicking on a selected node or double clicking on a node will show all the node information as follows:



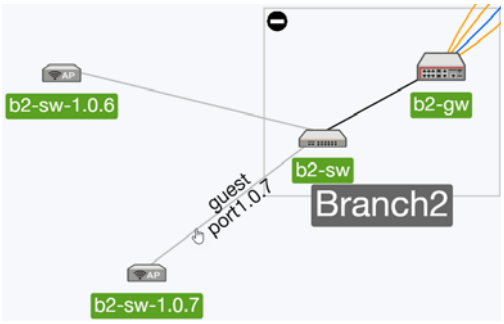
From this view you can check the status of a node at a glance. Status is indicated by the node title background color. Down is red, abnormal is orange and normal is green.

Blue indicates an unmanaged node, which also carries a numbered blue circle tag until further zoomed into, at which time the guest nodes will be displayed.





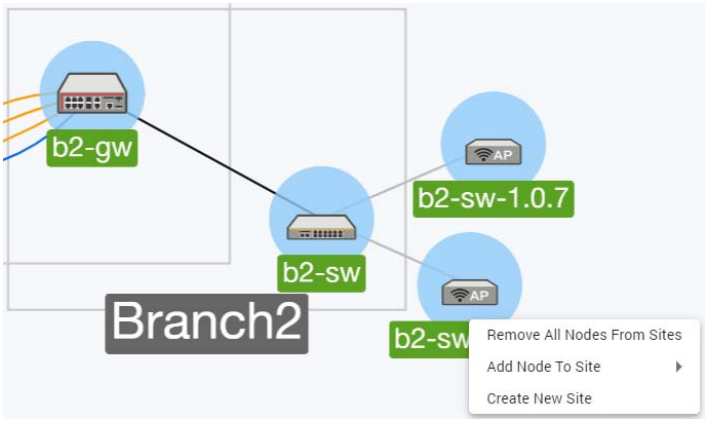
Managed guest nodes attached to a node are indicated by grey links. Hovering over a grey link displays the port number.



You can click on the device icons and drag them into different positions on the map.

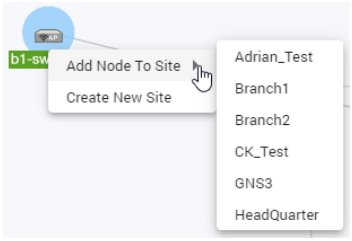
To select a node or nodes, hold **Ctrl** and select each node you want selected. Alternatively, hold **Ctrl**, then click on the area and drag over the nodes you want selected.

Selected nodes are highlighted in blue as follows:



To remove or create a new site for all selected nodes, right-click on them for such options.

To add a node to a site, right-click on a selected node and select **Add Node To Site**:

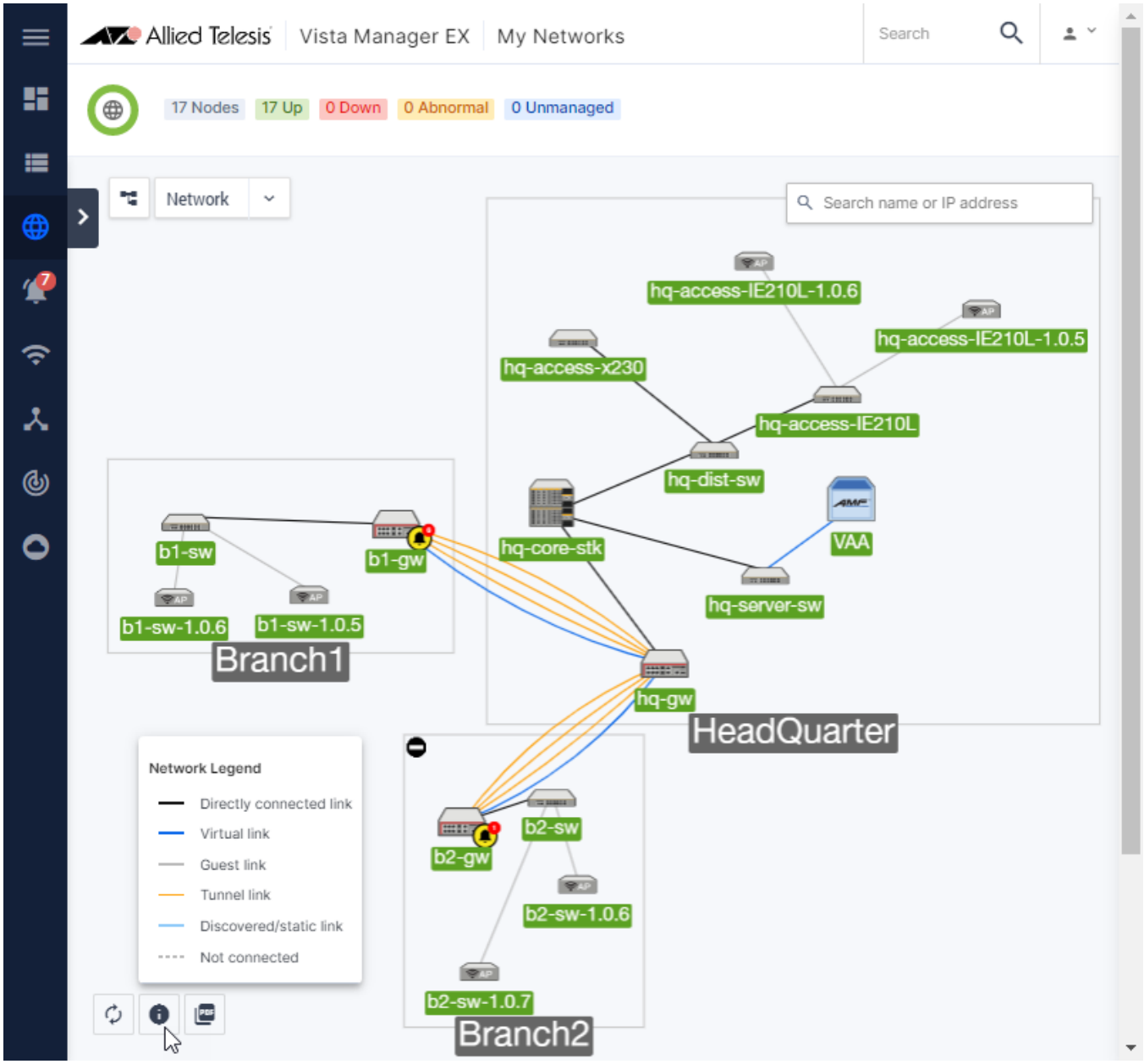


For more information on backing up a node, see **"Backup a node" on page 27**.

For more information on SSH to Master, see **"SSH/Shell to a node" on page 27**.

Network links and icons displayed in the network map

Physical (directly connected), virtual, guest, and tunnel links are displayed differently. Physical links have a black line color, virtual links have a blue line color, guest links have a grey line color, and tunnel links have an orange line color. You may refer to the network legend at the bottom left corner of the map.

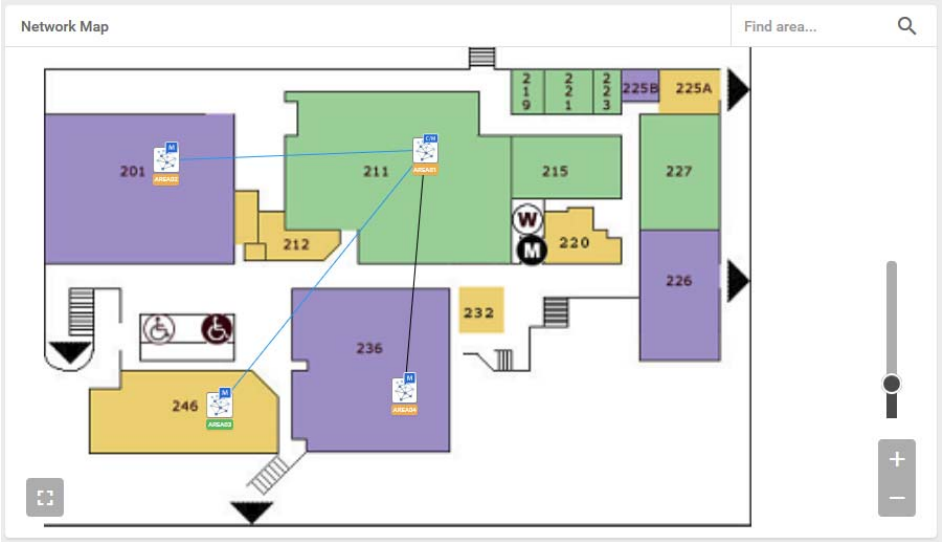


Importing a building or floor map to sit behind the network diagram

You can import an image as a background on a map screen. This enables you to add a building or floor map and show the physical location of devices.

From the **Network Map** click on the camera icon in the bottom left-hand corner. Click **Select** to browse for your floor plan and select the file. Click **Open** and then select the image. You can change the opacity of the image by adjusting the slider below the image. Click the **Save** button to upload the image to your Network Map.

The image will appear as the background of your network. You can then move the areas, devices or guest nodes so they are located in the correct areas in the diagram as follows:



To delete an image, click on the camera icon and select **Delete**. Check that you are sure you want to delete the Network Map background image, and if you are sure, click the **Delete** button.

Refreshing the map when your AMF network changes

New devices will appear automatically via polling, or you can click the Refresh icon on a map screen for an immediate result.

1. Click the **Refresh** icon at the bottom left of the map screen to trigger polling.
2. After polling is complete, the Web browser will update the status of the equipment and new devices will appear.

Exporting a PDF of the network map

You can export a network map in PDF format.

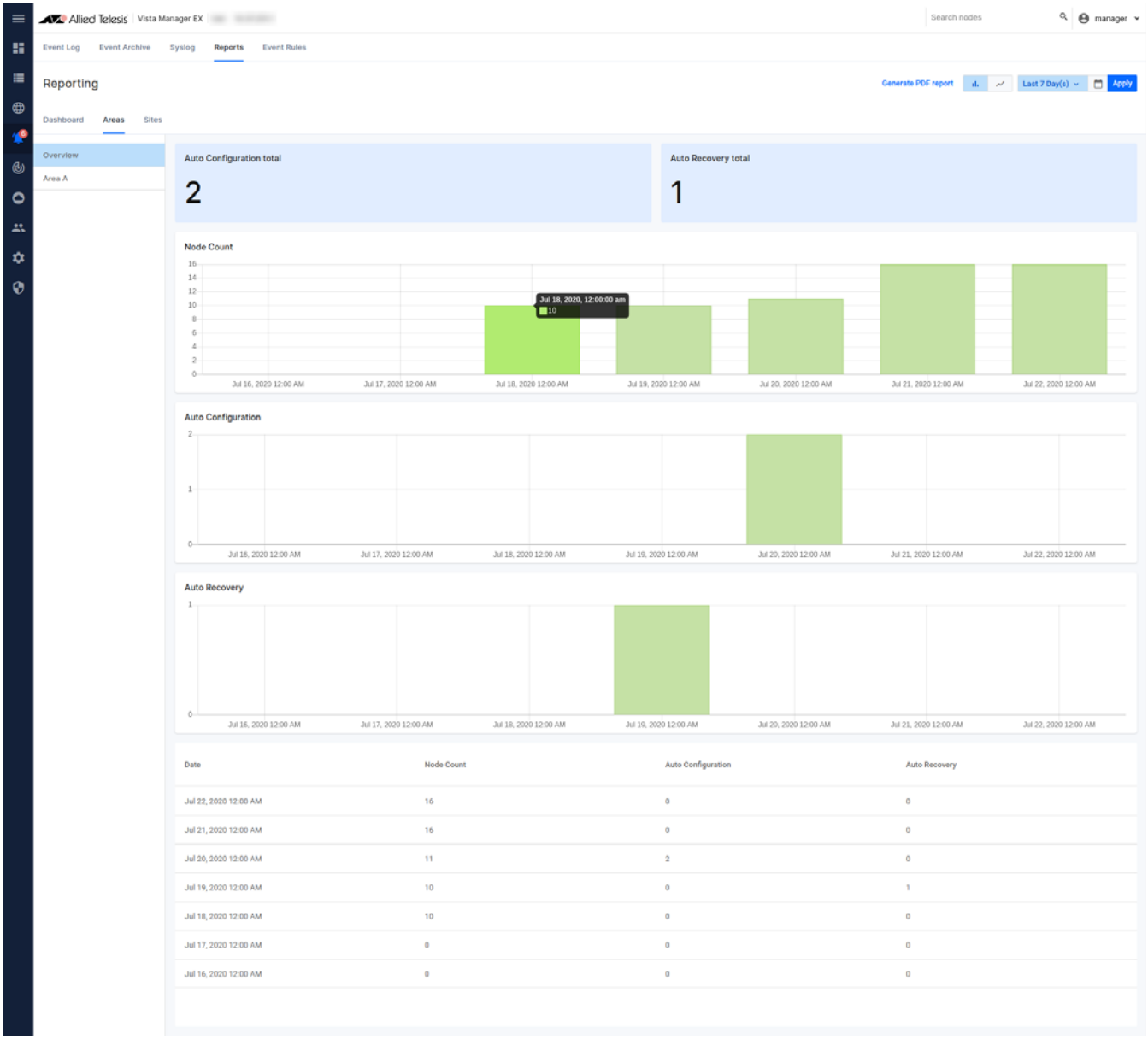
In the bottom left corner, click on the **Export PDF** button.

Integrated map reporting support

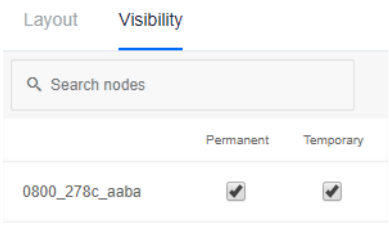
You can generate reports that provide detailed statistics of actions performed by the AMF networks. Specify a time range between 7 days to 6 years. For users, you can see how the size of your network has changed over time. For administrators, you will be able to justify why and when you have to renew your AMF subscription license.

Data for reports is compiled daily at midnight UTC time. Reports are presented in easy-to-understand charts and tables available in PDF format.

To use this feature, navigate to the **Events** page from the left-hand menu, then select the **Reports** tab.



Static icons on map support



You can change which nodes are visible on the network map. For example, you may only be interested in seeing servers on the network map, and can therefore hide the other nodes.

An administrative user can modify the default view of the map. You can temporarily or permanently hide nodes. Temporarily hidden nodes will be hidden for your session, but will return when you log back in. Permanently hidden nodes will be hidden for all users until you choose to show them again.

A regular user can only temporarily hide nodes that you are not interested in seeing. They will remain hidden while you are logged in, but if you log back in, the map will return to the default view set by the administrator.

To change the visibility of nodes, click on Edit in the dropdown on the network map screen. Click on the Visibility tab to show a list of nodes.

- Nodes with the Permanent checkbox checked will be visible to all users when they log in.
- Nodes with the Permanent checkbox unchecked will be hidden.

Note: Only administrative users can change the Permanent status of a node.

- A user can check the Temporary checkbox, making that node visible during their session.
- A user can uncheck the Temporary checkbox, making that node hidden during their session.

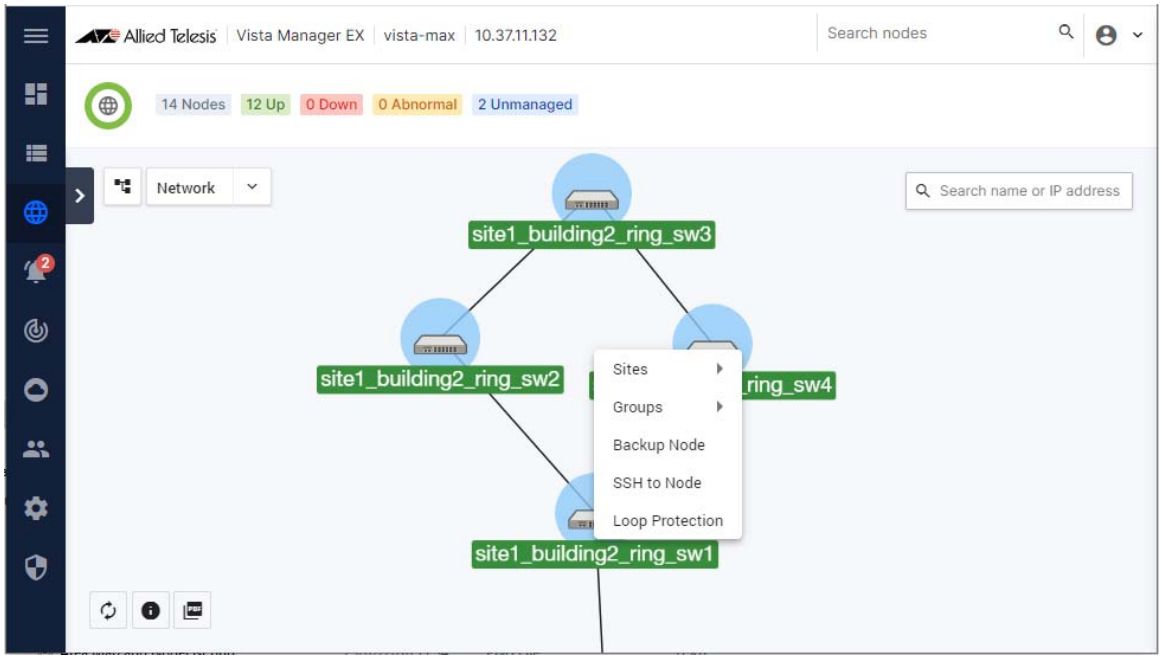
Note: Any user can change the Temporary status of a node during their session.

Changes to the Permanent status of a node are persistent. Changes to the Temporary status only persist for the session.

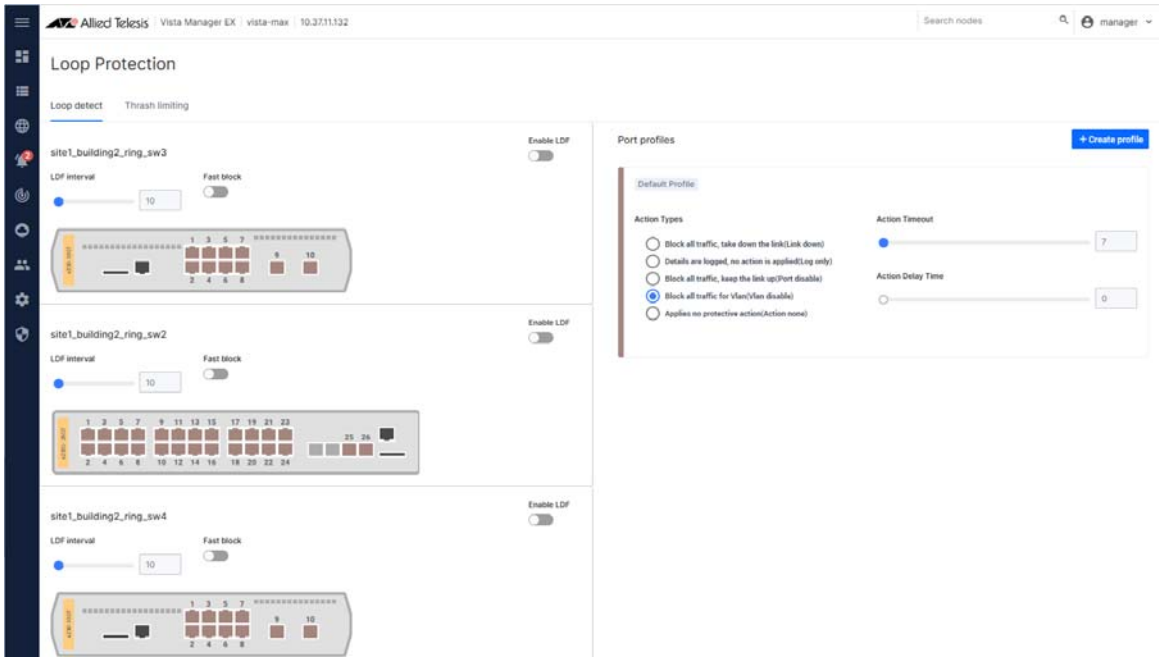
Note: The visibility of base nodes cannot be changed. Therefore, on an AMF network, AMF nodes will always be visible and cannot be hidden. Likewise, if the network is a plug-in view, then the plug-in nodes will always be visible.

Loop Protection

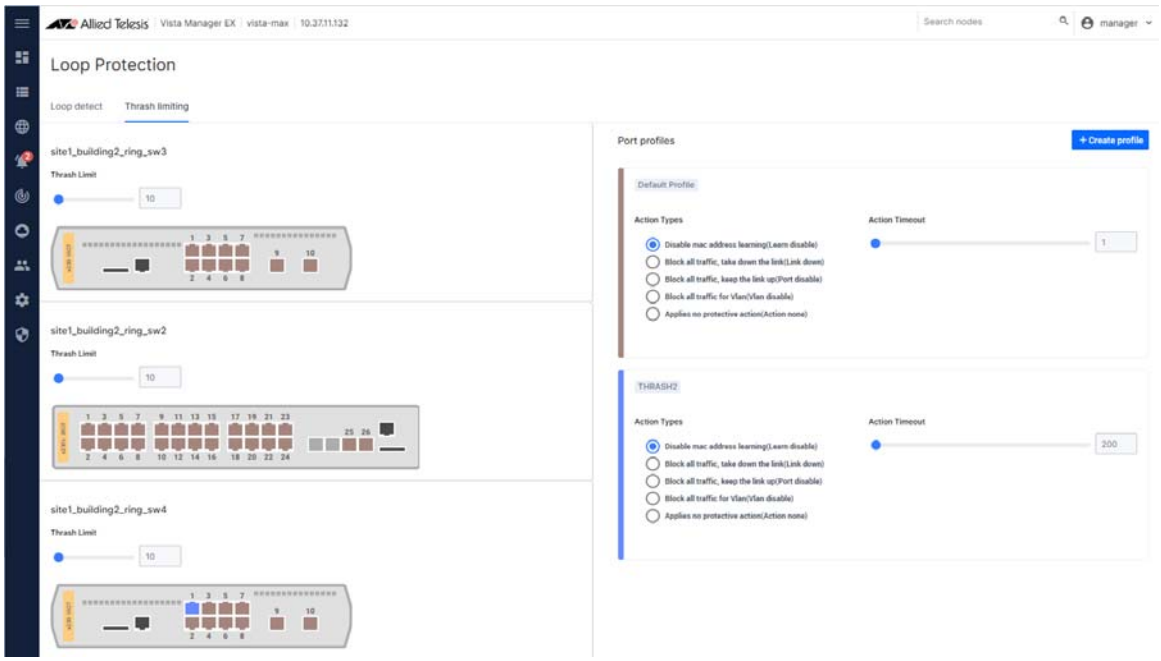
The loop protection feature helps you manage the loop protection settings of the AlliedWare Plus devices in the Vista Manager GUI. You can use Vista Manager to manage the loop detection and thrash limiting of your network.



Loop protection is managed from the integrated map. You can select one or multiple (up to 10) devices from the integrated map for loop protection configuration. Once you have selected the devices that you want to configure, right click on one of them and select Loop Protection from the pop-up menu.



On the Loop detect tab, you can configure loop detection for the selected devices. The Enable LDF button lets you enable or disable loop-detect frames (LDF) for each device. The LDF interval slider lets you set the loop-detect frame interval. And the Fast block button lets you enable or disable fast block.



On the Thrash limiting tab, you can configure thrash limiting for the selected devices. The Thrash Limit slider lets you set the thrash limit.

The Port profile panel lets you create and edit port profiles. By default, the settings of the Default Profile apply to all ports on the device. To create a new profile, click on the +Create profile button.

For loop detection port profiles, you can choose the action type, the action timeout, and the action delay time for the profile. For thrash limiting port profiles, you can choose the action type and action timeout. You can then assign the profile to device ports. You can select multiple ports across one or multiple devices, and apply the profile to all of them at the same time. Click on Save profile to save the changes.

Asset Management

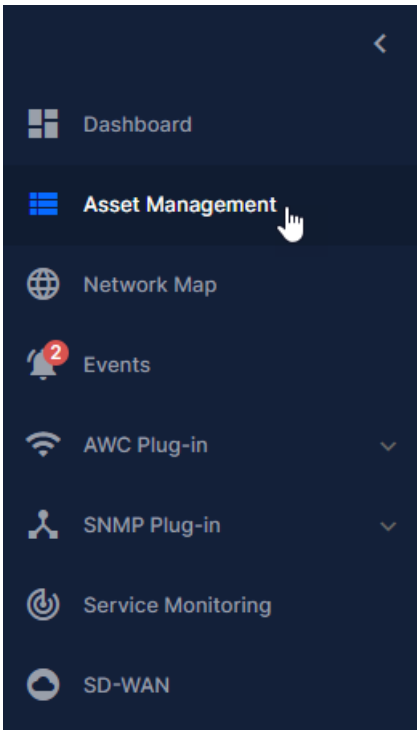
You can use the Asset Management screen to manage the assets in your network. It is made up of several components.

- Device discovery - devices on the network are discovered via AMF and plug-ins.
- Device classification - during discovery, a best effort is made to categorize what type of device has been discovered. However, this may be incorrect, so it allows you to specify what type of device has actually been discovered.
- Device management - once discovery is complete, the asset information should be available to you.

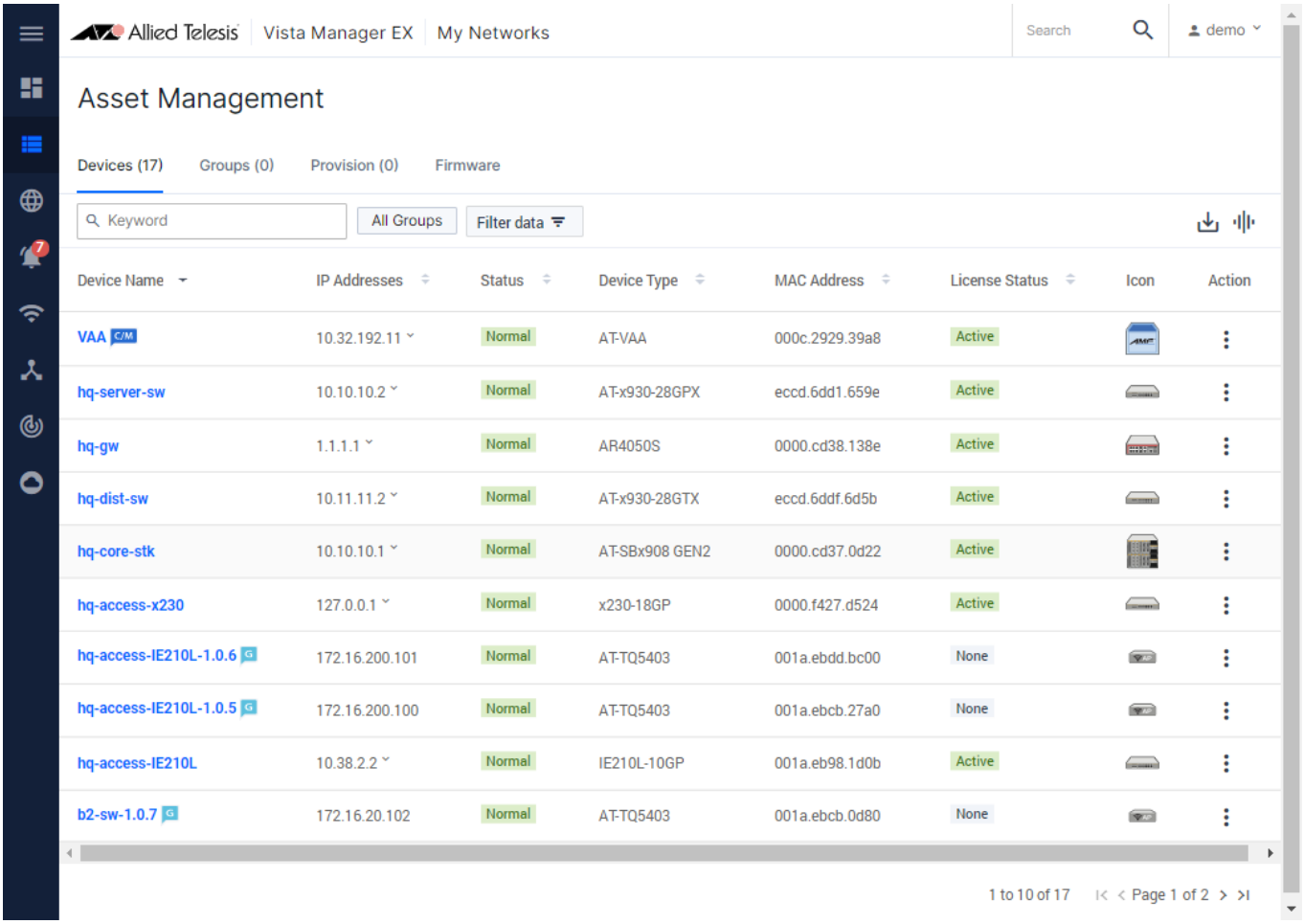
You can use Asset Management to:

- get a complete list of all assets on your network.
- display the assets on the integrated map, and select the most relevant icon for each device.
- view the license information for all Allied Ware Plus devices.
- be notified when a license is about to expire or has recently expired.
- create a group defined by either IP/MAC address range or Vendor, and assign an icon to this group.
- filter the list of assets, and print/export this list.

Asset Management can be accessed from the sidebar menu.

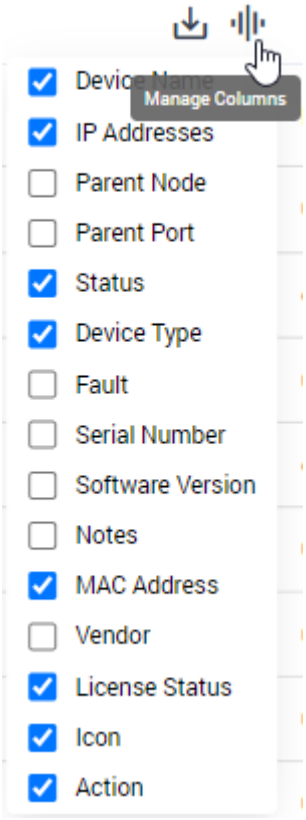


The Asset Management screen shows you the details of the items in your network. It also allows you to search for particular devices.



The list of assets can be downloaded as a CSV file by clicking on the Export as CSV button at the top right corner.

The columns that are shown can be changed by clicking on the Manage Columns button.

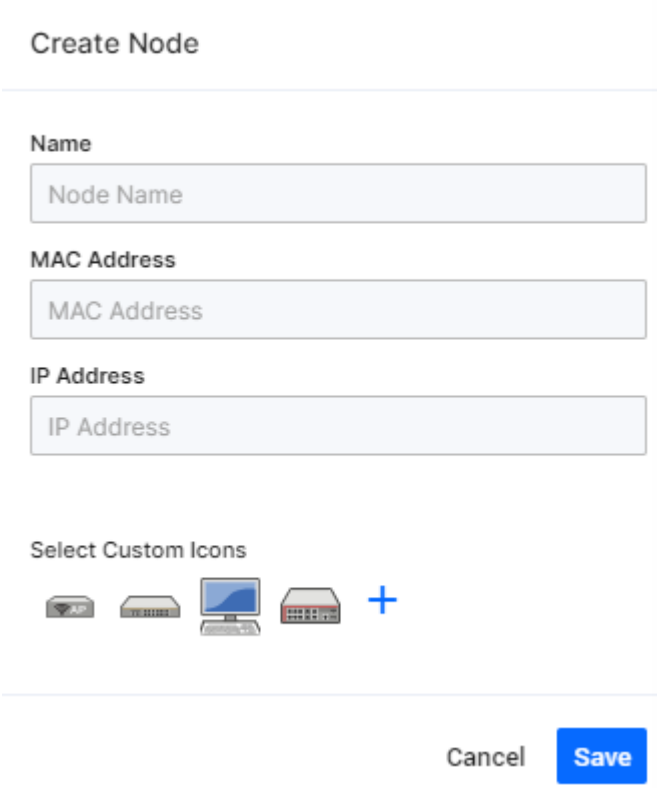


You can discover devices from the Asset Management screen. By clicking on Discover Devices, Vista Manager will use ARP to discover any new devices, and return a list to you. A message will appear indicating the number of new devices found.

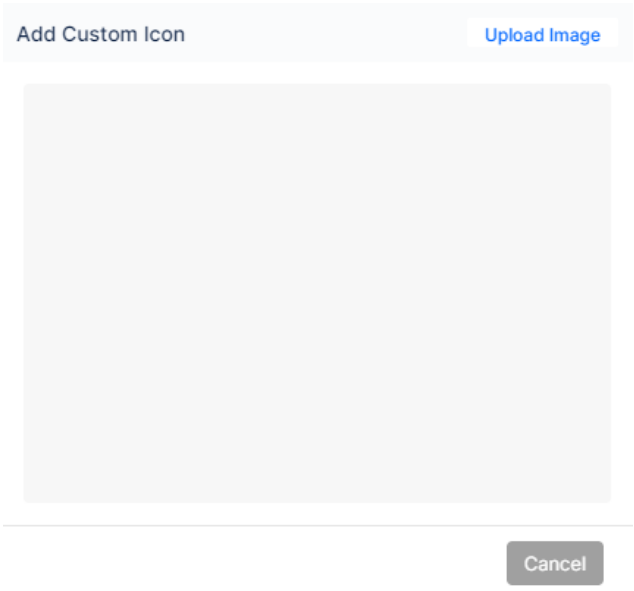
Discover device will only discover IPv4 neighbors. Any detected devices will not automatically appear on the map, but will require you to add them manually once they have been discovered. The detected devices will not provide link information, but you can manually add the links. Detected devices that fall into a user defined inventory group will inherit the assigned custom icon.

You can add a new node by clicking on the Add Node button.

You will be prompted to name the node, as well as specify the MAC address and IP address. You can also select an icon to represent the node.

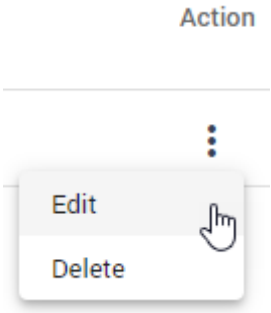


If you click on the Plus button, you can choose to upload a custom icon for the node. The custom icon dialog supports SVG, JPG, and PNG image files. Only administrators have the permission to upload and change custom icons.



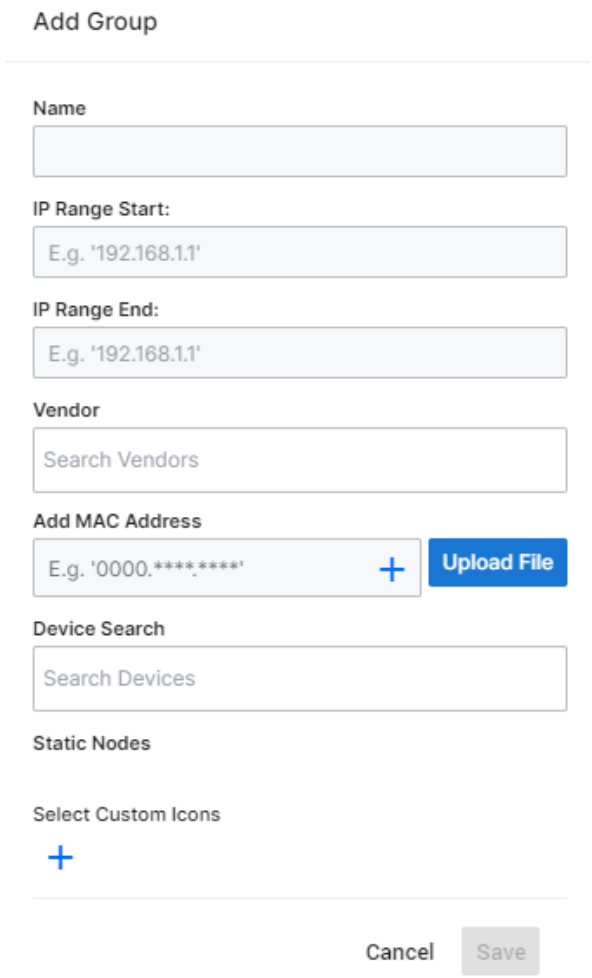
Note: AMF nodes cannot have their default icon changed.

You can also edit existing nodes, change their properties, and assign them a different icon. Nodes can also be deleted from Asset Management. To edit or delete a node, click on the appropriate menu item in the Action column.

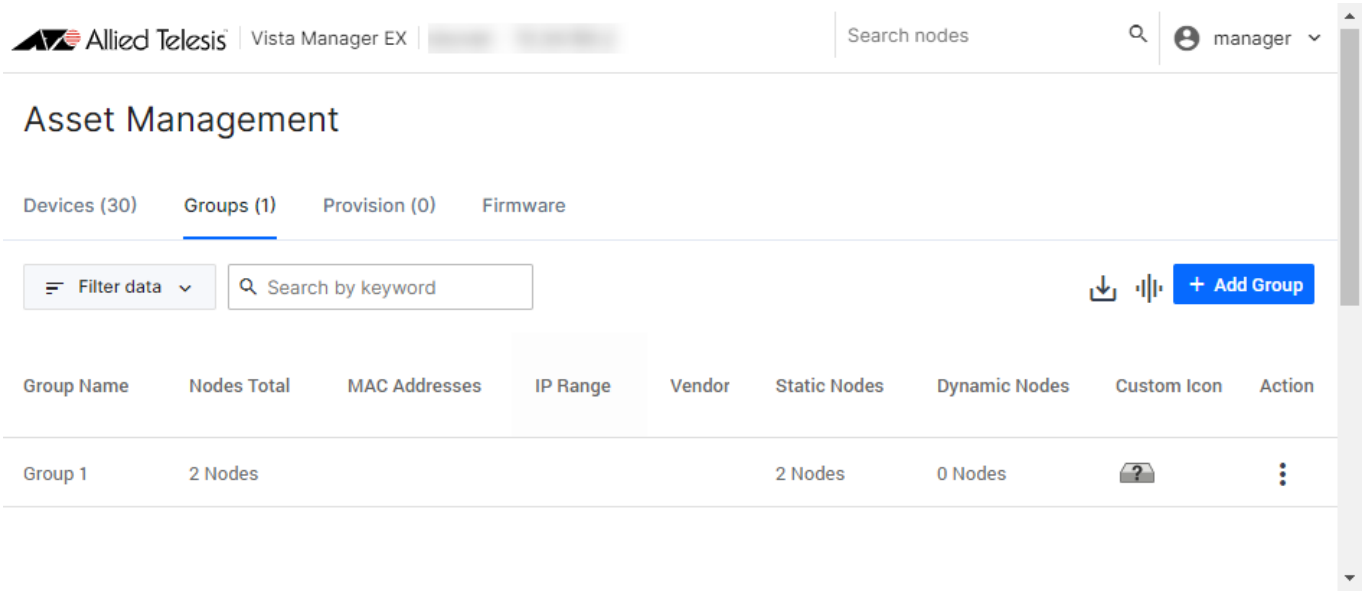


Asset Management also allows you to create groups to organize your inventory. To create a group, click on the Groups tab, and then click on the Add Group button.

You will be prompted to name the group. You can also specify which nodes will be added to the group. You can specify a MAC address range, an IP address range, a vendor, or a combination of these. You can also select an icon to represent the group.



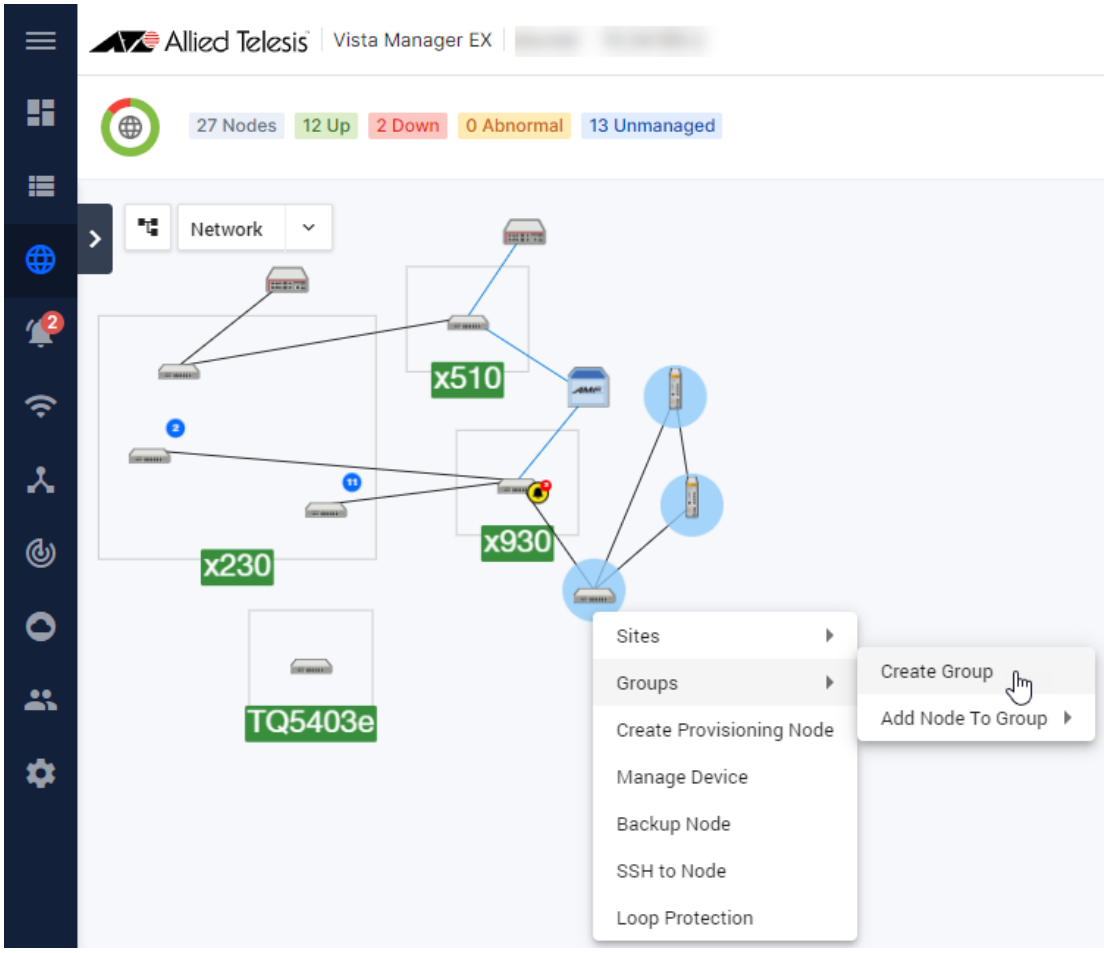
Once the group has been created, you can use it to view the details of the members of that group, as well as export that information to CSV. New devices that are discovered and meet the group's criteria will automatically be added to the group.



As an admin user, you may choose to manually assign devices to a group when creating or editing a group in the Groups tab.

1. Navigate to the Asset Management page.
2. Click on the Groups tab, then click on **Add Group**.
3. The Add Group form will appear on the right hand side of the screen.
4. Click on the Device Search input box.
5. Type the first three characters of a device name into the input box.
6. A list of devices with matching names will be displayed below.
7. Either click **Add all** to add all matching devices or click on a specific device to assign it to the group.
8. Manually assigned devices will be visible below the input box.

Alternatively, you can also create a group from selected nodes on the Network Map page. From the map itself, you may add/remove manually assigned nodes to/from a group.



Automatic allocation of static icons via MAC address list

Multiple MAC addresses can be added to a group, providing you the ability to create a group by uploading a file containing a list of MAC addresses. Vista Manager EX then extracts the MAC addresses from the uploaded file and registers them with the group.

You may select a custom icon for the group. Devices that match the MAC addresses of the group will automatically use the customized icon as their device icon.

Take note of the following file specifications:

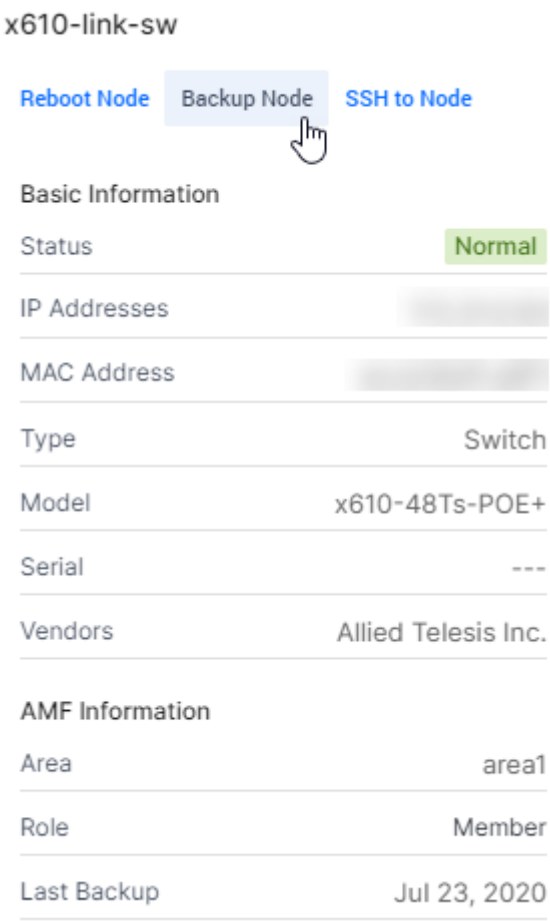
- Supported file formats are **.txt** and .**csv**.
- Commas, spaces, and new lines can be used to separate the MAC addresses.
- Supported MAC address formats are:
  - 000000000000
  - 0000.0000.0000
  - 0000:0000:0000
  - 0000-0000-0000
  - 00:00:00:00:00:00
  - 00-00-00-00-00-00
  - wildcard with asterisk (*)
- Any unrecognizable MAC address formats will be ignored, no errors will show to indicate this.
- While there is no limitation to the file size, the recommended number of MAC addresses should not exceed 10,000.

Managing sites and devices

Vista Manager enables you to easily back up nodes, restore the network from back up, reboot nodes, and manage nodes by using SSH to access their command line.

Backup a node

Select the device that you want to back up:



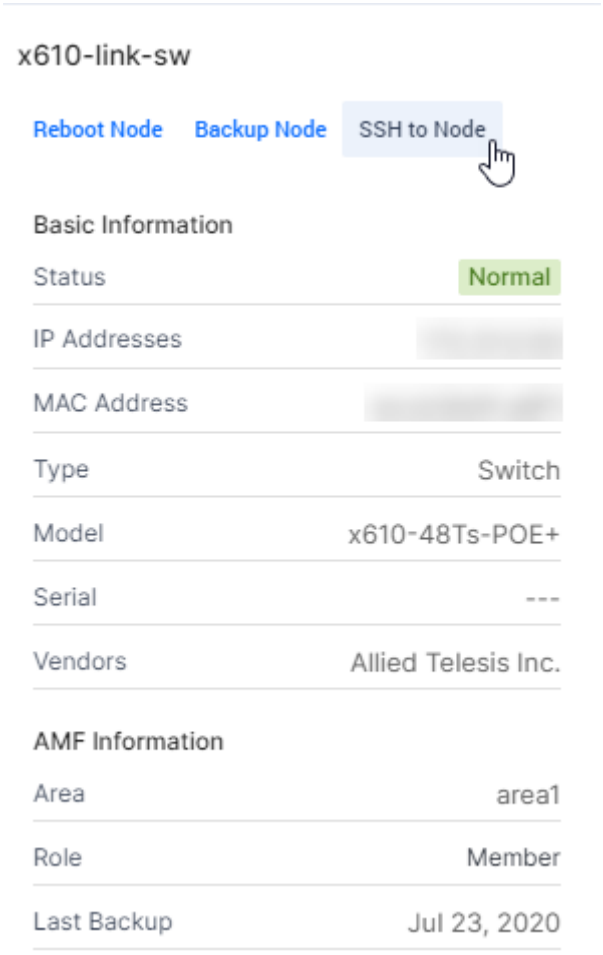
Click on the **Backup Node** button.

An information message is displayed showing that the backup has occurred:

SSH/Shell to a node

From Vista Manager EX you can open a Secure Shell connection to a device. From this session you can connect to the device and issue CLI commands as if you were directly logged into the device itself.

Select the device that you want to connect to:



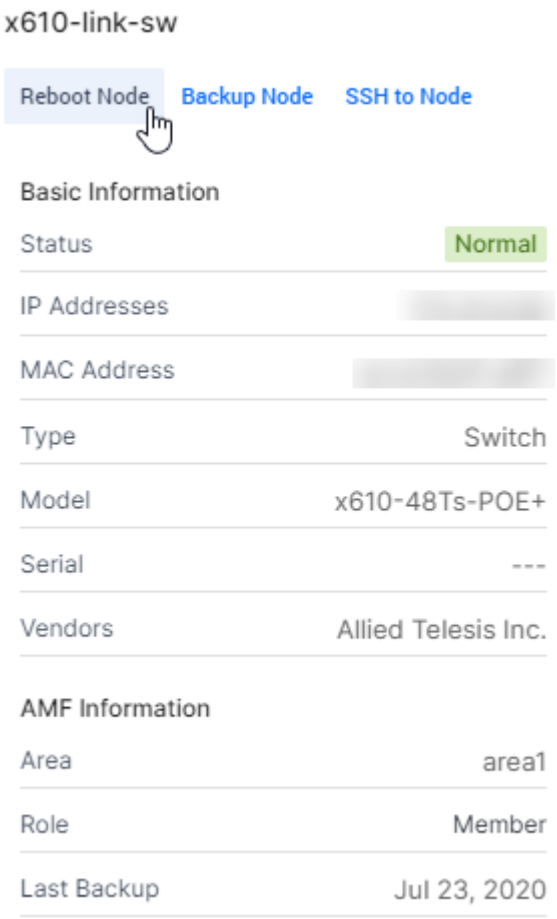
Click the **SSH to Node** button to start a CLI session.

The following window is displayed:

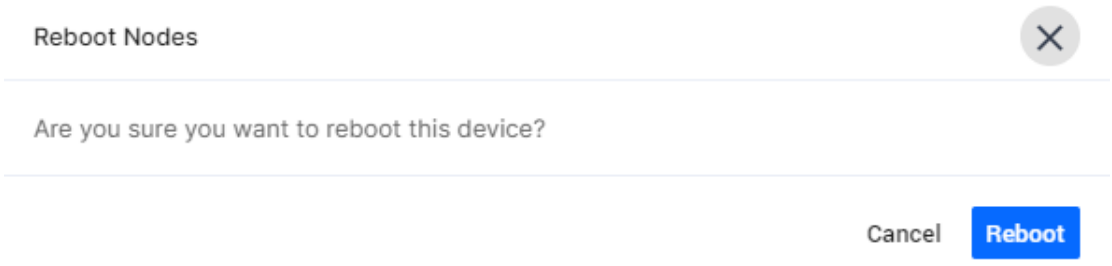
From this session you can carry out any CLI commands as if you were directly logged on to the device.

Reboot a node

Select the device that you want to reboot (in this case from the Network Map pop up window):

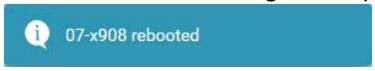


Click the **Reboot Node** button.

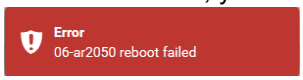


Check that you have the correct device selected and click the **Reboot** button if you are sure that you want to reboot the device.

An information message is displayed showing that the selected device has rebooted:



If the reboot fails, you will see an error message as follows:



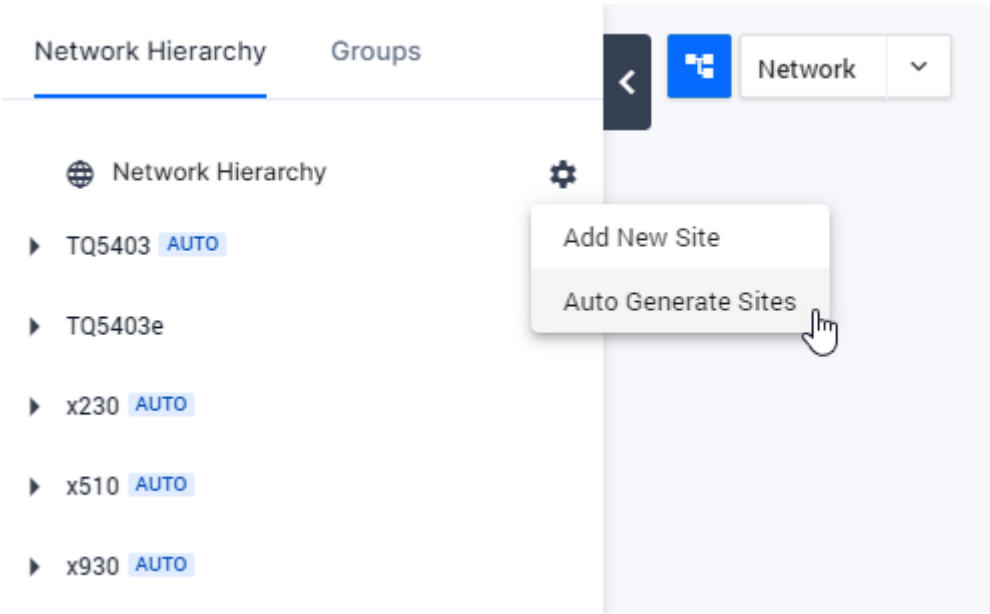
Intelligent device grouping

By selecting a Network Hierarchy preference, you can organize your network easily. When a new device is added into the network, it can be automatically assigned to a site based on its hostname. Intelligent device grouping comes with a range of functionalities:

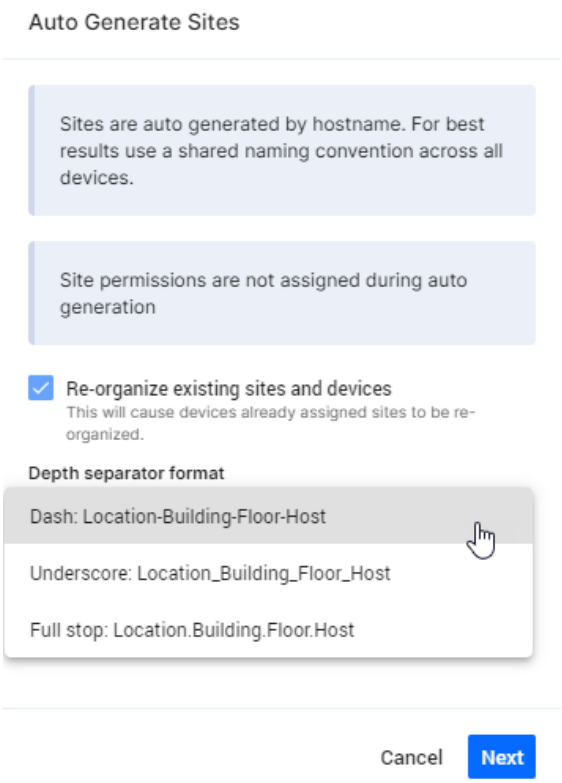
- initiate a request to automatically generate the Network Hierarchy sites at any time
- select the strategy of the automatic generation, based on the hostname of the devices
- preview auto-generated sites showing up to 5 auto-assigned devices before finalizing changes
- rename or remove auto-generated sites during the preview
- reorganize existing sites after finalizing auto-generated sites

Note: Removing a site only stops the automatic assignment, it does not remove the site from Vista Manager EX.

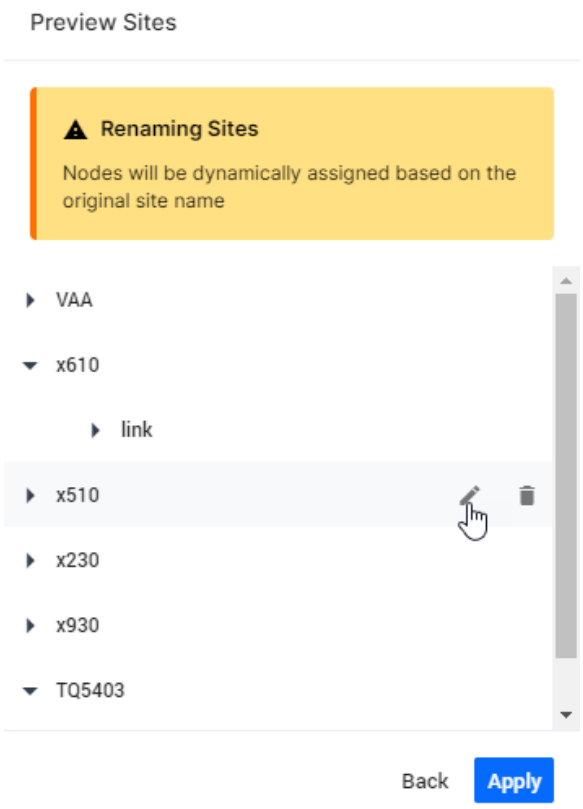
To use this feature, navigate to the **Network Map** page. Click on the **Network Hierarchy** icon at the top left of the map screen to display the side panel list of sites. Click on the cogwheel and select **Auto Generate Sites**.



From the drop-down, select a separator format for the hostname to match on, such as a dash, underscore, or full stop. Click **Next** to preview sites.



In the preview, you may rename or remove sites. Click **Apply** to finalize changes.



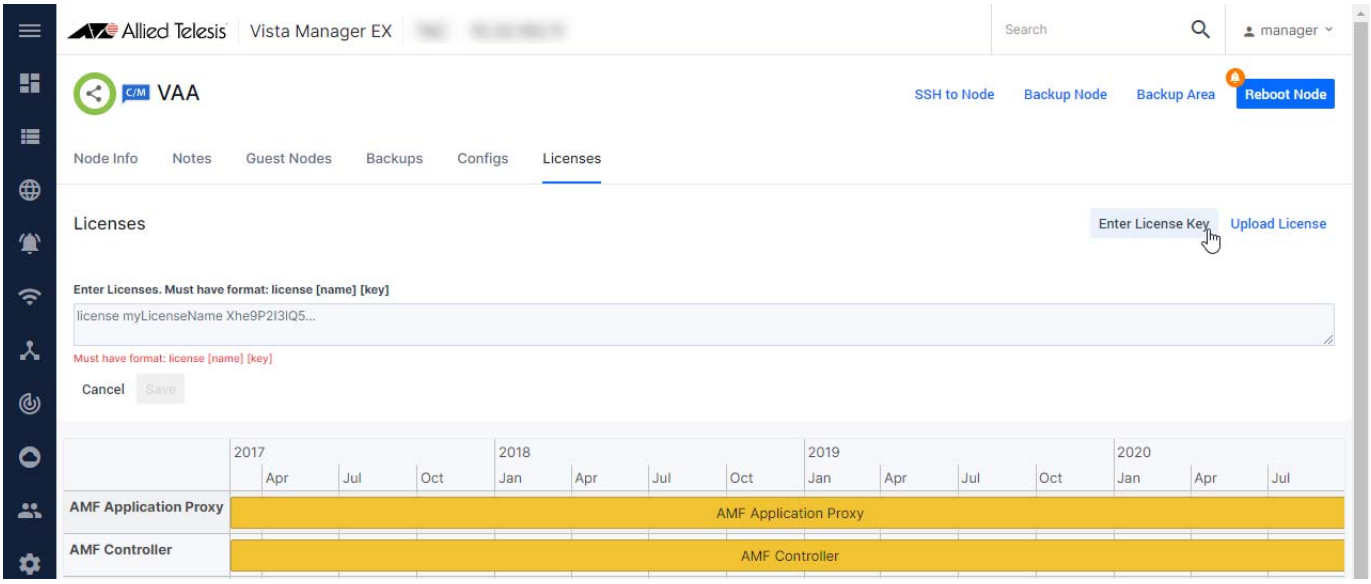
All devices will be automatically grouped into an appropriate Network Hierarchy group. You can manually collapse other devices on the integrated map, which allows you to focus only on the high-level networks.

Take note of the following limitations:

- The automatic generation of sites supports up to 3 levels of network.
- The automatic generation of sites overwrites existing Network Hierarchy sites if they have the same name.
- When the sites are overwritten, the devices belonging to the original site will be unconditionally moved to the new auto-generated site.
- If the overwritten site is also an auto-generated one, it loses its auto-assignment functionality and gets overwritten by the new, auto-generated one.
- If a site has a duplicate name with an existing one in the preview stage, a confirmation dialog pops up, indicating the site will be overwritten.
- New nodes will not be positioned near others in a site when they join a network and match the automatic assignment criteria.
- Renaming or removing auto-generated sites stops the automatic assignment.

AMF node licenses

You can add and examine licenses on an AMF node from the **Licenses** tab.

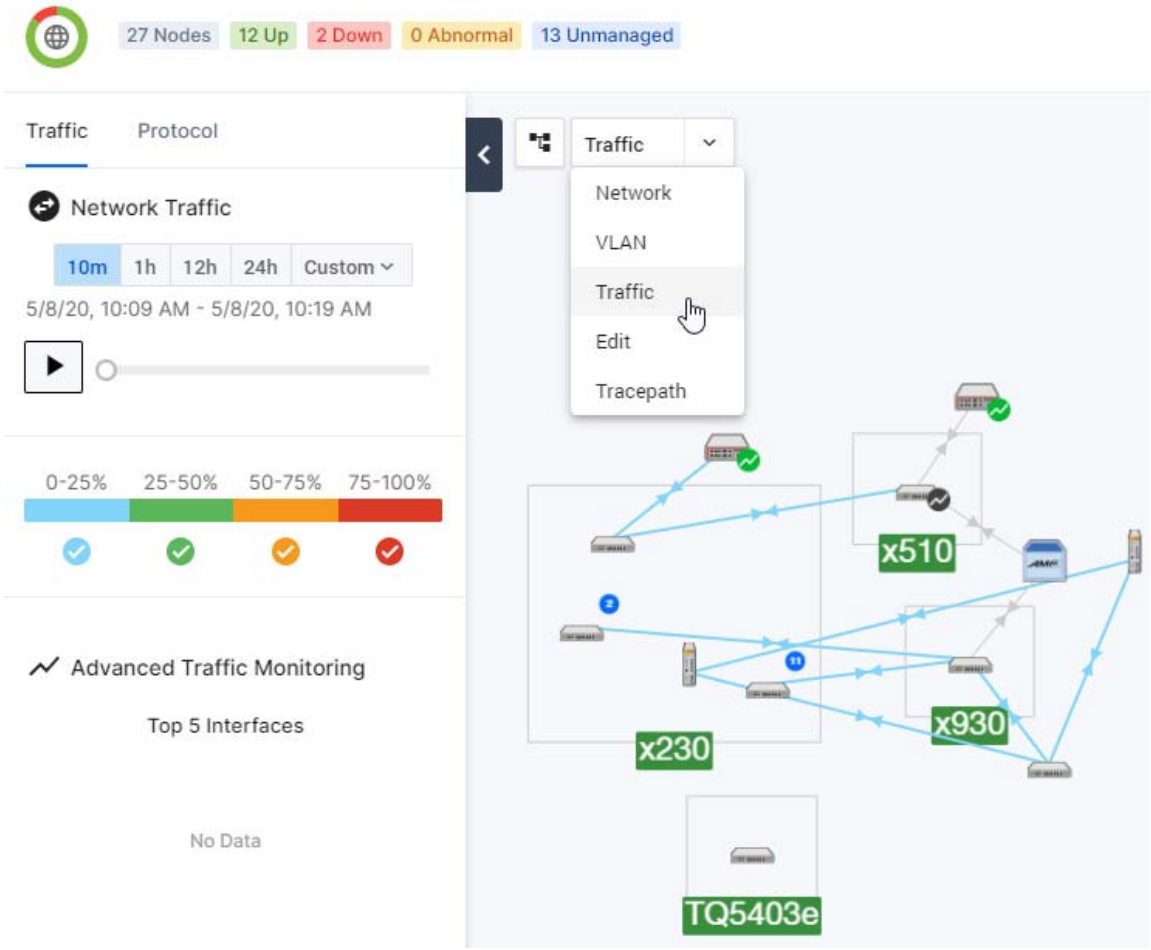


The **Enter License Key** button allows you to add a license by copy-and-pasting the license enable command. The **Upload License** button allows you to select either a system license certificate (.csv) file or a flexera license capability response (.bin) file.

Hovering over a license bar displays a pop-up with additional information about that license.

Traffic monitoring

Vista Manager's color-coded traffic monitoring map provides a visual status of network utilization, across all links in both directions. It is constantly updated to keep the latest traffic pattern information readily available.



Colors and line thickness highlight link utilization and available bandwidth, allowing for instant performance monitoring. It also allows you to change which information is displayed, so that you can focus on your network priorities.

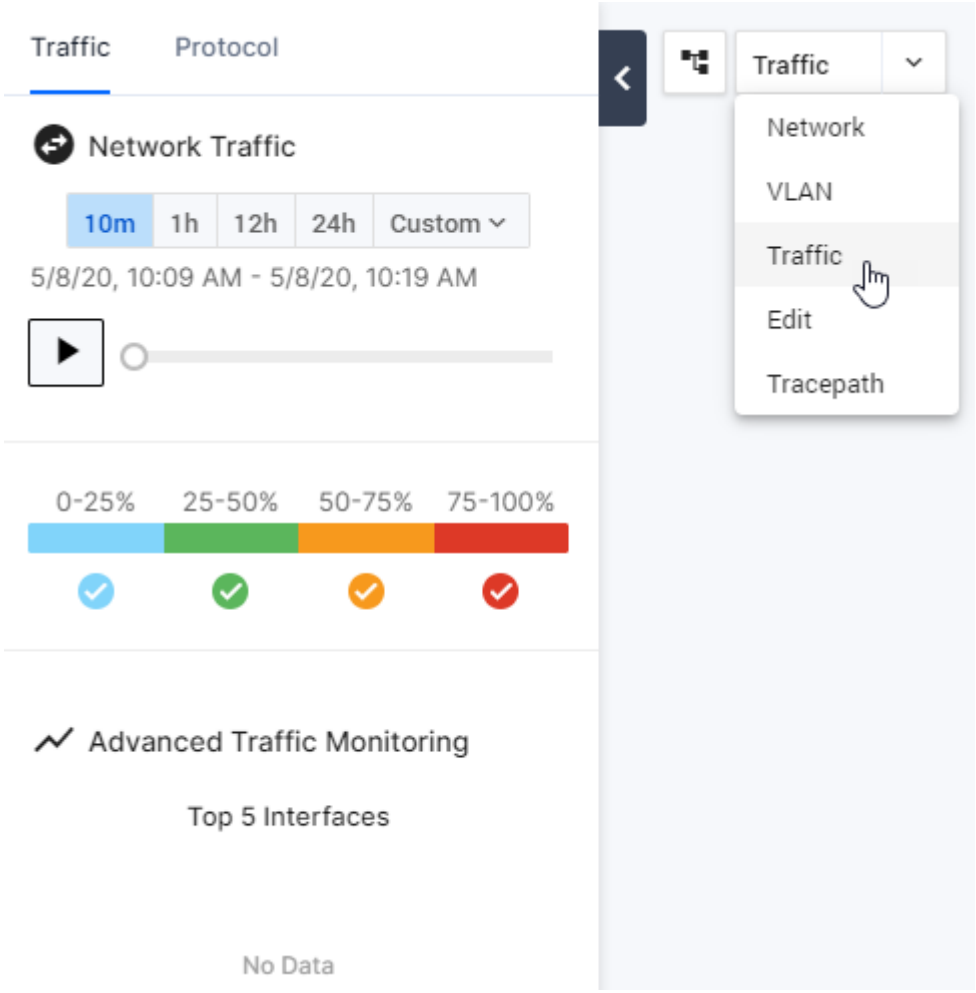
It also enables you to improve your network planning by analyzing data traffic from any chosen time over the last week. In addition, you can monitor any link by clicking to show bi-directional traffic on all aggregated ports over the last 24 hours.

For additional information and to see how to use the traffic monitoring functionality, refer to the Traffic Monitoring video on the Allied Telesis website.

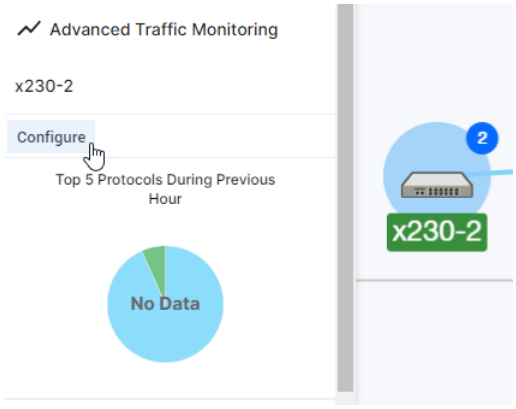
Advanced traffic monitoring with sFlow

Vista Manager allows you to monitor traffic in your network using sFlow (sampled flow). After configuring sFlow on your network devices, you can use advanced traffic monitoring to view information about network traffic, protocols, and applications.

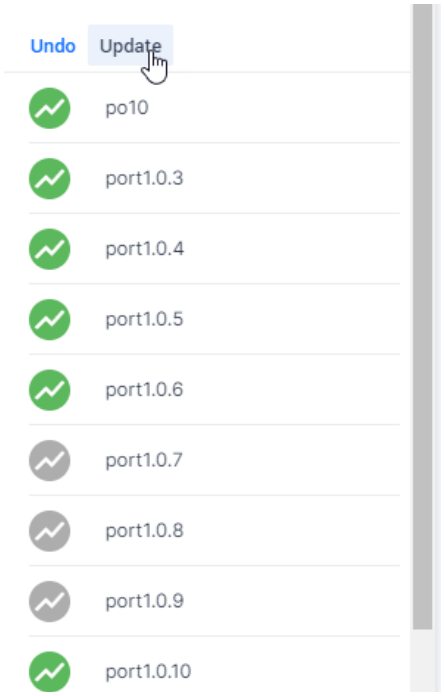
Advanced traffic monitoring can be accessed from the network map menu. Click on the dropdown, then select Traffic. This opens the Traffic sidebar. Advanced Traffic Monitoring will appear at the bottom of the sidebar. When you first open it, there will be no data, since you will not have configured any nodes for sFlow.



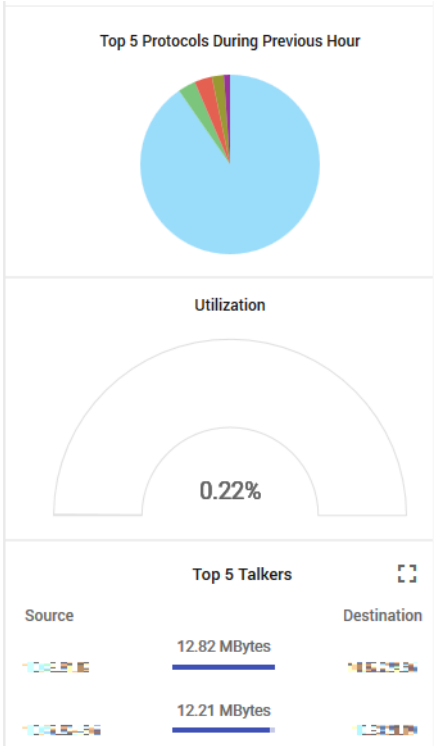
Select a node from your network map, and click on Configure to configure it.



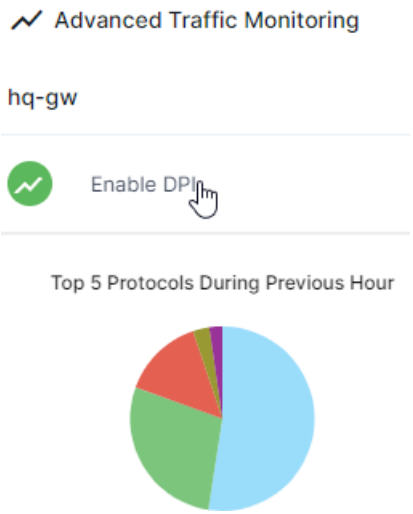
The side panel will show a list of the ports on the node. Click on a port to enable (green) or disable (grey) sFlow on the port. Click Update to save the changes.



The side panel will then show monitoring output from the selected switch, including the protocols, utilizations, and talkers.

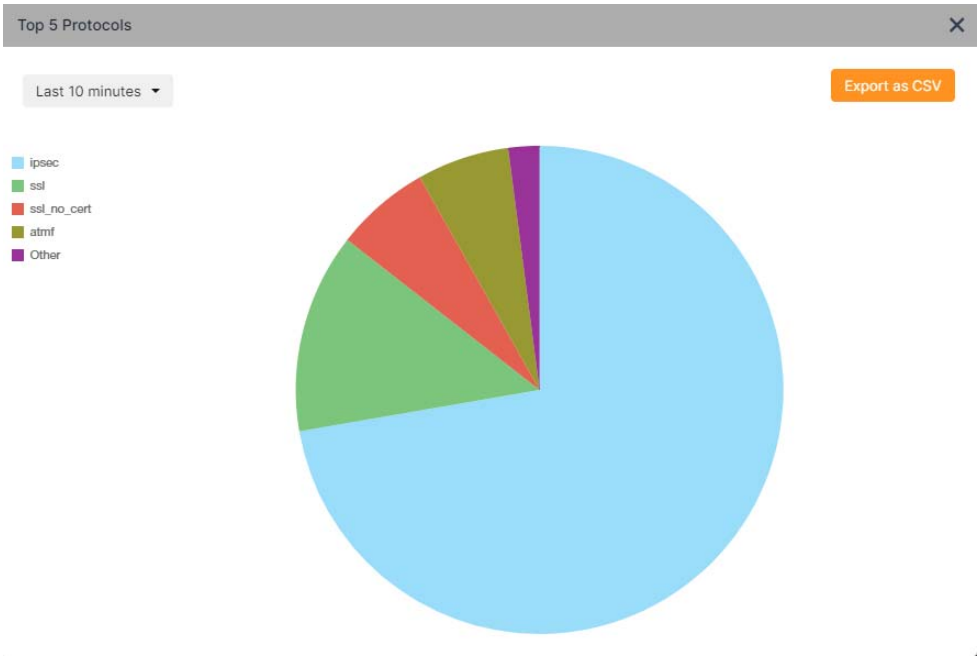


Routers do not support sFlow. However, by enabling DPI on a router, some traffic monitoring can be carried out. Click to enable DPI.

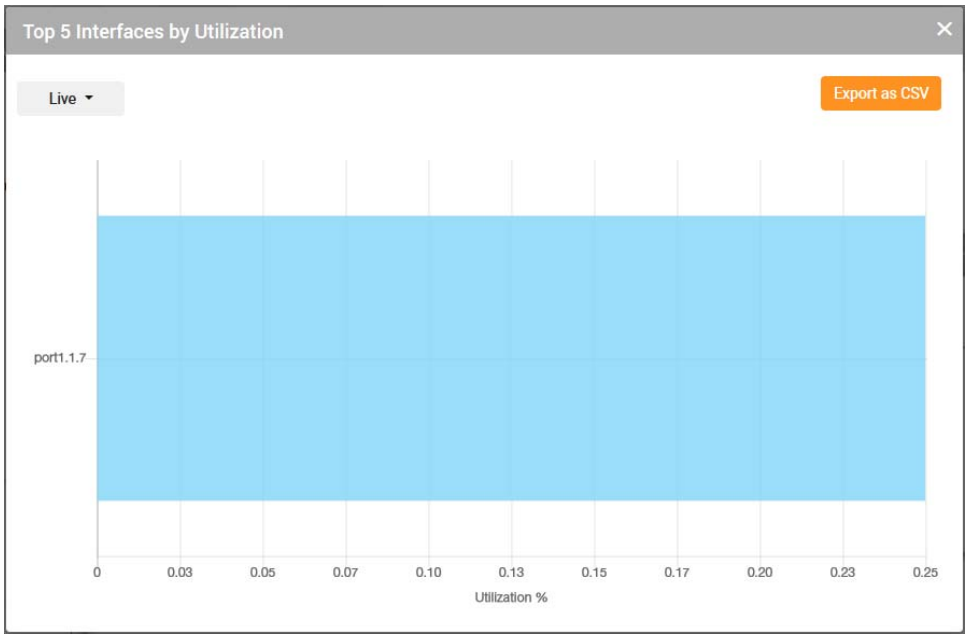


The side panel will show the protocols being used by the router.You can click on the items in the side panel to open the associated widget.

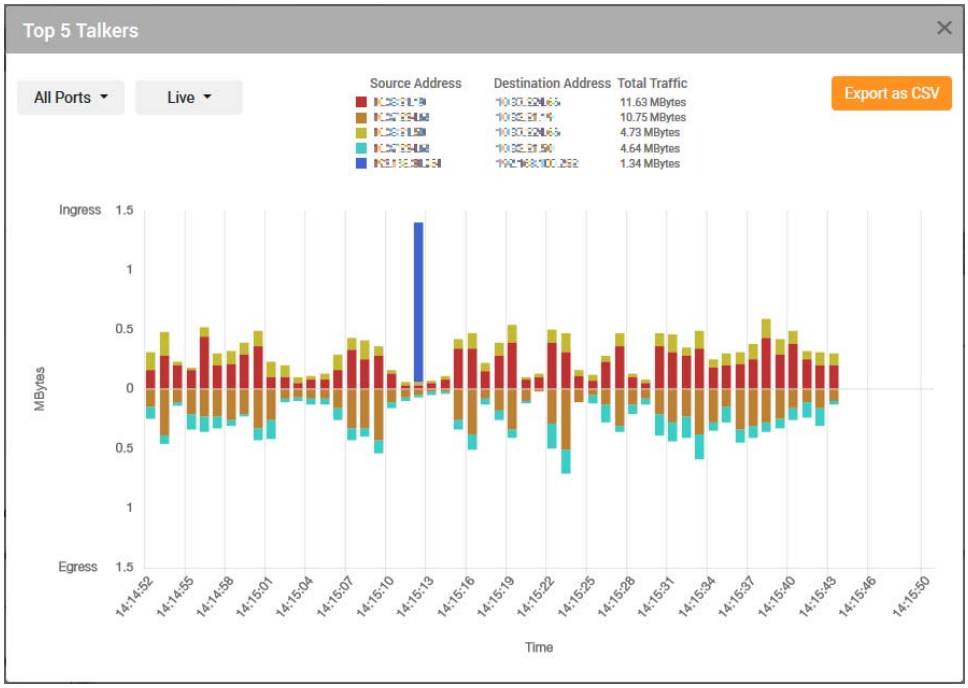
Top 5 Protocols:



Top 5 Interfaces by Utilization:



Top 5 Talkers:



Information from the widgets can also be exported to a CSV file. To do so, click on the Export as CSV button in the top right corner.

Note: Configuring devices for sFlow using Vista Manager requires the device to be running Alliedware Plus version 5.4.8-2 or later. Devices running older releases are still compatible with this feature; however, the sFlow configuration will have to be done manually through the CLI.

Sample sFlow CLI configuration:

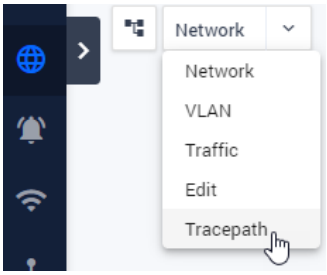
```
sflow agent ip 172.31.1.245
sflow collector ip 192.168.1.1
sflow enable
!
interface port1.1.1
sflow sampling-rate 8192
sflow polling-interval 60
```

Vista Manager uses the sFlow agent IP address to match the data received with the correct AMF device. The agent IP address must be the same as the AMF Management IP address. The IP address can be found using the **show atmf detail** command.

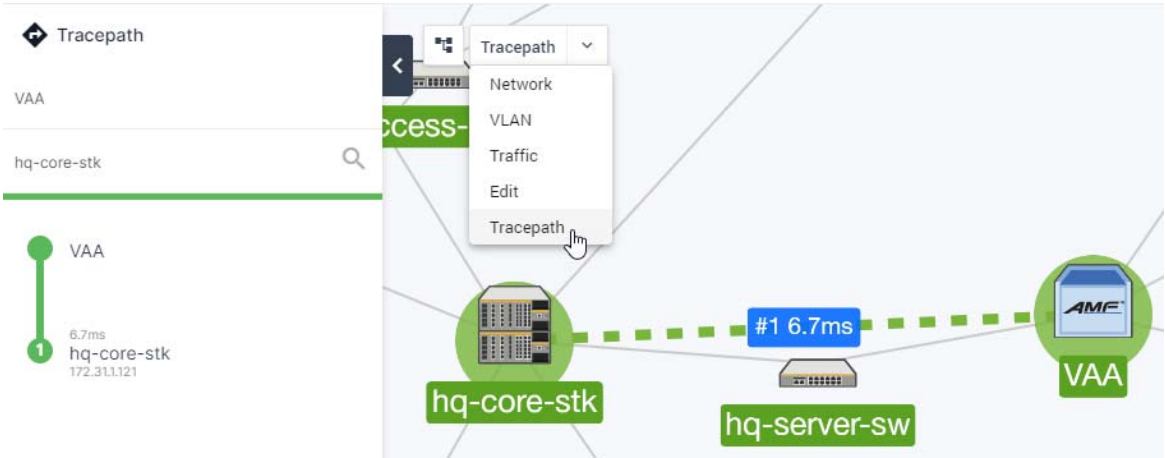
Tracepath

Tracepath allows you to determine where traffic is flowing. You can click on two nodes in the Vista Manager network map, the source and destination. Vista Manager will display the path between them and show RTT (round trip time) information.

To use tracepath, open the Network Map in Vista Manager. Click on the dropdown and select **Tracepath**.



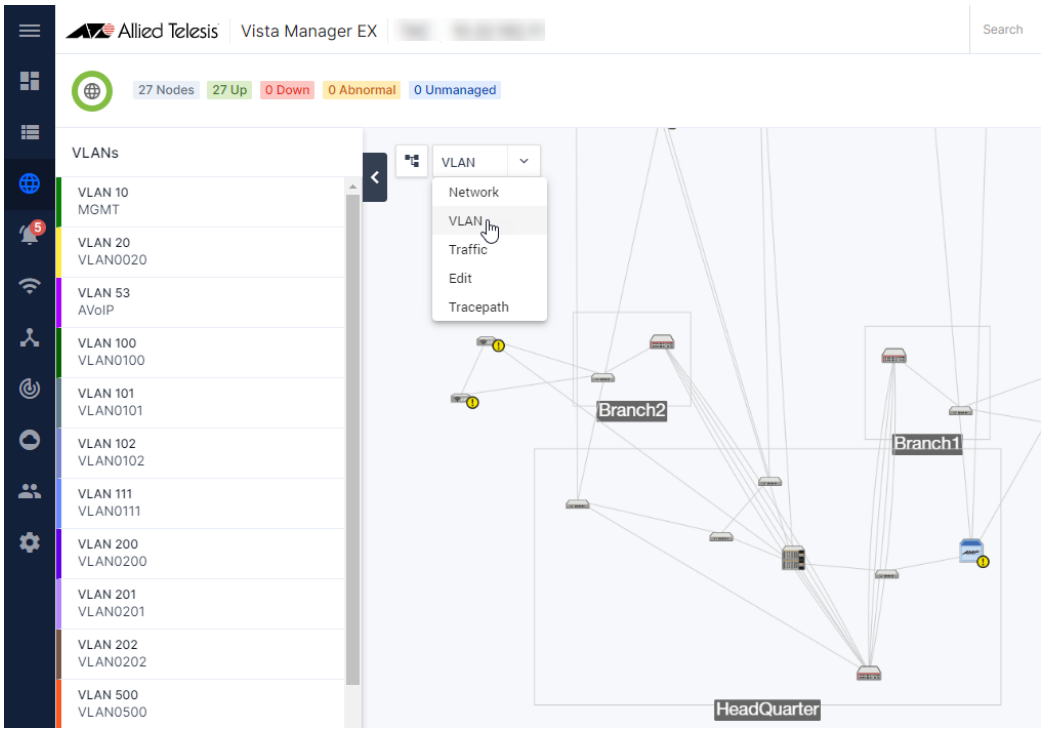
You can manually enter the source and destination from the list on the left, or click on the nodes on the map to select them.



VLAN management

The color-coded Vista Manager VLAN Map lets you manage VLANs across multiple devices, including support for aggregators and stacking. Using the VLAN configuration tool, you can:

- create new VLANs
- destroy existing VLANs
- configure VLAN Names, VLAN Types, and VLAN IDs
- add ports to VLANs
- delete ports from VLANs
- set VLAN ports as tagged or untagged
- save the configuration



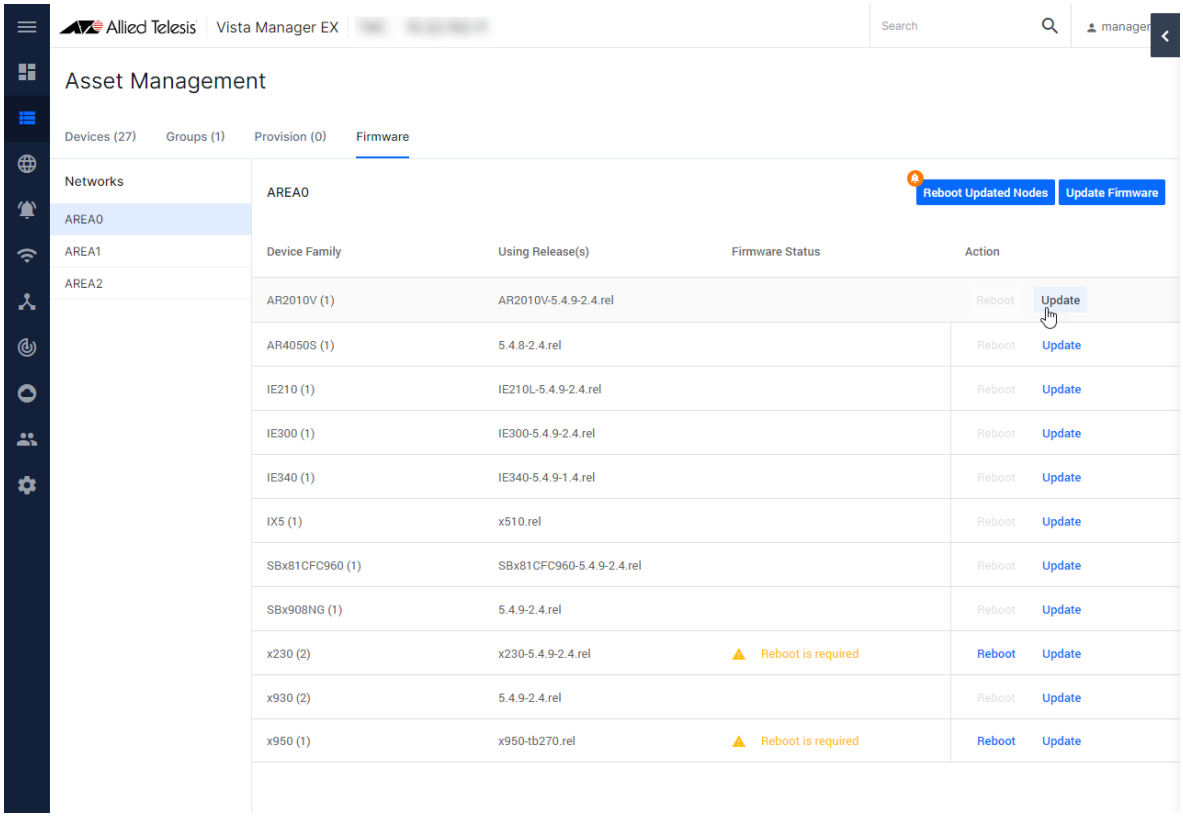
The VLAN map shows all your VLANs at a glance, across the whole network. You can narrow the focus to individual VLANs to show application deployment.

Creating new VLANs across multiple switches can be done quickly using the simple point-and-click interface. You can also edit any VLAN, at any time, to support new users and changes in business requirements.

For additional information and to see how to use the VLAN management functionality, refer to the VLAN Management video on the Allied Telesis website.

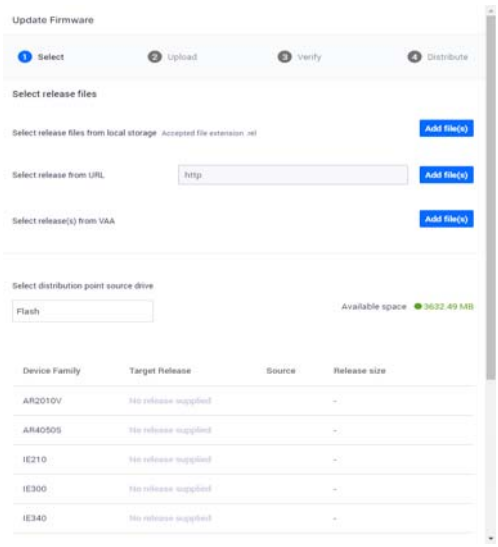
Firmware management

This feature provides you with the ability to update firmware across a node or family of nodes on a network (AMF area), and then schedule a time when the nodes will reboot to install the firmware release.



1. From the left-hand menu, click Asset Management and click on the **Firmware** tab.
2. To the right, you will see buttons to "Update" a family of nodes, or an **Update Firmware** button to update all families in an AMF area. Click any of the blue **Update** actions.
3. The side panel opens, showing 4 steps. For this process, you will need a firmware release file for that family.

Note: This file is not the same release as the current file running on the nodes.



Step 1. **Select release files for the Area Master. Permitted file types are .zip and .rel files. The source options are:**

- from local storage
- from a URL
- existing file on the AMF Master (distribution point)

Note: Users also have the option to copy the file to a USB drive if their Flash drive is full on the distribution point.

Note: If updating multiple families, target release files will appear in each row at the bottom.

Click the Add file(s) button and select the release file you wish to add. Then click Next.

Step 2. **The progress bar advances as the file uploads. Click Next once it completes.**

Step 3. **The status shows as "*Verifying...*", and then either success or that a number of nodes failed. If any failed, click More info to see exactly which nodes failed and why. Assuming that some succeeded, click Update device.**

Step 4. **The status shows as "*Distributing to...*". Click Done once distribution finishes.**

4. Click **Reboot Updated Nodes**, then select the date and time for the reboot. After the reboot, those nodes will be running the release file provided.

Zip folder support

The zip folder feature allows you to run firmware distribution with a URL that points to a zip file. Vista Manager EX first extracts the zip file onto a temporary directory. The release file will then be distributed to the device family if there is a match. Otherwise, you will be notified of any invalid extract files. Non-release files in the zipped folder will be ignored.

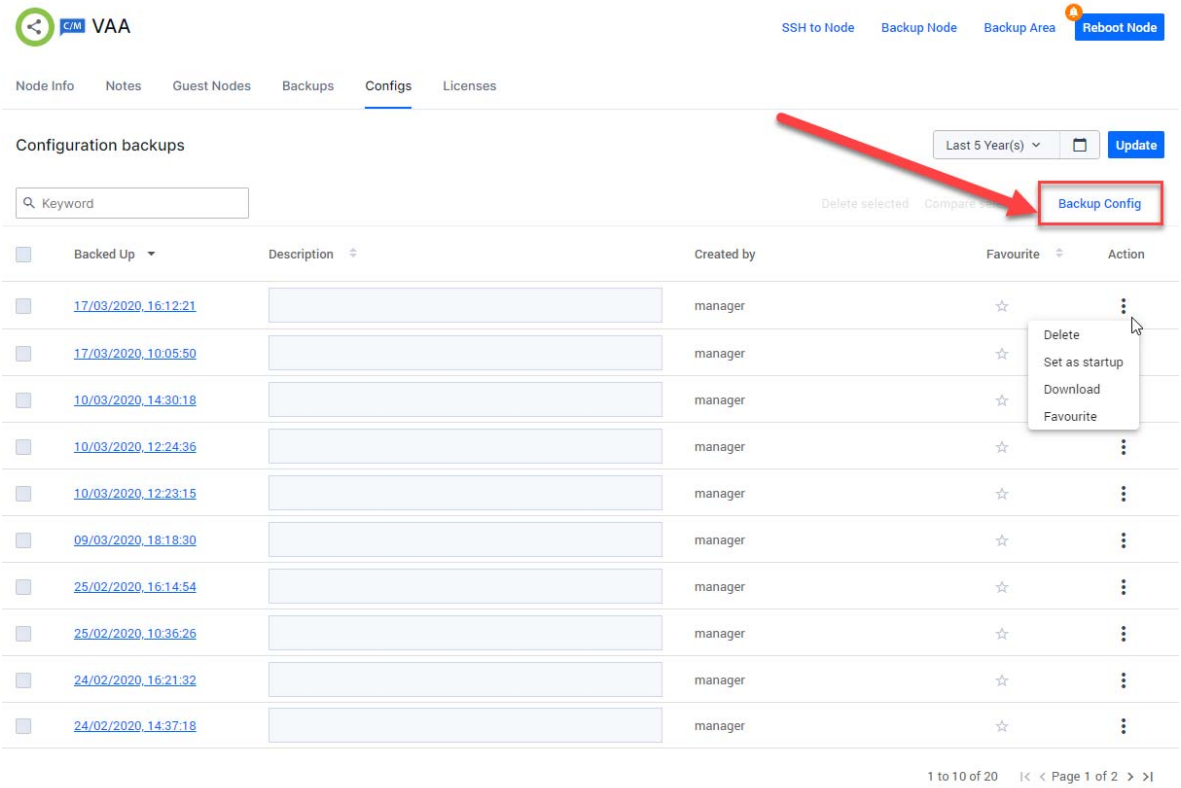
This feature is supported for firmware version AlliedWare Plus v5.4.9-1 or later.

Configuration management

This feature provides you with the ability to manage startup configuration files, including backing up, restoring and comparing configuration files. With the configuration management tool, you can:

- save a configuration file
- view details of a backup configuration
- compare two backup configuration files
- apply a saved configuration to a device
- delete a configuration backup
- set unlimited favourite configuration files

Note: Favourite config files cannot be accidentally deleted, unless unfavourited first.



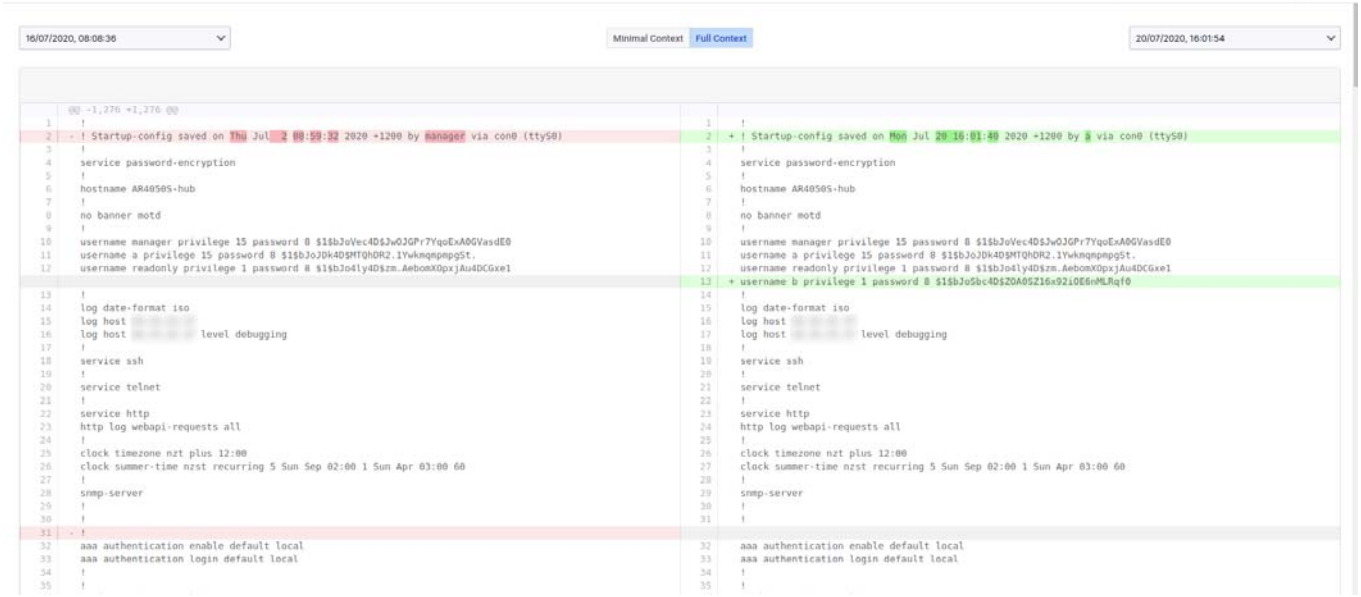
1. From the left-hand menu, click Asset Management and select the device you wish to work with, for example, VAA.
2. Click on the Configs tab.
3. Click on the **Backup Config** button. A notification on successful backup will appear.
4. Type a brief description in the Description textbox. Click outside the textbox to save.
5. Click on the Action drop-down for a config backup that you wish to set as startup, and select **Set as startup**.
6. A reboot would be required to load the new config. Click the **Reboot Node** button immediately, or schedule a time for it.

Note: Restoring a config overwrites the contents of the current startup-config only. The original filename and location of the backup config will not be used during the restore.

Note: When a device config is saved using the CLI, Vista Manager detects this and automatically runs a backup without requiring any user action.

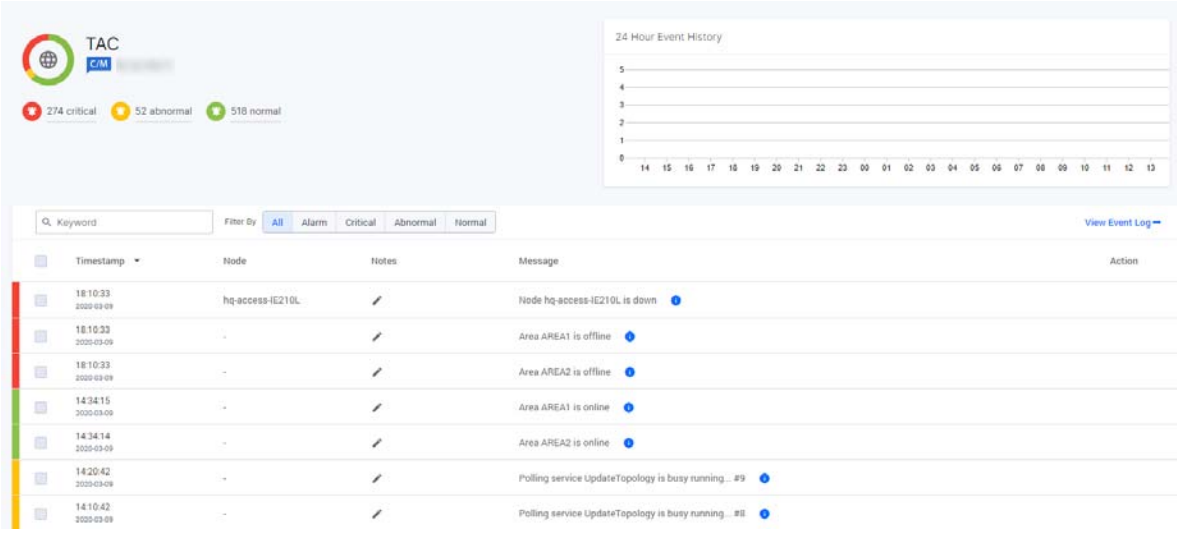
Comparing configuration files

When comparing two configuration files, the tool displays differences in full, or just five lines of either side, highlighting differences in bold and in color. Toggle between settings using the **Minimal** and **Full** buttons. This enhancement provides better context to the overall configuration and helps you make a more informed decision about the changes being written to your device.



Using the event log

From the left-hand menu select **Events** to display all events in the log, as follows:



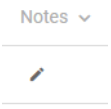
The event log shows currently uncleared events. Critical events have a red background, abnormal events are yellow, and normal events are green.

You can enter notes on any event, clear events, and filter on different fields in the event display.

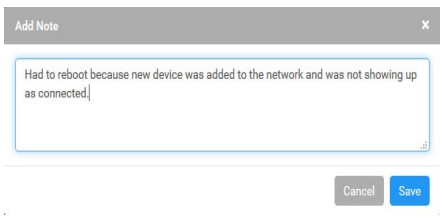
You can search the event log based on details of the event such as the time period in which it occurred. A graph at the top of the screen shows how many events have been received over certain time periods.

Adding descriptions or notes to events

Click on the **Note** icon to add a note:



The following dialog box displays and enables you to add or edit the note.



Click on the **Save** button to save the note to the event.

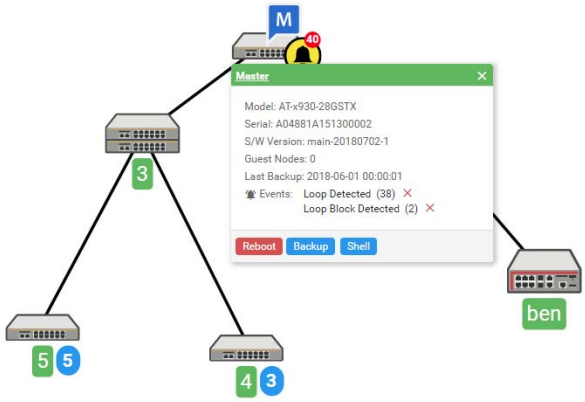
Archiving event notifications

If you want to archive old or cleared events, click on the check box on the left-hand side of each event to select the events to be archived. This activates the **Archive selected events** button. You

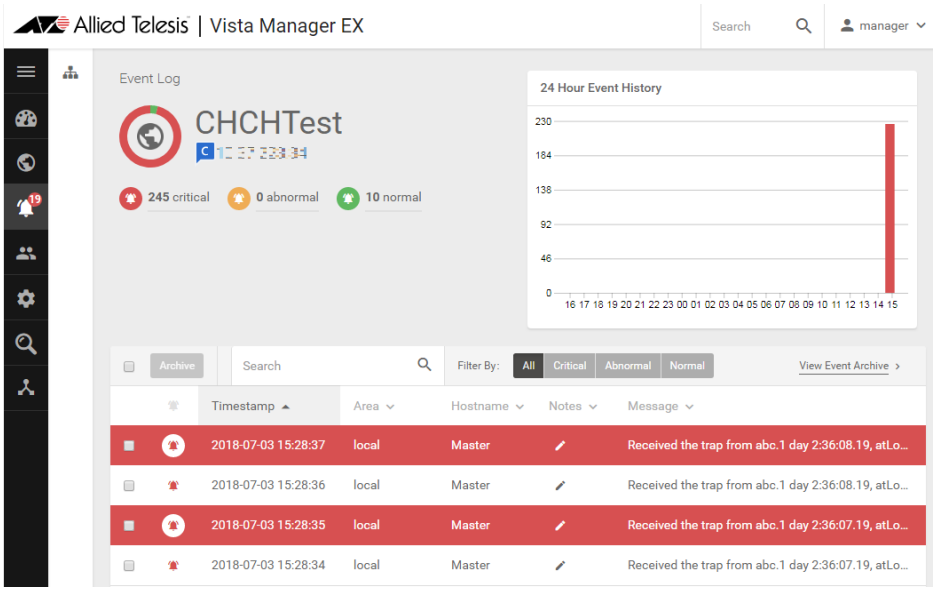
can select all listed events by clicking the check box at the top of the list. You can view archived events by clicking on the **Event Archive** tab.

High priority events

Critical events are displayed as a red number on the alert icon of the node they occur on. Click on the node to display a pop-up with node information and a list of critical events. Dismiss events by clicking on the red-cross next to the event description.



Events can also be dismissed by viewing the event's details on the Event Log page. Dismissing an event changes the log entry background color from red to white and decreases the alarm icon's event count in the side bar.



SES block actions

Secure Enterprise Software Defined Networking™ (SES) blocking actions, configured using AMF application proxy, are displayed as high priority events. SES blocking actions configured using OpenFlow are not yet supported.

The following SES blocks will be shown on the Area Map and in the Event Log:

- SES Drop
- SES Quarantine
- SES Link Down

In addition, the following SES action will appear in the Event Log only:

- SES IP Filter

See the SES Controller and Autonomous Management Framework (AMF) Application Proxy Installation and User Guide for more information on configuring SES and the AMF application proxy.

SNMP traps

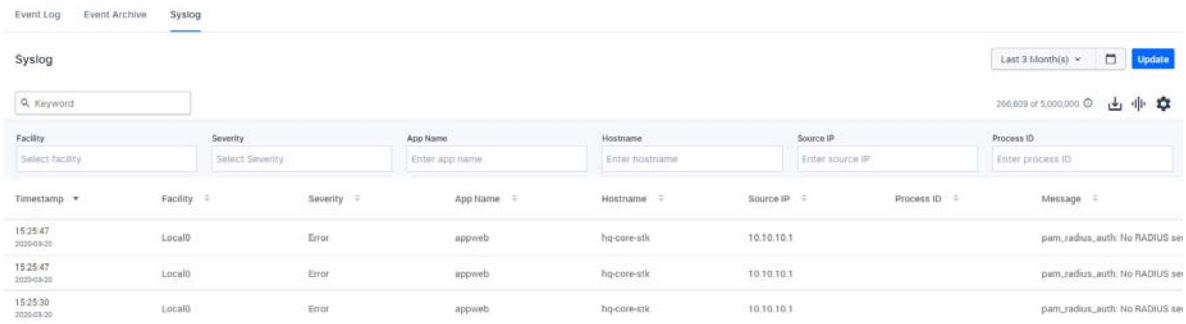
If they are configured, the following SNMP traps will appear as high priority events:

- SNMP loop detection traps
- SNMP active fiber monitoring traps

Both these events require the SNMP plug-in.

Using the syslog server

From the left-hand menu click **Events** then select the **Syslog** tab, as follows:



The syslog server shows messages from the network or for a specific device on the network. Depending on your level of access, Administrator access allows you to configure how long to store syslog messages. The default configuration is 365 days. Messages older than the default or configured length of time are automatically deleted. The syslog storage is limited to 5 million entries.

Permissions for syslog

- Only an admin user can view all syslog messages received from an IP address that Vista Manager has not discovered in the network.
- Any device can send syslog messages. If the source IP address does not correspond with a Vista node, only an admin user can view the message.
- A user can only view and search for syslog messages on the network or for a specific device they have read/write access to.
- A user cannot edit or delete syslog messages.

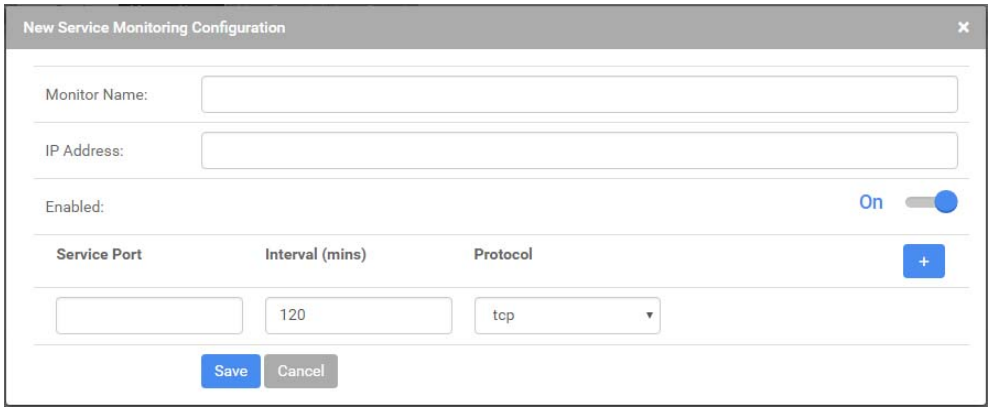
Service monitoring

Service monitoring allows a network administrator to learn the status of services running on devices within Vista Manager EX. You can configure a monitoring task to run periodically, or to monitor services on demand.

Service Monitoring will display the status of the services. It helps you track the status of services of critical importance, and be updated as soon as they go down. Knowing the status of services may also help when performing diagnostic tasks.

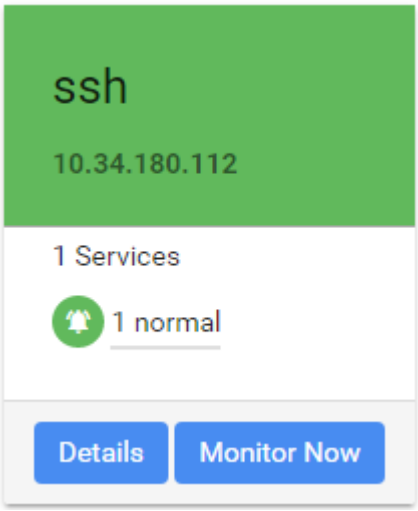
To configure service monitoring:

- Open Service Monitoring in Vista Manager.
- Click on Create Monitor.
- Enter the following details:



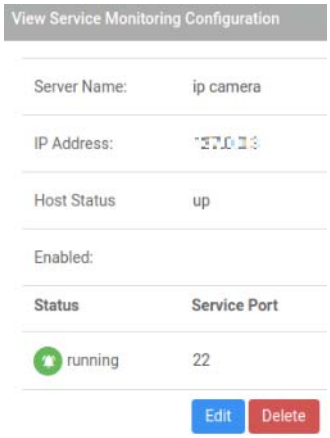
  - Monitor Name - a name to identify the monitor
  - IP Address - the IP address of the device you want to monitor
  - Service Port - the port that the service is running on
  - Interval - how often to monitor the service
  - Protocol - the protocol of the service, either TCP or UDP
- Click Save.

The monitor has now been created. Click on Monitor Now to begin monitoring the service.



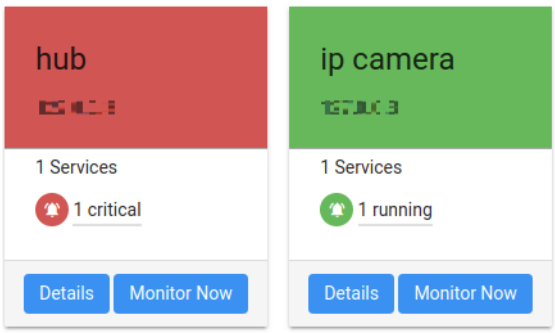
The service statuses may be one of the following:

- Pending: The service has not been monitored yet.
- Running: The service has responded to the latest monitoring probe.
- Filtered: Unable to determine the status of the service, because it is blocked by a network obstacle such as a firewall.
- Indeterminate: Unable to determine the status of the service. It may be blocked by a network obstacle, up, or down.
- Closed: No application is listening on the specified port.
- Unresponsive: A service exists on the port, but is not responding to probes.
- Unreachable: Unable to monitor the service, because the target IP address is unreachable.
- Error: Unable to monitor this service, because an error occurred while attempting to do so.



The status categories and the statuses that fall into each category are as follows:

- Category Pending - Pending status
- Category Normal - Running status
- Category Unknown - Filtered and Indeterminate statuses
- Category Critical - Closed, Unresponsive, Unreachable, and Error statuses



HTTPS access to Vista Manager EX

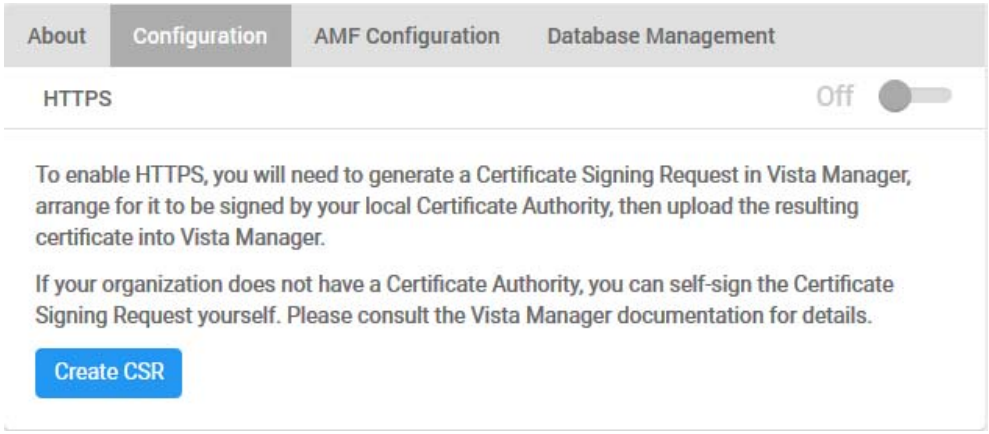
All traffic between Vista Manager EX and users is able to be secured with HTTPS. This option can be turned on in your Vista Manager EX configuration settings. Enabling HTTPS requires a signed certificate.

Vista Manager EX can generate a Certificate Signing Request (CSR) which you can then submit to a Certificate Authority (CA). The CA will then give you a signed certificate which you can import back into Vista Manager EX. Note that both the application's and CA's private key are never transmitted; this is essential to maintaining proper security.

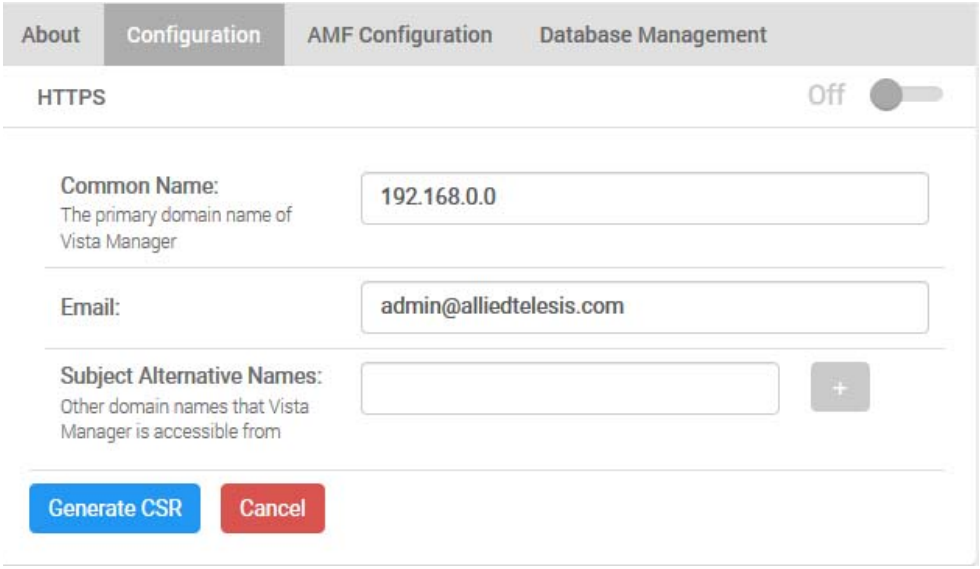
Alternatively, you can use OpenSSL to self-sign the CSR. For more information, visit https://www.openssl.org/.

To enable HTTPS:

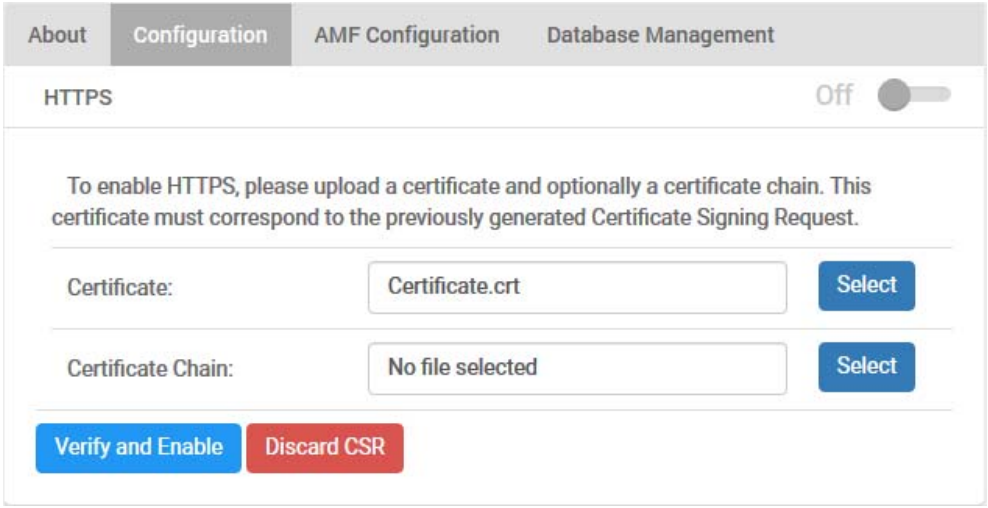
- In Vista Manager, open the System Management menu item and click on the Configuration tab.
- Click on Create CSR.



- Make sure the primary domain name and email are correct. You can also add other domain names if required.



- Once the CSR has been generated, save it somewhere safe. Send this CSR to your CA to be signed.
- Once the CA has returned to you with a certificate, click the Next button. Then upload the certificate to Vista Manager. You can also optionally upload a certificate chain.



- Click on Verify and Enable. Once your certificate has been verified, HTTPS will be enabled.

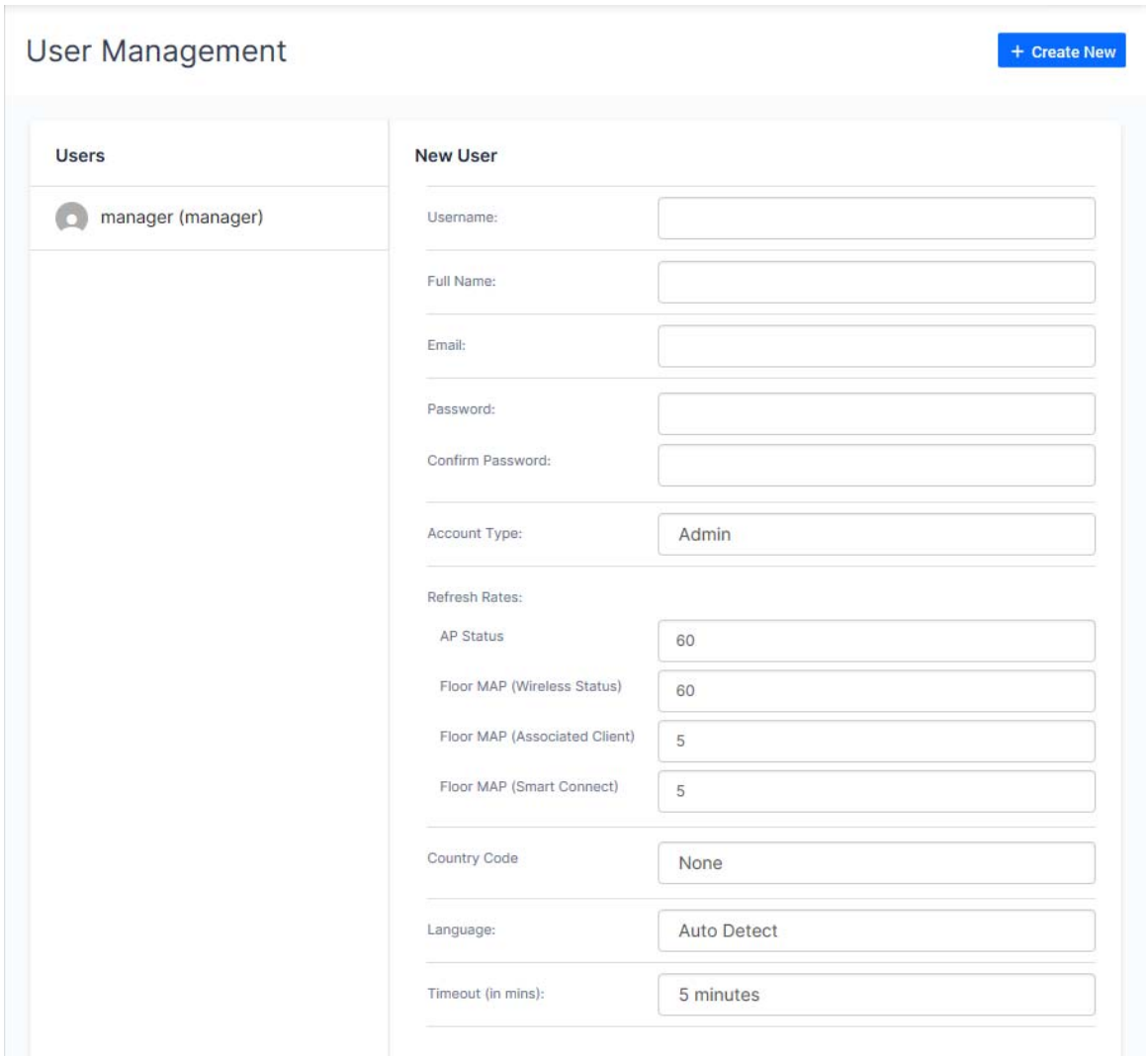
Once you have configured HTTPS for Vista Manager, you access it using the default SSL port. To connect via HTTPS, use either of the following URLs:

- https://<ip address>
- https://<ip address>:443

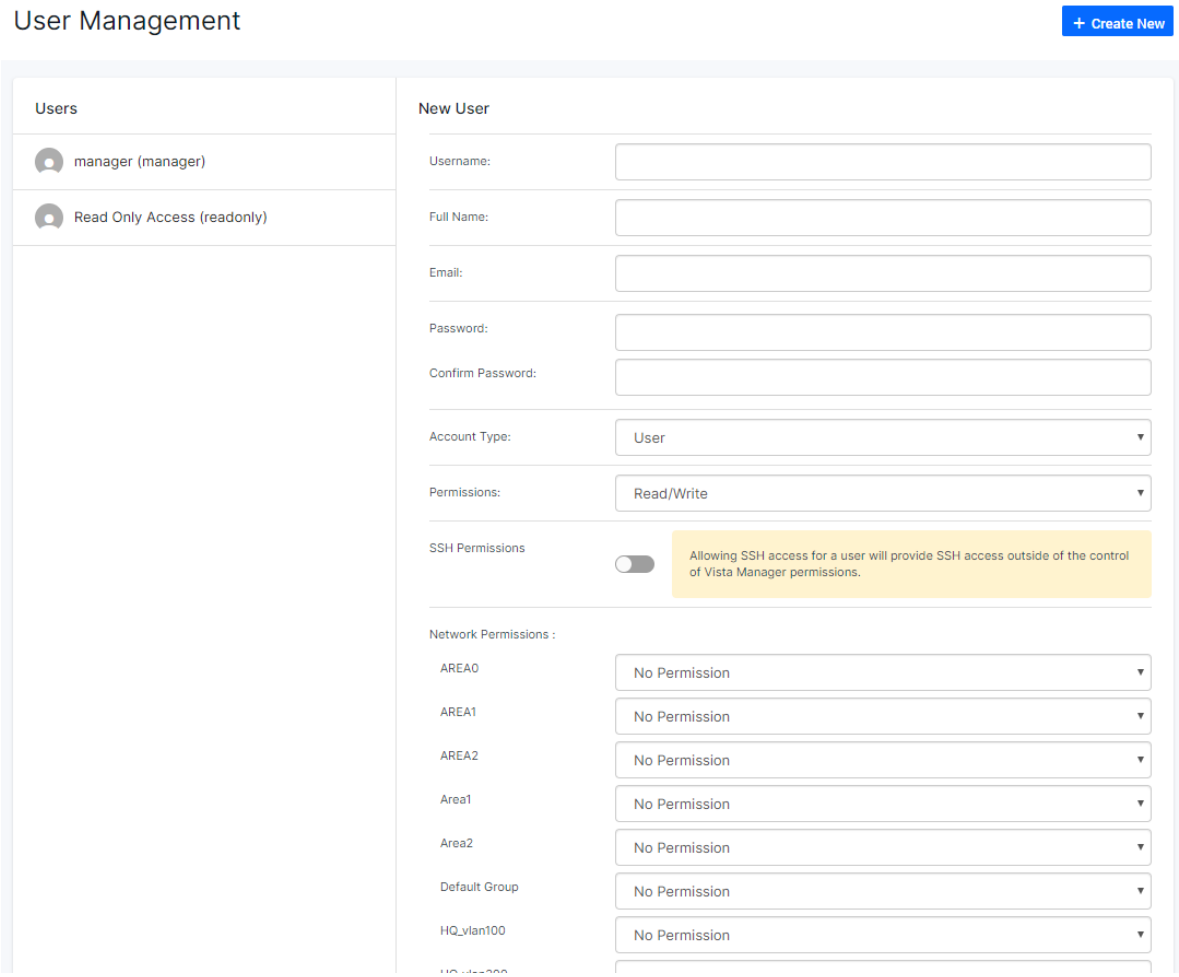
Managing user accounts

There are two types of user account, **Admin** and **User**.

Admin accounts have read/write access across all AMF areas.



User accounts are configured to have **Read Only** or **Read/Write** access on the specified AMF area(s).



Create an account

1. Log in with an Administrator account type
2. Select **User Management** from the menu
3. Click the **Create New** button in the upper right hand corner of the screen
4. In the **New User** dialog box enter the relevant user details.
5. Click the **Save** button

Edit an existing account

1. Log in with an Administrator account type
2. Select **User Management** from the menu
3. Select the account you want to edit from the account list
4. Click the **Edit** button
5. From the Edit User dialog box make the changes
6. Click the **Save** button

Set the time-out for an account

1. Log in with an Administrator account type
2. Select **User Management** from the menu
3. Select the account you want to edit from the account list
4. Click the **Edit** button
5. From the Timeout dialog box, select how long until a user is automatically logged out, or select Never to disable automatic logout for that user
6. Click the **Save** button

Delete an existing account

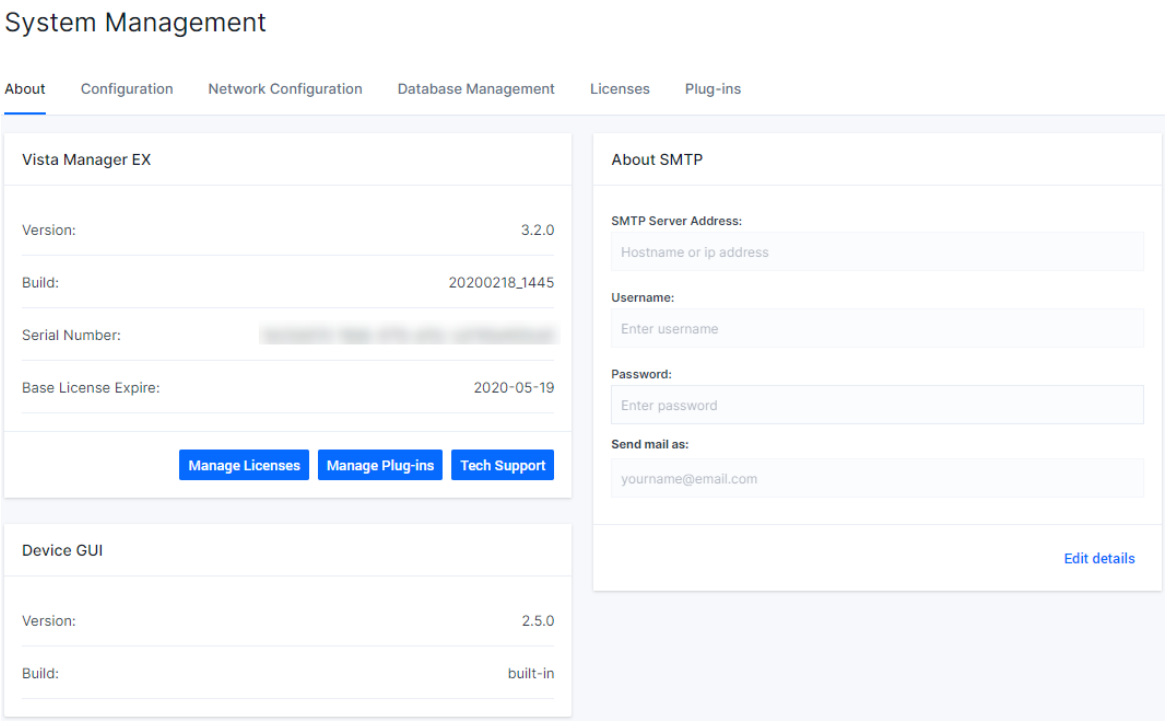
1. Log in with an Administrator account type
2. Select **User Management** from the menu
3. Select the account you want to delete from the account list
4. Click the **Delete** button
5. From the Delete User dialog box click the **Delete** button again

Note: The default Admin (Manager) account cannot be deleted.

Managing the Vista Manager EX system

The Vista Manager EX system itself can be managed:

- Licenses and Plug-ins can be displayed and updated
- The Username and Password can be changed for a network
- The Vista Manager EX database can be backed up, restored from backup, or reset to the factory default
- The SMTP Server Username, Password and email address can be changed

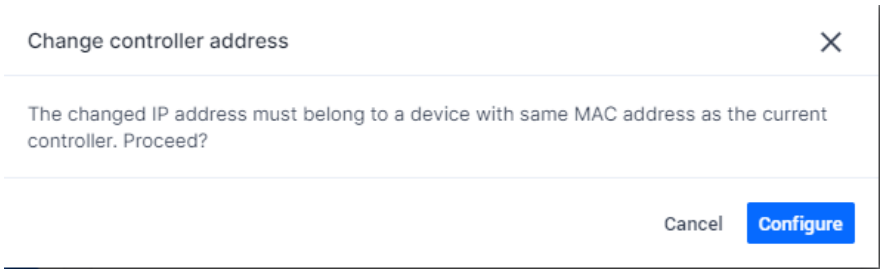


Changing the Vista Manager EX controller IP address

You may need to change the IP address of the Vista Manager EX controller in Vista Manager EX. For example, if the IP address of the controller has changed, this also needs to be changed in Vista Manager EX. To change the IP address:

1. Click on System Management, and select the Network Configuration tab.
2. Under AMF Network Configuration, click on the Edit button.

3. Click on the Change controller address button. Once you have confirmed that the changed IP address belongs to a device with the same MAC address as the current controller, click on the Configure button.



4. The **Upload Licence File** dialog will then be displayed. Select your license file, and click Next.
5. The **Set Up Your Network** dialog will then be displayed. You can change the IP address to the new address. Click Next.

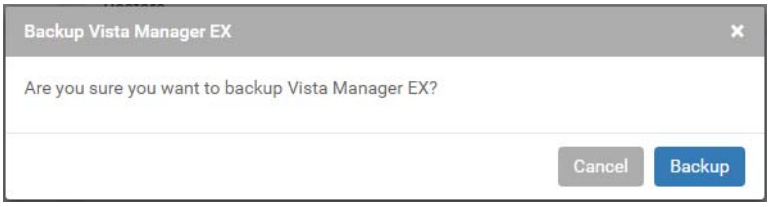
Note: The changed IP address must belong to a device with the same MAC address as the current controller.

6. The **Set Up Your SMTP settings** dialog will then be displayed. Click Proceed.

Note: This does not provide a method to change your controller to a new network. That requires a reinitialization of Vista Manager EX.

Backup Vista Manager EX

1. Click on System Management, and select the Database Management tab.
2. Click on the Backup button in the Backup Pane.
3. Click Backup again to confirm you wish to make a backup.



4. This automatically downloads a **tar** file backup to your default download location.
5. Keep this **tar** file in a safe location.

Note: Restoring Vista Manager backups from a newer version into an older version is not supported. It is not possible, for example, to restore a backup made in Vista Manager 3.2.0 into a Vista Manager 3.1.0 installation.

Using the SD-WAN Feature

Introduction

Software Defined WAN (SD-WAN) provides you with improved inter-branch network performance and reduced cost, by automatically optimizing application traffic over multiple VPN links between offices.

The SD-WAN orchestrator integrated into Vista Manager EX provides centralized management of your WAN infrastructure, and dynamically configures the firewall/router endpoints at each branch location. You can easily set acceptable performance metrics for any application, and load-balance traffic to meet requirements. By monitoring VPN link quality, time-sensitive or critical traffic is automatically switched over to the optimal link as required.

Visual monitoring enables easy management of the WAN, with the ability to drill down to specific VPN links or applications to assess live and historical operation.

For more information on SD-WAN, and details on instead configuring it via the CLI of individual firewall/router endpoints, refer to the SD-WAN Feature Overview and Configuration Guide.

Limitations

The initial implementation of SD-WAN in Vista Manager EX does not offer all the functionality available through the CLI. The following limitations apply.

- You cannot apply asymmetric rules between two devices using Vista Manager EX. This means you cannot specify different rules at each end of the same tunnel. This has further limitations when Vista Manager EX is configured on an existing network that already has SD-WAN rules defined. This behaviour is outlined in the “Rule Discovery” section.
- You cannot specify the exact values associated with a probe. Default values are set by the SD-WAN feature for:
  - IP Version (IPv4 or IPv6)
  - Interval (ms)
  - Packet size (bytes)
- You also cannot create groups, profiles, or linkmon probes directly. These are all handled automatically by Vista Manager EX.
- Rule Discovery
  - You cannot see a PBR rule in Vista Manager if it was created in the CLI.
  - You should not alter any SD-WAN rules in the CLI if you intend to use Vista Manager to maintain your SD-WAN rules.
  - A naming convention is applied to all SD-WAN configurations performed by Vista Manager. These configurations are prefixed with "VM_" and should never be altered via the CLI. This will cause unexpected behaviour in Vista Manager EX.

- Vista Manager EX only discovers rules from a device upon start-up, or the discovery of a new device. Any changes in the CLI will not be reflected in Vista Manager at run time.

- There are specific pre-configuration steps required to get SD-WAN working on Vista Manager. These are noted in the "Configuring devices for SD-WAN" section.
- The following tunnel types are supported:
  - ipv4 (ipsec)
  - ipv6 (ipsec)
- You cannot edit a tunnel name from Vista Manager EX. The configuration of tunnel names is described in the "Tunnel Names" section.
- No more than 500 rules can be configured on any one device. This is an existing AlliedWare Plus SD-WAN constraint on PBR rules.

Configuring devices for SD-WAN

The Vista Manager EX SD-WAN feature provides a GUI for you to set up your network. Before that can be done, the devices first need some initial configuration via the CLI.

Tunnel Setup

Vista Manager detects tunnels using an algorithm. Only tunnels that match that algorithm can be shown on the map. IP Sec tunnels must be pre-configured on the network as shown below.

```
interface tunnel10
   tunnel source
   tunnel destination
   tunnel local name
   tunnel remote name
   tunnel protection ipsec
   tunnel mode ipsec
   description <<<tunnel name>>>
```

STATUS	DESCRIPTION
`interface tunnel10`	This does not need to match the other end of the tunnel.
`tunnel source`	This must be either eth, subinterface, or PPP, or the IP of those. The API must return an IP address.
`tunnel destination`	This must match the source IP address of the other end of the tunnel. Where the destination is a domain, the API must return an IP address.
`tunnel local name`	Not used for tunnel matching logic.
`tunnel remote name`	Not used for tunnel matching logic.
`tunnel protection ipsec`	Must be present.
`tunnel mode ipsec`	Must be only this mode, and either ipv4 or ipv6. Must match the config of the other end of the tunnel.

STATUS	DESCRIPTION
`description <<<tunnel name>>>`	Optional. If description is not present, the VTI name is used (e.g. tunnel10).

Tunnel Names

If you want to set a custom tunnel name inside Vista Manager EX, you can specify the name in the description field of the interface. An example can be found above, or in the example configuration file below.

Routing

Routing must be set up and working before SD-WAN functionality will work in Vista Manager EX.

DPI Engine

When creating a rule, you have the ability to select an application to monitor. The application is determined using DPI on the device. The SD-WAN feature uses the enabled DPI Engine. If no DPI Engine is set, it will default to the built-in engine. DPI is not enabled for SD-WAN by default. You must pre-configure DPI on the device, or enable it via Traffic Monitoring in Vista Manager EX.

Note: If you have purchased a Procera license, it is strongly recommended that Procera is set as your DPI Engine, and enabled on all of your devices before running the SD-WAN feature.

Network time protocol

Network time protocol (NTP) is a protocol designed to synchronize the clocks of computers over a network. The objective of NTP is simple: to allow a client to synchronize its clock with Coordinated Universal Time (UTC), and to do so with a high degree of accuracy and stability.

To allow SD-WAN to work correctly, NTP should be running on the network so that all clocks are synchronized. For more information on NTP, refer to the Network Time Protocol (NTP) Feature Overview and Configuration Guide.

Configuration example

Below is an example of a configuration for a device that will be used in a Vista Manager EX SD-WAN network.

```
!
service password-encryption
!
hostname AR3050S-Master
!
no banner motd
!
username manager privilege 15 password 8 $1$bJoVec4D$JwOJGPr7YqoExA0GVasdE0
!
!
no service ssh
!
service telnet
!
service http
!
snmp-server
!
!

aaa authentication enable default local
aaa authentication login default local
!
!
atmf network-name SDWAN
atmf master
atmf area B id 2 local
atmf area B password 8 rnTNKv0fF4iHLJO+qhWojjIeSpzhx7FdZTOUyOPEtxE=
atmf area A id 1
atmf area A password 8 FtzApz+UFXW792nmEuo/TbLSxIuPYiQ8tbu8Mt4Z6a0=
atmf topology-gui enable
!
!
dpi
provider built-in ←DPI engine should be specified, otherwise Vista Manager will default to built-in
enable
!

crypto isakmp key 8 356oBeBg/eKTE/uhg5C5MayOdrVTlL4o0bB1kauVp9c= hostname
TUNNEL10
crypto isakmp key 8 2efK2dZ6h0EMVG7+8qfBEKIm73JX3UurzJ2+MVpiH7I= hostname
TUNNEL100
crypto isakmp key 8 jv6hbNiRdjwN0luRU/3KFkkKQ8Cq6XJ9+otnF+SahaA= hostname
TUNNEL1000
crypto isakmp key 8 wXyMxF5WzvFVc/BtCk5JatDonDQfLMct4pjnK+N5Lzk= hostname
TUNNEL11
crypto isakmp key 8 c/KHKV6pkaCDimGlrFqsTZBIdsZYNIh7UnlGC3cYaeA= hostname
TUNNEL2100
crypto isakmp key 8 Sg3MBtl8tCHZD9aPkwrqK5F/FBJiduj1NAFF/rFyknE= hostname
TUNNEL2101
!
!
!
!
ip domain-lookup
!
no service dhcp-server
!
no ip multicast-routing
!
spanning-tree mode rstp
!
tunnel security-reprocessing
no lacp global-passive-mode enable
!
```

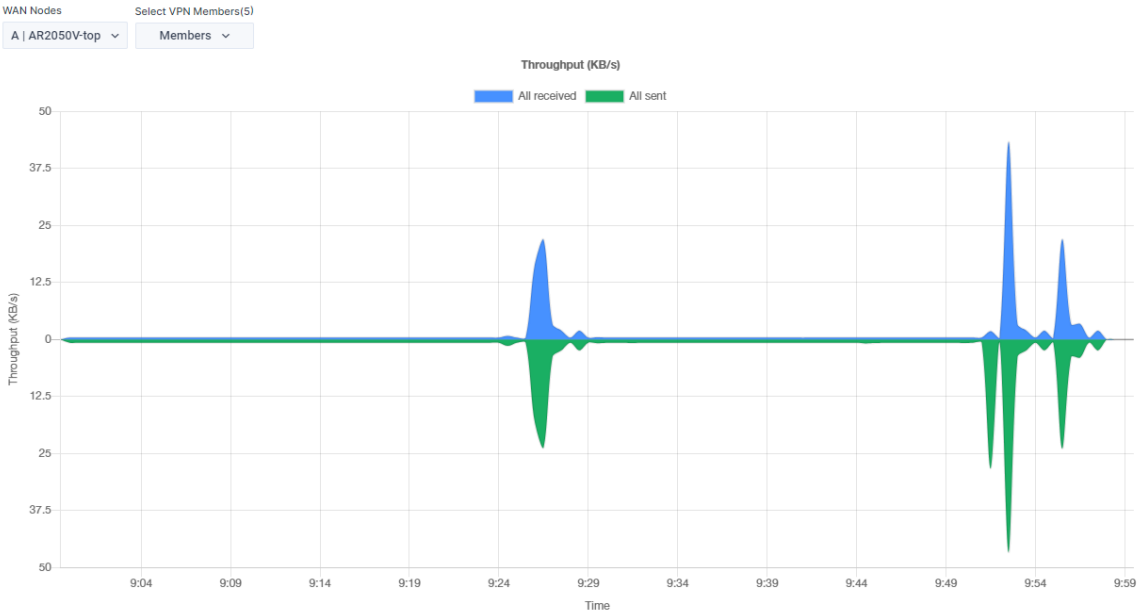
```
vlan database
vlan 4000 name testNet
vlan 4000 state enable
!
interface port1.0.1
switchport
switchport mode access
switchport access vlan 4000
!
interface port1.0.2-1.0.6
switchport
switchport mode access
!
interface port1.0.7
switchport
switchport mode trunk
switchport atmf-link
!

interface port1.0.8
switchport
switchport mode trunk
rmon collection history 4 buckets 10 interval 30 owner VISTA
switchport atmf-link
!
interface eth1
encapsulation dot1q 2
encapsulation dot1q 3
encapsulation dot1q 1000
!
interface eth1.1000
ipv6 address 2001:db9:1:1::2/64
!
interface eth1.3
ip address 11.0.5.1/30
!
interface eth1.2
ip address 11.0.4.1/30
!

interface eth2
encapsulation dot1q 100
!
interface eth2.100
ip address 12.0.100.1/30
!
interface mgmt
ip address 10.37.130.10/27
!
interface tunnel11 ←Ipsec tunnel interfaces must already be configured
tunnel source eth1.2
tunnel destination 11.0.2.1
tunnel local name TUNNEL11
tunnel remote name TUNNEL10
tunnel protection ipsec
tunnel mode ipsec ipv4
ip address 192.168.10.2/30
!
```

```
interface tunnel100
tunnel source eth1.3
tunnel destination 11.0.3.1
tunnel local name TUNNEL100
tunnel remote name TUNNEL100
tunnel protection ipsec
tunnel mode ipsec ipv4
ip address 192.168.100.2/30
!
interface tunnel1000
description <<<IPv6 Tunnel>>> ←Example tunnel name configuration
tunnel source eth1.1000
tunnel destination 2001:db9:2:1::2
tunnel local name TUNNEL1000
tunnel remote name TUNNEL1000
tunnel protection ipsec
tunnel mode ipsec ipv6
ipv6 address fd00:10::2/64
!

interface tunnel2100
tunnel source eth2.100
tunnel destination 12.0.100.2
tunnel local name TUNNEL2100
tunnel remote name TUNNEL2100
tunnel protection ipsec
tunnel mode ipsec ipv4
ip address 192.168.200.2/30
!
atmf virtual-link id 11 interface eth1.2 remote-id 10 remote-ip 11.0.2.1 remote-
area A
atmf virtual-link id 200 ip 12.0.100.1 remote-id 201 remote-ip 12.0.100.2
!
ipv6 forwarding
!

ip route 11.0.2.0/30 11.0.4.2 ←Routing must already be set up and working for SD-WAN features to
work
ip route 11.0.3.0/30 11.0.5.2
!
ipv6 route 2001:db9:2:1::/64 2001:db9:1:1::1
!
line con 0
exec-timeout 0 0
line vty 0 4
!
end
```

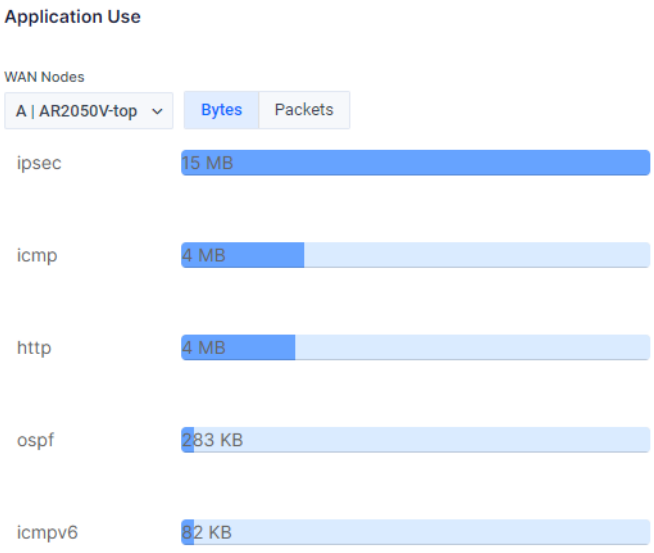
Dashboard

The SD-WAN dashboard provides you with an overview of the current state of your network. You can see throughput, a breakdown of application use, the state of rules that have been applied, and events in the network.

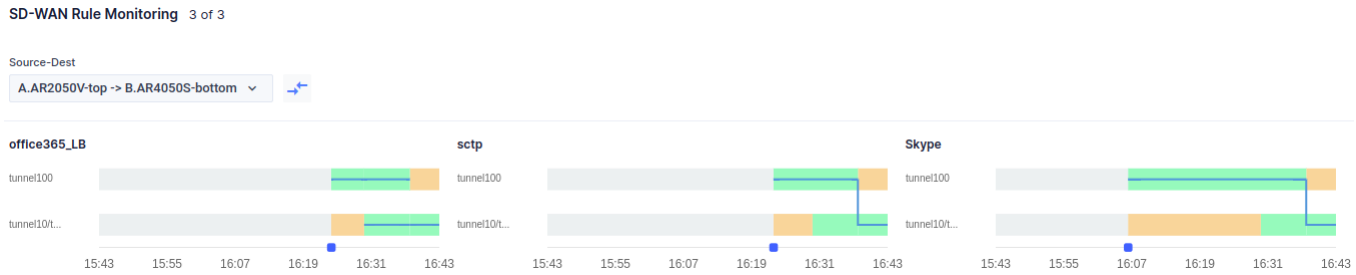
You can also choose the time-frame you wish to display; either the last 1 hour, the last 12 hours, the last 24 hours, or a custom range.



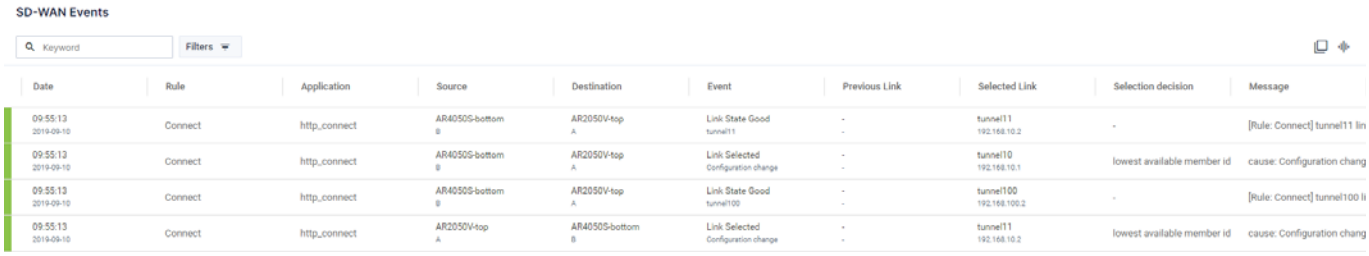
The throughput chart shows an overview of sent and received data for a node. You can select which node to view from the WAN Nodes drop-down. You can also choose which members to include from the Select VPN Members drop-down.



The application use chart shows the amount of data sent and received for a node, broken down by application.You can select which node to view from the WAN Nodes drop-down. You can also choose whether to view bytes or packets by choosing the appropriate toggle.



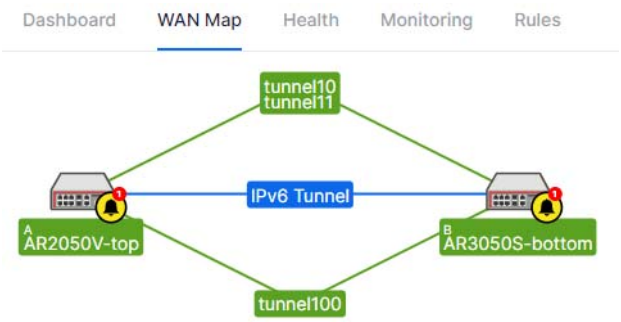
The rule monitoring chart shows the status of rules in your network. You can change which rules are shown from the Source-Destination drop-down.



The SD-WAN Events chart shows all of the events that have occurred. You can limit which events are shown by using a keyword to filter the results. Click on the Export as CSV button to export all values. Click on the Columns button to choose which columns are shown.

Topology map

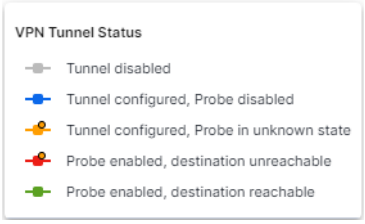
The SD-WAN topology map gives you a visual overview of your network.



You can see the state of all tunnels on the map. The state of each tunnel is indicated by the following colors:

- Grey with dashed line - Tunnel disabled or tunnel configuration incorrect
- Blue - Tunnel configured, probe disabled
- Orange - Tunnel configured, probe in unknown state
- Red - Probe enabled and tunnel destination is not reachable
- Green - Probe enabled and tunnel destination reachable

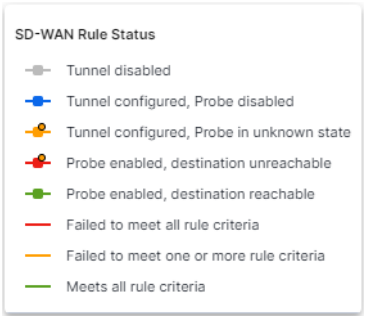
You can click on the Information button to bring up a key explaining each of the colors.



You can also see the health of SD-WAN rules on the map. The health of each rule is indicated by the following colors:

- Red - Failed to meet all rule criteria
- Orange - Failed to meet one or more rule criteria
- Green - Meets all rule criteria

As with the VPN Tunnel Status, you can click on the Information button to bring up a key explaining each of the colors.



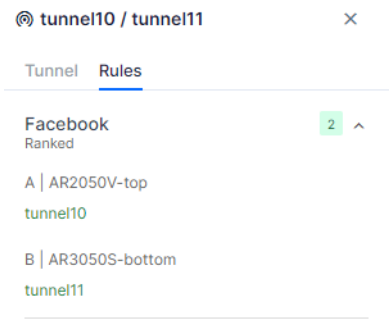
To change between showing the health of the tunnels or the rules, select either VPN Tunnels or Rules by clicking on the control in the top right corner.

When you click on a tunnel, the tunnel details are displayed in the side panel. The side panel shows the following information:

Tunnel details tab:

- Probe Status. You can use this slider to enable or disable a probe.
- Protection
- Mode
- Interface Name
- Source
- Source IP
- Destination

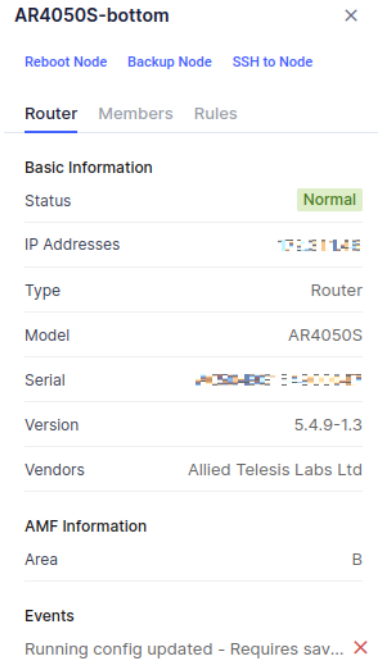
SD-WAN rules tab:



- Rule Name
- Rule Details

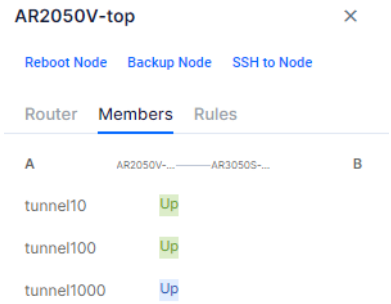
When you click on a router, the router details are displayed in the side panel. The side panel shows the following information:

Router details:



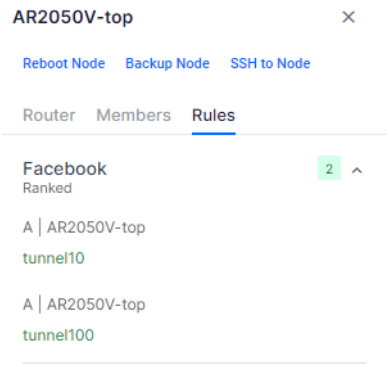
- Status
- IP Address
- Type
- Model
- Serial
- Version
- Vendors
- AMF Information

VPN members:



- SD-WAN rules associated with this router. The colours here represent the status of each tunnel as described above.

Rules:

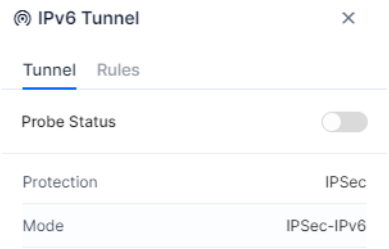


- Rule Name
- Rule Details

Linkmon probes

When a rule is created, any required probes will also be created and enabled. However, you can also create, enable, and disable probes from the SD-WAN map screen.

On the SD-WAN map, you can enable a probe for a specific link. To enable a probe, select the tunnel by clicking on it on the map. In the side panel, click on the Probe Status slider to enable the probe.



The Probe Status slider will then show the status as enabled.

The SD-WAN feature will create the probe and provide sensible default values for:

- IP Version (IPv4 or IPv6)
- Interval (ms)
- Packet size (bytes)

Probes that are created use ICMP by default, and this cannot be changed by a user.

You can disable a probe again by clicking on the Probe Status slider.

You can also use the SD-WAN map to see which links have probes enabled and disabled.

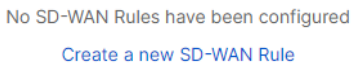
On the VPN-Members health screen, you can see a table of all VPN members in the network. You can also see which VPN Members have a probe enabled or disabled.

Note: If a probe has been configured by the CLI, it is not visible in the SD-WAN feature. It is recommended that you use the SD-WAN feature in Vista Manager EX to create the probes.

SD-WAN rules

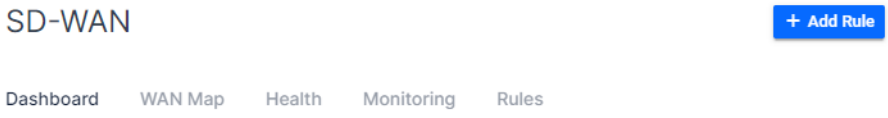
SD-WAN rules, also known as PBR (policy-based routing), allow your network to determine the best path for network traffic. SD-WAN uses metrics about the health of the link to decide if the link is “good” or “bad”. This allows traffic to be re-directed from a “bad” link to a “good” link, even if both links are still up. The metrics that SD-WAN can use to judge the health of a link are jitter, latency, and packet loss. Each metric is examined separately, so that a link that is “bad” for voice traffic due to high latency may still be “good” for bulk data due to low packet loss.

When there are no rules configured, you will see the following message on the SD-WAN rules landing page:

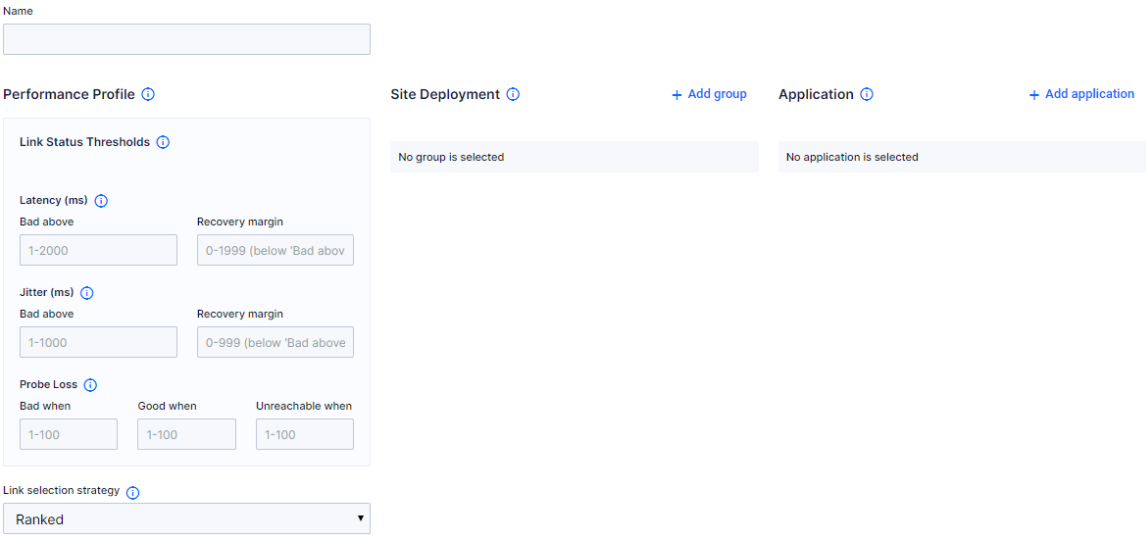


Click on the **Create a new SD-WAN Rule** link to create your first rule.

If you already have SD-WAN rules configured, you can create a new rule by clicking on the Add Rule button.

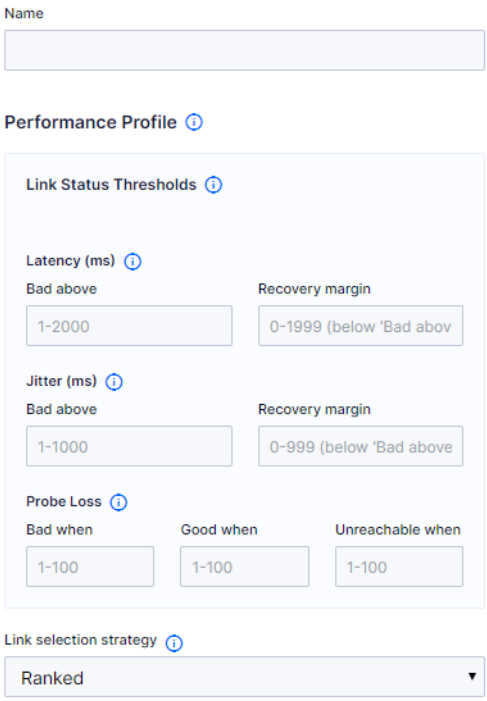


You will then see the Application Rule screen.



The Name field allows you to specify a name for your new rule.

The Performance Profile is made of two parts. The Link Status Thresholds are used to determine each link's status (good/bad/unreachable). The Link Selection Strategy is used when any selected link moves from good to bad status. The Link Selection Strategy is used to pick the new selected link to use.



Link status thresholds

Each link in a rule has a set of metrics collected for it using probes. When these metrics for a particular link break or move back within the Link Status Thresholds, the status of that link changes between bad/good/unreachable.

Each row in Link Status Thresholds sets thresholds for a particular metric. At least one row needs to be configured. The rows configured are independent of the Link Selection Strategy.

A link must be within all three thresholds to be considered good. If a link is breaking at least one of the three thresholds it is considered bad.

Latency

- Bad above - If a link's latency increases past this threshold then the link's status becomes bad.
- Recovery margin - A bad link will be considered good again (at least in terms of latency) once latency has reduced below the 'Bad Above' threshold by this amount.

Jitter

- Bad above - If a link's jitter increases past this threshold then the link's status becomes bad.
- Recovery margin - A bad link will be considered good again (at least in terms of jitter) once jitter has reduced below the 'Bad Above' threshold by this amount.

Probe loss

- Bad when - A link will be considered bad (at least in terms of probe loss) if this many probes are lost in succession.
- Good when - A bad link will be considered good again (at least in terms of probe loss) once this many probes are successful.
- Unreachable when - A link will be considered unreachable if this many probes are lost in succession.

Link selection strategy

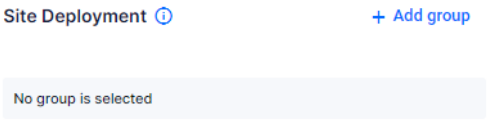
For each group of links, a rule is applied so there will always be a selected link (when not load-balanced). This selected link is the link that all traffic for that rule is directed through. If that selected link's metrics breaks one or more thresholds (configured by link status thresholds), then the Link Selection Strategy is used to determine the new selected link.

Regardless of Link Selection Strategy, links within threshold are always preferred over links breaking one or more thresholds.

Selection Strategies

- Latency - the link with the lowest latency is picked.
- Jitter - the link with the lowest jitter is picked.
- Probe Loss - the link with least current consecutive probe loss is selected.
- Ranked - the link highest in the groups list is selected.
- Combined - takes latency, jitter, and probe loss metrics into account to determine a single combined score. The link with the best (lowest) score is selected.

Site deployment

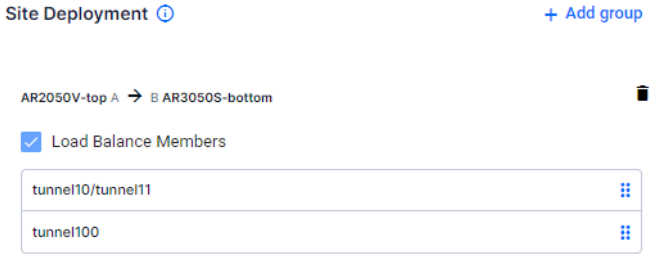


Links picked to make up the groups for a rule determine where the rule will be deployed. Between each router pair selected, two identical instances of the rule will be deployed, one on each of the routers.

Even though a 'source' and 'destination' router are selected, the rules are deployed identically on each router pairing.

Selecting a router pairing as Load Balanced means that when there are more than one link with a status of good (status determined by Link Status Thresholds) then traffic flows will proceed evenly over all those good links. If all links have gone bad then the Link Selection Strategy is used to pick one link for the traffic to use.

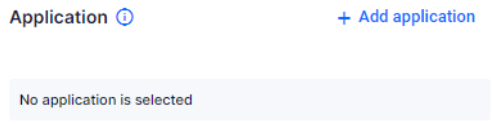
Within each router pair, links can be moved to have a higher or lower ranking within the group. This ranking is solely used for the Link Selection Strategy of 'Ranked'.



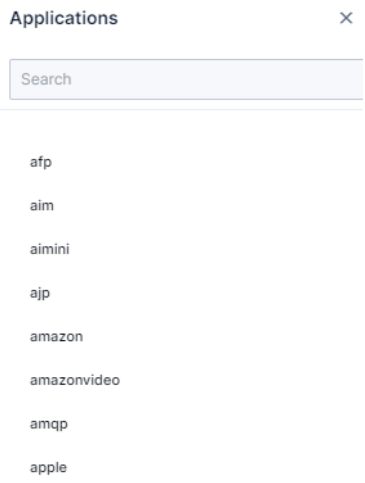
When selecting a VPN member, you will be notified how many more rules can be created on the device. Remaining rule spaces are calculated by taking the highest rule ID and subtracting it from 500. When there are 0 rules available, you cannot select the member as a source or destination.

When selecting a VPN member, you can only select links between a source and destination node that have the same IP Version. If you select a link of type IPV6, then an IPV4 link cannot be selected in the same rule. Likewise, if you select a link of type IPV4, then an IPV6 link cannot be selected in the same rule. You will see a warning message if you attempt to select links that do not match.

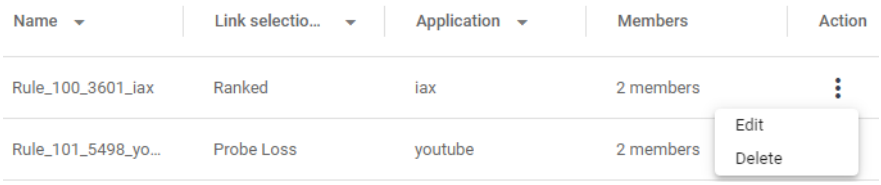
Application



The application list is provided by the active DPI engine. If there is no active DPI engine, then SD-WAN will enable the built-in DPI engine by default.



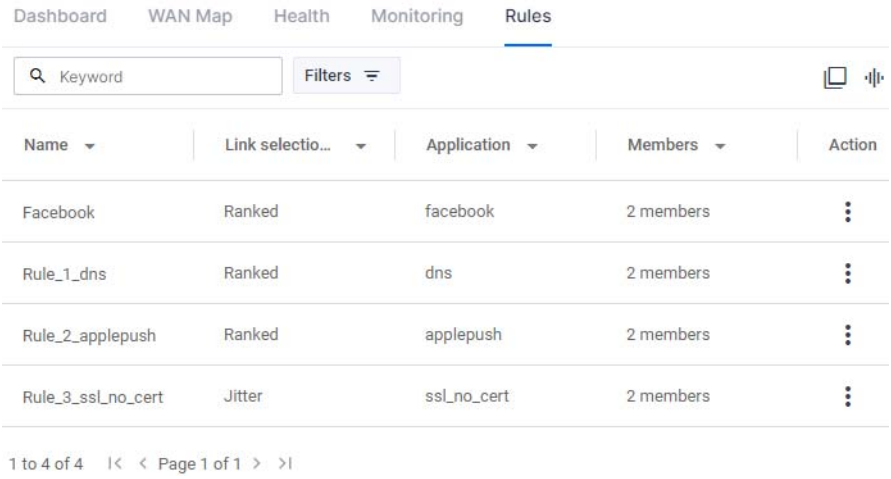
Editing and deleting an SD-WAN rule



To edit an SD-WAN rule, click on the Action drop-down, and select Edit. This will take you to the Application Rule screen for that rule.

To delete an SD-WAN rule, click on the Action drop-down, and select Delete. This will prompt you whether you want to delete the rule, and clicking on Delete will remove it.

Managing SD-WAN rules in Vista Manager



You can see a table of the existing rules by clicking on the Rules tab.

Rules that have been configured using the CLI will not be visible in Vista Manager. If a rule was configured by Vista Manager, and then is altered via the CLI, the changes made in the CLI will not be visible inside Vista Manager. Therefore, you should not alter rules created in Vista Manager from the CLI.

The table of existing rules contains link state history. History information is polled and stored, so may be up to one minute out-of-date in the rule table.

Rule Discovery

If the Vista Manager database is reset or initialized, the SD-WAN configuration will be read from each router in the network. The naming convention used by Vista Manager will be used to retrieve this information.

When the Vista Manager server is started, or when a new router is added to the network, the SD-WAN configuration will be read from the device and compared with the current database state. If there is a mis-match, then an event will be generated in Vista Manager to tell the user that the

configuration of the device is not compatible with Vista Manager's SD-WAN feature. The event log entry will be created when:

- Any rule configuration parameter differs between the Vista Manager database and the device.
- Any profile configuration parameter differs between the Vista Manager database and the device.
- Any group configuration information differs between the Vista Manager database and the device.
- Any probe configuration parameter differs between the Vista Manager database and the device.
- A rule on a device does not have an equivalent rule on another device, to maintain Vista Manager's rule of symmetry.

When Vista Manager detects a configuration mismatch, it will generate one event for the device that has the mismatch:

SD-WAN configuration on the device does not match Vista Manager.

When Vista Manager detects a configuration mismatch, a notification will be displayed on the rule configuration table. The user will have the option to:

- Fix the rule using the **Reconcile** action, or
- Delete and recreate the rule.

User permissions for rules

- A user can only create or edit a rule if they have read/write permissions for all routers specified in that rule.
- If a user has at least read-only permissions to one router in a rule, then they are able to view the rule configuration.
- If a router in a rule is down, the user cannot edit that rule. They can press delete for the rule, but this will only do a partial delete. This will only remove it from the online routers in the rule. They will be warned that the rule cannot be deleted from the routers that are offline. The rule containing the offline routers will remain in the configured rules table.

Health

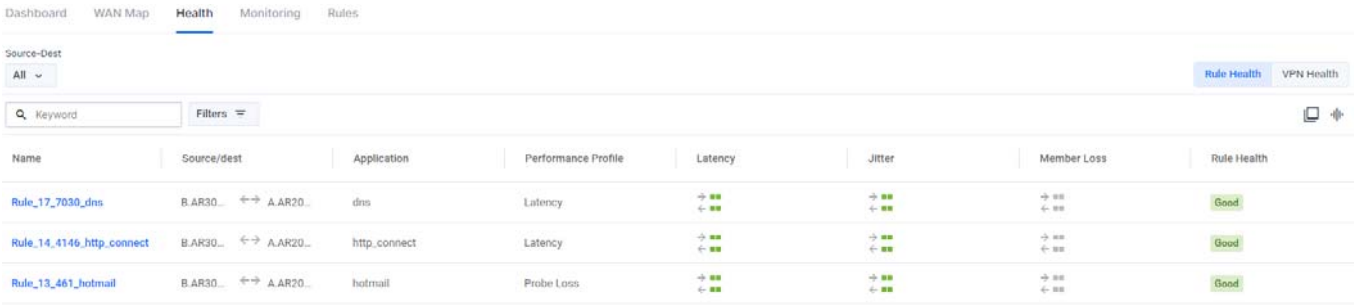
The health tab gives you an overview of the current health of your network in a single location.

The Source-Destination drop-down allows you to select a specific router, or show all routers. You can also limit which rules are shown by using a keyword to filter the results.

Click on the Export as CSV button to export all values. Click on the Columns button to choose which columns are shown.

Clicking on the toggle allows you to change the view between Rule Health and VPN Health.

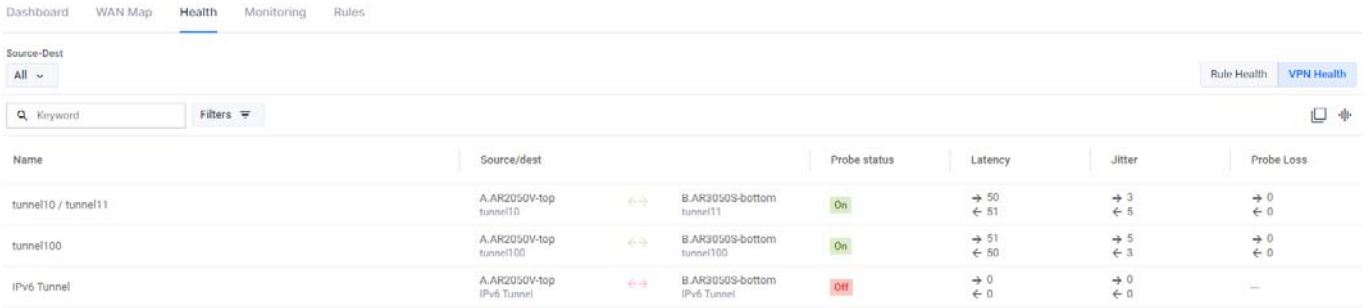
Rule health



The rule health tab shows a summary of the state of all the rules in the network. You can click on a specific rule to see more information about that rule:

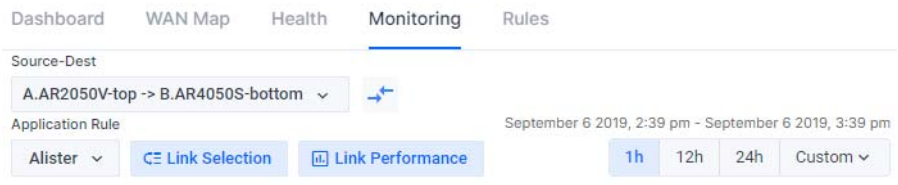
- the rule settings
- the rule status
- the current settings for:
  - latency
  - jitter
  - probe loss

VPN health



The VPN health tab shows a summary of the state of all the VPNs in the network.

Monitoring



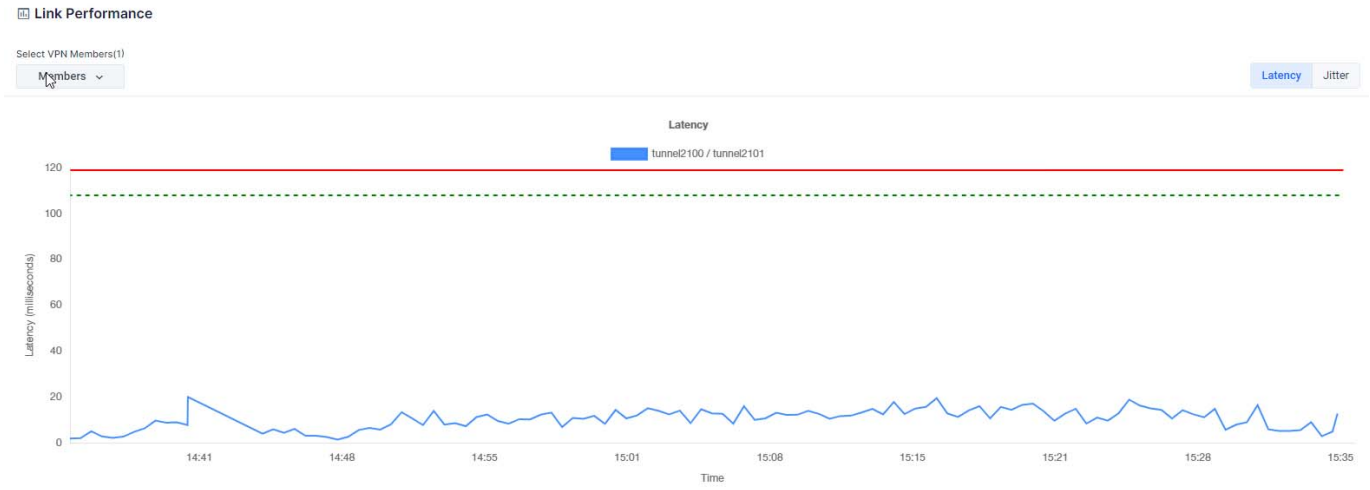
The monitoring tab displays historic link and rule information. Vista Manager EX allows you to view up to 7 days of historic data.

The Source-Destination drop-down allows you to select a specific router, or show all routers. The Application Rule drop-down lets you select which rule to show. You can also choose the time-frame you wish to display; either the last 1 hour, the last 12 hours, the last 24 hours, or a custom range.

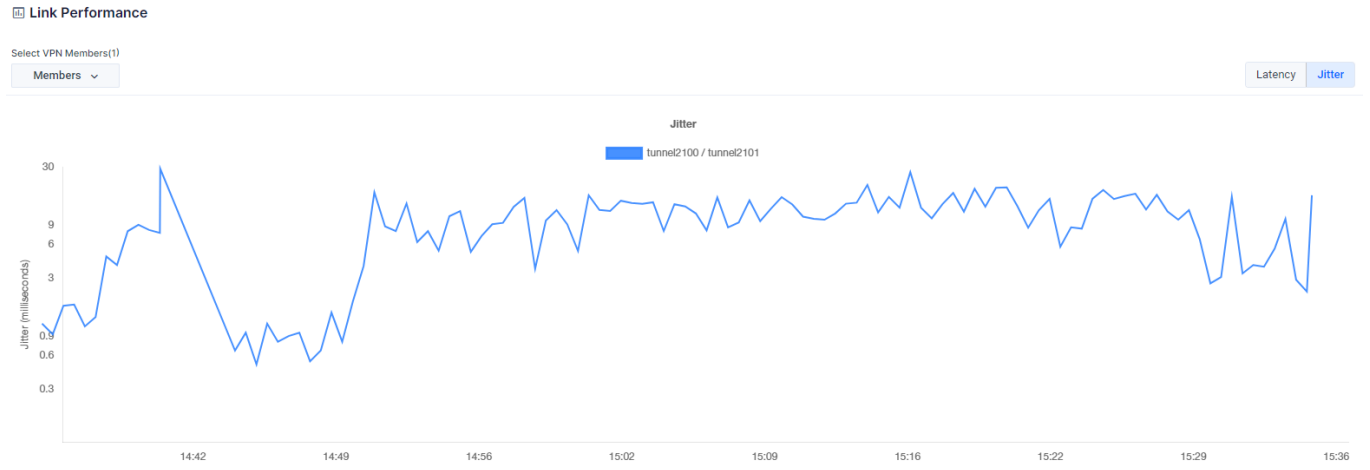
You can toggle which charts are shown. The Performance Routing Events chart is always available. The Link Selection Path and Link Performance charts are only available after a source and destination have been selected.

The Link Selection Path chart shows a time-line of which link is being used for the selected rule. You can see which link selection strategy is being used, and the history of which link has been chosen.

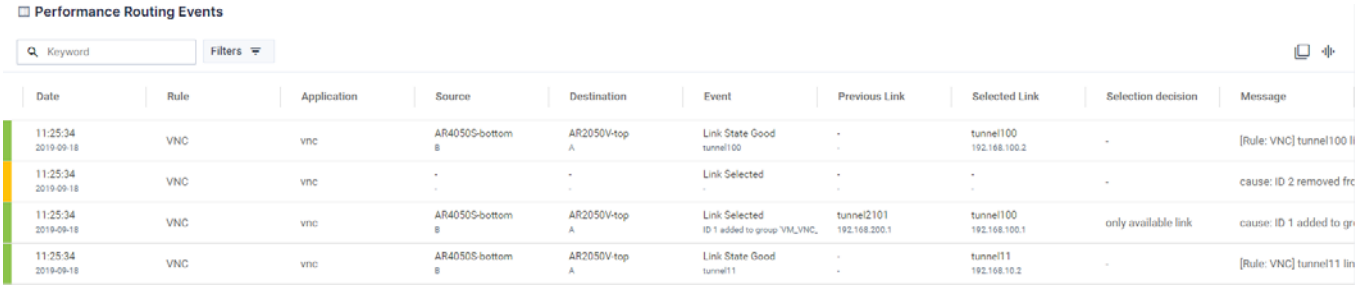
The Link Performance charts show the performance history of a link for either latency or jitter. You can select which member you would like to see from the Members drop-down, or select multiple members to compare them.



The latency chart shows the history of the latency for the link. It also shows the good-below (green line) and bad-above (red line) thresholds for the link if they have been configured.



The jitter chart shows the amount of jitter for the link.

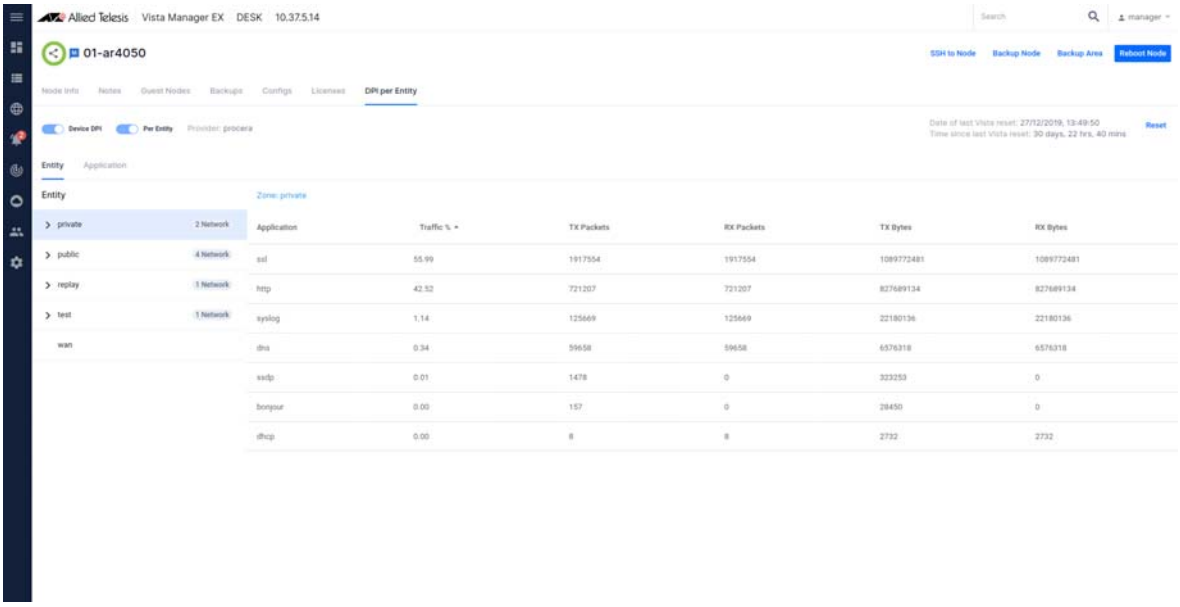


The Performance Routing Events chart shows all of the events that have occurred. You can limit which events are shown by using a keyword to filter the results. Click on the Export as CSV button to export all values. Click on the Columns button to choose which columns are shown.

User permissions

A user must have read permissions to at least one router in a router pair in order to view rule information for that router pair. This applies to both viewing rule configuration, and viewing the historic link selection path. A user can only see events in the SD-WAN Routing Events table when they have at least read permissions on the source router for that event.

DPI statistics



You can view DPI statistics for each entity for SD-WAN. To view the DPI statistics, navigate to Asset Management and click on a device. On the row of tabs, to the right of Licenses, click DPI per Entity. If Device DPI and Per Entity aren't already toggled on, click each of them to toggle them on.

Clicking on each entity on the left will show the stats, sorted by the highest % of traffic at the top. Clicking on a column sorts by that field. Clicking the > arrow to the left of the entity name will show the networks inside. If there's an arrow to the left of the network name, you can drill down to see each host. By clicking the Application tab, you can click on a particular application to see their stats. In the table, you can click on the zone to see the stats for networks, and drill down into a network and into hosts.

Troubleshooting

Ports and URLs used by Vista Manager EX

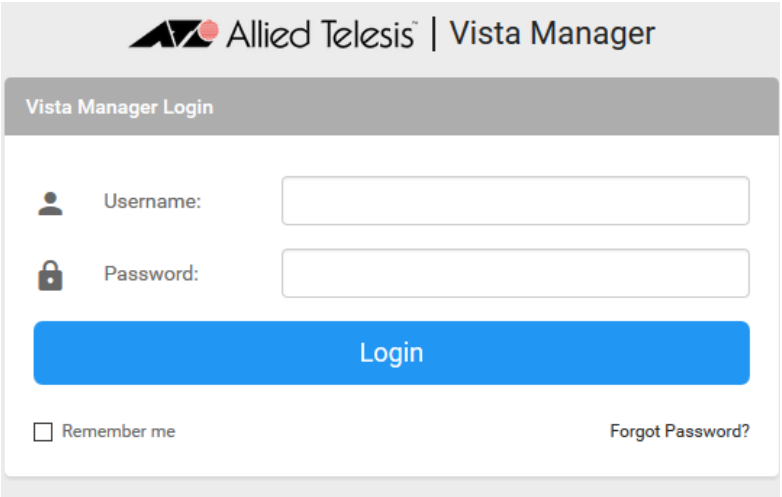
You can use these settings to check that Vista Manager and the plug-ins are installed correctly.

1. After installation, Vista Manager EX, and the plug-ins, will be installed on the following ports.

Vista Manager	Port 5000
AT-AWC	Port 5443
AT-SNMP	Port 6443

2. You can test that Vista Manager is working correctly by using the following URL:

   - http://localhost:5000



3. You can test whether the plug-in APIs are active using the following URLs:

   - https://localhost:5443/wireless_plugin/api/plugin_registration

{"version":"100","baseUrl":"http:\/\/localhost:8080\/wireless_plugin\/api","product":{"name":"AT-Vista Mana
plugin","type":"awc","version":{"major":"1","minor":"2","revision":"0","build":"B06"},"capabilities":["node

   - https://localhost:6443/netmanager/api/plugin_registration

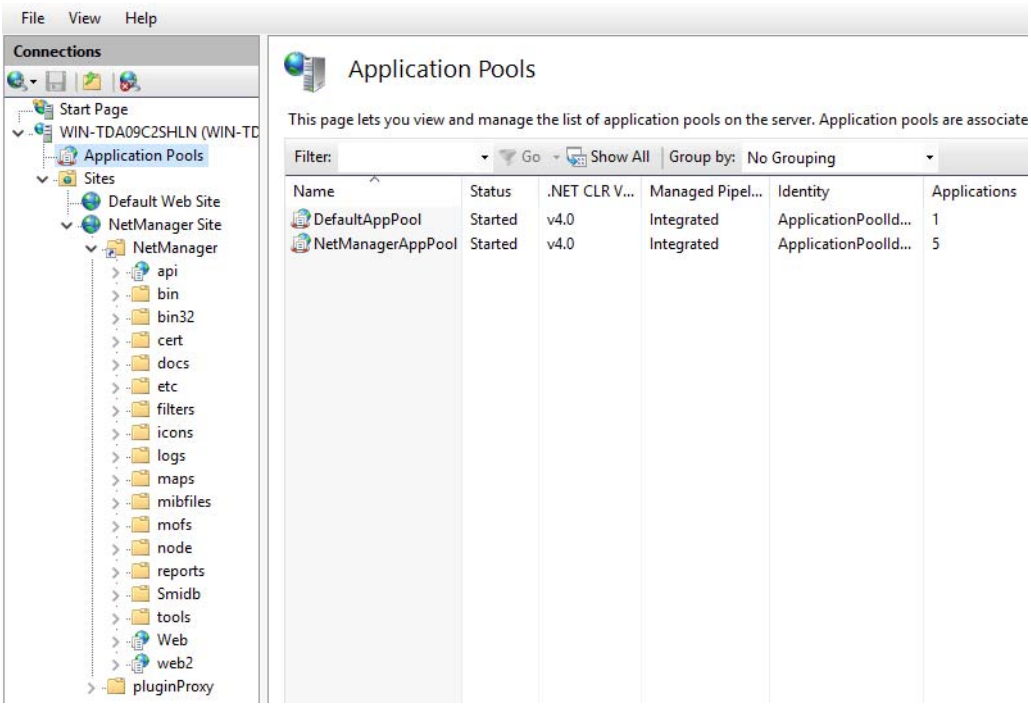
{"version":"1.0.0","baseUrl":"http://10.33.24.38/NetManager/api","product":{"name":"SNMP Plugin","type":"ann
{"major":1,"minor":0,"revision":0,"build":"B04"},"capabilities":["menu","event"]}}

Note: These URLs can only be used locally on the Vista Manager server using “localhost”.

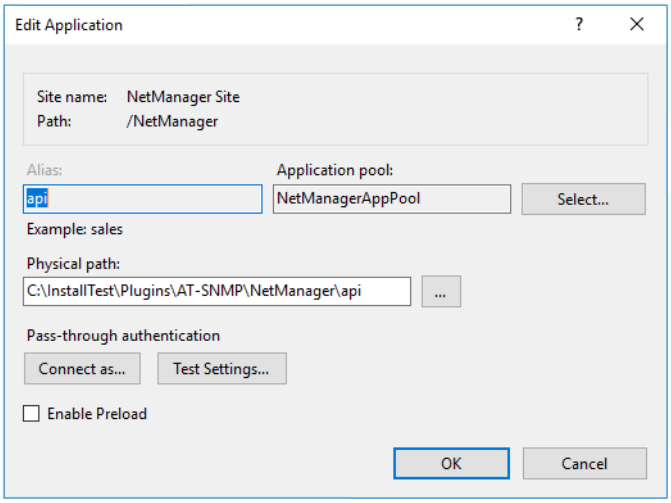
SNMP plug-in application pool settings

If you are having issues with the SNMP plug-in, you can check the IIS settings are correct.

1. Launch **Internet Information Services (IIS) Manager** on the Vista Manager EX server.
2. Expand out the following items in the Connections pane tree on the left-hand side:
   Computer name -> Sites -> NetManager Site -> NetManager
3. Make sure that the **api** and **web2** applications are available, and configured, as per the following screenshots.

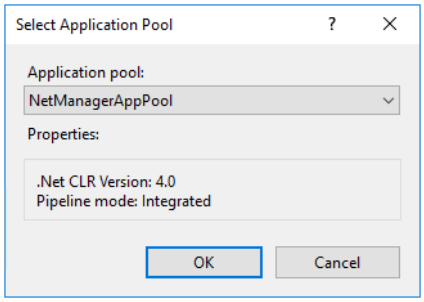


4. Select **api** in the Connections pane and then select Basic Settings in the Actions pane.

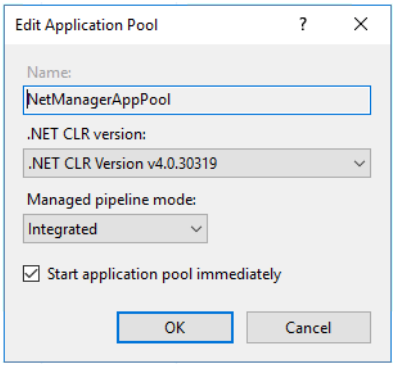


5. Click the select button and check that the Select Application Pool settings have the following properties:

   - .Net CLR version: 4.0
   - Pipeline mode: integration



6. Repeat for the **web** application.
7. If the **NetManagerAppPool** does not have the required properties, then select Application Pool in the Connections pane.
8. Select **NetManagerAppPool** from the Application Pools screen and select Basic Settings from the Edit Application Pool pane.
9. The application pool settings should look like the following:



Note: The “xxxxx” portion of the **.Net CLR Version v4.0.xxxxx** version will vary depending on the Windows OS installed.

Supported Device List

AlliedWare Plus devices

The following table lists the AlliedWare Plus devices supported by Vista Manager EX 3.3.1.

We recommend you run the most recent AlliedWare Plus version available for your device. The new features for version 3.3.1 are only available on devices running AlliedWare Plus version 5.4.9-2.3 or later.

Table 1: AlliedWare Plus devices supported by Vista Manager EX 3.3.1

Models	Family
AMF Cloud	
AR2050V AR2010V AR1050V	AR-series VPN routers
AR4050S AR3050S	AR-series UTM firewalls
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28DP FS980M/28PS FS980M/52 FS980M/52PS	FS980M
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX
GS970M/10 GS970M/18 GS970M/28	GS970M
GS980M/52 GS980M/52PS	GS980M
GS980EM/10GH	GS980EM
GS980MX/10HSm	GS980MX
IE200-6GP IE200-6GT	IE200
IE210L-10GP IE210L-18GP	IE210L
IE340-12GP IE340-12GT	IE340
IE340-20GP	IE340
IE340L-18GP	IE340L
IX5-28GPX	IX5
SBx81CFC400 SBx81CFC960 SBx81CFC960 v2	SBx8100

Table 1: AlliedWare Plus devices supported by Vista Manager EX 3.3.1

Models	Family
SBx908 GEN2	SBx908 GEN2
x220-28GS x220-52GP x220-52GT	x220
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230-52GP x230-52GT x230L-17GT x230L-26GT	x230
x310-26FT x310-50FT x310-26FP x310-50FP	x310
x320-10GH	x320
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510
x530-28GPXm x530-28GTXm x530-52GPXm x530-52GTXm x530L-10GHXm x530L-28GPX x530L-28GTX x530L-52GPX x530L-52GTX	x530
x550-18SXQ x550-18XTQ x550-18XSPQm	x550
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930
x950-28XSQ x950-28XTQm x950-52XSQ	x950
XS916MXS XS916MXT	XS900MX

Allied Telesis Wireless APs

The following table lists the Allied Telesis wireless APs, and the firmware versions, supported by Vista Manager EX 3.3.1.

Table 2: Allied Telesis wireless APs supported by Vista Manager EX 3.3.1

Models	Supported
AT-TQ2450	4.3.x[1]
AT-TQ3200	4.3.x[1]
AT-TQ3400	4.3.x[1]
AT-TQ3600	4.3.x[1]
AT-TQ4400	4.3.x[1]
AT-TQ4400e	4.3.x[1]
AT-TQ4600	4.3.x[1]
AT-TQ4400 (SDN version)	4.1.1-S05[1]
AT-TQ4600 (SDN version)	4.1.1-S05[1]
AT-TQ1402	6.0.0-0.x[2]
AT-TQ1402m	6.0.0-0.x[2]
AT-TQ5403	5.4.x, 5.3.x[2]
AT-TQ5403e	5.4.x, 5.3.x[2]
AT-TQm5403	5.4.x, 5.3.x[2]

Notes:

[1] The latest features added in this version of Vista Manager EX and the AWC plug-in are not supported. Management by the AWC plug-in and output of the AWC calculation result are supported.

[2] Support for some of the latest AWC features will be in the next software version, which is coming soon.

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

© 2020 Allied Telesis, Inc. All rights reserved. Information in this document is subject to change without notice. All company names, logos, and product designs that are trademarks or registered trademarks are the property of their respective owners.